Entanglement breaking rank

Jitendra Prakash
Department of Pure Mathematics and Institute for Quantum Computing
University of Waterloo

Based on arXiv:1805.04583
(With Vern I. Paulsen, Mizanur Rahaman, Satish Pandey)

June 15, 2018
The 11th Annual Ottawa Conference in Mathematics

Outline

1. Two conjectures

Outline

1. Two conjectures
2. What is a quantum channel?

Outline

1. Two conjectures
2. What is a quantum channel?
3. What is separability and entanglement?

Outline

1. Two conjectures
2. What is a quantum channel?
3. What is separability and entanglement?
4. Entanglement breaking channels

Outline

1. Two conjectures
2. What is a quantum channel?
3. What is separability and entanglement?
4. Entanglement breaking channels
5. The conjectures and a particular entanglement breaking channel

Outline

1. Two conjectures
2. What is a quantum channel?
3. What is separability and entanglement?
4. Entanglement breaking channels
5. The conjectures and a particular entanglement breaking channel
6. Other directions

Two conjectures

Two conjectures

Conjecture (Zauner)

For each $d \geq 2$*, there exist* d^2 *unit vectors* $\{v_i\}_{i=1}^{d^2}$ *in* $\mathbb{C}^d$ *such that*

$$|\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}, \qquad \textit{for all } i \neq j.$$

Two conjectures

Conjecture (Zauner)

For each $d \geq 2$, there exist d^2 unit vectors $\{v_i\}_{i=1}^{d^2}$ in $\mathbb{C}^d$ such that

$$|\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}, \qquad \text{for all } i \neq j.$$

Definition (Mutually unbiased bases)

Two orthonormal bases $\{e_1, ..., e_d\}$ and $\{f_1, ..., f_d\}$ of $\mathbb{C}^d$ are called *mutually unbiased* if

$$|\langle e_i, f_j \rangle|^2 = \frac{1}{d}, \qquad \text{for all } 1 \leq i, j \leq d.$$

Two conjectures

Conjecture (Zauner)

For each $d \geq 2$, *there exist* d^2 *unit vectors* $\{v_i\}_{i=1}^{d^2}$ *in* $\mathbb{C}^d$ *such that*

$$|\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}, \qquad \text{for all } i \neq j.$$

Definition (Mutually unbiased bases)

Two orthonormal bases $\{e_1, ..., e_d\}$ and $\{f_1, ..., f_d\}$ of $\mathbb{C}^d$ are called *mutually unbiased* if

$$|\langle e_i, f_j \rangle|^2 = \frac{1}{d}, \qquad \text{for all } 1 \leq i, j \leq d.$$

Conjecture (MUB)

For each $d \geq 2$, *there exist* $d+1$ *mutually unbiases bases in* $\mathbb{C}^d$.

Status

Status

- Zauner's conjecture:

Status

- Zauner's conjecture: known to hold in finitely many dimensions;

Status

- Zauner's conjecture: known to hold in finitely many dimensions; for high dimensions numerical evidence is present.

Status

- Zauner's conjecture: known to hold in finitely many dimensions; for high dimensions numerical evidence is present.
- MUB conjecture:

Status

- Zauner's conjecture: known to hold in finitely many dimensions; for high dimensions numerical evidence is present.
- MUB conjecture: known to hold in infinitely many dimensions, $d = p^n$ where p is prime and $n \in \mathbb{N}$;

Status

- Zauner's conjecture: known to hold in finitely many dimensions; for high dimensions numerical evidence is present.
- MUB conjecture: known to hold in infinitely many dimensions, $d = p^n$ where p is prime and $n \in \mathbb{N}$; not known whether it holds in dimension 6.

Status

- Zauner's conjecture: known to hold in finitely many dimensions; for high dimensions numerical evidence is present.
- MUB conjecture: known to hold in infinitely many dimensions, $d = p^n$ where p is prime and $n \in \mathbb{N}$; not known whether it holds in dimension 6.
- Both have important applications in quantum information theory, for example, in quantum cryptography and quantum tomography.

Quantum channels

Quantum channels

- $\mathbb{M}_d$ - space of all $d \times d$ complex matrices.

Quantum channels

- $\mathbb{M}_d$ - space of all $d \times d$ complex matrices.
- $P \in \mathbb{M}_d$ is *positive semi-definite* if $\langle P\xi, \xi \rangle \geq 0$ for all $\xi \in \mathbb{C}^d$.

Quantum channels

- $\mathbb{M}_d$ - space of all $d \times d$ complex matrices.
- $P \in \mathbb{M}_d$ is *positive semi-definite* if $\langle P\xi, \xi \rangle \geq 0$ for all $\xi \in \mathbb{C}^d$.
- Tensor product of two matrices $P, Q \in \mathbb{M}_d$ is

$$P \otimes Q = \begin{bmatrix} p_{1,1}Q & \dots & p_{1,d}Q \\ \vdots & \ddots & \vdots \\ p_{d,1}Q & \dots & p_{d,d}Q \end{bmatrix} \in \mathbb{M}_d \otimes \mathbb{M}_d \cong \mathbb{M}_{d^2}.$$

Quantum channels

- $\mathbb{M}_d$ - space of all $d \times d$ complex matrices.
- $P \in \mathbb{M}_d$ is *positive semi-definite* if $\langle P\xi, \xi \rangle \geq 0$ for all $\xi \in \mathbb{C}^d$.
- Tensor product of two matrices $P, Q \in \mathbb{M}_d$ is

$$P \otimes Q = \begin{bmatrix} p_{1,1}Q & \dots & p_{1,d}Q \\ \vdots & \ddots & \vdots \\ p_{d,1}Q & \dots & p_{d,d}Q \end{bmatrix} \in \mathbb{M}_d \otimes \mathbb{M}_d \cong \mathbb{M}_{d^2}.$$

Definition (Quantum channel)

A linear map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is called a *quantum channel* if it is

(a) *completely positive*: the *Choi matrix*

Quantum channels

- $\mathbb{M}_d$ - space of all $d \times d$ complex matrices.
- $P \in \mathbb{M}_d$ is *positive semi-definite* if $\langle P\xi, \xi \rangle \geq 0$ for all $\xi \in \mathbb{C}^d$.
- Tensor product of two matrices $P, Q \in \mathbb{M}_d$ is

$$P \otimes Q = \begin{bmatrix} p_{1,1}Q & \dots & p_{1,d}Q \\ \vdots & \ddots & \vdots \\ p_{d,1}Q & \dots & p_{d,d}Q \end{bmatrix} \in \mathbb{M}_d \otimes \mathbb{M}_d \cong \mathbb{M}_{d^2}.$$

Definition (Quantum channel)

A linear map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is called a *quantum channel* if it is

(a) *completely positive*: the *Choi matrix*

$$C_\Phi := \begin{bmatrix} \Phi(E_{1,1}) & \dots & \Phi(E_{1,d}) \\ \vdots & \ddots & \vdots \\ \Phi(E_{d,1}) & \dots & \Phi(E_{d,d}) \end{bmatrix} \in M_d(\mathbb{M}_d) \cong \mathbb{M}_d \otimes \mathbb{M}_d.$$

is positive semi-definite.

Quantum channels

- $\mathbb{M}_d$ - space of all $d \times d$ complex matrices.
- $P \in \mathbb{M}_d$ is *positive semi-definite* if $\langle P\xi, \xi \rangle \geq 0$ for all $\xi \in \mathbb{C}^d$.
- Tensor product of two matrices $P, Q \in \mathbb{M}_d$ is

$$P \otimes Q = \begin{bmatrix} p_{1,1}Q & \dots & p_{1,d}Q \\ \vdots & \ddots & \vdots \\ p_{d,1}Q & \dots & p_{d,d}Q \end{bmatrix} \in \mathbb{M}_d \otimes \mathbb{M}_d \cong \mathbb{M}_{d^2}.$$

Definition (Quantum channel)

A linear map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is called a *quantum channel* if it is

(a) *completely positive*: the *Choi matrix*

$$C_\Phi := \begin{bmatrix} \Phi(E_{1,1}) & \dots & \Phi(E_{1,d}) \\ \vdots & \ddots & \vdots \\ \Phi(E_{d,1}) & \dots & \Phi(E_{d,d}) \end{bmatrix} \in M_d(\mathbb{M}_d) \cong \mathbb{M}_d \otimes \mathbb{M}_d.$$

is positive semi-definite.

(b) *trace preserving*: $\mathrm{Tr}(\Phi(X)) = \mathrm{Tr}(X)$, for all $X \in \mathbb{M}_d$.

Quantum channels (cotd.)

Theorem (Choi (1975))

A linear map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ *is a quantum channel if and only if*

Quantum channels (cotd.)

Theorem (Choi (1975))

A linear map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ *is a quantum channel if and only if* Φ *has a Choi-Kraus representation:*

$$\Phi(X) = \sum_{k=1}^{K} B_k X B_k^*, \quad X \in \mathbb{M}_d,$$

Quantum channels (cotd.)

Theorem (Choi (1975))

A linear map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ *is a quantum channel if and only if* Φ *has a Choi-Kraus representation:*

$$\Phi(X) = \sum_{k=1}^{K} B_k X B_k^*, \quad X \in \mathbb{M}_d,$$

with $\sum_{k=1}^{K} B_k^* B_k = \mathbb{I}_d$.

Quantum channels (cotd.)

Theorem (Choi (1975))

A linear map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is a quantum channel if and only if Φ has a Choi-Kraus representation:

$$\Phi(X) = \sum_{k=1}^{K} B_k X B_k^*, \quad X \in \mathbb{M}_d,$$

with $\sum_{k=1}^{K} B_k^* B_k = \mathbb{I}_d$.

Remark: Choi-Kraus representations of a quantum channel are not unique.

Quantum channels (cotd.)

Theorem (Choi (1975))

A linear map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ *is a quantum channel if and only if* Φ *has a Choi-Kraus representation:*

$$\Phi(X) = \sum_{k=1}^{K} B_k X B_k^*, \quad X \in \mathbb{M}_d,$$

with $\sum_{k=1}^{K} B_k^* B_k = \mathbb{I}_d$.

Remark: Choi-Kraus representations of a quantum channel are not unique.

Definition (Choi rank)

The Choi rank of a quantum channel $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is the minimum number of operators $B_1, \ldots, B_K$ required in its Choi-Kraus representation, and is denoted by $\mathrm{cr}(\Phi)$.

Separability and entanglement

- If $P, Q \in \mathbb{M}_d$ are positive semi-definite matrices, then $P \otimes Q \in \mathbb{M}_d \otimes \mathbb{M}_d$ is also positive semi-definite.

Separability and entanglement

- If $P, Q \in \mathbb{M}_d$ are positive semi-definite matrices, then $P \otimes Q \in \mathbb{M}_d \otimes \mathbb{M}_d$ is also positive semi-definite. Similarly, $\sum_{i=1}^{n} P_i \otimes Q_i \geq 0$, whenever $P_i, Q_i \geq 0$.

Separability and entanglement

- If $P, Q \in \mathbb{M}_d$ are positive semi-definite matrices, then $P \otimes Q \in \mathbb{M}_d \otimes \mathbb{M}_d$ is also positive semi-definite. Similarly, $\sum_{i=1}^{n} P_i \otimes Q_i \geq 0$, whenever $P_i, Q_i \geq 0$.
- What about the converse?

Separability and entanglement

- If $P, Q \in \mathbb{M}_d$ are positive semi-definite matrices, then $P \otimes Q \in \mathbb{M}_d \otimes \mathbb{M}_d$ is also positive semi-definite. Similarly, $\sum_{i=1}^{n} P_i \otimes Q_i \geq 0$, whenever $P_i, Q_i \geq 0$.
- What about the converse? Let $A \in \mathbb{M}_d \otimes \mathbb{M}_d$ be positive semi-definite. Can it be expressed as $A = \sum_{i=1}^{n} P_i \otimes Q_i$, where $P_i, Q_i \geq 0$?

Separability and entanglement

- If $P, Q \in \mathbb{M}_d$ are positive semi-definite matrices, then $P \otimes Q \in \mathbb{M}_d \otimes \mathbb{M}_d$ is also positive semi-definite. Similarly, $\sum_{i=1}^n P_i \otimes Q_i \geq 0$, whenever $P_i, Q_i \geq 0$.
- What about the converse? Let $A \in \mathbb{M}_d \otimes \mathbb{M}_d$ be positive semi-definite. Can it be expressed as $A = \sum_{i=1}^n P_i \otimes Q_i$, where $P_i, Q_i \geq 0$?
- Answer: In general, no!

Separability and entanglement

- If $P, Q \in \mathbb{M}_d$ are positive semi-definite matrices, then $P \otimes Q \in \mathbb{M}_d \otimes \mathbb{M}_d$ is also positive semi-definite. Similarly, $\sum_{i=1}^{n} P_i \otimes Q_i \geq 0$, whenever $P_i, Q_i \geq 0$.
- What about the converse? Let $A \in \mathbb{M}_d \otimes \mathbb{M}_d$ be positive semi-definite. Can it be expressed as $A = \sum_{i=1}^{n} P_i \otimes Q_i$, where $P_i, Q_i \geq 0$?
- Answer: In general, no! If yes, then A is called *separable*.

Separability and entanglement

- If $P, Q \in \mathbb{M}_d$ are positive semi-definite matrices, then $P \otimes Q \in \mathbb{M}_d \otimes \mathbb{M}_d$ is also positive semi-definite. Similarly, $\sum_{i=1}^{n} P_i \otimes Q_i \geq 0$, whenever $P_i, Q_i \geq 0$.
- What about the converse? Let $A \in \mathbb{M}_d \otimes \mathbb{M}_d$ be positive semi-definite. Can it be expressed as $A = \sum_{i=1}^{n} P_i \otimes Q_i$, where $P_i, Q_i \geq 0$?
- Answer: In general, no! If yes, then A is called *separable*.
- Example: Consider,

$$A = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix} \in \mathbb{M}_2 \otimes \mathbb{M}_2.$$

Separability and entanglement

- If $P, Q \in \mathbb{M}_d$ are positive semi-definite matrices, then $P \otimes Q \in \mathbb{M}_d \otimes \mathbb{M}_d$ is also positive semi-definite. Similarly, $\sum_{i=1}^n P_i \otimes Q_i \geq 0$, whenever $P_i, Q_i \geq 0$.
- What about the converse? Let $A \in \mathbb{M}_d \otimes \mathbb{M}_d$ be positive semi-definite. Can it be expressed as $A = \sum_{i=1}^n P_i \otimes Q_i$, where $P_i, Q_i \geq 0$?
- Answer: In general, no! If yes, then A is called *separable*.
- Example: Consider,

$$A = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix} \in \mathbb{M}_2 \otimes \mathbb{M}_2.$$

Then A *cannot* be expressed as $A = \sum_{i=1}^n P_i \otimes Q_i$, where $P_i, Q_i \geq 0$? Such matrices are called, obviously,

Separability and entanglement

- If $P, Q \in \mathbb{M}_d$ are positive semi-definite matrices, then $P \otimes Q \in \mathbb{M}_d \otimes \mathbb{M}_d$ is also positive semi-definite. Similarly, $\sum_{i=1}^n P_i \otimes Q_i \geq 0$, whenever $P_i, Q_i \geq 0$.
- What about the converse? Let $A \in \mathbb{M}_d \otimes \mathbb{M}_d$ be positive semi-definite. Can it be expressed as $A = \sum_{i=1}^n P_i \otimes Q_i$, where $P_i, Q_i \geq 0$?
- Answer: In general, no! If yes, then A is called *separable*.
- Example: Consider,

$$A = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix} \in \mathbb{M}_2 \otimes \mathbb{M}_2.$$

  Then A *cannot* be expressed as $A = \sum_{i=1}^n P_i \otimes Q_i$, where $P_i, Q_i \geq 0$? Such matrices are called, obviously, *entangled*.

Entanglement breaking maps

Entanglement breaking maps

Definition (Horodecki, Shor, Ruskai (2003))

A quantum channel $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is called *entanglement breaking* if its Choi matrix

$$C_\Phi = \begin{bmatrix} \Phi(E_{1,1}) & \dots & \Phi(E_{1,d}) \\ \vdots & \ddots & \vdots \\ \Phi(E_{d,1}) & \dots & \Phi(E_{d,d}) \end{bmatrix} \in \mathbb{M}_d \otimes \mathbb{M}_d,$$

Entanglement breaking maps

Definition (Horodecki, Shor, Ruskai (2003))

A quantum channel $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is called *entanglement breaking* if its Choi matrix

$$C_\Phi = \begin{bmatrix} \Phi(E_{1,1}) & \dots & \Phi(E_{1,d}) \\ \vdots & \ddots & \vdots \\ \Phi(E_{d,1}) & \dots & \Phi(E_{d,d}) \end{bmatrix} \in \mathbb{M}_d \otimes \mathbb{M}_d,$$

is separable.

Entanglement breaking maps

Definition (Horodecki, Shor, Ruskai (2003))

A quantum channel $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is called *entanglement breaking* if its Choi matrix

$$C_\Phi = \begin{bmatrix} \Phi(E_{1,1}) & \dots & \Phi(E_{1,d}) \\ \vdots & \ddots & \vdots \\ \Phi(E_{d,1}) & \dots & \Phi(E_{d,d}) \end{bmatrix} \in \mathbb{M}_d \otimes \mathbb{M}_d,$$

is separable.

Theorem (Horodeck, Shor, Ruskai (2003))

A quantum channel $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is entanglement breaking if and only if it has a Choi-Kraus representation

$$\Phi(X) = \sum_{k=1}^{K} R_k X R_k^*,$$

Entanglement breaking maps

Definition (Horodecki, Shor, Ruskai (2003))

A quantum channel $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is called *entanglement breaking* if its Choi matrix

$$C_\Phi = \begin{bmatrix} \Phi(E_{1,1}) & \dots & \Phi(E_{1,d}) \\ \vdots & \ddots & \vdots \\ \Phi(E_{d,1}) & \dots & \Phi(E_{d,d}) \end{bmatrix} \in \mathbb{M}_d \otimes \mathbb{M}_d,$$

is separable.

Theorem (Horodeck, Shor, Ruskai (2003))

A quantum channel $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ is entanglement breaking if and only if it has a Choi-Kraus representation

$$\Phi(X) = \sum_{k=1}^{K} R_k X R_k^*,$$

where each R_k is a rank one matrix.

Entanglement breaking rank

Definition

Let $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ be an entanglement breaking map.

Entanglement breaking rank

Definition

Let $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ be an entanglement breaking map. The *entanglement breaking rank* of Φ, denoted by $\mathrm{ebr}(\Phi)$, is the minimum number of rank-one matrices R_k required when Φ is written in the form $\Phi(X) = \sum_{k=1}^{K} R_k X R_k^*$.

Entanglement breaking rank

Definition

Let $\Phi : \mathbb{M}_d \to \mathbb{M}_d$ be an entanglement breaking map. The *entanglement breaking rank* of Φ, denoted by $\mathrm{ebr}(\Phi)$, is the minimum number of rank-one matrices R_k required when Φ is written in the form $\Phi(X) = \sum_{k=1}^{K} R_k X R_k^*$.

Clearly, $\mathrm{ebr}(\Phi) \geq \mathrm{cr}(\Phi)$, where $\mathrm{cr}(\Phi)$ is the Choi rank of Φ.

Zauner's conjecture (again)

Let $d \geq 2$. Suppose there exist d^2 unit vectors $\{v_i\}_{i=1}^{d^2}$ in $\mathbb{C}^d$ such that

$$|\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}, \qquad \text{for all } i \neq j.$$

Zauner's conjecture (again)

Let $d \geq 2$. Suppose there exist d^2 unit vectors $\{v_i\}_{i=1}^{d^2}$ in $\mathbb{C}^d$ such that

$$|\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}, \qquad \text{for all } i \neq j.$$

Consider the rank one orthogonal projections $P_i = v_i v_i^*$ on the $\mathrm{span}\{v_i\}$. Then

(a) $\frac{1}{d}\sum_{i=1}^{d^2} P_i = \mathbb{I}_d$,

Zauner's conjecture (again)

Let $d \geq 2$. Suppose there exist d^2 unit vectors $\{v_i\}_{i=1}^{d^2}$ in $\mathbb{C}^d$ such that

$$|\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}, \qquad \text{for all } i \neq j.$$

Consider the rank one orthogonal projections $P_i = v_i v_i^*$ on the $\mathrm{span}\{v_i\}$. Then

(a) $\frac{1}{d}\sum_{i=1}^{d^2} P_i = \mathbb{I}_d$,

(b) $\{P_i : 1 \leq i \leq d^2\}$ is a basis for $\mathbb{M}_d$, and,

Zauner's conjecture (again)

Let $d \geq 2$. Suppose there exist d^2 unit vectors $\{v_i\}_{i=1}^{d^2}$ in $\mathbb{C}^d$ such that

$$|\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}, \qquad \text{for all } i \neq j.$$

Consider the rank one orthogonal projections $P_i = v_i v_i^*$ on the $\mathrm{span}\{v_i\}$. Then

(a) $\frac{1}{d} \sum_{i=1}^{d^2} P_i = \mathbb{I}_d$,

(b) $\{P_i : 1 \leq i \leq d^2\}$ is a basis for $\mathbb{M}_d$, and,

(c) $\mathrm{Tr}(P_i P_j) = |\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}$, for all $i \neq j$.

In quantum information such a set of d^2 rank one projections $\{P_i\}_{i=1}^{d^2}$ is called a *symmetric*

Zauner's conjecture (again)

Let $d \geq 2$. Suppose there exist d^2 unit vectors $\{v_i\}_{i=1}^{d^2}$ in $\mathbb{C}^d$ such that

$$|\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}, \qquad \text{for all } i \neq j.$$

Consider the rank one orthogonal projections $P_i = v_i v_i^*$ on the $\mathrm{span}\{v_i\}$. Then

(a) $\frac{1}{d} \sum_{i=1}^{d^2} P_i = \mathbb{I}_d$,

(b) $\{P_i : 1 \leq i \leq d^2\}$ is a basis for $\mathbb{M}_d$, and,

(c) $\mathrm{Tr}(P_i P_j) = |\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}$, for all $i \neq j$.

In quantum information such a set of d^2 rank one projections $\{P_i\}_{i=1}^{d^2}$ is called a *symmetric informationally complete*

Zauner's conjecture (again)

Let $d \geq 2$. Suppose there exist d^2 unit vectors $\{v_i\}_{i=1}^{d^2}$ in $\mathbb{C}^d$ such that

$$|\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}, \qquad \text{for all } i \neq j.$$

Consider the rank one orthogonal projections $P_i = v_i v_i^*$ on the $\mathrm{span}\{v_i\}$. Then

(a) $\frac{1}{d} \sum_{i=1}^{d^2} P_i = \mathbb{I}_d$,

(b) $\{P_i : 1 \leq i \leq d^2\}$ is a basis for $\mathbb{M}_d$, and,

(c) $\mathrm{Tr}(P_i P_j) = |\langle v_i, v_j \rangle|^2 = \frac{1}{d+1}$, for all $i \neq j$.

In quantum information such a set of d^2 rank one projections $\{P_i\}_{i=1}^{d^2}$ is called a *symmetric informationally complete positive operator-valued measure* (SIC POVM).

Channel from SIC POVM

If there exists a SIC POVM $\{P_i\}_{i=1}^{d^2} \subset \mathbb{M}_d$, consider the map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$,

Channel from SIC POVM

If there exists a SIC POVM $\{P_i\}_{i=1}^{d^2} \subset \mathbb{M}_d$, consider the map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Phi(X) = \frac{1}{d} \sum_{i=1}^{d^2} P_i X P_i^*.$$

Channel from SIC POVM

If there exists a SIC POVM $\{P_i\}_{i=1}^{d^2} \subset \mathbb{M}_d$, consider the map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Phi(X) = \frac{1}{d} \sum_{i=1}^{d^2} P_i X P_i^*.$$

This is an entanglement breaking map,

Channel from SIC POVM

If there exists a SIC POVM $\{P_i\}_{i=1}^{d^2} \subset \mathbb{M}_d$, consider the map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Phi(X) = \frac{1}{d} \sum_{i=1}^{d^2} P_i X P_i^*.$$

This is an entanglement breaking map, and actually

$$\Phi(X) = Z(X) := \frac{1}{d+1} X + \frac{d}{d+1} \frac{\mathrm{Tr}(X)}{d} \mathbb{I}_d.$$

Channel from SIC POVM

If there exists a SIC POVM $\{P_i\}_{i=1}^{d^2} \subset \mathbb{M}_d$, consider the map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Phi(X) = \frac{1}{d} \sum_{i=1}^{d^2} P_i X P_i^*.$$

This is an entanglement breaking map, and actually

$$\Phi(X) = Z(X) := \frac{1}{d+1} X + \frac{d}{d+1} \frac{\mathrm{Tr}(X)}{d} \mathbb{I}_d.$$

Easy to show: $\mathrm{cr}(Z) = d^2$.

Channel from SIC POVM

If there exists a SIC POVM $\{P_i\}_{i=1}^{d^2} \subset \mathbb{M}_d$, consider the map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Phi(X) = \frac{1}{d} \sum_{i=1}^{d^2} P_i X P_i^*.$$

This is an entanglement breaking map, and actually

$$\Phi(X) = Z(X) := \frac{1}{d+1} X + \frac{d}{d+1} \frac{\mathrm{Tr}(X)}{d} \mathbb{I}_d.$$

Easy to show: $\mathrm{cr}(Z) = d^2$.
Can be shown independently: Z is entanglement breaking.

Channel from SIC POVM

If there exists a SIC POVM $\{P_i\}_{i=1}^{d^2} \subset \mathbb{M}_d$, consider the map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Phi(X) = \frac{1}{d} \sum_{i=1}^{d^2} P_i X P_i^*.$$

This is an entanglement breaking map, and actually

$$\Phi(X) = Z(X) := \frac{1}{d+1} X + \frac{d}{d+1} \frac{\mathrm{Tr}(X)}{d} \mathbb{I}_d.$$

Easy to show: $\mathrm{cr}(Z) = d^2$.
Can be shown independently: Z is entanglement breaking. So,

$$Z(X) = \sum_{k=1}^{K} R_k X R_k^*,$$

where each R_k is of rank one.

Channel from SIC POVM

If there exists a SIC POVM $\{P_i\}_{i=1}^{d^2} \subset \mathbb{M}_d$, consider the map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Phi(X) = \frac{1}{d} \sum_{i=1}^{d^2} P_i X P_i^*.$$

This is an entanglement breaking map, and actually

$$\Phi(X) = Z(X) := \frac{1}{d+1} X + \frac{d}{d+1} \frac{\mathrm{Tr}(X)}{d} \mathbb{I}_d.$$

Easy to show: $\mathrm{cr}(Z) = d^2$.
Can be shown independently: Z is entanglement breaking. So,

$$Z(X) = \sum_{k=1}^{K} R_k X R_k^*,$$

where each R_k is of rank one.
Questions: What is $\mathrm{ebr}(Z)$? In other words, what is the least number of rank one matrices required in its Choi Kraus representation?

Channel from SIC POVM

If there exists a SIC POVM $\{P_i\}_{i=1}^{d^2} \subset \mathbb{M}_d$, consider the map $\Phi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Phi(X) = \frac{1}{d} \sum_{i=1}^{d^2} P_i X P_i^*.$$

This is an entanglement breaking map, and actually

$$\Phi(X) = Z(X) := \frac{1}{d+1} X + \frac{d}{d+1} \frac{\mathrm{Tr}(X)}{d} \mathbb{I}_d.$$

Easy to show: $\mathrm{cr}(Z) = d^2$.
Can be shown independently: Z is entanglement breaking. So,

$$Z(X) = \sum_{k=1}^{K} R_k X R_k^*,$$

where each R_k is of rank one.
Questions: What is $\mathrm{ebr}(Z)$? In other words, what is the least number of rank one matrices required in its Choi Kraus representation? Can it be d^2?

SIC POVM from channel

Theorem (Pandey, Paulsen, P., Rahaman)

The following are equivalent:

(a) *Zauner's conjecture is true in dimension d.*

SIC POVM from channel

Theorem (Pandey, Paulsen, P., Rahaman)

The following are equivalent:

(a) *Zauner's conjecture is true in dimension d.*

(b) $\mathrm{ebr}(Z) = d^2$.

SIC POVM from channel

Theorem (Pandey, Paulsen, P., Rahaman)

The following are equivalent:

(a) *Zauner's conjecture is true in dimension d.*

(b) $\mathrm{ebr}(Z) = d^2$.

(c) $\mathrm{ebr}(Z^T) = d^2$.

SIC POVM from channel

Theorem (Pandey, Paulsen, P., Rahaman)

The following are equivalent:

(a) *Zauner's conjecture is true in dimension d.*

(b) $\mathrm{ebr}(Z) = d^2$.

(c) $\mathrm{ebr}(Z^T) = d^2$. *(Z^T is a Werner-Holevo channel.)*

MUB conjecture (again)

Suppose there are $d+1$ orthonormal bases of $\mathbb{C}^2$,

$$\begin{aligned}
\mathcal{E}_1 &= \{e_{1,1}, e_{1,2}, ..., e_{1,d}\}, \\
\mathcal{E}_2 &= \{e_{2,1}, e_{2,2}, ..., e_{2,d}\}, \\
&\vdots \\
\mathcal{E}_{d+1} &= \{e_{d+1,1}, e_{d+1,2}, ..., e_{d+1,d}\},
\end{aligned}$$

which are mutually unbiased.

MUB conjecture (again)

Suppose there are $d+1$ orthonormal bases of $\mathbb{C}^2$,

$$\begin{aligned} \mathcal{E}_1 &= \{e_{1,1}, e_{1,2}, ..., e_{1,d}\}, \\ \mathcal{E}_2 &= \{e_{2,1}, e_{2,2}, ..., e_{2,d}\}, \\ &\vdots \\ \mathcal{E}_{d+1} &= \{e_{d+1,1}, e_{d+1,2}, ..., e_{d+1,d}\}, \end{aligned}$$

which are mutually unbiased. Let $P_{i,j} = e_{i,j}e_{i,j}^*$ be the orthogonal projection on the subspace spanned by each vector $e_{i,j}$.

MUB conjecture (again)

Suppose there are $d+1$ orthonormal bases of $\mathbb{C}^2$,

$$\begin{aligned}
\mathcal{E}_1 &= \{e_{1,1}, e_{1,2}, \dots, e_{1,d}\},\\
\mathcal{E}_2 &= \{e_{2,1}, e_{2,2}, \dots, e_{2,d}\},\\
&\vdots\\
\mathcal{E}_{d+1} &= \{e_{d+1,1}, e_{d+1,2}, \dots, e_{d+1,d}\},
\end{aligned}$$

which are mutually unbiased. Let $P_{i,j} = e_{i,j}e_{i,j}^*$ be the orthogonal projection on the subspace spanned by each vector $e_{i,j}$.
Consider the map $\Psi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Psi(X) = \frac{1}{d+1}\sum_{i=1}^{d+1}\sum_{j=1}^{d} P_{i,j} X P_{i,j}^*.$$

MUB conjecture (again)

Suppose there are $d+1$ orthonormal bases of $\mathbb{C}^2$,

$$\mathcal{E}_1 = \{e_{1,1}, e_{1,2}, ..., e_{1,d}\},$$
$$\mathcal{E}_2 = \{e_{2,1}, e_{2,2}, ..., e_{2,d}\},$$
$$\vdots$$
$$\mathcal{E}_{d+1} = \{e_{d+1,1}, e_{d+1,2}, ..., e_{d+1,d}\},$$

which are mutually unbiased. Let $P_{i,j} = e_{i,j}e_{i,j}^*$ be the orthogonal projection on the subspace spanned by each vector $e_{i,j}$.
Consider the map $\Psi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Psi(X) = \frac{1}{d+1} \sum_{i=1}^{d+1} \sum_{j=1}^{d} P_{i,j} X P_{i,j}^*.$$

Then again Ψ is entanglement breaking.

MUB conjecture (again)

Suppose there are $d+1$ orthonormal bases of $\mathbb{C}^2$,

$$\mathcal{E}_1 = \{e_{1,1}, e_{1,2}, ..., e_{1,d}\},$$
$$\mathcal{E}_2 = \{e_{2,1}, e_{2,2}, ..., e_{2,d}\},$$
$$\vdots$$
$$\mathcal{E}_{d+1} = \{e_{d+1,1}, e_{d+1,2}, ..., e_{d+1,d}\},$$

which are mutually unbiased. Let $P_{i,j} = e_{i,j}e_{i,j}^*$ be the orthogonal projection on the subspace spanned by each vector $e_{i,j}$.
Consider the map $\Psi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Psi(X) = \frac{1}{d+1} \sum_{i=1}^{d+1} \sum_{j=1}^{d} P_{i,j} X P_{i,j}^*.$$

Then again Ψ is entanglement breaking. Moreover,

$$\Psi(X) = Z(X) = \frac{1}{d+1} X + \frac{d}{d+1} \frac{\mathrm{Tr}(X)}{d} \mathbb{I}_d.$$

MUB conjecture (again)

Suppose there are $d+1$ orthonormal bases of $\mathbb{C}^2$,

$$\begin{aligned} \mathcal{E}_1 &= \{e_{1,1}, e_{1,2}, ..., e_{1,d}\}, \\ \mathcal{E}_2 &= \{e_{2,1}, e_{2,2}, ..., e_{2,d}\}, \\ &\vdots \\ \mathcal{E}_{d+1} &= \{e_{d+1,1}, e_{d+1,2}, ..., e_{d+1,d}\}, \end{aligned}$$

which are mutually unbiased. Let $P_{i,j} = e_{i,j}e_{i,j}^*$ be the orthogonal projection on the subspace spanned by each vector $e_{i,j}$.
Consider the map $\Psi : \mathbb{M}_d \to \mathbb{M}_d$,

$$\Psi(X) = \frac{1}{d+1}\sum_{i=1}^{d+1}\sum_{j=1}^{d} P_{i,j}XP_{i,j}^*.$$

Then again Ψ is entanglement breaking. Moreover,

$$\Psi(X) = Z(X) = \frac{1}{d+1}X + \frac{d}{d+1}\frac{\mathrm{Tr}(X)}{d}\mathbb{I}_d.$$

Question: Converse?

Other convex combinations

Theorem

Let $t \in \left[0, \frac{1}{d+1}\right]$*. If* $\Phi_t = t\mathcal{I}_d + (1-t)\Psi_d$*, then* Φ_t *is entanglement breaking.*

Other convex combinations

Theorem

Let $t \in \left[0, \frac{1}{d+1}\right]$. *If* $\Phi_t = t\mathcal{I}_d + (1-t)\Psi_d$, *then* Φ_t *is entanglement breaking.*

Easy to see: $\mathrm{cr}(\Phi_t) = d^2$.

Other convex combinations

Theorem

Let $t \in \left[0, \frac{1}{d+1}\right]$. *If* $\Phi_t = t\mathcal{I}_d + (1-t)\Psi_d$, *then* Φ_t *is entanglement breaking.*

Easy to see: $\mathrm{cr}(\Phi_t) = d^2$.

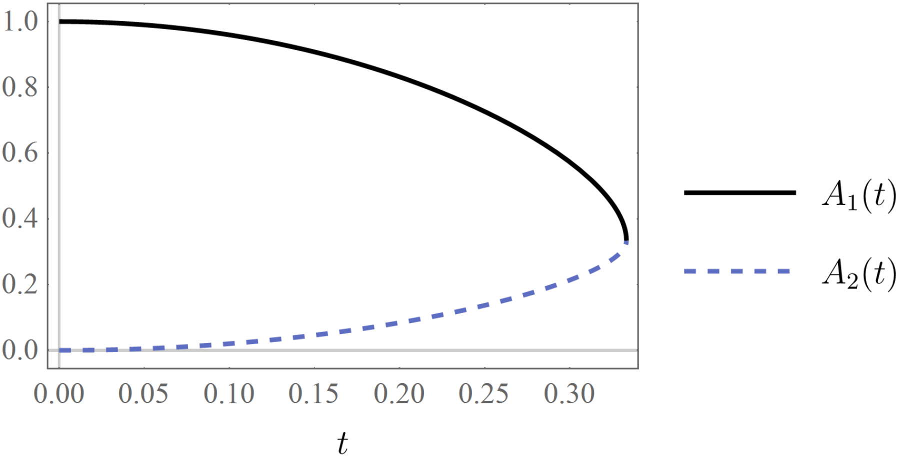
Conjecture

There exist a continuous family of d^2 *rank-one matrices* $R_i(t)$ *such that*

$$\Phi_t(X) = \sum_{i=1}^{d^2} R_i(t) X R_i(t)^*,$$

for all $0 \leq t \leq \frac{1}{d+1}$.

$d = 2$



Thank you!