Quasi-orthogonal decomposition of matrix algebras

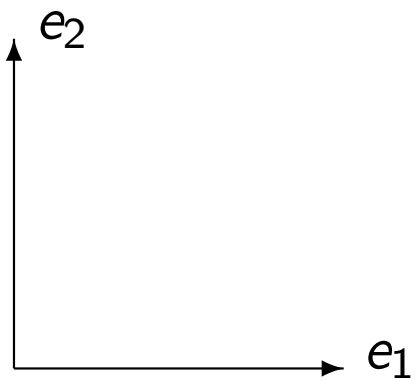
Mihály Weiner

Alfréd Rényi Institute of Mathematics, Budapest
Hungarian Academy of Sciences

February 2, 2009

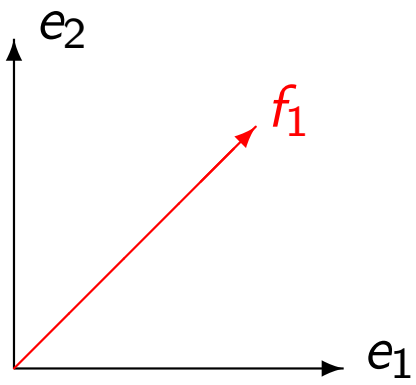
The concept of unbiased vectors and bases

Here is an ONB in two dimensions:



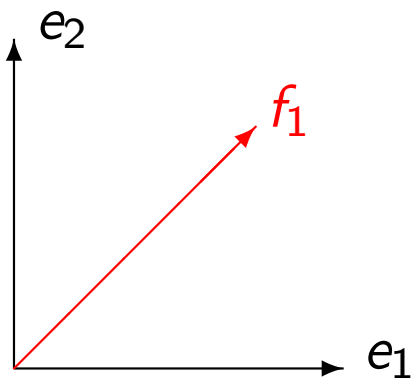
The concept of unbiased vectors and bases

Here is an ONB in two dimensions:



The concept of unbiased vectors and bases

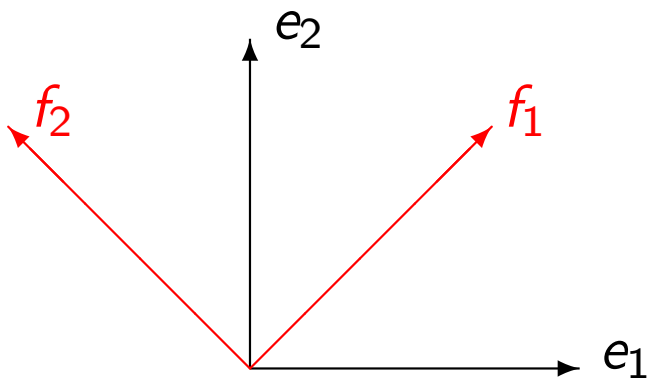
Here is an ONB in two dimensions:



f_1 is **unbiased** for (e_1, e_2)

The concept of unbiased vectors and bases

Here is an ONB in two dimensions:

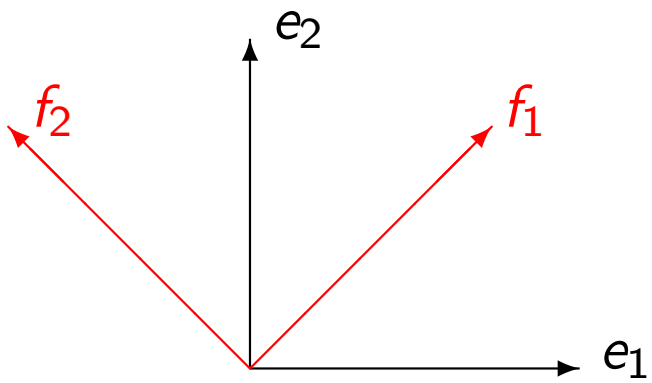


f_1 is **unbiased** for (e_1, e_2)

so is f_2

The concept of unbiased vectors and bases

Here is an ONB in two dimensions:



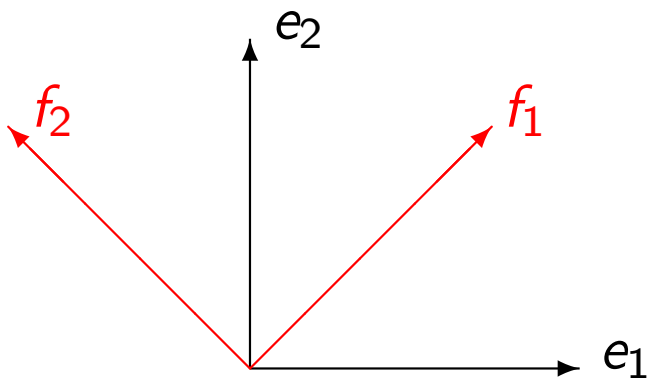
f_1 is **unbiased** for (e_1, e_2)

so is f_2

(f_1, f_2) is another ONB which is **unbiased** for (e_1, e_2)

The concept of unbiased vectors and bases

Here is an ONB in two dimensions:



f_1 is **unbiased** for (e_1, e_2)

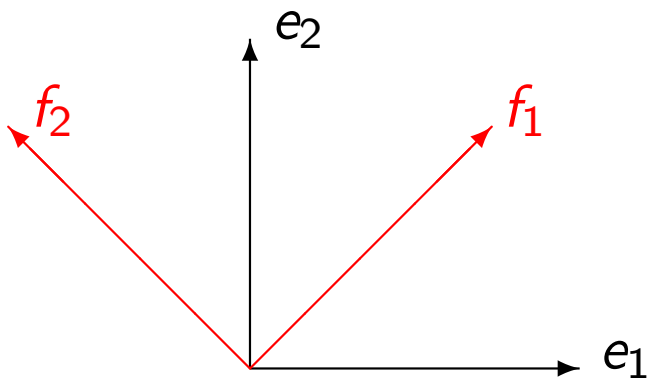
so is f_2

(f_1, f_2) is another ONB which is **unbiased** for (e_1, e_2)

Note: (e_1, e_2) is also unbiased for (f_1, f_2).

The concept of unbiased vectors and bases

Here is an ONB in two dimensions:



f_1 is **unbiased** for (e_1, e_2)

so is f_2

(f_1, f_2) is another ONB which is **unbiased** for (e_1, e_2)

Note: (e_1, e_2) is also unbiased for (f_1, f_2). Unbiasedness is automatically **mutual**.

Definition

Let $\mathcal{H}$ be a finite dimensional Hilbert space. Two bases $(e_1, \ldots, e_n)$ and $(f_1, \ldots, f_n)$ in $\mathcal{H}$ satisfying

$$|\langle e_j, f_k \rangle| = |\langle e_{j'}, f_{k'} \rangle|$$

for all $j, k, j', k' \in \{1, \ldots n\}$ are called **mutually unbiased**.

Definition

Let $\mathcal{H}$ be a finite dimensional Hilbert space. Two bases $(e_1, \ldots, e_n)$ and $(f_1, \ldots, f_n)$ in $\mathcal{H}$ satisfying

$$|\langle e_j, f_k \rangle| = |\langle e_{j'}, f_{k'} \rangle|$$

for all $j, k, j', k' \in \{1, \ldots n\}$ are called **mutually unbiased**.

Remark

If $(e_1, \ldots, e_n)$ and $(f_1, \ldots, f_n)$ are mutually unbiased, then infact $|\langle e_j, f_k \rangle| = \frac{1}{\sqrt{n}}$ for all $j, k \in \{1, \ldots n\}$.

Problem

In an n-dimensional (complex) space, at most how many ONB can be given, such that any two of them is mutually unbiased?

An equivalent description

- Instead of a basis consider the algebra of operators spanned by the ortho-projections onto the basis vectors

An equivalent description

- Instead of a basis consider the algebra of operators spanned by the ortho-projections onto the basis vectors
- $\mathcal{A} \subset M_n(\mathbb{C})$ is such an algebra if and only if it is a maximal abelian *-subalgebra (MASA)

An equivalent description

- Instead of a basis consider the algebra of operators spanned by the ortho-projections onto the basis vectors
- $\mathcal{A} \subset M_n(\mathbb{C})$ is such an algebra if and only if it is a maximal abelian *-subalgebra (MASA)
- Two maximal abelian *-subalgebras $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$ correspond to mutually unbiased bases if and only if

$$\tau(AB) = \tau(A)\tau(B)$$

for all $A \in \mathcal{A}, B \in \mathcal{B}$ ("**statistical independence**")

Quasi-orthogonality

The formula

$$\langle A, B \rangle := \tau(A^* B)$$

defines a scalar product (called: the "Hilbert-Schmidt" scalar product) on $M_n(\mathbb{C})$.

Quasi-orthogonality

The formula

$$\langle A, B\rangle := \tau(A^* B)$$

defines a scalar product (called: the "Hilbert-Schmidt" scalar product) on $M_n(\mathbb{C})$.

- Two *-subalgebras $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$, as linear subspaces, cannot be orthogonal: $\mathbb{1} \in \mathcal{A} \cap \mathcal{B} \neq \{0\}$

Quasi-orthogonality

The formula

$$\langle A, B\rangle := \tau(A^* B)$$

defines a scalar product (called: the "Hilbert-Schmidt" scalar product) on $M_n(\mathbb{C})$.

- Two *-subalgebras $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$, as linear subspaces, cannot be orthogonal: $\mathbb{1} \in \mathcal{A} \cap \mathcal{B} \neq \{0\}$
- But $\mathcal{A} \cap \{\mathbb{1}\}^\perp$ may be orthogonal to $\mathcal{B} \cap \{\mathbb{1}\}^\perp$, in which case we say that they are **quasi-orthogonal**

Quasi-orthogonality

The formula

$$\langle A, B\rangle := \tau(A^* B)$$

defines a scalar product (called: the "Hilbert-Schmidt" scalar product) on $M_n(\mathbb{C})$.

- Two *-subalgebras $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$, as linear subspaces, cannot be orthogonal: $\mathbb{1} \in \mathcal{A} \cap \mathcal{B} \neq \{0\}$
- But $\mathcal{A} \cap \{\mathbb{1}\}^\perp$ may be orthogonal to $\mathcal{B} \cap \{\mathbb{1}\}^\perp$, in which case we say that they are **quasi-orthogonal**
- Note that $\{\mathbb{1}\}^\perp =$ traceless operators, so: $\mathcal{A}$ and $\mathcal{B}$ are quasi-orthogonal $\Leftrightarrow$ their traceless parts are orthogonal

Mutually unbiased bases

MUB $\Leftrightarrow$ quasi-orthogonal maximal abelian *-subalgebras $\dim(M_n(\mathbb{C})) = n^2$ and

Mutually unbiased bases

MUB $\Leftrightarrow$ quasi-orthogonal maximal abelian *-subalgebras $\dim(M_n(\mathbb{C})) = n^2$ and

- dimension of the traceless part of $M_n(\mathbb{C})$ is $n^2 - 1$

Mutually unbiased bases

MUB $\Leftrightarrow$ quasi-orthogonal maximal abelian *-subalgebras $\dim(M_n(\mathbb{C})) = n^2$ and

- dimension of the traceless part of $M_n(\mathbb{C})$ is $n^2 - 1$
- dimension of the traceless part of a maximal abelian *-subalgebra of $M_n(\mathbb{C})$ is $n - 1$, so if $n > 1$

Mutually unbiased bases

MUB $\Leftrightarrow$ quasi-orthogonal maximal abelian *-subalgebras

$\dim(M_n(\mathbb{C})) = n^2$ and

- dimension of the traceless part of $M_n(\mathbb{C})$ is $n^2 - 1$
- dimension of the traceless part of a maximal abelian *-subalgebra of $M_n(\mathbb{C})$ is $n - 1$, so if $n > 1$

$\Rightarrow \frac{n^2-1}{n-1} = n + 1$ is an upper bound on the number of MUB.

Mutually unbiased bases

MUB $\Leftrightarrow$ quasi-orthogonal maximal abelian *-subalgebras

$\dim(M_n(\mathbb{C})) = n^2$ and

- dimension of the traceless part of $M_n(\mathbb{C})$ is $n^2 - 1$
- dimension of the traceless part of a maximal abelian *-subalgebra of $M_n(\mathbb{C})$ is $n - 1$, so if $n > 1$

$\Rightarrow \frac{n^2-1}{n-1} = n + 1$ is an upper bound on the number of MUB.

Complete collection of MUB: the corresponding subalgebras linearly span $M_n(\mathbb{C}) \Leftrightarrow$ their number is $n + 1$.

What is known?

$N(n) :=$ maximum number of MUB in dimension n. Then $N(1) = 1$ and by what was said $N(n) \leq n + 1$. Moreover

What is known?

$N(n) :=$ maximum number of MUB in dimension n. Then $N(1) = 1$ and by what was said $N(n) \leq n + 1$. Moreover

- ☺ for $n =$ a power of a prime, $N(n) = n + 1$ by construction

What is known?

$N(n) :=$ maximum number of MUB in dimension n. Then $N(1) = 1$ and by what was said $N(n) \leq n + 1$. Moreover

- ☺ for $n =$ a power of a prime, $N(n) = n + 1$ by construction
- ☺ some properties can be established in general, e.g. that $N(n_1 n_2) \geq \min\{N(n_1), N(n_2)\}$

What is known?

$N(n) :=$ maximum number of MUB in dimension n. Then $N(1) = 1$ and by what was said $N(n) \leq n + 1$. Moreover

- ☺ for $n =$ a power of a prime, $N(n) = n + 1$ by construction
- ☺ some properties can be established in general, e.g. that $N(n_1 n_2) \geq \min\{N(n_1), N(n_2)\}$
- ☹ but apart from $n = 1$ or $n = p^r$, there is not a single value of n for which $N(n)$ would be known

What is known?

$N(n) :=$ maximum number of MUB in dimension n. Then $N(1) = 1$ and by what was said $N(n) \leq n + 1$. Moreover

- ☺ for $n =$ a power of a prime, $N(n) = n + 1$ by construction
- ☺ some properties can be established in general, e.g. that $N(n_1 n_2) \geq \min\{N(n_1), N(n_2)\}$
- ☹ but apart from $n = 1$ or $n = p^r$, there is not a single value of n for which $N(n)$ would be known
- ▶ i.e. already in 6 dimensions the question is unsolved: $N(6) =?$

What is known?

$N(n) :=$ maximum number of MUB in dimension n. Then $N(1) = 1$ and by what was said $N(n) \leq n + 1$. Moreover

- ☺ for $n =$ a power of a prime, $N(n) = n + 1$ by construction
- ☺ some properties can be established in general, e.g. that $N(n_1 n_2) \geq \min\{N(n_1), N(n_2)\}$
- ☹ but apart from $n = 1$ or $n = p^r$, there is not a single value of n for which $N(n)$ would be known
- i.e. already in 6 dimensions the question is unsolved: $N(6) =?$
- numerical calculations done with computers seem to indicate that $N(6) = 3$

MUBs in dimension 6

Numerical "experimenting" with computers is nice . . .

MUBs in dimension 6

Numerical "experimenting" with computers is nice . . .

- ☺ can help to formulate the right conjecture,

MUBs in dimension 6

Numerical "experimenting" with computers is nice . . .

- ☺ can help to formulate the right conjecture,
- ☹ but cannot substitute a mathematical proof.

MUBs in dimension 6

Numerical "experimenting" with computers is nice . . .

- ☺ can help to formulate the right conjecture,
- ☹ but cannot substitute a mathematical proof.

P. Jaming, M. Maté, P. Móra, F. Szöllösi, M. Weiner (work in preparation):

- use computers but *not* for numerical experimentation

MUBs in dimension 6

Numerical "experimenting" with computers is nice . . .

- ☺ can help to formulate the right conjecture,
- ☹ but cannot substitute a mathematical proof.

P. Jaming, M. Maté, P. Móra, F. Szöllösi, M. Weiner (work in preparation):

- use computers but *not* for numerical experimentation
- can possibly lead to a *"computer aided proof"* of $N(6) = 3$

MUBs in dimension 6

Numerical "experimenting" with computers is nice . . .

- ☺ can help to formulate the right conjecture,
- ☹ but cannot substitute a mathematical proof.

P. Jaming, M. Maté, P. Móra, F. Szöllösi, M. Weiner (work in preparation):

- use computers but *not* for numerical experimentation
- can possibly lead to a *"computer aided proof"* of $N(6) = 3$
- at the moment our algorithm is not fast enough

MUBs in dimension 6

Numerical "experimenting" with computers is nice . . .

- ☺ can help to formulate the right conjecture,
- ☹ but cannot substitute a mathematical proof.

P. Jaming, M. Maté, P. Móra, F. Szöllösi, M. Weiner (work in preparation):

- use computers but *not* for numerical experimentation
- can possibly lead to a *"computer aided proof"* of $N(6) = 3$
- at the moment our algorithm is not fast enough
- but fast enough to exclude the existence of 4 MUBs satisfying certain additional conditions

MUBs in dimension 6

Numerical "experimenting" with computers is nice . . .

- ☺ can help to formulate the right conjecture,
- ☹ but cannot substitute a mathematical proof.

P. Jaming, M. Maté, P. Móra, F. Szöllösi, M. Weiner (work in preparation):

- use computers but *not* for numerical experimentation
- can possibly lead to a *"computer aided proof"* of $N(6) = 3$
- at the moment our algorithm is not fast enough
- but fast enough to exclude the existence of 4 MUBs satisfying certain additional conditions
- exhibition of continuous families of MUB triplets

MUBs in dimension 6

Numerical "experimenting" with computers is nice . . .

- ☺ can help to formulate the right conjecture,
- ☹ but cannot substitute a mathematical proof.

P. Jaming, M. Maté, P. Móra, F. Szöllösi, M. Weiner (work in preparation):

- use computers but *not* for numerical experimentation
- can possibly lead to a *"computer aided proof"* of $N(6) = 3$
- at the moment our algorithm is not fast enough
- but fast enough to exclude the existence of 4 MUBs satisfying certain additional conditions
- exhibition of continuous families of MUB triplets
- better understanding of the role of symmetries

Measurements and maximal abelian subalgebras

- (real-valued) physical quantity $\Leftrightarrow$ self-adjoint operator

Measurements and maximal abelian subalgebras

- (real-valued) physical quantity $\Leftrightarrow$ self-adjoint operator
- A and B are simultaneously measurable: $[A, B] = 0$

Measurements and maximal abelian subalgebras

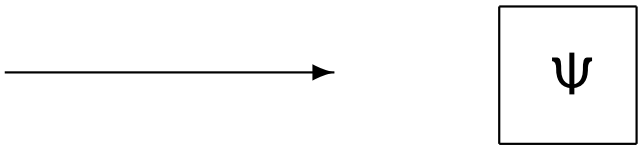
- (real-valued) physical quantity $\Leftrightarrow$ self-adjoint operator
- A and B are simultaneously measurable: $[A, B] = 0$
- best measurement: simultaneously measuring as many quantities as possible

Measurements and maximal abelian subalgebras

- (real-valued) physical quantity $\Leftrightarrow$ self-adjoint operator
- A and B are simultaneously measurable: $[A, B] = 0$
- best measurement: simultaneously measuring as many quantities as possible
- best measurements $\Leftrightarrow$ maximal abelian C^*-subalgebras

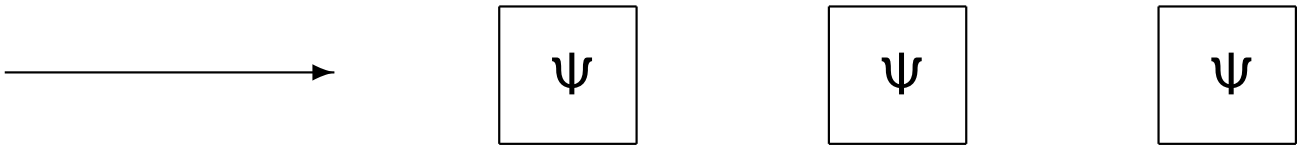
Copies of a finite-level q-system produced in the same state Ψ.

Copies of a finite-level q-system produced in the same state Ψ.

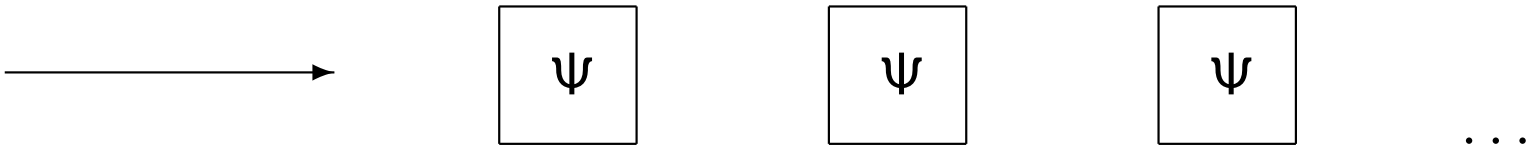


Copies of a finite-level q-system produced in the same state Ψ.

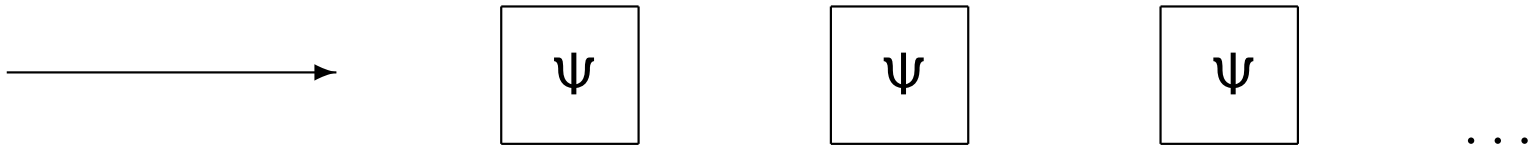
Copies of a finite-level q-system produced in the same state Ψ.



Copies of a finite-level q-system produced in the same state Ψ.

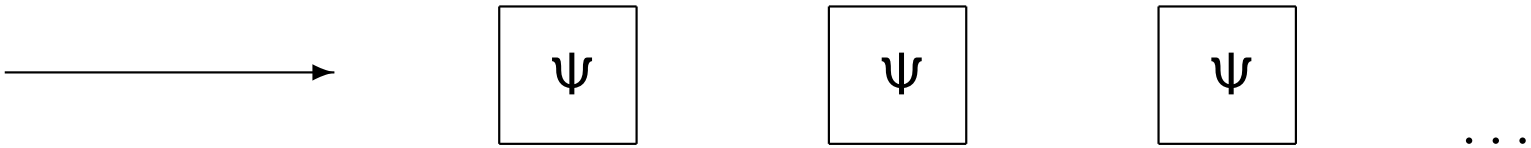


Copies of a finite-level q-system produced in the same state Ψ.



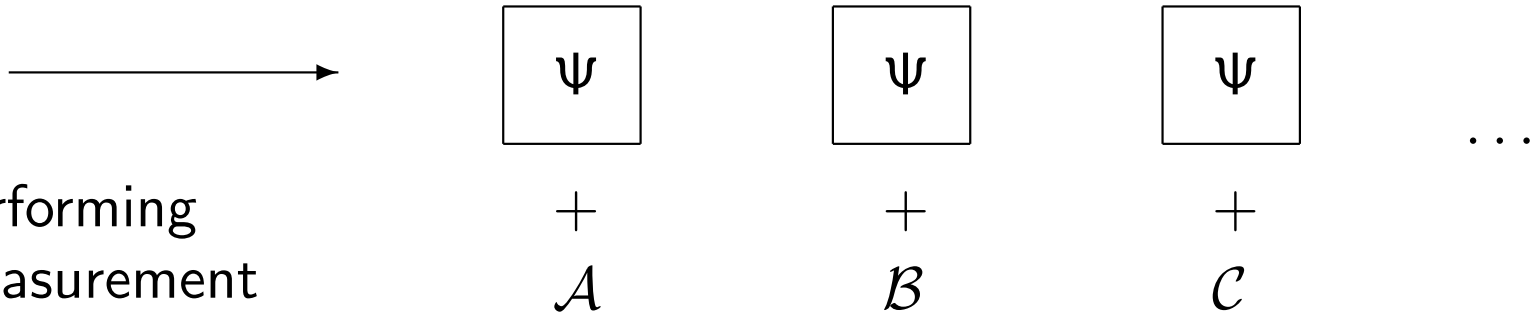
performing measurement type: $+$ $\mathcal{A}$

Copies of a finite-level q-system produced in the same state Ψ.

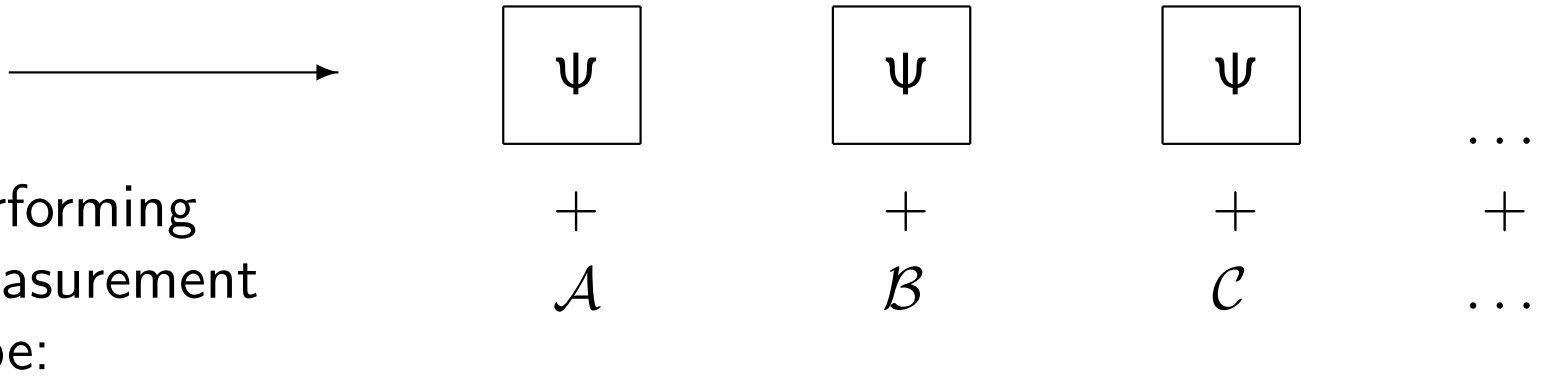


performing measurement type: $+$ $\mathcal{A}$ $+$ $\mathcal{B}$

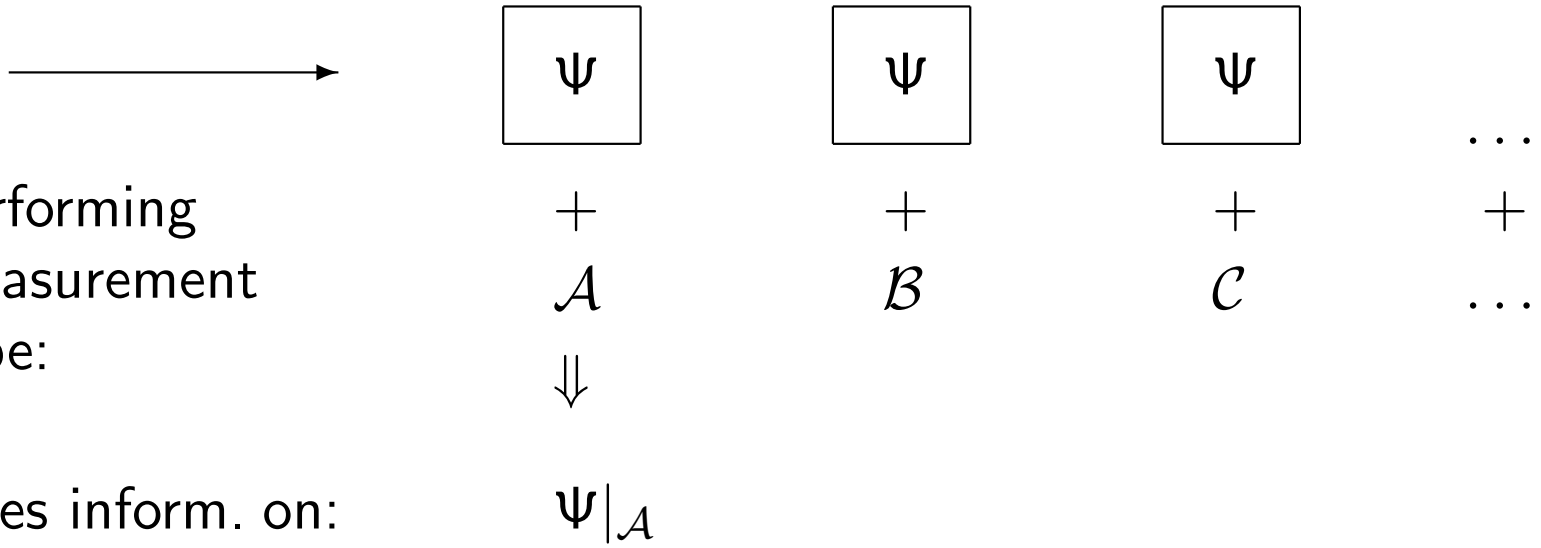
Copies of a finite-level q-system produced in the same state Ψ.



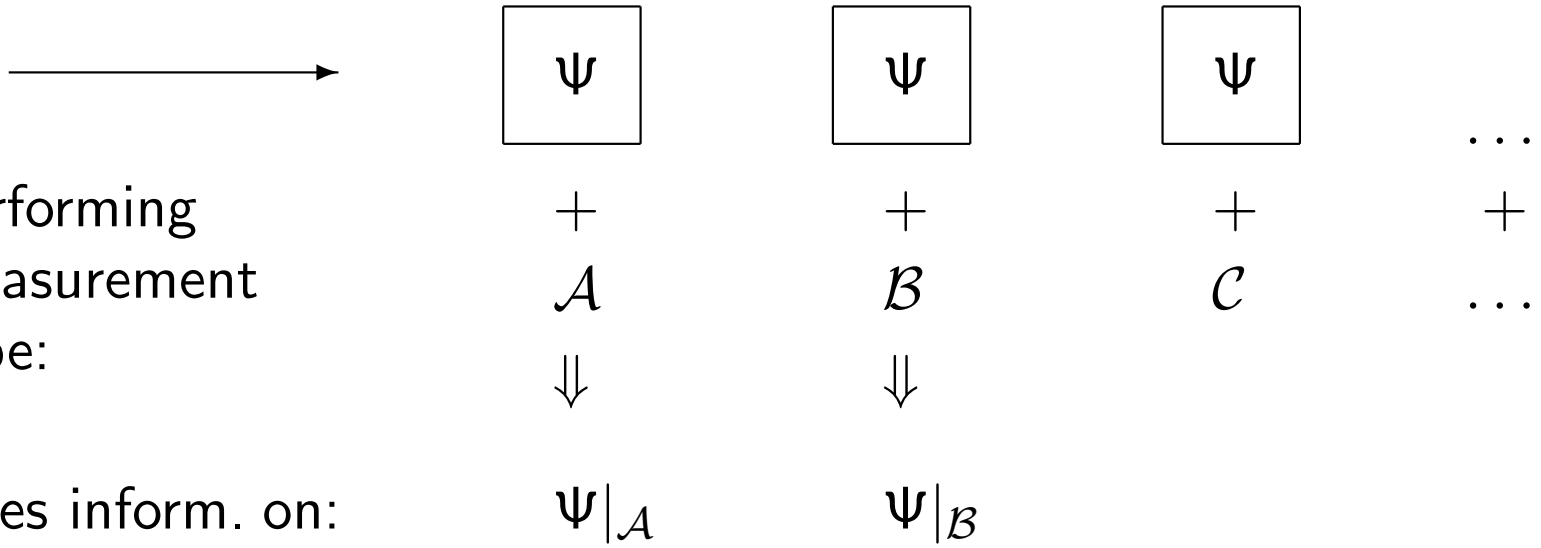
Copies of a finite-level q-system produced in the same state Ψ.



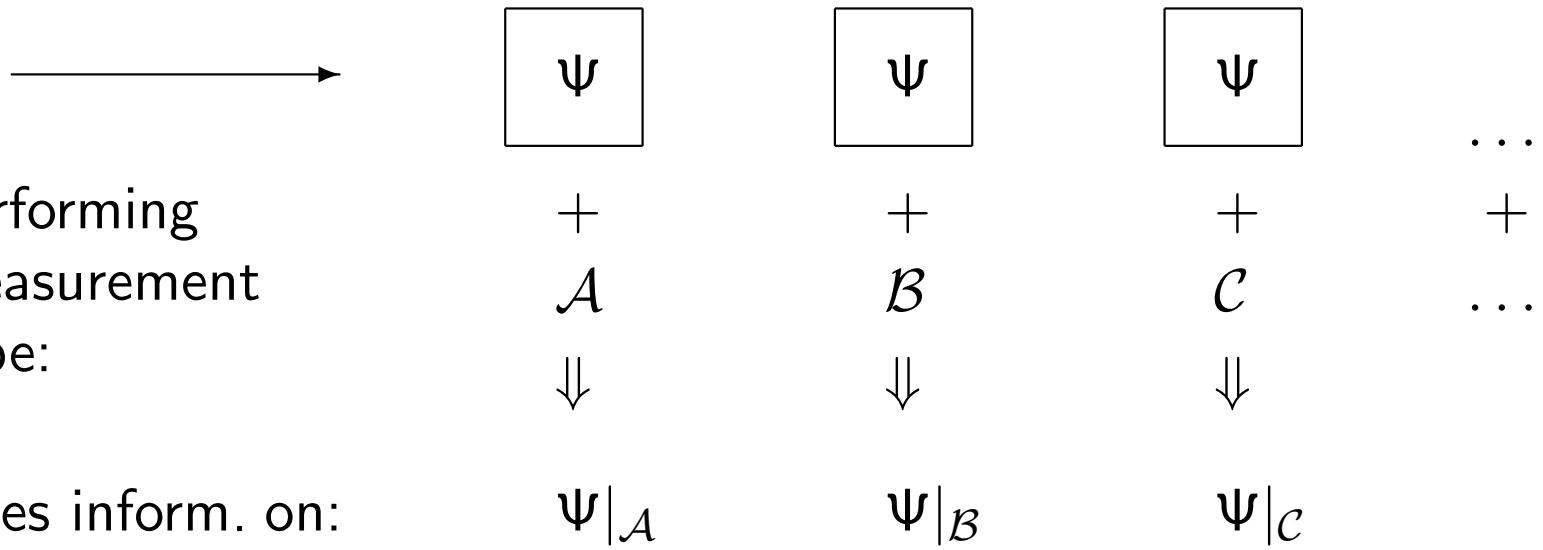
Copies of a finite-level q-system produced in the same state Ψ.



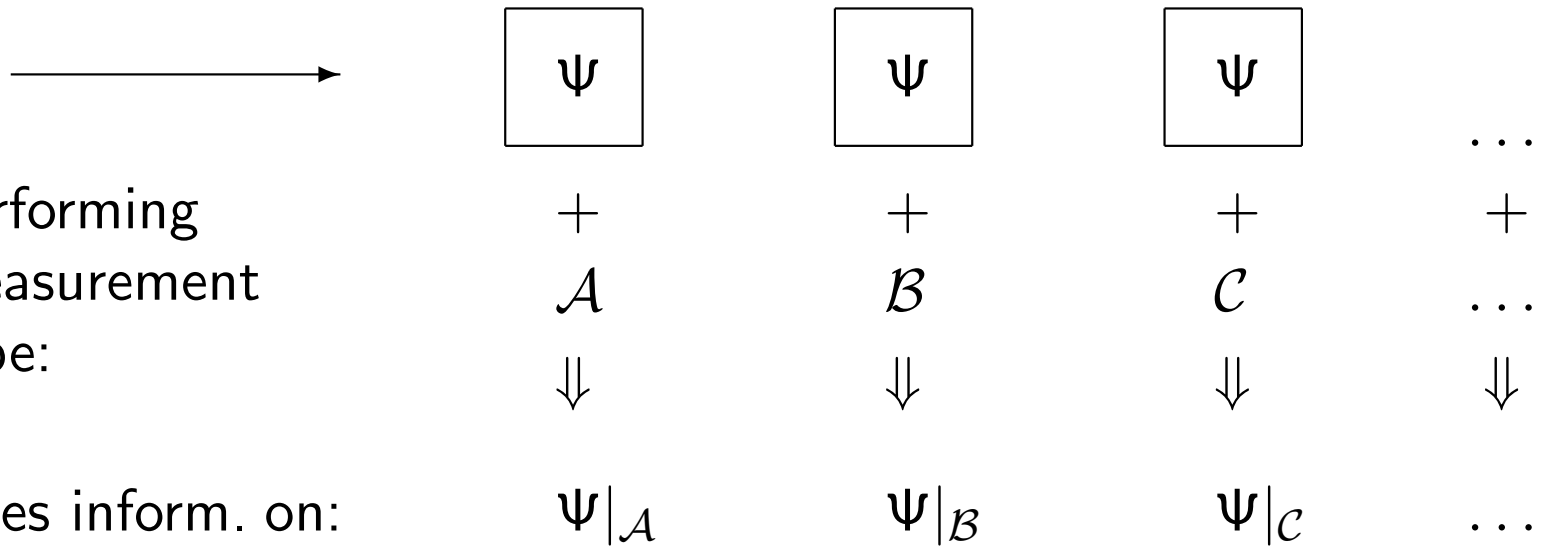
Copies of a finite-level q-system produced in the same state Ψ.



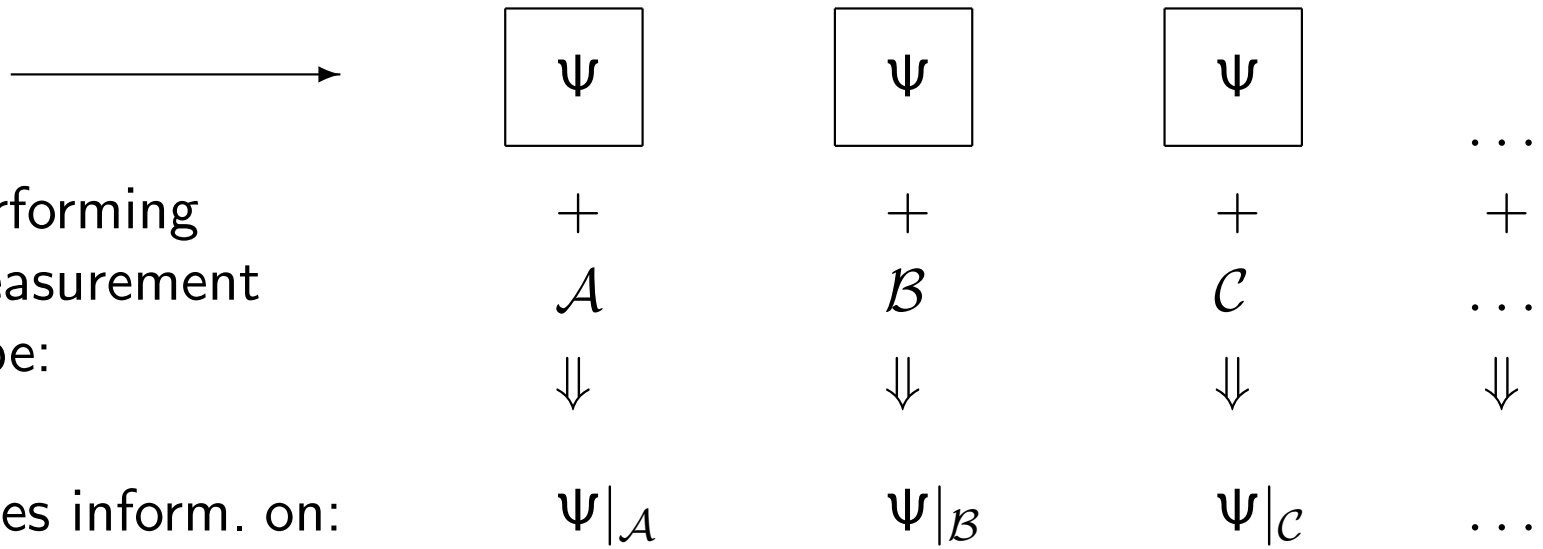
Copies of a finite-level q-system produced in the same state Ψ.



Copies of a finite-level q-system produced in the same state Ψ.

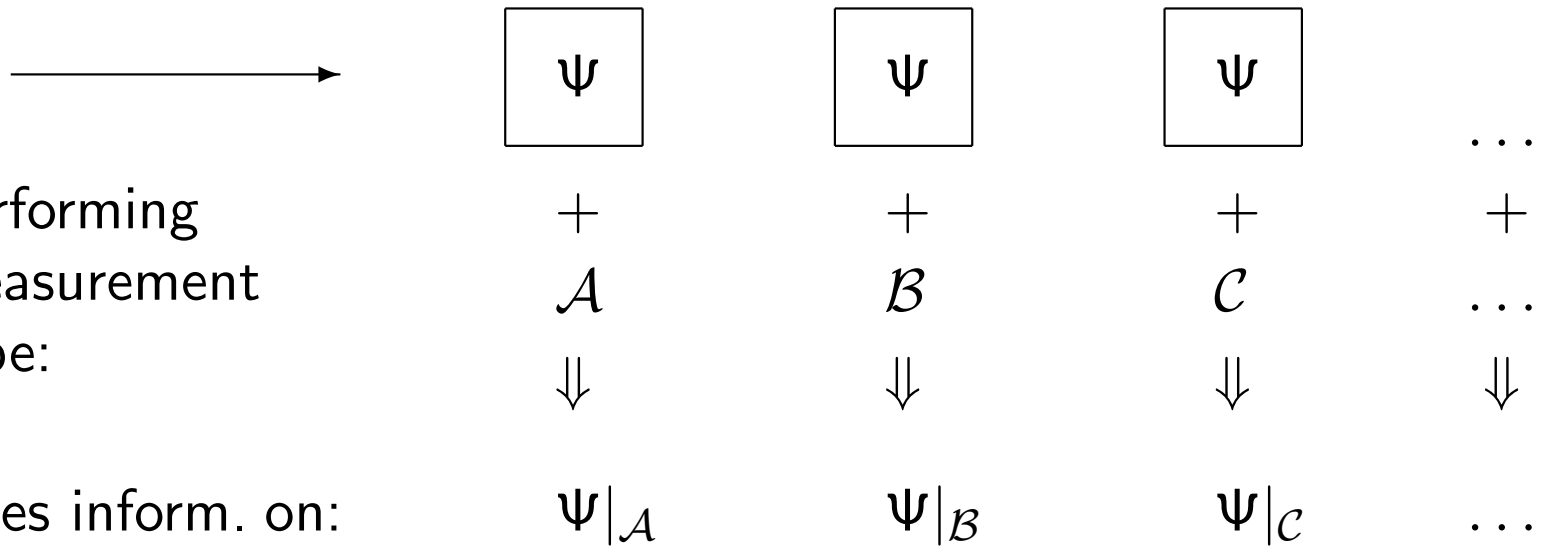


Copies of a finite-level q-system produced in the same state Ψ.



The best is to choose $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ so that they are statistically independent.

Copies of a finite-level q-system produced in the same state Ψ.



The best is to choose $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ so that they are statistically independent. Moreover, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ is a **complete set of measurables** $\Leftrightarrow$ they span $\mathcal{B}(\mathcal{H})$.

Historical remarks

- notion of MUB: around '60 in the work of Schwinger (?):

Historical remarks

- notion of MUB: around '60 in the work of Schwinger (?): if $(\mathcal{A}, \mathcal{B})$ is MUB and the q-system is prepared so that it has a certain $\mathcal{A}$-value, then its $\mathcal{B}$-value is a white noise

Historical remarks

- notion of MUB: around '60 in the work of Schwinger (?): if $(\mathcal{A}, \mathcal{B})$ is MUB and the q-system is prepared so that it has a certain $\mathcal{A}$-value, then its $\mathcal{B}$-value is a white noise
- most striking application: protocol of Bennett and Brassard to distribute secret keys over a public channel in an information theoretically secure way

Historical remarks

- notion of MUB: around '60 in the work of Schwinger (?): if $(\mathcal{A}, \mathcal{B})$ is MUB and the q-system is prepared so that it has a certain $\mathcal{A}$-value, then its $\mathcal{B}$-value is a white noise
- most striking application: protocol of Bennett and Brassard to distribute secret keys over a public channel in an information theoretically secure way
- in '80, Alltop constructed complex sequences with low correlation for spread spectrum radar and communication applications

Historical remarks

- notion of MUB: around '60 in the work of Schwinger (?): if $(\mathcal{A}, \mathcal{B})$ is MUB and the q-system is prepared so that it has a certain $\mathcal{A}$-value, then its $\mathcal{B}$-value is a white noise
- most striking application: protocol of Bennett and Brassard to distribute secret keys over a public channel in an information theoretically secure way
- in '80, Alltop constructed complex sequences with low correlation for spread spectrum radar and communication applications $\Rightarrow$ provided $p+1$ MUB in $p \geq 5$ prime dimension

Historical remarks

- notion of MUB: around '60 in the work of Schwinger (?): if $(\mathcal{A}, \mathcal{B})$ is MUB and the q-system is prepared so that it has a certain $\mathcal{A}$-value, then its $\mathcal{B}$-value is a white noise
- most striking application: protocol of Bennett and Brassard to distribute secret keys over a public channel in an information theoretically secure way
- in '80, Alltop constructed complex sequences with low correlation for spread spectrum radar and communication applications $\Rightarrow$ provided $p+1$ MUB in $p \geq 5$ prime dimension
- by explicit construction, Ivanovič, '81: $N(p) = p+1$;

Historical remarks

- notion of MUB: around '60 in the work of Schwinger (?): if $(\mathcal{A}, \mathcal{B})$ is MUB and the q-system is prepared so that it has a certain $\mathcal{A}$-value, then its $\mathcal{B}$-value is a white noise
- most striking application: protocol of Bennett and Brassard to distribute secret keys over a public channel in an information theoretically secure way
- in '80, Alltop constructed complex sequences with low correlation for spread spectrum radar and communication applications $\Rightarrow$ provided $p+1$ MUB in $p \geq 5$ prime dimension
- by explicit construction, Ivanovič, '81: $N(p) = p+1$; Wootters and Fields, '89: $N(p^r) = p^r + 1$

Finite geometry, latin squares, MUB and the king's problem

- obvious similarity with the existence of finite projective planes, existence of complete sets of orthogonal Latin squares

Finite geometry, latin squares, MUB and the king's problem

- obvious similarity with the existence of finite projective planes, existence of complete sets of orthogonal Latin squares
- there are indications that they are the *same* problem, e.g. the construction of Wocjan and Beth (2004)

Finite geometry, latin squares, MUB and the king's problem

- obvious similarity with the existence of finite projective planes, existence of complete sets of orthogonal Latin squares
- there are indications that they are the *same* problem, e.g. the construction of Wocjan and Beth (2004)
- the "king's problem" of Vaidman, Aharonov and Albert has a simple generalisation for an n-level q-system, given that there is a complete set of MUB..

Finite geometry, latin squares, MUB and the king's problem

- obvious similarity with the existence of finite projective planes, existence of complete sets of orthogonal Latin squares
- there are indications that they are the *same* problem, e.g. the construction of Wocjan and Beth (2004)
- the "king's problem" of Vaidman, Aharonov and Albert has a simple generalisation for an n-level q-system, given that there is a complete set of MUB.. but solution of this problem exists if and only if there exists a complete sets of orthogonal Latin squares of order n (Hayashi, Horibe, Hashimoto, 2005)

New indications & similarities

Finding a complete set of quasi-orthogonal copies of $\mathbb{C}^n$ in $M_n(\mathbb{C})$ is difficult because

New indications & similarities

Finding a complete set of quasi-orthogonal copies of $\mathbb{C}^n$ in $M_n(\mathbb{C})$ is difficult because

- classical "combinatorical" problems (like at finding finite affine planes)

New indications & similarities

Finding a complete set of quasi-orthogonal copies of $\mathbb{C}^n$ in $M_n(\mathbb{C})$ is difficult because

- classical "combinatorical" problems (like at finding finite affine planes)
- non-classical, "quantum" problems: $M_n(\mathbb{C})$ is not abelian.

New indications & similarities

Finding a complete set of quasi-orthogonal copies of $\mathbb{C}^n$ in $M_n(\mathbb{C})$ is difficult because

- classical "combinatorical" problems (like at finding finite affine planes)
- non-classical, "quantum" problems: $M_n(\mathbb{C})$ is not abelian.

How about replacing $M_n(\mathbb{C})$ by an abelian algebra?

New indications & similarities

Finding a complete set of quasi-orthogonal copies of $\mathbb{C}^n$ in $M_n(\mathbb{C})$ is difficult because

- classical "combinatorical" problems (like at finding finite affine planes)
- non-classical, "quantum" problems: $M_n(\mathbb{C})$ is not abelian.

How about replacing $M_n(\mathbb{C})$ by an abelian algebra?

New indications & similarities

Theorem (M. Weiner)

There exists a complete set of quasi-orthogonal copies of $\mathbb{C}^n$ in $\mathbb{C}^{n^2}$ if and only if there exists a finite affine plane of order n.

New indications & similarities

Theorem (M. Weiner)

There exists a complete set of quasi-orthogonal copies of $\mathbb{C}^n$ in $\mathbb{C}^{n^2}$ if and only if there exists a finite affine plane of order n.

Here is another similarity.

New indications & similarities

Theorem (M. Weiner)

There exists a complete set of quasi-orthogonal copies of $\mathbb{C}^n$ in $\mathbb{C}^{n^2}$ if and only if there exists a finite affine plane of order n.

Here is another similarity.

Theorem (M. Weiner)

Suppose $\mathcal{E}_1, \dots, \mathcal{E}_n$ is a collection of MUB in $\mathbb{C}^n$. Then there exists an ONB $\mathcal{E}_{n+1}$ such that $\mathcal{E}_1, \dots, \mathcal{E}_n, \mathcal{E}_{n+1}$ is a complete collection of MUB.

About hard problems

What to do when facing a hard problem?

About hard problems

What to do when facing a hard problem?

- Generalise (i.e. create new problems),

About hard problems

What to do when facing a hard problem?

- Generalise (i.e. create new problems),
- relate it to other problems,

About hard problems

What to do when facing a hard problem?

- Generalise (i.e. create new problems),
- relate it to other problems,
- or possibly do both.

About hard problems

What to do when facing a hard problem?

- Generalise (i.e. create new problems),
- relate it to other problems,
- or possibly do both.

(Occasionaly mathematicians even resolve some problems.)

Quasi-orthogonal decompositions

Def. A collection of pairwise quasi-orthogonal *-subalgebras $\mathcal{A}, \mathcal{B}, \mathcal{C} \ldots M_n(\mathbb{C})$ such that $\mathcal{A} + \mathcal{B} + \mathcal{C} \ldots = M_n(\mathbb{C})$ is called a **quasi-orthogonal decomposition** of $M_n(\mathbb{C})$.

Quasi-orthogonal decompositions

Def. A collection of pairwise quasi-orthogonal *-subalgebras $\mathcal{A}, \mathcal{B}, \mathcal{C} \ldots M_n(\mathbb{C})$ such that $\mathcal{A} + \mathcal{B} + \mathcal{C} \ldots = M_n(\mathbb{C})$ is called a **quasi-orthogonal decomposition** of $M_n(\mathbb{C})$.

- A complete collection of MUB gives a particular decomposition,

Quasi-orthogonal decompositions

Def. A collection of pairwise quasi-orthogonal *-subalgebras $\mathcal{A}, \mathcal{B}, \mathcal{C} \ldots M_n(\mathbb{C})$ such that $\mathcal{A} + \mathcal{B} + \mathcal{C} \ldots = M_n(\mathbb{C})$ is called a **quasi-orthogonal decomposition** of $M_n(\mathbb{C})$.

- A complete collection of MUB gives a particular decomposition,
- but why looking for decompositions consisting of MASAs *only*?

Quasi-orthogonal decompositions

Def. A collection of pairwise quasi-orthogonal *-subalgebras $\mathcal{A}, \mathcal{B}, \mathcal{C} \ldots M_n(\mathbb{C})$ such that $\mathcal{A} + \mathcal{B} + \mathcal{C} \ldots = M_n(\mathbb{C})$ is called a **quasi-orthogonal decomposition** of $M_n(\mathbb{C})$.

- A complete collection of MUB gives a particular decomposition,
- but why looking for decompositions consisting of MASAs *only*?
- New question (D. Petz): what kind of decompositions exist in general?

Motivation for the generalized question

A q-bit is sent from one q-computer to another one:

Motivation for the generalized question

A q-bit is sent from one q-computer to another one:

REGISTER: $M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \otimes \ldots \otimes M_2(\mathbb{C})$

Motivation for the generalized question

A q-bit is sent from one q-computer to another one:

REGISTER: $M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \otimes \ldots \otimes M_2(\mathbb{C})$
STATE IN THE REGISTER: Ψ

Motivation for the generalized question

A q-bit is sent from one q-computer to another one:

REGISTER:	$M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \otimes \ldots \otimes M_2(\mathbb{C})$
STATE IN THE REGISTER:	Ψ
SENT:	$\Psi\big\vert_{(\mathbb{1} \otimes M_2(\mathbb{C}))}$

Motivation for the generalized question

more q-computers, on each one we run a different program

Motivation for the generalized question

more q-computers, on each one we run a different program

INITIAL STATE (or DATA INPUT) for each: Ψ_0

Motivation for the generalized question

more q-computers, on each one we run a different program

INITIAL STATE (or DATA INPUT) for each: Ψ_0
FINAL STATE: $\Psi_1, \ldots, \Psi_m$ where $\Psi_j = \Psi_0 \cdot \mathrm{Ad}(U_j)$

Motivation for the generalized question

more q-computers, on each one we run a different program

INITIAL STATE (or DATA INPUT) for each: Ψ_0
FINAL STATE: $\Psi_1, \ldots, \Psi_m$ where $\Psi_j = \Psi_0 \cdot \mathrm{Ad}(U_j)$
SENT: $\Psi_j|_{(\mathbb{1}\otimes M_2(\mathbb{C}))} = \Psi_0|_{\mathcal{A}_j}$, where $\mathcal{A}_j = U_j(\mathbb{1} \otimes M_2(\mathbb{C}))$

Motivation for the generalized question

more q-computers, on each one we run a different program

INITIAL STATE (or DATA INPUT) for each: Ψ_0
FINAL STATE: $\Psi_1, \ldots, \Psi_m$ where $\Psi_j = \Psi_0 \cdot \mathrm{Ad}(U_j)$
SENT: $\Psi_j|_{(\mathbb{1}\otimes M_2(\mathbb{C}))} = \Psi_0|_{\mathcal{A}_j}$, where $\mathcal{A}_j = U_j(\mathbb{1} \otimes M_2(\mathbb{C}))$

$\Rightarrow$ in general $\Psi_0|_{\mathcal{A}_1}, \ldots, \Psi_0|_{\mathcal{A}_m}$ contains the most information about Ψ_0 when $\mathcal{A}_1, \ldots \mathcal{A}_m$ are statistically independent

Motivation for the generalized question

more q-computers, on each one we run a different program

INITIAL STATE (or DATA INPUT) for each: Ψ_0
FINAL STATE: $\Psi_1, \ldots, \Psi_m$ where $\Psi_j = \Psi_0 \cdot \mathrm{Ad}(U_j)$
SENT: $\Psi_j|_{(\mathbb{1}\otimes M_2(\mathbb{C}))} = \Psi_0|_{\mathcal{A}_j}$, where $\mathcal{A}_j = U_j(\mathbb{1} \otimes M_2(\mathbb{C}))$

$\Rightarrow$ in general $\Psi_0|_{\mathcal{A}_1}, \ldots, \Psi_0|_{\mathcal{A}_m}$ contains the most information about Ψ_0 when $\mathcal{A}_1, \ldots \mathcal{A}_m$ are statistically independent

$\Rightarrow$ study quasi-orthogonal copies of $M_2(\mathbb{C})$ in $\otimes_k M_2(\mathbb{C}) \equiv M_{2^k}(\mathbb{C})$

Trivial necessary conditions

To find a quasi-orthogonal decomposition $\mathcal{B}_1, \mathcal{B}_2, \ldots$ of $M_n(\mathbb{C})$ in which $\mathcal{B}_k \simeq \mathcal{A}_k$, where $\mathcal{A}_1, \mathcal{A}_2, \ldots$ are given algebras,

Trivial necessary conditions

To find a quasi-orthogonal decomposition $\mathcal{B}_1, \mathcal{B}_2, \ldots$ of $M_n(\mathbb{C})$ in which $\mathcal{B}_k \simeq \mathcal{A}_k$, where $\mathcal{A}_1, \mathcal{A}_2, \ldots$ are given algebras,

- the dimensions must add up:

$$(\dim A_1 - 1) + (\dim A_2 - 1) + \ldots = \dim(M_n(\mathbb{C}) - 1) = n^2 - 1,$$

Trivial necessary conditions

To find a quasi-orthogonal decomposition $\mathcal{B}_1, \mathcal{B}_2, \ldots$ of $M_n(\mathbb{C})$ in which $\mathcal{B}_k \simeq \mathcal{A}_k$, where $\mathcal{A}_1, \mathcal{A}_2, \ldots$ are given algebras,

- the dimensions must add up:

$$(\dim A_1 - 1) + (\dim A_2 - 1) + \ldots = \dim(M_n(\mathbb{C}) - 1) = n^2 - 1,$$

- the types cannot be arbitrary: $\mathcal{A}_1, \mathcal{A}_2, \ldots$ must have realizations in $M_n(\mathbb{C})$ (e.g. no subalgebra of $M_6(\mathbb{C})$ is isomorphic to M_5)

Trivial necessary conditions

To find a quasi-orthogonal decomposition $\mathcal{B}_1, \mathcal{B}_2, \ldots$ of $M_n(\mathbb{C})$ in which $\mathcal{B}_k \simeq \mathcal{A}_k$, where $\mathcal{A}_1, \mathcal{A}_2, \ldots$ are given algebras,

- the dimensions must add up:

$$(\dim A_1 - 1) + (\dim A_2 - 1) + \ldots = \dim(M_n(\mathbb{C}) - 1) = n^2 - 1,$$

- the types cannot be arbitrary: $\mathcal{A}_1, \mathcal{A}_2, \ldots$ must have realizations in $M_n(\mathbb{C})$ (e.g. no subalgebra of $M_6(\mathbb{C})$ is isomorphic to M_5)
- $\dim A_k \dim A_l \leq n^2$ for any $k \neq l$.

Quasi-orthogonal copies of M_n in M_{n^k}

Can $M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \otimes \ldots \otimes M_2(\mathbb{C}) \equiv M_{2^k}(\mathbb{C})$ be decomposed into a sum of quasi-orthogonal copies of $M_2(\mathbb{C})$?

Quasi-orthogonal copies of M_n in M_{n^k}

Can $M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \otimes \ldots \otimes M_2(\mathbb{C}) \equiv M_{2^k}(\mathbb{C})$ be decomposed into a sum of quasi-orthogonal copies of $M_2(\mathbb{C})$?

Regardless of n and k, the decomposition of $M_n(\mathbb{C}) \otimes M_n(\mathbb{C}) \otimes \ldots \otimes M_n(\mathbb{C}) \equiv M_{n^k}(\mathbb{C})$ into quasi-orthogonal copies of $M_n(\mathbb{C})$ cannot be excluded by the trivial necessary conditions.

Quasi-orthogonal copies of M_n in M_{n^k}

Can $M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \otimes \ldots \otimes M_2(\mathbb{C}) \equiv M_{2^k}(\mathbb{C})$ be decomposed into a sum of quasi-orthogonal copies of $M_2(\mathbb{C})$?

Regardless of n and k, the decomposition of $M_n(\mathbb{C}) \otimes M_n(\mathbb{C}) \otimes \ldots \otimes M_n(\mathbb{C}) \equiv M_{n^k}(\mathbb{C})$ into quasi-orthogonal copies of $M_n(\mathbb{C})$ cannot be excluded by the trivial necessary conditions.

$k := 2 \Rightarrow$ dimensional similarity to the MUB case (but from the point of view of commutations it is exactly the *opposite* case)

Quasi-orthogonal copies of M_n in M_{n^k}

Theorem (M. Weiner)

For $n = p$ prime it is possible to give $\frac{n^{2k}-1}{n^2-1} - 1$ quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_{n^2}(\mathbb{C})$

Quasi-orthogonal copies of M_n in M_{n^k}

Theorem (M. Weiner)

For $n = p$ prime it is possible to give $\frac{n^{2k}-1}{n^2-1} - 1$ quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_{n^2}(\mathbb{C})$

Theorem (H. Ohno, 2008)

For $n = p^\alpha$ where $p > 2$ it is possible to give $\frac{n^{2k}-1}{n^2-1}$ quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_{n^k}(\mathbb{C})$; that is, $M_{n^k}(\mathbb{C})$ can be decomposed into a sum of quasi-orthogonal copies of $M_n(\mathbb{C})$.

Quasi-orthogonal copies of M_n in M_{n^k}

Theorem (M. Weiner)

For $n = p$ prime it is possible to give $\frac{n^{2k}-1}{n^2-1} - 1$ quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_{n^2}(\mathbb{C})$

Theorem (H. Ohno, 2008)

For $n = p^\alpha$ where $p > 2$ it is possible to give $\frac{n^{2k}-1}{n^2-1}$ quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_{n^k}(\mathbb{C})$; that is, $M_{n^k}(\mathbb{C})$ can be decomposed into a sum of quasi-orthogonal copies of $M_n(\mathbb{C})$.

Theorem (D. Petz, J. Kahn, 2006)

$M_4(\mathbb{C})$ cannot be decomposed into a sum of quasi-orthogonal copies of $M_2(\mathbb{C})$. The maximum number of quasi-orthogonal copies of $M_2(\mathbb{C})$ in $M_4(\mathbb{C})$ is 4.

Decompositions into factors and abelians subalgebras

Quantum Information Theory $\Rightarrow$ factors (complete matrix algebras) and abelian subalgebras are of special interest.

Decompositions into factors and abelians subalgebras

Quantum Information Theory $\Rightarrow$ factors (complete matrix algebras) and abelian subalgebras are of special interest.

By the trivial necessary conditions: if we use only copies of $\mathbb{C}^4$ and $M_2(\mathbb{C})$, then $M_4(\mathbb{C})$ is to be decomposed into 5 subalgebras.

Decompositions into factors and abelians subalgebras

Quantum Information Theory $\Rightarrow$ factors (complete matrix algebras) and abelian subalgebras are of special interest.

By the trivial necessary conditions: if we use only copies of $\mathbb{C}^4$ and $M_2(\mathbb{C})$, then $M_4(\mathbb{C})$ is to be decomposed into 5 subalgebras.

Theorem (D. Petz, A. Szántó, M. Weiner, 2008)

$M_4(\mathbb{C})$ can be decomposed into a quas-orthogonal sum of k copies of $M_4(\mathbb{C})$ and $5-k$ copies of $\mathbb{C}^4$ iff $k = 0, 2$ or 4.

Decompositions into factors and abelian subalgebras

So far: constructions + exclusions in special cases (namely, in 4 dimensions). General methods of finding non-trivial obstructions?

Decompositions into factors and abelian subalgebras

So far: constructions + exclusions in special cases (namely, in 4 dimensions). General methods of finding non-trivial obstructions?

$\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$: *-subalgebras, not neccessarily MASAs

Decompositions into factors and abelian subalgebras

So far: constructions + exclusions in special cases (namely, in 4 dimensions). General methods of finding non-trivial obstructions?

$\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$: *-subalgebras, not neccessarily MASAs $\Rightarrow$ consider their commutants $\mathcal{A}'$ and $\mathcal{B}'$.

Decompositions into factors and abelian subalgebras

So far: constructions + exclusions in special cases (namely, in 4 dimensions). General methods of finding non-trivial obstructions?

$\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$: *-subalgebras, not neccessarily MASAs $\Rightarrow$ consider their commutants $\mathcal{A}'$ and $\mathcal{B}'$.

$\mathcal{A}, \mathcal{B}$ quasi-orthogonal $\not\Rightarrow$ $\mathcal{A}', \mathcal{B}'$ quasi-orthogonal.

Decompositions into factors and abelian subalgebras

$E_{\mathcal{A}}, E_{\mathcal{B}}$: ortho-projections onto $\mathcal{A}$ and $\mathcal{B}$. Then $1 = \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ iff $\mathcal{A}$ and $\mathcal{B}$ are quasi-orthogonal and in general

$$1 \leq \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}}) \leq \min\{\dim(\mathcal{A}), \dim(\mathcal{B})\}.$$

Decompositions into factors and abelian subalgebras

$E_{\mathcal{A}}, E_{\mathcal{B}}$: ortho-projections onto $\mathcal{A}$ and $\mathcal{B}$. Then $1 = \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ iff $\mathcal{A}$ and $\mathcal{B}$ are quasi-orthogonal and in general

$$1 \leq \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}}) \leq \min\{\dim(\mathcal{A}), \dim(\mathcal{B})\}.$$

Connection between $\mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ and $\mathrm{Tr}(E_{\mathcal{A}'} E_{\mathcal{B}'})$?

Decompositions into factors and abelian subalgebras

$E_{\mathcal{A}}, E_{\mathcal{B}}$: ortho-projections onto $\mathcal{A}$ and $\mathcal{B}$. Then $1 = \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ iff $\mathcal{A}$ and $\mathcal{B}$ are quasi-orthogonal and in general

$$1 \leq \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}}) \leq \min\{\dim(\mathcal{A}), \dim(\mathcal{B})\}.$$

Connection between $\mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ and $\mathrm{Tr}(E_{\mathcal{A}'} E_{\mathcal{B}'})$? In general, none.

Decompositions into factors and abelian subalgebras

$E_{\mathcal{A}}, E_{\mathcal{B}}$: ortho-projections onto $\mathcal{A}$ and $\mathcal{B}$. Then $1 = \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ iff $\mathcal{A}$ and $\mathcal{B}$ are quasi-orthogonal and in general

$$1 \leq \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}}) \leq \min\{\dim(\mathcal{A}), \dim(\mathcal{B})\}.$$

Connection between $\mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ and $\mathrm{Tr}(E_{\mathcal{A}'} E_{\mathcal{B}'})$? In general, none.

Theorem (M. Weiner)

Let $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$ homogeneously ballanced *-subalgebras. Then

$$\mathrm{Tr}(E_{\mathcal{A}'} E_{\mathcal{B}'}) = \frac{n^2}{\dim(\mathcal{A})\dim(\mathcal{B})} \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}}).$$

Decompositions into factors and abelian subalgebras

$E_{\mathcal{A}}, E_{\mathcal{B}}$: ortho-projections onto $\mathcal{A}$ and $\mathcal{B}$. Then $1 = \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ iff $\mathcal{A}$ and $\mathcal{B}$ are quasi-orthogonal and in general

$$1 \leq \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}}) \leq \min\{\dim(\mathcal{A}), \dim(\mathcal{B})\}.$$

Connection between $\mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ and $\mathrm{Tr}(E_{\mathcal{A}'} E_{\mathcal{B}'})$? In general, none.

Theorem (M. Weiner)

Let $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$ homogeneously ballanced *-subalgebras. Then

$$\mathrm{Tr}(E_{\mathcal{A}'} E_{\mathcal{B}'}) = \frac{n^2}{\dim(\mathcal{A})\dim(\mathcal{B})} \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}}).$$

Applying the above theorem $\Longrightarrow$ various nontrivial obstruction.

Decompositions into factors and abelian subalgebras

$E_{\mathcal{A}}, E_{\mathcal{B}}$: ortho-projections onto $\mathcal{A}$ and $\mathcal{B}$. Then $1 = \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ iff $\mathcal{A}$ and $\mathcal{B}$ are quasi-orthogonal and in general

$$1 \leq \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}}) \leq \min\{\dim(\mathcal{A}), \dim(\mathcal{B})\}.$$

Connection between $\mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}})$ and $\mathrm{Tr}(E_{\mathcal{A}'} E_{\mathcal{B}'})$? In general, none.

Theorem (M. Weiner)

Let $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$ homogeneously ballanced *-subalgebras. Then

$$\mathrm{Tr}(E_{\mathcal{A}'} E_{\mathcal{B}'}) = \frac{n^2}{\dim(\mathcal{A})\dim(\mathcal{B})} \mathrm{Tr}(E_{\mathcal{A}} E_{\mathcal{B}}).$$

Applying the above theorem $\Longrightarrow$ various nontrivial obstruction. Can be considered a new general method.