Quantum Information Theory and pairwise quasi-orthogonal subalgebras

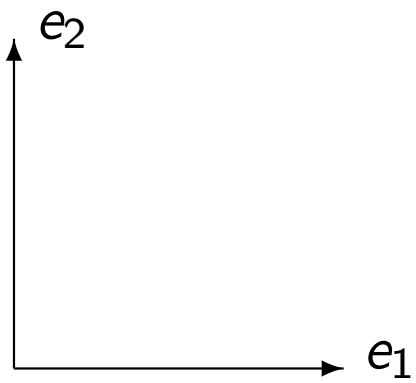
Mihály Weiner

Alfréd Rényi Institute of Mathematics, Budapest
Hungarian Academy of Sciences

October 22, 2008

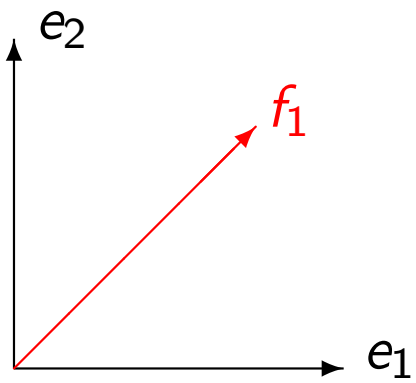
The concept of unbiased vectors and bases

Here is an ONB in two dimensions:



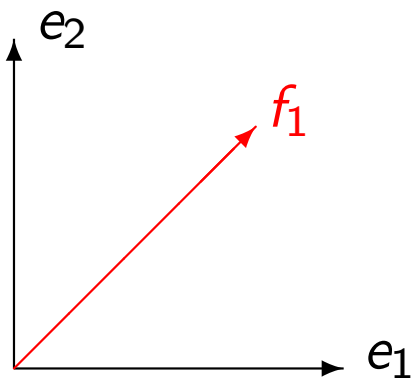
The concept of unbiased vectors and bases

Here is an ONB in two dimensions:



The concept of unbiased vectors and bases

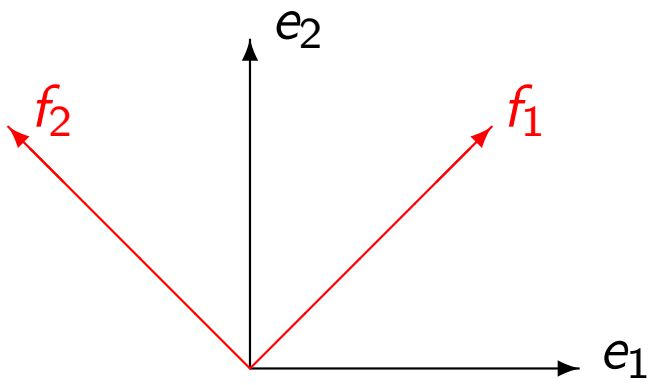
Here is an ONB in two dimensions:



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

The concept of unbiased vectors and bases

Here is an ONB in two dimensions:

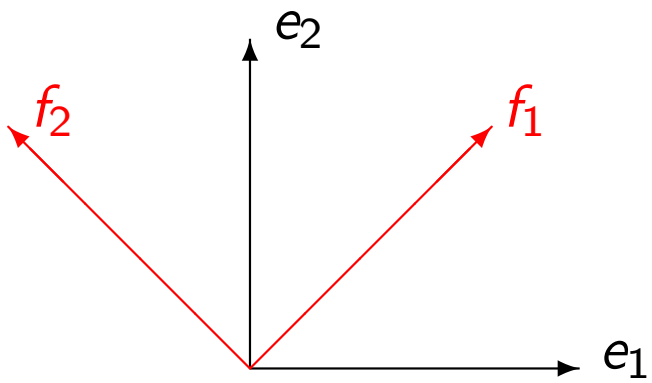


f_1 is **unbiased** for (e_1, e_2)

so is f_2

The concept of unbiased vectors and bases

Here is an ONB in two dimensions:



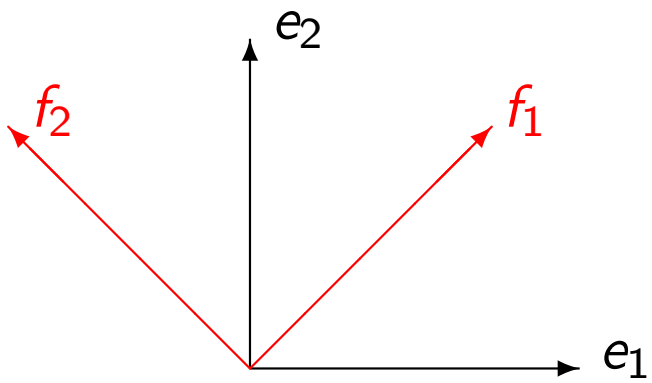
f_1 is **unbiased** for (e_1, e_2)

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)

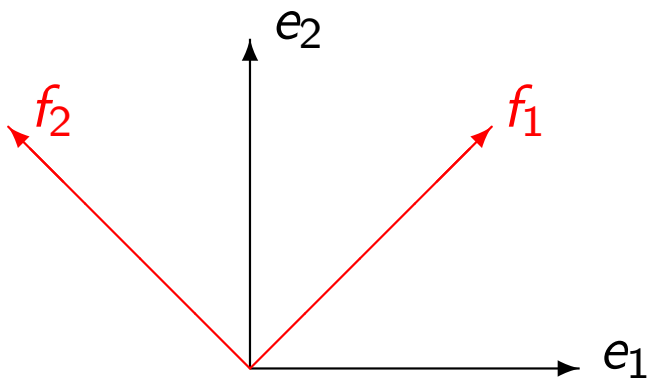
so is f_2

(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 base $\mathcal{E}$ consider the algebra of operators whose matrix is diagonal in the base $\mathcal{E}$

An equivalent description

- Instead of a base $\mathcal{E}$ consider the algebra of operators whose matrix is diagonal in the base $\mathcal{E}$
- $\mathcal{A} \subset \mathcal{B}(\mathcal{H})$ is such an algebra if and only if it is a maximal abelian C^*-subalgebra of $\mathcal{B}(\mathcal{H})$

An equivalent description

- Instead of a base $\mathcal{E}$ consider the algebra of operators whose matrix is diagonal in the base $\mathcal{E}$
- $\mathcal{A} \subset \mathcal{B}(\mathcal{H})$ is such an algebra if and only if it is a maximal abelian C^*-subalgebra of $\mathcal{B}(\mathcal{H})$
- Two maximal abelian C^*-subalgebras $\mathcal{A}, \mathcal{B} \subset \mathcal{B}(\mathcal{H})$ 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**")

$\mathcal{A}$ and $\mathcal{B}$ are statistically independent

$\mathcal{A}$ and $\mathcal{B}$ form a commuting square with trivial intersection

$\Updownarrow$

$\mathcal{A}$ and $\mathcal{B}$ are statistically independent

$\mathcal{A}$ and $\mathcal{B}$ form a commuting square with trivial intersection

$\Updownarrow$

$\mathcal{A}$ and $\mathcal{B}$ are statistically independent

$\Updownarrow$

$\mathcal{A}$ and $\mathcal{B}$ are quasi-orthogonal

Quasi-orthogonality

The formula

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

defines a scalar product (called: "Hilbert-Schmidt") on $\mathcal{B}(\mathcal{H})$.

Quasi-orthogonality

The formula

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

defines a scalar product (called: "Hilbert-Schmidt") on $\mathcal{B}(\mathcal{H})$.

- Two C^*-subalgebras $\mathcal{A}, \mathcal{B} \subset \mathcal{B}(\mathcal{H})$, 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: "Hilbert-Schmidt") on $\mathcal{B}(\mathcal{H})$.

- Two C^*-subalgebras $\mathcal{A}, \mathcal{B} \subset \mathcal{B}(\mathcal{H})$, 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: "Hilbert-Schmidt") on $\mathcal{B}(\mathcal{H})$.

- Two C^*-subalgebras $\mathcal{A}, \mathcal{B} \subset \mathcal{B}(\mathcal{H})$, 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 and quasi-orthogonality

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

So $n := \dim(\mathcal{H}) > 1$, then $\dim(\mathcal{B}(\mathcal{H})) = n^2$ and

Mutually unbiased bases and quasi-orthogonality

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

So $n := \dim(\mathcal{H}) > 1$, then $\dim(\mathcal{B}(\mathcal{H})) = n^2$ and

- dimension of the traceless part of $\mathcal{B}(\mathcal{H})$ is $n^2 - 1$

Mutually unbiased bases and quasi-orthogonality

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

So $n := \dim(\mathcal{H}) > 1$, then $\dim(\mathcal{B}(\mathcal{H})) = n^2$ and

- dimension of the traceless part of $\mathcal{B}(\mathcal{H})$ is $n^2 - 1$
- dimension of the traceless part of a maximal abelian C^*-subalgebra of $\mathcal{B}(\mathcal{H})$ is $n - 1$

Mutually unbiased bases and quasi-orthogonality

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

So $n := \dim(\mathcal{H}) > 1$, then $\dim(\mathcal{B}(\mathcal{H})) = n^2$ and

- dimension of the traceless part of $\mathcal{B}(\mathcal{H})$ is $n^2 - 1$
- dimension of the traceless part of a maximal abelian C^*-subalgebra of $\mathcal{B}(\mathcal{H})$ is $n - 1$

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

Mutually unbiased bases and quasi-orthogonality

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

So $n := \dim(\mathcal{H}) > 1$, then $\dim(\mathcal{B}(\mathcal{H})) = n^2$ and

- dimension of the traceless part of $\mathcal{B}(\mathcal{H})$ is $n^2 - 1$
- dimension of the traceless part of a maximal abelian C^*-subalgebra of $\mathcal{B}(\mathcal{H})$ is $n - 1$

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

Complete collection of MUB: the corresponding subalgebras linearly span $\mathcal{B}(\mathcal{H}) \Leftrightarrow$ 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 $N(6) = 3$

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

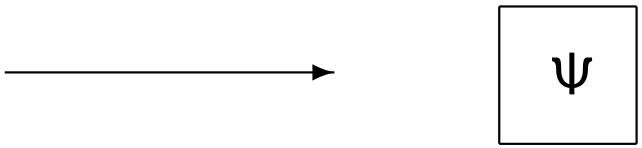
- (real-valued) physical quantity $\Leftrightarrow$ self-adjoint operator
- A and B are simultaneously measurable: $[A, B] = 0$
- best measurement: simultaneously measuring as many quantities as possible

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

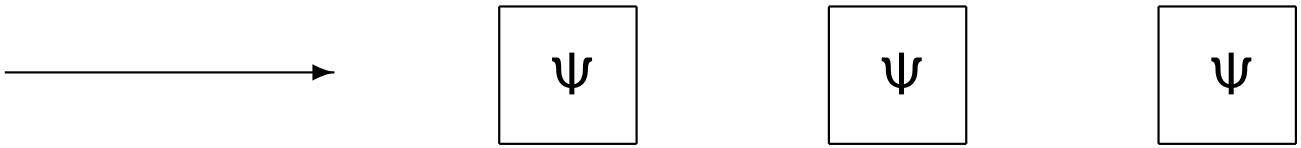
Copies of a finite-level q-system produced in the same state Ψ.

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

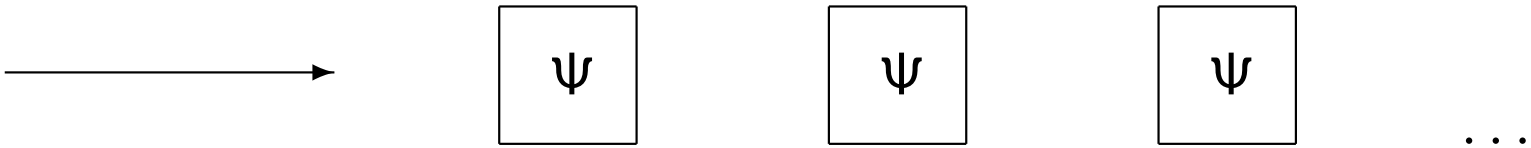


Copies of a finite-level q-system produced in the same state Ψ.

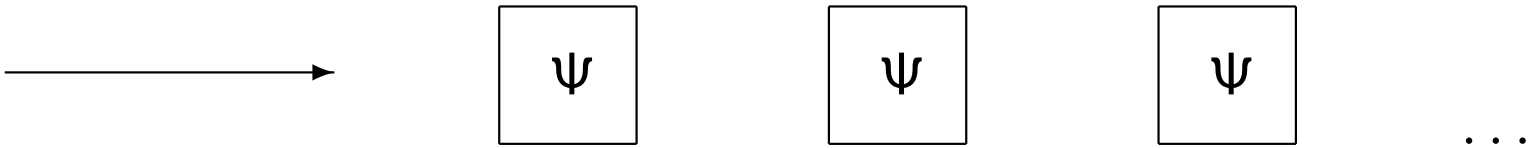
Copies of a finite-level q-system produced in the same state Ψ.



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

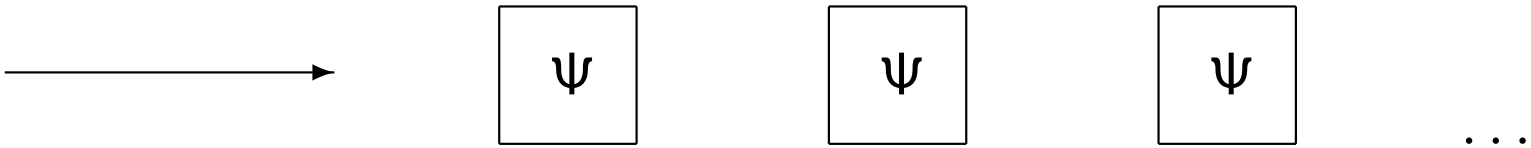


Copies of a finite-level q-system produced in the same state Ψ.



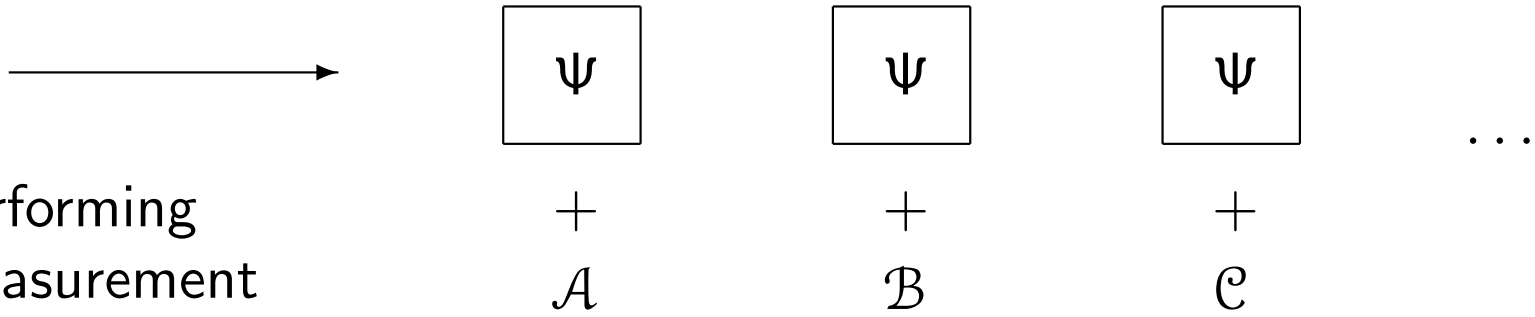
performing measurement type: $+$ $\mathcal{A}$

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

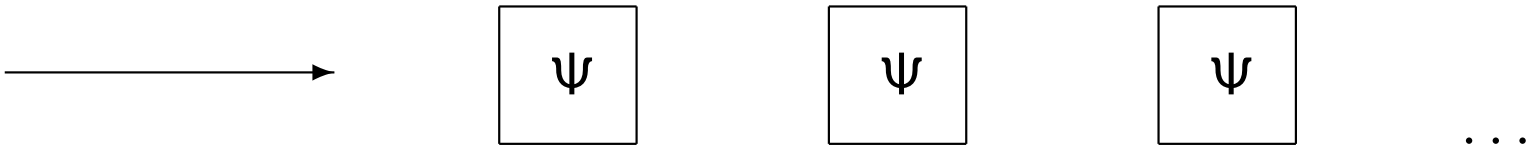


performing	+	+
measurement	$\mathcal{A}$	$\mathcal{B}$
type:		

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

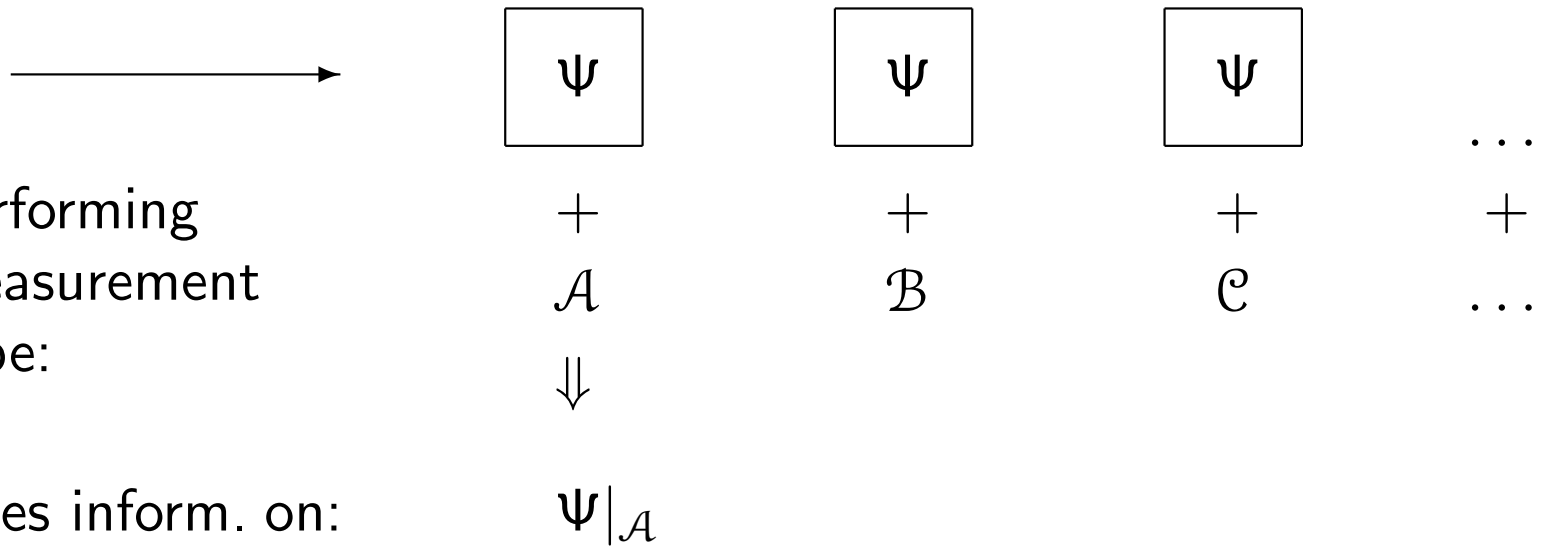


Copies of a finite-level q-system produced in the same state Ψ.

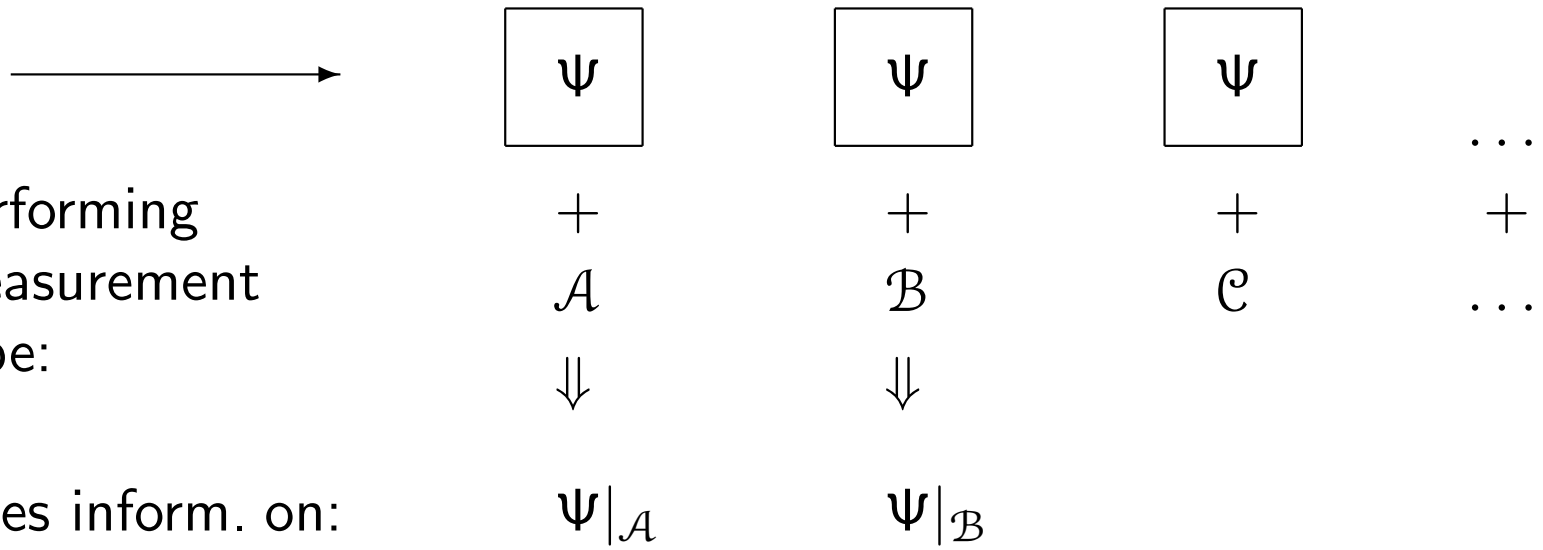


performing	+	+	+	+
measurement	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	...
type:				

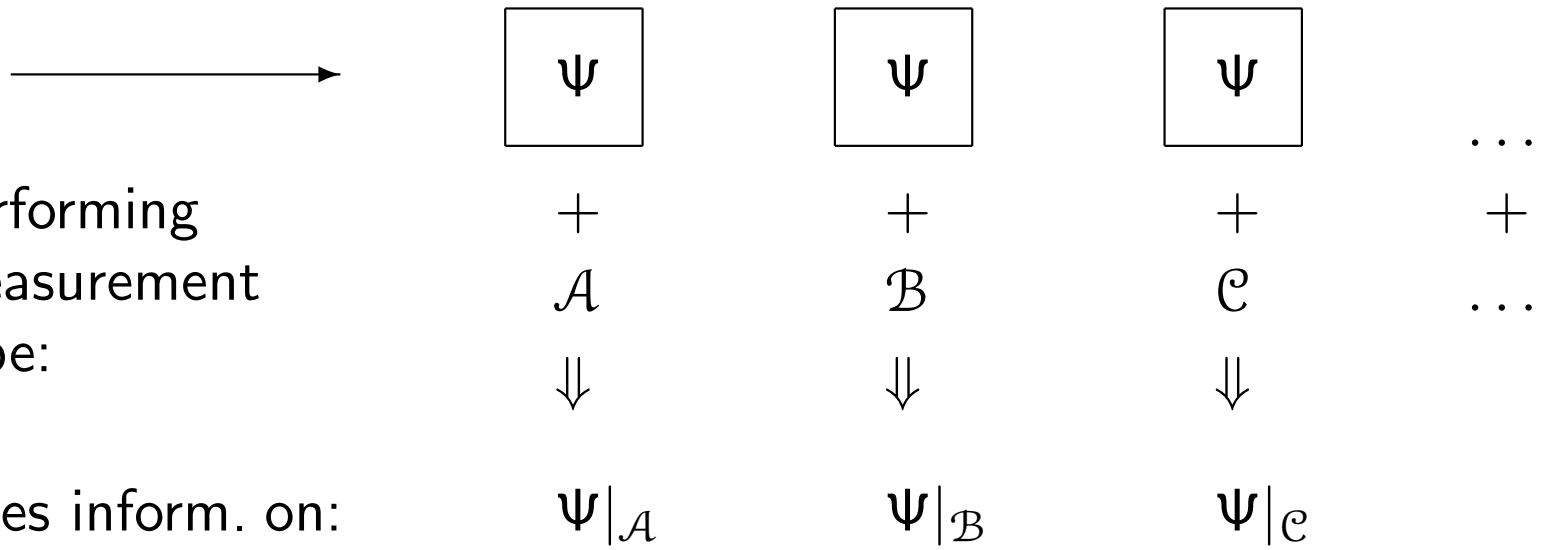
Copies of a finite-level q-system produced in the same state Ψ.



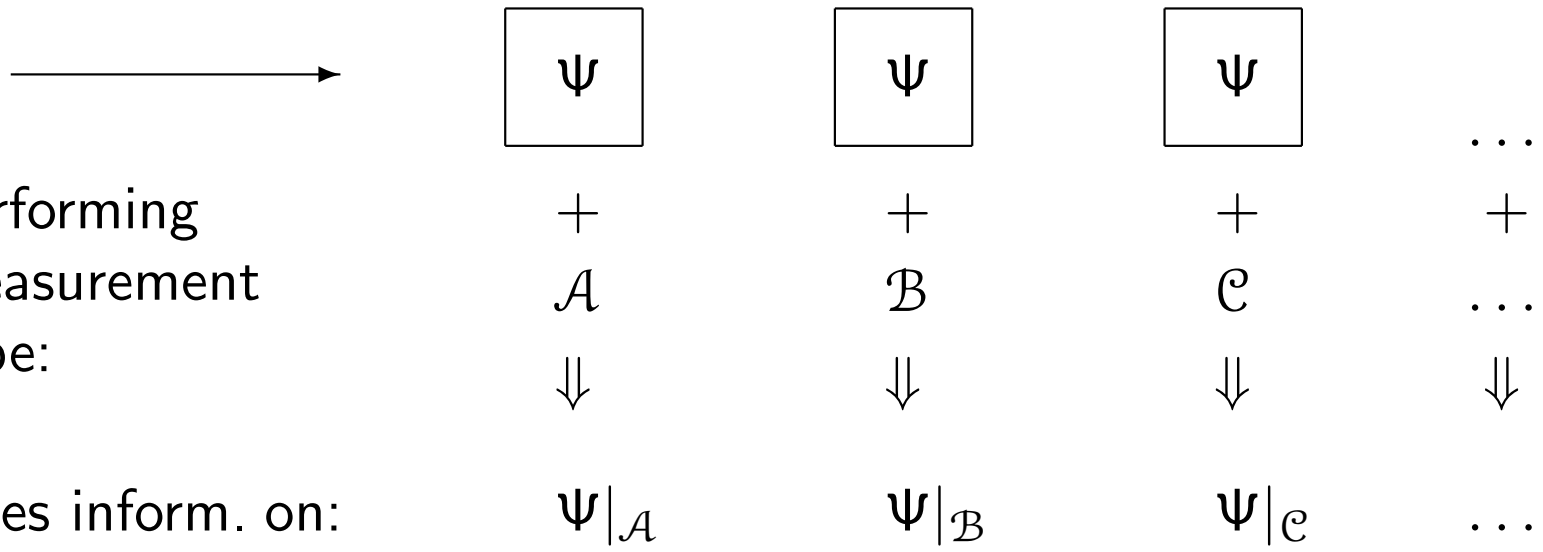
Copies of a finite-level q-system produced in the same state Ψ.



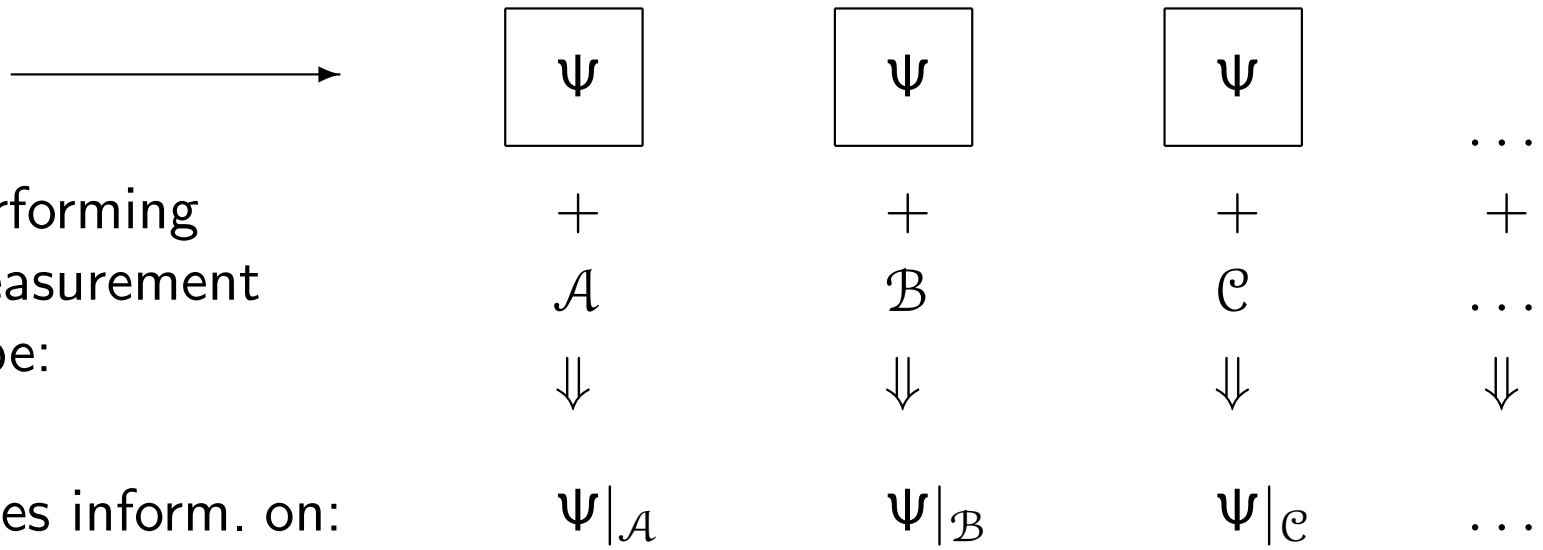
Copies of a finite-level q-system produced in the same state Ψ.



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

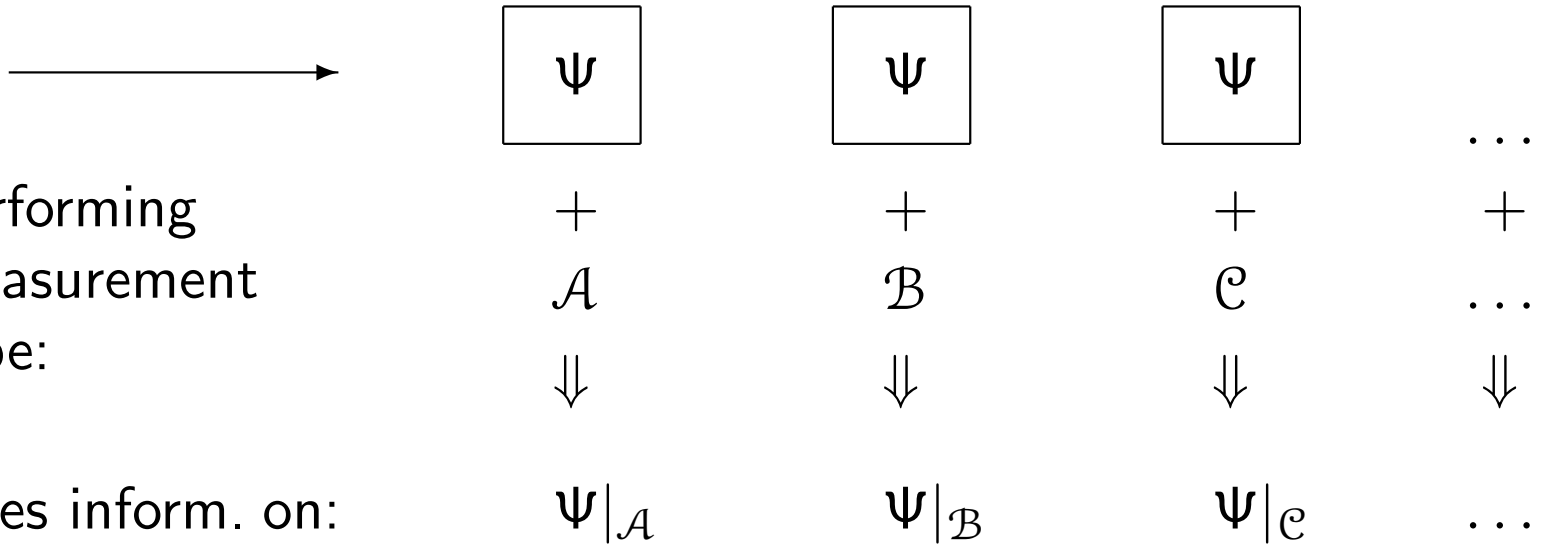


Copies of a finite-level q-system produced in the same state Ψ.



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)

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)
- a new indication: consider the problem of finding a complete set of quasi-orthogonal copies of $\mathbb{C}^n$ in $\mathbb{C}^{n^2}$

About hard problems

What do mathematicians do when facing a hard problem? They..

About hard problems

What do mathematicians do when facing a hard problem? They..

- either generalise (i.e. they create new problems)

About hard problems

What do mathematicians do when facing a hard problem? They..

- either generalise (i.e. they create new problems)
- or they relate it to other problems

About hard problems

What do mathematicians do when facing a hard problem? They..

- either generalise (i.e. they create new problems)
- or they relate it to other problems
- or they do both.

About hard problems

What do mathematicians do when facing a hard problem? They..

- either generalise (i.e. they create new problems)
- or they relate it to other problems
- or they do both.

Some even resolve some problems — but they are not the mainstream.

Non-classical measurements on a q-system

commutative C^*-subalgebra $\Leftrightarrow$ "classical" measurement
noncommutative C^*-subalgebra $\Leftrightarrow$ "non-classical" measurement.. ?

Non-classical measurements on a q-system

commutative C^*-subalgebra $\Leftrightarrow$ "classical" measurement
noncommutative C^*-subalgebra $\Leftrightarrow$ "non-classical" measurement.. ?

E.g. a q-bit is sent from one q-computer to another one:

Non-classical measurements on a q-system

commutative C^*-subalgebra $\Leftrightarrow$ "classical" measurement
noncommutative C^*-subalgebra $\Leftrightarrow$ "non-classical" measurement.. ?

E.g. a q-bit is sent from one q-computer to another one:

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

Non-classical measurements on a q-system

commutative C^*-subalgebra $\Leftrightarrow$ "classical" measurement
noncommutative C^*-subalgebra $\Leftrightarrow$ "non-classical" measurement.. ?

E.g. 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

Non-classical measurements on a q-system

commutative C^*-subalgebra $\Leftrightarrow$ "classical" measurement
noncommutative C^*-subalgebra $\Leftrightarrow$ "non-classical" measurement.. ?

E.g. 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:	$\Psi\big\vert_{(\mathbb{1} \otimes M_2(\mathbb{C}))}$

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

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

INITIAL STATE (or DATA INPUT) for each: Ψ_0

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 $\Psi_j = \Psi_0 \cdot \mathrm{Ad}(U_j)$

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 $\mathcal{A}_j = U_j(\mathbb{1} \otimes M_2(\mathbb{C}))$

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 independet

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 independet

$\Rightarrow$ study quasi-orthogonal copies of $M_2(\mathbb{C})$ in $\otimes_k M_2(\mathbb{C})$

The case of a 2 q-bits long register

$$\frac{\dim(M_2(\mathbb{C}) \otimes M_2(\mathbb{C})) - 1}{\dim(M_2(\mathbb{C})) - 1} = \frac{4^2 - 1}{2^2 - 1} = 5,$$

so by dimensional reasons, there could be quasi-orthogonal copies of $M_2(\mathbb{C})$ in $M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \simeq M_4(\mathbb{C})$. Less then 5 copies do not form a complete set.

The case of a 2 q-bits long register

$$\frac{\dim(M_2(\mathbb{C}) \otimes M_2(\mathbb{C})) - 1}{\dim(M_2(\mathbb{C})) - 1} = \frac{4^2 - 1}{2^2 - 1} = 5,$$

so by dimensional reasons, there could be quasi-orthogonal copies of $M_2(\mathbb{C})$ in $M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \simeq M_4(\mathbb{C})$. Less then 5 copies do not form a complete set.

Dénes Petz and Jonas Kahn in 2006: there is only 4 of them!

The case of a 2 q-bits long register

$$\frac{\dim(M_2(\mathbb{C}) \otimes M_2(\mathbb{C})) - 1}{\dim(M_2(\mathbb{C})) - 1} = \frac{4^2 - 1}{2^2 - 1} = 5,$$

so by dimensional reasons, there could be quasi-orthogonal copies of $M_2(\mathbb{C})$ in $M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \simeq M_4(\mathbb{C})$. Less then 5 copies do not form a complete set.

Dénes Petz and Jonas Kahn in 2006: there is only 4 of them!

Obstruction found: if $\mathcal{A}$ and $\mathcal{B}$ are quasi-orthogonal copies of $M_2(\mathbb{C})$ in $M_4(\mathbb{C})$, then

$$\mathcal{A}' \cap \mathcal{B} \neq \mathbb{C}\mathbb{1}$$

The case of a k q-bits long register

Ohno, Petz, Szánto in 2007:

The case of a k q-bits long register

Ohno, Petz, Szánto in 2007:

- construction relying on (tensor products of) Pauli-matrices $\rightsquigarrow$ show that the "defect number" is always ≤ 1

The case of a k q-bits long register

Ohno, Petz, Szánto in 2007:

- construction relying on (tensor products of) Pauli-matrices $\rightsquigarrow$ show that the "defect number" is always ≤ 1
- conjecture that it is actually 1

The case of a k q-bits long register

Ohno, Petz, Szánto in 2007:

- construction relying on (tensor products of) Pauli-matrices $\rightsquigarrow$ show that the "defect number" is always ≤ 1
- conjecture that it is actually 1
- but unless $k = 2$, they could not find an obstruction

Further questions

- q-computer with "n-level bits" sends an n-level bit, (or a "normal" q-computer sends a packet containing more than 1 bit)

Further questions

- q-computer with "n-level bits" sends an n-level bit, (or a "normal" q-computer sends a packet containing more than 1 bit) $\rightsquigarrow$ quasi-orthogonal copies of $M_n(\mathbb{C})$ in $\otimes_k M_n(\mathbb{C})$?

Further questions

- q-computer with "n-level bits" sends an n-level bit, (or a "normal" q-computer sends a packet containing more than 1 bit) $\rightsquigarrow$ quasi-orthogonal copies of $M_n(\mathbb{C})$ in $\otimes_k M_n(\mathbb{C})$?
- relationship between MUB and the new questions?

Quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$.

$n = 2$: there is already a construction. Generalisation?

Quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$.

$n = 2$: there is already a construction. Generalisation? How much is four? $4 = n^2, 2n, n + 2$..

Quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$.

$n = 2$: there is already a construction. Generalisation? How much is four? $4 = n^2, 2n, n + 2$..

a complete set would consists of $\frac{n^4-1}{n^2-1} = n^2 + 1$ copies

Quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$.

$n = 2$: there is already a construction. Generalisation? How much is four? $4 = n^2, 2n, n+2$..

a complete set would consists of $\frac{n^4-1}{n^2-1} = n^2 + 1$ copies

Proposition (First generalisation)

There exists a collection of $N(n) + 1$ quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$

Quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$.

$n = 2$: there is already a construction. Generalisation? How much is four? $4 = n^2, 2n, n + 2$..

a complete set would consists of $\frac{n^4-1}{n^2-1} = n^2 + 1$ copies

Proposition (First generalisation)

There exists a collection of $N(n) + 1$ quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$

Proposition (Second generalisation)

For $n = p$, there exists a collection of n^2 quasi-orthogonal copies of $M_n(\mathbb{C})$ in $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$.

How about the obstruction found in case of $n = 2$? Can it be generalised?

How about the obstruction found in case of $n = 2$? Can it be generalised? No, not even for $n = 3$.

How about the obstruction found in case of $n = 2$? Can it be generalised? No, not even for $n = 3$.

Example is found for $\mathcal{A}, \mathcal{B} \subset M_3(\mathbb{C}) \otimes M_3(\mathbb{C})$ two copies of $M_3(\mathbb{C})$ such that $\mathcal{A}, \mathcal{B}$ and $\mathcal{A}'$ are all quasi-orthogonal.

Constructions for $n =$ prime number

Let $e_1, \dots e_p$ an ONB, and define $X, Z \in \mathcal{B}(\mathcal{H})$ by

$$Xe_j = e_{j+1}, \quad Ze_j = e^{i\frac{2\pi}{p}j} e_j.$$

Then $XX^* = ZZ^* = X^p = Z^p = \mathbb{1}$, $ZX = e^{i\frac{2\pi}{p}} XZ$ and the unitary operators $X^\alpha Z^\beta$ where $(\alpha, \beta) \in \mathbb{F}_p^2$, form an ONB in $M_p(\mathbb{C})$.

Constructions for $n =$ prime number

Let $e_1, \dots e_p$ an ONB, and define $X, Z \in \mathcal{B}(\mathcal{H})$ by

$$Xe_j = e_{j+1}, \quad Ze_j = e^{i\frac{2\pi}{p}j} e_j.$$

Then $XX^* = ZZ^* = X^p = Z^p = \mathbb{1}$, $ZX = e^{i\frac{2\pi}{p}} XZ$ and the unitary operators $X^\alpha Z^\beta$ where $(\alpha, \beta) \in \mathbb{F}_p^2$, form an ONB in $M_p(\mathbb{C})$.

Generalisation: the unitary operators

$$W_{(\alpha,\beta)} := X^{\alpha_1} Z^{\beta_1} \otimes X^{\alpha_2} Z^{\beta_2} \otimes \dots \otimes X^{\alpha_k} Z^{\beta_k}$$

where $(\alpha, \beta) \in \mathbb{F}_p^{2k}$, form an ONB in $\otimes_k M_p(\mathbb{C})$.

With $B((\alpha,\beta),(\eta,\zeta)) := \sum_{j=1}^{k} \det \begin{pmatrix} \alpha_j & \beta_j \\ \eta_j & \zeta_j \end{pmatrix}$ bilinear form,

With $B((\alpha,\beta),(\eta,\zeta)) := \sum_{j=1}^{k} \det \begin{pmatrix} \alpha_j & \beta_j \\ \eta_j & \zeta_j \end{pmatrix}$ bilinear form,

Lemma

If $V \subset \mathbb{F}_p^{2k}$ is an $\mathbb{F}_p$-linear subspace, then

$$\mathcal{A}(V) := \mathrm{Span}\{W_{(\alpha,\beta)} \,|\, (\alpha,\beta) \in V\}$$

is a $\mathcal{C}^*$-subalgebra of $\otimes_k M_p(\mathbb{C})$ of dimension $p^{\dim(V)}$. Moreover,

With $B((\alpha,\beta),(\eta,\zeta)) := \sum_{j=1}^{k} \det \begin{pmatrix} \alpha_j & \beta_j \\ \eta_j & \zeta_j \end{pmatrix}$ bilinear form,

Lemma

If $V \subset \mathbb{F}_p^{2k}$ is an $\mathbb{F}_p$-linear subspace, then

$$\mathcal{A}(V) := \mathrm{Span}\{W_{(\alpha,\beta)} \,|\, (\alpha,\beta) \in V\}$$

is a $\mathcal{C}^*$-subalgebra of $\otimes_k M_p(\mathbb{C})$ of dimension $p^{\dim(V)}$. Moreover,

- $\mathcal{A}(V)$ is Abelian iff $B|_{V\times V} = 0$,

With $B((\alpha,\beta),(\eta,\zeta)) := \sum_{j=1}^{k} \det \begin{pmatrix} \alpha_j & \beta_j \\ \eta_j & \zeta_j \end{pmatrix}$ bilinear form,

Lemma

If $V \subset \mathbb{F}_p^{2k}$ is an $\mathbb{F}_p$-linear subspace, then

$$\mathcal{A}(V) := \mathrm{Span}\{W_{(\alpha,\beta)} \,|\, (\alpha,\beta) \in V\}$$

is a $\mathcal{C}^*$-subalgebra of $\otimes_k M_p(\mathbb{C})$ of dimension $p^{\dim(V)}$. Moreover,

- $\mathcal{A}(V)$ is Abelian iff $B|_{V\times V} = 0$,
- $\mathcal{A}(V_1)$ is quasi-orthogonal to $\mathcal{A}(V_2)$ iff $V_1 \cap V_2 = \{0\}$,

With $B((\alpha,\beta),(\eta,\zeta)) := \sum_{j=1}^{k} \det \begin{pmatrix} \alpha_j & \beta_j \\ \eta_j & \zeta_j \end{pmatrix}$ bilinear form,

Lemma

If $V \subset \mathbb{F}_p^{2k}$ is an $\mathbb{F}_p$-linear subspace, then

$$\mathcal{A}(V) := \mathrm{Span}\{W_{(\alpha,\beta)} \,|\, (\alpha,\beta) \in V\}$$

is a $\mathcal{C}^*$-subalgebra of $\otimes_k M_p(\mathbb{C})$ of dimension $p^{\dim(V)}$. Moreover,

- $\mathcal{A}(V)$ is Abelian iff $B|_{V\times V} = 0$,
- $\mathcal{A}(V_1)$ is quasi-orthogonal to $\mathcal{A}(V_2)$ iff $V_1 \cap V_2 = \{0\}$,
- $\mathcal{A}(V) \simeq M_p(\mathbb{C})$ iff $\dim(V) = 2$ and $B|_{V\times V} \neq 0$

studying 2-dimensional subspaces of the symplectic space $(\mathbb{F}_p^{2k}, B)$

studying 2-dimensional subspaces of the symplectic space $(\mathbb{F}_p^{2k}, B)$

$$\Downarrow$$

finding quasi-orthogonal copies of $M_p(\mathbb{C})$ in $\otimes_k M_p(\mathbb{C})$

studying 2-dimensional subspaces of the symplectic space $(\mathbb{F}_p^{2k}, B)$

$$\Downarrow$$

finding quasi-orthogonal copies of $M_p(\mathbb{C})$ in $\otimes_k M_p(\mathbb{C})$

So the problem is reduced to finite geometry. (This is how that "second generalisation" was also obtained.) Further results:

studying 2-dimensional subspaces of the symplectic space $(\mathbb{F}_p^{2k}, B)$

$$\Downarrow$$

finding quasi-orthogonal copies of $M_p(\mathbb{C})$ in $\otimes_k M_p(\mathbb{C})$

So the problem is reduced to finite geometry. (This is how that "second generalisation" was also obtained.) Further results:

Proposition

The "deficit number" of $M_3(\mathbb{C})$ in $\otimes_k M_3(\mathbb{C})$ is ≤ 1.