Introduction to Quantum Information Theory II

Open Problems

Quantum Physics

[Submitted on 8 Feb 2020 (v1), last revised 21 Dec 2020 (this version, v2)]

Five open problems in quantum information

Paweł Horodecki, Łukasz Rudnicki, Karol Życzkowski

We identify five selected open problems in the theory of quantum information, which are rather simple to formulate, were well-studied in the literature, but are technically not easy. As these problems enjoy diverse mathematical connections, they offer a huge breakthrough potential. The first four concern existence of certain objects relevant for quantum information, namely a family of symmetric informationally complete generalized measurements in an infinite sequence of dimensions, mutually unbiased bases in dimension six, absolutely maximally entangled states for four subsystems with six levels each and bound entangled states with negative partial transpose. The fifth problem requires checking whether a certain state of a two-ququart system is 2-copy distillable. An award for solving each of them is announced.

Subjects: **Quantum Physics (quant-ph)**

Cite as: arXiv:2002.03233 **[quant-ph]**

(or arXiv:2002.03233v2 **[quant-ph]** for this version)

https://doi.org/10.48550/arXiv.2002.03233

Quantum Physics

[Submitted on 8 Feb 2020 (v1), last revised 21 Dec 2020 (this version, v2)]

Five open problems in quantum information

A. Existence of SIC POVMs

Problem 1: *Construct SIC POVMs in an infinite sequence of dimensions,* $N_1, N_2, N_3, \ldots$

B. MUBs in dimension six

Problem 2: *Construct a set of at least 4 mutually unbiased bases in dimension six or prove that there are no 7 MUBs in* $\mathcal{H}_6$.

C. Quantum Orthogonal Latin Squares

Problem 3: *Determine whether there exist two quantum orthogonal Latin squares [77, 78] of order six. In other words, find a solution of the problem of 36 'entangled officers' of Euler or demonstrate that it does not exist.*

arXiv > quant-ph > arXiv:2002.03233

Search...

Help | Advance

Quantum Physics

[Submitted on 8 Feb 2020 (v1), last revised 21 Dec 2020 (this version, v2)]

Five open problems in quantum information

A. Existence of SIC POVMs

Problem 1: *Construct SIC POVMs in an infinite sequence of dimensions, $N_1, N_2, N_3, \dots$*

B. MUBs in dimension six

Problem 2: *Construct a set of at least 4 mutually unbiased bases in dimension six or prove that there are no 7 MUBs in $\mathcal{H}_6$.*

C. Quantum Orthogonal Latin Squares

Problem 3: *Determine whether there exist two quantum orthogonal Latin squares [77, 78] of order six. In other words, find a solution of the problem of 36 'entangled officers' of Euler or demonstrate that it does not exist.*

- Quantum states: $|v\rangle \in \mathbb{C}^d$ such that $\| |v\rangle \| = 1$ and $|v\rangle \sim \mathrm{e}^{i\theta} |v\rangle$.
- Measurement: orthonormal basis $|1\rangle, \ldots, |d\rangle$.
- If

$$|v\rangle = \sum_{j=1}^{d} \alpha_j |j\rangle \quad \text{where } \alpha_j \in \mathbb{C} \text{ with } \sum_j |\alpha_j|^2 = 1,$$

  then the probability of observing the outcome j is $|\alpha_j|^2$.

- Quantum states: $|v\rangle \in \mathbb{C}^d$ such that $\| \, |v\rangle \, \| = 1$ and $|v\rangle \sim \mathrm{e}^{i\theta} |v\rangle$.
- Measurement: orthonormal basis $|1\rangle, \ldots, |d\rangle$.
- If
$$|v\rangle = \sum_{j=1}^{d} \alpha_j |j\rangle \quad \text{where } \alpha_j \in \mathbb{C} \text{ with } \sum_j |\alpha_j|^2 = 1,$$
then the probability of observing the outcome j is $|\alpha_j|^2$.

Example. Let $|1\rangle, |2\rangle$ be any orthonormal basis of $\mathbb{C}^2$. For the state $|\blacksquare\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$ the probabilities of the results 1 and 2 are $50\%, 50\%$.

Same for the states $|\blacktriangle\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$ and $|\heartsuit\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle)$.

Observe that $|\blacksquare\rangle, |\blacktriangle\rangle$ is another orthonormal basis $\sim$ measurement.

- Quantum states: $|v\rangle \in \mathbb{C}^d$ such that $\| |v\rangle \| = 1$ and $|v\rangle \sim \mathrm{e}^{i\theta} |v\rangle$.
- Measurement: orthonormal basis $|1\rangle, \dots, |d\rangle$.
- If
$$|v\rangle = \sum_{j=1}^{d} \alpha_j |j\rangle \quad \text{where } \alpha_j \in \mathbb{C} \text{ with } \sum_j |\alpha_j|^2 = 1,$$
then the probability of observing the outcome j is $|\alpha_j|^2$.

Example. Let $|1\rangle, |2\rangle$ be any orthonormal basis of $\mathbb{C}^2$. For the state $|\blacksquare\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$ the probabilities of the results 1 and 2 are 50%, 50%.

Same for the states $|\blacktriangle\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$ and $|\heartsuit\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle)$.

Observe that $|\blacksquare\rangle, |\blacktriangle\rangle$ is another orthonormal basis ~ measurement.

$$|1\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \quad |2\rangle = \begin{bmatrix}0\\1\end{bmatrix}, \quad |\blacksquare\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \quad |\blacktriangle\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}, \quad |\heartsuit\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}$$

- Quantum states: $|v\rangle \in \mathbb{C}^d$ such that $\| |v\rangle \| = 1$ and $|v\rangle \sim e^{i\theta} |v\rangle$.
- Measurement: orthonormal basis $|1\rangle, \dots, |d\rangle$.
- If
$$|v\rangle = \sum_{j=1}^{d} \alpha_j |j\rangle \quad \text{where } \alpha_j \in \mathbb{C} \text{ with } \sum_j |\alpha_j|^2 = 1,$$
then the probability of observing the outcome j is $|\alpha_j|^2$.

Example. Let $|1\rangle, |2\rangle$ be any orthonormal basis of $\mathbb{C}^2$. For the state $|\blacksquare\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$ the probabilities of the results 1 and 2 are $50\%, 50\%$.

Same for the states $|\blacktriangle\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$ and $|\heartsuit\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle)$.

Observe that $|\blacksquare\rangle, |\blacktriangle\rangle$ is another orthonormal basis $\sim$ measurement.

- For $|\blacksquare\rangle$ the probabilities of the results $\blacksquare$ and $\blacktriangle$ are $100\%, 0\%$.
- For $|\heartsuit\rangle$ and $|1\rangle$ the probabilities of the results $\blacksquare$ and $\blacktriangle$ are $50\%, 50\%$.

- Quantum states: $|v\rangle \in \mathbb{C}^d$ such that $\| |v\rangle \| = 1$ and $|v\rangle \sim e^{i\theta} |v\rangle$.
- Measurement: orthonormal basis $|1\rangle, \ldots, |d\rangle$.
- If

$$|v\rangle = \sum_{j=1}^{d} \alpha_j |j\rangle \quad \text{where } \alpha_j \in \mathbb{C} \text{ with } \sum_j |\alpha_j|^2 = 1,$$

  then the probability of observing the outcome j is $|\alpha_j|^2$.

Example. Let $|1\rangle, |2\rangle$ be any orthonormal basis of $\mathbb{C}^2$. For the state $|\blacksquare\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$ the probabilities of the results 1 and 2 are $50\%, 50\%$.

Same for the states $|\blacktriangle\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$ and $|\heartsuit\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle)$.

Observe that $|\blacksquare\rangle, |\blacktriangle\rangle$ is another orthonormal basis $\sim$ measurement.

- For $|\blacksquare\rangle$ the probabilities of the results $\blacksquare$ and $\blacktriangle$ are $100\%, 0\%$.
- For $|\heartsuit\rangle$ and $|1\rangle$ the probabilities of the results $\blacksquare$ and $\blacktriangle$ are $50\%, 50\%$.

Quantum Tomography: reconstructing a state based on the outcomes of a series of measurements (on an ensemble of state copies).

MUBs

Let $\mathcal{B}_1 = \{e_1, \ldots, e_d\}$ and $\mathcal{B}_2 = \{f_1, \ldots, f_d\}$ be two orthonormal bases of $\mathbb{C}^d$. We say that $\mathcal{B}_1$ and $\mathcal{B}_2$ are **mutually unbiased bases** (MUBs) if

$$|\langle e_i, f_j \rangle|^2 = \frac{1}{d} \quad \text{for all } i, j \in \{1, \ldots, d\}$$

If a system is prepared in a state belonging to one of the bases, all outcomes of the measurement with respect to the other basis are equally likely.

Example. Three MUBs in $\mathbb{C}^2$:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \qquad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix}$$

Why? Maximal sets of $d+1$ MUBs are optimal projective measurements for quantum state tomography. Plus various applications in quantum computing (error correction, teleportation, entanglement detection).

MUBs - what we know

$$N_{MUB}(d) := \text{the maximal number of MUBs in } \mathbb{C}^d.$$

- $N_{MUB}(d) \leq d + 1$ [Wootters & Field 1989]
- $N_{MUB}(d) = d + 1$ if d is prime or a prime power [Ivanovic 1981, W&F 1989]
- If $d = p_1^{k_1} \cdots p_n^{k_n}$, where $p_1, \ldots, p_n$ are distinct primes, and $p_1^{k_1} < \ldots < p_n^{k_n}$, then $N_{MUB}(d) \geq N_{MUB}(p_1^{k_1}) = p_1^{k_1} + 1$
    - $N_{MUB}(d) \geq 3$ for all d and $M(d) \geq 4$ if d is odd
    - $N_{MUB}(d) > N_{MUB}(p_1^{k_1})$ in infinitely many dimensions [Wocjan & Beth 2005]
- $N_{MUB}(d^2) \geq d^{1/14.8}$ for almost all square dimensions. [W&B 2005]
- If $N_{MUB}(d) \geq d$, then $N_{MUB}(d) = d + 1$. [Weiner 2013] *"Last one is for free"*

MUBs - what we know

$$N_{MUB}(d) := \text{the maximal number of MUBs in } \mathbb{C}^d.$$

- $N_{MUB}(d) \leq d+1$ [Wootters & Field 1989]
- $N_{MUB}(d) = d+1$ if d is prime or a prime power [Ivanovic 1981, W&F 1989]
- If $d = p_1^{k_1} \cdots p_n^{k_n}$, where $p_1, \ldots, p_n$ are distinct primes, and $p_1^{k_1} < \ldots < p_n^{k_n}$, then $N_{MUB}(d) \geq N_{MUB}(p_1^{k_1}) = p_1^{k_1} + 1$
    - $N_{MUB}(d) \geq 3$ for all d and $M(d) \geq 4$ if d is odd
    - $N_{MUB}(d) > N_{MUB}(p_1^{k_1})$ in infinitely many dimensions [Wocjan & Beth 2005]
- $N_{MUB}(d^2) \geq d^{1/14.8}$ for almost all square dimensions. [W&B 2005]
- If $N_{MUB}(d) \geq d$, then $N_{MUB}(d) = d+1$. [Weiner 2013] *"Last one is for free"*

Problem 2: *Construct a set of at least 4 mutually unbiased bases in dimension six or prove that there are no 7 MUBs in $\mathcal{H}_6$.*

MUBs - what we know

Example. The three MUBs in $\mathbb{C}^2$

$$\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix} \qquad \tfrac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix},\tfrac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \qquad \tfrac{1}{\sqrt{2}}\begin{bmatrix}1\\\mathrm{i}\end{bmatrix},\tfrac{1}{\sqrt{2}}\begin{bmatrix}1\\-\mathrm{i}\end{bmatrix}$$

are the eigenvectors of the three Pauli matrices

$$Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix} \qquad X=\begin{pmatrix}0&1\\1&0\end{pmatrix} \qquad Y=\mathrm{i}XZ=\begin{pmatrix}0&-\mathrm{i}\\\mathrm{i}&0\end{pmatrix}$$

Theorem. Fix a basis $e_1,\ldots,e_d$ of $\mathbb{C}^d$ and define the operators X and Z as

$$Xe_j=e_{j+1} \quad\text{and}\quad Ze_j=\omega^j e_j$$

where $\omega:=\exp(2\pi\mathrm{i}/d)$ for $j=1,\ldots d$. If d is prime, then the eigenbases of $Z,X,XZ,\ldots XZ^{d-1}$ form a complete set of MUBs.

MUBs - what we (don't) know

- In every dimension X, Z, XZ give a set of three MUBs.
- In every odd dimension X, Z, XZ, XZ^{d-1} give a set of four MUBs.
- **Conjecture**: in even dimensions X, Z, XZ give a (strongly) unextendible set of three MUBs. Confirmed for $d \leq 12$, in particular for $d = 6$.
- If we start from the eigenbases of X, Z:
  - in dim 6 they can be extended to three MUBs at most
  - in dim 7 there are 532 unbiased vectors, which form 146 bases. Among them we find $XZ, \ldots, XZ^6$. Each of the remaining 140 bases gives a (strongly) unextendible set of three MUBs.
- **Zauner's Conjecture**: There are no more than 3 MUBs in dim 6.

Problem 2: *Construct a set of at least 4 mutually unbiased bases in dimension six or prove that there are no 7 MUBs in $\mathcal{H}_6$.*

Latin Squares

Latin Square is a $d \times d$ array with coefficients $1, \ldots, d$ such that each row and each column contains all the coefficients.

Two Latin Squares are **Orthogonal** (OLS) if by superimposing them we get an array where every ordered pair of symbols appears exactly once.

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

Latin Squares

Latin Square is a $d \times d$ array with coefficients $1, \ldots, d$ such that each row and each column contains all the coefficients.

Two Latin Squares are **Orthogonal** (OLS) if by superimposing them we get an array where every ordered pair of symbols appears exactly once.

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \quad \begin{bmatrix} (1,2) & (2,1) \\ (2,1) & (1,2) \end{bmatrix} \leftarrow \text{BAD :(}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \quad \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix} \leftarrow \text{GOOD!}$$

So there are no OLS of size 2. There is at least one pair of OLS of size 3.

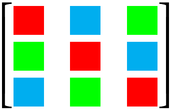
Latin Squares

Latin Square is a $d \times d$ array with coefficients $1, \ldots, d$ such that each row and each column contains all the coefficients.

Two Latin Squares are **Orthogonal** (OLS) if by superimposing them we get an array where every ordered pair of symbols appears exactly once.

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \qquad \begin{bmatrix} (1,2) & (2,1) \\ (2,1) & (1,2) \end{bmatrix} \leftarrow \text{BAD :(}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$



$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \leftarrow \text{GOOD!}$$

So there are no OLS of size 2. There is at least one pair of OLS of size 3.

Latin Squares

Latin Square is a $d \times d$ array with coefficients $1, \ldots, d$ such that each row and each column contains all the coefficients.

Two Latin Squares are **Orthogonal** (OLS) if by superimposing them we get an array where every ordered pair of symbols appears exactly once.

36 officers of Euler

Six army regiments each have six officers of six different ranks.

The Emperor (Joseph II?) was to visit a garrison town (St. Petersburg?). The commanding general wanted to arrange 36 officers in a square, so that, whichever row or column the Emperor walked along, he would meet one officer of each of the six ranks and one from each of the six regiments.

Can the 36 officers be arranged in a 6-by-6 square so that no row or column repeats a rank or regiment?

36 officers of Euler

Euler's Problem: Do there exist OLS of size 6?

After we have put a lot of thought into finding a solution, we have to admit that such an arrangement is impossible, though we can't give a rigorous demonstration of this. (Euler 1782)

36 officers of Euler

Euler's Problem: Do there exist OLS of size 6?

After we have put a lot of thought into finding a solution, we have to admit that such an arrangement is impossible, though we can't give a rigorous demonstration of this. (Euler 1782)

- Euler: At least two OLS exist for all odd d and all d divisible by 4. Conjecture: No OLS exist if $d = 2 \mod 4$.

36 officers of Euler

Euler's Problem: Do there exist OLS of size 6?

After we have put a lot of thought into finding a solution, we have to admit that such an arrangement is impossible, though we can't give a rigorous demonstration of this. (Euler 1782)

- Euler: At least two OLS exist for all odd d and all d divisible by 4. Conjecture: No OLS exist if $d = 2 \mod 4$.
- Theorem: No OLS exist for $d = 6$. [Tarry 1901]

36 officers of Euler

Euler's Problem: Do there exist OLS of size 6?

After we have put a lot of thought into finding a solution, we have to admit that such an arrangement is impossible, though we can't give a rigorous demonstration of this. (Euler 1782)

- Euler: At least two OLS exist for all odd d and all d divisible by 4. Conjecture: No OLS exist if $d = 2 \mod 4$.
- Theorem: No OLS exist for $d = 6$. [Tarry 1901]
- Theorem: Two OLS **do exist** for all sizes except 2 and 6, i.e., Euler's conjecture is (mostly) false. [Bose, Shrikhande, Parker 1960] ← *Euler's spoilers*

OLS and MUB are *strangely* similar

$N_{OLS}(d) :=$ the maximal number of OLS of size d.

- $N_{OLS}(d) \leq d-1$ for all d.
- $N_{OLS}(d) = d-1$ if d is prime or prime power.
- If $d = p_1^{k_1} \cdots p_n^{k_n}$, where $p_1, \ldots, p_n$ are distinct primes, and $p_1^{k_1} < \ldots < p_n^{k_n}$, then $N_{OLS}(d) \geq N_{OLS}(p_1^{k_1}) = p_1^{k_1} - 1$. (MacNeish's Theorem)
- $N_{OLS}(d) \geq d^{1/14.8}$ for d large enough
- If $N_{OLS}(d) = d-2$, then $N_{OLS}(d) = d-1$ (*"Last one is for free"*)

OLS and MUB are *strangely* similar

$$N_{OLS}(d) := \text{the maximal number of OLS of size } d.$$

- $N_{OLS}(d) \leq d - 1$ for all d.
- $N_{OLS}(d) = d - 1$ if d is prime or prime power.
- If $d = p_1^{k_1} \cdots p_n^{k_n}$, where $p_1, \ldots, p_n$ are distinct primes, and $p_1^{k_1} < \ldots < p_n^{k_n}$, then $N_{OLS}(d) \geq N_{OLS}(p_1^{k_1}) = p_1^{k_1} - 1$. (MacNeish's Theorem)
- $N_{OLS}(d) \geq d^{1/14.8}$ for d large enough
- If $N_{OLS}(d) = d - 2$, then $N_{OLS}(d) = d - 1$ (*"Last one is for free"*)
- If $N_{OLS}(d) = k$, then $N_{MUB}(d^2) = k + 2$.
- $N_{OLS}(6) = 1 \overset{???}{\Longrightarrow} N_{MUB}(6) = 3$

Quantization

	Elements	Rule
Classical	symbols $1, \ldots, d$	don't repeat symbols
Quantum	unit vectors in $\mathbb{C}^d$	build orthonormal bases

A **quantum Latin square** of order d is a $d \times d$ array of vectors from $\mathbb{C}^d$ such that each row and each column is an orthonormal basis.

Quantum orthogonal Latin square: pair of tensored quantum Latin squares such that all the elements form an orthonomal basis in $\mathbb{C}^d \otimes \mathbb{C}^d$.

Quantization

	Elements	Rule
Classical	symbols $1, \ldots, d$	don't repeat symbols
Quantum	unit vectors in $\mathbb{C}^d$	build orthonormal bases

A **quantum Latin square** of order d is a $d \times d$ array of vectors from $\mathbb{C}^d$ such that each row and each column is an orthonormal basis.

Quantum orthogonal Latin square: pair of tensored quantum Latin squares such that all the elements form an orthonomal basis in $\mathbb{C}^d \otimes \mathbb{C}^d$.

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

$$\begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}$$

Quantization

	Elements	Rule
Classical	symbols $1, \ldots, d$	don't repeat symbols
Quantum	unit vectors in $\mathbb{C}^d$	build orthonormal bases

A **quantum Latin square** of order d is a $d \times d$ array of vectors from $\mathbb{C}^d$ such that each row and each column is an orthonormal basis.

Quantum orthogonal Latin square: pair of tensored quantum Latin squares such that all the elements form an orthonomal basis in $\mathbb{C}^d \otimes \mathbb{C}^d$.

$$\begin{bmatrix} |1\rangle & |2\rangle & |3\rangle \\ |2\rangle & |3\rangle & |1\rangle \\ |3\rangle & |1\rangle & |2\rangle \end{bmatrix} \begin{bmatrix} |1\rangle & |2\rangle & |3\rangle \\ |3\rangle & |1\rangle & |2\rangle \\ |2\rangle & |3\rangle & |1\rangle \end{bmatrix}$$

$$\begin{bmatrix} |11\rangle & |22\rangle & |33\rangle \\ |23\rangle & |31\rangle & |12\rangle \\ |32\rangle & |13\rangle & |21\rangle \end{bmatrix}$$

Quantization

	Elements	Rule
Classical	symbols $1, \ldots, d$	don't repeat symbols
Quantum	unit vectors in $\mathbb{C}^d$	build orthonormal bases

A **quantum Latin square** of order d is a $d \times d$ array of vectors from $\mathbb{C}^d$ such that each row and each column is an orthonormal basis.

Quantum orthogonal Latin square: pair of tensored quantum Latin squares such that all the elements form an orthonomal basis in $\mathbb{C}^d \otimes \mathbb{C}^d$.

$$\begin{bmatrix} |1\rangle & |2\rangle & |3\rangle \\ |3\rangle & |1\rangle & |2\rangle \\ |2\rangle & |3\rangle & |1\rangle \end{bmatrix} \quad \begin{bmatrix} \frac{\sqrt{3}}{2}|1\rangle + \frac{1}{2}|3\rangle & -\frac{1}{2}|1\rangle + \frac{\sqrt{3}}{2}|3\rangle & |2\rangle \\ \frac{1}{2}|1\rangle - \frac{\sqrt{3}}{2}|3\rangle & |2\rangle & \frac{\sqrt{3}}{2}|1\rangle + \frac{1}{2}|3\rangle \\ |2\rangle & \frac{\sqrt{3}}{2}|1\rangle + \frac{1}{2}|3\rangle & -\frac{1}{2}|1\rangle + \frac{\sqrt{3}}{2}|3\rangle \end{bmatrix}$$

$$\begin{bmatrix} \frac{\sqrt{3}}{2}|11\rangle + \frac{1}{2}|13\rangle & -\frac{1}{2}|21\rangle + \frac{\sqrt{3}}{2}|23\rangle & |32\rangle \\ \frac{1}{2}|31\rangle - \frac{\sqrt{3}}{2}|33\rangle & |12\rangle & \frac{\sqrt{3}}{2}|21\rangle + \frac{1}{2}|23\rangle \\ |22\rangle & \frac{\sqrt{3}}{2}|31\rangle + \frac{1}{2}|33\rangle & -\frac{1}{2}|11\rangle + \frac{\sqrt{3}}{2}|13\rangle \end{bmatrix}$$

Quantization

	Elements	Rule
Classical	symbols $1, \ldots, d$	don't repeat symbols
Quantum	unit vectors in $\mathbb{C}^d$	build orthonormal bases

A **quantum Latin square** of order d is a $d \times d$ array of vectors from $\mathbb{C}^d$ such that each row and each column is an orthonormal basis.

Quantum orthogonal Latin square: pair of tensored quantum Latin squares such that all the elements form an orthonomal basis in $\mathbb{C}^d \otimes \mathbb{C}^d$.

Classical OLS of size d → Quantum OLS of size d

Problem 3: *Determine whether there exist two quantum orthogonal Latin squares [77, 78] of order six. In other words, find a solution of the problem of 36 'entangled officers' of Euler or demonstrate that it does not exist.*

AME(N,d) state *(Absolutely Maximally Entangled)*

AME(4,6): 4 subsystems, each of dim 6.

System consisting of 4 "quantum dice" (qu-hexes) such that any pair of dice is unbiased, but their outcome determines the state of the other two dice.

Why? quantum teleportation, entanglement swapping, quantum secret sharing, error-correcting codes

- Quantum OLS of size d → AME(4,d).

36 Entangled Officers of Euler

AME(N,d) state *(Absolutely Maximally Entangled)*

AME(4,6): 4 subsystems, each of dim 6.

System consisting of 4 "quantum dice" (qu-hexes) such that any pair of dice is unbiased, but their outcome determines the state of the other two dice.

Why? quantum teleportation, entanglement swapping, quantum secret sharing, error-correcting codes

- Quantum OLS of size d → AME(4,d).
- Classical OLS of size d → AME(4,d) for every $d \neq 2$ and $d \neq 6$.
- AME(4,2) does not exists [Higuchi, Sudbery 2000]. AME(4,6) is open.
- ~~Classical OLS of size 6~~ → Quantum OLS of size 6 → AME(4,6)

AME(N,d) state *(Absolutely Maximally Entangled)*

AME(4,6): 4 subsystems, each of dim 6.

System consisting of 4 "quantum dice" (qu-hexes) such that any pair of dice is unbiased, but their outcome determines the state of the other two dice.

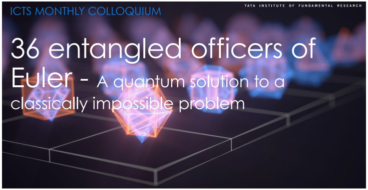
Why? quantum teleportation, entanglement swapping, quantum secret sharing, error-correcting codes

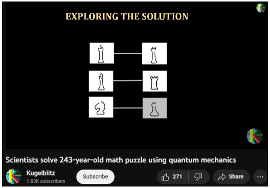
- Quantum OLS of size d → AME(4,d).
- Classical OLS of size d → AME(4,d) for every $d \neq 2$ and $d \neq 6$.
- AME(4,2) does not exists [Higuchi, Sudbery 2000]. AME(4,6) ~~is~~ was open.
- ~~Classical OLS of size 6~~ → Quantum OLS of size 6 → AME(4,6)

36 Entangled Officers of Euler

Thirty-six Entangled Officers of Euler: Quantum Solution to a Classically Impossible Problem

Suhail Ahmad Rather, Adam Burchardt, Wojciech Bruzda, Grzegorz Rajchel-Mieldzioć, Arul Lakshminarayan, and Karol Życzkowski
Phys. Rev. Lett. **128**, 080507 – Published 25 February 2022





Quanta magazine

MATHEMATICAL PHYSICS

Euler's 243-Year-Old 'Impossible' Puzzle Gets a Quantum Solution

25

A surprising new solution to Leonhard Euler's famous "36 officers puzzle" offers a novel way of encoding quantum information.

36 Entangled Officers of Euler

Sizes mean the absolute value of coefficients

Numbers mean k in

$$e^{i\pi \frac{k}{20}}$$

Quantum Physics

[Submitted on 8 Feb 2020 (v1), last revised 21 Dec 2020 (this version, v2)]

Five open problems in quantum information

A. Existence of SIC POVMs

Problem 1: *Construct SIC POVMs in an infinite sequence of dimensions,* $N_1, N_2, N_3, \ldots$

B. MUBs in dimension six

Problem 2: *Construct a set of at least 4 mutually unbiased bases in dimension six or prove that there are no 7 MUBs in* $\mathcal{H}_6$.

C. Quantum Orthogonal Latin Squares

Problem 3: *Determine whether there exist two quantum orthogonal Latin squares [77, 78] of order six. In other words, find a solution of the problem of 36 'entangled officers' of Euler or demonstrate that it does not exist.*

SIC POVMs

- Up to now: (projective) measurement $\longleftrightarrow$ orthonormal basis in $\mathbb{C}^d$.
- Generalized measurement POVM $\longleftrightarrow$ set of vectors $v_1, \ldots, v_k \in \mathbb{C}^d$ such that $\frac{d}{k} \sum_{i=1}^{k} \mathrm{P}_{v_i} = \mathbb{I}_d$.

A SIC-POVM is a POVM with d^2 elements $v_1, \ldots, v_{d^2} \in \mathbb{C}^d$ such that

$$|\langle v_i, v_j \rangle|^2 = \frac{1}{d+1} \quad \text{if } i \neq j$$

- Math: SIC POVM is a **maximal set of complex equiangular lines**. They are connected to Hilbert's 12th problem!

Example in $\mathbb{C}^2$:
$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \sqrt{2} \end{bmatrix}, \quad \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \sqrt{2} e^{i \frac{2\pi}{3}} \end{bmatrix}, \quad \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \sqrt{2} e^{i \frac{4\pi}{3}} \end{bmatrix}$$

SIC POVMs

- Up to now: (projective) measurement $\longleftrightarrow$ orthonormal basis in $\mathbb{C}^d$.
- Generalized measurement POVM $\longleftrightarrow$ set of vectors $v_1, \ldots, v_k \in \mathbb{C}^d$ such that $\frac{d}{k}\sum_{i=1}^k \mathrm{P}_{v_i} = \mathbb{I}_d$.

A SIC-POVM is a POVM with d^2 elements $v_1, \ldots, v_{d^2} \in \mathbb{C}^d$ such that

$$|\langle v_i, v_j\rangle|^2 = \frac{1}{d+1} \quad \text{if } i \neq j$$

- Math: SIC POVM is a **maximal set of complex equiangular lines**. They are connected to Hilbert's 12th problem!
- Physics: SIC POVM is a kind of optimal quantum measurement. Useful in various **quantum computing** protocols, crucial in some **interpretations** of QM (*QBism*). But they appear also in "standard" applications like **signal-processing** (radars, speech recognition etc.).

SIC POVMs - where they come up

Table 1. References classified by the topics to which they give significant coverage.

Topic	References
Abstract algebra	[8,10,11,71]
Algebraic number theory	[5–7,26,62,72]
Category theory	[73,74]
Compressed sensing and signal processing	[75–78]
Elliptic curves	[41,50,79,80]
Exact solutions	[4,8,25,26,81–86]
Frame theory	[25,37,63,77,78,87–101]
Finite group theory	[9,12,13,21,47,101–107]
Generalized and approximate SICs	[71,74,108–116]
Historical overview	[45,117,118]
Informational power and entropy	[13,21,53,119–129]
Laboratory experiments	[28–35]
Multipartite systems and sequential measurements	[47,83,130–136]
Quantum communication and cryptography	[28,29,137–143]
Quantum computing and contextuality	[13,20,40,53,135,144–151]
Quantum decoherence	[152,153]
Quantum entanglement	[19,112–114,137,139,154]
Quantum tomography	[18,31,36,63,71,133,134,138,140,155–165]
Quaternions and octonions	[9,13,48,49,73,166,167]
Reconstructing quantum theory	[14,17,22,23,40,74,117,135,168–172]
SICs and Mutually Unbiased Bases	[16,53,80,125,145,151,173–186]
SICs, Wigner functions and phase space representations	[20,29,40,53,83,89,90,144,174,187–190]

SIC POVMs - what we (don't) know

The existence of SIC POVMs is known in dimensions $d \leq 53$ and:

- 20 more dimensions between 57 and 99
- 42 more between 103 and 964
- 10 more between 1027 and 5779
- dimensions 19603 and 39604
- numerical solutions: for $d \leq 193$ and a few other dimensions.

All known SICs are **group covariant**: they are constructed by starting with a single vector (called a *fiducial vector*), and acting on it with the elements of the Weyl-Heisenberg* group.

SIC POVMs - what we (don't) know

The existence of SIC POVMs is known in dimensions $d \leq 53$ and:

- 20 more dimensions between 57 and 99
- 42 more between 103 and 964
- 10 more between 1027 and 5779
- dimensions 19603 and 39604
- numerical solutions: for $d \leq 193$ and a few other dimensions.

All known SICs are **group covariant**: they are constructed by starting with a single vector (called a *fiducial vector*), and acting on it with the elements of the Weyl-Heisenberg* group.

Zauner's conjecture. In every dimension there exists a SIC-POVM and its elements are the orbit of a fiducial vector under the Weyl-Heisenberg group.

Problem 1: *Construct SIC POVMs in an infinite sequence of dimensions,* $N_1, N_2, N_3, \ldots$

Story of Dr Gerhard Zauner

- *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*, Ph.D. Thesis, University of Vienna, 1999
- *Quantum Designs: Foundations of a non-commutative Design Theory*, English translation of the Ph.D. Thesis. Published in the International Journal of Quantum Information, 2011

Quantum designs are a generalization of both MUBs and SICs. In general: sets of states with some "nice" properties, kind of "symmetry"/"regularity".

Story of Dr Gerhard Zauner

- *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*, Ph.D. Thesis, University of Vienna, 1999
- *Quantum Designs: Foundations of a non-commutative Design Theory*, English translation of the Ph.D. Thesis. Published in the International Journal of Quantum Information, 2011

Quantum designs are a generalization of both MUBs and SICs. In general: sets of states with some "nice" properties, kind of "symmetry"/"regularity".

- *Orthogonale Lateinische Quadrate und Anordnungen, Verallgemeinerte Hadamard-Matrizen und Unabhängigkeit in der Quanten-Wahrscheinlichkeitstheorie*, Master Thesis, University of Vienna, 1991

Summary & Recommendation

- Five Open Problems in Quantum Information (yes, there are five again!)
- (Quantum) Orthogonal Latin Squares & 36 Entangled Officers of Euler
- MUBs, SICs & Quantum Designs
- Your PhD thesis matters (but you may have to wait)