Quantum combinatorial designs

Dardo Goyeneche

Jagiellonian University - Politechnika Gdańska

In collaboration with Z. Raissi, S. Di Martino, K. Życzkowski

University of Ostrava, October 3, 2017

Mathematics

Hadamard matrices

Latin and Graeco-Latin squares

Orthogonal Latin arrangements

Orthogonal arrays

Quantum Mechanics

AME states

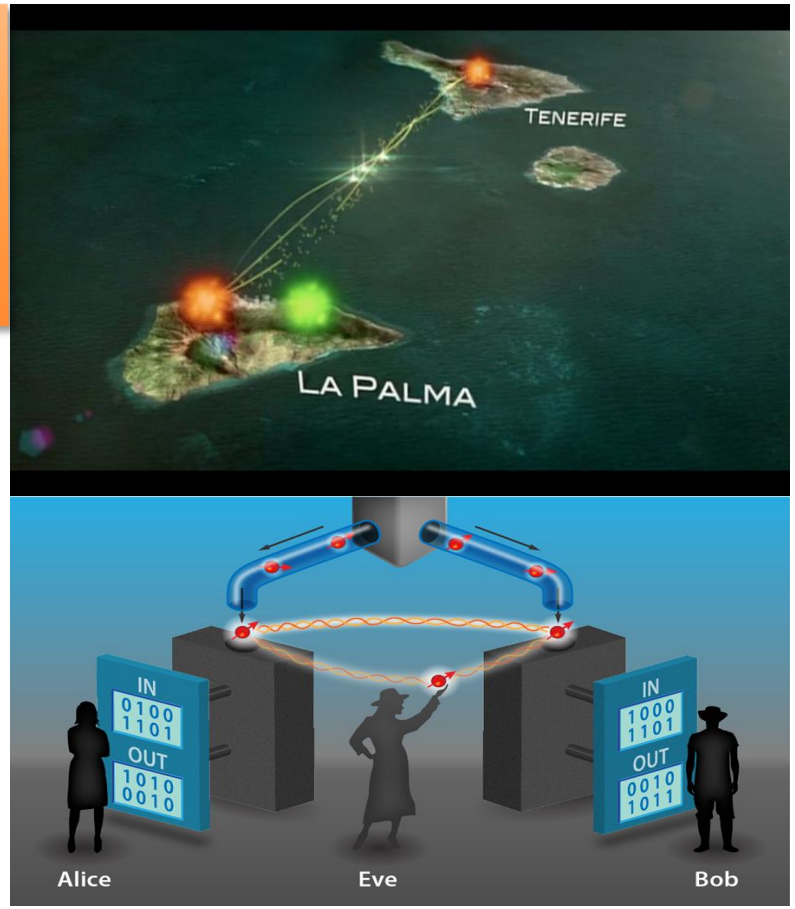
Quantum Latin Squares

Quantum Latin arrangements

Quantum orthogonal arrays

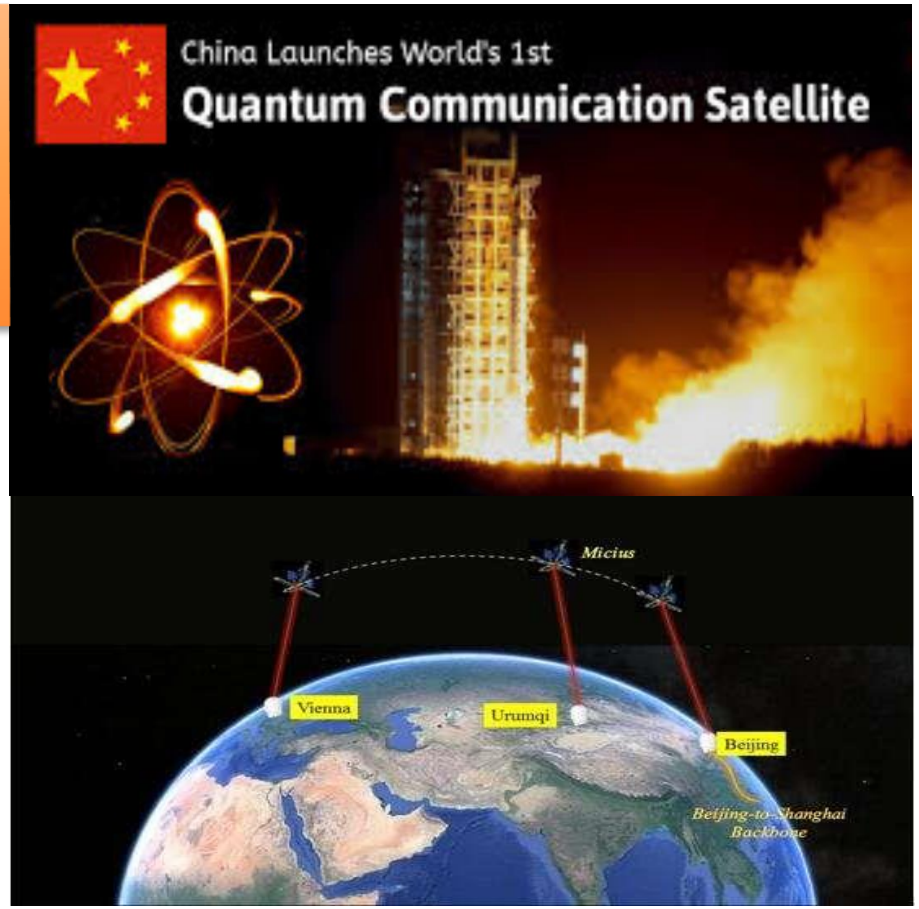
Motivation 1: secure quantum communication

2012



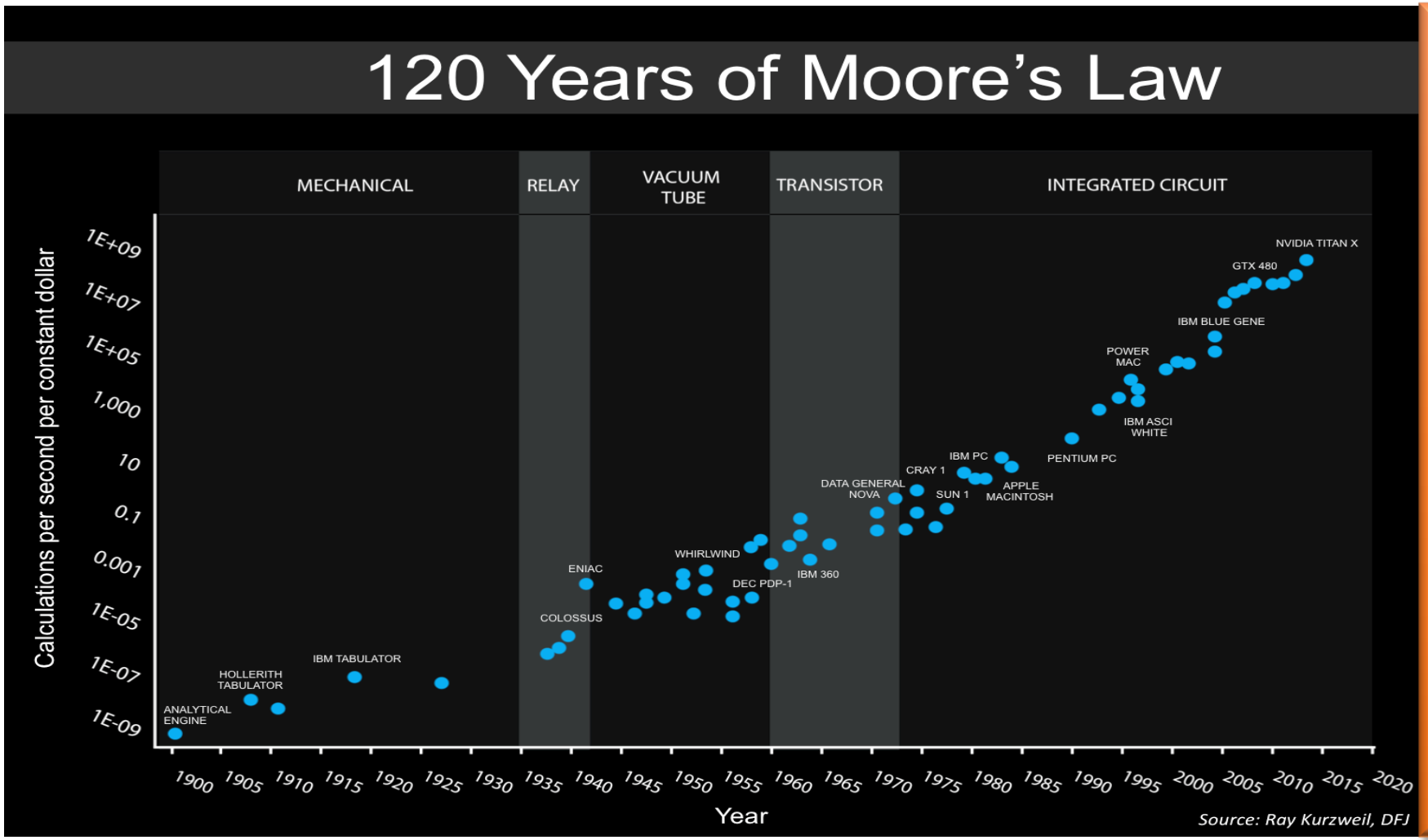
X. Song Ma *et al*, Quantum teleportation over 143 kilometres using active feed-forward, Nature 489, 269 (2012)

2017



Ji-Gang Ren *et al*, Ground-to-satellite quantum teleportation, Nature 549, 70–73 (2017)

Motivation 2: quantum computing



The number of transistors in a dense integrated circuit doubles approximately every two years.

G. Moore, 1965

Moore Law will be saturated within the next decade

1996

Database search

A fast quantum mechanical algorithm for database search

Lov K. Grover
3C-404A, Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkgrover@bell-labs.com

Summary

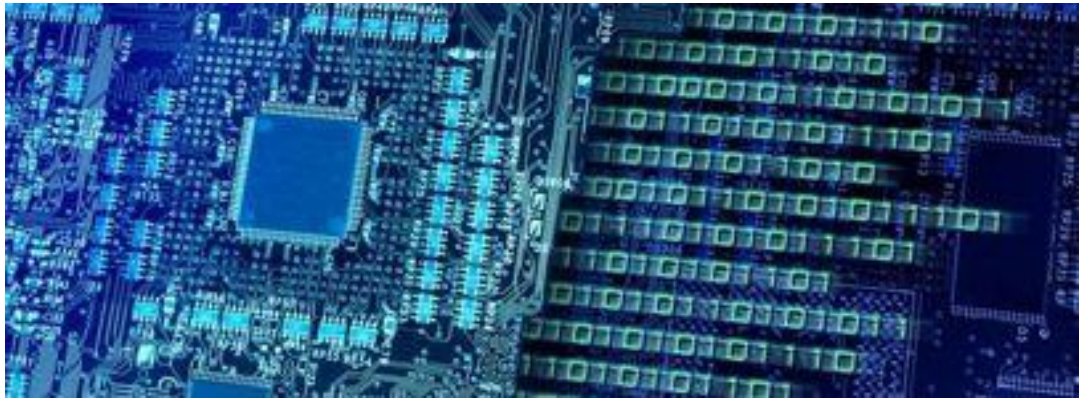
Imagine a phone directory containing N names arranged in completely random order. In order to find someone's phone number with a probability of $\frac{1}{2}$, any classical algorithm (whether deterministic or probabilistic) will need to look at a minimum of $\frac{N}{2}$ names. Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple names. By properly adjusting the phases of various operations, successful computations reinforce each other while others interfere randomly. As a result, the desired phone number can be obtained in only $O(\sqrt{N})$ steps. The algorithm is within a small constant factor of the fastest possible quantum mechanical algorithm.

This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing N items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition stop; if it does not, keep track of this item so that it is not examined again. It is easily seen that this algorithm will need to look at an average of $\frac{N}{2}$ items before finding the desired item.

L. Grover, Proc. 28th ACM Symposium on the Theory of Computing (STOC), 212-219 (1996)

1997

Prime factorization



Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

P. Shor, SIAM J.Sci.Statist.Comput. 26, 1484 (1997)

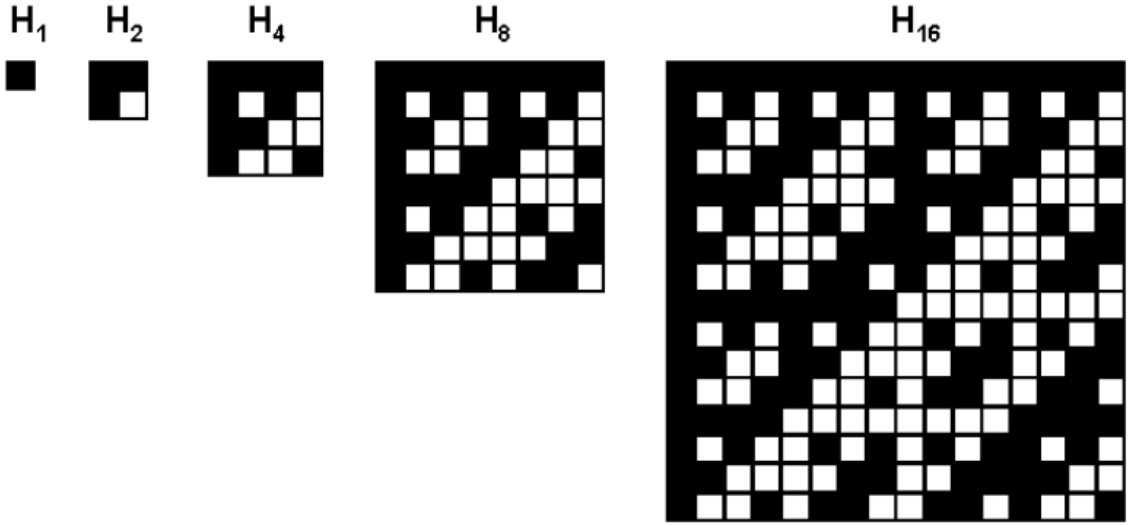
Table 5: *Quantum factorization records*

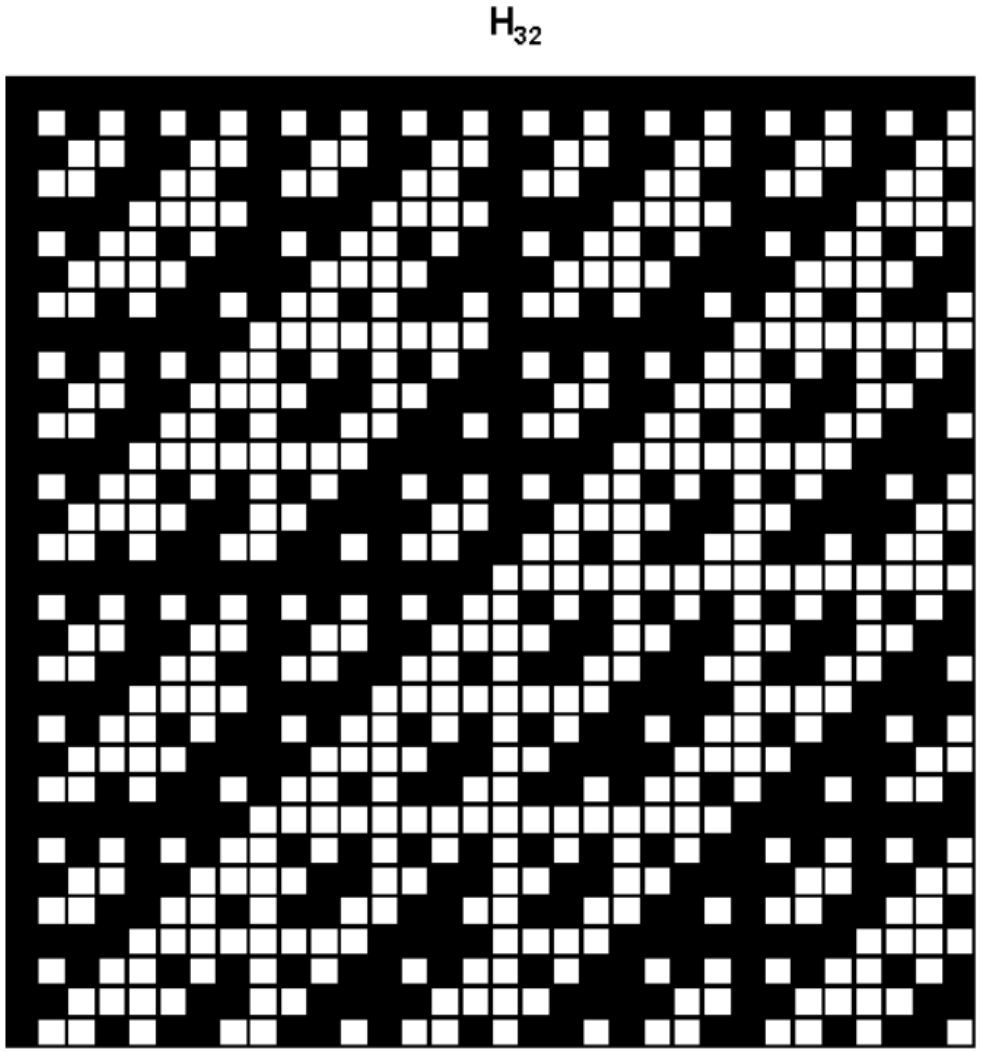
Number	# of factors	# of qubits needed	Algorithm	Year implemented
15	2	8	Shor	2001 [2]
	2	8	Shor	2007 [3]
	2	8	Shor	2007 [3]
	2	8	Shor	2009 [5]
	2	8	Shor	2012 [6]
21	2	10	Shor	2012 [7]
143	2	4	minimization	2012 [1]
56153	2	4	minimization	2012 [1]
291311	2	6	minimization	not yet
175	3	3	minimization	not yet

Nikesh S. Dattani, Nathaniel Bryans, Quantum factorization of 56153 with only 4 qubits, arXiv:1411.6758 (2014)

Combinatorial designs

Hadamard matrices





Matrices having entries ±1

and orthogonal columns

Existence of Hadamard matrices

Only possible for size $d = 2$ or d multiple of four.

Tensor product of two Hadamard matrices is a Hadamard matrix

First open case is $d = 4 \times 167 = 668$

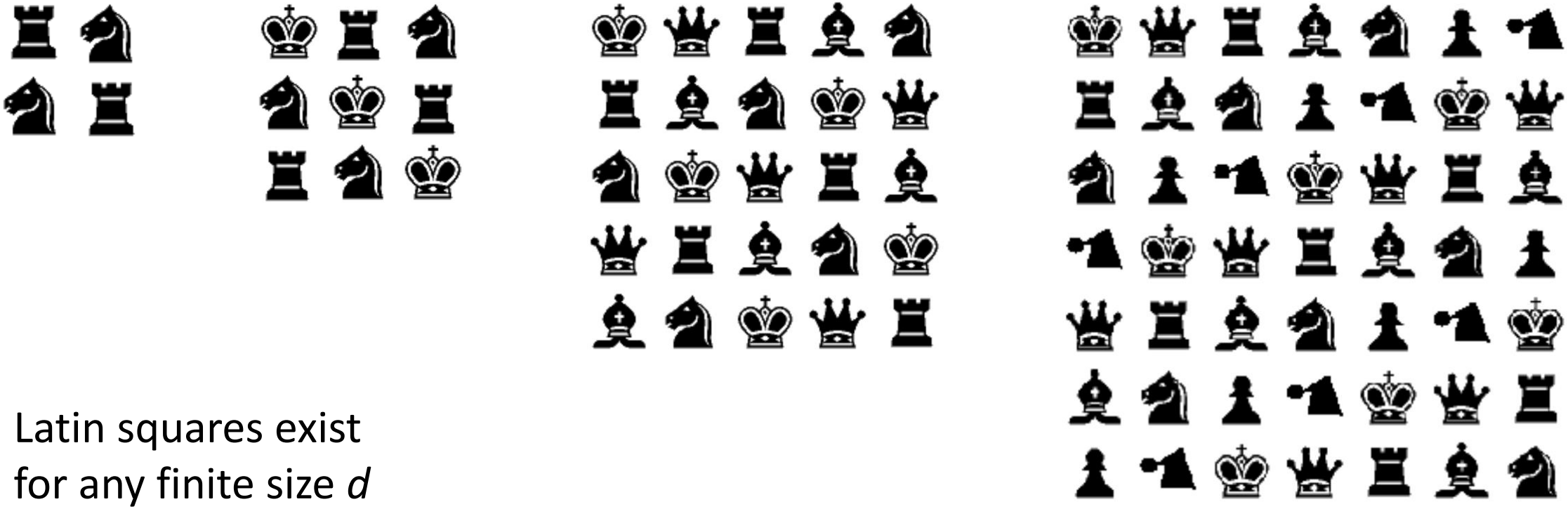
<u>Hadamard Conjecture</u>

There exists a Hadamard matrix for every size d multiple of four

Latin squares

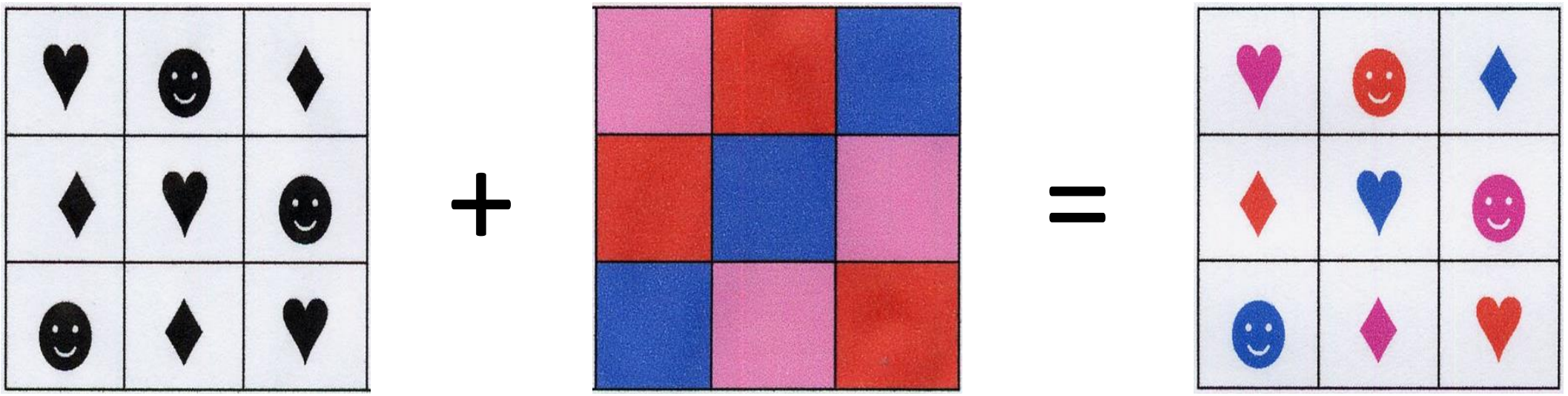
Square arrangements of size *d* having *d* different symbols.

Symbols are not repeated along every row/column.



Latin squares exist
for any finite size *d*

Graeco-Latin squares



Graeco-Latin squares exist for every finite size $d>2$, except d=6

Derrick Niederman (MIT)

36 officers of Euler

How can a delegation of six regiments, each of which sends a coronel, a lieutenant-colonel, a major, a captain, a lieutenant, and a sub-lieutenant be arranged in a regular 6 x 6 array such that no row or column duplicates a rank or a regiment?

Euler conjectured in 1782 that such configuration is not possible.

The conjecture was proved by Gaston Tarry in 1901

36 officers of Euler

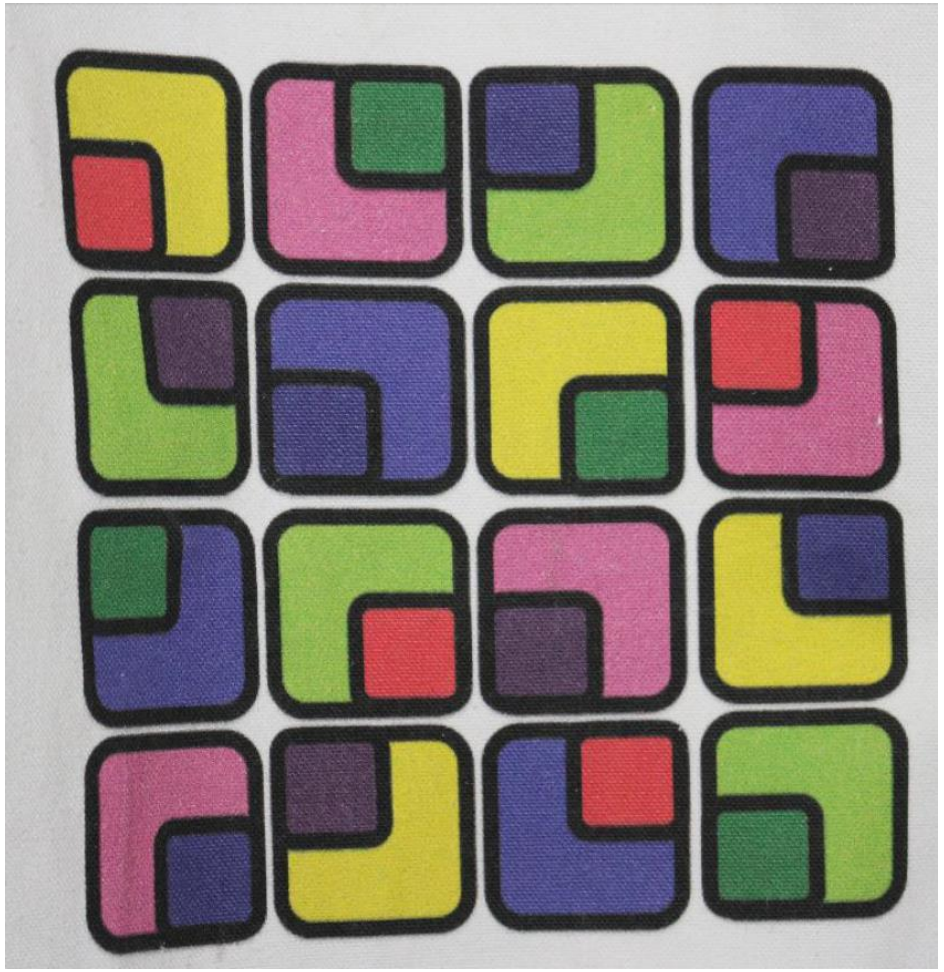
How can a delegation of six regiments, each of which sends a coronel, a lieutenant-colonel, a major, a captain, a lieutenant, and a sub-lieutenant be arranged in a regular 6 x 6 array such that no row or column duplicates a rank or a regiment?

Euler conjectured in 1782 that such configuration is not possible.

The conjecture was proved by Gaston Tarry in 1901

Derrick Niederman (MIT)

Mutually orthogonal Latin squares



Three MOLS of size four

LS1: Orientation of L's

LS2: Color of L's

LS3: Color of squares

There are, at most, *d-1* MOLS of size *d*

Karol Życzkowski – Jagiellonian University

Orthogonal arrays

An orthogonal array OA(*r, N, d, k*) is an arrangement of symbols taken from the alphabet {0,…,d-1}, having *r* rows and *N* columns such that for every subarray made up of *k* columns and *r* rows, all possible combination of symbols appear along the rows. Repetition of all possible combinations of symbols are allowed.

		0	0	1	0	0	0
		1	1	0	1	0	0
				0	0	1	0
				0	0	0	1
0	0	0		0	1	1	1
0	1	1		1	0	1	1
1	0	1		1	1	0	1
1	1	0		1	1	1	0

Orthogonal arrays

Orthogonal array of strength *k*:
every **subset of k columns** contains all possible combination of symbols (repetitions of all combinations are allowed).

Strength *k=2*

0	0	0
0	1	1
1	0	1
1	1	0

Orthogonal arrays

Orthogonal array of strength *k*:
every **subset of k columns** contains all possible combination of symbols (repetitions of all combinations are allowed).

Strength *k=2*

0	0	0
0	1	1
1	0	1
1	1	0

Orthogonal arrays

Orthogonal array of strength *k*:
every **subset of k columns** contains all possible combination of symbols (repetitions of all combinations are allowed).

Strength *k=2*

0	0	0
0	1	1
1	0	1
1	1	0

Orthogonal arrays

Orthogonal array of strength *k*:
every **subset of k columns** contains all possible combination of symbols (repetitions of all combinations are allowed).

Strength *k=2*

0	0	0
0	1	1
1	0	1
1	1	0

Strength *k=2*

0	0	0	0
0	1	2	1
0	2	1	2
1	1	1	0
1	2	0	1
1	0	2	2
2	2	2	0
2	0	1	1
2	1	0	2

Orthogonal arrays

Orthogonal array of strength *k*:
every **subset of k columns** contains all possible combination of symbols (repetitions of all combinations are allowed).

Strength *k=2*

0	0	0
0	1	1
1	0	1
1	1	0

Strength *k=2*

0	0	0	0
0	1	2	1
0	2	1	2
1	1	1	0
1	2	0	1
1	0	2	2
2	2	2	0
2	0	1	1
2	1	0	2

Orthogonal arrays

Orthogonal array of strength *k*:
every **subset of k columns** contains all possible combination of symbols (repetitions of all combinations are allowed).

Strength *k=2*

0	0	0
0	1	1
1	0	1
1	1	0

Strength *k=2*

0	0	0	0
0	1	2	1
0	2	1	2
1	1	1	0
1	2	0	1
1	0	2	2
2	2	2	0
2	0	1	1
2	1	0	2

Orthogonal arrays

Orthogonal array of strength *k*:
every **subset of k columns** contains all possible combination of symbols (repetitions of all combinations are allowed).

Strength *k=2*

0	0	0
0	1	1
1	0	1
1	1	0

Strength *k=2*

0	0	0	0
0	1	2	1
0	2	1	2
1	1	1	0
1	2	0	1
1	0	2	2
2	2	2	0
2	0	1	1
2	1	0	2

Orthogonal arrays

Orthogonal array of strength *k*:
every **subset of k columns** contains all possible combination of symbols (repetitions of all combinations are allowed).

Strength *k=2*

0	0	0
0	1	1
1	0	1
1	1	0

Strength *k=2*

0	0	0	0
0	1	2	1
0	2	1	2
1	1	1	0
1	2	0	1
1	0	2	2
2	2	2	0
2	0	1	1
2	1	0	2

Orthogonal arrays

Orthogonal array of strength *k*:
every **subset of k columns** contains all possible combination of symbols (repetitions of all combinations are allowed).

Strength *k=2*

0	0	0
0	1	1
1	0	1
1	1	0

Strength *k=2*

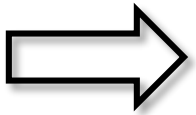
0	0	0	0
0	1	2	1
0	2	1	2
1	1	1	0
1	2	0	1
1	0	2	2
2	2	2	0
2	0	1	1
2	1	0	2

Hadamard matrices from orthogonal arrays

$$\begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{matrix} \quad \Rightarrow \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

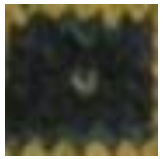
An OA(4λ,4λ-1,2,2) exists if an only if a Hadamard matrix of size 4λ exists

MOLS from orthogonal arrays



= 0

= 1



= 2

MOLHipercubes from orthogonal arrays

In general, an OA(*d^k,N,d,k*) determines *N-2* MOLH
of size *d* in dimension *k*

Quantum combinatorial designs

Two-qubit quantum states

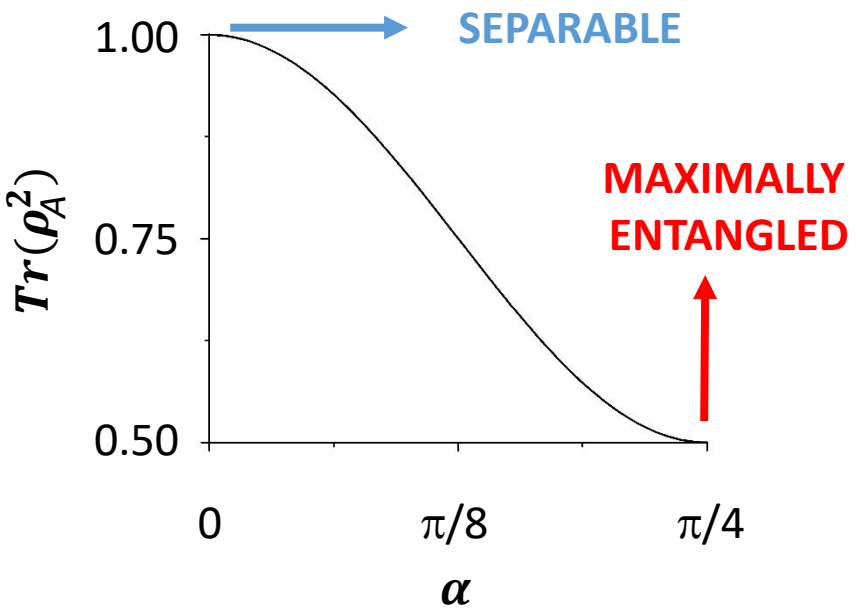
A two-qubit quantum state $|\phi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ is **separable** if

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$$

Otherwise $|\phi\rangle$ is **entangled**.

$$|\phi\rangle = \sin\alpha\,|00\rangle + \cos\alpha\,|11\rangle$$

$$\rho_A = Tr_B(|\phi\rangle\langle\phi|)$$



Maximally entangled states

Two qubit systems

$$|Bell\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Three qubit systems

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$$

Borromean rings

I. Bengtsson, K. Życzkowski,
Geometry of Quantum states
Cambridge University Press (2017)

Absolutely maximally entangled states

N partite quantum pure states such that
every reduction to $\lfloor N/2 \rfloor$ parties is maximally mixed

Two qubits

$$|AME(2,2)\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$

Three qubits

$$|AME(3,2)\rangle = \frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)$$

Four qutrits

$$|AME(4,3)\rangle = \frac{1}{3}(|0000\rangle+|0121\rangle+|0212\rangle+$$
$$|1110\rangle+|1201\rangle+|1022\rangle+$$
$$|2220\rangle+|2011\rangle+|2102\rangle)$$

Quantum orthogonal arrays

A quantum orthogonal array QOA(*r, N, d, k*), also denoted as $|OA\rangle$, is an arrangement composed by *d*-dimensional quantum states, having *r* rows and *N* columns such that every reduction to *k* columns forms a POVM.

$$OA = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \quad \Rightarrow \quad |OA\rangle = \begin{matrix} |0\rangle & |1\rangle \\ |1\rangle & |0\rangle \end{matrix}$$

$$Tr_B(|OA\rangle\langle OA|) = \begin{matrix} |0\rangle\langle 0| \\ |1\rangle\langle 1| \end{matrix}$$

$$|OA\rangle\langle OA| = \begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \otimes \begin{matrix} |1\rangle \\ |0\rangle \end{matrix} \begin{matrix} \langle 0| \\ \langle 1| \end{matrix} \otimes \begin{matrix} \langle 1| \\ \langle 0| \end{matrix} = \begin{matrix} |0\rangle\langle 0| & |1\rangle\langle 1| \\ |0\rangle\langle 1| & |1\rangle\langle 0| \\ |1\rangle\langle 0| & |0\rangle\langle 1| \\ |1\rangle\langle 1| & |0\rangle\langle 0| \end{matrix}$$

$$Tr_A(|OA\rangle\langle OA|) = \begin{matrix} |1\rangle\langle 1| \\ |0\rangle\langle 0| \end{matrix}$$

D. Goyeneche, Z. Raissi, S. Di Martino, K. Życzkowski, Entanglement and quantum combinatorial designs, arXiv:1708.05946 (2017)

Quantum orthogonal arrays

$$(\mathbb{I} \otimes H) \begin{matrix} |0\rangle & |0\rangle \\ |1\rangle & |1\rangle \end{matrix} = \begin{matrix} |0\rangle & |+\rangle \\ |1\rangle & |-\rangle \end{matrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad |\pm\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle)$$

Quantum orthogonal arrays

$$
\begin{array}{cccc}
|0\rangle & |0\rangle & |0\rangle & |\Phi^+\rangle \\
|0\rangle & |1\rangle & |1\rangle & |\Psi^+\rangle \\
|1\rangle & |0\rangle & |1\rangle & |\Psi^-\rangle \\
|1\rangle & |1\rangle & |0\rangle & |\Phi^-\rangle
\end{array}
$$

$$
\left.
\begin{aligned}
|\Phi^\pm\rangle &= (|00\rangle \pm |11\rangle)/\sqrt{2} \\
|\Psi^\pm\rangle &= (|01\rangle \pm |10\rangle)/\sqrt{2}
\end{aligned}
\right\}
$$

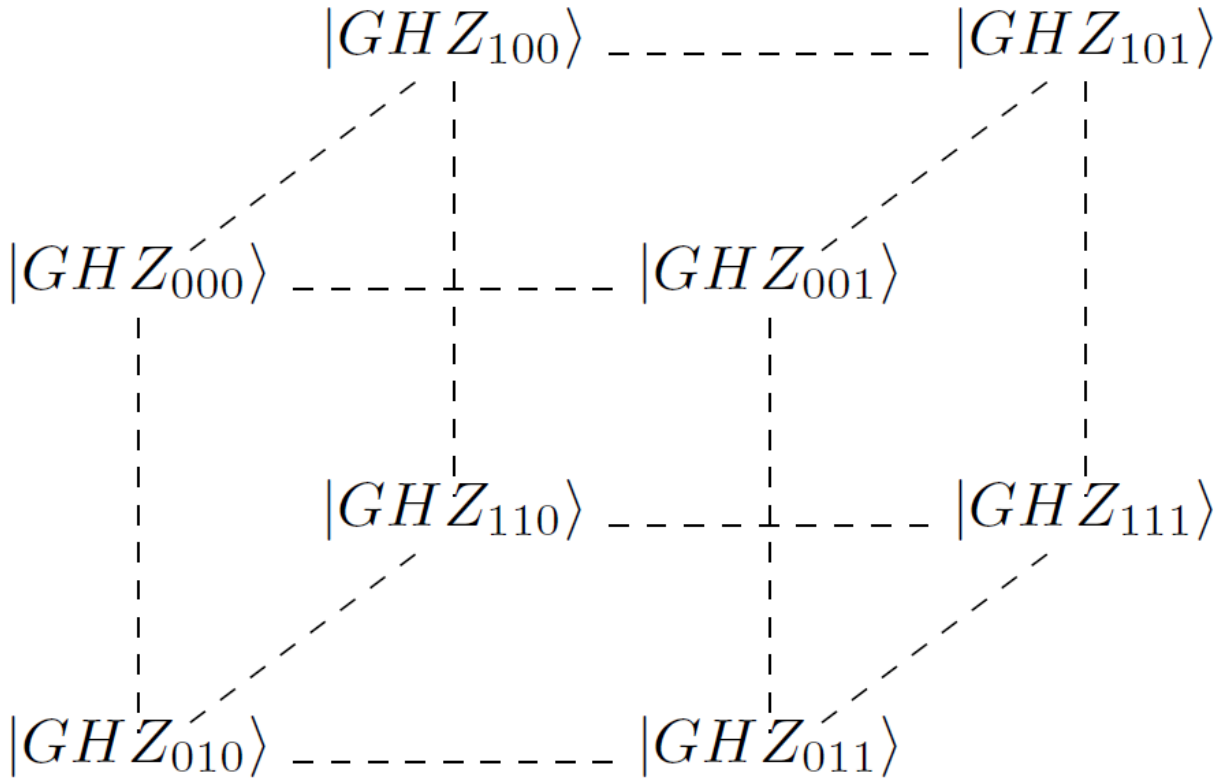
Bell basis

$$
\begin{array}{cc}
|0\rangle|\Phi^+\rangle & |1\rangle|\Psi^+\rangle \\
|1\rangle|\Psi^-\rangle & |0\rangle|\Phi^-\rangle
\end{array}
$$

Three MOQLS of size two

Quantum Latin cube

$$
\begin{array}{ccc|c}
0 & 0 & 0 & |GHZ_{000}\rangle \\
0 & 0 & 1 & |GHZ_{001}\rangle \\
0 & 1 & 0 & |GHZ_{010}\rangle \\
0 & 1 & 1 & |GHZ_{011}\rangle \\
1 & 0 & 0 & |GHZ_{100}\rangle \\
1 & 0 & 1 & |GHZ_{101}\rangle \\
1 & 1 & 0 & |GHZ_{110}\rangle \\
1 & 1 & 1 & |GHZ_{111}\rangle
\end{array}
$$



$$|GHZ\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i,i,i\rangle$$

$$|GHZ_{ijk}\rangle = (-1)^{\alpha_{ijk}} \sigma_i \otimes \sigma_j \otimes \sigma_k |GHZ\rangle$$

Quantum Orthogonal arrays of 5 columns

$$
\begin{array}{cccc}
|0\rangle & |0\rangle & |0\rangle & |\phi_{0,0}\rangle \\
|0\rangle & |1\rangle & |1\rangle & |\phi_{0,1}\rangle \\
\vdots & \vdots & \vdots & \vdots \\
|d-1\rangle & |d-1\rangle & |d-2\rangle & |\phi_{d-1,d-1}\rangle
\end{array}
$$

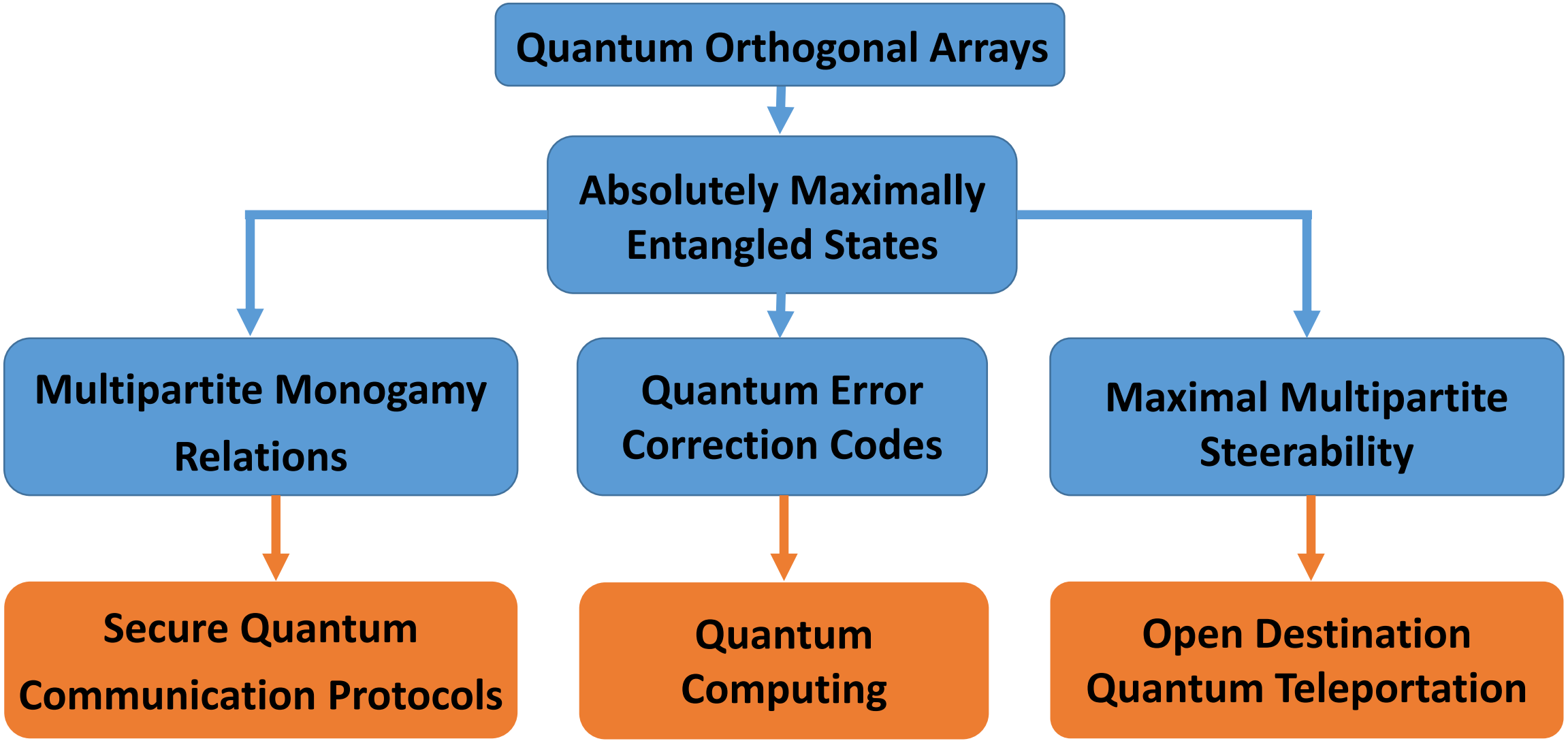
Classical part
OA(d^2,3,d,2)

Quantum part
(2-qudit Bell basis)

$$
\begin{array}{cccc}
|0\rangle\,|\phi_{0,0}\rangle & \cdots & |d-1\rangle\,|\phi_{0,d-1}\rangle \\
\vdots & \ddots & \vdots \\
|d-1\rangle\,|\phi_{d-1,0}\rangle & \cdots & |d-2\rangle\,|\phi_{d-1,d-1}\rangle
\end{array}
$$

3 MOQLS of size d

Role of QOA in quantum technologies



Thank you
for your attention

D. Goyeneche, Z. Raissi, S. Di Martino, K. Życzkowski,
Entanglement and quantum combinatorial designs,
arXiv:1708.05946 (2017)