Quantum Orthogonal Latin Squares: Local Classical Equivalence and 2-Unitary Matrix Block Rank

Connor O'Reilly
Dr. John Sheekey

August 2022

Abstract
We provide an introduction to Latin squares and quantum Latin squares, before studying the recent quantum solution of Rather et al. to the classically impossible Euler's 36 Officers problem. We then begin work on an open problem proposed by Życzkowski et al. regarding the existence of genuinely quantum orthogonal Latin squares of size 3 that are not locally classical-equivalent, by finding conditions for the block-wise rank of classical-equivalent 2-unitary matrices.

School of Mathematics and Statistics

University College Dublin

Acknowledgements

I would like to thank Dr. John Sheekey for supervising and guiding my research, as well as Dr. Anthony Cronin and the UCD School of Mathematics and Statistics for giving me the opportunity to carry out this project.

1 Introduction

Latin squares are combinatorial objects with applications across statistics and mathematics, particularly in coding theory, as well as being related to sudoku and other board games.[6] An example of a Latin square was first published by Choi Seok-jeong in 1700, although it has been remarked that Latin squares date back to c.1200 with links to medieval Islam.[3]

The name “Latin square” originates from Leonhard Euler’s study of the objects and his usage of the Roman alphabet for the set of symbols.[19] Pairs of orthogonal Latin squares are also sometimes known as Euler squares, and Euler’s study of Latin squares is thought to be the first development of a general theory of these objects. Our first chapter will be an introduction to Latin squares, and an overview of the historical work of Euler and other key figures.

As the field of quantum information theory grows, with Latin squares having applications in classical coding theory, it is natural to consider quantum analogues of Latin squares. The idea of a quantum Latin square was proposed by B. Musto and J. Vicary in 2015.[12] These objects have since been shown to have relations to absolutely maximally entangled (AME) states, [14] which have various applications in quantum information. [9] [16] We will discuss in detail a recent result from Rather et al. [15] regarding the existence of a quantum orthogonal Latin square of size 6×6, an object for which no classical equivalent exists. [18] An important open question is that of the existence of quantum orthogonal Latin squares of any order that are in some sense not equivalent to known classical Latin squares. [21] We will then begin work on this question for quantum orthogonal Latin squares of size 3×3 by considering computational and algebraic techniques.

2 Latin Squares and Orthogonality

We begin with a key definition:

Definition 2.1 A Latin square of order n is an $n \times n$ array L whose entries are taken from a set S of n symbols such that each symbol from S occurs exactly once in each row and column of L. [5]

For example, for $n = 3$ and $S = \{A, B, C\}$, one such Latin square is shown:

$$\begin{bmatrix} A & B & C \\ C & A & B \\ B & C & A \end{bmatrix}$$

An interesting method of generating Latin squares involves multiplication tables. For example, observing the table for multiplication modulo 5:

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Removing the first row and first column (all zeros), we get the following Latin square:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

Recalling the definition of a quasigroup, we can express this result more generally:

Definition 2.2 A quasigroup $(Q, \cdot)$ is a non-empty set Q with binary operation $\cdot$ such that for all $a, b \in Q$, there exists unique $x, y \in Q$ such that $a \cdot x = b$ and $y \cdot a = b$.

Theorem 2.3 *Every multiplication table of a quasigroup is a latin square and conversely, any bordered latin square is the multiplication table of a quasigroup. [6]*

A notion of equivalence exists between Latin squares:

Definition 2.4 A pair of Latin squares are equivalent, or isotopic, if one can be obtained from the other by row permutation, column permutation, or renaming of symbols. [5]

There is a concept of isotopy between quasigroups also:

Definition 2.5 For two quasigroups $(G, \cdot)$ and $(H, *)$, an ordered triple (θ, ϕ, ψ) of bijections from G to H is called an isotopy of G upon H if $\theta(x) * \phi(y) = \psi(x \cdot y)$. We then call G and H isotopic.

By taking two Latin squares and their associated quasigroups, it can be shown that these concepts are equivalent. In the above notation, when transformed into Latin squares/Cayley tables, ψ permutes the elements inside the table (symbols of the Latin square), where as θ and ϕ permute the table border (rows and columns of the Latin square). Isotopy forms an equivalence relation, and gives the concept of an isotopy class.[6]

Finally, when constructing Latin squares, there is a helpful assumption that we can always make:

Definition 2.6 A Latin square is said to be reduced, or in standard form, if the elements of the first row and first column are in natural order. [6]

Lemma 2.7 *Every Latin square is equivalent to a reduced Latin square.*

Proof. Suppose we have a Latin square L with entries a_{ij}, for $i, j \in S = \{1, \ldots, n\}$. Then we can permute the columns of L such that the first row is in natural order, i.e. $a_{1j} = j$. We have already then that $a_{11} = 1$, thus we can permute rows $2, \ldots, n$ such that the first column is in natural order, i.e. $a_{i1} = i$, without affecting the first row. L is now in reduced form. □

A much stronger condition is that of a pair of orthogonal Latin squares:

Definition 2.8 A pair of Latin squares $L_1 = ||a_{ij}||$ and $L_2 = ||b_{ij}||$ on n symbols are said to be orthogonal if every ordered pair of symbols occurs exactly once among the n^2 pairs (a_{ij}, b_{ij}), where $i, j \in \{1, \cdots, n\}$ [6]

For example, L_1 and L_2 below are orthogonal:

$$L_1 = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix},\ L_2 = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \\ 3 & 2 & 1 \end{bmatrix} \implies L_1 \odot L_2 = \begin{bmatrix} (2,2) & (3,1) & (1,3) \\ (1,1) & (2,3) & (3,2) \\ (3,3) & (1,2) & (2,1) \end{bmatrix}$$

Similar to single Latin squares, two pairs of orthogonal Latin squares are equivalent under row or column permutation, and renaming of symbols within the constituent single Latin squares.[5]

Recalling Theorem 2.3, we have the following results:

Theorem 2.9 *The multiplication table of any group of odd order forms a Latin square which possesses an orthogonal mate.[6]*

Corollary 2.10 *There exist pairs of orthogonal Latin squares of every odd order.*

Euler was able to construct orthogonal Latin squares for every order divisible by four, but not for any order of the form $4k + 2$, which led him to conjecture that no orthogonal Latin squares exist for any oddly even order. [7] It is straightforward to see that no orthogonal Latin square of order 2 exists. Notice that there is no way of completing the Latin square below that maintains orthogonality:

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix} \odot \begin{bmatrix} 1 & 2 \\ ? & ? \end{bmatrix} = \begin{bmatrix} (A,1) & (B,2) \\ (B,?) & (A,?) \end{bmatrix}$$

An example of an orthogonal Latin square of order 3 has been given above. The following are examples for orders 4 and 5:

$$\begin{bmatrix} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{bmatrix} \odot \begin{bmatrix} 1 & 3 & 4 & 2 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} A1 & B3 & C4 & D2 \\ B2 & A4 & D3 & C1 \\ C3 & D1 & A2 & B4 \\ D4 & C2 & B1 & A3 \end{bmatrix}$$

$$\begin{bmatrix} A & B & C & D & E \\ B & C & D & E & A \\ C & D & E & A & B \\ D & E & A & B & C \\ E & A & B & C & D \end{bmatrix} \odot \begin{bmatrix} 1 & 4 & 2 & 5 & 3 \\ 2 & 5 & 3 & 1 & 4 \\ 3 & 1 & 4 & 2 & 5 \\ 4 & 2 & 5 & 3 & 1 \\ 5 & 3 & 1 & 4 & 2 \end{bmatrix} = \begin{bmatrix} A1 & B4 & C2 & D5 & E3 \\ B2 & C5 & D3 & E1 & A4 \\ C3 & D1 & E4 & A2 & B5 \\ D4 & E2 & A5 & B3 & C1 \\ E5 & A3 & B1 & C4 & D2 \end{bmatrix}$$

From now on, we will drop the bracket notation and write, for example, $(A, 1)$ as $A1$. The notation of the $\odot$ symbol was chosen as it is commonly used to represent the similar-looking Hadamard product for matrices.

So we have solved the problem of existence for orders 2 to 5. What about order $n = 6$?

> *"Six different regiments have six officers, each one belonging to different ranks. Can these 36 officers be arranged in a square formation so that each row and column contains one officer of each rank and one of each regiment?"* - L. Euler

This famous problem by Euler [7] is exactly the question of existence of an orthogonal Latin square of order 6, by labeling the regiments and ranks with symbols. Notice that this is the case for $k = 1$ for Euler's $4k + 2$ conjecture stated earlier. This problem was solved by exhaustion by Gaston Tarry in 1900 [18], and later with a concise algebraic method by D.R. Stinson in 1984 [17]:

Theorem 2.11 (Tarry, 1900) *There does not exist an orthogonal Latin square of order 6.*

However, Euler's conjecture is not true. In 1959, R.C. Bose and S.S Shrikhande found a counterexample by constructing an orthogonal Latin square of order 22. [1] Later in the same year, Bose, Shrikhande and E.T. Parker proved the following theorem:

Theorem 2.12 (Bose, Shrikhande, Parker, 1959) *There exists an orthogonal Latin square for all all* $n \equiv 2$ *(mod 4),* $n \geq 10$*. [2]*

Connecting this result with earlier results of existence for multiples of 4 and odd orders:

Corollary 2.13 *There exists an orthogonal Latin square for all orders* $n \neq 2, 6$.

3 Notation and Definitions

As the related literature is often focused on quantum theory and applications, we will require some notation and definitions commonly used within physics, as well as some mathematical tools. This section covers these requirements.

Throughout quantum theory, it is standard to write vectors and dual vectors in Dirac notation, otherwise known as bra-ket notation. The following is a quick overview. Let V be a complex inner product space.

- A vector $v \in V$ is denoted as a ket, and is written as $|v\rangle$.
- It is common to write basis vectors $e_1, e_2, \ldots, e_n$ as $|1\rangle, |2\rangle, \ldots, |n\rangle$. This basis is known as the computational basis.
- A covector $f \in V^*$ is denoted as a bra, and is written as $\langle f|$.
- The inner product of $u, v \in V$ is denoted as $\langle u|v\rangle$, and similarly the outer product is denoted as $|u\rangle\langle v|$. [4]

The following notes on Hilbert spaces and quantum states are based on Chapter 3 of *Quantum Algorithms via Linear Algebra: A Primer* by Richard J. Lipton and Kenneth W. Regan. [11]

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be m-dimensional and n-dimensional Hilbert spaces respectively. Then the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ is the space of vectors of the form a_k where $1 \leq k \leq mn$. This has a one-to-one correspondence with pairs (i, j) for $1 \leq i \leq m$ and $1 \leq j \leq n$, so each a_k can be written as a_{ij}. Then the tensor product of two vectors $a \in \mathcal{H}_1$ and $b \in \mathcal{H}_2$ is the vector $c = a \otimes b$ where $c_{ij} = a_i b_j$.

When working with quantum experiments, Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ represent two separate systems, and the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ is used to study them simultaneously. We will thus refer to $\mathcal{H}_A$ and $\mathcal{H}_B$ as the A and B subsystems respectively. The vectors of $\mathcal{H}_A \otimes \mathcal{H}_B$ are called quantum states.

The elements of the computational basis are known as basis states. The basis states for $\mathcal{H}_A \otimes \mathcal{H}_B$ are written as $|ij\rangle$ where $1 \leq i \leq m$ and $1 \leq j \leq n$ as before. For example, where $e_i \in \mathcal{H}_A$ and $f_j \in \mathcal{H}_B$, $e_1 \otimes f_2 = |1\rangle\langle 2| := |12\rangle$, etc.

Definition 3.1 A pure quantum state is a state which can be described as a linear combination of basis states.

For our purposes, we will only deal with pure quantum states.

Definition 3.2 A vector representing a pure quantum state is separable if it is the tensor product of two other vectors. Otherwise, it is called entangled.

For example, $|11\rangle = |1\rangle\langle 1|$ and $|22\rangle = |2\rangle\langle 2|$ are separable, but $\frac{1}{\sqrt{2}}(|11\rangle + |22\rangle)$ is entangled. The computational basis elements of $\mathcal{H}_A \otimes \mathcal{H}_B$ are separable by definition, but their linear combinations are not necessarily.

Definition 3.3 A complex square matrix U is unitary if its conjugate transpose $U^\dagger$ is its inverse, i.e. $UU^\dagger = I$.

We will use unitary matrices to represent transformations on vectors within subsystems.

4 Quantum Latin Squares

As mentioned in the previous section, the space of states in quantum theory is described as a complex vector space. In a quantum analogue of Latin squares, this will replace our set of symbols S. The natural replacement for the concept of distinct set elements or symbols is the concept of orthogonal vectors. The following definition was given by B. Musto and J. Vicary in 2016 [12]:

Definition 4.1 A quantum Latin square of order d, or $QLS(d)$ is an array of d^2 states $|\psi_{ij}\rangle \in \mathcal{H}_d$, such that each row and column forms an orthonormal basis.

Here $\mathcal{H}_d$ represents a d-dimensional Hilbert space. We will always use $\mathbb{C}^d$ as our choice of space. Our classical notion of equivalence also has a quantum analogue:

Definition 4.2 A pair of quantum Latin squares are equivalent if one can be obtained from the other by row permutation, column permutation, or by multiplying every element by some unitary matrix U.

Here we replace the idea of relabeling of symbols by applying transformations upon the states. Applying a fixed unitary transformation to every state maintains orthonormality. The concept of equivalence allows us to categorise quantum Latin squares based on how close to classical objects they are.

Definition 4.3 A quantum Latin square is classical if every element is an element of the computational basis. [13]

For example, the quantum Latin square L below is classical.

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

Definition 4.4 The cardinality, c, of a quantum Latin square is the number of distinct elements in the array. [13]

Definition 4.5 A $QLS(d)$ is genuinely quantum if $c > d$. Otherwise, $c = d$, and the $QLS(d)$ is apparently quantum. [13]

Apparently quantum Latin squares are unitarily equivalent to classical quantum Latin squares. As $d \leq c \leq d^2$, they have minimal cardinality.

We can ask the question of existence for genuinely quantum Latin squares. The following was shown by J. Paczos et al. in 2021: [13]

Theorem 4.6 *There exists no genuinely quantum Latin squares of orders 2 and 3.*

However, the same paper constructs a quantum Latin square of order 4. This is thus the smallest case where genuinely quantum solutions exist.

$$\begin{bmatrix} |1\rangle & |2\rangle & |3\rangle & |4\rangle \\ |3\rangle + |4\rangle & |3\rangle - |4\rangle & |1\rangle - |2\rangle & |1\rangle + |2\rangle \\ |2\rangle + \frac{1}{\sqrt{2}}(|3\rangle - |4\rangle) & |1\rangle - \frac{1}{\sqrt{2}}(|3\rangle + |4\rangle) & |1\rangle + |2\rangle + \sqrt{2}|4\rangle & |1\rangle + |2\rangle + \sqrt{2}|3\rangle \\ |2\rangle - \frac{1}{\sqrt{2}}(|3\rangle - |4\rangle) & |1\rangle + \frac{1}{\sqrt{2}}(|3\rangle + |4\rangle) & |1\rangle + |2\rangle - \sqrt{2}|4\rangle & |1\rangle + |2\rangle - \sqrt{2}|3\rangle \end{bmatrix}$$

Note that in this form, the entries are not normalised; this is to improve legibility. The above is in fact a transformation of the originally constructed $QLS(4)$ to emphasise the next fact.

Remark A quantum Latin square of any order can always be unitarily transformed so that the first row (or column) consists of the computational basis in natural order.

To further understand the structure of a $QLS(4)$, we show the following:

Lemma 4.7 *Given a $QLS(4)$ with one row consisting of the computational basis β in natural order, each row must contain 0, 2, or 4 elements of β.*

Proof. Assume that the first row consists of the computational basis β in natural order. Then we have a row with 4 elements of β, in the following form:

$$\begin{bmatrix} |1\rangle & |2\rangle & |3\rangle & |4\rangle \\ |a_{21}\rangle & |a_{22}\rangle & |a_{23}\rangle & |a_{24}\rangle \\ |a_{31}\rangle & |a_{32}\rangle & |a_{33}\rangle & |a_{34}\rangle \\ |a_{41}\rangle & |a_{42}\rangle & |a_{43}\rangle & |a_{44}\rangle \end{bmatrix}$$

If the second row contained 3 elements of β, then it must contain the fourth element, by dimension, thus we can not have only 3. Also, the example above shows that it is possible to have 0 elements in β. For the other cases, suppose there is at least one element of β in the second row.

Assume $|a_{21}\rangle = |2\rangle$. Then, by orthogonality:

$$\begin{aligned} |a_{22}\rangle &= \alpha_1|1\rangle + \alpha_3|3\rangle + \alpha_4|4\rangle \\ |a_{23}\rangle &= \beta_1|1\rangle + \beta_4|4\rangle \\ |a_{24}\rangle &= \gamma_1|1\rangle + \gamma_3|3\rangle \end{aligned}$$

By $\langle a_{23}|a_{24}\rangle = \beta_1\overline{\gamma}_1 = 0$, we have two cases:

- If $\beta_1 = 0$, then $|a_{23}\rangle = |4\rangle$, so $\alpha_4 = 0$. Then:

$$|a_{22}\rangle = \alpha_1|1\rangle + \alpha_3|3\rangle \quad \text{and} \quad |a_{24}\rangle = \gamma_1|1\rangle + \gamma_3|3\rangle$$
$$\implies \alpha_1\overline{\gamma}_1 + \alpha_3\overline{\gamma}_3 = 0$$

which does have complex solutions.

- If $\gamma_1 = 0$, then $|a_{24}\rangle = |3\rangle$, so $\alpha_3 = 0$. Then:

$$|a_{22}\rangle = \alpha_1|1\rangle + \alpha_4|4\rangle \quad \text{and} \quad |a_{23}\rangle = \beta_1|1\rangle + \beta_4|4\rangle$$
$$\implies \alpha_1\overline{\beta}_1 + \alpha_4\overline{\beta}_4 = 0$$

which also has complex solutions.

Notice that instead assuming $|a_{21}\rangle = 3$ or $|a_{21}\rangle = 4$ results in the same cases after permutation of columns. Thus it is possible to have exactly two elements of β in one row. However, it is impossible to have only one element of β in the second row, as this would result in both $\beta_1 \neq 0$ and $\gamma_1 \neq 0$, which is a contradiction. Thus we can have 0, 2, or 4 elements of β in the second row. Note that this applies to all rows by row permutation. □

Note however that this does not apply to columns, as it relies on the assumption that the first row consists of the computational basis. If we instead assumed that the first column consists of the computational basis, the result would apply to columns, but not rows.

5 Quantum Orthogonal Latin Squares

The definition of a classical orthogonal Latin square requires the constituent "subsquares" to satisfy the conditions of being a Latin square. However, recalling definition 3.2, it may not always be straightforward to separate a quantum state into its subsystems. Thus we require the following definition:

Definition 5.1 Let M be a matrix of dimension $d_A d_B$, with $M = M_A \otimes M_B$. Then: [14]

$$Tr_B(M) = (I_d \otimes Tr)(M_A \otimes M_B) = Tr(M_B)M_A$$

is the partial trace over subsystem B of M. The partial trace over subsystem A is defined similarly.

This partial trace function thus maps elements of $\mathcal{H}_A \otimes \mathcal{H}_B$ to $\mathcal{H}_A$ or $\mathcal{H}_B$. By linearity of the trace function, it is straightforward to define the partial trace for any element of $\mathcal{H}_A \otimes \mathcal{H}_B$, separable or entangled. We can now define the quantum analogue of a pair of orthogonal Latin squares: [14]

Definition 5.2 A quantum orthogonal Latin square of order d, or $QOLS(d)$, is a $d \times d$ array of elements of $\mathcal{H}_d$ such that:

- All d^2 states form an orthonormal basis.
- All rows satisfy

$$Tr_B\left(\sum_{k=0}^{d-1} |\psi_{ik}\rangle\langle\psi_{jk}|\right) = \delta_{ij}\mathbb{I}_d$$

- All columns satisfy

$$Tr_B\left(\sum_{k=0}^{d-1}|\psi_{ki}\rangle\langle\psi_{kj}|\right) = \delta_{ij}\mathbb{I}_d$$

It is straightforward to see that the first condition is the quantum equivalent of each entry being a different object, and that the set of every entry spans the entire space just as every pair appears in the classical orthogonal Latin square. The other conditions represent the idea of subsquares being Latin squares, by requiring orthonormality within the subsystems for both rows and columns.

Our first question is of existence for quantum orthogonal Latin squares. Again, any classical orthogonal Latin square can be turned into a $QOLS$ of the same order using the computational basis. Recalling corollary 2.13, these do not however exist for $d = 2, 6$. But does a quantum orthogonal Latin square exist for these sizes? The following definition is relevant: [14]

Definition 5.3 An absolutely maximally entangled state, or AME state, is a pure quantum state $|\psi\rangle$, with reduced density matrices $\rho_i = Tr_i(|\psi\rangle\langle\psi|)$, such that the von Neumann entropy $S = -Tr(\rho_i \ln(\rho_i))$ is maximal in every subsystem i.

It can be shown that the existence of AME states for four subsystems of d dimension, or $AME(4, d)$ is equivalent to the existence of a $QOLS(d)$. [14] Thus the following result from A. Higuchi and A. Sudbery in 2000 is of interest here. [10]

Theorem 5.4 *There does not exist an $AME(4, 2)$ state.*

Corollary 5.5 *There does not exist a $QOLS(2)$.*

Each $AME(4, d)$ state can be written in the following form:

$$|\psi\rangle = \frac{1}{d}\sum_{i,j,k,l=0}^{d-1} T_{ijkl}|i\rangle_A|j\rangle_B|k\rangle_C|l\rangle_D$$

where A,B,C,D are the four subsystems, and T_{ijkl} is a four index tensor. This tensor T_{ijkl} can be reshaped into a unitary matrix U of size d^2 in six different ways by bi-partitioning the indices. As transposing unitary matrices maintains unitarity, we can consider only three of these matrices. Thus the construction of an $AME(4, d)$ state is equivalent to the construction of three matrices $U_{(ij)(kl)}$, $U_{(ik)(jl)}$, $U_{(ij)(lk)}$. [8] We define these matrices as follows:

Definition 5.6 Given a unitary matrix U, the reshuffle of U, denoted U^R, is defined by the index swap $U^R_{ijkl} = U_{ikjl}$.

Definition 5.7 Given a unitary matrix U, the partial transpose of U over the B subsystem, denoted U^{Γ_B}, is defined by the index swap $U^R_{ijkl} = U_{ijlk}$.

[14] The reshuffle of a size d^2 matrix can be thought of as reshaping each $d \times d$ block into row vectors and then placing these vectors on top of each other. The partial transpose of a size d^2 matrix over the B subsystem can be thought of as transposing each block.

$$U = \sum_i A_i \otimes B_i \implies U^{\Gamma_B} = \sum_i A_i \otimes B_i^T$$

The partial transpose over the A subsystem is defined similarly, but we won't use this. Note also that $(U^{\Gamma_A})^T = U^{\Gamma_B}$.

The above definitions are gathered into the following condition: [14]

Definition 5.8 A matrix U is 2-unitary if U, U^R, and U^{Γ_B} are unitary.

The equivalence between 2-unitary matrices and AME states, as well as the equivalence between AME states and quantum orthogonal Latin squares, allows us to state the following:

Theorem 5.9 *The existence of a 2-unitary matrix of size d^2 is equivalent to the existence of a $QOLS(d)$.*

Thus the existence question for quantum orthogonal Latin squares can be solved by searching for 2-unitary matrices of the respective size.

6 The 36 Entangled Officers

Recalling that no orthogonal Latin square of order 6 exists, we discuss the 2021 result from Rather et al. [15] that proved the existence of a quantum orthogonal Latin square of order 6 by constructing an example. The paper uses the following algorithm to generate 2-unitary matrices:

$$\mathcal{M}_{\Gamma R} : U_0 \mapsto U_0^R \mapsto (U_0^R)^\Gamma = U_1 H \mapsto U_1$$

where R is the reshuffle, Γ is the partial transpose (over subsystem B), and U_0 is an initial unitary "seed" matrix. The final part of the map uses the polar decomposition, which factorises a square matrix into a multiplication of a unitary matrix U_1 and a positive semi-definite Hermitian matrix H, to output a new unitary matrix U_1. 2-unitary matrices are period-3 orbits of this map, and seed matrices can be chosen such that the output of $\mathcal{M}_{\Gamma R}^n$ is 2-unitary with high probability for large n.

By choosing a permutation matrix as an initial seed, a numerical solution was found by this algorithm. Local unitary transformations (see definition 7.1) were applied to generate an equivalent matrix solution with more zero entries. Then an analytical form was constructed by hand by observing this numerical form, which was then verified. Thus a $QOLS(6)$ exists in analytical form. The full AME state will not be given here, but a visual representation is given in Figure 1 on the next page.

7 Genuinely Quantum Solutions

As there does not exist a classical 6×6 orthogonal Latin square, the Rather et al. result is genuinely quantum, i.e. it is not equivalent to any classical solution. However, it is an open question as to whether there exist quantum orthogonal Latin squares of other sizes that are not equivalent to classical squares. We begin work on this question as stated in the paper by Życzkowski et al. from 2022. [21]

> *Are there genuinely quantum $OLS(d)$ for $d = 3, 4,$ or 5, which are not locally equivalent to a classical solution?*

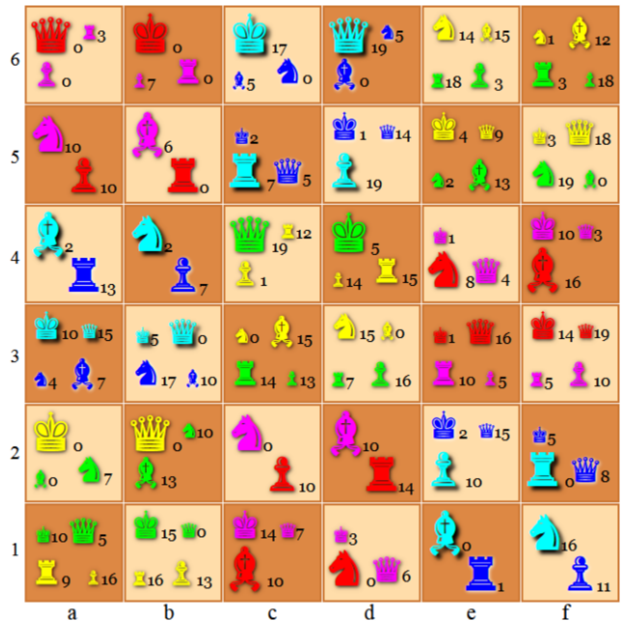

Figure 1: A visual representation of the $QOLS(6)$ solution. Chess pieces and colours represent symbols on each subsystem, with the number $k \in \{0, 1, \dots, 19\}$ next to each figure representing a complex phase $\exp(\pi i k/10)$. [15]

We work only on the case of $d = 3$. First, let's define what is meant by local equivalence. [20]

Definition 7.1 Let $M = \sum_i A_i \otimes B_i$ be a $d^2 \times d^2$ 2-unitary matrix representing a $QOLS(d)$, L, and let M' be a $d^2 \times d^2$ 2-unitary matrix representing a $QOLS(d)$, L'. Then L and L' are locally equivalent if $M' = (U_1 \otimes U_2)M(U_3 \otimes U_4)$, for $d \times d$ unitary matrices U_j.

By expanding M as defined, we see the following:

$$M' = (U_1 \otimes U_2)M(U_3 \otimes U_4) \implies M' = \sum_i U_1 A_i U_3 \otimes U_2 B_i U_4$$

We can write this expansion in a way such that every A_i is a basis element of $\mathcal{H}_d \otimes \mathcal{H}_d$. Then U_2, U_4 correspond to multiplying each entry of the $QOLS(d)$ by unitary transformations on each side, while U_1, U_3 correspond to linear row and column operations. This is the natural quantum analogue of equivalence of classical orthogonal Latin squares, allowing for possibly complex linear combinations of rows and columns, rather than just permuting.

We can write classical orthogonal Latin squares as 2-unitary matrices also. For example, take the following orthogonal Latin square of order 3 and its quantum equivalent:

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

By writing each entry as a 3×3 block, we get the following permutation matrix:

$$\left[\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Note that every block is rank 1. Thus if a quantum orthogonal Latin square were equivalent to a classical square, it would be possible to apply local unitary transformations as above such that every block becomes rank 1. However, the following fact allows us to simplify the task:

Lemma 7.2 *Given a square matrix M, and unitary matrices U_1, U_2 of the same size, $rank(M) = rank(U_1 M U_2)$.*

In other words, applying unitary transformations on the blocks will not change their rank. Recalling that the same unitary transformation is applied to every block, we find then that, if at least one of the blocks has rank greater than 1, applying unitary transformations on the B subsystem will not bring the solution any closer to being entirely classical. Thus a classical equivalence would depend entirely on transformations on the A subsystem.

We provide the following result:

Theorem 7.3 *Let M be a 9×9 2-unitary matrix. If two or more of the 3×3 blocks of M are rank 1, M is equivalent to a classical solution.*

Proof. Let n be the number of blocks assumed to be rank 1 in M, and label the remaining blocks A_k. By performing unitary transformations on the B subsystem, we can always assume that the rank 1 blocks are computational basis elements of $\mathbb{C}^{3\times 3}$. Here M^{Γ_B} is written as M^{Γ}. We work with cases for choices of n:

- $n = 9$: M is a permutation matrix and thus is classical by definition.
- $n = 8$: As M^R is unitary, the blocks of M are orthonormal, and so the ninth block is forced to be rank 1.
- $n = 7$: As M and M^{Γ} are unitary, a block A being in the same block row or block column as a basis element $|ij\rangle$ forces the i-th row and j-th column of A to be zero. As every placement requires each A_k share either a block row or block column with two basis elements, each of these A_k must be rank 1.
- $n = 6$: Again, every placement of six rank 1 blocks forces the other A_k to be rank 1.
- $n = 5$: Up to permutation, the only placement which doesn't immediately collapse to nine rank 1 blocks is below. By relabeling basis elements and permutation, without

loss of generality, we can choose the following rank 1 elements:

$$\begin{bmatrix} \cdot & \cdot & \cdot \\ \cdot & A_1 & A_2 \\ \cdot & A_3 & A_4 \end{bmatrix} \implies \begin{bmatrix} |11\rangle & |22\rangle & |33\rangle \\ |23\rangle & A_1 & A_2 \\ |32\rangle & A_3 & A_4 \end{bmatrix}$$

By orthonormality of blocks, and sharing rows or columns with $|22\rangle$ or $|33\rangle$, and $|23\rangle$:

$$A_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Thus we have found six rank 1 blocks, so M is classical.

- $n = 4$: Any placement of four rank 1 blocks will collapse to either cases $n = 5$ or $n = 6$ above, as it must have either one full block row/column of rank 1 blocks, or 2 block rows/columns of two rank 1 blocks.

- $n = 3$: We have three cases. Firstly, suppose each rank 1 block is in one row of M:

$$M = \begin{bmatrix} |11\rangle & |22\rangle & |33\rangle \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix}$$

By 2-unitarity, the blocks have the following structure:

$$A_{21} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & a \\ 0 & b & 0 \end{bmatrix} \quad A_{22} = \begin{bmatrix} 0 & 0 & c \\ 0 & 0 & 0 \\ d & 0 & 0 \end{bmatrix} \quad A_{23} = \begin{bmatrix} 0 & e & 0 \\ f & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$
$$A_{31} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & g \\ 0 & h & 0 \end{bmatrix} \quad A_{32} = \begin{bmatrix} 0 & 0 & k \\ 0 & 0 & 0 \\ l & 0 & 0 \end{bmatrix} \quad A_{33} = \begin{bmatrix} 0 & m & 0 \\ n & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

By orthogonality of rows and orthogonality of blocks we get a list of equations, expressed here in matrix form:

$$\begin{bmatrix} a & 0 & 0 & 0 & 0 & f \\ 0 & b & 0 & d & 0 & 0 \\ 0 & 0 & c & 0 & e & 0 \\ a & b & 0 & 0 & 0 & 0 \\ 0 & 0 & c & d & 0 & 0 \\ 0 & 0 & 0 & 0 & e & f \end{bmatrix} \begin{bmatrix} \overline{g} \\ \overline{h} \\ \overline{k} \\ \overline{l} \\ \overline{m} \\ \overline{n} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Row-reducing gives the following solution set:

$$\begin{bmatrix} \overline{g} \\ \overline{h} \\ \overline{k} \\ \overline{l} \\ \overline{m} \\ \overline{n} \end{bmatrix} = \overline{n} \begin{bmatrix} -f/a \\ f/b \\ f/c \\ -f/d \\ -f/e \\ 1 \end{bmatrix}$$

Also, by normality of rows, columns and blocks:

$$\begin{aligned}
|a|^2 + |f|^2 &= 1 \\
|a|^2 + |g|^2 &= 1 \\
|a|^2 + |b|^2 &= 1 \\
\implies |f|^2 &= |g|^2 = |b|^2
\end{aligned}$$

Applying this to all rows, columns and blocks, we get the following:

$$\begin{aligned}
|a|^2 = |d|^2 = |e|^2 = |h|^2 = |k|^2 = |n|^2 \\
|b|^2 = |c|^2 = |f|^2 = |g|^2 = |l|^2 = |m|^2
\end{aligned}$$

Thus there are only two distinct moduli over all of the constants. They may still have distinct complex phases however, so we relabel them, for $\alpha, \beta \in \mathbb{R}$:

$$a \mapsto \alpha e^{ia}, \; b \mapsto \beta e^{ib} \; \ldots$$

We then have the following relation between A_{21} and A_{31}:

$$\begin{aligned}
g &= -n\overline{f}/\overline{a} \\
&\mapsto -\alpha e^{in} \beta e^{-if} / \alpha e^{-ia} \\
&= -\beta e^{i(n-f+a)}
\end{aligned}$$

Thus the A subsystem row operation $R_2 \mapsto \beta R_2 + \alpha e^{i(a-g)} R_3$ results in A_{21} and thus A_{31} being rank 1. Since we have now found five rank 1 blocks, we find that M is classical.

Secondly, notice that if only two blocks are in one row/column, with the remaining block in another row/column, we immediately have a fourth rank 1 block, and so M is classical.

Finally, suppose that the rank 1 blocks are on the block diagonal of M. Then the rank 1 blocks $|ab\rangle, |cd\rangle, |ef\rangle$ must have $a = c = e$ or $b = d = f$; otherwise no solutions exist. Assume M to be the first choice, as the second corresponds to M^Γ.

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

By 2-unitarity, we have the following structure:

$$A_{12} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & a \\ 0 & 0 & b \end{bmatrix} \quad A_{13} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & c & 0 \\ 0 & d & 0 \end{bmatrix} \quad A_{21} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & e \\ 0 & 0 & f \end{bmatrix}$$
$$A_{23} = \begin{bmatrix} 0 & 0 & 0 \\ g & 0 & 0 \\ h & 0 & 0 \end{bmatrix} \quad A_{31} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & k & 0 \\ 0 & l & 0 \end{bmatrix} \quad A_{32} = \begin{bmatrix} 0 & 0 & 0 \\ m & 0 & 0 \\ n & 0 & 0 \end{bmatrix}$$

which gives us the following list of equations by orthonormality:

$$\begin{bmatrix} a & b & 0 & 0 & 0 & 0 \\ 0 & 0 & c & d & 0 & 0 \\ 0 & 0 & 0 & 0 & g & h \\ 0 & 0 & 0 & 0 & a & b \\ g & h & 0 & 0 & 0 & 0 \\ 0 & 0 & \overline{h} & \overline{g} & 0 & 0 \end{bmatrix} \begin{bmatrix} \overline{e} \\ \overline{f} \\ \overline{k} \\ \overline{l} \\ \overline{m} \\ \overline{n} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

However, row-reducing shows that this has no non-zero solutions. Thus this case can not result in a non-classical example either.

- $n = 2$: Firstly, notice that if both blocks were in the same row/column, it would immediately result in a third block, which is classical as above. So assume that both blocks are along the block diagonal again.

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

But then we have the following structure for A_{13}, A_{23}, A_{33}:

$$A_{21} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & \cdot & \cdot \\ 0 & \cdot & \cdot \end{bmatrix} \quad A_{23} = \begin{bmatrix} 0 & \cdot & \cdot \\ 0 & 0 & 0 \\ 0 & \cdot & \cdot \end{bmatrix} \quad A_{33} = \begin{bmatrix} 0 & \cdot & \cdot \\ 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix}$$

But notice that the first columns of all of these blocks make up one column in M, so by normality, A_{33} must be rank 1. Thus we have found a third rank 1 block, and so M is classical.

□

This shows that a genuinely quantum orthogonal Latin square would have to consist of at most one rank 1 entry, which may reduce the area of search for future study.

8 Computational Search

We conclude with a brief section on computational methods for finding quantum orthogonal Latin squares. Using the map $\mathcal{M}_{\Gamma R}$ given in section 6, we were able to find numerical examples of 9×9 2-unitary matrices using Python. The algorithm used a randomly generated unitary seed matrix. All of the examples generated consisted of nine rank 3 blocks, and satisfied the conditions of 2-unitarity up to computational precision. However, we were unable to find an analytical form of these matrices as in the case of the 6×6 quantum orthogonal Latin square. Inputting a seed with known analytical form, or with many zeroes, did not help with producing a 2-unitary matrix of simpler analytical form, due to the numerical technique of the computational polar decomposition. In contrast with the $QOLS(6)$, the order 3 examples generated elements all with distinct magnitudes. Furthermore, the classical equivalence of these matrices was not tested. So while the algorithm produced numerical 2-unitary matrices, it is inconclusive as to whether these examples have a useful analytical form that can be claimed as non-classical.

9 Conclusion

The result of Rather et al. has opened new quantum-related possibilities to the many applications of combinatorial objects, specifically in the 6×6 case, and has produced new quantum error-correcting codes. It has also highlighted the question of whether these objects exist for other orders. This work begins to understand the complexity of properties of genuinely quantum orthogonal Latin squares even for low orders, and reduces the search area for examples of these objects by putting a restraint on the rank of the elements of the array. Furthermore, it was found possible to generate numerical examples of $QOLS(3)$ of maximum element-wise rank using an existing algorithm, putting the focus of further study on techniques of checking classical equivalence. We conclude with some questions for further study:

- Does the existence of one rank 1 block in a 2-unitary M result in classical equivalence? In other words, can we extend the proof of theorem 7.3 to include $n = 1$? Techniques similar to the $n = 3$ cases were attempted, however assuming only one rank 1 block results in much fewer known zeroes. As a result of this, the number of equations increases by a large amount, and we do not get the case of only two distinct moduli.

- Which 3-dimensional subspaces of 3×3 complex matrices contain a matrix of rank 1? Having a block row or column consisting of any basis of such a subspace would mean that there is always a unitary transformation resulting in a rank 1 element in that block row or column. This question, along with the previous one, would give further requirements for a genuinely quantum object. However, it is possible to construct a basis such that no linear combination is rank 1, so it is not every subspace.

- M. Ziman, 2001 [20] states eigenvalues are invariant under local unitary operations, and gives a condition for local equivalence based on the eigenvalues of the reduced density matrices of two states. Generally, can properties of the eigenvalues/vectors of 2-unitary matrices provide conditions for equivalence of $QOLS(d)$?

References

[1] R. C. Bose and S. S. Shrikhande. On the falsity of euler's conjecture about the non-existence of two orthogonal latin squares of order 4t + 2. *Proceedings of the National Academy of Sciences*, 45(5):734–737, 1959.

[2] R. C. Bose, S. S. Shrikhande, and E. T. Parker. Further results on the construction of mutually orthogonal latin squares and the falsity of euler's conjecture. *Canadian Journal of Mathematics*, 12:189–203, 1960.

[3] C.J. Colbourn and J.H. Dinitz. *Handbook of Combinatorial Designs*. Discrete Mathematics and Its Applications. CRC Press, 2006.

[4] P. A. M. Dirac. A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, 35(3):416–418, 1939.

[5] J. Dénes and A.D. Keedwell. Chapter 1 - introduction (j. dénes and a. d. keedwell). In *Latin Squares*, volume 46 of *Annals of Discrete Mathematics*, pages 1–6. Elsevier, 1991.

[6] J. Dénes and A.D. Keedwell. Preface to the first edition. In A. Donald Keedwell and József Dénes, editors, *Latin Squares and their Applications (Second Edition)*. North-Holland, Boston, second edition edition, 2015.

[7] Leonhard Euler. Recherches sur un nouvelle espèce de quarrés magiques, 1782.

[8] Dardo Goyeneche, Daniel Alsina, José I. Latorre, Arnau Riera, and Karol Życzkowski. Absolutely maximally entangled states, combinatorial designs, and multiunitary matrices. *Phys. Rev. A*, 92:032316, Sep 2015.

[9] Wolfram Helwig, Wei Cui, José Ignacio Latorre, Arnau Riera, and Hoi-Kwong Lo. Absolute maximal entanglement and quantum secret sharing. *Phys. Rev. A*, 86:052335, Nov 2012.

[10] A. Higuchi and A. Sudbery. How entangled can two couples get? *Physics Letters A*, 273(4):213–217, 2000.

[11] Richard J. Lipton and Kenneth W. Regan. *Basic Linear Algebra*, page 16–20. MIT-Press, 2014.

[12] Benjamin Musto and Jamie Vicary. Quantum latin squares and unitary error bases. *Quantum Information and Computation*, 16, 04 2015.

[13] Jerzy Paczos, Marcin Wierzbiński, Grzegorz Rajchel-Mieldzioć, Adam Burchardt, and Karol Życzkowski. Genuinely quantum solutions of the game sudoku and their cardinality. *Phys. Rev. A*, 104:042423, Oct 2021.

[14] Grzegorz Rajchel-Mieldzioć. Quantum mappings and designs, 04 2022.

[15] Suhail Ahmad Rather, Adam Burchardt, Wojciech Bruzda, Grzegorz Rajchel-Mieldzioć, Arul Lakshminarayan, and Karol Życzkowski. Thirty-six entangled officers of euler: Quantum solution to a classically impossible problem. *Phys. Rev. Lett.*, 128:080507, Feb 2022.

[16] A. J. Scott. Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions. *Phys. Rev. A*, 69:052330, May 2004.

[17] D.R Stinson. A short proof of the nonexistence of a pair of orthogonal latin squares of order six. *Journal of Combinatorial Theory, Series A*, 36(3):373–376, 1984.

[18] Gaston Tarry. Le problème des 36 officiers. *Compte Rendu de l'Association Française pour l'Avancement des Sciences*, 1, 1901.

[19] W.D. Wallis and J. George. *Introduction to Combinatorics*. Discrete Mathematics and Its Applications. Taylor & Francis, 2011.

[20] M. Ziman, P. Štelmachovič, and V. Bužek. On the local unitary equivalence of states of multi-partite systems. *Fortschritte der Physik*, 49(10-11):1123–1131, 2001.

[21] Karol Zyczkowski, Wojciech Bruzda, Grzegorz Rajchel-Mieldzioć, Adam Burchardt, Suhail Ahmad Rather, and Arul Lakshminarayan. $9 \times 4 = 6 \times 6$: Understanding the quantum solution to the euler's problem of 36 officers, 04 2022.