



Jagiellonian University in Kraków

Faculty of Physics, Astronomy
and Applied Computer Science

Structured Unitary Matrices and Quantum Entanglement

A doctoral dissertation

written under the supervision of Prof. Karol Życzkowski

Wojciech Bruzda

Kraków, November 2021

Wydział Fizyki, Astronomii i Informatyki Stosowanej
Uniwersytet Jagielloński

Oświadczenie

Ja niżej podpisany Wojciech Bruzda (nr indeksu: WFAI-D-120) doktorant Wydziału Fizyki, Astronomii i Informatyki Stosowanej Uniwersytetu Jagiellońskiego oświadczam, że przedłożona przeze mnie rozprawa doktorska pt. “Structured Unitary Matrices and Quantum Entanglement” jest oryginalna i przedstawia wyniki badań wykonanych przeze mnie osobiście, pod kierunkiem

prof. dra hab. Karola Życzkowskiego.

Pracę napisałem samodzielnie.

Oświadczam, że moja rozprawa doktorska została opracowana zgodnie z Ustawą o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. (Dziennik Ustaw 1994 nr 24 poz. 83 wraz z późniejszymi zmianami).

Jestem świadom, że niezgodność niniejszego oświadczenia z prawdą ujawniona w dowolnym czasie, niezależnie od skutków prawnych wynikających z ww. ustawy, może spowodować unieważnienie stopnia nabytego na podstawie tej rozprawy.

Kraków, dnia 2021/11/21

.....
podpis doktoranta

Acknowledgments

I am grateful to my supervisor Karol Życzkowski who guided me this far over all these years and supported by all means.

I acknowledge with gratitude the fruitful cooperation of the following people:

Daniel Alsina, Ingemar Bengtsson, Adam Burchardt, Valerio Cappellini, Åsa Ericsson, Jonith Fischmann, Shmuel Friedland, Dardo Goyeneche, Boris Khoruzhenko, Arul Lakshminarayan, Jan-Åke Larsson, Grzegorz Rajchel-Mieldzioć, Suhail Ahmad Rather, Marek Smaczyński, Hans-Jürgen Sommers, Wojciech Tadej, Ondřej Turek, all colleagues from Jagiellonian Quantum Information Team, and of course APPB Crew.

I am indebted to Anna Szymusiak and Dardo Goyeneche who carefully read appropriate chapters and whose criticism and remarks were instrumental for the final version of this work.

Special thanks to:

Ania Głowacka, pan Jacek, Sabrina, Zuzik, Mirosław ($\vec{F} = m\vec{g}$) Klewec, Rockford, Cycurek, #119, unit 456, and every sea $\square$ square.

for us
and them

Abstract

In this Thesis we explore the set of unitary matrices characterized by a given structure in the context of their applications in the field of quantum information. In the first part of the Thesis we focus on classification of special classes of unitary matrices and possibility of introducing certain internal parameterizations. Several new results and conjectures are discussed. In particular, we propose the construction of families of isolated complex Hadamard matrices in infinitely many dimensions. Second part of the Thesis is devoted to the concept of multipartite quantum entanglement. We present a solution to the long-standing problem in theory of quantum information concerning the status of absolutely maximally entangled states of four subsystems with six levels each. Finally, we propose a fusion of two areas of research and we analyze the excess of a matrix and the corresponding Bell inequalities. This combination allows us to draw new conclusions related to quantum nonlocality.

Streszczenie

Dysertacja jest poświęcona badaniu macierzy unitarnych posiadających pewną zadaną strukturę w kontekście ich zastosowań w teorii kwantowej informacji. W pierwszej części pracy skupiamy się na problemie klasyfikacji specjalnych klas macierzy unitarnych oraz możliwości wprowadzenia pewnych wewnętrznych parametryzacji. Przedstawiamy i dyskutujemy szereg nowych rezultatów oraz hipotez. W szczególności omawiamy konstrukcję rodzin izolowanych zespolonych macierzy Hadamarda w nieskończenie wielu wymiarach. Druga część pracy jest poświęcona wielocząstkowemu kwantowemu splątaniu. Prezentujemy długo oczekiwane rozwiązanie jednego z problemów w teorii kwantowej informacji, który dotyczy istnienia stanów absolutnie maksymalnie splątanych dla czterech podukładów o sześciu stopniach swobody. Ostatni rozdział pracy zawiera propozycję zintegrowania dwóch obszarów badań: ekscesu macierzowego oraz nierówności Bella. Połączenie tych dwóch zagadnień pozwala nam wyciągnąć nowe wnioski dotyczące kwantowej nielokalności.

Contents

1	Introduction	3
1.1	Purpose and Structure of the Thesis	4
1.2	Notation Used	6
2	Complex Hadamard Matrices	9
2.1	Classification and Invariants	11
2.2	Extension of the Set $\mathbb{H}(8)$ of CHM of Order 8	14
2.2.1	Random Walk over Core Phases	14
2.2.2	New Nonaffine Family $T_8^{(1)}$	14
2.3	Extension of the Set $\mathbb{H}(9)$ of CHM of Order 9	17
2.3.1	Sinkhorn Algorithm Revisited	17
2.3.2	A Novel Isolated Matrix $T_9^{(0)}$	18
2.4	Families of (Isolated) Complex Hadamard Matrices	21
2.4.1	Family of Complex Hadamard Matrices L_N	22
2.4.2	Family of Complex Hadamard Matrices V_N	24
2.5	Comment on the Structure of the Set $\mathbb{H}(8)$	24
2.6	Summary	27
3	Restricted Defect of a Unitary Matrix	29
3.1	Quantum Measurement	30
3.2	Gram Matrix	33
3.3	Restricted Defect Δ	33
3.3.1	Elementary Examples	36
3.4	Isolated Mutually Unbiased Bases (MUB) and Symmetric, Informationally Complete Positive-Operator Valued Measures (SIC-POVM)	38
3.4.1	Isolated Kochen–Specker Sets	40
3.5	Free Parameters in MUB, Equiangular Tight Frames and SIC-POVM	41
3.6	Robustness of the Restricted Defect Δ	42
3.7	Summary	44

4	Absolutely Maximally Entangled States (AME) of Four Quhexes	47
4.1	Quantum Entanglement	47
4.2	Absolutely Maximally Entangled States	49
4.2.1	Multipartite Entanglement Algebra	50
4.2.2	Entangling Power and Gate Typicality	52
4.3	Quantization of the Problem of 36 Officers of Euler	54
4.4	Orthogonal Approximation of AME(4, 6)	55
4.4.1	Permutation Matrix P of Order 36	55
4.4.2	Orthogonal Matrix Q of Order 36	57
4.4.3	Orthogonal Matrix V of Order 36	59
4.5	Isoentropic Triplets of Matrices	65
4.6	Unitary Approximation of AME(4, 6)	74
4.6.1	Dynamical Map	74
4.6.2	Golden AME(4, 6) State	76
4.7	Summary	80
5	Excess of a Matrix and Bell Inequalities	83
5.1	Initial Observation	85
5.2	Bell Inequalities	86
5.3	Excess of a Matrix Σ	89
5.4	Excess of a Matrix and Classical Value of Bell Inequality	90
5.4.1	Family of Bell Inequalities with Quantum Advantage	92
5.5	Excess and Mutually Unbiased Bases	96
5.6	Tight Bell Inequalities	97
5.7	Summary	98
6	Concluding Remarks	101
6.1	Open Questions and Future Work	103
	References	105
A	Papers	117

Chapter 1

Introduction

Why do we do physics?

Nowadays it is a tricky question but let us be so bold to suggest the following generic answer, which we believe is still valid to some extent, regardless the circumstances: we do physics to ultimately understand the Universe.

We do not focus much on the philosophical aspects and the purpose of this all, but we are happy to know the mechanisms explaining all processes at every scale; from elementary particles, through the classical world we live in, to the mechanics of the most remote galaxies. Probably, once we get the knowledge about everything that surrounds us and what is deep inside of our bodies, we will eventually go back to the question concerning the objectives, or maybe the answer will come itself. Either way, fortunately there is a long (very long indeed) way before us.

Doing physics is a synergy of observation, intuition, imagination and mathematics.¹ But in contrary to the last ingredient, which describes ideal concepts in its ideal realm, physicists notoriously face the problem of permanent approximations and imprecision. At the subatomic scales, and in this Thesis we are implicitly interested exactly in subatomic scales, this property of our reality is exhibited exceptionally harsh. Let us take a very concrete example. Suppose we want to build (actually, we badly want to build!) a fully operative “pocket” quantum computer, a successor of classical machines with computational power that is incomparably greater than the one of the currently biggest superclusters. Quantum mechanics, the mathematical framework that provides all necessary tools to operate at such low level, imposes natural constraints and limits for the physical systems and their possible applications. Roughly speaking, an action of a quantum computer can be described as a sequence of unitary operations (quantum gates) applied to initial states (vectors in Hilbert space) which are subjected to measurement (outcomes of our calculations). Somewhere in between the input and output, the unitary evolution should be maintained and supported

¹Some say the patience and humility too.

by error correction procedures to minimize consequences of immediate decoherence. Process of decoherence, which is the interaction of quantum system with the environment causes noise and the loss of interference, and the lack of interference in the quantum system makes it simply a classical one. This is one of the biggest obstacles that we presently encounter. If ever resolved, it will pave the way for further milestones on the way to quantum computing.

Quantum information theory (QIT) [1] being a relatively young branch of contemporary physics, deals with the aforementioned problems. At the heart of the QIT there is a notion of *quantum information*, which can be understood as a everything what we can infer from the quantum system described mathematically by a wave function. As such, quantum information is the root of: entanglement, computation, randomness, currency, metrology, cryptography, thermodynamics, Darwinism, teleportation, etc., where every item in the list deserves the prefix “quantum”.

In the further perspective, apart from obviously attractive problem of quantum computers, for which already awaits a bunch of problems to be solved, we eagerly wish to address one additional issue concerning the quantum description of gravity, which is apparently not included in the list above. This is actually the last missing step in understanding the properties of all four known fundamental interactions. Meanwhile, short term expectations and the most imperative open problems in QIT have been summarized in many lists. The priority of problems strongly depends on the community preparing such motivational aggregates. However, the common idea remains the same — to gradually discover and understand the more areas of physics. Here we recall two such lists. “Five Open Problems in Theory of Quantum Information” [2], and another one, taken from the Blog of Scott Aaronson, entitled suggestively “The Ten Most Annoying Questions in Quantum Computing” [3].

Some problems from these lists like the existence of mutually unbiased bases, absolutely maximally entangled states or special families of quantum measurement, will be carefully (sometimes indirectly) explored in the chapters that follow.

1.1 Purpose and Structure of the Thesis

This theoretically oriented dissertation contributes to few branches of QIT; quantum computation, quantum measurement, quantum combinatorics and quantum nonlocality. During the preparation of the Thesis some open problems have been partially or fully resolved. Only the most interesting and, in large part, unpublished results will be presented.

Each chapter covers one specific topic and should be considered either as a detailed supplement to the associated papers: [A1], [A2], [A3], [A4], and [A5], or a different view of the published (or to be published) results. We focus only on the original contributions and, any time it is required to preserve the continuity of exposition, we highlight references to our collaborators to emphasize their own achievements.

The logical composition of this Thesis can be divided onto two parts. Chapters 2 and 3 present the general approach to understanding the structure of some classes of unitary matrices in arbitrary dimension. While the remaining part with Chapters 4 and 5 regards the idea of quantum entanglement described in the language of matrix formalism. This should comprehensively explain the concept, the structure and the title of the work.

Recall the schematic description of quantum computer mentioned at the beginning. Three general ingredients involving quantum computation can be in some sense associated with the three first chapters:

- Chapter 2 $\leftrightarrow$ quantum unitary evolution (quantum gates),
- Chapter 3 $\leftrightarrow$ quantum measurement,
- Chapter 4 $\leftrightarrow$ quantum error correcting codes.

In each chapter we make (a successful) attempt to a better understanding of a given subject.

The paper is organized as follows. We begin with the problem of classification of *complex Hadamard matrices* (CHM). Both, numerical and analytical aspects of searching for new examples of CHM are described. We present a new family of CHM of size 8 and continue the subject over the particular subset of CHM — isolated CHM, which leads to other previously unknown matrices of order $N > 8$. Two new constructions of isolated CHM are introduced, and we propose two conjectures concerning existence of such objects in infinitely many dimensions.

Third chapter deals with the issue of extension of the notion of the defect of a unitary matrix adapted to the special class of Hermitian unitary matrices corresponding to generalized quantum measurements POVM (*positive operator-valued measures*). We provide case studies and concrete examples of geometrical structures being examined by this tool, which allow us to draw conclusions about possibility of introduction of free parameters in special classes of POVM including *mutually unbiased bases* (MUB) and *symmetric informationally complete POVM* (SIC-POVM), and also in other interesting objects used in the foundations of quantum mechanics and theory of quantum information.

In the second part of the Thesis we concentrate on the quantum entanglement. Fourth chapter is devoted to the idea of multipartite entanglement and the long-awaited status of existence of *absolutely maximally entangled* (AME) state of four quhexes, AME(4,6). We provide elegant analytical solution along with some off-topics related to this yet-to-be-fully-understood problem. In particular, we elaborate on the problem of construction a real counterpart of such a complex state.

The last short chapter contains generalization of the notion of excess of a (real) Hadamard matrix and its applications in quantum nonlocality, bipartite entanglement and special classes of Bell inequalities with the property of quantum advantage.

We summarize all addressed topics at the end. Despite the fact that several issues have been “disentangled”, we stumbled upon many new unknown facts, which certainly require further investigation. Hence, we also present a list of open questions along with a plan of the future research.

1.2 Notation Used

We are going to employ standard mathematical notation with minor exceptions where there is no general agreement upon the style or symbols. We assume the set of natural numbers contains zero, $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$. And every time we use p (not being a subscript, nor having any subscript), it should be viewed as a prime number (Chapter 2 and 3). Bold symbols $\mathbf{p}$ and $\mathbf{q}$ in Chapter 2 are reserved for polynomials.

We denote the set of permutation, orthogonal, unitary and general matrices of size N by $\mathbb{P}(N)$, $\mathbb{O}(N)$, $\mathbb{U}(N)$, and $\mathbb{F}^{N \times N}$, respectively, where N indicates the dimension and $\mathbb{F}$ is a field of real ($\mathbb{R}$) or complex ($\mathbb{C}$) numbers. Other specific classes of matrices are defined in appropriate sections. For instance, $\mathbb{H}(N)$ denotes the set of complex Hadamard matrices (CHM) of order N .

To be consistent with the notation used in publications, when traversing between chapters, we use letters N and d to indicate dimension of the system, interchangeably. It should not cause too much confusion. Special attention is only needed in Chapter 3, where the defect of a unitary matrix (always in bold), $\mathbf{d}(U)$, might clash with the dimension d .

In many cases (mainly in Chapter 2 and 4), when presenting matrices and associated operations, we adapt the notation introduced in [4], developed in *Catalogue of Complex Hadamard Matrices* [5] and widely accepted by community, e.g. operations $\text{EXP}(\text{iM})$ and $M_1 \circ M_2$, which stand for entrywise exponential acting on M , and entrywise (Hadamard) product of two matrices M_1 and M_2 , respectively. To enhance clarity, all vanishing entries in M are represented by black dots ($\bullet$) or completely omitted. This form speeds up orientation over the structure of M and highlights its most important features. In general, we prefer concrete examples in place of abstract definitions for which necessary resources are provided. Even, for further simplification, in few cases we reduce discussions to purely pictorial description. However, occasionally we feel obliged to preserve rigorous mathematical formalism.

In the physics realm we switch to bra-ket notation and we use different (but equivalent) forms of tensor multiplication $|ab\rangle = |a, b\rangle = |a\rangle|b\rangle = |a\rangle \otimes |b\rangle$, which are chosen at the convenience according to the situation. We assume the Reader is familiar with the fundamental concepts of quantum mechanics and basics of theory of quantum information, so we intentionally omit some frequently used definitions and we avoid to explain the notions, the meaning of which should be well known or inferred directly from the context or, in the

last resort, can be found in the attached papers. We only provide detailed description of objects, which are crucial for our considerations. In particular, we consistently adhere to the standard course of quantum mechanics and the generally accepted postulates of this theory, without much deliberation about possible alternatives and different interpretations. The sections containing main results are sometimes preceded by a short and popular introduction to outline the physical background and motivation. These descriptive fragments of the work by no means aspire to be an exhaustive source of information on a given topic. We make it clear by providing specific sources and the most relevant or up-to-date references.

Chapter 2

Complex Hadamard Matrices

Chapter based on [A1], [A2].

A complex Hadamard matrix [4] H is a rescaled unitary matrix with unimodular entries

$$HH^\dagger = N\mathbb{I}_N \quad : \quad H_{jk} = e^{i2\pi\varphi_{jk}} \quad \text{for some } \varphi_{jk} \in [0, 1). \quad (2.0.1)$$

Let $\mathbb{H}(N)$ be the set of all *complex Hadamard matrices* (CHM) of size N . If matrix H has all its entries in the form of q^{th} roots of unity, $\varphi_{jk} = m_{jk}/q$ for $m_{jk} \in \mathbb{N}$, we call it a *Butson type* [6, 7]. Such matrices constitute a proper subset of CHM and will be denoted by

$$\text{BH}(N, q) \subsetneq \mathbb{H}(N). \quad (2.0.2)$$

CHM is a natural extension of a real (with only ± 1 entries) Hadamard matrix [8] and as such can be further generalized over quaternions [9] or general groups [10, 11]. Note that real Hadamard matrices form a special case of Butson type matrices, $\text{BH}(N, 2)$. Here we focus only on the pure complex variant, while we return to classical real Hadamards in Chapter 5.

We also put here the definition of *mutually unbiased bases* (MUB), which are tightly connected to CHM and relevantly motivate the searching for new examples of CHM. MUB will be recalled several times here, in Chapter 3, and Chapter 5. Let $\mathcal{B}_j = \{|\psi_1^{(j)}\rangle, \dots, |\psi_N^{(j)}\rangle\}$ for $j \in \{2, \dots, m\}$ be a collection of $2 \leq m \leq N + 1$ orthonormal bases in $\mathbb{C}^N$. We call them *mutually unbiased* if the overlap between each basis has constant magnitude,

$$|\langle \psi_a^{(j)} | \psi_b^{(k)} \rangle|^2 = \delta_{jk} \delta_{ab} + \frac{1 - \delta_{jk}}{N} \quad (2.0.3)$$

for $a, b \in \{1, 2, \dots, N\}$ and $j, k \in \{1, 2, \dots, m\}$. It is well known that the upper bound for MUB (complete set) in $\mathbb{C}^N$ is $N + 1$, which is saturated for $N = p^l$ for prime p and $l \geq 1$ [12, 13]. In general, the problem of existence of such bases (not necessarily a complete set) in non-prime-power dimensions is a major open problem, especially for $N = 6$ [14].

Given two or more MUB; $\mathcal{B}_1, \mathcal{B}_2, \dots$ one such basis can be represented by $\mathbb{I}_N$. It is then easy to infer that the remaining bases, when represented as matrices, comprise the set of different CHM. We call such matrices *mutually unbiased Hadamards* (MUH). Hence, searching for MUB of a given dimension is equivalent to searching for a particular set of CHM [15].

The role of complex Hadamard matrices in theoretical and experimental physics cannot be overestimated. Let us briefly recall the most crucial examples of applications only in quantum information theory. CHM are significant components behind the concept of *dense coding* and *quantum teleportation schemes* [16]. They form building blocks for *nice error bases* [17] and *quantum designs* [11, 18]. Constructions of *unitary error bases* (UEB), *bases of maximally entangled states* and *unitary depolarizers* directly exploit the existence of elements from $\mathbb{H}(N)$ [16, 19, 20]. Optimal *tomography of quantum states* is possible due to measurement performed by means of MUB, which — as we have just mentioned — can be built out of CHM [12, 13]. Additional applications of such matrices in pure mathematics can be found in the comprehensive monograph of Teo Banica [21].

There are many constructions of CHM. From simply rearranging of elements and/or expanding the size of a given matrix [22, 23], through more advanced mathematical apparatus involving tiling abelian groups [24], graph theory [25, 26], Golay sequences [27], and orthogonal maximal abelian $*$ -subalgebras [28]. Further examples and references are summarized in the Catalogue of CHM [5].

It is easy to notice that $\forall N : \mathbb{H}(N) \neq \emptyset$ since such an example is provided for any dimension N by the Fourier matrix F_N ,

$$F_N = \frac{1}{\sqrt{N}} \sum_{j,k=0}^{N-1} |j\rangle\langle k| \exp \left\{ \frac{2\pi i j k}{N} \right\} \in \text{BH}(N, N) \subset \mathbb{H}(N). \quad (2.0.4)$$

A bit more complicated example of a single parameter family of CHM of order $N = 6$ reads

$$T_6^{(1)}(\gamma) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & b & c & a & d \\ 1 & b & a & a & c & d \\ 1 & b & a & -a & -1 & -d \\ 1 & a & b & -1 & -a & -d \\ 1 & c & c & -c & -c & -1 \end{bmatrix}, \quad (2.0.5)$$

where an arbitrary phase γ varies continuously, $\gamma \in [\frac{1}{2}, \frac{3}{2}]$, and the unimodular numbers are

$a = \exp\{i\pi\gamma\}$, and

$$b = a^2, \quad (2.0.6)$$

$$c = \frac{-2a - 1 - b - \sqrt{a^4 + 4a^3 + 2a^2 + 4a + 1}}{2}, \quad (2.0.7)$$

$$d = \frac{-2a - 1 - b + \sqrt{a^4 + 4a^3 + 2a^2 + 4a + 1}}{2}. \quad (2.0.8)$$

Matrix $T_6^{(1)}$ is a slight modification of the first family in $\mathbb{H}(6)$ whose elements depend on each other in a nonlinear way. It was found independently in 2006 [15], and quickly shadowed by the equivalent and simpler form [28].

2.1 Classification and Invariants

The main problem concerning CHM is their classification [4, 5, 29]. Classifying all CHM of a given order, say $N = 6$, would be helpful in tackling various problems in quantum information theory, for instance the existence of MUB in this dimension. There is no simple method that can tell if a given matrix represents a new or already known example of CHM. It is mainly caused by additional degrees of freedom in $\mathbb{H}(N)$. Two matrices $H_1, H_2 \in \mathbb{H}(N)$ are called *equivalent* [30], written $H_1 \simeq H_2$, if there exist two diagonal unitary matrices $D_1, D_2 \in \mathbb{U}(N)$ and two permutation matrices $P_1, P_2 \in \mathbb{P}(N)$ such that

$$H_1 = D_1 P_1 H_2 P_2 D_2. \quad (2.1.1)$$

CHM come in a variety of forms. We distinguish here three general classes: *isolated points*, *affine* and *nonaffine families* (orbits). We say that H is an *isolated* matrix, if its neighborhood¹ contains only equivalent matrices. Otherwise, it is a part of a family of inequivalent matrices. We decorate matrices with a superscript to indicate whether it is an isolated point, e.g. isolated matrix $S_6^{(0)}$ of order six, or it represents δ -dimensional orbit (orbit depending on δ independent parameters), for instance, a single parameter orbit $T_6^{(1)}$ of order six too. The character of variability of phases φ_{jk} in $H_{jk} = e^{i2\pi\varphi_{jk}}$ as functions of orbit parameters can be linear (*affine*) or nonlinear (*nonaffine*). The latter case is represented by $T_6^{(1)}$ (2.0.5) and drawn schematically in Figure 2.1. Obviously, the dependence $c = c(a) = c(\gamma)$ in (2.0.7), where γ is the only orbit parameter, is highly nonlinear. Plethora of examples of affine families can be found in [4, 5], and the construction of a bit complicated nonaffine family will be presented in Section 2.2.2.

We will mostly present matrices in the special *dephased form* in which first row and first column consists of ones. Every CHM can be brought to its dephased form by multiplying

¹By a matrix neighborhood we understand a natural generalization of a standard point-like neighborhood extended over $\mathbb{C}^{N \times N}$ endowed with Euclidean topology.

by two diagonal unitary matrices. This *normalized* representation allows us to consider only permutation matrices in the equivalence relation, and effectively work with the $(N - 1)$ -dimensional *core* of a given matrix.

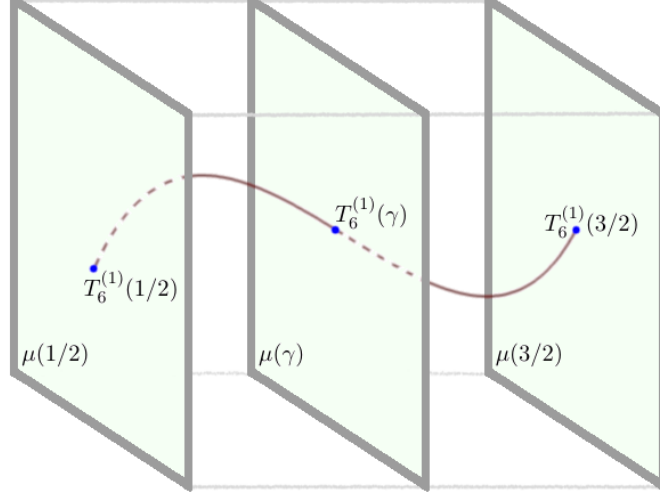


Figure 2.1: Schematic illustration of the orbit of $T_6^{(1)}(\gamma)$ (2.0.5) as a function of parameter $\frac{1}{2} \leq \gamma \leq \frac{3}{2}$. Given γ , each $\mu = \mu(\gamma)$ represents the equivalence space for $T_6^{(1)}(\gamma)$, that is the set of all possible products $D_1 P_1 T_6^{(1)}(\gamma) P_2 D_2$ for diagonal and permutation matrices defined in (2.1.1). Equivalence space may form a multidimensional continuous manifold as above, where only three particular sections are depicted. For an isolated matrix there would be only one such space.

Having equivalence relation we can introduce the notion of the quotient set $\mathbb{H}(N)/\simeq = [H_{(1)}] \cup [H_{(2)}] \cup \dots \cup [H_{(j)}] \cup \dots$, so the classification of CHM boils down to determining all equivalence classes with respect to $\simeq$. Low dimensions, $N = 2, 3, 4$, and 5 , have been completely described in [30, 31] and the first open problem arises at $N = 6$. It is widely believed that the set of six-dimensional CHM consists of a single isolated spectral matrix [32] and 4-parameter nonaffine family [33] that connects all other 6-dimensional examples,

$$\mathbb{H}(6) \stackrel{?}{=} S_6^{(0)} \cup \left\{ G_6^{(4)} \right\}. \quad (2.1.2)$$

The diversity of forms for any $N \geq 6$ prevents us from giving a single and simple answer to the question about the structure of $\mathbb{H}(N)$. The task of checking whether a given matrix belongs to a known class is not easy indeed, but there exist several methods [34, 35, 36] which can be used to classify or rule out a matrix from a given subset of CHM. We will briefly recall two of them: *defect of a unitary matrix* and the set of *Haagerup invariants* [30] as the main tools used in the rest of the chapter.

Defect of a matrix $H \in \mathbb{H}(N)$, denoted $\mathbf{d}(H)$, was introduced and investigated in [37, 38] as an algebraic tool to solve the problem of possibility of deriving from a given matrix a smooth family of inequivalent matrices. Not only it can serve as a binary oracle that tells whether it is possible (or not) to stem an orbit out of a given Hadamard matrix H , but it can also assist in identifying and classifying the equivalence classes. We skip here all mathematical formalism related to this concept however, in Chapter 3 we will present the sketch of derivation of a similar tool in the context of Hermitian unitary matrices. Informally, we can treat $\mathbf{d}(H)$ as a non-negative number associated with a matrix H , which provides the information about possible independent directions on the manifold of $\sqrt{N}\mathbf{U}(N)$ that H can follow preserving the property of being CHM. In other words, non-zero value of $\mathbf{d}(H)$ determines the upper bound of dimensionality of a family that H might (but not necessarily should) belong to. In particular, we will extensively use the following fact (Lemma 3.3 in [4]):

$$\mathbf{d}(H_N) = 0 \implies H_N = H_N^{(0)}, \quad (2.1.3)$$

so vanishing defect implies that H_N cannot be part of any orbit of inequivalent matrices, and it is an isolated Hadamard matrix. However, this is only one-way criterion and we know examples of isolated matrices for which defect does not vanish [39]. Matrix H which has non-zero defect and is a member of multidimensional orbit depending on several parameters γ_j for $1 < j \leq \mathbf{d}(H)$ can have different defects for different values of γ_j . This is simply explained by the fact that such hyperorbit might intersect other orbits of different characteristics.

The Haagerup set [30] of H , denoted by $\Lambda(H)$ is defined by all possible products of quartets of matrix elements

$$\Lambda(H) = \left\{ H_{jk} H_{lm} H_{jm}^* H_{lk}^* : j, k, l, m \in \{1, \dots, N\} \right\}, \quad (2.1.4)$$

where $*$ is complex conjugate. Both, defect and Haagerup set are invariant with respect to equivalence relation (2.1.1), which means that $\mathbf{d}(H) = \mathbf{d}(P_1 D_1 H D_2 P_2)$ and $\Lambda(H) = \Lambda(P_1 D_1 H D_2 P_2)$, hence we can formulate another helpful, criterion

$$\Lambda(H_1) \neq \Lambda(H_2) \implies H_1 \not\sim H_2. \quad (2.1.5)$$

Again, the converse is not true, and it is possible to find two inequivalent matrices with identical sets Λ . Nevertheless, even though (2.1.3) and (2.1.5) work only one way, they will be extremely helpful in discriminating several cases of new matrices.

We are ready to proceed to extend the set of known CHM. As the work on dimension $N = 6$ can be roughly considered done and the next 7-dimensional set proved to be exceptionally hard, we start with $N = 8$.

2.2 Extension of the Set $\mathbb{H}(8)$ of CHM of Order 8

As of 2018, the set of CHM of size eight contained the following elements: $D_8^{(4)}$ [40], $S_8^{(4)}$ [24], Fourier $F_8^{(5)}$, tensor product of two Fouriers $F_2 \otimes F_4 \in \text{B}\mathbb{H}(8, 4)$ [4], and $V_8^{(0)}$ [41]. Also a collection of Butson type matrices introduced in [42] contribute to $\mathbb{H}(8)$. It will be shown below that this list of matrices in $\mathbb{H}(8)$ can be extended.

2.2.1 Random Walk over Core Phases

Numerical algorithm used to search for new matrices $H \in \mathbb{H}(8)$ comes down to three simple stages:

1. draw phases φ_{jk} of the core of $M = M(\varphi_{jk})$ at random, possibly fix some of them to impose a desired pattern,
2. gradually change the values of (unfixed) phases in order to minimize a target function

$$\mathcal{Z}(M) = \|MM^\dagger - N\mathbb{I}_N\|_{\text{F}}, \quad (2.2.1)$$

where subscript F denotes Frobenius norm of a matrix and, here, $N = 8$,

3. check the output for belonging to a given equivalence class and retrieve the analytical form.

For $N \in \{6, 7, 8, 9, 10\}$ almost every initial (randomly chosen) matrix M swiftly converges to H such that $\mathcal{Z}(H) \approx 0$, so H can be considered as a numerical approximation of CHM with arbitrarily high precision. However, it is very common that in the last phase we cannot simply discard or accept H due to the lack of mathematical tools that can unequivocally determine the status of the newly obtained matrix. In general the most difficult task is to recover analytical values of the numerical result. This can be slowly done in a systematic process of fixing phases and reiterating the optimization procedure until we begin to observe more easy-to-guess numbers. With this method we can quite efficiently determine individual matrices. If we anticipate that matrix may belong to a family (especially, a nonaffine family), we should fix phases in a clever way, customized to a particular problem, so that subsequent optimizations ought to return some apparent patterns. Eventually, mixing all together, and solving orthogonality constraints for H , we can get ultimate functional dependencies among the entries of the matrix.

2.2.2 New Nonaffine Family $T_8^{(1)}$

During numerical generation of matrices we noted that in the sequence of many outputs there is one, T_8 , such that its defect amounts to 3. This specific value had not been observed before

for any matrix in $\mathbb{H}(8)$, and according to the aforementioned fact that defect is invariant with respect to permutations, it was a clear signature that T_8 may represent a new class of equivalence. Then, after several attempts, we were able to extrapolate analytically some numerically expressed relations in the matrix core and reconstruct entire character of the matrix T_8 admitting the form of a nonaffine family:

$$T_8^{(1)}(\gamma) = \text{EXP} \left(i \frac{\pi}{10} R_8 \right) \circ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & y & z & -\frac{yz}{x} & 1 & 1 & 1 \\ 1 & -\frac{u}{y} & \frac{u}{x} & -\frac{uz}{xy} & -\frac{uz}{x^2} & 1 & 1 & 1 \\ 1 & y & x & -\frac{yz}{x} & z & 1 & 1 & 1 \\ 1 & \frac{u}{x} & -\frac{u}{y} & -\frac{uz}{x^2} & -\frac{uz}{xy} & 1 & 1 & 1 \\ 1 & -i\frac{x}{z} & i\frac{x}{z} & -i\frac{z}{x} & i\frac{z}{x} & 1 & 1 & 1 \\ 1 & u & -u & -\frac{uz^2}{x^2} & \frac{uz^2}{x^2} & 1 & 1 & 1 \\ 1 & i\frac{uz}{x} & i\frac{uz}{x} & -i\frac{uz}{x} & -i\frac{uz}{x} & 1 & 1 & 1 \end{bmatrix} \quad (2.2.2)$$

where the matrix of phases reads ($\bullet = 0$)

$$R_8 = \begin{bmatrix} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet & 3 & 15 & 18 \\ \bullet & 8 & 8 & 8 & 8 & 13 & 15 & 8 \\ \bullet & 2 & 2 & 2 & 2 & 17 & 5 & 2 \\ \bullet & \bullet & \bullet & \bullet & \bullet & 7 & 5 & 12 \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & 10 & 10 \\ \bullet & \bullet & \bullet & \bullet & \bullet & 10 & \bullet & 10 \\ \bullet & \bullet & \bullet & \bullet & \bullet & 10 & 10 & \bullet \end{bmatrix}, \quad (2.2.3)$$

and depends on a single parameter $\gamma \in [\frac{2}{5}, \frac{4}{5}] \cup [1, \frac{7}{5}]$ hidden in $x = e^{i\pi\gamma}$. The range of the orbit parameter γ , being the sum of two intervals, is given only as the approximation. Accurate limits require complex calculations, but the presented scope is absolutely sufficient to ensure unimodularity of entries of $T_8^{(1)}$. For the same reason, formulas for $y = y(x)$, $z = z(x, y)$, and $u = u(x, y, z)$ which are overly complicated, should not be reproduced here in full. Their explicit forms do not add anything to the further analysis, perhaps except the fact how rich the structure of $\mathbb{H}(N)$ is as $N \rightarrow \infty$. Detailed description of $T_8^{(1)}$ can be found in [A1].

Meanwhile, let us observe that for particular values of γ , two different Butson type matrices can be extracted from the orbit $T_8^{(1)}(\gamma)$. For $\gamma \in \{\frac{1}{2}, 1, \frac{13}{10}\}$ we obtain three matrices

equivalent to

$$B_{8a} = \text{EXP} \left(i \frac{\pi}{10} \begin{bmatrix} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & 5 & 10 & 13 & 8 & 3 & 15 & 18 \\ \bullet & 10 & 5 & 18 & 3 & 13 & 15 & 8 \\ \bullet & 12 & 7 & 10 & 15 & 17 & 5 & 2 \\ \bullet & 17 & 2 & 15 & 10 & 7 & 5 & 12 \\ \bullet & 7 & 17 & 3 & 13 & \bullet & 10 & 10 \\ \bullet & 2 & 12 & 8 & 18 & 10 & \bullet & 10 \\ \bullet & 15 & 15 & 5 & 5 & 10 & 10 & \bullet \end{bmatrix} \right) \in \text{BH}(8, 20), \quad (2.2.4)$$

and another Butson type matrix for $\gamma = \frac{4}{5}$

$$B_{8b} = \text{EXP} \left(i \frac{\pi}{10} \begin{bmatrix} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & 8 & 10 & 13 & 5 & 3 & 15 & 18 \\ \bullet & 18 & 10 & 3 & 5 & 13 & 15 & 8 \\ \bullet & 12 & 10 & 7 & 15 & 17 & 5 & 2 \\ \bullet & 2 & 10 & 17 & 15 & 7 & 5 & 12 \\ \bullet & 10 & \bullet & \bullet & 10 & \bullet & 10 & 10 \\ \bullet & 10 & \bullet & 10 & \bullet & 10 & \bullet & 10 \\ \bullet & \bullet & \bullet & 10 & 10 & 10 & 10 & \bullet \end{bmatrix} \right) \in \text{BH}(8, 20). \quad (2.2.5)$$

Different defects $\mathbf{d}(B_{8a}) = 7$ and $\mathbf{d}(B_{8b}) = 11$ prove inequivalence of the two representatives, and value of $q = 20$ (2.0.2) confirms the novelty of the finding, since at the time of publication of [A1], such matrices did not appear in the literature nor in online catalogs [5, 43].

The defect $\mathbf{d}(T_8^{(1)}) = 3$ theoretically allows $T_8^{(1)}$ to be a part of at most three-dimensional family, and during the laborious numerical analysis, we encountered strong numerical evidence supporting such possibility; $\{T_8^{(1)}\} \subset \{T_8^{(3)}\}$. However, the complexity of the internal structure prevents us from determining (or even from guessing) the explicit formulas of such a family. At this stage we should consider Eq. (2.2.2) as the final form.

Dimension $N = 8 = 2^3$, being a square of prime, facilitates several constructions [44], implications and applications mentioned at the beginning of this section. Nevertheless, still, apart from a one step further in full classification of CHM, we can use the matrix $T_8^{(1)}$ as an ingredient to build new pairs of MUB, UEB, quantum gates, or just special orthogonal bases in $\mathbb{C}^8$.

In the next section, we present another method to obtain CHM numerically, and later we will (re)use it as a starting point for a more general construction leading to special families of CHM.

2.3 Extension of the Set $\mathbb{H}(9)$ of CHM of Order 9

Similarly to $\mathbb{H}(8)$, all known CHM of order $N = 9$ forming $\mathbb{H}(9)$ can be listed as follows: $F_3 \otimes F_3$ and $F_9^{(4)}$ [4], $S_9^{(0)}$ [45], $B_9^{(0)}$ [28], $N_9^{(0)}$ [28], and $K_9^{(2)}$ [46]. Again, a number of Butson type matrices [42] must be added to complete the picture.

2.3.1 Sinkhorn Algorithm Revisited

Before we continue the subject of CHM, we shall recall another numerical recipe proposed by Richard Sinkhorn in 1964 that was originally designed to generate (random) bistochastic matrices [47, 48].

Suppose we have a mathematical object (e.g. matrix) which is characterized by at least two properties $\mathcal{P}_j$ ($j \geq 1$). They need not be complementary, nor disjoint. For example $\mathbb{H}(N)$ can be equivalently redefined as intersection of two sets (properties): rescaled unitary matrices and unimodular matrices,

$$\mathbb{H}(N) = \sqrt{N}\mathbb{U}(N) \cap \mathbb{T}(N), \quad (2.3.1)$$

where $\mathbb{T}(N)$ denotes an N -dimensional torus.

To get a matrix M^* having all desired properties, $M^* \in \mathcal{P}_1 \cap \mathcal{P}_2 \cap \dots$ we can try to perform alternating mappings (projections) π_j onto $\mathcal{P}_j$, applied to a given initial argument M , so that $\pi_j(M) \in \mathcal{P}_j$. Provided that such iterative procedure exhibits contractive behavior, it should also be convergent to an element in a non-empty subset $\mathcal{P}$, common for all $\mathcal{P}_j$,

$$\lim_{k \rightarrow \infty} \left(\prod_{j=1}^k \pi_j \right) (M) = M^* \in \mathcal{P} \subset \bigcap_j \mathcal{P}_j, \quad (2.3.2)$$

where the product of π_j 's above should be understood in terms of map compositions.

In the particular case of CHM, the algorithm takes the following form:

1. draw a complex matrix $M \in (\mathbb{C} \setminus \{(0, 0)\})^{N \times N}$ at random (we exclude zeros to avoid problems in the next step),
2. normalize (unimodularize) each entry of M so $M \rightarrow M' = \pi_1(M) \in \mathbb{T}^N$ such that $M'_{jk} = M_{jk}/|M_{jk}|$,
3. perform polar decomposition of $M' = U\sqrt{M'^{\dagger}M'}$ to obtain (nearest) unitary matrix $U = M'/\sqrt{M'^{\dagger}M'}$, so $M' \rightarrow M'' = \pi_2(M')$ such that $M'' = M'/\sqrt{M'^{\dagger}M'}$,
4. repeat steps 2. and 3. until $\mathcal{Z}(\pi_2(\pi_1(\dots(\pi_1(M))\dots))) \approx 0$ up to a given precision (where the target function $\mathcal{Z}$ is defined in (2.2.1)).

The convergence of the alternating procedure is assured in the case of convexity of all components $\mathcal{P}_j$ [49]. Despite the fact that none of subsets determining $\mathbb{H}(N)$ is convex, the above method applied to an initial matrix $M \in (\mathbb{C} \setminus \{(0,0)\})^{N \times N}$ can effectively produce very accurate approximations of CHM from $\mathbb{H}(N)$. We are not going to investigate mathematical details of this algorithm, instead, we will use it as a reliable tool that proved its fitness in many numerical simulations. The advantage of this technique over the previous one is the speed and performance. However, one pays the price of loosing full control over the matrix structure, as it is no longer possible to easily fix given entries of M imposing a concrete appearance. Nevertheless, as we will see, this method can produce matrices with a surprisingly high degree of symmetry. Original variant of this algorithm was successfully used in construction of bistochastic matrices [50]. Slightly modified version will provide the main result in Chapter 4. In the next section we present a 9-dimensional CHM obtained in this way, the form of which will trigger additional observations and further results.

2.3.2 A Novel Isolated Matrix $T_9^{(0)}$

We present another CHM obtained during numerical studies with the help of Sinkhorn algorithm described in previous section.² Originally, after dephasing,³ which sets all entries of the first row and the first column to one, the matrix emerged in the form of

$$T_9 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & d & a^* & c^* & b^* & c & b & d^* \\ 1 & b & c & b^* & a & d^* & a^* & d & c^* \\ 1 & c & b^* & c^* & d & a & d^* & a^* & b \\ 1 & b^* & c^* & b & a^* & d & a & d^* & c \\ 1 & d & a^* & d^* & b & c^* & b^* & c & a \\ 1 & a^* & d^* & a & c & b & c^* & b^* & d \\ 1 & c^* & b & c & d^* & a^* & d & a & b^* \\ 1 & d^* & a & d & b^* & c & b & c^* & a^* \end{bmatrix} \quad (2.3.3)$$

$$\text{with :} \quad a \approx -0.3396 + 0.9406i, \quad b \approx -0.9635 + 0.2676i, \quad (2.3.4)$$

$$c \approx -0.0365 + 0.9993i, \quad d \approx +0.8396 + 0.5432i, \quad (2.3.5)$$

and $x^* = \frac{1}{x}$ denoting complex conjugate of unimodular numbers. As in the previous case, attention was focused on this particular example because of the individual features that distinguish it from other 9-dimensional candidates. Namely, its defect vanishes and rough analysis shows that it does not belong to the Butson type class (2.0.2).

²No phases were fixed, all entries were initially drawn at random according to normal distribution and such initial point was supplied to the algorithm.

³Usually matrices produced in this way are not in the dephased form. We call them *undephased*.

There are only four different parameters a , b , c , and d in T_9 , which is very favorable circumstance (in comparison with a core of 64 different values that in general would make it hardly possible to deal with). To express these parameters analytically, one can try to solve the unitarity constraints for T_9 . They form a system of five nonlinear equations with four variables

$$\left\{ \begin{array}{l} 1 + a + \frac{1}{a} + b + \frac{1}{b} + c + \frac{1}{c} + d + \frac{1}{d} = 0, \\ 1 + a^2 + \frac{1}{a^2} + b^2 + \frac{1}{b^2} + c^2 + \frac{1}{c^2} + d^2 + \frac{1}{d^2} = 0, \\ 1 + \frac{a}{b} + \frac{b}{a} + \frac{b}{d} + \frac{d}{b} + \frac{c}{d} + \frac{d}{c} + ac + \frac{1}{ac} = 0, \\ 1 + \frac{a}{c} + \frac{c}{a} + ab + \frac{1}{ab} + cd + \frac{1}{cd} + bd + \frac{1}{bd} = 0, \\ 1 + \frac{a}{d} + \frac{d}{a} + \frac{b}{c} + \frac{c}{b} + bc + \frac{1}{bc} + ad + \frac{1}{ad} = 0. \end{array} \right. \quad (2.3.6)$$

There are many solutions of the above system, including those which do not meet the condition of unimodularity. Supported by numerical software, we find that 128 possible quadruplets (a, b, c, d) fulfilling (2.3.6) can be divided onto three distinct classes. Class a) solutions that correspond to T_9 , class b) can be used to build a Butson type matrix of size 9, and class c) to be discarded as they do not provide CHM. We should not continue the thread about the Butson solution, because in this very case it does not reveal anything new. Let us focus on the class a) — solution for T_9 .

After rearranging, reducing and simplifying (2.3.6), we observe that numbers in (2.3.4) and (2.3.5) can be calculated as roots of two monic palindromic polynomials⁴ or degree 12 (see Figure 2.2)

$$\mathbf{p}_1(x) = (1, -3, 9, -16, -12, 6, \underline{3}, 6, -12, -16, 9, -3, 1), \quad (2.3.7)$$

$$\mathbf{p}_2(x) = (1, 6, 15, 26, 3, -24, \underline{-27}, -24, 3, 26, 15, 6, 1). \quad (2.3.8)$$

We exploit the well known fact from algebra of palindromic polynomials which says that every such $\mathbf{p}(x)$ of even degree $2k$ can be expressed as

$$\mathbf{p}(x) = x^k \mathbf{q}(x + 1/x), \quad (2.3.9)$$

where $\mathbf{q}$ is another polynomial (in variable $y = x + 1/x$) of degree k (cf. Section C.2 in [29]). Sometimes, this can shorten the form of $\mathbf{p}(x)$ significantly. Indeed, in our case the problem

⁴Monic polynomial $\mathbf{p}$ of degree n has leading coefficient $c_n = 1$. For brevity, we write only coefficients of $\mathbf{p}$ (in ascending order). For example, the standard polynomial notation $\mathbf{p}(x) = 1 + 2x + 3x^2 + 2x^3 + x^4$ corresponds to $(1, 2, \underline{3}, 2, 1)$, where we emphasized the middle factor to ease confirmation that they really form a palindromic sequence: $c_j = c_{n-j}$ for $j \in \{0, \dots, n\}$.

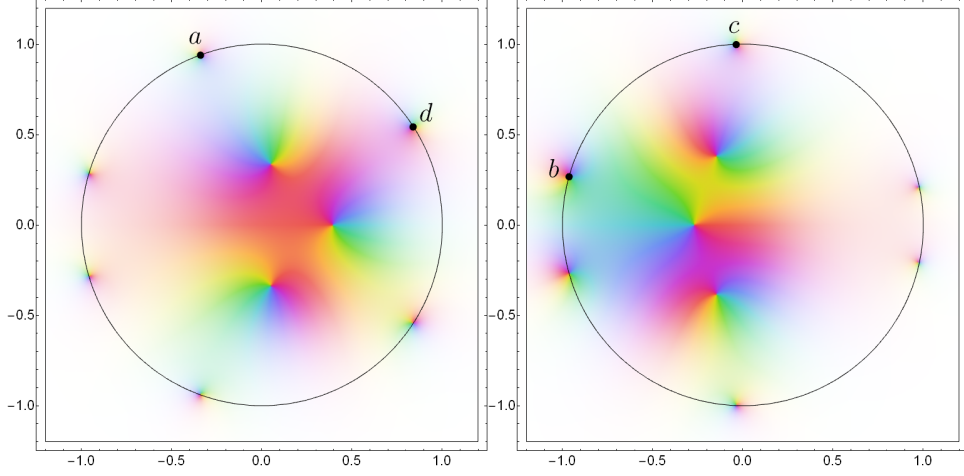


Figure 2.2: Complex roots of two palindromic polynomials $\mathbf{p}_1$ and $\mathbf{p}_2$ associated with unitarity constraints (2.3.6) for T_9 . Six of them (excluding complex conjugates) from the unit circle contain four parameters a , b , c , and d (2.3.4)–(2.3.5) that characterize T_9 .

can be reduced to calculating the roots of polynomials of 3rd degree and, eventually, we arrive at⁵

$$a = \sqrt{\gamma_1^2 - 1} - \gamma_1, \quad b = \sqrt{\gamma_2^2 - 1} - \gamma_2, \quad (2.3.10)$$

$$c = \sqrt{\gamma_3^2 - 1} + \gamma_3, \quad d = \sqrt{\gamma_4^2 - 1} + \gamma_4, \quad (2.3.11)$$

where

$$\gamma_1 = \frac{1}{4} \sqrt{1 - \zeta_2 - \zeta_2^*} - \frac{1}{4}, \quad \gamma_2 = \frac{\sqrt{2}}{2} \sqrt{1 - \zeta_1 - \zeta_1^*} + \frac{1}{2}, \quad (2.3.12)$$

$$\gamma_4 = \frac{1}{4} \sqrt{1 - \zeta_2 - \zeta_2^*} + \frac{1}{4}, \quad \gamma_3 = \frac{\sqrt{2}}{2} \sqrt{1 - \zeta_1 - \zeta_1^*} - \frac{1}{2}, \quad (2.3.13)$$

and

$$\zeta_1 = \frac{\omega}{2^{4/3}} \left(43 - 3i\sqrt{771} \right)^{1/3}, \quad (2.3.14)$$

$$\zeta_2 = 2^{5/3} \omega^2 \left(43 + 3i\sqrt{771} \right)^{1/3} \quad \text{with} \quad \omega = \exp \left\{ i\pi \frac{5}{3} \right\}. \quad (2.3.15)$$

Analytic expressions for a , b , c and d match perfectly numerical values in (2.3.4) and (2.3.5).

Now we can formally confirm that $T_9 \in \mathbb{H}(9)$ and its defect $\mathbf{d}(T_9) = 0$, so $T_9 = T_9^{(0)}$ is an isolated matrix. Obviously $T_9 \notin \text{BH}(9, q)$ for any q . Since the only known isolated

⁵The Author is indebted to Oliver Reardon-Smith for pointing out an error in earlier calculations.

matrices in $\mathbb{H}(9)$ are $N_9^{(0)}$ whose entries belong to $\mathbb{Q}[\frac{1}{4}(1 - i\sqrt{15})]$, $S_9^{(0)} \in \text{BH}(9, 6)$, and several other Butson type examples, we ultimately prove that the matrix $T_9^{(0)}$ is the next new representative of 9-dimensional set of CHM.

2.4 Families of (Isolated) Complex Hadamard Matrices

Up to this moment we were generating CHM numerically and then, in the post-processing phase, they underwent tedious analysis to be finally presented in an analytic form. In this section, we propose a more systematic construction which might lead to infinite families of CHM with additional property of being isolated.

Let us recall the definition of an object that will be intensively studied in Chapter 4. A *Latin square* (LS) of size N is an array of $N \times N$ elements (numbers or symbols) such that in every row and in every column there is no repetition of two identical components. Two Latin squares are said to be *orthogonal* (OLS) if, when superimposed, they contain distinct (ordered) pairs of symbols [51]. The example below explains why OLS are also called Graeco-Latin squares

$$\begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix} \cup \begin{bmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \\ \gamma & \alpha & \beta \end{bmatrix} = \begin{bmatrix} a\alpha & b\beta & c\gamma \\ c\beta & a\gamma & b\alpha \\ b\gamma & c\alpha & a\beta \end{bmatrix}. \quad (2.4.1)$$

There are known connections that employ both of LS and (complex) Hadamard matrices and combine them together in order to build more advanced structures. One of these is a method of building MUB in square dimensions [52]. Also, they are tightly connected via the construction of orthonormal bases of unitary operators, for which the existence of Hadamard matrix and LS is required [16, 20]. Also, the existence of special classes of (real) Hadamard matrices can be related to orthogonal LS [53]. However, it is not known to us, whether there exists a systematic method of constructing complex Hadamard matrices that explicitly makes use of the idea of LS. In the recent paper [54] contributing to the field of statistical analysis, the author introduces the term “Latin Hadamard Matrix”, but beside a familiar name, it is by no means related to our current problem.

Our proposition directly involves the concept of LS (or even more general combinatorial structures). As we have seen, to build a CHM one can a priori impose certain initial configuration on entries in a matrix (like in Eq. (2.3.3)), and solve the associated system of nonlinear equations representing unitarity constraints. However, not every configuration is valid, as there might exist some patterns for which the only solution is the empty set. This technique, already presented in the previous section, gave rise to a new matrix $T_9^{(0)} \in \mathbb{H}(9)$. We will show that particularly chosen configuration of entries leads to several other previously unknown CHM of order $N \geq 9$, and may set the ground for a more general conjecture.

2.4.1 Family of Complex Hadamard Matrices L_N

We will follow a heuristic reasoning. Consider again the very first form of $T_9^{(0)}$ (2.3.3). Permuting rows and columns allows us to present it equivalently as

$$T_9^{(0)} \simeq \left[\begin{array}{c|c|c|c|c|c|c|c} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & a & a^* & b & b^* & c & c^* & d & d^* \\ 1 & a^* & a & b^* & b & c^* & c & d^* & d \\ \hline 1 & b & b^* & d & d^* & a^* & a & c & c^* \\ 1 & b^* & b & d^* & d & a & a^* & c^* & c \\ \hline 1 & c & c^* & a^* & a & d^* & d & b^* & b \\ 1 & c^* & c & a & a^* & d & d^* & b & b^* \\ \hline 1 & d & d^* & c & c^* & b^* & b & a^* & a \\ 1 & d^* & d & c^* & c & b & b^* & a & a^* \end{array} \right], \quad (2.4.2)$$

where grid lines additionally accent the internal structure. Suddenly, the core of the matrix resembles symmetric LS with additional complex conjugates (*) in few places,

$$\text{core}(T_9^{(0)}) = \left[\begin{array}{cc|cc} \boxed{A} & \boxed{B} & \boxed{C} & \boxed{D} \\ \boxed{B} & \boxed{D} & \boxed{A}^* & \boxed{C} \\ \boxed{C} & \boxed{A}^* & \boxed{D}^* & \boxed{B}^* \\ \boxed{D} & \boxed{C} & \boxed{B}^* & \boxed{A}^* \end{array} \right], \quad (2.4.3)$$

where every $\boxed{X}$ corresponds to a 2×2 matrix

$$\boxed{X} = \begin{bmatrix} x & x^* \\ x^* & x \end{bmatrix} \quad (2.4.4)$$

for $(x, X) \in \{(a, A), (b, B), (c, C), (d, D)\}$. This observation may gently suggest a deeper relationship between the CHM and LS. Let us tentatively propose a formal construction and then test it for several dimensions.

Define

$$L_N = \begin{bmatrix} 1 & 1^{1 \times (N-1)} \\ 1^{(N-1) \times 1} & \text{core}(L_N) \end{bmatrix} \in \mathbb{C}^{N \times N}, \quad (2.4.5)$$

where $1^{a \times b}$ denotes vectors of ones of size $a \times b$ and

$$\text{core}(L_N) = \text{circ} \left(\left[\begin{array}{cc} c_0 & c_0^* \\ c_0^* & c_0 \end{array} \right], \left[\begin{array}{cc} c_1 & c_1^* \\ c_1^* & c_1 \end{array} \right], \dots, \left[\begin{array}{cc} c_{n-1} & c_{n-1}^* \\ c_{n-1}^* & c_{n-1} \end{array} \right] \right) : c_j \in \mathbb{C} \quad (2.4.6)$$

forms a submatrix being a (2×2) -block circulant Latin square⁶ of size $N - 1$ with $n = (N - 3)/2$. By construction N must be odd. The question is: For what values of N , the matrix L_N can be a member of the set $\mathbb{H}(N)$ of complex Hadamard matrices?

⁶Note that we do not introduce complex conjugates in blocks, as it was in the case of $T_9^{(0)}$ (2.4.2).

Given N , we can immediately build L_N , write unitarity constraints and try to solve them. It turned out that this particular construction stemming from the circulant LS provides CHM only under one additional restriction. Namely, we can find a solution only in every second odd dimension, $N = 3 + 4k$ for $k \in \mathbb{N}_0$. Due to circulant symmetries, the total number of possible equations forming a nonlinear system associated with unitarity constraints can be reduced from $N(N-1)/2$ to only $2 + 3k$ such equations with $k \geq 0$. This significant simplification allows us to solve such systems for N ranging from 11 to 127 with a very high precision, and initial analysis shows that in each case the defect of L_N vanishes and $L_N \notin \text{BH}(N, q)$ for any $1 < q < 2^{16}$.

Obviously for $N = 3$ we recover the well known Fourier matrix $F_3^{(0)}$ as well as $F_7^{(0)}$ for $k = 1$ and $N = 7$. But for $k \geq 2$ which implies $N \geq 11$, all constructed matrices are believed to be new as the fact of being isolated non-Butson-like matrices automatically excludes them from many known families. Additionally, computer assisted proof confirms that the cardinalities of the Haagerup invariants (2.1.4) are unique. For $N = 11$ we have

$$\#\Lambda \left(C_{11A}^{(0)} \right) = \#\Lambda \left(C_{11B}^{(0)} \right) = 5, \quad (2.4.7)$$

$$\#\Lambda \left(N_{11A}^{(0)} \right) = \#\Lambda \left(N_{11B}^{(0)} \right) = \#\Lambda \left(N_{11C}^{(0)} \right) = 10, \quad (2.4.8)$$

$$\#\Lambda \left(F_{11}^{(0)} \right) = 11, \quad (2.4.9)$$

$$\#\Lambda \left(Q_{11A}^{(0)} \right) = \#\Lambda \left(Q_{11B}^{(0)} \right) = 63, \quad (2.4.10)$$

$$\#\Lambda \left(L_{11}^{(0)} \right) = \mathbf{191}, \quad (2.4.11)$$

and similarly for $N = 15$

$$\#\Lambda \left(A_{15A}^{(0)} \right) = \#\Lambda \left(A_{15B}^{(0)} \right) = 5, \quad (2.4.12)$$

$$\#\Lambda \left(A_{15G}^{(0)} \right) = \#\Lambda \left(A_{15H}^{(0)} \right) = 38, \quad (2.4.13)$$

$$\#\Lambda \left(L_{15}^{(0)} \right) = \mathbf{461}. \quad (2.4.14)$$

There is no need to check invariants in higher dimensions because, to the best of our knowledge, no isolated matrices of this size (apart of Butson matrices [43, 45]) were ever presented in the literature. All these observations allow us to formulate

Conjecture 1. *For any $k \in \mathbb{N}_0$ and $N = 3 + 4k$, there exists an isolated matrix $L_N^{(0)} \in \mathbb{H}(N)$ which is not of the Butson type.*

Before we comment the possible implications of this conjecture, in the next section we shall introduce even simpler method producing a sequence of matrices with identical properties.

2.4.2 Family of Complex Hadamard Matrices V_N

Instead of struggling with a circulant core, let us simply analyze entire circulant matrix

$$V_N = \text{circ}[c_0, c_1, c_2, \dots, c_{N-1}] \in \mathbb{C}^{N \times N} \quad : \quad c_j \in \mathbb{C}. \quad (2.4.15)$$

Unusual undeprased representation of V_N provides an extremely nice and compact form of the unitarity constraints:

$$\sum_{j=0}^{N-1} \frac{c_j}{c_{(j+k) \bmod N}} = 0 \quad \text{for} \quad k \in \{1, 2, \dots, N-1\}. \quad (2.4.16)$$

This time the above $N-1$ nonlinear equations for $c_j \in \mathbb{C}$ can be solved in any dimension $6 \leq N \leq 64$ resulting in a sequence of isolated and non-Butson matrices. We intentionally discarded all solutions reproducing Butson type matrices as it is very unlikely to find something new in this way. Also, we ignored the possibility of getting something new for $9 \leq N \leq 16$ as these cases have been studied for a long time. Instead we focused on checking how far we can go with N still getting matrices with the given properties, to draw

Conjecture 2. *For any $N \geq 6$ the solution of Eq. (2.4.16) contains at least one isolated CHM matrix $V_N^{(0)}$ which is not of the Butson type.*

While for the previous sequence of L_N numerical simulations suggest that each (proper) solution leads only to an isolated matrix, for V_N the defect is not strictly restricted to zero. We observed such a situation already for $N = 8$, and also for some slightly higher orders. However, the bigger N , the less chance of hitting any potential representative of a multidimensional family. A curiosity concerning $N = 8$ will be explained in the last section of this chapter.

2.5 Comment on the Structure of the Set $\mathbb{H}(8)$

In light of the facts from the previous sections, we end this chapter with two short remarks concerning Elser's results from 2011. Veit Elser found the matrix $V_8^{(0)}$ quite accidentally as a by-product of computations with a completely different purpose [41]. It has been identified as an isolated point, put into the Catalogue of CHM [5] and apparently forgotten for years.

Its nice undephased structure reads

$$V_8^{(0)} = \begin{bmatrix} -1 & -1 & b & b & c & c & a & a \\ -1 & b & -1 & c & b & a & c & -a \\ b & -1 & c & -1 & a & b & -a & c \\ b & c & -1 & a & -1 & -a & b & -c \\ c & b & a & -1 & -a & -1 & -c & b \\ c & a & b & -a & -1 & -c & -1 & -b \\ a & c & -a & b & -c & -1 & -b & -1 \\ a & -a & c & -c & b & -b & -1 & 1 \end{bmatrix}. \quad (2.5.1)$$

The shape of the characteristic bands of numbers revolving symmetrically around the diagonals remains the mystery of the Sinkhorn's algorithm that was used to find this matrix. The only difference in the Elser's version of the routine was that he used QR decomposition instead of polar decomposition, to get a projection onto the set $\mathbb{U}(8)$.

Firstly, let us quickly resolve one issue concerning $V_8^{(0)}$ and recover its pure analytic form. Unitarity constraints for $V_8^{(0)}$

$$\begin{cases} -\frac{1}{b} - b + \frac{b}{c} + \frac{c}{b} + \frac{c}{a} + \frac{a}{c} = 0, \\ -\frac{1}{b} - b - \frac{1}{c} - c - \frac{c}{a} - \frac{a}{c} + \frac{b}{a} + \frac{a}{b} = 0, \\ \frac{1}{c} + c + \frac{1}{a} + a + \frac{b}{a} + \frac{a}{b} = 0, \end{cases} \quad (2.5.2)$$

can be rearranged as in the case of $T_9^{(0)}$ and presented in the form of a monic palindromic polynomial $\mathbf{p}$, so the set of roots of $\mathbf{p}$ contains parameters a , b , and c . Seemingly, the less parameters the better, since computational complexity grows rapidly with dimension $N \gg 1$. But in this case, with only three parameters and very special symmetries among the entries of $V_8^{(0)}$, the polynomial $\mathbf{p}$ turns out to be more complicated than the one for $T_9^{(0)}$, and its degree is as much as 16. Thus, to save space, we show only the first half of its 17 coefficients

$$\mathbf{p}(x) = (1, 16, 64, 16, -332, -1040, -1984, -2832, -3194, \dots) \quad (2.5.3)$$

Fortunately, using (2.3.9), it can be simply reduced to an octic polynomial $\mathbf{q}(x)$,

$$\mathbf{q}(x) = (-16, 256, -96, -896, -696, -96, 56, 16, 1), \quad (2.5.4)$$

which can be further factorized into

$$\begin{aligned} \mathbf{q}(x) &= (x^4 + 8x^3 + \alpha(0)x^2 + \beta(0)x + \gamma(0)) \times \\ &\times (x^4 + 8x^3 + \alpha(1)x^2 + \beta(1)x + \gamma(1)) \end{aligned} \quad (2.5.5)$$

where

$$\alpha(\nu) = -4 + 2(-1)^\nu \sqrt{116 - 2\sqrt{2}}, \quad (2.5.6)$$

$$\beta(\nu) = -16 + 8(-1)^\nu \sqrt{10 - \sqrt{2}}, \quad (2.5.7)$$

$$\gamma(\nu) = -4\sqrt{2} + 4 - 4(-1)^\nu \sqrt{4 - 2\sqrt{2}}, \quad (2.5.8)$$

and $\nu \in \{0, 1\}$. Applying well known formulas for roots of a quatric polynomial and taking into account all changes of variables, we can obtain analytically all the triplets that fully determine $V_8^{(0)}$. Due to the complicated character of the final results we do not present them here. An example solution reads⁷

$$a \approx -0.6509 \mp 0.7592i, \quad b \approx -0.7799 \pm 0.6258i, \quad c \approx +0.6183 \mp 0.7859i. \quad (2.5.9)$$

Hence, $V_8^{(0)}$ can be formally accepted as the (isolated) member of $\mathbb{H}(8)$. The matrix $V_8^{(0)}$ with non-commensurable phases cannot belong to the Butson class.

Secondly, the sequence V_N presented in the previous section⁸ tightly relates $V_8^{(0)}$ with other 8-dimensional matrices. Surprisingly, the unitarity constraints (2.4.16) for $N = 8$ include the solution for matrices equivalent to $V_8^{(0)}$, $A_8^{(0)}$, possibly $S_8^{(4)}$, and perhaps some other elements of $\mathbb{H}(8)$. Before $A_8^{(0)}$ was rediscovered as the solution of the system (2.4.16), it was found numerically [A1] using a random walk procedure over core phases (see Section 2.2.1) with additional symmetry constraints, $A_8^{(0)} = A_8^{(0)\text{T}}$. Now we see that this symmetry is just a special case of a more general structure that covers also more complicated patterns of $V_8^{(0)}$. In general, one can readily check, that the core of any matrix from the family V_N is symmetric along the antidiagonal.

Shortly, the two matrices $V_8^{(0)}$ and $A_8^{(0)}$ surely originate from the same general circulant seed, $\text{circ}[c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7]$. Actually, these are their equivalent forms. Other 8-dimensional representatives of $\mathbb{H}(8)$ are still waiting for a confirmation whether they belong to this super-class of CHM. This previously unknown observation might be a clue for a more detailed analytic research.

We have reached the point that slowly exceeds the scope of this Thesis, so we stop here further considerations concerning the contents of the set of complex Hadamard matrices. All these insights along with the result from Section 2.2.2 contribute to a more accurate description of $\mathbb{H}(N)$. We encourage those interested in the topic to follow up the preprint [A2] that will appear soon.

⁷Details can be found in the Catalogue of CHM [5].

⁸Coincidence of the family name V_N and the matrix $V_8^{(0)}$ is intentional.

2.6 Summary

In this chapter we have extended two sets of complex Hadamard matrices, which can be used for diverse purposes in constructing novel objects relevant for quantum theory. We introduced the nonaffine family $T_8^{(1)}$ and the isolated point $T_9^{(0)}$. We also discussed some other details concerning the analytic description of set $\mathbb{H}(8)$.

We asked if there was any deeper relationship between complex Hadamard matrices and Latin squares, and it turns out that in fact it is possible to identify some extremely simple connections between the two, that lead to previously unknown observations and, above all, to discovery of new examples of CHM.

Based on the numerical evidence we put forward two conjectures concerning existence of a sequence of isolated CHM in infinitely many dimensions. In each conjecture we consider only two possible patterns of CHM, both related to some extent to the notion of LS. Certainly, this does not exhaust the whole range of the other possibilities, in particular those which, as shown in the initial case of $T_9^{(0)}$ (2.3.3), can be enriched with additional, carefully selected, complex conjugates or even more advanced features (symmetries). For a moment we cannot see how they could be possibly classified into any systematic or coherent way. Hence, we are not going to explore other configurations at least until they prove to exhibit some particularly desirable physical (or mathematical) properties.

There are roughly three systematic methods of construction of isolated CHM. The first one is based purely on numerical approach. Second one follows from the theorem, which says that for any prime dimension p the Fourier matrix is isolated [4],

$$N = p \implies F_p = F_p^{(0)}. \quad (2.6.1)$$

The third one has its source in the construction described in Theorem 3 in [45]. If these conjectures were proven, a new way to get an infinite sequence of isolated CHM would be found. But even if they fail to be true, we are left with two manageable constructions that so far generated several dozen examples of CHM in a number of dimensions $N \geq 8$. One could ask here what is the physical motivation for searching isolated matrices and why we put so much effort to classify them. Again, one possible answer is the straightforward connection of CHM with MUB. It is much easier to examine multidimensional families and check if their representatives form possible sets of MUB. But what if the complete set of MUB in $\mathbb{C}^6$ or $\mathbb{C}^{10}$ is built of (yet unknown) isolated CHM?⁹ Another reason to study isolated structures will be explained in the next chapter.

Looking at the final forms for $T_8^{(1)}$, $V_8^{(0)}$, and $T_9^{(0)}$ it seems that analytic approach to solve the system of equations corresponding to unitarity constraints for L_N and V_N for any

⁹Actually, it is very unlikely that for $N = 6$ new isolated matrices will be discovered, but for $N = 10$ our knowledge is more limited.

N might be out of reach. On the other hand, it does not require much effort to obtain highly accurate numerical approximations. The aforementioned sequences $\{L_N\}_{N=3+4k}$ for $k \geq 0$ and $\{V_N\}_{N \geq 6}$ supporting both conjectures were calculated quite quickly without much pressure on optimization in terms of speed, we rather wanted good quality solutions. Mathematical computation software was chosen to be Matlab/Octave serving appropriately tuned function `fsolve`, which proved to be more than enough for our purpose. We are aware of many other specialized methods designed to solve such problems, but (upon examination) none of them can provide immediate results at the analytic level.

Presented facts may find applications in several branches of modern physics, including creation of new pairs of MUB, being building blocks for unitary error bases (UEB) [20] or used in entanglement detection [55, 56]. As it has been recently shown, even incomplete (unextendible) set of MUB can be more effective to detect entanglement [57]. We will return to the problem of unextendible sets of MUB in Chapter 5, where we also present the relation of CHM to some classes of Bell inequalities, while the phenomenon of entanglement will be treated in Chapter 4.

Let us conclude this chapter with a list of some open questions:

1. Are Conjecture 1 and 2 true? Especially, how to prove that the construction of L_N lead only to zero-defect matrices?
2. What about different patterns (2.4.5) which might provide a solution? How to classify them? Is the presented connection between CHM and Latin squares accidental or fundamental?

We shall mention here that apart from $T_8^{(0)}$, $T_9^{(0)}$, $\{L_N\}$, and $\{V_N\}$ we found several other matrices of order $N \in \{11, 12, 13, 14, 15, 16\}$. They all can be found online [58] and look promising. Currently they await to be discarded or accepted as valid members of the set $\mathbb{H}(N)$ of inequivalent complex Hadamard matrices.

3. Are there any other genuine numerical methods to generate CHM? Inspired by [59] we made some attempts to employ machine learning and artificial intelligence techniques to estimate possibilities of finding new classes of CHM. But currently such research is at the very preliminary stage.



In the next chapter we are going to explore more advanced structures. Based on the presented notion of defect of a unitary matrix, we will propose another analytical tool to examine possibility of introduction of free parameters in several objects representing quantum measurement operators.

Chapter 3

Restricted Defect of a Unitary Matrix

Chapter based on [A3].

In our approach to explore quantum mechanics various classes of matrices are the main framework for many concepts. Matrix algebra provides a comprehensive mathematical description of physical systems and dynamics at the subatomic level. Having chosen convenient reference frame (a basis), they represent operators, states or just special purpose bases in Hilbert spaces being a background for our considerations. We have already investigated very particular class of complex Hadamard matrices. Every such matrix rescaled by the square root of its size¹ automatically becomes unitary, $\frac{1}{\sqrt{d}}\mathbb{H}(d) \subsetneq \mathbb{U}(d)$. We have shown that these matrices might admit special parameterization forming families depending on free parameters.

Unitarity is the first fundamental property of quantum dynamics. Evolution of quantum states represented by density matrices ρ of size d is governed by unitary matrices, $\rho \rightarrow U\rho U^\dagger$, $U \in \mathbb{U}(d)$. Another mathematical attribute pertaining to the quantum world is hermiticity. All operators corresponding to physical observables must be Hermitian (self-adjoint) to guarantee the fact that eigenvalues representing possible measurement outcomes are real. In theory of quantum information we encounter many structures that are Hermitian by construction or by demand. In some cases they allow to introduce free parameters as it is for CHM. The question is when and how many degrees of freedom can we expect.

In this chapter, we will answer that question by adapting the idea of the defect of a unitary matrix [37, 38] used in Chapter 2 to a very particular subset of $\mathbb{U}(d)$, namely unitary and Hermitian matrices having constant diagonal. Due to its character, it should be called *restricted defect* (denoted Δ), and it will serve as a suitable tool to determine the

¹Caution. In Chapter 2 we used the notion of defect usually denoted by $\mathbf{d}(H)$. In the current chapter letter d is reserved for a (local) dimension and wherever it is needed, the defect of a unitary matrix is always denoted by $\mathbf{d}(U)$.

maximal number of free parameters allowed by a given structure. As a consequence, we will calculate Δ for a wide range of special operators, identify some families and classify isolated objects.

3.1 Quantum Measurement

Measurement is a primordial concept in physics. No matter how attractive theory to model our reality we propose, it is completely useless unless we can confirm and reproduce its expectations in a series of independent experiments, and every experiment must involve at least one measurement of a physical quantity. The measurement process has destructive nature, as by definition it is an interaction of an apparatus with the physical system. Such interaction might invoke some changes, either in the system or in the measuring tool (or both), which are represented by real numbers out of which we may draw appropriate conclusions. In the classical world, we do not observe this invasive property, since the analysis of the system does not influence on it at all or the impact is so tiny that it is immeasurable and negligible. However, at the mesoscopic or subatomic level, if the act of measurement can destroy the system and reflects probabilistic character, this has much more profound consequences making it an irreversible step versus fully reversible unitary evolution.²

In the axiomatic approach to quantum mechanics [60], classical probability vectors are replaced by states $|\psi\rangle$ represented by normalized complex vectors from Hilbert space $\mathcal{H}_d$ of a given dimension d . Such a state vector $|\psi\rangle$, called a *pure state*, carries all information about the isolated (closed) system. In general, for open systems (interacting with an environment) we should consider a statistical ensemble $\{(|\psi_j\rangle, p_j)\}$, where p_j is the probability that the system is in the state $|\psi_j\rangle$. This leads to a formalism of *density matrices* (operators) defined as

$$\rho = \sum_j p_j |\psi_j\rangle \langle \psi_j|, \quad (3.1.1)$$

so that ρ is Hermitian ($\rho = \rho^\dagger$), positive-semidefinite ($\rho \geq 0$) and normalized ($\text{Tr}(\rho) = 1$) operator acting on $\mathcal{H}_d$.

To obtain the information about the quantum system, one must perform a measurement. The most general form of the quantum measurement is described by a set of Kraus operators K_j , such that the following resolution of identity holds

$$\sum_j K_j^\dagger K_j = \mathbb{I}_d. \quad (3.1.2)$$

Such a form can be explained by the fact that given a density matrix ρ , all the information that is contained in ρ can be extracted by means of the expectation values, $q_j = \text{Tr}(O_j \rho)$,

²We express the hope that the Reader is aware of the fact that such a naively presented essence of quantum measurement hides much more content and nuances. For instance, see [61] and references therein.

for some operators O_j . If we require q_j to be probabilities, i.e. $q_j \geq 0$ and $\sum_j q_j = 1$, then it implies that $O_j \geq 0$ and $\sum_j O_j = \mathbb{I}_d$. Hence, the probability of j^{th} measurement outcome is

$$p_j = \text{Tr}(K_j \rho K_j^\dagger) \quad (3.1.3)$$

and the system collapses to the state

$$\rho' = \frac{K_j \rho K_j^\dagger}{p_j}. \quad (3.1.4)$$

In this work, we consider a particular scenario called *positive-operator valued measure* (POVM) restricted to the variant with rank-1 projectors. Thus, we define POVM as a set of N semi-definite normalized operators Γ_j of size d such that

$$\sum_{j=0}^{N-1} \Gamma_j = \mathbb{I}_d, \quad (3.1.5)$$

where each Γ_j is proportional to a rank-1 projector Π_j and corresponds to the j^{th} measurement outcome. Projectors Π_j satisfy the geometrical relation

$$\text{Tr}(\Pi_j \Pi_k) = S_{jk} \quad (3.1.6)$$

for a symmetric matrix $S = S^T \in \mathbb{C}^{N \times N}$.

Let us put formal definitions of some distinguished subclasses of POVM having prescribed symmetry given by the real symmetric matrix S . A matrix

$$S = \mathbb{I}_N + \frac{N-d}{d(N-1)} (\mathbb{J}_N - \mathbb{I}_N) \quad (3.1.7)$$

corresponds to *equiangular tight frames* (ETF) composed of N vectors each of size d [62]. The symbol $\mathbb{J}_N$ denotes the flat matrix of size N with all entries equal to 1. For $N = d^2$, one obtains an important subclass of ETF called *symmetric, informationally complete POVM* (SIC-POVM) [63] which, for $d = 8$, includes a very particular example called the *Hoggar lines* [64]. In Chapter 2, we frequently referred to *mutually unbiased bases* (MUB) — see definition in Eq. (2.0.3). Associated symmetric matrix (3.1.6) reads

$$S = \mathbb{I}_{dm} + \frac{1}{d} (\mathbb{J}_m - \mathbb{I}_m) \otimes \mathbb{J}_d. \quad (3.1.8)$$

These geometrical structures, visualized in the hierarchical scheme

$$\text{POVM} \supset \begin{cases} \text{MUB} \\ \text{ETF} \supset \text{SIC-POVM}, \end{cases} \quad (3.1.9)$$

have important applications in quantum physics. For example, ETF serve in coding theory [65] and error correction [66]. SIC-POVM and MUB are widely used in quantum tomography i.e. reconstruction of density matrix of an unknown system [12, 67], as they maximize the information gained during measurement while minimizing influence of statistical errors. They also define entropic uncertainty relations [68], find applications in detecting entanglement [55], bound entanglement [56], and locking classical information in quantum states [69].

Having presented above categories one might rightly suppose they will be subjected to examination in view of possibility of introduction of free parameters. Indeed, our current objective can be briefly summarized in the following question:

$$\begin{aligned} & \textit{Given generalized quantum measurement of predefined geometrical structure,} \\ & \textit{is it possible to extend it to a smooth family of POVM?} \end{aligned} \tag{3.1.10}$$

For $d > 3$, the presence of free parameters in SIC-POVM is an unresolved task. On the other hand, some families of MUB in low dimensions are known [70]. Construction of such families can find pragmatic applications providing flexibility when designing experimental implementations of measurement settings. Free parameters can be tuned to produce customized machinery for concrete purposes. For instance, taking the well known one-parameter family of SIC-POVM in $d = 3$ [63], only one particular representative maximizes the informational power, that is, the classical capacity of a quantum-classical channel generated by the SIC-POVM [71]. It is also worth to mention another class of measurements not belonging to any family. Such isolated objects might play important role when there is a need to have a unique solution which optimizes a certain problem, like a unique maximal violation of a Bell inequality, which is a crucial component in procedures of self-testing [72].

The general question about the existence of SIC-POVM and MUB is a completely different story. We will not deal with this subject here and only mention the two biggest problems. In his thesis [73], Gerhard Zauner posed a conjecture that in every dimension $d \geq 2$, there exist a special vector called *fiducial* one, which is a kind of a generator for SIC-POVM (we will later see one such vector for $d = 3$). Since currently only finitely many SIC-POVM are known analytically (this includes aforementioned one-parameter family in $d = 3$), there are many attempts to tackle the problem numerically [74]. Mutually unbiased bases, first introduced in [75] have been investigated since early 1980s [12]. Alike SIC-POVM, MUB are also far from being completely classified. Despite many efforts, the seemingly simple six-dimensional case contributes to the both lists of the most wanted open problems [2, 3].

3.2 Gram Matrix

Before we attempt to give an answer to (3.1.10), we need two things for completeness. First, we recall the notion of the Gram matrix. Consider N vectors $|\varphi_j\rangle \in \mathbb{C}^d$. The Gram matrix $G(|\varphi_1\rangle, \dots, |\varphi_N\rangle)$ associated with $\{|\varphi_j\rangle\}$ is given by

$$G_{jk} = \langle \varphi_j | \varphi_k \rangle \quad (3.2.1)$$

for $j, k \in \{1, 2, \dots, N\}$. One can show [76] that $G^2 = GN/d$ is the necessary and sufficient condition for a Gram matrix G to represent a POVM with N vectors in $\mathbb{C}^d$ for $d \leq N$. Then, from the fact that $\text{Tr}(G) = N$ and

$$\text{eig}(G) = \left\{ \underbrace{\frac{N}{d}, \dots, \frac{N}{d}}_d, \underbrace{0, \dots, 0}_{N-d} \right\}, \quad (3.2.2)$$

we infer that $U = \mathbb{I}_N - 2dG/N$ is unitary, $U \in \mathbb{U}(N)$. Thus the existence of a POVM with a symmetry imposed by matrix S given in (3.1.6) can be considered in terms of a Hermitian unitary matrix $|U_{jk}| = 2d\sqrt{S_{jk}}/N$ having positive constant diagonal, $U_{jj} = 1 - 2d/N$.

As an example [77], the Gram matrix of a generic ETF corresponding to (3.1.7) has the form

$$G_{\text{ETF}} = \begin{bmatrix} 1 & \alpha e^{i\beta_{12}} & \dots & \alpha e^{i\beta_{1N}} \\ * & 1 & \dots & \alpha e^{i\beta_{2N}} \\ \vdots & \vdots & & \vdots \\ * & * & \dots & 1 \end{bmatrix} : \alpha = \sqrt{\frac{N-d}{d(N-1)}}, \quad \beta_{jk} \in [0, 2\pi). \quad (3.2.3)$$

The symbols $*$ below the diagonal denote complex conjugated entries.

The last missing link is a counterpart of the defect of a unitary matrix tailored to Hermitian unitary matrices with constant diagonal. We will derive it in the next section.

3.3 Restricted Defect Δ

Based on the idea of the defect of a unitary matrix U (Chapter 2), we will present a heuristic derivation of a similar formula for the restricted defect applicable to a Hermitian unitary matrix with constant diagonal. In mathematical language, restricted defect is defined in full analogy to its unitary equivalent as a dimension of a real space of possible directions that preserve unitarity, hermiticity, diagonal entries and the moduli of all matrix elements in the first order or perturbations. We shall not strictly adhere to mathematical rigor to make the description more accessible and easier to understand. Formal derivation details including the special treatment of the case of matrices with zero entries³ can be found in [38].

³We thank Wojciech Tadej for his patient explanations of mathematical details of multidimensional tangent spaces and manifolds.

Let $d > 1$. Consider a unitary matrix

$$U = \begin{bmatrix} c & U_{12} & U_{13} & \dots & U_{1d} \\ U_{12}^* & c & U_{23} & \dots & U_{2d} \\ U_{13}^* & U_{23}^* & c & \dots & U_{3d} \\ \vdots & \vdots & \vdots & & \vdots \\ U_{1d}^* & U_{2d}^* & U_{3d}^* & \dots & c \end{bmatrix}, \quad (3.3.1)$$

such that (by construction)

1. U is unitary and Hermitian; $UU^\dagger = U^2 \propto \mathbb{I}_d$ (we relax strict normalization, hence only proportionality is required),
2. U has constant diagonal; $c \in \mathbb{R}$,
3. $|U_{jk}|$ is constant for $j \neq k$ (not necessarily unimodular).

We look for the most general antisymmetric perturbation matrix R such that

$$U(R) = U \circ \text{EXP}(itR) \quad : \quad t \in \mathbb{R} \quad (3.3.2)$$

fulfills the three conditions above.⁴ In other words, we examine all possible (independent) “directions”, we can follow so that the properties of U are not violated. For example, for $d = 3$ relevant calculations lead to

$$(U(R))^2 = \begin{bmatrix} c & U_{12}e^{itR_{12}} & U_{13}e^{itR_{13}} \\ U_{12}^*e^{-itR_{12}} & c & U_{23}e^{itR_{13}} \\ U_{13}^*e^{-itR_{12}} & U_{23}^*e^{-itR_{13}} & c \end{bmatrix}^2 = \quad (3.3.3)$$

$$= \begin{bmatrix} c^2 + |U_{12}|^2 + |U_{13}|^2 & * & * \\ 2cU_{12}e^{-itR_{12}} + U_{23}U_{13}^*e^{it(R_{23}-R_{13})} & \text{constant} & * \\ \dots & \dots & \text{constant} \end{bmatrix} \propto \mathbb{I}_d. \quad (3.3.4)$$

For brevity we do not fill the places over the diagonal, and the diagonal itself is obviously constant. Also, in (3.3.4) we present only one product in the second entry in the first column since the other off-diagonal elements take exactly the same form, differing only in indices. One readily recognizes the general pattern

$$2cU_{jk}^*e^{-iR_{jk}} + \sum_{l \neq j,k} U_{kl}U_{jl}^*e^{i(R_{kl}-R_{jl})} = 0 \quad (3.3.5)$$

for $1 \leq j < k \leq d$. The system of nonlinear equations (3.3.5) contains full information about the conditions that the perturbation matrix R must meet in order for (3.3.2) to represent the

⁴Entrywise product of two matrices is denoted by $\circ$, while entrywise exponent of a matrix A reads $[\text{EXP}(iA)]_{jk} = e^{iA_{jk}}$, see [4].

matrix with all the required properties. However, the solution of such a system of equations is generally intractable.

A dummy real parameter $t \in \mathbb{R}$, which has been artificially introduced in (3.3.2), now allows us to perform linearization of (3.3.5). We write

$$\lim_{t \rightarrow 0} \frac{d}{dt} \left(U(R) \right)^2 = [0, \dots, 0]^T \in \mathbb{R}^d \quad (3.3.6)$$

which gives us explicit first order approximation on conditions for (3.3.2). This eventually implies the system of linear equations for real variables R_{jk} ,

$$-2cU_{kj}R_{jk} + \sum_{l \neq j,k} U_{kl}U_{lj}(R_{kl} - R_{jl}) = 0 \quad (3.3.7)$$

for $1 \leq j < k \leq d$ and $1 \leq l \leq d$. Note, that $U_{j\dots}^* = U_{\dots j}$. System (3.3.7) consists of $\tau = d(d-1)/2$ linear equations but usually it is not of full rank. Let r denote the rank of the matrix $\mathcal{R}$ associated with the system (3.3.7).

Equivalence relation $U \simeq DUD^*$ for $D = \text{diag}[1, e^{i\beta_2}, e^{i\beta_3}, \dots, e^{i\beta_d}]$ with appropriately chosen β_j , $j \in \{2, \dots, d\}$, preserves the diagonal of U and absorbs $f = d-1$ phases (this corresponds to 1st row/column of U). Moreover, zeros that might appear in U are obviously not affected by the relation $\simeq$ and further reduce the number of phases (free parameters). Let the number of zeros above the main diagonal in the matrix U be denoted by z .

Putting all together, we are in a position to pose a definition of the *restricted defect* Δ of the Hermitian unitary matrix U of size d . It reads

$$\Delta(U) = \tau - f - z - r. \quad (3.3.8)$$

Originally, the defect $\mathbf{d}(U)$ of the unitary matrix U was used to determine an upper bound on the number of free parameters allowed by a complex Hadamard matrix [4]. Looking at the definition of Δ (3.3.8) we recognize a close relation between $\Delta(U)$ and $\mathbf{d}(U)$ which has been adapted to the set of matrices of a special structure. By construction, in the particular case of a Hermitian unitary matrix $U \in \mathbb{U}(d)$ with constant diagonal without off-diagonal zeros ($z = 0$), the following bounds hold

$$0 \leq \Delta(U) \leq \mathbf{d}(U) \leq (d-1)^2. \quad (3.3.9)$$

All properties of the unitary defect are naturally transferred to Δ . In both cases, defect is invariant with respect to the equivalence relation which for Δ takes the simpler form (to preserve constant diagonal and hermiticity) of

$$\Delta(U) = \Delta(PDUD^*P^T), \quad (3.3.10)$$

for $D = \text{diag}[1, e^{i\beta_2}, \dots, e^{i\beta_d}]$ and $P \in \mathbb{P}(d)$. And, its vanishing value implies the impossibility of introduction of free parameters, hence it detects isolated matrices. In the case of the restricted defect, this fact has further consequences.

It should be adverted that the way of deriving the Hermitian defect of a matrix U , as well as its standard unitary defect, provides an explicit construction of affine families stemming from a given matrix U . We are not going to construct such families here and we refer the Reader to [A3] or [37] for more information.

3.3.1 Elementary Examples

To gain some practice, let us discuss some examples of simple matrices of size $d = 3, 4, 5$, and 6. Take a matrix U of the form

$$U = \begin{bmatrix} -1/2 & 1 & 1 \\ 1 & -1/2 & 1 \\ 1 & 1 & -1/2 \end{bmatrix}. \quad (3.3.11)$$

Matrix U perturbed by an affine entrywise rotation by phase t reads

$$U(R) = \begin{bmatrix} -1/2 & 1 & 1 \\ 1 & -1/2 & 1 \\ 1 & 1 & -1/2 \end{bmatrix} \circ \text{EXP}(itR). \quad (3.3.12)$$

Quick arithmetic,

$$\left. \frac{d}{dt} (U^2(R)) \right|_{t=0} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \iff \mathcal{R} = \begin{cases} R_{12} + R_{23} - R_{13} = 0 \\ R_{13} - R_{12} - R_{23} = 0, \\ R_{23} + R_{12} - R_{13} = 0 \end{cases} \quad (3.3.13)$$

shows that all equations in (3.3.13) are linearly dependent so $r = 1$ and the restricted defect given by Eq. (3.3.8) reads $\Delta(U) = 0$.

Similar calculations for $U = \text{circ}[-1, 1, 1, 1]$ of size $d = 4$ lead to a system of $d(d-1)/2 = 6$ linear equations whose matrix form is given by a matrix $\mathcal{R}$ of order six

$$\mathcal{R} = \begin{bmatrix} 2 & -1 & -1 & 1 & 1 & 0 \\ -1 & 2 & -1 & -1 & 0 & 1 \\ -1 & -1 & 2 & 0 & -1 & -1 \\ 1 & -1 & 0 & 2 & -1 & 1 \\ 1 & 0 & -1 & -1 & 2 & -1 \\ 0 & 1 & -1 & 1 & -1 & 2 \end{bmatrix}. \quad (3.3.14)$$

Hence $r = r(\mathcal{R}) = 3$, again $z = 0$, so $\Delta(U) = 0$ as well. The same vanishing value for the restricted defect Δ we obtain for another circulant matrix $U = \text{circ}[-\frac{3}{2}, 1, 1, 1, 1]$.

A slightly more complicated example involves MUB for a single-qubit system, $|\varphi_j\rangle = |j\rangle$ for $j = 0, 1$ and $|\psi_{\mp}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \mp |1\rangle)$. The Gram matrix associated with the set of two unbiased bases reads

$$G_{\text{MUB}} = \frac{1}{2} \begin{bmatrix} 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & -1 \\ 1 & 1 & 2 & 0 \\ 1 & -1 & 0 & 2 \end{bmatrix}. \quad (3.3.15)$$

In general we can introduce four parameters, so the Gram matrix takes the form of

$$G_{\text{MUB}} = \frac{1}{2} \begin{bmatrix} 2 & 0 & e^{itR_{13}} & e^{itR_{14}} \\ 0 & 2 & e^{itR_{23}} & -e^{itR_{24}} \\ e^{-itR_{13}} & e^{-itR_{23}} & 2 & 0 \\ e^{-itR_{14}} & -e^{-itR_{24}} & 0 & 2 \end{bmatrix}. \quad (3.3.16)$$

After absorbing three phases by acting with $D = \text{diag}[1, e^{-R_{23}}, e^{itR_{13}}, e^{itR_{14}}]$ on G_{MUB} , we arrive at the unitary matrix

$$U(R) = \mathbb{I}_4 - \frac{2 \cdot 2}{4} G_{\text{MUB}} \quad (3.3.17)$$

$$= \frac{1}{2} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -e^{itR_{24}} \\ 1 & 1 & 0 & 0 \\ 1 & -e^{-itR_{24}} & 0 & 0 \end{bmatrix}. \quad (3.3.18)$$

It is easy to notice that the rank of the associated system of equations for (3.3.7) is $r = 1$, and $z = 2$, therefore $\Delta = 0$. This result is in accordance with the well known fact that the pair of MUB in $\mathbb{C}^2$ is unique up to a global rotation [78].

Lastly, consider a one-parameter family of Hermitian conference⁵ matrices [79]

$$C_6(b) = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & -1 & e^{ib} & 1 & -e^{ib} \\ 1 & -1 & 0 & -e^{ib} & 1 & e^{ib} \\ 1 & e^{-ib} & -e^{-ib} & 0 & -1 & 1 \\ 1 & 1 & 1 & -1 & 0 & -1 \\ 1 & -e^{-ib} & e^{-ib} & 1 & -1 & 0 \end{bmatrix} : b \in [0, 2\pi). \quad (3.3.19)$$

For a generic value of $b \in [0, 2\pi)$, the restricted defect $\Delta(C_6(b)) = 1$, while $\Delta(C_6(0)) = \Delta(C_6(\pi)) = 4$. This fact implies that the family of conference matrices $C_6(b)$ is one-dimensional and one cannot extend it to the second dimension.

⁵Complex conference matrix C of size d satisfies two conditions: $|C_{jk}| = 1 - \delta_{jk}$ and $CC^\dagger = (d-1)\mathbb{I}_d$.

3.4 Isolated Mutually Unbiased Bases (MUB) and Symmetric, Informationally Complete Positive-Operator Valued Measures (SIC-POVM)

Our first main results in this chapter are summarized in the two following statements:

Proposition 1. *Maximal sets of $d + 1$ MUB for $d = 4, 8, 9$, and 16 are isolated.*

Proposition 2. *SIC-POVM in dimension $4 \leq d \leq 16$ are isolated.*

Let us briefly comment these observations. For a maximal set of $m = d + 1$ MUB in dimension d , one can prove that the number of zeros in the upper triangular part of the associated Gram matrix G is $z = \frac{1}{2}d(d^2 - 1)$, hence the total number of parameters in G is $\tau - f - z = \frac{1}{2}d^4 + \frac{1}{2}d^3 - d^2 - d + 1$. For $d = 4, 8, 9$, and 16 the rank of the corresponding system of linear equations (3.3.7) reads: 141, 2233, 3556 and 34545, respectively — See Table 3.1. We took maximal sets of MUB from [13, 44, 80].

d	$\tau - f - z$	r	$\Delta = \tau - f - z - r$
4	141	141	0
8	2233	2233	0
9	3556	3556	0
16	34545	34545	0

Table 3.1: Values of the restricted defect for maximal set of $d + 1$ MUB in dimension $d = 4, 8, 9$, and 16 . As $\Delta = 0$, each set of analyzed MUB is isolated.

Another observation concerns certain incomplete sets of MUB in dimensions $2 \leq d \leq 9$. The restricted defects Δ calculated for sets of $2 \leq m \leq d + 1$ MUB are presented in Table 3.2. Most of all, question marks in Table 3.2 for $d = 6$ denote the current status of the six-dimensional MUB problem, while $\diamond$ points to the case of three such bases in $\mathbb{C}^6$, which is still obscured and not fully understood issue [81].

One sees that for prime dimensions, $d = p = 2, 3, 5, 7$, the Hermitian defect vanishes for every $2 \leq m \leq d + 1$. This can be explained by the fact that every CHM contributing to a particular set of MUB is equivalent to the isolated Fourier $F_d = F_p^{(0)}$, see (2.6.1). Note that for $m = 2$ (pair of MUB), Δ coincides with the standard unitary defect. That is because the Gram matrix associated with two MUB $\mathcal{B}_1$ and $\mathcal{B}_2$,

$$G_{\text{MUB}} = \begin{bmatrix} \mathbb{I}_d & H \\ H^\dagger & \mathbb{I}_d \end{bmatrix} \quad : \quad H = \mathcal{B}_1^\dagger \mathcal{B}_2, \quad (3.4.1)$$

allows one to introduce exactly as many free parameters as it is required for H itself. Here, each basis $\mathcal{B}_j$ represents a CHM. This clarifies the first row ($m = 2$) in Table 3.2 — for

$m \setminus d$	2	3	4	5	6	7	8	9
2	$\Delta = 0$	0	3	0	4	0	21	16
3	0	0	3	0	$\diamond$	0	27	20
4		0	0	0	?	0	19	32
5			0	0	?	0	7	0
6				0	?	0	0	0
7					?	0	0	0
8						0	0	0
9							0	0
10								0

Table 3.2: Values of the restricted defect for subsets of MUB in dimension $2 \leq d \leq 9$. The results do not depend on the choice of m subsets of MUB out of the full set of $d + 1$ MUB.

non-prime dimensions there are non-zero values of Δ . However, since we know that in every low dimension (excluding $d = 4$), there exists an isolated CHM (and probably for infinitely many dimensions greater than 4 — see Chapter 2), we can always construct exceptional pairs of MUB, e.g.

$$\left\{ \mathbb{I}_6, \frac{1}{\sqrt{6}} S_6^{(0)} \right\}, \left\{ \mathbb{I}_7, \frac{1}{\sqrt{7}} F_7^{(0)} \right\}, \left\{ \mathbb{I}_8, \frac{1}{\sqrt{8}} A_8^{(0)} \right\}, \left\{ \mathbb{I}_9, \frac{1}{\sqrt{9}} N_9^{(0)} \right\}, \dots, \left\{ \mathbb{I}_d, \frac{1}{\sqrt{d}} V_d^{(0)} \right\}, \dots \quad (3.4.2)$$

such that Δ vanishes. For $d = 8$ and 9 , we examined subsets of MUB taken from maximal sets [13, 80]. For $m \geq 6$ and $m \geq 5$ respectively, these subsets are isolated too.

The last observation regarding MUB explains the coincidence between the value of the restricted defect Δ for d and $d + 1$ sets, as maximal set of $d + 1$ MUB is explicitly determined by the first d elements. It is not the case for $2 \leq m < d$, where Δ might depend on the choice of a given subset. Table 3.2 contains values of Hermitian defect consistent for every subset of MUB.

The case of SIC-POVM also reflects isolated character, at least in low dimensions. For a qubit ($d = 2$) and qutrit systems ($d = 3$) the existence of SIC-POVM is well known. In the former case, we have a unique (up to a global rotation) solution in form of a tetrahedron inscribed into the Bloch sphere, while in the latter case there exists a one-parameter family [82]. As we have already mentioned, for $d > 4$ the problem of SIC families remains open. We solved associated system of linear equations built from analytical [73, 83, 84] and numerical formulas [74], and computer simulations indicate impossibility of introduction of free parameters into all SIC-POVM solutions for $4 \leq d \leq 16$. For $d = 8$ this includes a particular example of Hoggar lines [64], being a very special class of supersymmetric SIC-POVM that finds applications in the theory of quantum-classical channels [85].

3.4.1 Isolated Kochen–Specker Sets

In Chapter 5 of this Thesis we are going to describe some problems concerning foundations of quantum mechanics, local hidden variables theories and Bell inequalities. Here we preliminarily mention a single aspect of this subject. In 1967 Simon Kochen and Ernst Specker [86] proved that a deterministic local hidden variable theory cannot exist, unless we make some additional assumptions. This result accompanies the work of John Bell and implies that a determinism in quantum mechanics leads to a conclusion that physical observables can be understood only in the context of a given measurement, while the context stands for the whole idea describing an event. In other words, local hidden variable theories, which are non-contextual are incompatible with quantum mechanics and should be discarded. Detailed review of this topic can be found in the recent paper [87].

The original reasoning presented in [86] is based on $N = 117$ vectors (KS vectors) in dimension $d = 3$. Then it can be shown that a system prepared in a state ρ together with KS vectors $\{\phi_j\}_{j=1,\dots,N}$, out of which we can prepare a number of orthonormal bases, cannot provide N deterministic probabilities $p_j = \text{Tr}(\rho|\phi_j\rangle\langle\phi_j|) \in \{0, 1\}$ and, in consequence, any predefined values of observables must depend on the measurement's context. Later, another inequivalent KS sets were introduced: $N = 13$ vectors in $d = 3$ [88], $N = 18$, $d = 4$ [89], and $N = 21$, $d = 6$ [90]. Observe that they all form POVM, hence proceeding as in the previous cases we can build associated Gram matrix, and our mechanism of restricted defect can be applied to check the possibility of introduction of free variables. Appropriate values are tabulated below,

N	d	z	τ	r	Δ	# free parameters
13	3	24	78	66	12	0
18	4	63	90	83	7	0
21	6	105	105	103	2	0

Table 3.3: Values of the restricted defect for the three KS sets. Despite the fact that $\Delta \neq 0$, each set is isolated.

One immediately notes that in no case the restricted defect Δ vanishes, which does not automatically excludes these sets from the isolated domain. However, all possible free parameters allowed by a positive restricted defect are absorbed as global phases of the KS vectors. Hence, our reasoning implies that all presented sets of KS vectors are isolated.

3.5 Free Parameters in MUB, Equiangular Tight Frames and SIC-POVM

Let us return for a moment to Table 3.2, which contains upper bounds for the maximal number of free parameters allowed by all possible subsets of $2 \leq m \leq d+1$ MUB in dimension $2 \leq d \leq 9$. Now, let us start the analysis beginning from the third row, corresponding to $m = 3$. The restricted defect Δ for the triplets in dimension $d = 4$ is three, which perfectly matches the maximal number of free parameters [78]. The possibility of existing of multidimensional families is also allowed in $d = 8$ for $m = 2, 3, 4, 5$ and $d = 9$ for $m = 2, 3, 4$. In particular for $(d, m) = (8, 5)$ several such families do exist [70].

Equiangular tight frames $\text{ETF}(d, N)$ composed of $N = k^2$ vectors, each of dimension $d = k(k-1)/2$, are associated with the Hermitian Fourier matrices

$$[F_N]_{ab} = \exp \left\{ \frac{2\pi i}{k} \left(\text{mod}(a, k) \left\lfloor \frac{b}{k} \right\rfloor - \text{mod}(b, k) \left\lfloor \frac{a}{k} \right\rfloor \right) \right\}, \quad (3.5.1)$$

where $\text{mod}(\cdot, k)$ denotes remainder of the integer division $\cdot/k$. For prime values of $k = p$ our results suggest that the following statement might be true.

Conjecture 3. *Given a Fourier matrix F_{p^2} defined in (3.5.1) for prime $p \geq 2$, its Hermitian unitary defect reads*

$$\Delta(F_{p^2}) = \frac{1}{2}(p-2)(p-1)(p+1). \quad (3.5.2)$$

Formula (3.5.2) matches (for primes) all values of Δ presented in the table

k	2	3	4	5	6	7	8	9	10	11	12	13	14
$\Delta(F_{k^2})$	0	4	21	36	112	120	273	352	576	540	1237	924	1632

(3.5.3)

where calculated values of restricted defect Δ of Hermitian Fourier matrices for $2 \leq k \leq 14$ are presented. The only case of $k = 2$ represents isolated regular three-dimensional simplex $\text{ETF}(3, 4)$. For $k = 3$, we have $\Delta = 4$, however only two-dimensional orbit exist [63], while for $k = 4$ several six-dimensional families of $\text{ETF}(6, 16)$ can be found [77]. Other cases of $k \geq 5$ allow us to introduce several free parameters. Currently we are not able to provide a single formula for $\Delta = \Delta(k)$ nor to prove equation (3.5.2).

Finally, we switch to families of SIC-POVM. Consider $d = 3$ and a fiducial vector

$$|\phi_{00}\rangle = \frac{1}{\sqrt{2}}[1, -1, 0]^T. \quad (3.5.4)$$

Following [73] we define the Weyl-Heisenberg SIC-POVM

$$|\phi_{ab}\rangle = X^a Z^b |\phi_{00}\rangle, \quad (3.5.5)$$

where, conventionally, $X|j\rangle = |j \oplus_3 1\rangle$, $Z|j\rangle = \exp\{\frac{2\pi i j}{3}\}|j\rangle$ and $\oplus_3$ denotes addition mod 3. After constructing the appropriate Gram matrix and solving associated system of linear equations, we arrive at the restricted defect $\Delta = 4$ and six one-dimensional families of SIC-POVM. All solutions are equivalent — see (2.1.1) applied to the Gram matrix. Moreover, they belong to the four-dimensional tangent plane described by Eq. (3.3.6) and cannot fit into a lower-dimensional space. Hence, the defect Δ cannot be decreased. This solution is the most general SIC-POVM in $d = 3$ [82] up to equivalence. The family reads

$$\phi(\gamma) = \frac{1}{\sqrt{2}} [1, e^{i\gamma}, 0]^T \quad : \quad \gamma \in [0, 2\pi). \quad (3.5.6)$$

The value of the Hermitian defect Δ for a generic value of $\gamma \in [0, 2\pi)$ is 2, while only for $|\phi_{00}\rangle$ we have $\Delta = 4$. This is yet another example of a situation when the value of the defect is larger than a maximal possible family of solutions.

3.6 Robustness of the Restricted Defect Δ

As we already mentioned, imperfect nature of physical systems provides several obstacles in quantum computing. On the other hand, calculations performed by classical machines are not free from their own issues either. Vast majority of problems, even if they can be easily expressed in simple algebra, are usually not computable analytically due to the complicated character of possible solutions. Such numerical data can later serve as input for further analysis and, independently of the initial precision set, the error propagation might lead to unreliable results when they are subjected to many subsequent iterations and transformations. The best example in the context of this Thesis was already presented in Chapter 2, where we calculated several dozens of CHM (solving numbers of unitarity constraints numerically) and claimed they all provide isolated examples of Hadamard matrices, as the unitary defect vanishes for every matrix. However, in that particular case such a statement is absolutely justified, due to the properties of the numerical algorithm for the defect.

In this section we will study the robustness of the Hermitian unitary defect under the presence of errors introduced to the POVM. We only present the sketch of the reasoning with all mathematical details left in Appendix of [A3]. Obviously, all arguments and calculations can be applied directly to the standard unitary defect too.

Consider a Gram matrix defined in (3.2.1) by means of vectors $|\varphi_j\rangle \in \mathbb{C}^d$ and now we let these vectors be slightly perturbed, $|\varphi'_j\rangle = |\varphi_j + s\xi_j\rangle$, where ξ_j is a random variable distributed uniformly in the interval $[-1, 1]$ and

$$s = \frac{1}{\sqrt{d}} \max_j \left\| |\varphi'_j\rangle - |\varphi_j\rangle \right\| \quad (3.6.1)$$

is the factor quantifying⁶ the maximal allowed inaccuracy in components of $|\varphi_j\rangle$.

⁶For example, if we set the working precision to k decimal digits, that is the components of $|\varphi'_j\rangle$ differ

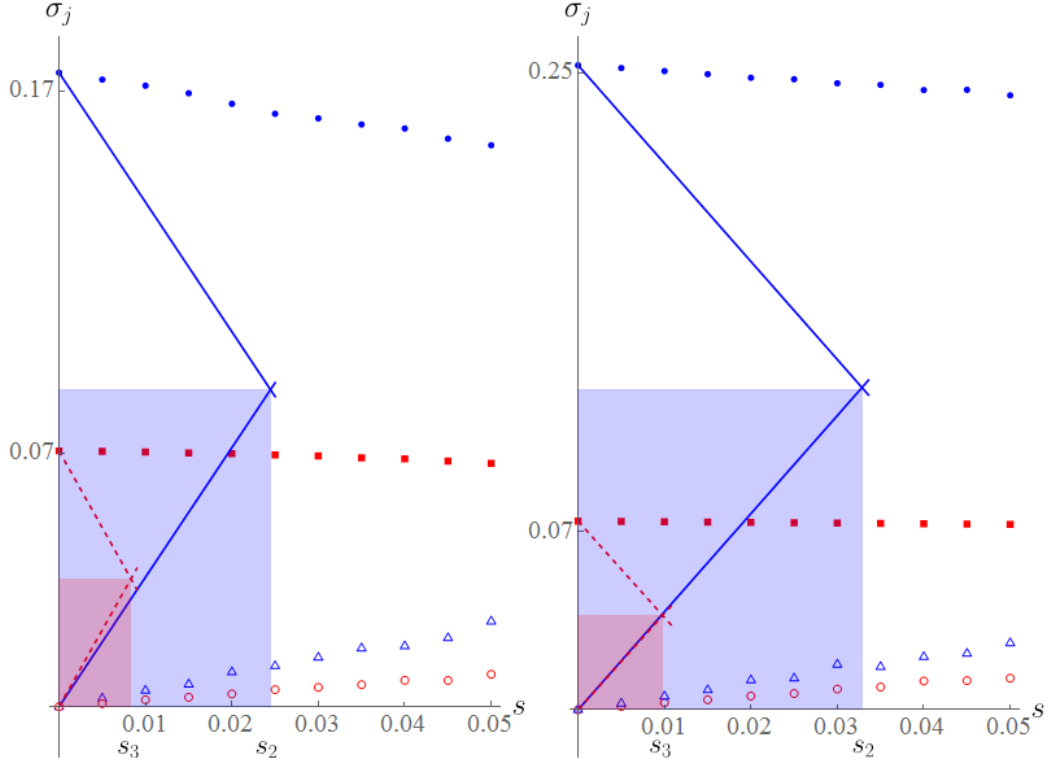


Figure 3.1: Two smallest singular values σ_0 and σ_1 of the matrix $\mathcal{R}$ representing system (3.3.7) associated with the SIC-POVM of order $d = 4$ and 8 are presented on the left panel. Singular values σ_j (for $j = 0, 1$) are functions of the inaccuracy factor s (3.6.1). Open and solid symbols represent σ_0 and σ_1 , respectively, for two- ($\bullet$ $\triangle$) and three-qubit ($\blacksquare$ $\circ$) systems. Each case is averaged over eight samples randomly chosen from the highly accurate SIC-POVM [74] (we do not plot error bars for clarity). The confidence regions depicted by light red and blue rectangles (color online) are described by values of $0 \leq s \leq s_{\max}$, where $s_{\max}$ is determined by the intersection of the lower and upper bounds. Values s_2 and s_3 represent two- and three-qubits systems, respectively. Similar picture on the right panel holds for the full set of MUB of size $d = 4$ and 8 prepared from analytic formulas [13, 44, 80].

At the heart of calculations of the restricted defect Δ is the problem of determining the rank of the system of equations (3.3.7). Hence, we are interested how perturbation of the vectors $|\varphi'_j\rangle$ affects the values of the two smallest singular values $\sigma_0 = 0$ and $\sigma_1 > 0$ of a matrix $\mathcal{R}$ associated with system (3.3.7). As long as we can distinguish the two singular values, we can correctly calculate the rank of the system and, in consequence, we know the

from the actual values $|\varphi_j\rangle$ on the $(k+1)^{\text{th}}$ decimal place, the value of the inaccuracy factor is $s \approx 10^{-k}$. In definition of s we use the standard Euclidean norm.

proper value of Δ . We must estimate an upper bound for the maximal perturbation of σ_0 and a lower bound for the maximal perturbation of σ_1 which leads to the inequality,

$$|\sigma'_{0,1} - \sigma_{0,1}| \leq \frac{64sd^2}{N} \left(1 - \frac{2d}{N}\right)^2 \sqrt{\frac{N-d}{N(N-1)}}, \quad (3.6.2)$$

where s is the inaccuracy factor (3.6.1), N and d such that $N > 2d$ are appropriate dimensions introduced earlier, the prime symbol indicates a perturbed singular value, and the double subscript $\sigma_{0,1}$ denotes the fact that the above bound is valid for both σ_0 and σ_1 .

The minimal value of s such that the critical condition $\sigma'_0 = \sigma'_1$ holds, determines the upper bound for the confidence region of Δ . The value of Δ will not change if

$$0 \leq s \leq s_{\max} = \frac{\sigma_1}{2f(d, N)} \leq \frac{\sigma'_1 + f(d, N)s}{2f(d, N)}, \quad (3.6.3)$$

where $f(d, N)$ is the right-hand side of (3.6.2) and the last inequality (since σ_1 depends on unavailable exact solution) can be inferred from (3.6.2) too, under the assumption that $f(d, N)s \ll 1$.

In Figure 3.1 we depicted confidence regions for maximal sets of MUB and SIC-POVM for two and three qubits. When leaving the confidence regions we no longer can discriminate σ_0 and σ_1 . Numerical simulations show that setting an appropriate threshold we can calculate the correct value of the (restricted) defect even for considerably disturbed matrices. Nevertheless, in all cases here and in previous chapter, we worked with highly accurate objects, so that all presented results concerning $\mathbf{d}(U)$ and Δ are absolutely credible.

3.7 Summary

In this chapter we investigated the possibility to introduce free parameters to a given generalized quantum measurement with a prescribed symmetry. Two most relevant examples of generalized measurements in low dimensions have been thoroughly examined, namely: mutually unbiased bases (MUB) and symmetric informationally complete-positive operator-valued measures (SIC-POVM).

Based on the notion of unitary defect we introduced its symmetric analog Δ applicable to Hermitian unitary matrices with constant diagonal, which represent Gram matrices corresponding to given POVM. This tool allows us to prove that known maximal sets of MUB in squared dimensions $d \in \{4, 8, 9, 16\}$ as well as SIC-POVM in dimensions $d \in \{4, 5, \dots, 16\}$ are isolated. The result includes a special class of the three-qubit system called Hoggar lines. Also, we showed that three Kochen–Specker sets of vectors, used in the theorem indicating contextuality of quantum mechanics, are isolated, so they cannot be extended.

Moreover, calculating Hermitian unitary defect we can estimate the upper bound for the maximal possible number of free parameters that can exist in incomplete subsets of

$2 \leq m < d$ MUB in dimension $d \in \{2, 3, \dots, 9\}$. Similar calculations have been done for SIC-POVM and we recovered one-dimensional family of this kind of POVM for $d = 3$.

Several open questions are in order:

1. Are maximal sets of $d + 1$ MUB isolated in prime power dimensions?
2. Are SIC-POVM isolated in every dimension $d \neq 3$?
3. Can defect of a unitary matrix be extended over different classes of matrices?

To answer the two first questions one needs a more efficient software to solve very large systems of linear equations. The last question should become clear after the next chapter where we will investigate a very special class of unitary matrices. However, one cannot generalize the defect too far, because the idea of a tangent space, that is the core of the defect, is well established in differential and algebraic geometry and imposes natural constraints on conditions that should be fulfilled by matrices under consideration. One should focus on manifolds defined by matrix equations, where the linear algebra machinery to manipulate an enormous number of equations can be used.



We close the first part of this Thesis. In the next chapter we recall the phenomenon of quantum entanglement and provide an unexpected solution related to the particular state describing four-partite entanglement of six-level systems.

Chapter 4

Absolutely Maximally Entangled States (AME) of Four Quhexes

Chapter based on [\[A4\]](#).

There were many twists and dead-ends in the history of searching for the AME(4, 6) state of four subsystems with six levels each, which eventually have led us in [\[A4\]](#) to the conclusion in the form of

Theorem 3. *There exists an AME(4, 6) state.*

Before we present a proof of this statement, we begin with preliminary results that should be found interesting and might shed some light on additional properties of such a state, which (at the time of preparing this Thesis) are still obscured and not entirely understood.

4.1 Quantum Entanglement

Consider two linear spaces $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$ of dimension d_1 and d_2 , respectively. It turns out, that a tensor product $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is not equal to $\mathbb{C}^{d_1 d_2}$ (individual tensors do not span the entire space) and it can only be presented as a sum of two subsets,

$$\begin{aligned} \mathbb{C}^{d_1 d_2} = & \{x \otimes y : x \in \mathbb{C}^{d_1}, y \in \mathbb{C}^{d_2}\} \cup \\ & \cup \left\{ \sum_{j=1}^r x_j \otimes y_j : x_j \in \mathbb{C}^{d_1}, y_j \in \mathbb{C}^{d_2}, r \geq 2 \right\}. \end{aligned} \quad (4.1.1)$$

This means that not every vector $z \in \mathbb{C}^{d_1 d_2}$ can be factorized onto the tensor product $z = x \otimes y$ of two vectors $x \in \mathbb{C}^{d_1}$ and $y \in \mathbb{C}^{d_2}$. To span entire space $\mathbb{C}^d$ (imposing a particular tensor structure allowed by the factorization $d = d_1 d_2$) we must include additional linear

combinations of $x_j \otimes y_j$. This observation can be generalized for any composite dimension $d = d_1 d_2 \dots d_n$. The most celebrated example of this fact is usually illustrated by the bipartite Bell state

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}[1, 0, 0, 1]^T \neq |x\rangle \otimes |y\rangle \quad : \quad |x\rangle, |y\rangle \in \mathbb{C}^2. \quad (4.1.2)$$

This nontrivial property of tensor spaces is a mathematical counterpart of the most intriguing non-classical phenomenon of the quantum world, called *quantum entanglement*, which describes strong correlations between composite physical systems when subjected to a measurement process.

Every quantum system has an associated Hilbert space $\mathcal{H}_d \equiv \mathbb{C}^d$ (complex vector space) of size d . Throughout this work we assume only finite-dimensional cases and composite systems, i.e an appropriate Hilbert space takes the form of the tensor product of individual components (also finitely many) $\mathcal{H}_d = \mathcal{H}_{d_1} \otimes \dots \otimes \mathcal{H}_{d_n}$ with $d = d_1 d_2 \dots d_n$ for some $n \geq 2$. Each $\mathcal{H}_{d_j}$ is called a local subspace and corresponds to particular degrees of freedom of a given quantum object. However, in a general picture, $\mathcal{H}_{d_j}$ might represent different microscopic objects or even distant laboratories. Now, the information about the system carried by the quantum state, described by the density matrix $\rho \in \mathbb{C}^{d \times d}$, is spread nonlocally over all components (parties), which is a background for physical manifestation of entanglement.

Formally, we define a mixed state ρ to be *entangled*, if the following convex factorization does not exist,

$$\rho = \sum_k p_k \bigotimes_{j=1}^n \rho_{d_j, k}, \quad (4.1.3)$$

where operators $\rho_{d_j, k}$ belong to $\mathcal{L}(\mathcal{H}_{d_j})$ (space of linear maps in $\mathcal{H}_{d_j}$) and $p_k \geq 0$ are probabilities satisfying the normalization condition $\sum_k p_k = 1$. In the case of a pure state this simplifies to the statement that $|\psi\rangle \in \mathcal{H}_d$ is said to be *entangled pure state* if it cannot be expressed as the product of states from the individual subspaces

$$|\psi\rangle = \bigotimes_{j=1}^n |\psi_j\rangle \quad : \quad |\psi_j\rangle \in \mathcal{H}_{d_j}. \quad (4.1.4)$$

Any state which is not entangled should be called *separable*.

It must be emphasized that the entanglement makes sense only in the context of the imposed tensor structure. For example, consider a dimension $d = d_1 d_2 = d_3 d_4$. States, which are entangled with respect to $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ might not necessarily be entangled as elements of $\mathbb{C}^{d_3} \otimes \mathbb{C}^{d_4}$.

Certainly, we shall not delve into the problem of investigating and quantifying the problem of entanglement, which is a good topic for a dozen of such theses [91, 92]. Instead, let us only recall the major applications of this quantum resource [1, 93] shared by different parties

of the entire system, that can be used as a footing of other important processes like dense coding schemes and teleportation [16], quantum cryptography [94, 95], quantum thermodynamics [93] and many others, which would be impossible without existence of entangled states.

4.2 Absolutely Maximally Entangled States

Working with entanglement we distinguish two extrema. Fully separable states for which entanglement vanishes, and the most entangled states called maximally entangled, to which we devote the rest of this chapter. What is in between goes beyond the scope of the story. One should find many additional introductory information to the problem of measuring the amount of entanglement in the survey [96].

Suppose we have a system composed of N parties, and each party is represented by the Hilbert space $\mathcal{H}_d$ of size d , so in the QIT jargon it is called a *qudit* (being a natural extension of 2-dimensional qubits). We say that a pure state $|\psi\rangle$ of such multipartite system is *k-uniform* [97], if it maximizes the entanglement among all possible bipartitions. In other words, we set $1 \leq k \leq \lfloor N/2 \rfloor$ and check whether the state of k subsystems becomes maximally mixed after tracing out $N - k$ other subsystems, that is, its reduced density matrix ρ_{N-k} is proportional to identity,

$$\text{Tr}_{N-k}(\rho_N) = \rho_k = \mathbb{I}_{d^k}/d^k, \quad (4.2.1)$$

where $\rho_N = |\psi\rangle\langle\psi|$ is a density matrix of the entire system and Tr_{N-k} denotes partial trace [98] over $N - k$ subsystems. We have already seen one such maximally entangled Bell state (4.1.2) for which $N = 2$ and $k = 1$. Finally, we define *absolutely maximally entangled* (AME) states [97, 99] as those for which $k = \lfloor N/2 \rfloor$.

From now on, the symbol $\text{AME}(N, d)$ represents AME state of N qudits. In the work, we are interested in AME states of four quhexes, $\text{AME}(4, 6)$, which describe¹ a physical system consisting of four parties with six degrees of freedom each.

As we did for CHM and POVM, let us briefly review the applications and existence aspects of AME states. Most of all, highly entangled AME states are widely used in the field of quantum error correction [100, 101]. Each $\text{AME}(N, d)$ is related to a quantum pure error correcting code [102]

$$\text{AME}(N, d) \leftrightarrow ((N, 1, N/2 + 1))_d, \quad (4.2.2)$$

where the triplet $((N, K, D))_d$ denotes K codewords in $\mathcal{H}_d \otimes \dots \otimes \mathcal{H}_d$ (N times) characterized by distance D [100]. Such a code can be used in detection and recovering all errors acting

¹Actually, we should say “which should describe...”, because at this stage we do not know yet if such states exist.

on less than $D/2$ qudits. Quantum error correcting codes (QECC) can be constructed from particular AME states (treated as codewords), and conversely some AME states arise from QECC [103]. Another applications of AME states include quantum secret sharing protocols [104], multipartite teleportation [105], and even they can be found in such areas of modern physics like quantum holography [106], modeling the AdS/CFT correspondence [102, 107, 108], quantum gravity [109] or string theory [110].

Existence of AME states is yet another open problem, which deserves a lot of effort [111]. They do not exist for four qubit system, $\mathcal{H}_2^{\otimes 4}$ [112], but they do exist for four qudit systems $\mathcal{H}_d^{\otimes 4}$ with $d = 3, 4, 5, 7, 8, \dots$ [113] (where number 6 for quhex system is temporarily missing), and for six qudit systems, $\mathcal{H}_d^{\otimes 6}$ with $d \geq 2$ [114]. It has been also recently proved [115] that for all dimensions N one can find arbitrarily large value of d such that $\text{AME}(N, d)$ exists. Comprehensive list including the most current state-of-the-art concerning AME states is shown in the online *Table of AME states and Perfect Tensors* [116].

4.2.1 Multipartite Entanglement Algebra

We slowly set the stage for the main result of this Thesis. Without loss of generality, let us restrict to the scenario of four qudits (general discussion can be found in the supplementary material of [A4]). So, we assume the system composed of $N = 4$ parties, each of dimension d , described by a pure state $|\psi\rangle \in \mathcal{H} = \mathcal{H}_d \otimes \mathcal{H}_d \otimes \mathcal{H}_d \otimes \mathcal{H}_d$. According to definition, $|\psi\rangle$ is $\text{AME}(4, d)$, if the partial trace of $|\psi\rangle\langle\psi|$ over any subsystem composed of $\lfloor N/2 \rfloor = 2$ parties is proportional to identity. Let us expand $|\psi\rangle$ in the product basis of $\mathcal{H}$

$$|\psi\rangle = \sum_{j,k,l,m=1}^d \mathcal{T}_{jklm} |j\rangle |k\rangle |l\rangle |m\rangle, \quad (4.2.3)$$

where a four-index tensor $\mathcal{T}_{jklm}$ can be transformed (reshaped) into a matrix $U \in \mathbb{C}^{d^2 \times d^2}$ addressed by $U_{\alpha,\beta}$ with $\alpha = k + d(j-1)$ and $\beta = m + d(l-1)$. Note that it is actually possible to obtain six different matrices because there are six possible ways of performing bipartition on a fourpartite system. The tensor $\mathcal{T}$ describes $\text{AME}(4, d)$ iff every matrix obtained in this way is unitary [97]. Since unitarity is invariant under transposition, we can reduce considerations to only three matrices (dropping three particular reorderings of the four-index $_{jklm}$), and it turns out, it is enough for being $\text{AME}(4, d)$ to require that $\mathcal{T}_{jklm}$, $\mathcal{T}_{jmlk}$ and $\mathcal{T}_{jlk m}$ give rise to three different unitary matrices of size d^2 . Such tensors $\mathcal{T}$ are called *perfect* while matrices $U \in \mathbb{U}(d^2)$ are called *2-unitary*. Analogously, in the general case of N subsystems, where N is even, we can introduce the notion of k -unitarity² of a matrix of order d^k with $k = N/2$, see Appendix C in [97].

²Index k in $\mathcal{T}_{jklm}$ has nothing in common with $\underline{k}$ -unitarity.

To describe entanglement qualitatively, we must recall two simple tools from the matrix algebra. The first one is partial transpose operation taken on a given subsystem of a bipartite system of size $d_1 d_2$ described by a matrix $U = U_{d_1} \otimes U_{d_2}$. It can be defined as

$$U^{T_1} = (T \otimes \mathbb{I}_{d_2})(U_{d_1} \otimes U_{d_2}) = U_{d_1}^T \otimes U_{d_2}, \quad (4.2.4)$$

$$U^{T_2} = (\mathbb{I}_{d_1} \otimes T)(U_{d_1} \otimes U_{d_2}) = U_{d_1} \otimes U_{d_2}^T, \quad (4.2.5)$$

where T denotes the standard matrix transpose. The second one is reshuffling (realignment), denoted by U^R , which transforms each block of U into a consecutive row. For a schematic matrix representing a two spin- $\frac{1}{2}$ system ($\mathbb{U}(2) \otimes \mathbb{U}(2)$) the reshuffling transformation looks like,

$$\left[\begin{array}{cc|cc} a_1 & a_2 & b_1 & b_2 \\ a_3 & a_4 & b_3 & b_4 \\ \hline c_1 & c_2 & d_1 & d_2 \\ c_3 & c_4 & d_3 & d_4 \end{array} \right] \xrightarrow{R} \left[\begin{array}{cccc} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ \hline c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{array} \right]. \quad (4.2.6)$$

Note, that while global transpose operation T is, by definition, dimension-agnostic, its partial counterparts T_1 and T_2 (as well as R) strongly depend on the internal structure of the system. However, in our case, the situation is quite simplified, because the size of two local subsystems is equal and fixed $d = (d_1 = d_2) = 6$. Moreover, from

$$(U^{T_2})^{T_1} = U^T \implies U^{T_2} = (U^{T_1})^T \quad (4.2.7)$$

we infer that the spectra of U^{T_1} and U^{T_2} coincide. Therefore, we can concentrate only on one such operation and, skipping irrelevant indices, we denote the partial transpose T_2 by Γ , as the symbol Γ resembles a part of T . If U is represented in a product basis, $U_{jklm} = \langle j, k | U | l, m \rangle$, both operations can be formally defined using multi-indices as

$$U_{jklm}^\Gamma = U_{jmlk} \quad \text{and} \quad U_{jklm}^R = U_{jlk m} \quad \text{for} \quad 1 \leq j, l \leq d_1, 1 \leq k, m \leq d_2. \quad (4.2.8)$$

Physical interpretation of Γ is adapted straightforwardly from the one of T and can be viewed as a time reversal process applied to a single subsystem under consideration [117]. It also plays the fundamental role in the PPT criterion of separability [118, 119]. In contrary, the transformation R , which maps vectors of length d^2 into matrices of size d , does not have any simple physical explanation. Both operations Γ and R can be found in theory of superoperators [60, 120] or in dynamics in dual-unitary quantum circuits [121].

Putting this all together, we can conclude that searching for AME(4, d) state is equivalent to searching a 2-unitary matrix $U \in \mathbb{C}^{d^2 \times d^2}$ such that it remains unitary after operations of reshuffling and partial transposition. Three possible splittings of fourpartite system of qudits corresponding to the three configurations of indices of unitary matrix are shown below

$$\begin{array}{c|c} \mathcal{A} & \mathcal{B} \\ \hline \mathcal{C} & \mathcal{D} \end{array} \leftrightarrow U, \quad \begin{array}{c|c} \mathcal{A} & \mathcal{B} \\ \hline \mathcal{C} & \mathcal{D} \end{array} \leftrightarrow U^\Gamma, \quad \begin{array}{c|c} \mathcal{A} & \mathcal{B} \\ \hline \mathcal{C} & \mathcal{D} \end{array} \leftrightarrow U^R, \quad (4.2.9)$$

where, for a better perception, all four subsystems have been assigned a name.

4.2.2 Entangling Power and Gate Typicality

To measure the entanglement, we are going to use the following linear entropy characterizing distribution of singular values of an arbitrary matrix $M \in \mathbb{C}^{d^2 \times d^2}$,

$$E(M) = \frac{d^2}{d^2 - 1} \left(1 - \frac{\text{Tr}(MM^\dagger MM^\dagger)}{\text{Tr}^2(MM^\dagger)} \right) = \frac{d^2}{d^2 - 1} \left(1 - \frac{1}{\text{Tr}^2(MM^\dagger)} \sum_{j=1}^{d^2} \lambda_j^2 \right), \quad (4.2.10)$$

where λ_j is j^{th} eigenvalue of $MM^\dagger$ (squared singular value of M). This entropy is normalized so that $E \in [0, 1]$ and the maximum value is attained for unitary matrices for which $\lambda_j = 1$.

Entangling power of a bipartite unitary matrix U , can be defined by the entropy E ,

$$e_p(U) = E(U^R) + E(US)^R - 1, \quad (4.2.11)$$

where S is the swap operator, $S(U_{d_1} \otimes U_{d_2})S = U_{d_2} \otimes U_{d_1}$. This is very particular formulation, designed to facilitate operational applicability (especially numerical investigation). For a general definition of entangling power, refer to the original paper [122].

Entangling power is interpreted as the average entanglement created when U acts on a generic product state. The swap does not create any entanglement when acting on any bipartite product state, which is a motivation for the definition of another indicator called *gate typicality* [123], denoted by $g_t(U)$, which distinguishes local operations from the swap

$$g_t(U) = E(U^R) - E(US)^R + 1. \quad (4.2.12)$$

Both quantities are normalized,³ $e_p \in [0, 1]$ and $g_t \in [0, 2]$. Notably, a hypothetical 2-unitary matrix T_{d^2} (T for target⁴) corresponding to AME(N, d) state, if one exists, is characterized by $e_p(T_{d^2}) = g_t(T_{d^2}) = 1$.

Given dimension $d > 1$, all possible values of $e_p(U)$ and $g_t(U)$ for $U \in \mathbb{U}(d^2)$ form a characteristic triangle-shaped area. We call this informally as an (e_p, g_t) -plane. For $d = 3$ it is sketched in Figure 4.1. In this particular case, all the dots within the triangular confinement depict permutation matrices of size 9. We see as, despite they do not cover the available area uniformly, one distinguished point appears in the rightmost corner — this is T_9 representing an AME state of four qutrits [97],

$$\begin{aligned} |\text{AME}(4, 3)\rangle = & (|0000\rangle + |0112\rangle + |0221\rangle + \\ & |1011\rangle + |1120\rangle + |1202\rangle + \\ & |2022\rangle + |2101\rangle + |2210\rangle)/3, \end{aligned} \quad (4.2.13)$$

³Note that other authors can use different normalization for e_p , g_t and E .

⁴One should not be confused when see transpose symbol T or ^{T} , matrix T , and tensor $\mathcal{T}$ and also R , and R or ^{R} for a rotation matrix and reshuffling operation, respectively.

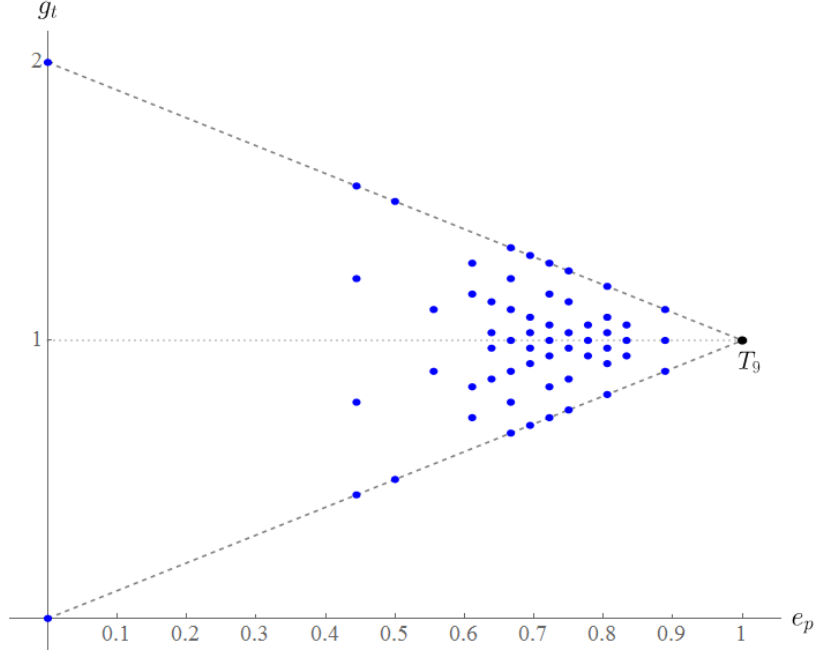


Figure 4.1: Given $d > 1$, all possible values of entangling power and gate typicality form a characteristic triangular shape. Picture shows the case of $d = 3$ with 60 dots representing possible classes of permutation matrices from $\mathbb{P}(9)$. One particular point at $(e_p, g_t) = (1, 1)$ denotes a 2-unitary permutation matrix T_9 representing an AME(4, 3) state (4.2.13).

which in this case can also be expressed in the form of permutation

$$P_{\text{AME}(4,3)} = [3, 7, 5, 4, 2, 9, 8, 6, 1], \quad (4.2.14)$$

where each number denotes the column with unity at j^{th} position.

Obviously, each point on the (e_p, g_t) -plane (not necessarily a permutation matrix) does not describe a single matrix, but rather a whole continuum of matrices. It is easy to see that entangling power is invariant with respect to local operations (rotations)

$$e_p(U) = e_p \left(\left(U_d^{(1)} \otimes U_d^{(2)} \right) U \left(U_d^{(3)} \otimes U_d^{(4)} \right) \right). \quad (4.2.15)$$

for $U_d^{(1)}, U_d^{(2)}, U_d^{(3)}$ and $U_d^{(4)} \in \mathbb{U}(d)$ and $U \in \mathbb{U}(d^2)$. This fact will be extremely useful in Section 4.6.2. Another property of (e_p, g_t) -plane is its symmetry along the bisector ($g_t \equiv 1$). Moreover, the lower and upper edges are related by the mapping

$$\left(X \in \text{lower edge} \implies X\sqrt{S} \in \text{bisector} \right) \implies XS \in \text{upper edge}, \quad (4.2.16)$$

for S be the swap. We will use (e_p, g_t) -plane to present pictorially several interesting features of matrices from $\mathbb{O}(36)$ in Section 4.4.3.

4.3 Quantization of the Problem of 36 Officers of Euler

Since searching for AME states can be performed in the domain of unitary matrices and in particular, the state $\text{AME}(4, 6)$ corresponds to a 2-unitary matrix from $\mathbb{U}(36)$, we should find such a matrix. We start our search from the reminder of some classical problem and its transformation to the quantum realm.

We have already recalled the definition of (orthogonal) Latin square in Section 2.4 of Chapter 2. Problem of existence of OLS emerges at the very beginning for $d = 2$. In general, there are only two dimensions for which the answer concerning orthogonality of Latin squares is negative; it is for $d = 2$ and $d = 6$ [51, 124], and the latter case corresponds directly to the famous problem of thirty-six officers of Euler [125]. In the classical formulation, the question pertains to the arrangement of 36 officers, six of different rank, and six of different regiment (assignment), in a 6×6 square such that no rank nor regiment repeats in any row and column. Equivalently, one asks about two Latin squares (one of ranks and another of regiments) related by orthogonality. While the case of $d = 2$ is trivial, it took more than a century to prove that no solution of the 6-dimensional problem exists [126].

Such problems can be conceivably solved in the quantum realm, which provides more room for potential solutions as it was shown e.g. in the case of SudoQ [127] or as we will see in Chapter 5. But, in the first place, the issue must be properly quantized.

After [20] we recall the definition of *quantum Latin square* (QLS), which is a $d \times d$ array of elements of the Hilbert space $\mathcal{H}_d$ such that every row and every column forms an orthonormal basis in $\mathcal{H}_d$. For example, the following constellation of quantum states from $\mathcal{H}_4$ forms a QLS,

$$\begin{bmatrix} |0\rangle & |1\rangle & |2\rangle & |3\rangle \\ |1\rangle & |0\rangle & |3\rangle & |2\rangle \\ |2\rangle & |3\rangle & |0\rangle & |1\rangle \\ |3\rangle & |2\rangle & |1\rangle & |0\rangle \end{bmatrix}. \quad (4.3.1)$$

Two such quantum squares $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are called *orthogonal quantum Latin squares* (OQLS) iff the pointwise inner product of any row from $\mathcal{Q}_1$ with any row from $\mathcal{Q}_2$ provides only a single 1 among all zeros. Above QLS (4.3.1) can be complemented⁵ with the following one,

$$\begin{bmatrix} |0\rangle & |1\rangle & |2\rangle & |3\rangle \\ |1\rangle & |0\rangle & |3\rangle & |2\rangle \\ |2\rangle & |3\rangle & |0\rangle & |1\rangle \\ |3\rangle & |2\rangle & |1\rangle & |0\rangle \end{bmatrix} \perp \begin{bmatrix} |0\rangle & |2\rangle & |3\rangle & |1\rangle \\ |1\rangle & |3\rangle & |2\rangle & |0\rangle \\ |2\rangle & |0\rangle & |1\rangle & |3\rangle \\ |3\rangle & |1\rangle & |0\rangle & |2\rangle \end{bmatrix}. \quad (4.3.2)$$

One particular open problem concerns the question about existence of a pair of quantum orthogonal LS in every dimension [128]. If it was possible to find such OQLS of size six

⁵We apply standard orthogonality symbol $\perp$ to denote orthogonality of two QLS.

then, apart from filling one blank spot in quantum combinatorics discipline, the quantum analog of the classical problem of Euler would be solved.

4.4 Orthogonal Approximation of AME(4, 6)

Even though, there are no two orthogonal Latin squares of order six, one can examine pairs of such objects, which are as close to be orthogonal as possible. This problem has its roots in the studies of Horton [129]. Later, Lieven Clarisse et al. [130] investigated permutation matrices and Latin squares in the context of entangling power. Here, we briefly recall one particular result, which from our perspective is the most interesting. It states that there exists a permutation matrix $P \in \mathbb{P}(36)$ such that⁶ $e_p(P) = 314/315 \approx 0.9968$ and this value is maximal possible over all permutation matrices of this size. This result approximates the solution of the Euler's problem in the best possible (classical) way.

4.4.1 Permutation Matrix P of Order 36

Matrix P is given implicitly in the form of two Latin squares, L_1 and L_2 , which are “almost” orthogonal. When superimposed, they form the following array $\tilde{P}$ (we keep the original notation),

$$\underbrace{\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 3 & 4 & 6 & 5 & 1 & 2 \\ 4 & 3 & 5 & 6 & 2 & 1 \\ 5 & 6 & 2 & 1 & 4 & 3 \\ 6 & 5 & 1 & 2 & 3 & 4 \end{bmatrix}}_{=L_1} \cup \underbrace{\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 6 & 5 & 1 & 2 & 4 & 3 \\ 4 & 3 & 6 & 5 & 2 & 1 \\ 5 & 6 & 2 & 1 & 3 & 4 \end{bmatrix}}_{=L_2} = \begin{bmatrix} 11 & 22 & \mathbf{33} & \mathbf{44} & 55 & 66 \\ 24 & 14 & 45 & 36 & 61 & 52 \\ 32 & 41 & 64 & 53 & 16 & 25 \\ 46 & 35 & 51 & 62 & 24 & 13 \\ 54 & 63 & 26 & 15 & 42 & 31 \\ 65 & 56 & 12 & 21 & \mathbf{33} & \mathbf{44} \end{bmatrix} = \tilde{P}. \quad (4.4.1)$$

Array in (4.4.1) encodes aforementioned permutation matrix $P \in \mathbb{P}(36)$ in the following way. Every ordered pair $jk \in \tilde{P}$ can be viewed as a 6×6 matrix $|j\rangle\langle k|$ and forms an appropriate block of P . In other words, if P is seen as a block matrix with 36 blocks of size

⁶Note that our customized normalization differs from the one used in [130].

6×6 , then

$$P = \sum_{a,b=1}^6 |aj\rangle\langle bk|, \quad (4.4.2)$$

where j and k correspond to a proper element of $\tilde{P}$, i.e. $jk = \tilde{P}_{ab}$ (note that jk is not a product but a string of symbols). Apparent conflicts in two pairs of blocks, **33** and **44** prevent $\tilde{P}$ from being a six-dimensional OLS. Note also that the symbols 34 and 43 do not appear in the square.

Matrix P in the decoded form is shown in Figure 4.2. It has additional property as it lies on the lower edge of the (e_p, g_t) -plane, so both P and P^Γ are permutations too. Explicit vectorized, alas unhandy, form of permutation matrix P reads

$$P = [1, 15, 8, 29, 36, 22, 16, 2, 30, 7, 21, 35, 23, 31, 3, 18, 10, 26, \\ 32, 24, 17, 4, 25, 9, 12, 28, 33, 20, 5, 13, 27, 11, 19, 34, 14, 6], \quad (4.4.3)$$

which should be understood like (4.2.14).

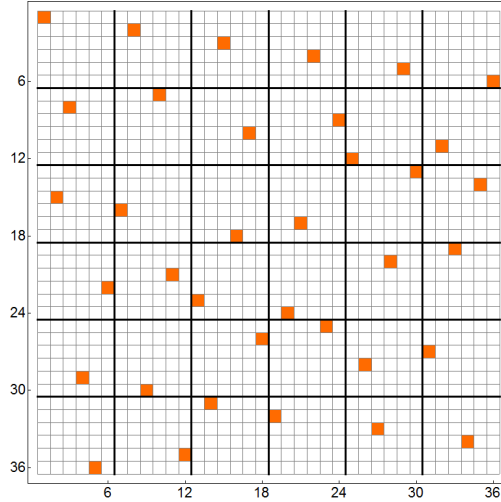


Figure 4.2: Permutation matrix P of order 36 associated with two “almost” orthogonal Latin squares (4.4.1) that maximizes entangling power in the set $\mathbb{P}(36)$. Blank squares represent zeros, while filled squares represent ones.

Authors conclude the paper [130] with a sequence of open questions. One of them concerns the existence of unitary matrix for which entangling power would exceed the value $e_p(P)$. Hence, the next natural step is to ask about extension of the domain of searching over orthogonal or unitary matrices. We will follow the gradual path: $\mathbb{P}(36) \rightarrow \mathbb{O}(36) \rightarrow \mathbb{C}^{36 \times 36} \rightarrow \mathbb{U}(36)$ with one unnatural deviation in the penultimate step. Meanwhile, let us start with the real case, and take permutation P as the starting point for our research.

4.4.2 Orthogonal Matrix Q of Order 36

Two pairs of blocks, $|3\rangle\langle 3|$ and $|4\rangle\langle 4|$, in $\tilde{P}$ are in conflict of (Latin) orthogonality. This observation might tentatively suggest a sort hidden functional dependence that has been temporarily suppressed when projected onto the meager set of permutations. As we already noticed, sometimes such obstacles turn to be resolvable when the problem is embedded into a more general environment. One obvious thing that comes for consideration is a notion of entanglement between particular elements of the matrix P , or even better, of $\tilde{P}$, where it would be easier to visualize inseparability in the form of combinations of particular elements from $\tilde{P}$. However, at this stage it is nothing but pure intuition.

Let us then introduce additional structures in P to leave permutations and immerse into the set of orthogonal matrices, to check whether this can somehow improve the value of entangling power. To this end, take two problematic blocks, **33** and **44** in P and extend them in the following way (allowing entangled states):

$$\mathbf{33} \leftrightarrow |3\rangle\langle 3| \rightarrow |3\rangle\langle 3| \cos \omega_1 - |4\rangle\langle 3| \sin \omega_1, \quad (4.4.4)$$

$$\mathbf{44} \leftrightarrow |3\rangle\langle 4| \rightarrow |3\rangle\langle 4| \sin \omega_1 + |4\rangle\langle 4| \cos \omega_1, \quad (4.4.5)$$

so that each unity is overridden by $\cos \omega_1$. Then, we complete appropriate spaces with $\mp \sin \omega_1$ to preserve global orthogonality. Now, the fragment of the first block-row (first six rows) of P looks like ($\bullet = 0$)

$$\dots \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|} \hline \bullet & \bullet & & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \hline \bullet & \bullet & & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \hline \bullet & \bullet & \cos \omega_1 & \bullet & \bullet & \bullet & \bullet & \bullet & -\sin \omega_1 & \bullet & \bullet & \bullet \\ \hline \bullet & \bullet & \sin \omega_1 & \bullet & \bullet & \bullet & \bullet & \bullet & \cos \omega_1 & \bullet & \bullet & \bullet \\ \hline \bullet & \bullet & & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \hline \bullet & \bullet & & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \hline \end{array} \dots \quad (4.4.6)$$

If we repeat this replacement for two lower **33** and **44** blocks, matrix P becomes⁷ Q

$$P \rightarrow Q = Q(\omega_1, \omega_2) \in \mathbb{O}(36), \quad (4.4.7)$$

which is orthogonal and depends on two arbitrary phases $\omega_j \in [0, 2\pi)$.

This procedure can be rephrased formally. We start with a *template* matrix Q_0 of the form

$$Q_0(\omega_1, \omega_2) = \mathbb{I}_2 \oplus R(\omega_1) \oplus \mathbb{I}_{28} \oplus R(\omega_2) \oplus \mathbb{I}_2, \quad (4.4.8)$$

where

$$R(\omega_j) = \begin{bmatrix} \cos \omega_j & -\sin \omega_j \\ \sin \omega_j & \cos \omega_j \end{bmatrix}$$

⁷ Q is the next unused character in the Latin alphabet. Next in the line are V and W , as R , S , T and U are reserved for rotation, swap, target and unitary matrices, respectively.

is an ordinary two-dimensional rotation matrix, and we apply the permutation matrix P from the previous section to $Q_0(\omega_1, \omega_2)$ obtaining

$$Q(\omega_1, \omega_2) = Q_0(\omega_1, \omega_2)P. \quad (4.4.9)$$

One can readily validate the correctness of this construction. The structure of the block matrix Q_0 corresponds directly to the form we wish to impose on P . Here, two orthogonal blocks $R(\omega_1)$ and $R(\omega_2)$ are going to overlap colliding unities in two pairs of blocks in P .

Matrix Q can be immediately optimized over all possible phases to maximize the value of the entangling power $e_p(Q(\omega_1, \omega_2))$. It turns out that for

$$\omega^* = (\omega_1^*, \omega_2^*) = \pi \left(\frac{5}{6}, \frac{1}{6} \right) \quad (4.4.10)$$

we observe slightly increasing trend

$$0.9968 = e_p(P) < e_p(Q^*) = \frac{419}{420} \approx 0.9976. \quad (4.4.11)$$

We will denote the best representation of Q by Q^* for some ω^* .⁸ The reason the first phase is in bold will be explained below. Matrices Q_0^* and Q^* of order 36 are shown in Figure 4.3.

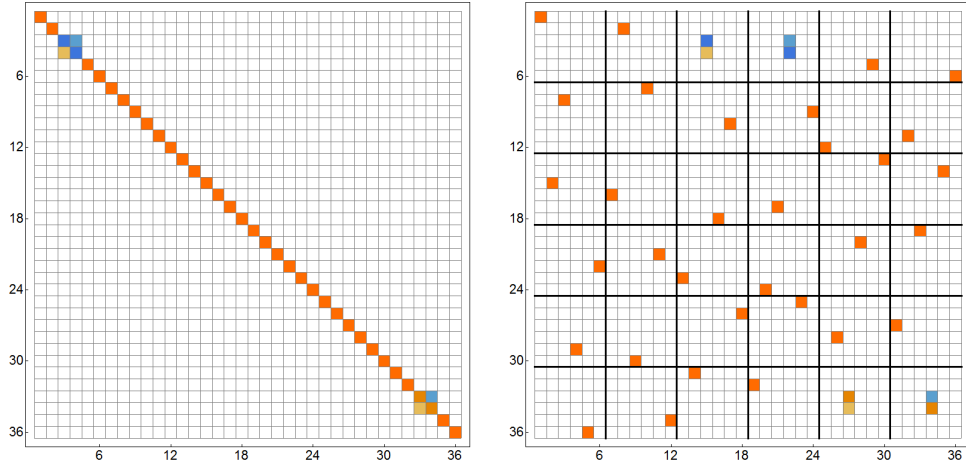


Figure 4.3: Template Q_0^* (4.4.8) (left panel) and its final form Q^* (right panel) after optimization procedure. Note the difference with respect to Figure 4.2, as the conflict in entries **33** and **44** is partially cured by allowing entangled states.

This is the first minor achievement on the way to $\text{AME}(4, 6)$ that, at least, answers a one 15-years-old question from [130] in the affirmative way by means of quite primitive machinery. But, it is possible to get even more.

⁸Symbol of star $*$ is not a complex conjugate $\bar{\cdot}$.

Instead of probing two particular blocks, one can do this for a different pair, or even, for any sequence of different blocks. The problem is, which setup to choose to start with, because clearly the scale of the problem prevents any sequential work, to go through every possible initial configuration, in any reasonable time. To omit this problem, we shall try to attack this issue globally.

4.4.3 Orthogonal Matrix V of Order 36

Let us prepare an orthogonal block-diagonal matrix

$$V_0(\omega) = \bigoplus_{j=1}^{18} R(\omega_j), \quad (4.4.12)$$

where $\omega = (\omega_1, \dots, \omega_{18})$ denotes the vector of phases. And then, as in the case of Q , we put

$$V = V(\omega) = V_0(\omega)P. \quad (4.4.13)$$

Such construction obviously overlaps all direct regions containing unities in P . By introducing 18 orthogonal variables we hope to overstep the current value of $e_p(Q^*)$. Indeed, it is possible to improve previous results and to find unitary matrix V^* such that

$$0.9976 = e_p(Q^*) < e_p(V^*) = \frac{208 + \sqrt{3}}{210} \approx 0.9987 \quad (4.4.14)$$

for some phases ω^* , which will be provided below. Additionally we have $g_t(V^*) = 1$ so this matrix lies exactly on the bisector of (e_p, g_t) -plane. The structure of matrices V_0^* and V^* is presented in Figure 4.4.

Let us elaborate on this result. After all, actually almost identical random walk routine over multidimensional real space has already been described in Chapter 2. The distinction is that here we optimize (maximize) slightly different target function $\mathcal{Z}(M) \propto e_p(M)$. Regardless of the initial choice of phases $\omega \in [0, 2\pi)^{\times 18}$, such optimization procedure is almost always convergent to a configuration, which is usually much better than previously considered matrices. It very rarely gets stuck on $V(\omega_{\text{stuck}})$ such that $e_p(V(\omega_{\text{stuck}})) \leq e_p(Q^*)$ for some set of parameters ω_{stuck} .

The space of phases is quite large and this allows us to fix some particular values of ω to recover all other components analytically. One particular example of ω^* , out of continuum possibilities, that maximizes entangling power, is

$$\omega^* = \pi \left(\frac{1}{5}, \frac{5}{6}, \frac{1}{4}, \frac{6}{5}, \frac{3}{4}, \frac{1}{4}, \frac{6}{5}, \frac{7}{12}, \frac{5}{4}, \frac{6}{5}, \frac{5}{3}, \frac{5}{4}, \frac{6}{5}, \frac{3}{2}, \frac{5}{4}, \frac{6}{5}, \frac{17}{12}, \frac{5}{4} \right). \quad (4.4.15)$$

Note, that for simplicity, in Q^* , here, and in the next example, the second 2×2 block in the template matrix has been fixed to $R(5\pi/6)$.

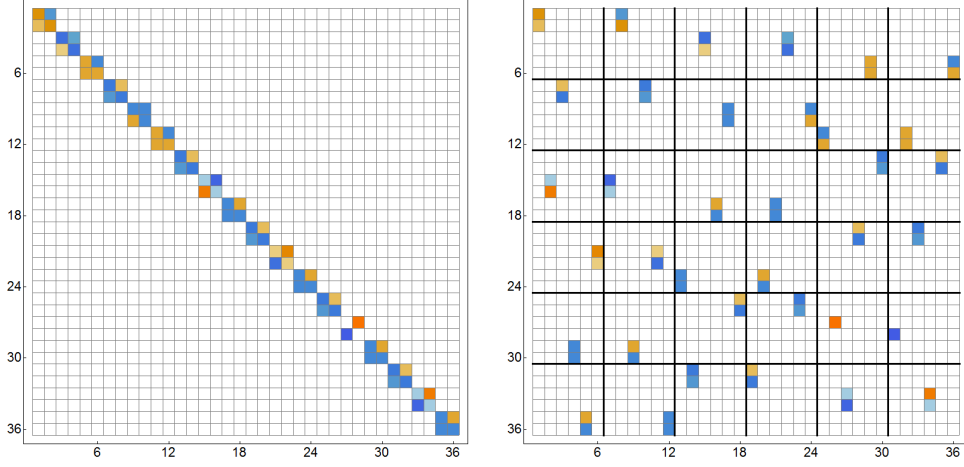


Figure 4.4: Block diagonal template V_0^* (4.4.12) (left panel) and its final form V^* (right panel).

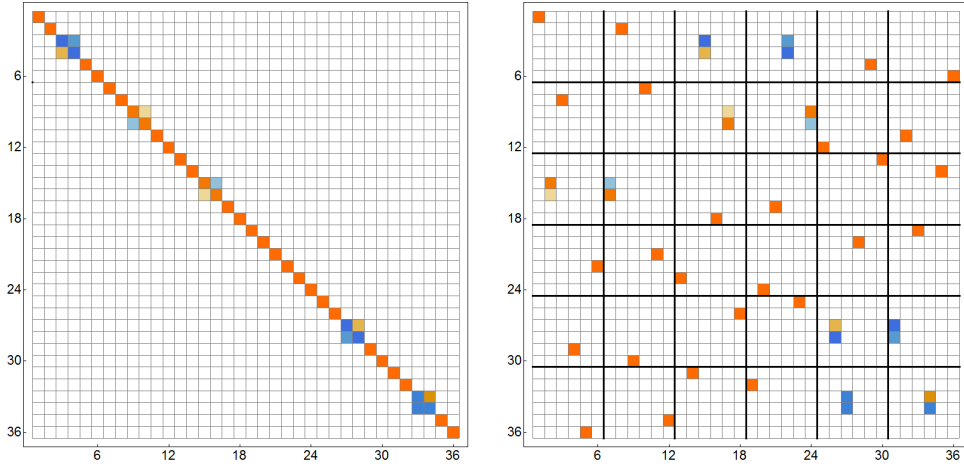


Figure 4.5: Template W_0 (4.4.17) (left panel) and its final form W (right panel), which represents V^* reduced to only 5 nontrivial phases.

In particular, one can reduce the set of non-zero elements in ω not decreasing the value of e_p . This leads to the following simplified form of V called W ,

$$W = W_0 \left(\pi \left(\frac{5}{6}, \frac{23}{12}, \frac{1}{12}, 0, \frac{7}{6}, \frac{5}{4} \right) \right) P, \quad (4.4.16)$$

where

$$W_0(\omega_1, \dots, \omega_6) = \bigoplus_{j=1}^6 (\mathbb{I}_2 \oplus R(\omega_j) \oplus \mathbb{I}_2) \quad (4.4.17)$$

so that $e_p(W) = e_p(V^*)$ and effectively, we have only 5 degrees of freedom. It is not known, whether it is possible to further shrink the number of phases down, or to reduce the number of nonvanishing entries of V in any other way, keeping the value of entangling power unchanged. Matrices W_0 and W are drawn in Figure 4.5 and from now on we will refer to W (instead of V^*) as the best orthogonal approximation of T_{36} .

Such a wealth of phases allows us to penetrate the (e_p, g_t) -plane in many previously unknown directions. In some sense, the family of V includes Q , P and other interesting objects, for instance those laying on the edges of the triangle plotted in Figure 4.6. Knowing exact phases, we can easily interpolate between P , Q and W . For example, using the parameterization

$$\omega(t) = \frac{\pi}{6} t (5, 1) \quad : \quad t \in [0, 1] \quad (4.4.18)$$

applied to Q_0 we can smoothly travel from P to Q^* , while

$$\omega(t) = \frac{\pi}{12} (10, 23t, t, 0, 14t, 13t + 2) \quad : \quad t \in [0, 1] \quad (4.4.19)$$

applied to W_0 connects Q^* and W (or V^*), see Figure 4.7.

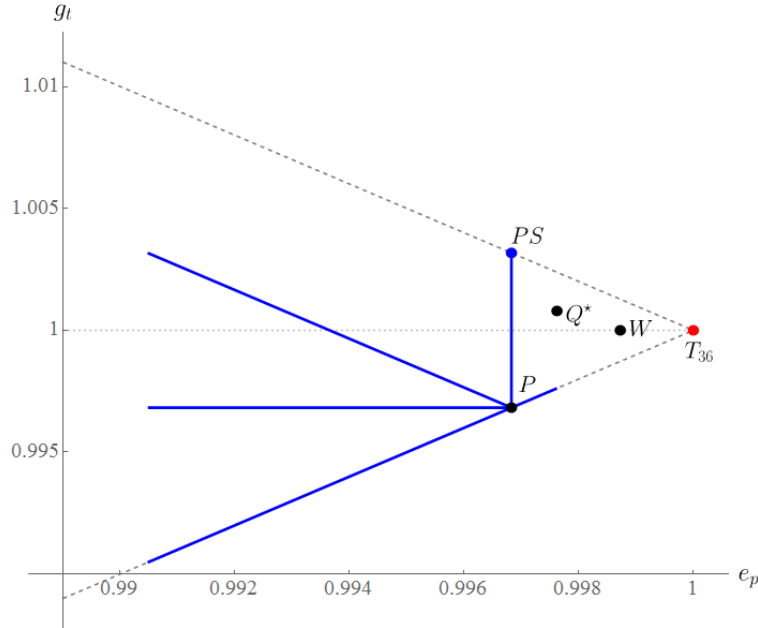


Figure 4.6: Unitary matrices of order 36 projected onto the (e_p, g_t) -plane. Four simple trajectories starting at P , obtained by means of $V(\omega)$ for different parameterizations of the vector of phases ω in Eq. (4.4.17), are drawn. In particular, we can thoroughly describe the families lying on the edges of the triangle, however, no trajectory can get close enough to the corner of the triangle representing the desired 2-unitary matrix T_{36} .

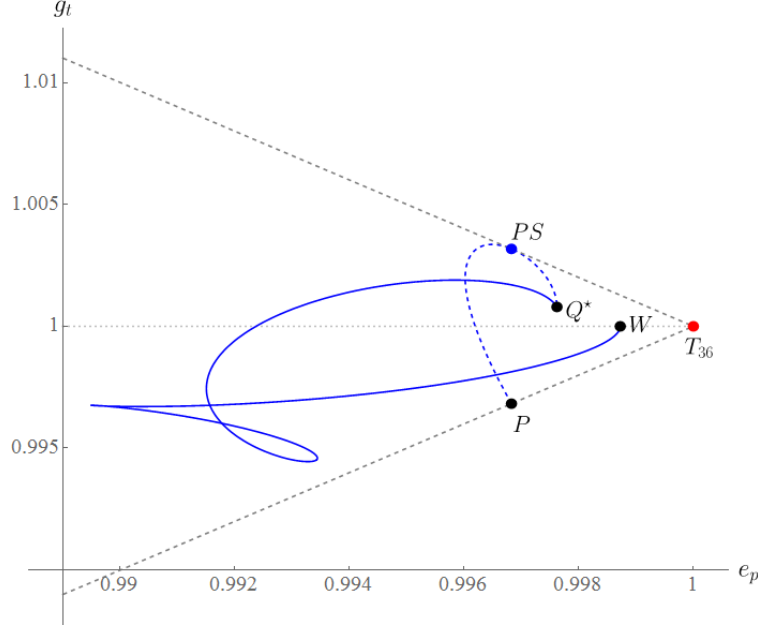


Figure 4.7: Example of two trajectories (4.4.18) and (4.4.19) connecting P with Q^* (dashed line) and Q^* with W (solid line). Note that the first trajectory crosses PS on the upper edge before it gets to Q^* . Both trajectories representing orthogonal matrices are relatively far from the target 2-unitary matrix T_{36} .

Another curious feature of all matrices from the family of V is an attractive character towards CUE⁹ under the action of swap, which is represented by the following map,

$$s : \mathbb{U}(36) \ni U \mapsto US^t \in \mathbb{U}(36) \quad \text{for } t \in [0, 1]. \quad (4.4.20)$$

This seems to be a general attribute of any unitary matrix since no matter what we take as a starting point, we always observe either parabolas bending to the center of the (e_p, g_t) -plane, or straight lines, when we start from points of $g_t \equiv 1$, see Figure 4.8. Such behavior, which makes CUE to be a kind of an attractor, is very suggestive and might lead one to a conclusion that a hypothetical solution T_{36} , if exists, must be extremely isolated and it differs from a generic form of an orthogonal matrix significantly.

Next generalization of the permutation matrix P consist of gradually increasing the size of the blocks used to overlap unities in P . We have already checked the case of eighteen 2×2 orthogonal blocks spread over an 36×36 array according to the permutation matrix P .

⁹By CUE (*circulant unitary ensemble*) we mean a class of random unitary matrices drawn according to the Haar measure on the unitary group $\mathbb{U}(36)$, for which the average values of e_p and g_t read $\langle (e_p, g_t) \rangle = \left(\frac{d^2 - 1}{d^2 + 1}, 1 \right) \approx (0.9459, 1)$ in case of $d = 6$.

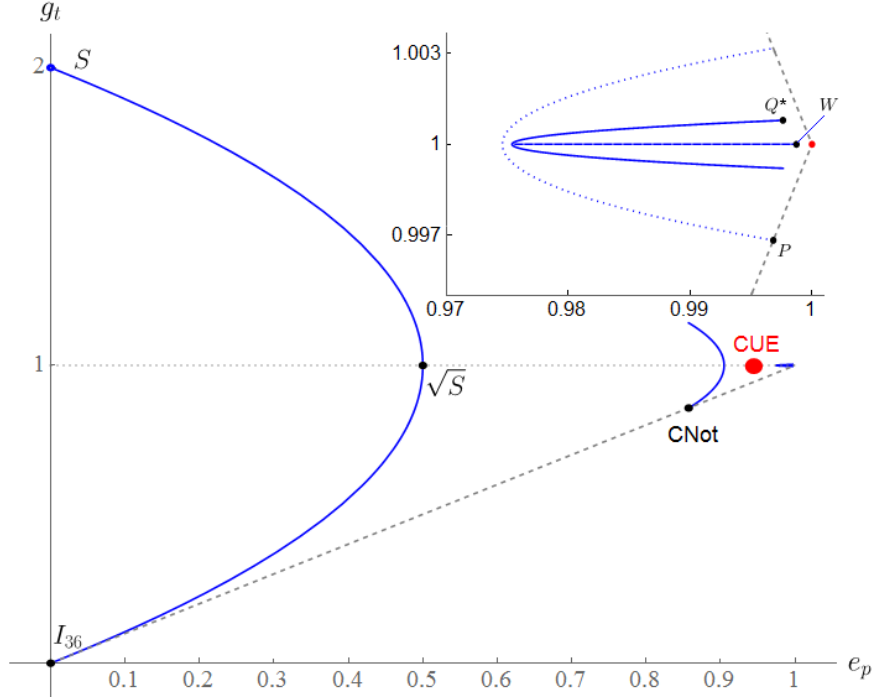


Figure 4.8: The (e_p, g_t) -plane for unitary matrices of order 36. Orbits of identity matrix and representation of the CNot gate under the powers of swap (4.4.20) exhibit attractive character towards the CUE area. This is universal observation also for other randomly taken matrices (not plotted here for clarity). In the magnified vicinity of the corner around $(1, 1)$ one recognizes similar behavior for P (dotted), Q^* (solid) and W (dashed line) matrices. Upper edge of (e_p, g_t) -plane and T_{36} are not drawn.

Factorization the number 36 provides 9 such possibilities. We start with 36 blocks of size 1×1 , through 18 blocks of size 2×2 , then 12 blocks of size 3×3 , ... up to a single block of size 36×36 . In each case we can apply optimization procedure to maximize the entangling power. The results are collected in Table 4.1.

In the first case $36 \times (1 \times 1)$ (not included in Table 4.1), we cannot get a matrix with a greater entangling power, just by definition of P . Only in the configuration of 18 blocks of size two we used parameterization of blocks in the form of rotation matrix. In other cases, we mainly used generic orthogonal matrices obtained from polar decomposition procedure. Some attempts with analytical parameterization of orthogonal matrices of order 3 and 4 did not bring any better result. In the last two cases, it was even impossible to recover the best values because the space accessible for a random searching was too large. In general, despite many different attempts and putting much computational effort, we were unable to

#blocks	block size	$\max\{e_p\}$
18	2×2	$= e_p(W)$
12	3×3	$= e_p(Q^*)$
9	4×4	$= e_p(W)$
6	6×6	$= e_p(W)$
4	9×9	$= e_p(W)$
3	12×12	$= e_p(W)$
2	18×18	$\ll e_p(Q^*)$
1	36×36	$\ll e_p(Q^*)$

Table 4.1: Numerical simulations using block structures of different size introduced in the permutation matrix P . In each case the highest value of entangling power cannot exceed $e_p(W)$, which might suggest that W is the global maximum.

find anything better than W . Interestingly, in the case $9 \times (4 \times 4)$ we observe as optimal 4×4 blocks almost always simplify to the form $R(\alpha_j) \oplus R(\beta_k)$ for some $\alpha_j, \beta_k \in [0, 2\pi)$, which reduces this case to the “best” one of $18 \times (2 \times 2)$. This gently suggests, that W might be the global optimum.

Permutation matrix P , as a base for further calculations, has been chosen unquestionably because of its distinguished role in the set of all permutations matrices. Nevertheless, one can naturally ask about picking something different than P . We checked “a few” other permutations out of

$$36! = 371\,993\,326\,789\,901\,217\,467\,999\,448\,150\,835\,200\,000\,000 \quad (4.4.21)$$

— the total number of possibilities, and in no case any matrix with better e_p signature was found. Different starting points did not lead to any better findings than those represented by Q^* or W . Neither, no better results are obtained when we temporarily switch to complex domain, replacing orthogonal rotations $R(\omega_j)$ by unitary counterparts or similar complex structures. This last remark is exceptionally puzzling, particularly in the context of the results described in Section 4.6.1!

Exhaustive numerical and theoretical research did not lead to anything beyond W in the class of orthogonal matrices. Instead, matrices P , Q^* , W and others have been thoroughly examined in the matter of being local extrema of e_p , by Grzegorz Rajchel-Mieldzioć — the coauthor of [A4]. Grzegorz also performed detailed analysis of the reduced family W , which was roughly presented in Figure 4.6. Please refer to his thesis¹⁰ for more interesting insights and details concerning analytical description of the (e_p, g_t) -plane.

¹⁰Under preparation.

We briefly conclude this section with the following chain of inequalities

$$0 < \underbrace{e_p(P)}_{\approx 0.9968} < \underbrace{e_p(Q^\star)}_{\approx 0.9976} < \underbrace{e_p(W)}_{\approx 0.9987} < 1 \quad (4.4.22)$$

that significantly improves the state of knowledge about the set of orthogonal matrices $\mathbb{O}(36)$ in the context of entangling power and approximation of AME(4, 6) state. In view of the numerical evidence, we tend to believe that a real AME(4, 6) state does not exist. And the matrix W is, so far, the best approximation of such an object. In the next section we present another prospective idea, which might help to support the fact of nonexistence of a real AME(4, 6) state.

4.5 Isoentropic Triplets of Matrices

So far, we have proved that the set of orthogonal matrices can be investigated in new directions, which provided much better metrics for entangling power, getting us closer to the hypothetical target T_{36} at the cusp in the (e_p, g_t) -plane.

Let us look at the vectors of singular values corresponding to matrices P , $Q^\star$ and W and how they progressively flatten. We have, for P

$$\text{svd}(P) = \text{svd}(P^\Gamma) = [\{1\}^{36}]^T, \quad (4.5.1)$$

$$\text{svd}(P^R) = [\{\sqrt{2}\}^2, \{1\}^{34}]^T, \quad (4.5.2)$$

for $Q^\star$

$$\text{svd}(Q^\star) = [\{1\}^{36}]^T, \quad (4.5.3)$$

$$\text{svd}((Q^\star)^R) = \left[\left\{ \sqrt{\frac{3}{2}} \right\}^2, \{1\}^{32}, \left\{ \frac{1}{\sqrt{2}} \right\}^2 \right]^T, \quad (4.5.4)$$

$$\text{svd}(Q^\star)^\Gamma = \left[\left\{ \sqrt{\frac{3}{2}} \right\}^4, \{1\}^{28}, \left\{ \frac{1}{\sqrt{2}} \right\}^4 \right]^T, \quad (4.5.5)$$

and for W

$$\text{svd}(W) = [\{1\}^{36}]^T, \quad (4.5.6)$$

$$\text{svd}(W^R) = \text{svd}(W^\Gamma) = \quad (4.5.7)$$

$$= \left[\left\{ \frac{1}{2} \sqrt{4 - \sqrt{2} + \sqrt{6}} \right\}^6, \{1\}^{20}, \left\{ \frac{1}{2} \sqrt{4 + \sqrt{2} - \sqrt{6}} \right\}^6 \right]^T, \quad (4.5.8)$$

where symbol $\{x\}^m = \overbrace{x, \dots, x}^{\times m}$ denotes m repetitions of the number x . We observe as the number of non-unity components gradually grows but their values get equalized and obviously on the way to T_{36} these vectors should be all ones also for R and Γ realignments. To see this better, let us look at the suitably presented numerical values:

$$\begin{aligned}
& \left[\{1.4142\}^2, \{1\}^{34} \right]^T \\
& \left[\{1.2247\}^2, \{1\}^{32}, \{0.7071\}^2 \right]^T \\
& \left[\{1.2247\}^4, \{1\}^{28}, \{0.7071\}^4 \right]^T \\
& \left[\{1.1219\}^6, \{1\}^{20}, \{0.8609\}^6 \right]^T \\
& \quad \downarrow \\
& \left[\{1 \mp \varepsilon\}^{36} \right]^T \text{ for } \varepsilon\text{-neighborhood of } T_{36},
\end{aligned}$$

where the last entry makes sense (for $\varepsilon \ll 1$) provided that T_{36} is not a topologically isolated point.

All previous calculations assumed restriction to the set of orthogonal matrices $\mathbb{O}(36)$. We can still stay in the real domain but relaxing the constraint of orthogonality. This should allow us to examine a broader class of generic matrices of size 36 and possibly find another path to T_{36} . However, even in the set of matrices “without any structure”, we should focus our attention on a special subclass. We will consider the set of matrices

$$\mathcal{J}_{36} = \left\{ M \in \mathbb{R}^{36 \times 36} : \text{svd}(M) = \text{svd}(M^\Gamma) = \text{svd}(M^R) \right\} \quad (4.5.9)$$

for which each realignment yields the same singular value decomposition, or equivalently, the same entropy E . A matrix $M \in \mathcal{J}_{36}$ will be called *isoentropic*.

As we will no longer sample the set $\mathbb{O}(36)$, we cannot use e_p and g_t . Thus we should switch to a general measure in form of the linear entropy (4.2.10) adapted for $d = 6$ to real domain

$$E(M) = \frac{36}{35} \left(1 - \frac{\text{Tr}(MM^T MM^T)}{\text{Tr}^2(MM^T)} \right). \quad (4.5.10)$$

One must be careful and notice that if all vectors of singular value of M , its partial transpose M^Γ , and reshuffling M^R are equal then M has equal entropies for each realignment too. But the converse statement does not hold true.

The set $\mathcal{J}_{36}$ is not empty, as for example zero-entropy flat matrix $J_{jk} = \text{const} \in \mathbb{R} (\forall j, k)$ belongs there. Soon it will be clear that $\mathcal{J}_{36}$ has a much richer internal structure with continuum of other nontrivial elements. We can envision $\mathcal{J}_{36}$ as the main diagonal of the unit cube for which each principal edge corresponds to $E(M)$, $E(M^R)$ and $E(M^\Gamma)$, see

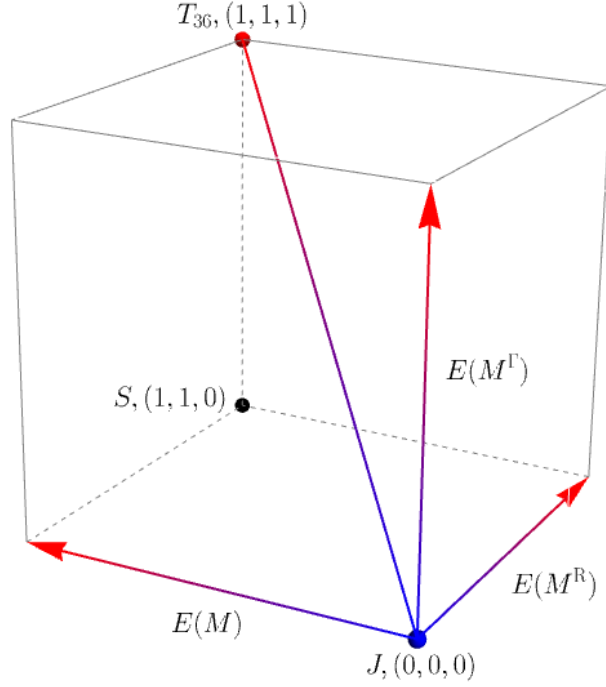


Figure 4.9: Visualization of the E -cube with its main diagonal. Two antipodal points of E -diagonal are occupied by T_{36} and the flat matrix J . Swap matrix S for which $E(S) = E(S^R) = 1$ and $E(S^\Gamma) = 0$ is located in the $(1, 1, 0)$ vertex.

Figure 4.9. We will call it E -cube and E -diagonal, respectively. So J lies at the beginning of the E -diagonal, while the real AME(4, 6) representation in the form of T_{36} , if exists, would obviously be found on the other end.

Suppose for a moment a general case and put $d > 1$. In the remaining part of this section we will investigate a simple map in $\mathbb{R}^{d^2 \times d^2}$ that transforms any real matrix M into an isoentropic one. We will check the properties of this map and draw a conjecture concerning the existence of real a AME(4, 6) state.

Take any real matrix $X = X_0$ of size $d^2 \times d^2$ and define a recursive sequence

$$X_{k+1} = \frac{1}{2}X_k^R + \frac{1}{2}X_k^\Gamma \quad \text{for } k \in \mathbb{N}_0. \quad (4.5.11)$$

Suppose the limit of X_k for $k \rightarrow \infty$ exists, put $Y = \lim_{k \rightarrow \infty} X_k$ and denote the limit operation by Ξ , hence $Y = \Xi(X)$.

Proposition 4. $\forall d \in \mathbb{N}$ and $\forall X \in \mathbb{R}^{d^2 \times d^2}$ the limit of the sequence (4.5.11) exists and the image of $\Xi(X)$ is isoentropic.

We present the proof of this Proposition at the end of this section. The reasoning is technical and does not bring any additional information to the subject. Meanwhile, let us examine the map Ξ in details. Explicit expression for X_k takes the form of

$$X_1 = \frac{1}{2} \left(X_0^R + X_0^\Gamma \right), \quad (4.5.12)$$

$$X_2 = \frac{1}{4} \left(X_0^{RR} + X_0^{R\Gamma} + X_0^{\Gamma R} + X_0^{\Gamma\Gamma} \right), \quad (4.5.13)$$

$$X_3 = \frac{1}{8} \left(X_0^{RRR} + X_0^{RR\Gamma} + X_0^{\Gamma RR} + X_0^{\Gamma R\Gamma} + X_0^{R\Gamma R} + X_0^{\Gamma\Gamma R} + X_0^{\Gamma R\Gamma} + X_0^{\Gamma\Gamma\Gamma} \right), \quad (4.5.14)$$

$\vdots$

In general,

$$X_k = \frac{1}{2^k} \sum_{\alpha_j \in \{R, \Gamma\}^{\times k}} X_0^{\alpha_1 \alpha_2 \dots \alpha_k}. \quad (4.5.15)$$

For simplicity, we informally rewrite operations X^R and X^Γ in the form of operators $RX = X^R$ and $\Gamma X = X^\Gamma$. Then, (4.5.15) can be expressed as the sum of compositions of R and Γ

$$X_k = \frac{1}{2^k} \left(\sum_{m=1}^{2^k} \prod_{\alpha_{j_m} \in \{R, \Gamma\}^{\times k}} \alpha_{j_m} \right) X_0 = A_k X_0. \quad (4.5.16)$$

Operations R and Γ do not commute in general, however when applied to a given matrix, they can only produce six different combinations¹¹

$$\left\{ \mathbb{I}_{d^2}, R, \Gamma, R\Gamma, \Gamma R, R\Gamma R = \Gamma R\Gamma \right\}. \quad (4.5.17)$$

This is an immediate consequence of definition R and Γ by means of multi-indices, see (4.2.8). All other sequences of R and Γ reproduce one particular element from (4.5.17). Thus, for $k \rightarrow \infty$, one readily sees that A_k in (4.5.16) reduces to

$$A_k \rightarrow \frac{1}{3} \mathbb{I}_{d^2} + \frac{1}{3} R\Gamma + \frac{1}{3} \Gamma R \quad (4.5.18)$$

or, equivalently,

$$A_k \rightarrow \frac{1}{3} R + \frac{1}{3} \Gamma + \frac{1}{6} R\Gamma R + \frac{1}{6} \Gamma R\Gamma = \frac{1}{3} R + \frac{1}{3} \Gamma + \frac{1}{3} R\Gamma R. \quad (4.5.19)$$

This provides the final, compact and elegant form for (4.5.11)

$$\Xi(X) = Y = \frac{1}{3} (X + X^{R\Gamma} + X^{\Gamma R}) \quad \text{or} \quad (4.5.20)$$

$$Y = \frac{1}{3} (X^R + X^\Gamma + X^{R\Gamma R}), \quad (4.5.21)$$

¹¹Recall six different ways of producing unitary matrix out of the splitting of a fourpartite system.

where $X \in \mathbb{R}^{d^2 \times d^2}$. Hence, infinite (albeit quickly convergent) sequence can be replaced by a simple algebraic formula. Using relations (4.5.17) and the fact that R and Γ are involutions, $R^2 = \Gamma^2 = \mathbb{I}_{d^2}$, one can easily infer that $\Xi = \Xi^2$ is a projection onto E -diagonal, which is in full accordance with expectations.

Values of Ξ for random arguments M reflect similar behavior like probing entangling power with generic unitary matrices (CUE) — they concentrate quite close to the corner where T_{36} should be, but without any occasion to reach it. The average value of entropy oscillates around 0.9678, see Figure 4.10. Slightly better results are obtained when one systematically tries to increase the entropy performing a random walk over $\mathbb{R}^{36 \times 36}$ and maximizing the target function $\mathcal{Z}(M) \propto E(M)$. Unfortunately, in no case can it reach a direct vicinity of T_{36} . The best output from Ξ subjected to such procedure is given by a matrix Z for which $E(\Xi(Z)) = 0.9982$. Matrix Z has no apparent structure and cannot be presented in any straightforward analytic form.

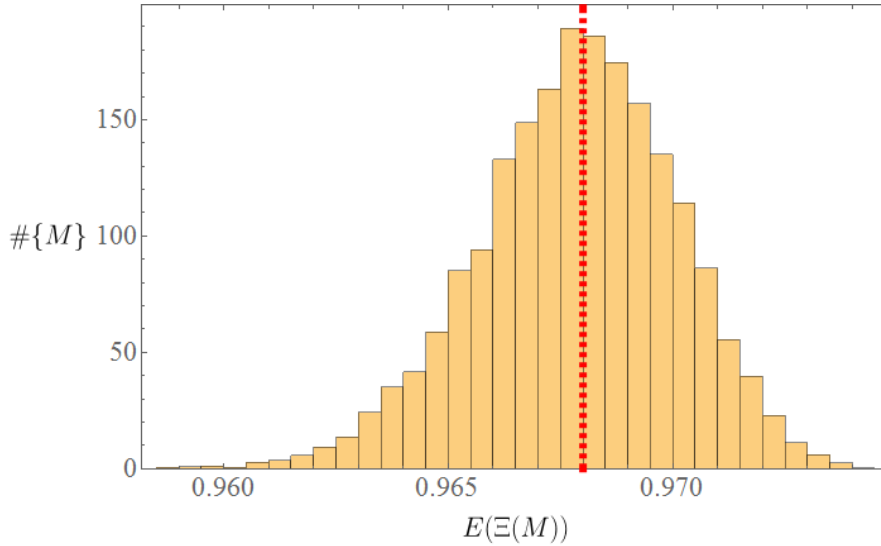


Figure 4.10: Normalized histogram of entropy distribution for 2^{14} samples of matrices of order 36, drawn at random according to real normal distribution $M \sim \mathcal{N}(0, 1)^{\times 36^2}$ and transformed by Ξ onto E -diagonal. Mean value $\langle E(\Xi(M)) \rangle = \langle E(\Xi^R(M)) \rangle = \langle E(\Xi^\Gamma(M)) \rangle$ (red dotted line) concentrates around 0.9678 with standard deviation of 0.0022.

Additional evidence supporting impossibility of reaching the second verge of E -diagonal can be carried out by means of semi-analytical calculations. We would like to have $X \in \mathbb{R}^{36 \times 36}$ such that $\Xi(X) = T_{36}$. As it was mentioned, the maximal value of E (4.5.10) is attained by orthogonal matrices. Hence, for $Y = \Xi(X)$ one should check the condition $YY^T = \mathbb{I}_{36}$, which translates into the system of $d^2(d^2 + 1)/2$ nonlinear equations involving entries of X (or Y). Attempting to solve such system for $d = 2$ yields empty set, which

confirms the lack of four-qubit AME(4, 2) states [112]. In turn, numerical calculations for $d = 3$ provide a solution in compliance with the situation concerning four-qutrit systems [97]. For $d = 4$ and higher everything complicates rapidly and really smart numerical methods are needed to get a credible solution. We were only able to roughly estimate the anticipated fact that (perhaps)

$$\{YY^T = \mathbb{I}_{36}\} = \emptyset. \quad (4.5.22)$$

But this approach still requires more computational power. Needless to say, that any analytical hack is beyond reach for such complicated expressions.

To exemplify the problem of analyzing the map Ξ , let us write down explicit form of image of $\Xi(X)$ for some $X \in \mathbb{R}^{d^2 \times d^2}$. For $d = 2$ it can be presented as

$$\Xi(X) = \frac{1}{3} \begin{bmatrix} 3x_1 & x_2 & x_2 & x_3 \\ x_2 & x_3 & x_3 & 3x_4 \\ 3x_5 & x_6 & x_6 & x_7 \\ x_6 & x_7 & x_7 & 3x_8 \end{bmatrix} \quad (4.5.23)$$

for $x_j \in \mathbb{R}$. This implies the rank $r(\Xi(X)) \leq 3$. Indeed, when assuming that all non-zero singular values are all equal, $\text{svd}(\Xi(X)) = [\{\sigma\}^3, 0]^T$, for some $\sigma \neq 0$, then one has $E(\Xi(X)) = 8/9$, which is immediately confirmed numerically. Here we use alternative (equivalent) formula for entropy (4.2.10), expressed by singular values

$$E(\sigma_1, \dots, \sigma_{d^2}) = \frac{d^2}{d^2 - 1} \left(1 - \frac{\sum_{j=1}^{d^2} \sigma_j^4}{\left(\sum_{j=1}^{d^2} \sigma_j^2\right)^2} \right), \quad (4.5.24)$$

which is directly related to the rank of the matrix.

For $d > 2$, a generic matrix $\Xi(X)$ is no longer singular, i.e. the rank takes its maximal value, $r(\Xi(X)) = d^2$. When trying to recover any pattern for $d = 6$, one finds a great difficulty. Consider $X \in \mathbb{R}^{36 \times 36}$ and its realignments, where only six first, additionally stripped (to save space) rows are shown

$$X = \left[\begin{array}{cccccc|ccc|cccc} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} & b_{11} & b_{12} & \dots & f_{11} & \underline{\mathbf{f_{12}}} & f_{13} & \dots \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & \underline{\mathbf{a_{26}}} & b_{21} & b_{22} & \dots & f_{21} & f_{22} & f_{23} & \dots \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} & b_{31} & b_{32} & \dots & f_{31} & f_{32} & f_{33} & \dots \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & a_{46} & b_{41} & b_{42} & \dots & f_{41} & f_{42} & f_{43} & \dots \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} & a_{56} & b_{51} & b_{52} & \dots & f_{51} & f_{52} & f_{53} & \dots \\ a_{61} & a_{62} & a_{63} & a_{64} & a_{65} & a_{66} & \underline{\mathbf{b_{61}}} & b_{62} & \dots & f_{61} & f_{62} & f_{63} & \dots \end{array} \right], \quad (4.5.25)$$

$$X^{\text{R}\Gamma} = \left[\begin{array}{cccccc|ccc|cccc} a_{11} & b_{11} & c_{11} & d_{11} & e_{11} & f_{11} & a_{21} & b_{21} & \dots & a_{61} & \underline{\mathbf{b_{61}}} & c_{61} & \dots \\ a_{12} & b_{12} & c_{12} & d_{12} & e_{12} & \underline{\mathbf{f_{12}}} & a_{22} & b_{22} & \dots & a_{62} & b_{62} & c_{62} & \dots \\ a_{13} & b_{13} & c_{13} & d_{13} & e_{13} & f_{13} & a_{23} & b_{23} & \dots & a_{63} & b_{63} & c_{63} & \dots \\ a_{14} & b_{14} & c_{14} & d_{14} & e_{14} & f_{14} & a_{24} & b_{24} & \dots & a_{64} & b_{64} & c_{64} & \dots \\ a_{15} & b_{15} & c_{15} & d_{15} & e_{15} & f_{15} & a_{25} & b_{25} & \dots & a_{65} & b_{65} & c_{65} & \dots \\ a_{16} & b_{16} & c_{16} & d_{16} & e_{16} & f_{16} & \underline{\mathbf{a_{26}}} & b_{26} & \dots & a_{66} & b_{66} & c_{66} & \dots \end{array} \right], \quad (4.5.26)$$

$$X^{\Gamma\text{R}} = \left[\begin{array}{cccccc|ccc|cccc} a_{11} & a_{21} & a_{31} & a_{41} & a_{51} & a_{61} & a_{12} & a_{22} & \dots & a_{16} & \underline{\mathbf{a_{26}}} & a_{36} & \dots \\ b_{11} & b_{21} & b_{31} & b_{41} & b_{51} & \underline{\mathbf{b_{61}}} & b_{12} & b_{22} & \dots & b_{16} & b_{26} & b_{36} & \dots \\ c_{11} & c_{21} & c_{31} & c_{41} & c_{51} & c_{61} & c_{12} & c_{22} & \dots & c_{16} & c_{26} & c_{36} & \dots \\ d_{11} & d_{21} & d_{31} & d_{41} & d_{51} & d_{61} & d_{12} & d_{22} & \dots & d_{16} & d_{26} & d_{36} & \dots \\ e_{11} & e_{21} & e_{31} & e_{41} & e_{51} & e_{61} & e_{12} & e_{22} & \dots & e_{16} & e_{26} & e_{36} & \dots \\ f_{11} & f_{21} & f_{31} & f_{41} & f_{51} & f_{61} & \underline{\mathbf{f_{12}}} & f_{22} & \dots & f_{16} & f_{26} & f_{36} & \dots \end{array} \right]. \quad (4.5.27)$$

After summing them up, the explicit form of $Y = \Xi(X)$ for $d = 6$ reads (we intentionally omit the factor $1/3$ and change indexing of y , hence one should not be surprised that indices with value 7 do appear)

$$Y = X + X^{\text{R}\Gamma} + X^{\Gamma\text{R}} = \left[\begin{array}{cccccc|ccc|cccc} \mathbf{a_{11}} & y_{02} & y_{03} & y_{04} & y_{05} & y_{06} & y_{02} & y_{07} & \dots & y_{06} & \underline{\mathbf{y_{27}}} & y_{28} & y_{29} & y_{30} & y_{31} \\ y_{02} & y_{07} & y_{12} & y_{17} & y_{22} & \underline{\mathbf{y_{27}}} & y_{07} & \mathbf{b_{22}} & \dots & y_{11} & y_{36} & y_{49} & y_{50} & y_{51} & y_{52} \\ y_{03} & y_{08} & y_{13} & y_{18} & y_{23} & y_{28} & y_{12} & y_{33} & \dots & y_{16} & y_{40} & y_{56} & y_{63} & y_{64} & y_{65} \\ y_{04} & y_{09} & y_{14} & y_{19} & y_{24} & y_{29} & y_{17} & y_{34} & \dots & y_{21} & y_{44} & y_{59} & y_{68} & y_{71} & y_{72} \\ y_{05} & y_{10} & y_{15} & y_{20} & y_{25} & y_{30} & y_{22} & y_{35} & \dots & y_{26} & y_{48} & y_{62} & y_{70} & y_{74} & y_{75} \\ y_{06} & y_{11} & y_{16} & y_{21} & y_{26} & y_{31} & \underline{\mathbf{y_{27}}} & y_{36} & \dots & y_{31} & y_{52} & y_{65} & y_{72} & y_{75} & \mathbf{f_{66}} \\ \vdots & & & & & & & & & & & & & & \end{array} \right]. \quad (4.5.28)$$

One should recognize the pattern: 6 independent invariants depicted by bold font in (4.5.28), and 70 independent sums of three entries, e.g. $y_{27} = a_{26} + f_{12} + b_{61}$ in underlined-bold font in (4.5.25), (4.5.26) and (4.5.27). After including remaining rows (not drawn above) it gives 36 invariants and $70 \times 6 = 420$ others independent entries in total.

As stated before, a generic matrix Y of such form has full rank. However, it is not so hard to decrease the rank of Y by setting appropriate y_{jk} values. One must be careful to choose columns wisely, since some pairs of columns might have repeated values. Assuming Y has rank 35, 34 or 33, (no need to take lower values, because we can get such matrices using other methods), numerical analysis cannot provide the best theoretical matrix T_{36} in any case. We do not know whether there exists any “magic” combination of columns that make them linearly dependent, so that it recovers the best hypothetical value for a given rank, and in consequence the entropy exceeds, say 0.999. For example, suppose that the rank of Y is 34. Then, the expected maximal value of $E(Y) = \frac{36}{35} \left(1 - \frac{1}{34}\right) = 0.9983$ cannot be reached (so far) by any matrix X , being transformed by Ξ . Currently the best value that can be achieved is 0.9982. It must be stressed, that all these considerations make sense assuming that all singular values are equal or “almost” equal (recall the comment concerning “flatness” of singular value vectors in (4.5.1) and subsequent formulas).

Here comes one final remark. All above attempts when applied to dimensions $d = 3, 4, 5$, and 7 always lead to a solution for $\text{AME}(4, d)$. For $d = 3$, the target is being found almost immediately, while for $d > 3$ the process of searching gradually slows down, but one can always reach the point that resembles T_{d^2} up to an arbitrary precision. This is not the case for the analyzed problem $d = 6(!)$.

We stop here the investigation of potential real AME states. There are many other ideas, which are beyond the scope of this Thesis. None of them brought us any closer to a real AME state of four quhexes. But as usual, several open questions are in order:

1. Is there a real matrix $Y^* \in \mathbb{R}^{36 \times 36}$ such that either $e_p(Y^*) > e_p(W)$ or $E(\Xi(Y^*)) > 0.9982$?
2. Is it possible to calculate the preimage of Ξ to prepare a full analysis of this map?
3. Are there other isoentropic maps, which lead to a higher value of e_p ?

Based on the observations from this and previous sections, let us conclude this part with the following

Conjecture 4. *There is no real state $\text{AME}(4, 6)$.*

Proof of the Proposition 4

Below we present the sketch of proof of the Proposition 4. First consider the case of $d = 2$ and a 4×4 real matrix

$$X_0 = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ * & * & * & * \\ * & * & * & * \end{bmatrix}.$$

Without loss of generality, consider only two first rows of X_0 , since X_0^R and X_0^Γ affect only entire d contiguous blocks of size $d \times d^2$ in X_0 . Write down a few initial elements of $X_{k>0}$ to recognize the general pattern (for brevity, only two first rows are shown), $X_0 = X$,

$$X_1 = \frac{1}{2} \begin{bmatrix} 2x_{11} & x_{12} + x_{13} & x_{13} + x_{21} & x_{14} + x_{23} \\ x_{12} + x_{21} & x_{14} + x_{22} & x_{22} + x_{23} & 2x_{24} \end{bmatrix}, \quad (4.5.29)$$

$$X_2 = \frac{1}{4} \begin{bmatrix} 4x_{11} & 2x_{12} + x_{13} + x_{21} & x_{12} + 2x_{13} + x_{21} & 2x_{14} + x_{22} + x_{23} \\ x_{12} + x_{13} + 2x_{21} & x_{14} + 2x_{22} + x_{23} & x_{14} + 2x_{23} + x_{22} & 4x_{24} \end{bmatrix}, \quad (4.5.30)$$

$\vdots$

Observe that matrix elements $\{x_{11}, x_{12}, \dots, x_{24}\}$ tend to group into three classes: $\{x_{11}, x_{24}\}$, $\{x_{12}, x_{13}, x_{21}\}$ and $\{x_{14}, x_{22}, x_{23}\}$. Group $\{x_{11}, x_{24}\}$ is invariant with respect to Ξ . Group $\{x_{12}, x_{13}, x_{21}\}$ is of the form of $(k_1 x_{12} + k_2 x_{13} + k_3 x_{21})/2^k$ for k^{th} step of Ξ where the (unordered) triplet $\{k_1, k_2, k_3\}$ takes the values $\{\kappa, \kappa, \kappa \pm 1\}$ for κ being the limit of the recursive sequence

$$\begin{cases} \kappa(1) = 1, \\ \kappa(j) = 2\kappa(j-1) - \delta \quad \text{with} \quad \delta = (j \bmod 2) \quad \text{and} \quad j \rightarrow k. \end{cases} \quad (4.5.31)$$

Note that $\kappa(k)$ is not greater than 2^k . A similarly property holds for $\{x_{14}, x_{22}, x_{23}\}$. Hence, as $k \rightarrow \infty$, one has

$$X_k \rightarrow \begin{bmatrix} x_{11} & \xi(x_{12}, x_{13}, x_{21}) & \xi(x_{12}, x_{13}, x_{21}) & \zeta(x_{14}, x_{22}, x_{23}) \\ \xi(x_{12}, x_{13}, x_{21}) & \zeta(x_{14}, x_{22}, x_{23}) & \zeta(x_{14}, x_{22}, x_{23}) & x_{24} \\ * & * & * & * \\ * & * & * & * \end{bmatrix}, \quad (4.5.32)$$

where ξ and ζ are limits of combinations of $\{x_{12}, x_{13}, x_{21}\}$ and $\{x_{14}, x_{22}, x_{23}\}$, respectively. Both limits exist because appropriate sequences are bounded and monotonic. The limit of $\kappa/2^k$ is $1/3$ or $1/6$, depending on the associated group of elements, which is useful in derivation of the simplified version of the map Ξ , see (4.5.18) or (4.5.19).

The matrix $Y = \lim_{k \rightarrow \infty} X_k$ is invariant with respect to reshuffling and partial transpose, $Y = Y^R = Y^\Gamma$. However, last equality (as a result of Ξ) holds only for $d = 2$. Hence, we see that $\text{svd}(Y) = \text{svd}(Y^R) = \text{svd}(Y^\Gamma)$ and additionally, $\text{eig}(Y) = \text{eig}(Y^R) = \text{eig}(Y^\Gamma)$. In the case $d > 2$, one has only $Y \neq Y^R = Y^\Gamma$ but the structure of the matrix Y reflects similar symmetries like for $d = 2$. To end the proof, one exploits the fact that $YY^\dagger = Y^R(Y^R)^\dagger = Y^\Gamma(Y^\Gamma)^\dagger$. Thus $\text{svd}(Y) = \sqrt{\text{eig}(YY^\dagger)} = \text{svd}(Y^R) = \text{svd}(Y^\Gamma)$, and $Y \in \mathcal{J}_{d^2}$ (4.5.9). $\square$

4.6 Unitary Approximation of AME(4, 6)

Let us finally switch to the complex domain. Being the richest structure in our research, it should provide the best results in search of the desired AME state.

4.6.1 Dynamical Map

Recall the Sinkhorn alternating algorithm [47, 48] used extensively in Section 2.3.1 of the second chapter to generate complex Hadamard matrices. The use of such algorithm, in the case when we are dealing with a very similar pattern of “projections” in the form of two consecutive operations, $R \rightarrow R\Gamma \rightarrow R\Gamma R \rightarrow \dots$, is even imposed as a natural method of numerical search for a solution.

Formally, we define a nonlinear dynamical map

$$\mathcal{M} : \mathbb{C}^{d^2 \times d^2} \ni M \mapsto \mathcal{M}(M) \in \mathbb{U}(d^2), \quad (4.6.1)$$

where $\mathcal{M}(M)$ is the limit of the following recursive sequence (provided that it is convergent),

$$\begin{cases} M_0 \in \mathbb{C}^{d^2 \times d^2}, \\ M_{j+1} = \pi(M_j^{R\Gamma}) : j \in \mathbb{N}_0, \end{cases} \quad (4.6.2)$$

where M_0 is any complex starting point (a seed) and π denotes polar decomposition procedure to restrict the mapping to the set of unitary matrices. That is, $\pi(X) = X/\sqrt{X^\dagger X}$ (cf. Section 2.3.1 in Chapter 2). Actually, π projects any matrix $M_{j>1}$ onto a nearest unitary one. Our goal is to find such a seed M_0 that $\mathcal{M}(M_0) = T_{36}$ is a 2-unitary matrix.

Encouraged by the fact that for $d = 3, 4$, and 5 the algorithm converges without much impediments, we hope to recover similar solution for $d = 6$. But the main problem that kept us from solving it for a number of years was the right form of the starting point. Again, a natural choice for a seed seems to be the matrix P , as the one with help of whom, we already obtained most, previously undiscovered, results. But this is not the case anymore. A detailed search of the available space with a special focus on P, Q^*, W and other seemingly distinguished points remained unsuccessful for a bit long, when, eventually, Suhail Ahmad Rather (another crucial contributor to [A4]), worked out that a very particular starting point

should be taken. Surprisingly, it is a permutation P^* , slightly disturbed in the complex direction

$$M_0^* = P^* \exp \left\{ i \frac{\varepsilon}{2} (G + G^T) \right\} \quad : \quad \varepsilon \ll 1, \quad (4.6.3)$$

where $G \in \mathbb{R}^{36 \times 36}$ is an appropriately chosen real random matrix. Counterintuitively, P^* is characterized by a bit worse value of entangling power than P , which makes it closer to CUE, which as we saw in Figure 4.8, is the very strong attractor for any evolution on the (e_p, g_t) -plane.

Hence, an AME state of four subsystems, each of local dimension six, does exist! At least numerically. This is a rather surprising observation in the light of many facts that over the years could prove that such a state is unlikely to be constructed. Having this done finally opened a more systematic way of numerical generation of AME states for $d = 6$. In Figure 4.11 we present three locations of seeds that, together with a proper choice of perturbation G , provide a solution when supplied to $\mathcal{M}$. One particular trajectory of consecutive steps of $\mathcal{M}$ showing quite irregular behavior is drawn in the same figure.

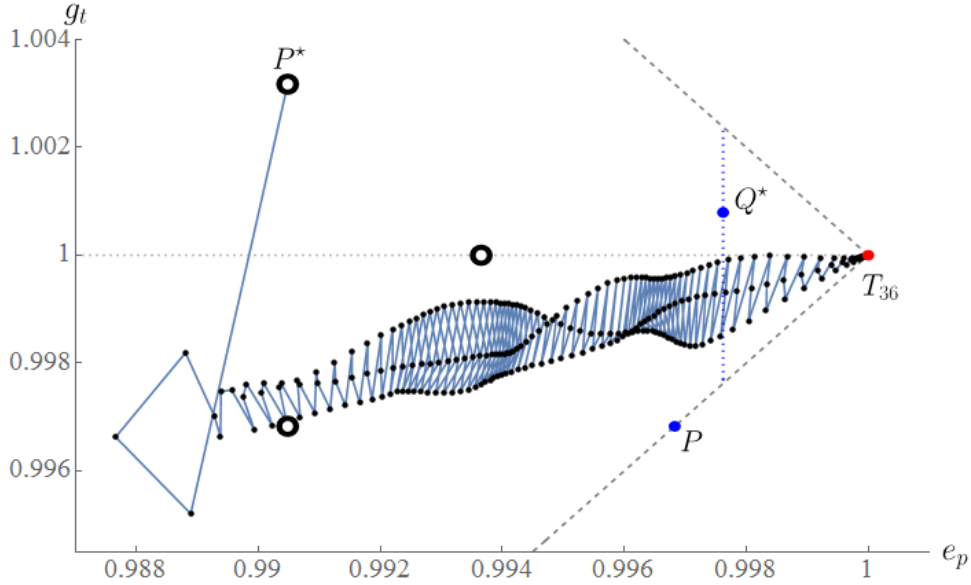


Figure 4.11: Numerical procedure to find a 2-unitary matrix $T_{36} \in \mathbb{U}(36)$, which leads to AME(4, 6). Example of a successful trajectory of $\mathcal{M}$ for a given starting point P^* (seed) in the (e_p, g_t) -plane. For this particular seed, convergence is very fast, and approximately after 200 iterations the desired solution T_{36} (with arbitrary precision) is reached. Other two possible seeds (black rings), which are closest to P are depicted too. Every third iteration follows individual sub-path (small black dots), which might correspond to three operations: $\mathbb{I}$, $\mathbb{R}$ and $\mathbb{I}$. Vertical line crossing Q^* denotes the area of strong attraction for the map $\mathcal{M}$.

It is worth to mention that really few matrices have a property of being a good initial point M_0 , which generates a trajectory converging to 2-unitary matrix T_{36} . This was an annoying obstacle for many researchers who tried to tackle this problem and it led to the common belief that such a construction is not possible. Now, at the time of preparing this Thesis, we know about 20 different seeds from the entire set $\mathbb{P}(36)$ that, mixed with appropriate perturbations G , can serve as the seeds for $\mathcal{M}$. Vast majority of permutation matrices, even those close¹² to P , provided as arguments for $\mathcal{M}$, give $e_p(\mathcal{M}(P_{\text{generic}})) = e_p(Q^*)$, which makes matrices on the vertical line $e_p = e_p(Q^*)$ of the (e_p, g_t) -plane extremely strong attractors for $\mathcal{M}$. No other matrix, beside carefully selected and perturbed permutation, was found so far as an appropriate seed for $\mathcal{M}$. We recommend the Reader to follow [A4] for more interesting features of the map $\mathcal{M}$.

4.6.2 Golden AME(4, 6) State

Representations of AME states, T_{36} , being the output from the map $\mathcal{M}$ (4.6.2) are usually given in the form of 1296 complex numbers arranged without any order into an array of size 36 by 36. Sometimes, algorithm converges to a simpler matrix with only 432 non-zero elements that can be rearranged¹³ into three blocks of size 12×12 ; see left panel in Figure 4.12. Despite the fact that we can set the precision of the output arbitrarily, i.e. $e_p(T_{36}) = 1$ within the limits of machine precision, this cannot in any way be considered a formal proof of Theorem 3. Thus we have to follow a sort of a similar path as in Chapter 2 when we had to work out the analytical formulas for entries of CHM out of their numerical forms.

We already mentioned the invariant operations (4.2.15) that act locally and do not change the value of e_p , while at the same time, they can significantly divert the numerical representation. We modified the optimization procedure, and redesigned it to seek four local rotations $U_6^{(1)}$, $U_6^{(2)}$, $U_6^{(3)}$, and $U_6^{(4)}$ from $\mathbb{U}(6)$, which transform T_{36} in the following way

$$T_{36} \mapsto \left(U_6^{(1)} \otimes U_6^{(2)} \right) T_{36} \left(U_6^{(3)} \otimes U_6^{(4)} \right) \quad (4.6.4)$$

and eventually provided the analytic formulas for elements of T_{36} . This time, the function $\mathcal{Z}$ to be optimized took the form of complicated dependencies between certain groups of elements of T_{36} . The general idea was to make as many different 6×2 blocks of T_{36} (see Figure 4.12) mutually orthogonal as possible, and eventually turn some of them into

¹²We say that a permutation matrix P' is close to P , if an arbitrarily small number (say 1 or 2) of transpositions of rows (or columns) is required to obtain P from P' .

¹³Be cautious at this stage! The state AME(4, 6) is very sensitive to the tiniest value changes and element shuffling, including highly devastating process of permutations of rows or columns. Such rearrangements should be considered only as temporary visual representation. The only operations, presented in this Thesis, that preserve the AME property are: R, Γ , global transpose T and local unitary rotations from $\mathbb{U}(6) \otimes \mathbb{U}(6)$.

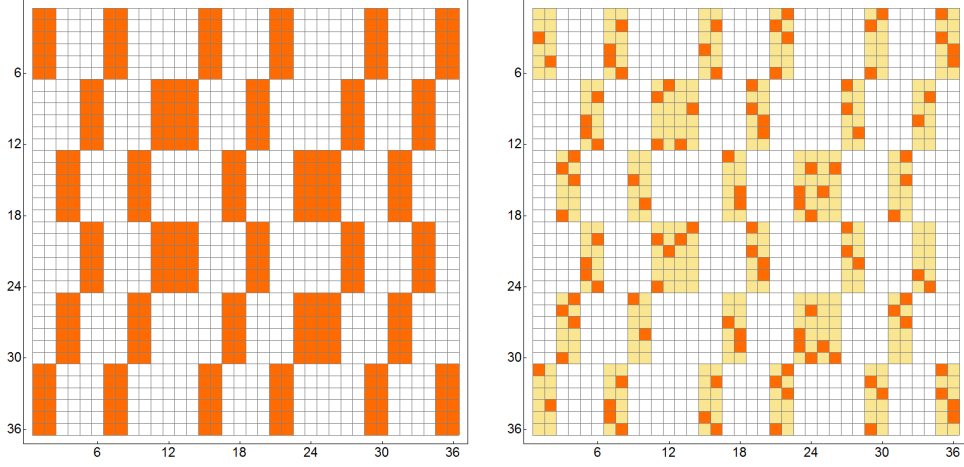


Figure 4.12: Left panel represents 432 nonvanishing elements of a numerical representation of T_{36} . On the right panel we observe as local unitary rotations (4.6.4) transform T_{36} into analytical form where only 112 entries (dark squares) are nontrivial, while the rest eventually vanish (light squares). Such a sparse and scattered form partially explains the fact that we were unable to find a complex representation of T_{36} in Section 4.4.3.

a standard (canonical) basis $|j\rangle \in \mathbb{C}^6$ to simplify the entire structure. Several dozens of different forms of the target functions $\mathcal{Z}$'s, combining different areas of T_{36} , applied one after another, have led in the end to such a representation that allowed us to guess some analytical values and the rest was easily calculated from unitarity constraints. As partially expected, during the optimization procedure, it turned out that only 112 entries remained with non-zero values, which makes the final analytic form of T_{36} quite sparse, see right panel in Figure 4.12.

Let us present the AME(4, 6) state in its full grandness. There are many ways of presenting such state: as a matrix, a vector, a (perfect) tensor, or as a pair of OQLS. Each of these methods has its advantages and disadvantages, however, the main problem that emerges in all cases is always the same — its size. Drawing a 36×36 matrix on any surface is always a challenge. Here, using algebraic tricks, we have prepared a special version, which should consume a decent amount of space and simultaneously to reveal some peculiar properties.

Put $\omega = \exp\{i\pi/10\}$ and¹⁴

$$a = \frac{1}{\sqrt{2}}, \quad b = \frac{a}{\omega + \omega^*} = \frac{1}{\sqrt{5 + \sqrt{5}}}, \quad c = \frac{a}{\omega^3 + (\omega^*)^3} = \frac{1}{2\sqrt{5}}\sqrt{5 + \sqrt{5}}, \quad (4.6.5)$$

and note that $a^2 = 1/2 = b^2 + c^2$. This implies unitarity of the following blocks ($\bullet = 0$):

¹⁴Asterisk $*$ in b and c denotes complex conjugate.

Now, the absolutely maximally entangled state of four quhexes can be concisely represented by a unitary matrix A of order 36,

$$A = (B_1 \oplus B_2 \oplus B_3) P^T, \quad (4.6.9)$$

with help of the inverse of P (4.4.1) to recover desired structure. With some effort one can confirm that

$$E(A) = E(A^R) = E(A^T) = e_p(A) = g_t(A) = 1 \quad (4.6.10)$$

which implicitly ends the proof of Theorem 3. $\square$

The state $\text{AME}(4, 6)$ can be written as

$$|\text{AME}(4, 6)\rangle = \frac{1}{6} \sum_{j=1}^6 \sum_{k=1}^6 |j\rangle \otimes |k\rangle \otimes (A|j\rangle \otimes |k\rangle) \in \mathcal{H}_6^{\otimes 4}. \quad (4.6.11)$$

Blocks B_1 , B_2 and B_3 are presented on the left panel of Figure 4.13. Such representation can be further visually simplified with help of two permutations, $\tilde{A} = P_r A P_c$, which is depicted on the right panel of Figure 4.13, while the two permutations P_r and P_c are shown in Figure 4.14.

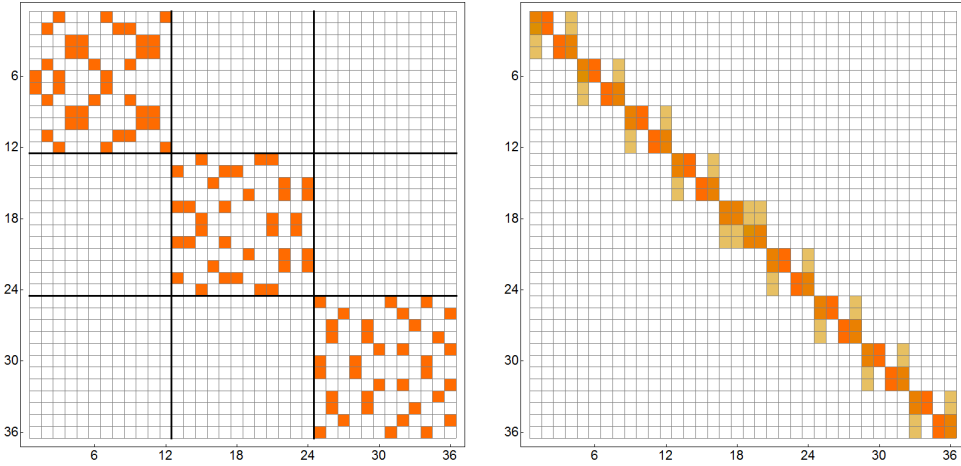


Figure 4.13: Left panel shows non-zero elements of AP in the form of a block-diagonal structure $3 \times (12 \times 12)$ with additional internal vertical symmetries. On the right panel we see absolute values of entries of $\tilde{A} = P_r A P_c$, forming another extra-ordinary symmetric block-diagonal $9 \times (4 \times 4)$ matrix. This pattern implies that 36 officers of Euler can be divided into 9 groups of 4 entangled officers. Matrices P_r and P_c are shown in Figure 4.14.

Intriguing relation between the building blocks of A in the form of the golden ratio, $c/b = \varphi$, should explain the proposition to call A the *golden AME state*. We are not going

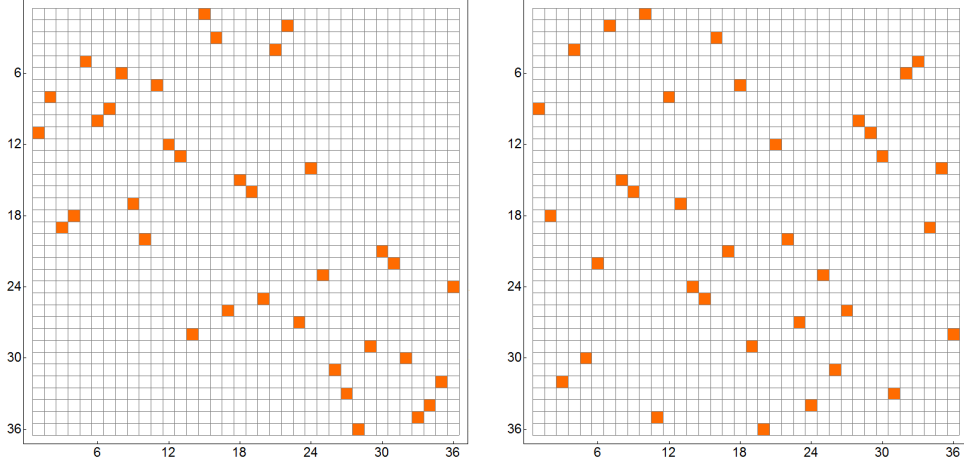


Figure 4.14: Permutation matrices P_r (left panel) and P_c (right panel) that bring A to a block-diagonal $9 \times (4 \times 4)$ form $\tilde{A} = P_r A P_c$.

to describe the internal structure of A , which has been studied in details by Adam Burchardt in his thesis¹⁵ — the third major contributor to [A4] — who, armed with the optimizing software, written by the Author, was patiently recovering the analytical form of the matrix T_{36} turning it finally to a representation equivalent to the matrix A .

4.7 Summary

In this chapter we have proven the unexpected existence of the absolutely maximally entangled state of four quhexes. Many groups tried to solve this problem over the years and almost everybody (including us!) shared the belief that such states do not exist. Unclear difficulties related to the relatively small number 6 are common to other objects of this size: MUB in $\mathbb{C}^6$ and CHM (incomplete classification of $\mathbb{H}(6)$). But we believe that our result will bring us closer to a full understanding of this puzzling property.

With analytic construction of $\text{AME}(4, 6)$ we solved several equivalent problems. They are: existence of a 2-unitary matrix of size 36 with maximal entangling power, existence of a perfect tensor with four indices (each running from 1 to 6), existence of pure quantum error correcting code $((4, 1, 3))_6$, and existence of a pair of orthogonal quantum Latin squares of order 6. Note that this last result disproves Conjecture 1 from [131]. However, despite putting many efforts we failed to resolve the problem of finding an orthogonal counterpart of the complex state $\text{AME}(4, 6)$.

¹⁵In preparation.

Further open questions include:

1. Is it possible to redefine the notion of the defect (Chapters 2 and 3) so that it is applicable to AME? If so, would it be possible to stem a family of inequivalent states from the discovered state $\text{AME}(4, 6)$ or to prove that this is an isolated point, up to local unitary rotations?
2. What about different seeds that can be supplied to the numerical procedure (4.6.1)? Is there any systematic method of constructing $\text{AME}(4, 6)$ state(s)? Or, how to systematize and simplify the sequence of optimizations that led us after many laborious months to the analytic form of A given in Eq. (4.6.9)? How to make it applicable for other allowed dimensions N and d ?
3. Is the existence of the state $\text{AME}(4, 6)$ somehow related to the MUB problem in $\mathbb{C}^6$?
4. What is the most optimal way to represent a quantum circuit corresponding to the AME state four quhexes?



In the next, and the last chapter of this Thesis, we are going to continue research concerning the concept of quantum entanglement from the perspective of the foundations of quantum mechanics and Bell's theorem.

Chapter 5

Excess of a Matrix and Bell Inequalities

Chapter based on [A5].

The preprint [A5] on which this chapter is based, is rooted on ideas of collaborators thus, in contrary to all previous chapters, this short one has mostly descriptive character. As promised in the introduction, we restrict the work merely to original contributions of the Author, which in this case were mainly focused on numerical research to confirm analytical predictions and scrutinous studying the literature in search for a similar approach (to exclude the possibility of accidental reuse of the same concept). One particular example that we found interesting will be used in Section 5.4.1 to illustrate Bell inequalities with quantum advantage induced by a special class of matrices. The presence of this chapter is justified from the perspective of the integrity and general appearance of the Thesis. Its content refers to many raised topics and neatly concludes some problems mentioned previously. For example, we will recall MUB, (real) Hadamard, unitary, and circulant matrices for the last time and examine them for completely different purposes.

We already signalized the “problems” with quantum mechanics (QM) in Chapter 3 during the investigation a possibility of introduction of free parameters in the set of Kochen–Specker vectors (which, anyway, turned out to be isolated structures). QM undoubtedly reached a status of a successful theory as it provides many explanations of physical processes at the microscopic level, and opens a great variety of possible applications unavailable in the classical approach. However, many questions concerning the foundations and self-consistency of QM that arose almost immediately with its advent, still remain unanswered. Needless to say, we refer to the famous EPR Gedankenexperiment [132] as the origin of the long-standing disputes [133] regarding the interpretation of quantum mechanics.

In short, it all began with the problem of allegedly immediate transfer of information between spatially separated objects. Consider two entangled¹ photons traveling in two opposite directions. It turns out that when we measure the polarization of one photon, no matter how much they are apart, the polarization of the other one is always strongly correlated to the first one. Famous authors of [132] questioned this fact, as it openly contradicts the rules of the special theory of relativity (STR), and they postulated the notion of *local realism*, according to which objects can interact only within their neighborhood. So, if there is a correlation between distant objects (events), invoked by some interaction (measurement), then local realism implies existence of some *local hidden variables* (LHV), which carry additional information. In consequence, something is wrong with the Copenhagen interpretation of quantum mechanics, because the associated wave function apparently does not provide full description of the system. In general, QM seems incomplete.

In 1964 John Bell [134] suggested a solution to the paradox of LHV in a form of a simple arithmetic relation, which can be verified experimentally. If we assume the local realism and hidden variables model then one can conclude a set of inequalities, *Bell inequalities* (BI), which must hold in the classical case. In the simplest formulation, it involves linear combinations of correlations of measurement outputs that, when combined into a single number, it must not exceed a particular bound. However, in the quantum world one observes violation of these inequalities, that is the quantum value of BI is strictly bigger than its classical counterpart. Hence, local realism is not a proper assumption to explain physics and separated objects can “communicate” over long distances. Formally this means that measurement affects entire physical system, no matter how huge, not only its parts. It is worth to note that the concept of Bell does not refute the existence of hidden variables, it only demonstrates that correlations at the quantum level cannot be derived from deterministic and LHV models. Moreover, there is no conflict with STR (no “spooky action at a distance”) because, despite the fact we observe strong correlations, they appear in a purely random fashion and as such they cannot transfer any information. Simply speaking, quantum mechanics describes *nonlocal* Universe.

First experiments confirming violation of Bell inequalities were performed in the early eighties of the last century [135]. Since then several practical modifications at the very high level were proposed in order to avoid possible loopholes, for example [136], and also many different classes (families of) Bell inequalities were investigated for testing QM and its possible generalizations [137]. There are several technological applications of quantum nonlocality, which significantly outperforms similar classical tasks. This includes: device-independent protocols [138, 139], communication [140, 141], quantum key distribution and general quantum cryptography [142, 143, 144, 145], testing quantumness [146, 147], and random numbers generation [148, 149, 150].

¹Now we know that entanglement is crucial to understand this paradox.

The main open question in quantum nonlocality concerns the existence of quantum advantage in comparison with the classical (LHV) scenario for a given Bell inequality. Seeking a solution to this problem, one must find the biggest possible value of the Bell inequality in LHV² theories and in the quantum case. But there is at least one crucial impediment: finding the LHV value of a given BI is NP-hard problem [151] — the complexity grows with the number of measurement settings m and the number of outcomes q . Even the case of two-party scenarios for relatively small values of m and q remains unsolved [152, 153]. Thus, it would be of great importance to introduce a method of estimating the LHV value in a simple way. In order to address this task, we propose a connection between the LHV value of bipartite BI and mathematical notion of the excess of a given matrix. We replace the problem of finding LHV value associated with a bipartite BI with equivalent problem of finding matrices with the maximal excess (a number associated with matrix, to be defined in Section 5.3). Having this, we are able to characterize infinite number of families of bipartite BI describing a variety of scenarios. Since the properties of the excess have been studied in mathematics for decades, we can have many results “out of the box” and apply them in the field of quantum nonlocality.

5.1 Initial Observation

Consider a special case of BI — the celebrated CHSH inequality [154]. The associated Bell operator reads

$$\mathbb{B} = A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1, \quad (5.1.1)$$

where A_j and B_k are observables represented by Hermitian operators having ∓ 1 eigenvalues. To calculate the classical value $\mathcal{C}$ of $\mathbb{B}$, we replace the operators with variables $a_j, b_k \in \{-1, 1\}$, so

$$\mathcal{C} = \max_{a_j, b_k = \mp 1} \{ +a_0b_0 + a_0b_1 + a_1b_0 - a_1b_1 \} = 2. \quad (5.1.2)$$

Note that (5.1.2) can be equivalently expressed in the form of

$$\mathcal{C} = \max_{a_j, b_k = \mp 1} \left\{ \sum \begin{bmatrix} +a_0b_0 & +a_0b_1 \\ +a_1b_0 & -a_1b_1 \end{bmatrix} \right\} = \sum \begin{bmatrix} + & + \\ + & - \end{bmatrix} = 2, \quad (5.1.3)$$

where $\sum$ denotes the sum of all matrix elements, and the last equality assumes such relating of values of a_j and b_k that their products are equal to unity. One readily recognizes that the matrix under the operator $\sum$ is just a real Hadamard matrix H_2 of order 2. This observation suggests that instead of looking for a maximum in (5.1.2), we can find a matrix with certain properties to obtain (or estimate) the classical value of the Bell inequality immediately. We will formalize this procedure in the next sections.

²Following the convention from the preprint, in place of the “classical scenario” we should use the abbreviation LHV.

5.2 Bell Inequalities

We assume a scenario of two parties (A and B), m measurement settings (for each party) and q outcomes for each measurement. Let $P(a, b|x, y)$ denote a joint probability distribution of outcomes $a, b \in \{0, \dots, q-1\}$ for A and B , given measurement settings $x, y \in \{0, \dots, m-1\}$, respectively. The value of $P(a, b|x, y)$ can be obtained from a sequence of identically prepared quantum states subjected to a measurement process. As shown in [155], single correlation $P(a, b|x, y)$ does not provide a contradiction with LHV models, but a linear combination of $P(a, b|x, y)$, which appears in a Bell inequality, might attain values that are out of reach in any LHV models [134]. Any Bell inequality can be defined in the following way [152]

$$\sum_{x,y=0}^{m-1} \sum_{a,b=0}^{q-1} S_{xy}^{ab} P(a, b|x, y) \leq \mathcal{C}, \quad (5.2.1)$$

where S_{xy}^{ab} is a real-valued function and $\mathcal{C}$ is the maximal possible value that can be achieved in a local deterministic theory³. We call $\mathcal{C}$ a *classical value* or a *local hidden variable* (LHV) value.

Furthermore, the *quantum value* $\mathcal{Q}$ denotes the maximal possible value of the left-hand side of (5.2.1), when optimization takes place over all possible joint probability distributions allowed in quantum realm, provided that two parties A and B do not communicate (to exclude the possibility of “instantaneous” transfer of information). As described in Chapter 3, quantum probabilities take the form $P(a, b|x, y) = \text{Tr}((\Pi_a^x \otimes \Pi_b^y) \rho_{AB})$, where $\{\Pi_a^x\}$ and $\{\Pi_b^y\}$ represent POVM⁴, and ρ_{AB} is a bipartite quantum state shared by parties A and B . Using discrete Fourier transform, we can write probabilities in (5.2.1) as expectation values of correlators [156]

$$P(a, b|x, y) = \frac{1}{\sqrt{q}} \sum_{s,t=0}^{q-1} \omega^{as+bt} \langle A_x^s \otimes B_y^t \rangle, \quad (5.2.2)$$

where $\omega = \exp\{\frac{2\pi i}{q}\}$. Here, A_x^s (similarly for B_y^t) denotes the s^{th} power of observable A_x related to A . Both observables are chosen to have q eigenvalues, associated with q different roots of unity. Now Eq. (5.2.1) can be expressed as

$$\sum_{x,y=0}^{m-1} \sum_{s,t=0}^{q-1} M_{ms+x,mt+y} \langle A_x^s \otimes B_y^t \rangle \leq \mathcal{C}, \quad (5.2.3)$$

³This means that there is statistical independence between the results of A and B expressed as $P(a, b|x, y) = P(a|x)P(b|y)$, and the deterministic character of the outcomes, say $P(a|x), P(b|y) \in \{0, 1\}$, for every pair of measurement settings $x, y \in \{0, \dots, m-1\}$ and outcomes $a, b \in \{0, \dots, q-1\}$, respectively for A and B .

⁴Positive-operator valued measure.

where M is a square matrix of size $N = qm$ with elements defined as

$$M_{ms+x,mt+y} = \frac{1}{\sqrt{q}} \sum_{a,b=0}^{q-1} \omega^{sa+tb} S_{xy}^{ab}, \quad (5.2.4)$$

for every $0 \leq s, t < q$ and $0 \leq x, y < m$.

We must assert that the left-hand side of (5.2.3) is real for any $q \geq 2$ and $m \geq 2$. Provided that both A_x^s and B_y^t are unitary and imposing the following symmetry constraint

$$M_{m[q-s]_q+x, m[q-t]_q+y} = M_{ms+x, mt+y}^*, \quad (5.2.5)$$

for $0 \leq s, t < q$ and $0 \leq x, y < m$, with $*$ representing the complex conjugate and $[x]_q$ denoting x modulo q , the left-hand side of (5.2.3) indeed remains real for any value of $q \geq 2$. In particular, if $q = 2$ (two outcome scenario) we have $[2-s]_2 = s$, for any $s \in \{0, 1\}$. This means, that condition (5.2.5) guarantees that M is a real matrix for any value of m . The constant prefactor $\frac{1}{\sqrt{q}}$ in (5.2.4) is sometimes absorbed into S_{xy}^{ab} , but to remain consistent with some mathematical results presented in [A5], one must explicitly adjust its value.

We distinguish a special class of matrices M corresponding to Bell inequalities (5.2.3) without marginal terms, i.e. those for which $s = 0$ or $t = 0$. In other words, we take into account only such scenarios, where there is a correlation between parties A and B ($s > 0$ and $t > 0$), so that we discard zeroth powers of observables A_x and B_y . We call such a matrix M *correlation matrix*. Condition (5.2.5) implies that the marginal terms are always located at the first m rows and first m columns of matrix M . What remains is the nontrivial *core* of order $n = (q-1)m$. Note the similarity to the core of the complex Hadamard matrix, defined in the context of its dephased (normalized) form — see Chapter 2.

For further convenience, in the real case ($q = 2$), $M \in \mathbb{R}^{2m \times 2m}$, as matrix M fulfills condition (5.2.5) trivially, we can remove all rows and columns from M corresponding to the marginal terms, and consider only its core. Again, let us take for example the case of CHSH. Corresponding matrix M of order $N = qm = 2 \cdot 2 = 4$ has the following form

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} \begin{array}{c|c|c|c} t_{00}^{00} & t_{01}^{00} & t_{00}^{01} & t_{01}^{01} \\ \hline t_{10}^{00} & t_{11}^{00} & t_{10}^{01} & t_{11}^{01} \\ \hline t_{00}^{10} & t_{01}^{10} & \mathbf{t_{00}^{11}} & \mathbf{t_{01}^{11}} \\ \hline t_{10}^{10} & t_{11}^{10} & \mathbf{t_{10}^{11}} & \mathbf{t_{11}^{11}} \end{array} \end{bmatrix}, \quad (5.2.6)$$

where every matrix element, denoted by t_{xy}^{st} is an appropriate sum of products of powers of ω and S_{xy}^{st} — here all are real. Therefore, only the core (of order $n = 2$) entries marked in bold contribute to (5.1.1), whereas all other elements represent irrelevant numbers contributing to marginal terms. In two examples that will be presented later, we will consider only the core of real matrices M , hence the actual dimension $N = qm$ will be reduced to $n = (q-1)m$, which for $q = 2$ simplifies to $n = m$.

In a general case, the matrix $M \in \mathbb{C}^{qm \times qm}$ obeying (5.2.5) has a form of a tensor structure with q^2 blocks each of size $m \times m$. For even values of $q = 2, 4, 6, \dots$ it contains four $\mathbb{R}$ -valued blocks of size $m \times m$ located at $M_{0,0}$, $M_{0,qm/2}$, $M_{qm/2,0}$, and $M_{qm/2,qm/2}$ (matrix is indexed from 0 to $N - 1 = qm - 1$). After removing marginal terms, the remaining $(q - 1)^2$ blocks reveal a central symmetric structure with respect to the $\mathbb{R}$ -valued block at $(qm/2, qm/2)$ which now occupies the central place in M . For example, for $(q, m) = (6, 2)$ we have

$$M = \left[\begin{array}{cc|cc|cc|cc|cc|cc} \mathbb{R} & \mathbb{R} & t_{00}^{01} & t_{01}^{01} & t_{00}^{02} & t_{01}^{02} & \mathbb{R} & \mathbb{R} & t_{00}^{04} & t_{01}^{04} & t_{00}^{05} & t_{01}^{05} \\ \mathbb{R} & \mathbb{R} & t_{10}^{01} & t_{11}^{01} & t_{10}^{02} & t_{11}^{02} & \mathbb{R} & \mathbb{R} & t_{10}^{04} & t_{11}^{04} & t_{10}^{05} & t_{11}^{05} \\ \hline t_{00}^{10} & t_{01}^{10} & t_{00}^{11} & t_{01}^{11} & t_{00}^{12} & t_{01}^{12} & t_{00}^{13} & t_{01}^{13} & t_{00}^{14} & t_{01}^{14} & t_{00}^{15} & t_{01}^{15} \\ t_{10}^{10} & t_{11}^{10} & t_{10}^{11} & t_{11}^{11} & t_{10}^{12} & t_{11}^{12} & t_{10}^{13} & t_{11}^{13} & t_{10}^{14} & t_{11}^{14} & t_{10}^{15} & t_{11}^{15} \\ \hline t_{00}^{20} & t_{01}^{20} & t_{00}^{21} & t_{01}^{21} & t_{00}^{22} & t_{01}^{22} & t_{00}^{23} & t_{01}^{23} & t_{00}^{24} & t_{01}^{24} & t_{00}^{25} & t_{01}^{25} \\ t_{10}^{20} & t_{11}^{20} & t_{10}^{21} & t_{11}^{21} & t_{10}^{22} & t_{11}^{22} & t_{10}^{23} & t_{11}^{23} & t_{10}^{24} & t_{11}^{24} & t_{10}^{25} & t_{11}^{25} \\ \hline \mathbb{R} & \mathbb{R} & t_{00}^{31} & t_{01}^{31} & t_{00}^{32} & t_{01}^{32} & \mathbb{R} & \mathbb{R} & t_{00}^{34} & t_{01}^{34} & t_{00}^{35} & t_{01}^{35} \\ \mathbb{R} & \mathbb{R} & t_{10}^{31} & t_{11}^{31} & t_{10}^{32} & t_{11}^{32} & \mathbb{R} & \mathbb{R} & t_{10}^{34} & t_{11}^{34} & t_{10}^{35} & t_{11}^{35} \\ \hline t_{00}^{40} & t_{01}^{40} & t_{00}^{41} & t_{01}^{41} & t_{00}^{42} & t_{01}^{42} & t_{00}^{43} & t_{01}^{43} & t_{00}^{44} & t_{01}^{44} & t_{00}^{45} & t_{01}^{45} \\ t_{10}^{40} & t_{11}^{40} & t_{10}^{41} & t_{11}^{41} & t_{10}^{42} & t_{11}^{42} & t_{10}^{43} & t_{11}^{43} & t_{10}^{44} & t_{11}^{44} & t_{10}^{45} & t_{11}^{45} \\ \hline t_{00}^{50} & t_{01}^{50} & t_{00}^{51} & t_{01}^{51} & t_{00}^{52} & t_{01}^{52} & t_{00}^{53} & t_{01}^{53} & t_{00}^{54} & t_{01}^{54} & t_{00}^{55} & t_{01}^{55} \\ t_{10}^{50} & t_{11}^{50} & t_{10}^{51} & t_{11}^{51} & t_{10}^{52} & t_{11}^{52} & t_{10}^{53} & t_{11}^{53} & t_{10}^{54} & t_{11}^{54} & t_{10}^{55} & t_{11}^{55} \end{array} \right] \cdot \quad (5.2.7)$$

marginals

After removing the marginal terms, and if we temporarily change the reference point and assume that the central block is located at the relative position $(0, 0)$, then all other blocks denoted by $b_{j,k}$ indexed by j and k are in relation $b_{j,k} = b_{-j,-k}^*$. Therefore, the core of the matrix in (5.2.7) of order $n = (q - 1)m$ can be symbolically represented as

$$\text{core}(M) = \left[\begin{array}{c|c|c|c|c} b_{-2,2} & b_{-1,2} & b_{0,2} & b_{1,2} & b_{2,2} \\ \hline b_{-2,1} & b_{-1,1} & b_{0,1} & b_{1,1} & b_{2,1} \\ \hline b_{-2,0} & b_{-1,0} & b_{0,0} & b_{1,0} & b_{2,0} \\ \hline b_{-2,-1} & b_{-1,-1} & b_{0,-1} & b_{1,-1} & b_{2,-1} \\ \hline b_{-2,-2} & b_{-1,-2} & b_{0,-2} & b_{1,-2} & b_{2,-2} \end{array} \right] \quad (5.2.8)$$

$$= \left[\begin{array}{c|c|c|c|c} b_{-2,2} & b_{-1,2} & b_{0,2} & b_{1,2} & b_{2,2} \\ \hline b_{-2,1} & b_{-1,1} & b_{0,1} & b_{1,1} & b_{2,1} \\ \hline b_{-2,0} & b_{-1,0} & b_{0,0} & b_{-1,0}^* & b_{-2,0}^* \\ \hline b_{-2,1}^* & b_{-1,1}^* & b_{0,1}^* & b_{-1,1}^* & b_{-2,1}^* \\ \hline b_{-2,2}^* & b_{-1,2}^* & b_{0,2}^* & b_{-1,2}^* & b_{-2,2}^* \end{array} \right], \quad (5.2.9)$$

where each $b_{j,k}$ for $(j, k) \in [-2, 2] \times [-2, 2]$ is a $m \times m = 2 \times 2$ block with one particular representative $b_{0,0}$ with all four real entries, being a center of symmetry for relation (5.2.5).

For odd values of $q \in \{3, 5, 7, \dots\}$ matrix M has only one $\mathbb{R}$ -valued block of size $m \times m$ located at the upper-leftmost corner of M (at $(0, 0)$), which lies exactly at the marginal region outside the core of M . Remaining blocks exhibit the same central symmetry according to condition (5.2.5).

5.3 Excess of a Matrix Σ

Recall the notion of (real) Hadamard matrix H , which is a square $N \times N$ matrix H with entries ± 1 and pairwise orthogonal columns. We will use the symbol $\text{BH}(N, 2)$ (introduced in Chapter 2) to indicate the set of real Hadamard matrices of size N .

Given a real Hadamard matrix H , the *excess* of H , denoted by $\Sigma(H)$, is defined as the difference between the number of the positive and negative entries of H [157]. For any dimension N , for which real Hadamard matrix exists, we consider the *maximal excess*, maximized over all Hadamard matrices of this order. It is known [158] that the maximal excess obeys the following bounds

$$\frac{N^2}{2^N} \binom{N}{N/2} \leq \max_{H \in \text{BH}(N, 2)} \Sigma(H) \leq N\sqrt{N}. \quad (5.3.1)$$

It can be shown [158] that for a Hadamard matrix H , the upper bound (5.3.1) is attained iff the sum of all elements in each row of H yields the same value. We call such matrix a *regular* or *constant row sum* Hadamard matrix. It is easy to prove that such Hadamard matrices with a constant row sum exist only in squared dimensions $N = k^2$ for some $k > 1$. One can equivalently define the excess of a $H \in \text{BH}(N, 2)$ as the sum of all entries of H ,

$$\Sigma(H) = \sum_{j,k=0}^{N-1} H_{jk} \quad : \quad H \in \text{BH}(N, 2). \quad (5.3.2)$$

In analogy to (2.1.1), we say that two matrices M_1 and M_2 of order N obeying (5.2.5) are *q-equivalent* if there exist two diagonal unitary matrices D_1 and D_2 whose $(ms+x)^{\text{th}}$ diagonal entries are s^{th} power of a q^{th} root of the unity $\omega = \exp\{\frac{2\pi i}{q}\}$, for every $s \in \{0, \dots, q-1\}$ and $x \in \{0, \dots, m-1\}$, such that $M_1 = D_1 M_2 D_2$. We write $M_1 \simeq_q M_2$. For example, the explicit form of the diagonal matrix for $q = 3$ and $m = 2$ reads

$$D_j = \text{diag}[1, 1, \omega, \omega, \omega^2, \omega^2] = \text{diag}[1, \omega, \omega^2] \otimes \text{diag}[1, 1] \quad : \quad j \in \{1, 2\}, \quad (5.3.3)$$

where the emphasized tensor structure corresponds to the internal form of matrix M_j , $j \in \{1, 2\}$. Observe that two q -equivalent matrices M_1 and M_2 induce the same Bell inequality (5.2.3) up to a relabeling of the outcomes for A and B . We do not include permutations (permutation matrices) in the definition of q -equivalence, because the excess does not depend on the order of summands — entries of a matrix. Such permutation matrices would correspond to a relabeling of measurement settings, which are irrelevant in this scenario.

Finally, we extend the definition of the standard maximal excess over any matrices beyond Hadamard ones. Given $q \geq 2$, we say that matrix M of order $N = qm$ has *maximal excess* with respect to q -equivalence, if

$$\Sigma(M) = \max \left\{ \Sigma(\widetilde{M}) : \widetilde{M} \simeq_q M \right\}. \quad (5.3.4)$$

Note that for any matrix M related to a Bell inequality (5.2.3), there exists a relabeling of outputs that produces another inequality, related to a matrix $\widetilde{M}$, with maximal excess. If M is a real Hadamard matrix and $q = 2$, above definition coincides with the standard maximal excess for Hadamard matrices.

5.4 Excess of a Matrix and Classical Value of Bell Inequality

There is a one-to-one link between the notion of excess of a matrix applied to a certain class of matrices and the classical (LHV) value of Bell inequality (BI).

Proposition 5. *If M is a matrix of dimension $N = qm$ having maximal excess with respect to q -equivalence then, the LHV value of Bell inequality (5.2.3) induced by M , having q outcomes for each setting, equals to the excess of M , i.e. $\mathcal{C}(M) = \Sigma(M)$. Conversely, for any Bell inequality (5.2.3) induced by M , there exists a q -equivalent matrix $\widetilde{M}$ satisfying (5.2.5) such that $\mathcal{C}(\widetilde{M}) = \Sigma(\widetilde{M})$.*

This can be explained by noting that given a BI (5.2.3) induced by M , there exist two diagonal matrices D_1, D_2 composed of q^{th} roots of the unity such that a q -equivalent matrix $\widetilde{M} = D_1 M D_2$ provides an optimal LHV strategy if all outputs for A and B are equal to $+1$. Changing $M \rightarrow \widetilde{M}$ in (5.2.3) imposes a relabeling of outputs of the measurement devices for A and B . Hence, the LHV value of BI can be calculated as the excess of $\widetilde{M}$. Clearly, for matrices $\widetilde{M}$ with this property we have $\Sigma(\widetilde{M}) = \Sigma(M) = \mathcal{C}$.

There are infinitely many known cases for which the maximum excess of Hadamard matrix can be calculated exactly [159, 160, 161, 162, 163]. Also another classes of matrices having maximal excess have been deeply examined: complex Hadamard matrices [164], orthogonal designs [165], and tensors [166]. This last class of objects provides a way of extension the area of research over multipartite systems. This implies the importance of Proposition 5, because we can simply extend the set of BI for which the LHV value is known. Supported by many mathematical results related to maximal excess, we can construct families of matrices that allow us to achieve the LHV value of Bell inequalities representing scenarios with arbitrary (unbounded) number of measurement settings per party. Moreover, we can do this without applying any optimization procedure. This connection might inspire researchers to develop more efficient methods to find the LHV value for other classes of Bell inequalities. In the paper [A5] we summarize several known mathematical methods to

calculate maximal excess and we show how to construct some families of correlation matrices M of order $n = (q - 1)m$, which provide classical value of BI for bipartite scenarios with unbounded number of measurement settings. Meanwhile, let us present a sequence of additional observations⁵ concerning the classical value of a matrix M .

Proposition 6. *If a matrix M of order $N = qm$ achieves the maximal excess with respect to q -equivalence, then*

$$\mathcal{C}(M) \leq Nr(M), \quad (5.4.1)$$

where $r(M)$ is the numerical radius of the matrix M , defined as

$$r(M) = \max \{ |\langle \psi | M | \psi \rangle| : |\psi\rangle \in \mathcal{H}_N, \langle \psi | \psi \rangle = 1 \}. \quad (5.4.2)$$

Note that the above upper bound for the classical value $\mathcal{C}$ is more restrictive than the upper bound for the quantum value [167, 168], which is presented below.

Observation 7. *The quantum value of a BI induced by M satisfies*

$$\mathcal{Q}(M) \leq N\sigma(M), \quad (5.4.3)$$

where $\sigma(M)$ denotes the maximal singular value of M .

In general, full classification of matrices M that saturate the above bounds is an open problem. Let us provide here a new upper bound for bipartite scenario, for which we can fully characterize its tightness.

Proposition 8. *If the excess of a matrix M of order $N = qm$ is maximal with respect to q -equivalence, then*

$$\mathcal{C}(M) \leq \sqrt{N} \nu(M), \quad (5.4.4)$$

where $\nu(M) = \sqrt{\sum_{j=0}^{N-1} \left| \sum_{k=0}^{N-1} M_{jk} \right|^2}$. Upper bound (5.4.4) is saturated iff the matrix M has a constant row sum equal to s and then $\mathcal{C}(M) = Ns$.

The constant row sum value s presented above is always a positive real number provided that M has maximal excess and obeys the symmetry condition in (5.2.5).

From Observation 7 and Proposition 8 we conclude that for a unitary matrix M with constant row sum having maximal excess, related BI does not have quantum advantage, $\mathcal{C}(M) = \mathcal{Q}(M) = N$. For example, the three inequivalent not normalized Hadamard matrices of size $N = 16$ [169] with constant row sum, define three inequivalent bipartite BI with $m = 16$ measurement settings and $q = 2$ outcomes. In this case, we have $\mathcal{C}(M) = \mathcal{Q}(M) = 64 = 16\sqrt{16}$.

⁵Proofs of all observations and corollaries are provided in Appendix of [A5].

Non-unitary matrices with constant row sum can imply a correlation BI having quantum advantage. For instance, a circulant matrix M with $\text{core}(M) = \text{circ}[0, -1, 1]$ of order three,⁶ satisfies the relation $\mathcal{C}(M) = 4 < 3\sqrt{3} = \mathcal{Q}(M)$. The quantum value $\mathcal{Q}(M)$ is achieved with assistance of the following measurement settings A_j and B_j (corresponding to parties A and B , respectively) of the form of $X_j D X_j^\dagger$, for

$$X_j = \begin{bmatrix} \cos \varphi_j & \sin \varphi_j \\ -\sin \varphi_j & \cos \varphi_j \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad (5.4.5)$$

and $\varphi_j = 0, \frac{2}{3}\pi, \frac{1}{3}\pi$ for A_0, A_1, A_2 and $\varphi_j = \frac{1}{4}\pi, \frac{7}{12}\pi, \frac{11}{12}\pi$ for B_0, B_1, B_2 , respectively.

5.4.1 Family of Bell Inequalities with Quantum Advantage

Further investigations led us to a more extended example and a tentative statement concerning the existence of infinite family of constant row sum matrices with a quantum advantage. We did not actually prove that this statement holds in every dimension, but detailed numerical analysis suggests this might be true.⁷

Consider n two-dimensional measurement operators $A_j = X(\alpha_j)$ and $B_j = X(\beta_j)$, where

$$X(\varphi_j) = \begin{bmatrix} \cos \frac{2\pi\varphi_j}{n} & -\sin \frac{2\pi\varphi_j}{n} \\ -\sin \frac{2\pi\varphi_j}{n} & -\cos \frac{2\pi\varphi_j}{n} \end{bmatrix}, \quad (5.4.6)$$

so that each operator depends on a single phase φ_j , which corresponds to $n\alpha_j/2\pi$ or $n\beta_j/2\pi$ for $j \in \{1, 2, \dots, n\}$. For further brevity, we collectively write all the phases of A_j and B_j as vectors

$$\alpha^{(n)} = (\alpha_1, \alpha_2, \dots, \alpha_n) \quad \text{and} \quad \beta^{(n)} = (\beta_1, \beta_2, \dots, \beta_n), \quad (5.4.7)$$

where $\alpha_j, \beta_j \in \mathbb{R}$. Hence, we have the following scenario: $m = n$ measurement settings and $q = 2$ outputs per party.

Define a family of non-unitary real circulant matrices M_n of size n taking the form of

$$M_n = \text{circ}[c_1, c_2, \dots, c_n] = \text{circ}\left[\underbrace{-1, \dots, -1}_{\lfloor n/2 \rfloor}, \underbrace{1, \dots, 1}_{\lceil n/2 \rceil}\right] \in \mathbb{R}^{n \times n}. \quad (5.4.8)$$

⁶Note that in this case $q = 2$ and $m = 3$, and the dimension $N = 6$ is reduced to $n = 3$, which is the size of the core of M . See Section 5.2.

⁷In this example we also consider the core of a real matrix but we do not write it explicitly.

For example:

$$M_3 = \text{circ}[-1, 1, 1] \quad (5.4.9)$$

$$M_4 = \text{circ}[-1, -1, 1, 1] \quad (5.4.10)$$

$$M_5 = \text{circ}[-1, -1, 1, 1, 1] \quad (5.4.11)$$

$$M_6 = \text{circ}[-1, -1, -1, 1, 1, 1] \quad (5.4.12)$$

$\vdots$

By definition a circulant matrix, M_n has a constant row sum. Using a well known formula for eigenvalues λ_j of a circulant matrix [170],

$$\lambda_j = \sum_{k=1}^n c_k \omega_n^{(j-1)k} \quad : \quad \omega_N = \exp\left\{\frac{2\pi i}{n}\right\}, \quad j \in \{1, \dots, n\}, \quad (5.4.13)$$

we can calculate the maximal singular value for even orders of M_n ,

$$\sigma_n = |\lambda_n| = \frac{2}{\sin \frac{\pi}{n}}, \quad (5.4.14)$$

from which we get the limit

$$\lim_{n \rightarrow \infty} \frac{\sigma_n(M_n)}{n} = \frac{2}{\pi}. \quad (5.4.15)$$

Similar calculations can be done for odd values of n .

From numerical simulations, we obtain the following sequence of classical values of the Bell operator induced by a matrix M_n of order n ,

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...
$\mathcal{C}(M_n)$	5	8	13	20	25	32	41	52	61	72	85	100	113	128	145	...

(5.4.16)

One can see that numbers $\mathcal{C}(M_n)$ form a logical pattern⁸. To see this better, we shall divide the sequence $\mathcal{C}(M_n)$ onto two subsequences for odd and even values of the parameter n ,

$$\mathcal{A} = (5, 13, 25, 41, 61, 85, 113, 145, \dots), \quad (5.4.17)$$

$$\mathcal{B} = (8, 20, 32, 52, 72, 100, 128, \dots). \quad (5.4.18)$$

Such splitting is additionally justified by the natural asymmetric form of M_n depending on the parity of dimension n , or equivalently, the number of -1 's in M_n . See Eqs. (5.4.9)–(5.4.12). Clearly, $\mathcal{A}$ is a progression with increasing difference $\delta = 8 + 4k$ with $k \in \mathbb{N}_0$.

⁸Actually, this is only an observation and we cannot present yet a formal proof of this fact.

As for the second subsequence $\mathcal{B}$, one observes that every two consecutive numbers differ by 12, 12, 20, 20, 28, 28, ..., $12 + 8k, \dots$ for $k \in \mathbb{N}_0$, respectively. One can split it further onto other two subsequences to see that they can be expressed as $\mathcal{B}_{\text{odd}} = (8, 32, 72, 128, \dots)$ so $\mathcal{B}_{\text{odd}}(k) = 8k^2$ and $\mathcal{B}_{\text{even}} = (20, 52, 100, \dots)$ which implies $\mathcal{B}_{\text{even}}(k) = 4\mathcal{A}(k)$.

To calculate the quantum value $\mathcal{Q}$ of the Bell inequality induced by the matrix M_n , we should optimize the quantity $\langle \psi | \mathbb{B} | \psi \rangle$, where $\mathbb{B}$ represents the left-hand side of (5.2.3) and we choose the particular form of the state $|\psi\rangle = |\psi(\gamma)\rangle = [\cos \gamma, 0, 0, \sin \gamma]^T$, which depends on a single parameter γ . Clearly, the Bell operator depends on phases $\alpha^{(n)}$ and $\beta^{(n)}$, which were introduced in (5.4.7). It turns out that we can find such (optimal) values of $\alpha^{(n)}$, $\beta^{(n)}$, and γ , that $\langle \psi | \mathbb{B} | \psi \rangle = n\sigma_n$. Moreover, we can simplify the problem fixing $\gamma = \pi/4$ and $\alpha^{(n)} = (0, 1, \dots, n-1)$ since, observing results from many simulations, such configuration provided exceptionally elegant outputs for any dimension $3 \leq n \leq 14$.

Two classes of results presented in Table 5.1 can be distinguished. For $n = 3 + 4k$ or $n = 4 + 4k$ and $k \in \mathbb{N}_0$, we see that phases for B_j always take half-integer values (highlighted rows), while for complementary values of n , there are only pure integers for both $\alpha^{(n)}$ and $\beta^{(n)}$. Perfect monotonic alignment in each numerical simulation allows us to present the following compact formulas:

$$\begin{cases} \alpha^{(n)} &= (0, 1, 2, \dots, n-1) \\ \beta^{(n)} &= (2k+3, (2k+3) \oplus_{2n} 2, (2k+3) \oplus_{2n} 4, \dots)^{\frac{1}{2}} \end{cases} \quad (5.4.19)$$

for $n = 3 + 4k$ or $n = 4 + 4k$ and $k \in \mathbb{N}_0$ where $\oplus_{2n}$ denotes addition modulo $2n$. Similarly,

$$\begin{cases} \alpha^{(n)} &= (0, 1, 2, \dots, n-1) \\ \beta^{(n)} &= (2+k, (2+k) \oplus_n 1, (2+k) \oplus_n 2, \dots) \end{cases} \quad (5.4.20)$$

for $k \in \mathbb{N}_0$ and remaining values of n .

We claim that for any $n \geq 3$, matrices M_n (5.4.8) give rise to a Bell inequality, such that it provides a quantum advantage as the quantum value reads

$$\mathcal{C}(M_n) < \mathcal{Q}(M_n) = n\sigma_n. \quad (5.4.21)$$

This fact can be easily inferred from the following observation. In the bipartite scenario with $m = n$ and $q = 2$, the Bell operator $\mathbb{B}$ takes a very simple form depending only on a single real parameter c ,

$$\mathbb{B} = \mathbb{B}(c) = \begin{bmatrix} c & 0 & 0 & c \\ 0 & -c & c & 0 \\ 0 & c & -c & 0 \\ c & 0 & 0 & c \end{bmatrix} \quad (5.4.22)$$

where

$$c = \sum_{j,k=1}^n [M_n]_{jk} \cos \frac{2\pi}{n} \alpha_j \cos \frac{2\pi}{n} \beta_k. \quad (5.4.23)$$

$\alpha^{(3)} =$	0	1	2											
$2\beta^{(3)} =$	3	5	1											
$\alpha^{(4)} =$	0	1	2	3										
$2\beta^{(4)} =$	3	5	7	1										
$\alpha^{(5)} =$	0	1	2	3	4									
$b^{(5)} =$	2	3	4	0	1									
$\alpha^{(6)} =$	0	1	2	3	4	5								
$\beta^{(6)} =$	2	3	4	5	0	1								
$\alpha^{(7)} =$	0	1	2	3	4	5	6							
$2\beta^{(7)} =$	5	7	9	11	13	1	3							
$\alpha^{(8)} =$	0	1	2	3	4	5	6	7						
$2\beta^{(8)} =$	5	7	9	11	13	15	1	3						
$\alpha^{(9)} =$	0	1	2	3	4	5	6	7	8					
$\beta^{(9)} =$	3	4	5	6	7	8	0	1	2					
$\alpha^{(10)} =$	0	1	2	3	4	5	6	7	8	9				
$b^{(10)} =$	3	4	5	6	7	8	9	0	1	2				
$\alpha^{(11)} =$	0	1	2	3	4	5	6	7	8	9	10			
$2\beta^{(11)} =$	7	9	11	13	15	17	19	21	1	3	5			
$\alpha^{(12)} =$	0	1	2	3	4	5	6	7	8	9	10	11		
$2\beta^{(12)} =$	7	9	11	13	15	17	19	21	23	1	3	5		
$\alpha^{(13)} =$	0	1	2	3	4	5	6	7	8	9	10	11	12	
$\beta^{(13)} =$	4	5	6	7	8	9	10	11	12	0	1	2	3	
$\alpha^{(14)} =$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$\beta^{(14)} =$	4	5	6	7	8	9	10	11	12	13	0	1	2	3
$\vdots$	$\vdots$													

Table 5.1: Optimal vectors of phases $\alpha^{(n)}$ and $\beta^{(n)}$ introduced in (5.4.7) for measurement operators for dimension $3 \leq n \leq 14$. Each row should be understood as components of vectors $\alpha^{(n)}$ or $\beta^{(n)}$. Phases for B_k in every second pair of dimensions, $(3, 4), (7, 8), (11, 12), \dots$, are characterized by half-integer values, in contrary to other values of n .

Simple, although technical proof of this fact requires elementary trigonometry and, provided that M_n is of the form of (5.4.8), one can show that for even values of n , the maximal singular value of $\mathbb{B}$ reads

$$\sigma_n(\mathbb{B}) = 2c = \frac{2}{\sin \frac{\pi}{n}}. \quad (5.4.24)$$

Comparing this with classical sequences (5.4.17) and (5.4.18), we observe strict inequality $\mathcal{C} < \mathcal{Q}$ for every $n \geq 3$. Similar reasoning can be done for odd values of n .

All of this, together with (5.4.15), allows us to estimate the asymptotic behavior of the quantum advantage Q ,

$$Q = \lim_{n=2k+1 \rightarrow \infty} \frac{\mathcal{Q}(M_n)}{\mathcal{A}(M_n)} = \frac{2}{\pi} \lim_{k \rightarrow \infty} \frac{(2k+1)^2}{2k(k+1)+1} = \quad (5.4.25)$$

$$\lim_{n=4k \rightarrow \infty} \frac{\mathcal{Q}(M_n)}{\mathcal{B}(M_n)} = \frac{2}{\pi} \lim_{k \rightarrow \infty} \frac{(4k)^2}{8k^2} = \quad (5.4.26)$$

$$\lim_{n \rightarrow \infty} \frac{\mathcal{Q}(M_n)}{\mathcal{C}(M_n)} = \frac{4}{\pi}. \quad (5.4.27)$$

Numerical value of the ratio $Q = \mathcal{Q}/\mathcal{C}$ can be compared with the maximal bound obtained in the CHSH scenario

$$\frac{4}{\pi} \approx 1.2732 < 1.4142 = \sqrt{2} = \frac{\mathcal{Q}_{\text{CHSH}}}{\mathcal{C}_{\text{CHSH}}}. \quad (5.4.28)$$

5.5 Excess and Mutually Unbiased Bases

In this section, we show that the classical value of the Bell inequality induced by a correlation matrix M with a core equal to a Hadamard matrix is closely related to the notion of MUB (mutually unbiased bases) [14]. We start with the following observation based on Theorem 3 in [158] and [171] (where a method of reducing the number of dichotomic variables involved in calculations of the maximal excess of a Hadamard matrix was introduced).

Observation 9. *The LHV value of a BI with two outcomes ∓ 1 induced by a correlation matrix M with a core, written $\text{core}(M)$, of order $n = (q-1)m$ is given by*

$$\mathcal{C}(M) = \max_{x \in \{-1,1\}^n} \|\text{core}(M)|x\rangle\|_1, \quad (5.5.1)$$

where $\left\| \sum_{j=0}^{n-1} v_j |j\rangle \right\|_1 = \sum_{j=0}^{n-1} |v_j|$ is the taxicab norm of a vector.

From this observation we infer

Proposition 10. *Let M be a correlation matrix with a core being a Hadamard matrix of order $n = (q-1)m$. If there exists a vector $|x\rangle$ with entries ± 1 , which is unbiased to the rows of M , then the classical value $\mathcal{C}(M) = n\sqrt{n}$. Conversely, if $\mathcal{C}(M) = n\sqrt{n}$, then there exists a vector $|x\rangle$ unbiased to the rows of M .*

In particular, if M is a correlation matrix, $\text{core}(M)$ has constant row sum, and a vector $|x\rangle \in \mathbb{R}^n$ has all its entries equal to unity, then $\mathcal{C}(M) = \sqrt{n}\nu(M)$, in accordance with Observation 8.

Corollary 10.1. *If $\forall k : n \neq k^2$ (not a square number that corresponds to the size of core of M), then any pair of real mutually unbiased bases in $\mathbb{R}^n$ is strongly unextendible (there is no single vector unbiased to the pair of bases [57, 172, 173]).*

Corollary 10.2. *Suppose, there exist three real MUB $\{\mathbb{I}, H_1, H_2\}$ in $\mathbb{R}^n$. Then both H_1 and H_2 are 2-equivalent to a Hadamard matrix with a constant row sum.*

Corollary 10.3. *For any pair of real MUB $\{\mathbb{I}, H\}$, with H being a Hadamard matrix with a constant row sum, there exists at least a single vector mutually unbiased with respect to both bases.*

One readily notices that in dimensions $n = 2, 8$, and 12 , which are not squared numbers, no triplets of real MUB exist. There are no Hadamard matrices of this size with a constant row sum either.

5.6 Tight Bell Inequalities

Tight Bell inequalities are defined as the facets (hyperplanes that completely characterize correlations compatible with a LHV model) of the LHV polytope [174]. In the quantum case, the space of correlations for a two-party scenario with m measurement settings and q outcomes, is defined by all real vectors $v \in \mathbb{R}^{q^2 m^2}$ with entries of the form of $\langle A_x^s \otimes B_y^t \rangle$, for $x, y \in \{0, \dots, m-1\}$ and $s, t \in \{0, \dots, q-1\}$. Unitary operators A_x and B_y have eigenvalues being q^{th} roots of the unity. Taking into consideration the no-signaling conditions [175], correlations are further restricted to a subspace of size $d = (q-1)^2 m^2$. Facets of the LHV polytope have dimension of $d-1$, so for $q = 2$ (two outcomes scenario) there are $d-1 = m^2-1$ linearly independent vectors (v), associated to LHV strategies $\langle A_x^s \otimes B_y^t \rangle = a_x^s b_y^t$, with $a_x, b_y = \pm 1$. We examined tightness of correlation BI induced by Hadamard matrices $H = \text{core}(M)$ of orders $2 \leq n \leq 20$ (for some M), and the numerical results, summarized in Table 5.2, suggest the following conjecture:

Conjecture 5. *A Hadamard matrix of order $n = (q-1)m$ induces a tight correlation Bell inequality with $m = n$ settings and $q = 2$, iff it is not 2-equivalent to matrix with a constant row sum.*

# settings (m)	# vertices	# affine independent vertices	tightness
2	4	3	tight
4^{crs}	4	3	non-tight
8	64	63	tight*
12	2640	143	tight*
$16_{[1]}^{\text{crs}}$	896	105	non-tight
$16_{[2]}^{\text{crs}}$	192	81	non-tight
$16_{[3]}^{\text{crs}}$	64	45	non-tight
$16_{[4]}$	21504	255	tight*
$16_{[5]}$	21504	255	tight*
$20_{[1]}$	20064	399	tight*
$20_{[2]}$	20064	399	tight*
$20_{[3]}$	20064	399	tight*

Table 5.2: Study of tightness for bipartite correlation Bell inequalities with m measurement settings and $q = 2$ outcomes of the form of $\left\langle \sum_{x,y=0}^{n-1} H_{xy} A_x \otimes B_y \right\rangle \leq \mathcal{C}(H)$, where H denotes a Hadamard matrix of order $n = (q - 1)m = m$. Note that $H = \text{core}(M)$ and M has dimension $N = qm$. For a tight Bell inequality, the number of affine independent vertices must be equal to $N^2 - 1$. Symbol $^{\text{crs}}$ tells that a matrix H has a constant row sum and subscripts in brackets enumerate inequivalent Hadamard matrices. All cases denoted by $*$ are believed to be new.

5.7 Summary

In this chapter, we have established a relation between the classical (LHV) value of bipartite Bell inequalities and the mathematical notion of the excess of a matrix. This one-to-one connection can be used to obtain the LHV value for infinitely many families of Bell inequalities with an arbitrarily high number of measurement settings per party without solving any optimization problem. We derived upper bounds for the LHV value for a bipartite BI, which are stronger than the upper bounds for the quantum value.

Furthermore, we described a relation of some classes of BI to mutually unbiased bases. Full set of optimal LHV strategies of BI, which are induced by a Hadamard matrix H coincide with the entire set of vectors, which are mutually unbiased to the pair $\{\mathbb{I}, H\}$.

Studying LHV strategies can identify tight BI. We showed seven tight BI for the scenario with two outcomes and a number of measurement settings between 8 and 20. This led us to a conjecture that every Hadamard matrix that is not equivalent to the one with a constant row sum, induces a tight Bell inequality. To the best of our knowledge, presented observations and results are new and should provide new insights in the field of quantum nonlocality.



Chapter 6

Concluding Remarks

Quantum entanglement, no matter how accessibly expressed, either by means of matrices with a particularly designed structure or in any other mathematical language, still remains a mysterious and elusive (although quite practical) property of the quantum world. On the other hand, the analytical classification of certain classes of unitary matrices is far beyond the reach of current theoretical and numerical tools due to their enormous complexity. The objective of this Thesis was twofold. Firstly, we wanted to broaden our knowledge of the analytical treatment of a set of unitary matrices and their significant subsets. Secondly, we accepted the challenge of improving the description of particular aspects of quantum entanglement, especially those concerning correlations among multipartite physical systems associated with states, the existence of which was questioned by many experts. We are convinced that in both cases, the goal was achieved.

Let us recapitulate the main results presented in this work. In the second chapter (2), we started with the problem of classification of complex Hadamard matrices (CHM) which is a long-term project, launched in 2006 [4]. The first unresolved case in the set of CHM concerns the six-dimensional case and all consecutive dimensions are pending for a complete description too. We provided two new important analytical representatives of eight- and nine-dimensional CHM. Former one being a nontrivial one-parameter nonaffine family of inequivalent matrices, while the latter one is isolated. Based on the particularly interesting form of the nine-dimensional solution, we proposed a general construction in any dimension $N \geq 8$. This observation allowed us to combine the notion of Latin squares (or circulant structures) with the set of CHM. Supported by the numerical evidence, we drew two conjectures concerning the existence of infinitely many isolated CHM. We also resolved some other minor issues regarding the analytical description of CHM in low dimensions.

In Chapter 3, we developed the idea of the restricted defect of a Hermitian unitary matrix, which can be considered as an extension of the notion of the defect of an arbitrary unitary matrix, extensively used in work on classification of CHM. While the standard uni-

tary defect can serve as a simple criterion to distinguish isolated and potentially non-isolated (CHM) matrices, its Hermitian counterpart is applicable to a subset of Hermitian unitary matrices having constant diagonal. Having this, we were able to identify the internal structure of quantum measurement operators in terms of the possibility of introduction of free parameters. We checked several classes of quantum measurements with prescribed symmetry: mutually unbiased bases, equiangular tight frames and symmetric informationally complete positive-operator valued measures. It turned out that in several cases such objects reflect isolated character, but it is also possible to find examples for which the restricted defect does not vanish so that they might be extended to multidimensional orbits of solutions labeled by free parameters. Relatively large robustness of defect with respect to numerical inaccuracies made it possible to calculate the value of the defect for a wide range of complex Hadamard matrices. These results contribute to our understanding of the complicated structure of the set of complex Hadamard matrices for intermediate dimensions $8 \leq N \leq 16$.

The fourth chapter (4) opens the second part of the Thesis where we directly focused on (multipartite) quantum entanglement. After many attempts, checking numerous possibilities, drawing a dozen of (often false) conjectures, we arrived with an affirmative answer to the long-standing question concerning the existence of absolutely maximally entangled states of four parties, each having six degrees of freedom. In view of many facts pointing out that such a state apparently does not exist, this unexpected result solved several problems at once. This includes the existence of 2-unitary matrices of size 36 for which very particular realignment of entries does not affect unitarity (these matrices maximize entangling power), perfect tensors of four indices, a pair of orthogonal quantum Latin squares of size six (a quantum counterpart of the classical Euler problem of 36 officers), and special classes of pure quantum error correcting codes designed for the alphabet consisting of six letters. Several other interesting properties of such state were investigated.

In the last chapter (5), we briefly reviewed the concept of combining two seemingly distinct areas: excess of a matrix and bipartite Bell inequalities. Excess of a real matrix defined as the sum of all its elements provides a way for introducing new families of the Bell inequalities. This correspondence allows us to calculate the classical value for infinitely many Bell inequalities without applying any optimizations. In some cases we obtained stronger results than these offered by currently known bounds. Relation to mutually unbiased bases was described and most likely new results regarding tight Bell inequalities were presented.

We hope that these modest results and propositions will find some place in the contemporary theoretical and experimental fields of physics and will be used to develop even more interesting theories in the vividly developing branches of quantum information, quantum combinatorics, quantum computation and nonlocality.

Lastly, we would like to emphasize something. When looking at the mentioned at the beginning two lists with “the hottest” open problems [2, 3] one recognizes a common thing. Almost every problem can be expressed in a simple language which does not require extraordinary expert knowledge to comprehend the overall idea. Some people say that all low hanging fruits have already been harvested. That might not necessarily be true. Anyway, we believe, that even nowadays there is a niche that permits us to use some simplest methods in order to accomplish long-awaited or just new results in many areas. We witnessed this phenomenon mainly in Chapter 4 but also in Chapters 2 and 5, where by means of relatively easy tools or observations we arrived at moderately important conclusions.

All numerical problems presented in this Thesis were calculated using: *GNU Octave*, version 5.2.0, *Matlab 9.1.0.441655 (R2016b)* and occasionally *Mathematica 12.0.0.0*, which was mostly used to generate pictures and to confirm outputs from the previous software. Most *.m scripts and *.nb notebooks are publicly available on the GitHub platform [58].

6.1 Open Questions and Future Work

Many problems presented in this Thesis are far from being complete. At the end of three first chapters we listed a sequence of open questions associated with a given topic. Let us recall the most important problems that we plan to continue to work on.

First of all, the paper concerning isolated complex Hadamard matrices [A2], which is the scaffolding of the second chapter, is currently being prepared in parallel with the Thesis. It should be released by the end of 2021 independently with another paper being a continuation of exploring mathematical aspects of the excess of non-Hadamard matrices, which is in some sense a mathematical supplement to [A5] containing physical aspects of excess. Preprints [A4] and [A5] are waiting for the referees’ decision.

Remaining problems, which are going to be considered in the next stage, focus mainly on further development of the ideas described in the second part of the Thesis. They are listed below:

- Does real $\text{AME}(4, 6)$ state exist? There are many clues that such state does not exist. But, a year and half ago we had twice as many clues that a complex $\text{AME}(4, 6)$ state should not exist and we were ready to publish a paper with very convincing arguments supporting such a statement!
- It is roughly possible to introduce strictly analytical and deterministic algorithm to construct an $\text{AME}(4, 6)$ state, however at this stage it is very cumbersome and suffers from many unclear statements. How to fix and simplify this process and, moreover, how to adapt it for other dimensions, for which other AME states are expected to be found?

- Complex $\text{AME}(4, 6)$ state can be realized experimentally or simulated on the quantum computer (suppose there exists such advanced simulator). What is the most optimal decomposition of this state onto smaller/universal gates?
- Do four or more mutually unbiased bases exist in dimension six? What about a complete set of seven MUB in $\mathbb{C}^6$? Does the existence of $\text{AME}(4, 6)$, related to dimension six, help us to make any progress in this direction?
- What about new classes of Bell inequalities that can be constructed by the method we proposed in Chapter 5? Will application of the excess of a matrix to quantum nonlocality reveal some previously unknown properties of Bell inequalities?

Bibliography

- [1] R. Horodecki, “Quantum Information”, *A. Phys. Pol. A* **139**(3) (2021).
- [2] P. Horodecki, Ł. Rudnicki, K. Życzkowski, “Five Open Problems in Quantum Information”, *arXiv:2002.03233* (2020).
- [3] S. Aaronson, Shtetl-Optimized, <https://www.scottaaronson.com/blog/?p=112> (access: 2021/10/06).
- [4] W. Tadej, K. Życzkowski, “A Concise Guide to Complex Hadamard Matrices”, *Open Syst. Inf. Dyn.* **13**(02), 133–177 (2006).
- [5] W. Bruzda, W. Tadej, K. Życzkowski, Catalogue of Complex Hadamard Matrices, <https://chaos.if.uj.edu.pl/~karol/hadamard/>, (access: 2021/10/08).
- [6] A.T. Butson, “Generalized Hadamard Matrices”, *Proc. Amer. Math. Soc.* **13**, 894–898 (1962).
- [7] A.T. Butson, “Relations Among Generalized Hadamard Matrices, Relative Difference Sets, and Maximal Length Linear Recurring Sequences”, *Can. J. Math.* **15**, 42–48 (1963).
- [8] J.S. Hadamard, “Résolution d’une question relative aux déterminants”, *Bull. Sci. Math.* **17**, 240–246, (1893).
- [9] O. Chterental, D.Ž. Đoković, “On Orthostochastic, Unistochastic and Qustochastic Matrices”, *Linear Alg. Appl.* **428**(4), 1178–1201 (2008).
- [10] B.W. Brock, “Hermitian Congruence and the Existence and Completion of Generalized Hadamard Matrices”, *J. Comb. Theory A* **49**(2), 233–261 (1988).
- [11] J.L. Hayden, “Generalized Hadamard Matrices”, *Des. Codes Crypt.* **12**, 69–73 (1997).
- [12] I.D. Ivanović, “Geometrical Description of Quantal State Determination”, *J. Phys A: Math. Gen.* **14**(12), 3241–3245 (1981).

- [13] W.K. Wootters, B.D. Fields, “Optimal State-Determination by Mutually Unbiased Measurements”, *Ann. Phys.* **191**(2), 363–381 (1989).
- [14] T. Durt, B.-G. Englert, I. Bengtsson, K. Życzkowski, “On Mutually Unbiased Bases”, *Int. J. Quantum Inf.* **8**(4), 535–640 (2010).
- [15] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej, K. Życzkowski, “Mutually Unbiased Bases and Hadamards of Order Six”, *J. Math. Phys.* **48**(5), 052106 (2007).
- [16] R.F. Werner, “All Teleportation and Dense Coding Scheme”, *J. Phys. A: Math. Gen.* **34**(35), 7081–7094 (2001).
- [17] E. Knill, “Group Representations, Error Bases and Quantum Codes”, *LANL report LAUR-96-2807* (1996).
- [18] A.V. Geramita, J. Seberry, “Orthogonal Designs: Hadamard Matrices and Quadratic Forms”, M. Dekker Press – Taylor & Francis US (1979).
- [19] A. Klappenecker, M. Rötteler, “Constructions of Mutually Unbiased Bases”, *Lect. Notes Comput. Sci.* **2948**, 137–144 (2004).
- [20] B. Musto, J. Vicary, “Quantum Latin Squares and Unitary Error Bases”, *Quant. Inf. Comput.* **16**(15–16), 1318–1332 (2016).
- [21] T. Banica, “Complex Hadamard Matrices and Applications”, *hal-02317067v2* (2021).
- [22] J. Williamson, “Hadamard’s Determinant Theorem and the Sum of Four Squares”, *Duke Math. J.* **11**(1), 65–81 (1944).
- [23] P. Diţă, “Some Results on the Parametrization of Complex Hadamard Matrices”, *J. Phys. A: Math. Gen.* **37**, 5355–5374 (2004).
- [24] M. Matolcsi, J. Réffy, F. Szöllősi, “Constructions of Complex Hadamard Matrices via Tiling Abelian Groups”, *Open Syst. Inf. Dyn.* **14**(3), 247–263 (2007).
- [25] J.M. Goethals, J.J. Seidel, “Strongly Regular Graphs Derived from Combinatorial Designs”, *Canad. J. Math.* **22**(3), 597–614 (1970).
- [26] A.J. LaClair, “A Survey on Hadamard Matrices”, *Chancellor’s Honors Program Projects, University of Tennessee, Knoxville* (2016).
- [27] P. Lampio, F. Szöllősi, P. Östregård, “The Quaternary Complex Hadamard Matrices of Orders 10, 12, and 14”, *Discr. Math.* **313**(2), 189–206 (2013).

- [28] K. Beauchamp, R. Nicoară, “Orthogonal Maximal Abelian *-Subalgebras of the 6×6 Matrices”, *Linear Alg. Appl.* **428**(8–9), 1833–1853 (2006).
- [29] F. Szöllősi, “Construction, Classification and Parametrization of Complex Hadamard Matrices”, *Ph.D. Thesis, Central European University, Budapest* (2011).
- [30] U. Haagerup, *Operator Algebras and Quantum Field Theory* (Rome 1996), Int. Press, Cambridge, MA, 296–322 (1997).
- [31] R. Craigen, “Equivalence Classes of Inverse Orthogonal and Unit Hadamard Matrices”, *Bull. Austral. Math. Soc.* **44**(1), 109–115 (1991).
- [32] T. Tao, “Fuglede’s Conjecture is False in 5 and Higher Dimensions”, *Math. Res. Lett.* **11**(2), 251–258 (2004).
- [33] F. Szöllősi, “Complex Hadamard Matrices of Order 6: a Four-Parameter Family”, *J. London Math. Soc.* **85**(3), 616–632, (2012).
- [34] K.-T. Fang, G. Ge, “A Sensitive Algorithm for Detecting the Inequivalence of Hadamard Matrices”, *J. Math. Comp.* **73**(246), 843–851 (2003).
- [35] R. Nicoară, “A Finiteness Result for Commuting Squares of Matrix Algebras”, *J. Operator Theory* **55**(2), 295–310 (2006).
- [36] F. Szöllősi, “Exotic Complex Hadamard Matrices and Their Equivalence”, *Cryptogr. Commun.* **2**, 187–198 (2010).
- [37] W. Tadej, K. Życzkowski, “Defect of a Unitary Matrix”, *Linear Alg. Appl.* **429**(2–3), 447–481 (2008).
- [38] W. Tadej, “Defect and Equivalence of Unitary Matrices. The Fourier Case. Part I”, *Open Syst. Inf. Dyn.* **25**(4), 1850020 (2018).
- [39] F.C. Motta, P.D. Shipman, “Informing the Structure of Complex Hadamard Matrix Spaces Using a Flow”, *Discr. Cont. Dyn. Sys. S* **12**(8), 2349–2364 (2019).
- [40] P. Diță, “Complex Hadamard Matrices from Sylvester Inverse Orthogonal Matrices”, *Open Syst. Inf. Dyn.* **16**(4), 387–405 (2009).
- [41] V. Elser, *private communication* (2011).
- [42] P. Östregård, P. Lampio, F. Szöllősi, “Orderly Generation of Butson Hadamard Matrices”, *Math. Comp.* **89**, 313–331 (2020).

- [43] Butson Home, <https://wiki.aalto.fi/display/Butson/Butson+Home>, Online supplement to [42] maintained by P. Lampio (access: 2021/09/21).
- [44] S. Chaturvedi, “Aspects of Mutually Unbiased Bases in Odd-Prime-Power Dimensions”, *Phys. Rev. A* **65**, 044301 (2002).
- [45] D. McNulty, S. Weigert, “Isolated Hadamard Matrices from Mutually Unbiased Product Bases”, *J. Math. Phys.* **53**, 122202 (2012).
- [46] B.R. Karlsson, “*BCCB* Complex Hadamard Matrices of Order 9, and MUBs”, *Linear Alg. Appl.* **504**(1), 309–324 (2016).
- [47] R. Sinkhorn, “A Relationship Between Arbitrary Positive Matrices and Doubly Stochastic Matrices”, *Ann. Math. Statist.* **35**(2), 876–879 (1964).
- [48] R. Sinkhorn, P. Knopp, “Concerning Nonnegative Matrices and Doubly Stochastic Matrices”, *Pacific Journal of Math.* **21**(2), 343–348 (1967).
- [49] H.H. Bauschke, J.M. Borwein, “On Projection Algorithms for Solving Convex Feasibility Problems”, *SIAM Rev.* **38**(3), 367–426 (1996).
- [50] V. Cappellini, H.-J. Sommers, W. Bruzda, K. Życzkowski, “Random Bistochastic Matrices”, *J. Phys. A: Math. Theor.* **42**, 365209 (2009).
- [51] C. Colbourn, J.H. Dinitz, *Handbook of Combinatorial Designs*, CRC Press (2006).
- [52] P. Wocjan, T. Beth, “New Construction of Mutually Unbiased Bases in Square Dimensions”, *Quantum Inf. Comput.* **5**(2), 93–101 (2005).
- [53] E. Verheiden, “Hadamard Matrices and Projective Planes”, *J. Comb. Theory A* **32**(2), 126–131 (1982).
- [54] A.M. Alakhim, “Hadamard Matrices, Quaternions, and the Pearson Chi-Square Statistic”, [arXiv:1806.09348](https://arxiv.org/abs/1806.09348) (2018).
- [55] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, B.C. Hiesmayr, “Entanglement Detection via Mutually Unbiased Bases”, *Phys. Rev. A* **86**(2), 022311 (2012).
- [56] B.C. Hiesmayr, W. Löffler, “Mutually Unbiased Bases and Bound Entanglement”, *Phys. Scr.* **2014**, T160, 014017 (2014).
- [57] B. C. Hiesmayr, D. McNulty, S. Baek, S. Singha Roy, J. Bae, D. Chruściński, “Detecting Entanglement can be More Effective with Inequivalent Mutually Unbiased Bases”, *New J. Phys.* **23**, 093018 (2021).

- [58] GitHub Platform, <https://github.com/matrix-toolbox> (access: 2021/10/01).
- [59] A. Bayu Suksmono, Y. Minato, “Finding Hadamard Matrices by a Quantum Annealing Machine”, [arXiv:1902.07890](#) (2019).
- [60] I. Bengtsson, K. Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, II ed. (2017).
- [61] L.A. de Castro, O.P. de Sá Neto, C.A. Brasil, “An Introduction to Quantum Measurements with a Historical Motivation”, *Acta Phys. Slovaca* **69**(1), 1–74 (2019).
- [62] M.A. Sustik, J.A. Tropp, I.S. Dhillon, R.W. Heath Jr., “On the Existence of Equiangular Tight Frames”, *Linear Alg. Appl.* **426**(2–3), 619–635 (2007).
- [63] J. Renes, R. Blume-Kohout, A. Scott, C. Caves, “Symmetric Informationally Complete Quantum Measurements”, *J. Math. Phys.* **45**(6), 2171 (2004).
- [64] S.G. Hoggar, “64 Lines from a Quaternionic Polytope”, *Geom. Dedicata* **69**, 287–289 (1998).
- [65] P.G. Casazza, J. Kovačević, “Equal-Norm Tight Frames with Erasures”, *Adv. Comput. Math.* **18**, 387–430 (2003).
- [66] R.B. Holmes, V.I. Paulsen, “Optimal Frames for Erasures”, *Linear Alg. Appl.* **377**, 31–51 (2004).
- [67] R.B.A. Adamson, A.M. Steinberg, “Improving Quantum State Estimation with Mutually Unbiased Bases”, *Phys. Rev. Lett.* **105**(3), 030406 (2010).
- [68] A. Rastegin, “Uncertainty Relations for MUBs and SIC-POVMs in Terms of Generalized Entropies”, *Eur. Phys. J. D* **67**, 269 (2013).
- [69] M.A. Ballester, S. Wehner, “Entropic Uncertainty Relations and Locking: Tight Bounds for Mutually Unbiased Bases”, *Phys. Rev. A* **75**(2), 022319 (2007).
- [70] D. Goyeneche, S. Gómez, “Mutually Unbiased Bases with Free Parameters”, *Phys. Rev. A* **92**(6), 062325 (2015).
- [71] A. Szymusiak, “Maximally Informative Ensembles for SIC-POVMs in Dimension 3”, *J. Phys. A: Math. Theor.* **47**(44), 445301 (2014).
- [72] D. Mayers, A. Yao, “Self Testing Quantum Apparatus”, *QIC* **4**(4), 273–286 (2004).
- [73] G. Zauner, “Quantum Designs”, *Ph.D. Thesis, University of Vienna* (1999).

- [74] A.J. Scott, M. Grassl, “Symmetric Informationally Complete Positive-Operator-Valued Measures: A New Computer Study”, *J. Math. Phys.* **51**(4), 042203 (2010).
- [75] J. Schwinger, “Unitary Operator Bases”, *PNAS* **46**(4), 570–579 (1960).
- [76] J.A. Tropp, I.S. Dhillon, R.W. Heath, T. Strohmer, “Designing Structured Tight Frames via an Alternating Projection Method”, *IEEE Trans. Inf. Theory* **51**(1), 188–209 (2005).
- [77] D. Goyeneche, O. Turek, “Equiangular Tight Frames and Unistochastic Matrices”, *J. Phys. A: Math. Theor.* **50**(24), 245304 (2017).
- [78] S. Brierley, S. Weigert, I. Bengtsson, “All Mutually Unbiased Bases in Dimensions Two to Five”, *Quant. Info. Comp.* **10**(9), 803–820 (2010).
- [79] B. Et-Taoui, “Complex Conference Matrices, Complex Hadamard Matrices and Complex Equiangular Tight Frames”, *Springer Proc. Math. Stat.* **148**, 181–191 (2014).
- [80] A. Sehrawat, A.B. Klimov, “Unitarily Inequivalent Mutually Unbiased Bases for n Qubits”, *Phys. Rev. A* **90**(6), 062308 (2014).
- [81] D. Goyeneche, “Mutually Unbiased Triplets from Non-Affine Families of Complex Hadamard Matrices in Dimension 6”, *J. Phys. A: Math. Theor.* **46**(10), 105301 (2015).
- [82] F. Szöllősi, “All Complex Equiangular Tight Frames in Dimension 3”, [arXiv:1402.6429](#) (2014).
- [83] M. Grassl, “On SIC-POVMs and MUBs in Dimension 6”, [arXiv:quant-ph/0406175](#) (2009).
- [84] D.M. Appleby, “Symmetric Informationally Complete–Positive Operator Valued Measures and the Extended Clifford Group”, *J. Math. Phys.* **46**(5), 052107 (2005).
- [85] A. Szymusiak, W. Słomczyński, “Informational Power of the Hoggar Symmetric Informationally Complete Positive Operator-Valued Measure”, *Phys. Rev. A* **94**(1), 022122 (2016).
- [86] S. Kochen, E.P. Specker, “The Problem of Hidden Variables in Quantum Mechanics”, *J. Math. Mech.* **17**(1), 59–87 (1967).
- [87] C. Budroni, A. Cabello, O. Gühne, M. Kleinmann, J.-Å. Larsson, “Quantum Contextuality”, [arXiv:2102.13036](#) (2021).
- [88] S. Yu, C.H. Oh, “State-Independent Proof of Kochen–Specker Theorem with 13 Rays”, *Phys. Rev. Lett.* **108**(3), 030402 (2012).

- [89] A. Cabello, J.M. Estebaranz, G. García-Alcaine, “Bell–Kochen–Specker Theorem: A Proof with 18 Vectors”, *Phys. Lett. A* **212**(4), 183–187 (1996).
- [90] P. Lisoněk, P. Badziąg, J.R. Portillo, A. Cabello, “Kochen–Specker Set with Seven Contexts”, *Phys. Rev. A* **89**(4), 042101 (2014).
- [91] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, “Quantum Entanglement”, *Rev. Mod. Phys.* **81**(2), 865 (2009).
- [92] W. Bruzda, S. Friedland, K. Życzkowski, “Tensor Rank and Entanglement of Pure Quantum States”, *arXiv:1912.06854* (2021).
- [93] E. Chitambar, G. Gour, “Quantum Resource Theories”, *Rev. Mod. Phys.* **91**(2), 025001 (2019).
- [94] C.H. Bennet, G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing”, *Theor. Comput. Sci.* **560**(1), 7–11 (2014).
- [95] A.K. Ekert, “Quantum Cryptography Based on Bell’s Theorem”, *Phys. Rev. Lett.* **67**(6), 661 (1991).
- [96] M.B. Plenio, S. Virmani, “An Introduction to Entanglement Measures”, *Quant. Inf. Comput.* **7**(1), 1–51 (2007).
- [97] D. Goyeneche, D. Alsina, J.I. Latorre, A. Riera, K. Życzkowski, “Absolutely Maximally Entangled States, Combinatorial Designs, and Multiunitary Matrices”, *Phys. Rev. A* **92**(3), 032316 (2015).
- [98] J. Maziero, “Computing Partial Traces and Reduced Density Matrices”, *Int. J. Mod. Phys. C* **28**(1), 1750005 (2017).
- [99] P. Facchi, “Multipartite Entanglement in Qubit Systems”, *Rend. Lincei Mat. Appl.* **20**(1), 25–67 (2009).
- [100] A.J. Scott, “Multipartite Entanglement, Quantum-Error-Correcting Codes, and Entangling Power of Quantum Evolutions”, *Phys. Rev. A* **69**(5), 052330 (2004).
- [101] R. Laflamme, C. Miquel, J.P. Paz, W.H. Żurek, “Perfect Quantum Error Correcting Code”, *Phys. Rev. Lett.* **77**(1), 198 (1996).
- [102] P. Mazurek, M. Farkas, A. Grudka, M. Horodecki, M. Studziński, “Quantum Error-Correction Codes and Absolutely Maximally Entangled States”, *Phys. Rev. A* **101**(4), 042305 (2020).

- [103] Z. Raissi, C. Gogolin, A. Riera, A. Acín, “Constructing Optimal Quantum Error Correcting Codes from Absolute Maximally Entangled States”, *J. Phys. A: Math. Theor.* **51**(7), 075301 (2018).
- [104] W. Helwig, W. Cui, J.I. Latorre, A. Riera, H.-K. Lo, “Absolute Maximal Entanglement and Quantum Secret Sharing”, *Phys. Rev. A* **86**(5), 052335 (2012).
- [105] W. Helwig, W. Cui, “Absolutely Maximally Entangled States: Existence and Applications”, *arXiv:1306.2536* (2013).
- [106] F. Pastawski, B. Yoshida, D. Harlow, J. Preskill, “Holographic Quantum Error-Correcting Codes: Toy Models for the Bulk/Boundary Correspondence”, *J. High Energy Phys.* **2015**, 149 (2015).
- [107] J. Maldacena, “The Large- N Limit of Superconformal Field Theories and Supergravity”, *Int. J. Theor. Phys.* **38**, 1113–1133 (1999).
- [108] A. Almheiri, X. Dong, D. Harlow, “Bulk Locality and Quantum Error Correction in AdS/CFT”, *J. High Energy Phys.* **2015**, 163 (2015).
- [109] D. Vaid, “Quantum Error Correction in Loop Quantum Gravity”, *arXiv:1912.11725* (2019).
- [110] L. Borsten, M.J. Duff, A. Marrani, W. Rubens, “On the Black-Hole/Qubit Correspondence”, *Eur. Phys. J. Plus* **126**, 37 (2011).
- [111] F. Huber, C. Eltschka, J. Siewert, O. Gühne, “Bounds on Absolutely Maximally Entangled States from Shadow Inequalities, and the Quantum MacWilliams Identity”, *J. Phys. A: Math. Theor.* **51**, 175301 (2018).
- [112] A. Higuchi, A. Sudbery, “How Entangled Can Two Couples Get?”, *Phys. Lett A* **273**(4), 213–217 (2000).
- [113] D. Goyeneche, K. Życzkowski, “Genuinely Multipartite Entangled States and Orthogonal Arrays”, *Phys. Rev. A* **90**(2), 022316 (2014).
- [114] E.M. Rains, “Nonbinary Quantum Codes”, *IEEE Trans. Inf. Theory* **45**(6), 1827–1832 (1999).
- [115] F. Huber, M. Grassl, “Quantum Codes of Maximal Distance and Highly Entangled Subspaces”, *Quantum* **4**, 284 (2020).
- [116] F. Huber, N. Wyderka, “Online Table of AME States”, <https://www.tp.nt.uni-siegen.de/+fhuber/ame.html> (access: 2020/10/11).

- [117] D. Bruß, C. Macchiavello, “How the First Partial Transpose was Written”, *Found. Phys.* **35**, 1921–1926 (2005).
- [118] A. Peres, “Separability Criterion for Density Matrices”, *Phys. Rev. Lett.* **77**(8), 1413 (1996).
- [119] M. Horodecki, P. Horodecki, R. Horodecki, “Separability of Mixed States: Necessary and Sufficient Conditions”, *Phys. Lett. A* **223**(1–2), 1–8 (1996).
- [120] W. Bruzda, V. Cappellini, H.-J. Sommers, K. Życzkowski, “Random Quantum Operations”, *Phys. Lett. A* **373**(3), 320–324 (2009).
- [121] L. Piroli, B. Bertini, J.I. Cirac, T. Prosen, “Exact Dynamics in Dual-Unitary Quantum Circuits”, *Phys. Rev. B* **101**(9), 094304 (2020).
- [122] P. Zanardi, “Entanglement of Quantum Evolutions”, *Phys. Rev. A* **63**(4), 040304 (2001).
- [123] B. Jonnadula, P. Mandayam, K. Życzkowski, A. Lakshminarayan, “Impact of Local Dynamics on Entangling Power”, *Phys. Rev. A* **95**(4), 040302 (2017).
- [124] R.C. Bose, S.S. Shrikhande, E.T. Parker, “Further Results on the Construction of Mutually Orthogonal Latin Squares and the Falsity of Euler’s Conjecture”, *Can. J. Math.* **12**, 189–203 (1960).
- [125] L. Euler, “Recherches sur un nouvelle espèce de quarrés magiques”, *Euler Archive* (access: 2021/10/01).
- [126] G. Tarry, “Le problème des 36 officiers”, *Compte Rendu de l’Assoc. Fr. Avanc. Sci. Nat.* **1**, 122–123 and **2**, 170–203 (1901).
- [127] J. Paczos, M. Wierzbński, G. Rajchel-Mieldzioć, A. Burchardt, K. Życzkowski, “Genuinely Quantum SudoQ and its Cardinality”, *Phys. Rev. A* **104**(4), 042423 (2021).
- [128] B. Musto, J. Vicary, “Orthogonality for Quantum Latin Isometry Squares”, *EPTCS* **287**, 253–266 (2019).
- [129] J.D. Horton, “Sub-Latin Squares and Incomplete Orthogonal Arrays”, *J. Comb. Theory A*, **16**(1), 23–33 (1974).
- [130] L. Clarisse, S. Ghosh, S. Severini, A. Sudbery, “Entangling Power of Permutations”, *Phys. Rev. A* **72**(1), 012314 (2005).
- [131] D. Goyeneche, Z. Raissi, S. Di Martino, K. Życzkowski, “Entanglement and Quantum Combinatorial Designs”, *Phys. Rev. A* **97**(6), 062326 (2018).

- [132] A. Einstein, B. Podolsky, N. Rosen, “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?”, *Phys. Rev.* **47**(10), 777–780 (1935).
- [133] J. Bricmont, “History of Quantum Mechanics or the Comedy of Errors”, *Int. J. Quant. Found.* **3**, 31–64 (2017).
- [134] J.S. Bell, “On the Einstein Podolsky Rosen Paradox”, *Physics* **1**(3), 195–200 (1964).
- [135] A. Aspect, P. Grangier, G. Roger, “Experimental Tests of Realistic Local Theories via Bell’s Theorem”, *Phys. Rev. Lett.* **47**(7), 460 (1981).
- [136] B. Hensen, H. Bernien, A.E. Dréau et al., “Loophole-Free Bell Inequality Violation Using Electron Spins Separated by 1.3 kilometres”, *Nature* **526**, 682–686 (2015).
- [137] M. Gachechiladze, B. Bąk, M. Pawłowski, N. Miklin, “Quantum Bell Inequalities from Information Causality – Tight for Macroscopic Locality”, *arXiv:2103.05029* (2021).
- [138] Y. Liu, T.-Y. Chen, L.-J. Wang et al., “Experimental Measurement-Device-Independent Quantum Key Distribution”, *Phys. Rev. Lett.* **111**(13), 130502 (2013).
- [139] T.F. da Silva, D. Vitoireti, G.B. Xavier, G.C. do Amaral, G.P. Temporão, J.P. von der Weid, “Proof-of-Principle Demonstration of Measurement-Device-Independent Quantum Key Distribution Using Polarization Qubits”, *Phys. Rev. A* **88**(5), 052303 (2013).
- [140] R. Cleve, H. Buhrmann, “Substituting Quantum Entanglement for Communication”, *Phys. Rev. A* **56**(2), 1201 (1997).
- [141] T.S. Cubitt, D. Leung, W. Matthews, A. Winter, “Zero-Error Channel Capacity and Simulation Assisted by Non-Local Correlations”, *IEEE Transf. Theory* **57**(8), 5509–5523 (2011).
- [142] A. Acín, N. Gisin, Ll. Masanes, “From Bell’s Theorem to Secure Quantum Key Distribution”, *Phys. Rev. Lett.* **97**(12), 120405 (2006).
- [143] Ll. Masanes, S. Pironio, A. Acín, “Secure Device-Independent Quantum Key Distribution with Causally Independent Measurement Devices”, *Nature Comm.* **2**, 238 (2011).
- [144] U. Vazirani, T. Vidick, “Fully Device-Independent Quantum Key Distribution”, *Phys. Rev. Lett.* **113**(14), 140501 (2014).
- [145] J. Kaniewski, S. Wehner, “Device-Independent Two-Party Cryptography Secure Against Sequential Attacks”, *New J. Phys.* **18**(5), 055004 (2016).
- [146] D. Alsina, J.I. Latorre, “Experimental Test of Mermin Inequalities on a Five-Qubit Quantum Computer”, *Phys. Rev. A* **94**(1), 012314 (2016).

- [147] D. García-Martín, G. Sierra, “Five Experimental Tests on the 5-Qubit IBM Quantum Computer”, *J. Appl. Math. Phys.* **6**(7), 1460–1475 (2018).
- [148] R. Colbeck, A. Kent, “Private Randomness Expansion with Untrusted Devices”, *J. Phys. A: Math. Theor.* **44**(9), 095305 (2011).
- [149] S. Pironio, A. Acín, S. Massar, et al., “Random Numbers Certified by Bell’s Theorem”, *Nature* **464**, 1021–1024 (2010).
- [150] R. Colbeck, R. Renner, “Free Randomness Can Be Amplified”, *Nature Physics* **8**, 450–453 (2012).
- [151] S. Arora, C. Lund, R. Motwani, M. Sudan, M. Szegedy, “Proof Verification and the Hardness of Approximation Problems”, *J. ACM* **45**(3), 501–555 (1998).
- [152] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, “Bell Nonlocality”, *Rev. Mod. Phys.* **86**(2), 419 (2014).
- [153] D. Rosset, J.-D. Bancal, N. Gisin, “Classifying 50 Years of Bell Inequalities”, *J. Phys. A: Math. Theor.* **47**(42), 424022 (2014).
- [154] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, “Proposed Experiment to Test Local Hidden-Variable Theories”, *Phys. Rev. Lett.* **23**(15), 880 (1969).
- [155] A. Fine, “Hidden Variables, Joint Probability, and the Bell Inequalities”, *Phys. Rev. Lett.* **48**(5), 291 (1982).
- [156] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, S. Pironio, “Bell Inequalities Tailored to Maximally Entangled States”, *Phys. Rev. Lett.* **119**(4), 040402 (2017).
- [157] K.W. Schmidt, “Problem 863”, *Math. Mag.* **46**, 103 (1973).
- [158] M. Best, “The Excess of a Hadamard Matrix”, *Indag. Math.* **80**(5), 357–361 (1977).
- [159] N. Farmakis, S. Kounias, “The Excess of Hadamard Matrices and Optimal Designs”, *Discr. Math.* **67**(2), 165–176 (1987).
- [160] S. Kounias, N. Farmakis, “On the Excess of Hadamard Matrices”, *Discr. Math.* **68**(1), 59–69 (1988).
- [161] C. Koukouvinos, J. Seberry, “Hadamard Matrices of Order $\equiv 8 \pmod{16}$ with Maximal Excess”, *Discr. Math.* **92**, 173–176 (1991).
- [162] H. Kharaghani, “An Infinite Class of Hadamard Matrices of Maximal Excess”, *Discr. Math.* **89**(3), 307–312 (1991).

- [163] T. Xia, M. Xia, J. Seberry, “Regular Hadamard Matrices, Maximum Excess and SBIBD”, *Australas. J. Comb.* **27**, 263–275 (2003).
- [164] H. Kharaghani, J. Seberry, “The Excess of Complex Hadamard Matrices”, *Graphs Combin.* **9**, 47–56 (1993).
- [165] J. Ford, A. Gál, *Hadamard Tensors and Lower Bounds on Multiparty Communication Complexity*, *ICALP’05*, 1163–1175 (2005).
- [166] J. Hammer, R. Levingston, J. Seberry, “A Remark on the Excess of Hadamard Matrices and Orthogonal Designs”, *Ars Comb.* **5**, 237–254 (1978).
- [167] M. Epping, H. Kampermann, D. Bruß, “Designing Bell Inequalities from a Tsirelson Bound”, *Phys. Rev. Lett.* **111**(24), 240404 (2013).
- [168] J.I. de Vicente, “Simple Conditions Constraining the Set of Quantum Correlations”, *Phys. Rev. A* **92**(3), 032103 (2015).
- [169] M. Hall, “Hadamard Matrices of Order 16”, *J.P.L. Research Summary* **1**, 36–10, 21–26 (1961).
- [170] D. Uzcátegui Contreras, D. Goyeneche, O. Turek, Z. Václavíková, “Circulant Matrices With Orthogonal Rows and off-Diagonal Entries of Absolute Value 1”, *Comm. Math.* **29**(1), 15–34 (2021).
- [171] P. Diviánszky, E. Bene, T. Vértesi, “Qutrit Witness from the Grothendieck Constant of Order Four”, *Phys. Rev. A* **96**(1), 012113 (2017).
- [172] P. Mandayam, S. Bandyopadhyay, M. Grassl, W.K. Wootters, “Unextendible Mutually Unbiased Bases from Pauli Classes”, *Quant. Inf. Comput.* **14**(9), 823–844 (2014).
- [173] K. Thas, “Unextendible Mutually Unbiased Bases (After Mandayam, Bandyopadhyay, Grassl and Wootters)”, *Entropy* **18**(11), 395 (2016).
- [174] R. Augusiak, T. Fritz, Ma. Kotowski, Mi. Kotowski, M. Pawłowski, M. Lewenstein, A. Acín, “Tight Bell Inequalities with no Quantum Violation from Qubit Unextendible Product Bases”, *Phys. Rev. A* **85**(4), 042113 (2012).
- [175] S. Popescu, D. Rohrlich, “Quantum Nonlocality as an Axiom”, *Found. Phys.* **24**(3), 379–385 (1994).

Appendix A

Papers

In the Appendix we present papers contributing to this work in the style and formatting of the journals they were published in. Exceptions are preprints which, at the time of preparing the Thesis, undergo the process of revision — they are included in the generic form, the same, in which they were submitted to the `arXiv` e-Print service.

The papers do not belong to the main body of the Thesis. They were added here at the convenience of the Reader who might wish to confront the content or quickly follow some additional information which was intentionally abandoned in the previous chapters.

List of papers (in order of appearance in the text):

- [A1] **W. Bruzda**,
Extension of the Set of Complex Hadamard Matrices of Size 8,
Math. Comput. Sci. **12**(4), 459–464 (2018).
- [A2] **W. Bruzda**,
Isolated Complex Hadamard Matrices,
in preparation, (2021).
- [A3] **W. Bruzda**, D. Goyeneche, K. Życzkowski,
Quantum Measurements with Prescribed Symmetry,
Phys. Rev. A **96**, 022105 (2017).
- [A4] S. Ahmad Rather, A. Burchardt, **W. Bruzda**, G. Rajchel-Mieldzioć, A. Lakshmi-
narayan, K. Życzkowski,
Thirty-six Entangled Officers of Euler,
arXiv:2104.05122 (2021).
- [A5] D. Goyeneche, **W. Bruzda**, O. Turek, D. Alsina, K. Życzkowski,
Local Hidden Variable Value Without Optimization Procedures,
arXiv:2004.00695 (2021).

Extension of the Set of Complex Hadamard Matrices of Size 8

Wojciech T. Bruzda

Received: 10 January 2018 / Revised: 5 February 2018 / Accepted: 20 March 2018 /

Published online: 19 September 2018

© The Author(s) 2018

Abstract A complex Hadamard matrix is defined as a matrix H which fulfills two conditions, $|H_{j,k}| = 1$ for all j and k and $HH^* = N\mathbb{I}_N$ where $\mathbb{I}_N$ is an identity matrix of size N . We explore the set of complex Hadamard matrices $\mathcal{H}_N$ of size $N = 8$ and present two previously unknown structures: a one-parametric, non-affine family $T_8^{(1)}$ of complex Hadamard matrices and a single symmetric and isolated matrix $A_8^{(0)}$.

Keywords Complex Hadamard matrix · Non-affine family · Isolated matrix · Butson class

Mathematics Subject Classification 15A03 · 65F25 · 15B34 · 05B20

1 Introduction

The description of the set $\mathcal{H}_N$ of complex Hadamard matrices (CHMs) is exhausted for $N \in \{2, 3, 4, 5\}$ [1,2], while beginning from $N = 6$, general knowledge of the structure of $\mathcal{H}_N$ can be considered incomplete. CHMs and their subset containing only real ∓ 1 -entry objects are a subject of great interest in many fields of contemporary mathematics and physics. Let us only mention applications in quantum optics, telecommunication and signal processing, assistance in error correcting codes, background for equiangular lines, and many others [2–6].

Two matrices H_1 and $H_2 \in \mathcal{H}_N$ are said to be *equivalent* if one of them can be expressed in terms of the other by means of two permutation matrices P_1 and P_2 and two unitary diagonal matrices D_1 and D_2 as $H_1 = P_1 D_1 H_2 P_2 D_2$ [2,7]. In general, the recognition of equivalence is not trivial and requires additional tools such as Haagerup invariants [2] or matrix fingerprint [8]. Another signature assigned to a matrix is its *defect* [7,9]. The defect of a unitary matrix $d(H)$ tells us what is the largest possible size of a smooth family of CHMs stemming from H . This one-way criterion is useful when searching for isolated matrices for which the defect vanishes. There are two possible types of CHM families: *affine* and *non-affine*. In the first case, the particular constant entries in given matrix H can be extended to complex variables so that their phases vary linearly as in the following example of the 4-dimensional Fourier matrix [1]

W. T. Bruzda (✉)
Institute of Physics, Jagiellonian University, Kraków, Poland
e-mail: w.bruzda@uj.edu.pl

$$F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \mapsto \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & ie^{i\alpha} & -1 & -ie^{i\alpha} \\ 1 & -1 & 1 & -1 \\ 1 & -ie^{i\alpha} & -1 & ie^{i\alpha} \end{bmatrix} : \alpha \in [0, 2\pi). \quad (1.1)$$

The second case involves non-linear formulas for the phases of the variable entries [7, 12].

Every CHM can be transformed by an equivalence preserving operation into the form in which its first row and its first column has only ones. The remaining $(N - 1) \times (N - 1)$ elements shall be called the *core* of the matrix. All matrices in this paper are worked out in the above *dephased* form.

A special subclass of CHMs is called Butson type matrices [10, 11], denoted by $BH(N, q) \subset \mathcal{H}_N$, with the property that each entry of $H \in BH(N, q)$ is the q th root of unity, $(H_{j,k})^q = 1$ for any j and k . For instance, the standard class of real Hadamard matrices of size N forms the class $BH(N, 2)$, while the Fourier matrix F_N of order N belongs to the set $BH(N, N)$.

The notation adopted in this work is entirely taken from the on-line CHM catalogue [12] based on [7] and, to save space, we use the symbol $[\beta]$ as a shortcut for the exponent expression $\exp(i\pi\beta)$.

2 Looking for a New Matrix $H \in \mathcal{H}_8$

Searching for new CHMs supports the description of the set $\mathcal{H}_N$ and provides better understanding of its elements. Moreover, additional profit from having new examples of CHMs is extension of the area for searching for new mutually unbiased pairs of Hadamard matrices H_1 and H_2 such that $H_1^* H_2 / \sqrt{N} \in \mathcal{H}_N$, which is directly related to *mutually unbiased bases* [13–15].

Looking for possibly new complex Hadamard matrices, the following procedure was used. Let us take any dephased matrix H with unimodular entries $H_{j,k} = [\varphi_{j,k}]$ for $\varphi_{j,k} \in [0, 2)$. Define a target function $Z(H) \equiv \|HH^* - N\mathbb{I}_N\|_F$, where the Frobenius norm of matrix is applied, $\|X\|_F^2 = \text{tr}XX^*$. Using a random-walk procedure over the core phases we try to minimize $Z(H)$ and for $Z(H) < 10^{-16}$ we can stop having a matrix H that belongs to $\mathcal{H}_N$ with respect to a given precision. Such raw matrices are ready for further analytical processing. The most interesting outcomes show up when only a subset of core phases undergoes variation while the other elements are fixed to certain values. The algorithm is very fast and even using an average desktop PC for $N < 9$ one can obtain results within seconds.

The case of $N = 6$, however without any formal proof of completeness, seems to be already understood and it is conjectured that the families $G_6^{(4)}$ of Szöllősi [16] and $K_6^{(3)}$ of Karlsson [17] along with the isolated Tao matrix $S_6^{(0)}$ [18, 19] constitute the set in which any $H \in \mathcal{H}_6$ is included. The set $\mathcal{H}_7$ consists of several isolated matrices: $F_7^{(0)}$ [7], $C_7^{(0)}$ [2, 20] and $Q_7^{(0)}$ [21] together with one affine family $P_7^{(1)}$ [22]. The investigation of this case is far from being closed but proved to be hard for any numerical attempts. Hence, in this short paper, we focus on the next promising case for $N = 8$ and, as a consequence, we present previously unknown:

- a 1-parametric, non-affine family $T_8^{(1)}$ of CHMs that contains Butson $BH(8, 20)$ matrices,
- an isolated matrix $A_8^{(0)}$ of a non-Butson type.

3 Non-affine Family $T_8^{(1)}$ of $N = 8$ Complex Hadamard Matrices

Let us start with the matrix $T_8 \in \mathcal{H}_8$ that was found numerically (see Sect. 2) and then expressed in the analytic form using symmetric patterns in the elements and phases of the core and orthogonality constraints with respect to the rows and columns. Define a constant matrix:

$$T = \text{EXP} \left(i \frac{\pi}{10} \begin{bmatrix} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet & 3 & 15 & 18 \\ \bullet & \bullet & \bullet & \bullet & \bullet & 13 & 15 & 8 \\ \bullet & 2 & 2 & 2 & 2 & 17 & 5 & 2 \\ \bullet & 2 & 2 & 2 & 2 & 7 & 5 & 12 \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & 10 & 10 \\ \bullet & 2 & 2 & 12 & 12 & 10 & \bullet & 10 \\ \bullet & 2 & 2 & 12 & 12 & 10 & 10 & \bullet \end{bmatrix} \right) \quad (3.1)$$

where $T = \text{EXP}(A)$ denotes the entrywise exponent of a matrix, $T_{j,k} = \exp(A_{j,k})$ and $\bullet$ replaces zero. Furthermore, we shall use the matrix

$$T_c = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & c_3 & c_2 & c_1 & -i/c_1 & 1 & 1 & 1 \\ 1 & -c_1 & i/c_1 & -i/c_2 & -i/c_3 & 1 & 1 & 1 \\ 1 & c_2 & c_3 & -i/c_1 & c_1 & 1 & 1 & 1 \\ 1 & -i/c_1 & c_1 & i/c_3 & i/c_2 & 1 & 1 & 1 \\ 1 & e^{i\alpha} & -e^{i\alpha} & -e^{-i\alpha} & e^{-i\alpha} & 1 & 1 & 1 \\ 1 & e^{i\alpha} & -e^{i\alpha} & -e^{-i\alpha} & e^{-i\alpha} & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}. \quad (3.2)$$

with

$$c_1 = \frac{1}{4} \sqrt{8 - \sqrt{50 - 6\sqrt{5}}} + i \frac{1}{4} \sqrt{8 + \sqrt{50 - 6\sqrt{5}}}, \quad (3.3)$$

$$c_2 = \frac{i - 1 - \left[\frac{3}{10}\right] + \left[\frac{4}{5}\right] - c_1 + i/c_1}{1 - ic_1^2}, \quad (3.4)$$

$$c_3 = -ic_2c_1^2, \quad (3.5)$$

where $\alpha = -\text{arccot}(1 - \sqrt{5})$ and $[\beta] = \exp(i\pi\beta)$. This allows us to define the following complex Hadamard matrix $T_8 = T_c \circ T$ where $\circ$ is the entrywise product of matrices.

One can check that the defect $d(T_8) = 3$ which is an indication that the matrix can be a part of a family of inequivalent CHMs. Moreover, the structure of the three last columns resembles the form of a Butson type object which might suggest that a Butson matrix lies on a trajectory of the orbit stemming from a given matrix and some entries $(T_8)_{j,k}$ for $2 \leq j \leq 7$ and $2 \leq k \leq 5$ could be functionally dependent. Indeed, when one assigns to two particular elements $u(\mu) = (T_8)_{7,2}$ and $-u(\mu) = (T_8)_{7,3}$ a value $\mu \in [0, 1/2]$ for $u = [\mu]$, having the last three columns fixed, there always can be found a CHM with the second row of the form

$$\left[1, x, y, z, -\frac{yz}{x}, \left[\frac{3}{10} \right], -i, \left[\frac{18}{10} \right] \right]. \quad (3.6)$$

Again, using symmetries amongst phases and orthogonality constraints, one recovers a full matrix in the form of

$$T_8^{(1)}(x) = \text{EXP} \left(i \frac{\pi}{10} \begin{bmatrix} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet & 3 & 15 & 18 \\ \bullet & 8 & 8 & 8 & 8 & 13 & 15 & 8 \\ \bullet & 2 & 2 & 2 & 2 & 17 & 5 & 2 \\ \bullet & \bullet & \bullet & \bullet & \bullet & 7 & 5 & 12 \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & 10 & 10 \\ \bullet & \bullet & \bullet & \bullet & \bullet & 10 & \bullet & 10 \\ \bullet & \bullet & \bullet & \bullet & \bullet & 10 & 10 & \bullet \end{bmatrix} \right) \circ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & y & z & -\frac{yz}{x} & 1 & 1 & 1 \\ 1 & -\frac{u}{y} & \frac{u}{x} & -\frac{uz}{xy} & -\frac{uz}{x^2} & 1 & 1 & 1 \\ 1 & y & x & -\frac{yz}{x} & z & 1 & 1 & 1 \\ 1 & \frac{u}{x} & -\frac{u}{y} & -\frac{uz}{x^2} & -\frac{uz}{xy} & 1 & 1 & 1 \\ 1 & -i\frac{x}{z} & i\frac{x}{z} & -i\frac{z}{x} & i\frac{z}{x} & 1 & 1 & 1 \\ 1 & u & -u & -\frac{uz^2}{x^2} & \frac{uz^2}{x^2} & 1 & 1 & 1 \\ 1 & i\frac{uz}{x} & i\frac{uz}{x} & -i\frac{uz}{x} & -i\frac{uz}{x} & 1 & 1 & 1 \end{bmatrix} \quad (3.7)$$

where

$$\chi_1 = 5 - 3\sqrt{5} + 4\sqrt{5 - 2\sqrt{5}} + (1 + i)\frac{1}{x} + \zeta_2, \quad (3.8)$$

$$\chi_2 = 45 - 9i - (17 - 7i)\sqrt{5} - 2\sqrt{620 - 500i - (285 - 234i)\sqrt{5}} - (1 + i)\frac{\chi_1}{x}, \quad (3.9)$$

$$\chi_3 = 10i - 10 + (6 - 2i)\sqrt{5} + 4\sqrt{10 - 10i - (5 - 4i)\sqrt{5}} + (1 + i)\frac{\chi_2}{x}, \quad (3.10)$$

$$\chi_4 = \sqrt{5} - 1 + i\sqrt{2}\sqrt{5 + \sqrt{5}} + (1 + i)\frac{\chi_3}{x}, \quad (3.11)$$

$$\chi_5 = (1 + i)\sqrt{1 - \sqrt{5}} + \zeta_4 - (1 - i)\left(2x^2 + (\sqrt{\chi_4})^*\right) - x(1 - 4i + \sqrt{5} + \zeta_1), \quad (3.12)$$

$$\chi_6 = \sqrt{5} - 1 - i - \sqrt{5 - 2\sqrt{5}} + (1 - i)x, \quad (3.13)$$

$$y = \frac{1}{4} \frac{\chi_5}{\chi_6}, \quad (3.14)$$

$$z = \frac{x}{x - y} \left((1 + i) \begin{bmatrix} 4 \\ 5 \end{bmatrix} - x - y - 1 + i \right), \quad (3.15)$$

with $\zeta_1 = -i\sqrt{10 - 2\sqrt{5}}$, $\zeta_2 = -\zeta_1$ and $\zeta_4 = i\sqrt{10 + 2\sqrt{5}}$ being the roots of the polynomial equation $\zeta^4 + 20\zeta^2 + 80 = 0$ and eventually

$$u = \frac{i x^2 - zx + xy + yz}{z \frac{1}{1 + i} - \left[\frac{3}{10} \right] - \left[\frac{4}{5} \right]}. \quad (3.16)$$

Unimodular number $x = [\gamma]$ is a free non-affine parameter.¹ In order to assure unimodularity of all other entries one can select phase γ from the range² $\gamma \in [2/5, 4/5] \cup [1, 7/5]$.

¹ Ready-to-use scripts in Matlab and Mathematica are available on-line [12].

² The actual range for γ is slightly broader, however, it does not reveal any more information.

As presumed, there are two Butson matrices that can be found inside the orbit $T_8^{(1)}$. For $\gamma \in \{1/2, 1, 13/10\}$ one obtains three matrices equivalent to $B_{8a} \in BH(8, 20)$ with defect 7,

$$B_{8a} = \text{EXP} \left(i \frac{\pi}{10} \begin{bmatrix} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & 5 & 10 & 13 & 8 & 3 & 15 & 18 \\ \bullet & 10 & 5 & 18 & 3 & 13 & 15 & 8 \\ \bullet & 12 & 7 & 10 & 15 & 17 & 5 & 2 \\ \bullet & 17 & 2 & 15 & 10 & 7 & 5 & 12 \\ \bullet & 7 & 17 & 3 & 13 & \bullet & 10 & 10 \\ \bullet & 2 & 12 & 8 & 18 & 10 & \bullet & 10 \\ \bullet & 15 & 15 & 5 & 5 & 10 & 10 & \bullet \end{bmatrix} \right), \quad (3.17)$$

while for $\gamma = 4/5$ there exists another Butson matrix $B_{8b} \in BH(8, 20)$ with defect 11,

$$B_{8b} = \text{EXP} \left(i \frac{\pi}{10} \begin{bmatrix} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & 8 & 10 & 13 & 5 & 3 & 15 & 18 \\ \bullet & 18 & 10 & 3 & 5 & 13 & 15 & 8 \\ \bullet & 12 & 10 & 7 & 15 & 17 & 5 & 2 \\ \bullet & 2 & 10 & 17 & 15 & 7 & 5 & 12 \\ \bullet & 10 & \bullet & \bullet & 10 & \bullet & 10 & 10 \\ \bullet & 10 & \bullet & 10 & \bullet & 10 & \bullet & 10 \\ \bullet & \bullet & \bullet & 10 & 10 & 10 & 10 & \bullet \end{bmatrix} \right). \quad (3.18)$$

It is likely that the above Butson matrices have not yet appeared in the literature, as they are not listed in the on-line catalogues [12, 23, 24].

No other Butson matrices intersect the orbit $T_8^{(1)}$ which implies that this family does not affect any other matrices of size 8 known up to date: $F_8^{(5)}$ [7], $S_8^{(4)}$ [25], $D_8^{(4)}$ [26] or $V_8^{(0)}$ [27].

4 New Isolated Matrix $A_8^{(0)}$

Using the random walk procedure with additional constraint for H to be symmetric we were able to find the following matrix:

$$A_8^{(0)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -a^2 & -1 & a^2 & a & -a & -a & a \\ 1 & -1 & -1 & -a & 1/a & 1 & -1/a & a \\ 1 & a^2 & -a & a & -1 & a & -a & -a^2 \\ 1 & a & 1/a & -1 & 1 & -1 & -1/a & -a \\ 1 & -a & 1 & a & -1 & 1/a & -1/a & -1 \\ 1 & -a & -1/a & -a & -1/a & -1/a & 1 & -a \\ 1 & a & a & -a^2 & -a & -1 & -a & a^2 \end{bmatrix}, \quad (4.1)$$

with $a = \frac{1}{3} + i \frac{2\sqrt{2}}{3}$ being a solution of the equation $3a^2 - 2a + 3 = 0$.

The matrix is not of the Butson type for its elements are incommensurate with any root of unity. Its defect value is 0 thus the matrix is isolated and no family can stem from it. Obviously, this matrix does not touch any objects discussed above.

5 Concluding Remarks

In this paper we have found two previously unknown objects from the set of complex Hadamard matrices $\mathcal{H}_8$ of size 8—the isolated matrix $A_8^{(0)}$ which is not of the Butson type and 1-parametric, non-affine family of inequivalent matrices $T_8^{(1)}$. This does not provide complete classification of the case $N = 8$ but hopefully will help to develop another ideas to describe a full structure of $\mathcal{H}_8$. Generic defect of $T_8^{(1)}$ is 3 so it might be a part of a higher dimensional structure. An imposing question is whether there exist any other 8-dimensional families which possibly connect some of currently known non-isolated elements of $\mathcal{H}_8$.

Acknowledgements The author is indebted to Dardo Goyeneche, Ferenc Szöllősi, Konrad Szymański and Karol Życzkowski for helpful discussions. Furthermore, the author would like to thank the anonymous referee for several remarks that allowed to improve the paper significantly. Financial support by Narodowe Centrum Nauki under the *grant number* DEC-2015/18/A/ST2/00274 is gratefully acknowledged.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Craigen, R.: Equivalence classes of inverse orthogonal and unit Hadamard matrices. *Bull. Austral. Math. Soc.* **44**, 109–115 (1991)
2. Haagerup, U.: Orthogonal Maximal Abelian *-Subalgebras of the $n \times n$ Matrices and Cyclic n -roots, pp. 296–322. International Press, Cambridge (1996)
3. Seberry, J., Wysocki, B.J., Wysocki, T.: On some applications of Hadamard matrices. *Metrika* **62**, 221–239 (2005)
4. Werner, R.: All teleportation and dense coding schemes. *J. Phys. A* **34**, 7081–7094 (2001)
5. Heng, I., Cooke, C.H.: Error correcting codes associated with complex Hadamard matrices. *Appl. Math. Lett.* **11**, 77–80 (1998)
6. Godsil, C.D., Roy, A.: Equiangular lines, mutually unbiased bases, and spin models. *Eur. J. Comb.* **30**, 246–262 (2009)
7. Tadej, W., Życzkowski, K.: A concise guide to complex Hadamard matrices. *Open Syst. Inf. Dyn.* **13**, 133–177 (2006)
8. Szöllősi, F.: Exotic complex Hadamard matrices and their equivalence. *Cryptogr. Commun.* **2**, 187–198 (2010)
9. Tadej, W., Życzkowski, K.: Defect of a unitary matrix. *Linear Algebra Appl.* **429**(2–3), 447–481 (2008)
10. Butson, A.T.: Generalized Hadamard matrices. *Proc. AMS* **13**, 894–898 (1962)
11. Butson, A.T.: Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences. *Can. J. Math.* **15**, 42–48 (1963)
12. Bruzda, W., Tadej, W., Życzkowski, K.: On-line Catalogue of Complex Harnard Matrices. <http://chaos.if.uj.edu.pl/~karol/hadamard/>. Accessed 25 Feb 2018
13. Zauner, G.: Ph.D. Thesis, University of Wien (1999)
14. Wootters, W., Fields, B.: Optimal state-determination by mutually unbiased measurements. *Ann. Phys.* **191**, 363–381 (1989)
15. Grassl, M.: On SIC-POVMs and MUBs in Dimension 6 (2009). [arXiv:quant-ph/0406175](https://arxiv.org/abs/quant-ph/0406175)
16. Szöllősi, F.: Complex Hadamard matrices of order 6: a four-parameter family. *J. Lond. Math. Soc.* **85**(3), 616–632 (2012)
17. Karlsson, B.R.: Three parameter complex Hadamard matrices of order 6. *Linear Algebra Appl.* **434**, 247–258 (2011)
18. Moorhouse, G.E.: The 2-Transitive Complex Hadamard Matrices (2001). <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.32.4884>. Accessed 25 Feb 2018
19. Tao, T.: Fuglede’s conjecture is false in 5 and higher dimensions. *Math. Res. Lett.* **11**, 251–258 (2004)
20. Björck, G., Fröberg, R.: A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n -roots. *J. Symb. Comput.* **12**, 329–336 (1991)
21. Szöllősi, F.: Ph.D. Thesis, CEU Hungary (2011)
22. Petrescu, M.: Ph.D. Thesis, UCLA (1997)
23. Lampio, P.H.J., Ostergård, P.R.J., Szöllősi, F.: Orderly Generation of Butson Hadamard Matrices (2017). [arXiv:1707.02287](https://arxiv.org/abs/1707.02287)
24. Lampio, P.H.J.: On-line Catalogue of Butson Matrices. <https://wiki.aalto.fi/display/Butson/Butson+Home>. Accessed 25 Feb 2018
25. Matolcsi, M., Réffy, J., Szöllősi, F.: Constructions of complex Hadamard matrices via tiling Abelian groups. *Open Syst. Inf. Dyn.* **14**, 247–263 (2006)
26. Diță, P.: Complex Hadamard Matrices from Sylvester Inverse Orthogonal Matrices (2010). [arXiv:0901.0982v3](https://arxiv.org/abs/0901.0982v3)
27. Elser, V.: Private communication (2011), <http://chaos.if.uj.edu.pl/~karol/hadamard/?q=0804>

Quantum measurements with prescribed symmetry

Wojciech Bruzda

Institute of Physics, Jagiellonian University, 30-348, Kraków, Poland

Dardo Goyeneche

Institute of Physics, Jagiellonian University, 30-348, Kraków, Poland

and Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-233 Gdańsk, Poland

Karol Życzkowski

Institute of Physics, Jagiellonian University, 30-348, Kraków, Poland

and Center for Theoretical Physics, Polish Academy of Sciences, 02-668, Warsaw, Poland

(Received 28 April 2017; published 3 August 2017)

We introduce a method to determine whether a given generalized quantum measurement is isolated or if it belongs to a family of measurements having the same prescribed symmetry. The technique proposed reduces to solving a linear system of equations in some relevant cases. As a consequence, we provide a simple derivation of the maximal family of symmetric informationally complete positive operator-valued measure SIC-POVM in dimension 3. Furthermore, we show that the following remarkable geometrical structures are isolated, so that free parameters cannot be introduced: (a) maximal sets of mutually unbiased bases in prime power dimensions from 4 to 16, (b) SIC-POVM in dimensions from 4 to 16, and (c) contextual Kochen-Specker sets in dimension 3, 4, and 6, composed of 13, 18, and 21 vectors, respectively.

DOI: [10.1103/PhysRevA.96.022105](https://doi.org/10.1103/PhysRevA.96.022105)

I. INTRODUCTION

Positive operator-valued measure (POVM) is the most general kind of measurement in quantum mechanics, which generalizes projective measurements. Some POVMs having a prescribed symmetry play a crucial role in quantum mechanics: symmetric informationally complete (SIC)-POVM [1,2] and mutually unbiased bases (MUBs) [3,4]. These geometrical structures have important applications in quantum theory: SIC-POVM and MUBs allow us to unambiguously reconstruct any density matrix of size d [1,3] and define entropic uncertainty relations [5,6]. Even more, MUBs are important to detect entanglement [7] and bound entanglement [8], and to lock classical information in quantum states [9].

Finitely many SIC-POVMs are known in dimension $d \leq 64$ [10], including a one-parameter family in dimension 3 [1]. The existence of SIC-POVM with free parameters in dimension $d > 3$ is still an open problem. Moreover, maximal sets of MUBs are known to be isolated in dimensions 2–5 [11] and finitely many nonequivalent maximal sets of MUBs are known for dimensions 3–5 [12] and N qudit systems [13]. On the other hand, families of symmetric POVMs are useful for practical applications, as the parameters can be optimized for different convenient purposes. For example, from the one-parameter family of SIC-POVM existing in dimension 3 [1] only a single member maximizes the informational power, that is, the classical capacity of a quantum-classical channel generated by the SIC-POVM [14]. Furthermore, inequivalent sets of MUBs provide different estimation of errors in quantum tomography [15].

Highly symmetric quantum measurements, like SIC-POVM or MUBs, play an important role in quantum information and foundations of quantum theory. On the one hand, it is interesting itself to design a mathematical tool that allows one to construct a family of POVMs having a

prescribed symmetry from a given particular solution. On the other hand, construction of such families of solutions provides flexibility when designing experimental implementations of these measurement sets. For instance, a detailed description of a complete list of solutions of a set of k MUBs in dimension d may be helpful in tackling the problem whether an extended set of $k + 1$ MUBs exists. Furthermore, it is also interesting to highlight those quantum measurements having a prescribed symmetry that do not belong to a family, which makes them special. A possible application of such isolated cases is the existence of a unique solution optimizing a given function. For instance, isolated solutions might define sets of measurement having a unique maximal violation of a Bell inequality, which is a fundamental ingredient for *self-testing* [16].

In this work, we present a method to introduce free parameters in generalized measurements having a predefined geometrical structure. The method proposed divides the entire nonlinear problem, called $\mathcal{P}_{NL}^{(1)}$, into a linear problem $\mathcal{P}_L^{(2)}$ and a secondary nonlinear problem $\mathcal{P}_{NL}^{(3)}$, which is simpler than $\mathcal{P}_{NL}^{(1)}$. Remarkably, in some cases the linear problem $\mathcal{P}_L^{(2)}$ provides a definite answer to the full problem $\mathcal{P}_{NL}$.

The paper is organized as follows: In Sec. II we establish a connection between any given POVM and certain Hermitian unitary matrices having constant diagonal.

In Sec. III we apply the notion of a defect of a unitary matrix to identify isolated cases of generalized quantum measurements having a prescribed symmetry, for which no free parameters can be introduced. Furthermore, in other cases we present a constructive method to extend known solutions to an entire family by introducing free parameters.

In Sec. IV we show that known maximal sets of MUBs in dimensions 4, 8, 9, and 16 and known SIC-POVMs in dimensions 4–16 are isolated. We also study the robustness of our results for a given accuracy in specifying the POVM,

which allows us to derive conclusive results from approximate solutions. In Sec. V we find an upper bound for the maximal number of free parameters that can be introduced in sets of $2 \leq m \leq d + 1$ MUBs in dimension d and in some classes of equiangular tight frames. Moreover, we show how the method works to give the known one-parameter families of SIC-POVMs in dimension 3. In Sec. VI we prove that some existing Kochen-Specker sets from quantum contextuality are isolated. In Sec. VII we summarize our results and pose open questions.

II. QUANTUM MEASUREMENTS AND TIGHT FRAMES

A POVM $\{\Gamma_j\}$ is a set of N positive-semidefinite sub-normalized operators defined in dimension d such that $\sum_{j=0}^{N-1} \Gamma_j = \mathbb{I}_d$, where $\mathbb{I}_d$ is the identity matrix of size d . Throughout the work, we restrict our attention to rank-1 POVMs and consider rank-1 projectors Π_j , being proportional to the elements of POVM; that is, $\Pi_j = c\Gamma_j$, where $c = N/d$. For simplicity, we refer to the set of projectors $\{\Pi_j\}$ as a POVM, understanding that they are formally proportional to the elements of a POVM. The rank-1 projectors Π_j satisfy the geometrical relation

$$\text{Tr}(\Pi_i \Pi_j) = S_{ij}, \quad (1)$$

where S is a real symmetric matrix of size N . It is interesting to ask about the most general projectors having the prescribed symmetry (1) given by a real symmetric matrix S . For example, the case $S = \mathbb{I}_N + \frac{N-d}{d(N-1)}(\mathbb{J}_N - \mathbb{I}_N)$ corresponds to equiangular tight frames composed of N vectors in dimension d . Here, $\mathbb{J}_N$ denotes the matrix of size N having all entries equal to unity. We recall that a set of N vectors $\{|\phi_i\rangle\}$ defined in dimension d forms an equiangular tight frame (ETF) if $|\langle\phi_i|\phi_j\rangle|^2 = d(N-1)/(N-d)$, for every $i \neq j = 0, \dots, d^2 - 1$.

A remarkably important subclass of ETF is given by the so-called SIC-POVM [1], corresponding to the case $N = d^2$. Also, two orthonormal bases $|\phi_i\rangle$ and $|\psi_j\rangle$ in dimension d define a pair of MUBs if $|\langle\phi_i|\psi_j\rangle|^2 = 1/d$, for every $i, j = 0, \dots, d-1$. A set of m orthonormal bases is mutually unbiased if every pair of the set is mutually unbiased. Also, a set of m MUBs in dimension d has associated the symmetric matrix $S = \mathbb{I}_{dm} + \frac{1}{d}(\mathbb{J}_m - \mathbb{I}_m) \otimes \mathbb{J}_d$. For a recent review on discrete structures in Hilbert spaces, including MUBs and SIC-POVM, see Ref. [17].

Let us recall a close connection existing between POVM and *tight frames*. A set of rank-1 projectors $\{\Pi_j\}$ defines a tight frame if there exists a real number $A > 0$ such that $\sum_{j=0}^{N-1} \text{Tr}(\Omega \Pi_j) = A \text{Tr}(\Omega^2) = A$, for any rank-1 projector Ω acting on dimension d . Therefore, POVMs are tight frames for $A = c$. A crucial property for our work is the fact that the Gram matrix associated to a tight frame, or POVM, is closely related to an Hermitian unitary matrix, as we see in Proposition 1. We recall that the Gram matrix of a set of N vectors $|\phi_j\rangle$ is given by

$$G_{ij} = \langle\phi_i|\phi_j\rangle, \quad (2)$$

where $i, j = 0, \dots, N-1$. For example, the Gram matrix of an equiangular tight frame composed of N vectors in dimension

d has the form

$$G_{\text{ETF}} = \begin{pmatrix} 1 & re^{i\alpha_{12}} & \dots & re^{i\alpha_{1N}} \\ re^{-i\alpha_{12}} & 1 & \dots & re^{i\alpha_{2N}} \\ \vdots & \vdots & \ddots & \vdots \\ re^{-i\alpha_{1N}} & re^{-i\alpha_{2N}} & \dots & 1 \end{pmatrix}, \quad (3)$$

where $r^2 = d(N-1)/(N-d)$. Furthermore, the Gram matrix of a set of $m+1$ MUBs $\{\mathbb{I}_d, H_1, H_2, \dots, H_m\}$ in dimension d is given by

$$G_{\text{MUB}} = \begin{pmatrix} \mathbb{I}_d & H_1 & H_2 & \dots & H_m \\ H_1^\dagger & \mathbb{I}_d & H_1^\dagger H_2 & \dots & H_1^\dagger H_m \\ H_2^\dagger & H_2^\dagger H_1 & \mathbb{I}_d & \dots & H_2^\dagger H_m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ H_m^\dagger & H_m^\dagger H_1 & H_m^\dagger H_2 & \dots & \mathbb{I}_d \end{pmatrix}, \quad (4)$$

where $H_1, H_2, \dots, H_m$ are suitable unitary complex Hadamard matrices, so that $H_i H_i^\dagger = \mathbb{I}$ and $|(H_i)_{jk}|^2 = 1/d$ for every $j, k = 0, \dots, N-1$ and $i = 1, \dots, m$; see Ref. [18]. Let us establish a connection between Gram matrices of POVM and a special kind of unitary Hermitian matrices.

Proposition 1. Let Π_j be a rank-1 POVM composed of N vectors in dimension d and G be the corresponding Gram matrix. Then, the matrix $U = \mathbb{I}_N - \frac{2d}{N}G$ is unitary.

Proof. A Gram matrix G represents a POVM composed of N vectors in dimension $d \leq N$ if and only if $G^2 = \frac{N}{d}G$ (cf. Proposition 1 in Ref. [19]). From this property and taking into account that $\text{Tr}(G) = N$, the spectrum of G satisfies

$$\lambda(G) = \underbrace{(N/d, \dots, N/d)}_d, \underbrace{(0, \dots, 0)}_{N-d}. \quad (5)$$

Therefore, $U = \mathbb{I}_N - \frac{2d}{N}G$ is a unitary matrix. ■

From Proposition 1 we realize that the existence of a POVM with a symmetry prescribed by the matrix S from Eq. (1) is equivalent to prove the existence of a unitary Hermitian matrix U having positive constant diagonal $U_{ii} = 1 - 2d/N$ and satisfying $|U_{ij}| = \frac{2d}{N}\sqrt{S_{ij}}$ for $i \neq j$. Unitary matrices $U = \mathbb{I}_N - \frac{2d}{N}G$ have been recently studied for the particular case of equiangular tight frames [20]. In the Bloch sphere associated to a one-qubit system we have some relevant geometrical structures: the orthonormal basis (line), three MUBs (three orthogonal lines), and SIC-POVM (tetrahedron). All these structures are unique, up to a global rotation. In higher dimensions, however, some geometrical structures allow one to introduce free parameters, which cannot be absorbed in a global rotation. In Sec. III we introduce the method which considerably simplifies the study of this problem.

III. RESTRICTED DEFECT AND FREE PARAMETERS

In this section, we derive the method to introduce the maximal possible number of free parameters into a given POVM composed by N vectors in dimension d associated to a given symmetric matrix S ; see Eq. (1). Using Proposition 1, this problem is equivalent to finding the most general real antisymmetric matrix R of size N such that

$$V_{ij}(t) = U_{ij}e^{itR_{ij}} \quad (6)$$

is a unitary matrix, provided that $U = \mathbb{I}_N - \frac{2d}{N}G$ is associated to a given particular POVM satisfying Eq. (1); that is, U is an Hermitian unitary matrix having constant diagonal $U_{ii} = 1 - 2d/N$ and $|U_{ij}| = \delta_{ij} - \frac{2d}{N}\sqrt{S_{ij}}$. Note that we have introduced a parameter t in Eq. (6) for convenience, which can be set to $t = 1$ after applying our method. The full problem is given as follows:

Problem $\mathcal{P}_{NL}^{(1)}$. Find the most general matrix $V_\tau(t)$ of size N of the form of Eq. (6), initially depending on τ parameters, such that

$$V_\tau(t)V_\tau(t)^\dagger = \mathbb{I}_N. \quad (7)$$

This problem implies solving a system of nonlinear coupled equations, which depends on $\tau = [N(N-1)/2 - z] - (N-1)$ nontrivial variables, where z is the number of zeros existing in the strictly upper triangular part of the matrix R . Note that τ is composed of the total number of parameters R_{ij} , i.e., $N(N-1)/2 - z$, minus the number of trivial variables $(N-1)$. These trivial parameters can be absorbed by applying the transformation $V \rightarrow EVE^\dagger$, where $E = \text{Diag}(1, e^{itR_{01}}, \dots, e^{itR_{0(N-1)}})$. In order to simplify the resolution of problem $\mathcal{P}_{NL}$ we define the following linear problem:

Problem $\mathcal{P}_L^{(2)}$. Find the most general matrix $V_\tau(t)$ of size N , initially depending on τ parameters, such that

$$\lim_{t \rightarrow 0} \frac{d}{dt} [V_\tau(t)V_\tau(t)^\dagger] = 0. \quad (8)$$

Using Eq. (6), we can explicitly write Eq. (8) as

$$-2V_{k,k}V_{k,j}R_{j,k} + \sum_{l \neq j,k} V_{k,l}V_{l,j}(R_{k,l} - R_{j,l}) = 0, \quad (9)$$

for $1 \leq j < k \leq N$ and $1 \leq l \leq N$, which is a linear problem on variables R_{ij} . Note that $\mathcal{P}_L^{(2)} \subset \mathcal{P}_{NL}^{(1)}$, as Eq. (8) is a necessary condition to obtain Eq. (7).

The linear problem $\mathcal{P}_L^{(2)}$ allows us to simplify the full problem $\mathcal{P}_{NL}$ by determining r out of τ variables R_{ij} , where r is the number of linearly independent equations (9). After solving $\mathcal{P}_L^{(1)}$, the remaining number of free parameters R_{ij} lead us to the definition of the *restricted defect* Δ of the Hermitian unitary matrix U . It reads

$$\Delta = \tau - r, \quad (10)$$

where $\tau = (N-1)(N-2)/2 - z$ and z is the number of zeros existing in the strictly upper triangular part of the matrix U . Note that this quantity is closely related to the defect of a unitary matrix [21], adapted to the case of matrices with a special structure. The standard defect was used to define an upper bound on the number of free parameters allowed by complex Hadamard matrices [18] and forms, by construction, an upper bound for the restricted defect. In both cases, the defect equal to zero implies that a given solution is isolated, so no free parameters can be introduced.

In general, the restricted defect represents an upper bound for the maximal number of free parameters allowed by the full problem $\mathcal{P}_{NL}$. If $\Delta = 0$, then the full problem $\mathcal{P}_{NL}$ is solved by the linear problem $\mathcal{P}_L^{(1)}$. In this case, it is not possible to introduce free parameters into the matrix V . On the other hand, if $\Delta > 0$, it is necessary to solve an additional

nonlinear problem in order to determine the continuous family of solutions.

Problem $\mathcal{P}_{NL}^{(3)}$. Find the most general matrix $V_\Delta(t)$ of size N , initially depending on Δ parameters, such that

$$V_\Delta(t)V_\Delta(t)^\dagger = \mathbb{I}_N. \quad (11)$$

Note that problem $\mathcal{P}_{NL}^{(2)}$ is simpler than problem $\mathcal{P}_{NL}$ as $\Delta < \tau$. This is so because $r > 0$ in Eq. (10). After solving problem $\mathcal{P}_{NL}^{(2)}$ we can assume that $t = 1$, without loss of generality. In Sec. IV we apply our results to SIC-POVM and maximal sets of MUBs.

Let us first illustrate the method in action by considering two MUBs for a single-qubit system: $|\phi_i\rangle = |i\rangle$, $i = 0, 1$, and $|\psi_\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The Gram matrix (4) associated to this set of $m = 2$ MUBs is given by

$$G_{\text{MUB}} = \frac{1}{2} \begin{pmatrix} 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & -1 \\ 1 & 1 & 2 & 0 \\ 1 & -1 & 0 & 2 \end{pmatrix}. \quad (12)$$

A family of two MUBs stemming from this fixed set would have associated a Gram matrix of the form

$$G_{\text{MUB}} = \frac{1}{2} \begin{pmatrix} 2 & 0 & e^{itR_{13}} & e^{itR_{14}} \\ 0 & 2 & e^{itR_{23}} & -e^{itR_{24}} \\ e^{-itR_{13}} & e^{-itR_{23}} & 2 & 0 \\ e^{-itR_{14}} & -e^{-itR_{24}} & 0 & 2 \end{pmatrix}, \quad (13)$$

and, from Proposition 1, the unitary matrix $U = \mathbb{I}_N - \frac{2d}{N}G_{\text{MUB}}$. Note that the full problem $\mathcal{P}_{NL}^{(1)}$ initially depends on $\tau = 1$ nontrivial parameter, as R_{13} , R_{14} , and R_{23} can be absorbed by considering the diagonal unitary operator $E = \text{diag}[1, e^{-iR_{23}}, e^{iR_{13}}, e^{iR_{14}}]$ and the redefinition $V \rightarrow EVE^\dagger$. Therefore, according to Eq. (6), and after considering the diagonal transformation E , we find that

$$V_\tau(t) = \frac{1}{2} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -e^{itR_{24}} \\ 1 & 1 & 0 & 0 \\ 1 & -e^{-itR_{24}} & 0 & 0 \end{pmatrix}. \quad (14)$$

Problem $\mathcal{P}_L^{(2)}$ implies the following equation:

$$R_{24} = 0, \quad (15)$$

where $r = 1$ and, therefore, $\Delta = 0$. Thus, we cannot introduce free parameters in Eq. (14), which implies that the considered pair of MUBs is isolated. Indeed, $|\phi_i\rangle = |i\rangle$, $i = 0, 1$, and $|\psi_\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ is the unique pair of MUBs existing in dimension 2, up to a global rotation [11].

IV. ISOLATED MUB AND SIC-POVM

In this section, we study the problem of introducing free parameters in MUB and SIC-POVM. Our first main result consists in proving that maximal sets of MUBs exist in low prime power dimensions.

Proposition 2. Maximal sets of $d + 1$ MUBs in dimensions $d = 4, 8, 9$, and 16 are isolated.

The results arises as follows. The upper triangular part of the Gram matrix associated to a set of m MUBs in dimension d contains $z = md(d-1)/2$ zero entries. Given that the size

of the Gram matrix of the set is $N_{\text{MUB}} = md$ and $m = d + 1$ we have $z = d(d^2 - 1)/2$. Therefore, the matrix G contains $\tau = (N_{\text{MUB}} - 1)(N_{\text{MUB}} - 2)/2 - z$ parameters. The next step consists in determining how many of these parameters are remaining after solving the linear problem $\mathcal{P}_L^{(1)}$. To this end, we calculated the number of linearly independent equations of the linear system defined in Eq. (9) for the cases $d = 4, 8, 9$, and 16 , finding $r_4 = 141$, $r_8 = 2233$, $r_9 = 3556$, and $r_{16} = 34545$, respectively. By using these results and Eq. (10) we find that the restricted defect Δ vanished in all these cases. We based our calculation of the restricted defect Δ on the maximal sets of MUBs provided in Refs. [4,12]. In dimension $d = 9$, we considered Ref. [22] to obtain simpler expressions of results presented in Ref. [4].

Let us now consider the case of SIC-POVM. It is well known that SIC-POVM for a qubit system is essentially unique, as it represents the regular tetrahedron inscribed into the Bloch sphere, up to a global rotation. Furthermore, single-parameter families of SIC-POVM for a qutrit system exist [1], which represents the most general solution [23]. For higher dimensions, the problem of introducing free parameters in SIC-POVM is still open. As a preliminary result, exhaustive numerical simulations indicate that free parameters cannot be introduced in SIC-POVM, at least in low dimensions higher than three. For this problem, we have solved the linear problem $\mathcal{P}_L^{(1)}$ in dimensions $d = 4, \dots, 16$, obtaining the following results.

Proposition 3. SIC-POVMs in dimensions $d = 4, \dots, 16$ are isolated.

This result also includes the *Hoggar lines* [24], a special class of SIC-POVM defined in dimension $d = 8$. We considered the total number of parameters $\tau = (N_{\text{SIC}} - 1)(N_{\text{SIC}} - 2)/2$, as there is no pair of orthogonal vectors in SIC-POVM ($z = 0$), and $N_{\text{SIC}} = d^2$. In order to prove Proposition 3 we solved the linear problem $\mathcal{P}_L^{(1)}$ for both analytical [24–28] and highly accurate numerical SIC-POVMs [10]. In all the cases we have found $\Delta = 0$, which implies that free parameters cannot be introduced. Calculations of the restricted defect have been done in MATLAB.

Let us now study the robustness of the restricted defect Δ under the presence of inaccuracies in describing the POVM. Given the set of vectors $\{\phi_j\}$ defined in Eq. (2) we quantify the inaccuracy in approximate vectors $\{\phi'_j\} \approx \{\phi_j\}$ by introducing the inaccuracy factor:

$$s = \frac{1}{\sqrt{d}} \max_j \|\phi'_j - \phi_j\|. \quad (16)$$

The factor s_μ quantifies the maximal allowed inaccuracy in entries of vectors ϕ_j . For example, in the case of approximate solutions $\{\phi'_j\}$ having k digits of precision we have $s \approx 10^{-k}$. In our study of robustness of the defect Δ , we simulate the introduction of inaccuracies by considering

$$(\phi'_j)_i = (\phi_j)_i + s\xi_i, \quad (17)$$

where $(x)_i$ denotes the i th entry of the vector x and ξ_i are random numbers uniformly distributed in the interval $[-1, 1]$.

Let us assume that $\mathcal{R}$ is the real matrix associated to the linear system of equations (9). Note that the number of linearly independent equations of such a system is given by $\text{rank}(\mathcal{R}) = r$. When considering inaccuracies in the POVM the

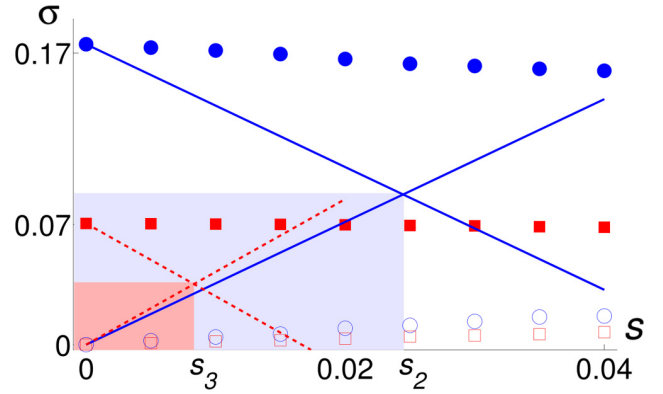


FIG. 1. Smallest singular values σ_0 and σ_1 of $\mathcal{R}$ as a function of the inaccuracy factor s for SIC-POVM. Open and solid symbols represent σ_0 and σ_1 , respectively, for two- ($\circ$) and three-qubit ($\square$) systems. Each case is averaged over eight samples randomly chosen and generated from the approximate SIC-POVM provided in Ref. [10], which has accuracy $s = 1 \times 10^{-32}$. The confidence regions (blue and red rectangles) are given by values of s existing between zero and the value determined by the intersection of the lower and upper bounds. Here, s_2 and s_3 stand for two- and three-qubits systems, respectively. Outside the confidence regions it is not possible to discriminate between singular values σ_0 and σ_1 .

rank of the perturbed matrix $\mathcal{R}'$ and $\mathcal{R}$ may differ. Therefore, we need to study how much the singular values of $\mathcal{R}'$ are affected under the presence of inaccuracies. In particular, we are interested in the perturbation of the two smallest singular values $\sigma_0 = 0$ and $\sigma_1 > 0$, which are responsible for the variation of the rank. In order to obtain a confidence region for the restricted defect (10) we need to consider the following two bounds: (i) an upper bound for the maximal perturbation of σ_0 and (ii) a lower bound for the maximal perturbation of σ_1 . In Appendix we show that

$$|\sigma'_i - \sigma_i| \leq f(d, N) s \quad (18)$$

for $i = 0, 1$, where s is the inaccuracy quantifier defined in Eq. (16) and

$$f(d, N) = \frac{2^6 d^2}{N} \left(1 - \frac{2d}{N}\right)^2 \sqrt{\frac{N-d}{N(N-1)}} \quad (19)$$

for $N > 2d$. Let us now find the smallest possible value of s such that the critical condition $\sigma'_0 = \sigma'_1$ holds, which imposes an upper bound for the confidence region of the restricted defect Δ . By considering Eq. (18) we find that Δ does not change its value for $0 \leq s \leq s_{\text{max}}$, where $s_{\text{max}} = \sigma_1(2f(d, N))^{-1}$. Note that σ_1 depends on the exact solution, which is not known if the exact solution is not available. By using Eq. (18) we find that $\sigma_1 \leq \sigma'_1 + f(d, N) s$, which implies

$$s_{\text{max}} \leq \frac{\sigma'_1 + f(d, N) s}{2f(d, N)}. \quad (20)$$

Note that this inequality provides a confidence region only if $f(d, N) s \ll 1$.

Confidence regions for SIC-POVM and maximal sets of MUBs for two and three qubits are depicted in Figs. 1 and 2, respectively. For the case of four-qubit systems we

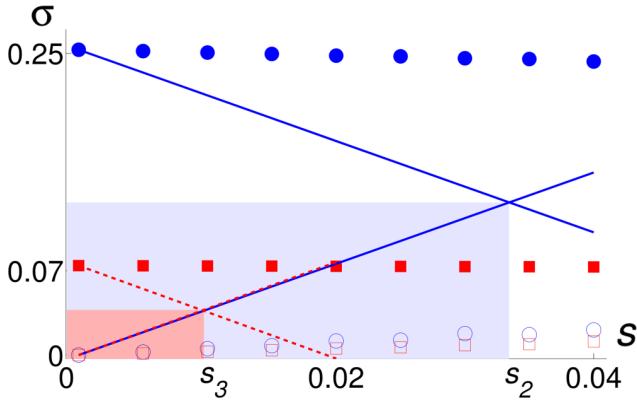


FIG. 2. Smallest singular values σ_0 and σ_1 of $\mathcal{R}$ as a function of the inaccuracy factor s for maximal sets of MUBs. Open and solid symbols represent σ_0 and σ_1 , respectively, for two- ($\circ$) and three-qubit ($\square$) systems. Each case is averaged over eight samples randomly chosen and generated from analytic solutions.

have solutions with precision $s = 1 \times 10^{-32}$, whereas the upper bound for the confidence region is $s_4 \approx 4 \times 10^{-3}$. For MUBs, we calculated the restricted defect Δ by considering analytic solutions in all the cases [4,12,22].

V. FREE PARAMETERS IN MUB AND SIC-POVM

In Sec. IV we prove that some maximal sets of MUBs and SIC-POVMs are isolated in low dimensions. In this section, we first calculate the restricted defect for sets of $m = 2, \dots, d+1$ MUBs in dimensions $d = 2, \dots, 8$ (see Table I). Interestingly, the restricted defect for a pair of MUBs B_1 and B_2 coincides with the standard defect of the complex Hadamard matrix $H = B_1^\dagger B_2$. Indeed, the maximal number of free parameters that can be introduced in the Gram matrix

$$G_{\text{MUB}} = \begin{pmatrix} \mathbb{I}_d & H \\ H^\dagger & \mathbb{I}_d \end{pmatrix} \quad (21)$$

TABLE I. Upper bound on the maximal number of free parameters Δ allowed by subsets of m MUBs in dimension d . The results do not depend on selecting m subsets of MUBs out of the full set of $d+1$ MUBs. As a remarkable observation, maximal sets of MUBs are isolated. Also, subsets of $m \geq 6$ in dimension 8 and $m \geq 5$ MUBs in dimension 9 are isolated in all the cases. Question marks denote our lack of knowledge about given number of MUB, while $\diamond$ indicates the case of three MUBs in dimension 6, which is still considered unresolved.

$m \setminus d$	2	3	4	5	6	7	8	9
2	0	0	3	0	4	0	21	16
3	0	0	3	0	$\diamond$	0	27	20
4		0	0	0	?	0	19	32
5			0	0	?	0	7	0
6				0	?	0	0	0
7					?	0	0	0
8						0	0	0
9							0	0
10								0

coincides with the maximal number of parameters that can be introduced in H . Let us explain some details concerning Table I. First, note that $\Delta = 0$ for every subset of $2 \leq m \leq d+1$ MUBs in prime dimensions $d = 2, 3, 5, 7$. This is so because every complex Hadamard matrix involved in the set is equivalent to the Fourier matrix, which is isolated in prime dimensions [18]. For triplets in dimension 4, we have $\Delta = 3$, which coincides with the maximal number of free parameters that can be introduced [11]. The number of generic restricted defects for a pair of MUBs in dimension 6 is four, coinciding with the generic defects of complex Hadamard matrices of size 6 [21]. However, note that there is an exceptional pair of MUBs for which $\Delta = 0$, as an isolated complex Hadamard matrix of size 6 exists [29]. Generic defects for triplets of MUBs are not well understood ($\diamond$); see Table I and Ref. [30].

In dimensions 8 and 9 we restricted our attention to subsets of MUBs arising from the maximal sets defined in Refs. [4,12]. Note that subsets of $m \geq 6$ MUBs are isolated in dimension 8, whereas several families of $m = 5$ MUBs exist [31]. Another observation is that the restricted defect Δ for maximal sets of $d+1$ MUBs in dimension d coincides with the defect for d MUBs. This is so because the $(d+1)$ th MUB is univocally determined by the first d MUBs. For subsets of $m < d$, the restricted defect for m MUBs may depend on the subset chosen. However, results presented in Table I are consistent for every subset of MUB.

We also studied the restricted defect for equiangular tight frames composed of $N = k^2$ vectors in dimension $d = k(k-1)/2$, typically denoted as ETF(d, N) [32]. These ETFs have associated the following Hermitian unitary matrices [20]:

$$U_{i_1 + ki_2 + 1, j_1 + kj_2 + 1} = \omega^{i_1 j_2 - j_1 i_2}, \quad (22)$$

where $i_1, i_2, j_1, j_2 \in \{0, \dots, k-1\}$ and $\omega = e^{2\pi i/k}$. Matrix (22) is equivalent to the tensor product of Fourier matrices, $F_k \otimes F_k$, where $(F_k)_{st} = \omega^{st}$. Table II summarizes the restricted defect for matrix U in low dimensions. Results are shown in Table II. For prime values of k , the formula

$$\Delta = \frac{1}{2}(k+1)(k-1)(k-2) \quad (23)$$

matches all solutions presented in Table II, so we are tempted to believe that it holds for any prime k .

Let us now study the SIC-POVM problem in dimension $d = 3$. By considering the fiducial state $|\phi_{00}\rangle = (1, -1, 0)/\sqrt{2}$ a

TABLE II. Maximal number of free parameters that can be introduced in ETF composed by $N = k^2$ vectors in dimension $d = k(k-1)/2$. The case $k = 2$ corresponds to an ETF(3,4) which is isolated (regular simplex in dimension 3). Also, $k = 3$ has associated a SIC-POVM in dimension 3, where $\Delta = 4$ but only two-parameter families exist [1]. For the case $k = 4$ there exists several six-parameter families of ETF(6,16) [20].

k	Δ	k	Δ	k	Δ
2	0	7	120	12	1237
3	4	8	273	13	924
4	21	9	352	14	1632
5	36	10	576		
6	112	11	540		

SIC-POVM is given by [25]

$$|\phi_{st}\rangle = X^s Z^t |\phi_{00}\rangle, \quad (24)$$

where $X|j\rangle = |[j \oplus 1]\rangle$, $Z|j\rangle = \omega^j |j\rangle$, $\omega = e^{2\pi i/3}$, and $\oplus$ means addition modulo 3. The 9×9 Gram matrix G_{SIC} of the SIC-POVM and its associated unitary matrix $U = \mathbb{I}_N - \frac{2d}{N} G_{\text{SIC}}$ depends on $\tau = 36 - 8 = 28$ parameters, where the $N - 1 = 8$ trivial parameters $R_{1,j}$ for $j = 2, \dots, 9$ have been set as zero. The linear system of equations (8) associated with problem $\mathcal{P}_L^{(1)}$ has $r = 24$ linearly independent equations, which provides a four-dimensional complex set of solutions R_{ij} , depending on four parameters: R_{23} , R_{26} , R_{48} , and R_{89} . The additional restriction to have real parameters implies

$$R_{23} - 3R_{89} = R_{23} - 3R_{26} = R_{89} - R_{26} = 0,$$

which is equivalent to $R_{26} = R_{89} = R_{23}/3$. After setting $t = 1$, we obtain three solutions to problem $\mathcal{P}_L^{(1)}$: $V_\Delta(R_{23}, R_{48})$, $V_\Delta(R_{26}, R_{48})$, and $V_\Delta(R_{89}, R_{48})$. Now, we are in position to solve the nonlinear problem $\mathcal{P}_{NL}^{(2)}$, which is much simpler than the full nonlinear problem $\mathcal{P}_{NL}$. Indeed, $\mathcal{P}_{NL}^{(2)}$ implies solving trivial trigonometric equations, which give us the solutions $R_{26} \in \{0, \pi\}$, $R_{89} \in \{0, \pi\}$, and $R_{23} \in \{0, \pi\}$, respectively. Therefore, we generate six one-parameter families of SIC-POVM in dimension 3:

$$\begin{aligned} \mathcal{S}_1 : V_\Delta(R_{23} = 0, R_{48}), \quad \mathcal{S}_2 : V_\Delta(R_{23} = \pi, R_{48}), \\ \mathcal{S}_3 : V_\Delta(R_{26} = 0, R_{48}), \quad \mathcal{S}_4 : V_\Delta(R_{26} = \pi, R_{48}), \\ \mathcal{S}_5 : V_\Delta(R_{89} = 0, R_{48}), \quad \mathcal{S}_6 : V_\Delta(R_{23} = \pi, R_{48}). \end{aligned} \quad (25)$$

Here we note that $\Delta = 4$ and six one-parameter real solutions exist. These six solutions belong to the four-dimensional tangent plane defined by Eq. (8) and do not fit into a lower-dimensional tangent space, which explains why Δ cannot take a lower value. Furthermore, solutions (25) are equivalent, in the sense that we can transform one into the other by applying a permutation of rows or columns and multiplication of diagonal unitary operations to the Gram matrix, which is equivalent to relabeling and applying global phases to vectors. Solution (25) represents the most general SIC-POVM existing in dimension 3 [23], up to equivalence. We remark that the generic Hermitian defect for a SIC-POVM in dimension 3 is $\Delta = 2$, with the only exception of the particular vector $|\phi_{00}\rangle$, where $\Delta = 4$; however, from this fact we cannot define a larger family.

VI. ISOLATED KOCHEN-SPECKER SETS

In this section, we apply our method presented in Sec. III to show that some sets of vectors used in a proof of the Kochen-Specker contextually theorem [33], typically called KS sets, are isolated.

KS sets are collections of N vectors in dimension d , which contain m subsets of d vectors forming orthonormal basis. Some of these orthonormal bases have common vectors, so that $N < md$. These intersections are crucial to prove that a deterministic local hidden variable theory is not possible [33]. That is, for a system prepared in a quantum state ρ and a set of KS vectors $\{\phi_0, \dots, \phi_{N-1}\}$ it is not possible to end up with N deterministic probabilities $P_k = \text{Tr}(\rho |\phi_k\rangle\langle\phi_k|) \in \{0, 1\}$, for $k = 0, \dots, N - 1$. Therefore, the assumption of hidden determinism in quantum mechanics implies that predefined values

TABLE III. Isolated KS sets composed of 13 vectors in dimension 3, 18 vectors in dimension 4, and 21 vectors in dimension 6. The number of zeros (z) appearing into the upper triangular part of the Gram matrix of the KS set, total number of parameters (τ), rank of the linear system defined in Eq. 8 (r), and restricted defect ($\Delta = \tau - r$) are defined in Sec. III. For these three KS sets the free parameters produced by a positive restricted defect Δ can be absorbed as global phases of the vectors.

N	d	z	τ	r	Δ	No. free parameters
13	3	24	78	66	12	0
18	4	63	90	83	7	0
21	6	105	105	103	2	0

of observables depend on the context in which measurements were implemented. The original proof given by Kochen and Specker involves $N = 117$ vectors in dimension $d = 3$ [33]. Subsequently, examples exhibiting a lower number of vectors were found. Some remarkable examples are KS sets composed of $N = 13$ vectors in dimension $d = 3$ [34], $N = 18$ vectors in dimension $d = 4$ [35], and $N = 21$ vectors in dimension $d = 6$ [36].

Let us now apply our method to prove that these three inequivalent KS sets are isolated. The first important observation is that the three KS sets form three POVMs. This means that Proposition 1 holds for these sets and, therefore, the method to introduce free parameters presented in Sec. III can be applied. In order to do so we have to calculate the restricted defect Δ defined in Eq. (10), which is a function of the total number of parameters τ and the number of linearly independent equations associated to problem $\mathcal{P}_L^{(2)}$ (see Sec. III). The geometrical structure is determined by the orthogonality restrictions imposed by the KS sets. For the above-mentioned three KS sets we have shown that they are isolated. The way to proceed is similar to the proof that maximal sets of MUBs or SIC-POVMs are isolated (see Proposition 2). However, there is a minor additional remark: the sets are isolated despite that the restricted defect Δ of the sets is nonzero. This is so because the apparently remaining Δ free parameters can be absorbed by considering a sequence of nontrivial emphasizing in the Gram matrices, which means that the free parameters can be absorbed as global phases of the KS vectors. Table III resumes the details of our calculations.

VII. CONCLUSION

We studied the problem to introduce free parameters in a given POVM having prescribed symmetry, where mutually unbiased bases (MUBs) and symmetric informationally complete-positive operator-valued measurement (SIC-POVM) are relevant examples (see Sec. II). In particular, our method allows us to determine whether a given quantum t design having prescribed symmetry [25] forms an isolated structure. We introduced a powerful method that divides this fully nonlinear problem into a linear problem and a simpler nonlinear problem (see Sec. III).

Using our method, we proved that known maximal sets of MUBs in dimensions 4, 8, 9, and 16 and known SIC-POVM in dimensions 4–16 are isolated. In particular, a special class

of SIC-POVM existing for three-qubit systems, called Hoggar lines, is isolated (see Sec. IV). Moreover, we calculated an upper bound for the maximal number of free parameters that can be introduced in subsets of $2 \leq m \leq d+1$ MUBs in dimensions $d = 2-9$ (see Sec. V). The same study has been done for equiangular tight frames in low dimensions, which define equiangular POVM (see Table II).

As a further result, we studied the robustness of our method under the presence of inaccuracies in defining the generalized measurement, which allowed us to establish a confidence region for the maximal possible number of free parameters that can be introduced (see Sec. IV). The importance of robustness relies on the fact that some geometrical structures, like SIC-POVM, are established analytically in low dimension only, whereas accurate numerical solutions exist in every dimension $d \leq 121$ and also in $d = 124, 143, 147, 168, 172, 195, 199, 228, 259$, and 323 [10,37].

Additionally, we proved that three Kochen-Specker contextuality sets are isolated (see Sec. VI). Namely, 13 vectors in dimension 3 [34], 18 vectors in dimension 4 [35], and 21 vectors in dimension 6 [36].

Finally, we pose some intriguing open questions: (i) Are maximal sets of MUBs isolated in every prime power dimension? (ii) Are SIC-POVMs isolated in every dimension $d > 3$? Furthermore, it would be welcome to develop a more efficient software to solve the linear problem $\mathcal{P}_L^{(1)}$ for POVMs having $N > 300$ elements, e.g., maximal sets of MUBs or SIC-POVM in dimension $d > 16$.

A MATLAB source code to support calculation of the restricted defect and additional features is available on the GitHub platform: <https://github.com/matrix-toolbox/defect>.

ACKNOWLEDGMENTS

We are grateful to Markus Grassl for his advice to study the robustness of the Hermitian defect under the presence of inaccuracies, to Wojciech Tadej for discussions and fruitful correspondence concerning the restricted defect of a unitary matrix, and to Ingemar Bengtsson for discussions about the restricted defect for SIC-POVM in dimension 3. Financial support by Narodowe Centrum Nauki under Grant No. DEC-2015/18/A/ST2/00274 and by the John Templeton Foundation under Project No. 56033 is gratefully acknowledged. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation.

APPENDIX: ROBUSTNESS OF RESTRICTED DEFECT

In this Appendix we derive the function $f(d, N)$ which appears in Eq. (18) and allows us to show that the restricted defect of a unitary matrix associated to a given generalized

measurement is stable with respect to small perturbations. Consider a set of vectors ϕ_j and the approximate vectors $\phi'_j = \phi_j + \delta\phi_j$. The perturbed Gram matrix is given by

$$(G + \delta G)_{ij} = \langle \phi_i + \delta\phi_i | \phi_j + \delta\phi_j \rangle \\ \approx \langle \phi_i | \phi_j \rangle + \langle \delta\phi_i | \phi_j \rangle + \langle \phi_i | \delta\phi_j \rangle,$$

which implies that

$$|\delta G_{ij}| \leq \|\phi_i\| \|\delta\phi_i\| + \|\phi_j\| \|\delta\phi_j\| \leq 2\sqrt{d} s. \quad (\text{A1})$$

Here, we used Eq. (16). Also, from $U = \mathbb{I} - \frac{2d}{N}G$ we have $|\delta U_{ii}| = 0$ and $|\delta U_{ij}| \leq 4d^{3/2} s/N$ for $i \neq j$. Let us now calculate the perturbations on entries of the matrix $\mathcal{R}$, which defines the system of equations (9). It is simple to show that if $N > 2d$ the maximal perturbations are produced by the entries of $\mathcal{R}_{jk} = -2U_{kk}U_{kj}$, associated to the left-hand term of Eq. (9). Therefore,

$$|\delta \mathcal{R}_{ij}| = 2|U_{kk}| |\delta U_{ij}| \leq 2 \left(1 - \frac{2d}{N}\right) \frac{4d^{3/2}}{N} s \\ \leq \frac{8d^{3/2}}{N} \left(1 - \frac{2d}{N}\right) s. \quad (\text{A2})$$

Using this result, we have

$$|\delta(\mathcal{R}^\dagger \mathcal{R})_{ij}| = |\delta(\mathcal{R}^\dagger)_{ij} \mathcal{R}_{ij} + (\mathcal{R}^\dagger)_{ij} \delta(\mathcal{R})_{ij}| \\ \leq 2 \max_{\mathcal{R}_{ij}} |\delta(\mathcal{R}^\dagger)_{ij} \mathcal{R}_{ij}| \\ \leq 2 \max_{\mathcal{R}_{ij}} |\delta(\mathcal{R}^\dagger)_{ij}| \max_{\mathcal{R}_{ij}} |\mathcal{R}_{ij}| \\ \leq \frac{2^6 d^{5/2}}{N^2} \left(1 - \frac{2d}{N}\right)^2 \sqrt{\frac{N-d}{d(N-1)}} s. \quad (\text{A3})$$

Now we are in position to estimate the maximal perturbation on the eigenvalues of $\mathcal{R}^\dagger \mathcal{R}$:

$$\lambda' = \lambda_k + \delta\lambda_k \approx \lambda_k + \langle \delta(\mathcal{R}^\dagger \mathcal{R}) \rangle. \quad (\text{A4})$$

From the Gerschgorin circle theorem [38] we have

$$|\langle \delta(\mathcal{R}^\dagger \mathcal{R}) \rangle| \leq \sum_{ij} |\delta(\mathcal{R}^\dagger \mathcal{R})_{ij}|. \quad (\text{A5})$$

From combining Eqs. (A3), (A4), and (A5) we find that $|\lambda'_i - \lambda_i| \leq f(d, N) s$, where

$$f(d, N) = \frac{2^6 d^{5/2}}{N^2} \left(1 - \frac{2d}{N}\right)^2 \sqrt{\frac{N-d}{d(N-1)}} s.$$

Given that $\mathcal{R}^\dagger \mathcal{R}$ is a positive operator, its eigenvalues λ_i coincide with its singular values σ_i . Therefore, $|\sigma'_i - \sigma_i| \leq f(d, N) s$, which proves Eq. (18).

- [1] J. Renes, R. Blume-Kohout, A. Scott, and C. Caves, Symmetric informationally complete quantum measurements, *J. Math. Phys.* **45**, 2171 (2004).
- [2] C. A. Fuchs, M. C. Hoang, and B. C. Stacey, The SIC question: History and state of play, *Axioms* **6**, 21 (2017).

- [3] I. D. Ivanovic, Geometrical description of quantal state determination, *J. Phys. A* **14**, 3241 (1981).
- [4] W. Wootters and B. Fields, Optimal state-determination by mutually unbiased measurements, *Ann. Phys.* **191**, 363 (1989).

- [5] S. Wu, S. Yu, and K. Mølmer, Entropic uncertainty relation for mutually unbiased bases, *Phys. Rev. A* **79**, 022104 (2009).
- [6] A. Rastegin, Uncertainty relations for MUBs and SIC-POVMs in terms of generalized entropies, *Eur. Phys. J. D* **67**, 269 (2013).
- [7] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. Hiesmayr, Entanglement detection via mutually unbiased bases, *Phys. Rev. A* **86**, 022311 (2012).
- [8] B. Hiesmayr and W. Löffler, Mutually unbiased bases and bound entanglement, *Phys. Scr.* **T160**, 014017 (2014).
- [9] M. Ballester and S. Wehner, Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases, *Phys. Rev. A* **75**, 022319 (2007).
- [10] A. Scott and M. Grassl, SIC-POVMs: A new computer study, *J. Math. Phys.* **51**, 042203 (2010).
- [11] S. Brierley, S. Weigert, and I. Bengtsson, All mutually unbiased bases in dimensions two to five, *Quantum Inf. Comput.* **10**, 0803 (2010).
- [12] A. Sehrawat and A. Klimov, Unitarily inequivalent mutually unbiased bases for n qubits, *Phys. Rev. A* **90**, 062308 (2014).
- [13] W. Kantor, MUBs inequivalence and affine planes, *J. Math. Phys.* **53**, 032204 (2012).
- [14] A. Szymusiak, Maximally informative ensembles for SIC-POVMs in dimension 3, *J. Phys. A: Math. Theor.* **47**, 445301 (2014).
- [15] J. Rehacek, Z. Hradil, A. Klimov, G. Leuchs, and L. Sanchez-Soto, Sizing up entanglement in mutually unbiased bases with Fisher information, *Phys. Rev. A* **88**, 052110 (2013).
- [16] D. Mayers and A. Yao, Self testing quantum apparatus, *Quantum Inf. Comput.* **4**, 273 (2004).
- [17] I. Bengtsson and K. Życzkowski, On discrete structures in finite Hilbert spaces, [arXiv:1701.07902](https://arxiv.org/abs/1701.07902).
- [18] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, *Open Syst. Inf. Dyn.* **13**, 133 (2006).
- [19] J. Tropp, I. Dhillon, R. Heath, Jr., and T. Strohmer, Designing structured tight frames via alternating projection, *IEEE Trans. Inf. Theory* **51**, 188 (2005).
- [20] D. Goyeneche and O. Turek, Equiangular tight frames and unistochastic matrices, *J. Phys. A: Math. Theor.* **50**, 245304 (2017).
- [21] W. Tadej and K. Życzkowski, Defect of a unitary matrix, *Linear Alg. Appl.* **429**, 447 (2008).
- [22] S. Chaturvedi, Aspects of mutually unbiased bases in odd prime power dimensions, *Phys. Rev. A* **65**, 044301 (2002).
- [23] F. Szöllősi, All complex equiangular tight frames in dimension 3, [arXiv:1402.6429](https://arxiv.org/abs/1402.6429).
- [24] S. Hoggar, 64 lines from a quaternionic polytope, *Geom. Dedicata* **69**, 287 (1998).
- [25] G. Zauner, Quantum designs: Foundations of a non-commutative design theory, Ph.D. thesis, University of Vienna, 1999; <http://www.gerhardzauner.at/documents/gz-quantumdesigns.pdf>
- [26] M. Grassl, On SIC-POVMs and MUBs in dimension 6, [arXiv:quant-ph/0406175](https://arxiv.org/abs/quant-ph/0406175).
- [27] D. Appleby, SIC-POVMs and the extended Clifford group, *J. Math. Phys.* **46**, 052107 (2005).
- [28] M. Grassl, Finding equiangular lines in complex space, <http://magma.maths.usyd.edu.au/Magma2006/>
- [29] I. Bengtsson, W. Bruzda, A. Ericsson, J. Larsson, W. Tadej, and K. Życzkowski, Mutually unbiased bases and Hadamards of order six, *J. Math. Phys.* **48**, 052106 (2007).
- [30] D. Goyeneche, Mutually unbiased triplets from non-affine families of complex Hadamard matrices in dimension six, *J. Phys. A: Math. Theor.* **46**, 105301 (2013).
- [31] D. Goyeneche and S. Gomez, Mutually unbiased bases with free parameters, *Phys. Rev. A* **92**, 062325 (2015).
- [32] M. Fickus and D. G. Mixon, Tables of the existence of equiangular tight frames, [arXiv:1504.00253](https://arxiv.org/abs/1504.00253).
- [33] S. Kochen and E. Specker, *J. Math. Mech.* **17**, 59 (1967).
- [34] S. Yu and C. Oh, State-Independent Proof of Kochen-Specker Theorem with 13 Rays, *Phys. Rev. Lett.* **108**, 030402 (2012).
- [35] A. Cabello, J. Estebarez, and G. Garcia Alcaide, Bell-Kochen-Specker theorem: A proof with 18 vectors, *Phys. Lett. A* **212**, 183 (1996).
- [36] P. Lisonek, P. Badziąg, J. Portillo, and A. Cabello, Kochen-Specker set with seven contexts, *Phys. Rev. A* **89**, 042101 (2014).
- [37] A. J. Scott, SICs: Extending the list of solutions, [arXiv:1703.03993](https://arxiv.org/abs/1703.03993).
- [38] S. Gerschgorin, Über die Abgrenzung der Eigenwerte einer Matrix, *Izv. Akad. Nauk. USSR Otd. Fiz.-Mat. Nauk*, **6**, 749 (1931).

Thirty-six entangled officers of Euler: Quantum solution to a classically impossible problem

Suhail Ahmad Rather,^{1,*} Adam Burchardt,^{2,*} Wojciech Bruzda,²
Grzegorz Rajchel-Mieldzioć,³ Arul Lakshminarayan,¹ and Karol Życzkowski^{2,3}

¹Department of Physics, Indian Institute of Technology Madras, Chennai 600036, India

²Institute of Theoretical Physics, Jagiellonian University, ul. Łojasiewicza 11, 30-348 Kraków, Poland

³Center for Theoretical Physics, Polish Academy of Sciences, Al. Lotników 32/46, 02-668 Warszawa, Poland
(Dated: August 6, 2021)

The negative solution to the famous problem of 36 officers of Euler implies that there are no two orthogonal Latin squares of order six. We show that the problem has a solution, provided the officers are entangled, and construct orthogonal quantum Latin squares of this size. As a consequence, we find an example of the long elusive Absolutely Maximally Entangled state AME(4,6) of four subsystems with six levels each, equivalently a 2-unitary matrix of size 36, which maximizes the entangling power among all bipartite unitary gates of this dimension, or a perfect tensor with four indices, each running from one to six. This special state deserves the appellation *golden AME state* as the golden ratio appears prominently in its elements. This result allows us to construct a pure nonadditive quhex quantum error detection code $((3,6,2))_6$, which saturates the Singleton bound and allows one to encode a 6-level state into a triplet of such states.

Introduction: It is well-known that quantum entanglement leads to peculiar consequences, and enable technical tasks such as teleportation, secret sharing, secure key cryptography, and error correcting codes [1]. Special entangled states such as the cluster states are a resource for measurement based quantum computing [2, 3]. Multipartite entanglement is also implicated in quantum many-body states and leads to thermalization in isolated systems [4, 5]. While the understanding of multipartite entanglement is still evolving, an extreme class of states: the absolutely maximally entangled (AME) ones are clearly singled out and easily defined. AME states find applications in several quantum protocols including quantum secret sharing and parallel teleportation [2], holographic quantum error correcting codes [4, 8], and quantum repeaters [9]. However, they are not easy to construct and often their very existence is unknown.

A pure quantum state, $|\psi\rangle \in \mathcal{H}_d^{\otimes N}$ of N parties, each of a local dimension d , is *absolutely maximally entangled* [1, 2], written as AME(N, d), if it is maximally entangled for every bipartition. For $N = 2$ and $N = 3$ parties, generalizations of the Bell and GHZ states, $\sum_{k=1}^d |kk\rangle/\sqrt{d}$ and $\sum_{k=1}^d |kkk\rangle/\sqrt{d}$ are AME states. The smallest number of parties of interest is therefore $N = 4$ where it is known that AME(4,2) does not exist, four qubits cannot be absolutely maximally entangled [15, 20]. However for all $d > 2$, except for $d = 6$, AME states of 4 parties are known to exist. Thus arguably the most interesting open case was the existence of AME(4,6). It has featured on open-problem lists of quantum information [13, 14] and in this Letter we settle this positively by explicitly constructing an example, leaving only four qubits as exceptional.

To shed light on the peculiar properties of such states, consider a collection of four dice. Alice selects *any* two dice and rolls them, obtaining one of 36 equally likely outcomes, as Bob rolls the remaining ones. If the entire state is AME(4,6), Alice can always deduce the result obtained in Bob's part of

the 4-party system.



FIG. 1: Four dice in the golden absolutely maximally entangled state of four-quhex, AME(4,6), corresponding to 36 entangled officers of Euler. Any pair of dice is unbiased, although their outcome determines the state of the other two. This is not possible if the four dice are replaced by four coins (qubits).

Furthermore, such a state allows one to teleport any unknown, two-dice quantum state, from any two owners of two subsystems to the lab possessing the two other dice of the entangled state of the four-party system. These are not possible if the dice is replaced by two-sided coins as AME(4,2) states do not exist [20].

The existence of AME(4, d) for all $d > 2$ and $d \neq 6$ has been known from the existence of particular combinatorial designs, namely orthogonal Latin squares (OLS), also known as Graeco-Latin squares. A simple example of a combinatorial design [15] is given by a single *Latin square*: a $d \times d$ array filled with d copies of d different symbols, such that each occurs once in each row and each column. For the design of experiments, one uses Graeco-Latin squares: two Latin squares arranged in such a way that the ordered pairs of entries in all cells of the square are distinct. The name of the design refers to a popular way to represent such a pair by one Greek character and one Latin.

It is easy to see that there are no Graeco-Latin squares of size two. Furthermore, it is not difficult to construct such a combinatorial design for $d = 3$ – see Fig. 2. Analogous con-

*Both authors contributed equally

βC	γA	αB	=	$K\heartsuit$	$Q\spadesuit$	$A\clubsuit$	=	$2, 3$	$3, 1$	$1, 2$
γB	αC	βA		$Q\clubsuit$	$A\heartsuit$	$K\spadesuit$		$3, 2$	$1, 3$	$2, 1$
αA	βB	γC		$A\spadesuit$	$K\clubsuit$	$Q\heartsuit$		$1, 1$	$2, 2$	$3, 3$

FIG. 2: An example of Graeco-Latin square of order $d = 3$. In the middle, Greek and Latin letters are replaced by ranks and suits of cards, on the right by pairs of numbers.

structions also work for $d = 4, 5$, and in general, for odd numbers d and multiples of four [16]. The case of $d = 6$ is thus special. Leonhard Euler examined the now-famous problem [17]: “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?” As Euler observed, such an arrangement, equivalent to a Graeco-Latin square of order 6, written OLS(6), does not exist, which was proven much later by Gaston Tarry [18]. Two OLS of size $d = 10$ were constructed in the 20th century and it is known that such designs exist [19] for any natural number $d \neq 2$, or $\neq 6$. This enables the construction of AME(4, d) for any d other than $d = 2$ and $d = 6$ [19].

While classical designs are built of discrete objects, their quantum analogs, introduced in the seminal thesis of Zauner [21], are composed of pure quantum states: normalized vectors from a complex Hilbert space $\mathcal{H}_d$ of dimension d . Such distinguished configurations of states play a significant role in quantum information, as they describe generalized quantum measurements with special properties. In particular, quantum analogs of Latin squares were introduced in [22], while various approaches to orthogonal quantum LS were advocated in [9–11].

In this work, we formulate a quantum analog of Euler’s problem of 36 officers [9] and present its complete analytic solution. As AME(4, 2) does not exist and standard OLS exist for any natural d , different from 2 and 6, the latter case corresponding to the quantum version of the Euler problem of 36 officers, was the only open problem for 4-partite systems [3, 27]. Our construction of an AME(4, 6) state, shows that for 4 parties, $d = 6$ is the only dimension in which there are no classical OLS, but there exists a quantum one. Even though OLS of order six do not exist, we present a coarse-grained OLS of that order, whose structure stands behind its constructed quantum analog.

Multipartite entangled states from Graeco-Latin squares: A pure quantum state $|\psi\rangle \in \mathcal{H}_d^A \otimes \mathcal{H}_d^B$ of a bipartite $d \times d$ system can be expanded in a product basis, $|\psi\rangle = \sum_{i,j=1}^d C_{ij} |i\rangle |j\rangle$, where the matrix C of coefficients satisfies the normalization condition, $\|C\|^2 = \text{Tr} CC^\dagger = 1$. A pure state is maximally entangled if its partial trace is maximally mixed, so that the matrix of coefficients is unitary up to rescaling, $CC^\dagger = I/d$. A pure quantum state, $|\psi\rangle \in \mathcal{H}_d^{\otimes N}$ of N parties, each of a local dimension d is AME(N, d) if the partial trace $\text{Tr}_S |\psi\rangle \langle \psi| \propto I$, for any subsystem S of $|S| = \lfloor N/2 \rfloor$ parties.

Any Graeco-Latin square of order d determines a 4-party quantum state $|\Psi\rangle \in \mathcal{H}_d^{\otimes 4}$,

$$|\Psi\rangle = \frac{1}{d} \sum_{i,j,k,\ell=1}^d T_{ijkl} |i\rangle |j\rangle |k\rangle |\ell\rangle, \quad (1)$$

where coefficients $T_{ijkl} = 1$ if the pair (k, ℓ) is an entry in i -th row and j -th column, while $T_{ijkl} = 0$ otherwise. Note that the matrix of order d^2 , indexed by doubled indices, $U_{ij,kl} := T_{ijkl}$, forms a permutation. Orthogonality conditions imposed on Latin squares implies that the matrices corresponding to the other two bipartitions of the four indices into pairs: $ik|j\ell$ and $i\ell|jk$, also form permutations. This follows as every relation between any two pairs of features (such as the column number and the card suit versus the row number and the card rank shown in Fig. 2) is a bijection.

It is convenient to recall reorderings of entries of a matrix of size d^2 used in quantum theory [17]. Representing the matrix in a product basis as $U_{ij,kl} = \langle i, j | U | k, \ell \rangle$, one defines the partially transposed matrix, U^Γ and the reshuffled matrix U^R ,

$$U_{ij,kl}^\Gamma = U_{i\ell,kj}, \quad U_{ij,kl}^R = U_{ik,j\ell}. \quad (2)$$

Making use of this notation, one can say that a permutation matrix U of order d^2 yields an OLS(d) if the reordered matrices, U^R and U^Γ are also permutations. In this case, the 4-partite state of Eq. 1 has a particular property: It is maximally entangled with respect to any bipartition of four indices i, j, k, ℓ into two pairs, and is hence an AME(4, d) state.

Orthogonal quantum Latin squares: To obtain other AME states of this class, we retain the condition that the matrices U, U^R and U^Γ be unitary while relaxing the condition that they are permutations. Such a matrix U is called 2-unitary [5], see supplemental material section I for more details. In fact, any 2-unitary matrix $U \in \mathbb{U}(d^2)$ yields an AME(4, d) state

$$|\text{AME}(4, d)\rangle = \frac{1}{d} \sum_{i,j=1}^d |i\rangle |j\rangle |\psi_{ij}\rangle, \quad (3)$$

where $|\psi_{ij}\rangle = U|i\rangle |j\rangle$. This allows one to say that the corresponding quantum design of d^2 bipartite quantum states $|\psi_{ij}\rangle$, $i, j = 1, \dots, d$, forms an orthogonal quantum Latin square (OQLS) – for a formal definition see supplemental material (SM) section I.

It may be noted that a 2-unitary matrix U of size d^2 , treated as a 4-index tensor, $T_{ijkl} := U_{(ij),(kl)}$ has been called a *perfect tensor* [8] and used in constructing quantum error correcting codes. Any of its 2-index flattenings $T_{ij}^{kl}, T_{ik}^{jl}, T_{il}^{jk}$ is unitary and provides an *isometry* between any pair of its indices. The partial trace of the 4-party state $|\Psi\rangle$ related to a perfect tensor as in Eq. 3 is maximally mixed for any symmetric bipartition of the system. Thus existence of such a perfect tensor with 4 indices running from 1 to d is equivalent to the existence of an AME state of four qudits and OQLS of size d .

Searching for 36 entangled officers: To tackle the quan-

tum Euler problem of AME(4,6), equivalent to finding a 2-unitary matrix of order 36, we used an iterative numerical technique based on nonlinear maps in the space of unitary matrices $\mathbb{U}(d^2)$ introduced recently in [7]. A closely related Sinkhorn-like algorithm to generate unitary matrices such that only their partial transpose is unitary was presented earlier in [12]. One map that produces 2-unitaries $\mathcal{M}_{\Gamma R} : U_0 \mapsto U_1$, consists of two parts (i) R and Γ operations in that order $U_0 \mapsto U_0^R \mapsto (U_0^R)^\Gamma := U_0^{\Gamma R}$, and (ii) projection onto the nearest unitary matrix $U_0^{\Gamma R} \mapsto U_1$ using the polar decomposition, $U_0^{\Gamma R} = U_1 H$, where H is a positive semi-definite matrix. It is straightforward to see that 2-unitary matrices are fixed points of the map $\mathcal{M}_{\Gamma R}^3$, or period-3 orbits of $\mathcal{M}_{\Gamma R}$. After n iterations of the map, $\mathcal{M}_{\Gamma R}^n[U_0] = U_n$, and as $n \rightarrow \infty$ this converges to 2-unitary matrices with high probabilities for $d = 3$ and $d = 4$, even using seeds U_0 sampled randomly according to the Haar measure on the unitary group [7].

The key to generating a 2-unitary matrix for $d > 4$ is to choose an appropriate seed matrix. The neighborhood of permutation matrices approximating OLS is a natural choice. In the most interesting case of $d = 6$, for which there are no OLS, seeds in the vicinity of the permutation matrix P_{36} [19] that is closest to an OLS, surprisingly, do not lead to a 2-unitary. However, there do exist other suitable permutation matrices whose vicinity contains seeds that under the map $\mathcal{M}_{\Gamma R}$ converge to 2-unitaries. An example of a seed that leads to the 2-unitary solution displayed in this work is provided in section III of SM.

A 2-unitary matrix remains 2-unitary on multiplication by local unitary operators. Using this freedom, we applied a search algorithm over the group $\mathbb{U}(6) \otimes \mathbb{U}(6)$ of local unitary operations, to orthogonalize certain rows and columns in a given numerical 2-unitary matrix U and its rearrangements U^R , $(U^R)^\Gamma$. We searched for block structures in all these three matrices abstracting from the exact form of the matrices. The particular choice of the orthogonality relations corresponds to the block structure of the eventually obtained analytical solution. These tools can be generalized to construct multi-unitary operators and corresponding AME states in other local dimensions and number of parties. While the solution presented is the smallest one of arguably greatest interest, namely AME(4,6), the methods can potentially yield maximally entangled states that are not created by presently known techniques.

Solution found: To present the solution to the problem of the 36 entangled officers of Euler, we display the coefficients T_{ijkl} of the AME(4,6) quantum state $\in \mathcal{H}_6^{\otimes 4}$ (four quhex state), see Eq. 3. Non-vanishing coefficients T_{ijkl} might be conveniently written in form of a table, see Fig. 3. The provided construction is based on the root of unity of order 20, denoted by $\omega = \exp(i\pi/10)$. There exist only three non-zero ampli-

tudes:

$$\begin{aligned} a &= (\sqrt{2}(\omega + \bar{\omega}))^{-1} = (5 + \sqrt{5})^{-1/2}, \\ b &= (\sqrt{2}(\omega^3 + \bar{\omega}^3))^{-1} = ((5 + \sqrt{5})/20)^{1/2}, \\ c &= 1/\sqrt{2}, \end{aligned} \quad (4)$$

whose numerical values are $\simeq (0.3717, 0.6015, 0.7071)$, respectively. The bar over the symbol indicates the complex conjugate. The relations $a^2 + b^2 = c^2 = 1/2$ and $b/a = \varphi = (1 + \sqrt{5})/2$ the golden ratio, determine all amplitudes appearing in the solution and explain why the constructed AME state deserves to be called the *golden AME state*. Checking the property of being an AME state reduces to verification of several equations involving roots of unity of order 20, which we elaborate in a detailed way in SM section II. The key result of this work consists, therefore, of the following assertion proved in SM:

Theorem 1. *There exists an AME(4,6) state of 4 parties with 6 levels each.*

This statement is equivalent to the existence of a 2-unitary matrix $\mathcal{U}_{36} \in \mathbb{U}(36)$, and a perfect tensor $T_{ijkl} := \mathcal{U}_{36}(ij)(kl)$, and a solution to the quantum analog of the 36-officers problem of Euler.

An explicit solution of the generalized Euler problem can be conveniently written in terms of a *quantum* OLS in the form of 36 states $|\psi_{ij}\rangle = \mathcal{U}_{36}|i\rangle|j\rangle \in \mathcal{H}_6^{\otimes 2}$ representing the entangled officers. Following Euler's notation used for Graeco-Latin squares we label the rank of each officer by a rank of the card A, K, Q, J, 10, 9, and (extended set of) suits ♠, ♣, ♦, ♥, ♣, * are used to label her regiment:

$$\begin{aligned} |\psi_{11}\rangle &= c|A\spadesuit\rangle + c|K\spadesuit\rangle, \\ |\psi_{12}\rangle &= c\omega^{17}|A\diamondsuit\rangle + c\omega^{19}|K\heartsuit\rangle, \\ &\vdots \\ |\psi_{66}\rangle &= b\omega^9|10\spadesuit\rangle + b\omega^{13}|9\clubsuit\rangle + a\omega^{16}|10\clubsuit\rangle + a\omega^{16}|9\spadesuit\rangle, \end{aligned} \quad (5)$$

while expressions for the remaining thirty-three states can be directly read out from the 2-unitary matrix presented in Fig. 3. Notice that the related state in Eq. 3 is an AME state. Remarkably, all the 36 states $|\psi_{ij}\rangle$ are maximally entangled as two-qubit states. While this is evident for states such as $|\psi_{11}\rangle$, even $|\psi_{66}\rangle$ and others with support on 4 states are maximally entangled, thanks to the special value of the phases.

Structure of the AME(4,6) state: Recall that a classical OLS corresponds to a 2-unitary permutation matrix. Since there is no solution to the original problem of Euler, the 2-unitary permutation matrix of size 36 does not exist. Nonetheless, we can present the AME(4,6) state obtained by us in a form similar to the classical solution of AME(4,3) generated from classical OLS in Fig. 2. Let us consider every row of a 2-unitary matrix as a place to put an “officer” in, then we can express the entanglement in our solution by showing which two (or four) officers are entangled, thus producing Fig. 4.

The 2-unitary matrix $\mathcal{U}_{36}$ described here has, up to permutations, the structure of nine unitary blocks of size 4. Moreover, the block structure is also characteristic for the reshuffled

(1,1)	(2,2)	(1,2)	(2,1)		(1,3)	(2,4)	(1,4)	(2,3)		(1,5)	(2,6)	(1,6)	(2,5)	
$a \omega^{10}$	a	$b \omega^{15}$	$b \omega^5$	(6,3)	$a \omega^2$	$a \omega^{14}$	$b \omega$	$b \omega^5$	(2,5)	$a \omega$	$a \omega^{19}$	$b \omega^{14}$	$b \omega^{16}$	(4,1)
		c	c	(1,1)			$c \omega^5$	$c \omega^{19}$	(3,3)	$a \omega$	$a \omega^3$	$b \omega^{10}$	$b \omega^4$	(3,4)
c	c			(5,6)	$c \omega^{17}$	$c \omega^{19}$			(1,2)	$b \omega^4$	$b \omega^{18}$	$a \omega^3$	$a \omega^9$	(2,6)
$b \omega^{10}$	b	$a \omega^5$	$a \omega^{15}$	(4,2)	$b \omega^{14}$	$b \omega^6$	$a \omega^3$	$a \omega^7$	(6,4)	$b \omega^2$	$b \omega^8$	$a \omega^5$	$a \omega^{15}$	(5,5)
(3,1)	(4,2)	(3,2)	(4,1)		(3,3)	(4,4)	(3,4)	(4,3)		(3,5)	(4,6)	(3,6)	(4,5)	
$a \omega^4$	$a \omega^{10}$	$b \omega^{17}$	$b \omega^7$	(4,5)	a	a	$b \omega^{15}$	$b \omega^{15}$	(4,6)	$a \omega^2$	a	$b \omega^{19}$	$b \omega^{13}$	(2,3)
		$c \omega^2$	$c \omega^2$	(3,2)			c	$c \omega^{10}$	(6,1)			$c \omega^{16}$	c	(6,2)
$c \omega^{10}$	$c \omega^6$			(2,4)	c	$c \omega^{10}$			(5,4)	$c \omega^8$	$c \omega^{16}$			(3,1)
$b \omega^7$	$b \omega^{13}$	$a \omega^{10}$	a	(5,3)	b	b	$a \omega^5$	$a \omega^5$	(1,5)	$b \omega^{14}$	$b \omega^{12}$	$a \omega$	$a \omega^{15}$	(1,6)
(5,1)	(6,2)	(5,2)	(6,1)		(5,3)	(6,4)	(5,4)	(6,3)		(5,5)	(6,6)	(5,6)	(6,5)	
$a \omega^3$	$a \omega^7$	b	b	(1,4)	$a \omega^{12}$	$a \omega^{14}$	$b \omega^{15}$	$b \omega$	(3,6)	$a \omega^{18}$	$a \omega^{18}$	$b \omega^3$	$b \omega^3$	(1,3)
		c	$c \omega^{10}$	(2,1)			$c \omega^{14}$	$c \omega^{10}$	(5,1)			c	$c \omega^{10}$	(5,2)
$c \omega^{13}$	$c \omega^7$			(3,5)	$c \omega^7$	$c \omega^{19}$			(2,2)	$c \omega$	$c \omega^{11}$			(6,5)
$b \omega^9$	$b \omega^{13}$	$a \omega^{16}$	$a \omega^{16}$	(6,6)	$b \omega^{14}$	$b \omega^{16}$	$a \omega^7$	$a \omega^{13}$	(4,3)	$b \omega^{10}$	$b \omega^{10}$	$a \omega^5$	$a \omega^5$	(4,4)

FIG. 3: Non-vanishing coefficients T_{ijkl} of the AME(4,6) state $|\Psi\rangle$. Indices (i, j) are indicated in rows, (k, l) in columns, respectively. Treating each coordinates (i, j) as a position (row and column) of Euler's officer, its rank and regiment are in superposition of two or four canonical ranks and regiments. Equivalently, the picture shows non-zero entries of 2-unitary matrix $\mathcal{U}_{36}$ of size 36 where $j + 6(i - 1)$ labels the relevant row while $\ell + 6(k - 1)$ determines the column. Note that all 36 officers, each represented by a single row of the matrix, are maximally entangled qubit states, 16 of them have minimal support being bipartite Bell states (red rows), while the remaining 20 have maximal support (yellow/green rows) – see Eq. 5 and SM. The order of the blocks reflects an additional structure as the numbering of columns increases by six as we proceed to a block below. Depicted matrix preserves its structure of nine unitary blocks of size four with respect to transformations of reshuffling $j \longleftrightarrow k$, and partial transpose $j \longleftrightarrow \ell$.

matrix $\mathcal{U}_{36}^R$ and the partially transposed matrix $\mathcal{U}_{36}^F$. In other words, in the original matrix $\mathcal{U}_{36}$ we found the block structure *invariant* under reshuffling and partial transpose. The problem of finding 36 entangled officers of Euler splits into two sub-problems: to identify first a block-invariant structure and then to select adequate non-zero elements within them. A particular combinatorial design underlies the invariant structure. Grouping symbols of indices k and ℓ in the presented perfect tensor T_{ijkl} in pairs: $1, 2 \rightarrow A/\alpha$, and $3, 4 \rightarrow B/\beta$, and $5, 6 \rightarrow C/\gamma$ for k/ℓ respectively, results in a coarse-grained OLS, which reveals the described block structure, see Fig. 5.

Quantum codes: Several examples of quantum error correction codes discussed in the literature belong to the class of *additive (stabilizer) codes*, quantum analogs of classical additive codes [9, 32]. In particular all hitherto known AME states, are either stabilizer states [9], or might be derived from the stabilizer construction [33]. Stabilizer codes have the structure of an eigenspace of an abelian group generated by multilocal generalized Pauli operators. The stabilizer approach is especially effective for codes with local prime power dimensions d . Stabilizers of an additive code might be presented in their standard form [9]. We examined all stabilizer sets of four quhex in their standard form and did not find an AME(4,6) state. Therefore, the presented AME(4,6) state is a nonadditive one.

Nonadditive quantum codes are in general more difficult to construct, however, in many cases, they outperform the stabi-

lizer codes [34]. Thus far, the stabilizer approach practically contained the combinatorial approach to constructing AME and k -uniform states. As we demonstrated, the consideration of coarse-grained combinatorial structures might be successful in constructing genuinely entangled states and have advantages over the stabilizer approach.

In order to successfully use a pure $((4, 1, 3))_6$ code in an error correction scheme, one may apply the shortening procedure [35, 36] and obtain $((3, 6, 2))_6$ code. In such way, a single quhex $|i\rangle \in \mathcal{H}_6$ is encoded into a three quhex state $|\tilde{i}\rangle \in \mathcal{H}_6^{\otimes 3}$ defined by

$$|i\rangle \rightarrow |\tilde{i}\rangle := \frac{1}{\sqrt{6}} \sum_{j,k,\ell=1}^6 T_{ijk\ell} |j, k, \ell\rangle.$$

Both codes, the initial and shortened ones, are optimal, meeting the quantum Singleton bound [36]. Thus, the presented construction of AME states of four subsystems with 6 levels each sheds some light on how to construct nonadditive quantum error correction codes, in a case for which the stabilizer approach fails.

Summary and Outlook: The famous combinatorial problem of 36 officers was posed by Euler, who claimed in 1779 that no solution exists. The first paper with proof of this statement, by Tarry [18], came only 121 years later, in 1900. After another 121 years, we have presented a solution to the quan-

$ K\spadesuit\rangle$	$ A\clubsuit\rangle$	$ A\diamond\rangle$	$ 10\spadesuit\rangle$	$ 10\star\rangle$	$ 10\spadesuit\rangle$	$ 10\clubsuit\rangle$	$ Q\diamond\rangle$	$ Q\heartsuit\rangle$	$ Q\spadesuit\rangle$	$ Q\star\rangle$
		$ K\heartsuit\rangle$	$ 9\spadesuit\rangle$	$ 9\star\rangle$	$ 9\spadesuit\rangle$	$ 9\clubsuit\rangle$	$ J\diamond\rangle$	$ J\heartsuit\rangle$	$ J\spadesuit\rangle$	$ J\star\rangle$
$ 9\spadesuit\rangle$	$ 10\clubsuit\rangle$	$ 10\diamond\rangle$	$ Q\spadesuit\rangle$	$ Q\star\rangle$	$ Q\spadesuit\rangle$	$ J\clubsuit\rangle$	$ A\diamond\rangle$	$ A\heartsuit\rangle$	$ A\spadesuit\rangle$	$ A\star\rangle$
$ Q\spadesuit\rangle$		$ 9\heartsuit\rangle$	$ J\spadesuit\rangle$	$ J\star\rangle$			$ K\diamond\rangle$	$ K\heartsuit\rangle$	$ K\spadesuit\rangle$	$ K\star\rangle$
	$ J\star\rangle$		$ Q\clubsuit\rangle$	$ A\heartsuit\rangle$	$ A\spadesuit\rangle$	$ A\spadesuit\rangle$	$ 10\spadesuit\rangle$		$ 10\diamond\rangle$	$ 10\heartsuit\rangle$
$ A\spadesuit\rangle$	$ A\star\rangle$	$ A\spadesuit\rangle$	$ A\clubsuit\rangle$	$ 10\diamond\rangle$	$ 10\heartsuit\rangle$	$ 10\spadesuit\rangle$	$ 10\clubsuit\rangle$	$ 10\star\rangle$	$ Q\spadesuit\rangle$	$ Q\clubsuit\rangle$
$ K\spadesuit\rangle$	$ K\star\rangle$	$ K\spadesuit\rangle$	$ K\clubsuit\rangle$	$ 9\diamond\rangle$	$ 9\heartsuit\rangle$	$ 9\spadesuit\rangle$	$ 9\clubsuit\rangle$	$ 9\star\rangle$	$ J\spadesuit\rangle$	$ J\clubsuit\rangle$
$ 9\diamond\rangle$	$ 10\heartsuit\rangle$		$ 10\star\rangle$	$ Q\spadesuit\rangle$	$ Q\clubsuit\rangle$	$ Q\diamond\rangle$	$ A\spadesuit\rangle$	$ A\star\rangle$	$ A\spadesuit\rangle$	$ K\clubsuit\rangle$
$ J\diamond\rangle$	$ Q\heartsuit\rangle$		$ Q\star\rangle$	$ A\spadesuit\rangle$	$ A\clubsuit\rangle$	$ A\diamond\rangle$	$ A\heartsuit\rangle$	$ 10\spadesuit\rangle$	$ 10\clubsuit\rangle$	$ 10\star\rangle$
	$ J\spadesuit\rangle$		$ K\spadesuit\rangle$	$ K\clubsuit\rangle$	$ K\diamond\rangle$	$ K\heartsuit\rangle$		$ 9\star\rangle$	$ 9\spadesuit\rangle$	$ 9\clubsuit\rangle$

FIG. 4: Visualization of entanglement between Euler’s officers. Position of each officer: i -th row and j -th column, is presented in appropriate row and column on the array. Ranks and regiments of officers (relevant to the indices k and ℓ in $T_{ijk\ell}$) are represented in form of cards with corresponding ranks and suits (in particular, $1 \rightarrow A/\spadesuit$, $2 \rightarrow K/\clubsuit$, $3 \rightarrow Q/\diamond$, $4 \rightarrow J/\heartsuit$, $5 \rightarrow 10/\spadesuit$, $6 \rightarrow 9/\star$, for k/ℓ respectively). The grade of each officer is in a superposition of four basic grades: two ranks, and two regiments. The font size of each ket corresponds to the amplitude of the related tensor element. Notice that a classical solution to Euler’s problem would correspond to the array with only one card in each entry. Note the structures arising in the array, e.g. aces are entangled only with kings, queens with jacks, and 10s with 9s. Moreover, the *colors* of the cards are not entangled with each other. Hence, officers are grouped into nine sets with four elements, each sharing the same pairs of figures and colors of the card. For example, officers on positions $(1, 1)$, $(4, 2)$, $(5, 6)$, $(6, 3)$ share two black figures A, K of a black suits $\spadesuit, \clubsuit$, which corresponds to the top-left clique on Fig. 3.

$A\alpha$	$A\beta$	$C\gamma$	$C\alpha$	$B\beta$	$B\gamma$
$C\alpha$	$C\beta$	$B\gamma$	$B\alpha$	$A\beta$	$A\gamma$
$B\gamma$	$B\alpha$	$A\beta$	$A\gamma$	$C\alpha$	$C\beta$
$A\gamma$	$A\alpha$	$C\beta$	$C\gamma$	$B\alpha$	$B\beta$
$C\beta$	$C\gamma$	$B\alpha$	$B\beta$	$A\gamma$	$A\alpha$
$B\beta$	$B\gamma$	$A\alpha$	$A\beta$	$C\gamma$	$C\alpha$

FIG. 5: A coarse-grained OLS of order 6, which reveals the block structure of a perfect tensor $T_{ijk\ell}$. Indices of non-vanishing elements of the tensor $T_{ijk\ell}$ are presented: i in row, j in column, while a pair of coarse-grained indices k, ℓ in the entry. Each pair of symbols repeats exactly four times in the array. Moreover, each symbol on each position repeats exactly twice in each row and column. Notice that the array above corresponds to Fig. 4 by coarse-graining figures $A/K \rightarrow A$; $Q/J \rightarrow B$; $10/9 \rightarrow C$, and suits $\spadesuit/\clubsuit \rightarrow \alpha$; $\diamond/\heartsuit \rightarrow \beta$; $\spadesuit/\star \rightarrow \gamma$ of cards in entries.

tum version wherein the officers can be entangled. This unexpected result implies constructive solutions to the related problems of the existence of absolutely maximally entangled states of four subsystems with six levels each, a 2-unitary ma-

trix $\mathcal{U}_{36}$ of size 36 with maximal entangling power and a perfect tensor $T_{ijk\ell}$ with four indices, each running from one to six. Our results allowed us to construct original quantum error correction codes: a pure code $((4, 1, 3))_6$, and a shortened code $((3, 6, 2))_6$, which allows encoding a 6-level state into a set of three such subsystems. It is tempting to believe that the quantum design presented here will trigger further research on quantum combinatorics.

Acknowledgments

It is a pleasure to thank S. Aravinda, J. Czartowski, D. Goyeneche, M. Grassl, F. Huber, P. Mazurek, Z. Puchała and A. Rico for several inspiring discussions and helpful remarks. Financial support by Narodowe Centrum Nauki under the Maestro grant number DEC-2015/18/A/ST2/00274, by Foundation for Polish Science under the Team-Net project no. POIR.04.04.00-00-17C1/18-00 and by the Department of Science and Technology, Govt. of India, under grant number DST/ICPS/QuST/Theme-3/2019/Q69 are gratefully acknowledged.

- [1] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press (2010).
- [2] R. Raussendorf and H. J. Briegel, A One-Way Quantum Computer *Phys. Rev. Lett.* **86**, 5188 (2001).

- [3] R. Raussendorf, R. Browne and H. J. Briegel, Measurement-based quantum computation on cluster states *Phys. Rev. A* **68**, 022312 (2003).
- [4] L. Amico, R. Fazio, A. Osterloh, and V. Vedral, Entanglement

- in many-body systems, *Rev. Mod. Phys.* **80** 517 (2008).
- [5] A. M. Kaufman, M. E. Tai, A. Lukin, M. Rispoli, R. Schittko, P. M. Preiss, and M. Greiner, Quantum thermalization through entanglement in an isolated many-body system, *Science* **353** 6301 (2016).
 - [6] W. Helwig, W. Cui, A. Riera, J. Latorre, and H.K. Lo, Absolute maximal entanglement and quantum secret sharing, *Phys. Rev. A* **86**, 052335 (2012).
 - [7] F. Pastawski, B. Yoshida, D. C. Harlow, and J. Preskill, Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence, *Journal High Energy Phys.*, **2015**, 1 (2015).
 - [8] P. Mazurek, M. Farkas, A. Grudka, M. Horodecki, and M. Studziński, Quantum error-correction codes and absolutely maximally entangled states, *Phys. Rev. A* **101**, 042305 (2020).
 - [9] D. Alsina and M. Razavi, Absolutely maximally entangled states, quantum-maximum-distance-separable codes, and quantum repeaters, *Phys. Rev. A* **103**, 022402 (2021).
 - [10] A. J. Scott, Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions, *Phys. Rev. A* **69**, 052330 (2004).
 - [11] A. Higuchi and A. Sudbery, How entangled can two couples get?, *Phys. Lett. A* **273**, 213 (2000).
 - [12] F. Huber, C. Eltschka, J. Siewert, and O. Gühne, Bounds on absolutely maximally entangled states from shadow inequalities, and the quantum MacWilliams identity, *J. Phys.* **51**, 175301 (2018).
 - [13] List of Open Quantum Problems, Problem 35, IQOQI Vienna.
 - [14] P. Horodecki, Ł. Rudnicki, and K. Życzkowski, Five open problems in quantum information, arXiv:2002.03233.
 - [15] C. J. Colbourn and J. H. Dinitz (eds.), *Handbook of Combinatorial Designs*, CRC Press, Boca Raton (2007).
 - [16] J. Dénes and A. D. Keedwell (eds.), *Latin Squares: New Developments in the Theory and Applications*, North-Holland, Amsterdam, (1991).
 - [17] L. Euler, “Recherches sur une nouvelle espece de quares magiques,” *Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen* **9**, Middelburg, 85–239 (1782). Also published in *Commentationes Arithmeticae* **2**, 302–361 1(849). Available online in The Euler Archive: <http://eulerarchive.maa.org/pages/E530.html>. Accessed, April 2021.
 - [18] G. Tarry, “Le problème de 36 officiers,” *Compte Rendu de l’Association Française pour l’Avancement des Sciences*. Secrétariat de l’Association. **1**, 122 (1900).
 - [19] C. J. Colbourn and J. H. Dinitz, Mutually orthogonal Latin squares: a brief survey of constructions, *J. Stat. Planning Inference* **95**, 9 (2001).
 - [20] L. Clarisse, S. Ghosh, S. Severini, and A. Sudbery, Entangling power of permutations, *Phys. Rev. A* **72** (2005).
 - [21] G. Zauner, Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie, Ph. D. thesis, Universität Wien (1999).
 - [22] B. Musto and J. Vicary, Quantum Latin squares and unitary error bases, *Quantum Inf. Comput.* **16**, 1318 (2016).
 - [23] D. Goyeneche, Z. Raissi, S. Di Martino, and K. Życzkowski, Entanglement and quantum combinatorial designs, *Phys. Rev. A* **97**, 062326 (2018).
 - [24] B. Musto and J. Vicary, Orthogonality for Quantum Latin Isometry Squares, *EPTCS* **287**, 253 (2019).
 - [25] A. Rico, Absolutely maximally entangled states in small system sizes, Master Thesis, Innsbruck (2020).
 - [26] F. Huber and N. Wyderka, Table of AME states, 2021.
 - [27] X.-D. Yu, T. Simnacher, N. Wyderka, H. C. Nguyen, and O. Gühne, A complete hierarchy for the pure state marginal problem in quantum mechanics, *Nature Communications* **12**, 1012 (2021).
 - [28] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States*. 2 Ed., Cambridge (2017).
 - [29] D. Goyeneche, D. Alsina, A. Riera, J. Latorre, and K. Życzkowski, Absolutely maximally entangled states, combinatorial designs and multi-unitary matrices, *Phys. Rev. A* **92**, 032316 (2015).
 - [30] S. A. Rather, S. Aravinda, and A. Lakshminarayan, Creating ensembles of dual unitary and maximally entangling quantum evolutions, *Phys. Rev. Lett.* **125**, 070501 (2020).
 - [31] T. Benoist and I. Nechita, On bipartite unitary matrices generating subalgebra-preserving quantum operations, *Linear Algebra and Appl.* **521**, 70 (2017).
 - [32] A. Cross, G. Smith, J. A. Smolin, and B. Zeng, Codeword stabilized quantum codes, *IEEE Transactions on Information Theory*, **55**, 433 (2009).
 - [33] A. Burchardt and Z. Raissi, Stochastic local operations with classical communication of absolutely maximally entangled states, *Phys. Rev. A*, **102**, 022413 (2020).
 - [34] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, Nonadditive quantum error-correcting code, *Phys. Rev. Lett.* **101**, 090501 (2008).
 - [35] E. M. Rains, Nonbinary quantum codes, *IEEE Trans. Inf. Theory*, **45**, 1827 (1999).
 - [36] F. Huber and M. Grassl, Quantum codes of maximal distance and highly entangled subspaces, *Quantum*, **4**, 284 (2020).

Supplemental Material for “Thirty-six entangled officers of Euler: Quantum solution to a classically impossible problem”

I. ORTHOGONAL QUANTUM LATIN SQUARES AND 4-PARTITE ENTANGLED STATES.

In this section, we collect the definitions introduced in the literature in various contexts and demonstrate the equivalence between different notions used in the main body of the work.

Definition 1. AME state [S1, S2]. A pure quantum state, $|\psi\rangle \in \mathcal{H}_d^{\otimes N}$ of N parties, each of a local dimension d , is called *absolutely maximally entangled (AME)*, written as $|\text{AME}(N, d)\rangle$, if it is maximally entangled for every bipartition, i.e. the partial trace $\text{Tr}_S |\psi\rangle\langle\psi| \propto \mathbb{I}$, for any subsystem S of $|S| = \lfloor N/2 \rfloor$ parties.

In this work, we analyze the case of a fourpartite state, $N = 4$. A list of known AME states is available at [S3]. In general, an AME state consisting of an even number N of subsystems with d levels each leads to a pure quantum error correction code $((N, 1, N/2 + 1))_d$, which saturates the Singleton bound [S4].

Definition 2. Multiunitary matrix [S5]. A unitary matrix U of order d^2 is called *2-unitary* if the reshuffled matrix U^R and partially transposed matrix U^Γ are also unitary.

Matrices with the last condition relaxed also play a role in studies on many-body quantum dynamics: A unitary matrix U of size d^2 , for which U^R is unitary, is called *dual-unitary* [S6, S7]. In general, a matrix U of order d^k is called *k-unitary* (or multiunitary), if it remains unitary for all $(2k-1)(k-1)$ reorderings of $2k$ indices which define the matrix. Any 2-unitary matrix U of size d^2 describes a bipartite quantum gate, which maximizes the entangling power, $e_p(U) = 1$, see Supplementary Material Section 3.

Definition 3. Perfect tensor [S8]. A tensor $T_{i_1 \dots i_{2k}}$ with $2k$ indices, each running from 1 to d is called *perfect*, if any of its flattening into a matrix of order d^k is unitary.

The notion of orthogonal quantum Latin squares (OQLS) was introduced in [S9, S10]. Here we follow an alternative approach of Rico [S11] to assure full consistency with 2-unitarity. Let $|\chi^+\rangle = \sum_{i=1}^d |i, i\rangle$ denote the (non-normalized) maximally entangled Bell state of a 2-qudit system. Any bipartite quantum state, $|\psi\rangle = \sum_{k, \ell=1}^d C_{k, \ell} |k, \ell\rangle$, can be also written as $|\psi\rangle = (C \otimes \mathbb{I}) |\chi^+\rangle$.

Definition 4. OQLS. Consider a set of d^2 bipartite states in $\mathcal{H}_d \otimes \mathcal{H}_d$, which can be written in a product basis, $|\psi_{ij}\rangle = \sum_{k, \ell=1}^d C_{k\ell}^{i,j} |k, \ell\rangle$ for $i, j = 1, \dots, d$. Such a set forms an *OQLS* if (a) the states satisfy orthogonality relations, $\langle \psi_{ij} | \psi_{kl} \rangle = \delta_{ik} \delta_{jl}$; and the block matrix $\tilde{C}$ of size d^2 written $\tilde{C} = (C^{1,1}, \dots, C^{1,d}; \dots; C^{d,1}, \dots, C^{d,d})$ is block unitary, so that the conditions (b) $\sum_{i=1}^d C^{i,j} (C^{i,\ell})^\dagger = \delta_{j,\ell} \mathbb{I}$, and (c) $\sum_{j=1}^d C^{i,j} (C^{k,j})^\dagger = \delta_{i,k} \mathbb{I}$, are satisfied.

Observe that the orthogonality relations, equivalent to $\text{Tr } C^{i,j} (C^{k,\ell})^\dagger = \delta_{ik} \delta_{j\ell}$, correspond to the ‘different location’ conditions for strong sudoku satisfied by the 2-unitary permutations presented in Eq. S3 and S4. Furthermore, note that the block unitarity of $\tilde{C}$ implies that the related block matrix, $\tilde{B}$ with blocks $B^{i,j} = C^{i,j} (C^{i,j})^\dagger$ is block bistochastic, $\sum_{i=1}^d B^{i,j} = \mathbb{I}$, and $\sum_{j=1}^d B^{i,j} = \mathbb{I}$. Hence any OQLS described by the block matrix $\tilde{C}$ implies a block bistochastic matrix $\tilde{B}$ introduced in [S12], and recently studied in [S13] under the name of *quantum magic square*.

To show these notions in action, we shall analyze the case of a Graeco-Latin square (OLS) of size three, shown in Fig. 2. To get a set of 9 bipartite vectors $|\psi_{ij}\rangle$ in a given cell (A, α) we replace the classical symbols by a bipartite quantum state $|A, \alpha\rangle$. Thus each state has a product form, $|\psi_{i,j}\rangle = |i \oplus j\rangle \otimes |i \oplus 2j\rangle$, which is a consequence of the fact that OLS are classical. Notice that the operations inside kets are performed modulo 3.

The same information is encoded in the tensor determined by

$$T_{ijk\ell} = \delta_{k, i \oplus j} \delta_{\ell, i \oplus 2j}, \quad (\text{S1})$$

with addition operations performed modulo 3. It is easy to check that this tensor is perfect. Furthermore, the corresponding state

$$|\text{AME}(4, 3)\rangle = \frac{1}{3} \sum_{i, j=1,2,3} |i\rangle |j\rangle |i \oplus j\rangle |i \oplus 2j\rangle \quad (\text{S2})$$

belongs to AME states, as all reduced density matrices to two qutrits are equal to $\mathbb{I}_9/9$. One may present the tensor $T_{ijk\ell}$ in a form of 9×9 permutation matrix P_9 , where non-vanishing element of $T_{ijk\ell}$ corresponds to a non-zero entry of P_9 on the intersection

of $j + 3(i - 1)$ -th row with $\ell + 3(k - 1)$ -th column. In other words, the corresponding permutation matrix

$$P_9 = \left(\begin{array}{ccc|ccc|ccc} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right) \quad (S3)$$

is 2-unitary, since the reshuffled and partially transposed matrices

$$P_9^R = \left(\begin{array}{ccc|ccc|ccc} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right) \quad \text{and} \quad P_9^\Gamma = \left(\begin{array}{ccc|ccc|ccc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right) \quad (S4)$$

also form permutation matrices. Observe that positions of non-zero entries obey the rules of a strong Sudoku: in each row, column and block there is a single entry equal to 1. Furthermore, all the locations of these entries in each block are different.

Let us return now to the general case of an arbitrary dimension d and relax the assumption that the 2-unitary matrix of order d^2 is a permutation. To demonstrate relations between different notions introduced independently in different communities we recall the equivalence relations.

Proposition 1. *The following statements are equivalent:*

1. *There exist orthogonal quantum Latin squares of size d ,*
2. *There exists an AME state of four subsystems with d levels each,*
3. *There exists a 2-unitary matrix U of size d^2 ,*
4. *There exists a perfect tensor with four indices, each running from 1 to d .*

To show that this is the case, note first that definition 3 of a perfect tensor is equivalent to definition 2 of a multiunitary matrix. Furthermore, these properties imply that the state given by Eq. 1 has all reductions of size two maximally mixed, so according to definition 1 it forms an AME state $|\Psi_{ABCD}\rangle$ of four parties. The three constraints, (a), (b) and (c) in definition 4 are equivalent to the fact that partial traces over selected subsystems, CD , BD and AD , respectively are maximally mixed, so existence of OQLS and an AME state of the corresponding system, is equivalent.

Observe that a matrix U is 2-unitary if and only if the corresponding matrix U^R , or equivalently U^Γ , is 2-unitary. Indeed, all three corresponding states are related by the permutation of subsystems. Note that conditions imposed on AME states are invariant under the permutation of subsystems.

Furthermore, a 2-unitary matrix U remains 2-unitary after any local operation, i.e. $U \mapsto \tilde{U}(U_A \otimes U_B)U(U_C \otimes U_D)$ where $U_A, U_B, U_C, U_D \in \mathbb{U}(6)$ are unitary matrices of size 6. Thus, by this mean one can entangle officers from a classical OLS, creating *apparently* quantum solution of OQLS. By apparent, we express the fact that it can be disentangled to a classical OLS by applying reverse local operation $(U_A^\dagger \otimes U_B^\dagger)\tilde{U}(U_C^\dagger \otimes U_D^\dagger)$. Observe that a similar disentangling procedure is not feasible in the case of any AME(4,6) state, since it could not have been produced using classical designs. Consequently, we call our result a *genuinely* quantum solution to OQLS of size $d = 6$.

Note that the state AME(4,3) corresponds to a classical OLS, as the 2-unitary matrix is a permutation P_9 , so the entries of the design are product states. We are not aware whether for $d = 3$ there exist genuinely quantum orthogonal Latin squares. However, such a design exists for $d = 6$, as will be demonstrated below.

II. PROOF OF THEOREM 1 ON THE EXISTENCE OF AME(4,6)

In this section we prove Theorem 1 by construction. We introduce a matrix $\mathcal{U}$ of size 36 and show that it is 2-unitary. Its non vanishing entries, determined by the tensor, $\mathcal{U}_{p,s} = T_{ijkl}$, with $p = j + 6(i - 1)$ and $s = \ell(k - 1)$, are shown in Fig 3. To show 2-unitarity of the matrix $\mathcal{U}$ (also denoted $\mathcal{U}_{36}$ in the main text) we verify that three related matrices: $\mathcal{U}$, $\mathcal{U}^R$ and $(\mathcal{U}^R)^\Gamma$ are unitary. By definition 2, this implies that the matrix $\mathcal{U}^R$ is 2-unitary, which is equivalent to the fact that the matrix $\mathcal{U}$ is 2-unitary. Each of those matrices has the structure of nine 4×4 blocks. Hence our task simplifies to verification that constituent blocks are unitary matrices.

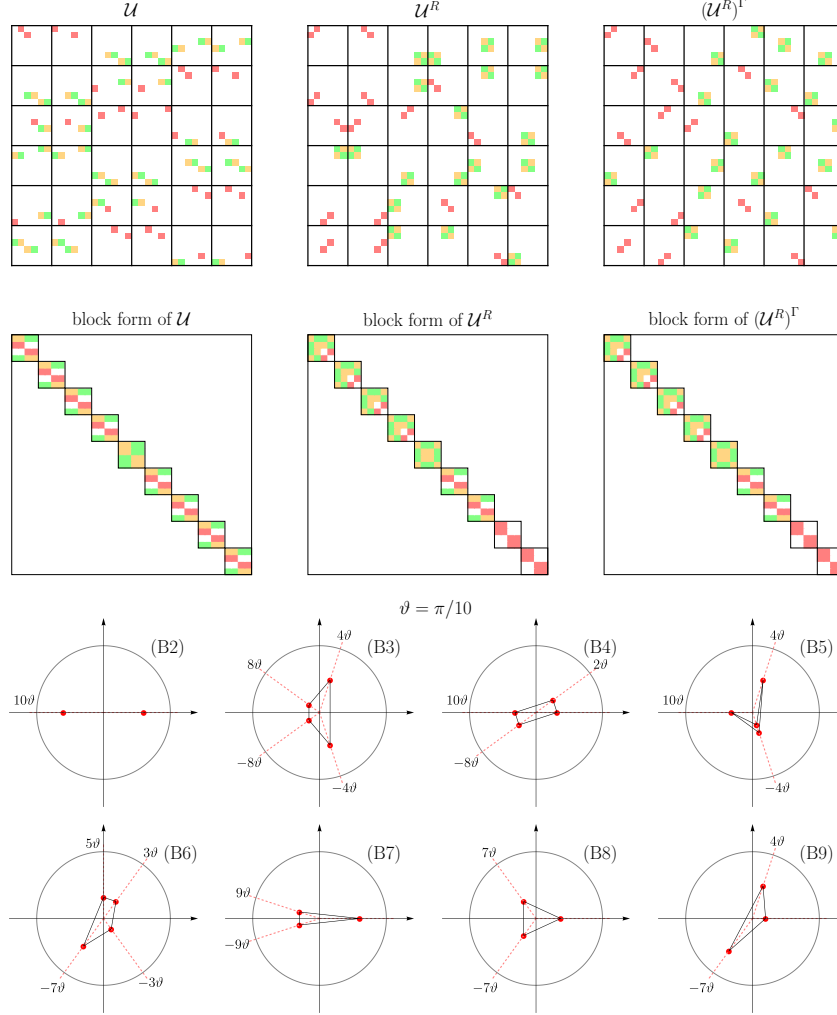


FIG. S1: Structure of three related matrices $\mathcal{U}$, $\mathcal{U}^R$ and $(\mathcal{U}^R)^\Gamma$ of order 36 are presented on top. The modulus of a non-vanishing element is represented by the intensity of the background color. Note that similarly to rows and columns, blocks also satisfy orthogonality conditions b) and c) from definition 4 of OQLS. Each matrix has the structure of nine 4×4 blocks, the structure within the blocks, however, is different for matrix $\mathcal{U}$ and matrices $\mathcal{U}^R$, $(\mathcal{U}^R)^\Gamma$. Orthogonality between pairs of rows in block matrices might be presented as a constellation of two, three, or four points on the complex plane which sum up to zero. Constellations related to Eqs. S5-S12 are indicated. In most cases, constellations are simply pairs or double pairs of antipodal points, which clearly sum up to zero. There are six non-trivial constellations, all of them are depicted. Note that all phases are multiples of $\vartheta = \pi/10$.

Consider the 2-unitary matrix $\mathcal{U}$. Interestingly, except for one block component in the matrix $\mathcal{U}$, all eight block components

are equivalent (up to a multiplication of rows and columns by adequate phases) to the following 4×4 unitary matrix:

$$V = \begin{bmatrix} a & a & b & b \\ 0 & 0 & c & -c \\ c & -c & 0 & 0 \\ b & b & -a & -a \end{bmatrix}.$$

Orthogonality relations between rows in the matrix above might be presented as pairs of antipodal points on the complex plane, for example, orthogonality between the first two rows reads

$$bc(1 - 1) = 0. \quad (\text{S5})$$

The exceptional block of matrix $\mathcal{U}$ is presented on the right top corner in Fig. 3. Six orthogonality relations between rows read

$$a^2(\omega^8 + \omega^{-8}) + b^2(\omega^4 + \omega^{-4}) = 0, \quad (\text{S6})$$

$$ab(1 + \omega^2 + \omega^{-8} - 1) = 0, \quad (\text{S7})$$

$$ab(\omega^{-2} + \omega^2 + \omega^{-8} + \omega^8) = 0,$$

up to a phase factor, with $\omega = \exp(i\pi/10)$. Each equation might be presented as a unitarity rectangle - a constellation of four points in the complex plane which sum up to zero, as it is shown on Fig. S1. Observe that the second and third equations above are relevant to two pairs of antipodal points on the complex plane. Geometric interpretation of the numbers a and b is shown in Fig. S2.

Although the matrices $\mathcal{U}^R$ and $(\mathcal{U}^R)^\Gamma$ enjoy the structure of nine 4×4 blocks, similar to $\mathcal{U}$, the particular arrangement inside their blocks is significantly different from the $\mathcal{U}$ matrix. Blocks in $\mathcal{U}^R$ and $(\mathcal{U}^R)^\Gamma$ matrices are of four distinct types up to multiplication of their rows and columns by phase factors, see Fig. S1. Orthogonality relations between rows of both matrices reflect their diversified structure. In particular, we distinguished five additional orthogonality relations given by the following equations:

$$a^2\omega^4 + ab(\omega^{10} + \omega^{-4}) + b^2\omega^{-4} = 0, \quad (\text{S8})$$

$$a^2\omega^{-3} + ab(\omega^5 + \omega^3) + b^2\omega^{-7} = 0, \quad (\text{S9})$$

$$ab(\omega^{-4} + \omega^{-6}) + bc\omega^5 = 0, \quad (\text{S10})$$

$$ab(\omega^{-8} + \omega^{-2}) + ac\omega^5 = 0, \quad (\text{S11})$$

$$a^2 + b^2\omega^4 + bc\omega^{-7} = 0. \quad (\text{S12})$$

Related constellations are presented on Fig. S1. The above-listed equalities provide orthogonality between rows in the three matrices $\mathcal{U}$, $\mathcal{U}^R$ and $(\mathcal{U}^R)^\Gamma$.

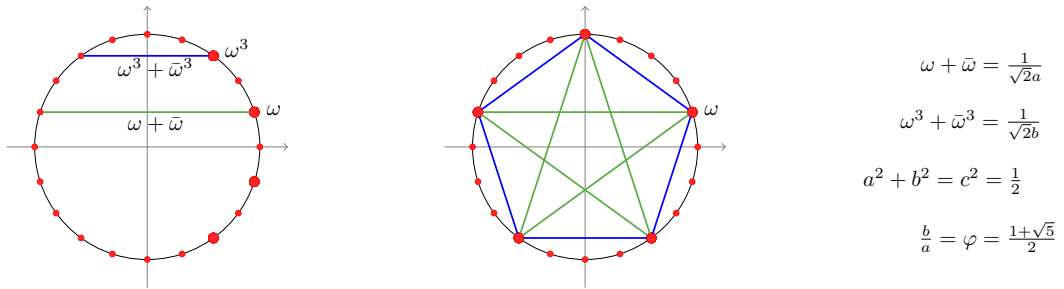


FIG. S2: Geometric interpretation of the constants a, b and c appearing in Eq. 4 with use of a regular pentagon. First two numbers contain the phase $\omega = \exp(i\pi/10)$ and are related to the golden ratio φ .

Observe that in the presented solution each officer is entangled with no more than 3 officers out of remaining 35. This implies the 2-unitary matrix $\mathcal{U}$ is sparse. An explicit form of the matrix $\mathcal{U}$ is available on line in several formats [S14], together with an explicit form of the corresponding AME(4,6) state determined by $\mathcal{U}$ and Eq. 3. Further numerical results suggest that any 2-unitary matrix $\mathcal{U}_{36}$ has complex entries. Therefore, it is tempting to conjecture that there exists no solution in the set $\mathbb{O}(36)$ of orthogonal matrices of this size.

Three amplitudes a, b, c which appear in the presented construction might be defined as the unique solution of the following algebraic equations: $a^2 + b^2 = c^2 = 1/2$ and $b/a = \varphi = (1 + \sqrt{5})/2$, see Fig. S2. Notice the similarities between algebraic equations which lead to values a, b, c , and the algebraic equations which lead to the amplitudes in a heterogeneous AME state in $2 \times 3 \times 3 \times 3$ system presented in [S15].

The phases of the coefficients shown in Fig. 3 of the main body of the paper, being multiples of $\omega = \exp(i\pi/10)$, are chosen in such a way that all 36 quantum states $|\psi_{ij}\rangle$, each represented by a single row of the 2-unitary matrix $\mathcal{U}$, are equivalent to the standard, two-qubit Bell state. This is fact easy to see for any state formed by two coefficients of moduli, $|c| = 1/\sqrt{2}$, as states $|\psi_{11}\rangle$ or $|\psi_{56}\rangle$ represented in the second and the third line in the upper left block in Fig. 3 respectively. To show that this property holds also for other states, note that the state $|\psi_{63}\rangle$ corresponding to the first line of the aforementioned block can be written in the product basis as

$$|\psi_{63}\rangle = a\omega^{10}|11\rangle + b\omega^{15}|12\rangle + b\omega^5|21\rangle + a|22\rangle.$$

Thus the partial trace of the projector reads, $\text{Tr}_B|\psi_{63}\rangle\langle\psi_{63}| = \text{diag}(a^2 + b^2, a^2 + b^2) = \mathbb{I}/2$. This proves that $|\psi_{63}\rangle$ is locally equivalent to the maximally entangled Bell state. A similar reasoning works for all other states consisting of four terms and represented in Fig. 3 by green and yellow elements. Hence all 36 states, corresponding to 36 entangled officers of Euler, can be considered as maximally entangled, two qubit states.

III. GENERATING 2-UNITARY MATRIX OF ORDER 36 USING A DYNAMICAL MAP

Entangling power of a bipartite unitary gate U is defined as the mean entanglement produced by the gate, $e_p(U) = C_d \overline{\mathcal{E}(|\psi_{AB}\rangle)}$ with $|\psi_{AB}\rangle = U(|\phi_A\rangle \otimes |\phi_B\rangle)$. The average, indicated by the overline, is taken over the Haar measure of random states in each subsystem [S16] and we choose the normalization $C_d = (d+1)/(d-1)$ so that the maximum value of the entangling power is 1. As a measure of entanglement it is convenient to choose the linear entropy of the reduced density matrix, $\mathcal{E}(|\psi\rangle_{AB}) = 1 - \text{Tr}(\rho_A^2)$, where $\rho_A = \text{Tr}_B|\psi_{AB}\rangle\langle\psi_{AB}|$. An alternative approach to measure entanglement in a bipartite gate U of order d^2 is to use its operator Schmidt decomposition [S17] $U = \sum_{j=1}^{d^2} \sqrt{\lambda_j} A_j \otimes B_j$, where the matrices A_j and B_j form an orthonormal basis in the space of operators, while the Schmidt coefficients λ_j are given by squared singular values of the reshuffled matrix U^R – see Eq. 2. To quantify non-locality of the gate one uses the *operator entanglement*, defined by the linear entropy of the Schmidt vector, $E(U) = 1 - (\sum_{j=1}^{d^2} \lambda_j^2)/d^4$. It is convenient to introduce the SWAP operator S , defined by the relation $S(|\phi_A\rangle \otimes |\phi_B\rangle) = |\phi_B\rangle \otimes |\phi_A\rangle$. Note that S^R is unitary, which implies that $E(S) = 1 - 1/d^2$. It allows one to show a direct link between both quantities and express the entangling power of U in terms of the operator entanglement [S16],

$$e_p(U) = \frac{1}{E(S)} (E(U) + E(US) - E(S)), \quad (\text{S13})$$

which implies the normalization, $0 \leq e_p(U) \leq 1$. Lower bound, $e_p(U) = 0$ is saturated by any local gate of a product form, $U = u_A \otimes u_B$, and the SWAP gate S .

$\tilde{P} =$	11	22	33	44	55	66	$=$	$A\spadesuit$	$K\clubsuit$	$Q\diamondsuit$	$J\heartsuit$	$10\clubsuit$	$9\spadesuit$
	23	14	45	36	61	52		$K\diamondsuit$	$A\heartsuit$	$J\clubsuit$	$Q\spadesuit$	$9\spadesuit$	$10\clubsuit$
	32	41	64	53	16	25		$Q\clubsuit$	$J\spadesuit$	$9\heartsuit$	$10\diamondsuit$	$A\spadesuit$	$K\clubsuit$
	46	35	51	62	24	13		$J\spadesuit$	$Q\clubsuit$	$10\spadesuit$	$9\clubsuit$	$K\heartsuit$	$A\diamondsuit$
	54	63	26	15	42	31		$10\heartsuit$	$9\diamondsuit$	$K\spadesuit$	$A\clubsuit$	$J\clubsuit$	$Q\spadesuit$
	65	56	12	21	33	44		$9\clubsuit$	$10\spadesuit$	$A\clubsuit$	$K\spadesuit$	$Q\diamondsuit$	$J\heartsuit$

FIG. S3: The design in $d = 6$ that is the closest possible to being an OLS [S19]. The two pairs of marked entries are repeated and not all possible 36 pairs are found.

Entangling power does not distinguish between locally inequivalent gates like U and US , as $e_p(U) = e_p(US)$. To distinguish

them one can use a complementary quantity called *gate typicality* [S18],

$$g_t(U) = \frac{1}{2E(S)} \left(E(U) - E(US) + E(S) \right), \quad (\text{S14})$$

satisfying $0 \leq g_t(U) \leq 1$. Lower bound, $g_t(U) = 0$, is attained by gates of a product form, while the upper bound $g_t(U) = 1$ is achieved by the SWAP gate and locally equivalent gates. Any 2-unitary matrix $\mathcal{U}$ is maximally non-local, also if composed with SWAP, and one has $E(\mathcal{U}) = E(\mathcal{U}S) = E(S)$, so that $g_t(\mathcal{U}) = 1/2$ and $e_p(\mathcal{U}) = 1$. Note that there is no 2-unitary matrix of size $d^2 = 4$, for which the maximal value $e_p = 1$ of the entangling power is achieved [S16, S19]. This is equivalent to the fact that there are no AME states for a four-qubit system [S20].

To look for 2-unitary matrices of size d^2 using the dynamical map, $U_{n+1} = \mathcal{M}_{\Gamma R}[U_n]$, presented in the main body of the text one needs to find an appropriate initial matrix. While for $d = 3$ a random unitary matrix of order nine with a significant probability generates a 2-unitary matrix, finding a suitable seed for $d = 6$ is considerably more demanding. It is natural to consider the design which gives the best approximation to a Graeco-Latin square [S19] and this is shown in Fig. S3.

$\tilde{P}_s =$	11 22 33 44 55 66	$=$	A♠	K♣	Q♦	J♥	10♣	9*
	23 14 45 36 61 52		K♦	A♥	J♣	Q*	9♠	10♣
	32 41 64 53 16 25		Q♣	J♠	9♥	10♦	A*	K♣
	46 35 51 62 24 13		J*	Q♣	10♠	9♣	K♥	A♦
	64 56 26 15 43 31		9♥	10*	K*	A♣	J♦	Q♠
	55 63 12 21 42 34		10♣	9♦	A♣	K♠	J♣	Q♥

FIG. S4: The design in $\tilde{P}_s$ does not form an OLS of dimension 6 since two pair of ranks are in the same columns. Its small perturbation used as a seed to the algorithm gives the 2-unitary matrix $\mathcal{U}_{36}$ and the desired state $|\text{AME}(4, 6)\rangle$.

A permutation matrix of order 36, denoted as P_{36} , can be obtained from $\tilde{P}$: if P_{36} is partitioned into 6×6 blocks, the only nonzero ($= 1$) entry of the ij -th block is given by the corresponding entry in $\tilde{P}$. For example, the $(5, 1)$ block is such that its 4th column and 5th row is 1. This has the maximum entangling power over all permutations of order 36 and is given by $e_p(P_{36}) = 314/315 \approx 0.996825$. If one starts with P_{36} as the seed, then $e_p(U_n) \rightarrow e_p(A) = 419/420 \approx 0.9976$ as $n \rightarrow \infty$ where $U_n = \mathcal{M}_{\Gamma R}^n[P_{36}]$. Interestingly, A is an orthogonal matrix such that A^Γ is unitary but A^R fails to be one.

This is an encouraging result and gives a way to explore unitary operators which have entangling powers larger than that of P_{36} . Similarly, if we start in the neighborhood of P_{36} , *i.e.* we take seeds of the form $P_{36} \exp(i\varepsilon H)$ where $\varepsilon \ll 1$ and H is Hermitian; $H = (M + M^\Gamma)/2$ with entries of M sampled from the normal distribution, then the map converges to unitaries with larger values of entangling power. However, $e_p(U_n) \approx 0.9991$ is the largest value obtained by us while starting in the vicinity of P_{36} (and for sufficiently large n).

In order to generate a 2-unitary matrix of size 36, one can search in the vicinity of other permutation matrices. Since the search space is very large ($36! \approx 10^{41}$), we restrict our attention to permutations that are in the vicinity of P_{36} . One of the permutations that works, denoted below as P_s , can be constructed from the design in Fig. S4 as described above.

The matrix $\tilde{P}_s$ differs from $\tilde{P}$ in the last two rows, see Fig. S4. The entangling power of the permutation matrix P_s is $e_p(P_s) = 104/105 \approx 0.9905$. Much better results can be obtained if one starts with a matrix from the neighborhood of P_s , as indicated above. The dynamical map with a finite probability ($p \approx 6\%$) converges to a 2-unitary matrix such that $e_p(U_n) = 1$ up to a machine precision for $n \sim 10^3$. Trajectories of some initial seed unitaries in the neighborhood of P_s are shown in Fig. S5. Every third iteration is marked. Most of these seed unitaries converge to strongly attracting fixed points of the map, such as A or AS (local extrema) while a few converge to 2-unitaries (global extrema). Nearby initial conditions with almost the same values of entangling power and gate typicality converge to different fixed points and explain the complex dynamics induced by the map on the (e_p, g_t) plane. The iteration procedure and convergence of the trajectory U_n to 2-unitary matrix on the (e_p, g_t) plane is visualised in Fig. S5. Convergence speed and the accuracy obtained is quantitatively described in Fig. S6. and implies that after a sufficiently large number of iterations, matrix U_n becomes 2-unitary. The output matrix, $\mathcal{U} = U_n$, can be put in a block diagonal form consisting of three blocks of size 12. There are also other ways of getting appropriate seeds to generate 2-unitary operators, such as enphasing of the permutation P_s (equivalent to multiplication by a diagonal unitary).

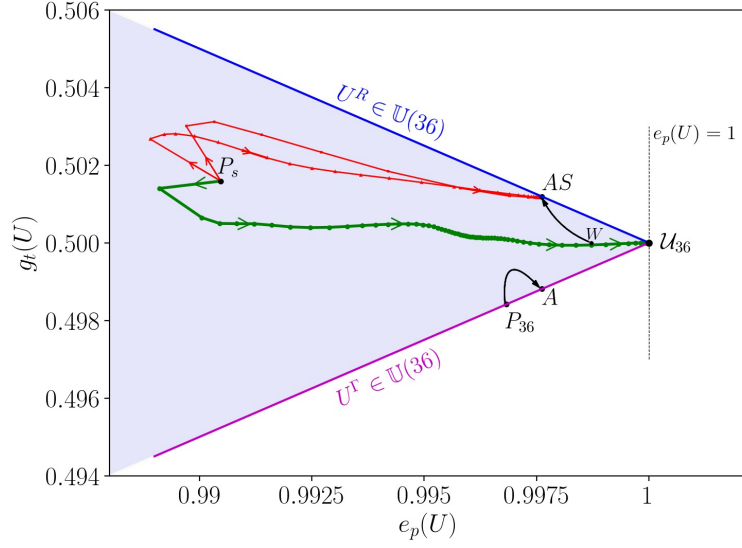


FIG. S5: A sample of trajectories initiated in the neighborhood of P_s and generated by the map $\mathcal{M}_{\Gamma_R}$ are shown, where every third iteration is marked. Many of the trajectories end up at a strongly attracting fixed point labelled A or its partner that is multiplied by the SWAP gate S , AS while a small fraction are able to reach the 2-unitary fixed point, $\mathcal{U}_{36}$. If the map is initiated from the best approximation to an OLS, P_{36} , or from its neighborhood the trajectory ends up mostly at the point corresponding to the matrix A , which has a larger entangling power than P_{36} . If one starts from W which is an orthogonal matrix with an even larger entangling power than A , it ends up at the point corresponding to AS .

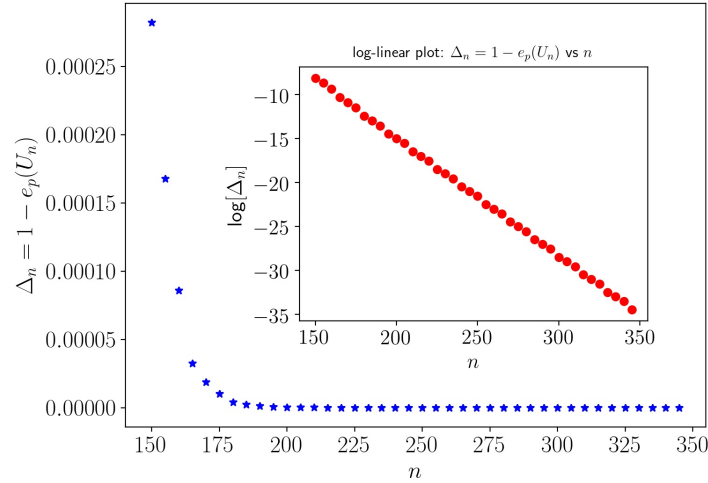


FIG. S6: Convergence of a trajectory initiated in the neighborhood of P_s to a 2-unitary matrix quantified by the deviation $\Delta_n = 1 - e_p(U_n)$ is plotted as a function of the number n of iterations. For $n > 150$ the deviation Δ_n decays exponentially as shown in the inset.

IV. AN APPARENT SOLUTION OF THE EULER'S PROBLEM FOR $d = 6$

An interesting practical application of the standard Euler's problem of 36 officers is worth to be mentioned here. A puzzle called *36cuBe* designed in 2008 by D. C. Niederman is directly linked to this mathematical question: the player obtains 36 pieces of six colors and of six different heights and is supposed to place them in the square to obey all the rules of OLS - see Fig. S7.

[S1] A. J. Scott, Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions, *Phys. Rev. A* **69**, 052330 (2004).

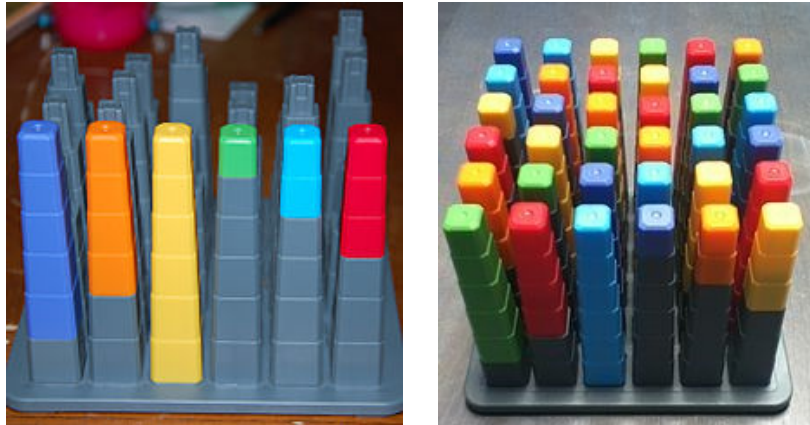


FIG. S7: Left panel: Puzzle 36cub advertised as *the World's Most Challenging Puzzle* consisting of 36 pieces of six colors and six heights and (right panel) its apparent solution. Closer inspection of all the pieces reveals that it corresponds to the pattern presented in Fig. S4, as two columns contain two pieces of the same height, in agreement with the conjecture of Euler and the theorem of Tarry.

- [S2] W. Helwig, W. Cui, A. Riera, J. Latorre, and H.-K. Lo, Absolute maximal entanglement and quantum secret sharing, *Phys. Rev. A* **86**, 052335 (2012).
- [S3] F. Huber and N. Wyderka, Table of AME states, Accessed: July 2021.
- [S4] P. Mazurek, M. Farkas, A. Grudka, M. Horodecki, and M. Studziński, Quantum error-correction codes and absolutely maximally entangled states, *Phys. Rev. A* **101**, 042305 (2020).
- [S5] D. Goyeneche, D. Alsina, A. Riera, J. Latorre, and K. Życzkowski, Absolutely maximally entangled states, combinatorial designs and multi-unitary matrices, *Phys. Rev. A* **92**, 032316 (2015).
- [S6] B. Bertini, P. Kos, and T. Prosen, Operator Entanglement in Local Quantum Circuits I: Chaotic Dual-Unitary Circuits, *SciPost Phys.* **8**, 067 (2020).
- [S7] S. A. Rather, S. Aravinda, and A. Lakshminarayan, Creating ensembles of dual unitary and maximally entangling quantum evolutions, *Phys. Rev. Lett.* **125**, 070501 (2020).
- [S8] F. Pastawski, B. Yoshida, D. C. Harlow, and J. Preskill, Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence, *Journal High Energy Phys.*, **2015**, 1 (2015).
- [S9] D. Goyeneche, Z. Raissi, S. Di Martino, and K. Życzkowski, Entanglement and quantum combinatorial designs, *Phys. Rev. A* **97**, 062326 (2018).
- [S10] B. Musto and J. Vicary, Orthogonality for Quantum Latin Isometry Squares, *EPTCS* **287**, 253 (2019).
- [S11] A. Rico, Absolutely maximally entangled states in small system sizes, Master Thesis, Innsbruck (2020).
- [S12] T. Benoist and I. Nechita, On bipartite unitary matrices generating subalgebra-preserving quantum operations, *Linear Algebra and Appl.* **521**, 70 (2017).
- [S13] G. De las Cuevas, T. Drescher and T. Netzer, Quantum magic squares: dilations and their limitations, *J. Math. Phys.* **61**, 111704 (2020).
- [S14] Consult mathematical files [available here](#); A. Rico, *unpublished note*, 2021
- [S15] F. Huber, C. Eltschka, J. Siewert, and O. Gühne, Bounds on absolutely maximally entangled states from shadow inequalities, and the quantum MacWilliams identity, *J. Phys.* **51**, 175301 (2018).
- [S16] P. Zanardi, Entanglement of quantum evolutions, *Phys. Rev. A* **63**, 040304 (2001).
- [S17] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States*. 2 Ed., Cambridge (2017).
- [S18] B. Jonnadula, P. Mandayam, K. Życzkowski, and A. Lakshminarayan, Impact of local dynamics on entangling power, *Phys. Rev. A* **95**, 040302 (2017).
- [S19] L. Clarisse, S. Ghosh, S. Severini, and A. Sudbery, Entangling power of permutations, *Phys. Rev.*, **A 72** (2005).
- [S20] A. Higuchi and A. Sudbery, How entangled can two couples get?, *Phys. Lett. A* **273**, 213 (2000).

Local hidden variable value without optimization procedures

Dardo Goyeneche¹, Wojciech Bruzda², Ondřej Turek³, Daniel Alsina⁴, and Karol Życzkowski^{2,5}

¹Departamento de Física, Facultad de Ciencias Básicas, Universidad de Antofagasta, Casilla 170, Antofagasta, Chile

²Institute of Theoretical Physics, Jagiellonian University, ul. Łojasiewicza 11, 30-348 Kraków, Poland

³Department of Mathematics, Faculty of Science, University of Ostrava, 701 03 Ostrava, Czech Republic

⁴School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, UK

⁵Center for Theoretical Physics, Polish Academy of Sciences, Al. Lotników 32/46, 02-668 Warsaw, Poland

November 23, 2021

The problem to compute the local hidden variable (LHV) value of a Bell inequality plays a central role in quantum nonlocality. In particular, this problem is the first step to characterize the LHV polytope in a given scenario. In this work, we establish a relation between the LHV value of bipartite Bell inequalities and the mathematical notion of excess of a matrix. Inspired by the strongly developed theory of excess, we derive several results having a direct impact in the field of quantum nonlocality. As consequence, we provide the LHV value for infinite families of bipartite Bell inequalities, with an unbounded number of measurement settings, without requiring to solve any optimization problem. We also find tight Bell inequalities for a large number of measurement settings. Furthermore, we show that the entire set of optimal LHV strategies of Bell inequalities, induced by certain Hadamard matrices, equals the entire set of vectors mutually unbiased to certain pair of bases.

1 Introduction

In a seminal paper [1], John Bell proved that quantum correlations cannot be explained from deterministic and local hidden variable (LHV) models [2]. Since then, an increasing interest in the field has triggered a large development of the theory, supported by experimental implementations and practical applications. A feasible generation and certification of quantum nonlocality permits to design quantum technological applications having practical advantage with respect to their classical counterpart. For instance, quan-

tum nonlocality can be used as a resource to outperform classical communication in certain distributed computing tasks [3], and enhances the communication power in the context of information theory [4]. Quantum nonlocality has also led to the emergence of device-independent protocols, where the involved parties do not need to trust their measurement devices [5, 6]. Concrete practical applications include quantum key distribution [7, 8, 9, 10, 11, 12, 13], random number generation [14, 15, 16, 17], quantum cryptography [10, 11, 12, 13], and testing quantumness of clouds of quantum computers [18, 19, 20], among others.

A fundamental open question in quantum nonlocality is the following: *when does a given Bell inequality exhibit quantum advantage with respect to LHV models?* Finding the answer to this question is crucial for the development of the practical applications shown above. For instance, a way to generate genuine random numbers [21], quantum cryptographic [22] and device independent [23] protocols rely on the nonlocal essence of Nature. In order to answer the aforementioned question, one needs to find both the LHV and quantum values. However, the problem of finding the LHV value of a given Bell inequality is NP-hard, as a function of the number of measurement settings and outcomes. It is thus of fundamental relevance to search for a way to estimate the LHV value without involving any optimization procedure. In spite of a considerable effort made during the last decades – see [24] and references therein – the complete understanding of the boundary between LHV theories and quantum nonlocality remains open even in bipartite scenarios composed by a small number of measurement settings and outcomes [25].

In this work, we introduce an interesting tool that might shed some light to the above described problem. That is, we link the problem to find the LHV of bipartite Bell inequalities to the problem of finding matrices with maximal *excess* [26, 27]. This one-to-one correspondence allows us to find the LHV value for infinitely many families of bipartite Bell inequalities in a wide range of scenarios. The observed connection plays an important role, specially when taking into account that identification of tight Bell inequalities relies on the study of LHV strategies.

This work is organized as follows. In Section 2, we introduce our main tool, i.e. the theory of excess of a matrix. In Section 3, we give a brief introduction to Bell inequalities. In Section 4, we establish the one-to-one connection between maximal excess and the LHV value of bipartite Bell inequalities. This connection allows us to derive an upper for the LHV value that is stronger than known upper bounds for the quantum value. In Section 5, we show how to find the LHV value of several classes of Bell inequalities without requiring to implement any optimization procedure. In Section 6, we find a link between some classes of Bell inequalities and the mutually unbiased bases problem. Additionally, in Section 7 we find seven tight Bell inequalities for the two outcomes scenario with a large number of measurement settings, ranging between 8 and 20. Proofs of all our results are provided in Appendix C.

2 Excess of a matrix

A square matrix H with entries ± 1 is called *Hadamard* if its columns are pairwise orthogonal. In 1973, Schmidt [26] asked about the maximal number of 1's that could be present in a Hadamard matrix of a given order n . To that sake he introduced the notion of *excess* of a Hadamard matrix H as the difference between the number of the positive and negative entries of H . This value is usually denoted by $\Sigma(H)$.

The maximal possible value of $\Sigma(H)$, among all Hadamard matrices of a given order n , called *maximal excess*, was analyzed by Best [27], who found the following bounds:

$$n^2 2^{-n} \binom{n}{\frac{n}{2}} \leq \max \Sigma(H) \leq n\sqrt{n}. \quad (1)$$

where the maximum is taken over all existing Hadamard matrices of order n .

Moreover, there are infinitely many orders n for which $\max \Sigma(H)$ is already known [27, 33, 34, 35, 36, 37]. For a Hadamard matrix of order n , upper bound (1) is attained if and only if H is a *constant row sum Hadamard matrix*, i.e. the sum of each row gives the same value [27]. Let us note that constant row sum matrices are sometimes called *regular* in the context of Hadamard matrices [27]. Constant row sum Hadamard matrices of order n only exist when n is a square number. Thus, the upper bound (1) is not saturated when $n = 2$. As we will see later, this has a direct connection with the fact that the CHSH Bell inequality has quantum advantage.

Note that the excess of a Hadamard matrix is also equal to the sum of all entries of H . This allows a straightforward extension of the notion of excess to any complex square matrix M of order n .

Definition 1. *The sum of all entries of a square matrix M of order n is called its excess, denoted*

$$\Sigma(M) = \sum_{j,k=0}^{n-1} M_{jk}. \quad (2)$$

In the next section, we introduce the notion of maximal excess for all matrices M related to bipartite Bell inequalities.

3 Bell inequalities

Suppose a bipartite scenario where both observers, Alice and Bob, implement m measurement settings per side having q outcomes each. From an ensemble of identically prepared quantum states they can estimate a joint probability distribution $P(a, b|x, y)$, where $a, b \in [0, \dots, q-1]$ denote outcomes for Alice and Bob, respectively, conditioned to the measurement settings $x, y \in [0, \dots, m-1]$, respectively. It can be shown that a single correlation of the form $P(a, b|x, y)$ is not enough evidence to ensure a conflict with LHV models [28]. However, a linear combination of such quantum probabilities attains values that cannot be reproduced by any LHV model [1]. Such expressions, known as *Bell inequalities* [24], are defined as follows:

$$\sum_{x,y=0}^{m-1} \sum_{a,b=0}^{q-1} S_{xy}^{ab} P(a, b|x, y) \leq \mathcal{C}, \quad (3)$$

where S_{xy}^{ab} is a real-valued function and $\mathcal{C}$, so called *classical* or local hidden variable (LHV) value, is defined as the maximal achievable value of the left hand side in Eq. (3) in a local deterministic theory. That is, there is statistical independence between Alice's and Bob's results, $P(a, b|x, y) = P(a|x)P(b|y)$, and the outcomes are deterministic, i.e. $P(a|x), P(b|y) \in \{0, 1\}$, for every pair of measurement settings $x, y \in \{0, \dots, m-1\}$ and outcomes $a, b \in \{0, \dots, q-1\}$. The quantum value $\mathcal{Q}$ is defined as the maximal possible value of the left hand side in (3), if optimization is implemented over all joint probability distributions admissible in quantum theory when observers implement local measurements and do not communicate their results. Probabilities in quantum theory take the form $P(a, b|x, y) = \text{Tr}[(\Pi_a^x \otimes \Pi_b^y)\rho_{AB}]$, where $\{\Pi_a^x\}$ and $\{\Pi_b^y\}$ define Positive-Operator Valued Measure (POVM), while ρ_{AB} is a bipartite quantum state. The remarkable observation of Bell is that LHV correlations can be weaker than quantum correlations under certain conditions, thus it is possible to have $\mathcal{C} < \mathcal{Q}$. This important result, together with its experimental verification [29], confirmed the nonlocal behavior of Nature.

Inequality (3), when restricted to quantum mechanics, can be equivalently represented with expectation values of correlators through the discrete double Fourier transform of the joint probability distribution [30]:

$$P(a, b|x, y) = \frac{1}{\sqrt{q}} \sum_{s,t=0}^{q-1} \omega^{as+bt} \langle A_x^s \otimes B_y^t \rangle, \quad (4)$$

where $\omega = e^{2\pi i/q}$. Here, A_x^s denotes the s^{th} power of the quantum observable A_x associated to Alice, analogously for Bob. We assume that every observable has q outcomes, associated with q different roots of unity as eigenvalues.

Note that relation (4) is constrained to quantum joint probability distributions, thus it agrees the no-signaling principle [31]. That is,

$$\begin{aligned} \sum_{b=0}^{q-1} P(a, b|x, y) &= \sum_{b=0}^{q-1} P(a, b|x, y'), \\ \sum_{a=0}^{q-1} P(a, b|x, y) &= \sum_{a=0}^{q-1} P(a, b|x', y), \end{aligned} \quad (5)$$

for every $a, b = 0, \dots, q-1$ and $x, y, x', y' = 0, \dots, m-1$. Conditions (5) imply that parties cannot have instantaneous communication.

Equation (4) assumes quantum mechanics on the right hand side, agreeing with the no-signaling principle due to the fact that $A_x^0 = B_y^0 = \mathbb{I}$, for any x, y .

Due to (4), inequality (3) can be then rewritten as

$$\sum_{x,y=0}^{m-1} \sum_{s,t=0}^{q-1} M_{m(s+1)+x, m(t+1)+y} \langle A_x^s \otimes B_y^t \rangle \leq \mathcal{C}, \quad (6)$$

where M is a square matrix of order $n = mq$ having entries

$$M_{ms+x, mt+y} = \frac{1}{\sqrt{q}} \sum_{a,b=0}^{q-1} \omega^{(s-\lceil \frac{q}{2} \rceil)a + (t-\lceil \frac{q}{2} \rceil)b} S_{xy}^{ab}, \quad (7)$$

for every $0 \leq s, t < q$, $0 \leq x, y < m$. The shifts by $\lceil q/2 \rceil$ appearing in the right hand side of (7) are introduced to have the symmetry explained below. For scenarios considering two outcomes, i.e. $q = 2$, matrix M has to be real. When $q > 2$, matrix M can have complex entries but it has to satisfy a symmetry relation. Given that operators A_x^s and B_y^t are unitary, the left hand side of (6) is real for any $q \geq 2$ if M satisfies the condition

$$M_{m[2\lceil \frac{q}{2} \rceil - s]_q + x, m[2\lceil \frac{q}{2} \rceil - t]_q + y} = (M_{ms+x, mt+y})^*, \quad (8)$$

for every $0 \leq s, t < q$, $0 \leq x, y < m$, where the asterisk denotes complex conjugation and $[x]_q$ denotes x modulo q . Matrices M satisfying (8) generalize centro-hermitian matrices defined in [32], and they will be called *block centro-hermitian*. These matrices contain real blocks of order m that are centers of the hermitian symmetry, i.e. every pair of opposite blocks with respect to a center of symmetry are related by hermitian conjugation. The general structure of this new class of matrices is shown in Appendix A. For odd values of q there is only one center of hermitian symmetry, located at the center of the matrix. For even q , there are 4 equidistant centers of symmetry.

Remark 1. Notice that if $q = 2$, we have $[2\lceil \frac{2}{2} \rceil - s]_2 = s$ and $[2\lceil \frac{2}{2} \rceil - t]_2 = t$ for every $0 \leq s, t < 2$. Consequently, if $q = 2$, condition (8) asserts that M is real. In general, any matrix $M \in \mathbb{C}^{mq \times mq}$ obeying condition (8) has the following property:

- If q is even, entries $M_{ms+x,mt+y}$ are real for all $0 \leq x, y < m$ and $s, t \in \{0, q/2\}$ (due to $[2\lceil q/2 \rceil - 0]_q = 0$ and $[2\lceil q/2 \rceil - q/2]_q = q/2$).
- If $q > 1$ is odd, entries $M_{m\lceil q/2 \rceil + x, m\lceil q/2 \rceil + y}$ are real for all $0 \leq x, y < m$ (due to $[2\lceil q/2 \rceil - \lceil q/2 \rceil]_q = \lceil q/2 \rceil$).

We are now ready to introduce a notion of equivalence.

Definition 2. Let $q \geq 2$. We say that two matrices M and M' of order mq are q -equivalent if they obey (8) and $M' = D_1 M D_2$, where D_1 and D_2 are diagonal matrices whose $(ms+x)$ -th diagonal entries are s -th powers of a q -th root of the unity, for every $0 \leq s < q$ and $0 \leq x < m$.

Note that two q -equivalent matrices M and M' induce the same Bell inequality (6), up to a relabeling of outcomes for both Alice and Bob. Relabeling of settings holds in a similar way but it requires permutations instead of diagonal matrices. However, this case needs not to be considered as the excess is invariant under permutations. Definition 2 induces the following notion of maximal excess.

Definition 3. Let $q \geq 2$. We say that M of order mq has maximal excess with respect to q -equivalence if M obeys (8) and

$$\Sigma(M) = \max\{\Sigma(M'); M' \text{ is } q\text{-equivalent to } M\}.$$

An important class of inequalities are the so-called *correlation* Bell inequalities. These are inequalities of the form (6) such that there are no marginal terms, i.e. it has no terms associated to either $s = 0$ or $t = 0$. Physically, this means that every term of the inequality is composed by a quantity that exhibits correlations existing between the parties, whereas $s = 0$ and $t = 0$ depend on local phenomena for Bob and Alice, respectively. Let us introduce the entire set of matrices related to correlation Bell inequalities.

Definition 4. Let $q \geq 2$. We say that a matrix M is a correlation matrix if it satisfies (8) and $M_{\alpha,\beta} = 0$ when either $\alpha \leq m-1$ or $\beta \leq m-1$. The nontrivial part of M , i.e. the submatrix of order $n = m(q-1)$ having entries $M_{\alpha,\beta}$ with $m \leq \alpha, \beta \leq mq-1$ is called the *core* of M .

In Appendix A, we illustrate the structure of matrices M for odd and even orders, and the notion of core of M . Note that if M is a correlation matrix, the core of M is a Hadamard matrix, and if $q = 2$, Definition 3 reduces to the standard notion of the maximal excess for Hadamard matrices, introduced in Section 2

4 Excess and LHV models

In this section, we establish a connection between the notion of excess of certain class of matrices and the LHV value of a Bell inequality. The key observation is the following. Given a Bell inequality (6), we can always find diagonal unitary matrices D_1 and D_2 , having the q^{th} roots of the unity along their main diagonal, such that $M' = D_1 M D_2$ has optimal LHV strategy when all outputs for Alice and Bob are equal to $+1$. Transformation $M \rightarrow M'$ in (6) implies a relabeling of outputs of the measurement apparatuses for both Alice and Bob. Thus, the LHV of the related Bell inequality is given by the sum of all the entries of matrix M' . Clearly, matrices M' with this property are those having excess $\Sigma(M)$ equal to the LHV of the related Bell inequality. Let us now formalize this observation.

Proposition 1. Let M be a matrix of order mq having maximal excess with respect to q -equivalence. Then, the Bell inequality (6), having q outcomes per setting, has LHV value $\mathcal{C}(M)$ equal to the excess of the matrix M , $\Sigma(M)$. Conversely, for any Bell inequality (6) induced by a matrix M , there is a matrix M' satisfying the symmetry (8) such that $\mathcal{C}(M') = \Sigma(M')$.

The relevance of Prop. 1 relies in the fact that matrices M having maximal excess have been exhaustively studied by mathematicians during the last five decades, including a wide range of Hadamard matrices [27, 33, 34, 35, 36, 37, 38], complex Hadamard matrices [39], Hadamard tensors [40] and orthogonal designs [41]. These results considerably extend the set of Bell inequalities for which the LHV value is known [24], which is not a minor observation taking into account that the computational complexity of calculating the LHV value of a bipartite Bell inequality is NP-hard [42]. For the rest of the work, we restrict our attention to matrices M associated to Bell inequalities achieving the LHV value when

the local deterministic strategies of both Alice and Bob have outcomes $+1$.

Let us illustrate Prop. 1 with the celebrated CHSH inequality [43], associated to the matrix $M = \{\{0, 0, 0, 0\}, \{0, 0, 1, 1\}, \{0, 0, 1, -1\}\}$, whose core is a Hadamard matrix of order $n = 2$:

$$\langle A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1 \rangle \leq 2. \quad (9)$$

Here, A_i and B_j are dichotomic quantum observables represented by Hermitian operators having eigenvalues ± 1 each. This Hadamard matrix has maximal excess $\Sigma(M) = 2$ [27], coinciding with the LHV value of the CHSH inequality [43].

The next result requires the introduction of the numerical radius $r(M) = \max_{|\psi\rangle \in \mathcal{H}_n} |\langle \psi | M | \psi \rangle|$. Now, let us express an upper bound for excess in terms of the numerical radius.

Proposition 2. *Let M be a matrix of order $n = mq$ having maximal excess with respect to q -equivalence. Then, the following upper bound holds for the induced Bell inequality:*

$$\mathcal{C}(M) \leq nr(M). \quad (10)$$

For any matrix M , we have that $\rho(M) \leq r(M) \leq \sigma(M)$, where $\rho(M) = \max_j |\lambda_j(M)|$ is the spectral radius and $\sigma(M) = \max_j \sqrt{\lambda_j(MM^\dagger)}$ is the maximal singular value of M , also called spectral norm. For normal matrices, equalities $\rho(M) = r(M) = \sigma(M)$ hold. Consequently, the upper bound (10) is more restrictive than a well-known upper bound for the quantum value, which we recall in the following Observation.

Observation 1 ([44, 45]). *The quantum value of a bipartite Bell inequality, induced by a matrix M of order n , satisfies*

$$\mathcal{Q}(M) \leq n\sigma(M). \quad (11)$$

The characterization of the entire set of matrices M that saturate the bound (10) or (11) is open in every scenario. Let us now provide a new upper bound for which we can fully characterize its tightness, in every bipartite scenario.

Proposition 3. *Let M be a matrix of order $n = mq$ having maximal excess with respect to q -equivalence. Then we have*

$$\mathcal{C}(M) \leq \sqrt{n} \nu(M), \quad (12)$$

where $\nu(M) = \sqrt{\sum_{i=0}^{n-1} |\sum_{j=0}^{n-1} M_{ij}|^2}$. Moreover, upper bound (12) is saturated if and only if M is a constant row sum matrix. In such case, $\mathcal{C}(M) = ns$, where s is the constant row sum value.

Notice that the constant row sum value s occurring in Proposition 3 is always a positive number due to the assumption that M has maximal excess and to our initial assumption (8).

Let us show a further consequence of Prop. 3. If a matrix M with maximal excess is both constant row sum and unitary, then $\mathcal{C}(M) = n$, coinciding with the upper bound (11). Thus, $\mathcal{C}(M) = \mathcal{Q}(M) = n$, and the related Bell inequality does not have quantum advantage. In particular, if M is an unnormalized constant row sum Hadamard matrix, then $\mathcal{C}(M) = \mathcal{Q}(M) = n\sqrt{n}$. That is, we saturate both the Best bound (1) and the Epping-De Vicente bound (11), where the former one is a particular case of the second one. Interestingly, inequality (12) is saturated by all the matrices considered in nonlocal computation [46] and quantum games having no quantum advantage [47].

To illustrate Prop. 3, note that the correlation Bell inequality associated to the circulant Hadamard matrix $\text{core}(M) = \text{circ}[-1, 1, 1, 1]$ satisfies $\mathcal{C}(M) = \mathcal{Q}(M) = 8$, where there is no need to calculate the quantum value, as the LHV value saturates (11). As a further example, consider the three inequivalent constant row sum Hadamard matrices of order 16 [48], defining three inequivalent correlation Bell inequalities in the bipartite scenario composed of 16 measurement settings per side having 2 outcomes each. These three inequalities have both LHV and quantum values equal to 64. The same conclusion does not apply to the Hadamard matrix of order 2 (CHSH), as this Hadamard matrix does not have constant row sum.

On the other hand, non-unitary constant row sum matrices can imply a correlation Bell inequality having a quantum advantage. For instance, for $n = 3$ the matrix $\text{core}(M) = \text{circ}[(0, -1, 1)]$ satisfies $\mathcal{C}(M) = 4 < 3\sqrt{3} = \mathcal{Q}(M)$. Here, the quantum value $\mathcal{Q}(M)$ is achieved when considering measurement settings A_j and B_k of the form $U_j D U_j^\dagger$, for

$$U_j = \begin{bmatrix} \cos \alpha_j & \sin \alpha_j \\ \sin \alpha_j & \cos \alpha_j \end{bmatrix}, \quad (13)$$

$D = \{\{1, 0\}, \{0, -1\}\}$ and $\alpha_j = 0, \frac{2\pi}{3}, \frac{\pi}{3}$ for A_0, A_1, A_2 and $\alpha_j = \frac{\pi}{4}, \frac{7\pi}{12}, \frac{11\pi}{12}$ for B_0, B_1, B_2 , respectively.

Note that a weaker version of the bound (12) occurs when $\nu(M) = \|M\phi\| \leq \|M\|\|\phi\| = \sqrt{n}\sigma(M)$. In such case, the bound reduces to $\Sigma(M) \leq n\sigma(M)$, coinciding with the upper bound for the quantum value (11). From here and Prop. 2, an interesting observation arises.

Observation 2. *The problem to classify all correlation Bell inequalities with n settings for which there is no quantum advantage contains, as a subproblem, the problem of finding all constant row sum correlation matrices M of order n for which $\nu(M)$, defined in Prop. 3, equals the maximal singular value $\sigma(M)$. In particular, the problem contains the circulant Hadamard conjecture [49].*

There is a simple property that sometimes can reduce the complexity of calculating excess of a matrix: excess of a tensor product is the product of excesses, see Obs. 2.4 in [50]. Applying this property to Bell inequalities we have the following result.

Proposition 4. *Let M_1, M_2 be matrices of order $n_1 = m_1q$ and $n_2 = m_2q$, respectively. If both M_1 and M_2 have maximal excess with respect to q -equivalence and M_2 is real, then the LHV value of the Bell inequality induced by the tensor product matrix $M = M_1 \otimes M_2$, having q outcomes per setting, is given by $\mathcal{C}(M) = \mathcal{C}(M_1)\mathcal{C}(M_2)$.*

Note that the product of matrices producing a tight Bell inequality does not induce a tight inequality, in general. Indeed, the inequality induced by cores $H_4 = H_2 \otimes H_2$ is not tight, despite CHSH, induced by core H_2 , is tight. On the other hand, sometimes this occurs, as the core $H_8 = H_2 \otimes H_2 \otimes H_2$ induces a tight Bell inequality, see Section 7.

5 LHV value without requiring optimization

In this section, we show how to construct some families of correlation matrices M of order $n = m(q-1)$ that allow us to achieve the LHV of Bell inequalities with an unbounded number of measurement settings each, for $q = 2$ outcomes. The following results summarize some relevant contributions to excess theory achieved in the last four

decades. Before showing the results, let us recall some required notions. A matrix M is called skew symmetric if $M^T = -M$, where T denotes transposition. A conference matrix is a square matrix having zero main diagonal, ± 1 off-diagonal entries and orthogonal columns. A Hadamard matrix H is skew-type if $H - \mathbb{I}$ is skew symmetric.

Observation 3 ([51]). *If M is a skew-type Hadamard matrix of order $k \equiv 0 \pmod{4}$ or a conference matrix of order $k \equiv 2 \pmod{4}$, then there is a Hadamard matrix M of order $n = 4k(k-1)$ (thus $n \equiv 0 \pmod{16}$ and $n \equiv 8 \pmod{16}$, respectively), with maximal excess*

$$\Sigma(M) = 4(k-1)^2(2k+1). \quad (14)$$

Note that none of the Hadamard matrices from Observation 3 are equivalent to one having constant row sum, as the order n is not a square number. Thus, the related Bell inequalities are potential candidates to have a quantum advantage, in the sense that the upper bound (11) for the quantum value is not saturated.

Observation 4 ([52]). *Let M be a conference matrix of order n and let k be an odd integer such that $k \leq \sqrt{n-1} < k+2$. Then we have*

$$\Sigma(M) \leq \frac{n(k^2 + 2k + n - 1)}{2(k+1)}.$$

Equality holds if and only if either (i) $n-1$ is a square and M has constant row sum equal to k , or (ii) $n-1$ is not a square and row sums are either k or $k+2$.

For instance, let us show an infinite family of Bell inequalities, arising from Hadamard matrices of order $n = \ell + 1$, with $\ell \equiv 3 \pmod{4}$, for which the maximal excess is known. The Hadamard matrices have the form

$$M = \begin{pmatrix} -1 & \mathbf{1}_\ell^T \\ \mathbf{1}_\ell & A \end{pmatrix}, \quad (15)$$

where $\mathbf{1}_\ell$ is the all-one vector of length ℓ and the square matrix A of order ℓ is given by

$$A_{ij} = \begin{cases} 1 & \text{if } j-i \in C \cup \{0\} \\ -1 & \text{if } j-i \in \mathbb{F}_\ell \setminus (C \cup \{0\}) \end{cases}. \quad (16)$$

Here, $\mathbb{F}_\ell$ denotes the finite field of order ℓ and C is the set of nonzero squares of $\mathbb{F}_\ell$. This leads to the following observation.

Observation 5 ([53]). *Let m be an integer number such that $\ell = (2m + 1)^2 + 2$ is the power of a prime, and k be an even integer such that $k \leq \sqrt{n} < k + 2$. Also, let $t = k$ if $|n - k^2| < |n - (k + 2)^2|$ and $t = k - 2$ otherwise. Then the Hadamard matrix (15) of order $n = \ell + 1$ has maximal excess*

$$\Sigma(M) = n(t + 4) - 4s, \quad (17)$$

where s is the integer part of $n((t + 4)^2 - n)/(8t + 16)$.

As complementary information, a lower bound for the maximal excess of known Hadamard matrices has been found up to order $n = 1000$, in many cases achieving the maximal excess [51]. There are much more explicit results for the maximal excess of Hadamard matrices than those shown above. See for instance [54, 55, 56, 57] and references therein. Also, maximal excess has been found for weaving Hadamard matrices [38], complex Hadamard matrices [39] and orthogonal designs [41]. Furthermore, maximal excess for tensors [40] opens the possibility to naturally extend our results to multipartite systems. Interestingly, maximal excess for tensors is connected with the so-called *discrepancy of multi-variable functions*, associated with certain multiparty communication problems, see [40] and references therein. This connection might contribute to a better understanding of communication complexity for multipartite quantum systems [58].

We believe the results and references shown in this section provide a valuable contribution to quantum nonlocality theory. On the one hand, this considerably extends the set of Bell inequalities for which the classical value is currently known [24]. On the other hand, the same refined techniques used in these references might inspire researchers to develop more efficient ways to find the LHV value for larger classes of Bell inequalities.

6 Excess and mutually unbiased bases

In this section, we show that the LHV value of a Bell inequality induced by a correlation matrix M with core equal to a Hadamard matrix is closely related to the notion of *mutually unbiased bases* [59]. Two orthonormal bases in $\mathbb{R}^n$,

$\{\phi_j\}$ and $\{\psi_k\}$, are mutually unbiased (MUB) if $|\langle \phi_j | \psi_k \rangle|^2 = 1/n$, for every $j, k = 0, \dots, n-1$. Let us start with the following observation, see proof of Theorem 3 in [27] and [60].

Observation 6. *The LHV value of a Bell inequality with two outcomes, induced by a correlation matrix M with core of order $n = m(q - 1)$, is given by*

$$\mathcal{C}(M) = \max_{x \in \{-1, 1\}^n} \|\text{core}(M)|x\rangle\|_1, \quad (18)$$

where $\|\sum_{i=1}^n v_i |i\rangle\|_1 = \sum_{i=1}^n |v_i|$ is the taxicab norm.

On the one hand, this result reduces the number of dichotomic variables involved in maximal excess calculation. This fact has been independently found in the context of Bell inequalities, see (5) in [60]. On the other hand, it allows us to establish a remarkable connection between the LHV value of a Bell inequality and the mutually unbiased bases problem.

Proposition 5. *Let M be a correlation matrix with core equal to a Hadamard matrix of order n . If there is a real vector $|x\rangle$ with entries ± 1 , unbiased to the rows of M , then $\mathcal{C}(M) = n\sqrt{n}$. Conversely, if $\mathcal{C}(M) = n\sqrt{n}$, then there exists a vector $|x\rangle$ having entries ± 1 that is unbiased to the rows of $\text{core}(M)$.*

In particular, if M is a correlation matrix, $\text{core}(M)$ is a constant row sum matrix, and $|x\rangle$ is the all-one entries vector then $\mathcal{C}(M) = \sqrt{n}\nu(M)$, in agreement with Prop. 3. An interesting corollary arises.

Corollary 1. *If n is not a square number, then any pair of real mutually unbiased bases in dimension n is strongly unextendible. That is, there is no single vector unbiased to the pair of bases.*

Additionally, we have the following consequence.

Corollary 2. *If three real mutually unbiased bases $\{\mathbb{I}, H_1, H_2\}$ exist in dimension n , then both matrices H_1 and H_2 are equivalent to a constant row sum Hadamard matrix.*

Note that for $n = 2, 8, 12$ there are no triplets of real MUB, which coincides with the fact that there are no Hadamard matrices with constant row sum. For $n = 4$ there is a triplet, and a

unique class of Hadamard matrices, represented by the circulant one, that has a constant row sum. A non-trivial result occurs for $n = 16$, where there are 5 inequivalent Hadamard matrices, three of them having constant row sum [48].

Corollary 3. *For any pair of real mutually unbiased bases $\{\mathbb{I}, H\}$, with H being a constant row sum Hadamard matrix, there is at least one mutually unbiased vector. That is, such pairs of MUB are not strongly unextendible, in every dimension where such matrix H exists.*

As a final comment of the section, let us mention an interesting observation about the robustness of quantum nonlocality of maximally entangled states under the presence of white noise. The lower bound for excess (1) is $\sqrt{n/2}$, which is attainable for $n = 2$ only, as already noted by Best [27]. Bound (1) for the LHV value, together with the bound (11) for the quantum value, imply that the maximal possible quantum over classical ratio, when considering a correlation Bell inequality induced by a Hadamard matrix M of order n , is given by $Q/C = \sqrt{2}$, attainable for $n = 2$ only [27]. This result immediately implies the following statement: Any correlation Bell inequality induced by a core Hadamard matrix of order $n > 2$ has a quantum over classical ratio smaller than the one established by CHSH ($n = 2$), i.e. $Q/C = \sqrt{2}$. This further implies that the most efficient detection of nonlocality for noisy maximally entangled two-qubit state occurs for the CHSH inequality, among all bipartite correlation Bell inequalities with n settings and $q = 2$ outcomes generated by a Hadamard matrix of order n [61].

7 Tight Bell inequalities

Tight Bell inequalities define the facets of the LHV polytope. These hyperplanes completely characterize the set of correlations compatible with a LHV model. The quantum correlations space, for a bipartite scenario with m settings and q outcomes per party, is defined by all real vectors $v \in \mathbb{R}^{m^2 q^2}$ having entries of the form $\langle A_x^s \otimes B_y^t \rangle$, $x, y \in \{0, \dots, m-1\}$ and $s, t \in \{0, \dots, q-1\}$, where A_x and B_y are unitary operators having the q^{th} roots of unity as eigenvalues. The no-signaling conditions (5) restrict quantum correlations to a $d = m^2(q-1)^2$ di-

Number of settings (m)	Number of vertices	Number of affine independent vertices	Tightness
2	4	3	Tight
4*	4	3	Non-tight
8	64	63	Tight [†]
12	2640	143	Tight [†]
16 (1)*	896	105	Non-tight
16 (2)*	192	81	Non-tight
16 (3)*	64	45	Non-tight
16 (4)	21504	255	Tight [†]
16 (5)	21504	255	Tight [†]
20 (1)	20064	399	Tight [†]
20 (2)	20064	399	Tight [†]
20 (3)	20064	399	Tight [†]

Table 1: Study of tightness for bipartite correlation Bell inequalities of the form $\langle \sum_{\alpha, \beta=0}^{n-1} H_{\alpha\beta} A_\alpha \otimes B_\beta \rangle \leq \mathcal{C}(H)$, with $m = n$ measurement settings and $q = 2$ outcomes. Here, H is a Hadamard matrix of order $n = m(q-1)$. Note that $H = \text{core}(M)$ in (6), where M has order $n = mq$. All entries outside the core of M are zero. The table shows the number of vertices of the LHV polytope that is touched by the inequality, and the number of affine independent vertices. For a tight Bell inequality, the latter number has to be equal to $n^2 - 1$, implying that the hyperplane is a facet of the LHV polytope. The asterisk in the first column of the table means that the related Hadamard matrix has constant row sum. The seven tight cases denoted with symbol [†] in the fourth column are new, to the best of our knowledge.

mensional subspace, when single party measurements are not considered. Given that facets of the LHV polytope are faces with maximal dimension, they define hyperplanes in the correlation space. That is, they have dimension $d - 1$. This means that for a two outcomes scenario there are $d - 1 = m^2 - 1$ linearly independent vectors v , associated to LHV strategies $\langle A_x^s \otimes B_y^t \rangle = a_x^s b_y^t$, where $a_x, b_y = \pm 1$. Based on the above findings, in this section we study tightness of correlation Bell inequalities induced by Hadamard matrices $\text{core}(M)$ up to order $n = 20$. Results are summarized in Table 1, which lead us to establish the following conjecture:

Conjecture 1. *A Hadamard matrix of order n induces a tight correlation Bell inequality with $m = n$ settings and $q = 2$ outcomes per party if and only if it is not equivalent to a one having constant row sum.*

Furthermore, in the study described in Table 1,

we noted that the set of optimal LHV values can be arranged as *mutually quasi-unbiased weighing matrices* [62, 63], for both Alice and Bob strategies. See Appendix B for further details.

8 Conclusions

We introduced a one-to-one relation between the local hidden variable (LHV) value of Bell inequalities and the mathematical notion of excess of a matrix, see Prop. 1. This connection allowed us to obtain the LHV value of infinitely many families of Bell inequalities with an unbounded number of measurement settings per party, see Section 5.

We proposed the conjecture that every Hadamard matrix, not equivalent to a constant row sum one, induces a tight Bell inequality. We supported this conjecture with Hadamard matrices up to order 20, see Table 1.

Furthermore, we derived two upper bounds for the LHV value of bipartite Bell inequalities that are stronger than the upper bound for the quantum value, see Props. 2 and 3. Tightness of the last bound has been fully characterized in every scenario, including some remarkable cases like all Bell inequalities related to nonlocal computation [46] and quantum XOR games without quantum advantage [47].

As a further result, we found an intriguing connection between some classes of Bell inequalities and the mutually unbiased bases problem, see Observation 6 and the subsequent results.

Finally, we have shown that the problem to characterize the set of bipartite Bell inequalities with no quantum advantage for two outcomes contains the circulant Hadamard conjecture, a longstanding open problem in Combinatorics, see Observation 2.

Our results provide new insights by merging two extensively studied areas of research coming from different fields. Quantum nonlocality seems to be the most benefited side, as the mathematical theory of excess is considerably more advanced than currently known techniques to find local hidden variable values, as far as we know. We believe our results will deepen the interest in quantum nonlocality among both physicists and mathematicians.

Acknowledgements Authors kindly acknowledge valuable discussions with A. Acín, R. Augu-

siak, A. Cabello, J. Calsamiglia, D. Cavalcanti, J. De Vicente, P. Horodecki, R. Ramanathan, G. Senno, J. Tura and A. Winter. D.G. is supported by MINEDUC-UA project code ANT 1855 and Grant FONDECYT Iniciación number 11180474, Chile. W.B. and K.Ż. are supported by Narodowe Centrum Nauki under the Maestro grant number DEC-2015/18/A/ST2/00274, by Foundation for Polish Science under the Team-Net project no. POIR.04.04.00-00-17C1/18-00. D.A. is supported by UK EPSRC Grant No. EP/M013472/1.

A Block centro-hermitian matrices

In this Appendix, we show the structure of matrices M obeying (8) for some small scenarios. Let us start with the case of $m = 2, q = 3$, which leads to the matrix M of order $n = mq = 6$ of the form:

$$M = \begin{pmatrix} A & B & C \\ D & \mathbf{E} & D^* \\ C^* & B^* & A^* \end{pmatrix}, \quad (19)$$

where A, B, C, D are complex matrices of order $m = 2$, in general, and the red bold matrix $\mathbf{E}$, the center of symmetry, is a real matrix of order $m = 2$. In the case $m = 2, q = 4$, the matrix M of order $n = mq = 8$ has the structure:

$$M = \begin{pmatrix} \mathbf{A} & B & \mathbf{C} & B^* \\ D & E & F & G \\ \mathbf{I} & J & \mathbf{H} & J^* \\ D^* & G^* & F^* & E^* \end{pmatrix}, \quad (20)$$

where B, D, E, F, G, J are complex matrices of order $m = 2$, in general, and the red bold matrices $\mathbf{A}, \mathbf{C}, \mathbf{I}, \mathbf{H}$, the centers of symmetry, are real matrices of order $m = 2$. For higher values of m and q the structure is similar to the above cases. When q is odd, there is a unique center of symmetry, located at the center of the matrix. When q is even, there are 4 centers of symmetry.

Let us also illustrate the notion of core of a matrix, which plays a central role in our work. For $m = q = 2$, the following matrix M of order $n = mq = 4$ defines a correlation Bell inequality:

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}. \quad (21)$$

The core of this matrix has order $\mathbf{n} = m(q-1) = 2$, given by

$$\text{core}(M) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \quad (22)$$

As $q = 2$, the only constraint for M to define a Bell inequality is that $a, b, c, d \in \mathbb{R}$, see Remark 1 in the main text. For instance, when $a = b = c = -d = 1$, we have the CHSH inequality

$$\langle A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1 \rangle \leq 2.$$

B Optimal LHV strategies

This Appendix is devoted to showing that optimal LHV strategies for both Alice and Bob, when arranged as rows of matrices, define Mutually quasi-unbiased weighing matrices, for some correlation Bell inequalities arising from Hadamard matrices of orders $\mathbf{n} = 2$ and $\mathbf{n} = 8$. Each of these matrices is the core of the matrix M that generates the corresponding correlation Bell inequality, in the scenario of two parties, $m = \mathbf{n}$ settings and 2 outcomes each.

A weighing matrix W of weight k is a square matrix of order m having entries from the set $\{-1, 0, 1\}$, such that $WW^T = k\mathbb{I}$. Two weighing matrices W_1 and W_2 of order m and weight k are *mutually quasi-unbiased weighing matrices* (MQUWM) [63] for parameters (m, k, l, a) if there exists positive integers a and l such that $(1/\sqrt{a})W_1W_2^T$ is a weighing matrix of weight $l = k^2/a$. We denote these matrices as MQUWM(m, k, l, a).

Case $\mathbf{m} = 2$ settings (CHSH):

There are 4 optimal LHV strategies in this case. For Alice and Bob, the strategies define the following two sets of two MQUWM(2,2,1,4):

$$W_1^A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad W_2^A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad (23)$$

and

$$W_1^B = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad W_2^B = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad (24)$$

respectively. That is, we have two orthonormal bases in each case, all of them identical up to global phases and reordering of vectors.

Case $\mathbf{m} = 4$ settings:

There are 4 optimal LHV strategies. For both Alice and Bob, the strategies can be arranged in rows as the following weighing matrices of weight 4, i.e. Hadamard matrices:

$$W_1^A = \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}, \quad (25)$$

and

$$W_1^B = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}, \quad (26)$$

respectively. In this case, we also have two orthonormal bases.

Case $\mathbf{m} = 8$ settings:

There are 64 optimal LHV strategies. For Alice, her local strategies can be arranged as the following maximal set of 8 MQUWM(8,8,16,4), along the rows:

$$W_1^A = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{pmatrix}$$

$$W_2^A = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}$$

$$W_3^A = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \end{pmatrix}$$

$$W_4^A = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$W_5^A = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \end{pmatrix}$$

$$W_6^A = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \end{pmatrix}$$

$$W_7^A = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 \end{pmatrix}$$

$$W_8^A = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \end{pmatrix}.$$

For Bob, we also have a maximal set of 8 MQUWM(8,8,16,4), with a different ordering of vectors:

$$W_1^B = \begin{pmatrix} -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \end{pmatrix}$$

$$W_2^B = \begin{pmatrix} -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \end{pmatrix}$$

$$W_3^B = \begin{pmatrix} -1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$W_4^B = \begin{pmatrix} -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{pmatrix}$$

$$W_5^B = \begin{pmatrix} -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 \end{pmatrix}$$

$$W_6^B = \begin{pmatrix} -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \end{pmatrix}$$

$$W_7^B = \begin{pmatrix} -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \end{pmatrix}$$

$$W_8^B = \begin{pmatrix} 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \end{pmatrix}$$

Let us now see how these optimal LHV strategies of Alice and Bob are connected. The i^{th} element of the j^{th} basis W_j^A is connected with the k^{th} element of the l^{th} basis W_l^B through the following ordering

(i, j, k, l) :

(1, 1, 1, 1), (2, 1, 1, 8), (3, 1, 4, 4), (4, 1, 4, 5), (5, 1, 5, 6),
(6, 1, 7, 7), (7, 1, 7, 2), (8, 1, 7, 3), (1, 2, 1, 2), (2, 2, 1, 7),
(3, 2, 4, 6), (4, 2, 4, 3), (5, 2, 5, 1), (6, 2, 7, 5), (7, 2, 7, 4),
(8, 2, 7, 8), (1, 3, 1, 3), (2, 3, 1, 6), (3, 3, 4, 1), (4, 3, 4, 8),
(5, 3, 6, 4), (6, 3, 6, 2), (7, 3, 8, 5), (8, 3, 8, 7), (1, 4, 1, 4),
(2, 4, 1, 5), (3, 4, 4, 7), (4, 4, 4, 2), (5, 4, 6, 8), (6, 4, 6, 3),
(7, 4, 6, 6), (8, 4, 6, 1), (1, 5, 2, 5), (2, 5, 3, 1), (3, 5, 3, 8),
(4, 5, 3, 2), (5, 5, 5, 7), (6, 5, 5, 4), (7, 5, 8, 3), (8, 5, 8, 6),
(1, 6, 2, 3), (2, 6, 2, 4), (3, 6, 2, 7), (4, 6, 3, 6), (5, 6, 6, 5),
(6, 6, 5, 2), (7, 6, 8, 8), (8, 6, 7, 1), (1, 7, 2, 2), (2, 7, 3, 5),
(3, 7, 3, 7), (4, 7, 3, 4), (5, 7, 5, 8), (6, 7, 5, 3), (7, 7, 7, 6),
(8, 7, 8, 1), (1, 8, 2, 1), (2, 8, 2, 8), (3, 8, 3, 3), (4, 8, 2, 6),
(5, 8, 5, 5), (6, 8, 6, 7), (7, 8, 8, 2), (8, 8, 8, 4).

Regarding higher order Hadamard matrices, we studied tightness without analyzing their geometrical structure, due to the large number of classical strategies achieving the LHV value.

Case $m = 12$ settings:

For order 12, there is an unique Hadamard matrix, see the catalog of Hadamard matrices by J. Seberry [64]. In this case, we find a tight Bell inequality, composed by 12 measurement settings per party and 2 outcomes each.

Case $m = 16$ settings:

We noted that the three constant row sum Hadamard matrices of order 16, denoted H_1, H_2 and H_3 [64], do not imply a tight Bell inequality, for two outcomes. This is consistent with the fact that correlation tight Bell inequalities always have a quantum violation [65]. The remaining two non-constant row sum Hadamard matrices, H_4 and H_5 , have a quantum violation and produce inequivalent tight Bell inequalities, composed by 16 measurement settings per party and 2 outcomes each.

Case $m = 20$ settings:

For order $m = 20$, we found that the three Hadamard matrices H_1, H_2, H_3 [64] induce inequivalent tight Bell inequalities, composed by 20 measurement settings per party and 2 outcomes each.

The above analysis include the entire set of classes of Hadamard matrices existing up to order $m = 20$. Recall that two equivalent Hadamard matrices imply essentially the same Bell inequality, up to a relabeling of inputs and outputs. See Table 1 and Conjecture 1 for a summary of these results.

C Proofs of results

In this section, we provide the proofs of the results presented in previous sections.

Proposition 1. *Let M be a matrix of order mq having maximal excess with respect to q -equivalence. Then, the Bell inequality (6), having q outcomes per setting, has LHV value $\mathcal{C}(M)$ equal to the excess of the matrix M , $\Sigma(M)$. Conversely, for any Bell inequality (6) induced by a matrix M , there is a matrix M' satisfying the symmetry (8) such that $\mathcal{C}(M') = \Sigma(M')$.*

Proof. The optimal LHV strategy is given by all-one outcomes for both Alice and Bob. Thus, the LHV value is given by the sum of all the entries of matrix M . Conversely, if the local variables producing the LHV value are $\{a_x\}$ and $\{b_y\}$, for Alice and Bob, respectively, then $M'_{[sx][ty]} = (a_x^s b_y^t)^* M_{[sx][ty]}$ produces an equivalent Bell inequality satisfying $\mathcal{C}(M') = \Sigma(M')$. Note that M' satisfies the symmetry (8). $\square$

Proposition 2. *Let M be a matrix of order $n = mq$ having maximal excess with respect to q -equivalence. Then, the following upper bound holds for the induced Bell inequality:*

$$\mathcal{C}(M) \leq nr(M). \quad (27)$$

Proof. Let M be a matrix having maximal excess. The numerical radius is given by $r = \max_{|\psi\rangle \in \mathcal{H}} |\langle \psi | M | \psi \rangle| \geq \langle \phi | M | \phi \rangle$, where $|\phi\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle = \frac{1}{\sqrt{n}} (1, 1, \dots, 1)^T$. Thus $r \geq \langle \phi | M | \phi \rangle = \frac{1}{n} \Sigma(M) = \frac{1}{n} \mathcal{C}(M)$. $\square$

Proposition 3. *Let M be a matrix of order $n = mq$ having maximal excess with respect to q -equivalence. Then we have*

$$\mathcal{C}(M) \leq \sqrt{n} \nu(M), \quad (28)$$

where $\nu(M) = \sqrt{\sum_{i=0}^{n-1} |\sum_{j=0}^{n-1} M_{ij}|^2}$. Moreover, upper bound (12) is saturated if and only if M is a constant row sum matrix. In such case, $\mathcal{C}(M) = n|s|$, where s is the constant row sum value.

Proof. Upper bound (12) simply arises from the Cauchy-Schwarz inequality

$$\mathcal{C}(M) = \Sigma(M) = n \langle \phi | M | \phi \rangle \leq n \|M | \phi \rangle\| = n \frac{1}{\sqrt{n}} \nu(M). \quad (29)$$

Here, equality is attained if and only if $|\phi\rangle$ and $M|\phi\rangle$ are parallel, which occurs when each row of matrix M has the same sum, i.e. M is a constant row sum matrix. $\square$

Proposition 4. *Let M_1, M_2 be matrices of order m_1q and m_2q , respectively. If both M_1 and M_2 have maximal excess with respect to q -equivalence and M_2 is real, then the LHV value of the Bell inequality induced by the tensor product matrix $M = M_1 \otimes M_2$, having q outcomes per setting, is given by $\mathcal{C}(M) = \mathcal{C}(M_1)\mathcal{C}(M_2)$.*

Proof. The proof is straightforward from the fact that excess of a tensor product is the product of excesses, see Obs. 2.4 in [50]. We only have to demonstrate that the matrix $M = M_1 \otimes M_2$ obeys condition (8). By the definition of the tensor product, we have $[M_1 \otimes M_2]_{ij} = [M_1]_{k_1 l_1} \cdot [M_2]_{k_2 l_2}$, where $i = k_1 m_2 q + k_2$, $j = l_1 m_2 + l_2$, $0 \leq k_1, l_1 < m_1 q$, $0 \leq k_2, l_2 < m_2 q$. Let $0 \leq s, t < q$ and $0 \leq x, y < m_1 m_2 q$. Writing $x = m_2 q e_x + f_x$ and $y = m_2 q e_y + f_y$ for $0 \leq e_x, e_y < m_1$ and $0 \leq f_x, f_y < m_2 q$, we have

$$\begin{aligned} & [M_1 \otimes M_2]_{m_1 m_2 q[q-s]_q + x, m_1 m_2 q[q-t]_q + y} \\ &= [M_1 \otimes M_2]_{(m_1[q-s]_q + e_x)m_2 q + f_x, (m_1[q-t]_q + e_y)m_2 q + f_y} \\ &= [M_1]_{m_1[q-s]_q + e_x, m_1[q-t]_q + e_y} \cdot [M_2]_{f_x, f_y}, \end{aligned}$$

and since M_1 obeys (8), we have

$$= ([M_1]_{m_1 s + e_x, m_1 t + e_y})^* \cdot [M_2]_{f_x, f_y}.$$

Also, it holds

$$\begin{aligned} & ([M_1 \otimes M_2]_{m_1 m_2 q s + x, m_1 m_2 q t + y})^* \\ &= ([M_1 \otimes M_2]_{(m_1 s + e_x)m_2 q + f_x, (m_1 t + e_y)m_2 q + f_y})^* \\ &= ([M_1]_{m_1 s + e_x, m_1 t + e_y})^* \cdot [M_2]_{f_x, f_y}^* \\ &= ([M_1]_{m_1 s + e_x, m_1 t + e_y})^* \cdot ([M_2]_{f_x, f_y})^*. \end{aligned}$$

Comparing these two expressions, we see that $M_1 \otimes M_2$ obeys (8) if M_2 is real. $\square$

Proposition 5. *Let M be a Hadamard matrix of order n . If there is a real vector $|x\rangle$ with entries ± 1 , unbiased to the rows of M , then $\mathcal{C}(M) = n\sqrt{n}$. Conversely, if $\mathcal{C}(M) = n\sqrt{n}$, then there exists a vector $|x\rangle$ that is unbiased to the rows of M .*

Proof. If $|x\rangle$ is unbiased to M , then clearly $\|M|x\rangle\|_1 = n\sqrt{n}$. This is the maximal possible value, as the upper bound (1) is saturated. Contrarily, if $\mathcal{C}(M) = n\sqrt{n}$, then M is a constant row sum matrix. This is so, as the only Hadamard matrices attaining excess equal to $n\sqrt{n}$ are those having constant row sum [27]. Therefore, vector $|x\rangle$ chosen as $|x\rangle = (1, 1, \dots, 1)^T$ is obviously unbiased to M , because every entry of $M|x\rangle$ has the same value, which is equal to the constant row sum value. $\square$

Corollary 1. *If n is not a square number, then any pair of real mutually unbiased bases in dimension n is strongly unextendible. That is, there is no single vector unbiased to the pair of bases.*

Proof. Any pair of real MUB is equivalent to a pair of the form $\{\mathbb{I}, H\}$, where $\mathbb{I}$ is the identity matrix and H is a real Hadamard matrix. Vectors of the bases are represented by the columns of these matrices. Any real vector mutually unbiased to this pair is necessarily composed by ± 1 entries, up to normalization. On the other hand, the maximal LHV value $\mathcal{C}(H) = n\sqrt{n}$ ($= \Sigma(H)$) in (18) is only attained for

constant row sum Hadamard matrices H [27]. Here, recall that constant row sum Hadamard matrices exist for square order n only. Thus, from Prop. 5 we have that there is no single vector mutually unbiased to the pair $\{\mathbb{I}, H\}$ when n is not a square number. $\square$

Corollary 2. *If three real mutually unbiased bases $\{\mathbb{I}, H_1, H_2\}$ exist in dimension n , then both H_1 and H_2 are equivalent to a constant row sum Hadamard matrix.*

Proof. Every row of H_2 is unbiased to the rows of H_1 , and vice versa. Therefore, from Prop. 5 we have that $\mathcal{C}(H_1) = \mathcal{C}(H_2) = n\sqrt{n}$. As we have seen, this implies that both Hadamard matrices H_1 and H_2 are equivalent to constant row sum matrices. $\square$

Corollary 3. *For any pair of real mutually unbiased bases $\{\mathbb{I}, H\}$, with H being a constant row sum Hadamard matrix, there is at least one mutually unbiased vector. That is, such pairs of MUB are not strongly unextendible, in every dimension where they exist.*

Proof. Following the proof of Prop. 5, the unnormalized vector $x = (1, \dots, 1)^T$ is mutually unbiased to $\{\mathbb{I}, H\}$. $\square$

References

- [1] J. Bell, Physics 1, 3, 195–200 (1964).
- [2] A. Einstein, B. Podolsky, N. Rosen, Phys. Rev. **47**, 777–780 (1935).
- [3] R. Cleve and H. Buhrmann, Phys. Rev. A **56**, 1201 (1997).
- [4] T.S. Cubitt, D. Leung, W. Matthews, A. Winter, IEEE Trans. Theory **57**(8), 5509 (2011).
- [5] Y. Liu *et al.*, Phys. Rev. Lett. **111**, 13, 130502 (2013).
- [6] T.F. da Silva *et al.*, Phys. Rev. A **88**, 052303 (2013).
- [7] J. Barrett, L. Hardy, A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
- [8] A. Acín, N. Gisin, Ll. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).
- [9] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
- [10] Ll. Masanes, S. Pironio, A. Acín, Nature Comm. **2**, 238 (2011).
- [11] S. Pironio, Ll. Masanes, A. Leverrier, A. Acín, Phys. Rev. X, **3**, 031007 (2013).
- [12] U. Vazirani, T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).
- [13] J. Kaniewski, S. Wehner, New J. Phys. **18**, 5, 055004 (2016).

- [14] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge (2007).
- [15] R. Colbeck, A. Kent, J. Phys. A: Math. Theor. **44**, 095305 (2011).
- [16] S. Pironio *et al.*, Nature **464**, 1021 (2010).
- [17] R. Colbeck, R. Renner, Nature Physics **8**, 450 (2012).
- [18] D. Alsina, J.I. Latorre, Phys. Rev. A **94**, 012314 (2016).
- [19] D. García Martín, G. Sierra, J. Appl. Math. Phys. **6**(7), 1460–1475 (2018).
- [20] A. Smith, M.S. Kim, F. Pollmann, J. Knolle, [arXiv:1906.06343](https://arxiv.org/abs/1906.06343) [quant-ph] (2019).
- [21] M. Herrero-Collantes, J.C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).
- [22] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
- [23] N. Brunner, Device-Independent Quantum Information Processing, in Research in Optical Sciences, OSA Technical Digest (online), Optical Society of America, paper QW3A.2 (2014).
- [24] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
- [25] D. Rosset, J.-D. Bancal, N. Gisin, J. Phys. A: Math. & Theor. **47**, 424022 (2014).
- [26] K.W. Schmidt, Math. Mag. **46**, 103 (1973).
- [27] M. Best, Indag. Math. **80**, 5, 357–361 (1977).
- [28] A. Fine, Phys. Rev. Lett. **48**, 291 (1982).
- [29] A. Aspect, P. Grangier, G. Roger, Phys. Rev. Lett. **47**, 460 (1981).
- [30] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, S. Pironio, Phys. Rev. Lett. **119**, 040402 (2017).
- [31] S. Popescu, D. Rohrlich, Found. Phys. **24**, 379–385 (1994).
- [32] A. Lee, Centrohermitian and skew-centrohermitian matrices, Linear Algebra and its Applications **29**, 205–210 (1980)
- [33] N. Farmakis, S. Kounias, Discr. Math. **67**, 2 165–176 (1987).
- [34] S. Kounias, N. Farmakis, Discr. Math. **68**, 1 59–69 (1988).
- [35] C. Koukouvinos, J. Seberry, Discr. Math. **92**, 1–3, 173–176 (1991).
- [36] H. Kharaghani, Discr. Math. **89**, 3, 307–312 (1991)
- [37] T. Xia, M. Xia, J. Seberry, Australas. J. Comb. **27**, 263–275 (2003).
- [38] R. Craigen, H. Kharaghani, J. Comb. Designs **12**, 4, 233–255 (2004).
- [39] H. Kharaghani, J. Seberry, The excess of complex Hadamard matrices, Graphs Combin. **9**, 47–56 (1993).
- [40] J. Ford, A. Gál, Hadamard Tensors and Lower Bounds on Multiparty Communication Complexity, In Proc. 32nd International Conference on Automata, Languages and Programming (ICALP’05), 1163–1175, (2005).
- [41] J. Hammer, R. Levingston, J. Seberry, Ars Comb. **5**, 237–254 (1978).
- [42] S. Arora, C. Lund, R. Motwani, M. Sudan, M. Szegedy. J. ACM, **45**(3), 501–555, (1998).
- [43] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
- [44] M. Epping, H. Kampermann, D. Bruß, Phys. Rev. Lett. **111**, 240404 (2013).
- [45] J. de Vicente, Phys. Rev. A **92**, 032103 (2015).
- [46] N. Linden, S. Popescu, A.J. Short, A. Winter, Phys. Rev. Lett. **99**, 180502 (2007).
- [47] R. Ramanathan, A. Kay, G. Murta, P. Horodecki, Phys. Rev. Lett. **113**, 240401 (2014).
- [48] M. Hall, J.P.L. Research Summary **1**, 36–10, 21–26 (1961).
- [49] H.J. Ryser, Combinatorial mathematics, Willey, New York (1963).
- [50] W.P. Orrick, B. Solomon, Discr. Math. **307**, 2, 226–236 (2007).
- [51] B. Jenkins, C. Koukouvinos, S. Kounias, J. Seberry, R. Seberry, J. Comb. Math. Comput. **4**, 155–188 (1988).
- [52] K. Momihara, S. Suda, Conference matrices with maximum excess and two-intersection sets, Integers **17**, A30 (2017)
- [53] M. Hirasaka, K. Momihara, S. Suda, Algebr. Comb. **1**, 5, 697–722 (2018).
- [54] M. Yamada, Graphs Combin. **4**, 297–301 (1988).
- [55] J. Seberry, Graphs Combin. **5**, 373–383 (1989).
- [56] C. Koukouvinos, S. Kounias, Discr. Math. **85**, 295–300 (1990).
- [57] C. Koukouvinos, S. Kounias, J. Seberry, Discr. Math. **88**, 1, 49–58 (1991).
- [58] H. Buhrman, W. van Dam, P. Hoyer, A. Tapp, Phys. Rev. A **60**, 2737–2741 (1999).
- [59] T. Durt, B.-G. Englert, I. Bengtsson, K. Życzkowski, Int. J. Quant. Inf. **8**, 4, 535–640 (2010).
- [60] P. Diviánszky, E. Bene, T. Vértesi, Phys. Rev A **96**, 012113 (2017).
- [61] We acknowledge A. Acín for noting that the ratio of the upper over lower bound (1) cannot be larger than $\sqrt{2}$, and its implication in robustness of quantum nonlocality under the presence of noise.

- [62] H. Nozaki, S. Suda, J. Algebr. Comb. **42**, 283–291 (2015).
- [63] H. Kharaghani, S. Suda, Des. Codes Cryptogr. **86**, 1573–1588 (2018).
- [64] <https://documents.uow.edu.au/~jennie/hadamard.html> (access: 2021-08-09).
- [65] L. Escolà, J. Calsamiglia, A. Winter, Phys. Rev. Research **2**, 012044(R), (2020).