COMPLEX HADAMARD MATRICES AND APPLICATIONS

TEO BANICA

ABSTRACT. A complex Hadamard matrix is a square matrix $H \in M_N(\mathbb{C})$ whose entries are on the unit circle, $|H_{ij}| = 1$, and whose rows and pairwise orthogonal. The main example is the Fourier matrix, $F_N = (w^{ij})$ with $w = e^{2\pi i/N}$. We discuss here the basic theory of such matrices, with emphasis on geometric and analytic aspects.

CONTENTS

2010 *Mathematics Subject Classification.* 15B10.
Key words and phrases. Hadamard matrix, Fourier matrix.

Introduction

A complex Hadamard matrix is a square matrix $H\in M_N(\mathbb C)$ whose entries are the unit circle, $|H_{ij}|=1$, and whose rows are pairwise orthogonal with respect to the usual scalar product of $\mathbb C^N$. These matrices appear in connection with many questions, the basic example being the Fourier matrix, which is as follows, with $w=e^{2\pi i/N}$:

$$F_N=(w^{ij})_{ij}$$

In standard matrix form, and with the standard discrete Fourier analysis convention that the indices vary as $i,j=0,1,\ldots,N-1$, this matrix is as follows:

$$F_N=\begin{pmatrix}1&1&1&\ldots&1\\ 1&w&w^2&\ldots&w^{N-1}\\ 1&w^2&w^4&\ldots&w^{2(N-1)}\\ \vdots&\vdots&\vdots&&\vdots\\ 1&w^{N-1}&w^{2(N-1)}&\ldots&w^{(N-1)^2}\end{pmatrix}$$

Observe that this matrix is indeed Hadamard, with the orthogonality formulae between rows coming from the fact that the barycenter of any centered regular polygon is 0. This matrix is the matrix of the discrete Fourier transform over $\mathbb Z_N$, and the arbitrary complex Hadamard matrices can be thought of as being "generalized Fourier matrices".

As an illustration, the complex Hadamard matrices cover in fact all the classical discrete Fourier transforms. Consider indeed the Fourier coupling of an arbitrary finite abelian group G, regarded via the isomorphism $G\simeq\widehat{G}$ as a square matrix, $F_G\in M_G(\mathbb C)$:

$$F_G=<i,j>_{i\in G,j\in\widehat{G}}$$

For the cyclic group $G=\mathbb Z_N$ we obtain in this way the above matrix F_N. In general, we can write $G=\mathbb Z_{N_1}\times\ldots\times\mathbb Z_{N_k}$, and modulo some standard identifications, the corresponding Fourier matrix decomposes then over components, as follows:

$$F_G=F_{N_1}\otimes\ldots\otimes F_{N_k}$$

Now since the tensor product of complex Hadamard matrices is Hadamard, we conclude that this generalized Fourier matrix F_G is a complex Hadamard matrix.

The above generalization is particularly interesting when taking as input the groups $G=\mathbb Z_2^n$. Indeed, for such groups the corresponding Fourier matrices are real. As a first example here, at $n=1$ we obtain the Fourier matrix F_2, which is as follows:

$$F_2=\begin{pmatrix}1&1\\ 1&-1\end{pmatrix}$$

This matrix is also denoted W_2, and called first Walsh matrix. At $n = 2$ now, we obtain the second Walsh matrix, $W_4 = W_2 \otimes W_2$, which is given by:

$$W_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

In general, we obtain in this way the tensor powers $W_{2^n} = F_2^{\otimes n}$ of the Fourier matrix F_2, having size $N = 2^n$, called Walsh matrices, and having many applications.

The world of the real Hadamard matrices, $H \in M_N(\pm 1)$, is quite fascinating, having deep ties with combinatorics, coding, and design theory. Due to the orthogonality conditions between the first 3 rows, the size of such a matrix must satisfy:

$$N \in \{2\} \cup 4\mathbb{N}$$

The celebrated Hadamard Conjecture (HC), which is more than 100 years old, and is one of the most beautiful problems in combinatorics, and mathematics in general, states that real Hadamard matrices should exist at any $N \in 4\mathbb{N}$. Famous as well is the Circulant Hadamard Conjecture (CHC), which is more than 50 years old, stating that the following "conjugate" of the above matrix W_4, and its other conjugates, are the unique circulant real Hadamard matrices, and this regardless of the value of $N \in \mathbb{N}$:

$$K_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

There are many other interesting questions regarding the real Hadamard matrices, mostly of algebraic nature, but with some subtle analytic aspects as well.

Getting back now to the general complex case, $H \in M_N(\mathbb{T})$, the situation here is quite different. We know that at any $N \in \mathbb{N}$ we have the Fourier matrix F_N, so the HC dissapears. The CHC dissapears in fact as well, because the Fourier matrix F_N can be put in circulant form, up to some simple operations on the rows and columns. As an example, consider the Fourier matrix F_3, which is as follows, with $w = e^{2\pi i/3}$:

$$F_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{pmatrix}$$

By doing some suitable manipulations on the rows and columns, namely permuting them, or multiplying them by numbers $w \in \mathbb{T}$, which are operations which preserve the class of complex Hadamard matrices, we can put F_3 in circulant form, as follows:

$$F_3' = \begin{pmatrix} w & 1 & 1 \\ 1 & w & 1 \\ 1 & 1 & w \end{pmatrix}$$

The situation at general $N \in \mathbb{N}$ is similar, and as a conclusion, both the HC and CHC dissapear, in the general complex setting $H \in M_N(\mathbb{T})$. It is possible however to recover these conjectures, in a more complicated form, by looking at the Hadamard matrices $H \in M_N(\mathbb{Z}_s)$ having as entries roots of unity of a given order $s \in \mathbb{N}$.

In the purely complex case, where $H \in M_N(\mathbb{T})$ is allowed to have non-roots of unity as entries, the whole subject rather belongs to geometry. Indeed, for a matrix $H \in M_N(\mathbb{T})$, the orthogonality condition between the rows tells us that the rescaled matrix $U = H/\sqrt{N}$ must be unitary. Thus, the $N \times N$ complex Hadamard matrices form a real algebraic manifold, appearing as an intersection of smooth manifolds, as follows:

$$X_N = M_N(\mathbb{T}) \cap \sqrt{N} U_N$$

This intersection is far from being smooth, and generally speaking, the study of the complex Hadamard matrices belongs to real algebraic geometry, and more specifically to a real algebraic geometry of rather arithmetic type, related to Fourier analysis.

As an illustration for the various phenomena that might appear, let us briefly discuss now the classification of the complex Hadamard matrices, at small values of $N \in \mathbb{N}$. At $N = 2, 3$ the situation is elementary, with F_2, F_3 being the unique matrices, up to equivalence. At $N = 4$ now, the solutions are the affine deformations of the Walsh matrix W_4, depending on complex number of modulus one $q \in \mathbb{T}$, as follows:

$$W_4^q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & q & -1 & -q \\ 1 & -q & -1 & q \end{pmatrix}$$

At $N = 5$ now, the situation becomes quite complicated, but Haagerup was able to prove in [69] that, up to equivalence as usual, the unique complex Hadamard matrix is the Fourier matrix F_5, which is as follows, with $w = e^{2\pi i/5}$:

$$F_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & w^3 & w^4 \\ 1 & w^2 & w^4 & w & w^3 \\ 1 & w^3 & w & w^4 & w^2 \\ 1 & w^4 & w^3 & w^2 & w \end{pmatrix}$$

At $N = 6$ the complex Hadamard matrices are not classified yet, but there are many known interesting examples. First, since $6 = 2 \times 3$ is a composite number, the Fourier matrix F_6 admits certain affine deformations, which are well understood. Next, we have the following matrix from [69], depending on a parameter on the unit circle, $q \in \mathbb{T}$:

$$H_6^q = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & i & i & -i & -i \\ 1 & i & -1 & -i & q & -q \\ 1 & i & -i & -1 & -q & q \\ 1 & -i & \bar{q} & -\bar{q} & i & -1 \\ 1 & -i & -\bar{q} & \bar{q} & -1 & i \end{pmatrix}$$

We have as well the following matrix discovered and used by Tao in [131], with $w = e^{2\pi i/3}$, which has the property of being "isolated", in an appropriate sense:

$$T_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & w & w & w^2 & w^2 \\ 1 & w & 1 & w^2 & w^2 & w \\ 1 & w & w^2 & 1 & w & w^2 \\ 1 & w^2 & w^2 & w & 1 & w \\ 1 & w^2 & w & w^2 & w & 1 \end{pmatrix}$$

As explained in [17], up to the Hadamard equivalence relation, the above-mentioned matrices are the only ones at $N = 6$, whose combinatorics is based on the roots of unity. Finally, at $N = 7$, even the matrices whose combinatorics is based on the roots of unity are not classified yet. Conjecturally, there are only 2 such matrices, namely the Fourier matrix F_7, and a parametric matrix P_7^q, constructed by Petrescu in [111] by using a computer, and which was later put in a design theory framework by Szöllősi [127].

Passed these difficult structure and classification problems, the complex Hadamard matrices remain however something very nice, and constructive. From an abstract viewpoint these matrices can be thought of as being "generalized Fourier matrices", and due to this fact, they appear in a wide array of questions in mathematics and physics:

(1) Operator algebras. One important concept in the theory of von Neumann algebras [99], [100], [101], [141] is that of a maximal abelian subalgebra (MASA). In the "finite" case, where the algebra has a trace, one can talk about pairs of orthogonal MASA. And in the simplest such case, that of the matrix algebra $M_N(\mathbb{C})$, the orthogonal MASA are, up to conjugation, $A = \Delta, B = H\Delta H^*$, where $\Delta \subset M_N(\mathbb{C})$ are the diagonal matrices, and $H \in M_N(\mathbb{C})$ is Hadamard, as discovered by Popa some 30 years ago [113].

(2) Subfactor theory. Along the same lines, but at a more advanced level, associated to any Hadamard matrix $H \in M_N(\mathbb{C})$ is the square diagram $\mathbb{C} \subset \Delta, H\Delta H^* \subset M_N(\mathbb{C})$ formed by the associated MASA, which is a commuting square in the sense of subfactor theory. The Jones basic construction produces, out of this diagram, an index N subfactor

of the Murray-von Neumann hyperfinite II_1 factor R, whose study a key problem. The corresponding planar algebra was computed by Jones in [81].

(3) Quantum groups. Associated to any complex Hadamard matrix $H \in M_N(\mathbb{C})$ is a certain quantum permutation group $G \subset S_N^+$, obtained by factorizing the flat representation $\pi : C(S_N^+) \to M_N(\mathbb{C})$ associated to H, with this construction heavily relying on the work of Woronowicz [149], [150] and Wang [142]. As a basic example, the Fourier matrix F_G produces the group G itself. In general, as explained in [7], the above-mentioned subfactor can be recovered from G, whose computation is a key problem.

(4) Lattice models. According to the work of Jones [78], [79], [80], [81], the combinatorics of the subfactor associated to a complex Hadamard matrix $H \in M_N(\mathbb{C})$ can be thought of as being the combinatorics of a certain "spin model", in the context of statistical mechanics, taken in an abstract sense. By the above this spin model combinatorics can be recovered from the representation theory of the associated quantum group $G \subset S_N^+$, a bit in the spirit of [65], although this still remains to be worked out.

Our aim here is to survey this material, theory and applications of the complex Hadamard matrices, with emphasis on geometric and analytic aspects. Organizing all this was not easy, and we have chosen an algebra/geometry/analysis/physics lineup for our presentation, vaguely coming from the amount of background which is needed:

(1) Sections 1-4 discuss the basic theory in the real case.

(2) Sections 5-8 deal with various algebraic and geometric aspects.

(3) Sections 9-12 are concerned with various analytic considerations.

(4) Sections 13-16 deal with various mathematical physics aspects.

Acknowledgements.

I would like to thank Vaughan Jones for suggesting me, back to a discussion that we had in 1997, when we first met, to look at vertex models, and related topics.

Stepping into bare Hadamard matrices is quite an experience, and very inspiring was the work of Uffe Haagerup on the subject, and his papers [45], [69], [70].

The present text is heavily based on a number of research papers on the subject that I wrote or co-signed, mostly during 2005–2015, and I would like to thank my coworkers Julien Bichon, Benoît Collins, Ion Nechita, Remus Nicoară, Duygu Özteke, Lorenzo Pittau, Jean-Marc Schlenker, Adam Skalski and Karol Życzkowski.

Finally, many thanks go to my cats, for advice with hunting techniques, martial arts, and more. When doing linear algebra, all this knowledge is very useful.

1. Hadamard matrices

We will be mainly interested in this book in the complex Hadamard matrices, but we will start with some beautiful pure mathematics, regarding the real case. The definition that we need, going back to 19th century work of Sylvester [124], on topics such as tessellated pavements and ornamental tile-work, is as follows:

Definition 1.1. *An Hadamard matrix is a square binary matrix,*

$$H\in M_N(\pm 1)$$

whose rows are pairwise orthogonal, with respect to the scalar product on $\mathbb R^N$.

There are many examples of such matrices, and we will discuss this, in what follows. To start with, here is an example, which is a particularly beautiful one:

$$K_4=\begin{pmatrix}-1&1&1&1\\ 1&-1&1&1\\ 1&1&-1&1\\ 1&1&1&-1\end{pmatrix}$$

As a first observation, we do not really need real numbers in order to talk about the Hadamard matrices, because we have:

Proposition 1.2. *A binary matrix $H\in M_N(\pm 1)$ is Hadamard when its rows have the property that, when comparing any two of them*

$$\begin{matrix}e_1&\ldots&e_N\\ f_1&\ldots&f_N\end{matrix}$$

the number of matchings $(e_i=f_i)$ equals the number of mismatchings $(e_i\neq f_i)$.

Proof. This is clear from definitions. Indeed, the scalar product on $\mathbb R^N$ is given by:

$$<x,y>=\sum_i x_iy_i$$

Thus, when computing the scalar product between two rows, the matchings contribute with 1 factors, and the mismatchings with -1 factors, and this gives the result. $\square$

Thus, we can replace if we want the $1,-1$ entries of our matrix by any two symbols, of our choice. Here is an example of an Hadamard matrix, written with this convention:

$$\begin{matrix}\heartsuit&\heartsuit&\heartsuit&\heartsuit\\ \heartsuit&\clubsuit&\heartsuit&\clubsuit\\ \heartsuit&\heartsuit&\clubsuit&\clubsuit\\ \heartsuit&\clubsuit&\clubsuit&\heartsuit\end{matrix}$$

However, it is probably better to run away from this, and use real numbers instead, as in Definition 1.1, with the idea in mind of connecting the Hadamard matrices to the foundations of modern mathematics, namely Calculus 1 and Calculus 2. So, getting back now to the real numbers, here is our first result:

Theorem 1.3. *For a square matrix $H \in M_N(\pm 1)$, the following are equivalent:*

1. *The rows of H are pairwise orthogonal, and so H is Hadamard.*
2. *The columns of H are pairwise orthogonal, and so H^t is Hadamard.*
3. *The rescaled matrix $U = H/\sqrt{N}$ is orthogonal, $U \in O_N$.*

Proof. The idea here is that the equivalence between (1) and (2) is not exactly obvious, but both these conditions can be shown to be equivalent to (3), as follows:

(1) $\iff$ (3) Since the rows of $U = H/\sqrt{N}$ have norm 1, this matrix is orthogonal precisely when its rows are pairwise orthogonal. But this latter condition is equivalent to the fact that the rows of $H = \sqrt{N}U$ are pairwise orthogonal, as desired.

(2) $\iff$ (3) The same argument as above shows that H^t is Hadamard precisely when its rescaling $U^t = H^t/\sqrt{N}$ is orthogonal. But since a matrix $U \in M_N(\mathbb{R})$ is orthogonal precisely when its transpose $U^t \in M_N(\mathbb{R})$ is orthogonal, this gives the result. $\square$

As an abstract consequence of the above result, let us record:

Theorem 1.4. *The set of the $N \times N$ Hadamard matrices is*

$$Y_N = M_N(\pm 1) \cap \sqrt{N} O_N$$

where O_N is the orthogonal group, the intersection being taken inside $M_N(\mathbb{R})$.

Proof. This follows from the equivalence (1) $\iff$ (3) in Theorem 1.3, which tells us that an arbitrary $H \in M_N(\pm 1)$ belongs to Y_N if and only if it belongs to $\sqrt{N} O_N$. $\square$

Summarizing, the set Y_N that we are interested in appears as a kind of set of "special rational points" of the real algebraic manifold $\sqrt{N} O_N$. In the simplest case, $N = 2$, the set Y_2 consists precisely of the rational points of $\sqrt{2} O_2$, as follows:

Theorem 1.5. *The binary matrices $H \in M_2(\pm 1)$ are split* 50-50 *between Hadamard and non-Hadamard, the Hadamard ones being as follows,*

$$\begin{pmatrix}1&1\\1&-1\end{pmatrix}\qquad\begin{pmatrix}1&1\\-1&1\end{pmatrix}\qquad\begin{pmatrix}1&-1\\1&1\end{pmatrix}\qquad\begin{pmatrix}-1&1\\1&1\end{pmatrix}$$

$$\begin{pmatrix}1&-1\\-1&-1\end{pmatrix}\qquad\begin{pmatrix}-1&1\\-1&-1\end{pmatrix}\qquad\begin{pmatrix}-1&-1\\1&-1\end{pmatrix}\qquad\begin{pmatrix}-1&-1\\-1&1\end{pmatrix}$$

and the non-Hadamard ones being the remaining ones. Also, we have $Y_2 = M_2(\mathbb{Q}) \cap \sqrt{2} O_2$, with the intersection being taken inside $M_N(\mathbb{R})$.

Proof. There are two assertions to be proved, which are both elementary:

(1) In what regards the classification, this is best done by using the Hadamard matrix criterion from Proposition 1.2, which at $N = 2$ simply tells us that, once the first row is chosen, the choices for the second row, as for our matrix to be Hadamard, are exactly 50%. The solutions are those in the statement, listed according to the lexicographic order, with respect to the standard way of reading, left to right, and top to bottom.

(2) In order to prove the second assertion, we use the fact that O_2 consists of 2 types of matrices, namely rotations R_t and symmetries S_t. To be more precise, we first have the rotation of angle $t \in \mathbb{R}$, which is given by the following formula:

$$R_t = \begin{pmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{pmatrix}$$

We also have the symmetry with respect to the Ox axis rotated by $t/2 \in \mathbb{R}$:

$$S_t = \begin{pmatrix}\cos t & \sin t\\ \sin t & -\cos t\end{pmatrix}$$

Now by multiplying everything by $\sqrt{2}$, we are led to the following formula:

$$\sqrt{2}O_2 = \left\{\begin{pmatrix}c & -s\\ s & c\end{pmatrix}\ ,\ \begin{pmatrix}c & s\\ s & -c\end{pmatrix}\Big|c^2 + s^2 = 2\right\}$$

In order to find now the matrices from $\sqrt{2}O_2$ having rational entries, we must solve the equation $x^2 + y^2 = 2z^2$, over the integers. But this is equivalent to $y^2 - z^2 = z^2 - x^2$, which is impossible, unless when $x^2 = y^2 = z^2$. Thus, the rational points come from $c^2 = s^2 = 1$, and so we have $2 \times 2 \times 2 = 8$ rational points, which can only be the points of Y_2. □

At higher values of N, we cannot expect Y_N to consist of the rational points of $\sqrt{N}O_N$. As a basic counterexample, we have the following matrix, which is not Hadamard:

$$\begin{pmatrix}2 & 0 & 0 & 0\\ 0 & 2 & 0 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & 2\end{pmatrix} \in 2O_4$$

Summarizing, it is quite unclear what Y_N is, geometrically speaking. We can, however, solve this question by using complex numbers, in the following way:

Theorem 1.6. *The Hadamard matrices appear as the real points,*

$$Y_N = M_N(\mathbb{R}) \cap X_N$$

of the complex Hadamard matrix manifold, which is given by:

$$X_N = M_N(\mathbb{T}) \cap \sqrt{N}U_N$$

Thus, Y_N is the real part of an intersection of smooth real algebraic manifolds.

Proof. This is a version of Theorem 1.4, which can be established in two ways:

(1) We can either define a complex Hadamard matrix to be a matrix $H \in M_N(\mathbb{T})$ whose rows are pairwise orthogonal, with respect to the scalar product of $\mathbb{C}^N$, then work out a straightforward complex analogue of Theorem 1.3, which gives the formula of X_N in the statement, and then observe that the real points of X_N are the Hadamard matrices.

(2) Or, we can directly use Theorem 1.4, which formally gives the result, as follows:

$$\begin{aligned}
Y_N &= M_N(\pm 1) \cap \sqrt{N} O_N \\
&= \left[M_N(\mathbb{R}) \cap M_N(\mathbb{T})\right] \cap \left[M_N(\mathbb{R}) \cap \sqrt{N} U_N\right] \\
&= M_N(\mathbb{R}) \cap \left[M_N(\mathbb{T}) \cap \sqrt{N} U_N\right] \\
&= M_N(\mathbb{R}) \cap X_N
\end{aligned}$$

We will be back to this, and more precisely with full details regarding (1), starting from section 5 below, when studying the complex Hadamard matrices. □

Summarizing, the Hadamard matrices do belong to real algebraic geometry, but in a quite subtle way. Let us discuss now the examples of Hadamard matrices, with a systematic study at $N = 4, 6, 8, 10$ and so on, continuing the study from Theorem 1.5. In order to cut a bit from complexity, we can use the following notion:

Definition 1.7. *Two Hadamard matrices are called equivalent, and we write $H \sim K$, when it is possible to pass from H to K via the following operations:*

1. *Permuting the rows, or the columns.*
2. *Multiplying the rows or columns by -1.*

Given an Hadamard matrix $H \in M_N(\pm 1)$, we can use the above two operations in order to put H in a "nice" form. Although there is no clear definition for what "nice" should mean, for the Hadamard matrices, with this being actually a quite subtle problem, that we will discuss later on, here are two things that we can look for:

Definition 1.8. *An Hadamard matrix is called dephased when it is of the form*

$$H = \begin{pmatrix} 1 & \ldots & 1 \\ \vdots & * & \\ 1 & & \end{pmatrix}$$

that is, when the first row and the first column consist of 1 *entries only.*

Here the terminology comes from physics, or rather from the complex Hadamard matrices. Indeed, when regarding $H \in M_N(\pm 1)$ as a complex matrix, $H \in M_N(\mathbb{T})$, the -1 entries have "phases", equal to π, and assuming that H is dephased means to assume that we have no phases, on the first row and the first column.

Observe that, up to the equivalence relation, any Hadamard matrix $H \in M_N(\pm 1)$ can be put in dephased form. Moreover, the dephasing operation is unique, if we use only the operations (2) in Definition 1.7, namely row and column multiplications by -1.

With the above notions in hand, we can formulate a nice classification result:

Theorem 1.9. *There is only one Hadamard matrix at $N = 2$, namely*

$$W_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

up to the above equivalence relation for such matrices.

Proof. The matrix in the statement W_2, called Walsh matrix, is clearly Hadamard. Conversely, given $H \in M_N(\pm 1)$ Hadamard, we can dephase it, as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ ac & bd \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ 1 & abcd \end{pmatrix}$$

Now since the dephasing operation preserves the class of the Hadamard matrices, we must have $abcd = -1$, and so we obtain by dephasing the matrix W_2. $\square$

At $N = 3$ we cannot have examples, due to the orthogonality condition between the rows, which forces N to be even, for obvious reasons. At $N = 4$ now, we have several examples. In order to discuss them, let us start with:

Proposition 1.10. *If $H \in M_M(\pm 1)$ and $K \in M_N(\pm 1)$ are Hadamard matrices, then so is their tensor product, constructed in double index notation as follows:*

$$H \otimes K \in M_{MN}(\pm 1)$$

$$(H \otimes K)_{ia,jb} = H_{ij} K_{ab}$$

In particular the Walsh matrices, $W_N = W_2^{\otimes n}$ with $N = 2^n$, are all Hadamard.

Proof. The matrix in the statement $H \otimes K$ has indeed ± 1 entries, and its rows R_{ia} are pairwise orthogonal, as shown by the following computation:

$$\begin{aligned} < R_{ia}, R_{kc} > &= \sum_{jb} H_{ij} K_{ab} \cdot H_{kj} K_{cb} \\ &= \sum_j H_{ij} H_{kj} \sum_b K_{ab} K_{cb} \\ &= M \delta_{ik} \cdot N \delta_{ac} \\ &= MN \delta_{ia,kc} \end{aligned}$$

As for the second assertion, this follows from this, W_2 being Hadamard. $\square$

Before going further, we should clarify a bit our tensor product notations. In order to write $H\in M_N(\pm1)$ the indices of H must belong to $\{1,\ldots,N\}$, or at least to an ordered set $\{I_1,\ldots,I_N\}$. But with double indices we are indeed in this latter situation, because we can use the lexicographic order on these indices. To be more precise, by using the lexicographic order on the double indices, we have the following result:

Proposition 1.11. *Given $H\in M_M(\pm1)$ and $K\in M_N(\pm1)$, we have*

$$H\otimes K=\begin{pmatrix}H_{11}K&\ldots&H_{1M}K\\ \vdots&&\vdots\\ H_{M1}K&\ldots&H_{MM}K\end{pmatrix}$$

with respect to the lexicographic order on the double indices.

Proof. We recall that the tensor product is given by $(H\otimes K)_{ia,jb}=H_{ij}K_{ab}$. Now by using the lexicographic order on the double indices, we obtain:

$$\begin{aligned}H\otimes K&=\begin{pmatrix}(H\otimes K)_{11,11}&(H\otimes K)_{11,12}&\ldots&(H\otimes K)_{11,MN}\\ (H\otimes K)_{12,11}&(H\otimes K)_{12,12}&\ldots&(H\otimes K)_{12,MN}\\ \vdots&\vdots&&\vdots\\ \vdots&\vdots&&\vdots\\ (H\otimes K)_{MN,11}&(H\otimes K)_{MN,12}&\ldots&(H\otimes K)_{MN,MN}\end{pmatrix}\\ &=\begin{pmatrix}H_{11}K_{11}&H_{11}K_{12}&\ldots&H_{1M}K_{MN}\\ H_{11}K_{21}&H_{11}K_{22}&\ldots&H_{1M}K_{2N}\\ \vdots&\vdots&&\vdots\\ \vdots&\vdots&&\vdots\\ H_{M1}K_{N1}&H_{M1}K_{N2}&\ldots&H_{MM}K_{NN}\end{pmatrix}\end{aligned}$$

Thus, by making blocks, we are led to the formula in the statement. □

As a basic example for the tensor product construction, the matrix W_4, obtained by tensoring the matrix W_2 with itself, is given by:

$$W_4=\begin{pmatrix}W_2&W_2\\ W_2&-W_2\end{pmatrix}=\begin{pmatrix}1&1&1&1\\ 1&-1&1&-1\\ 1&1&-1&-1\\ 1&-1&-1&1\end{pmatrix}$$

Getting back now to our classification work, here is the result at $N=4$:

Theorem 1.12. *There is only one Hadamard matrix at $N=4$, namely*

$$W_4=W_2\otimes W_2$$

up to the standard equivalence relation for such matrices.

Proof. Consider an Hadamard matrix $H\in M_4(\pm 1)$, assumed to be dephased:

$$H=\begin{pmatrix}1&1&1&1\\1&a&b&c\\1&d&e&f\\1&g&h&i\end{pmatrix}$$

By orthogonality of the first 2 rows, we must have $\{a,b,c\}=\{-1,-1,1\}$. Thus by permuting the last 3 columns, we can assume that our matrix is as follows:

$$H=\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&m&n&o\\1&p&q&r\end{pmatrix}$$

Now by orthogonality of the first 2 columns, we must have $\{m,p\}=\{-1,1\}$. Thus by permuting the last 2 rows, we can further that our matrix is as follows:

$$H=\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&x&y\\1&-1&z&t\end{pmatrix}$$

But this gives the result, because the orthogonality of the rows gives $x=y=-1$. Indeed, with these values of x,y plugged in, our matrix becomes:

$$H=\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&z&t\end{pmatrix}$$

Now from the orthogonality of the columns we obtain $z=-1,t=1$. Thus, up to equivalence we have $H=W_4$, as claimed. $\square$

The case $N=5$ is excluded, because the orthogonality condition between the rows forces $N\in 2\mathbb N$. The point now is that $N=6$ is excluded as well, because we have:

Theorem 1.13. *The size of an Hadamard matrix $H\in M_N(\pm 1)$ must satisfy*

$$N\in\{2\}\cup 4\mathbb N$$

with this coming from the orthogonality condition between the first 3 rows.

Proof. By permuting the rows and columns or by multiplying them by -1, as to rearrange the first 3 rows, we can always assume that our matrix looks as follows:

$$H=\begin{pmatrix}1\ldots\ldots1&1\ldots\ldots1&1\ldots\ldots1&1\ldots\ldots1\\1\ldots\ldots1&1\ldots\ldots1&-1\ldots-1&-1\ldots-1\\1\ldots\ldots1&-1\ldots-1&1\ldots\ldots1&-1\ldots-1\\\underbrace{\ldots\ldots\ldots}_x&\underbrace{\ldots\ldots\ldots}_y&\underbrace{\ldots\ldots\ldots}_z&\underbrace{\ldots\ldots\ldots}_t\end{pmatrix}$$

Now if we denote by x,y,z,t the sizes of the 4 block columns, as indicated, the orthogonality conditions between the first 3 rows give the following system of equations:

$$(1\perp 2)\quad:\quad x+y=z+t$$

$$(1\perp 3)\quad:\quad x+z=y+t$$

$$(2\perp 3)\quad:\quad x+t=y+z$$

The numbers x,y,z,t being such that the average of any two equals the average of the other two, and so equals the global average, the solution of our system is:

$$x=y=z=t$$

We therefore conclude that the size of our Hadamard matrix, which is the number $N=x+y+z+t$, must be a multiple of 4, as claimed. □

Now back to our small N study, the case $N=6$ being excluded, we have to discuss the case $N=8$. We will use here the $3\times N$ matrix analysis from the proof of Theorem 1.13. Let us start by giving a name to the rectangular matrices that we are interested in:

Definition 1.14. *A partial Hadamard matrix (PHM) is a rectangular matrix*

$$H\in M_{M\times N}(\pm1)$$

whose rows are pairwise orthogonal, with respect to the scalar product of $\mathbb R^N$.

We refer to [72], [76], [119], [137] for a number of results regarding the PHM. In what follows we will just develop some basic theory, useful in connection with our $N=8$ questions, but we will be back to the PHM, on several occasions. We first have:

Definition 1.15. *Two PHM are called equivalent when we can pass from one to the other by permuting the rows or columns, or multiplying the rows or columns by* -1. *Also:*

1. *We say that a PHM is in dephased form when its first row and its first column consist of* 1 *entries.*
2. *We say that a PHM is in standard form when it is dephased, with the* 1 *entries moved to the left as much as possible, by proceeding from top to bottom.*

With these notions in hand, let us go back now to the proof of Theorem 1.13. The study there concerns the $3\times N$ case, and we can improve this, as follows:

Theorem 1.16. *The standard form of the dephased PHM at $M = 2, 3, 4$ is as follows, with $\pm$ standing respectively for various horizontal vectors filled with ± 1,*

$$H = \begin{pmatrix} + & + \\ \underbrace{+}_{N/2} & \underbrace{-}_{N/2} \end{pmatrix}$$

$$H = \begin{pmatrix} + & + & + & + \\ + & + & - & - \\ \underbrace{+}_{N/4} & \underbrace{-}_{N/4} & \underbrace{+}_{N/4} & \underbrace{-}_{N/4} \end{pmatrix}$$

$$H = \begin{pmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & + & + & - & - \\ \underbrace{+}_{a} & \underbrace{-}_{b} & \underbrace{+}_{b} & \underbrace{-}_{a} & \underbrace{+}_{b} & \underbrace{-}_{a} & \underbrace{+}_{a} & \underbrace{-}_{b} \end{pmatrix}$$

and with $a, b \in \mathbb{N}$ being subject to the condition $a + b = N/4$.

Proof. Here the $2 \times N$ assertion is clear, and the $3 \times N$ assertion is something that we already know. Let us pick now an arbitrary partial Hadamard matrix $H \in M_{4\times N}(\pm 1)$, assumed to be in standard form, as in Definition 1.15 (2). According to the $3 \times N$ result, applied to the upper $3 \times N$ part of our matrix, our matrix must look as follows:

$$H = \begin{pmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & + & + & - & - \\ \underbrace{+}_{x} & \underbrace{-}_{x'} & \underbrace{+}_{y'} & \underbrace{-}_{y} & \underbrace{+}_{z'} & \underbrace{-}_{z} & \underbrace{+}_{t} & \underbrace{-}_{t'} \end{pmatrix}$$

To be more precise, our matrix must be indeed of the above form, with x, y, z, t and x', y', z', t' being certain integers, subject to the following relations:

$$x + x' = y + y' = z + z' = t + t' = \frac{N}{4}$$

In terms of these parameters, the missing orthogonality conditions are:

$$\begin{aligned} (1 \perp 4) \quad &: \quad x + y' + z' + t = x' + y + z + t' \\ (2 \perp 4) \quad &: \quad x + y' + z + t' = x' + y + z' + t \\ (3 \perp 4) \quad &: \quad x + y + z' + t' = x' + y' + z + t \end{aligned}$$

Now observe that these orthogonality conditions can be written as follows:

$$(x - x') - (y - y') - (z - z') + (t - t') = 0$$
$$(x - x') - (y - y') + (z - z') - (t - t') = 0$$
$$(x - x') + (y - y') - (z - z') - (t - t') = 0$$

Thus $x-x'=y-y'=z-z'=t-t'$, and so the conditions to be satisfied by the block lengths are $x=y=z=t=a$ and $x'=y'=z'=t'=b$, with $a,b\in\mathbb{N}$ being subject to the condition $a+b=N/4$. Thus, we are led to the conclusion in the statement. $\square$

In the case $N=8$, we have the following more precise result:

Proposition 1.17. *There are exactly two 4×8 partial Hadamard matrices, namely*

$$I=(W_4\ W_4)\quad,\quad J=(W_4\ K_4)$$

us to the standard equivalence relation for such matrices.

Proof. We use the last assertion in Theorem 1.16, regarding the $4\times N$ partial Hadamard matrices, at $N=8$. In the case $a=2,b=0$, the solution is:

$$P=\begin{pmatrix}+&+&+&+&&+&+&+&+\\+&+&+&+&&-&-&-&-\\+&+&-&-&&+&+&-&-\\+&+&-&-&&-&-&+&+\end{pmatrix}$$

In the case $a=1,b=1$, the solution is:

$$Q=\begin{pmatrix}+&+&+&+&&+&+&+&+\\+&+&+&+&&-&-&-&-\\+&+&-&-&&+&+&-&-\\+&-&+&-&&+&-&+&-\end{pmatrix}$$

Finally, in the case $a=0,b=2$, the solution is:

$$R=\begin{pmatrix}+&+&+&+&&+&+&+&+\\+&+&+&+&&-&-&-&-\\+&+&-&-&&+&+&-&-\\-&-&+&+&&+&+&-&-\end{pmatrix}$$

Now observe that, by permuting the columns of P, we can obtain the following matrix, which is precisely the matrix $I=(W_4\ W_4)$ from the statement:

$$I=\begin{pmatrix}+&+&+&+&&+&+&+&+\\+&-&+&-&&+&-&+&-\\+&+&-&-&&+&+&-&-\\+&-&-&+&&+&-&-&+\end{pmatrix}$$

Also, by permuting the columns of Q, we can obtain the following matrix, which is equivalent to the matrix $J=(W_4\ K_4)$ from the statement:

$$J'=\begin{pmatrix}+&+&+&+&&+&+&+&+\\+&-&+&-&&-&-&+&+\\+&+&-&-&&-&+&-&+\\+&-&-&+&&-&+&+&-\end{pmatrix}$$

Finally, regarding the last solution, R, by switching the sign on the last row we obtain $R \sim P$, and so we have $R \sim P \sim I$, which finishes the proof. $\square$

We can now go back to the usual, square Hadamard matrices, and we have:

Theorem 1.18. *The third Walsh matrix, namely*

$$W_8 = \begin{pmatrix} W_4 & W_4 \\ W_4 & -W_4 \end{pmatrix}$$

is the unique Hadamard matrix at $N = 8$, up to equivalence.

Proof. We use Proposition 1.17, which splits the discussion into two cases:

Case 1. We must look here for completions of the following matrix I:

$$I = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \end{pmatrix}$$

Let us first try to complete this partial 4×8 Hadamard matrix into a partial 5×8 Hadamard matrix. The completion must look as follows:

$$I' = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ a & b & c & d & a' & b' & c' & d' \end{pmatrix}$$

The system of equations for the orthogonality conditions is as follows:

$$\begin{aligned} (1 \perp 5) &\quad : \quad a + b + c + d + a' + b' + c' + d' = 0 \\ (2 \perp 5) &\quad : \quad a - b + c - d + a' - b' + c' - d' = 0 \\ (3 \perp 5) &\quad : \quad a + b - c - d + a' + b' - c' - d' = 0 \\ (4 \perp 5) &\quad : \quad a - b - c + d + a' - b' - c' + d' = 0 \end{aligned}$$

Now observe that this system of equations can be written as follows:

$$\begin{aligned} (a + a') + (b + b') + (c + c') + (d + d') = 0 \\ (a + a') - (b + b') + (c + c') - (d + d') = 0 \\ (a + a') + (b + b') - (c + c') - (d + d') = 0 \\ (a + a') - (b + b') - (c + c') + (d + d') = 0 \end{aligned}$$

Since the matrix of this latter system is the Walsh W_4, which is Hadamard, and so rescaled orthogonal, and in particular invertible, the solution is:

$$(a', b', c', d') = -(a, b, c, d)$$

Thus, in order to complete I into a partial 5×8 Hadamard matrix, we can pick any vector $(a,b,c,d)\in(\pm1)^4$, and then set $(a',b',c',d')=-(a,b,c,d)$.

Now let us try to complete I into a full Hadamard matrix $H\in M_8(\pm1)$. By using the above observation, applied to each of the 4 lower rows of H, we conclude that H must be of the following special form, with $L\in M_4(\pm1)$ being a certain matrix:

$$H=\begin{pmatrix}W_4&W_4\\ L&-L\end{pmatrix}$$

Now observe that, in order for H to be Hadamard, L must be Hadamard. Thus, the solutions are those above, with $L\in M_4(\pm1)$ being Hadamard.

As a third step now, let us recall from Theorem 1.12 that we must have $L\sim W_4$. However, in relation with our problem, we cannot really use this in order to conclude directly that we have $H\sim W_8$. To be more precise, in order not to mess up the structure of $I=(W_4\ W_4)$, we are allowed now to use only operations on the rows. And the conclusion here is that, up to equivalence, we have 2 solutions, as follows:

$$P=\begin{pmatrix}W_4&W_4\\ W_4&-W_4\end{pmatrix}\quad,\quad Q=\begin{pmatrix}W_4&W_4\\ K_4&-K_4\end{pmatrix}$$

We will see in moment that these two solutions are actually equivalent, but let us pause now our study of Case 1, after all this work done, and discuss Case 2.

<u>Case 2</u>. Here we must look for completions of the following matrix J:

$$J=\begin{pmatrix}1&1&1&1&-1&1&1&1\\ 1&-1&1&-1&1&-1&1&1\\ 1&1&-1&-1&1&1&-1&1\\ 1&-1&-1&1&1&1&1&-1\end{pmatrix}$$

Let us first try to complete this partial 4×8 Hadamard matrix into a partial 5×8 Hadamard matrix. The completion must look as follows:

$$J'=\begin{pmatrix}1&1&1&1&-1&1&1&1\\ 1&-1&1&-1&1&-1&1&1\\ 1&1&-1&-1&1&1&-1&1\\ 1&-1&-1&1&1&1&1&-1\\ a&b&c&d&x&y&z&t\end{pmatrix}$$

The system of equations for the orthogonality conditions is as follows:

$$(1\perp 5)\quad:\quad a+b+c+d-x+y+z+t=0$$

$$(2\perp 5)\quad:\quad a-b+c-d+x-y+z+t=0$$

$$(3\perp 5)\quad:\quad a+b-c-d+x+y-z+t=0$$

$$(4\perp 5)\quad:\quad a-b-c+d+x+y+z-t=0$$

When regarded as a system in x,y,z,t, the matrix of the system is K_4, which is invertible. Thus, the vector (x,y,z,t) is uniquely determined by the vector (a,b,c,d):

$$(a,b,c,d)\to(x,y,z,t)$$

We have 16 vectors $(a,b,c,d)\in(\pm1)^4$ to be tried, and the first case, covering 8 of them, is that of the row vectors of $\pm W_4$. Here we have an obvious solution, with (x,y,z,t) appearing at right of (a,b,c,d) inside the following matrices, which are Hadamard:

$$R=\begin{pmatrix}W_4&K_4\\W_4&-K_4\end{pmatrix}\quad,\quad S=\begin{pmatrix}W_4&K_4\\-W_4&K_4\end{pmatrix}$$

As for the second situation, this is that of the 8 vectors $(a,b,c,d)\in(\pm1)^4$ which are not row vectors of $\pm W_4$. But this is the same as saying that, up to permutations, we have $(a,b,c,d)=\pm(-1,1,1,1)$. In this case, and with $+$ sign, the system of equations is:

$$-x+y+z+t=-2$$

$$x-y+z+t=2$$

$$x+y-z+t=2$$

$$x+y+z-t=2$$

By summing the first equation with the other ones we obtain:

$$y+z=y+t=z+t=0$$

Thus $y=z=t=0$, and this solution does not correspond to an Hadamard matrix.

Summarizing, we are done with the 5×8 completion problem in Case 2, the solutions coming from the rows of the matrices R,S given above. Now when using this, as for getting up to full 8×8 completions, the R,S cases obviously cannot mix, and so we are left with the Hadamard matrices R,S above, as being the only solutions.

In order to conclude now, observe that we have $R=Q^t$ and $R\sim S$. Also, it is elementary to check that we have $P\sim Q$, and this finishes the proof. $\square$

At $N=12$ now, we can use a construction due to Paley [109]. Let $q=p^r$ be an odd prime power, and consider the quadratic character $\chi:\mathbb F_q\to\{-1,0,1\}$, given by:

$$\chi(a)=\begin{cases}0&\text{if }a=0\\1&\text{if }a=b^2,b\neq0\\-1&\text{otherwise}\end{cases}$$

We can construct then the following matrix, with indices in $\mathbb F_q$:

$$Q_{ab}=\chi(b-a)$$

With these conventions, the Paley construction is as follows:

Theorem 1.19. *Given an odd prime power $q=p^r$, construct $Q_{ab}=\chi(b-a)$ as above. We have then constructions of Hadamard matrices, as follows:*

(1) *Paley 1: if $q=3(4)$ we have a matrix of size $N=q+1$, as follows:*

$$P_N^1=1+\begin{pmatrix}0&1&\ldots&1\\ -1&&&\\ \vdots&&Q&\\ -1&&&\end{pmatrix}$$

(2) *Paley 2: if $q=1(4)$ we have a matrix of size $N=2q+2$, as follows:*

$$P_N^2=\begin{pmatrix}0&1&\ldots&1\\ 1&&&\\ \vdots&&Q&\\ 1&&&\end{pmatrix}\quad:\quad 0\to\begin{pmatrix}1&-1\\ -1&-1\end{pmatrix}\quad,\quad \pm1\to\pm\begin{pmatrix}1&1\\ 1&-1\end{pmatrix}$$

These matrices are skew-symmetric ($H+H^t=2$), respectively symmetric ($H=H^t$).

Proof. In order to simplify the presentation, we will denote by 1 all the identity matrices, of any size, and by $\mathbb{I}$ all the rectangular all-one matrices, of any size as well.

It is elementary to check that the matrix $Q_{ab}=\chi(a-b)$ has the following properties:

$$QQ^t=q1-\mathbb{I}$$

$$Q\mathbb{I}=\mathbb{I}Q=0$$

In addition, we have the following formulae, which are elementary as well, coming from the fact that -1 is a square in $\mathbb{F}_q$ precisely when $q=1(4)$:

$$q=1(4)\implies Q=Q^t$$

$$q=3(4)\implies Q=-Q^t$$

With these observations in hand, the proof goes as follows:

(1) With our conventions for the symbols 1 and $\mathbb{I}$, explained above, the matrix in the statement is as follows:

$$P_N^1=\begin{pmatrix}1&\mathbb{I}\\ -\mathbb{I}&1+Q\end{pmatrix}$$

With this formula in hand, the Hadamard matrix condition follows from:

$$\begin{aligned}P_N^1(P_N^1)^t&=\begin{pmatrix}1&\mathbb{I}\\ -\mathbb{I}&1+Q\end{pmatrix}\begin{pmatrix}1&-\mathbb{I}\\ \mathbb{I}&1-Q\end{pmatrix}\\ &=\begin{pmatrix}N&0\\ 0&\mathbb{I}+1-Q^2\end{pmatrix}\\ &=\begin{pmatrix}N&0\\ 0&N\end{pmatrix}\end{aligned}$$

(2) If we denote by G,F the matrices in the statement, which replace respectively the $0,1$ entries, then we have the following formula for our matrix:

$$P_N^2=\begin{pmatrix}0&\mathbb{I}\\ \mathbb{I}&Q\end{pmatrix}\otimes F+1\otimes G$$

With this formula in hand, the Hadamard matrix condition follows from:

$$\begin{aligned}(P_N^2)^2&=\begin{pmatrix}0&\mathbb{I}\\ \mathbb{I}&Q\end{pmatrix}^2\otimes F^2+\begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes G^2+\begin{pmatrix}0&\mathbb{I}\\ \mathbb{I}&Q\end{pmatrix}\otimes(FG+GF)\\&=\begin{pmatrix}q&0\\0&q\end{pmatrix}\otimes 2+\begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes 2+\begin{pmatrix}0&\mathbb{I}\\ \mathbb{I}&Q\end{pmatrix}\otimes 0\\&=\begin{pmatrix}N&0\\0&N\end{pmatrix}\end{aligned}$$

Finally, the last assertion is clear, from the above formulae relating Q,Q^t. □

As an illustration for the above result, we have:

Theorem 1.20. *We have Paley 1 and 2 matrices at $N=12$, which are equivalent:*

$$P_{12}^1\sim P_{12}^2$$

In fact, this matrix is the unique Hadamard one at $N=12$, up to equivalence.

Proof. This is a mixture of elementary and difficult results, the idea being as follows:

(1) We have $12=11+1$, with $11=3(4)$ being prime, so the Paley 1 construction applies indeed, with the first row vector of Q being $(0+-+++---+-)$.

(2) Also, we have $12=2\times5+2$, with $5=1(4)$ being prime, so the Paley 2 construction applies as well, with the first row vector of Q being $(0+--+)$.

(3) It is routine to check that we have $P_{12}^1\sim P_{12}^2$, by some computations in the spirit of those from the end of the proof of Theorem 1.18 above.

(4) As for the last assertion, regarding the global uniqueness, this is something quite technical, requiring some clever block decomposition techniques. □

At $N=16$ now, the situation becomes fairly complicated, as follows:

Theorem 1.21. *The Hadamard matrices at $N=16$ are as follows:*

1. *We have the Walsh matrix W_{16}.*
2. *There are no Paley matrices.*
3. *Besides W_{16}, we have 4 more matrices, up to equivalence.*

Proof. Once again, this is a mixture of elementary and more advanced results:

(1) This is clear.

(2) This comes from the fact that we have $16 = 15 + 1$, with 15 not being a prime power, and from the fact that we have $16 = 2 \times 7 + 2$, with $7 \neq 1(4)$.

(3) This is something very technical, basically requiring a computer. □

At $N = 20$ and bigger, the situation becomes extremely complicated, and the study is usually done with a mix of advanced algebraic methods, and computer techniques. The overall conclusion is the number of Hadamard matrices of size $N \in 4\mathbb{N}$ grows with N, and in a rather exponential fashion. In particular, we are led in this way into:

Conjecture 1.22 (Hadamard Conjecture (HC))**.** *There is at least one Hadamard matrix*

$$H \in M_N(\pm 1)$$

for any integer $N \in 4\mathbb{N}$.

This conjecture, going back to the 19th century, is one of the most beautiful statements in combinatorics, linear algebra, and mathematics in general. Quite remarkably, the numeric verification so far goes up to the number of the beast:

$$\mathfrak{N} = 666$$

Our purpose now will be that of gathering some evidence for this conjecture. By using the Walsh construction, we have examples at each $N = 2^n$. We can add various examples coming from the Paley 1 and Paley 2 constructions, and we are led to:

Theorem 1.23. *The HC is verified at least up to $N = 88$, as follows:*

(1) *At $N = 4, 8, 16, 32, 64$ we have Walsh matrices.*
(2) *At $N = 12, 20, 24, 28, 44, 48, 60, 68, 72, 80, 84, 88$ we have Paley 1 matrices.*
(3) *At $N = 36, 52, 76$ we have Paley 2 matrices.*
(4) *At $N = 40, 56$ we have Paley 1 matrices tensored with W_2.*

However, at $N = 92$ these constructions (Walsh, Paley, tensoring) don't work.

Proof. First of all, the numbers in (1-4) are indeed all the multiples of 4, up to 88. As for the various assertions, the proof here goes as follows:

(1) This is clear.

(2) Here the number $N - 1$ takes the following values:

$$q = 11, 19, 23, 27, 43, 47, 59, 67, 71, 79, 83, 87$$

These are all prime powers, so we can apply the Paley 1 construction, in all these cases.

(3) Since $N = 4(8)$ here, and $N/2 - 1$ takes the values $q = 17, 25, 37$, all prime powers, we can indeed apply the Paley 2 construction, in these cases.

(4) At $N=40$ we have indeed $P_{20}^1\otimes W_2$, and at $N=56$ we have $P_{28}^1\otimes W_2$.

Finally, we have $92-1=7\times 13$, so the Paley 1 construction does not work, and $92/2=46$, so the Paley 2 construction, or tensoring with W_2, does not work either. $\square$

At $N=92$ now, the situation is considerably more complicated, and we have:

Theorem 1.24. *Assuming that $A,B,C,D\in M_K(\pm 1)$ are circulant, symmetric, pairwise commute and satisfy the condition*

$$A^2+B^2+C^2+D^2=4K$$

the following $4K\times 4K$ matrix

$$H=\begin{pmatrix}A&B&C&D\\-B&A&-D&C\\-C&D&A&-B\\-D&-C&B&A\end{pmatrix}$$

is Hadamard, called of Williamson type. Moreover, such a matrix exists at $K=23$.

Proof. We use the same method as for the Paley theorem, namely tensor calculus.

Consider the following matrices $1,i,j,k\in M_4(0,1)$, called the quaternion units:

$$1=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\quad,\quad i=\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

$$j=\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}\quad,\quad k=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$$

These matrices describe the positions of the A,B,C,D entries in the matrix H from the statement, and so this matrix can be written as follows:

$$H=A\otimes 1+B\otimes i+C\otimes j+D\otimes k$$

Assuming now that A,B,C,D are symmetric, we have:

$$\begin{aligned}HH^t&=(A\otimes 1+B\otimes i+C\otimes j+D\otimes k)\\&\quad(A\otimes 1-B\otimes i-C\otimes j-D\otimes k)\\&=(A^2+B^2+C^2+D^2)\otimes 1-([A,B]-[C,D])\otimes i\\&\quad-([A,C]-[B,D])\otimes j-([A,D]-[B,C])\otimes k\end{aligned}$$

Now assume that our matrices A,B,C,D pairwise commute, and satisfy as well the condition in the statement, namely $A^2+B^2+C^2+D^2=4K$. In this case, it follows from the above formula that we have $HH^t=4K$, so we obtain indeed an Hadamard matrix.

In general, finding such matrices is a difficult task, and this is where Williamson's extra assumption that A, B, C, D should be taken circulant comes from. Regarding now the $K = 23$ construction, which produces an Hadamard matrix of order $N = 92$, this comes via a computer search. We refer here to [34], [147]. $\square$

Things get even worse at higher values of N, where more and more complicated constructions are needed. The whole subject is quite technical, and, as already mentioned, human knowledge here stops so far at $\mathfrak{N} = 666$. See [1], [55], [57], [74], [86], [119].

As a conceptual finding on the subject, however, we have the recent theory of the cocyclic Hadamard matrices, which is based on the following notion:

Definition 1.25. *A cocycle on a finite group G is a matrix $H \in M_G(\pm 1)$ satisfying:*

$$H_{gh}H_{gh,k} = H_{g,hk}H_{hk}$$

$$H_{11} = 1$$

If the rows of H are pairwise orthogonal, we say that H is a cocyclic Hadamard matrix.

Here the definition of the cocycles is the usual one, with the equations coming from the fact that $F = \mathbb{Z}_2 \times G$ must be a group, with multiplication as follows:

$$(u, g)(v, h) = (H_{gh} \cdot uv, gh)$$

As a basic example here, the Walsh matrix $H = W_{2^n}$ is cocyclic, coming from the group $G = \mathbb{Z}_2^n$, with cocycle as follows:

$$H_{gh} = (-1)^{<g,h>}$$

As explained in [56], and in other papers, many other known examples of Hadamard matrices are cocyclic, and this leads to the following conjecture:

Conjecture 1.26 (Cocyclic Hadamard Conjecture)**.** *There is at least one cocyclic Hadamard matrix $H \in M_N(\pm 1)$, for any $N \in 4\mathbb{N}$.*

Having such a statement formulated is certainly a big advance with respect to the HC, and this is probably the main achievement of modern Hadamard matrix theory. However, in what regards a potential proof, there is no clear strategy here, at least so far.

We will be back to these questions in sections 13-16 below, with the remark that the construction $\mathbb{Z}_2^n \to W_{2^n}$ can be extended as to cover all the Hadamard matrices, by replacing $\mathbb{Z}_2^n$ with a suitable quantum permutation group. However, in what regards the potential applications to the HC, there is no clear strategy here either.

2. Analytic aspects

We have seen so far that the algebraic theory of the Hadamard matrices, while very nice at the elementary level, ultimately leads into some difficult questions. So, let us step now into analytic questions. The first result here, found in 1893 by Hadamard [71], about 25 years after Sylvester's 1867 founding paper [124], and which actually led to such matrices being called Hadamard, is a determinant bound, as follows:

Theorem 2.1. *Given a matrix $H \in M_N(\pm 1)$, we have*

$$|\det H| \leq N^{N/2}$$

with equality precisely when H is Hadamard.

Proof. We use here the fact, which often tends to be forgotten, that the determinant of a system of N vectors in $\mathbb{R}^N$ is the signed volume of the associated parallelepiped:

$$\det(H_1, \ldots, H_N) = \pm vol < H_1, \ldots, H_N >$$

This is actually the definition of the determinant, in case you have forgotten the basics (!), with the need for the sign coming for having good additivity properties.

In the case where our vectors take their entries in ± 1, we therefore have the following inequality, with equality precisely when our vectors are pairwise orthogonal:

$$|\det(H_1, \ldots, H_N)| \leq ||H_1|| \times \ldots \times ||H_N|| = (\sqrt{N})^N$$

Thus, we have obtained the result, straight from the definition of det. □

The above result suggests doing several analytic things, as for instance looking at the maximizers $H \in M_N(\pm 1)$ of the quantity $|\det H|$, at values $N \in \mathbb{N}$ which are not multiples of 4. As a basic result here, at $N = 3$ the situation is as follows:

Proposition 2.2. *For a matrix $H \in M_3(\pm 1)$ we have $|\det H| \leq 4$, and this estimate is sharp, with the equality case being attained by the matrix*

$$Q_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}$$

and its conjugates, via the Hadamard equivalence relation.

Proof. In order to get started, observe that Theorem 2.1 above provides us with the following bound, which is of course not sharp, $\det H$ being an integer:

$$|\det H| \leq 3\sqrt{3} = 5.1961..$$

Now observe that, $\det H$ being a sum of six ± 1 terms, it must be en even number. Thus, we obtain $|\det H| \leq 4$. Our claim now is that the following happens, with the nonzero situation appearing precisely for the matrix Q_3 in the statement, and its conjugates:

$$\det H \in \{-4, 0, 4\}$$

Indeed, let us try to find the matrices $H\in M_3(\pm 1)$ having the property $\det H\neq 0$. Up to equivalence, we can assume that the first row is $(1,1,1)$. Then, once again up to equivalence, we can assume that the second row is $(1,1,-1)$. And then, once again up to equivalence, we can assume that the third row is $(1,-1,1)$. Thus, we must have:

$$H=\begin{pmatrix}1&1&1\\1&1&-1\\1&-1&1\end{pmatrix}$$

The determinant of this matrix being -4, we have proved our claim, and the last assertion in the statement too, as a consequence of our study. $\square$

In general, all this suggests the following definition:

Definition 2.3. *A quasi-Hadamard matrix is a square binary matrix*

$$H\in M_N(\pm 1)$$

which maximizes the quantity $|\det H|$.

We know from Theorem 2.1 that at $N\in 4\mathbb{N}$ such matrices are precisely the Hadamard matrices, provided that the Hadamard Conjecture holds at N. At values $N\notin 4\mathbb{N}$, what we have are certain matrices which can be thought of as being "generalized Hadamard matrices", the simplest examples being the matrix Q_3 from Proposition 2.2, and its Hadamard conjugates. For more on all this, we refer to [110].

As a comment, however, Proposition 2.2 might look a bit dissapointing, because it is hard to imagine that the matrix Q_3 there, which is not a very interesting matrix, can really play the role of a "generalized Hadamard matrix" at $N=3$. We will come later with more interesting solutions to this problem, a first solution being as follows:

$$K_3=\frac{1}{\sqrt{3}}\begin{pmatrix}-1&2&2\\2&-1&2\\2&2&-1\end{pmatrix}$$

To be more precise, this matrix is of course not binary, but it is definitely an interesting matrix, that we will see to be sharing many properties with the Hadamard matrices. We have as well another solution to the $N=3$ problem, which uses complex numbers, and more specifically the number $w=e^{2\pi i/3}$, which is as follows:

$$F_3=\begin{pmatrix}1&1&1\\1&w&w^2\\1&w^2&w\end{pmatrix}$$

Once again, this matrix is not binary, and not even real, but it is an interesting matrix, that we will see to be sharing as well many properties with the Hadamard matrices.

As a conclusion, looking at the maximizers $H\in M_N(\pm1)$ of the quantity $|\det H|$ is not exactly an ideal method, when looking for analogues of the Hadamard matrices at the forbidden size values $N\notin 4\mathbb N$, at least when N is small. The situation changes, however, when looking at such questions at big values of $N\in\mathbb N$. We have here:

Theorem 2.4. *We have estimates of type*

$$\max_{H\in M_N(\pm1)}|\det H|\simeq N^{N/2}$$

which are valid in the $N\to\infty$ limit, modulo the Hadamard Conjectuere.

Proof. As already mentioned, this is just an informal statement, which is there as an introduction to the subject, in the lack of something more precise, and elementary. There are basically two ways of dealing with such questions, namely:

(1) A first idea is that of using the existence of an Hadamard matrix $H_N\in M_N(\pm1)$, at values $N\in 4\mathbb N$, modulo the Hadamard Conjecture of course, and then completing it into binary matrices H_{N+k} of size $N+1,2,3$, for instance in the following way:

$$H_{N+k}=\begin{pmatrix}&&&1&\ldots&1\\&H_N&&&&\\&&&1&\ldots&1\\1&&1&-1&&1\\\vdots&&\vdots&&\ddots&\\1&&1&1&&-1\end{pmatrix}$$

The determinant estimates for such matrices are however quite technical, and we refer here to the literature on the subject [110].

(2) A second method is by using probability theory. The set of binary matrices $M_N(\pm1)$ is of course a probability space, when endowed with the counting measure rescaled by $1/2^{N^2}$, and the determinant can be regarded as a random variable on this space:

$$\det:M_N(\pm1)\to\mathbb Z$$

The point now is that the distribution of this variable can be computed, in the $N\to\infty$ limit, and as a consequence, we can investigate the maximizers of $|\det H|$. Once again, all this is quite technical, and we refer here to the literature [133], [134]. $\square$

From a "dual" point of view, the question of locating Y_N inside $\sqrt N O_N$, once again via analytic methods, makes sense as well. The result here, from [19], is as follows:

Theorem 2.5. *Given a matrix $U\in O_N$ we have*

$$||U||_1\leq N\sqrt N$$

with equality precisely when $H=\sqrt NU$ is Hadamard.

Proof. We have indeed the following estimate, for any $U\in O_N$, which uses the Cauchy-Schwarz inequality, and the trivial fact that we have $||U||_2=\sqrt{N}$:

$$||U||_1=\sum_{ij}|U_{ij}|\leq N\left(\sum_{ij}|U_{ij}|^2\right)^{1/2}=N\sqrt{N}$$

The equality case holds when we have $|U_{ij}|=\frac{1}{\sqrt{N}}$, for any i,j. But this amounts in saying that $H=\sqrt{N}U$ must satisfy $H\in M_N(\pm1)$, as desired. □

We will need more general norms as well, so let record the following result:

Proposition 2.6. *If $\psi:[0,\infty)\to\mathbb{R}$ is strictly concave/convex, the quantity*

$$F(U)=\sum_{ij}\psi(U_{ij}^2)$$

over U_N is maximized/minimized by the rescaled Hadamard matrices, $U=H/\sqrt{N}$.

Proof. We recall that the Jensen inequality states that for ψ convex we have:

$$\psi\left(\frac{x_1+\ldots+x_n}{n}\right)\leq\frac{\psi(x_1)+\ldots+\psi(x_n)}{n}$$

In our case, let us take $n=N^2$ and:

$$\{x_1,\ldots,x_n\}=\left\{U_{ij}^2\Big|i,j=1,\ldots,N\right\}$$

We obtain that for any convex function ψ, the following holds:

$$\psi\left(\frac{1}{N}\right)\leq\frac{F(U)}{N^2}$$

Thus we have the folloowing estimate:

$$F(U)\geq N^2\psi\left(\frac{1}{N}\right)$$

Now by assuming as in the statement that ψ is strictly convex, the equality case holds precisely when the numbers U_{ij}^2 are all equal, so when $H=\sqrt{N}U$ is Hadamard.
The proof for concave functions is similar. □

Of particular interest for our considerations are the power functions $\psi(x)=x^{p/2}$, which are concave at $p\in[1,2)$, and convex at $p\in(2,\infty)$. These functions lead to:

Theorem 2.7. *The rescaled versions $U=H/\sqrt{N}$ of the Hadamard matrices $H\in M_N(\pm1)$ can be characterized as being:*

1. *The maximizers of the p-norm on O_N, at any $p\in[1,2)$.*
2. *The minimizers of the p-norm on O_N, at any $p\in(2,\infty]$.*

Proof. Consider indeed the p-norm on O_N, which at $p\in[1,\infty)$ is given by:

$$||U||_p=\left(\sum_{ij}|U_{ij}|^p\right)^{1/p}$$

By the above discussion, involving the functions $\psi(x)=x^{p/2}$, Proposition 2.6 applies and gives the results at $p\in[1,\infty)$, the precise estimates being as follows:

$$||U||_p=\begin{cases}\leq N^{2/p-1/2}&\text{if } p<2\\ =N^{1/2}&\text{if } p=2\\ \geq N^{2/p-1/2}&\text{if } p>2\end{cases}$$

As for the case $p=\infty$, this follows with $p\to\infty$, or directly via Cauchy-Schwarz. $\square$

As it was the case with the Hadamard determinant bound, all this suggests doing some further geometry and analysis, this time on the Lie group O_N, with a notion of "almost Hadamard matrix" at stake. Let us formulate indeed, in analogy with Definition 2.3:

Definition 2.8. *An optimal almost Hadamard matrix is a rescaled orthogonal matrix*

$$H\in\sqrt{N}O_N$$

which maximizes the 1*-norm.*

Here the adjective "optimal" comes from the fact that, in contrast with what happens over $M_N(\pm1)$, in connection with the determinant bound, here over $\sqrt{N}O_N$ we have more flexibility, and we can talk if we want about the local maximizers of the 1-norm. These latter matrices are called "almost Hadamard", and we will investigate them in the next section. Also, we will talk there about more general p-norms as well.

We know from Theorem 2.6 that at $N\in4\mathbb{N}$ the absolute almost Hadamard matrices are precisely the Hadamard matrices, provided that the Hadamard Conjecture holds at N. At values $N\notin4\mathbb{N}$, what we have are certain matrices which can be thought of as being "generalized Hadamard matrices", and are waiting to be investigated. Let us begin with a preliminary study, at $N=3$. The result here, from [19], is as follows:

Theorem 2.9. *For any matrix $U\in O_3$ we have the estimate*

$$||U||_1\leq5$$

and this is sharp, with the equality case being attained by the matrix

$$U=\frac{1}{3}\begin{pmatrix}-1&2&2\\2&-1&2\\2&2&-1\end{pmatrix}$$

and its conjugates, via the Hadamard equivalence relation.

Proof. By dividing by $\det U$, we can assume that we have $U\in SO_3$. We use the Euler-Rodrigues parametrization for the elements of SO_3, namely:

$$U=\begin{pmatrix}x^2+y^2-z^2-t^2&2(yz-xt)&2(xz+yt)\\2(xt+yz)&x^2+z^2-y^2-t^2&2(zt-xy)\\2(yt-xz)&2(xy+zt)&x^2+t^2-y^2-z^2\end{pmatrix}$$

Here $(x,y,z,t)\in S^3$ come from the map $SU_2\to SO_3$. Now in order to obtain the estimate, we linearize. We must prove that for any numbers $x,y,z,t\in\mathbb R$ we have:

$$\begin{aligned}&|x^2+y^2-z^2-t^2|+|x^2+z^2-y^2-t^2|+|x^2+t^2-y^2-z^2|\\&+2\left(|yz-xt|+|xz+yt|+|xt+yz|+|zt-xy|+|yt-xz|+|xy+zt|\right)\\&\leq 5(x^2+y^2+z^2+t^2)\end{aligned}$$

The problem being symmetric in x,y,z,t, and invariant under sign changes, we may assume that we have:

$$x\geq y\geq z\geq t\geq 0$$

Now if we look at the 9 absolute values in the above formula, in 7 of them the sign is known, and in the remaining 2 ones the sign is undetermined.

More precisely, the inequality to be proved is:

$$\begin{aligned}&(x^2+y^2-z^2-t^2)+(x^2+z^2-y^2-t^2)+|x^2+t^2-y^2-z^2|\\&+2\left(|yz-xt|+(xz+yt)+(xt+yz)+(xy-zt)+(xz-yt)+(xy+zt)\right)\\&\leq 5(x^2+y^2+z^2+t^2)\end{aligned}$$

After simplification and rearrangement of the terms, this inequality reads:

$$\begin{aligned}&|x^2+t^2-y^2-z^2|+2|xt-yz|\\\leq\ \ &3x^2+5y^2+5z^2+7t^2-4xy-4xz-2xt-2yz\end{aligned}$$

In principle we have now 4 cases to discuss, depending on the possible signs appearing at left. It is, however, easier to proceed simply by searching for the optimal case.

First, by writing $y=\alpha+\varepsilon,z=\alpha-\varepsilon$ and by making ε vary over the real line, we see that the optimal case is when $\varepsilon=0$, hence when $y=z$.

The case $y=z=0$ or $y=z=\infty$ being clear, and not sharp, we can assume that we have $y=z=1$. Thus we must prove that for $x\geq 1\geq t\geq 0$ we have:

$$|x^2+t^2-2|+2|xt-1|\leq 3x^2+8+7t^2-8x-2xt$$

In the case $xt\geq 1$ we have $x^2+t^2\geq 2$, and the inequality becomes:

$$2xt+4x\leq x^2+3t^2+6$$

In the case $xt\leq 1,x^2+t^2\leq 2$ we get:

$$x^2+1+2t^2\geq 2x$$

In the remaining case $xt \leq 1, x^2 + t^2 \geq 2$ we get:

$$x^2 + 4 + 3t^2 \geq 4x$$

But these inequalities are all true, and this finishes the proof of the estimate.

Now regarding the maximum, according to the above discussion this is attained at $(xyzt) = (1110)$ or at $(xyzt) = (2110)$, plus permutations.

The corresponding matrix is, modulo permutations:

$$V = \frac{1}{3}\begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ -2 & 2 & -1 \end{pmatrix}$$

For this matrix we have indeed $||V||_1 = 5$, and we are done. $\square$

In terms of Definition 2.8, the conclusion is as follows:

Theorem 2.10. *The optimal almost Hadamard matrices at $N = 3$ are*

$$K_3 = \frac{1}{\sqrt{3}}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}$$

and its conjugates, via the Hadamard equivalence relation.

Proof. This is indeed a reformulation of Theorem 2.9, using Definition 2.8. $\square$

The above result and the matrix K_3 appearing there are quite interesting, because they remind the Hadamard matrix K_4 studied in section 1 above, given by:

$$K_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

To be more precise, all this suggests looking at the following matrices $K_N \in \sqrt{N}O_N$, having arbitrary size $N \in \mathbb{N}$:

$$K_N = \frac{1}{\sqrt{N}}\begin{pmatrix} 2-N & & 2 \\ & \ddots & \\ 2 & & 2-N \end{pmatrix}$$

These matrices are in general not optimal almost Hadamard, in the sense of Definition 2.8 above, for instance because at $N = 2$ or $N = 8, 12, 16, \ldots$ they are not Hadamard. We will see in the next section that these matrices are however "almost Hadamard", in the sense that they locally maximize the 1-norm on $\sqrt{N}O_N$.

To summarize, the computation of the maximizers of the 1-norm on O_N is a difficult question, a bit like the computation of the maximizers of $|\det|$ on $M_N(\pm 1)$ was, and looking instead at the local maximizers of the 1-norm on O_N is the way to be followed, with some interesting examples and combinatorics at stake. We will be back to this.

Let us discuss now, as a continuation of all this, an analytic reformulation of the Hadamard Conjecture. Following [19], the starting statement here is:

Proposition 2.11. *We have the following estimate,*

$$\sup_{U\in O_N}||U||_1\leq N\sqrt{N}$$

with equality if and only if there exists an Hadamard matrix of order N.

Proof. This follows indeed from the inequality $||U||_1\leq N\sqrt{N}$, with equality in the rescaled Hadamard matrix case, $U=H/\sqrt{N}$, from Theorem 2.5 above. □

We begin our study with the following observation:

Proposition 2.12. *If the Hadamard conjecture holds, then*

$$\sup_{U\in O_N}||U||_1\geq(N-4.5)\sqrt{N}$$

for any $N\in\mathbb{N}$.

Proof. If N is a multiple of 4 we can use an Hadamard matrix, and we are done. In general, we can write $N=M+k$ with $4|M$ and $0\leq k\leq 3$, and use an Hadamard matrix of order N, completed with an identity matrix of order k. This gives:

$$\begin{aligned}\sup_{U\in O_N}||U||_1&\geq M\sqrt{M}+k\\&\geq(N-3)\sqrt{N-3}+3\\&\geq(N-4.5)\sqrt{N}+3\end{aligned}$$

Here the last inequality, proved by taking squares, is valid for any $N\geq 5$. □

We would like to understand now which estimates on the quantity in Proposition 2.12 imply the Hadamard conjecture. We first have the following result:

Proposition 2.13. *For any norm one vector $U\in\mathbb{R}^N$ we have the formula*

$$||U||_1=\sqrt{N}\left(1-\frac{||U-H||^2}{2}\right)$$

where $H\in\mathbb{R}^N$ is the vector given by:

$$H_i=\frac{\mathrm{sgn}(U_i)}{\sqrt{N}}$$

Proof. We indeed have the following computation:

$$\begin{aligned} ||U-H||^2 &= \sum_i \left(U_i - \frac{\mathrm{sgn}(U_i)}{\sqrt{N}}\right)^2 \\ &= \sum_i U_i^2 - \frac{2|U_i|}{\sqrt{N}} + \frac{1}{N} \\ &= ||U||^2 - \frac{2||U||_1}{\sqrt{N}} + 1 \\ &= 2 - \frac{2||U||_1}{\sqrt{N}} \end{aligned}$$

But this gives the formula in the statement. □

Next, we have the following estimate, also from [19]:

Proposition 2.14. *Let N be even, and let $U \in O_N$ be a matrix such that*

$$H = \frac{S}{\sqrt{N}}$$

is not Hadamard, where $S_{ij} = \mathrm{sgn}(U_{ij})$. We have then the following estimate:

$$||U||_1 \leq N\sqrt{N} - \frac{1}{N\sqrt{N}}$$

Proof. Since H is not Hadamard, this matrix has two distinct rows H_1, H_2 which are not orthogonal. Since N is even, we must have:

$$|<H_1, H_2>| \geq \frac{2}{N}$$

We obtain from this the following estimate:

$$\begin{aligned} ||U_1 - H_1|| + ||U_2 - H_2|| &\geq |<U_1 - H_1, H_2>| + |<U_2 - H_2, U_1>| \\ &\geq |<U_1 - H_1, H_2> + <U_2 - H_2, U_1>| \\ &= |<U_2, U_1> - <H_1, H_2>| \\ &= |<H_1, H_2>| \\ &\geq \frac{2}{N} \end{aligned}$$

Now by applying the estimate in Proposition 2.13 to U_1, U_2, we obtain:

$$\begin{aligned} ||U_1||_1 + ||U_2||_1 &= \sqrt{N}\left(2 - \frac{||U_1 - H_1||^2 + ||U_2 - H_2||^2}{2}\right) \\ &\leq \sqrt{N}\left(2 - \left(\frac{||U_1 - H_1|| + ||U_2 - H_2||}{2}\right)^2\right) \\ &\leq \sqrt{N}\left(2 - \frac{1}{N^2}\right) \\ &= 2\sqrt{N} - \frac{1}{N\sqrt{N}} \end{aligned}$$

By adding to this inequality the 1-norms of the remaining $N-2$ rows, all bounded from above by $\sqrt{N}$, we obtain the result. □

We can now answer the question raised above, as follows:

Theorem 2.15. *If N is even and the following holds,*

$$\sup_{U \in O_N} ||U||_1 \geq N\sqrt{N} - \frac{1}{N\sqrt{N}}$$

then the Hadamard conjecture holds at N.

Proof. Indeed, if the Hadamard conjecture does not hold at N, then the assumption of Proposition 2.14 is satisfied for any $U \in O_N$, and this gives the result. □

As a related result now, let us compute the average of the 1-norm on O_N. We have here the following estimate, from [19]:

Theorem 2.16. *We have the following estimate,*

$$\int_{O_N} ||U||_1 \, dU \simeq \sqrt{\frac{2}{\pi}} \cdot N\sqrt{N}$$

valid in the $N \to \infty$ limit.

Proof. We use the well-known fact that the row slices of O_N are all isomorphic to the sphere S^{N-1}, with the restriction of the Haar measure of O_N corresponding in this way to the uniform measure on S^{N-1}. Together with a standard symmetry argument, this shows that the average of the 1-norm on O_N is given by:

$$\begin{aligned}
\int_{O_N}||U||_1\,dU &= \sum_{ij}\int_{O_N}|U_{ij}|\,dU\\
&= N^2\int_{O_N}|U_{11}|\,dU\\
&= N^2\int_{S^{N-1}}|x_1|\,dx
\end{aligned}$$

We denote by I the integral on the right. By standard calculus, we obtain:

$$\begin{aligned}
I &= \begin{cases}\frac{2}{\pi}\cdot\frac{2\cdot4\cdot6\ldots(N-2)}{3\cdot5\cdot7\ldots(N-1)} & (N\text{ even})\\ 1\cdot\frac{3\cdot5\cdot7\ldots(N-2)}{2\cdot4\cdot6\ldots(N-1)} & (N\text{ odd})\end{cases}\\
&= \begin{cases}\frac{4^M}{\pi M}\binom{2M}{M}^{-1} & (N=2M)\\ 4^{-M}\binom{2M}{M} & (N=2M+1)\end{cases}
\end{aligned}$$

Now by using the Stirling formula, we get:

$$\begin{aligned}
I &\simeq \begin{cases}\frac{4^M}{\pi M}\cdot\frac{\sqrt{\pi M}}{4^M} & (N=2M)\\ 4^{-M}\cdot\frac{4^M}{\sqrt{\pi M}} & (N=2M+1)\end{cases}\\
&= \begin{cases}\frac{1}{\sqrt{\pi M}} & (N=2M)\\ \frac{1}{\sqrt{\pi M}} & (N=2M+1)\end{cases}\\
&\simeq \sqrt{\frac{2}{\pi N}}
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

The above result gives in particular the following estimate, in the $N\to\infty$ limit:

$$\sup_{U\in O_N}||U||_1\geq\sqrt{\frac{2}{\pi}}\cdot N\sqrt{N}$$

In order to find better estimates, the problem is to compute the higher moments of the 1-norm, which are the following integrals, depending on a parameter $k \in \mathbb{N}$:

$$I_k = \int_{O_N} ||U||_1^k \, dU$$

The computation of these integrals is however a difficult problem, and no concrete applications to the Hadamard Conjecture have been found so far. See [19], [20].

Let us discuss now a third and final analytic topic, in connection with the bistochastic Hadamard matrices. The motivation here comes from the fact that the bistochastic matrices look better than their non-bistochastic counterparts. As an illustration here, the Walsh matrix W_4 looks better in its bistochastic form, which is the matrix K_4:

$$\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix} \sim \begin{pmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix}$$

We have the following algebraic result on the subject, which shows in particular that we cannot put any Hadamard matrix in bistochastic form:

Theorem 2.17. *For an Hadamard matrix $H \in M_N(\mathbb{C})$, the following are equivalent:*

1. *H is bistochastic, with sums λ.*
2. *H is row-stochastic, with sums λ, and $\lambda^2 = N$.*

In particular, is such a matrix exists, then $N \in 4\mathbb{N}$ must be a square.

Proof. Both the implications are elementary, as follows:

(1) $\implies$ (2) If we denote by $H_1, \ldots, H_N \in (\pm 1)^N$ the rows of H, we have indeed:

$$\begin{aligned} N &= \sum_i < H_1, H_i > \\ &= \sum_j H_{1j} \sum_i H_{ij} \\ &= \sum_j H_{1j} \cdot \lambda \\ &= \lambda^2 \end{aligned}$$

(2) $\implies$ (1) Consider the all-one vector $\xi = (1)_i \in \mathbb{R}^N$. The fact that H is row-stochastic with sums λ reads:

$$\begin{aligned} \sum_j H_{ij} = \lambda, \forall i &\iff \sum_j H_{ij}\xi_j = \lambda \xi_i, \forall i \\ &\iff H\xi = \lambda \xi \end{aligned}$$

Also, the fact that H is column-stochastic with sums λ reads:

$$\begin{aligned}\sum_i H_{ij}=\lambda,\forall j &\iff \sum_j H_{ij}\xi_i=\lambda\xi_j,\forall j\\ &\iff H^t\xi=\lambda\xi\end{aligned}$$

We must prove that the first condition implies the second one, provided that the row sum λ satisfies $\lambda^2=N$. But this follows from the following computation:

$$\begin{aligned}H\xi=\lambda\xi &\implies H^tH\xi=\lambda H^t\xi\\ &\implies N\xi=\lambda H^t\xi\\ &\implies H^t\xi=\lambda\xi\end{aligned}$$

Thus, we have proved both the implications, and we are done. □

In practice now, the even Walsh matrices, having size $N=4^n$, which is a square as required above, can be put in bistochastic form, as follows:

$$W_{4^n}\sim K_4^{\otimes n}$$

As for the odd Walsh matrices, having size $N=2\times 4^n$, these cannot be put in bistochastic form. However, we can do this over the complex numbers, with the equivalence being as follows at $N=2$, and then by tensoring with $K_4^{\otimes n}$ in general:

$$\begin{pmatrix}1&1\\1&-1\end{pmatrix}\sim\begin{pmatrix}i&1\\1&i\end{pmatrix}$$

This is quite interesting, and in general now, it is known from [75] that any complex Hadamard matrix can be put in bistochastic form, by a certain non-explicit method. Thus, we have here some theory to be developed. We will be back to this.

There is as well an analytic approach to these questions, based on:

Theorem 2.18. *For an Hadamard matrix $H\in M_N(\pm1)$, the excess,*

$$E(H)=\sum_{ij}H_{ij}$$

satisfies $|E(H)|\leq N\sqrt{N}$, with equality if and only if H is bistochastic.

Proof. In terms of the all-one vector $\xi=(1)_i\in\mathbb{R}^N$, we have:

$$E(H)=\sum_{ij}H_{ij}=\sum_{ij}H_{ij}\xi_j\xi_i=\sum_i(H\xi)_i\xi_i=<H\xi,\xi>$$

Now by using the Cauchy-Schwarz inequality, along with the fact that $U=H/\sqrt{N}$ is orthogonal, and hence of norm 1, we obtain, as claimed:

$$|E(H)|\leq||H\xi||\cdot||\xi||\leq||H||\cdot||\xi||^2=N\sqrt{N}$$

Regarding now the equality case, this requires the vectors $H\xi,\xi$ to be proportional, and so our matrix H to be row-stochastic. But since $U=H/\sqrt{N}$ is orthogonal, we have:

$$H\xi\sim\xi\iff H^t\xi\sim\xi$$

Thus our matrix H must be bistochastic, as claimed. □

One interesting question, that we would like to discuss now, is that of computing the law of the excess over the equivalence class of H. Following [11], let us start with:

Definition 2.19. *The glow of $H\in M_N(\pm1)$ is the distribution of the excess,*

$$E=\sum_{ij}H_{ij}$$

over the Hadamard equivalence class of H.

Since the excess is invariant under permutations of rows and columns, we can restrict the attention to the matrices $\widetilde{H}\simeq H$ obtained by switching signs on rows and columns. More precisely, let $(a,b)\in\mathbb{Z}_2^N\times\mathbb{Z}_2^N$, and consider the following matrix:

$$\widetilde{H}_{ij}=a_ib_jH_{ij}$$

We can regard the sum of entries of $\widetilde{H}$ as a random variable, over the group $\mathbb{Z}_2^N\times\mathbb{Z}_2^N$, and we have the following equivalent description of the glow:

Proposition 2.20. *Given a matrix $H\in M_N(\pm1)$, if we define $\varphi:\mathbb{Z}_2^N\times\mathbb{Z}_2^N\to\mathbb{Z}$ as the excess of the corresponding Hadamard equivalent of H,*

$$\varphi(a,b)=\sum_{ij}a_ib_jH_{ij}$$

then the glow is the probability measure on $\mathbb{Z}$ given by $\mu(\{k\})=P(\varphi=k)$.

Proof. The function φ in the statement can indeed be regarded as a random variable over the group $\mathbb{Z}_2^N\times\mathbb{Z}_2^N$, with this latter group being endowed with its uniform probability measure P. The distribution μ of this variable φ is then given by:

$$\mu(\{k\})=\frac{1}{4^N}\#\left\{(a,b)\in\mathbb{Z}_2^N\times\mathbb{Z}_2^N\Big|\varphi(a,b)=k\right\}$$

By the above discussion, this distribution is exactly the glow. □

The terminology in Definition 2.19 comes from the following picture. Assume that we have a square city, with N horizontal streets and N vertical streets, and with street lights at each crossroads. When evening comes the lights are switched on at the positions (i,j)

where $H_{ij}=1$, and then, all night long, they are randomly switched on and off, with the help of $2N$ master switches, one at the end of each street:

$$\begin{matrix}
\to&&\diamondsuit&\diamondsuit&\diamondsuit&\diamondsuit\\
\to&&\diamondsuit&\times&\diamondsuit&\times\\
\to&&\diamondsuit&\diamondsuit&\times&\times\\
\to&&\diamondsuit&\times&\times&\diamondsuit\\
\\
&&\uparrow&\uparrow&\uparrow&\uparrow
\end{matrix}$$

With this picture in mind, μ describes indeed the glow of the city. At a more advanced level now, all this is related to the Gale-Berlekamp game [67], [116]. In order to compute the glow, it is useful to have in mind the following picture:

$$\begin{matrix}
&&b_1&\ldots&b_N&&\\
&&\downarrow&&\downarrow&&\\
(a_1)&\to&H_{11}&\ldots&H_{1N}&\Rightarrow&S_1\\
\vdots&&\vdots&&\vdots&&\vdots\\
(a_N)&\to&H_{N1}&\ldots&H_{NN}&\Rightarrow&S_N
\end{matrix}$$

Here the columns of H have been multiplied by the entries of the horizontal switching vector b, the resulting sums on rows are denoted $S_1,\ldots,S_N$, and the vertical switching vector a still has to act on these sums, and produce the glow component at b. With this picture in mind, we first have the following result, from [11]:

Proposition 2.21. *The glow of a matrix $H\in M_N(\pm1)$ is given by*

$$\mu=\frac{1}{2^N}\sum_{b\in\mathbb Z_2^N}\beta_1(c_1)*\ldots*\beta_N(c_N)$$

where the measures on the right are convolution powers of Bernoulli laws,

$$\beta_r(c)=\left(\frac{\delta_r+\delta_{-r}}{2}\right)^{*c}$$

and where $c_r=\#\{r\in|S_1|,\ldots,|S_N|\}$, with $S=Hb$.

Proof. We use the interpretation of the glow explained above. So, consider the decomposition of the glow over b components:

$$\mu=\frac{1}{2^N}\sum_{b\in\mathbb Z_2^N}\mu_b$$

With the notation $S=Hb$, as in the statement, the numbers $S_1,\ldots,S_N$ are the row sums of $\widetilde{H}_{ij}=H_{ij}a_ib_j$. Thus the glow components are given by:

$$\mu_b=law\left(\pm S_1\pm S_2\ldots\pm S_N\right)$$

By permuting now the sums on the right, we have the following formula:

$$\mu_b = law\Big(\underbrace{\pm 0 \ldots \pm 0}_{c_0}\ \underbrace{\pm 1 \ldots \pm 1}_{c_1} \ldots\ldots \underbrace{\pm N \ldots \pm N}_{c_N}\Big)$$

Now since the $\pm$ variables each follow a Bernoulli law, and these Bernoulli laws are independent, we obtain a convolution product as in the statement. $\square$

We will need the following elementary fact:

Proposition 2.22. *Let $H \in M_N(\pm 1)$ be an Hadamard matrix of order $N \geq 4$.*

(1) *The sums of entries on rows $S_1, \ldots, S_N$ are even, and equal modulo 4.*

(2) *If the sums on the rows $S_1, \ldots, S_N$ are all 0 modulo 4, then the number of rows whose sum is 4 modulo 8 is odd for $N = 4(8)$, and even for $N = 0(8)$.*

Proof. This is something elementary, the proof being as follows:

(1) Let us pick two rows of our matrix, and then permute the columns such that these two rows look as follows:

$$\begin{pmatrix}1\ldots\ldots 1 & 1\ldots\ldots 1 & -1\ldots -1 & -1\ldots -1\\ \underbrace{1\ldots\ldots 1}_{a} & \underbrace{-1\ldots -1}_{b} & \underbrace{1\ldots\ldots 1}_{c} & \underbrace{-1\ldots -1}_{d}\end{pmatrix}$$

We have $a + b + c + d = N$, and by orthogonality we obtain $a + d = b + c$. Thus $a + d = b + c = N/2$, and since $N/2$ is even we have $b = c(2)$, which gives the result.

(2) In the case where H is "row-dephased", in the sense that its first row consists of 1 entries only, the row sums are $N, 0, \ldots, 0$, and so the result holds. In general now, by permuting the columns we can assume that our matrix looks as follows:

$$H = \begin{pmatrix}1\ldots\ldots 1 & -1\ldots -1\\ \underbrace{\vdots}_{x} & \underbrace{\vdots}_{y}\end{pmatrix}$$

We have $x + y = N = 0(4)$, and since the first row sum $S_1 = x - y$ is by assumption 0 modulo 4, we conclude that x, y are even. In particular, since y is even, the passage from H to its row-dephased version $\widetilde{H}$ can be done via $y/2$ double sign switches.

Now, in view of the above, it is enough to prove that the conclusion in the statement is stable under a double sign switch. So, let $H \in M_N(\pm 1)$ be Hadamard, and let us perform to it a double sign switch, say on the first two columns. Depending on the values of the entries on these first two columns, the total sums on the rows change as follows:

$$\begin{matrix}(+ & + & \ldots & \ldots) & : & S \to S - 4\\ (+ & - & \ldots & \ldots) & : & S \to S\\ (- & + & \ldots & \ldots) & : & S \to S\\ (- & - & \ldots & \ldots) & : & S \to S + 4\end{matrix}$$

We can see that the changes modulo 8 of the row sum S occur precisely in the first and in the fourth case. But, since the first two columns of our matrix $H \in M_N(\pm 1)$ are orthogonal, the total number of these cases is even, and this finishes the proof. □

Observe that Proposition 2.21 and Proposition 2.22 (1) show that the glow of an Hadamard matrix of order $N \geq 4$ is supported by $4\mathbb{Z}$. With this in hand, we have:

Theorem 2.23. *Let $H \in M_N(\pm 1)$ be an Hadamard matrix of order $N \geq 4$, and denote by μ^{even}, μ^{odd} the mass one-rescaled restrictions of $\mu \in \mathcal{P}(4\mathbb{Z})$ to $8\mathbb{Z}, 8\mathbb{Z}+4$.*

1. *At $N = 0(8)$ we have $\mu = \frac{3}{4}\mu^{even} + \frac{1}{4}\mu^{odd}$.*
2. *At $N = 4(8)$ we have $\mu = \frac{1}{4}\mu^{even} + \frac{3}{4}\mu^{odd}$.*

Proof. We use the glow decomposition over b components, from Proposition 2.21:

$$\mu = \frac{1}{2^N}\sum_{b \in \mathbb{Z}_2^N} \mu_b$$

The idea is that the decomposition formula in the statement will occur over averages of the following type, over truncated sign vectors $c \in \mathbb{Z}_2^{N-1}$:

$$\mu_c' = \frac{1}{2}(\mu_{+c} + \mu_{-c})$$

Indeed, we know from Proposition 2.22 (1) that modulo 4, the sums on rows are either $0, \ldots, 0$ or $2, \ldots, 2$. Now since these two cases are complementary when pairing switch vectors $(+c, -c)$, we can assume that we are in the case $0, \ldots, 0$ modulo 4.

Now by looking at this sequence modulo 8, and letting x be the number of 4 components, so that the number of 0 components is $N - x$, we have:

$$\frac{1}{2}(\mu_{+c} + \mu_{-c}) = \frac{1}{2}\left(law(\underbrace{\pm 0 \ldots \pm 0}_{N-x}\ \underbrace{\pm 4 \ldots \pm 4}_{x}) + law(\underbrace{\pm 2 \ldots \pm 2}_{N}) \right)$$

Now by using Proposition 2.22 (2), the first summand splits $1-0$ or $0-1$ on $8\mathbb{Z}, 8\mathbb{Z}+4$, depending on the class of N modulo 8. As for the second summand, since N is even this always splits $\frac{1}{2} - \frac{1}{2}$ on $8\mathbb{Z}, 8\mathbb{Z}+4$. Thus, by making the average we obtain either a $\frac{3}{4} - \frac{1}{4}$ or a $\frac{1}{4} - \frac{3}{4}$ splitting on $8\mathbb{Z}, 8\mathbb{Z}+4$, depending on the class of N modulo 8, as claimed. □

Various computer simulations suggest that the above measures μ^{even}, μ^{odd} don't have further general algebraic properties. Analytically speaking now, we have:

Theorem 2.24. *The glow moments of $H \in M_N(\pm 1)$ are given by:*

$$\int_{\mathbb{Z}_2^N \times \mathbb{Z}_2^N} \left(\frac{E}{N}\right)^{2p} = (2p)!! + O(N^{-1})$$

In particular the normalized variable $F = E/N$ becomes Gaussian with $N \to \infty$.

Proof. Consider the variable in the statement, written as before, as a function of two vectors a,b, belonging to the group $\mathbb{Z}_2^N\times\mathbb{Z}_2^N$:

$$E=\sum_{ij}a_ib_jH_{ij}$$

Let $P_{even}(r)\subset P(r)$ be the set of partitions of $\{1,\ldots,r\}$ having all blocks of even size. The moments of E are then given by:

$$\begin{aligned}\int_{\mathbb{Z}_2^N\times\mathbb{Z}_2^N}E^r\qquad&\int_{\mathbb{Z}_2^N\times\mathbb{Z}_2^N}\sum_{ix}a_{i_1}\ldots a_{i_r}b_{x_1}\ldots b_{x_r}H_{i_1x_1}\ldots H_{i_rx_r}\\&=\sum_{ix}H_{i_1x_1}\ldots H_{i_rx_r}\int_{\mathbb{Z}_2^N}a_{i_1}\ldots a_{i_r}\int_{\mathbb{Z}_2^N}b_{x_1}\ldots b_{x_r}\\&=\sum_{\pi,\sigma\in P_{even}(r)}\sum_{\ker i=\pi,\ker x=\sigma}H_{i_1x_1}\ldots H_{i_rx_r}\end{aligned}$$

Thus the moments decompose over partitions $\pi\in P_{even}(r)$, with the contributions being obtained by integrating the following quantities:

$$C(\sigma)=\sum_{\ker x=\sigma}\sum_i H_{i_1x_1}\ldots H_{i_rx_r}\cdot a_{i_1}\ldots a_{i_r}$$

Now by Möbius inversion, we obtain a formula as follows:

$$\int_{\mathbb{Z}_2^N\times\mathbb{Z}_2^N}E^r=\sum_{\pi\in P_{even}(r)}K(\pi)N^{|\pi|}I(\pi)$$

To be more precise, here the coefficients on the right are as follows, where μ is the Möbius function of $P_{even}(r)$:

$$K(\pi)=\sum_{\sigma\in P_{even}(r)}\mu(\pi,\sigma)$$

As for the contributions on the right, with the convention that $H_1,\ldots,H_N\in\mathbb{Z}_2^N$ are the rows of our matrix H, these are as follows:

$$I(\pi)=\sum_i\prod_{b\in\pi}\frac{1}{N}\left\langle\prod_{r\in b}H_{i_r},1\right\rangle$$

With this formula in hand, the first assertion follows, because the biggest elements of the lattice $P_{even}(2p)$ are the $(2p)!!$ partitions consisting of p copies of a 2-block:

$$\int_{\mathbb{Z}_2^N\times\mathbb{Z}_2^N}\left(\frac{E}{N}\right)^{2p}=(2p)!!+O(N^{-1})$$

As for the second assertion, this follows from the moment formula, and from the fact that the glow of $H\in M_N(\pm1)$ is real, and symmetric with respect to 0. See [11]. $\square$

3. Norm maximizers

We have seen in the previous section that the set $Y_N = M_N(\pm 1) \cap \sqrt{N}O_N$ formed by the $N \times N$ Hadamard matrices can be located inside $\sqrt{N}O_N$ by using analytic techniques, and more precisely variations of the following result:

Theorem 3.1. *Given a matrix $H \in \sqrt{N}O_N$ we have:*

(1) $||H||_1 \leq N^{2/p}$ *for $p \in [1, 2)$, with equality precisely when H is Hadamard.*
(2) $||H||_1 \geq N^{2/p}$ *for $p \in (2, \infty]$, with equality precisely when H is Hadamard.*

Proof. This is something that we know from section 2, the idea being that for $H \in \sqrt{N}O_N$ we have $||H||_2 = N$, and by using this, together with the Jensen inequality for $\psi(x) = x^{p/2}$, or simply the Hölder inequality for the norms, we obtain the results. As for the case $p = \infty$, this follows with $p \to \infty$, or directly via Cauchy-Schwarz. □

In general, computing the maximizers of the 1-norm on $\sqrt{N}O_N$ remains a difficult question. So, based on the above, let us formulate the following definition:

Definition 3.2. *A matrix $H \in \sqrt{N}O_N$ is called:*

(1) *Almost Hadamard, if it locally maximizes the 1-norm on $\sqrt{N}O_N$.*
(2) *Optimal almost Hadamard, if it maximizes the 1-norm on $\sqrt{N}O_N$.*

More generally, we can talk about p-almost Hadamard matrices, at any $p \in [1, \infty] - \{2\}$, exactly in the same way, by using the results in Theorem 3.1. When a matrix $H \in \sqrt{N}O_N$ is almost Hadamard at any p, we call it "absolute almost Hadamard".

In order to get started, let us study the local mazimizers of the 1-norm on $\sqrt{N}O_N$. It is technically convenient here to rescale by $1\sqrt{N}$, and work instead over the orthogonal group O_N, by using the avaliable tools here. Following [19], we first have:

Theorem 3.3. *If $U \in O_N$ locally maximizes the 1-norm, then*

$$U_{ij} \neq 0$$

must hold for any i, j.

Proof. Assume that U has a 0 entry. By permuting the rows we can assume that this 0 entry is in the first row, having under it a nonzero entry in the second row.

We denote by $U_1, \ldots, U_N$ the rows of U. By permuting the columns we can assume that we have a block decomposition of the following type:

$$\begin{pmatrix} U_1 \\ U_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & Y & A & B \\ 0 & X & 0 & C & D \end{pmatrix}$$

Here X, Y, A, B, C, D are certain vectors with nonzero entries, with A, B, C, D chosen such that each entry of A has the same sign as the corresponding entry of C, and each entry of B has sign opposite to the sign of the corresponding entry of D.

Our above assumption states that X is not the null vector.

For $t>0$ small consider the matrix U^t obtained by rotating by t the first two rows of U. In row notation, this matrix is given by:

$$U^t=\begin{pmatrix}\cos t&\sin t\\ -\sin t&\cos t\\ &&1\\ &&&\ddots\\ &&&&1\end{pmatrix}\begin{pmatrix}U_1\\ U_2\\ U_3\\ \vdots\\ U_N\end{pmatrix}=\begin{pmatrix}\cos t\cdot U_1+\sin t\cdot U_2\\ -\sin t\cdot U_1+\cos t\cdot U_2\\ U_3\\ \vdots\\ U_N\end{pmatrix}$$

We make the convention that the lower-case letters denote the 1-norms of the corresponding upper-case vectors. According to the above sign conventions, we have:

$$\begin{aligned}||U^t||_1&=||\cos t\cdot U_1+\sin t\cdot U_2||_1+||-\sin t\cdot U_1+\cos t\cdot U_2||_1+\sum_{i=3}^N u_i\\ &=(\cos t+\sin t)(x+y+b+c)+(\cos t-\sin t)(a+d)+\sum_{i=3}^N u_i\\ &=||U||_1+(\cos t+\sin t-1)(x+y+b+c)+(\cos t-\sin t-1)(a+d)\end{aligned}$$

By using $\sin t=t+O(t^2)$ and $\cos t=1+O(t^2)$ we obtain:

$$\begin{aligned}||U^t||_1&=||U||_1+t(x+y+b+c)-t(a+d)+O(t^2)\\ &=||U||_1+t(x+y+b+c-a-d)+O(t^2)\end{aligned}$$

In order to conclude, we have to prove that U cannot be a local maximizer of the 1-norm. This will basically follow by comparing the norm of U to the norm of U^t, with $t>0$ small or $t<0$ big. However, since in the above computation it was technically convenient to assume $t>0$, we actually have three cases:

Case 1: $b+c>a+d$. Here for $t>0$ small enough the above formula shows that we have $||U^t||_1>||U||_1$, and we are done.

Case 2: $b+c=a+d$. Here we use the fact that X is not null, which gives $x>0$. Once again for $t>0$ small enough we have $||U^t||_1>||U||_1$, and we are done.

Case 3: $b+c<a+d$. In this case we can interchange the first two rows of U and restart the whole procedure: we fall in Case 1, and we are done again. $\square$

Let us study now the critical points. It is convenient here to talk about more general p-norms, or even more general functions of the quantities $|U_{ij}|$, because this will lead to some interesting combinatorics. Following [19], [25], we have the following result:

Theorem 3.4. *Consider a differentiable function $\varphi:[0,\infty)\to\mathbb{R}$. A matrix $U\in O_N^*$ is then a critical point of the quantity*

$$F(U)=\sum_{ij}\varphi(|U_{ij}|)$$

precisely when the matrix WU^t is symmetric, where:

$$W_{ij}=\mathrm{sgn}(U_{ij})\varphi'(|U_{ij}|)$$

In particular, for $F(U)=||U||_1$ we need SU^t to be symmetric, where $S_{ij}=\mathrm{sgn}(U_{ij})$.

Proof. We regard O_N as a real algebraic manifold, with coordinates U_{ij}. This manifold consists by definition of the zeroes of the following polynomials:

$$A_{ij}=\sum_k U_{ik}U_{jk}-\delta_{ij}$$

Since O_N is smooth, and so is a differential manifold in the usual sense, it follows from the general theory of Lagrange multipliers that a given matrix $U\in O_N$ is a critical point of F precisely when the following condition is satisfied:

$$dF\in span(dA_{ij})$$

Regarding the space $span(dA_{ij})$, this consists of the following quantities:

$$\begin{aligned}\sum_{ij}M_{ij}dA_{ij}&=\sum_{ijk}M_{ij}(U_{ik}dU_{jk}+U_{jk}dU_{ik})\\&=\sum_{jk}(M^tU)_{jk}dU_{jk}+\sum_{ik}(MU)_{ik}dU_{ik}\\&=\sum_{ij}(M^tU)_{ij}dU_{ij}+\sum_{ij}(MU)_{ij}dU_{ij}\end{aligned}$$

In order to compute dF, observe first that, with $S_{ij}=sgn(U_{ij})$, we have:

$$d|U_{ij}|=d\sqrt{U_{ij}^2}=\frac{U_{ij}dU_{ij}}{|U_{ij}|}=S_{ij}dU_{ij}$$

Now let us set, as in the statement:

$$W_{ij}=sgn(U_{ij})\varphi'(|U_{ij}|)$$

In terms of these variables, we obtain:

$$dF=\sum_{ij}d\left(\varphi(|U_{ij}|)\right)=\sum_{ij}\varphi'(|U_{ij}|)d|U_{ij}|=\sum_{ij}W_{ij}dU_{ij}$$

We conclude that $U\in O_N$ is a critical point of F if and only if there exists a matrix $M\in M_N(\mathbb{R})$ such that the following two conditions are satisfied:

$$W=M^tU\quad,\quad W=MU$$

Now observe that these two equations can be written as follows:

$$M^t = WU^t \quad , \quad M = WU^t$$

Thus, the matrix WU^t must be symmetric, as claimed. $\square$

In order to process the above result, we can use the following notion:

Definition 3.5. *Given $U \in O_N$, we consider its "color decomposition"*

$$U = \sum_{r>0} rU_r$$

with $U_r \in M_N(-1,0,1)$ containing the sign components at $r > 0$, and we call U:

1. *Semi-balanced, if U_rU^t and U^tU_r, with $r > 0$, are all symmetric.*
2. *Balanced, if $U_rU_s^t$ and $U_r^tU_s$, with $r,s > 0$, are all symmetric.*

These conditions are quite natural, because for an orthogonal matrix $U \in O_N$, the relations $UU^t = U^tU = 1$ translate as follows, in terms of the color decomposition:

$$\sum_{r>0} rU_rU^t = \sum_{r>0} rU^tU_r = 1$$

$$\sum_{r,s>0} rsU_rU_s^t = \sum_{r,s>0} rsU_r^tU_s = 1$$

Thus, our balancing conditions express the fact that the various components of the above sums are all symmetric. Now back to our critical point questions, we have:

Theorem 3.6. *For a matrix $U \in O_N^*$, the following are equivalent:*

1. *U is a critical point of $F(U) = \sum_{ij} \varphi(|U_{ij}|)$, for any $\varphi : [0,\infty) \to \mathbb{R}$.*
2. *U is a critical point of all the p-norms, with $p \in [1,\infty)$.*
3. *U is semi-balanced, in the above sense.*

Proof. We use the critical point criterion found in Theorem 3.4 above. In terms of the color decomposition, the matrix constructed there is given by:

$$\begin{aligned}
(WU^t)_{ij} &= \sum_k \mathrm{sgn}(U_{ik})\varphi'(|U_{ik}|)U_{jk} \\
&= \sum_{r>0} \varphi'(r) \sum_{k,|U_{ik}|=r} \mathrm{sgn}(U_{ik})U_{jk} \\
&= \sum_{r>0} \varphi'(r) \sum_k (U_r)_{ik}U_{jk} \\
&= \sum_{r>0} \varphi'(r)(U_rU^t)_{ij}
\end{aligned}$$

Thus we have the following formula:

$$WU^t = \sum_{r>0} \varphi'(r) U_r U^t$$

Now when the function $\varphi : [0,\infty) \to \mathbb{R}$ varies, either as an arbitrary differentiable function, or as a power function $\varphi(x) = x^p$ with $p \in [1,\infty)$, the individual components of this sum must be all self-adjoint, and this leads to the conclusion in the statement. $\square$

In practice now, most of the known examples of semi-balanced matrices are actually balanced, so we will investigate instead this latter class of matrices. Following [25], we have the following collection of simple facts, regarding such matrices:

Theorem 3.7. *The class of balanced matrices is as follows:*

1. *It contains the matrices $U = H/\sqrt{N}$, with $H \in M_N(\pm 1)$ Hadamard.*
2. *It is stable under transposition.*
3. *It is stable under taking tensor products.*
4. *It is stable under Hadamard equivalence.*
5. *It contains the matrix $V_N = \frac{1}{N}(2\mathbb{I}_N - N1_N)$, where $\mathbb{I}_N$ is the all-1 matrix.*

Proof. All these results are elementary, the proof being as follows:

(1) Here $U \in O_N$ follows from the Hadamard condition, and since there is only one color component, namely $U_{1/\sqrt{N}} = H$, the balancing condition is satisfied as well.

(2) Assuming that $U = \sum_{r>0} rU_r$ is the color decomposition of a given matrix $U \in O_N$, the color decomposition of the transposed matrix U^t is as follows:

$$U^t = \sum_{r>0} rU_r^t$$

It follows that if U is balanced, so is the transposed matrix U^t.

(3) Assuming that $U = \sum_{r>0} rU_r$ and $V = \sum_{s>0} sV_s$ are the color decompositions of two given orthogonal matrices U, V, we have:

$$U \otimes V = \sum_{r,s>0} rs \cdot U_r \otimes V_s = \sum_{p>0} p \sum_{p=rs} U_r \otimes V_s$$

Thus the color components of $W = U \otimes V$ are the following matrices:

$$W_p = \sum_{p=rs} U_r \otimes V_s$$

It follows that if U, V are both balanced, then so is $W = U \otimes V$.

(4) We recall that the Hadamard equivalence consists in permuting rows and columns, and switching signs on rows and columns. Since all these operations correspond to certain conjugations at the level of the matrices $U_r U_s^t, U_r^t U_s$, we obtain the result.

(5) The matrix in the statement, which goes back to [28], is as follows:

$$V_N=\frac{1}{N}\begin{pmatrix}2-N&2&\ldots&2\\ 2&2-N&\ldots&2\\ \ldots&\ldots&\ldots&\ldots\\ 2&2&\ldots&2-N\end{pmatrix}$$

Observe that this matrix is indeed orthogonal, its rows being of norm one, and pairwise orthogonal. The color components of this matrix being $V_{2/N-1}=1_N$ and $V_{2/N}=\mathbb{I}_N-1_N$, it follows that this matrix is balanced as well, as claimed. □

Let us look now more in detail at the matrix V_N from the above statement, and at the matrices having similar properties. Following [28], let us start our study with:

Definition 3.8. *An (a,b,c) pattern is a matrix $M\in M_N(0,1)$, with $N=a+2b+c$, such that any two rows look as follows,*

$$\begin{matrix}0\ldots0&0\ldots0&1\ldots1&1\ldots1\\ \underbrace{0\ldots0}_a&\underbrace{1\ldots1}_b&\underbrace{0\ldots0}_b&\underbrace{1\ldots1}_c\end{matrix}$$

up to a permutation of the columns.

As explained in [28], there are many interesting examples of (a,b,c) patterns, coming from the balanced incomplete block designs (BIBD), and all these examples can produce two-entry unitary matrices, by replacing the $0,1$ entries with suitable numbers x,y. Now back to the matrix V_N from Theorem 3.7 (5), observe that this matrix comes from a $(0,1,N-2)$ pattern. And also, independently of this, this matrix has the remarkable property of being at the same time circulant and self-adjoint. We have in fact:

Theorem 3.9. *The following matrices are balanced:*

1. *The orthogonal matrices coming from (a,b,c) patterns.*
2. *The orthogonal matrices which are circulant and symmetric.*

Proof. These observations basically go back to [28], the proofs being as follows:

(1) If we denote by $P,Q\in M_N(0,1)$ the matrices describing the positions of the $0,1$ entries inside the pattern, then we have the following formulae:

$$\begin{aligned}PP^t=P^tP&=a\mathbb{I}_N+b1_N\\ QQ^t=Q^tQ&=c\mathbb{I}_N+b1_N\\ PQ^t=P^tQ=QP^t=Q^tP&=b\mathbb{I}_N-b1_N\end{aligned}$$

Since all these matrices are symmetric, U is balanced, as claimed.

(2) Assume that $U\in O_N$ is circulant, $U_{ij}=\gamma_{j-i}$, and in addition symmetric, which means $\gamma_i=\gamma_{-i}$. Consider the following sets, which must satisfy $D_r=-D_r$:

$$D_r=\{k:|\gamma_r|=k\}$$

In terms of these sets, we have the following formula:

$$\begin{aligned}(U_rU_s^t)_{ij} &= \sum_k (U_r)_{ik}(U_s)_{jk}\\ &= \sum_k \delta_{|\gamma_{k-i}|,r}\,\mathrm{sgn}(\gamma_{k-i})\cdot\delta_{|\gamma_{k-j}|,s}\,\mathrm{sgn}(\gamma_{k-j})\\ &= \sum_{k\in(D_r+i)\cap(D_s+j)} \mathrm{sgn}(\gamma_{k-i})\,\mathrm{sgn}(\gamma_{k-j})\end{aligned}$$

With $k=i+j-m$ we obtain, by using $D_r=-D_r$, and then $\gamma_i=\gamma_{-i}$:

$$\begin{aligned}(U_rU_s^t)_{ij} &= \sum_{m\in(-D_r+j)\cap(-D_s+i)} \mathrm{sgn}(\gamma_{j-m})\,\mathrm{sgn}(\gamma_{i-m})\\ &= \sum_{m\in(D_r+i)\cap(D_r+j)} \mathrm{sgn}(\gamma_{j-m})\,\mathrm{sgn}(\gamma_{i-m})\\ &= \sum_{m\in(D_r+i)\cap(D_r+j)} \mathrm{sgn}(\gamma_{m-j})\,\mathrm{sgn}(\gamma_{m-i})\end{aligned}$$

Now by interchanging $i\leftrightarrow j$, and with $m\to k$, this formula becomes:

$$(U_rU_s^t)_{ji} = \sum_{k\in(D_r+i)\cap(D_r+j)} \mathrm{sgn}(\gamma_{k-i})\,\mathrm{sgn}(\gamma_{k-j})$$

By comparing with the previous formula, we deduce that the matrix $U_rU_s^t$ is symmetric, as claimed. The proof for $U_r^tU_s$ is similar. □

Let us get now into analytic questions. As in Theorem 3.4, it is convenient to do the computations in a general framework, with a function as follows:

$$F(U)=\sum_{ij}\psi(U_{ij}^2)$$

Consider the following function, depending on $t>0$ small:

$$f(t)=F(Ue^{tA})=\sum_{ij}\psi((Ue^{tA})_{ij}^2)$$

Here $U\in O_N$ is an arbitrary orthogonal matrix, and $A\in M_N(\mathbb{R})$ is assumed to be antisymmetric, $A^t=-A$, with this latter assumption needed for having $e^A\in O_N$. Let us first compute the derivative of f. Following [25], we have the following result:

Proposition 3.10. *We have the following formula,*

$$f'(t)=2\sum_{ij}\psi'((Ue^{tA})_{ij}^2)(UAe^{tA})_{ij}(Ue^{tA})_{ij}$$

valid for any $U\in O_N$, and any $A\in M_N(\mathbb{R})$ antisymmetric.

Proof. The matrices U, e^{tA} being both orthogonal, we have:

$$\begin{aligned}(Ue^{tA})_{ij}^2 &= (Ue^{tA})_{ij}((Ue^{tA})^t)_{ji}\\ &= (Ue^{tA})_{ij}(e^{tA^t}U^t)_{ji}\\ &= (Ue^{tA})_{ij}(e^{-tA}U^t)_{ji}\end{aligned}$$

We can now differentiate our function f, and by using once again the orthogonality of the matrices U, e^{tA}, along with the formula $A^t = -A$, we obtain:

$$\begin{aligned}f'(t) &= \sum_{ij}\psi'((Ue^{tA})_{ij}^2)\left[(UAe^{tA})_{ij}(e^{-tA}U^t)_{ji} - (Ue^{tA})_{ij}(e^{-tA}AU^t)_{ji}\right]\\ &= \sum_{ij}\psi'((Ue^{tA})_{ij}^2)\left[(UAe^{tA})_{ij}((e^{-tA}U^t)^t)_{ij} - (Ue^{tA})_{ij}((e^{-tA}AU^t)^t)_{ij}\right]\\ &= \sum_{ij}\psi'((Ue^{tA})_{ij}^2)\left[(UAe^{tA})_{ij}(Ue^{tA})_{ij} + (Ue^{tA})_{ij}(UAe^{tA})_{ij}\right]\end{aligned}$$

But this gives the formula in the statement, and we are done. □

Before computing the second derivative, let us evaluate $f'(0)$. In terms of the color decomposition $U = \sum_{r>0} rU_r$ of our matrix, the result is:

Proposition 3.11. *We have the following formula,*

$$f'(0) = 2\sum_{r>0} r\psi'(r^2)Tr(U_r^tUA)$$

where the matrices $U_r \in M_N(-1,0,1)$ are the color components of U.

Proof. We use the formula in Proposition 3.10 above. At $t = 0$, we obtain:

$$f'(0) = 2\sum_{ij}\psi'(U_{ij}^2)(UA)_{ij}U_{ij}$$

Consider now the color decomposition of U. We have the following formulae:

$$\begin{aligned}U_{ij} = \sum_{r>0} r(U_r)_{ij} \quad &\implies \quad U_{ij}^2 = \sum_{r>0} r^2|(U_r)_{ij}|\\ &\implies \quad \psi'(U_{ij}^2) = \sum_{r>0}\psi'(r^2)|(U_r)_{ij}|\end{aligned}$$

Now by getting back to the above formula of $f'(0)$, we obtain:

$$f'(0) = 2\sum_{r>0}\psi'(r^2)\sum_{ij}(UA)_{ij}U_{ij}|(U_r)_{ij}|$$

Our claim now is that we have:

$$U_{ij}|(U_r)_{ij}| = r(U_r)_{ij}$$

Indeed, in the case $|U_{ij}|\neq r$ this formula reads $U_{ij}\cdot 0=r\cdot 0$, which is true, and in the case $|U_{ij}|=r$ this formula reads $rS_{ij}\cdot 1=r\cdot S_{ij}$, which is once again true. Thus:

$$f'(0)=2\sum_{r>0}r\psi'(r^2)\sum_{ij}(UA)_{ij}(U_r)_{ij}$$

But this gives the formula in the statement, and we are done. $\square$

Let us compute now the second derivative. The result here is as follows:

Proposition 3.12. *We have the following formula,*

$$\begin{aligned}
f''(0) &= 4\sum_{ij}\psi''(U_{ij}^2)\left[(UA)_{ij}U_{ij}\right]^2\\
&\quad +2\sum_{ij}\psi'(U_{ij}^2)\left[(UA^2)_{ij}U_{ij}\right]\\
&\quad +2\sum_{ij}\psi'(U_{ij}^2)(UA)_{ij}^2
\end{aligned}$$

valid for any $U\in O_N$, and any $A\in M_N(\mathbb{R})$ antisymmetric.

Proof. We use the formula in Proposition 3.10 above, namely:

$$f'(t)=2\sum_{ij}\psi'((Ue^{tA})_{ij}^2)(UAe^{tA})_{ij}(Ue^{tA})_{ij}$$

Since the term on the right, or rather its double, appears as the derivative of the quantity $(Ue^{tA})_{ij}^2$, when differentiating a second time, we obtain:

$$\begin{aligned}
f''(t) &= 4\sum_{ij}\psi''((Ue^{tA})_{ij}^2)\left[(UAe^{tA})_{ij}(Ue^{tA})_{ij}\right]^2\\
&\quad +2\sum_{ij}\psi'((Ue^{tA})_{ij}^2)\left[(UAe^{tA})_{ij}(Ue^{tA})_{ij}\right]'
\end{aligned}$$

In order to compute now the missing derivative, observe that we have:

$$\left[(UAe^{tA})_{ij}(Ue^{tA})_{ij}\right]'=(UA^2e^{tA})_{ij}(Ue^{tA})_{ij}+(UAe^{tA})_{ij}^2$$

Summing up, we have obtained the following formula:

$$\begin{aligned}
f''(t) &= 4\sum_{ij}\psi''((Ue^{tA})_{ij}^2)\left[(UAe^{tA})_{ij}(Ue^{tA})_{ij}\right]^2\\
&\quad +2\sum_{ij}\psi'((Ue^{tA})_{ij}^2)\left[(UA^2e^{tA})_{ij}(Ue^{tA})_{ij}\right]\\
&\quad +2\sum_{ij}\psi'((Ue^{tA})_{ij}^2)(UAe^{tA})_{ij}^2
\end{aligned}$$

But at $t=0$ this gives the formula in the statement, and we are done. $\square$

For the function $\psi(x)=\sqrt{x}$, corresponding to the functional $F(U)=||U||_1$, there are some simplifications, that we will work out now in detail. First, we have:

Proposition 3.13. *For the function $F(U)=||U||_1$ we have the formula*

$$f''(0)=Tr(S^tUA^2)$$

valid for any antisymmetric matrix A, where $S_{ij}=\mathrm{sgn}(U_{ij})$.

Proof. We use the formula in Proposition 3.12 above, with $\psi(x)=\sqrt{x}$. We ibtain:

$$\begin{aligned}
f''(0) &= -\sum_{ij}\frac{[(UA)_{ij}U_{ij}]^2}{|U_{ij}|^3}+\sum_{ij}\frac{(UA^2)_{ij}U_{ij}}{|U_{ij}|}+\sum_{ij}\frac{(UA)_{ij}^2}{|U_{ij}|}\\
&= -\sum_{ij}\frac{(UA)_{ij}^2}{|U_{ij}|}+\sum_{ij}(UA^2)_{ij}S_{ij}+\sum_{ij}\frac{(UA)_{ij}^2}{|U_{ij}|}\\
&= \sum_{ij}(UA^2)_{ij}S_{ij}
\end{aligned}$$

But this gives the formula in the statement, and we are done. □

We are therefore led to the following result, from [25], regarding the 1-norm:

Theorem 3.14. *A matrix $U\in O_N$ locally maximizes the 1-norm on O_N precisely when the following conditions are satisfied:*

1. *The matrix U has nonzero entries, $U\in O_N^*$.*
2. *The matrix $X=S^tU$ is symmetric, where $S_{ij}=\mathrm{sgn}(U_{ij})$.*
3. *We have $Tr(XA^2)\leq 0$, for any antisymmetric matrix $A\in M_N(\mathbb{R})$.*

Proof. This follows the results that we have, with (1,2,3) coming respectively from Theorem 3.3, Theorem 3.4 and Proposition 3.13. □

In order to further improve the above result, we will need:

Proposition 3.15. *For a symmetric matrix $X\in M_N(\mathbb{R})$, the following are equivalent:*

1. *$Tr(XA^2)\leq 0$, for any antisymmetric matrix A.*
2. *The sum of the two smallest eigenvalues of X is positive.*

Proof. In terms of the vector $a=\sum_{ij}A_{ij}e_i\otimes e_j$, we have the following formula:

$$\begin{aligned}
Tr(XA^2) &= <X,A^2>\\
&= -<AX,A>\\
&= -<a,(1\otimes X)a>
\end{aligned}$$

Thus the condition (1) is equivalent to $P(1\otimes X)P$ being positive, with P being the orthogonal projection on the antisymmetric subspace in $\mathbb{R}^N\otimes\mathbb{R}^N$.

For any two eigenvectors $x_i \perp x_j$ of X, with eigenvalues λ_i, λ_j, we have:

$$\begin{aligned} P(1 \otimes X)P(x_i \otimes x_j - x_j \otimes x_i) &= P(\lambda_j x_i \otimes x_j - \lambda_i x_j \otimes x_i) \\ &= \frac{\lambda_i + \lambda_j}{2}(x_i \otimes x_j - x_j \otimes x_i) \end{aligned}$$

Thus, we obtain the conclusion in the statement. □

Following [25], we can now formulate a final result on the subject, which improves some previous findings from [19], and from [28], as follows:

Theorem 3.16. *A matrix $U \in O_N$ locally maximizes the 1-norm on O_N precisely when it has nonzero entries, and when the following matrix, with $S_{ij} = \mathrm{sgn}(U_{ij})$,*

$$X = S^t U$$

is symmetric, and the sum of its two smallest eigenvalues is positive.

Proof. This follows indeed from our main result so far, Theorem 3.14 above, by taking into account the positivity criterion from Proposition 3.15. □

In terms of the almost Hadamard matrices, as introduced in Definition 3.2 above, as rescaled versions of the above matrices, the above result reformulates as follows:

Theorem 3.17. *The almost Hadamard matrices are the matrices $H \in \sqrt{N} O_N$ having nonzero entries, and which are such that the following matrix, with $S_{ij} = \mathrm{sgn}(H_{ij})$,*

$$X = S^t H$$

is symmetric, and the sum of its two smallest eigenvalues is positive.

Proof. This is a reformulation of Theorem 3.16, by rescaling everything by $\sqrt{N}$, as to reach to the objects axiomatized in Definition 3.2 above. □

We can now state and prove the following theoretical result, from [19], [28]:

Theorem 3.18. *The class of almost Hadamard matrices has the following properties:*

(1) *It contains all the Hadamard matrices.*
(2) *It is stable under transposition.*
(3) *It is stable under taking tensor products.*
(4) *It is stable under Hadamard equivalence.*
(5) *It contains the matrix $K_N = \frac{1}{\sqrt{N}}(2\mathbb{I}_N - N 1_N)$.*

Proof. All the assertions are clear from what we have, as follows:

(1) This follows either from Theorem 3.1, which shows that Hadamard implies almost Hadamard, without any need for further computations, or from the fact that if H is Hadamard then $U = H/\sqrt{N}$ is orthogonal, and $SU^t = HU^t = \sqrt{N} 1_N$ is positive.

(2) This follows either from definitions, because the transposition operation preserves the local maximizers of the 1-norm, or from Theorem 3.17 above.

(3) For a tensor product of almost Hadamard matrices $H = H' \otimes H''$ we have $U = U' \otimes U''$ and $S = S' \otimes S''$, so that U is unitary and SU^t is symmetric, with the sum of the two smallest eigenvalues being positive, as claimed.

(4) This follows either from definitions, because the Hadamard equivalence preserves the local maximizers of the 1-norm, or from Theorem 3.17 above.

(5) We know from Theorem 3.7 that the matrix $U = K_N/\sqrt{N}$ is orthogonal. Also, we have $S = \mathbb{I}_N - 21_N$, and so SU^t is positive, because with $J_N = \mathbb{I}_N/N$ we have:

$$\begin{aligned} SU^t &= (NJ_N - 21_N)(2J_N - 1_N) \\ &= (N-2)J_N + 2(1_N - J_N) \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

In the above statement the main result is (5), and we will discuss now various generalizations of it, first concerning the circulant matrices, and then the 2-entry matrices. Let us first discuss the circulant case. Let $F \in U_N$ be the normalized Fourier matrix, given by $F_{ij} = w^{ij}/\sqrt{N}$, where $w = e^{2\pi i/N}$. Given a vector $\alpha \in \mathbb{C}^n$, we associate to it the diagonal matrix $\alpha' = diag(\alpha_0, \ldots, \alpha_{N-1})$. We will need the following well-known result:

Proposition 3.19. *For a matrix $H \in M_N(\mathbb{C})$, the following are equivalent:*
(1) *H is circulant, i.e. $H_{ij} = \gamma_{j-i}$, for a certain vector $\gamma \in \mathbb{C}^N$.*
(2) *H is Fourier-diagonal, i.e. $H = FDF^*$, with $D \in M_N(\mathbb{C})$ diagonal.*

In addition, if so is the case, then with $D = \sqrt{N}\alpha'$ we have $\gamma = F\alpha$.

Proof. (1) $\Longrightarrow$ (2) The matrix $D = F^*HF$ is indeed diagonal, given by:

$$D_{ij} = \frac{1}{N}\sum_{kl} w^{jl-ik}\gamma_{l-k} = \delta_{ij}\sum_r w^{jr}\gamma_r$$

(2) $\Longrightarrow$ (1) The matrix $H = FDF^*$ is indeed circulant, given by:

$$H_{ij} = \sum_k F_{ik}D_{kk}\bar{F}_{jk} = \frac{1}{N}\sum_k w^{(i-j)k}D_{kk}$$

Finally, the last assertion is clear from the above formula of H_{ij}. □

Let us investigate now the circulant orthogonal matrices. We have:

Proposition 3.20. *For a matrix $U \in M_N(\mathbb{C})$, the following are equivalent:*
(1) *U is orthogonal and circulant.*
(2) *$U = F\alpha' F^*$ with $\alpha \in \mathbb{T}^N$ satisfying $\bar{\alpha}_i = \alpha_{-i}$ for any i.*

Proof. We will use many times the fact that given $\alpha \in \mathbb{C}^N$, the vector $\gamma = F\alpha$ is real if and only if $\bar{\alpha}_i = \alpha_{-i}$ for any i. This follows indeed from $\overline{F\alpha} = F\tilde{\alpha}$, with $\tilde{\alpha}_i = \bar{\alpha}_{-i}$.

(1) $\Longrightarrow$ (2) Write $H_{ij} = \gamma_{j-i}$ with $\gamma \in \mathbb{R}^N$. By using Proposition 3.19 we obtain $H = FDF^*$ with $D = \sqrt{N}\alpha'$ and $\gamma = F\alpha$. Now since $U = F\alpha' F^*$ is unitary, so is α', so we must have $\alpha \in \mathbb{T}^N$. Finally, since γ is real we have $\bar{\alpha}_i = \alpha_{-i}$, and we are done.

(2) $\Longrightarrow$ (1) We know from Proposition 3.19 that U is circulant. Also, from $\alpha \in \mathbb{T}^N$ we obtain that α' is unitary, and so must be U. Finally, since we have $\bar{\alpha}_i = \alpha_{-i}$, the vector $\gamma = F\alpha$ is real, and hence we have $U \in M_N(\mathbb{R})$, which finishes the proof. □

Let us discuss now the almost Hadamard case. First, in the usual Hadamard case, the known examples and the corresponding α-vectors are as follows:

Proposition 3.21. *The known circulant Hadamard matrices, namely*

$$\pm\begin{pmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix} \quad , \quad \pm\begin{pmatrix}1&-1&1&1\\1&1&-1&1\\1&1&1&-1\\-1&1&1&1\end{pmatrix}$$

$$\pm\begin{pmatrix}1&1&-1&1\\1&1&1&-1\\-1&1&1&1\\1&-1&1&1\end{pmatrix} \quad , \quad \pm\begin{pmatrix}1&1&1&-1\\-1&1&1&1\\1&-1&1&1\\1&1&-1&1\end{pmatrix}$$

come respectively from the following α vectors, via the above construction:

$$\pm(1,-1,-1,-1) \quad , \quad \pm(1,-i,1,i)$$

$$\pm(1,1,-1,1) \quad , \quad \pm(1,i,1,-i)$$

Proof. At $N = 4$ the conjugate of the Fourier matrix is given by:

$$F^* = \frac{1}{2}\begin{pmatrix}1&1&1&1\\1&-i&-1&i\\1&-1&1&-1\\1&i&-1&-i\end{pmatrix}$$

Thus the vectors $\alpha = F^*\gamma$ are indeed those in the statement. □

Following [28], we have the following generalization of the above matrices:

Proposition 3.22. *If $q^N = 1$ then the vector*

$$\alpha = \pm(1, -q, -q^2, \ldots, -q^{N-1})$$

produces an almost Hadamard matrix, equivalent to $K_N = \frac{1}{\sqrt{N}}(2\mathbb{I}_N - N1_N)$.

Proof. Observe first that these matrices generalize those in Proposition 3.21. Indeed, at $N=4$ the choices for q are $1,i,-1,-i$, and this gives the above α-vectors.

Assume that the $\pm$ sign in the statement is $+$. With $q=w^r$, we have:

$$\sqrt{N}\gamma_i=\sum_{k=0}^{N-1}w^{ik}\alpha_k=2-\sum_{k=0}^{N-1}w^{(i+r)k}=2-\delta_{i,-r}N$$

In terms of the standard long cycle $(C_N)_{ij}=\delta_{i+1,j}$, we obtain:

$$H=\frac{1}{\sqrt{N}}(2\mathbb{I}_N-NC_N^{-r})$$

Thus H is equivalent to K_N, and by Theorem 3.18, it is almost Hadamard. $\square$

In general, the construction of circulant almost Hadamard matrices is quite a tricky problem. At the abstract level, we have the following result, from [28]:

Proposition 3.23. *A circulant matrix $H\in M_N(\mathbb{R}^*)$, written $H_{ij}=\gamma_{j-i}$, is almost Hadamard provided that the following conditions are satisfied:*

(1) *The vector $\alpha=F^*\gamma$ satisfies $\alpha\in\mathbb{T}^N$.*
(2) *With $\varepsilon=\mathrm{sgn}(\gamma)$, $\rho_i=\sum_r\varepsilon_r\gamma_{i+r}$ and $\nu=F^*\rho$, we have $\nu>0$.*

In addition, if so is the case, then $\bar{\alpha}_i=\alpha_{-i}$, $\rho_i=\rho_{-i}$ and $\nu_i=\nu_{-i}$ for any i.

Proof. We know from Theorem 3.17 our matrix H is almost Hadamard if the matrix $U=H/\sqrt{N}$ is orthogonal and $SU^t>0$, where $S_{ij}=\mathrm{sgn}(U_{ij})$. By Proposition 3.19 the orthogonality of U is equivalent to the condition (1). Regarding now the condition $SU^t>0$, this is equivalent to $S^tU>0$. But, with $k=i-r$, we have:

$$(S^tH)_{ij}=\sum_kS_{ki}H_{kj}=\sum_k\varepsilon_{i-k}\gamma_{j-k}=\sum_r\varepsilon_r\gamma_{j-i+r}=\rho_{j-i}$$

Thus S^tU is circulant, with $\rho/\sqrt{N}$ as first row. From Proposition 3.19 we get $S^tU=FLF^*$ with $L=\nu'$ and $\nu=F^*\rho$, so $S^tU>0$ iff $\nu>0$, which is the condition (2).

Finally, the assertions about α,ν follow from the fact that $F\alpha,F\nu$ are real. As for the assertion about ρ, this follows from the fact that S^tU is symmetric. $\square$

Here are now the main examples of such matrices, once again following [28]:

Theorem 3.24. *For N odd the following matrix is almost Hadamard,*

$$L_N=\frac{1}{\sqrt{N}}\begin{pmatrix}1&-\cos^{-1}\frac{\pi}{N}&\cos^{-1}\frac{2\pi}{N}&\ldots\ldots&\cos^{-1}\frac{(N-1)\pi}{N}\\ \cos^{-1}\frac{(N-1)\pi}{N}&1&-\cos^{-1}\frac{\pi}{N}&\ldots\ldots&-\cos^{-1}\frac{(N-2)\pi}{N}\\ \vdots&\vdots&\vdots&&\vdots\\ \vdots&\vdots&\vdots&&\vdots\\ -\cos^{-1}\frac{\pi}{N}&\cos^{-1}\frac{2\pi}{N}&-\cos^{-1}\frac{3\pi}{N}&\ldots\ldots&1\end{pmatrix}$$

and comes from an α-vector having all entries equal to 1 or -1.

Proof. Write $N=2n+1$, and consider the following vector:

$$\alpha_i=\begin{cases}(-1)^{n+i}&\text{for } i=0,1,\ldots,n\\(-1)^{n+i+1}&\text{for } i=n+1,\ldots,2n\end{cases}$$

Let us first prove that $(L_N)_{ij}=\gamma_{j-i}$, where $\gamma=F\alpha$. With $w=e^{2\pi i/N}$ we have:

$$\sqrt{N}\gamma_i=\sum_{j=0}^n(-1)^{n+j}w^{ij}+\sum_{j=1}^n(-1)^{n+(N-j)+1}w^{i(N-j)}$$

Now since N is odd, and since $w^N=1$, we obtain:

$$\sqrt{N}\gamma_i=\sum_{j=-n}^n(-1)^{n+j}w^{ij}$$

By computing the sum on the right, with $\xi=e^{\pi i/N}$ we get, as claimed:

$$\sqrt{N}\gamma_i=\frac{2w^{-ni}}{1+w^i}=\frac{2\xi^{-2ni}}{1+\xi^{2i}}=\frac{2\xi^{-Ni}}{\xi^{-i}+\xi^i}=(-1)^i\cos^{-1}\frac{i\pi}{N}$$

In order to prove now that L_N is almost Hadamard, we use Proposition 3.23. Since the sign vector is simply $\varepsilon=(-1)^n\alpha$, the vector $\rho_i=\sum_r\varepsilon_r\gamma_{i+r}$ is given by:

$$\sqrt{N}\rho_i=\sum_{j=-n}^n(-1)^jw^{ij}\sum_{r=0}^{2n}\alpha_rw^{rj}$$

Now since the last sum on the right is $(\sqrt{N}F\alpha)_j=\sqrt{N}\gamma_j$, we obtain:

$$\rho_i=\frac{1}{\sqrt{N}}\sum_{j=-n}^n(-1)^jw^{ij}\sum_{k=-n}^n(-1)^{n+k}w^{jk}$$

Thus we have the following formula:

$$\rho_i=\frac{(-1)^n}{\sqrt{N}}\sum_{j=-n}^n\sum_{k=-n}^n(-1)^{j+k}w^{(i+k)j}$$

Let us compute now the vector $\nu=F^*\rho$. We have:

$$\nu_l=\frac{(-1)^n}{N}\sum_{j=-n}^n\sum_{k=-n}^n(-1)^{j+k}w^{jk}\sum_{i=0}^{2n}w^{i(j-l)}$$

The sum on the right is $N\delta_{jl}$, with both j,l taken modulo N, so it is equal to $N\delta_{jL}$, where $L=l$ for $l\leq n$, and $L=l-N$ for $l>n$. We obtain:

$$\nu_l=(-1)^{n+L}\sum_{k=-n}^n(-w^L)^k$$

With $\xi = e^{\pi i/N}$ as before, this gives the following formula:

$$\nu_l = (-1)^L \frac{2w^{-nL}}{1+w^L}$$

In terms of the variable $\xi = e^{\pi i/N}$, we obtain the following formula:

$$\nu_l = (-1)^L \frac{2\xi^{-2nL}}{1+\xi^{2L}} = (-1)^L \frac{2\xi^{-NL}}{\xi^{-L}+\xi^L} = \cos^{-1}\frac{L\pi}{N}$$

Now since $L \in [-n, n]$, all the entries of ν are positive, and we are done. □

Let us study now the almost Hadamard matrices having only two entries, $H \in M_N(x, y)$, with $x, y \in \mathbb{R}$. Following [25], [28], we have the following definition:

Definition 3.25. *An (a, b, c) pattern is a matrix $M \in M_N(x, y)$, with $N = a + 2b + c$, such that, in any two rows, the number of $x/y/x/y$ sitting below $x/x/y/y$ is $a/b/b/c$.*

In other words, given any two rows of our matrix, we are asking for the existence of a permutation of the columns such that these two rows become:

$$\begin{matrix} x\ldots x & x\ldots x & y\ldots y & y\ldots y \\ \underbrace{x\ldots x}_a & \underbrace{y\ldots y}_b & \underbrace{x\ldots x}_b & \underbrace{y\ldots y}_c \end{matrix}$$

The Hadamard matrices do not come in general from such patterns. However, there are many interesting examples of patterns coming from block designs [49], [123]:

Definition 3.26. *A (v, k, λ) symmetric balanced incomplete block design is a collection B of subsets of a set X, called blocks, with the following properties:*

1. *$|X| = |B| = v$.*
2. *Each block contains exactly k points from X.*
3. *Each pair of distinct points is contained in exactly λ blocks of B.*

The incidence matrix of a such block design is the $v \times v$ matrix defined by:

$$M_{bx} = \begin{cases} 1 & \text{if } x \in b \\ 0 & \text{if } x \notin b \end{cases}$$

The connection between designs and patterns comes from:

Proposition 3.27. *If $N = a + 2b + c$ then the adjacency matrix of any $(N, a + b, a)$ symmetric balanced incomplete block design is an (a, b, c) pattern.*

Proof. Indeed, let us replace the $0-1$ values in the adjacency matrix M by abstract $x - y$ values. Then each row of M contains $a+b$ copies of x and $b+c$ copies of y, and since every pair of distinct blocks intersect in exactly a points, cf. [123], we see that every pair of rows has exactly a variables x in matching positions, so that M is an (a, b, c) pattern. □

As a basic application of the above, we have:

Proposition 3.28. *Assume that $q=p^k$ is a prime power. Then the point-line incidence matrix of the projective plane over $\mathbb{F}_q$ is a $(1,q,q^2-q)$ pattern.*

Proof. The sets X,B of points and lines of the projective plane over $\mathbb{F}_q$ are known to form a $(q^2+q+1,q+1,1)$ block design, and this gives the result. □

We consider now the problem of associating real values to the symbols x,y in an (a,b,c) pattern such that the resulting matrix $U(x,y)$ is orthogonal. We have:

Proposition 3.29. *Given $a,b,c\in\mathbb{N}$, there exists an orthogonal matrix having pattern (a,b,c) iff $b^2\geq ac$. In this case the solutions are $U(x,y)$ and $-U(x,y)$, where*

$$x=-\frac{t}{\sqrt{b}(t+1)}\quad,\quad y=\frac{1}{\sqrt{b}(t+1)}$$

with $t=(b\pm\sqrt{b^2-ac})/a$ being one of the solutions of $at^2-2bt+c=0$.

Proof. In order for U to be orthogonal, the following conditions must be satisfied:

$$ax^2+2bxy+cy^2=0$$

$$(a+b)x^2+(b+c)y^2=1$$

But this gives the formulae in the statement. □

Following [25], [28], we have the following result:

Proposition 3.30. *Let $U=U(x,y)$ be orthogonal, corresponding to an (a,b,c) pattern. Then $H=\sqrt{N}U$ is almost Hadamard if:*

$$(N(a-b)+2b)|x|+(N(c-b)+2b)|y|\geq 0$$

Proof. Let $S_{ij}=\mathrm{sgn}(U_{ij})$. Since any row of U consists of $a+b$ copies of x and $b+c$ copies of y, we have:

$$(SU^t)_{ii}=\sum_k\mathrm{sgn}(U_{ik})U_{ik}=(a+b)|x|+(b+c)|y|$$

Regarding now $(SU^t)_{ij}$ with $i\neq j$, we can assume in the computation that the i-th and j-th row of U are exactly those pictured after Definition 3.25 above. Thus:

$$\begin{aligned}(SU^t)_{ij}&=\sum_k\mathrm{sgn}(U_{ik})U_{jk}\\&=a\,\mathrm{sgn}(x)x+b\,\mathrm{sgn}(x)y+b\,\mathrm{sgn}(y)x+c\,\mathrm{sgn}(y)y\\&=a|x|-b|y|-b|x|+c|y|\\&=(a-b)|x|+(c-b)|y|\end{aligned}$$

We obtain the following formula for the matrix SU^t itself, with $J_N=\mathbb{I}_N/N$:

$$\begin{aligned}SU^t&=2b(|x|+|y|)1_N+((a-b)|x|+(c-b)|y|)NJ_N\\&=2b(|x|+|y|)(1_N-J_N)+((N(a-b)+2b)|x|+(N(c-b)+2b)|y|))J_N\end{aligned}$$

Now since the matrices $1_N-J_N,J_N$ are orthogonal projections, we have $SU^t>0$ if and only if the coefficients of these matrices in the above expression are both positive. Since the coefficient of 1_N-J_N is clearly positive, the condition left is:

$$(N(a-b)+2b)|x|+(N(c-b)+2b)|y|\geq 0$$

So, we have obtained the condition in the statement, and we are done. $\square$

Once again following [25], [28], we have the following result:

Proposition 3.31. *Assume that $a,b,c\in\mathbb{N}$ satisfy $c\geq a$ and $b(b-1)=ac$, and consider the (a,b,c) pattern $U=U(x,y)$, where:*

$$x=\frac{a+(1-a-b)\sqrt{b}}{Na}\quad,\quad y=\frac{b+(a+b)\sqrt{b}}{Nb}$$

Then $H=\sqrt{N}U$ is an almost Hadamard matrix.

Proof. We have $b^2-ac=b$, so Proposition 3.30 applies, and shows that with $t=(b-\sqrt{b})/a$ we have an orthogonal matrix $U=U(x,y)$. But this gives the result. $\square$

We have the following result, from [25], [28]:

Theorem 3.32. *Assume that $q=p^k$ is a prime power. Then the matrix $I_N\in M_N(x,y)$, where $N=q^2+q+1$ and*

$$x=\frac{1-q\sqrt{q}}{\sqrt{N}}\quad,\quad y=\frac{q+(q+1)\sqrt{q}}{q\sqrt{N}}$$

having $(1,q,q^2-q)$ pattern coming from the point-line incidence of the projective plane over $\mathbb{F}_q$ is an almost Hadamard matrix.

Proof. Indeed, the conditions $c\geq a$ and $b(b-1)=ac$ which are needed are satisfied, and the variables constructed there are $x'=x/\sqrt{N}$ and $y'=y/\sqrt{N}$. $\square$

We refer to [25], [28] for more on such matrices, and we will be back to this.

4. Partial matrices

In this section we discuss a number of more specialized questions in the real case, regarding the square or rectangular submatrices of the Hadamard matrices $H \in M_N(\pm 1)$, and some related classes of square or rectangular real matrices.

We have already met an interesting class of such matrices in section 1 above, namely the partial Hadamard matrices (PHM), which naturally appear when classifying the Hadamard matrices $H \in M_N(\pm 1)$ at small values of N. So, let us start by reviewing the material there. The definition of these matrices is as follows:

Definition 4.1. *A partial Hadamard matrix (PHM) is a rectangular matrix*

$$H \in M_{M\times N}(\pm 1)$$

whose rows are pairwise orthogonal, with respect to the scalar product of $\mathbb{R}^N$.

The motivating examples are the usual Hadamard matrices $H \in M_N(\pm 1)$, and their various $M \times N$ submatrices, with $M \leq N$. See [52], [59], [72], [76], [137]. However, there are as well many examples which are not of this form, and the PHM are interesting combinatorial objects, on their own. We will discuss this in what follows.

Following the study from the square case, we first have:

Proposition 4.2. *The set $Y_{M,N}$ formed by the $M \times N$ partial Hadamard matrices is*

$$Y_{M,N} = M_{M\times N}(\pm 1) \cap \sqrt{N} O_{M,N}$$

where $O_{M,N}$ is the following space of rectangular matrices:

$$O_{M,N} = \left\{ U \in M_{M\times N}(\mathbb{R}) \Big| UU^t = 1_M \right\}$$

Proof. This follows exactly as in the square case, the idea being that for a rectangular matrix $U \in M_{M\times N}(\mathbb{R})$ having rows $U_1, \ldots, U_M \in \mathbb{R}^N$ of norm 1, the condition $UU^t = 1_M$ expresses the fact that these row vectors are pairwise orthogonal. □

The space $O_{M,N}$ appearing above has several interpretations, as follows:

Theorem 4.3. *The space $O_{M,N}$ has the following properties:*

1. *It is the space of surjective partial isometries $f : \mathbb{R}^N \to \mathbb{R}^M$.*
2. *It is the space of vectors $U_1, \ldots, U_M \in S^{N-1}$ which are pairwise orthogonal.*
3. *It is also an homogeneous space, given by $O_{M,N} \simeq O_N / O_{N-M}$.*
4. *It is also the space determined by the first M rows of coordinates on O_N.*

Proof. All this is standard algebra and geometry, the idea being as follows:

(1) This follows from the condition $UU^t = 1$ defining $O_{M,N}$.

(2) This follows again from the condition $UU^t = 1$ defining $O_{M,N}$.

(3) We have indeed an action $O_N \curvearrowright O_{M,N}$, and the stabilizer is O_{N-M}.

(4) This follows from some basic functional analysis, or algebraic geometry. □

As already mentioned, there are matrices in $Y_{M,N}$ which do not complete into matrices of Y_N, and we will give some explicit counterexamples in a moment. This is in contrast with the fact that any matrix from $O_{M,N}$ can be completed, for instance via the Gram-Schmidt procedure, into a matrix of O_N. We will be back later to this phenomenon.

Let us discuss as well, as a continuation of the study from the real case, some basic analytic aspects. In what regards the 1-norm bound, we have the following result:

Theorem 4.4. *Given a matrix $U\in O_{M,N}$ we have*

$$||U||_1\leq M\sqrt{N}$$

with equality precisely when $H=\sqrt{N}U$ is partial Hadamard.

Proof. We have indeed the following estimate, valid for any $U\in O_{M,N}$:

$$\begin{aligned}||U||_1&=\sum_{ij}|U_{ij}|\\&\leq\sqrt{MN}\left(\sum_{ij}|U_{ij}|^2\right)^{1/2}\\&=M\sqrt{N}\end{aligned}$$

In this estimate the equality case holds when we have, for any i,j:

$$|U_{ij}|=\frac{1}{\sqrt{N}}$$

But this amounts in saying that the rescaled matrix $H=\sqrt{N}U$ must satisfy $H\in M_{M\times N}(\pm1)$, and so must be a partial Hadamard matrix, as claimed. □

Similar estimates hold for the p-norms, with $p\neq 2$. Thus, we have a subsequent notion of "almost PHM matrix". This subject is largely unexplored.

Following the study from the square case, let us formulate now:

Definition 4.5. *Two PHM are called equivalent when we can pass from one to the other by permuting the rows or columns, or multiplying the rows or columns by -1. Also:*

1. *We say that a PHM is in dephased form when its first row and its first column consist of 1 entries.*
2. *We say that a PHM is in standard form when it is dephased, with the 1 entries moved to the left as much as possible, by proceeding from top to bottom.*

Unlike in the square case, where the standard form is generally not used, putting a rectangular matrix in standard form is something quite useful.

As an illustration here, here is a result that we already know, regarding the partial Hadamard matrices put in standard form, at small values of M:

Proposition 4.6. *The standard form of dephased PHM at $M = 2, 3, 4$ is*

$$H = \begin{pmatrix} + & + \\ \underbrace{+}_{N/2} & \underbrace{-}_{N/2} \end{pmatrix}$$

$$H = \begin{pmatrix} + & + & + & + \\ + & + & - & - \\ \underbrace{+}_{N/4} & \underbrace{-}_{N/4} & \underbrace{+}_{N/4} & \underbrace{-}_{N/4} \end{pmatrix}$$

$$H = \begin{pmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & + & + & - & - \\ \underbrace{+}_{a} & \underbrace{-}_{b} & \underbrace{+}_{b} & \underbrace{-}_{a} & \underbrace{+}_{b} & \underbrace{-}_{a} & \underbrace{+}_{a} & \underbrace{-}_{b} \end{pmatrix}$$

where the numbers $a, b \in \mathbb{N}$ satisfy $a + b = N/4$.

Proof. This is something that we already know, from section 1 above, the idea being that the $M = 2$ result is obvious, the $M = 3$ result follows from the orthogonality conditions between the rows, and the $M = 4$ result follows from the $M = 3$ result, by writing down and then solving the supplementary equations coming from the 4th row. □

The above result and its proof might suggest that the standard form of the PHM can be worked out by recurrence. However, this is not exactly true, the combinatorics becoming quite complicated starting from $M = 5$. We will be back to this, later on.

We can fine-tune the $M = 4$ result, by using the equivalence relation, as follows:

Theorem 4.7. *The $4 \times N$ partial Hadamard matrices are of the form*

$$H = (\underbrace{W_4 \ \ldots \ W_4}_{a} \ \underbrace{K_4 \ \ldots \ K_4}_{b})$$

with $a + b = N/4$. Moreover, we can assume $a \geq b$.

Proof. Let $H \in M_{4\times N}(\pm 1)$ be as in Proposition 4.6. The matrix formed by the a type columns, one from each block, is equivalent to W_4, via a permutation of the columns:

$$\begin{pmatrix}+&+&+&+\\+&+&-&-\\+&-&+&-\\+&-&-&+\end{pmatrix}\sim W_4$$

Also, the matrix formed by the b type columns, one from each block, is equivalent to K_4, via a first column sign switch, plus a certain permutation of the columns:

$$\begin{pmatrix}+&+&+&+\\+&+&-&-\\+&-&+&-\\-&+&+&-\end{pmatrix}\sim K_4$$

Thus, just by performing operations on the columns, we are led to the conclusion in the statement, namely:

$$H\sim(\underbrace{W_4\ \ldots\ W_4}_a\ \underbrace{K_4\ \ldots\ K_4}_b)$$

In order to prove now the last assertion, we must prove that we have:

$$(\underbrace{W_4\ \ldots\ W_4}_a\ \underbrace{K_4\ \ldots\ K_4}_b)\sim(\underbrace{K_4\ \ldots\ K_4}_a\ \underbrace{W_4\ \ldots\ W_4}_b)$$

But this can be seen by performing a sign switch on the last row, and then permuting the columns. Equivalently, we can start with the original matrix, in standard form, and perform a sign switch on the last row. The matrix becomes:

$$H\sim\begin{pmatrix}+&+&+&+&+&+&+&+\\+&+&+&+&-&-&-&-\\+&+&-&-&+&+&-&-\\\underbrace{-}_a&\underbrace{+}_b&\underbrace{-}_b&\underbrace{+}_a&\underbrace{-}_b&\underbrace{+}_a&\underbrace{-}_a&\underbrace{+}_b\end{pmatrix}$$

Now by putting this matrix in standard form, we obtain:

$$H=\begin{pmatrix}+&+&+&+&+&+&+&+\\+&+&+&+&-&-&-&-\\+&+&-&-&+&+&-&-\\\underbrace{+}_b&\underbrace{-}_a&\underbrace{+}_a&\underbrace{-}_b&\underbrace{+}_a&\underbrace{-}_b&\underbrace{+}_b&\underbrace{-}_a\end{pmatrix}$$

Thus a,b got interchanged, and this gives the result. □

At $M=5$ now, as already mentioned above, the combinatorics becomes quite complicated, and we will see in a moment that there are $5\times N$ partial Hadamard matrices which do not complete into Hadamard matrices. We first have the following result:

Proposition 4.8. *The $5 \times N$ partial Hadamard matrices are of the form*

$$H = \begin{pmatrix} W_4 & \ldots & W_4 & K_4 & \ldots & K_4 \\ v_1 & \ldots & v_a & x_1 & \ldots & x_b \end{pmatrix}$$

with $a \geq b$, $a + b = N/4$ and with $v_i, x_j \in (\pm 1)^4$ satisfying

$$W_4 \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix} = -K_4 \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix}$$

where $r_t = \sum_i (v_i)_t$ and $s_t = \sum_j (v_j)_t$.

Proof. This is something that we already worked out at $N = 8$, in section 1 above, in both of the cases that can appear, namely $a = 2, b = 0$ and $a = 1, b = 1$. The proof in general is similar, with the equations in the statement coming by processing the orthogonality conditions between the 5th row and the first 4 rows. □

As a first observation, the equations in the above statement can be written in the following more convenient form:

$$K_4^{-1} W_4 \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix} = -\begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix}$$

Now observe that the matrix of this system is as follows:

$$K_4^{-1} W_4 = \frac{1}{2} \begin{pmatrix} - & + & + & + \\ - & - & + & - \\ - & + & - & - \\ - & - & - & + \end{pmatrix}$$

Thus, the system can be written as follows:

$$\begin{pmatrix} - & + & + & + \\ - & - & + & - \\ - & + & - & - \\ - & - & - & + \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix} = -2 \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix}$$

We can see that we are led into parity and positivity questions, regarding the vectors $r_t = \sum_i (v_i)_t$ and $s_t = \sum_j (v_j)_t$. It is possible to further go along these lines, but the structure of the $5 \times N$ partial Hadamard matrices remains something quite complicated. As an explicit consequence, however, of all this, we have the following result:

Theorem 4.9. *Consider an arbitrary $4 \times N$ partial Hadamard matrix, written as*

$$H = (\underbrace{W_4 \ \ldots \ W_4}_{a} \ \underbrace{K_4 \ \ldots \ K_4}_{b})$$

with $a \geq b$, $a + b = N/4$, up to equivalence. In order for this matrix to complete into a $5 \times N$ partial Hadamard matrix, the following condition must be satisfied:

$$ab = 0 \implies N = 0(8)$$

In particular, the following $4 \times N$ partial Hadamard matrix does not complete into a $5 \times N$ partial Hadamard matrix:

$$Z = (W_4 \ W_4 \ W_4)$$

Proof. This follows from Proposition 4.8, because with the notations there, $b = 0$ implies that the system there is simply:

$$W_4 \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix} = 0$$

Since the Walsh matrix W_4 is invertible, the solution of this system is $r = 0$. Now observe that, by definition of the numbers r_i, as sums a quantities of type ± 1, we have $r_i = a(2)$ for any i. Thus, we must have $a = 0(2)$, and since we have $a = N/4$, this gives $N = 0(8)$, as desired. The proof in the case $a = 0$ is similar. □

In general, the full classification of all the possible 5×8 completions of a given $4 \times N$ partial Hadamard matrix are quite difficult, and we have already seen this at $N = 8$, where a careful study is needed, the result being as follows:

Theorem 4.10. *The 4×8 partial Hadamard matrices, namely*

$$A = (W_4 \ W_4)$$

$$B = (W_4 \ K_4)$$

both complete into 5×8 partial Hadamard matrices, with the solutions being those coming from the lower rows of the following matrices, which are Hadamard:

$$\begin{pmatrix} W_4 & W_4 \\ W_4 & -W_4 \end{pmatrix} \quad , \quad \begin{pmatrix} W_4 & W_4 \\ K_4 & -K_4 \end{pmatrix}$$

$$\begin{pmatrix} W_4 & K_4 \\ W_4 & -K_4 \end{pmatrix} \quad , \quad \begin{pmatrix} W_4 & K_4 \\ K_4 & -W_4 \end{pmatrix}$$

This gives as well the higher completions, $M \times 8$ with $M = 6, 7, 8$.

Proof. This is something that we aready know, from section 1 above. □

At $N=12$ now, we have only one matrix to be studied, namely:

$$P=(W_4\ W_4\ K_4)$$

Observe that we have at least 8 solutions to the completion problem, coming from the Paley matrix, which can be written as:

$$P_{12}=\begin{pmatrix}
+&+&+&+&&-&+&+&+&&-&+&+&+\\
+&-&+&-&&+&-&+&+&&+&-&+&+\\
+&+&-&-&&+&+&-&+&&+&+&-&+\\
+&-&-&+&&+&+&+&-&&+&+&+&-\\
\\
-&+&-&-&&+&-&+&+&&-&+&+&-\\
-&+&+&+&&+&+&-&+&&+&-&+&-\\
-&-&-&+&&+&+&+&+&&-&-&-&+\\
+&+&+&-&&+&+&+&-&&-&-&-&-\\
\\
-&+&+&+&&+&-&+&-&&+&+&-&+\\
+&+&-&+&&+&-&-&-&&-&-&+&+\\
+&-&+&+&&+&-&-&+&&-&+&-&-\\
-&-&+&-&&+&+&-&-&&-&+&+&+
\end{pmatrix}$$

In general, all this leads to quite complicated algebra and combinatorics. We refer to [52], [59], [72], [76], [137] for more on the combinatorics of the PHM.

Let us try now to count the partial Hadamard matrices $H\in M_{M\times N}(\pm1)$. This is an easy task at $M=2,3,4$, where the answer is as follows:

Proposition 4.11. *The number of PHM at $M=2,3,4$ is*

$$\begin{aligned}
\#PHM_{2\times N}&=&2^N\binom{N}{N/2}\\
\#PHM_{3\times N}&=&2^N\binom{N}{N/4,N/4,N/4,N/4}\\
\#PHM_{4\times N}&=&2^N\sum_{a+b=N/4}\binom{N}{a,b,b,a,b,a,a,b}
\end{aligned}$$

where the quantities on the right are multinomial coefficients.

Proof. Indeed, the multinomial coefficients at right count the matrices having the first row consisting of 1 entries only, and the 2^N factor comes from this. □

In order to convert the above result into $N\to\infty$ estimates, we will need the following technical result regarding the multinomial coefficients, from [115]:

Theorem 4.12. *We have the estimate*

$$\sum_{a_1+\ldots+a_s=N}\binom{N}{a_1,\ldots,a_s}^p\simeq s^{pN}\sqrt{\frac{s^{s(p-1)}}{p^{s-1}(2\pi N)^{(s-1)(p-1)}}}$$

in the $N\to\infty$ limit.

Proof. This is proved by Richmond and Shallit in [115] at $p=2$, and the proof in the general case, $p\in\mathbb{N}$, is similar. More precisely, let us denote by c_{sp} the sum on the left:

$$c_{sp}=\sum_{a_1+\ldots+a_s=N}\binom{N}{a_1,\ldots,a_s}^p$$

Let us set now:

$$a_i=\frac{N}{s}+x_i\sqrt{N}$$

By using the various formulae in [115], we obtain:

$$\begin{aligned}
&c_{sp}\\
\simeq\ & s^{pN}(2\pi N)^{\frac{(1-s)p}{2}}s^{\frac{sp}{2}}\exp\left(-\frac{sp}{2}\sum_{i=1}^sx_i^2\right)\\
\simeq\ & s^{pN}(2\pi N)^{\frac{(1-s)p}{2}}s^{\frac{sp}{2}}\underbrace{\int_0^N\ldots\int_0^N}_{s-1}\exp\left(-\frac{sp}{2}\sum_{i=1}^sx_i^2\right)da_1\ldots da_{s-1}\\
=\ & s^{pN}(2\pi N)^{\frac{(1-s)p}{2}}s^{\frac{sp}{2}}N^{\frac{s-1}{2}}\underbrace{\int_0^N\ldots\int_0^N}_{s-1}\exp\left(-\frac{sp}{2}\sum_{i=1}^{s-1}x_i^2-\frac{sp}{2}\left(\sum_{i=1}^{s-1}x_i\right)^2\right)dx_1\ldots dx_{s-1}\\
=\ & s^{pN}(2\pi N)^{\frac{(1-s)p}{2}}s^{\frac{sp}{2}}N^{\frac{s-1}{2}}\times\pi^{\frac{s-1}{2}}s^{-\frac{1}{2}}\left(\frac{sp}{2}\right)^{\frac{1-s}{2}}\\
=\ & s^{pN}(2\pi N)^{\frac{(1-s)p}{2}}s^{\frac{sp}{2}-\frac{1}{2}+\frac{1-s}{2}}\left(\frac{p}{2\pi N}\right)^{\frac{1-s}{2}}\\
=\ & s^{pN}(2\pi N)^{\frac{(1-s)(p-1)}{2}}s^{\frac{sp-s}{2}}p^{\frac{1-s}{2}}\\
=\ & s^{pN}\sqrt{\frac{s^{s(p-1)}}{p^{s-1}(2\pi N)^{(s-1)(p-1)}}}
\end{aligned}$$

Thus we have obtained the formula in the statement, and we are done. □

The above formula is something very useful, that we will heavily use in what follows. Getting back now to the PHM, we have the following result:

Theorem 4.13. *The probability for a random $H \in M_{M\times N}(\pm 1)$ to be a PHM is*

$$P_2 \simeq \frac{2}{\sqrt{2\pi N}}$$

$$P_3 \simeq \frac{16}{\sqrt{(2\pi N)^3}}$$

$$P_4 \simeq \frac{512}{(2\pi N)^3}$$

in the $N \in 4\mathbb{N}$, $N \to \infty$ limit.

Proof. Since there are exactly 2^{MN} sign matrices of size $N \times M$, the probability P_M for a random $H \in M_{M\times N}(\pm 1)$ to be a PHM is given by:

$$P_M = \frac{1}{2^{MN}} \# PHM_{M\times N}$$

With this formula in hand, the result follows from Proposition 4.11, by using the standard estimates for multinomial coefficients from Theorem 4.12. □

In their remarkable paper [59], de Launey and Levin were able to count the PHM, in the asymptotic limit $N \in 4\mathbb{N}$, $N \to \infty$. Their method is based on:

Proposition 4.14. *The probability for a random $H \in M_{M\times N}(\pm 1)$ to be partial Hadamard equals the probability for a length N random walk with increments drawn from*

$$E = \left\{ (e_i \bar{e}_j)_{i<j} \Big| e \in \mathbb{Z}_2^M \right\}$$

regarded as a subset of $\mathbb{Z}_2^{\binom{M}{2}}$ to return at the origin.

Proof. Indeed, with $T(e) = (e_i \bar{e}_j)_{i<j}$, a matrix $X = [e_1, \ldots, e_N] \in M_{M\times N}(\mathbb{Z}_2)$ is partial Hadamard if and only if:

$$T(e_1) + \ldots + T(e_N) = 0$$

But this gives the result. □

As explained in [59] the above probability can be indeed computed, and we have:

Theorem 4.15. *The probability for a random $H \in M_{M\times N}(\pm 1)$ to be PHM is*

$$P_M \simeq \frac{2^{(M-1)^2}}{\sqrt{(2\pi N)^{\binom{M}{2}}}}$$

in the $N \in 4\mathbb{N}$, $N \to \infty$ limit.

Proof. According to Proposition 4.14 above, we have:

$$\begin{aligned} P_M &= \frac{1}{q^{(M-1)N}}\#\left\{\xi_1,\ldots,\xi_N\in E\Big|\sum_i\xi_i=0\right\}\\ &= \frac{1}{q^{(M-1)N}}\sum_{\xi_1,\ldots,\xi_N\in E}\delta_{\Sigma\xi_i,0} \end{aligned}$$

By using the Fourier inversion formula we have, with $D=\binom{M}{2}$:

$$\delta_{\Sigma\xi_i,0}=\frac{1}{(2\pi)^D}\int_{[-\pi,\pi]^D}e^{i<\lambda,\Sigma\xi_i>}d\lambda$$

After many non-trivial computations, this leads to the result. See [59]. □

Let us mention as well that for the general matrices $H\in M_{M\times N}(\pm1)$, which are not necessarily PHM, such statistics can be deduced from the work of Tau-Vu [133]. All this is quite interesting, because it provides an alternative to the HC problematics.

Following now [27], and some previous work from [88], [89], let us discuss now another topic, namely the square submatrices of the Hadamard matrices. We will see that all this is related to the notion of almost Hadamard matrix (AHM), discussed in section 3 above. We will be actually interested in the sign matrices of the AHM:

Definition 4.16. *A matrix $S\in M_N(\pm1)$ is called an almost Hadamard sign pattern (AHP) if there exists an almost Hadamard matrix $H\in M_N(\mathbb R)$ such that:*

$$S_{ij}=sgn(H_{ij})$$

Note that if a sign matrix S is an AHP, then there exists a unique almost Hadamard matrix H such that $S_{ij}=sgn(H_{ij})$, namely:

$$H=\sqrt{N}Pol(S)$$

Since the polar part is not uniquely defined for singular sign matrices, in what follows, we will mostly be concerned with invertible AHP and AHM. We start analyzing square the submatrices of Hadamard matrices. By permuting rows and columns, we can always reduce the problem to the following situation:

Definition 4.17. *$D\in M_d(\pm1)$ is called a submatrix of $H\in M_N(\pm1)$ if we have*

$$H=\begin{bmatrix}A&B\\C&D\end{bmatrix}$$

up to a permutation of the rows and columns of H. We set $r=size(A)=N-d$.

Observe that any $D\in M_2(\pm1)$ having distinct columns appears as a submatrix of W_4, and that any $D\in M_2(\pm1)$ appears as a submatrix of W_8. In fact, we have:

Proposition 4.18. *Let $D \in M_d(\pm 1)$ be an arbitrary sign matrix.*

(1) *If D has distinct columns, then D is as submatrix of W_N, with $N = 2^d$.*
(2) *In general, D appears as submatrix of W_M, with $M = 2^{d+\lceil \log_2 d \rceil}$.*

Proof. This is elementary, as follows:

(1) Set $N = 2^d$. If we use length d bit strings $x, y \in \{0,1\}^d$ as indices, then:

$$(W_N)_{xy} = (-1)^{\sum x_i y_i}$$

Let $\widetilde{W}_N \in M_{d \times N}(\pm 1)$ be the submatrix of W_N having as row indices the strings of type:

$$x_i = (\underbrace{0 \ldots 0}_{i}\ 1\ \underbrace{0 \ldots 0}_{N-i-1})$$

Then for $i \in \{1, \ldots, d\}$ and $y \in \{0,1\}^d$, we have:

$$(\widetilde{W}_N)_{iy} = (-1)^{y_i}$$

Thus the columns of $\widetilde{W}_N$ are the N elements of $\{\pm 1\}^d$, which gives the result.

(2) Set $R = 2^{\lceil \log_2 d \rceil} \geq d$. Since the first row of W_R contains only ones, $W_R \otimes W_N$ contains as a submatrix R copies of $\widetilde{W}_N$, in which D can be embedded, as desired. $\square$

Let us go back now to Definition 4.17, and try to relate the matrices A, D appearing there. The following result, due to Szöllősi [127], is a first one in this direction:

Theorem 4.19. *If $U = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ is unitary, with $A \in M_r(\mathbb{C})$, $D \in M_d(\mathbb{C})$, then:*

(1) *The singular values of A, D are identical, up to $|r - d|$ values of 1.*
(2) *$\det A = \det U \cdot \overline{\det D}$, so in particular, $|\det A| = |\det D|$.*

Proof. Here is a simplified proof. From the unitarity of U, we get:

$$A^*A + C^*C = I_r$$
$$CC^* + DD^* = I_d$$
$$AC^* + BD^* = 0_{r \times d}$$

(1) This follows from the first two equations, and from the well-known fact that the matrices CC^*, C^*C have the same eigenvalues, up to $|r - d|$ values of 0.

(2) By using the above unitarity equations, we have:

$$\begin{bmatrix} A & 0 \\ C & I \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} I & C^* \\ 0 & D^* \end{bmatrix}$$

The result follows by taking determinants. $\square$

We state and prove now our main results on the submatrices of Hadamard matrices. Our first goal is to find a formula for the polar decomposition of D. Let us introduce:

Definition 4.20. *Associated to any $A\in M_r(\pm1)$ are the matrices*

$$X_A = (\sqrt{N}I_r+\sqrt{A^tA})^{-1}Pol(A)^t$$
$$Y_A = (\sqrt{N}I_r+\sqrt{AA^t})^{-1}$$

depending on a parameter N.

Observe that, in terms of the polar decomposition $A=VP$, we have:

$$X_A = (\sqrt{N}+P)^{-1}V^t$$
$$Y_A = V(\sqrt{N}+P)^{-1}V^t$$

The idea now is that, under the assumptions of Theorem 4.19, the polar parts of A,D are related by a simple formula, with the passage $Pol(A)\to Pol(D)$ involving the above matrices X_A,Y_A. In what follows we will focus on the case where $U\in U_N$ is replaced by $U=\sqrt{N}H$ with $H\in M_N(\pm1)$ Hadamard. In the non-singular case, we have:

Proposition 4.21. *Assuming that a matrix*

$$H=\begin{bmatrix}A&B\\ C&D\end{bmatrix}\in M_N(\pm1)$$

is Hadamard, with $A\in M_r(\pm1)$ invertible, $D\in M_d(\pm1)$, and $||A||<\sqrt{N}$, the polar decomposition $D=UT$ is given by

$$U=\frac{1}{\sqrt{N}}(D-E)$$

$$T=\sqrt{N}I_d-S$$

with $E=CX_AB$ and $S=B^tY_AB$.

Proof. Since H is Hadamard, we can use the formulae coming from:

$$\begin{bmatrix}A&B\\ C&D\end{bmatrix}\begin{bmatrix}A^t&C^t\\ B^t&D^t\end{bmatrix}=\begin{bmatrix}A^t&C^t\\ B^t&D^t\end{bmatrix}\begin{bmatrix}A&B\\ C&D\end{bmatrix}=\begin{bmatrix}N&0\\ 0&N\end{bmatrix}$$

We start from the singular value decomposition of A:

$$A=Vdiag(s_i)X^t$$

Here $V,X\in O(r)$, $s_i\in(0,||A||]$. From $AA^t+BB^t=NI_r$ we get:

$$BB^t=Vdiag(N-s_i^2)V^t$$

Thus, the singular value decomposition of B is as follows, with $Y\in O_d$:

$$B=V\left[diag(\sqrt{N-s_i^2})\quad 0_{r\times(d-r)}\right]Y^t$$

Similarly, from $A^tA + C^tC = I_r$, we infer the singular value decomposition for C, the result being that there exists an orthogonal matrix $\widetilde{Z} \in O(d)$ such that:

$$C = -\widetilde{Z} \begin{bmatrix} diag(\sqrt{N - s_i^2}) \\ 0_{(d-r)\times r} \end{bmatrix} X^t$$

From $B^tB + D^tD = NI_d$, we obtain:

$$D^tD = Y(diag(s_i^2) \oplus NI_{(d-r)})Y^t$$

Tus the polar decomposition of D reads:

$$D = UY(diag(s_i) \oplus \sqrt{N}I_{(d-r)})Y^t$$

Let $Z = UY$ and use the orthogonality relation $CA^t + DB^t = 0_{d\times r}$ to obtain:

$$\widetilde{Z} \begin{bmatrix} diag(s_i\sqrt{N - s_i^2}) \\ 0_{(d-r)\times r} \end{bmatrix} = Z \begin{bmatrix} diag(s_i\sqrt{N - s_i^2}) \\ 0_{(d-r)\times r} \end{bmatrix}$$

From the hypothesis, we have $s_i\sqrt{N - s_i^2} > 0$ and thus $Z^t\widetilde{Z} = I_r \oplus Q$, for some orthogonal matrix $Q \in O_d$. Plugging $\widetilde{Z} = Z(I_r \oplus Q)$ in the singular value decomposition formula for C, we obtain:

$$C = -Z(I_r \oplus Q) \begin{bmatrix} diag(\sqrt{N - s_i^2}) \\ 0_{(d-r)\times r} \end{bmatrix} X^t = -Z \begin{bmatrix} diag(\sqrt{N - s_i^2}) \\ 0_{(d-r)\times r} \end{bmatrix} X^t$$

To summarize, we have found $V, X \in O_r$ and $Y, Z \in O_d$ such that:

$$\begin{aligned} A &= V diag(s_i) X^t \\ B &= V \begin{bmatrix} diag(\sqrt{N - s_i^2}) & 0_{r\times(d-r)} \end{bmatrix} Y^t \\ C &= -Z \begin{bmatrix} diag(\sqrt{N - s_i^2}) \\ 0_{(d-r)\times r} \end{bmatrix} X^t \\ D &= Z(diag(s_i) \oplus \sqrt{N}I_{(d-r)})Y^t \end{aligned}$$

Now with U, T, E, S defined as in the statement, we obtain:

$$\begin{aligned} U &= ZY^t \\ E &= Z(diag(\sqrt{N} - s_i) \oplus 0_{d-r})Y^t \\ \sqrt{A^tA} &= X diag(s_i) X^t \\ (\sqrt{N}I_r + \sqrt{A^tA})^{-1} &= X diag(1/(\sqrt{N} + s_i))X^t \\ X_A &= X diag(1/(\sqrt{N} + s_i))V^t \\ CX_AB &= Z(diag(\sqrt{N} - s_i) \oplus 0_{d-r})Y^t \end{aligned}$$

Thus we have $E=CX_AB$, as claimed. Also, we have:

$$\begin{aligned}
T &= Y(diag(s_i)\oplus\sqrt{N}I_{d-r})Y^t\\
S &= Y(diag(\sqrt{N}-s_i)\oplus 0_{d-r})Y^t\\
\sqrt{AA^t} &= Vdiag(s_i)V^t\\
Y_A &= Vdiag(1/(\sqrt{N}+s_i))V^t\\
B^tY_AB &= Y(diag(\sqrt{N}-s_i)\oplus 0_{d-r})Y^t
\end{aligned}$$

Hence, $S=B^tY_AB$, as claimed, and we are done. □

Observe that, in the above statement, in the case where the size of the upper left block satisfies $r<\sqrt{N}$, the condition $||A||<\sqrt{N}$ is automatically satisfied.

As a first application, let us try to find out when D is AHP, in the sense of Definition 4.16. For this purpose, we must estimate the quantity $||E||_\infty=\max_{ij}|E_{ij}|$:

Proposition 4.22. *Assuming that*

$$H=\begin{bmatrix}A&B\\ C&D\end{bmatrix}\in M_N(\pm 1)$$

is an Hadamard matrix, with $A\in M_r(\pm 1)$, $D\in M_d(\pm 1)$ and $r\leq d$. Then,

$$Pol(D)=\frac{1}{\sqrt{N}}(D-E)$$

with E satisfying:

(1) $||E||_\infty\leq\frac{r\sqrt{r}}{\sqrt{r}+\sqrt{N}}$ *when A is Hadamard.*
(2) $||E||_\infty\leq\frac{r^2c\sqrt{N}}{N-r^2}$ *if $r^2<N$, with $c=||Pol(A)-\frac{A}{\sqrt{N}}||_\infty$.*
(3) $||E||_\infty\leq\frac{r^2(1+\sqrt{N})}{N-r^2}$ *if $r^2<N$.*

Proof. We use the basic fact that for two matrices $X\in M_{p\times r}(\mathbb{C}),Y\in M_{r\times q}(\mathbb{C})$ we have:

$$||XY||_\infty\leq r||X||_\infty||Y||_\infty$$

Thus, according to Proposition 4.21, we have:

$$\begin{aligned}
||E||_\infty &= ||CX_AB||_\infty\\
&\leq r^2||C||_\infty||X_A||_\infty||B||_\infty\\
&= r^2||X_A||_\infty
\end{aligned}$$

(1) If A is Hadamard, $AA^t = rI_r$, $Pol(A) = A/\sqrt{r}$ and thus:

$$\begin{aligned} X_A &= (\sqrt{N}I_r + \sqrt{r}I_r)^{-1}\frac{A^t}{\sqrt{r}} \\ &= \frac{A^t}{r+\sqrt{rN}} \end{aligned}$$

Thus $||X_A||_\infty = \frac{1}{r+\sqrt{rN}}$, which gives the result.

(2) According to the definition of X_A, we have:

$$\begin{aligned} X_A &= (\sqrt{N}I_r + \sqrt{A^tA})^{-1}Pol(A)^t \\ &= (NI_r - A^tA)^{-1}(\sqrt{N}I_r - \sqrt{A^tA})Pol(A)^t \\ &= (NI_r - A^tA)^{-1}(\sqrt{N}Pol(A) - A)^t \end{aligned}$$

We therefore obtain:

$$\begin{aligned} ||X_A||_\infty &\leq r||(NI_r - A^tA)^{-1}||_\infty||\sqrt{N}Pol(A) - A||_\infty \\ &= \frac{rc}{\sqrt{N}}\left|\left|\left(I_r - \frac{A^tA}{N}\right)^{-1}\right|\right|_\infty \end{aligned}$$

Now by using $||A^tA||_\infty \leq r$, we obtain:

$$\begin{aligned} \left|\left|\left(I_r - \frac{A^tA}{N}\right)^{-1}\right|\right|_\infty &\leq \sum_{k=0}^\infty \frac{||(A^tA)^k||_\infty}{N^k} \\ &\leq \sum_{k=0}^\infty \frac{r^{2k-1}}{N^k} \\ &= \frac{1}{r}\cdot\frac{1}{1-r^2/N} \\ &= \frac{N}{rN - r^3} \end{aligned}$$

Thus we have the following estimate:

$$||X_A||_\infty \leq \frac{rc}{\sqrt{N}}\cdot\frac{N}{rN-r^3} = \frac{c\sqrt{N}}{N-r^2}$$

But this gives the result.

(3) This follows from (2), because:

$$c \leq ||Pol(A)||_\infty + ||A/\sqrt{N}||_\infty \leq 1 + \frac{1}{\sqrt{N}}$$

The proof is now complete. □

Following [27], we can now state and prove a main result, as follows:

Theorem 4.23. *Assume that*

$$H=\begin{bmatrix}A&B\\C&D\end{bmatrix}$$

is Hadamard, with $A\in M_r(\pm1),H\in M_N(\pm1)$.

(1) *If A is Hadamard, and $N>r(r-1)^2$, then D is AHP.*
(2) *If $N>\frac{r^2}{4}(x+\sqrt{x^2+4})^2$, where $x=r||Pol(A)-\frac{A}{\sqrt{N}}||_\infty$, then D is AHP.*
(3) *If $N>\frac{r^2}{4}(r+\sqrt{r^2+8})^2$, then D is AHP.*

Proof. This basically follows from the various estimates that we have, as follows:

(1) This follows from Proposition 4.22 (1), because:

$$\frac{r\sqrt{r}}{\sqrt{r}+\sqrt{N}}<1\iff r<1+\sqrt{N/r}$$
$$\iff r(r-1)^2<N$$

(2) This follows from Proposition 4.22 (2), because:

$$\frac{r^2c\sqrt{N}}{N-r^2}<1\iff N-r^2c\sqrt{N}>r^2$$
$$\iff (2\sqrt{N}-r^2c)^2>r^4c^2+4r^2$$

Indeed, this is equivalent to:

$$2\sqrt{N}>r^2c+r\sqrt{r^2c^2+4}=r(x+\sqrt{x^2+4})$$

Here the value of x is as follows:

$$x=rc=r\left|\left|Pol(A)-\frac{A}{\sqrt{N}}\right|\right|_\infty$$

(3) This follows from Proposition 4.22 (3), because:

$$\frac{r^2(1+\sqrt{N})}{N-r^2}<1\iff N-r^2\sqrt{N}>2r^2$$
$$\iff (2\sqrt{N}-r^2)^2>r^4+8r^2$$

Indeed, this is equivalent to:

$$2\sqrt{N}>r^2+r\sqrt{r^2+8}$$

But this gives the result. □

As a technical comment, for $A\in M_r(\pm1)$ Hadamard, Proposition 4.22 (2) gives:

$$\begin{aligned}||E||_\infty &\leq \frac{r^2\sqrt{N}}{N-r^2}\left(\frac{1}{\sqrt{r}}-\frac{1}{\sqrt{N}}\right)\\ &= \frac{r\sqrt{r}N-r^2}{N-r^2}\end{aligned}$$

Thus $||E||_\infty<1$ for $N>r^3$, which is slightly weaker than Theorem 4.23 (1).

In view of the results above, it is convenient to make the following convention:

Definition 4.24. *We denote by $\{x\}_{m\times n}\in M_{m\times n}(\mathbb{R})$ the all-x, $m\times n$ matrix, and by*

$$\begin{Bmatrix}x_{11}&\ldots&x_{1l}\\ \ldots&\ldots&\ldots\\ x_{k1}&\ldots&x_{kl}\end{Bmatrix}_{(m_1,\ldots,m_k)\times(n_1,\ldots,n_l)}$$

the matrix having all-x_{ij} rectangular blocks $X_{ij}=\{x_{ij}\}_{m_i\times n_j}\in M_{m_i\times n_j}(\mathbb{R})$, of prescribed size. In the case of square diagonal blocks, we simply write $\{x\}_n=\{x\}_{n\times n}$ and

$$\begin{Bmatrix}x_{11}&\ldots&x_{1k}\\ \ldots&\ldots&\ldots\\ x_{kk}&\ldots&x_{kk}\end{Bmatrix}_{n_1,\ldots n_k}=\begin{Bmatrix}x_{11}&\ldots&x_{1k}\\ \ldots&\ldots&\ldots\\ x_{k1}&\ldots&x_{kk}\end{Bmatrix}_{(n_1,\ldots,n_k)\times(n_1,\ldots,n_k)}$$

Modulo equivalence, the ±1 matrices of size $r=1,2$ are as follows:

$$\begin{bmatrix}+\end{bmatrix}_{(1)}\quad,\quad\begin{bmatrix}+&+\\+&-\end{bmatrix}_{(2)}\quad,\quad\begin{bmatrix}+&+\\+&+\end{bmatrix}_{(2')}$$

In the cases (1) and (2) above, where the matrix A is invertible, the spectral properties of their complementary matrices are as follows:

Theorem 4.25. *For the $N\times N$ Hadamard matrices of type*

$$\begin{bmatrix}+&+\\+&D\end{bmatrix}_{(1)}\quad,\quad\begin{bmatrix}+&+&+&+\\+&-&+&-\\+&+&D_{00}&D_{01}\\+&-&D_{10}&D_{11}\end{bmatrix}_{(2)}$$

the polar decomposition $D=UT$ with $U=\frac{1}{\sqrt{N}}(D-E)$, $T=\sqrt{N}I-S$ is given by:

$$E_{(1)}=\left\{\tfrac{1}{1+\sqrt{N}}\right\}_{N-1}\quad,\quad E_{(2)}=\frac{2}{2+\sqrt{2N}}\begin{Bmatrix}1&1\\1&-1\end{Bmatrix}_{N/2-1,N/2-1}$$

$$S_{(1)}=\left\{\tfrac{1}{1+\sqrt{N}}\right\}_{N-1}\quad,\quad S_{(2)}=\frac{2}{\sqrt{2}+\sqrt{N}}\begin{Bmatrix}1&0\\0&1\end{Bmatrix}_{N/2-1,N/2-1}$$

In particular, all the matrices D above are AHP.

Proof. For $A\in M_r(\pm1)$ Hadamard, the quantities in Definition 4.20 are:

$$X_A=\frac{A^t}{r+\sqrt{rN}}\quad,\quad Y_A=\frac{I_r}{\sqrt{r}+\sqrt{N}}$$

These formulae follow indeed from $AA^t=A^tA=rI_r$ and $Pol(A)=A/\sqrt{r}$.

(1) Using the notation introduced in Definition 4.20, we have here $B_{(1)}=\{1\}_{1\times N-1}$ and $C_{(1)}=B_{(1)}^t$. Since $A_{(1)}=[+]$ is Hadamard we have $X_{A_{(1)}}=Y_{A_{(1)}}=\frac{1}{1+\sqrt{N}}$, and so:

$$\begin{aligned}E_{(1)}&=\frac{1}{1+\sqrt{N}}\{1\}_{N-1\times1}[1]\{1\}_{1\times N-1}=\frac{1}{1+\sqrt{N}}\{1\}_{N-1}\\ S_{(1)}&=\frac{1}{1+\sqrt{N}}\{1\}_{N-1\times1}\{1\}_{1\times N-1}=\frac{1}{1+\sqrt{N}}\{1\}_{N-1}\end{aligned}$$

(2) Using the orthogonality of the first two rows of $H_{(2)}$, we find that the matrices D_{00} and D_{11} have size $N/2-1$. Since since the matrix $A_{(2)}=[^+_+\ ^+_-]$ is Hadamard we have $X_{A_{(2)}}=\frac{A}{2+\sqrt{2N}}$ and $Y_{A_{(2)}}=\frac{I_2}{\sqrt{2}+\sqrt{N}}$, and this gives the following formulae:

$$\begin{aligned}E_{(2)}&=\frac{1}{2+\sqrt{2N}}\begin{Bmatrix}1&1\\1&-1\end{Bmatrix}_{(N/2-1,N/2-1)\times(1,1)}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{Bmatrix}1&1\\1&-1\end{Bmatrix}_{(1,1)\times(N/2-1,N/2-1)}\\ &=\frac{2}{2+\sqrt{2N}}\begin{Bmatrix}1&1\\1&-1\end{Bmatrix}_{N/2-1,N/2-1}\\ S_{(2)}&=\frac{1}{\sqrt{2}+\sqrt{N}}\begin{Bmatrix}1&1\\1&-1\end{Bmatrix}_{(N/2-1,N/2-1)\times(1,1)}\begin{Bmatrix}1&1\\1&-1\end{Bmatrix}_{(1,1)\times(N/2-1,N/2-1)}\\ &=\frac{2}{\sqrt{2}+\sqrt{N}}\begin{Bmatrix}1&0\\0&1\end{Bmatrix}_{N/2-1,N/2-1}\end{aligned}$$

Thus, we obtain the formulae in the statement. $\square$

We refer to [27] for a complete discussion in relation with the above.

5. **Complex matrices**

We have seen that the Hadamard matrices $H \in M_N(\pm 1)$ are very interesting objects. In what follows, we will be interested in their complex versions:

Definition 5.1. *A complex Hadamard matrix is a square matrix whose entries belong to the unit circle in the complex plane,*

$$H \in M_N(\mathbb{T})$$

and whose rows are pairwise orthogonal, with respect to the scalar product of $\mathbb{C}^N$.

Here, and in what follows, the scalar product is the usual one on $\mathbb{C}^N$, taken to be linear in the first variable and antilinear in the second one:

$$< x, y >= \sum_i x_i \bar{y}_i$$

As basic examples of complex Hamadard matrices, we have of course the real Hadamard matrices, $H \in M_N(\pm 1)$, which have sizes $N \in \{2\} \cup 4\mathbb{N}$. Here is now a new example, with $w = e^{2\pi i/3}$, which appears at the forbidden size value $N = 3$:

$$F_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{pmatrix}$$

We will see that there are many other examples, and in particular that there are such matrices at any $N \in \mathbb{N}$, which in addition can be chosen to be circulant. Thus, the HC and CHC problematics will dissapear in the general complex setting.

Let us start our study of the complex Hadamard matrices by extending some basic results from the real case, from section 1 above. First, we have:

Proposition 5.2. *The set formed by the $N \times N$ complex Hadamard matrices is the real algebraic manifold*

$$X_N = M_N(\mathbb{T}) \cap \sqrt{N} U_N$$

where U_N is the unitary group, the intersection being taken inside $M_N(\mathbb{C})$.

Proof. Let $H \in M_N(\mathbb{T})$. Then H is Hadamard if and only if its rescaling $U = H/\sqrt{N}$ belongs to the unitary group U_N, and so when $H \in X_N$, as claimed. □

We should mention that the above manifold X_N, while appearing by definition as an intersection of smooth manifolds, is very far from being smooth. We will be back to this, later on. As a basic consequence now of the above result, we have:

Proposition 5.3. *Let $H \in M_N(\mathbb{C})$ be an Hadamard matrix.*

(1) *The columns of H must be pairwise orthogonal.*
(2) *The matrices $H^t, \bar{H}, H^* \in M_N(\mathbb{C})$ are Hadamard as well.*

Proof. We use the well-known fact that if a matrix is unitary, $U \in U_N$, then so is its complex conjugate $\bar{U} = (\bar{U}_{ij})$, the inversion formulae being as follows:

$$U^* = U^{-1} \quad , \quad U^t = \bar{U}^{-1}$$

Thus the unitary group U_N is stable under the following operations:

$$U \to U^t \quad , \quad U \to \bar{U} \quad , \quad U \to U^*$$

It follows that the algebraic manifold X_N constructed in Proposition 5.2 is stable as well under these operations. But this gives all the assertions. □

Let us introduce now the following equivalence notion for the complex Hadamard matrices, taking into account some basic operations which can be performed:

Definition 5.4. *Two complex Hadamard matrices are called equivalent, and we write $H \sim K$, when it is possible to pass from H to K via the following operations:*

(1) *Permuting the rows, or permuting the columns.*
(2) *Multiplying the rows or columns by numbers in $\mathbb{T}$.*

Also, we say that H is dephased when its first row and column consist of 1 *entries.*

Observe that, up to the above equivalence relation, any complex Hadamard matrix $H \in M_N(\mathbb{T})$ can be put in dephased form. Moreover, the dephasing operation is unique, if we allow only the operations (2) in Definition 5.4, namely row and column multiplications by numbers in $\mathbb{T}$. In what follows, "dephasing the matrix" will have precisely this meaning, namely dephasing by using the operations (2) in Definition 5.4.

Regarding analytic aspects, once again in analogy with the study from the real case, we can locate the complex Hadamard matrices inside $M_N(\mathbb{T})$, as follows:

Theorem 5.5. *Given a matrix $H \in M_N(\mathbb{T})$, we have*

$$|\det(H)| \leq N^{N/2}$$

with equality precisely when H is Hadamard.

Proof. By using the basic properties of the determinant, we have indeed the following estimate, valid for any vectors $H_1, \ldots, H_N \in \mathbb{T}^N$:

$$|\det(H_1, \ldots, H_N)| \leq ||H_1|| \times \ldots \times ||H_N|| = (\sqrt{N})^N$$

The equality case appears precisely when our vectors $H_1, \ldots, H_N \in \mathbb{T}^N$ are pairwise orthogonal, and this gives the result. □

From a "dual" point of view, the question of locating X_N inside $\sqrt{N}U_N$, once again via analytic methods, makes sense as well, and we have here the following result:

Theorem 5.6. *Given a matrix $U\in U_N$ we have*

$$||U||_1\leq N\sqrt{N}$$

with equality precisely when $H=\sqrt{N}U$ is Hadamard.

Proof. We have indeed the following estimate, valid for any $U\in U_N$:

$$||U||_1=\sum_{ij}|U_{ij}|\leq N\left(\sum_{ij}|U_{ij}|^2\right)^{1/2}=N\sqrt{N}$$

The equality case holds when $|U_{ij}|=\sqrt{N}$, for any i,j. But this amounts in saying that the rescaled matrix $H=\sqrt{N}U$ must satisfy $H\in M_N(\mathbb{T})$, as desired. $\square$

At the level of the examples now, we have the following basic construction, which works at any $N\in\mathbb{N}$, in stark contrast with what happens in the real case:

Theorem 5.7. *The Fourier matrix, $F_N=(w^{ij})$ with $w=e^{2\pi i/N}$, which in standard matrix form, with indices $i,j=0,1,\ldots,N-1$, is as follows,*

$$F_N=\begin{pmatrix}1&1&1&\ldots&1\\1&w&w^2&\ldots&w^{N-1}\\1&w^2&w^4&\ldots&w^{2(N-1)}\\\vdots&\vdots&\vdots&&\vdots\\1&w^{N-1}&w^{2(N-1)}&\ldots&w^{(N-1)^2}\end{pmatrix}$$

is a complex Hadamard matrix, in dephased form.

Proof. By using the standard fact that the averages of complex numbers correspond to barycenters, we conclude that the scalar products between the rows of F_N are:

$$<R_a,R_b>=\sum_j w^{aj}w^{-bj}=\sum_j w^{(a-b)j}=N\delta_{ab}$$

Thus F_N is indeed a complex Hadamard matrix. As for the fact that F_N is dephased, this follows from our convention $i,j=0,1,\ldots,N-1$, which is there for this. $\square$

As a first classification result now, in the complex case, we have:

Proposition 5.8. *The Fourier matrices F_2,F_3, which are given by*

$$F_2=\begin{pmatrix}1&1\\1&-1\end{pmatrix}\quad,\quad F_3=\begin{pmatrix}1&1&1\\1&w&w^2\\1&w^2&w\end{pmatrix}$$

with $w=e^{2\pi i/3}$ are the only Hadamard matrices at $N=2,3$, up to equivalence.

Proof. The proof at $N=2$ is similar to the proof from the real case. Indeed, given $H\in M_N(\mathbb T)$ Hadamard, we can dephase it, as follows:

$$\begin{pmatrix}a&b\\ c&d\end{pmatrix}\to\begin{pmatrix}1&1\\ \bar{a}c&\bar{b}d\end{pmatrix}\to\begin{pmatrix}1&1\\ 1&a\bar{b}\bar{c}d\end{pmatrix}$$

Now since the dephasing operation preserves the class of the Hadamard matrices, we have $a\bar{b}\bar{c}d=-1$, and so we obtain by dephasing the matrix F_2. Regarding now the case $N=3$, consider an Hadamard matrix $H\in M_3(\mathbb T)$, assumed to be in dephased form:

$$H=\begin{pmatrix}1&1&1\\ 1&x&y\\ 1&z&t\end{pmatrix}$$

The orthogonality conditions between the rows of this matrix read:

$$(1\perp 2)\quad:\quad x+y=-1$$

$$(1\perp 3)\quad:\quad z+t=-1$$

$$(2\perp 3)\quad:\quad x\bar{z}+y\bar{t}=-1$$

In order to process these conditions, which are all of the same nature, consider an arbitrary equation of the following type:

$$p+q=-1\quad,\quad p,q\in\mathbb T$$

This equation tells us that the triangle having vertices at $1,p,q$ must be equilateral, and so that we must have $\{p,q\}=\{w,w^2\}$, with $w=e^{2\pi i/3}$. By using this fact, for the first two equations, we conclude that we must have:

$$\{x,y\}=\{w,w^2\}\quad,\quad\{z,t\}=\{w,w^2\}$$

As for the third equation, this tells us that we must have $x\neq z$.

Thus, our Hadamard matrix H is either the Fourier matrix F_3, or the matrix obtained from F_3 by permuting the last two columns, and we are done. □

In order to deal now with the case $N=4$, we already know, from our study in the real case, that we will need tensor products. So, let us formulate:

Definition 5.9. *The tensor product of complex Hadamard matrices is given, in double indices, by $(H\otimes K)_{ia,jb}=H_{ij}K_{ab}$. In other words, we have the formula*

$$H\otimes K=\begin{pmatrix}H_{11}K&\dots&H_{1M}K\\ \vdots&&\vdots\\ H_{M1}K&\dots&H_{MM}K\end{pmatrix}$$

by using the lexicographic order on the double indices.

Here the fact that $H \otimes K$ is indeed Hadamard comes from the fact that its rows R_{ia} are pairwise orthogonal, as shown by the following computation:

$$\begin{aligned} < R_{ia}, R_{kc} > &= \sum_{jb} H_{ij} K_{ab} \cdot \bar{H}_{kj} \bar{K}_{cb} \\ &= \sum_j H_{ij} \bar{H}_{kj} \sum_b K_{ab} \bar{K}_{cb} \\ &= M\delta_{ik} \cdot N\delta_{ac} \\ &= MN\delta_{ia,kc} \end{aligned}$$

In order to advance now, our first task will be that of tensoring the Fourier matrices. We have here the following statement, refining and generalizing Theorem 5.7:

Theorem 5.10. *Given a finite abelian group G, with dual group $\widehat{G} = \{\chi : G \to \mathbb{T}\}$, consider the Fourier coupling $\mathcal{F}_G : G \times \widehat{G} \to \mathbb{T}$, given by $(i, \chi) \to \chi(i)$.*

1. *Via the standard isomorphism $G \simeq \widehat{G}$, this Fourier coupling can be regarded as a square matrix, $F_G \in M_G(\mathbb{T})$, which is a complex Hadamard matrix.*
2. *In the case of the cyclic group $G = \mathbb{Z}_N$ we obtain in this way, via the standard identification $\mathbb{Z}_N = \{1, \ldots, N\}$, the Fourier matrix F_N.*
3. *In general, when using a decomposition $G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$, the corresponding Fourier matrix is given by $F_G = F_{N_1} \otimes \ldots \otimes F_{N_k}$.*

Proof. This follows indeed from some basic facts from group theory:

(1) With the identification $G \simeq \widehat{G}$ made our matrix is given by $(F_G)_{i\chi} = \chi(i)$, and the scalar products between the rows are computed as follows:

$$< R_i, R_j >= \sum_\chi \chi(i)\overline{\chi(j)} = \sum_\chi \chi(i - j) = |G| \cdot \delta_{ij}$$

Thus, we obtain indeed a complex Hadamard matrix.

(2) This follows from the well-known and elementary fact that, via the identifications $\mathbb{Z}_N = \widehat{\mathbb{Z}_N} = \{1, \ldots, N\}$, the Fourier coupling here is as follows, with $w = e^{2\pi i/N}$:

$$(i, j) \to w^{ij}$$

(3) We use here the following well-known formula, for the duals of products:

$$\widehat{H \times K} = \widehat{H} \times \widehat{K}$$

At the level of the corresponding Fourier couplings, we obtain from this:

$$F_{H \times K} = F_H \otimes F_K$$

Now by decomposing G into cyclic groups, as in the statement, and by using (2) for the cyclic components, we obtain the formula in the statement. □

As a first application of the above result, we have:

Proposition 5.11. *The Walsh matrix, W_N with $N = 2^n$, which is given by*

$$W_N = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n}$$

is the Fourier matrix of the finite abelian group $K_N = \mathbb{Z}_2^n$.

Proof. We know that the first Walsh matrix is a Fourier matrix, $W_2 = F_2 = F_{K_2}$. Now by taking tensor powers we obtain from this that we have, for any $N = 2^n$:

$$W_N = W_2^{\otimes n} = F_{K_2}^{\otimes n} = F_{K_2^n} = F_{K_N}$$

Thus, we are led to the conclusion in the statement. □

By getting back now to classification, we will need the following result, from [62]:

Theorem 5.12. *If $H \in M_M(\mathbb{T})$ and $K \in M_N(\mathbb{T})$ are Hadamard, then so are the following two matrices, for any choice of a parameter matrix $Q \in M_{M\times N}(\mathbb{T})$:*

1. *$H \otimes_Q K \in M_{MN}(\mathbb{T})$, given by $(H \otimes_Q K)_{ia,jb} = Q_{ib}H_{ij}K_{ab}$.*
2. *$H_Q\!\otimes K \in M_{MN}(\mathbb{T})$, given by $(H_Q\!\otimes K)_{ia,jb} = Q_{ja}H_{ij}K_{ab}$.*

These are called right and left Diţă deformations of $H \otimes K$, with parameter Q.

Proof. These results follow from the same computations as in the usual tensor product case, the idea being that the Q parameters will cancel:

(1) The rows R_{ia} of the matrix $H \otimes_Q K$ are indeed pairwise orthogonal, because:

$$\begin{aligned} < R_{ia}, R_{kc} > &= \sum_{jb} Q_{ib}H_{ij}K_{ab} \cdot \bar{Q}_{kb}\bar{H}_{kj}\bar{K}_{cb} \\ &= M\delta_{ik}\sum_b K_{ab}\bar{K}_{cb} \\ &= M\delta_{ik} \cdot N\delta_{ac} \\ &= MN\delta_{ik,ac} \end{aligned}$$

(2) The rows L_{ia} of the matrix $H_Q\!\otimes K$ are orthogonal as well, because:

$$\begin{aligned} < L_{ia}, L_{kc} > &= \sum_{jb} Q_{ja}H_{ij}K_{ab} \cdot \bar{Q}_{jc}\bar{H}_{kj}\bar{K}_{cb} \\ &= N\delta_{ac}\sum_j H_{ij}\bar{H}_{kj} \\ &= N\delta_{ac} \cdot M\delta_{ik} \\ &= MN\delta_{ik,ac} \end{aligned}$$

Thus, both the matrices in the statement are Hadamard, as claimed. □

As a first observation, when the parameter matrix is the all-one matrix $\mathbb{I} \in M_{M\times N}(\mathbb{T})$, we obtain in this way the usual tensor product of our matrices:

$$H \otimes_{\mathbb{I}} K = H_{\mathbb{I}} \otimes K = H \otimes K$$

As a non-trivial example now, let us compute the right deformations of the Walsh matrix $W_4 = F_2 \otimes F_2$, with arbitrary parameter matrix $Q = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$:

$$\begin{aligned} F_2 \otimes_Q F_2 &= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes_{\begin{pmatrix} p & q \\ r & s \end{pmatrix}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} p & q & p & q \\ p & -q & p & -q \\ r & s & -r & -s \\ r & -s & -r & s \end{pmatrix} \end{aligned}$$

This follows indeed by carefully working out what happens, by using the lexicographic order on the double indices, as explained in section 1 above. To be more precise, the usual tensor product $W_4 = F_2 \otimes F_2$ appears as follows:

$$W_4 = \begin{pmatrix} ia\backslash jb & 00 & 01 & 10 & 11 \\ & & & & \\ 00 & 1 & 1 & 1 & 1 \\ 01 & 1 & -1 & 1 & -1 \\ 10 & 1 & 1 & -1 & -1 \\ 11 & 1 & -1 & -1 & 1 \end{pmatrix}$$

The corresponding values of the parameters Q_{ib} to be inserted are as follows:

$$(Q_{ib}) = \begin{pmatrix} ia\backslash jb & 00 & 01 & 10 & 11 \\ & & & & \\ 00 & Q_{00} & Q_{01} & Q_{00} & Q_{01} \\ 01 & Q_{00} & Q_{01} & Q_{00} & Q_{01} \\ 10 & Q_{10} & Q_{11} & Q_{10} & Q_{11} \\ 11 & Q_{10} & Q_{11} & Q_{10} & Q_{11} \end{pmatrix}$$

With the notation $Q = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$, this latter matrix becomes:

$$(Q_{ib}) = \begin{pmatrix} ia\backslash jb & 00 & 01 & 10 & 11 \\ & & & & \\ 00 & p & q & p & q \\ 01 & p & q & p & q \\ 10 & r & s & r & s \\ 11 & r & s & r & s \end{pmatrix}$$

Now by pointwise multiplying this latter matrix with the matrix W_4 given above, we obtain the announced formula for the deformed tensor product $F_2 \otimes_Q F_2$.

As for the left deformations of $W_4 = F_2 \otimes F_2$, once again with arbitrary parameter matrix $Q = \binom{p\ q}{r\ s}$, these are given by a similar formula, as follows:

$$\begin{aligned} F_{2Q}\otimes F_2 &= \begin{pmatrix}1&1\\1&-1\end{pmatrix}_{\begin{pmatrix}p&q\\r&s\end{pmatrix}}\otimes\begin{pmatrix}1&1\\1&-1\end{pmatrix}\\ &= \begin{pmatrix}p&p&r&r\\q&-q&s&-s\\p&p&-r&-r\\q&-q&-s&s\end{pmatrix}\end{aligned}$$

Observe that this latter matrix is transpose to $F_2 \otimes_Q F_2$. However, this is something accidental, coming from the fact that F_2, and so W_4 as well, are self-transpose.

With the above constructions in hand, we have the following result:

Theorem 5.13. *The only complex Hadamard matrices at $N = 4$ are, up to the standard equivalence relation, the matrices*

$$F_4^s = \begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&s&-1&-s\\1&-s&-1&s\end{pmatrix}$$

with $s \in \mathbb{T}$, which appear as right Diţă deformations of $W_4 = F_2 \otimes F_2$.

Proof. First of all, the matrix F_4^s is indeed Hadamard, appearing from the construction in Theorem 5.12, assuming that the parameter matrix there $Q \in M_2(\mathbb{T})$ is dephased:

$$Q = \begin{pmatrix}1&1\\1&s\end{pmatrix}$$

Observe also that, conversely, any right Diţă deformation of $W_4 = F_2 \otimes F_2$ is of this form. Indeed, if we consider such a deformation, with general parameter matrix $Q = \binom{p\ q}{r\ s}$ as above, by dephasing we obtain an equivalence with $F_4^{s'}$, where $s' = ps/qr$:

$$\begin{aligned} \begin{pmatrix}p&q&p&q\\p&-q&p&-q\\r&s&-r&-s\\r&-s&-r&s\end{pmatrix} &\to \begin{pmatrix}1&1&1&1\\1&-1&1&-1\\r/p&s/q&-r/p&-s/q\\r/p&-s/q&-r/p&s/q\end{pmatrix}\\ &\to \begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&ps/qr&-1&-ps/qr\\1&-ps/qr&-1&ps/qr\end{pmatrix}\end{aligned}$$

It remains to prove that the matrices F_4^s are non-equivalent, and that any complex Hadamard matrix $H \in M_4(\mathbb{T})$ is equivalent to one of these matrices F_4^s.

But this follows by using the same kind of arguments as in the proof from the real case, and from the proof of Proposition 5.8. Indeed, let us first dephase our matrix:

$$H = \begin{pmatrix} 1&1&1&1\\ 1&a&b&c\\ 1&d&e&f\\ 1&g&h&i \end{pmatrix}$$

We use now the fact, coming from plane geometry, that the solutions $x, y, z, t \in \mathbb{T}$ of the equation $x + y + z + t = 0$ are as follows, with $p, q \in \mathbb{T}$:

$$\{x, y, z, t\} = \{p, q, -p, -q\}$$

In our case, we have $1 + a + d + g = 0$, and so up to a permutation of the last 3 rows, our matrix must look at follows, for a certain $s \in \mathbb{T}$:

$$H = \begin{pmatrix} 1&1&1&1\\ 1&-1&b&c\\ 1&s&e&f\\ 1&-s&h&i \end{pmatrix}$$

In the case $s = \pm 1$ we can permute the middle two columns, then repeat the same reasoning, and we end up with the matrix in the statement.

In the case $s \neq \pm 1$ we have $1 + s + e + f = 0$, and so $-1 \in \{e, f\}$. Up to a permutation of the last columns, we can assume $e = -1$, and our matrix becomes:

$$H = \begin{pmatrix} 1&1&1&1\\ 1&-1&b&c\\ 1&s&-1&-s\\ 1&-s&h&i \end{pmatrix}$$

Similarly, from $1 - s + h + i = 0$ we deduce that $-1 \in \{h, i\}$. In the case $h = -1$ our matrix must look as follows, and we are led to the matrix in the statement:

$$H = \begin{pmatrix} 1&1&1&1\\ 1&-1&b&c\\ 1&s&-1&-s\\ 1&-s&-1&i \end{pmatrix}$$

As for the remaining case $i = -1$, here our matrix must look as follows:

$$H = \begin{pmatrix} 1&1&1&1\\ 1&-1&b&c\\ 1&s&-1&-s\\ 1&-s&h&-1 \end{pmatrix}$$

We obtain from the last column $c = s$, then from the second row $b = -s$, then from the third column $h = s$, and so our matrix must be as follows:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -s & s \\ 1 & s & -1 & -s \\ 1 & -s & s & -1 \end{pmatrix}$$

But, in order for the second and third row to be orthogonal, we must have $s \in \mathbb{R}$, and so $s = \pm 1$, which contradicts our above assumption $s \neq \pm 1$.

Thus, we are done with the proof of the main assertion. As for the fact that the matrices in the statement are indeed not equivalent, this is standard as well. See [129]. □

At $N = 5$ now, the situation is considerably more complicated, with F_5 being the only matrix. The key technical result here, due to Haagerup [69], is as follows:

Proposition 5.14. *Given an Hadamard matrix $H \in M_5(\mathbb{T})$, chosen dephased,*

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & a & x & * & * \\ 1 & y & b & * & * \\ 1 & * & * & * & * \\ 1 & * & * & * & * \end{pmatrix}$$

the numbers a, b, x, y must satisfy the following equation:

$$(x - y)(x - ab)(y - ab) = 0$$

Proof. This is something quite surprising, and tricky, the proof in [69] being as follows. Let us look at the upper 3-row truncation of H, which is of the following form:

$$H' = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & a & x & p & q \\ 1 & y & b & r & s \end{pmatrix}$$

By using the orthogonality of the rows, we have:

$$(1 + a + x)(1 + \bar{b} + \bar{y})(1 + \bar{a}y + b\bar{x}) = -(p + q)(r + s)(\bar{p}r + \bar{q}s)$$

On the other hand, by using $p, q, r, s \in \mathbb{T}$, we have:

$$\begin{aligned} (p + q)(r + s)(\bar{p}r + \bar{q}s) &= (r + p\bar{q}s + \bar{p}qr + s)(\bar{r} + \bar{s}) \\ &= 1 + p\bar{q}\bar{r}s + \bar{p}q + \bar{r}s + r\bar{s} + p\bar{q} + \bar{p}qr\bar{s} + 1 \\ &= 2Re(1 + p\bar{q} + r\bar{s} + p\bar{q}r\bar{s}) \\ &= 2Re[(1 + p\bar{q})(1 + r\bar{s})] \end{aligned}$$

We conclude that we have the following formula, involving a, b, x, y only:

$$(1 + a + x)(1 + \bar{b} + \bar{y})(1 + \bar{a}y + b\bar{x}) \in \mathbb{R}$$

Now this is a product of type $(1+\alpha)(1+\beta)(1+\gamma)$, with the first summand being 1, and with the last summand, namely $\alpha\beta\gamma$, being real as well, as shown by the above general $p,q,r,s\in\mathbb T$ computation. Thus, when expanding, and we are left with:

$$\begin{aligned}&(a+x)+(\bar b+\bar y)+(\bar a y+b\bar x)+(a+x)(\bar b+\bar y)\\+\quad&(a+x)(\bar a y+b\bar x)+(\bar b+\bar y)(\bar a y+b\bar x)\in\mathbb R\end{aligned}$$

By expanding all the products, our formula looks as follows:

$$\begin{aligned}&a+x+\bar b+\bar y+\bar a y+b\bar x+a\bar b+a\bar y+\bar b x+x\bar y\\+\quad&1+ab\bar x+\bar a xy+b+\bar a\bar b y+\bar x+\bar a+b\bar x\bar y\in\mathbb R\end{aligned}$$

By removing from this all terms of type $z+\bar z$, we are left with:

$$a\bar b+x\bar y+ab\bar x+\bar a\bar b y+\bar a xy+b\bar x\bar y\in\mathbb R$$

Now by getting back to our Hadamard matrix, all this remains true when transposing it, which amounts in interchanging $x\leftrightarrow y$. Thus, we have as well:

$$a\bar b+\bar x y+ab\bar y+\bar a\bar b x+\bar a xy+b\bar x\bar y\in\mathbb R$$

By substracting now the two equations that we have, we obtain:

$$x\bar y-\bar x y+ab(\bar x-\bar y)+\bar a\bar b(y-x)\in\mathbb R$$

Now observe that this number, say Z, is purely imaginary, because $\bar Z=-Z$. Thus our equation reads $Z=0$. On the other hand, we have the following formula:

$$\begin{aligned}abxyZ&=abx^2-aby^2+a^2b^2(y-x)+xy(y-x)\\&=(y-x)(a^2b^2+xy-ab(x+y))\\&=(y-x)(ab-x)(ab-y)\end{aligned}$$

Thus, our equation $Z=0$ corresponds to the formula in the statement. □

By using the above result, we are led to the following theorem, also from [69]:

Theorem 5.15. *The only Hadamard matrix at $N=5$ is the Fourier matrix,*

$$F_5=\begin{pmatrix}1&1&1&1&1\\1&w&w^2&w^3&w^4\\1&w^2&w^4&w&w^3\\1&w^3&w&w^4&w^2\\1&w^4&w^3&w^2&w\end{pmatrix}$$

with $w=e^{2\pi i/5}$, up to the standard equivalence relation for such matrices.

Proof. Assume that have an Hadamard matrix $H\in M_5(\mathbb T)$, chosen dephased, and written as in Proposition 5.14, with emphasis on the upper left 2×2 subcorner:

$$H=\begin{pmatrix}1&1&1&1&1\\ 1&a&x&*&*\\ 1&y&b&*&*\\ 1&*&*&*&*\\ 1&*&*&*&*\end{pmatrix}$$

We know from Proposition 5.14, applied to H itself, and to its transpose H^t as well, that the entries a,b,x,y must satisfy the following equations:

$$(a-b)(a-xy)(b-xy)=0$$
$$(x-y)(x-ab)(y-ab)=0$$

Our first claim is that, by doing some combinatorics, we can actually obtain from this $a=b$ and $x=y$, up to the equivalence relation for the Hadamard matrices:

$$H\sim\begin{pmatrix}1&1&1&1&1\\ 1&a&x&*&*\\ 1&x&a&*&*\\ 1&*&*&*&*\\ 1&*&*&*&*\end{pmatrix}$$

Indeed, the above two equations lead to 9 possible cases, the first of which is, as desired, $a=b$ and $x=y$. As for the remaining 8 cases, here once again things are determined by 2 parameters, and in practice, we can always permute the first 3 rows and 3 columns, and then dephase our matrix, as for our matrix to take the above special form.

With this result in hand, the combinatorics of the scalar products between the first 3 rows, and between the first 3 columns as well, becomes something which is quite simple to investigate. By doing a routine study here, and then completing it with a study of the lower right 2×2 corner as well, we are led to 2 possible cases, as follows:

$$H\sim\begin{pmatrix}1&1&1&1&1\\ 1&a&b&c&d\\ 1&b&a&d&c\\ 1&c&d&a&b\\ 1&d&c&b&a\end{pmatrix}\quad,\quad H\sim\begin{pmatrix}1&1&1&1&1\\ 1&a&b&c&d\\ 1&b&a&d&c\\ 1&c&d&b&a\\ 1&d&c&a&b\end{pmatrix}$$

Our claim now is that the first case is in fact not possible. Indeed, we must have:

$$\begin{aligned}a+b+c+d&=-1\\ 2Re(a\bar b)+2Re(c\bar d)&=-1\\ 2Re(a\bar c)+2Re(b\bar d)&=-1\\ 2Re(a\bar d)+2Re(b\bar c)&=-1\end{aligned}$$

Now since $|Re(x)| \leq 1$ for any $x \in \mathbb{T}$, we deduce from the second equation that:

$$Re(a\bar{b}) \leq 1/2$$

In other words, the arc length between a, b satisfies $\theta(a, b) \geq \pi/3$. The same argument applies to c, d, and to the other pairs of numbers in the last 2 equations. Now since our equations are invariant under permutations of a, b, c, d, we can assume that our numbers a, b, c, d are ordered on the unit circle, and by the above, separated by $\geq \pi/3$ arc lengths. But this tells us that we have the following inequalities:

$$\theta(a, c) \geq 2\pi/3 \quad , \quad \theta(b, d) \geq 2\pi/3$$

These two inequalities give the following estimates:

$$Re(a\bar{c}) \leq -1/2 \quad , \quad Re(b\bar{d}) \leq -1/2$$

But these estimates contradict the third equation. Thus, our claim is proved.

Summarizing, we have proved so far that our matrix must be as follows:

$$H \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & a & b & c & d \\ 1 & b & a & d & c \\ 1 & c & d & b & a \\ 1 & d & c & a & b \end{pmatrix}$$

We are now in position of finishing. The orthogonality equations are as follows:

$$\begin{aligned} a + b + c + d &= -1 \\ 2Re(a\bar{b}) + 2Re(c\bar{d}) &= -1 \\ a\bar{c} + c\bar{b} + b\bar{d} + d\bar{a} &= -1 \end{aligned}$$

The third equation can be written in the following equivalent form:

$$\begin{aligned} Re[(a + b)(\bar{c} + \bar{d})] &= -1 \\ Im[(a - b)(\bar{c} - \bar{d})] &= 0 \end{aligned}$$

By using now $a, b, c, d \in \mathbb{T}$, we obtain from this:

$$\frac{a + b}{a - b} \in i\mathbb{R} \quad , \quad \frac{c + d}{c - d} \in i\mathbb{R}$$

Thus we can find $s, t \in \mathbb{R}$ such that:

$$a + b = is(a - b) \quad , \quad c + d = it(c - d)$$

By plugging in these values, our system of equations simplifies, as follows:

$$\begin{aligned} (a + b) + (c + d) &= -1 \\ |a + b|^2 + |c + d|^2 &= 3 \\ (a + b)(\bar{c} + \bar{d}) &= -1 \end{aligned}$$

Now observe that the last equation implies in particular that we have:

$$|a+b|^2 \cdot |c+d|^2 = 1$$

Thus $|a+b|^2, |c+d|^2$ must be roots of the following polynomial:

$$X^2 - 3X + 1 = 0$$

But this gives the following equality of sets:

$$\left\{ |a+b|\,,\,|c+d| \right\} = \left\{ \frac{\sqrt{5}+1}{2}\,,\,\frac{\sqrt{5}-1}{2} \right\}$$

This is good news, because we are now into 5-th roots of unity. To be more precise, we have 2 cases to be considered, the first one being as follows, with $z \in \mathbb{T}$:

$$a+b = \frac{\sqrt{5}+1}{2}\,z \quad , \quad c+d = -\frac{\sqrt{5}-1}{2}\,z$$

From $a+b+c+d=-1$ we obtain $z=-1$, and by using this we obtain:

$$b = \bar{a} \quad , \quad d = \bar{c}$$

Thus we have the following formulae:

$$Re(a) = \cos(2\pi/5) \quad , \quad Re(c) = \cos(\pi/5)$$

We conclude that we have $H \sim F_5$, as claimed. As for the second case, with a,b and c,d interchanged, this leads to $H \sim F_5$ as well. □

At $N=6$ now, the situation becomes complicated, with lots of "exotic" solutions. The simplest examples of Hadamard matrices at $N=6$ are as follows:

Theorem 5.16. *We have the following basic Hadamard matrices, at $N=6$:*

1. *The Fourier matrix F_6.*
2. *The Diţă deformations of $F_2 \otimes F_3$ and of $F_3 \otimes F_2$.*
3. *The Haagerup matrix H_6^q.*
4. *The Tao matrix T_6.*

Proof. All this is elementary, the idea, and formulae of the matrices, being as follows:

(1) This is something that we know well.

(2) Consider indeed the dephased Diţă deformations of $F_2 \otimes F_3$ and $F_3 \otimes F_2$:

$$F_6^{(rs)} = F_2 \otimes_{\begin{pmatrix}1&1&1\\1&r&s\end{pmatrix}} F_3 \qquad , \qquad F_6^{(\binom{r}{s})} = F_3 \otimes_{\begin{pmatrix}1&1\\1&r\\1&s\end{pmatrix}} F_2$$

Here r,s are two parameters on the unit circle, $r,s\in\mathbb{T}$. In matrix form:

$$F_6^{(rs)}=\begin{pmatrix}1&1&1&1&1&1\\1&w&w^2&1&w&w^2\\1&w^2&w&1&w^2&w\\ \\1&r&s&-1&-r&-s\\1&wr&w^2s&-1&-wr&-w^2s\\1&w^2r&ws&-1&-w^2r&-ws\end{pmatrix}$$

As for the other deformation, this is given by:

$$F_6^{\binom{r}{s}}=\begin{pmatrix}1&1&1&1&1&1\\1&-1&1&-1&1&-1\\ \\1&r&w&wr&w^2&w^2r\\1&-r&w&-wr&w^2&-w^2r\\ \\1&s&w^2&w^2s&w&ws\\1&-s&w^2&-w^2s&w&-ws\end{pmatrix}$$

(3) The matrix here, from [69], is as follows, with $q\in\mathbb{T}$:

$$H_6^q=\begin{pmatrix}1&1&1&1&1&1\\1&-1&i&i&-i&-i\\1&i&-1&-i&q&-q\\1&i&-i&-1&-q&q\\1&-i&\bar{q}&-\bar{q}&i&-1\\1&-i&-\bar{q}&\bar{q}&-1&i\end{pmatrix}$$

(4) The matrix here, from [131], is as follows, with $w=e^{2\pi i/3}$:

$$T_6=\begin{pmatrix}1&1&1&1&1&1\\1&1&w&w&w^2&w^2\\1&w&1&w^2&w^2&w\\1&w&w^2&1&w&w^2\\1&w^2&w^2&w&1&w\\1&w^2&w&w^2&w&1\end{pmatrix}$$

Observe that both H_6^q and T_6 are indeed complex Hadamard matrices. $\square$

The matrices in Theorem 5.16 are "regular", in the sense that the scalar products between rows appear in the simplest possible way, namely from vanishing sums of roots of unity, possibly rotated by a scalar. We will be back to this in section 6 below, with a result stating that these matrices are the only regular ones, at $N=6$.

In the non-regular case now, there are many known constructions at $N=6$. Here is one such construction, found by Björck and Fröberg in [44]:

Proposition 5.17. *The following is a complex Hadamard matrix,*

$$BF_6=\begin{pmatrix}1&ia&-a&-i&-\bar{a}&i\bar{a}\\ i\bar{a}&1&ia&-a&-i&-\bar{a}\\ -\bar{a}&i\bar{a}&1&ia&-a&-i\\ -i&-\bar{a}&i\bar{a}&1&ia&-a\\ -a&-i&-\bar{a}&i\bar{a}&1&ia\\ ia&-a&-i&-\bar{a}&i\bar{a}&1\end{pmatrix}$$

where $a\in\mathbb{T}$ is one of the roots of $a^2+(\sqrt{3}-1)a+1=0$.

Proof. Observe that the matrix in the statement is circulant, in the sense the rows appear by cyclically permuting the first row. Thus, we only have to check that the first row is orthogonal to the other 5 rows. But this follows from $a^2+(\sqrt{3}-1)a+1=0$. $\square$

Let us discuss now the case $N=7$. We will restrict the attention to case where the combinatorics comes from roots of unity. We use the following result, from [127]:

Theorem 5.18. *If $H\in M_N(\pm1)$ with $N\geq 8$ is dephased symmetric Hadamard, and*

$$w=\frac{(1\pm i\sqrt{N-5})^2}{N-4}$$

then the following procedure yields a complex Hadamard matrix $M\in M_{N-1}(\mathbb{T})$:

1. *Erase the first row and column of H.*
2. *Replace all diagonal 1 entries with $-w$.*
3. *Replace all off-diagonal -1 entries with w.*

Proof. We know that the scalar product between any two rows of H, normalized as there, appears as follows:

$$P=\frac{N}{4}\cdot1\cdot1+\frac{N}{4}\cdot1\cdot(-1)+\frac{N}{4}\cdot(-1)\cdot1+\frac{N}{4}\cdot(-1)\cdot(-1)=0$$

Let us peform now the above operations (1,2,3), in reverse order. When replacing $-1\to w$, all across the matrix, the above scalar product becomes:

$$P'=\frac{N}{4}\cdot1\cdot1+\frac{N}{4}\cdot1\cdot\bar{w}+\frac{N}{4}\cdot w\cdot1+\frac{N}{4}\cdot(-1)\cdot(-1)=\frac{N}{2}(1+Re(w))$$

Now when adjusting the diagonal via $w\to-1$ back, and $1\to-w$, this amounts in adding the quantity $-2(1+Re(w))$ to our product. Thus, our product becomes:

$$P''=\left(\frac{N}{2}-2\right)(1+Re(w))=\frac{N-4}{2}\left(1+\frac{6-N}{N-4}\right)=1$$

Finally, erasing the first row and column amounts in substracting 1 from our scalar product. Thus, our scalar product becomes $P'''=1-1=0$, and we are done. $\square$

Observe that the number w in the above statement is a root of unity precisely at $N = 8$, where the only matrix satisfying the conditions in the statement is the Walsh matrix W_8. So, let us apply, as in [127], the above construction to this matrix, namely:

$$W_8 = \begin{pmatrix}1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&1&-1&-1&1&1&-1&-1\\1&-1&-1&1&1&-1&-1&1\\1&1&1&1&-1&-1&-1&-1\\1&-1&1&-1&-1&1&-1&1\\1&-1&-1&-1&-1&-1&1&1\\1&-1&-1&1&-1&1&1&-1\end{pmatrix}$$

We obtain in this way the following matrix:

$$W_8' = \begin{pmatrix}*&*&*&*&*&*&*&*\\ *&-1&1&w&1&w&1&w\\ *&1&-1&w&1&1&w&w\\ *&w&w&-w&1&w&w&1\\ *&1&1&1&-1&w&w&w\\ *&w&1&w&w&-w&w&1\\ *&1&w&w&w&w&-w&1\\ *&w&w&1&w&1&1&-1\end{pmatrix}$$

The Hadamard matrix obtained in this way, by deleting the $*$ entries, is the Petrescu matrix P_7, found in [111]. Thus, we have the following result:

Theorem 5.19. *P_7 is the unique matrix formed by roots of unity that can be obtained by the Szöllősi construction. It appears at $N = 8$, from $H = W_8$. Its formula is*

$$(P_7)_{ijk,abc} = \begin{cases}-w & \text{if } (ijk) = (abc),\ ia + jb + kc = 0(2)\\ w & \text{if } (ijk) \neq (abc),\ ia + jb + kc \neq 0(2)\\ (-1)^{ia+jb+kc} & \text{otherwise}\end{cases}$$

where $w = e^{2\pi i/3}$, and with the indices belonging to the set $\{0, 1\}^3 - \{(0, 0, 0)\}$.

Proof. We know that the Szöllősi construction maps $W_8 \to P_7$. Since the formula of the second Fourier matrix is $(F_2)_{ij} = (-1)^{ij}$, the formula of the Walsh matrix W_8 is:

$$(W_8)_{ijk,abc} = (-1)^{ia+jb+kc}$$

But this gives the formula in the statement. □

Now observe that we are in the quite special situation $H = F_2 \otimes K$, with K being dephased and symmetric. Thus, we can search for a one-parameter affine deformation

$K(q)$ which is dephased and symmetric, and then build the following matrix:

$$H(q)=\begin{pmatrix}K(q)&K\\K&-K(\bar{q})\end{pmatrix}$$

In our case, such a deformation $K(q)=W_4(q)$ can be obtained by putting the q parameters in the 2×2 middle block. Now by performing the Szöllősi construction, with the parameters $q,\bar{q}$ left untouched, we obtain the parametric Petrescu matrix [111]:

Theorem 5.20. *The following is a complex Hadamard matrix,*

$$P_7^q=\begin{pmatrix}-q&q&w&1&w&1&w\\q&-q&w&1&1&w&w\\w&w&-w&1&w&w&1\\1&1&1&-1&w&w&w\\w&1&w&w&-\bar{q}w&\bar{q}w&1\\1&w&w&w&\bar{q}w&-\bar{q}w&1\\w&w&1&w&1&1&-1\end{pmatrix}$$

where $w=e^{2\pi i/3}$*, and* $q\in\mathbb{T}$*.*

Proof. This follows from the above considerations, or from a direct verification of the orthogonality of the rows, which uses either $1-1=0$, or $1+w+w^2=0$. $\square$

Observe that the above matrix P_7^q has the property of being "regular", in the sense that the scalar products between rows appear from vanishing sums of roots of unity, possibly rotated by a scalar. We will be back to this in the next section, with the conjectural statement that F_7,P_7^q are the only regular Hadamard matrices at $N=7$.

6. Roots of unity

Many interesting examples of complex Hadamard matrices $H \in M_N(\mathbb{T})$, including the real ones $H \in M_N(\pm 1)$, have as entries roots of unity, of finite order. We discuss here this case, and more generally the "regular" case, where the combinatorics of the scalar products between the rows comes from vanishing sums of roots of unity. Let us begin with the following definition, going back to the work in [47]:

Definition 6.1. *An Hadamard matrix is called of Butson type if its entries are roots of unity of finite order. The Butson class $H_N(l)$ consists of the Hadamard matrices*

$$H \in M_N(\mathbb{Z}_l)$$

where $\mathbb{Z}_l$ is the group of the l-th roots of unity. The level of a Butson matrix $H \in M_N(\mathbb{T})$ is the smallest integer $l \in \mathbb{N}$ such that $H \in H_N(l)$.

As basic examples, we have the real Hadamard matrices, which form the Butson class $H_N(2)$. The Fourier matrices are Butson matrices as well, because we have $F_N \in H_N(N)$, and more generally $F_G \in H_N(l)$, with $N = |G|$, and with $l \in \mathbb{N}$ being the smallest common order of the elements of G. There are many other examples of such matrices, as for instance those as $N = 6$ discussed in section 5, at 1 values of the parameters.

Generally speaking, the main question regarding the Butson matrices is that of understanding when $H_N(l) \neq 0$, via a theorem providing obstructions, and then a result or conjecture stating that these obstructions are the only ones. Let us begin with:

Proposition 6.2 (Sylvester obstruction)**.** *The following holds,*

$$H_N(2) \neq \emptyset \implies N \in \{2\} \cup 4\mathbb{N}$$

due to the orthogonality of the first 3 rows.

Proof. This is something that we know from section 1, with the obstruction, going back to Sylvester's paper [124], being explained there. □

The above obstruction is fully satisfactory, because according to the Hadamard Conjecture, its converse should hold. Thus, we are fully done with the case $l = 2$. Our purpose now will be that of finding analogous statements at $l \geq 3$, theorem plus conjecture. At very small values of l this is certainly possible, and in what regards the needed obstructions, we can get away with the following simple fact, from [47], [148]:

Proposition 6.3. *For a prime power $l = p^a$, the vanishing sums of l-th roots of unity*

$$\lambda_1 + \ldots + \lambda_N = 0 \quad , \quad \lambda_i \in \mathbb{Z}_l$$

appear as formal sums of rotated full sums of p-th roots of unity.

Proof. This is something elementary, coming from basic number theory. Consider indeed the full sum of p-th roots of unity, taken in a formal sense:

$$S=\sum_{k=1}^p(e^{2\pi i/p})^k$$

Let also $w=e^{2\pi i/l}$, and for $r\in\{1,2,\ldots,l/p\}$ let us denote by $S_p^r=w^r\cdot S$ the above formal sum of roots of unity, rotated by w^r:

$$S_p^r=\sum_{k=1}^p w^r(e^{2\pi i/p})^k$$

We must show that any vanishing sum of l-th roots of unity appears as a sum of such quantities S_p^r, with all this taken of course in a formal sense.

For this purpose, consider the following map, which assigns to the abstract elements of the group ring $\mathbb Z[\mathbb Z_l]$ their precise numeric values, inside $\mathbb Z(w)\subset\mathbb C$:

$$\Phi:\mathbb Z[\mathbb Z_l]\to\mathbb Z(w)$$

Our claim is that the elements $\{S_p^r\}$ form a basis of $\ker\Phi$. In order to prove this claim, observe first that $S_p^r\in\ker\Phi$. Also, these elements S_p^r are linearly independent, because the support of S_p^r contains a unique element of the subset $\{1,2,\ldots,p^{a-1}\}\subset\mathbb Z_l$, namely the element $r\in\mathbb Z_l$, so all the coefficients of a vanishing linear combination of such sums S_p^r must vanish. Thus, we are left with proving that $\ker\Phi$ is spanned by $\{S_p^r\}$. For this purpose, let us recall that the minimal polynomial of w is as follows:

$$\frac{X^{p^a}-1}{X^{p^{a-1}}-1}=1+X^{p^{a-1}}+X^{2p^{a-1}}+\ldots+X^{(p-1)p^{a-1}}$$

We conclude that the dimension of $\ker\Phi$ is given by:

$$\dim(\ker\Phi)=p^a-(p^a-p^{a-1})=p^{a-1}$$

Now since this is exactly the number of the sums S_p^r, this finishes the proof of our claim. Thus, any vanishing sum of l-th roots of unity must be of the form $\sum\pm S_p^r$, and the above support considerations show the coefficients must be positive, as desired. $\square$

We can now formulate a result in the spirit of Proposition 6.2, as follows:

Proposition 6.4 (Butson obstruction). *The following holds,*

$$H_N(p^a)\neq\emptyset\implies N\in p\mathbb N$$

due to the orthogonality of the first 2 *rows.*

Proof. This follows indeed from Proposition 6.3, because the scalar product between the first 2 rows of our matrix is a vanishing sum of l-th roots of unity. $\square$

WIth these obstructions in hand, we can discuss the case $l\leq 5$, as follows:

Theorem 6.5. *We have the following results,*

(1) $H_N(2) \neq \emptyset \implies N \in \{2\} \cup 4\mathbb{N}$,
(2) $H_N(3) \neq \emptyset \implies N \in 3\mathbb{N}$,
(3) $H_N(4) \neq \emptyset \implies N \in 2\mathbb{N}$,
(4) $H_N(5) \neq \emptyset \implies N \in 5\mathbb{N}$,

with in cases $(1,3)$, *a conjecture stating that the converse should hold as well.*

Proof. In this statement (1) is the Sylvester obstruction, and (2,3,4) are particular cases of the Butson obstruction. As for the last assertion, which is of course something rather informal, but which is important for our purposes, the situation is as follows:

(1) Here, as already mentioned, we have the Hadamard Conjecture, which comes with solid evidence, as explained in section 1 above.

(2) Here we have an old conjecture, dealing with complex Hadamard matrices over $\{\pm 1, \pm i\}$, going back to the work in [136], and called Turyn Conjecture. □

At $l = 3$ the situation is quite complicated, due to the following result, from [54]:

Proposition 6.6 (de Launey obstruction)**.** *The following holds,*

$$H_N(l) \neq \emptyset \implies \exists\, d \in \mathbb{Z}[e^{2\pi i/l}],\ |d|^2 = N^N$$

due to the orthogonality of all N rows. In particular, we have

$$5|N \implies H_N(6) = \emptyset$$

so in particular $H_{15}(3) = \emptyset$, showing that the Butson obstruction is too weak at $l = 3$.

Proof. The obstruction follows from the unitarity condition $HH^* = N$ for the complex Hadamard matrices, by applying the determinant, which gives:

$$|\det(H)|^2 = N^N$$

Regarding the second assertion, let $w = e^{2\pi i/3}$, and assume that $d = a + bw + cw^2$ with $a, b, c \in \mathbb{Z}$ satisfies $|d|^2 = 0(5)$. We have the following computation:

$$\begin{aligned} |d|^2 &= (a + bw + cw^2)(a + bw^2 + cw) \\ &= a^2 + b^2 + c^2 - ab - bc - ac \\ &= \frac{1}{2}[(a-b)^2 + (b-c)^2 + (c-a)^2] \end{aligned}$$

Thus our condition $|d|^2 = 0(5)$ leads to the following system, modulo 5:

$$x + y + z = 0$$

$$x^2 + y^2 + z^2 = 0$$

But this system has no solutions. Indeed, let us look at $x^2 + y^2 + z^2 = 0$:

(1) If this equality appears as $0+0+0=0$ we can divide x,y,z by 5 and redo the computation.

(2) Otherwise, this equality can only appear as $0+1+(-1)=0$.

Thus, modulo permutations, we must have $x=0, y=\pm 1, z=\pm 2$, which contradicts $x+y+z=0$. Finally, the last assertion follows from $H_{15}(3)\subset H_{15}(6)=\emptyset$. $\square$

At $l=5$ now, things are a bit unclear, with the converse of Theorem 6.5 (4) being something viable, at the conjectural level, at least to our knowledge. At $l=6$ the situation becomes again complicated, as follows:

Proposition 6.7 (Haagerup obstruction). *The following holds, due to Haagerup's $N=5$ classification result, involving the orthogonality of all 5 rows of the matrix:*

$$H_5(l)\neq\emptyset \implies 5|l$$

In particular we have $H_5(6)=\emptyset$, which follows by the way from the de Launey obstruction as well, in contrast with the fact that we generally have $H_N(6)\neq\emptyset$.

Proof. In this statement the obstruction $H_5(l)=\emptyset \implies 5|l$ comes indeed from Haagerup's classification result, explained in Theorem 5.15 above. As for the last assertion, this is something very informal, the situation at small values of N being as follows:

– At $N=2,3,4$ we have the matrices F_2,F_3,W_4.

– At $N=6,7,8,9$ we have the matrices $F_6,P_7^1,W_8,F_3\otimes F_3$.

– At $N=10$ we have the following matrix, found in [17] by using a computer, and written in logarithmic form, with k standing for $e^{k\pi i/3}$:

$$X_{10}^6=\begin{pmatrix}
0&0&0&0&0&0&0&0&0&0\\
0&4&1&5&3&1&3&3&5&1\\
0&1&2&3&5&5&1&3&5&3\\
0&5&3&2&1&5&3&5&3&1\\
0&3&5&1&4&1&1&5&3&3\\
0&3&3&3&3&3&0&0&0&0\\
0&1&1&5&3&4&3&0&2&4\\
0&1&5&3&5&2&4&3&2&0\\
0&5&3&5&1&2&0&2&3&4\\
0&3&5&1&1&4&4&2&0&3
\end{pmatrix}$$

We refer to [17] for more details on this topic. $\square$

All this is not good news. Indeed, there is no hope of conjecturally solving our $H_N(l)\neq\emptyset$ problem in general, because this would have to take into account, and in a simple and conceptual way, both the subtle arithmetic consequences of the de Launey obstruction, and the Haagerup classification result at $N=5$, and this does not seem feasible.

In order to further comment on these difficulties, let us discuss now a generalization of Proposition 6.3 above, and of the related Butson obstruction from Proposition 6.4, which has been our main source of obstructions, so far. Let us start with:

Definition 6.8. *A cycle is a full sum of roots of unity, possibly rotated by a scalar,*

$$C = q\sum_{k=1}^{l} w^k \quad , \quad w = e^{2\pi i/l} \quad , \quad q \in \mathbb{T}$$

and taken in a formal sense. A sum of cycles is a formal sum of cycles.

The actual sum of a cycle, or of a sum of cycles, is of course 0. This is why the word "formal" is there, for reminding us that we are working with formal sums. As an example, here is a sum of cycles, with $w = e^{2\pi i/6}$, and with $|q| = 1$:

$$1 + w^2 + w^4 + qw + qw^4 = 0$$

We know from Proposition 6.3 above that any vanishing sum of l-th roots of unity must be a sum of cycles, at least when $l = p^a$ is a prime power. However, this is not the case in general, the simplest counterexample being as follows, with $w = e^{2\pi i/30}$:

$$w^5 + w^6 + w^{12} + w^{18} + w^{24} + w^{25} = 0$$

The following deep result on the subject is due to Lam and Leung [90]:

Theorem 6.9. *Let $l = p_1^{a_1} \ldots p_k^{a_k}$, and assume that $\lambda_i \in \mathbb{Z}_l$ satisfy:*

$$\lambda_1 + \ldots + \lambda_N = 0$$

1. *$\sum \lambda_i$ is a sum of cycles, with $\mathbb{Z}$ coefficients.*
2. *If $k \leq 2$ then $\sum \lambda_i$ is a sum of cycles (with $\mathbb{N}$ coefficients).*
3. *If $k \geq 3$ then $\sum \lambda_i$ might not decompose as a sum of cycles.*
4. *$\sum \lambda_i$ has the same length as a sum of cycles: $N \in p_1\mathbb{N} + \ldots + p_k\mathbb{N}$.*

Proof. This is something that we will not really need in what follows, but that we included here, in view of its importance. The idea of the proof is as follows:

(1) This is a well-known result, which follows from basic number theory, by using arguments in the spirit of those in the proof of Proposition 6.3 above.

(2) This is something that we already know at $k = 1$, from Proposition 6.3. At $k = 2$ the proof is more technical, along the same lines. See [90].

(3) The smallest possible l potentially producing a counterexample is $l = 2 \cdot 3 \cdot 5 = 30$, and we have here indeed the sum given above, with $w = e^{2\pi i/30}$.

(4) This is a deep result, due to Lam and Leung, relying on advanced number theory knowledge. We refer to their paper [90] for the proof. □

As a consequence of the above result, we have the following generalization of the Butson obstruction, which is something final and optimal on this subject:

Theorem 6.10 (Lam-Leung obstruction)**.** *Assuming the we have*

$$l=p_1^{a_1}\ldots p_k^{a_k}$$

the following must hold, due to the orthogonality of the first 2 rows:

$$H_N(l)\neq\emptyset\implies N\in p_1\mathbb N+\ldots+p_k\mathbb N$$

In the case $k\geq 2$, the latter condition is automatically satisfied at $N>>0$.

Proof. Here the first assertion, which generalizes the $l=p^a$ obstruction from Proposition 6.4 above, comes from Theorem 6.9 (4), applied to the vanishing sum of l-th roots of unity coming from the scalar product between the first 2 rows. As for the second assertion, this is something well-known, coming from basic number theory. □

Summarizing, our study so far of the condition $H_N(l)\neq\emptyset$ has led us into an optimal obstruction coming from the first 2 rows, namely the Lam-Leung one, then an obstruction coming from the first 3 rows, namely the Sylvester one, and then two subtle obstructions coming from all N rows, namely the de Launey one, and the Haagerup one.

As an overall conclusion, by contemplating all these obstructions, nothing good in relation with our problem $H_N(l)\neq\emptyset$ is going on at small N. So, as a natural and more modest objective, we should perhaps try instead to solve this problem at $N>>0$.

The point indeed is that everything simplifies at $N>>0$, with some of the above obstructions dissapearing, and with some other known obstructions, not to be discussed here, dissapearing as well. We are therefore led to the following statement:

Conjecture 6.11 (Asymptotic Butson Conjecture (ABC))**.** *The following equivalences should hold, in an asymptotic sense, at $N>>0$,*

1. $H_N(2)\neq\emptyset\iff 4|N$,
2. $H_N(p^a)\neq\emptyset\iff p|N$, *for $p^a\geq 3$ prime power,*
3. $H_N(l)\neq\emptyset\iff\emptyset$, *for $l\in\mathbb N$ not a prime power,*

modulo the de Launey obstruction, $|d|^2=N^N$ for some $d\in\mathbb Z[e^{2\pi i/l}]$.

In short, our belief is that when imposing the condition $N>>0$, only the Sylvester, Butson and de Launey obstructions survive. This is of course something quite nice, but in what regards a possible proof, this looks difficult. Indeed, our above conjecture generalizes the HC in the $N>>0$ regime, which is so far something beyond reach.

One idea, however, in dealing with such questions, coming from the de Launey-Levin result from [59], is that of looking at the partial Butson matrices, at $N>>0$. Observe in particular that restricting the attention to the rectangular case, and this not even in the $N>>0$ regime, would make dissapear the de Launey obstruction from the ABC, which uses the orthogonality of all N rows. We will discuss this later on. For a number of related considerations, we refer as well to the papers [54], [57].

Getting away now from all these arithmetic difficulties, let us discuss now, following [17], the classification of the regular complex Hadamard matrices of small order. The definition here, which already appeared in the above, is as follows:

Definition 6.12. *A complex Hadamard matrix $H \in M_N(\mathbb{T})$ is called regular if the scalar products between rows decompose as sums of cycles.*

Our purpose in what follows will be that of showing that the notion of regularity can lead to full classification results at $N \leq 6$, and perhaps at $N = 7$ too, and all this while covering most of the interesting complex Hadamard matrices that we met, so far. As a first observation, supporting this last claim, we have the following result:

Proposition 6.13. *The following complex Hadamard matrices are regular:*

(1) *The matrices at $N \leq 5$, namely F_2, F_3, F_4^s, F_5.*
(2) *The main examples at $N = 6$, namely $F_6^{(rs)}, F_6^{(\frac{r}{s})}, H_6^q, T_6$.*
(3) *The main examples at $N = 7$, namely F_7, P_7^q.*

Proof. The Fourier matrices F_N are all regular, with the scalar products between rows appearing as certain sums of full sums of l-th roots of unity, with $l|N$. As for the other matrices appearing in the statement, with the convention that "cycle structure" means the lengths of the cycles in the regularity property, the situation is as follows:

(1) F_4^s has cycle structure $2 + 2$, and this because the verification of the Hadamard condition is always based on the formula $1 + (-1) = 0$, rotated by scalars.

(2) $F_6^{(rs)}, F_6^{(\frac{r}{s})}$ have mixed cycle structure $2 + 2 + 2/3 + 3$, in the sense that both cases appear, H_6^q has cycle structure $2 + 2 + 2$, and T_6 has cycle structure $3 + 3$.

(3) P_7^q has cycle structure $3+2+2$, its Hadamard property coming from $1+w+w^2 = 0$, with $w = e^{2\pi i/3}$, and from $1 + (-1) = 0$, applied twice, rotated by scalars. □

Let us discuss now the classification of regular matrices. We first have:

Theorem 6.14. *The regular Hadamard matrices at $N \leq 5$ are*

$$F_2, F_3, F_4^s, F_5$$

up to the equivalence relation for the complex Hadamard matrices.

Proof. This is something that we already know, coming from the classification results from section 5, and from Proposition 6.13 (1). However, and here comes our point, proving this result does not need in fact all this, the situation being as follows:

(1) At $N = 2$ the cycle structure can be only 2, and we obtain F_2.

(2) At $N = 3$ the cycle structure can be only 3, and we obtain F_3.

(3) At $N = 4$ the cycle structure can be only $2 + 2$, and we obtain F_4^s.

(4) At $N=5$ some elementary combinatorics shows that the cycle structure $3+2$ is excluded. Thus we are left with the cycle structure 5, and we obtain F_5. $\square$

Let us discuss now the classification at $N=6$. The result here, from [17], states that the matrices $F_6^{(rs)},F_6^{(\frac{r}{s})},H_6^q,T_6$ are the only solutions. The proof is quite long and technical, but we will present here its main ideas. Let us start with:

Proposition 6.15. *The regular Hadamard matrices at $N=6$ fall into 3 classes:*
1. *Cycle structure $3+3$, with T_6 being an example.*
2. *Cycle structure $2+2+2$, with H_6^q being an example.*
3. *Mixed cycle structure $3+3/2+2+2$, with $F_6^{(rs)},F_6^{(\frac{r}{s})}$ being examples.*

Proof. This is a bit of an empty statement, with the above (1,2,3) possibilities being the only ones, and with the various examples coming from Proposition 6.13 (2). $\square$

In order to do the classification, we must prove that the examples in (1,2,3) are the only ones. Let us start with the Tao matrix. The result here is as follows:

Proposition 6.16. *The Tao matrix, namely*

$$T_6=\begin{pmatrix}1&1&1&1&1&1\\ 1&1&w&w&w^2&w^2\\ 1&w&1&w^2&w^2&w\\ 1&w&w^2&1&w&w^2\\ 1&w^2&w^2&w&1&w\\ 1&w^2&w&w^2&w&1\end{pmatrix}$$

with $w=e^{2\pi i/3}$ is the only one with cycle structure $3+3$.

Proof. The proof of this fact, from [17], is quite long and technical, the idea being that of studying first the 3×6 case, then the 4×6 case, and finally the 6×6 case.

So, consider first a partial Hadamard matrix $A\in M_{3\times 6}(\mathbb T)$, with the scalar products between rows assumed to be all of type $3+3$.

By doing some elementary combinatorics, one can show that, modulo equivalence, either all the entries of A belong to $\mathbb Z_3=\{1,w,w^2\}$, or A has the following special form, for certain parameters $r,s\in\mathbb T$:

$$A=\begin{pmatrix}1&1&1&1&1&1\\ 1&w&w^2&r&wr&w^2r\\ 1&w^2&w&s&w^2s&ws\end{pmatrix}$$

With this result in hand, we can now investigate the 4×6 case.

Assume indeed that we have a partial Hadamard matrix $B\in M_{4\times 6}(\mathbb T)$, with the scalar products between rows assumed to be all of type $3+3$.

By looking at the 4 submatrices $A^{(1)}, A^{(2)}, A^{(3)}, A^{(4)}$ obtained from B by deleting one row, and applying the above 3×6 result, we are led, after doing some combinatorics, to the conclusion that all the possible parameters dissapear.

Thus, our matrix must be of the following type:

$$B \in M_{4\times 6}(\mathbb{Z}_3)$$

With this result in hand, we can now go for the general case. Indeed, an Hadamard matrix $M \in M_6(\mathbb{T})$ having cycle structure $3+3$ must be as follows:

$$M \in M_6(\mathbb{Z}_3)$$

But the study here is elementary, with T_6 as the only solution. See [17]. □

Regarding now the Haagerup matrix, the result is similar, as follows:

Proposition 6.17. *The Haagerup matrix, namely*

$$H_6^q = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & i & i & -i & -i \\ 1 & i & -1 & -i & q & -q \\ 1 & i & -i & -1 & -q & q \\ 1 & -i & \bar{q} & -\bar{q} & i & -1 \\ 1 & -i & -\bar{q} & \bar{q} & -1 & i \end{pmatrix}$$

with $q \in \mathbb{T}$ is the only one with cycle structure $2+2+2$.

Proof. The proof here, from [17], uses the same idea as in the proof of Proposition 6.16, namely a detailed combinatorial study, by increasing the number of rows.

First of all, the study of the 3×6 partial Hadamard matrices with cycle structure $2+2+2$ leads, up to equivalence, to the following 4 solutions, with $q \in \mathbb{T}$ being a parameter:

$$A_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -i & 1 & i & -1 & -1 \\ 1 & -1 & i & -i & q & -q \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & i & -1 & -i \\ 1 & -1 & q & -q & iq & -iq \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i & q & -q \\ 1 & -i & i & -1 & -q & q \end{pmatrix}$$

$$A_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i & q & -q \\ 1 & -1 & -q & -iq & iq & q \end{pmatrix}$$

With this result in hand, we can go directly for the 6×6 case.

Indeed, a careful examination of the 3×6 submatrices, and of the way that different parameters can overlap vertically, shows that our matrix must have a 3×3 block decomposition as follows:

$$M=\begin{pmatrix}A&B&C\\ D&xE&yF\\ G&zH&tI\end{pmatrix}$$

Here $A,\ldots,I$ are 2×2 matrices over $\{\pm 1,\pm i\}$, and x,y,z,t are in $\{1,q\}$. A more careful examination shows that the solution must be of the following form:

$$M=\begin{pmatrix}A&B&C\\ D&E&qF\\ G&qH&qI\end{pmatrix}$$

More precisely, the matrix must be as follows:

$$M=\begin{pmatrix}1&1&1&1&1&1\\ 1&1&-i&i&-1&-1\\ 1&i&-1&-i&-q&q\\ 1&-i&i&-1&-iq&iq\\ 1&-1&q&-iq&iq&-q\\ 1&-1&-q&iq&q&-iq\end{pmatrix}$$

But this matrix is equivalent to H_6^q, and we are done. See [17]. □

Regarding now the mixed case, where both $2+2+2$ and $3+3$ situations can appear, this is a bit more complicated. We can associate to any mixed Hadamard matrix $M\in M_6(\mathbb{C})$ its "row graph", having the 6 rows as vertices, and with each edge being called "binary" or "ternary", depending on whether the corresponding scalar product is of type $2+2+2$ or $3+3$. With this convention, we have the following result:

Proposition 6.18. *The row graph of a mixed matrix $M\in M_6(\mathbb{C})$ can be:*

(1) *Either the bipartite graph having 3 binary edges.*
(2) *Or the bipartite graph having 2 ternary triangles.*

Proof. This is once again something a bit technical, from [17], the idea being as follows. Let X be the row graph in the statement. By doing some combinatorics, of rather elementary type, we are led to the following conclusions about X:

– X has no binary triangle.
– X has no ternary square.
– X has at least one ternary triangle.

With these results in hand, we see that there are only two types of squares in our graph X, namely those having 1 binary edge and 5 ternary edges, and those consisting of a ternary triangle, connected to the 4-th point with 3 binary edges.

By looking at pentagons, then hexagons that can be built with these squares, we see that the above two types of squares cannot appear at the same time, at that at the level of hexagons, we have the two solutions in the statement. See [17]. □

We can now complete our classification at $N=6$, as follows:

Proposition 6.19. *The deformed Fourier matrices, namely*

$$F_6^{(rs)}=\begin{pmatrix}1&1&1&1&1&1\\1&w&w^2&1&w&w^2\\1&w^2&w&1&w^2&w\\ \\1&r&s&-1&-r&-s\\1&wr&w^2s&-1&-wr&-w^2s\\1&w^2r&ws&-1&-w^2r&-ws\end{pmatrix}$$

$$F_6^{(\frac{r}{s})}=\begin{pmatrix}1&1&1&1&1&1\\1&-1&1&-1&1&-1\\ \\1&r&w&wr&w^2&w^2r\\1&-r&w&-wr&w^2&-w^2r\\ \\1&s&w^2&w^2s&w&ws\\1&-s&w^2&-w^2s&w&-ws\end{pmatrix}$$

with $r,s\in\mathbb{T}$ are the only ones with mixed cycle structure.

Proof. According to Proposition 6.18, we have two cases:

(1) Assume first that the row graph is the bipartite one with 3 binary edges. By permuting the rows, the upper 4×6 submatrix of our matrix must be as follows:

$$B=\begin{pmatrix}1&1&1&1&1&1\\1&w&w^2&r&wr&w^2r\\1&w^2&w&s&w^2s&ws\\1&1&1&t&t&t\end{pmatrix}$$

Now since the scalar product between the first and the fourth row is binary, we must have $t=-1$, so the solution is:

$$B=\begin{pmatrix}1&1&1&1&1&1\\1&w&w^2&r&wr&w^2r\\1&w^2&w&s&w^2s&ws\\1&1&1&-1&-1&-1\end{pmatrix}$$

We can use the same argument for finding the fifth and sixth row, by arranging the matrix formed by the first three rows such as the second, respectively third row consist only of 1's. This will make appear some parameters of the form w, w^2, r, s in the extra row, and we obtain in this way a matrix which is equivalent to $F_6^{(rs)}$. See [17].

(2) Assume now that the row graph is the bipartite one with 2 ternary triangles. By permuting the rows, the upper 4×6 submatrix of our matrix must be as follows:

$$B=\begin{pmatrix}1&1&1&1&1&1\\ 1&1&w&w&w^2&w^2\\ 1&1&w^2&w^2&w&w\\ 1&-1&r&-r&s&-s\end{pmatrix}$$

We can use the same argument for finding the fifth and sixth row, and we conclude that the matrix is of the following type:

$$M=\begin{pmatrix}1&1&1&1&1&1\\ 1&1&w&w&w^2&w^2\\ 1&1&w^2&w^2&w&w\\ 1&-1&r&-r&s&-s\\ 1&-1&a&-a&b&-b\\ 1&-1&c&-c&d&-d\end{pmatrix}$$

Now since the last three rows must form a ternary triangle, we conclude that the matrix must be of the following form:

$$M=\begin{pmatrix}1&1&1&1&1&1\\ 1&1&w&w&w^2&w^2\\ 1&1&w^2&w^2&w&w\\ 1&-1&r&-r&s&-s\\ 1&-1&wr&-wr&w^2s&-w^2s\\ 1&-1&w^2r&-w^2r&ws&-ws\end{pmatrix}$$

But this matrix is equivalent to $F_6^{\binom{r}{s}}$, and we are done. See [17]. □

Summing up all the above, we have proved the following theorem, from [17]:

Theorem 6.20. *The regular complex Hadamard matrices at $N=6$ are:*

(1) *The deformations $F_6^{(rs)}, F_6^{\binom{r}{s}}$ of the Fourier matrix F_6.*
(2) *The Haagerup matrix H_6^q.*
(3) *The Tao matrix T_6.*

Proof. This follows indeed from the trichotomy from Proposition 6.15, and from the results in Proposition 6.16, Proposition 6.17 and Proposition 6.19. See [17]. □

All this is quite nice, and our belief is that the $N=7$ classification is doable as well. Here we have 3 possible cycle structures, namely $3+2+2$, $5+2$, 7, and some elementary number theory shows that $5+2$ is excluded, and that $3+2+2$ and 7 cannot interact. Thus we have a dichotomy, and our conjecture is as follows:

Conjecture 6.21. *The regular complex Hadamard matrices at $N = 7$ are:*

(1) *The Fourier matrix F_7.*
(2) *The Petrescu matrix P_7^q.*

Regarding (1), one can show indeed that F_7 is the only matrix having cycle structure 7, with this being related to more general results from [73]. As for (2), the problem is that of proving that P_7^q is the only matrix having cycle structure $3+2+2$. The computations here are unfortunately far more involved than those at $N = 6$, briefly presented above, and finishing the classification work here is not an easy question.

Besides the classification questions, there are as well a number of theoretical questions in relation with the notion of regularity, that we believe to be very interesting. We have for instance the following conjecture, going back to [17], and then to [30]:

Conjecture 6.22 (Regularity Conjecture)**.** *The following hold:*

(1) *Any Butson matrix $H \in M_N(\mathbb{C})$ is regular.*
(2) *Any regular matrix $H \in M_N(\mathbb{C})$ is an affine deformation of a Butson matrix.*

We refer to [17] and [30] for more on these topics.

As already mentioned above, after Conjecture 6.11, one way of getting away from these algebraic difficulties is by doing $N >> 0$ analysis for the partial Hadamard matrices, with counting results in the spirit of [59]. Following [10], let us start with:

Definition 6.23. *A partial Butson matrix (PBM) is a matrix*

$$H \in M_{M\times N}(\mathbb{Z}_q)$$

having its rows pairwise orthogonal, where $\mathbb{Z}_q \subset \mathbb{C}^\times$ is the group of q-roots of unity.

Two PBM are called equivalent if one can pass from one to the other by permuting the rows and columns, or by multiplying the rows and columns by numbers in $\mathbb{Z}_q$. Up to this equivalence, we can assume that H is dephased, in the sense that its first row consists of 1 entries only. We can also put H in "standard form", as follows:

Definition 6.24. *We say that $H \in M_{M\times N}(\mathbb{Z}_q)$ is in standard form if the low powers of*

$$w = e^{2\pi i/q}$$

are moved to the left as much as possible, by proceeding from top to bottom.

Let us first try to understand the case $M = 2$. Here a dephased partial Butson matrix $H \in M_{2\times N}(\mathbb{Z}_q)$ must look as follows, with $\lambda_i \in \mathbb{Z}_q$ satisfying $\lambda_1 + \ldots + \lambda_N = 0$:

$$H = \begin{pmatrix} 1 & \ldots & 1 \\ \lambda_1 & \ldots & \lambda_N \end{pmatrix}$$

With $q=p_1^{k_1}\ldots p_s^{k_s}$, we must have, according to Lam and Leung [90]:

$$N\in p_1\mathbb N+\ldots+p_s\mathbb N$$

Observe however that at $s\geq 2$ this obstruction dissapears at $N\geq p_1p_2$.

Let us discuss now the prime power case. We have:

Proposition 6.25. *When $q=p^k$ is a prime power, the standard form of the dephased partial Butson matrices at $M=2$ is*

$$H=\begin{pmatrix}1&1&\ldots&1&\ldots&\ldots&1&1&\ldots&1\\ \underbrace{1}_{a_1}&\underbrace{w}_{a_2}&\ldots&\underbrace{w^{q/p-1}}_{a_{q/p}}&\ldots&\ldots&\underbrace{w^{q-q/p}}_{a_1}&\underbrace{w^{q-q/p+1}}_{a_2}&\ldots&\underbrace{w^{q-1}}_{a_{q/p}}\end{pmatrix}$$

where $w=e^{2\pi i/q}$ and where $a_1,\ldots,a_{q/p}\in\mathbb N$ are multiplicities, summing up to N/p.

Proof. Indeed, it is well-known that for $q=p^k$ the solutions of $\lambda_1+\ldots+\lambda_N=0$ with $\lambda_i\in\mathbb Z_q$ are, up to permutations of the terms, exactly those in the statement. □

Now with Proposition 6.25 in hand, we can prove:

Theorem 6.26. *When $q=p^k$ is a prime power, the probability for a randomly chosen $M\in M_{2\times N}(\mathbb Z_q)$, with $N\in p\mathbb N$, $N\to\infty$, to be partial Butson is:*

$$P_2\simeq\sqrt{\frac{p^{2-\frac{q}{p}}q^{q-\frac{q}{p}}}{(2\pi N)^{q-\frac{q}{p}}}}$$

Proof. According to Proposition 6.25, we have the following formula:

$$\begin{aligned}P_2&=\frac{1}{q^N}\sum_{a_1+\ldots+a_{q/p}=N/p}\binom{N}{\underbrace{a_1\ldots a_1}_{p}\ldots\ldots\underbrace{a_{q/p}\ldots a_{q/p}}_{p}}\\&=\frac{1}{q^N}\binom{N}{\underbrace{N/p\ldots N/p}_{p}}\sum_{a_1+\ldots+a_{q/p}=N/p}\binom{N/p}{a_1\ldots a_{q/p}}^p\\&=\frac{1}{p^N}\binom{N}{\underbrace{N/p\ldots N/p}_{p}}\times\frac{1}{(q/p)^N}\sum_{a_1+\ldots+a_{q/p}=N/p}\binom{N/p}{a_1\ldots a_{q/p}}^p\end{aligned}$$

By using the standard estimate for multinomial coefficients from [115], explained in section 4 above, we obtain the formula in the statement. □

Let us discuss now the case where $M=2$ and $q=p_1^{k_1}p_2^{k_2}$ has two prime factors. We first examine the simplest such case, namely $q=p_1p_2$, with p_1,p_2 primes:

Proposition 6.27. *When $q = p_1 p_2$ is a product of distinct primes, the standard form of the dephased partial Butson matrices at $M = 2$ is*

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 & \ldots & \ldots & 1 & 1 & \ldots & 1 \\ \underbrace{1}_{A_{11}} & \underbrace{w}_{A_{12}} & \ldots & \underbrace{w^{p_2-1}}_{A_{1p_2}} & \ldots & \ldots & \underbrace{w^{q-p_2}}_{A_{p_1 1}} & \underbrace{w^{q-p_2+1}}_{A_{p_1 2}} & \ldots & \underbrace{w^{q-1}}_{A_{p_1 p_2}} \end{pmatrix}$$

where $w = e^{2\pi i/q}$, and $A \in M_{p_1 \times p_2}(\mathbb{N})$ is of the form $A_{ij} = B_i + C_j$, with $B_i, C_j \in \mathbb{N}$.

Proof. We use the fact that for $q = p_1 p_2$ any vanishing sum of q-roots of unity decomposes as a sum of cycles. Now if we denote by $B_i, C_j \in \mathbb{N}$ the multiplicities of the various p_2-cycles and p_1-cycles, then we must have $A_{ij} = B_i + C_j$, as claimed. □

Regarding now the matrices of type $A_{ij} = B_i + C_j$, when taking them over integers, $B_i, C_j \in \mathbb{Z}$, these form a vector space of dimension $d = p_1 + p_2 - 1$. Given $A \in M_{p_1 \times p_2}(\mathbb{Z})$, the "test" for deciding if we have $A_{ij} = B_i + C_j$ or not is:

$$A_{ij} + A_{kl} = A_{il} + A_{jk}$$

The problem comes of course from the assumption $B_i, C_j \geq 0$, which is quite a subtle one. In what follows we restrict the attention to the case $p_1 = 2$. Here we have:

Theorem 6.28. *For $q = 2p$ with $p \geq 3$ prime, P_2 equals the probability for a random walk on $\mathbb{Z}^p$ to end up on the diagonal, i.e. at a position of type $(t, \ldots, t)$, with $t \in \mathbb{Z}$.*

Proof. According to Proposition 6.27, we must understand the matrices $A \in M_{2 \times p}(\mathbb{N})$ which decompose as $A_{ij} = B_i + C_j$, with $B_i, C_j \geq 0$. But this is an easy task, because depending on A_{11} vs A_{21} we have 3 types of solutions, as follows:

$$\begin{pmatrix} a_1 & \ldots & a_p \\ a_1 & \ldots & a_p \end{pmatrix} \quad , \quad \begin{pmatrix} a_1 & \ldots & a_p \\ a_1 + t & \ldots & a_p + t \end{pmatrix} \quad , \quad \begin{pmatrix} a_1 + t & \ldots & a_p + t \\ a_1 & \ldots & a_p \end{pmatrix}$$

Here $a_i \geq 0$ and $t \geq 1$. Now since cases 2,3 contribute in the same way, we obtain:

$$\begin{aligned} P_2 &= \frac{1}{(2p)^N} \sum_{2\Sigma a_i = N} \binom{N}{a_1, a_1, \ldots, a_p, a_p} \\ &+ \frac{2}{(2p)^N} \sum_{t \geq 1} \sum_{2\Sigma a_i + pt = N} \binom{N}{a_1, a_1 + t, \ldots, a_p, a_p + t} \end{aligned}$$

We can write this formula in a more compact way, as follows:

$$P_2 = \frac{1}{(2p)^N} \sum_{t \in \mathbb{Z}} \sum_{2\Sigma a_i + p|t| = N} \binom{N}{a_1, a_1 + |t|, \ldots, a_p, a_p + |t|}$$

Now since the sum on the right, when rescaled by $\frac{1}{(2p)^N}$, is exactly the probability for a random walk on $\mathbb{Z}^p$ to end up at $(t, \ldots, t)$, this gives the result. □

Let us discuss now the exponents $q=3p$. The same method as in the proof of Theorem 6.28 works, with the "generic" solution for A being as follows:

$$A=\begin{pmatrix}a_1&\ldots&a_p\\ a_1+t&\ldots&a_p+t\\ a_1+s+t&\ldots&a_p+s+t\end{pmatrix}$$

Finally, regarding arbitrary exponents with two prime factors, we have:

Proposition 6.29. *When $q=p_1^{k_1}p_2^{k_2}$ has exactly two prime factors, the dephased partial Butson matrices at $M=2$ are indexed by the solutions of*

$$A_{ij,xy}=B_{ijy}+C_{jxy}$$

with $B_{ijy},C_{jxy}\in\mathbb N$, with $i\in\mathbb Z_{p_1}$, $j\in\mathbb Z_{p_1^{k_1-1}}$, $x\in\mathbb Z_{p_2}$, $y\in\mathbb Z_{p_2^{k_2-1}}$.

Proof. We follow the method in the proof of Proposition 6.27. First, according to [90], for $q=p_1^{k_1}p_2^{k_2}$ any vanishing sum of q-roots of unity decomposes as a sum of cycles.

Let us first work out a simple particular case, namely $q=4p$. Here the multiplicity matrices $A\in M_{4\times p}(\mathbb N)$ appear as follows:

$$A=\begin{pmatrix}B_1&\ldots&B_1\\ B_2&\ldots&B_2\\ B_3&\ldots&B_3\\ B_4&\ldots&B_4\end{pmatrix}+\begin{pmatrix}C_1&\ldots&C_p\\ D_1&\ldots&D_p\\ C_1&\ldots&C_p\\ D_1&\ldots&D_p\end{pmatrix}$$

Thus, if we use double binary indices for the elements of $\{1,2,3,4\}$, the condition is:

$$A_{ij,x}=B_{ij}+C_{jx}$$

The same method works for any exponent of type $q=p_1^{k_1}p_2^{k_2}$, the formula being:

$$A_{i_1\ldots i_{k_1},x_1\ldots x_{k_2}}=B_{i_1\ldots i_{k_1},x_2\ldots x_{k_2}}+C_{i_2\ldots i_{k_1},x_1\ldots x_{k_2}}$$

But this gives the formula in the statement, and we are done. $\square$

At $M=3$ now, we first restrict attention to the case where $q=p$ is prime. In this case, the general result in Proposition 6.29 becomes simply:

$$H=\begin{pmatrix}1&1&\ldots&1\\ \underbrace{1}_a&\underbrace{w}_a&\ldots&\underbrace{w^{p-1}}_a\end{pmatrix}$$

We call a matrix $A\in M_p(\mathbb N)$ "tristochastic" if the sums on its rows, columns and diagonals are all equal. Here, and in what follows, we call "diagonals" the main diagonal, and its $p-1$ translates to the right, obtained by using modulo p indices. With this convention, here is now the result at $M=3$:

Proposition 6.30. *For p prime, the standard form of the dephased PBM at $M=3$ is*

$$H=\begin{pmatrix}1&1&\ldots&1&\ldots&\ldots&1&1&\ldots&1\\ 1&1&\ldots&1&\ldots&\ldots&w^{p-1}&w^{p-1}&\ldots&w^{p-1}\\ \underbrace{1}_{A_{11}}&\underbrace{w}_{A_{12}}&\ldots&\underbrace{w^{p-1}}_{A_{1p}}&\ldots&\ldots&\underbrace{1}_{A_{p1}}&\underbrace{w}_{A_{p2}}&\ldots&\underbrace{w^{p-1}}_{A_{pp}}\end{pmatrix}$$

where $w=e^{2\pi i/p}$ and where $A\in M_p(\mathbb{N})$ is tristochastic, with sums N/p.

Proof. Consider a dephased matrix $H\in M_{3\times N}(\mathbb{Z}_p)$, written in standard form as in the statement. Then the orthogonality conditions between the rows are as follows:

$1\perp 2$ means $A_{11}+\ldots+A_{1p}=A_{21}+\ldots+A_{2p}=\ldots\ldots=A_{p1}+\ldots+A_{pp}$.

$1\perp 3$ means $A_{11}+\ldots+A_{p1}=A_{12}+\ldots+A_{p2}=\ldots\ldots=A_{1p}+\ldots+A_{pp}$.

$2\perp 3$ means $A_{11}+\ldots+A_{pp}=A_{12}+\ldots+A_{p1}=\ldots\ldots=A_{1p}+\ldots+A_{p,p-1}$.

Thus A must have constant sums on rows, columns and diagonals, as claimed. $\square$

It is quite unobvious on how to deal with the tristochastic matrices with bare hands. For the moment, let us just record a few elementary results:

Proposition 6.31. *For $p=2,3$, the standard form of the dephased PBM at $M=3$ is respectively as follows, with $w=e^{2\pi i/3}$ and $a+b+c=N/3$ at $p=3$:*

$$H=\begin{pmatrix}+&+&+&+\\ +&+&-&-\\ \underbrace{+}_{N/4}&\underbrace{-}_{N/4}&\underbrace{+}_{N/4}&\underbrace{-}_{N/4}\end{pmatrix}$$

$$H=\begin{pmatrix}1&1&1&1&1&1&1&1&1\\ 1&1&1&w&w&w&w^2&w^2&w^2\\ \underbrace{1}_{a}&\underbrace{w}_{b}&\underbrace{w^2}_{c}&\underbrace{1}_{b}&\underbrace{w}_{c}&\underbrace{w^2}_{a}&\underbrace{1}_{c}&\underbrace{w}_{a}&\underbrace{w^2}_{b}\end{pmatrix}$$

Also, for $p\geq 3$ prime and $N\in p\mathbb{N}$, there is at least one Butson matrix $H\in M_{3\times N}(\mathbb{Z}_p)$.

Proof. The idea is that the $p=2$ assertion follows from Proposition 6.30, and from the fact that the 2×2 tristochastic matrices are as follows:

$$A=\begin{pmatrix}a&a\\ a&a\end{pmatrix}$$

As for the $p=3$ assertion, once again the idea is that this follows from Proposition 6.30, and from the fact that the 3×3 tristochastic matrices are as follows:

$$A=\begin{pmatrix}a&b&c\\ b&c&a\\ c&a&b\end{pmatrix}$$

Indeed, the $p=2$ assertion is clear. Regarding now the $p=3$ assertion, consider an arbitary 3×3 bistochastic matrix, written as follows:

$$A=\begin{pmatrix}a&b&n-a-b\\ d&c&n-c-d\\ n-a-d&n-b-c&*\end{pmatrix}$$

Here $*=a+b+c+d-n$, but we won't use this value, because one of the 3 diagonal equations is redundant anyway. With these notations in hand, the conditions are:

$$b+(n-c-d)+(n-a-d)=n$$

$$(n-a-b)+d+(n-b-c)=n$$

Now since substracting these equations gives $b=d$, we obtain the result.

Regarding now the last assertion, consider the following $p\times p$ permutation matrix:

$$A=\begin{pmatrix}1&&&&\\ &&&&1\\ &&&1&\\ &&\ldots&&\\ &1&&&\end{pmatrix}$$

Since this matrix is tristochastic, for any $p\geq 3$ odd, this gives the result. $\square$

Regarding now the asymptotic count, we have here:

Theorem 6.32. *For $p=2,3$, the probability for a randomly chosen*

$$M\in M_{3\times N}(\mathbb Z_p)$$

with $N\in p\mathbb N$, $N\to\infty$, to be partial Butson is respectively given by

$$P_3^{(2)}\simeq\begin{cases}\frac{16}{\sqrt{(2\pi N)^3}}&\text{if }\ N\in 4\mathbb N\\ 0&\text{if }\ N\notin 4\mathbb N\end{cases}$$

at $p=2$, and

$$P_3^{(3)}\simeq\frac{243\sqrt{3}}{(2\pi N)^3}$$

at $p=3$. In addition, we have $P_3^{(p)}>0$ for any $N\in p\mathbb N$, for any $p\geq 3$ prime.

Proof. According to Proposition 6.31, and then to the Stirling formula, we have:

$$P_3^{(2)}=\frac{1}{4^N}\binom{N}{N/4,N/4,N/4,N/4}\simeq\frac{16}{\sqrt{(2\pi N)^3}}$$

The proof of the other assertions is standard as well. $\square$

It is possible to establish a few more results in this direction. See [10]. However, the main question remains that of adapting the methods in [90] to the root of unity case.

7. Geometry, defect

In this section and in the next one we discuss various geometric aspects of the complex Hadamard matrices. Let us recall that the complex Hadamard manifold appears as an intersection of smooth real algebraic manifolds, as follows:

$$X_N = M_N(\mathbb{T}) \cap \sqrt{N} U_N$$

We denote by X_p an unspecified neighborhood of a point in a manifold, $p \in X$. Also, for $q \in \mathbb{T}_1$, meaning that $q \in \mathbb{T}$ is close to 1, we define q^r with $r \in \mathbb{R}$ by $(e^{it})^r = e^{itr}$. With these conventions, we have the following result:

Proposition 7.1. *For $H \in X_N$ and $A \in M_N(\mathbb{R})$, the following are equivalent:*

(1) *The following is an Hadamard matrix, for any $q \in \mathbb{T}_1$:*
$$H_{ij}^q = H_{ij} q^{A_{ij}}$$

(2) *The following equations hold, for any $i \neq j$ and any $q \in \mathbb{T}_1$:*
$$\sum_k H_{ik} \bar{H}_{jk} q^{A_{ik} - A_{jk}} = 0$$

(3) *The following equations hold, for any $i \neq j$ and any $\varphi : \mathbb{R} \to \mathbb{C}$:*
$$\sum_k H_{ik} \bar{H}_{jk} \varphi(A_{ik} - A_{jk}) = 0$$

(4) *For any $i \neq j$ and any $r \in \mathbb{R}$, with $E_{ij}^r = \{k | A_{ik} - A_{jk} = r\}$, we have:*
$$\sum_{k \in E_{ij}^r} H_{ik} \bar{H}_{jk} = 0$$

Proof. These equivalences are all elementary, and can be proved as follows:

(1) $\iff$ (2) Indeed, the scalar products between the rows of H^q are:

$$< H_i^q, H_j^q >= \sum_k H_{ik} q^{A_{ik}} \bar{H}_{jk} \bar{q}^{A_{jk}} = \sum_k H_{ik} \bar{H}_{jk} q^{A_{ik} - A_{jk}}$$

(2) $\implies$ (4) This follows from the following formula, and from the fact that the power functions $\{q^r | r \in \mathbb{R}\}$ over the unit circle $\mathbb{T}$ are linearly independent:

$$\sum_k H_{ik} \bar{H}_{jk} q^{A_{ik} - A_{jk}} = \sum_{r \in \mathbb{R}} q^r \sum_{k \in E_{ij}^r} H_{ik} \bar{H}_{jk}$$

(4) $\implies$ (3) This follows from the following formula:

$$\sum_k H_{ik} \bar{H}_{jk} \varphi(A_{ik} - A_{jk}) = \sum_{r \in \mathbb{R}} \varphi(r) \sum_{k \in E_{ij}^r} H_{ik} \bar{H}_{jk}$$

(3) $\implies$ (2) This simply follows by taking $\varphi(r) = q^r$. $\square$

In order to understand the above deformations, which are "affine" in a certain sense, it is convenient to enlarge the attention to all types of deformations. We keep using the neighborhood notation X_p introduced above, and we consider functions of type $f : X_p \to Y_q$, which by definition satisfy $f(p) = q$. With these conventions, we have:

Definition 7.2. *Let $H \in M_N(\mathbb{C})$ be a complex Hadamard matrix.*

(1) *A deformation of H is a smooth function $f : \mathbb{T}_1 \to (X_N)_H$.*
(2) *The deformation is called "affine" if $f_{ij}(q) = H_{ij}q^{A_{ij}}$, with $A \in M_N(\mathbb{R})$.*
(3) *We call "trivial" the deformations of type $f_{ij}(q) = H_{ij}q^{a_i+b_j}$, with $a, b \in \mathbb{R}^N$.*

Here the adjective "affine" comes from $f_{ij}(e^{it}) = H_{ij}e^{iA_{ij}t}$, because the function $t \to A_{ij}t$ which produces the exponent is indeed affine. As for the adjective "trivial", this comes from the fact that $f(q) = (H_{ij}q^{a_i+b_j})_{ij}$ is obtained from H by multiplying the rows and columns by certain numbers in $\mathbb{T}$, so it is automatically Hadamard.

The basic example of an affine deformation comes from the Diţă deformations $H \otimes_Q K$, by taking all parameters $q_{ij} \in \mathbb{T}$ to be powers of $q \in \mathbb{T}$. As an example, here are the exponent matrices coming from the left and right Diţă deformations of $F_2 \otimes F_2$:

$$A_l = \begin{pmatrix} a&a&b&b\\ c&c&d&d\\ a&a&b&b\\ c&c&d&d \end{pmatrix} \quad , \quad A_r = \begin{pmatrix} a&b&a&b\\ a&b&a&b\\ c&d&c&d\\ c&d&c&d \end{pmatrix}$$

In order to investigate the above types of deformations, we will use the corresponding tangent vectors. So, let us recall that the manifold X_N is given by:

$$X_N = M_N(\mathbb{T}) \cap \sqrt{N}U_N$$

This observation leads to the following definition, where in the first part we denote by T_pX the tangent space to a point in a smooth manifold, $p \in X$:

Definition 7.3. *Associated to a point $H \in X_N$ are the following objects:*

(1) *The enveloping tangent space: $\widetilde{T}_HX_N = T_HM_N(\mathbb{T}) \cap T_H\sqrt{N}U_N$.*
(2) *The tangent cone T_HX_N: the set of tangent vectors to the deformations of H.*
(3) *The affine tangent cone $T_H^\circ X_N$: same as above, using affine deformations only.*
(4) *The trivial tangent cone $T_H^\times X_N$: as above, using trivial deformations only.*

Observe that $\widetilde{T}_HX_N, T_H^\times X_N$ are real linear spaces, and that $T_HX_N, T_H^\circ X_N$ are two-sided cones, in the sense that they satisfy the following condition:

$$\lambda \in \mathbb{R}, A \in T \implies \lambda A \in T$$

Observe also that we have inclusions of cones, as follows:

$$T_H^\times X_N \subset T_H^\circ X_N \subset T_HX_N \subset \widetilde{T}_HX_N$$

In more algebraic terms now, these various tangent cones are best described by the corresponding matrices, and we have here the following result:

Theorem 7.4. *The cones $T_H^\times X_N\subset T_H^\circ X_N\subset T_HX_N\subset\widetilde{T}_HX_N$ are as follows:*

(1) *$\widetilde{T}_HX_N$ can be identified with the linear space formed by the matrices $A\in M_N(\mathbb R)$ satisfying:*
$$\sum_kH_{ik}\bar{H}_{jk}(A_{ik}-A_{jk})=0$$
.

(2) *T_HX_N consists of those matrices $A\in M_N(\mathbb R)$ appearing as $A_{ij}=g_{ij}'(0)$, where $g:M_N(\mathbb R)_0\to M_N(\mathbb R)_0$ satisfies:*
$$\sum_kH_{ik}\bar{H}_{jk}e^{i(g_{ik}(t)-g_{jk}(t))}=0$$

(3) *$T_H^\circ X_N$ is formed by the matrices $A\in M_N(\mathbb R)$ satisfying the following condition, for any $i\neq j$ and any $q\in\mathbb T$:*
$$\sum_kH_{ik}\bar{H}_{jk}q^{A_{ik}-A_{jk}}=0$$

(4) *$T_H^\times X_N$ is formed by the matrices $A\in M_N(\mathbb R)$ which are of the form $A_{ij}=a_i+b_j$, for certain vectors $a,b\in\mathbb R^N$.*

Proof. All these assertions can be deduced by using basic differential geometry:

(1) This result is well-known, the idea being as follows. First, $M_N(\mathbb T)$ is defined by the algebraic relations $|H_{ij}|^2=1$, and with $H_{ij}=X_{ij}+iY_{ij}$ we have:
$$d|H_{ij}|^2=d(X_{ij}^2+Y_{ij}^2)=2(X_{ij}\dot{X}_{ij}+Y_{ij}\dot{Y}_{ij})$$

Consider now an arbitrary vector $\xi\in T_HM_N(\mathbb C)$, written as follows:
$$\xi=\sum_{ij}\alpha_{ij}\dot{X}_{ij}+\beta_{ij}\dot{Y}_{ij}$$

This vector belongs then to $T_HM_N(\mathbb T)$ if and only if we have $<\xi,d|H_{ij}|^2>=0$. We therefore obtain the following formula, for the tangent cone:
$$T_HM_N(\mathbb T)=\left\{\sum_{ij}A_{ij}(Y_{ij}\dot{X}_{ij}-X_{ij}\dot{Y}_{ij})\Big|A_{ij}\in\mathbb R\right\}$$

We also know that the rescaled unitary group $\sqrt{N}U_N$ is defined by the following algebraic relations, where $H_1,\ldots,H_N$ are the rows of H:
$$<H_i,H_j>=N\delta_{ij}$$

The relations $< H_i, H_i >= N$ being automatic for the matrices $H \in M_N(\mathbb{T})$, if for $i \neq j$ we let $L_{ij} =< H_i, H_j >$, then we have:

$$\widetilde{T}_H C_N = \left\{ \xi \in T_H M_N(\mathbb{T}) \Big| < \xi, \dot{L}_{ij} >= 0, \forall i \neq j \right\}$$

On the other hand, differentiating the formula of L_{ij} gives:

$$\dot{L}_{ij} = \sum_k (X_{ik} + iY_{ik})(\dot{X}_{jk} - i\dot{Y}_{jk}) + (X_{jk} - iY_{jk})(\dot{X}_{ik} + i\dot{Y}_{ik})$$

Now if we pick $\xi \in T_H M_N(\mathbb{T})$, written as above in terms of $A \in M_N(\mathbb{R})$, we obtain:

$$< \xi, \dot{L}_{ij} >= i \sum_k \bar{H}_{ik} H_{jk} (A_{ik} - A_{jk})$$

Thus we have reached to the description of $\widetilde{T}_H X_N$ in the statement.

(2) We pick an arbitrary deformation, and write it as $f_{ij}(e^{it}) = H_{ij} e^{i g_{ij}(t)}$. Observe first that the Hadamard condition corresponds to the equations in the statement, namely:

$$\sum_k H_{ik} \bar{H}_{jk} e^{i(g_{ik}(t) - g_{jk}(t))} = 0$$

Observe also that by differentiating this formula at $t = 0$, we obtain:

$$\sum_k H_{ik} \bar{H}_{jk} (g'_{ik}(0) - g'_{jk}(0)) = 0$$

Thus the matrix $A_{ij} = g'_{ij}(0)$ belongs indeed to $\widetilde{T}_H X_N$, so we obtain in this way a certain map, as follows:

$$T_H X_N \to \widetilde{T}_H X_N$$

In order to check that this map is indeed the correct one, we have to verify that, for any i, j, the tangent vector to our deformation is given by:

$$\xi_{ij} = g'_{ij}(0)(Y_{ij} \dot{X}_{ij} - X_{ij} \dot{Y}_{ij})$$

But this latter verification is just a one-variable problem. So, by dropping all i, j indices, which is the same as assuming $N = 1$, we have to check that for any point $H \in \mathbb{T}$, written $H = X + iY$, the tangent vector to the deformation $f(e^{it}) = He^{ig(t)}$ is:

$$\xi = g'(0)(Y\dot{X} - X\dot{Y})$$

But this is clear, because the unit tangent vector at $H \in \mathbb{T}$ is $\eta = -i(Y\dot{X} - X\dot{Y})$, and its coefficient coming from the deformation is:

$$(e^{ig(t)})'_{|t=0} = -ig'(0)$$

(3) Observe first that by taking the derivative at $q=1$ of the condition (2) in Proposition 7.1, of just by using the condition (3) there with the function $\varphi(r)=r$, we get:

$$\sum_k H_{ik}\bar{H}_{jk}\varphi(A_{ik}-A_{jk})=0$$

Thus we have a map $T_H^\circ X_N\to\widetilde{T}_H X_N$, and the fact that is map is indeed the correct one comes for instance from the computation in (2), with $g_{ij}(t)=A_{ij}t$.

(4) Observe first that the Hadamard matrix condition is satisfied, because:

$$\sum_k H_{ik}\bar{H}_{jk}q^{A_{ik}-A_{jk}}=q^{a_i-a_j}\sum_k H_{ik}\bar{H}_{jk}=\delta_{ij}$$

As for the fact that $T_H^\times X_N$ is indeed the space in the statement, this is clear. □

Let $Z_N\subset X_N$ be the real algebraic manifold formed by all the dephased $N\times N$ complex Hadamard matrices. Observe that we have a quotient map $X_N\to Z_N$, obtained by dephasing. With this notation, we have the following refinement of (4) above:

Proposition 7.5. *We have a direct sum decomposition of cones*

$$T_H^\circ X_N=T_H^\times X_N\oplus T_H^\circ Z_N$$

where at right we have the affine tangent cone to the dephased manifold $X_N\to Z_N$.

Proof. If we denote by $M_N^\circ(\mathbb{R})$ the set of matrices having 0 outside the first row and column, we have a direct sum decomposition, as follows:

$$\widetilde{T}_H^\circ X_N=M_N^\circ(\mathbb{R})\oplus\widetilde{T}_H^\circ Z_N$$

Now by looking at the affine cones, and using Theorem 7.4, this gives the result. □

As a concrete numerical invariant arising from all this, which can be effectively computed in many cases of interest, we have, following [129]:

Definition 7.6. *The real dimension $d(H)$ of the enveloping tangent space*

$$\widetilde{T}_H X_N=T_H M_N(\mathbb{T})\cap T_H\sqrt{N}U_N$$

is called undephased defect of a complex Hadamard matrix $H\in X_N$.

In view of Proposition 7.5, it is sometimes convenient to replace $d(H)$ by the related quantity $d'(H)=d(H)-2N+1$, called dephased defect of H. See [129]. In what follows we will rather use the quantity $d(H)$ defined above, which behaves better with respect to a number of operations, and simply call it "defect" of H.

We already know, from Theorem 7.4, what is the precise geometric meaning of the defect, and how to compute it. Let us record again these results, that we will use many times in what follows, in a slightly different form, closer to the spirit of [129]:

Theorem 7.7. *The defect $d(H)$ is the real dimension of the linear space*

$$\widetilde{T}_H X_N = \left\{ A \in M_N(\mathbb{R}) \Big| \sum_k H_{ik}\bar{H}_{jk}(A_{ik} - A_{jk}) = 0, \forall i, j \right\}$$

and the elements of this space are those making $H_{ij}^q = H_{ij} q^{A_{ij}}$ Hadamard at order 1.

Proof. Here the first assertion is something that we already know, from Theorem 7.4 (1), and the second assertion follows either from Theorem 7.4 and its proof, or directly from the definition of the enveloping tangent space $\widetilde{T}_H X_N$, as used in Definition 7.6. □

Here are a few basic properties of the defect:

Proposition 7.8. *Let $H \in X_N$ be a complex Hadamard matrix.*

1. *If $H \simeq \widetilde{H}$ then $d(H) = d(\widetilde{H})$.*
2. *We have $2N - 1 \leq d(H) \leq N^2$.*
3. *If $d(H) = 2N - 1$, the image of H in the dephased manifold $X_N \to Z_N$ is isolated.*

Proof. All these results are elementary, the proof being as follows:

(1) If we let $K_{ij} = a_i b_j H_{ij}$ with $|a_i| = |b_j| = 1$ be a trivial deformation of our matrix H, the equations for the enveloping tangent space for K are:

$$\sum_k a_i b_k H_{ik} \bar{a}_j \bar{b}_k \bar{H}_{jk}(A_{ik} - A_{jk}) = 0$$

By simplifying we obtain the equations for H, so $d(H)$ is invariant under trivial deformations. Since $d(H)$ is invariant as well by permuting rows or columns, we are done.

(2) Consider the inclusions $T_H^\times X_N \subset T_H X_N \subset \widetilde{T}_H X_N$. Since $\dim(T_H^\times X_N) = 2N - 1$, the inequality at left holds indeed. As for the inequality at right, this is clear.

(3) If $d(H) = 2N - 1$ then $T_H X_N = T_H^\times X_N$, so any deformation of H is trivial. Thus the image of H in the quotient manifold $X_N \to Z_N$ is indeed isolated, as stated. □

In order to deal with the real case, it is convenient to modify the general formula from Theorem 7.7, via a change of variables, as follows:

Proposition 7.9. *We have a linear space isomorphism as follows,*

$$\widetilde{T}_H X_N \simeq \left\{ E \in M_N(\mathbb{C}) \Big| E = E^*, (EH)_{ij}\bar{H}_{ij} \in \mathbb{R}, \forall i, j \right\}$$

the correspondences $A \to E$ and $E \to A$ being given by the formulae

$$E_{ij} = \sum_k H_{ik}\bar{H}_{jk}A_{ik} \quad , \quad A_{ij} = (EH)_{ij}\bar{H}_{ij}$$

with $A \in \widetilde{T}_H X_N$ being the usual components, from Theorem 7.7 above.

Proof. Given a matrix $A \in M_N(\mathbb{C})$, if we set $R_{ij} = A_{ij}H_{ij}$ and $E = RH^*$, the correspondence $A \to R \to E$ is then bijective onto $M_N(\mathbb{C})$, and we have:

$$E_{ij} = \sum_k H_{ik}\bar{H}_{jk}A_{ik}$$

In terms of these new variables, the equations in Theorem 7.7 become $E_{ij} = \bar{E}_{ji}$. Thus, when taking into account these conditions, we are simply left with the conditions $A_{ij} \in \mathbb{R}$. But these correspond to the conditions $(EH)_{ij}\bar{H}_{ij} \in \mathbb{R}$, as claimed. □

With the above result in hand, we can now compute the defect of the real Hadamard matrices. The result here, from [125], is as follows:

Theorem 7.10. *For any real Hadamard matrix $H \in M_N(\pm 1)$ we have*

$$\widetilde{T}_H X_N \simeq M_N(\mathbb{R})^{symm}$$

and so the corresponding defect is $d(H) = N(N+1)/2$.

Proof. We use Proposition 7.9. Since H is now real the condition $(EH)_{ij}\bar{H}_{ij} \in \mathbb{R}$ there simply tells us that E must be real, and this gives the result. □

As another computation now, let us discuss the case $N = 4$. Here we know from section 5 above that the only complex Hadamard matrices are, up to equivalence, the Diţă deformations of F_4. To be more precise, we have the following result:

Proposition 7.11. *The complex Hadamard matrices at $N = 4$ are, up to equivalence, the following matrices, appearing as Diţă deformations of F_4:*

$$F_{2,2}^q = \begin{pmatrix}1&1\\1&-1\end{pmatrix} \otimes_{\begin{pmatrix}1&1\\1&q\end{pmatrix}} \begin{pmatrix}1&1\\1&-1\end{pmatrix} = \begin{pmatrix}1&1&1&1\\1&-1&q&-q\\1&1&-1&-1\\1&-1&-q&q\end{pmatrix}$$

At $q \in \{1, i, -1, -i\}$ we obtain tensor products of Fourier matrices, as follows:

1. *At $q = 1$ we have $F_{2,2}^q = F_2 \otimes F_2$.*
2. *At $q = -1$ we have $F_{2,2}^q \simeq F_2 \otimes F_2$.*
3. *At $q = \pm i$ we have $F_{2,2}^q \simeq F_4$.*

Proof. The first assertion is something that we already know, from section 5 above. Regarding now the $q = 1, i, -1, -i$ specializations, the situation here is as follows:

(1) This is clear from definitions.

(2) This follows from (1), by permuting the third and the fourth columns:

$$F_{2,2}^{-1} = \begin{pmatrix}1&1&1&1\\1&-1&-1&1\\1&1&-1&-1\\1&-1&1&-1\end{pmatrix} \sim \begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix} = F_{2,2}^1$$

(3) This follows from the following computation:

$$F_{2,2}^{\pm i}=\begin{pmatrix}1&1&1&1\\1&-1&\pm i&\mp i\\1&1&-1&-1\\1&-1&\mp i&\pm i\end{pmatrix}\sim\begin{pmatrix}1&1&1&1\\1&i&-1&-i\\1&-1&1&-1\\1&-i&-1&i\end{pmatrix}=F_4$$

Here we have interchanged the second column with the third one in the case $q=i$, and we have used a cyclic permutation of the last 3 columns in the case $q=-i$. $\square$

Let us compute now the defect of the above matrices. We will work out everything in detail, as an illustration for how the equations in Theorem 7.7 work. The result is:

Theorem 7.12. *The defect of the* 4×4 *complex Hadamard matrices is given by*

$$d(F_{2,2}^q)=\begin{cases}10&(q=\pm 1)\\8&(q\neq\pm 1)\end{cases}$$

with $F_{2,2}^q$, *depending on* $q\in\mathbb{T}$, *being the matrix in Proposition 7.11.*

Proof. Our starting point are the equations in Theorem 7.7, namely:

$$\sum_h H_{ik}\bar{H}_{jk}(A_{ik}-A_{jk})=0$$

Since the $i>j$ equations are equivalent to the $i<j$ ones, and the $i=j$ equations are trivial, we just have to write down the equations corresponding to indices $i<j$. And, with $ij=01,02,03,12,13,23$, these equations are:

$$\begin{aligned}(A_{00}-A_{10})-(A_{01}-A_{11})+\bar{q}(A_{02}-A_{12})-\bar{q}(A_{03}-A_{13})&=0\\(A_{00}-A_{20})+(A_{01}-A_{21})-(A_{02}-A_{22})-(A_{03}-A_{23})&=0\\(A_{00}-A_{30})-(A_{01}-A_{31})-\bar{q}(A_{02}-A_{32})+\bar{q}(A_{03}-A_{33})&=0\\(A_{10}-A_{20})-(A_{11}-A_{21})-q(A_{12}-A_{22})+q(A_{13}-A_{23})&=0\\(A_{10}-A_{30})+(A_{11}-A_{31})-(A_{12}-A_{32})-(A_{13}-A_{33})&=0\\(A_{20}-A_{30})-(A_{21}-A_{31})+\bar{q}(A_{22}-A_{32})-\bar{q}(A_{23}-A_{33})&=0\end{aligned}$$

Assume first $q\neq\pm 1$. Then q is not real, and appears in 4 of the above equations. But these 4 equations can be written in the following way:

$$\begin{aligned}(A_{00}-A_{01})-(A_{10}-A_{11})+\bar{q}((A_{02}-A_{03})-(A_{12}-A_{13}))&=0\\(A_{00}-A_{01})-(A_{30}-A_{31})-\bar{q}((A_{02}-A_{03})-(A_{32}-A_{33}))&=0\\(A_{10}-A_{11})-(A_{20}-A_{21})-q((A_{12}-A_{13})-(A_{22}-A_{23}))&=0\\(A_{20}-A_{21})-(A_{30}-A_{31})+\bar{q}((A_{22}-A_{23})-(A_{32}-A_{33}))&=0\end{aligned}$$

Now since the unknowns are real, and q is not, we conclude that the terms between braces in the left part must be all equal, and that the same must happen at right:

$$\begin{aligned}A_{00}-A_{01} &= A_{10}-A_{11}=A_{20}-A_{21}=A_{30}-A_{31}\\ A_{02}-A_{03} &= A_{12}-A_{13}=A_{22}-A_{23}=A_{32}-A_{33}\end{aligned}$$

Thus, the equations involving q tell us that A must be of the following form:

$$A=\begin{pmatrix}a&a+x&e+y&e\\ b&b+x&f+y&f\\ c&c+x&g+y&g\\ d&d+x&h+y&h\end{pmatrix}$$

Let us plug now these values in the remaining 2 equations. We obtain:

$$\begin{aligned}a-c+a+x-c-x-e-y+g+y-e+g &= 0\\ b-d+b+x-d-x-f-y+h+y-f+h &= 0\end{aligned}$$

Thus we must have $a+g=c+e$ and $b+h=d+f$, which are independent conditions. We conclude that the dimension of the space of solutions is $10-2=8$, as claimed.

Assume now $q=\pm 1$. For simplicity we set $q=1$, and we compute the dephased defect. The dephased equations, obtained by setting $A_{i0}=A_{0j}=0$ in our system, are:

$$\begin{aligned}A_{11}-A_{12}+A_{13} &= 0\\ -A_{21}+A_{22}+A_{23} &= 0\\ A_{31}+A_{32}-A_{33} &= 0\\ -A_{11}+A_{21}-A_{12}+A_{22}+A_{13}-A_{23} &= 0\\ A_{11}-A_{31}-A_{12}+A_{32}-A_{13}+A_{33} &= 0\\ -A_{21}+A_{31}+A_{22}-A_{32}-A_{23}+A_{33} &= 0\end{aligned}$$

The first three equations tell us that our matrix must be of the following form:

$$A=\begin{pmatrix}a&a+b&b\\ c+d&c&d\\ e&f&e+f\end{pmatrix}$$

Now by plugging these values in the last three equations, these become:

$$\begin{aligned}-a+c+d-a-b+c+b-d &= 0\\ a-e-a-b+f-b+e+f &= 0\\ -c-d+e+c-f-d+e+f &= 0\end{aligned}$$

Thus we must have $a=c$, $b=f$, $d=e$, and since these conditions are independent, the dephased defect is 3, and so the undephased defect is $3+7=10$, as claimed. $\square$

Let us discuss now, following [8], [83], [104], [105], [129] the computation of the defect of the Fourier matrix F_G. As a first result on this subject, we have, following [129]:

Theorem 7.13. *For a Fourier matrix $F=F_G$, the matrices $A\in\widetilde{T}_FX_N$ with $N=|G|$, are those of the form $A=PF^*$, with $P\in M_N(\mathbb C)$ satisfying*

$$P_{ij}=P_{i+j,j}=\bar{P}_{i,-j}$$

where the indices i,j are by definition taken in the group G.

Proof. We use Theorem 7.7. By decomposing our group as $G=\mathbb Z_{N_1}\times\ldots\times\mathbb Z_{N_r}$ we can assume $F=F_{N_1}\otimes\ldots\otimes F_{N_r}$. Thus with $w_k=e^{2\pi i/k}$ we have:

$$F_{i_1\ldots i_r,j_1\ldots j_r}=(w_{N_1})^{i_1j_1}\ldots(w_{N_r})^{i_rj_r}$$

With $N=N_1\ldots N_r$ and $w=e^{2\pi i/N}$, we obtain:

$$F_{i_1\ldots i_r,j_1\ldots j_r}=w^{\left(\frac{i_1j_1}{N_1}+\ldots+\frac{i_rj_r}{N_r}\right)N}$$

Thus the matrix of our system is given by:

$$F_{i_1\ldots i_r,k_1\ldots k_r}\bar{F}_{j_1\ldots j_r,k_1\ldots k_r}=w^{\left(\frac{(i_1-j_1)k_1}{N_1}+\ldots+\frac{(i_r-j_r)k_r}{N_r}\right)N}$$

Now by plugging in a multi-indexed matrix A, our system becomes:

$$\sum_{k_1\ldots k_r}w^{\left(\frac{(i_1-j_1)k_1}{N_1}+\ldots+\frac{(i_r-j_r)k_r}{N_r}\right)N}(A_{i_1\ldots i_r,k_1\ldots k_r}-A_{j_1\ldots j_r,k_1\ldots k_r})=0$$

Now observe that in the above formula we have in fact two matrix multiplications, so our system can be simply written as:

$$(AF)_{i_1\ldots i_r,i_1-j_1\ldots i_r-j_r}-(AF)_{j_1\ldots j_r,i_1-j_1\ldots i_r-j_r}=0$$

Now recall that our indices have a "cyclic" meaning, so they belong in fact to the group G. So, with $P=AF$, and by using multi-indices, our system is simply:

$$P_{i,i-j}=P_{j,i-j}$$

With $i=I+J,j=I$ we obtain the condition $P_{I+J,J}=P_{IJ}$ in the statement. In addition, $A=PF^*$ must be a real matrix. But, if we set $\tilde{P}_{ij}=\bar{P}_{i,-j}$, we have:

$$\begin{aligned}\overline{(PF^*)}_{i_1\ldots i_r,j_1\ldots j_r}&=\sum_{k_1\ldots k_r}\bar{P}_{i_1\ldots i_r,k_1\ldots k_r}F_{j_1\ldots j_r,k_1\ldots k_r}\\&=\sum_{k_1\ldots k_r}\tilde{P}_{i_1\ldots i_r,-k_1\ldots -k_r}(F^*)_{-k_1\ldots -k_r,j_1\ldots j_r}\\&=(\tilde{P}F^*)_{i_1\ldots i_r,j_1\ldots j_r}\end{aligned}$$

Thus we have $\overline{PF^*}=\tilde{P}F^*$, so the fact that the matrix PF^* is real, which means by definition that we have $\overline{PF^*}=PF^*$, can be reformulated as $\tilde{P}F^*=PF^*$, and hence as $\tilde{P}=P$. So, we obtain the conditions $P_{ij}=\bar{P}_{i,-j}$ in the statement. ∎

We can now compute the defect, and we are led to the following formula:

Theorem 7.14. *The defect of a Fourier matrix F_G is given by*

$$d(F_G)=\sum_{g\in G}\frac{|G|}{ord(g)}$$

and equals as well the number of 1 *entries of the matrix F_G.*

Proof. According to the formula $A=PF^*$ from Theorem 7.13, the defect $d(F_G)$ is the dimension of the real vector space formed by the matrices $P\in M_N(\mathbb{C})$ satisfying:

$$P_{ij}=P_{i+j,j}=\bar{P}_{i,-j}$$

Here, and in what follows, the various indices $i,j,\ldots$ will be taken in G. Now the point is that, in terms of the columns of our matrix P, the above conditions are:

(1) The entries of the j-th column of P, say C, must satisfy $C_i=C_{i+j}$.

(2) The $(-j)$-th column of P must be conjugate to the j-th column of P.

Thus, in order to count the above matrices P, we can basically fill the columns one by one, by taking into account the above conditions. In order to do so, consider the subgroup $G_2=\{j\in G|2j=0\}$, and then write G as a disjoint union, as follows:

$$G=G_2\sqcup X\sqcup(-X)$$

With this notation, the algorithm is as follows. First, for any $j\in G_2$ we must fill the j-th column of P with real numbers, according to the periodicity rule:

$$C_i=C_{i+j}$$

Then, for any $j\in X$ we must fill the j-th column of P with complex numbers, according to the same periodicity rule $C_i=C_{i+j}$. And finally, once this is done, for any $j\in X$ we just have to set the $(-j)$-th column of P to be the conjugate of the j-th column.

So, let us compute the number of choices for filling these columns. Our claim is that, when uniformly distributing the choices for the j-th and $(-j)$-th columns, for $j\notin G_2$, there are exactly $[G:<j>]$ choices for the j-th column, for any j. Indeed:

(1) For the j-th column with $j\in G_2$ we must simply pick N real numbers subject to the condition $C_i=C_{i+j}$ for any i, so we have indeed $[G:<j>]$ such choices.

(2) For filling the j-th and $(-j)$-th column, with $j\notin G_2$, we must pick N complex numbers subject to the condition $C_i=C_{i+j}$ for any i. Now since there are $[G:<j>]$ choices for these numbers, so a total of $2[G:<j>]$ choices for their real and imaginary parts, on average over $j,-j$ we have $[G:<j>]$ choices, and we are done again.

Summarizing, the dimension of the vector space formed by the matrices P, which is equal to the number of choices for the real and imaginary parts of the entries of P, is:

$$d(F_G)=\sum_{j\in G}[G:<j>]$$

But this is exactly the number in the statement. Regarding now the second assertion, according to the definition of F_G, the number of 1 entries of F_G is given by:

$$\begin{aligned}\#(1\in F_G) &= \#\left\{(g,\chi)\in G\times\widehat{G}\Big|\chi(g)=1\right\}\\ &= \sum_{g\in G}\#\left\{\chi\in\widehat{G}\Big|\chi(g)=1\right\}\\ &= \sum_{g\in G}\frac{|G|}{ord(g)}\end{aligned}$$

Thus, the second assertion follows from the first one. □

Let us finish now the work, and explicitely compute the defect of F_G. It is convenient to consider the following quantity, which behaves better:

$$\delta(G)=\sum_{g\in G}\frac{1}{ord(g)}$$

As a first example, consider a cyclic group $G=\mathbb{Z}_N$, with $N=p^a$ power of a prime. The count here is very simple, over sets of elements having a given order:

$$\delta(\mathbb{Z}_{p^a})=1+(p-1)p^{-1}+(p^2-p)p^{-2}+\ldots+(p^a-p^{a-1})p^{-1}=1+a-\frac{a}{p}$$

In order to extend this kind of count to the general abelian case, we use two ingredients. First is the following result, which splits the computation over isotypic components:

Proposition 7.15. *For any finite groups G,H we have:*

$$\delta(G\times H)\geq\delta(G)\delta(H)$$

In addition, if $(|G|,|H|)=1$, we have equality.

Proof. Indeed, we have the following estimate:

$$\delta(G\times H)=\sum_{gh}\frac{1}{[ord(g),ord(h)]}\geq\sum_{gh}\frac{1}{ord(g)\cdot ord(h)}=\delta(G)\delta(H)$$

In the case $(|G|,|H|)=1$ the least common multiple appearing on the right becomes a product, $[ord(g),ord(h)]=ord(g)\cdot ord(h)$, so we have equality, as desired. □

We deduce from this that we have the following result:

Proposition 7.16. *For a finite abelian group G we have*

$$\delta(G)=\prod_p\delta(G_p)$$

where G_p with $G=\times_pG_p$ are the isotypic components of G.

Proof. This is clear from Proposition 7.15, the order of G_p being a power of p. □

As an illustration for the above results, we can recover in this way the following key defect computation, from [130]:

Theorem 7.17. *The defect of a usual Fourier matrix F_N is given by*

$$d(F_N) = N \prod_{i=1}^{s} \left(1 + a_i - \frac{a_i}{p_i}\right)$$

where $N = p_1^{a_1} \ldots p_s^{a_s}$ is the decomposition of N into prime factors.

Proof. The underlying group here is the cyclic group $G = \mathbb{Z}_N$, whose isotypic components are the following cyclic groups:

$$G_{p_i} = \mathbb{Z}_{p_i^{a_i}}$$

By applying now Proposition 7.16, and by using the computation for cyclic p-groups performed before Proposition 7.15, we obtain:

$$d(F_N) = N \prod_{i=1}^{s} \left(1 + p_i^{-1}(p_i - 1)a_i\right)$$

But this is exactly the formula in the statement. □

Now back to the general case, where we have an arbitrary Fourier matrix F_G, we will need, as a second ingredient for our computation, the following result:

Proposition 7.18. *For the p-groups, the quantities*

$$c_k = \# \left\{ g \in G \middle| ord(g) \leq p^k \right\}$$

are multiplicative, in the sense that $c_k(G \times H) = c_k(G)c_k(H)$.

Proof. Indeed, for a product of p-groups we have:

$$\begin{aligned} c_k(G \times H) &= \# \left\{ (g,h) \middle| ord(g,h) \leq p^k \right\} \\ &= \# \left\{ (g,h) \middle| ord(g) \leq p^k, ord(h) \leq p^k \right\} \\ &= \# \left\{ g \middle| ord(g) \leq p^k \right\} \# \left\{ h \middle| ord(h) \leq p^k \right\} \end{aligned}$$

We recognize at right $c_k(G)c_k(H)$, and we are done. □

Let us compute now δ in the general isotypic case:

Proposition 7.19. *For $G = \mathbb{Z}_{p^{a_1}} \times \ldots \times \mathbb{Z}_{p^{a_r}}$ with $a_1 \leq a_2 \leq \ldots \leq a_r$ we have*

$$\delta(G) = 1 + \sum_{k=1}^{r} p^{(r-k)a_{k-1} + (a_1 + \ldots + a_{k-1}) - 1}(p^{r-k+1} - 1)[a_k - a_{k-1}]_{p^{r-k}}$$

with the convention $a_0 = 0$, and with the notation $[a]_q = 1 + q + q^2 + \ldots + q^{a-1}$.

Proof. First, in terms of the numbers c_k, we have:

$$\delta(G)=1+\sum_{k\geq1}\frac{c_k-c_{k-1}}{p^k}$$

In the case of a cyclic group $G=\mathbb{Z}_{p^a}$ we have $c_k=p^{\min(k,a)}$. Thus, in the general isotypic case $G=\mathbb{Z}_{p^{a_1}}\times\ldots\times\mathbb{Z}_{p^{a_r}}$ we have:

$$c_k=p^{\min(k,a_1)}\ldots p^{\min(k,a_r)}=p^{\min(k,a_1)+\ldots+\min(k,a_r)}$$

Now observe that the exponent on the right is a piecewise linear function of k. More precisely, by assuming $a_1\leq a_2\leq\ldots\leq a_r$ as in the statement, the exponent is linear on each of the intervals $[0,a_1],[a_1,a_2],\ldots,[a_{r-1},a_r]$. So, the quantity $\delta(G)$ to be computed will be 1 plus the sum of $2r$ geometric progressions, 2 for each interval.

In practice now, the numbers c_k are as follows:

$$c_0=1,c_1=p^r,c_2=p^{2r},\ldots,c_{a_1}=p^{ra_1},$$

$$c_{a_1+1}=p^{a_1+(r-1)(a_1+1)},c_{a_1+2}=p^{a_1+(r-1)(a_1+2)},\ldots,c_{a_2}=p^{a_1+(r-1)a_2},$$

$$c_{a_2+1}=p^{a_1+a_2+(r-2)(a_2+1)},c_{a_2+2}=p^{a_1+a_2+(r-2)(a_2+2)},\ldots,c_{a_3}=p^{a_1+a_2+(r-2)a_3},$$

$$\vdots$$

$$c_{a_{r-1}+1}=p^{a_1+\ldots+a_{r-1}+(a_{r-1}+1)},c_{a_{r-1}+2}=p^{a_1+\ldots+a_{r-1}+(a_{r-1}+2)},\ldots,c_{a_r}=p^{a_1+\ldots+a_r}$$

Now by separating the positive and negative terms in the above formula of $\delta(G)$, we have indeed $2r$ geometric progressions to be summed, as follows:

$$\begin{aligned}\delta(G)\ &=\ 1+(p^{r-1}+p^{2r-2}+p^{3r-3}+\ldots+p^{a_1r-a_1})\\&\quad-(p^{-1}+p^{r-2}+p^{2r-3}+\ldots+p^{(a_1-1)r-a_1})\\&\quad+(p^{(r-1)(a_1+1)-1}+p^{(r-1)(a_1+2)-2}+\ldots+p^{a_1+(r-2)a_2})\\&\quad-(p^{a_1r-a_1-1}+p^{(r-1)(a_1+1)-2}+\ldots+p^{a_1+(r-1)(a_2-1)-a_2})\\&\quad\vdots\\&\quad+(p^{a_1+\ldots+a_{r-1}}+p^{a_1+\ldots+a_{r-1}}+\ldots+p^{a_1+\ldots+a_{r-1}})\\&\quad-(p^{a_1+\ldots+a_{r-1}-1}+p^{a_1+\ldots+a_{r-1}-1}+\ldots+p^{a_1+\ldots+a_{r-1}-1})\end{aligned}$$

Now by performing all the sums, we obtain:

$$\begin{aligned}\delta(G) &= 1 + p^{-1}(p^r - 1)\frac{p^{(r-1)a_1} - 1}{p^{r-1} - 1}\\ &\quad + p^{(r-2)a_1+(a_1-1)}(p^{r-1} - 1)\frac{p^{(r-2)(a_2-a_1)} - 1}{p^{r-2} - 1}\\ &\quad + p^{(r-3)a_2+(a_1+a_2-1)}(p^{r-2} - 1)\frac{p^{(r-3)(a_3-a_2)} - 1}{p^{r-3} - 1}\\ &\quad \vdots\\ &\quad + p^{a_1+\ldots+a_{r-1}-1}(p-1)(a_r - a_{r-1})\end{aligned}$$

By looking now at the general term, we get the formula in the statement. □

Let us go back now to the general defect formula in Theorem 7.14. By putting it together with the various results above, we obtain:

Theorem 7.20. *For a finite abelian group G, decomposed as $G = \times_p G_p$, we have*

$$d(F_G) = |G| \prod_p \left(1 + \sum_{k=1}^r p^{(r-k)a_{k-1}+(a_1+\ldots+a_{k-1})-1}(p^{r-k+1} - 1)[a_k - a_{k-1}]_{p^{r-k}} \right)$$

where $a_0 = 0$ and $a_1 \leq a_2 \leq \ldots \leq a_r$ are such that $G_p = \mathbb{Z}_{p^{a_1}} \times \ldots \times \mathbb{Z}_{p^{a_r}}$.

Proof. Indeed, we know from Theorem 7.14 that we have:

$$d(F_G) = |G|\delta(G)$$

The result follows then from Proposition 7.16 and Proposition 7.19. □

Let us prove now, following the paper of Nicoara and White [105], that for the Fourier matrices the defect is "attained", in the sense that the deformations at order 0 are true deformations, at order ∞. This is something quite surprising, and non-trivial.

Let us begin with some generalities. We first recall that we have:

Proposition 7.21. *The unitary matrices $U \in U_N$ around 1 are of the form*

$$U = e^A$$

with A being an antihermitian matrix, $A = -A^*$, around 0.

Proof. This is something well-known. Indeed, assuming that a matrix A is antihermitian, $A = -A^*$, the matrix $U = e^A$ follows to be unitary:

$$UU^* = e^A(e^A)^* = e^A e^{A^*} = e^A e^{-A} = 1$$

As for the converse, this follows either by using a dimension argument, which shows that the space of antihermitian matrices is the correct one, or by diagonalizing U. □

Now back to the Hadamard matrices, we will need to rewrite a part of the basic theory of the defect, using deformations of type $t \to U_tH$. First, we have:

Theorem 7.22. *Assume that $H \in M_N(\mathbb{C})$ is Hadamard, let $A \in M_N(\mathbb{C})$ be antihermitian, and consider the matrix UH, where $U = e^{tA}$, with $t \in \mathbb{R}$.*

(1) *UH is Hadamard when, for any p, q:*

$$\Big|\sum_{rs} H_{rq}\bar{H}_{sq}(e^{tA})_{pr}(e^{-tA})_{sp}\Big| = 1$$

(2) *UH is Hadamard at order 0 when, for any p, q:*

$$|(AH)_{pq}| = 1$$

Proof. We already know that UH is unitary, so we must find the conditions which guarantee that we have $UH \in M_N(\mathbb{T})$, in general, and then at order 0.

(1) We have the following computation, valid for any unitary U:

$$\begin{aligned}
|(UH)_{pq}|^2 &= (UH)_{pq}\overline{(UH)_{pq}} \\
&= (UH)_{pq}(H^*U^*)_{qp} \\
&= \sum_{rs} U_{pr}H_{rq}(H^*)_{qs}(U^*)_{sp} \\
&= \sum_{rs} H_{rq}\bar{H}_{sq}U_{pr}\bar{U}_{ps}
\end{aligned}$$

Now with $U = e^{tA}$ as in the statement, we obtain:

$$|(e^{tA}H)_{pq}|^2 = \sum_{rs} H_{rq}\bar{H}_{sq}(e^{tA})_{pr}(e^{-tA})_{sp}$$

Thus, we are led to the conclusion in the statement.

(2) The derivative of the function computed above, taken at 0, is as follows:

$$\begin{aligned}
\frac{\partial|(e^{tA}H)_{pq}|^2}{\partial t}_{|t=0} &= \sum_{rs} H_{rq}\bar{H}_{sq}(e^{tA}A)_{pr}(-e^{tA}A)_{sp\,|t=0} \\
&= \sum_{rs} H_{rq}\bar{H}_{sq}A_{pr}(-A)_{sp} \\
&= \sum_{r} A_{pr}H_{rq}\sum_{s}(H^*)_{qs}(A^*)_{sp} \\
&= (AH)_{pq}(H^*A^*)_{qp} \\
&= |(AH)_{pq}|^2
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

In the Fourier matrix case we can go beyond this, and we have:

Proposition 7.23. *Given a Fourier matrix $F_G \in M_G(\mathbb{C})$, and an antihermitian matrix $A \in M_G(\mathbb{C})$, the matrix $H = UF_G$, where $U = e^{tA}$ with $t \in \mathbb{R}$, is Hadamard when*

$$\left|\sum_s \sum_m \frac{t^m}{m!} \sum_{k+l=m} \binom{m}{l} \sum_s A^k_{p,s+n}(-A)^l_{sp}\right| = \delta_{n0}$$

for any p, with the indices being $k, l, m \in \mathbb{N}$, and $n, p, s \in G$.

Proof. According to the formula in the proof of Theorem 7.22 (1), we have:

$$\begin{aligned}
|(UF_G)_{pq}|^2 &= \sum_{rs} (F_G)_{rq}(\overline{F_G})_{sq}(e^{tA})_{pr}(e^{-tA})_{sp}\\
&= \sum_{rs} < r, q >< -s, q > (e^{tA})_{pr}(e^{-tA})_{sp}\\
&= \sum_{rs} < r - s, q > (e^{tA})_{pr}(e^{-tA})_{sp}
\end{aligned}$$

By setting $n = r - s$, can write this formula in the following way:

$$\begin{aligned}
|(UF_G)_{pq}|^2 &= \sum_{ns} < n, q > (e^{tA})_{p,s+n}(e^{-tA})_{sp}\\
&= \sum_n < n, q > \sum_s (e^{tA})_{p,s+n}(e^{-tA})_{sp}
\end{aligned}$$

Since this quantity must be 1 for any q, we must have:

$$\sum_s (e^{tA})_{p,s+n}(e^{-tA})_{sp} = \delta_{n0}$$

On the other hand, we have the following computation:

$$\begin{aligned}
\sum_s (e^{tA})_{p,s+n}(e^{-tA})_{sp} &= \sum_s \sum_{kl} \frac{(tA)^k_{p,s+n}}{k!} \cdot \frac{(-tA)^l_{sp}}{l!}\\
&= \sum_s \sum_{kl} \frac{1}{k!l!} \sum_s (tA)^k_{p,s+n}(-tA)^l_{sp}\\
&= \sum_s \sum_{kl} \frac{t^{k+l}}{k!l!} \sum_s A^k_{p,s+n}(-A)^l_{sp}\\
&= \sum_s \sum_m t^m \sum_{k+l=m} \frac{1}{k!l!} \sum_s A^k_{p,s+n}(-A)^l_{sp}\\
&= \sum_s \sum_m \frac{t^m}{m!} \sum_{k+l=m} \binom{m}{l} \sum_s A^k_{p,s+n}(-A)^l_{sp}
\end{aligned}$$

Thus, we are led to the conclusion in the statement. $\square$

Following [105], let us construct now the deformations. The result here is something quite surprising, which came a long time after the original defect paper [129], and even more time after the early computations in [83]:

Theorem 7.24. *Let G be a finite abelian group, and for any $g,h\in G$, let us set:*

$$B_{pq}=\begin{cases}1&\text{if }\exists k\in\mathbb N,p=h^kg,q=h^{k+1}g\\0&\text{otherwise}\end{cases}$$

When $(g,h)\in G^2$ range in suitable cosets, the unitary matrices

$$e^{it(B+B^t)}F_G\quad,\quad e^{t(B-B^t)}F_G$$

are both Hadamard, and make the defect of F_G to be attained.

Proof. The proof of this result, from [105], is quite long and technical, based on the Fourier computation from Proposition 7.23 above, the idea being as follows:

(1) First of all, an elementary algebraic study shows that when $(g,h)\in G^2$ range in some suitable cosets, coming from the proof of Theorem 7.14, the various matrices $B=B^{gh}$ constructed above are distinct, the matrices $A=i(B+B^t)$ and $A'=B-B^t$ are linearly independent, and the number of such matrices equals the defect of F_G.

(2) It is also standard to check that each $B=(B_{pq})$ is a partial isometry, and that B^k,B^{*k} are given by simple formulae. With this ingredients in hand, the Hadamard property follows from the Fourier computation from the proof of Proposition 7.23. Indeed, we can compute the exponentials there, and eventually use the binomial formula.

(3) Finally, the matrices in the statement can be shown to be non-equivalent, and this is something more technical, for which we refer to [105]. With this last ingredient in hand, a comparison with Theorem 7.14 shows that the defect of F_G is indeed attained, in the sense that all order 0 deformations are actually true deformations. See [105]. □

Finally, let us mention that [105] was written in terms of subfactor-theoretic commuting squares, with a larger class of squares actually under investigation. We will discuss the relation between Hadamard matrices and commuting squares in sections 12-16 below.

8. Special matrices

We have seen in the previous section that the defect theory from [129] can be successfully applied to the real Hadamard matrices, and to the generalized Fourier matrices. Following [4], [8], [9], [30], [97], [129], [130], we discuss here a number of more specialized questions, once again in relation with the defect, regarding the following types of matrices:

(1) The tensor products.
(2) The Diţă deformations of such tensor products.
(3) The Butson and the regular matrices.
(4) The master Hadamard matrices.
(5) The McNulty-Weigert matrices.
(6) The partial Hadamard matrices.

Let us begin with the tensor products. We have here the following result:

Proposition 8.1. *For a tensor product $L = H \otimes K$ we have*

$$d(L) \geq d(H)d(K)$$

coming from an inclusion of linear spaces, as follows:

$$\widetilde{T}_H X_M \otimes \widetilde{T}_K X_N \subset \widetilde{T}_L X_{MN}$$

Proof. For a tensor product $A = B \otimes C$, we have the following formula:

$$\begin{aligned}&\sum_{kc}(H\otimes K)_{ia,kc}\overline{(H\otimes K)}_{jb,kc}A_{ia,kc}\\ =&\sum_k H_{ik}\bar{H}_{jk}B_{ik}\sum_c K_{ac}\bar{K}_{bc}C_{ac}\end{aligned}$$

We have as well the following formula:

$$\begin{aligned}&\sum_{kc}(H\otimes K)_{ia,kc}\overline{(H\otimes K)}_{jb,kc}A_{jb,kc}\\ =&\sum_k H_{ik}\bar{H}_{jk}B_{jk}\sum_c K_{ac}\bar{K}_{bc}C_{bc}\end{aligned}$$

Now by assuming $B \in \widetilde{T}_H X_M$ and $C \in \widetilde{T}_K X_N$, the two quantities on the right are equal. Thus we have indeed $A \in \widetilde{T}_L X_{MN}$, and we are done. $\square$

Observe that we do not have equality in the tensor product estimate, even in very simple cases. For instance if we consider two Fourier matrices F_2, we obtain:

$$d(F_2 \otimes F_2) = 10 > 9 = d(F_2)^2$$

In fact, besides the isotypic decomposition results from section 7 above, valid for the Fourier matrices, there does not seem to be anything conceptual on this subject. We will be back to this, however, in Theorem 8.3 below, with a slight advance on all this.

In general, the computation of the defect for the Diţă deformations is a difficult question. Our only result here concerns the case when the deformation matrix is generic:

Definition 8.2. *A rectangular matrix $Q \in M_{M\times N}(\mathbb{T})$ is called "dephased and elsewhere generic" if the entries on its first row and column are all equal to 1, and the remaining $(M-1)(N-1)$ entries are algebrically independent over $\mathbb{Q}$.*

Here the last condition takes of course into account the fact that the entries of Q themselves have modulus 1, the independence assumption being modulo this fact. With this convention made, we have the following result, from [9]:

Theorem 8.3. *Assume that $H \in X_M, K \in X_N$ are dephased, of Butson type, and that $Q \in M_{M\times N}(\mathbb{T})$ is dephased and elsewhere generic. We have then*

$$A = (A_{ia,kc}) \in \widetilde{T}_{H\otimes_Q K} X_{MN}$$

when the following equations are satisfied,

$$A^{ij}_{ac} = A^{ij}_{bc}$$

$$A^{ij}_{ac} = \overline{A^{ji}_{ac}}$$

$$(A^{ii}_{xy})_{xy} \in \widetilde{T}_K X_N$$

for any a, b, c and $i \neq j$, where:

$$A^{ij}_{ac} = \sum_k H_{ik}\bar{H}_{jk} A_{ia,kc}$$

Proof. Consider the standard system of equations for the enveloping tangent space in the statement, namely:

$$\sum_{kc} (H \otimes_Q K)_{ia,kc} \overline{(H \otimes_Q K)}_{jb,kc} (A_{ia,kc} - A_{jb,kc}) = 0$$

We have the following formula:

$$(H \otimes_Q K)_{ia,jb} = q_{ib} H_{ij} K_{ab}$$

Thus, our system of equations is:

$$\sum_c q_{ic}\bar{q}_{jc} K_{ac}\bar{K}_{bc} \sum_k H_{ik}\bar{H}_{jk}(A_{ia,kc} - A_{jb,kc}) = 0$$

Consider now the variables in the statement, namely:

$$A^{ij}_{ac} = \sum_k H_{ik}\bar{H}_{jk} A_{ia,kc}$$

The conjugates of these variables are given by:

$$\begin{aligned}\overline{A_{ac}^{ij}} &= \sum_k \bar{H}_{ik}H_{jk}A_{ia,kc}\\ &= \sum_k H_{jk}\bar{H}_{ik}A_{ia,kc}\end{aligned}$$

Thus, in terms of these variables, our system becomes simply:

$$\sum_c q_{ic}\bar{q}_{jc}K_{ac}\bar{K}_{bc}(A_{ac}^{ij} - \overline{A_{bc}^{ji}}) = 0$$

More precisely, the above equations must hold for any i, j, a, b. By distinguishing now two cases, depending on whether i, j are equal or not, the situation is as follows:

(1) Case $i \neq j$. In this case, let us look at the row vector of parameters, namely:

$$(q_{ic}\bar{q}_{jc})_c = (1, q_{i1}\bar{q}_{j1}, \ldots, q_{iM}\bar{q}_{jM})$$

Now since Q was assumed to be dephased and elsewhere generic, and because of our assumption $i \neq j$, the entries of the above vector are linearly independent over $\bar{\mathbb{Q}}$. But, since by linear algebra we can restrict attention to the computation of the solutions over $\bar{\mathbb{Q}}$, the $i \neq j$ part of our system simply becomes:

$$A_{ac}^{ij} = \overline{A_{bc}^{ji}} \quad , \quad \forall a, b, c, \forall i \neq j$$

Now by making now a, b, c vary, we are led to the following equations:

$$A_{ac}^{ij} = A_{bc}^{ij}, \quad A_{ac}^{ij} = \overline{A_{ac}^{ji}}, \quad \forall a, b, c, i \neq j$$

(2) Case $i = j$. In this case the q parameters from our equations cancel, and our equations become:

$$\sum_c K_{ac}\bar{K}_{bc}(A_{ac}^{ii} - \overline{A_{bc}^{ii}}) = 0, \quad \forall a, b, c, i$$

Now observe that we have:

$$A_{ac}^{ii} = \sum_k A_{ia,kc}$$

Thus, our equations become:

$$\sum_c K_{ac}\bar{K}_{bc}(A_{ac}^{ii} - A_{bc}^{ii}) = 0, \quad \forall a, b, c, i$$

But these are precisely the equations for the space $\widetilde{T}_K X_N$, and we are done. $\square$

Let us go back now to the usual tensor product situation, and look at the affine cones. The problem here is that of finding the biggest subcone of $T^\circ_{H\otimes K}X_{MN}$, obtained by gluing $T^\circ_H X_M, T^\circ_K X_N$. Our answer here, which takes into account the two "semi-trivial" cones coming from the left and right Diţă deformations, is as follows:

Theorem 8.4. *The cones $T_H^\circ X_M=\{B\}$ and $T_K^\circ X_N=\{C\}$ glue via the formulae*
$$A_{ia,jb}=\lambda B_{ij}+\psi_jC_{ab}+X_{ia}+Y_{jb}+F_{aj}$$
$$A_{ia,jb}=\phi_bB_{ij}+\mu C_{ab}+X_{ia}+Y_{jb}+E_{ib}$$
producing in this way two subcones of the affine cone $T_{H\otimes K}^\circ X_{MN}=\{A\}$.

Proof. Indeed, the idea is that X_{ia},Y_{jb} are the trivial parameters, and that E_{ib},F_{aj} are the Diţă parameters. Given a matrix $A=(A_{ia,jb})$, consider the following quantity:
$$P=\sum_{kc}H_{ik}\bar{H}_{jk}K_{ac}\bar{K}_{bc}q^{A_{ia,kc}-A_{jb,kc}}$$

Let us prove now the first statement, namely that for any choice of matrices $B\in T_H^\circ X_M,C\in T_H^\circ X_N$ and of parameters $\lambda,\psi_j,X_{ia},Y_{jb},F_{aj}$, the first matrix $A=(A_{ia,jb})$ constructed in the statement belongs indeed to $T_{H\otimes K}^\circ X_{MN}$. We have:
$$A_{ia,kc}=\lambda B_{ik}+\psi_kC_{ac}+X_{ia}+Y_{kc}+F_{ak}$$
$$A_{jb,kc}=\lambda B_{jk}+\psi_kC_{bc}+X_{jb}+Y_{kc}+F_{bk}$$

Now by substracting these equations, we obtain:
$$A_{ia,kc}-A_{jb,kc}=\lambda(B_{ik}-B_{jk})+\psi_k(C_{ac}-C_{bc})+(X_{ia}-X_{jb})+(F_{ak}-F_{bk})$$

It follows that the above quantity P is given by:
$$\begin{aligned}P&=\sum_{kc}H_{ik}\bar{H}_{jk}K_{ac}\bar{K}_{bc}q^{\lambda(B_{ik}-B_{jk})+\psi_k(C_{ac}-C_{bc})+(X_{ia}-X_{jb})+(F_{ak}-F_{bk})}\\&=q^{X_{ia}-X_{jb}}\sum_kH_{ik}\bar{H}_{jk}q^{F_{ak}-F_{bk}}q^{\lambda(B_{ik}-B_{jk})}\sum_cK_{ac}\bar{K}_{bc}(q^{\psi_k})^{C_{ac}-C_{bc}}\\&=\delta_{ab}q^{X_{ia}-X_{ja}}\sum_kH_{ik}\bar{H}_{jk}(q^\lambda)^{B_{ik}-B_{jk}}\\&=\delta_{ab}\delta_{ij}\end{aligned}$$

We conclude that we have, as claimed:
$$A\in T_{H\otimes K}^\circ X_{MN}$$

In the second case now, the proof is similar. First, we have:
$$A_{ia,kc}=\phi_cB_{ik}+\mu C_{ac}+X_{ia}+Y_{kc}+E_{ic}$$
$$A_{jb,kc}=\phi_cB_{jk}+\mu C_{bc}+X_{jb}+Y_{kc}+E_{jc}$$

Thus by substracting, we obtain:
$$A_{ia,kc}-A_{jb,kc}=\phi_c(B_{ik}-B_{jk})+\mu(C_{ac}-C_{bc})+(X_{ia}-X_{jb})+(E_{ic}-E_{jc})$$

It follows that the above quantity P is given by:

$$\begin{aligned}P &= \sum_{kc} H_{ik}\bar{H}_{jk}K_{ac}\bar{K}_{bc}q^{\phi_c(B_{ik}-B_{jk})+\mu(C_{ac}-C_{bc})+(X_{ia}-X_{jb})+(E_{ic}-E_{jc})}\\ &= q^{X_{ia}-X_{jb}}\sum_c K_{ac}\bar{K}_{bc}q^{E_{ic}-E_{jc}}q^{\mu(C_{ac}-C_{bc})}\sum_k H_{ik}\bar{H}_{jk}(q^{\phi_c})^{B_{ik}-B_{jk}}\\ &= \delta_{ij}q^{X_{ia}-X_{ib}}\sum_c K_{ac}\bar{K}_{bc}(q^{\mu})^{C_{ac}-C_{bc}}\\ &= \delta_{ij}\delta_{ab}\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

We believe Theorem 8.4 above to be "optimal", in the sense that nothing more can be said about the affine tangent space $T^\circ_{H\otimes K}X_{MN}$, in the general case. See [9].

Let us discuss now some rationality questions, in relation with:

Definition 8.5. *The rational defect of $H\in X_N$ is the following number:*

$$d_{\mathbb{Q}}(H)=\dim_{\mathbb{Q}}(\widetilde{T}_HC_N\cap M_N(\mathbb{Q}))$$

The vector space on the right will be called rational enveloping tangent space at H.

As a first observation, this notion can be extended to all the tangent cones at H, and by using an arbitrary field $\mathbb{K}\subset\mathbb{C}$ instead of $\mathbb{Q}$. Indeed, we can set:

$$T^*_HX_N(\mathbb{K})=T^*_HX_N\cap M_N(\mathbb{K})$$

However, in what follows we will be interested only in the objects constructed in Definition 8.5. It follows from definitions that $d_{\mathbb{Q}}(H)\leq d(H)$, and we have:

Conjecture 8.6 (Rationality)**.** *For the Butson matrices we have:*

$$d_{\mathbb{Q}}(H)=d(H)$$

That is, for such matrices, the defect equals the rational defect.

More generally, we believe that the above equality should hold in the regular case. However, since the regular case is not known to fully cover the Butson matrix case, as explained in section 6, we prefer to state our conjecture as above. As a first piece of evidence now, we have the following elementary result:

Theorem 8.7. *The rationality conjecture holds for $H\in H_N(l)$ with $l=2,3,4,6$.*

Proof. Let us recall that the equations for the enveloping tangent space are:

$$\sum_k H_{ik}\bar{H}_{jk}(A_{ik}-A_{jk})=0$$

With these equations in hand, the proof goes as follows:

Case $l=2$. Here the above equations are all real, and have ± 1 coefficients, so in particular, have rational coefficients.

Case $l=3$. Here we can use the fact that, with $w=e^{2\pi i/3}$, the real solutions of $x+wy+w^2z=0$ are those satisfying $x=y=z$. We conclude that once again our system, after some manipulations, is equivalent to a real system having rational coefficients.

Case $l=4$. Here the coefficients are $1, i, -1, -i$, so by taking the real and imaginary parts, we reach once again to system with rational coefficients.

Case $l=6$. Here the study is similar to the study at $l=3$.

Thus, in all cases under investigation, $l=2,3,4,6$, we have a real system with rational coefficients, and the result follows from standard linear algebra. $\square$

Observe that the method in the above proof cannot work at $l=5$, where the equation $a+wb+w^2c+w^3d+w^4e=0$ with $w=e^{2\pi i/5}$ and $a,b,c,d,e\in\mathbb{R}$ can have "exotic" solutions. We refer to [9] for more on these topics, including more evidence for Conjecture 8.6.

Let us discuss now defect computations for an interesting class of Hadamard matrices, namely the "master" ones, introduced in [4]:

Definition 8.8. *A master Hadamard matrix is an Hadamard matrix of the form*

$$H_{ij}=\lambda_i^{n_j}$$

with $\lambda_i\in\mathbb{T}, n_j\in\mathbb{R}$. The associated "master function" is:

$$f(z)=\sum_j z^{n_j}$$

Observe that with $\lambda_i=e^{im_i}$ we have $H_{ij}=e^{im_in_j}$. The basic example of such a matrix is the Fourier matrix F_N, having master function as follows:

$$f(z)=\frac{z^N-1}{z-1}$$

Observe that, in terms of f, the Hadamard condition on H is simply:

$$f\left(\frac{\lambda_i}{\lambda_j}\right)=N\delta_{ij}$$

These matrices were introduced in [4], the motivating remark there being the fact that the following operator defines a representation of the Temperley-Lieb algebra [135]:

$$R=\sum_{ij}e_{ij}\otimes\Lambda^{n_i-n_j}$$

At the level of examples, the first observation, from [4], is that the standard 4×4 complex Hadamard matrices are, with 2 exceptions, master Hadamard matrices:

Proposition 8.9. *The following complex Hadamard matrix, with $|q| = 1$,*

$$F_{2,2}^q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & q & -1 & -q \\ 1 & -q & -1 & q \end{pmatrix}$$

is a master Hadamard matrix, for any $q \neq \pm 1$.

Proof. We use the exponentiation convention $(e^{it})^r = e^{itr}$, for $t \in [0, 2\pi)$ and $r \in \mathbb{R}$. Since we have $q^2 \neq 1$, we can find $k \in \mathbb{R}$ such that:

$$q^{2k} = -1$$

In terms of this parameter $k \in \mathbb{R}$, our matrix becomes:

$$F_{2,2}^q = \begin{pmatrix} 1^0 & 1^1 & 1^{2k} & 1^{2k+1} \\ (-1)^0 & (-1)^1 & (-1)^{2k} & (-1)^{2k+1} \\ q^0 & q^1 & q^{2k} & q^{2k+1} \\ (-q)^0 & (-q)^1 & (-q)^{2k} & (-q)^{2k+1} \end{pmatrix}$$

Now let us pick $\lambda \neq 1$ and write, by using our exponentiation convention above:

$$1 = \lambda^x \quad , \quad -1 = \lambda^y$$

$$q = \lambda^z \quad , \quad -q = \lambda^t$$

But this gives the formula in the statement. $\square$

Observe that the above result shows that any Hamadard matrix at $N \leq 5$ is master Hadamard. We have the following generalization of it, once again from [4]:

Theorem 8.10. *The deformed Fourier matrices $F_M \otimes_Q F_N$ are master Hadamard, for any $Q \in M_{M \times N}(\mathbb{T})$ of the form*

$$Q_{ib} = q^{i(Np_b + b)}$$

where $q = e^{2\pi i/MNk}$ with $k \in \mathbb{N}$, and $p_0, \ldots, p_{N-1} \in \mathbb{R}$.

Proof. The main construction in [4], in connection with deformations, that we will follow here, is, in terms of master functions, as follows:

$$f(z) = f_M(z^{Nk}) f_N(z)$$

Here $k \in \mathbb{N}$, and the functions on the right are by definition as follows:

$$f_M(z) = \sum_i z^{Mr_i + i}$$

$$f_N(z) = \sum_a z^{Np_a + a}$$

We use the eigenvalues $\lambda_{ia}=q^iw^a$, where $w=e^{2\pi i/N}$, and where $q^{Nk}=\nu$, where $\nu^M=1$. We have $f(z)=f_M(z^{Nk})f_N(z)$, so the exponents are:

$$n_{jb}=Nk(Mr_j+j)+Np_b+b$$

Thus the associated master Hadamard matrix is given by:

$$\begin{aligned}H_{ia,jb}&=(q^iw^a)^{Nk(Mr_j+j)+Np_b+b}\\&=\nu^{ij}q^{i(Np_b+b)}w^{a(Np_b+b)}\\&=\nu^{ij}w^{ab}q^{i(Np_b+b)}\end{aligned}$$

Now let us recall that we have the following formula:

$$(F_M\otimes F_N)_{ia,jb}=\nu^{ij}w^{ab}$$

Thus we have as claimed $H=F_M\otimes_Q F_N$, with:

$$Q_{ib}=q^{i(Np_b+b)}$$

Observe that Q itself is a "master matrix", because the indices split. □

In view of the above examples, and of the lack of other known examples of master Hadamard matrices, he following conjecture was made in [4]:

Conjecture 8.11 (Master Hadamard Conjecture)**.** *The master Hadamard matrices appear as Diţă deformations of F_N.*

There is a relation here with the notions of defect and isolation, that we would like to discuss now. First, we have the following defect computation:

Theorem 8.12. *The defect of a master Hadamard matrix is given by*

$$d(H)=\dim_{\mathbb R}\left\{B\in M_N(\mathbb C)\Big|\bar{B}=\frac{1}{N}BL,(BR)_{i,ij}=(BR)_{j,ij}\ \forall i,j\right\}$$

where the matrices on the right are given by

$$L_{ij}=f\left(\frac{1}{\lambda_i\lambda_j}\right)\quad,\quad R_{i,jk}=f\left(\frac{\lambda_j}{\lambda_i\lambda_k}\right)$$

with f being the master function.

Proof. The first order deformation equations are as follows:

$$\sum_k H_{ik}\bar{H}_{jk}(A_{ik}-A_{jk})=0$$

With $H_{ij}=\lambda_i^{n_j}$ we have the following formula:

$$H_{ij}\bar{H}_{jk}=\left(\frac{\lambda_i}{\lambda_j}\right)^{n_k}$$

Thus, the defect is given by the following formula:

$$d(H)=\dim_{\mathbb{R}}\left\{A\in M_N(\mathbb{R})\Big|\sum_kA_{ik}\left(\frac{\lambda_i}{\lambda_j}\right)^{n_k}=\sum_kA_{jk}\left(\frac{\lambda_i}{\lambda_j}\right)^{n_k}\ \forall i,j\right\}$$

Now, pick $A\in M_N(\mathbb{C})$ and set $B=AH^t$. We have the following formula:

$$A=\frac{1}{N}B\bar{H}$$

We have the following computation:

$$\begin{aligned}A\in M_N(\mathbb{R})&\iff B\bar{H}=\bar{B}H\\&\iff \bar{B}=\frac{1}{N}B\bar{H}H^*\end{aligned}$$

On the other hand, the matrix on the right is given by:

$$\begin{aligned}(\bar{H}H^*)_{ij}&=\sum_k\bar{H}_{ik}\bar{H}_{jk}\\&=\sum_k(\lambda_i\lambda_j)^{-n_k}\\&=L_{ij}\end{aligned}$$

Thus $A\in M_N(\mathbb{R})$ if and only the condition $\bar{B}=\frac{1}{N}BL$ in the statement is satisfied. Regarding now the second condition on A, observe that with $A=\frac{1}{N}B\bar{H}$ we have:

$$\begin{aligned}\sum_kA_{ik}\left(\frac{\lambda_i}{\lambda_j}\right)^{n_k}&=\frac{1}{N}\sum_{ks}B_{is}\left(\frac{\lambda_i}{\lambda_j\lambda_s}\right)^{n_k}\\&=\frac{1}{N}\sum_sB_{is}R_{s,ij}\\&=\frac{1}{N}(BR)_{i,ij}\end{aligned}$$

Thus the second condition on A reads $(BR)_{i,ij}=(BR)_{j,ij}$, which gives the result. □

In view of the above results, a conjecture would be that the only isolated master Hadamard matrices are the Fourier matrices F_p, with p prime. We refer here to [30].

Let us discuss now yet another interesting construction of complex Hadamard matrices, due to McNulty and Weigert [97]. The matrices constructed there generalize the Tao matrix T_6, and usually have the interesting feature of being isolated. The construction in [97] uses the theory of MUB, as developed in [36], [64], but we will follow here a more direct approach, from [30]. The starting observation from [97] is as follows:

Theorem 8.13. *Assuming that $K \in M_N(\mathbb{C})$ is Hadamard, so is the matrix*

$$H_{ia,jb} = \frac{1}{\sqrt{Q}} K_{ij} (L_i^* R_j)_{ab}$$

provided that $\{L_1, \ldots, L_N\} \subset \sqrt{Q} U_Q$ and $\{R_1, \ldots, R_N\} \subset \sqrt{Q} U_Q$ are such that

$$\frac{1}{\sqrt{Q}} L_i^* R_j \in \sqrt{Q} U_Q$$

with $i, j = 1, \ldots, N$, are complex Hadamard.

Proof. The check of the unitarity is done as follows:

$$\begin{aligned} < H_{ia}, H_{kc} > &= \frac{1}{Q} \sum_{jb} K_{ij} (L_i^* R_j)_{ab} \bar{K}_{kj} \overline{(L_k^* R_j)}_{cb} \\ &= \sum_j K_{ij} \bar{K}_{kj} (L_i^* L_k)_{ac} \\ &= N \delta_{ik} (L_i^* L_k)_{ac} \\ &= N Q \delta_{ik} \delta_{ac} \end{aligned}$$

The entries being in addition on the unit circle, we are done. □

As input for the above, we can use the following well-known Fourier construction:

Proposition 8.14. *For $q \geq 3$ prime, the matrices*

$$\{F_q, DF_q, \ldots, D^{q-1} F_q\}$$

where F_q is the Fourier matrix, and where

$$D = diag\left(1, 1, w, w^3, w^6, w^{10}, \ldots, w^{\frac{q^2-1}{8}}, \ldots, w^{10}, w^6, w^3, w\right)$$

with $w = e^{2\pi i/q}$, are such that $\frac{1}{\sqrt{q}} E_i^* E_j$ is complex Hadamard, for any $i \neq j$.

Proof. With $0, 1, \ldots, q-1$ as indices, the formula of the above matrix D is:

$$D_c = w^{0+1+\ldots+(c-1)} = w^{\frac{c(c-1)}{2}}$$

Since we have $\frac{1}{\sqrt{q}} E_i^* E_j \in \sqrt{q} U_q$, we just need to check that these matrices have entries belonging to $\mathbb{T}$, for any $i \neq j$. With $k = j - i$, these entries are given by:

$$\begin{aligned} \frac{1}{\sqrt{q}} (E_i^* E_j)_{ab} &= \frac{1}{\sqrt{q}} (F_q^* D^k F_q)_{ab} \\ &= \frac{1}{\sqrt{q}} \sum_c w^{c(b-a)} D_c^k \end{aligned}$$

Now observe that with $s=b-a$, we have the following formula:

$$\begin{aligned}\left|\sum_c w^{cs}D_c^k\right|^2 &= \sum_{cd} w^{cs-ds}w^{\frac{c(c-1)}{2}\cdot k-\frac{d(d-1)}{2}\cdot k}\\ &= \sum_{cd} w^{(c-d)\left(\frac{c+d-1}{2}\cdot k+s\right)}\\ &= \sum_{de} w^{e\left(\frac{2d+e-1}{2}\cdot k+s\right)}\\ &= \sum_e\left(w^{\frac{e(e-1)}{2}\cdot k+es}\sum_d w^{edk}\right)\\ &= \sum_e w^{\frac{e(e-1)}{2}\cdot k+es}\cdot q\delta_{e0}\\ &= q\end{aligned}$$

Thus the entries are on the unit circle, and we are done. □

We recall that the Legendre symbol is defined as follows:

$$\left(\frac{s}{q}\right)=\begin{cases}0 & \text{if } s=0\\ 1 & \text{if } \exists\,\alpha, s=\alpha^2\\ -1 & \text{if } \nexists\,\alpha, s=\alpha^2\end{cases}$$

With this convention, we have the following result from [30], following [97]:

Proposition 8.15. *The following matrices,*

$$G_k=\frac{1}{\sqrt{q}}F_q^*D^kF_q$$

with the matrix D being as above,

$$D=diag\left(w^{\frac{c(c-1)}{2}}\right)$$

and with $k\neq 0$ are circulant, their first row vectors V^k being given by

$$V_i^k=\delta_q\left(\frac{k/2}{q}\right)w^{\frac{q^2-1}{8}\cdot k}\cdot w^{-\frac{\frac{i}{k}(\frac{i}{k}-1)}{2}}$$

where $\delta_q=1$ if $q=1(4)$ and $\delta_q=i$ if $q=3(4)$, and with all inverses being taken in $\mathbb{Z}_q$.

Proof. This is a standard exercice on quadratic Gauss sums. First of all, the matrices G_k in the statement are indeed circulant, their first vectors being given by:

$$V_i^k=\frac{1}{\sqrt{q}}\sum_c w^{\frac{c(c-1)}{2}\cdot k+ic}$$

Let us first compute the square of this quantity. We have:

$$(V_i^k)^2=\frac{1}{q}\sum_{cd}w^{\left[\frac{c(c-1)}{2}+\frac{d(d-1)}{2}\right]k+i(c+d)}$$

The point now is that the sum S on the right, which has q^2 terms, decomposes as follows, where x is a certain exponent, depending on q,i,k:

$$S=\begin{cases}(q-1)(1+w+\ldots+w^{q-1})+qw^x&\text{if }q=1(4)\\(q+1)(1+w+\ldots+w^{q-1})-qw^x&\text{if }q=3(4)\end{cases}$$

We conclude that we have a formula as follows, where $\delta_q\in\{1,i\}$ is as in the statement, so that $\delta_q^2\in\{1,-1\}$ is given by $\delta_q^2=1$ if $q=1(4)$ and $\delta_q^2=-1$ if $q=3(4)$:

$$(V_i^k)^2=\delta_q^2\,w^x$$

In order to compute now the exponent x, we must go back to the above calculation of the sum S. We succesively have:

– First of all, at $k=1,i=0$ we have $x=\frac{q^2-1}{4}$.

– By translation we obtain $x=\frac{q^2-1}{4}-i(i-1)$, at $k=1$ and any i.

– By replacing $w\to w^k$ we obtain $x=\frac{q^2-1}{4}\cdot k-\frac{i}{k}(\frac{i}{k}-1)$, at any $k\neq0$ and any i.

Summarizing, we have computed the square of the quantity that we are interested in, the formula being as follows, with δ_q being as in the statement:

$$(V_i^k)^2=\delta_q^2\cdot w^{\frac{q^2-1}{4}\cdot k}\cdot w^{-\frac{i}{k}(\frac{i}{k}-1)}$$

By extracting now the square root, we obtain a formula as follows:

$$V_i^k=\pm\delta_q\cdot w^{\frac{q^2-1}{8}\cdot k}\cdot w^{-\frac{\frac{i}{k}(\frac{i}{k}-1)}{2}}$$

The computation of the missing sign is non-trivial, but by using the theory of quadratic Gauss sums, and more specifically a result of Gauss, computing precisely this kind of sign, we conclude that we have indeed a Legendre symbol, $\pm=\left(\frac{k/2}{q}\right)$, as claimed. □

Let us combine now all the above results. We obtain the following statement:

Theorem 8.16. *Let $q\geq3$ be prime, consider two subsets*

$$S,T\subset\{0,1,\ldots,q-1\}$$

satisfying the conditions $|S|=|T|$ and $S\cap T=\emptyset$, and write:

$$S=\{s_1,\ldots,s_N\}\quad,\quad T=\{t_1,\ldots,t_N\}$$

Then, with the matrix V being as above, the matrix

$$H_{ia,jb}=K_{ij}V_{b-a}^{t_j-s_i}$$

is complex Hadamard, provided that $K\in M_N(\mathbb{C})$ is.

Proof. This follows indeed by using the general construction in Theorem 8.13 above, with input coming from Proposition 8.14 and Proposition 8.15. □

As explained in [97], the above construction covers many interesting examples of Hadamard matrices, known from [129], [130] to be isolated, such as the Tao matrix:

$$T_6=\begin{pmatrix}1&1&1&1&1&1\\1&1&w&w&w^2&w^2\\1&w&1&w^2&w^2&w\\1&w&w^2&1&w&w^2\\1&w^2&w^2&w&1&w\\1&w^2&w&w^2&w&1\end{pmatrix}$$

In general, in order to find isolated matrices, the idea from [97] is that of starting with an isolated matrix, and then use suitable sets S,T. The defect computations are, however, quite difficult. As a concrete statement, however, we have the following conjecture:

Conjecture 8.17. *The complex Hadamard matrix constructed in Theorem 8.13 is isolated, provided that:*

1. *K is an isolated Fourier matrix, of prime order.*
2. *S,T consist of consecutive odd numbers, and consecutive even numbers.*

This statement is supported by the isolation result for T_6, and by several computer simulations in [97]. For further details on all this, we refer to [97], and to [30].

As a final topic now, we would like to discuss an extension of a part of our results, from here and from section 7, to the case of the partial Hadamard matrices (PHM). The extension, done in [30], is quite straightforward, but there are however a number of subtleties appearing. First of all, we can talk about deformations of PHM, as follows:

Definition 8.18. *Let $H\in X_{M,N}$ be a partial complex Hadamard matrix.*

1. *A deformation of H is a smooth function, as follows:*
$$f:\mathbb{T}_1\to(X_{M,N})_H$$
2. *The deformation is called "affine" if we have, with $A\in M_{M\times N}(\mathbb{R})$:*
$$f_{ij}(q)=H_{ij}q^{A_{ij}}$$
3. *We call "trivial" the deformations as follows, with $a\in\mathbb{R}^M,b\in\mathbb{R}^N$:*
$$f_{ij}(q)=H_{ij}q^{a_i+b_j}$$

Observe now that we have the following equality, where $U_{M,N}\subset M_{M\times N}(\mathbb{C})$ is the set of matrices having all rows of norm 1, and pairwise orthogonal:

$$X_{M,N}=M_{M\times N}(\mathbb{T})\cap\sqrt{N}U_{M,N}$$

As in the square case, this leads to the following definition:

Definition 8.19. *Associated to a point $H\in X_{M,N}$ are the enveloping tangent space*

$$\widetilde{T}_HX_{M,N}=T_HM_{M\times N}(\mathbb T)\cap T_H\sqrt{N}U_{M,N}$$

as well as the following subcones of this enveloping tangent space:

1. *The tangent cone $T_HX_{M,N}$: the set of tangent vectors to the deformations of H.*
2. *The affine tangent cone $T_H^\circ X_{M,N}$: same as above, using affine deformations only.*
3. *The trivial tangent cone $T_H^\times X_{M,N}$: as above, using trivial deformations only.*

Observe that $\widetilde{T}_HX_{M,N},T_HX_{M,N}$ are real vector spaces, and that $T_HX_{M,N},T_H^\circ X_{M,N}$ are two-sided cones, in the sense that they satisfy the following condition:

$$\lambda\in\mathbb R,A\in T\implies\lambda A\in T$$

Also, we have inclusions as follows:

$$T_H^\times X_{M,N}\subset T_H^\circ X_{M,N}\subset T_HX_{M,N}\subset\widetilde{T}_HX_{M,N}$$

As in the square matrix case, we can formulate the following definition:

Definition 8.20. *The defect of a matrix $H\in X_{M,N}$ is the dimension*

$$d(H)=\dim(\widetilde{T}_HX_{M,N})$$

of the real vector space $\widetilde{T}_HX_{M,N}$ constructed above.

The basic remarks and comments regarding the defect from the square matrix case extend then to this setting. In particular, we have the following basic result:

Theorem 8.21. *The enveloping tangent space at $H\in X_{M,N}$ is given by*

$$\widetilde{T}_HX_{M,N}\simeq\left\{A\in M_{M\times N}(\mathbb R)\Big|\sum_kH_{ik}\bar{H}_{jk}(A_{ik}-A_{jk})=0,\forall i,j\right\}$$

and the defect of H is the dimension of this real vector space.

Proof. In the square case this was done in section 7 above, and the extension of the computations there to the rectangular case is straightforward. □

At the level of non-trivial results now, we first have:

Theorem 8.22. *Let $H\in X_{M,N}$, and pick $K\in\sqrt{N}U_N$ extending H. We have then*

$$\widetilde{T}_HX_{M,N}\simeq\left\{E=(X\ Y)\in M_{M\times N}(\mathbb C)\Big|X=X^*,(EK)_{ij}\bar{H}_{ij}\in\mathbb R,\forall i,j\right\}$$

with the correspondence $A\to E$ being given by $E_{ij}=\sum_kH_{ik}\bar{K}_{jk}A_{ik}$, $A_{ij}=(EK)_{ij}\bar{H}_{ij}$.

Proof. Let us set indeed $R_{ij} = A_{ij}H_{ij}$ and $E = RK^*$. The correspondence $A \to R \to E$ is then bijective, and we have the following formula:

$$E_{ij} = \sum_k H_{ik}\bar{K}_{jk}A_{ik}$$

With these changes, the system of equations in Theorem 8.21 becomes $E_{ij} = \bar{E}_{ji}$ for any i, j with $j \leq M$. But this shows that we must have $E = (X\ Y)$ with $X = X^*$, and the condition $A_{ij} \in \mathbb{R}$ corresponds to the condition $(EK)_{ij}\bar{H}_{ij} \in \mathbb{R}$, as claimed. □

As an illustration, in the real case we obtain the following result:

Theorem 8.23. *For an Hadamard matrix $H \in M_{M\times N}(\pm 1)$ we have*

$$\widetilde{T}_H X_{M,N} \simeq M_M(\mathbb{R})^{symm} \oplus M_{M\times(N-M)}(\mathbb{R})$$

and so the defect is given by

$$d(H) = \frac{N(N+1)}{2} + M(N-M)$$

independently of the precise value of H.

Proof. We use Theorem 8.22. Since H is now real we can pick $K \in \sqrt{N}U_N$ extending it to be real too, and with nonzero entries, so the last condition appearing there, namely $(EK)_{ij}\bar{H}_{ij} \in \mathbb{R}$, simply tells us that E must be real. Thus we have:

$$\widetilde{T}_H X_{M,N} \simeq \left\{ E = (X\ Y) \in M_{M\times N}(\mathbb{R}) \Big| X = X^* \right\}$$

But this is the formula in the statement, and we are done. □

A matrix $H \in X_{M,N}$ cannot be isolated, simply because the space of its Hadamard equivalents provides a copy $\mathbb{T}^{MN} \subset X_{M,N}$, passing through H. However, if we restrict the attention to the matrices which are dephased, the notion of isolation makes sense:

Proposition 8.24. *The defect $d(H) = \dim(\widetilde{T}_H X_{M,N})$ satisfies*

$$d(H) \geq M + N - 1$$

and if $d(H) = M + N - 1$ then H is isolated inside the dephased quotient $X_{M,N} \to Z_{M,N}$.

Proof. Once again, the known results in the square case extend:

(1) We have indeed $\dim(T_H^\times X_{M,N}) = M + N - 1$, and since the tangent vectors to these trivial deformations belong to $\widetilde{T}_H X_{M,N}$, this gives the first assertion.

(2) Since $d(H) = M + N - 1$, the inclusions $T_H^\times X_{M,N} \subset T_H X_{M,N} \subset \widetilde{T}_H X_{M,N}$ must be equalities, and from $T_H X_{M,N} = T_H^\times X_{M,N}$ we obtain the result. □

Finally, still at the theoretical level, we have the following conjecture:

Conjecture 8.25. *An isolated matrix $H \in Z_{M,N}$ must have minimal defect, namely $d(H) = M + N - 1$.*

In other words, the conjecture is that if $H \in Z_{M,N}$ has only trivial first order deformations, then it has only trivial deformations at any order, including at ∞. In the square matrix case this statement comes with solid evidence, all known examples of complex Hadamard matrices $H \in X_N$ having non-minimal defect being known to admit one-parameter deformations. For more on this subject, see [129], [130].

Let us discuss now some examples of isolated partial Hadamard matrices, and provide some evidence for Conjecture 8.25. We are interested in the following matrices:

Definition 8.26. *The truncated Fourier matrix $F_{S,G}$, with G being a finite abelian group, and with $S \subset G$ being a subset, is constructed as follows:*

(1) *Given $N \in \mathbb{N}$, we set $F_N = (w^{ij})_{ij}$, where $w = e^{2\pi i/N}$.*
(2) *Assuming $G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_s}$, we set $F_G = F_{N_1} \otimes \ldots \otimes F_{N_s}$.*
(3) *We let $F_{S,G}$ be the submatrix of F_G having $S \subset G$ as row index set.*

Observe that F_N is the Fourier matrix of the cyclic group $\mathbb{Z}_N$. More generally, F_G is the Fourier matrix of the finite abelian group G. Observe also that $F_{G,G} = F_G$.

We can compute the defect of $F_{S,G}$ by using Theorem 8.21, and we obtain:

Theorem 8.27. *For a truncated Fourier matrix $F = F_{S,G}$ we have the formula*

$$\widetilde{T}_F X_{M,N} = \left\{ A \in M_{M\times N}(\mathbb{R}) \Big| P = AF^t \text{ satisfies } P_{ij} = P_{i+j,j} = \bar{P}_{i,-j}, \forall i,j \right\}$$

where $M = |S|, N = |G|$, and with all the indices being regarded as group elements.

Proof. We use Theorem 8.21. The defect equations there are as follows:

$$\sum_k F_{ik}\bar{F}_{jk}(A_{ik} - A_{jk}) = 0$$

For $F = F_{S,G}$ we have the following formula:

$$F_{ik}\bar{F}_{jk} = (F^t)_{k,i-j}$$

We therefore obtain the following formula:

$$\widetilde{T}_F X_{M,N} = \left\{ A \in M_{M\times N}(\mathbb{R}) \Big| (AF^t)_{i,i-j} = (AF^t)_{j,i-j}, \forall i,j \right\}$$

Now observe that for an arbitrary matrix $P \in M_M(\mathbb{C})$, we have:

$$\begin{aligned} P_{i,i-j} = P_{j,i-j}, \forall i,j &\iff P_{i+j,i} = P_{ji}, \forall i,j \\ &\iff P_{i+j,j} = P_{ij}, \forall i,j \end{aligned}$$

We therefore conclude that we have the following equality:

$$\widetilde{T}_F X_{M,N} = \left\{ A \in M_{M\times N}(\mathbb{R}) \middle| P = AF^t \text{ satisfies } P_{ij} = P_{i+j,j}, \forall i,j \right\}$$

Now observe that with $A \in M_{M\times N}(\mathbb{R})$ and $P = AF^t \in M_M(\mathbb{C})$ as above, we have:

$$\begin{aligned} \bar{P}_{ij} &= \sum_k A_{ik}(F^*)_{kj} \\ &= \sum_k A_{ik}(F^t)_{k,-j} \\ &= P_{i,-j} \end{aligned}$$

Thus, we obtain the formula in the statement, and we are done. □

Let us try to find some explicit examples of isolated matrices, of truncated Fourier type. For this purpose, we can use the following improved version of Theorem 8.27:

Theorem 8.28. *The defect of $F = F_{S,G}$ is the number*

$$d(F) = \dim(K) + \dim(I)$$

where K, I are the following linear spaces,

$$\begin{aligned} K &= \left\{ A \in M_{M\times N}(\mathbb{R}) \middle| AF^t = 0 \right\} \\ I &= \left\{ P \in L_M \middle| \exists A \in M_{M\times N}(\mathbb{R}), P = AF^t \right\} \end{aligned}$$

with L_M being the following linear space,

$$L_M = \left\{ P \in M_M(\mathbb{C}) \middle| P_{ij} = P_{i+j,j} = \bar{P}_{i,-j}, \forall i,j \right\}$$

with all the indices belonging by definition to the group G.

Proof. We use the general formula in Theorem 8.27. With the notations there, and with the linear space L_M being as above, we have a linear map as follows:

$$\Phi : \widetilde{T}_F X_{M,N} \to L_M$$
$$\Phi(A) = AF^t$$

By using this map, we obtain the following equality:

$$\dim(\widetilde{T}_F X_{M,N}) = \dim(\ker \Phi) + \dim(\operatorname{Im} \Phi)$$

Now since the spaces on the right are precisely those in the statement, $\ker \Phi = K$ and $\operatorname{Im} \Phi = I$, by applying Theorem 8.27 we obtain the result. □

In order to look now for isolated matrices, the first remark is that since a deformation of F_G will produce a deformation of $F_{S,G}$ too, we must restrict the attention to the case where $G = \mathbb{Z}_p$, with p prime. And here, we have the following conjecture:

Conjecture 8.29. *There exists a constant $\varepsilon > 0$ such that $F_{S,p}$ is isolated, for any p prime, once $S \subset \mathbb{Z}_p$ satisfies $|S| \geq (1-\varepsilon)p$.*

In principle this conjecture can be approached by using the formula in Theorem 8.28, and we have for instance evidence towards the fact that $F_{p-1,p}$ should be always isolated, that $F_{p-2,p}$ should be isolated too, provided that p is big enough, and so on. However, finding a number $\varepsilon > 0$ as above looks like a quite difficult question. See [30].

9. **Circulant matrices**

We discuss in this section another type of special complex Hadamard matrices, namely the circulant ones. There has been a lot of work here, starting with the Circulant Hadamard Conjecture (CHC) in the real case, and with many results in the complex case as well. We will present here the main techniques in dealing with such matrices. It is convenient to introduce the circulant matrices as follows:

Definition 9.1. *A complex matrix $H \in M_N(\mathbb{C})$ is called circulant when we have*

$$H_{ij} = \gamma_{j-i}$$

for some $\gamma \in \mathbb{C}^N$, with the matrix indices $i, j \in \{0, 1, \ldots, N-1\}$ taken modulo N.

Here the index convention is quite standard, as for the Fourier matrices F_N, and with this coming from Fourier analysis considerations, that we will get into later on.

As a basic example of such a matrix, in the real case, we have the matrix K_4. The circulant Hadamard conjecture states that this matrix is, up to equivalence, the only circulant Hadamard matrix $H \in M_N(\pm 1)$, regardless of the value of $N \in \mathbb{N}$:

Conjecture 9.2 (Circulant Hadamard Conjecture (CHC))**.** *The only circulant real Hadamard matrices $H \in M_N(\pm 1)$ are the matrix*

$$K_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

and its Hadamard conjugates, and this regardless of the value of $N \in \mathbb{N}$.

The fact that such a simple-looking problem is still open might seem quite surprising. Indeed, if we denote by $S \subset \{1, \ldots, N\}$ the set of positions of the -1 entries of the first row vector $\gamma \in (\pm 1)^N$, the Hadamard matrix condition is simply:

$$|S \cap (S + k)| = |S| - N/4$$

To be more precise, this must hold for any $k \neq 0$, taken modulo N. Thus, the above conjecture simply states that at $N \neq 4$, such a set S cannot exist. Let us record here this latter statement, originally due to Ryser [117]:

Conjecture 9.3 (Ryser Conjecture)**.** *Given an integer $N > 4$, there is no set*

$$S \subset \{1, \ldots, N\}$$

satisfying $|S \cap (S + k)| = |S| - N/4$ for any $k \neq 0$, taken modulo N.

Our purpose now will be that of showing that the CHC dissapears in the complex case, where we have examples at any $N \in \mathbb{N}$. As a first result here, we have:

Proposition 9.4. *The following are circulant and symmetric Hadamard matrices,*

$$F_2'=\begin{pmatrix}i&1\\1&i\end{pmatrix}\quad,\quad F_3'=\begin{pmatrix}w&1&1\\1&w&1\\1&1&w\end{pmatrix}\quad,\quad F_4''=\begin{pmatrix}-1&\nu&1&\nu\\\nu&-1&\nu&1\\1&\nu&-1&\nu\\\nu&1&\nu&-1\end{pmatrix}$$

where $w=e^{2\pi i/3},\nu=e^{\pi i/4}$, equivalent to the Fourier matrices F_2,F_3,F_4.

Proof. The orthogonality between rows being clear, we have here complex Hadamard matrices. The fact that we have an equivalence $F_2\sim F_2'$ follows from:

$$\begin{pmatrix}1&1\\1&-1\end{pmatrix}\sim\begin{pmatrix}i&i\\1&-1\end{pmatrix}\sim\begin{pmatrix}i&1\\1&i\end{pmatrix}$$

At $N=3$ now, the equivalence $F_3\sim F_3'$ can be constructed as follows:

$$\begin{pmatrix}1&1&1\\1&w&w^2\\1&w^2&w\end{pmatrix}\sim\begin{pmatrix}1&1&w\\1&w&1\\w&1&1\end{pmatrix}\sim\begin{pmatrix}w&1&1\\1&w&1\\1&1&w\end{pmatrix}$$

As for the case $N=4$, here the equivalence $F_4\sim F_4''$ can be constructed as follows, where we use the logarithmic notation $[k]_s=e^{2\pi ki/s}$, with respect to $s=8$:

$$\begin{bmatrix}0&0&0&0\\0&2&4&6\\0&4&0&4\\0&6&4&2\end{bmatrix}_8\sim\begin{bmatrix}0&1&4&1\\1&4&1&0\\4&1&0&1\\1&0&1&4\end{bmatrix}_8\sim\begin{bmatrix}4&1&0&1\\1&4&1&0\\0&1&4&1\\1&0&1&4\end{bmatrix}_8$$

Thus, the Fourier matrices F_2,F_3,F_4 can be put indeed in circulant form. □

We will explain later the reasons for denoting the above matrix F_4'', instead of F_4', the idea being that F_4' will be a matrix belonging to a certain series. Getting back now to the real circulant matrix K_4, this is equivalent to the Fourier matrix $F_G=F_2\otimes F_2$ of the Klein group $G=\mathbb{Z}_2\times\mathbb{Z}_2$, as shown by:

$$\begin{pmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix}\sim\begin{pmatrix}1&1&1&-1\\1&-1&1&1\\1&1&-1&1\\-1&1&1&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}$$

In fact, we have the following construction of circulant and symmetric Hadamard matrices at $N=4$, which involves an extra parameter $q\in\mathbb{T}$:

Proposition 9.5. *The following circulant and symmetric matrix is Hadamard,*

$$K_4^q = \begin{pmatrix} -1 & q & 1 & q \\ q & -1 & q & 1 \\ 1 & q & -1 & q \\ q & 1 & q & -1 \end{pmatrix}$$

for any $q \in \mathbb{T}$. At $q = 1, e^{\pi i/4}$ recover respectively the matrices K_4, F_4''.

Proof. The rows of the above matrix are pairwise orthogonal for any $q \in \mathbb{C}$, and so at $q \in \mathbb{T}$ we obtain a complex Hadamard matrix. The last assertion is clear. □

As a first conclusion, coming from the above considerations, we have:

Theorem 9.6. *The complex Hadamard matrices of order $N = 2, 3, 4, 5$, namely*

$$F_2, F_3, F_4^p, F_5$$

can be put, up to equivalence, in circulant and symmetric form.

Proof. As explained in section 5 above, the Hadamard matrices at $N = 2, 3, 4, 5$ are, up to equivalence, those in the statement. But at $N = 2, 3$ the problem is solved by Proposition 9.4 above. At $N = 4$ now, our claim is that, with $s = q^{-2}$, we have:

$$K_4^q \sim F_4^s$$

By multiplying the rows of K_4^q, and then the columns, by suitable scalars, we have:

$$K_4^q = \begin{pmatrix} -1 & q & 1 & q \\ q & -1 & q & 1 \\ 1 & q & -1 & q \\ q & 1 & q & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & -q & -1 & -q \\ 1 & -\bar{q} & 1 & \bar{q} \\ 1 & q & -1 & q \\ 1 & \bar{q} & 1 & -\bar{q} \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & s & -1 & -s \\ 1 & -1 & 1 & -1 \\ 1 & -s & -1 & s \end{pmatrix}$$

On the other hand, by permuting the second and third rows of F_4^s, we obtain:

$$F_4^s = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & s & -1 & -s \\ 1 & -s & -1 & s \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & s & -1 & -s \\ 1 & -1 & 1 & -1 \\ 1 & -s & -1 & s \end{pmatrix}$$

Thus these matrices are equivalent, and the result follows from Proposition 9.5. At $N = 5$ now, the matrix that we are looking for is as follows, with $w = e^{2\pi i/5}$:

$$F_5' = \begin{pmatrix} w^2 & 1 & w^4 & w^4 & 1 \\ 1 & w^2 & 1 & w^4 & w^4 \\ w^4 & 1 & w^2 & 1 & w^4 \\ w^4 & w^4 & 1 & w^2 & 1 \\ 1 & w^4 & w^4 & 1 & w^2 \end{pmatrix}$$

It is indeed clear that this matrix is circulant, symmetric, and complex Hadamard, and the fact that we have $F_5 \sim F_5'$ follows either directly, or by using [69]. $\square$

Summarizing, many interesting examples of complex Hadamard matrices are circulant. This is in stark contrast with the real case, where the CHC, discussed above, states that the only circulant real matrices should be those appearing at $N = 4$.

Let us prove now, as a generalization, that any Fourier matrix F_N can be put in circulant and symmetric form. We use Björck's cyclic root formalism [43], which is as follows:

Theorem 9.7. *Assume that a matrix $H \in M_N(\mathbb{T})$ is circulant, $H_{ij} = \gamma_{j-i}$. Then H is is a complex Hadamard matrix if and only if the vector*

$$z = (z_0, z_1, \ldots, z_{N-1})$$

given by $z_i = \gamma_i/\gamma_{i-1}$ satisfies the following equations:

$$\begin{aligned}
z_0 + z_1 + \ldots + z_{N-1} &= 0\\
z_0z_1 + z_1z_2 + \ldots + z_{N-1}z_0 &= 0\\
&\ldots\\
z_0z_1 \ldots z_{N-2} + \ldots + z_{N-1}z_0 \ldots z_{N-3} &= 0\\
z_0z_1 \ldots z_{N-1} &= 1
\end{aligned}$$

If so is the case, we say that $z = (z_0, \ldots, z_{N-1})$ is a cyclic N-root.

Proof. This follows from a direct computation, the idea being that, with $H_{ij} = \gamma_{j-i}$ as above, the orthogonality conditions between the rows are best written in terms of the variables $z_i = \gamma_i/\gamma_{i-1}$, and correspond to the equations in the statement. See [43]. $\square$

Observe that, up to a global multiplication by a scalar $w \in \mathbb{T}$, the first row vector $\gamma = (\gamma_0, \ldots, \gamma_{N-1})$ of the matrix $H \in M_N(\mathbb{T})$ constructed above is as follows:

$$\gamma = (z_0, z_0z_1, z_0z_1z_2, \ldots\ldots, z_0z_1 \ldots z_{N-1})$$

We will use this observation several times, in what follows. Now back to the Fourier matrices, we have the following result:

Theorem 9.8. *Given $N \in \mathbb{N}$, set $\nu = e^{\pi i/N}$ and $q = \nu^{N-1}$, $w = \nu^2$. Then we have a cyclic N-root as follows,*

$$(q, qw, qw^2, \ldots, qw^{N-1})$$

and the corresponding complex Hadamard matrix F_N' is circulant and symmetric, and equivalent to the Fourier matrix F_N.

Proof. Given $q, w \in \mathbb{T}$, let us find out when $(q, qw, qw^2, \ldots, qw^{N-1})$ is a cyclic root:

(1) In order for the $= 0$ equations in Theorem 9.7 to be satisfied, the value of q is irrelevant, and w must be a primitive N-root of unity.

(2) As for the $=1$ equation in Theorem 9.7, this states in our case that we must have:

$$q^N w^{\frac{N(N-1)}{2}} = 1$$

Thus, we must have $q^N = (-1)^{N-1}$, so with the values of $q, w \in \mathbb{T}$ in the statement, we have indeed a cyclic N-root. Now construct $H_{ij} = \gamma_{j-i}$ as in Theorem 9.7. We have:

$$\begin{aligned}\gamma_k = \gamma_{-k} &\iff q^{k+1} w^{\frac{k(k+1)}{2}} = q^{-k+1} w^{\frac{k(k-1)}{2}}\\ &\iff q^{2k} w^k = 1\\ &\iff q^2 = w^{-1}\end{aligned}$$

But this latter condition holds indeed, because we have:

$$q^2 = \nu^{2N-2} = \nu^{-2} = w^{-1}$$

We conclude that our circulant matrix H is symmetric as well, as claimed. It remains to construct an equivalence as follows:

$$H \sim F_N$$

In order to do this, observe that, due to our conventions $q = \nu^{N-1}, w = \nu^2$, the first row vector of H is given by:

$$\begin{aligned}\gamma_k &= q^{k+1} w^{\frac{k(k+1)}{2}}\\ &= \nu^{(N-1)(k+1)} \nu^{k(k+1)}\\ &= \nu^{(N+k-1)(k+1)}\end{aligned}$$

Thus, the entries of H are given by the following formula:

$$\begin{aligned}H_{-i,j} &= H_{0,i+j}\\ &= \nu^{(N+i+j-1)(i+j+1)}\\ &= \nu^{i^2+j^2+2ij+Ni+Nj+N-1}\\ &= \nu^{N-1} \cdot \nu^{i^2+Ni} \cdot \nu^{j^2+Nj} \cdot \nu^{2ij}\end{aligned}$$

With this formula in hand, we can now finish. Indeed, the matrix $H = (H_{ij})$ is equivalent to the following matrix:

$$H' = (H_{-i,j})$$

Now regarding this latter matrix H', observe that in the above formula, the factors ν^{N-1}, ν^{i^2+Ni}, ν^{j^2+Nj} correspond respectively to a global multiplication by a scalar, and to row and column multiplications by scalars. Thus this matrix H' is equivalent to the matrix H'' obtained from it by deleting these factors.

But this latter matrix, given by $H''_{ij} = \nu^{2ij}$ with $\nu = e^{\pi i/N}$, is precisely the Fourier matrix F_N, and we are done. $\square$

As an illustration, let us work out the cases $N = 2, 3, 4, 5$. We have here:

Proposition 9.9. *The matrices F_N' are as follows:*

(1) *At $N=2,3$ we obtain the old matrices F_2',F_3'.*

(2) *At $N=4$ we obtain the following matrix, with $\nu=e^{\pi i/4}$:*

$$F_4'=\begin{pmatrix}\nu^3&1&\nu^7&1\\ 1&\nu^3&1&\nu^7\\ \nu^7&1&\nu^3&1\\ 1&\nu^7&1&\nu^3\end{pmatrix}$$

(3) *At $N=5$ we obtain the old matrix F_5'.*

Proof. With notations from Theorem 9.8, the proof goes as follows:

(1) At $N=2$ we have $\nu=i,q=i,w=-1$, so the cyclic root is:

$$(i,-i)$$

The first row vector is $(i,1)$, and we obtain indeed the old matrix F_2'.

At $N=3$ we have $\nu=e^{\pi i/3}$ and $q=w=\nu^2=e^{2\pi i/3}$, the cyclic root is:

$$(w,w^2,1)$$

The first row vector is $(w,1,1)$, and we obtain indeed the old matrix F_3'.

(2) At $N=4$ we have $\nu=e^{\pi i/4}$ and $q=\nu^3,w=\nu^2$, the cyclic root is:

$$(\nu^3,\nu^5,\nu^7,\nu)$$

The first row vector is $(\nu^3,1,\nu^7,1)$, and we obtain the matrix in the statement.

(3) At $N=5$ we have $\nu=e^{\pi i/5}$ and $q=\nu^4=w^2$, with $w=\nu^2=e^{2\pi i/5}$, and the cyclic root is therefore:

$$(w^2,w^3,w^4,1,w)$$

The first row vector is $(w^2,1,w^4,w^4,1)$, and we obtain in this way the old matrix F_5', as claimed. □

Regarding the above matrix F_4', observe that this is equivalent to the matrix F_4'' from Proposition 9.4, with the equivalence $F_4'\sim F_4''$ being obtained by multiplying everything by $\nu=e^{\pi i/4}$. While both these matrices are circulant and symmetric, and of course equivalent to F_4, one of them, namely F_4', is "better" than the other, because the corresponding cyclic root comes from a progression. This is the reason for our notations F_4',F_4''.

Let us discuss now the case of the generalized Fourier matrices F_G. In this context, the assumption of being circulant is somewhat unnatural, because this comes from a $\mathbb Z_N$ symmetry, and the underlying group is no longer $\mathbb Z_N$. It is possible to fix this issue by talking about G-patterned Hadamard matrices, with G being no longer cyclic, but for our purposes here, best is to formulate the result in a weaker form, as follows:

Theorem 9.10. *The generalized Fourier matrices F_G, associated to the finite abelian groups G, can be put in symmetric and bistochastic form.*

Proof. We know from Theorem 9.8 that any usual Fourier matrix F_N can be put in circulant and symmetric form. Since circulant implies bistochastic, in the sense that the sums on all rows and all columns must be equal, the result holds for F_N.

In general now, if we decompose $G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$, we have:

$$F_G = F_{N_1} \otimes \ldots \otimes F_{N_k}$$

Now since the property of being circulant is stable under taking tensor products, and so is the property of being bistochastic, we therefore obtain the result. □

We have as well the following alternative generalization of Theorem 9.8, coming from Backelin's work in [5], and remaining in the circulant and symmetric setting:

Theorem 9.11. *Let $M|N$, and set $w = e^{2\pi i/N}$. We have a cyclic root as follows,*

$$(\underbrace{q_1, \ldots, q_M}_{M}, \underbrace{q_1 w, \ldots, q_M w}_{M}, \ldots\ldots, \underbrace{q_1 w^{N-1}, \ldots, q_M w^{N-1}}_{M})$$

provided that $q_1, \ldots, q_M \in \mathbb{T}$ satisfy the following condition:

$$(q_1 \ldots q_M)^N = (-1)^{M(N-1)}$$

Moreover, assuming that the following conditions are satisfied,

$$q_1 q_2 = 1 \quad , \quad q_3 q_M = q_4 q_{M-1} = \ldots = w$$

which imply $(q_1 \ldots q_M)^N = (-1)^{M(N-1)}$, the Hadamard matrix is symmetric.

Proof. Let us first check the $= 0$ equations for a cyclic root. Given arbitrary numbers $q_1, \ldots, q_M \in \mathbb{T}$, if we denote by (z_i) the vector in the statement, we have:

$$\begin{aligned}\sum_i z_{i+1} \ldots z_{i+K} &= \begin{pmatrix} q_1 \ldots q_K + q_2 \ldots q_{K+1} + \ldots\ldots + q_{M-K+1} \ldots q_M \\ + q_{M-K+2} \ldots q_M q_1 w + \ldots\ldots + q_M q_1 \ldots q_{K-1} w^{K-1} \end{pmatrix} \\ &\quad \times (1 + w^K + w^{2K} + \ldots + w^{(N-1)K})\end{aligned}$$

Now since the sum on the right vanishes, the $= 0$ conditions are satisfied. Regarding now the $= 1$ condition, the total product of the numbers z_i is given by:

$$\begin{aligned}\prod_i z_i &= (q_1 \ldots q_M)^N (1 \cdot w \cdot w^2 \ldots w^{N-1})^M \\ &= (q_1 \ldots q_M)^N w^{\frac{MN(N-1)}{2}}\end{aligned}$$

By using $w = e^{2\pi i/N}$ we obtain that the coefficient on the right is:

$$\begin{aligned}w^{\frac{MN(N-1)}{2}} &= e^{\frac{2\pi i}{N} \cdot \frac{MN(N-1)}{2}} \\ &= e^{\pi i M(N-1)} \\ &= (-1)^{M(N-1)}\end{aligned}$$

Thus, if $(q_1\ldots q_M)^N=(-1)^{M(N-1)}$, we obtain a cyclic root, as stated. See [5], [66]. The corresponding first row vector can be written as follows:

$$V=\left(\underbrace{q_1,q_1q_2,\ldots,q_1\ldots q_M}_M,\ldots\ldots\ldots,\underbrace{\frac{w^{M-1}}{q_2\ldots q_M},\ldots,\frac{w^2}{q_{M-1}q_M},\frac{w}{q_M},1}_M\right)$$

Thus, the corresponding circulant complex Hadamard matrix is as follows:

$$H=\begin{pmatrix}q_1&q_1q_2&q_1q_2q_3&q_1q_2q_3q_4&q_1q_2q_3q_4q_5&\ldots\\ 1&q_1&q_1q_2&q_1q_2q_3&q_1q_2q_3q_4&\ldots\\ \frac{w}{q_M}&1&q_1&q_1q_2&q_1q_2q_3&\ldots\\ \frac{w^2}{q_{M-1}q_M}&\frac{w}{q_M}&1&q_1&q_1q_2&\ldots\\ \frac{w^3}{q_{M-2}q_{M-1}q_M}&\frac{w^2}{q_{M-1}q_M}&\frac{w}{q_M}&1&q_1&\ldots\\ \vdots&\vdots&\vdots&\vdots&\vdots&\ddots\end{pmatrix}$$

We are therefore led to the symmetry conditions in the statement, and we are done. □

Still in relation with the CHC, the problem of investigating the existence of the circulant Butson matrices appears. The first result here, due to Turyn [136], is as follows:

Proposition 9.12. *The size of a circulant Hadamard matrix*

$$H\in M_N(\pm1)$$

must be of the form $N=4n^2$, with $n\in\mathbb N$.

Proof. Let $a,b\in\mathbb N$ with $a+b=N$ be the number of $1,-1$ entries in the first row of H. If we denote by $H_0,\ldots,H_{N-1}$ the rows of H, then by summing over columns we get:

$$\begin{aligned}\sum_{i=0}^{N-1}<H_0,H_i>&=a(a-b)+b(b-a)\\&=(a-b)^2\end{aligned}$$

On the other hand, by orthogonality of the rows, the quantity on the left is:

$$<H_0,H_0>=N$$

Thus the number $N=(a-b)^2$ is a square, and together with the fact that we have $N\in2\mathbb N$, this gives $N=4n^2$, with $n\in\mathbb N$. □

Also found by Turyn in [136] is the fact that the above number $n\in\mathbb N$ must be odd, and not a prime power. In the general Butson matrix setting now, we have:

Proposition 9.13. *Assume that $H \in H_N(l)$ is circulant, let $w = e^{2\pi i/l}$. If*

$$a_0, \ldots, a_{l-1} \in \mathbb{N}$$

with $\sum a_i = N$ are the number of $1, w, \ldots, w^{l-1}$ entries in the first row of H, then:

$$\sum_{ik} w^k a_i a_{i+k} = N$$

This condition, with $\sum a_i = N$, will be called "Turyn obstruction" on (N, l).

Proof. Indeed, by summing over the columns of H, we obtain:

$$\begin{aligned}\sum_i < H_0, H_i > &= \sum_{ij} < w^i, w^j > a_i a_j \\ &= \sum_{ij} w^{i-j} a_i a_j\end{aligned}$$

Now since the left term is $< H_0, H_0 >= N$, this gives the result. □

We can deduce from this a number of concrete obstructions, as follows:

Theorem 9.14. *When l is prime, the Turyn obstruction is*

$$\sum_i (a_i - a_{i+k})^2 = 2N$$

for any $k \neq 0$. Also, for small values of l, the Turyn obstruction is as follows:

(1) *At $l = 2$ the condition is:*
$$(a_0 - a_1)^2 = N$$
(2) *At $l = 3$ the condition is:*
$$(a_0 - a_1)^2 + (a_1 - a_2)^2 + (a_2 - a_3)^2 = 2N$$
(3) *At $l = 4$ the condition is:*
$$(a_0 - a_2)^2 + (a_1 - a_3)^2 = N$$
(4) *At $l = 5$ the condition is:*
$$\sum_i (a_i - a_{i+1})^2 = \sum_i (a_i - a_{i+2})^2 = 2N$$

Proof. We use the fact, from section 6 above, that when l is prime, the vanishing sums of l-roots of unity are exactly the sums of the following type, with $c \in \mathbb{N}$:

$$S = c + cw + \ldots + cw^{l-1}$$

We conclude that the Turyn obstruction is equivalent to the following system of equations, one for each $k \neq 0$:

$$\sum_i a_i^2 - \sum_i a_i a_{i+k} = N$$

Now by forming squares, this gives the equations in the statement. Regarding now the $l=2,3,4,5$ assertions, these follow from the first assertion when l is prime, $l=2,3,5$. Also, at $l=4$ we have $w=i$, so the Turyn obstruction reads:

$$(a_0^2+a_1^2+a_2^2+a_3^2)+i\sum a_ia_{i+1}-2(a_0a_2+a_1a_3)-i\sum a_ia_{i+1}=N$$

Thus the imaginary terms cancel, and we obtain the formula in the statement. □

The above results are of course just some basic observations on the subject, and the massive amount of work on the CHC has a number of interesting Butson matrix extensions. For some more advanced theory on all this, we refer to [26], [53].

Let us go back now to the pure complex case, and discuss Fourier analytic aspects. From a traditional linear algebra viewpoint, the circulant matrices are best understood as being the matrices which are Fourier-diagonal, and we will exploit this here.

Let us fix $N\in\mathbb N$, and denote by $F=(w^{ij})/\sqrt{N}$ with $w=e^{2\pi i/N}$ the rescaled Fourier matrix. Also, given a vector $q\in\mathbb C^N$, we denote by $Q\in M_N(\mathbb C)$ the diagonal matrix having q as vector of diagonal entries. That is, $Q_{ii}=q_i$, and $Q_{ij}=0$ for $i\neq j$. With these conventions, we have the following well-known result:

Theorem 9.15. *For a complex matrix $H\in M_N(\mathbb C)$, the following are equivalent:*

(1) *H is circulant, $H_{ij}=\xi_{j-i}$ for some $\xi\in\mathbb C^N$.*
(2) *H is Fourier-diagonal, $H=FQF^*$ with Q diagonal.*

In addition, the first row vector of FQF^* is given by $\xi=Fq/\sqrt{N}$.

Proof. If $H_{ij}=\xi_{j-i}$ is circulant then $Q=F^*HF$ is diagonal, given by:

$$\begin{aligned}Q_{ij}&=\frac{1}{N}\sum_{kl}w^{jl-ik}\xi_{l-k}\\&=\delta_{ij}\sum_r w^{jr}\xi_r\end{aligned}$$

Also, if $Q=diag(q)$ is diagonal then $H=FQF^*$ is circulant, given by:

$$\begin{aligned}H_{ij}&=\sum_k F_{ik}Q_{kk}\bar F_{jk}\\&=\frac{1}{N}\sum_k w^{(i-j)k}q_k\end{aligned}$$

Thus, we have proved the equivalence between the conditions in the statement. Finally, regarding $\xi=Fq/\sqrt{N}$, this follows from the last formula established above. □

The above result is useful in connection with any question regarding the circular matrices, and in relation with the orthogonal and unitary cases, we have:

Proposition 9.16. *The various sets of circulant matrices are as follows:*

(1) *The set of all circulant matrices is:*

$$M_N(\mathbb{C})^{circ} = \left\{FQF^*\Big|q \in \mathbb{C}^N\right\}$$

(2) *The set of all circulant unitary matrices is:*

$$U_N^{circ} = \left\{FQF^*\Big|q \in \mathbb{T}^N\right\}$$

(3) *The set of all circulant orhogonal matrices is:*

$$O_N^{circ} = \left\{FQF^*\Big|q \in \mathbb{T}^N, \bar{q}_i = q_{-i}, \forall i\right\}$$

In addition, the first row vector of FQF^* is given by $\xi = Fq/\sqrt{N}$.

Proof. All this follows from Theorem 9.15, as follows:

(1) This assertion, along with the last one, is Theorem 9.15 itself.

(2) This is clear from (1), because the eigenvalues must be on the unit circle $\mathbb{T}$.

(3) Observe first that for $q \in \mathbb{C}^N$ we have $\overline{Fq} = F\tilde{q}$, with $\tilde{q}_i = \bar{q}_{-i}$, and so $\xi = Fq$ is real if and only if $\bar{q}_i = q_{-i}$ for any i. Together with (2), this gives the result. □

Observe that in (3), the equations for the parameter space are $q_0 = \bar{q}_0$, $\bar{q}_1 = q_{n-1}$, $\bar{q}_2 = q_{n-2}$, and so on until $[N/2]+1$. Thus, with the convention $\mathbb{Z}_\infty = \mathbb{T}$ we have:

$$O_N^{circ} \simeq \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_\infty^{(N-1)/2} & (N \text{ odd}) \\ \mathbb{Z}_2^2 \times \mathbb{Z}_\infty^{(N-2)/2} & (N \text{ even}) \end{cases}$$

In terms of circulant Hadamard matrices, we have the following statement:

Theorem 9.17. *The sets of complex and real circulant Hadamard matrices are:*

$$X_N^{circ} = \left\{\sqrt{N}FQF^*\Big|q \in \mathbb{T}^N\right\} \cap M_N(\mathbb{T})$$

$$Y_N^{circ} = \left\{\sqrt{N}FQF^*\Big|q \in \mathbb{T}^N, \bar{q}_i = q_{-i}\right\} \cap M_N(\pm 1)$$

In addition, the sets of q parameters are invariant under cyclic permutations, and also under mutiplying by numbers in $\mathbb{T}$, respectively under multiplying by -1.

Proof. All the assertions are indeed clear from Proposition 9.16 above, by intersecting the sets there with $M_N(\mathbb{T})$. □

The above statement is of course something quite theoretical in the real case, where the CHC states that we should have $Y_N^{circ} = \emptyset$, at any $N \neq 4$. However, in the complex case all this is useful, and complementary to Björck's cyclic root formalism.

Let us discuss now a number of geometric and analytic aspects. First, we have the following deep counting result, due to Haagerup [70]:

Theorem 9.18. *When N is prime, the number of circulant $N\times N$ complex Hadamard matrices, counted with certain multiplicities, is exactly:*

$$N_{circ}=\binom{2N-2}{N-1}$$

Proof. This is something advanced, using a variety of techiques from Fourier analysis, number theory, complex analysis and algebraic geometry. The idea is as follows:

(1) As explained in [70], when N is prime, Björck's cyclic root formalism, explained above, can be further manipulated, by using discrete Fourier transforms, and we are eventually led to a simpler system of equations.

(2) This simplified system can be shown then to have a finite number of solutions, the key ingredient here being a well-known theorem of Chebotarev, which states that when N is prime, all the minors of the Fourier matrix F_N are nonzero.

(3) With this finiteness result in hand, the precise count can be done as well, by using various techniques from classical algebraic geometry, and we are led to the formula in the statement. For the details here, see [70]. □

When N is not prime, the situation is considerably more complicated, with some values leading to finitely many solutions, and with other values leading to an infinite number of solutions, and with many other new phenomena appearing. See [43], [44], [45], [70].

Let us discuss now an alternative take on these questions, based on the p-norm considerations from sections 2-3 above. As explained in [26], the most adapted exponent for the circulant case is $p=4$. So, as a starting point, let us formulate:

Proposition 9.19. *Given a matrix $U\in U_N$ we have*

$$||U||_4\geq 1$$

with equality precisely when $H=U/\sqrt{N}$ is Hadamard.

Proof. This follows from the Cauchy-Schwarz inequality, as follows:

$$\begin{aligned}||U||_4^4&=\sum_{ij}|U_{ij}|^4\\&\geq\frac{1}{N^2}\left(\sum_{ij}|U_{ij}|^2\right)^2\\&=1\end{aligned}$$

Thus we have $||U||_4\geq 1$, with equality if and only if $H=\sqrt{N}U$ is Hadamard. □

In the circulant case now, and in Fourier formulation, the estimate is as follows:

Theorem 9.20. *Given a vector $q \in \mathbb{T}^N$, written $q = (q_0, \ldots, q_{N-1})$ consider the following quantity, with all the indices being taken modulo N:*

$$\Phi = \sum_{i+k=j+l} \frac{q_i q_k}{q_j q_l}$$

Then this quantity Φ is real, and we have the estimate

$$\Phi \geq N^2$$

with equality happening precisely when $\sqrt{N}q$ is the eigenvalue vector of a circulant Hadamard matrix $H \in M_N(\mathbb{C})$.

Proof. By conjugating the formula of Φ we see that this quantity is indeed real. In fact, Φ appears by definition as a sum of N^3 terms, consisting of $N(2N-1)$ values of 1 and of $N(N-1)^2$ other complex numbers of modulus 1, coming in pairs $(a, \bar{a})$.

Regarding now the second assertion, by using the various identifications in Theorem 9.15 and Proposition 9.16, and the formula $\xi = Fq/\sqrt{N}$ there, we have:

$$\begin{aligned}
||U||_4^4 &= N \sum_s |\xi_s|^4 \\
&= \frac{1}{N^3} \sum_s |\sum_i w^{si} q_i|^4 \\
&= \frac{1}{N^3} \sum_s \sum_i w^{si} q_i \sum_j w^{-sj} \bar{q}_j \sum_k w^{sk} q_k \sum_l w^{-sl} \bar{q}_l \\
&= \frac{1}{N^3} \sum_s \sum_{ijkl} w^{(i-j+k-l)s} \frac{q_i q_k}{q_j q_l} \\
&= \frac{1}{N^2} \sum_{i+k=j+l} \frac{q_i q_k}{q_j q_l}
\end{aligned}$$

Thus Proposition 9.19 gives the following estimate:

$$\Phi = N^2 ||U||_4^4 \geq N^2$$

Moreover, we have equality precisely in the Hadamard matrix case, as claimed. $\square$

We have the following more direct explanation of the above result:

Proposition 9.21. *With the above notations, we have the formula*

$$\Phi = N^2 + \sum_{i \neq j} (|\nu_i|^2 - |\nu_j|^2)^2$$

where $\nu = (\nu_0, \ldots, \nu_{N-1})$ is the vector given by $\nu = Fq$.

Proof. This follows by replacing in the above proof the Cauchy-Schwarz estimate by the corresponding sum of squares. More precisely, we know from the above proof that:

$$\Phi = N^3 \sum_i |\xi_i|^4$$

On the other hand $U_{ij} = \xi_{j-i}$ being unitary, we have $\sum_i |\xi_i|^2 = 1$, and so:

$$\begin{aligned}
1 &= \sum_i |\xi_i|^4 + \sum_{i \neq j} |\xi_i|^2 \cdot |\xi_j|^2 \\
&= N \sum_i |\xi_i|^4 - \left((N-1) \sum_i |\xi_i|^4 - \sum_{i \neq j} |\xi_i|^2 \cdot |\xi_j|^2 \right) \\
&= \frac{1}{N^2} \Phi - \sum_{i \neq j} (|\xi_i|^2 - |\xi_j|^2)^2
\end{aligned}$$

Now by multiplying by N^2, this gives the formula in the statement. □

As an application of the above considerations, in the real Hadamard matrix case, we have the following analytic reformulation of the CHC, from [26]:

Theorem 9.22. *For a vector $q \in \mathbb{T}^N$ satisfying $\bar{q}_i = q_{-i}$ the following quantity is real,*

$$\Phi = \sum_{i+j+k+l=0} q_i q_j q_k q_l$$

and satisfies the following inequality:

$$\Phi \geq N^2$$

The CHC states that we cannot have equality at $N > 4$.

Proof. This follows from Theorem 9.20, via the identifications from Theorem 9.15, the parameter space in the real case being $\{q \in \mathbb{T}^N | \bar{q}_i = q_{-i}\}$. Thus, we obtain the result. □

Following [26], let us further discuss all this. We first have:

Theorem 9.23. *Let us decompose the above function as*

$$\Phi = \Phi_0 + \ldots + \Phi_{N-1}$$

with each Φ_i being given by the same formula as Φ, namely

$$\Phi = \sum_{i+k=j+l} \frac{q_i q_k}{q_j q_k}$$

but keeping the index i fixed. Then:

(1) *The critical points of Φ are those where $\Phi_i \in \mathbb{R}$, for any i.*
(2) *In the Hadamard case we have $\Phi_i = N$, for any i.*

Proof. This follows by doing some elementary computations, as follows:

(1) The first observation is that the non-constant terms in the definition of Φ involving the variable q_i are the terms of the sum $K_i + \bar{K}_i$, where:

$$K_i = \sum_{2i=j+l} \frac{q_i^2}{q_j q_l} + 2 \sum_{k \neq i} \sum_{i+k=j+l} \frac{q_i q_k}{q_j q_l}$$

Thus if we fix i and we write $q_i = e^{i\alpha_i}$, we obtain:

$$\begin{aligned}
\frac{\partial \Phi}{\partial \alpha_i} &= 4Re \left(\sum_k \sum_{i+k=j+l} i \cdot \frac{q_i q_k}{q_j q_l} \right) \\
&= 4Im \left(\sum_{i+k=j+l} \frac{q_i q_k}{q_j q_l} \right) \\
&= 4Im(\Phi_i)
\end{aligned}$$

Now since the derivative must vanish for any i, this gives the result.

(2) We first perform the end of the Fourier computation in the proof of Theorem 9.20 above backwards, by keeping the index i fixed. We obtain:

$$\begin{aligned}
\Phi_i &= \sum_{i+k=j+l} \frac{q_i q_k}{q_j q_l} \\
&= \frac{1}{N} \sum_s \sum_{ijkl} w^{(i-j+k-l)s} \frac{q_i q_k}{q_j q_l} \\
&= \frac{1}{N} \sum_s w^{si} q_i \sum_j w^{-sj} \bar{q}_j \sum_k w^{sk} q_k \sum_l w^{-sl} \bar{q}_l \\
&= N^2 \sum_s w^{si} q_i \bar{\xi}_s \xi_s \bar{\xi}_s
\end{aligned}$$

Here we have used the formula $\xi = Fq/\sqrt{N}$. Now by assuming that we are in the Hadamard case, we have $|\xi_s| = 1/\sqrt{N}$ for any s, and so we obtain:

$$\begin{aligned}
\Phi_i &= N \sum_s w^{si} q_i \bar{\xi}_s \\
&= N\sqrt{N} q_i \overline{(F^* \xi)}_i \\
&= N q_i \bar{q}_i \\
&= N
\end{aligned}$$

Thus, we have obtained the conclusion in the statement. $\square$

Let us discuss now a probabilistic approach to all this. Given a compact manifold X endowed with a probability measure, and a bounded function $\Theta : X \to [0,\infty)$, the maximum of this function can be recaptured via following well-known formula:

$$\max\Theta = \lim_{p\to\infty}\left(\int_X \Theta(x)^p\,dx\right)^{1/p}$$

In our case, we are rather interested in computing a minimum, and we have:

Proposition 9.24. *We have the formula*

$$\min\Phi = N^3 - \lim_{p\to\infty}\left(\int_{\mathbb{T}^N}(N^3-\Phi)^p\,dq\right)^{1/p}$$

where the torus $\mathbb{T}^N$ is endowed with its usual probability measure.

Proof. This follows from the above formula, with $\Theta = N^3 - \Phi$. Observe that Θ is indeed positive, because Φ is by definition a sum of N^3 complex numbers of modulus 1. □

Let us restrict now the attention to the problem of computing the moments of Φ, which is more or less the same as computing those of $N^3 - \Phi$. We have here:

Proposition 9.25. *The moments of Φ are given by*

$$\int_{\mathbb{T}^N}\Phi^p\,dq = \#\left\{\begin{pmatrix}i_1k_1\ldots i_pk_p\\ j_1l_1\ldots j_pl_p\end{pmatrix}\Big| i_s+k_s=j_s+l_s, [i_1k_1\ldots i_pk_p]=[j_1l_1\ldots j_pl_p]\right\}$$

where the sets between brackets are by definition sets with repetition.

Proof. This is indeed clear from the formula of Φ. See [27]. □

Regarding now the real case, an analogue of Proposition 9.25 holds, but the combinatorics does not get any simpler. One idea in dealing with this problem is by considering the "enveloping sum", obtained from Φ by dropping the condition $i+k=j+l$:

$$\tilde{\Phi} = \sum_{ijkl}\frac{q_iq_k}{q_jq_l}$$

The point is that the moments of Φ appear as "sub-quantities" of the moments of $\tilde{\Phi}$, so perhaps the question to start with is to understand very well the moments of $\tilde{\Phi}$. And this latter problem sounds like a quite familiar one, because:

$$\tilde{\Phi} = \left|\sum_i q_i\right|^4$$

We will be back to this later. For the moment, let us do some combinatorics:

Proposition 9.26. *We have the moment formula*

$$\int_{\mathbb{T}^N}\tilde{\Phi}^p\,dq=\sum_{\pi\in P(2p)}\binom{2p}{\pi}\frac{N!}{(N-|\pi|)!}$$

where the coefficients on the right are given by

$$\binom{2p}{\pi}=\binom{2p}{b_1,\ldots,b_{|\pi|}}$$

with $b_1,\ldots,b_{|\pi|}$ being the lengths of the blocks of π.

Proof. Indeed, by using the same method as for Φ, we obtain:

$$\int_{\mathbb{T}^N}\tilde{\Phi}(q)^p\,dq=\#\left\{\begin{pmatrix}i_1k_1\ldots i_pk_p\\ j_1l_1\ldots j_pl_p\end{pmatrix}\Big|[i_1k_1\ldots i_pk_p]=[j_1l_1\ldots j_pl_p]\right\}$$

The sets with repetitions on the right are best counted by introducing the corresponding partitions $\pi=\ker\left(i_1k_1\ldots i_pk_p\right)$, and this gives the formula in the statement. □

In order to discuss now the real case, we have to slightly generalize the above result, by computing all the half-moments of $\widetilde{\Phi}$. The result here is best formulated as:

Proposition 9.27. *We have the moment formula*

$$\int_{\mathbb{T}^N}\left|\sum_i q_i\right|^{2p}dq=\sum_k C_{pk}\frac{N!}{(N-k)!}$$

with the coefficients being given by

$$C_{pk}=\sum_{\pi\in P(p),|\pi|=k}\binom{p}{b_1,\ldots,b_{|\pi|}}$$

where $b_1,\ldots,b_{|\pi|}$ are the lengths of the blocks of π.

Proof. This follows indeed exactly as Proposition 9.26 above, by replacing the exponent p by the exponent $p/2$, and by splitting the resulting sum as in the statement. □

Finally, here is a random walk formulation of the problem:

Proposition 9.28. *The moments of Φ have the following interpretation:*

1. *First, the moments of the enveloping sum $\int\widetilde{\Phi}^p$ count the loops of length $4p$ on the standard lattice $\mathbb{Z}^N\subset\mathbb{R}^N$, based at the origin.*
2. *$\int\Phi^p$ counts those loops which are "piecewise balanced", in the sense that each of the p consecutive 4-paths forming the loop satisfy $i+k=j+l$ modulo N.*

Proof. The first assertion follows from the formula in the proof of Proposition 9.26, and the second assertion follows from the formula in Proposition 9.25. □

This statement looks quite encouraging, but passing from (1) to (2) is quite a delicate task, because in order to interpret the condition $i+k=j+l$ we have to label the coordinate axes of $\mathbb{R}^N$ by elements of the cyclic group $\mathbb{Z}_N$, and this is a quite unfamiliar operation. In addition, in the real case the combinatorics becomes more complex due to the symmetries of the parameter space, and no further results are available so far.

10. Bistochastic form

In this section and the next two ones we discuss certain further analytic aspects of the complex Hadamard matrices. Let us begin with the following definition:

Definition 10.1. *A complex Hadamard matrix $H\in M_N(\mathbb C)$ is called bistochastic when the sums on all rows and all columns are equal. We denote by*

$$X_N^{bis}=\left\{H\in X_N\Big|H=\text{bistochastic}\right\}$$

the real algebraic manifold formed by such matrices.

The bistochastic Hadamard matrices are quite interesting objects, and include for instance all the circulant Hadamard matrices, that we discussed in section 9. Indeed, assuming that $H_{ij}=\xi_{j-i}$ is circulant, all rows and columns sum up to:

$$\lambda=\sum_i\xi_i$$

Let us begin, however, with some considerations regarding the real case. As a first and trivial remark, the first Walsh matrix $W_2=F_2$ looks better in bistochastic form:

$$\begin{pmatrix}1&1\\1&-1\end{pmatrix}\sim\begin{pmatrix}i&1\\1&i\end{pmatrix}$$

The second Walsh matrix $W_4=W_2\otimes W_2$ looks as well better in bistochastic form:

$$\begin{aligned}\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}&\sim\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}\\&\sim\begin{pmatrix}1&-1&-1&-1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix}\\&\sim\begin{pmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix}\end{aligned}$$

All this is quite interesting, philosophically speaking. Indeed, we have here a new idea, in connection with the various questions explained in sections 1-4 above, namely that of studying the real Hadamard matrices $H\in M_N(\pm1)$ by putting them in complex bistochastic form, $H'\in M_N(\mathbb T)$, and then studying these latter matrices.

Let us record here, as a partial conclusion, the following simple fact:

Theorem 10.2. *All the Walsh matrices can be put in bistocastic form, as follows:*

(1) *The matrices W_N with $N=4^n$ admit a real bistochastic form, namely:*

$$W_N\sim\begin{pmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix}^{\otimes n}$$

(2) *The matrices W_N with $N=2\times 4^n$ admit a complex bistochastic form, namely:*

$$W_N\sim\begin{pmatrix}i&1\\1&i\end{pmatrix}\otimes\begin{pmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix}^{\otimes n}$$

Proof. This follows indeed from the above discussion. □

Let us review now the material in section 9. According to the results there, and to the above-mentioned fact that circulant implies bistochastic, we have:

Theorem 10.3. *The class of bistochastic Hadamard matrices is stable under permuting rows and columns, and under taking tensor products. As examples, we have:*

(1) *The circulant and symmetric forms F_N' of the Fourier matrices F_N.*
(2) *The bistochastic and symmetric forms F_G' of the Fourier matrices F_G.*
(3) *The circulant and symmetric Backelin matrices, having size MN with $M|N$.*

Proof. In this statement the claim regarding permutations of rows and columns is clear. Assuming now that H,K are bistochastic, with sums λ,μ, we have:

$$\sum_{ia}(H\otimes K)_{ia,jb}=\sum_{ia}H_{ij}K_{ab}=\sum_iH_{ij}\sum_aK_{ab}=\lambda\mu$$

We have as well the following computation:

$$\sum_{jb}(H\otimes K)_{ia,jb}=\sum_{jb}H_{ij}K_{ab}=\sum_jH_{ij}\sum_bK_{ab}=\lambda\mu$$

Thus, the matrix $H\otimes K$ is bistochastic as well. As for the assertions (1,2,3), we already know all this, from section 9 above. □

In the above list of examples, (2) is the key entry. Indeed, while many interesting complex Hadamard matrices, such as the usual Fourier ones F_N, can be put in circulant form, this is something quite exceptional, which does not work any longer when looking at the general Fourier matrices F_G. To be more precise, with $G=\mathbb Z_{N_1}\times\ldots\times\mathbb Z_{N_k}$, we can consider the following matrix, which is equivalent to F_G:

$$F_G'=F_{N_1}'\otimes\ldots\otimes F_{N_k}'$$

Now since the tensor product of circulant matrices is not necessarily circulant, we can only say that this matrix F_G' is bistochastic. As a conclusion, the bistochastic Hadamard matrices are interesting objects, definitely worth some study. So, let us develop now some general theory, for such matrices. First, we have the following elementary result:

Proposition 10.4. *For an Hadamard matrix $H \in M_N(\mathbb{C})$, the following are equivalent:*

(1) *H is bistochastic, with sums λ.*
(2) *H is row-stochastic, with sums λ, and $|\lambda|^2 = N$.*

Proof. Both the implications are elementary, as follows:

(1) $\implies$ (2) If we denote by $H_1, \ldots, H_N \in \mathbb{T}^N$ the rows of H, we have indeed:

$$\begin{aligned} N &= \sum_i < H_1, H_i > \\ &= \sum_i \sum_j H_{1j} \bar{H}_{ij} \\ &= \sum_j H_{1j} \sum_i \bar{H}_{ij} \\ &= \sum_j H_{1j} \cdot \bar{\lambda} \\ &= |\lambda|^2 \end{aligned}$$

(2) $\implies$ (1) Consider the all-one vector $\xi = (1)_i \in \mathbb{C}^N$. The fact that H is row-stochastic with sums λ reads:

$$\begin{aligned} \sum_j H_{ij} = \lambda, \forall i &\iff \sum_j H_{ij}\xi_j = \lambda \xi_i, \forall i \\ &\iff H\xi = \lambda \xi \end{aligned}$$

Also, the fact that H is column-stochastic with sums λ reads:

$$\begin{aligned} \sum_i H_{ij} = \lambda, \forall j &\iff \sum_j H_{ij}\xi_i = \lambda \xi_j, \forall j \\ &\iff H^t\xi = \lambda \xi \end{aligned}$$

We must prove that the first condition implies the second one, provided that the row sum λ satisfies $|\lambda|^2 = N$. But this follows from the following computation:

$$\begin{aligned} H\xi = \lambda\xi &\implies H^*H\xi = \lambda H^*\xi \\ &\implies N^2\xi = \lambda H^*\xi \\ &\implies N^2\xi = \bar{\lambda} H^t\xi \\ &\implies H^t\xi = \lambda\xi \end{aligned}$$

Thus, we have proved both the implications, and we are done. $\square$

Here is another basic result, that we will need as well in what follows:

Proposition 10.5. *For a complex Hadamard matrix $H \in M_N(\mathbb{C})$, and a number $\lambda \in \mathbb{C}$ satisfying $|\lambda|^2 = N$, the following are equivalent:*

(1) *We have $H \sim H'$, with H' being bistochastic, with sums λ.*
(2) *$K_{ij} = a_i b_j H_{ij}$ is bistochastic with sums λ, for some $a, b \in \mathbb{T}^N$.*
(3) *The equation $Hb = \lambda \bar{a}$ has solutions $a, b \in \mathbb{T}^N$.*

Proof. Once again, this is an elementary result, the proof being as follows:

(1) $\iff$ (2) Since the permutations of the rows and columns preserve the bistochasticity condition, the equivalence $H \sim H'$ that we are looking for can be assumed to come only from multiplying the rows and columns by numbers in $\mathbb{T}$. Thus, we are looking for scalars $a_i, b_j \in \mathbb{T}$ such that $K_{ij} = a_i b_j H_{ij}$ is bistochastic with sums λ, as claimed.

(2) $\iff$ (3) The row sums of the matrix $K_{ij} = a_i b_j H_{ij}$ are given by:

$$\sum_j K_{ij} = \sum_j a_i b_j H_{ij} = a_i (Hb)_i$$

Thus K is row-stochastic with sums λ precisely when $Hb = \lambda \bar{a}$, and by using the equivalence in Proposition 10.4, we obtain the result. □

Finally, here is an extension of the excess inequality from section 2 above:

Theorem 10.6. *For a complex Hadamard matrix $H \in M_N(\mathbb{C})$, the excess,*

$$E(H) = \sum_{ij} H_{ij}$$

satisfies $|E(H)| \leq N\sqrt{N}$, with equality if and only if H is bistochastic.

Proof. In terms of the all-one vector $\xi = (1)_i \in \mathbb{C}^N$, we have:

$$E(H) = \sum_{ij} H_{ij} = \sum_{ij} H_{ij} \xi_j \bar{\xi}_i = \sum_i (H\xi)_i \bar{\xi}_i =< H\xi, \xi >$$

Now by using the Cauchy-Schwarz inequality, along with the fact that $U = H/\sqrt{N}$ is unitary, and hence of norm 1, we obtain, as claimed:

$$|E(H)| \leq ||H\xi|| \cdot ||\xi|| \leq ||H|| \cdot ||\xi||^2 = N\sqrt{N}$$

Regarding now the equality case, this requires the vectors $H\xi, \xi$ to be proportional, and so our matrix H to be row-stochastic. Now, let us assume:

$$H\xi = \lambda \xi$$

We have then $|\lambda|^2 = N$, and by Proposition 10.4 we obtain the result. □

Let us go back now to the fundamental question, which already appeared several times in the above, of putting an arbitrary Hadamard matrix in bistochastic form. As already explained, we are interested in solving this question in general, and in particular in the real case, with potential complex reformulations of the HC and CHC at stake. What we know so far on this subject can be summarized as follows:

Proposition 10.7. *An Hadamard matrix $H \in M_N(\mathbb{C})$ can be put in bistochastic form when one of the following conditions is satisfied:*

(1) *The equations $|Ha|_i = \sqrt{N}$, with $i = 1, \ldots, N$, have solutions $a \in \mathbb{T}^N$.*
(2) *The quantity $|E|$ attains its maximum $N\sqrt{N}$ over the equivalence class of H.*

Proof. This follows indeed from Proposition 10.4 and Proposition 10.5 above, which altogether gives the equivalence between the two conditions in the statement. □

Thus, we have two approaches to the problem, one algebraic, and one analytic. Let us first discuss the algebraic approach, coming from (1) above. What we have there is a certain system of N equations, having as unknowns N real variables, namely the phases of $a_1, \ldots, a_N$. This system is highly non-linear, but can be solved, however, via a certain non-explicit method, as explained by Idel and Wolf in [75].

In order to discuss this material, which is quite advanced, let us begin with some preliminaries. The complex projective space appears by definition as follows:

$$P^{N-1}_{\mathbb{C}} = (\mathbb{C}^N - \{0\}) \big/ < x = \lambda y >$$

Inside this projective space, we have the Clifford torus, constructed as follows:

$$\mathbb{T}^{N-1} = \left\{ (z_1, \ldots, z_N) \in P^{N-1}_{\mathbb{C}} \Big| |z_1| = \ldots = |z_N| \right\}$$

With these conventions, we have the following result, from [75]:

Proposition 10.8. *For a unitary matrix $U \in U_N$, the following are equivalent:*

(1) *There exist $L, R \in U_N$ diagonal such that the following matrix is bistochastic:*
$$U' = LUR$$
(2) *The standard torus $\mathbb{T}^N \subset \mathbb{C}^N$ satisfies:*
$$\mathbb{T}^N \cap U\mathbb{T}^N \neq \emptyset$$
(3) *The Clifford torus $\mathbb{T}^{N-1} \subset P^{N-1}_{\mathbb{C}}$ satisfies:*
$$\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$$

Proof. These equivalences are all elementary, as follows:

(1) $\Longrightarrow$ (2) Assuming that $U' = LUR$ is bistochastic, which in terms of the all-1 vector ξ means $U'\xi = \xi$, if we set $f = R\xi \in \mathbb{T}^N$ we have:

$$Uf = \bar{L}U'\bar{R}f = \bar{L}U'\xi = \bar{L}\xi \in \mathbb{T}^N$$

Thus we have $Uf \in \mathbb{T}^N \cap U\mathbb{T}^N$, which gives the conclusion.

(2) $\implies$ (1) Given $g \in \mathbb{T}^N \cap U\mathbb{T}^N$, we can define R, L as follows:

$$R = diag(g_1, \ldots, g_N)$$

$$\bar{L} = diag((Ug)_1, \ldots, (Ug)_N)$$

With these values for L, R, we have then the following formulae:

$$R\xi = g \quad , \quad \bar{L}\xi = Ug$$

Thus the matrix $U' = LUR$ is bistochastic, because:

$$U'\xi = LUR\xi = LUg = \xi$$

(2) $\implies$ (3) This is clear, because $\mathbb{T}^{N-1} \subset P^{N-1}_{\mathbb{C}}$ appears as the projective image of $\mathbb{T}^N \subset \mathbb{C}^N$, and so $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1}$ appears as the projective image of $\mathbb{T}^N \cap U\mathbb{T}^N$.

(3) $\implies$ (2) We have indeed the following equivalence:

$$\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset \iff \exists \lambda \neq 0, \lambda\mathbb{T}^N \cap U\mathbb{T}^N \neq \emptyset$$

But $U \in U_N$ implies $|\lambda| = 1$, and this gives the result. □

The point now is that the condition (3) above is something familiar in symplectic geometry, and known to hold for any $U \in U_N$. Thus, following [75], we have:

Theorem 10.9. *Any unitary matrix $U \in U_N$ can be put in bistochastic form,*

$$U' = LUR$$

with $L, R \in U_N$ being both diagonal, via a certain non-explicit method.

Proof. As already mentioned, the condition $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$ in Proposition 10.8 (3) is something quite natural in symplectic geometry. To be more precise, $\mathbb{T}^{N-1} \subset P^{N-1}_{\mathbb{C}}$ is a Lagrangian submanifold, $\mathbb{T}^{N-1} \to U\mathbb{T}^{N-1}$ is a Hamiltonian isotopy, and a result from [42], [48] states that $\mathbb{T}^{N-1}$ cannot be displaced from itself via a Hamiltonian isotopy. Thus, the results in [42], [48] tells us that $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$ holds indeed, for any $U \in U_N$. We therefore obtain the result, via Proposition 10.8. See [75]. □

In relation now with our Hadamard matrix questions, we have:

Theorem 10.10. *Any complex Hadamard matrix can be put in bistochastic form, up to the standard equivalence relations for such matrices.*

Proof. This follows indeed from Theorem 10.9, because if $H = \sqrt{N}U$ is Hadamard then so is $H' = \sqrt{N}U'$, and with the remark that, in what regards the equivalence relation, we just need the multiplication of the rows and columns by scalars in $\mathbb{T}$. □

As explained in [75], the various technical results from [42], [48] show that in the generic, "transverse" situation, there are at least 2^{N-1} ways of putting a unitary matrix $U\in U_N$ in bistochastic form, and this modulo the obvious transformation $U\to zU$, with $|z|=1$. Thus, the question of explicitely putting the Hadamard matrices $H\in M_N(\mathbb C)$ in bistochastic form remains open, and open as well is the question of finding a simpler proof for the fact that this can be done indeed, without using [42], [48].

Regarding this latter question, a possible approach comes from the excess result from Theorem 10.6 above. Indeed, in view of the remark there, it is enough to show that the law of $|E|$ over the equivalence class of H has $N\sqrt{N}$ as upper support bound. In order to comment on this, let us first formulate:

Definition 10.11. *The glow of $H\in M_N(\mathbb C)$ is the measure $\mu\in\mathcal P(\mathbb C)$ given by:*

$$\int_{\mathbb C}\varphi(x)d\mu(x)=\int_{\mathbb T^N\times\mathbb T^N}\varphi\left(\sum_{ij}a_ib_jH_{ij}\right)d(a,b)$$

That is, the glow is the law of the excess $E=\sum_{ij}H_{ij}$ over the equivalence class of H.

In this definition H can be any complex matrix, but the equivalence relation is the one for the complex Hadamard matrices. To be more precise, let us call two matrices $H,K\in M_N(\mathbb C)$ equivalent if one can pass from one to the other by permuting rows and columns, or by multiplying the rows and columns by numbers in $\mathbb T$. Now since permuting rows and columns does not change the quantity $E=\sum_{ij}H_{ij}$, we can restrict attention from the full equivalence group $G=(S_N\rtimes\mathbb T^N)\times(S_N\rtimes\mathbb T^N)$ to the smaller group $G'=\mathbb T^N\times\mathbb T^N$, and we obtain the measure μ in Definition 10.11.

As in the real case, the terminology comes from a picture of the following type, with the stars $*$ representing the entries of our matrix, and with the switches being supposed now to be continuous, randomly changing the phases of the concerned entries:

$$\begin{matrix}\to&&*&*&*&*\\\to&&*&*&*&*\\\to&&*&*&*&*\\\to&&*&*&*&*\\\\&&\uparrow&\uparrow&\uparrow&\uparrow\end{matrix}$$

In short, what we have here is a complex generalization of the Gale-Berlekamp game [67], [116], and this is where the main motivation for studying the glow comes from.

We are in fact interested in computing a real measure, because we have:

Proposition 10.12. *The laws μ,μ^+ of $E,|E|$ over the torus $\mathbb{T}^N\times\mathbb{T}^N$ are related by*

$$\mu=\varepsilon\times\mu^+$$

where $\times$ is the multiplicative convolution, and ε is the uniform measure on $\mathbb{T}$.

Proof. We have $E(\lambda H)=\lambda E(H)$ for any $\lambda\in\mathbb{T}$, and so $\mu=law(E)$ is invariant under the action of $\mathbb{T}$. Thus μ must decompose as $\mu=\varepsilon\times\mu^+$, where μ^+ is a certain probability measure on $[0,\infty)$, and this measure μ^+ is the measure in the statement. □

In particular, we can see from the above result that the glow is invariant under rotations. With this observation made, we can formulate the following result:

Theorem 10.13. *The glow of any Hadamard matrix $H\in M_N(\mathbb{C})$, or more generally of any $H\in\sqrt{N}U_N$, satisfies the following conditions, where $\mathbb{D}$ is the unit disk,*

$$N\sqrt{N}\,\mathbb{T}\subset supp(\mu)\subset N\sqrt{N}\,\mathbb{D}$$

with the inclusion on the right coming from Cauchy-Schwarz, and with the inclusion on the left corresponding to the fact that H can be put in bistochastic form.

Proof. In this statement the inclusion on the right comes indeed from Cauchy-Schwarz, as explained in the proof of Theorem 10.6 above, with the remark that the computation there only uses the fact that the rescaled matrix $U=H/\sqrt{N}$ is unitary.

Regarding now the inclusion on the left, we know from Theorem 10.9 that H can be put in bistochastic form. According to Proposition 10.7, this tells us that we have:

$$N\sqrt{N}\,\mathbb{T}\cap supp(\mu)\neq\emptyset$$

Now by using the rotational invariance of the glow, and hence of its support, coming from Proposition 10.12, we obtain from this:

$$N\sqrt{N}\,\mathbb{T}\subset supp(\mu)$$

Thus, we are led to the conclusions in the statement. □

The challenging question is that of proving the above result by using probabilistic techniques. Indeed, as explained in section 9, the support of a measure can be recaptured from the moments, by computing a limit. Thus, knowing the moments of the glow well enough would solve the problem. Regarding these moments, the formula is as follows:

Proposition 10.14. *For $H\in M_N(\mathbb{T})$ the even moments of $|E|$ are given by*

$$\int_{\mathbb{T}^N\times\mathbb{T}^N}|E|^{2p}=\sum_{[i]=[k],[j]=[l]}\frac{H_{i_1j_1}\ldots H_{i_pj_p}}{H_{k_1l_1}\ldots H_{k_pl_p}}$$

where the sets between brackets are by definition sets with repetition.

Proof. We have indeed the following computation:

$$\begin{aligned}\int_{\mathbb{T}^N\times\mathbb{T}^N}|E|^{2p} &= \int_{\mathbb{T}^N\times\mathbb{T}^N}\Big|\sum_{ij}H_{ij}a_ib_j\Big|^{2p}\\ &= \int_{\mathbb{T}^N\times\mathbb{T}^N}\left(\sum_{ijkl}\frac{H_{ij}}{H_{kl}}\cdot\frac{a_ib_j}{a_kb_l}\right)^p\\ &= \sum_{ijkl}\frac{H_{i_1j_1}\ldots H_{i_pj_p}}{H_{k_1l_1}\ldots H_{k_pl_p}}\int_{\mathbb{T}^N}\frac{a_{i_1}\ldots a_{i_p}}{a_{k_1}\ldots a_{k_p}}\int_{\mathbb{T}^N}\frac{b_{j_1}\ldots b_{j_p}}{b_{l_1}\ldots b_{l_p}}\end{aligned}$$

Now since the integrals at right equal respectively the Kronecker symbols $\delta_{[i],[k]}$ and $\delta_{[j],[l]}$, we are led to the formula in the statement. $\square$

With this formula in hand, the main result, regarding the fact that the complex Hadamard matrices can be put in bistochastic form, reformulates as follows:

Theorem 10.15. *For a complex Hadamard matrix $H\in M_N(\mathbb{T})$ we have*

$$\lim_{p\to\infty}\left(\sum_{[i]=[k],[j]=[l]}\frac{H_{i_1j_1}\ldots H_{i_pj_p}}{H_{k_1l_1}\ldots H_{k_pl_p}}\right)^{1/p}=N^3$$

coming from the fact that H can be put in bistochastic form.

Proof. This follows from the well-known fact that the maximum of a bounded function $\Theta:X\to[0,\infty)$ can be recaptured via following formula:

$$\max(\Theta)=\lim_{p\to\infty}\left(\int_X\Theta(x)^p\,dx\right)^{1/p}$$

With $X=\mathbb{T}^N\times\mathbb{T}^N$ and with $\Theta=|E|^2$, we conclude that the limit in the statement is the square of the upper bound of the glow. But, according to Theorem 10.13, this upper bound is known to be $\leq N^3$ by Cauchy-Schwarz, and the equality holds by [75]. $\square$

To conclude now, the challenging question is that of finding a direct proof for Theorem 10.15. All this would provide an alternative aproach to the results in [75], which would be of course still not explicit, but which would use at least some more familiar tools. We will discuss such questions in section 11 below, with the remark however that the problems at $N\in\mathbb{N}$ fixed being quite difficult, we will do a $N\to\infty$ study only.

Getting away now from these difficult questions, we have nothing concrete so far, besides the list of examples from Theorem 10.3, coming from the circulant matrix considerations in section 9. So, our purpose will be that of extending that list. A first natural question is that of looking at the Butson matrix case. We have here the following result:

Proposition 10.16. *Assuming that $H_N(l)$ contains a bistochastic matrix, the equations*

$$\begin{aligned} a_0+a_1+\ldots+a_{l-1} &= N \\ |a_0+a_1w+\ldots+a_{l-1}w^{l-1}|^2 &= N \end{aligned}$$

must have solutions, over the positive integers.

Proof. This is a reformulation of the equality $|\lambda|^2=N$, from Proposition 10.5 above. Indeed, if we set $w=e^{2\pi i/l}$, and we denote by $a_i\in\mathbb{N}$ the number of w^i entries appearing in the first row of our matrix, then the row sum of the matrix is given by:

$$\lambda=a_0+a_1w+\ldots+a_{l-1}w^{l-1}$$

Thus, we obtain the system of equations in the statement. □

The point now is that, in practice, we are led precisely to the Turyn obstructions from section 9 above. At very small values of l, the obstructions are as follows:

Theorem 10.17. *Assuming that $H_N(l)$ contains a bistochastic matrix, the following equations must have solutions, over the integers:*

(1) $l=2$*:* $4n^2=N$.
(2) $l=3$*:* $x^2+y^2+z^2=2N$*, with* $x+y+z=0$.
(3) $l=4$*:* $a^2+b^2=N$.

Proof. This follows indeed from the results that we have:

(1) This is something well-known, which follows from Proposition 10.17.

(2) This is best viewed by using Proposition 10.17, and the following formula, that we already know, from section 5 above:

$$\left|a+bw+cw^2\right|^2=\frac{1}{2}[(a-b)^2+(b-c)^2+(c-a)^2]$$

At the level of the concrete obstructions, we must have for instance $5\nmid N$. Indeed, this follows as in the proof of the de Launey obstruction for $H_N(3)$ with $5|N$.

(3) This follows again from Proposition 10.17, and from $|a+ib|^2=a^2+b^2$. □

As a conclusion, nothing much interesting is going on in the Butson matrix case, with various arithmetic obstructions, that we partly already met, appearing here. See [85]. In order to reach, however, to a number of positive results, beyond those in Theorem 10.4, we can investigate various special classes of matrices, such as the Diţă products. In order to formulate our results, we will use the following notion:

Definition 10.18. *We say that a complex Hadamard matrix $H\in M_N(\mathbb{C})$ is in "almost bistochastic form" when all the row sums belong to $\sqrt{N}\cdot\mathbb{T}$.*

Observe that, assuming that this condition holds, the matrix H can be put in bistochastic form, just by multiplying its rows by suitable numbers from $\mathbb{T}$. We will be particularly interested here in the special situation where the affine deformations $H^q \in M_N(\mathbb{C})$ of a given complex Hadamard matrix $H \in M_N(\mathbb{C})$ can be put in almost bistochastic form, independently of the value of the parameter q. For the simplest deformations, namely those of $F_2 \otimes F_2$, this is indeed the case:

Proposition 10.19. *The deformations of $F_2 \otimes F_2$, with parameter matrix $Q = (\begin{smallmatrix} p & q \\ r & s \end{smallmatrix})$,*

$$F_2 \otimes_Q F_2 = \begin{pmatrix} p & q & p & q \\ p & -q & p & -q \\ r & s & -r & -s \\ r & -s & -r & s \end{pmatrix}$$

can be put in almost bistochastic form, independently of the value of Q.

Proof. By multiplying the columns of the matrix in the statement with $1, 1, -1, 1$ respectively, we obtain the following matrix:

$$F_2 \otimes''_Q F_2 = \begin{pmatrix} p & q & -p & q \\ p & -q & -p & -q \\ r & s & r & -s \\ r & -s & r & s \end{pmatrix}$$

The row sums of this matrix being $2q, -2q, 2r, 2r \in 2\mathbb{T}$, we are done. □

We will see later on that the above matrix $F_2 \otimes''_Q F_2$ is equivalent to a certain matrix $F_2 \otimes' F_2$, which looks a bit more complicated, but is part of a series $F_N \otimes' F_N$. Now back to the general case, we have the following result:

Theorem 10.20. *A deformed tensor product $H \otimes_Q K$ can be put in bistochastic form when there exist numbers $x_a^i \in \mathbb{T}$ such that with*

$$G_{ib} = \frac{(K^* x^i)_b}{Q_{ib}}$$

we have $|(H^* G)_{ib}| = \sqrt{MN}$, for any i, b.

Proof. The deformed tensor product $L = H \otimes_Q K$ is given by the following formula:

$$L_{ia,jb} = Q_{ib} H_{ij} K_{ab}$$

By multiplying the columns by scalars $R_{jb} \in \mathbb{T}$, this matrix becomes:

$$L'_{ia,jb} = R_{jb} Q_{ib} H_{ij} K_{ab}$$

The row sums of this matrix are given by:

$$\begin{aligned} S'_{ia} &= \sum_{jb} R_{jb}Q_{ib}H_{ij}K_{ab} \\ &= \sum_b K_{ab}Q_{ib}\sum_j H_{ij}R_{jb} \\ &= \sum_b K_{ab}Q_{ib}(HR)_{ib} \end{aligned}$$

Consider now the following variables:

$$C_b^i = Q_{ib}(HR)_{ib}$$

In terms of these variables, the rows sums are given by:

$$S'_{ia} = \sum_b K_{ab}C_b^i = (KC^i)_a$$

Thus $H \otimes_Q K$ can be put in bistochastic form when we can find scalars $R_{jb} \in \mathbb{T}$ and $x_a^i \in \mathbb{T}$ such that, with $C_b^i = Q_{ib}(HR)_{ib}$, the following condition is satisfied:

$$(KC^i)_a = \sqrt{MN}x_a^i \quad , \quad \forall i, a$$

But this condition is equivalent to the following condition:

$$KC^i = \sqrt{MN}x^i \quad , \quad \forall i$$

Now by multiplying to the left by K^*, we are led to the following condition:

$$\sqrt{N}C^i = \sqrt{M}K^*x^i \quad , \quad \forall i$$

Now by recalling that $C_b^i = Q_{ib}(HR)_{ib}$, this condition is equivalent to:

$$\sqrt{N}Q_{ib}(HR)_{ib} = \sqrt{M}(K^*x^i)_b \quad , \quad \forall i, b$$

Consider now the variables in the statement, namely:

$$G_{ib} = \frac{(K^*x^i)_b}{Q_{ib}}$$

In terms of these variables, the above condition reads:

$$\sqrt{N}(HR)_{ib} = \sqrt{M}G_{ib} \quad , \quad \forall i, b$$

But this condition is equivalent to:

$$\sqrt{N}HR = \sqrt{M}G$$

Now by multiplying to the left by H^*, we are led to the following condition:

$$\sqrt{MN}R = H^*G$$

Thus, we have obtained the condition in the statement. $\square$

As an illustration for the above result, assume that H, K can be put in bistochastic form, by using vectors $y \in \mathbb{T}^M, z \in \mathbb{T}^N$. If we set $x_a^i = y_i z_a$, with $Q = 1$ we have:

$$G_{ib} = (K^* x^i)_b = [K^*(y_i z)]_b = y_i (K^* z)_b$$

We therefore obtain the following formula:

$$(H^* G)_{ib} = \sum_j (H^*)_{ij} G_{jb} = \sum_j (H^*)_{ij} y_j (K^* z)_b = (H^* y)_i (K^* z)_b$$

Thus the usual tensor product $H \otimes K$ can be put in bistochastic form as well.

In the case $H = F_M$ the equations simplify, and we have:

Proposition 10.21. *A deformed tensor product $F_M \otimes_Q K$ can be put in bistochastic form when there exist numbers $x_a^i \in \mathbb{T}$ such that with*

$$G_{ib} = \frac{(K^* x^i)_b}{Q_{ib}}$$

we have the following formulae, with l being taken modulo M:

$$\sum_j G_{jb} \bar{G}_{j+l,b} = MN \delta_{l,0} \quad , \quad \forall l, b$$

Moreover, the $M \times N$ matrix $|G_{jb}|^2$ is row-stochastic with sums N^2, and the $l = 0$ equations state that this matrix must be column-stochastic, with sums MN.

Proof. With notations from Theorem 10.20, and with $w = e^{2\pi i/M}$, we have:

$$(H^* G)_{ib} = \sum_j w^{-ij} G_{jb}$$

The absolute value of this number can be computed as follows:

$$\begin{aligned} |(H^* G)_{ib}|^2 &= \sum_{jk} w^{i(k-j)} G_{jb} \bar{G}_{kb} \\ &= \sum_{jl} w^{il} G_{jb} \bar{G}_{j+l,b} \\ &= \sum_l w^{il} \sum_j G_{jb} \bar{G}_{j+l,b} \end{aligned}$$

If we denote by v_l^b the sum on the right, we obtain:

$$|(H^* G)_{ib}|^2 = \sum_l w^{il} v_l^b = (F_M v^b)_i$$

Now if we denote by ξ the all-one vector in $\mathbb{C}^M$, the condition $|(H^* G)_{ib}| = \sqrt{MN}$ for any i, b found in Theorem 10.20 above reformulates as follows:

$$F^M v^b = MN \xi \quad , \quad \forall b$$

By multiplying to the left by F_M^*/M, this condition is equivalent to:

$$v^b = NF_M^*\xi = \begin{pmatrix} MN \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Let us examine the first equation, $v_0^b = MN$. By definition of v_l^b, we have:

$$v_0^b = \sum_j G_{jb}\bar{G}_{jb} = \sum_j |G_{jb}|^2$$

Now recall from Theorem 10.20 that we have, for certain numbers $x_b^j \in \mathbb{T}$:

$$G_{jb} = \frac{(K^*x^j)_b}{Q_{jb}}$$

Since we have $Q_{jb} \in \mathbb{T}$ and $K^*/\sqrt{N} \in U_N$, we obtain:

$$\sum_b |G_{jb}|^2 = \sum_b |(K^*x^j)_b|^2 = ||K^*x^j||_2^2 = N||x^j||_2^2 = N^2$$

Thus the $M \times N$ matrix $|G_{jb}|^2$ is row-stochastic, with sums N^2, and our equations $v_0^b = MN$ for any b state that this matrix must be column-stochastic, with sums MN.

Regarding now the other equations that we found, namely $v_l^b = 0$ for $l \neq 0$, by definition of v_l^b and of the variables G_{jb}, these state that we must have:

$$\sum_j G_{jb}\bar{G}_{j+l,b} = 0 \quad , \quad \forall l \neq 0, \forall b$$

Thus, we are led to the conditions in the statement. $\square$

As an illustration for this result, let us go back to the $Q = 1$ situation, explained after Theorem 10.20. By using the formula $G_{ib} = y_i(K^*z)_b$ there, we have:

$$\begin{aligned}
\sum_j G_{jb}\bar{G}_{j+l,b} &= \sum_j y_j(K^*z)_b \, \overline{y}_{j+l}\overline{(K^*z)_b} \\
&= |(K^*z)_b|^2 \sum_j \frac{y_j}{y_{j+l}} \\
&= M \cdot N\delta_{l,0}
\end{aligned}$$

Thus, if K can be put in bistochastic form, then so can be put $F_M \otimes K$. As a second illustration, let us go back to the matrices $F_2 \otimes'_Q F_2$ from the proof of Proposition 10.19

above. The vector of the row sums being $S = (2q, -2q, 2r, 2r)$, we have $x = (q, -q, r, r)$, and so we obtain the following formulae for the upper entries of G:

$$G_{0b} = \frac{\left[\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}q\\-q\end{pmatrix}\right]_b}{Q_{0b}} = \frac{\begin{pmatrix}0\\2q\end{pmatrix}_b}{Q_{0b}}$$

As for the lower entries of G, these are as follows:

$$G_{1b} = \frac{\left[\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}r\\r\end{pmatrix}\right]_b}{Q_{1b}} = \frac{\begin{pmatrix}2r\\0\end{pmatrix}_b}{Q_{1b}}$$

Thus, in this case the matrix G is as follows, independently of Q:

$$G = \begin{pmatrix}0&2\\2&0\end{pmatrix}$$

In particular, we see that the conditions in Proposition 10.21 are satisfied. As a main application now, we have the following result:

Theorem 10.22. *The Diţă deformations of tensor squares of Fourier matrices,*

$$F_N \otimes_Q F_N$$

can be put in almost bistochastic form, independently of the value of $Q \in M_N(\mathbb{T})$.

Proof. We use Proposition 10.21 above, with $M = N$, and with $K = F_N$. Let $w = e^{2\pi i/N}$, and consider the vectors $x^i \in \mathbb{T}^N$ given by:

$$x^i = (w^{(i-1)a})_a$$

Since $K^*K = N1_N$, and x^i are the column vectors of K, shifted by 1, we have:

$$K^*x^0 = \begin{pmatrix}0\\0\\ \vdots\\0\\N\end{pmatrix} \quad , \quad K^*x^1 = \begin{pmatrix}N\\0\\ \vdots\\0\\0\end{pmatrix} \quad , \ \ldots\ , \quad K^*x^{N-1} = \begin{pmatrix}0\\0\\ \vdots\\N\\0\end{pmatrix}$$

We conclude that we have $(K^*x^i)_b = N\delta_{i-1,b}$, and so the matrix G is given by:

$$G_{ib} = \frac{N\delta_{i-1,b}}{Q_{ib}}$$

With this formula in hand, the sums in Proposition 10.21 are given by:

$$\sum_j G_{jb}\bar{G}_{j+l,b} = \sum_j \frac{N\delta_{j-1,b}}{Q_{jb}} \cdot \frac{N\delta_{j+l-1,b}}{Q_{j+l,b}}$$

In the case $l\neq 0$ we clearly get 0, because the products of Kronecker symbols are 0. In the case $l=0$ the denominators are $|Q_{jb}|^2=1$, and we obtain:

$$\sum_jG_{jb}\bar{G}_{jb}=N^2\sum_j\delta_{j-1,b}=N^2$$

Thus, the conditions in Proposition 10.21 are satisfied, and we obtain the result. □

Here is an equivalent formulation of the above result:

Theorem 10.23. *The matrix $F_N\otimes'_QF_N$, with $Q\in M_N(\mathbb T)$, defined by*

$$(F_N\otimes'_QF_N)_{ia,jb}=\frac{w^{ij+ab}}{w^{bj+j}}\cdot\frac{Q_{ib}}{Q_{b+1,b}}$$

where $w=e^{2\pi i/N}$ is almost bistochastic, and equivalent to $F_N\otimes_QF_N$.

Proof. Our claim is that this is the matrix constructed in the proof of Theorem 10.22. Indeed, let us first go back to the proof of Theorem 10.20. In the case $M=N$ and $H=K=F_N$, the Diţă deformation $L=H\otimes_QK$ studied there is given by:

$$L_{ia,jb}=Q_{ib}H_{ij}K_{ab}=w^{ij+ab}Q_{ib}$$

As explained in the proof of Theorem 10.22, if the conditions in the statement there are satisfied, then the matrix $L'_{ia,jb}=R_{jb}L_{ia,jb}$ is almost bistochastic, where:

$$\sqrt{MN}\cdot R=H^*G$$

In our case now, $M=N$ and $H=K=F_N$, we know from the proof of Proposition 10.21 that the choice of G which makes work Theorem 10.22 is as follows:

$$G_{ib}=\frac{N\delta_{i-1,b}}{Q_{ib}}$$

With this formula in hand, we can compute the matrix R, as follows:

$$R_{jb}=\frac{1}{N}(H^*G)_{jb}=\frac{1}{N}\sum_iw^{-ij}G_{ib}=\sum_iw^{ij}\cdot\frac{\delta_{i-1,b}}{Q_{ib}}=\frac{w^{-(b+1)j}}{Q_{b+1,b}}$$

Thus, the modified version of $F_N\otimes_QF_N$ which is almost bistochastic is given by:

$$\begin{aligned}L'_{ia,jb}&=R_{jb}L_{ia,jb}\\&=\frac{w^{-(b+1)j}}{Q_{b+1,b}}\cdot w^{ij+ab}Q_{ib}\\&=\frac{w^{ij+ab}}{w^{bj+j}}\cdot\frac{Q_{ib}}{Q_{b+1,b}}\end{aligned}$$

Thus we have obtained the formula in the statement, and we are done. □

As an illustration, let us work out the case $N=2$. Here we have $w=-1$, and with $Q=\binom{p\ q}{r\ s}$, and then with $u=\frac{p}{r}, v=\frac{s}{q}$, we obtain the following matrix:

$$F_2\otimes_Q F_2=\begin{pmatrix}\frac{p}{r}&\frac{q}{q}&-\frac{p}{r}&\frac{q}{q}\\ \frac{p}{r}&-\frac{q}{q}&-\frac{p}{r}&-\frac{q}{q}\\ \frac{r}{r}&\frac{s}{q}&\frac{r}{r}&-\frac{s}{q}\\ \frac{r}{r}&-\frac{s}{q}&\frac{r}{r}&\frac{s}{q}\end{pmatrix}=\begin{pmatrix}u&1&-u&1\\ u&-1&-u&-1\\ 1&v&1&-v\\ 1&-v&1&v\end{pmatrix}$$

In general, the question of putting the Diţă deformations of the tensor products in explicit bistochastic form remains open. Open as well is the question of putting the arbitrary affine deformations of the Fourier matrices in explicit bistochastic form.

A related interesting question, which can serve as a good motivation for all this, is whether the real Hadamard matrices, $H\in M_N(\pm1)$, can be put or not in bistochastic form, in an explicit way. This is certainly true for the Walsh matrices, but for the other basic examples, such as the Paley or the Williamson matrices, no results seem to be known so far. Having such a theory would be potentially very interesting, with a complex reformulation of the HC and of the other real Hadamard questions at stake.

We already know that we are done with the case $N\leq 8$. The next problem regards the Paley matrix at $N=12$, which is the unique real Hadamard matrix there:

$$P_{12}\sim P_{12}^1\sim P_{12}^2$$

This matrix cannot be put of course in real bistochastic form, its size being not of the form $N=4n^2$. Nor can it be put in bistochastic form over $\{\pm1,\pm i\}$, because the Turyn obstruction for matrices over $\{\pm1,\pm i\}$ is $N=a^2+b^2$, and we have:

$$12\neq a^2+b^2$$

However, the question of putting P_{12} in bistochastic form over the 3-roots of unity makes sense, because the Turyn obstruction here is:

$$x+y+z=0$$

$$x^2+y^2+z^2=2N$$

And, we do have solutions to these equations at $N=12$, as follows:

$$4^2+(-2)^2+(-2)^2=24$$

Another question is whether P_{12} can be put in bistochastic form over the 8-roots of unity. In order to comment on this, let us first work out the Turyn obstruction, for the bistochastic matrices having as entries the 8-roots of unity. The result is as follows:

Proposition 10.24. *The Turyn obstruction for the bistochastic matrices having as entries the 8-roots of unity is*

$$x^2+y^2+z^2+t^2=N$$
$$xy+yz+zt=xt$$

with $x,y,z,t\in\mathbb Z$.

Proof. The 8-roots of unity are as follows, with $w=e^{\pi i/4}$:

$$1,w,i,iw,-1,-w,-i,-iw$$

Thus, we are led to an equation as follows, with $x,y,z,t\in\mathbb Z$:

$$|x+wy+iz+iwt|^2=N$$

We have the following computation:

$$\begin{aligned}
&|x+wy+iz+iwt|^2\\
=&\ (x+wy+iz+iwt)(x-iwy-iz-wt)\\
=&\ x^2+y^2+z^2+t^2+w(1-i)(xy+yz+zt-xt)\\
=&\ x^2+y^2+z^2+t^2-\sqrt2(xy+yz+zt-xt)
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

The point now is that the equations in Proposition 10.24 do have solutions at $N=12$, namely:

$$x=0,y=2,z=-2,t=\pm2$$

Summarizing, the Paley matrix P_{12} cannot be put in bistochastic form over the 4-roots, but the question makes sense over the 3-roots, and over the 8-roots. There are many questions here, and as already mentioned above, all this can potentially lead to a complex reformulation of the HC and of the other real Hadamard matrix questions.

11. Glow computations

We discuss here the computation of the glow of the complex Hadamard matrices, in the $N \to \infty$ limit. As a first motivation, we have the Gale-Berlekamp game [67], [116]. Another motivation comes from the questions regarding the bistochastic matrices, in relation with [75], explained in section 10. Finally, we have the question of connecting the defect, and other invariants of the Hadamard matrices, to the glow.

Let us begin by reviewing the few theoretical things that we know about the glow, from section 10. The main results there can be summarized as follows:

Theorem 11.1. *The glow of $H \in M_N(\mathbb{C})$, which is the law $\mu \in \mathcal{P}(\mathbb{C})$ of the excess*

$$E = \sum_{ij} H_{ij}$$

over the Hadamard equivalence class of H, has the following properties:

(1) *$\mu = \varepsilon \times \mu^+$, where $\mu^+ = law(|E|)$.*
(2) *μ is invariant under rotations.*
(3) *$H \in \sqrt{N} U_N$ implies $supp(\mu) \subset N\sqrt{N}\,\mathbb{D}$.*
(4) *$H \in \sqrt{N} U_N$ implies as well $N\sqrt{N}\,\mathbb{T} \subset supp(\mu)$.*

Proof. We already know all this from section 10, the idea being as follows:

(1) This follows indeed by using $H \to zH$ with $|z| = 1$.

(2) This follows from (1), the convolution with ε bringing the invariance.

(3) This folllows indeed from Cauchy-Schwarz.

(4) This is something highly non-trivial, coming from [75]. □

In what follows we will be mainly interested in the Hadamard matrix case, but since the computations here are quite difficult, let us begin our study with other matrices. It is convenient to normalize our matrices, by assuming that the corresponding 2-norm $||H||_2 = \sqrt{\sum_{ij} |H_{ij}|^2}$ takes the same value as for the Hadamard matrices, namely:

$$||H||_2 = N$$

We recall that the complex Gaussian distribution $\mathcal{C}$ is the law of $z = \frac{1}{\sqrt{2}}(x + iy)$, where x, y are independent standard Gaussian variables. In order to detect this distribution, we can use the moment method, and the following well-known formula:

$$\mathbb{E}(|z|^{2p}) = p!$$

Finally, we use the symbol $\sim$ to denote an equality of distributions.

With these conventions, we have the following result:

Proposition 11.2. *We have the following computations:*

(1) *For the rescaled identity $\widetilde{I}_N=\sqrt{N}I_N$ we have*

$$E\sim\sqrt{N}(q_1+\ldots+q_N)$$

with $q\in\mathbb T^N$ random. With $N\to\infty$ we have $E/N\sim\mathcal C$.

(2) *For the flat matrix $J_N=(1)_{ij}$ we have*

$$E\sim(a_1+\ldots+a_N)(b_1+\ldots+b_N)$$

with $(a,b)\in\mathbb T^N\times\mathbb T^N$ random. With $N\to\infty$ we have $E/N\sim\mathcal C\times\mathcal C$.

Proof. We use Theorem 11.1, and the moment method:

(1) Here we have $E=\sqrt{N}\sum_ia_ib_i$, with $a,b\in\mathbb T^N$ random. With $q_i=a_ib_i$ this gives the first assertion. Let us estimate now the moments of $|E|^2$. We have:

$$\begin{aligned}
&\int_{\mathbb T^N\times\mathbb T^N}|E|^{2p}\\
&= N^p\int_{\mathbb T^N}|q_1+\ldots+q_N|^{2p}dq\\
&= N^p\int_{\mathbb T^N}\sum_{ij}\frac{q_{i_1}\ldots q_{i_p}}{q_{j_1}\ldots q_{j_p}}\,dq\\
&= N^p\#\left\{(i,j)\in\{1,\ldots,N\}^p\times\{1,\ldots,N\}^p\Big|[i_1,\ldots,i_p]=[j_1,\ldots,j_p]\right\}\\
&\simeq N^p\cdot p!N(N-1)\ldots(N-p+1)\\
&\simeq N^p\cdot p!N^p\\
&= p!N^{2p}
\end{aligned}$$

Here, and in what follows, the sets between brackets are by defintion sets with repetition, and the middle estimate comes from the fact that, with $N\to\infty$, only the multi-indices $i=(i_1,\ldots,i_p)$ having distinct entries contribute. But this gives the result.

(2) Here we have the following formula, which gives the first assertion:

$$E=\sum_{ij}a_ib_j=\sum_ia_i\sum_jb_j$$

Now since $a,b\in\mathbb T^N$ are independent, so are the quantities $\sum_ia_i,\sum_jb_j$, so we have:

$$\int_{\mathbb T^N\times\mathbb T^N}|E|^{2p}=\left(\int_{\mathbb T^N}|q_1+\ldots+q_N|^{2p}dq\right)^2\simeq(p!N^p)^2$$

Here we have used the estimate in the proof of (1), and this gives the result. □

As a first conclusion, the glow is intimately related to the basic hypertoral law, namely that of $q_1+\ldots+q_N$, with $q\in\mathbb T^N$ random. Observe that at $N=1$ this hypertoral law is simply δ_1, and that at $N=2$ we obtain the following law:

$$\begin{aligned}law|1+q| &= law\sqrt{(1+e^{it})(1+e^{-it})}\\ &= law\sqrt{2+2\cos t}\\ &= law\left(2\cos\frac{t}{2}\right)\end{aligned}$$

In general, the law of $\sum q_i$ is known to be related to the Pólya random walk [112]. Also, as explained for instance in section 9, the moments of this law are:

$$\int_{\mathbb T^N}|q_1+\ldots+q_N|^{2p}dq=\sum_{\pi\in P(p)}\binom{p}{\pi}\frac{N!}{(N-|\pi|)!}$$

As a second conclusion, even under the normalization $||H||_2=N$, the glow can behave quite differently in the $N\to\infty$ limit. So, let us restrict now the attention to the Hadamard matrices. At $N=2$ we only have F_2 to be invesigated, the result being:

Proposition 11.3. *For the Fourier matrix F_2 we have*

$$|E|^2=4+2Re(\alpha-\beta)$$

for certain variables $\alpha,\beta\in\mathbb T$ which are uniform, and independent.

Proof. The matrix that we interested in, namely the Fourier matrix F_2 altered by a vertical switching vector (a,b) and an horizontal switching vector (c,d), is:

$$\widetilde{F}_2=\begin{pmatrix}ac&ad\\ bc&-bd\end{pmatrix}$$

With this notation, we have the following formula:

$$\begin{aligned}|E|^2 &= |ac+ad+bc-bd|^2\\ &= 4+\frac{ad}{bc}+\frac{bc}{ad}-\frac{bd}{ac}-\frac{ac}{bd}\end{aligned}$$

For proving that the variables $\alpha=\frac{ad}{bc}$ and $\beta=\frac{bd}{ac}$ are independent, we can use the moment method, as follows:

$$\begin{aligned}\int_{\mathbb T^4}\left(\frac{ad}{bc}\right)^p\left(\frac{bd}{ac}\right)^q &= \int_{\mathbb T}a^{p-q}\int_{\mathbb T}b^{q-p}\int_{\mathbb T}c^{-p-q}\int_{\mathbb T}d^{p+q}\\ &= \delta_{pq}\delta_{pq}\delta_{p,-q}\delta_{p,-q}\\ &= \delta_{p,q,0}\end{aligned}$$

Thus α,β are indeed independent, and we are done. $\square$

It is possible of course to derive from this some more concrete formulae, but let us look instead at the case $N=3$. Here the matrix that we are interested in is:

$$\widetilde{F}_3=\begin{pmatrix}ad&ae&af\\ bd&wbe&w^2bf\\ cd&w^2ce&wcf\end{pmatrix}$$

Thus, we would like to compute the law of the following quantity:

$$|E|=|ad+ae+af+bd+wbe+w^2bf+cd+w^2ce+wcf|$$

The problem is that when trying to compute $|E|^2$, the terms won't cancel much. More precisely, we have a formula of the following type:

$$|E|^2=9+C_0+C_1w+C_2w^2$$

Here the quantities C_0,C_1,C_2 are as follows:

$$\begin{aligned}
C_0&=\frac{ae}{bd}+\frac{ae}{cd}+\frac{af}{bd}+\frac{af}{cd}+\frac{bd}{ae}+\frac{bd}{af}+\frac{be}{cf}+\frac{bf}{ce}+\frac{cd}{ae}+\frac{cd}{af}+\frac{ce}{bf}+\frac{cf}{be}\\
C_1&=\frac{ad}{bf}+\frac{ad}{ce}+\frac{ae}{bf}+\frac{af}{ce}+\frac{bd}{ce}+\frac{be}{ad}+\frac{be}{af}+\frac{be}{cd}+\frac{cd}{bf}+\frac{cf}{ad}+\frac{cf}{ae}+\frac{cf}{bd}\\
C_2&=\frac{ad}{be}+\frac{ad}{cf}+\frac{ae}{cf}+\frac{af}{be}+\frac{bd}{cf}+\frac{bf}{ad}+\frac{bf}{ae}+\frac{bf}{cd}+\frac{cd}{be}+\frac{ce}{ad}+\frac{ce}{af}+\frac{ce}{bd}
\end{aligned}$$

In short, all this leads nowhere, and the exact study stops at F_2. In general now, one idea is that of using Bernoulli-type variables coming from the row sums, as follows:

Theorem 11.4. *The glow of $H\in M_N(\mathbb{C})$ is given by the formula*

$$law(E)=\int_{a\in\mathbb{T}^N}B((Ha)_1,\ldots,(Ha)_N)$$

where the quantities on the right are

$$B(c_1,\ldots,c_N)=law\left(\sum_i\lambda_ic_i\right)$$

with $\lambda\in\mathbb{T}^N$ being random.

Proof. This is clear from $E=<a,Hb>$. Indeed, when the vector $a\in\mathbb{T}^N$ is assumed to be fixed, this variable E follows the law $B((Ha)_1,\ldots,(Ha)_N)$ in the statement. □

Observe that we can write a formula of the following type:

$$B(c_1,\ldots,c_N)=\varepsilon\times\beta(|c_1|,\ldots,|c_N|)$$

To be more precise, such a formula holds indeed, with the measure $\beta(r_1,\ldots,r_N)\in\mathcal{P}(\mathbb{R}_+)$ with $r_1,\ldots,r_N\geq 0$ being given by:

$$\beta(r_1,\ldots,r_N)=law\left|\sum_i\lambda_ir_i\right|$$

Regarding now the computation of β, we have:

$$\beta(r_1,\ldots,r_N)=law\sqrt{\sum_{ij}\frac{\lambda_i}{\lambda_j}\cdot r_ir_j}$$

Consider now the following variable, which is easily seen, for instance by using the moment method, to be uniform over the projective torus $\mathbb{T}^{N-1}=\mathbb{T}^N/\mathbb{T}$:

$$(\mu_1,\mu_2,\ldots,\mu_N)=\left(\frac{\lambda_1}{\lambda_2},\frac{\lambda_2}{\lambda_3},\ldots,\frac{\lambda_N}{\lambda_1}\right)$$

Now since we have $\lambda_i/\lambda_j=\mu_i\mu_{i+1}\ldots\mu_j$, with the convention $\mu_i\ldots\mu_j=\overline{\mu_j\ldots\mu_i}$ for $i>j$, this gives the following formula, with $\mu\in\mathbb{T}^{N-1}$ random:

$$\beta(r_1,\ldots,r_N)=law\sqrt{\sum_{ij}\mu_i\mu_{i+1}\ldots\mu_j\cdot r_ir_j}$$

It is possible to further study the laws β by using this formula. However, in practice, it is more convenient to use the complex measures B from Theorem 11.4.

Let us end these preliminaries with a discussion of the "arithmetic" version of the problem, which makes the link with the Gale-Berlekamp switching game [67], [116] and with the work in section 2. We have the following unifying formalism:

Definition 11.5. *Given $H\in M_N(\mathbb{C})$ and $s\in\mathbb{N}\cup\{\infty\}$, we define a measure $\mu_s\in\mathcal{P}(\mathbb{C})$ by the formula*

$$\int_{\mathbb{C}}\varphi(x)d\mu_s(x)=\int_{\mathbb{Z}_s^N\times\mathbb{Z}_s^N}\varphi\left(\sum_{ij}a_ib_jH_{ij}\right)d(a,b)$$

where $\mathbb{Z}_s\subset\mathbb{T}$ is the group of the s-roots of unity, with the convention $\mathbb{Z}_\infty=\mathbb{T}$.

Observe that at $s=\infty$ we obtain the measure in Theorem 11.1. Also, at $s=2$ and for a usual Hadamard matrix, $H\in M_N(\pm1)$, we obtain the measure from section 2. Observe also that for $H\in M_N(\pm1)$, knowing μ_2 is the same as knowing the statistics of the number of one entries, $|1\in H|$. This follows indeed from the following formula:

$$\sum_{ij}H_{ij}=|1\in H|-|-1\in H|=2|1\in H|-N^2$$

More generally, at $s=p$ prime, we have the following result:

Theorem 11.6. *When s is prime and $H\in M_N(\mathbb Z_s)$, the statistics of the number of one entries, $|1\in H|$, can be recovered from that of the total sum, $E=\sum_{ij}H_{ij}$.*

Proof. The problem here is of vectorial nature, so given $V\in\mathbb Z_s^n$, we would like to compare the quantities $|1\in V|$ and $\sum V_i$. Let us write, up to permutations:

$$V=(\underbrace{1\ldots1}_{a_0}\ \underbrace{w\ldots w}_{a_1}\ \ldots\ldots\ \underbrace{w^{s-1}\ldots w^{s-1}}_{a_{s-1}})$$

We have then $|1\in V|=a_0$, as well as:

$$\sum V_i=a_0+a_1w+\ldots+a_{s-1}w^{s-1}$$

We also know that $a_0+a_1+\ldots+a_{s-1}=n$. Now when s is prime, the only ambiguity in recovering a_0 from $a_0+a_1w+\ldots+a_{s-1}w^{s-1}$ can come from:

$$1+w+\ldots+w^{s-1}=0$$

But since the sum of the numbers a_i is fixed, $a_0+a_1+\ldots+a_{s-1}=n$, this ambiguity dissapears, and this gives the result. $\square$

Let us investigate now the glow of the complex Hadamard matrices, by using the moment method. We use the moment formula from section 10, namely:

Proposition 11.7. *For $H\in M_N(\mathbb T)$ the even moments of $|E|$ are given by*

$$\int_{\mathbb T^N\times\mathbb T^N}|E|^{2p}=\sum_{[i]=[k],[j]=[l]}\frac{H_{i_1j_1}\ldots H_{i_pj_p}}{H_{k_1l_1}\ldots H_{k_pl_p}}$$

where the sets between brackets are by definition sets with repetition.

Proof. As explained in section 10, with $E=\sum_{ij}H_{ij}a_ib_j$ we obtain:

$$\begin{aligned}\int_{\mathbb T^N\times\mathbb T^N}|E|^{2p}&=\int_{\mathbb T^N\times\mathbb T^N}\left(\sum_{ijkl}\frac{H_{ij}}{H_{kl}}\cdot\frac{a_ib_j}{a_kb_l}\right)^p\\&=\sum_{ijkl}\frac{H_{i_1j_1}\ldots H_{i_pj_p}}{H_{k_1l_1}\ldots H_{k_pl_p}}\int_{\mathbb T^N}\frac{a_{i_1}\ldots a_{i_p}}{a_{k_1}\ldots a_{k_p}}\int_{\mathbb T^N}\frac{b_{j_1}\ldots b_{j_p}}{b_{l_1}\ldots b_{l_p}}\end{aligned}$$

The integrals on the right being $\delta_{[i],[k]}$ and $\delta_{[j],[l]}$, we obtain the result. $\square$

As a first application, let us investigate the tensor products. We have:

Proposition 11.8. *The even moments of $|E|$ for a tensor product $L=H\otimes K$ are given by the formula*

$$\int_{\mathbb T^{NM}\times\mathbb T^{NM}}|E|^{2p}=\sum_{[ia]=[kc],[jb]=[ld]}\frac{H_{i_1j_1}\ldots H_{i_pj_p}}{H_{k_1l_1}\ldots H_{k_pl_p}}\cdot\frac{K_{a_1b_1}\ldots K_{a_pb_p}}{K_{c_1d_1}\ldots K_{c_pd_p}}$$

where the sets between brackets are as usual sets with repetition.

Proof. With $L = H \otimes K$, the formula in Proposition 11.7 reads:

$$\int_{\mathbb{T}^{NM}\times\mathbb{T}^{NM}} |E|^{2p} = \sum_{[ia]=[kc],[jb]=[ld]} \frac{L_{i_1a_1,j_1b_1}\ldots L_{i_pa_p,j_pb_p}}{L_{k_1c_1,l_1d_1}\ldots L_{k_pc_p,l_pd_p}}$$

But this gives the formula in the statement, and we are done. □

Let us develop now some moment machinery. Let $P(p)$ be the set of partitions of $\{1,\ldots,p\}$, with its standard order relation $\leq$, which is such that, for any $\pi \in P(p)$:

$$\sqcap\!\sqcap \ldots \leq \pi \leq |\,|\ldots|\,|$$

We denote by $\mu(\pi,\sigma)$ the associated Möbius function, given by:

$$\mu(\pi,\sigma) = \begin{cases} 1 & \text{if } \pi=\sigma \\ -\sum_{\pi\leq\tau<\sigma}\mu(\pi,\tau) & \text{if } \pi<\sigma \\ 0 & \text{if } \pi\not\leq\sigma \end{cases}$$

For $\pi \in P(p)$ we use the following notation, where $b_1,\ldots,b_{|\pi|}$ are the block lenghts:

$$\binom{p}{\pi} = \binom{p}{b_1\ldots b_{|\pi|}} = \frac{p!}{b_1!\ldots b_{|\pi|}!}$$

Finally, we use the following notation, where $H_1,\ldots,H_N \in \mathbb{T}^N$ are the rows of H:

$$H_\pi(i) = \bigotimes_{\beta\in\pi}\prod_{r\in\beta} H_{i_r}$$

With these notations, we have the following result:

Theorem 11.9. *The glow moments of a matrix $H \in M_N(\mathbb{T})$ are given by*

$$\int_{\mathbb{T}^N\times\mathbb{T}^N} |E|^{2p} = \sum_{\pi\in P(p)} K(\pi)N^{|\pi|}I(\pi)$$

where $K(\pi) = \sum_{\sigma\in P(p)}\mu(\pi,\sigma)\binom{p}{\sigma}$, and where the contributions are given by

$$I(\pi) = \frac{1}{N^{|\pi|}}\sum_{[i]=[j]} < H_\pi(i), H_\pi(j) >$$

by using the above notations and conventions.

Proof. We know from Proposition 11.7 that the moments are given by:

$$\int_{\mathbb{T}^N\times\mathbb{T}^N} |E|^{2p} = \sum_{[i]=[j],[x]=[y]} \frac{H_{i_1x_1}\ldots H_{i_px_p}}{H_{j_1y_1}\ldots H_{j_py_p}}$$

With $\sigma = \ker x, \rho = \ker y$, we deduce that the moments of $|E|^2$ decompose over partitions, according to a formula as follows:

$$\int_{\mathbb{T}^N \times \mathbb{T}^N} |E|^{2p} = \int_{\mathbb{T}^N} \sum_{\sigma,\rho \in P(p)} C(\sigma, \rho)$$

To be more precise, the contributions are as follows:

$$C(\sigma, \rho) = \sum_{\ker x = \sigma, \ker y = \rho} \delta_{[x],[y]} \sum_{ij} \frac{H_{i_1 x_1} \ldots H_{i_p x_p}}{H_{j_1 y_1} \ldots H_{j_p y_p}} \cdot \frac{a_{i_1} \ldots a_{i_p}}{a_{j_1} \ldots a_{j_p}}$$

We have $C(\sigma, \rho) = 0$ unless $\sigma \sim \rho$, in the sense that σ, ρ must have the same block structure. The point now is that the sums of type $\sum_{\ker x = \sigma}$ can be computed by using the Möbius inversion formula. We obtain a formula as follows:

$$C(\sigma, \rho) = \delta_{\sigma \sim \rho} \sum_{\pi \leq \sigma} \mu(\pi, \sigma) \prod_{\beta \in \pi} C_{|\beta|}(a)$$

Here the functions on the right are by definition given by:

$$\begin{aligned} C_r(a) &= \sum_x \sum_{ij} \frac{H_{i_1 x} \ldots H_{i_r x}}{H_{j_1 x} \ldots H_{j_r x}} \cdot \frac{a_{i_1} \ldots a_{i_r}}{a_{j_1} \ldots a_{j_r}} \\ &= \sum_{ij} < H_{i_1} \ldots H_{i_r}, H_{j_1} \ldots H_{j_r} > \cdot \frac{a_{i_1} \ldots a_{i_r}}{a_{j_1} \ldots a_{j_r}} \end{aligned}$$

Now since there are $\binom{p}{\sigma}$ partitions having the same block structure as σ, we obtain:

$$\begin{aligned} \int_{\mathbb{T}^N \times \mathbb{T}^N} |\Omega|^{2p} &= \int_{\mathbb{T}^N} \sum_{\pi \in P(p)} \left(\sum_{\sigma \sim \rho} \sum_{\mu \leq \sigma} \mu(\pi, \sigma) \right) \prod_{\beta \in \pi} C_{|\beta|}(a) \\ &= \sum_{\pi \in P(p)} \left(\sum_{\sigma \in P(p)} \mu(\pi, \sigma) \binom{p}{\sigma} \right) \int_{\mathbb{T}^N} \prod_{\beta \in \pi} C_{|\beta|}(a) \end{aligned}$$

But this gives the formula in the statement, and we are done. □

Let us discuss now the asymptotic behavior of the glow. For this purpose, we first study the coefficients $K(\pi)$ in Theorem 11.9. We have here the following result:

Proposition 11.10. $K(\pi) = \sum_{\pi \leq \sigma} \mu(\pi, \sigma) \binom{p}{\sigma}$ *has the following properties:*

(1) $\widetilde{K}(\pi) = \frac{K(\pi)}{p!}$ *is multiplicative:* $\widetilde{K}(\pi\pi') = \widetilde{K}(\pi)\widetilde{K}(\pi')$.
(2) $K(\sqcap\sqcap \ldots \sqcap) = \sum_{\sigma \in P(p)} (-1)^{|\sigma|-1} (|\sigma| - 1)! \binom{p}{\sigma}$.
(3) $K(\sqcap\sqcap \ldots \sqcap) = \sum_{r=1}^{p} (-1)^{r-1} (r-1)! C_{pr}$, *where* $C_{pr} = \sum_{p = a_1 + \ldots + a_r} \binom{p}{a_1, \ldots, a_r}^2$.

Proof. This follows from some standard computations, as follows:

(1) We can use here the formula $\mu(\pi\pi',\sigma\sigma')=\mu(\pi,\sigma)\mu(\pi',\sigma')$, which is a well-known property of the Möbius function, which can be proved by recurrence. Now if $b_1,\ldots,b_s$ and $c_1,\ldots,c_t$ are the block lengths of σ,σ', we obtain, as claimed:

$$\begin{aligned}\widetilde{K}(\pi\pi') &= \sum_{\pi\pi'\leq\sigma\sigma'}\mu(\pi\pi',\sigma\sigma')\cdot\frac{1}{b_1!\ldots b_s!}\cdot\frac{1}{c_1!\ldots c_t!}\\ &= \sum_{\pi\leq\sigma,\pi'\leq\sigma'}\mu(\pi,\sigma)\mu(\pi',\sigma')\cdot\frac{1}{b_1!\ldots b_s!}\cdot\frac{1}{c_1!\ldots c_t!}\\ &= \widetilde{K}(\pi)\widetilde{K}(\pi')\end{aligned}$$

(2) We can use here the following formula, which once again is well-known, and can be proved by recurrence on $|\sigma|$:

$$\mu(\sqcap\sqcap\ldots\sqcap,\sigma)=(-1)^{|\sigma|-1}(|\sigma|-1)!$$

We obtain, as claimed:

$$\begin{aligned}K(\sqcap\sqcap\ldots\sqcap) &= \sum_{\sigma\in P(p)}\mu(\sqcap\sqcap\ldots\sqcap,\sigma)\binom{p}{\sigma}\\ &= \sum_{\sigma\in P(p)}(-1)^{|\sigma|-1}(|\sigma|-1)!\binom{p}{\sigma}\end{aligned}$$

(3) By using the formula in (2), and summing over $r=|\sigma|$, we obtain:

$$K(\sqcap\sqcap\ldots\sqcap)=\sum_{r=1}^{p}(-1)^{r-1}(r-1)!\sum_{|\sigma|=r}\binom{p}{\sigma}$$

Now if we denote by $a_1,\ldots,a_r$ with $a_i\geq 1$ the block lengths of σ, then:

$$\binom{p}{\sigma}=\binom{p}{a_1,\ldots,a_r}$$

On the other hand, given $a_1,\ldots,a_r\geq 1$ with $a_1+\ldots+a_r=p$, there are exactly $\binom{p}{a_1,\ldots,a_r}$ partitions σ having these numbers as block lengths, and this gives the result. $\square$

Now let us take a closer look at the integrals $I(\pi)$. We have here:

Proposition 11.11. *Consider the one-block partition $\sqcap\sqcap\ldots\sqcap\in P(p)$.*

(1) $I(\sqcap\sqcap\ldots\sqcap)=\#\{i,j\in\{1,\ldots,N\}^p|[i]=[j]\}$.
(2) $I(\sqcap\sqcap\ldots\sqcap)=\int_{\mathbb{T}^N}|\sum_i a_i|^{2p}da$.
(3) $I(\sqcap\sqcap\ldots\sqcap)=\sum_{\sigma\in P(p)}\binom{p}{\sigma}\frac{N!}{(N-|\sigma|)!}$.
(4) $I(\sqcap\sqcap\ldots\sqcap)=\sum_{r=1}^{p-1}C_{pr}\frac{N!}{(N-r)!}$, *where* $C_{pr}=\sum_{p=b_1+\ldots+b_r}\binom{p}{b_1,\ldots,b_r}^2$.

Proof. Once again, this follows from some standard combinatorics, as follows:

(1) This follows indeed from the following computation:

$$I(\sqcap\!\sqcap\ldots\sqcap)=\sum_{[i]=[j]}\frac{1}{N}<H_{i_1}\ldots H_{i_r},H_{j_1}\ldots H_{j_r}>=\sum_{[i]=[j]}1$$

(2) This follows from the following computation:

$$\int_{\mathbb{T}^N}\left|\sum_i a_i\right|^{2p}=\int_{\mathbb{T}^N}\sum_{ij}\frac{a_{i_1}\ldots a_{i_p}}{a_{j_1}\ldots a_{j_p}}da=\#\left\{i,j\Big|[i]=[j]\right\}$$

(3) If we let $\sigma=\ker i$ in the above formula of $I(\sqcap\!\sqcap\ldots\sqcap)$, we obtain:

$$I(\sqcap\!\sqcap\ldots\sqcap)=\sum_{\sigma\in P(p)}\#\left\{i,j\Big|\ker i=\sigma,[i]=[j]\right\}$$

Now since there are $\frac{N!}{(N-|\sigma|)!}$ choices for i, and then $\binom{p}{\sigma}$ for j, this gives the result.

(4) If we set $r=|\sigma|$, the formula in (3) becomes:

$$I(\sqcap\!\sqcap\ldots\sqcap)=\sum_{r=1}^{p-1}\frac{N!}{(N-r)!}\sum_{\sigma\in P(p),|\sigma|=r}\binom{p}{\sigma}$$

Now since there are exactly $\binom{p}{b_1,\ldots,b_r}$ permutations $\sigma\in P(p)$ having $b_1,\ldots,b_r$ as block lengths, the sum on the right equals $\sum_{p=b_1+\ldots+b_r}\binom{p}{b_1,\ldots,b_r}^2$, as claimed. □

In general, the integrals $I(\pi)$ can be estimated as follows:

Proposition 11.12. *Let $H\in M_N(\mathbb{T})$, having its rows pairwise orthogonal.*

(1) $I(|\,|\ldots|)=N^p$.
(2) $I(|\,|\ldots|\ \pi)=N^aI(\pi)$, *for any* $\pi\in P(p-a)$.
(3) $|I(\pi)|\lesssim p!N^p$, *for any* $\pi\in P(p)$.

Proof. This is something elementary, as follows:

(1) Since the rows of H are pairwise orthogonal, we have:

$$I(|\,|\ldots|)=\sum_{[i]=[j]}\prod_{r=1}^p\delta_{i_r,j_r}=\sum_{[i]=[j]}\delta_{ij}=\sum_i 1=N^p$$

(2) This follows by the same computation as the above one for (1).

(3) We have indeed the following estimate:

$$\begin{aligned}|I(\pi)| &\leq \sum_{[i]=[j]}\prod_{\beta\in\pi}1\\ &= \sum_{[i]=[j]}1\\ &= \#\left\{i,j\in\{1,\ldots,N\}\Big|[i]=[j]\right\}\\ &\simeq p!N^p\end{aligned}$$

Thus we have obtained the formula in the statement, and we are done. □

We have now all needed ingredients for a universality result:

Theorem 11.13. *The glow of a complex Hadamard matrix $H\in M_N(\mathbb{T})$ is given by:*

$$\frac{1}{p!}\int_{\mathbb{T}^N\times\mathbb{T}^N}\left(\frac{|E|}{N}\right)^{2p}=1-\binom{p}{2}N^{-1}+O(N^{-2})$$

In particular, E/N becomes complex Gaussian in the $N\to\infty$ limit.

Proof. We use the moment formula in Theorem 11.9. By using Proposition 11.12 (3), we conclude that only the p-block and $(p-1)$-block partitions contribute at order 2, so:

$$\begin{aligned}\int_{\mathbb{T}^N\times\mathbb{T}^N}|E|^{2p} &= K(|\,|\ldots|)N^pI(|\,|\ldots|)\\ &+ \binom{p}{2}K(\sqcap|\ldots|)N^{p-1}I(\sqcap|\ldots|)\\ &+ O(N^{2p-2})\end{aligned}$$

Now by dividing by N^{2p} and then by using the various formulae in Proposition 11.10, Proposition 11.11 and Proposition 11.12 above, we obtain, as claimed:

$$\int_{\mathbb{T}^N\times\mathbb{T}^N}\left(\frac{|E|}{N}\right)^{2p}=p!-\binom{p}{2}\frac{p!}{2}\cdot\frac{2N-1}{N^2}+O(N^{-2})$$

Finally, since the law of E is invariant under centered rotations in the complex plane, this moment formula gives as well the last assertion. □

Let us study now the glow of the Fourier matrices, $F=F_G$. We use the following standard formulae:

$$F_{ix}F_{iy}=F_{i,x+y}$$
$$\overline{F}_{ix}=F_{i,-x}$$
$$\sum_xF_{ix}=N\delta_{i0}$$

We first have the following result:

Proposition 11.14. *For a Fourier matrix F_G we have*

$$I(\pi)=\#\left\{i,j\Big|[i]=[j],\sum_{r\in\beta}i_r=\sum_{r\in\beta}j_r,\forall\beta\in\pi\right\}$$

with all the indices, and with the sums at right, taken inside G.

Proof. The basic components of the integrals $I(\pi)$ are given by:

$$\begin{aligned}\frac{1}{N}\left\langle\prod_{r\in\beta}F_{i_r},\prod_{r\in\beta}F_{j_r}\right\rangle&=\frac{1}{N}\left\langle F_{\sum_{r\in\beta}i_r},F_{\sum_{r\in\beta}i_r}\right\rangle\\&=\delta_{\sum_{r\in\beta}i_r,\sum_{r\in\beta}j_r}\end{aligned}$$

But this gives the formula in the statement, and we are done. □

We have the following interpretation of the above integrals:

Proposition 11.15. *For any partition π we have the formula*

$$I(\pi)=\int_{\mathbb{T}^N}\prod_{b\in\pi}\left(\frac{1}{N^2}\sum_{ij}|H_{ij}|^{2|\beta|}\right)da$$

where $H=FAF^*$, with $F=F_G$ and $A=diag(a_0,\ldots,a_{N-1})$.

Proof. We have the following computation:

$$\begin{aligned}H=F^*AF\quad&\implies\quad|H_{xy}|^2=\sum_{ij}\frac{F_{iy}F_{jx}}{F_{ix}F_{jy}}\cdot\frac{a_i}{a_j}\\&\implies\quad|H_{xy}|^{2p}=\sum_{ij}\frac{F_{j_1x}\ldots F_{j_px}}{F_{i_1x}\ldots F_{i_px}}\cdot\frac{F_{i_1y}\ldots F_{i_py}}{F_{j_1y}\ldots F_{j_py}}\cdot\frac{a_{i_1}\ldots a_{i_p}}{a_{j_1}\ldots a_{j_p}}\\&\implies\quad\sum_{xy}|H_{xy}|^{2p}=\sum_{ij}\left|<H_{i_1}\ldots H_{i_p},H_{j_1}\ldots H_{j_p}>\right|^2\cdot\frac{a_{i_1}\ldots a_{i_p}}{a_{j_1}\ldots a_{j_p}}\end{aligned}$$

But this gives the formula in the statement, and we are done. □

We must estimate now the quantities $I(\pi)$. We first have the following result:

Proposition 11.16. *For F_G we have the estimate*

$$I(\pi)=b_1!\ldots b_{|\pi|}!N^p+O(N^{p-1})$$

where $b_1,\ldots,b_{|\pi|}$ with $b_1+\ldots+b_{|\pi|}=p$ are the block lengths of π.

Proof. With $\sigma=\ker i$ we obtain:

$$I(\pi)=\sum_{\sigma\in P(p)}\#\left\{i,j\Big|\ker i=\sigma,[i]=[j],\sum_{r\in\beta}i_r=\sum_{r\in\beta}j_r,\forall\beta\in\pi\right\}$$

There are $\frac{N!}{(N-|\sigma|)!} \simeq N^{|\sigma|}$ choices for i satisfying $\ker i = \sigma$. Then, there are $\binom{p}{\sigma} = O(1)$ choices for j satisfying $[i] = [j]$. We conclude that the main contribution comes from the partition $\sigma = ||\ldots|$. Thus, we have the following formula:

$$I(\pi) = \#\left\{i, j\Bigg| \ker i = ||\ldots|, [i] = [j], \sum_{r\in\beta} i_r = \sum_{r\in\beta} j_r, \forall\beta \in \pi\right\} + O(N^{p-1})$$

Now the condition $\ker i = ||\ldots|$ tells us that i must have distinct entries, and there are $\frac{N!}{(N-p)!} \simeq N^p$ choices for such multi-indices i. Regarding now the indices j, the main contribution comes from those obtained from i by permuting the entries over the blocks of π, and since there are $b_1! \ldots b_{|\pi|}!$ choices here, this gives the result. □

At the second order now, the estimate is as follows:

Proposition 11.17. *For F_G we have the formula*

$$\frac{I(\pi)}{b_1! \ldots b_s! N^p} = 1 + \left(\sum_{i<j}\sum_{c\geq 2}\binom{b_i}{c}\binom{b_j}{c} - \frac{1}{2}\sum_i \binom{b_i}{2}\right) N^{-1} + O(N^{-2})$$

where $b_1, \ldots, b_s$ being the block lengths of $\pi \in P(p)$.

Proof. Let us define the "non-arithmetic" part of $I(\pi)$ as follows:

$$I^\circ(\pi) = \#\left\{i, j\Big|[i_r|r \in \beta] = [j_r|r \in \beta], \forall\beta \in \pi\right\}$$

We then have the following formula:

$$I^\circ(\pi) = \prod_{\beta\in\pi}\left\{i, j \in I^{|\beta|}\Big|[i] = [j]\right\} = \prod_{\beta\in\pi} I(\beta)$$

Also, Proposition 11.16 shows that we have the following estimate:

$$I(\pi) = I^\circ(\pi) + O(N^{p-1})$$

Our claim now is that we have the following formula:

$$\frac{I(\pi) - I^\circ(\pi)}{b_1! \ldots b_s! N^p} = \sum_{i<j}\sum_{c\geq 2}\binom{b_i}{c}\binom{b_j}{c} N^{-1} + O(N^{-2})$$

Indeed, according to Proposition 11.16, we have a formula of the following type:

$$I(\pi) = I^\circ(\pi) + I^1(\pi) + O(N^{p-2})$$

More precisely, this formula holds indeed, with $I^1(\pi)$ coming from $i_1, \ldots, i_p$ distinct, $[i] = [j]$, and with one constraint of type:

$$\sum_{r\in\beta} i_r = \sum_{j\in\beta} j_r \quad , \quad [i_r|r \in \beta] \neq [j_r|r \in \beta]$$

Now observe that for a two-block partition $\pi = (a, b)$ this constraint is implemented, up to permutations which leave invariant the blocks of π, as follows:

$$\underbrace{\begin{matrix} i_1 \ldots i_c \\ j_1 \ldots j_c \end{matrix}}_{c} \ \underbrace{\begin{matrix} k_1 \ldots k_{a-c} \\ k_1 \ldots k_{a-c} \end{matrix}}_{a-c} \quad \underbrace{\begin{matrix} j_1 \ldots j_c \\ i_1 \ldots i_c \end{matrix}}_{c} \ \underbrace{\begin{matrix} l_1 \ldots l_{a-c} \\ l_1 \ldots l_{a-c} \end{matrix}}_{b-c}$$

Let us compute now $I^1(a, b)$. We cannot have $c = 0, 1$, and once $c \geq 2$ is given, we have $\binom{a}{c}, \binom{b}{c}$ choices for the positions of the i, j variables in the upper row, then $N^{p-1} + O(N^{p-2})$ choices for the variables in the upper row, and then finally we have $a!b!$ permutations which can produce the lower row. We therefore obtain the following formula:

$$I^1(a, b) = a!b! \sum_{c \geq 2} \binom{a}{c} \binom{b}{c} N^{p-1} + O(N^{p-2})$$

In the general case now, a similar discussion applies.

Indeed, the constraint of type $\sum_{r \in \beta} i_r = \sum_{r \in \beta} j_r$ with $[i_r | r \in \beta] \neq [j_r | r \in \beta]$ cannot affect ≤ 1 blocks, because we are not in the non-arithmetic case, and cannot affect either ≥ 3 blocks, because affecting ≥ 3 blocks would require ≥ 2 constraints.

Thus this condition affects exactly 2 blocks, and if we let $i < j$ be the indices in $\{1, \ldots, s\}$ corresponding to these 2 blocks, we obtain:

$$I^1(\pi) = b_1! \ldots b_s! \sum_{i<j} \sum_{c \geq 2} \binom{b_i}{c} \binom{b_j}{c} N^{p-1} + O(N^{p-2})$$

But this proves the above claim. Let us estimate now $I(\sqcap\sqcap \ldots \sqcap)$. We have:

$$\begin{aligned} I(\sqcap\sqcap \ldots \sqcap) &= p! \frac{N!}{(N-p)!} + \binom{p}{2} \frac{p!}{2} \cdot \frac{N!}{(N-p+1)!} + O(N^{p-2}) \\ &= p! N^r \left(1 - \binom{p}{2} N^{-1} + O(N^{-2})\right) + \binom{p}{2} \frac{p!}{2} N^{p-1} + O(N^{p-2}) \\ &= p! N^p \left(1 - \frac{1}{2} \binom{p}{2} N^{-1} + O(N^{-2})\right) \end{aligned}$$

Now recall that we have:

$$I^\circ(\pi) = \prod_{\beta \in \pi} I(\beta)$$

We therefore obtain:

$$I^\circ(\pi) = b_1! \ldots b_s! N^p \left(1 - \frac{1}{2} \sum_i \binom{b_i}{2} N^{-1} + O(N^{-2})\right)$$

By plugging this quantity into the above estimate, we obtain the result. $\square$

In order to estimate glow, we will need the explicit formula of $I(\sqcap\sqcap)$:

Proposition 11.18. *For F_G with $G=\mathbb{Z}_{N_1}\times\ldots\times\mathbb{Z}_{N_k}$ we have the formula*

$$I(\sqcap\sqcap)=N(4N^3-11N+2^e+7)$$

where $e\in\{0,1,\ldots,k\}$ is the number of even numbers among $N_1,\ldots,N_k$.

Proof. Let us first recall that the conditions defining the quantities $I(\pi)$ are as follows:

$$\sum_{r\in\beta}i_r=\sum_{r\in\beta}j_r$$

We use the fact that, when dealing with these conditions, one can always erase some of the variables i_r,j_r, as to reduce to the "purely arithmetic" case, namely:

$$\{i_r|r\in\beta\}\cap\{j_r|r\in\beta\}=\emptyset$$

We deduce from this that we have:

$$I(\sqcap\sqcap)=I^\circ(\sqcap\sqcap)+I^{ari}(\sqcap\sqcap)$$

Let us compute now $I^{ari}(\sqcap\sqcap)$. There are 3 contributions to this quantity, namely:

(1) <u>Case $\binom{iijj}{jjii}$</u>, with $i\neq j$, $2i=2j$. Since $2(i_1,\ldots,i_k)=2(j_1,\ldots,j_k)$ corresponds to the collection of conditions $2i_r=2j_r$, inside $\mathbb{Z}_{N_r}$, which each have 1 or 2 solutions, depending on whether N_r is odd or even, the contribution here is:

$$\begin{aligned}
I_1^{ari}(\sqcap\sqcap)&=\#\{i\neq j|2i=2j\}\\
&=\#\{i,j|2i=2j\}-\#\{i,j|i=j\}\\
&=2^eN-N\\
&=(2^e-1)N
\end{aligned}$$

(2) <u>Case $\binom{iijk}{jkii}$</u>, with i,j,k distinct, $2i=j+k$. The contribution here is:

$$\begin{aligned}
I_2^{ari}(\sqcap\sqcap)&=4\#\{i,j,k\text{ distinct}|2i=j+k\}\\
&=4\#\{i\neq j|2i-j\neq i,j\}\\
&=4\#\{i\neq j|2i\neq 2j\}\\
&=4(\#\{i,j|i\neq j\}-\#\{i\neq j|2i=2j\})\\
&=4(N(N-1)-(2^e-1)N)\\
&=4N(N-2^e)
\end{aligned}$$

(3) <u>Case $\binom{ijkl}{klij}$</u>, with i,j,k,l distinct, $i+j=k+l$. The contribution here is:

$$\begin{aligned}
I_3^{ari}(\sqcap\sqcap)&=4\#\{i,j,k,l\text{ distinct}|i+j=k+l\}\\
&=4\#\{i,j,k\text{ distinct}|i+j-k\neq i,j,k\}\\
&=4\#\{i,j,k\text{ distinct}|i+j-k\neq k\}\\
&=4\#\{i,j,k\text{ distinct}|i\neq 2k-j\}
\end{aligned}$$

We can split this quantity over two cases, $2j\neq 2k$ and $2j=2k$, and we obtain:

$$\begin{aligned}I_3^{ari}(\sqcap\sqcap) &= 4(\#\{i,j,k \text{ distinct}|2j\neq 2k, i\neq 2k-j\}\\ &\quad +\#\{i,j,k \text{ distinct}|2j=2k, i\neq 2k-j\})\end{aligned}$$

The point now is that in the first case, $2j\neq 2k$, the numbers $j,k,2k-j$ are distinct, while in the second case, $2j=2k$, we simply have $2k-j=j$. Thus, we obtain:

$$\begin{aligned}I_3^{ari}(\sqcap\sqcap) &= 4\left(\sum_{j\neq k,2j\neq 2k}\#\{i|i\neq j,k,2k-j\}+\sum_{j\neq k,2j=2k}\#\{i|i\neq j,k\}\right)\\ &= 4(N(N-2^e)(N-3)+N(2^e-1)(N-2))\\ &= 4N(N(N-3)-2^e(N-3)+2^e(N-2)-(N-2))\\ &= 4N(N^2-4N+2^e+2)\end{aligned}$$

We can now compute the arithmetic part. This is given by:

$$\begin{aligned}I^{ari}(\sqcap\sqcap) &= (2^e-1)N+4N(N-2^e)+4N(N^2-4N+2^e+2)\\ &= N(2^e-1+4(N-2^e)+4(N^2-4N+2^e+2))\\ &= N(4N^2-12N+2^e+7)\end{aligned}$$

Thus the integral to be computed is given by:

$$\begin{aligned}I(\sqcap\sqcap) &= N^2(2N-1)^2+N(4N^2-12N+2^e+7)\\ &= N(4N^3-4N^2+N+4N^2-12N+2^e+7)\\ &= N(4N^3-11N+2^e+7)\end{aligned}$$

Thus we have reached to the formula in the statement, and we are done. $\square$

We have the following asymptotic result, from [11]:

Theorem 11.19. *The glow of F_G, with $|G|=N$, is given by*

$$\frac{1}{p!}\int_{\mathbb{T}^N\times\mathbb{T}^N}\left(\frac{|E|}{N}\right)^{2p}=1-K_1N^{-1}+K_2N^{-2}-K_3N^{-3}+O(N^{-4})$$

with the coefficients being as follows:

$$K_1=\binom{p}{2}\quad,\quad K_2=\binom{p}{2}\frac{3p^2+p-8}{12}\quad,\quad K_3=\binom{p}{3}\frac{p^3+4p^2+p-18}{8}$$

Thus, the rescaled complex glow is asymptotically complex Gaussian,

$$\frac{E}{N}\sim\mathcal{C}$$

and we have in fact universality at least up to order 3.

Proof. We use the following quantities:

$$\widetilde{K}(\pi)=\frac{K(\pi)}{p!}\quad,\quad\widetilde{I}(\pi)=\frac{I(\pi)}{N^p}$$

These are subject to the following formulae:

$$\widetilde{K}(\pi|\ldots|)=\widetilde{K}(\pi)\quad,\quad\widetilde{I}(\pi|\ldots|)=\widetilde{I}(\pi)$$

Consider as well the following quantities:

$$J(\sigma)=\binom{p}{\sigma}\widetilde{K}(\sigma)\widetilde{I}(\sigma)$$

In terms of these quantities, we have:

$$\begin{aligned}\frac{1}{p!}\int_{\mathbb{T}^N\times\mathbb{T}^N}|E|^{2p}\ &=\ J(\emptyset)\\ &+\ N^{-1}J(\sqcap)\\ &+\ N^{-2}\left(J(\sqcap\!\!\sqcap)+J(\sqcap\sqcap)\right)\\ &+\ N^{-3}\left(J(\sqcap\!\!\sqcap\!\!\sqcap)+J(\sqcap\!\!\sqcap\,\sqcap)+J(\sqcap\,\sqcap\,\sqcap)\right)\\ &+\ O(N^{-4})\end{aligned}$$

We have the following formulae:

$$\widetilde{K}_0=1$$

$$\widetilde{K}_1=1$$

$$\widetilde{K}_2=\frac{1}{2}-1=-\frac{1}{2}$$

$$\widetilde{K}_3=\frac{1}{6}-\frac{3}{2}+2=\frac{2}{3}$$

$$\widetilde{K}_4=\frac{1}{24}-\frac{4}{6}-\frac{3}{4}+\frac{12}{2}-6=-\frac{11}{8}$$

Regarding now the numbers C_{pr} in Proposition 11.16, these are given by:

$$C_{p1}=1\quad,\quad C_{p2}=\frac{1}{2}\binom{2p}{p}-1\quad,\quad\ldots\quad,\quad C_{p,p-1}=\frac{p!}{2}\binom{p}{2},C_{pp}=p!$$

We deduce that we have the following formulae:

$$I(|)=N$$

$$I(\sqcap)=N(2N-1)$$

$$I(\sqcap\!\!\sqcap)=N(6N^2-9N+4)$$

$$I(\sqcap\!\!\sqcap\!\!\sqcap)=N(24N^3-72N^2+82N-33)$$

By using Proposition 11.17 and Proposition 11.18, we obtain the following formula:

$$\begin{aligned}
\frac{1}{p!}\int_{\mathbb{T}^N\times\mathbb{T}^N}|E|^{2p} &= 1-\frac{1}{2}\binom{p}{2}(2N^{-1}-N^{-2})+\frac{2}{3}\binom{p}{3}(6N^{-2}-9N^{-3})\\
&+ 3\binom{p}{4}N^{-2}-33\binom{p}{4}N^{-3}-40\binom{p}{5}N^{-3}\\
&- 15\binom{p}{6}N^{-3}+O(N^{-4})
\end{aligned}$$

But this gives the formulae of K_1, K_2, K_3 in the statement, and we are done. □

It is possible to compute the next term as well, the result being:

Theorem 11.20. *Let $G=\mathbb{Z}_{N_1}\times\ldots\times\mathbb{Z}_{N_k}$ be a finite abelian group, and set:*

$$N=N_1\ldots N_k$$

Then the glow of the associated Fourier matrix F_G is given by

$$\frac{1}{p!}\int_{\mathbb{T}^N\times\mathbb{T}^N}\left(\frac{|E|}{N}\right)^{2p}=1-K_1N^{-1}+K_2N^{-2}-K_3N^{-3}+K_4N^{-4}+O(N^{-5})$$

where the quantities K_1, K_2, K_3, K_4 are given by

$$\begin{aligned}
K_1 &= \binom{p}{2}\\
K_2 &= \binom{p}{2}\frac{3p^2+p-8}{12}\\
K_3 &= \binom{p}{3}\frac{p^3+4p^2+p-18}{8}\\
K_4 &= \frac{8}{3}\binom{p}{3}+\frac{3}{4}\left(121+\frac{2^e}{N}\right)\binom{p}{4}+416\binom{p}{5}+\frac{2915}{2}\binom{p}{6}+40\binom{p}{7}+105\binom{p}{8}
\end{aligned}$$

where $e\in\{0,1,\ldots,k\}$ is the number of even numbers among $N_1,\ldots,N_k$.

Proof. This is something that we already know, up to order 3, and the next coefficient K_4 can be computed in a similar way, based on results that we already have. □

The passage to Theorem 11.20 is quite interesting, because it shows that the glow of the Fourier matrices F_G is not polynomial in $N=|G|$. When restricting the attention to the usual Fourier matrices F_N, the glow up to order 4 is polynomial both in N odd, and in N even, but it is not clear what happens at higher order. An interesting question here is that of computing the glow of the Walsh matrices, where the integrals $I(\pi)$, and hence the glow, might be polynomial in N. We do not know if this is really the case.

12. Local estimates

We discuss here some further analytic questions, regarding the complex Hadamard matrices, following [25], in analogy with the considerations in sections 2-3 above. First, we have the following basic estimate, that we already know:

Theorem 12.1. *Given a function $\psi : [0,\infty) \to \mathbb{R}$, the following function over U_N*

$$F(U) = \sum_{ij} \psi(|U_{ij}|^2)$$

satisfies the following inequality, when ψ is convex,

$$F(U) \geq N^2 \psi\left(\frac{1}{N}\right)$$

and the following inequality, when ψ is concave,

$$F(U) \leq N^2 \psi\left(\frac{1}{N}\right)$$

and assuming that ψ is strictly convex/concave, the equality case appears precisely for the rescaled Hadamard matrices, $U = H/\sqrt{N}$ with $H \in M_N(\mathbb{T})$ Hadamard.

Proof. This follows indeed from the Jensen inequality, exactly as in the real case. $\square$

Of particular interest for us are the power functions $\psi(x) = x^{p/2}$, which are concave at $p \in [1,2)$, and convex at $p \in (2,\infty)$. These lead to the following statement:

Theorem 12.2. *Let $U \in U_N$, and set $H = \sqrt{N} U$.*

1. *For $p \in [1,2)$ we have $||U||_p \leq N^{2/p-1/2}$, with equality when H is Hadamard.*
2. *For $p \in (2,\infty]$ we have $||U||_p \geq N^{2/p-1/2}$, with equality when H is Hadamard.*

Proof. Consider indeed the p-norm on U_N, which at $p \in [1,\infty)$ is given by:

$$||U||_p = \left(\sum_{ij} |U_{ij}|^p\right)^{1/p}$$

By the above discussion, involving the functions $\psi(x) = x^{p/2}$, Theorem 12.1 applies and gives the results at $p \in [1,\infty)$, the precise estimates being as follows:

$$||U||_p = \begin{cases} \leq N^{2/p-1/2} & \text{if } p < 2 \\ = N^{1/2} & \text{if } p = 2 \\ \geq N^{2/p-1/2} & \text{if } p > 2 \end{cases}$$

As for the case $p = \infty$, this follows with $p \to \infty$, or directly via Cauchy-Schwarz. $\square$

For future reference, let us record as well the particular cases $p = 1, 4, \infty$ of the above result, that we already met before, and which are of particular interest:

Theorem 12.3. *For any matrix $U\in U_N$ we have the estimates*

$$||U||_1\leq N\sqrt{N}\quad,\quad ||U||_4\geq 1\quad,\quad ||U||_\infty\geq\frac{1}{\sqrt{N}}$$

which in terms of the rescaled matrix $H=\sqrt{N}U$ read

$$||H||_1\leq N^2\quad,\quad ||H||_4\geq\sqrt{N}\quad,\quad ||H||_\infty\geq 1$$

and in each case, the equality case holds when H is Hadamard.

Proof. These results follow from Theorem 12.2 at $p=1,4,\infty$, with the remark that for each of these particular exponents, we do not really need the Hölder inequality, with a basic application of the Cauchy-Schwarz inequality doing the job. □

The above results suggest the following definition:

Definition 12.4. *Given $U\in U_N$, the matrix $H=\sqrt{N}U$ is called:*

1. *Almost Hadamard, if U locally maximizes the 1-norm on U_N.*
2. *p-almost Hadamard, with $p<2$, if U locally maximizes the p-norm on U_N.*
3. *p-almost Hadamard, with $p>2$, if U locally minimizes the p-norm on U_N.*
4. *Absolute almost Hadamard, if it is p-almost Hadamard at any $p\neq 2$.*

We have as well real versions of these notions, with U_N replaced by O_N.

All this might seem a bit complicated, but this is the best way of presenting things. We are mainly interested in (1), but as explained in section 9, the exponent $p=4$ from (3) is interesting as well, and once we have (3) we must formulate (2) as well, and finally (4) is a useful thing too, because the absolute case is sometimes easier to study.

As for the "doubling" of all these notions, via the last sentence, this is necessary too, because given a function $F:U_N\to\mathbb{R}$, an element $U\in O_N$ can be a local extremum of the restriction $F_{|O_N}:O_N\to\mathbb{R}$, but not of the function F itself. And, we will see in what follows that this is the case, and in a quite surprising way, with the p-norms.

Let us first study the critical points. Things are quite tricky here, and complete results are available so far only at $p=1$. Following [25], we first have the following result:

Theorem 12.5. *If $U\in U_N$ locally maximizes the 1-norm, then*

$$U_{ij}\neq 0$$

must hold for any i,j.

Proof. We use the same method as in the real case, namely a "rotation trick". Let us denote by $U_1,\ldots,U_N$ the rows of U, and let us perform a rotation of U_1,U_2:

$$\begin{bmatrix}U_1^t\\ U_2^t\end{bmatrix}=\begin{bmatrix}\cos t\cdot U_1-\sin t\cdot U_2\\ \sin t\cdot U_1+\cos t\cdot U_2\end{bmatrix}$$

In order to compute the 1-norm, let us permute the columns of U, in such a way that the first two rows look as follows, with X, Y, A, B having nonzero entries:

$$\begin{bmatrix}U_1\\U_2\end{bmatrix}=\begin{bmatrix}0&0&Y&A\\0&X&0&B\end{bmatrix}$$

The rotated matrix will look then as follows:

$$\begin{bmatrix}U_1^t\\U_2^t\end{bmatrix}=\begin{bmatrix}0&-\sin t\cdot X&\cos t\cdot Y&\cos t\cdot A-\sin t\cdot B\\0&\cos t\cdot X&\sin t\cdot y&\sin t\cdot A+\cos t\cdot B\end{bmatrix}$$

Our claim is that X, Y must be empty. Indeed, if A and B are not empty, let us fix a column index k for both A, B, and set $\alpha = A_k$, $\beta = B_k$. We have then:

$$\begin{aligned}
|(U_1^t)_k|+|(U_2^t)_k| &= |\cos t\cdot\alpha-\sin t\cdot\beta|+|\sin t\cdot\alpha+\cos t\cdot\beta|\\
&= \sqrt{\cos^2 t\cdot|\alpha|^2+\sin^2 t\cdot|\beta|^2-\sin t\cos t(\alpha\bar{\beta}+\beta\bar{\alpha})}\\
&+ \sqrt{\sin^2 t\cdot|\alpha|^2+\cos^2 t\cdot|\beta|^2+\sin t\cos t(\alpha\bar{\beta}+\beta\bar{\alpha})}
\end{aligned}$$

Since $\alpha, \beta \neq 0$, the above function is derivable at $t = 0$, and we obtain:

$$\begin{aligned}
\frac{\partial\left(|(U_1^t)_k|+|(U_2^t)_k|\right)}{\partial t} &= \frac{\sin 2t(|\beta|^2-|\alpha|^2)-\cos 2t(\alpha\bar{\beta}+\beta\bar{\alpha})}{2\sqrt{\cos^2 t\cdot|\alpha|^2+\sin^2 t\cdot|\beta|^2-\sin t\cos t(\alpha\bar{\beta}+\beta\bar{\alpha})}}\\
&+ \frac{\sin 2t(|\alpha|^2-|\beta|^2)+\cos 2t(\alpha\bar{\beta}+\beta\bar{\alpha})}{2\sqrt{\sin^2 t\cdot|\alpha|^2+\cos^2 t\cdot|\beta|^2+\sin t\cos t(\alpha\bar{\beta}+\beta\bar{\alpha})}}
\end{aligned}$$

Thus at $t = 0$, we obtain the following formula:

$$\frac{\partial\left(|(U_1^t)_k|+|(U_2^t)_k|\right)}{\partial t}(0)=\frac{\alpha\bar{\beta}+\beta\bar{\alpha}}{2}\left(\frac{1}{|\beta|}-\frac{1}{|\alpha|}\right)$$

Now since U locally maximizes the 1-norm, both directional derivatives of $||U^t||_1$ must be negative in the limit $t \to 0$. On the other hand, if we denote by C the contribution coming from the right, which might be zero in the case where A and B are empty, i.e. the sum over k of the above quantities, we have:

$$\begin{aligned}
\frac{\partial||U^t||_1}{\partial t}\Big|_{t=0^+} &= \frac{\partial}{\partial t}\Big|_{t=0^+}(|\cos t|+|\sin t|)(||X||_1+||Y||_1)+C\\
&= (-\sin t+\cos t)\Big|_{t=0}(||X||_1+||Y||_1)+C\\
&= ||X||_1+||Y||_1+C
\end{aligned}$$

As for the derivative at left, this is given by the following formula:

$$\begin{aligned}\frac{\partial||U^t||_1}{\partial t}_{|t=0^-} &= \frac{\partial}{\partial t}_{|t=0^-}(|\cos t|+|\sin t|)(||X||_1+||Y||_1)+C\\ &= (-\sin t-\cos t)_{|t=0}(||X||_1+||Y||_1)+C\\ &= -||X||_1-||Y||_1+C\end{aligned}$$

We therefore obtain the following inequalities, where C is as above:

$$\begin{aligned}||X||_1+||Y||_1+C &\leq 0\\ -||X||_1-||Y||_1+C &\leq 0\end{aligned}$$

Consider now the matrix obtained from U by interchanging U_1,U_2. Since this matrix must be as well a local maximizer of the 1-norm, and since the above formula shows that C changes its sign when interchanging U_1,U_2, we obtain:

$$\begin{aligned}||X||_1+||Y||_1-C &\leq 0\\ -||X||_1-||Y||_1-C &\leq 0\end{aligned}$$

The four inequalities that we have give altogether $||X||_1+||Y||_1=C=0$, and from $||X||_1+||Y||_1=0$ we obtain that both X,Y must be empty, as claimed.

As a conclusion, up to a permutation of the columns, the first two rows must be of the following form, with A,B having only nonzero entries:

$$\begin{bmatrix}U_1\\ U_2\end{bmatrix}=\begin{bmatrix}0&A\\ 0&B\end{bmatrix}$$

By permuting the rows of U, the same must hold for any two rows U_i,U_j. Now since U cannot have a zero column, we conclude that U cannot have zero entries, as claimed. □

Let us compute now the critical points. Following [25], we have:

Theorem 12.6. *Let $\varphi:[0,\infty)\to\mathbb{R}$ be a differentiable function. A matrix $U\in U_N^*$ is a critical point of the quantity*

$$F(U)=\sum_{ij}\varphi(|U_{ij}|)$$

precisely when WU^* is self-adjoint, where:

$$W_{ij}=\mathrm{sgn}(U_{ij})\varphi'(|U_{ij}|)$$

Proof. We regard U_N as a real algebraic manifold, with coordinates $U_{ij},\bar{U}_{ij}$. This manifold consists by definition of the zeroes of the following polynomials:

$$A_{ij}=\sum_k U_{ik}\bar{U}_{jk}-\delta_{ij}$$

Since U_N is smooth, and so is a differential manifold in the usual sense, it follows from the general theory of Lagrange multipliers that a given matrix $U \in U_N$ is a critical point of F precisely when the following condition is satisfied:

$$dF \in span(dA_{ij})$$

Regarding the space $span(dA_{ij})$, this consists of the following quantities:

$$\begin{aligned}\sum_{ij} M_{ij} dA_{ij} &= \sum_{ijk} M_{ij}(U_{ik} d\bar{U}_{jk} + \bar{U}_{jk} dU_{ik})\\ &= \sum_{jk} (M^t U)_{jk} d\bar{U}_{jk} + \sum_{ik} (M\bar{U})_{ik} dU_{ik}\\ &= \sum_{ij} (M^t U)_{ij} d\bar{U}_{ij} + \sum_{ij} (M\bar{U})_{ij} dU_{ij}\end{aligned}$$

In order to compute dF, observe first that, with $S_{ij} = sgn(U_{ij})$, we have:

$$\begin{aligned}d|U_{ij}| &= d\sqrt{U_{ij}\bar{U}_{ij}}\\ &= \frac{U_{ij} d\bar{U}_{ij} + \bar{U}_{ij} dU_{ij}}{2|U_{ij}|}\\ &= \frac{1}{2}(S_{ij} d\bar{U}_{ij} + \bar{S}_{ij} dU_{ij})\end{aligned}$$

Now let us set, as in the statement:

$$W_{ij} = sgn(U_{ij})\varphi'(|U_{ij}|)$$

In terms of these variables, we obtain:

$$\begin{aligned}dF &= \sum_{ij} d\left(\varphi(|U_{ij}|)\right)\\ &= \sum_{ij} \varphi'(|U_{ij}|) d|U_{ij}|\\ &= \frac{1}{2}\sum_{ij} W_{ij} d\bar{U}_{ij} + \bar{W}_{ij} dU_{ij}\end{aligned}$$

We conclude that $U \in U_N$ is a critical point of F if and only if there exists a matrix $M \in M_N(\mathbb{C})$ such that the following two conditions are satisfied:

$$W = 2M^t U \quad , \quad \bar{W} = 2M\bar{U}$$

Now observe that these two equations can be written as follows:

$$M^t = \frac{1}{2} W U^* \quad , \quad M^t = \frac{1}{2} U W^*$$

Summing up, the critical point condition on $U\in U_N$ simply reads:

$$WU^*=UW^*$$

But this means that the matrix WU^* must be self-adjoint, as claimed. $\square$

In order to process the above result, we can use the following notion:

Definition 12.7. *Given $U\in U_N$, we consider its "color decomposition"*

$$U=\sum_{r>0}rU_r$$

with $U_r\in M_N(\mathbb T\cup\{0\})$ containing the phase components at $r>0$, and we call U:

1. *Semi-balanced, if U_rU^* and U^*U_r, with $r>0$, are all self-adjoint.*
2. *Balanced, if $U_rU_s^*$ and $U_r^*U_s$, with $r,s>0$, are all self-adjoint.*

These conditions are quite natural, because for a unitary matrix $U\in U_N$, the relations $UU^*=U^*U=1$ translate as follows, in terms of the color decomposition:

$$\sum_{r>0}rU_rU^*=\sum_{r>0}rU^*U_r=1$$

$$\sum_{r,s>0}rsU_rU_s^*=\sum_{r,s>0}rsU_r^*U_s=1$$

Thus, our balancing conditions express the fact that the various components of the above sums all self-adjoint. Now back to our critical point questions, we have:

Theorem 12.8. *For a matrix $U\in U_N^*$, the following are equivalent:*

1. *U is a critical point of $F(U)=\sum_{ij}\varphi(|U_{ij}|)$, for any $\varphi:[0,\infty)\to\mathbb R$.*
2. *U is a critical point of all the p-norms, with $p\in[1,\infty)$.*
3. *U is semi-balanced, in the above sense.*

Proof. We use Theorem 12.6 above. The matrix constructed there is given by:

$$\begin{aligned}(WU^*)_{ij}&=\sum_k\mathrm{sgn}(U_{ik})\varphi'(|U_{ik}|)\bar U_{jk}\\&=\sum_{r>0}\varphi'(r)\sum_{k,|U_{ik}|=r}\mathrm{sgn}(U_{ik})\bar U_{jk}\\&=\sum_{r>0}\varphi'(r)\sum_k(U_r)_{ik}\bar U_{jk}\\&=\sum_{r>0}\varphi'(r)(U_rU^*)_{ij}\end{aligned}$$

Thus we have the following formula:

$$WU^*=\sum_{r>0}\varphi'(r)U_rU^*$$

Now when $\varphi : [0,\infty) \to \mathbb{R}$ varies, as a differentiable function, or as a power function $\varphi(x) = x^p$ with $p \in [1,\infty)$, the individual components must be self-adjoint, as desired. $\square$

In practice now, most of the known examples of semi-balanced matrices are actually balanced. We have the following collection of simple facts, regarding such matrices:

Proposition 12.9. *The class of balanced matrices is as follows:*

1. *It contains the matrices $U = H/\sqrt{N}$, with $H \in M_N(\mathbb{C})$ Hadamard.*
2. *It is stable under transposition, complex conjugation, and taking adjoints.*
3. *It is stable under taking tensor products.*
4. *It is stable under the Hadamard equivalence relation.*
5. *It contains the matrix $V_N = \frac{1}{N}(2\mathbb{I}_N - N1_N)$, where $\mathbb{I}_N$ is the all-1 matrix.*

Proof. All these results are elementary, the proof being as follows:

(1) Here $U \in U_N$ follows from the Hadamard condition, and since there is only one color component, namely $U_{1/\sqrt{N}} = H$, the balancing condition is satisfied as well.

(2) Assuming that $U = \sum_{r>0} rU_r$ is a color decomposition of a given matrix $U \in U_N$, the following are color decompositions too, and this gives the assertions:

$$U^t = \sum_{r>0} rU_r^t$$

$$\bar{U} = \sum_{r>0} r\bar{U}_r$$

$$U^* = \sum_{r>0} rU_r^*$$

(3) Assuming that $U = \sum_{r>0} rU_r$ and $V = \sum_{s>0} sV_s$ are the color decompositions of two given unitary matrices U, V, we have:

$$\begin{aligned} U \otimes V &= \sum_{r,s>0} rs \cdot U_r \otimes V_s \\ &= \sum_{p>0} p \sum_{p=rs} U_r \otimes V_s \end{aligned}$$

Thus the color components of $W = U \otimes V$ are the following matrices:

$$W_p = \sum_{p=rs} U_r \otimes V_s$$

It follows that if U, V are both balanced, then so is $W = U \otimes V$.

(4) We recall that the Hadamard equivalence consists in permuting rows and columns, and switching signs on rows and columns. Since all these operations correspond to certain conjugations at the level of the matrices $U_rU_s^*, U_r^*U_s$, we obtain the result.

(5) The matrix in the statement, which goes back to [28], is as follows:

$$V_N=\frac{1}{N}\begin{pmatrix}2-N&2&\ldots&2\\2&2-N&\ldots&2\\\ldots&\ldots&\ldots&\ldots\\2&2&\ldots&2-N\end{pmatrix}$$

Observe that this matrix is indeed unitary, its rows being of norm one, and pairwise orthogonal. The color components of this matrix being $V_{2/N-1}=1_N$ and $V_{2/N}=\mathbb{I}_N-1_N$, it follows that this matrix is balanced as well, as claimed. $\square$

Let us look now more in detail at V_N, and at the matrices having similar properties. Following [28], let us call (a,b,c) pattern any matrix $M\in M_N(0,1)$, with $N=a+2b+c$, such that any two rows look as follows, up to a permutation of the columns:

$$\begin{matrix}0\ldots0&0\ldots0&1\ldots1&1\ldots1\\\underbrace{0\ldots0}_a&\underbrace{1\ldots1}_b&\underbrace{0\ldots0}_b&\underbrace{1\ldots1}_c\end{matrix}$$

As explained in [28], there are many interesting examples of (a,b,c) patterns, coming from the balanced incomplete block designs (BIBD), and all these examples can produce two-entry unitary matrices, by replacing the $0,1$ entries with suitable numbers x,y.

Now back to the matrix V_N from Proposition 12.9 (5), observe that this matrix comes from a $(0,1,N-2)$ pattern. And also, independently of this, this matrix has the remarkable property of being at the same time circulant and self-adjoint.

We have in fact the following result, generalizing Proposition 12.9 (5):

Theorem 12.10. *The following matrices are balanced:*

(1) *The orthogonal matrices coming from (a,b,c) patterns.*
(2) *The unitary matrices which are circulant and self-adjoint.*

Proof. These observations basically go back to [28], the proofs being as follows:

(1) If we denote by $P,Q\in M_N(0,1)$ the matrices describing the positions of the $0,1$ entries inside the pattern, then we have the following formulae:

$$\begin{aligned}PP^t=P^tP&=a\mathbb{I}_N+b1_N\\QQ^t=Q^tQ&=c\mathbb{I}_N+b1_N\\PQ^t=P^tQ=QP^t=Q^tP&=b\mathbb{I}_N-b1_N\end{aligned}$$

Since all these matrices are symmetric, U is balanced, as claimed.

(2) Assume that $U\in U_N$ is circulant, $U_{ij}=\gamma_{j-i}$, and in addition self-adjoint, which means $\bar{\gamma}_i=\gamma_{-i}$. Consider the following sets, which must satisfy $D_r=-D_r$:

$$D_r=\{k:|\gamma_r|=k\}$$

In terms of these sets, we have the following formula:

$$\begin{aligned}(U_rU_s^*)_{ij} &= \sum_k (U_r)_{ik}(\bar{U}_s)_{jk}\\ &= \sum_k \delta_{|\gamma_{k-i}|,r}\,\mathrm{sgn}(\gamma_{k-i})\cdot\delta_{|\gamma_{k-j}|,s}\,\mathrm{sgn}(\bar{\gamma}_{k-j})\\ &= \sum_{k\in(D_r+i)\cap(D_s+j)} \mathrm{sgn}(\gamma_{k-i})\,\mathrm{sgn}(\bar{\gamma}_{k-j})\end{aligned}$$

With $k=i+j-m$ we obtain, by using $D_r=-D_r$, and then $\bar{\gamma}_i=\gamma_{-i}$:

$$\begin{aligned}(U_rU_s^*)_{ij} &= \sum_{m\in(-D_r+j)\cap(-D_s+i)} \mathrm{sgn}(\gamma_{j-m})\,\mathrm{sgn}(\bar{\gamma}_{i-m})\\ &= \sum_{m\in(D_r+i)\cap(D_r+j)} \mathrm{sgn}(\gamma_{j-m})\,\mathrm{sgn}(\bar{\gamma}_{i-m})\\ &= \sum_{m\in(D_r+i)\cap(D_r+j)} \mathrm{sgn}(\bar{\gamma}_{m-j})\,\mathrm{sgn}(\gamma_{m-i})\end{aligned}$$

Now by interchanging $i\leftrightarrow j$, and with $m\to k$, this formula becomes:

$$(U_rU_s^*)_{ji}=\sum_{k\in(D_r+i)\cap(D_r+j)} \mathrm{sgn}(\bar{\gamma}_{k-i})\,\mathrm{sgn}(\gamma_{k-j})$$

We recognize here the complex conjugate of $(U_rU_s^*)_{ij}$, as previously computed above, and we therefore deduce that $U_rU_s^*$ is self-adjoint. The proof for $U_r^*U_s$ is similar. $\square$

Let us compute now derivatives. As in Theorem 12.6, it is convenient to do the computations in a more general framework, where we have a function as follows:

$$F(U)=\sum_{ij}\psi(|U_{ij}|^2)$$

In order to study the local extrema of these quantities, consider the following function, depending on $t>0$ small:

$$f(t)=F(Ue^{tA})=\sum_{ij}\psi(|(Ue^{tA})_{ij}|^2)$$

Here $U\in U_N$ is a unitary matrix, and $A\in M_N(\mathbb{C})$ is assumed to be anti-hermitian, $A^*=-A$, as for having $e^A\in U_N$. Let us first compute the derivative of f. We have:

Proposition 12.11. *We have the following formula,*

$$f'(t)=2\sum_{ij}\psi'(|(Ue^{tA})_{ij}|^2)Re\left[(UAe^{tA})_{ij}\overline{(Ue^{tA})_{ij}}\right]$$

valid for any $U\in U_N$, and any $A\in M_N(\mathbb{C})$ anti-hermitian.

Proof. The matrices U,e^{tA} being both unitary, we have:

$$\begin{aligned}|(Ue^{tA})_{ij}|^2&=(Ue^{tA})_{ij}\overline{(Ue^{tA})_{ij}}\\&=(Ue^{tA})_{ij}((Ue^{tA})^*)_{ji}\\&=(Ue^{tA})_{ij}(e^{tA^*}U^*)_{ji}\\&=(Ue^{tA})_{ij}(e^{-tA}U^*)_{ji}\end{aligned}$$

We can now differentiate our function f, and by using once again the unitarity of the matrices U,e^{tA}, along with the formula $A^*=-A$, we obtain:

$$\begin{aligned}f'(t)&=\sum_{ij}\psi'(|(Ue^{tA})_{ij}|^2)\left[(UAe^{tA})_{ij}(e^{-tA}U^*)_{ji}-(Ue^{tA})_{ij}(e^{-tA}AU^*)_{ji}\right]\\&=\sum_{ij}\psi'(|(Ue^{tA})_{ij}|^2)\left[(UAe^{tA})_{ij}\overline{((e^{-tA}U^*)^*)_{ij}}-(Ue^{tA})_{ij}\overline{((e^{-tA}AU^*)^*)_{ij}}\right]\\&=\sum_{ij}\psi'(|(Ue^{tA})_{ij}|^2)\left[(UAe^{tA})_{ij}\overline{(Ue^{tA})_{ij}}+(Ue^{tA})_{ij}\overline{(UAe^{tA})_{ij}}\right]\end{aligned}$$

But this gives the formula in the statement, and we are done. □

Before computing the second derivative, let us evaluate $f'(0)$. We have:

Proposition 12.12. *We have the following formula,*

$$f'(0)=2\sum_{r>0}r\psi'(r^2)Re\left[Tr(U_r^*UA)\right]$$

where the matrices $U_r\in M_N(\mathbb T\cup\{0\})$ are the color components of U.

Proof. We use the formula in Proposition 12.11 above. At $t=0$, we obtain:

$$f'(0)=2\sum_{ij}\psi'(|U_{ij}|^2)Re\left[(UA)_{ij}\overline{U}_{ij}\right]$$

Consider now the color decomposition of U. We have the following formulae:

$$\begin{aligned}U_{ij}=\sum_{r>0}r(U_r)_{ij}\quad&\implies\quad|U_{ij}|^2=\sum_{r>0}r^2|(U_r)_{ij}|\\&\implies\quad\psi'(|U_{ij}|^2)=\sum_{r>0}\psi'(r^2)|(U_r)_{ij}|\end{aligned}$$

Now by getting back to the above formula of $f'(0)$, we obtain:

$$f'(0)=2\sum_{r>0}\psi'(r^2)\sum_{ij}Re\left[(UA)_{ij}\overline{U}_{ij}|(U_r)_{ij}|\right]$$

Our claim now is that we have:

$$\overline{U}_{ij}|(U_r)_{ij}|=r\overline{(U_r)}_{ij}$$

Indeed, in the case $|U_{ij}|\neq r$ this formula reads $\overline{U}_{ij}\cdot 0=r\cdot 0$, which is true, and in the case $|U_{ij}|=r$ this formula reads $r\bar{S}_{ij}\cdot 1=r\cdot\bar{S}_{ij}$, which is once again true.

We therefore conclude that we have:

$$f'(0)=2\sum_{r>0}r\psi'(r^2)\sum_{ij}Re\left[(UA)_{ij}\overline{(U_r)}_{ij}\right]$$

But this gives the formula in the statement, and we are done. □

Let us compute now the second derivative. The result here is as follows:

Proposition 12.13. *We have the following formula,*

$$\begin{aligned}f''(0)&=&&4\sum_{ij}\psi''(|U_{ij}|^2)Re\left[(UA)_{ij}\overline{U}_{ij}\right]^2\\&&&+2\sum_{ij}\psi'(|U_{ij}|^2)Re\left[(UA^2)_{ij}\overline{U}_{ij}\right]\\&&&+2\sum_{ij}\psi'(|U_{ij}|^2)|(UA)_{ij}|^2\end{aligned}$$

valid for any $U\in U_N$, and any $A\in M_N(\mathbb{C})$ anti-hermitian.

Proof. We use the formula in Proposition 12.11 above, namely:

$$f'(t)=2\sum_{ij}\psi'(|(Ue^{tA})_{ij}|^2)Re\left[(UAe^{tA})_{ij}\overline{(Ue^{tA})_{ij}}\right]$$

Since the real part on the right, or rather its double, appears as the derivative of the quantity $|(Ue^{tA})_{ij}|^2$, when differentiating a second time, we obtain:

$$\begin{aligned}f''(t)&=&&4\sum_{ij}\psi''(|(Ue^{tA})_{ij}|^2)Re\left[(UAe^{tA})_{ij}\overline{(Ue^{tA})_{ij}}\right]^2\\&&&+2\sum_{ij}\psi'(|(Ue^{tA})_{ij}|^2)Re\left[(UAe^{tA})_{ij}\overline{(Ue^{tA})_{ij}}\right]'\end{aligned}$$

In order to compute now the missing derivative, observe that we have:

$$\begin{aligned}\left[(UAe^{tA})_{ij}\overline{(Ue^{tA})_{ij}}\right]'&=&&(UA^2e^{tA})_{ij}\overline{(Ue^{tA})_{ij}}+(UAe^{tA})_{ij}\overline{(UAe^{tA})_{ij}}\\&=&&(UA^2e^{tA})_{ij}\overline{(Ue^{tA})_{ij}}+|(UAe^{tA})_{ij}|^2\end{aligned}$$

Summing up, we have obtained the following formula:

$$\begin{aligned}
f''(t) &= 4\sum_{ij}\psi''(|(Ue^{tA})_{ij}|^2)Re\left[(UAe^{tA})_{ij}\overline{(Ue^{tA})_{ij}}\right]^2\\
&+2\sum_{ij}\psi'(|(Ue^{tA})_{ij}|^2)Re\left[(UA^2e^{tA})_{ij}\overline{(Ue^{tA})_{ij}}\right]\\
&+2\sum_{ij}\psi'(|(Ue^{tA})_{ij}|^2)|(UAe^{tA})_{ij}|^2
\end{aligned}$$

But at $t=0$ this gives the formula in the statement, and we are done. □

For the function $\psi(x)=\sqrt{x}$, corresponding to $F(U)=||U||_1$, we have:

Proposition 12.14. *Let $U\in U_N^*$. For the function $F(U)=||U||_1$ we have the formula*

$$f''(0)=Re\left[Tr(S^*UA^2)\right]+\sum_{ij}\frac{Im\left[(UA)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|}$$

valid for any anti-hermitian matrix A, where $U_{ij}=S_{ij}|U_{ij}|$.

Proof. We use the formula in Proposition 12.13 above, with the following data:

$$\psi(x)=\sqrt{x}\quad,\quad\psi'(x)=\frac{1}{2\sqrt{x}}\quad,\quad\psi''(x)=-\frac{1}{4x\sqrt{x}}$$

We obtain the following formula:

$$\begin{aligned}
f''(0) &= -\sum_{ij}\frac{Re\left[(UA)_{ij}\overline{U}_{ij}\right]^2}{|U_{ij}|^3}+\sum_{ij}\frac{Re\left[(UA^2)_{ij}\overline{U}_{ij}\right]}{|U_{ij}|}+\sum_{ij}\frac{|(UA)_{ij}|^2}{|U_{ij}|}\\
&= -\sum_{ij}\frac{Re\left[(UA)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|}+\sum_{ij}Re\left[(UA^2)_{ij}\overline{S}_{ij}\right]+\sum_{ij}\frac{|(UA)_{ij}|^2}{|U_{ij}|}\\
&= Re\left[Tr(S^*UA^2)\right]+\sum_{ij}\frac{|(UA)_{ij}|^2-Re\left[(UA)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|}
\end{aligned}$$

But this gives the formula in the statement, and we are done. □

We are therefore led to the following result, regarding the 1-norm:

Theorem 12.15. *A matrix $U\in U_N^*$ locally maximizes the one-norm on U_N precisely when S^*U is self-adjoint, where $S_{ij}=\mathrm{sgn}(U_{ij})$, and when*

$$Tr(S^*UA^2)+\sum_{ij}\frac{Im\left[(UA)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|}\leq 0$$

holds, for any anti-hermitian matrix $A\in M_N(\mathbb{C})$.

Proof. According to Theorem 12.6 and Proposition 12.14, the local maximizer condition requires $X = S^*U$ to be self-adjoint, and the following inequality to be satisfied:

$$Re\left[Tr(S^*UA^2)\right] + \sum_{ij} \frac{Im\left[(UA)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|} \leq 0$$

Now observe that since both X and A^2 are self-adjoint, we have:

$$\begin{aligned} Re\left[Tr(XA^2)\right] &= \frac{1}{2}\left[Tr(XA^2) + Tr(A^2X)\right] \\ &= Tr(XA^2) \end{aligned}$$

Thus we can remove the real part, and we obtain the inequality in the statement. □

In order to further improve the above result, we will need:

Proposition 12.16. *For a self-adjoint matrix $X \in M_N(\mathbb{C})$, the following are equivalent:*

(1) $Tr(XA^2) \leq 0$*, for any anti-hermitian matrix* $A \in M_N(\mathbb{C})$*.*
(2) $Tr(XB^2) \geq 0$*, for any hermitian matrix* $B \in M_N(\mathbb{C})$*.*
(3) $Tr(XC) \geq 0$*, for any positive matrix* $C \in M_N(\mathbb{C})$*.*
(4) $X \geq 0$*.*

Proof. These equivalences are well-known, the proof being as follows:

(1) $\implies$ (2) follows by taking $B = iA$.

(2) $\implies$ (3) follows by taking $C = B^2$.

(3) $\implies$ (4) follows by diagonalizing X, and then taking C to be diagonal.

(4) $\implies$ (1) is clear as well, because with $Y = \sqrt{X}$ we have:

$$\begin{aligned} Tr(XA^2) &= Tr(Y^2A^2) \\ &= Tr(YA^2Y) \\ &= -Tr((YA)(YA)^*) \\ &\leq 0 \end{aligned}$$

Thus, the above four conditions are indeed equivalent. □

Following [25], we can now formulate a final result on the subject, as follows:

Theorem 12.17. *Given $U \in U_N$, set $S_{ij} = \mathrm{sgn}(U_{ij})$, and $X = S^*U$. Then U locally maximizes the 1-norm on U_N precisely when $X \geq 0$, and when*

$$\Phi(U, B) = Tr(XB^2) - \sum_{ij} \frac{Re\left[(UB)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|}$$

is positive, for any hermitian matrix $B \in M_N(\mathbb{C})$.

Proof. This follows from Theorem 12.15, by setting $A = iB$, and by using Proposition 12.16, which shows that we must have indeed $X \geq 0$. $\square$

Quite surprisingly, the basic real almost Hadamard matrix K_N is not an almost Hadamard matrix in the complex sense. That is, while $K_N/\sqrt{N}$ locally maximizes the 1-norm on O_N, it does not do so over U_N. In fact, the same happens for the other basic real almost Hadamard matrices discussed in section 3 above, such as the circulant ones, and the 2-entry ones studied there. We are led in this way to:

Conjecture 12.18 (Almost Hadamard conjecture, (AHC))**.** *Any local maximizer of the* 1*-norm on* U_N *must be a global maximizer, i.e. must be a rescaled Hadamard matrix.*

In other words, our conjecture would be that, in the complex setting, almost Hadamard implies Hadamard. This would be something useful, because we would have here a new approach to the complex Hadamard matrices, which is by construction analytic and local. As an example of a potential application, numeric methods, such as the gradient descent one, could be used for finding new examples of complex Hadamard matrices.

In order to explain this, let us study now more in detail the quantity $\Phi(U,B)$ appearing in Theorem 12.17. As a first observation here, we have the following result:

Proposition 12.19. *With* $S_{ij} = sgn(U_{ij})$ *and* $X = S^*U$ *as above, we have*

$$\Phi(U,B) = \Phi(U,B+D)$$

for any $D \in M_N(\mathbb{R})$ *diagonal.*

Proof. The matrices X, B, D being all self-adjoint, we have:

$$(XBD)^* = DBX$$

Thus when computing $\Phi(U,B+D)$, the trace term decomposes as follows:

$$\begin{aligned} Tr(X(B+D)^2) &= Tr(XB^2) + Tr(XBD) + Tr(XDB) + Tr(XD^2) \\ &= Tr(XB^2) + Tr(XBD) + Tr(DBX) + Tr(XD^2) \\ &= Tr(XB^2) + 2Re[Tr(XBD)] + Tr(XD^2) \end{aligned}$$

Regarding now the second term, with $D = diag(\lambda_1, \ldots, \lambda_N)$ with $\lambda_i \in \mathbb{R}$ we have the following formula:

$$(UD)_{ij}\overline{S}_{ij} = U_{ij}\lambda_j\overline{S}_{ij} = \lambda_j|U_{ij}|$$

Thus the second term decomposes as follows:

$$\begin{aligned}
&\sum_{ij}\frac{Re\left[(UB+UD)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|}\\
= &\sum_{ij}\frac{Re\left[(UB)_{ij}\overline{S}_{ij}+\lambda_j|U_{ij}|\right]^2}{|U_{ij}|}\\
= &\sum_{ij}\frac{\left[Re\left[(UB)_{ij}\overline{S}_{ij}\right]+\lambda_j|U_{ij}|\right]^2}{|U_{ij}|}\\
= &\sum_{ij}\frac{Re\left[(UB)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|}+2\sum_{ij}\lambda_j Re\left[(UB)_{ij}\overline{S}_{ij}\right]+\sum_{ij}\lambda_j^2|U_{ij}|
\end{aligned}$$

Now observe that the middle term in this expression is given by:

$$\begin{aligned}
2\sum_{ij}\lambda_j Re\left[(UB)_{ij}\overline{S}_{ij}\right] &= 2Re\left[\sum_{ij}\lambda_j(UB)_{ij}\overline{S}_{ij}\right]\\
&= 2Re\left[\sum_{ij}(S^*)_{ji}(UB)_{ij}D_{jj}\right]\\
&= 2Re[Tr(XBD)]
\end{aligned}$$

As for the term on the right in the above expression, this is given by:

$$\begin{aligned}
\sum_{ij}\lambda_j^2|U_{ij}| &= \sum_{ij}\lambda_j^2\overline{S}_{ij}U_{ij}\\
&= \sum_{ij}\overline{S}_{ij}(UD^2)_{ij}\\
&= Tr(XD^2)
\end{aligned}$$

Thus when doing the substraction we obtain $\Phi(U,B+D)=\Phi(U,B)$, as claimed. $\square$

Observe that with $B=0$ we obtain $\Phi(U,D)=0$, for any $D\in M_N(\mathbb{R})$ diagonal. In other words, the inequality is Theorem 12.17 is an equality, when B is diagonal.

Consider now the following matrix, which is the basic example of a real AHM:

$$K_N=\frac{1}{\sqrt{N}}\begin{pmatrix}2-N&2&\ldots&2\\2&2-N&\ldots&2\\\ldots&\ldots&\ldots&\ldots\\2&2&\ldots&2-N\end{pmatrix}$$

We have the following result, which provides the first piece of evidence for the AHC:

Theorem 12.20. *Consider the matrix $U=\frac{1}{N}(2\mathbb{I}_N-N1_N)$. Assuming that $B\in M_N(\mathbb{R})$ is symmetric and satisfies $UB=\lambda B$, we have:*

$$\Phi(U,B)=\lambda\cdot\frac{N-4}{2}\left[Tr(B^2)+\frac{\lambda N}{N-2}\sum_i B_{ii}^2\right]$$

In particular, $K_N=\sqrt{N}U$ is not complex AHM at $N\neq 4$, because:

(1) *For $B=\mathbb{I}_N$ we have $\Phi(U,B)=\frac{N^2(N-1)(N-4)}{2(N-2)}$, which is negative at $N=3$.*
(2) *For $B\in M_N(\mathbb{R})$ nonzero, symmetric, and satisfying $B\mathbb{I}_N=0$, $diag(B)=0$ we have $\Phi(U,B)=(2-\frac{N}{2})Tr(B^2)$, which is negative at $N\geq 5$.*

Proof. With $U\in O(N)$, $B\in M_N(\mathbb{R})$, the formula in Theorem 12.17 reads:

$$\Phi(U,B)=Tr(S^tUB^2)-\sum_{ij}\frac{(UB)_{ij}^2}{|U_{ij}|}$$

Asusming now $U=\frac{1}{N}(2\mathbb{I}_N-N1_N)$ and $UB=\lambda B$, this formula becomes:

$$\Phi(U,B)=\lambda\left[Tr(S^tB^2)-\lambda N\sum_{ij}\frac{B_{ij}^2}{|2-N\delta_{ij}|}\right]$$

Now observe that in our case, we have:

$$\mathbb{I}_NB=\frac{N}{2}(U+1_N)B=\frac{(\lambda+1)N}{2}B$$

Thus the trace term is given by the following formula:

$$\begin{aligned}Tr(S^tB^2)&=Tr\left[(\mathbb{I}_N-21_N)B^2\right]\\&=\left(\frac{(\lambda+1)N}{2}-2\right)Tr(B^2)\end{aligned}$$

Regarding now the sum on the right, this can be computed as follows:

$$\begin{aligned}\sum_{ij}\frac{B_{ij}^2}{|2-N\delta_{ij}|}&=\sum_{ij}B_{ij}^2\left(\frac{1}{2}+\left(\frac{1}{N-2}-\frac{1}{2}\right)\delta_{ij}\right)\\&=\sum_{ij}B_{ij}^2\left(\frac{1}{2}-\frac{N-4}{2(N-2)}\delta_{ij}\right)\\&=\frac{1}{2}Tr(B^2)-\frac{N-4}{2(N-2)}\sum_i B_{ii}^2\end{aligned}$$

We obtain the following formula, which gives the one in the statement:

$$\Phi(U,B)=\lambda\left[\left(\frac{(\lambda+1)N}{2}-2-\frac{\lambda N}{2}\right)Tr(B^2)+\frac{\lambda N(N-4)}{2(N-2)}\sum_i B_{ii}^2\right]$$

We can now prove our various results, as follows:

(1) Here we have $\lambda = 1$, and we obtain, as claimed:

$$\begin{aligned}\Phi(U,B) &= \frac{N-4}{2}\left[N^2+\frac{N^2}{N-2}\right]\\ &= \frac{N^2(N-4)(N-1)}{2(N-2)}\end{aligned}$$

(2) Here we have $\lambda = -1$, and we obtain, as claimed:

$$\Phi(U,B) = \left(2-\frac{N}{2}\right)Tr(B^2)$$

It remains to prove that matrices B as in the statement exist, at any $N \geq 5$. As a first remark, such matrices cannot exist at $N = 2,3$. At $N = 4$, however, we have solutions, which are as follows, with $x+y+z = 0$, not all zero:

$$B = \begin{pmatrix}0&x&y&z\\ x&0&z&y\\ y&z&0&x\\ z&y&x&0\end{pmatrix}$$

At $N \geq 5$ now, we can simply use this matrix, completed with 0 entries. □

Let us go back now to the inequality in Theorem 12.17. When U is a rescaled complex Hadamard matrix we have of course equality, and in addition, the following happens:

Proposition 12.21. *For a rescaled complex Hadamard matrix, a stronger version of the inequality in Theorem 12.17 holds, with the real part replaced by the absolute value.*

Proof. Indeed, for a rescaled Hadamard matrix $U = H/\sqrt{N}$ we have $S = H = \sqrt{N}U$, and thus $X = \sqrt{N}1_N$. We therefore obtain:

$$\begin{aligned}\Phi(U,B) &= \sqrt{N}\left[Tr(B^2)-\sum_{ij}Re\left[(UB)_{ij}\overline{S}_{ij}\right]^2\right]\\ &\geq \sqrt{N}\left[Tr(B^2)-\sum_{ij}|(UB)_{ij}\overline{S}_{ij}|^2\right]\\ &= \sqrt{N}\left[Tr(B^2)-\sum_{ij}|(UB)_{ij}|^2\right]\\ &= \sqrt{N}\left[Tr(B^2)-Tr(UB^2U^*)\right]\\ &= 0\end{aligned}$$

But this proves our claim, and we are done. □

We have the following result, in relation with the notion of defect, from [130]:

Theorem 12.22. *For a rescaled complex Hadamard matrix, the space*

$$E_U = \left\{ B \in M_N(\mathbb{C}) \Big| B = B^*, \Phi(U, B) = 0 \right\}$$

is isomorphic, via $B \to [(UB)_{ij}\overline{U}_{ij}]_{ij}$, to the following space:

$$D_U = \left\{ A \in M_N(\mathbb{R}) \Big| \sum_k \bar{U}_{ki} U_{kj} (A_{ki} - A_{kj}) = 0, \forall i, j \right\}$$

In particular the two "defects" $\dim_{\mathbb{R}} E_U$ and $\dim_{\mathbb{R}} D_U$ coincide.

Proof. Since a self-adjoint matrix $B \in M_N(\mathbb{C})$ belongs to E_U precisely when the only inequality in the proof of Proposition 12.21 above is saturated, we have:

$$E_U = \left\{ B \in M_N(\mathbb{C}) \Big| B = B^*, Im \left[(UB)_{ij} \overline{U}_{ij} \right] = 0, \forall i, j \right\}$$

The condition on the right tells us that the matrix $A = (UB)_{ij}\bar{U}_{ij}$ must be real. Now since the construction $B \to A$ is injective, we obtain an isomorphism, as follows:

$$E_U \simeq \left\{ A \in M_N(\mathbb{R}) \Big| A_{ij} = (UB)_{ij} \bar{U}_{ij} \implies B = B^* \right\}$$

Our claim is that the space on the right is D_U. Indeed, let us pick $A \in M_N(\mathbb{R})$. The condition $A_{ij} = (UB)_{ij}\bar{U}_{ij}$ is then equivalent to $(UB)_{ij} = NU_{ij}A_{ij}$, and so in terms of the matrix $C_{ij} = U_{ij}A_{ij}$ we have $(UB)_{ij} = NC_{ij}$, and so $UB = NC$. Thus $B = NU^*C$, and we can now perform the study of the condition $B = B^*$, as follows:

$$\begin{aligned}
B = B^* &\iff U^*C = C^*U \\
&\iff \sum_k \bar{U}_{ki} C_{kj} = \sum_k \bar{C}_{ki} U_{kj}, \forall i, j \\
&\iff \sum_k \bar{U}_{ki} U_{kj} A_{kj} = \sum_k \bar{U}_{ki} A_{ki} U_{kj}, \forall i, j
\end{aligned}$$

Thus we have reached to the condition defining D_U, and we are done. □

Regarding now the known verifications of the AHC, as already mentioned above, these basically concern the natural "candidates" coming from Theorem 12.9 and Theorem 12.10, as well as some straightforward complex generalizations of these candidates. All this is quite technical, and generally speaking, we refer here to [25]. Let us mention, however, that the main idea that emerges from [25] is that of using a method based on a random derivative, pointing towards a suitable homogeneous space coset.

13. Quantum groups

We discuss in what follows the relation between the Hadamard matrices and the quantum groups, and its potential applications to certain mathematical physics questions. The idea is very simple, namely that associated to any Hadamard matrix $H \in M_N(\mathbb{C})$ is a certain quantum permutation group $G \subset S_N^+$, which describes the "symmetries" of the matrix. As a basic illustration, for a Fourier matrix $H = F_G$ we obtain the group G itself, acting on itself, $G \subset S_G$. In general, however, we obtain non-classical quantum groups.

We will need many preliminaries, namely operator algebras and quantum spaces, then compact quantum groups, then quantum permutation groups, and finally matrix models for such quantum groups. Let us begin with the following standard result:

Theorem 13.1. *Given a Hilbert space H, the linear operators $T : H \to H$ which are bounded, in the sense that $||T|| = \sup_{||x||\leq 1} ||Tx||$ is finite, form a complex algebra with unit, denoted $B(H)$. This algebra has the following properties:*

1. *$B(H)$ is complete with respect to $||.||$, so we have a Banach algebra.*
2. *$B(H)$ has an involution $T \to T^*$, given by $< Tx, y >=< x, T^*y >$.*

In addition, the norm and involution are related by the formula $||TT^*|| = ||T||^2$.

Proof. The fact that we have indeed an algebra follows from:

$$||S + T|| \leq ||S|| + ||T|| \quad , \quad ||\lambda T|| = |\lambda| \cdot ||T|| \quad , \quad ||ST|| \leq ||S|| \cdot ||T||$$

Regarding now (1), if $\{T_n\} \subset B(H)$ is Cauchy then $\{T_n x\}$ is Cauchy for any $x \in H$, so we can define the limit $T = \lim_{n\to\infty} T_n$ by setting $Tx = \lim_{n\to\infty} T_n x$.

As for (2), here the existence of T^* comes from the fact that $\varphi(x) =< Tx, y >$ being a linear map $H \to \mathbb{C}$, we must have $\varphi(x) =< x, T^*y >$, for a certain vector $T^*y \in H$. Moreover, since this vector is unique, T^* is unique too, and we have as well:

$$(S + T)^* = S^* + T^* \quad , \quad (\lambda T)^* = \bar{\lambda} T^* \quad , \quad (ST)^* = T^* S^* \quad , \quad (T^*)^* = T$$

Observe also that we have indeed $T^* \in B(H)$, because:

$$||T|| = \sup_{||x||=1} \sup_{||y||=1} < Tx, y >= \sup_{||y||=1} \sup_{||x||=1} < x, T^*y >= ||T^*||$$

Regarding the last assertion, we have:

$$||TT^*|| \leq ||T|| \cdot ||T^*|| = ||T||^2$$

Also, we have the following estimate:

$$||T||^2 = \sup_{||x||=1} | < Tx, Tx > | = \sup_{||x||=1} | < x, T^*Tx > | \leq ||T^*T||$$

By replacing $T \to T^*$ we obtain from this $||T||^2 \leq ||TT^*||$, and we are done. $\square$

We will be interested in fact in the algebras of operators, rather than in the operators themselves. The basic axioms here, inspired from Theorem 13.1, are as follows:

Definition 13.2. *A C^*-algebra is a complex algebra with unit A, having:*

(1) *A norm $a \to ||a||$, making it a Banach algebra (the Cauchy sequences converge).*
(2) *An involution $a \to a^*$, which satisfies $||aa^*|| = ||a||^2$, for any $a \in A$.*

According to Theorem 13.1, the operator algebra $B(H)$ itself is a C^*-algebra. More generally, we have as examples all the closed $*$-subalgebras $A \subset B(H)$. We will see later on (the "GNS theorem") that any C^*-algebra appears in fact in this way.

Generally speaking, the elements $a \in A$ are best thought of as being some kind of "generalized operators", on some Hilbert space which is not present. By using this idea, one can emulate spectral theory in this setting, in the following way:

Theorem 13.3. *Given $a \in A$, define its spectrum as $\sigma(a) = \{\lambda \in \mathbb{C} | a - \lambda \notin A^{-1}\}$, and its spectral radius $\rho(a)$ as the radius of the smallest centered disk containing $\sigma(a)$.*

(1) *The spectrum of a norm one element is in the unit disk.*
(2) *The spectrum of a unitary element ($a^* = a^{-1}$) is on the unit circle.*
(3) *The spectrum of a self-adjoint element ($a = a^*$) consists of real numbers.*
(4) *The spectral radius of a normal element ($aa^* = a^*a$) is equal to its norm.*

Proof. Our first claim is that for any polynomial $f \in \mathbb{C}[X]$, and more generally for any rational function $f \in \mathbb{C}(X)$ having poles outside $\sigma(a)$, we have:

$$\sigma(f(a)) = f(\sigma(a))$$

This indeed something well-known for the usual matrices. In the general case, assume first that we have a polynomial, $f \in \mathbb{C}[X]$. If we pick an arbitrary number $\lambda \in \mathbb{C}$, and write $f(X) - \lambda = c(X - r_1) \ldots (X - r_k)$, we have then, as desired:

$$\begin{aligned}
\lambda \notin \sigma(f(a)) &\iff f(a) - \lambda \in A^{-1} \\
&\iff c(a - r_1) \ldots (a - r_k) \in A^{-1} \\
&\iff a - r_1, \ldots, a - r_k \in A^{-1} \\
&\iff r_1, \ldots, r_k \notin \sigma(a) \\
&\iff \lambda \notin f(\sigma(a))
\end{aligned}$$

Assume now that we are in the general case, $f \in \mathbb{C}(X)$. We pick $\lambda \in \mathbb{C}$, we write $f = P/Q$, and we set $F = P - \lambda Q$. By using the above finding, we obtain, as desired:

$$\begin{aligned}
\lambda \in \sigma(f(a)) &\iff F(a) \notin A^{-1} \\
&\iff 0 \in \sigma(F(a)) \\
&\iff 0 \in F(\sigma(a)) \\
&\iff \exists \mu \in \sigma(a), F(\mu) = 0 \\
&\iff \lambda \in f(\sigma(a))
\end{aligned}$$

Regarding now the assertions in the statement, these basically follow from this:

(1) This comes from the following formula, valid when $||a||<1$:

$$\frac{1}{1-a}=1+a+a^2+\ldots$$

(2) Assuming $a^*=a^{-1}$, we have the following norm computations:

$$||a||=\sqrt{||aa^*||}=\sqrt{1}=1$$

$$||a^{-1}||=||a^*||=||a||=1$$

If we denote by D the unit disk, we obtain from this, by using (1):

$$||a||=1\implies\sigma(a)\subset D$$

$$||a^{-1}||=1\implies\sigma(a^{-1})\subset D$$

On the other hand, by using the rational function $f(z)=z^{-1}$, we have:

$$\sigma(a^{-1})\subset D\implies\sigma(a)\subset D^{-1}$$

Now by putting everything together we obtain, as desired:

$$\sigma(a)\subset D\cap D^{-1}=\mathbb{T}$$

(3) This follows by using (2), and the rational function $f(z)=(z+it)/(z-it)$, with $t\in\mathbb{R}$. Indeed, for $t>>0$ the element $f(a)$ is well-defined, and we have:

$$\left(\frac{a+it}{a-it}\right)^*=\frac{a-it}{a+it}=\left(\frac{a+it}{a-it}\right)^{-1}$$

Thus $f(a)$ is a unitary, and by (2) its spectrum is contained in $\mathbb{T}$. We conclude that we have $f(\sigma(a))=\sigma(f(a))\subset\mathbb{T}$, and so $\sigma(a)\subset f^{-1}(\mathbb{T})=\mathbb{R}$, as desired.

(4) We have $\rho(a)\leq||a||$ from (1). Conversely, given $\rho>\rho(a)$, we have:

$$\int_{|z|=\rho}\frac{z^n}{z-a}\,dz=\sum_{k=0}^\infty\left(\int_{|z|=\rho}z^{n-k-1}dz\right)a^k=a^{n-1}$$

By applying the norm and taking n-th roots we obtain:

$$\rho\geq\lim_{n\to\infty}||a^n||^{1/n}$$

In the case $a=a^*$ we have $||a^n||=||a||^n$ for any exponent of the form $n=2^k$, and by taking n-th roots we get $\rho\geq||a||$. This gives the missing inequality, namely:

$$\rho(a)\geq||a||$$

In the general case $aa^*=a^*a$ we have $a^n(a^n)^*=(aa^*)^n$, and we get:

$$\rho(a)^2=\rho(aa^*)$$

Now since aa^* is self-adjoint, we get $\rho(aa^*)=||a||^2$, and we are done. $\square$

With these preliminaries in hand, we can now formulate some theorems. The basic facts about the C^*-algebras, that we will need here, can be summarized as:

Theorem 13.4. *The C^*-algebras have the following properties:*
1. *The commutative ones are those of the form $C(X)$, with X compact space.*
2. *Any such algebra A embeds as $A \subset B(H)$, for some Hilbert space H.*
3. *In finite dimensions, these are the direct sums of matrix algebras.*

Proof. All this is standard, the idea being as follows:

(1) Given a compact space X, the algebra $C(X)$ of continuous functions $f : X \to \mathbb{C}$ is indeed a C^*-algebra, with norm $||f|| = \sup_{x\in X} |f(x)|$, and involution $f^*(x) = \overline{f(x)}$. Observe that this algebra is indeed commutative, because $f(x)g(x) = g(x)f(x)$.

Conversely, if A is commutative, we can define $X = Spec(A)$ to be the space of characters $\chi : A \to \mathbb{C}$, with topology making continuous all evaluation maps $ev_a : \chi \to \chi(a)$. We have then a morphism of algebras $ev : A \to C(X)$ given by $a \to ev_a$, and Theorem 13.3 (3) shows that ev is a $*$-morphism, Theorem 13.3 (4) shows that ev is isometric, and finally the Stone-Weierstrass theorem shows that ev is surjective.

(2) This is standard for $A = C(X)$, where we can pick a probability measure on X, and set $H = L^2(X)$, and use the embedding $A \subset B(H)$ given by $f \to (g \to fg)$.

In the general case, where A is no longer commutative, the proof is quite similar, by emulating basic measure theory in the abstract C^*-algebra setting.

(3) Assuming that A is finite dimensional, we can first decompose its unit as $1 = p_1 + \ldots + p_k$, with $p_i \in A$ being minimal projections. Each of the linear spaces $A_i = p_iAp_i$ is then a non-unital $*$-subalgebra of A, and we have a non-unital $*$-algebra sum decomposition $A = A_1 \oplus \ldots \oplus A_k$. On the other hand, since each p_i is minimal, we have unital $*$-algebra isomorphisms $A_i \simeq M_{r_i}(\mathbb{C})$, where $r_i = rank(p_i)$. Thus, we obtain a C^*-algebra isomorphism $A \simeq M_{r_1}(\mathbb{C}) \oplus \ldots \oplus M_{r_k}(\mathbb{C})$, as desired. □

All the above was of course quite brief, but full details on this, covering 10-15 pages, can be found in any book on operator algebras. In what concerns us, we will be mainly interested in Theorem 13.4 (1), called Gelfand theorem, which suggests formulating:

Definition 13.5. *Given a C^*-algebra A, not necessarily commutative, we write*
$$A = C(X)$$
and call the abstract object X a compact quantum space.

In other words, we define the category of the compact quantum spaces X to be the category of the C^*-algebras A, with the arrows reversed. Due to the Gelfand theorem, 13.4 (1) above, the category of the usual compact spaces embeds covariantly into the category of the compact quantum spaces, and the image of this embedding consists precisely of the compact quantum spaces X which are "classical", in the sense that the corresponding

C^*-algebra $A = C(X)$ is commutative. Thus, what we have done here is to extend the category of the usual compact spaces, and this justifies Definition 13.5.

In practice now, the general compact quantum spaces X do not have points, but we can perfectly study them via the associated algebras $A = C(X)$, a bit in the same way as we study a compact Lie group via its associated Lie algebra, or an algebraic manifold via the ideal of polynomials vanishing on it, and so on. In short, nothing that much abstract going on here, just another instance of the old idea "we will use algebras, no need for points", with the remark that for us, the use of points will be actually forbidden.

We will be interested in what follows in the case where the compact quantum space X is a "compact quantum group". The axioms for the corresponding C^*-algebras, found by Woronowicz in [149], are, in a soft form, as follows:

Definition 13.6. *A Woronowicz algebra is a C^*-algebra A, given with a unitary matrix $u \in M_N(A)$ whose coefficients generate A, such that the formulae*

$$\Delta(u_{ij}) = \sum_k u_{ik} \otimes u_{kj}$$

$$\varepsilon(u_{ij}) = \delta_{ij}$$

$$S(u_{ij}) = u_{ji}^*$$

define morphisms of C^*-algebras $\Delta : A \to A \otimes A$, $\varepsilon : A \to \mathbb{C}$, $S : A \to A^{opp}$.

The morphisms Δ, ε, S are called comultiplication, counit and antipode. We say that A is cocommutative when $\Sigma\Delta = \Delta$, where $\Sigma(a \otimes b) = b \otimes a$ is the flip. We have the following result, which justifies the terminology and axioms:

Proposition 13.7. *The following are Woronowicz algebras:*

(1) *$C(G)$, with $G \subset U_N$ compact Lie group. Here the structural maps are:*

$$\begin{aligned}\Delta(\varphi) &= (g,h) \to \varphi(gh)\\ \varepsilon(\varphi) &= \varphi(1)\\ S(\varphi) &= g \to \varphi(g^{-1})\end{aligned}$$

(2) *$C^*(\Gamma)$, with $F_N \to \Gamma$ finitely generated group. Here the structural maps are:*

$$\begin{aligned}\Delta(g) &= g \otimes g\\ \varepsilon(g) &= 1\\ S(g) &= g^{-1}\end{aligned}$$

Moreover, we obtain in this way all the commutative/cocommutative algebras.

Proof. This is something very standard, the idea being as follows:

(1) Consider a compact Lie group $G\subset U_N$. We can set $A=C(G)$, which is a Woronowicz algebra, together with the matrix $u=(u_{ij})$ formed by coordinates of G, given by:

$$g=\begin{pmatrix}u_{11}(g)&\ldots&u_{1N}(g)\\ \vdots&&\vdots\\ u_{N1}(g)&\ldots&u_{NN}(g)\end{pmatrix}$$

Conversely, if (A,u) is a commutative Woronowicz algebra, by using the Gelfand theorem we can write $A=C(X)$, with X being a certain compact space. The coordinates u_{ij} give then an embedding $X\subset M_N(\mathbb C)$, and since the matrix $u=(u_{ij})$ is unitary we actually obtain an embedding $X\subset U_N$, and finally by using the maps Δ,ε,S we conclude that our compact subspace $X\subset U_N$ is in fact a compact Lie group, as desired.

(2) Consider a finitely generated group $F_N\to\Gamma$. We can set $A=C^*(\Gamma)$, which is by definition the completion of the complex group algebra $\mathbb C[\Gamma]$, with involution given by $g^*=g^{-1}$, for any $g\in\Gamma$, with respect to the biggest C^*-norm, and we obtain a Woronowicz algebra, together with the diagonal matrix formed by the generators of Γ:

$$u=\begin{pmatrix}g_1&&0\\ &\ddots&\\ 0&&g_N\end{pmatrix}$$

Conversely, if (A,u) is a cocommutative Woronowicz algebra, the Peter-Weyl theory of Woronowicz, to be explained below, shows that the irreducible corepresentations of A are all 1-dimensional, and form a group Γ, and so we have $A=C^*(\Gamma)$, as desired. □

In relation with the above, starting from Definition 13.5, we should mention that there are some functional analysis subtleties here, coming from the fact that our quantum spaces and groups must be actually divided by an equivalence relation, for everything to work fine. To be more precise, in the context of Definition 13.6, we write $(A,u)=(B,v)$ when there is a $*$-algebra isomorphism $<u_{ij}>\simeq<v_{ij}>$ mapping $u_{ij}\to v_{ij}$. See [149].

In general now, the structural maps Δ,ε,S have the following properties:

Proposition 13.8. *Let (A,u) be a Woronowicz algebra.*

(1) *Δ,ε satisfy the usual axioms for a comultiplication and a counit, namely:*

$$\begin{aligned}(\Delta\otimes id)\Delta&=(id\otimes\Delta)\Delta\\ (\varepsilon\otimes id)\Delta&=(id\otimes\varepsilon)\Delta=id\end{aligned}$$

(2) *S satisfies the antipode axiom, on the $*$-subalgebra generated by entries of u:*

$$m(S\otimes id)\Delta=m(id\otimes S)\Delta=\varepsilon(.)1$$

(3) *In addition, the square of the antipode is the identity, $S^2=id$.*

Proof. The two comultiplication axioms follow from:

$$\begin{aligned}(\Delta\otimes id)\Delta(u_{ij}) &= (id\otimes\Delta)\Delta(u_{ij})=\sum_{kl}u_{ik}\otimes u_{kl}\otimes u_{lj}\\ (\varepsilon\otimes id)\Delta(u_{ij}) &= (id\otimes\varepsilon)\Delta(u_{ij})=u_{ij}\end{aligned}$$

As for the antipode formulae, the verification here is similar. □

Summarizing, the Woronowicz algebras appear to have nice properties. In view of Proposition 13.7 and Proposition 13.8, we can formulate the following definition:

Definition 13.9. *Given a Woronowicz algebra A, we formally write*

$$A=C(G)=C^*(\Gamma)$$

and call G compact quantum group, and Γ discrete quantum group.

When A is both commutative and cocommutative, G is a compact abelian group, Γ is a discrete abelian group, and these groups are dual to each other, $G=\widehat{\Gamma},\Gamma=\widehat{G}$. In general, we still agree to write, but in a formal sense:

$$G=\widehat{\Gamma}\quad,\quad\Gamma=\widehat{G}$$

With this in mind, let us call now corepresentation of A any unitary matrix $v\in M_n(A)$ satisfying the same conditions as those satisfied by u, namely:

$$\Delta(v_{ij})=\sum_k v_{ik}\otimes v_{kj}\quad,\quad\varepsilon(v_{ij})=\delta_{ij}\quad,\quad S(v_{ij})=v_{ji}^*$$

These corepresentations can be thought of as corresponding to the unitary representations of the underlying compact quantum group G. As main examples, we have $u=(u_{ij})$ itself, its conjugate $\bar{u}=(u_{ij}^*)$, as well as any tensor product between $u,\bar{u}$.

We have the following key result, due to Woronowicz [149]:

Theorem 13.10. *Any Woronowicz algebra has a unique Haar integration functional,*

$$\left(\int_G\otimes id\right)\Delta=\left(id\otimes\int_G\right)\Delta=\int_G(.)1$$

which can be constructed by starting with any faithful positive form $\varphi\in A^*$, and setting

$$\int_G=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^n\varphi^{*k}$$

where $\phi*\psi=(\phi\otimes\psi)\Delta$. Moreover, for any corepresentation $v\in M_n(\mathbb{C})\otimes A$ we have

$$\left(id\otimes\int_G\right)v=P$$

where P is the orthogonal projection onto $Fix(v)=\{\xi\in\mathbb{C}^n|v\xi=\xi\}$.

Proof. Following [149], this can be done in 3 steps, as follows:

(1) Given $\varphi\in A^*$, our claim is that the following limit converges, for any $a\in A$:

$$\int_\varphi a=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^n\varphi^{*k}(a)$$

Indeed, by linearity we can assume that a is the coefficient of corepresentation, $a=(\tau\otimes id)v$. But in this case, an elementary computation shows that we have the following formula, where P_φ is the orthogonal projection onto the 1-eigenspace of $(id\otimes\varphi)v$:

$$\left(id\otimes\int_\varphi\right)v=P_\varphi$$

(2) Since $v\xi=\xi$ implies $[(id\otimes\varphi)v]\xi=\xi$, we have $P_\varphi\geq P$, where P is the orthogonal projection onto the space $Fix(v)=\{\xi\in\mathbb C^n|v\xi=\xi\}$. The point now is that when $\varphi\in A^*$ is faithful, by using a positivity trick, one can prove that we have $P_\varphi=P$. Thus our linear form $\int_\varphi$ is independent of φ, and is given on coefficients $a=(\tau\otimes id)v$ by:

$$\left(id\otimes\int_\varphi\right)v=P$$

(3) With the above formula in hand, the left and right invariance of $\int_G=\int_\varphi$ is clear on coefficients, and so in general, and this gives all the assertions. See [149]. □

Consider the dense $*$-subalgebra $\mathcal A\subset A$ generated by the coefficients of the fundamental corepresentation u, and endow it with the following scalar product:

$$<a,b>=\int_G ab^*$$

We have then the following result, also from [149]:

Theorem 13.11. *We have the following Peter-Weyl type results:*

1. *Any corepresentation decomposes as a sum of irreducible corepresentations.*
2. *Each irreducible corepresentation appears inside a certain $u^{\otimes k}$.*
3. *$\mathcal A=\bigoplus_{v\in Irr(A)}M_{\dim(v)}(\mathbb C)$, the summands being pairwise orthogonal.*
4. *The characters of irreducible corepresentations form an orthonormal system.*

Proof. All these results are from [149], the idea being as follows:

(1) Given $v\in M_n(A)$, its intertwiner algebra $End(v)=\{T\in M_n(\mathbb C)|Tv=vT\}$ is a finite dimensional C^*-algebra, and so decomposes as $End(v)=M_{n_1}(\mathbb C)\oplus\ldots\oplus M_{n_r}(\mathbb C)$. But this gives a decomposition of type $v=v_1+\ldots+v_r$, as desired.

(2) Consider indeed the Peter-Weyl corepresentations, $u^{\otimes k}$ with k colored integer, defined by $u^{\otimes\emptyset}=1$, $u^{\otimes\circ}=u$, $u^{\otimes\bullet}=\bar u$ and multiplicativity. The coefficients of these corepresentations span the dense algebra $\mathcal A$, and by using (1), this gives the result.

(3) Here the direct sum decomposition, which is technically a $*$-coalgebra isomorphism, follows from (2). As for the second assertion, this follows from the fact that $(id\otimes\int_G)v$ is the orthogonal projection P_v onto the space $Fix(v)$, for any corepresentation v.

(4) Let us define indeed the character of $v\in M_n(A)$ to be the matrix trace, $\chi_v=Tr(v)$. Since this character is a coefficient of v, the orthogonality assertion follows from (3). As for the norm 1 claim, this follows once again from $(id\otimes\int_G)v=P_v$. □

Observe that in the cocommutative case, we obtain from (4) that the irreducible corepresentations must be all 1-dimensional, and so that we must have $A=C^*(\Gamma)$ for some discrete group Γ, as mentioned in Proposition 13.7 above.

We will be interested here in the quantum permutation groups, and their relation with the Hadamard matrices. The following key definition is due to Wang [142]:

Definition 13.12. *A magic unitary matrix is a square matrix over a C^*-algebra,*

$$u\in M_N(A)$$

whose entries are projections, summing up to 1 on each row and each column.

The basic examples of such matrices come from the usual permutation groups, $G\subset S_N$. Indeed, given such subgroup, the following matrix is magic:

$$u_{ij}=\chi\left(\sigma\in G\middle|\sigma(j)=i\right)$$

The interest in these matrices comes from the following functional analytic description of the usual symmetric group, from [142]:

Proposition 13.13. *Consider the symmetric group S_N.*

1. *The standard coordinates $v_{ij}\in C(S_N)$, coming from the embedding $S_N\subset O_N$ given by the permutation matrices, are given by $v_{ij}=\chi(\sigma|\sigma(j)=i)$.*
2. *The matrix $v=(v_{ij})$ is magic, in the sense that its entries are orthogonal projections, summing up to 1 on each row and each column.*
3. *The algebra $C(S_N)$ is isomorphic to the universal commutative C^*-algebra generated by the entries of a $N\times N$ magic matrix.*

Proof. These results are all elementary, as follows:

(1) The canonical embedding $S_N\subset O_N$, coming from the standard permutation matrices, is given by $\sigma(e_j)=e_{\sigma(j)}$. Thus, we have $\sigma=\sum_j e_{\sigma(j)j}$, so the standard coordinates on $S_N\subset O_N$ are given by $v_{ij}(\sigma)=\delta_{i,\sigma(j)}$. Thus, we must have, as claimed:

$$v_{ij}=\chi\left(\sigma\middle|\sigma(j)=i\right)$$

(2) Any characteristic function $\chi\in\{0,1\}$ being a projection in the operator algebra sense ($\chi^2=\chi^*=\chi$), we have indeed a matrix of projections. As for the sum 1 condition on rows and columns, this is clear from the formula of the elements v_{ij}.

(3) Consider the universal algebra in the statement, namely:

$$A = C^*_{comm}\left((w_{ij})_{i,j=1,\ldots,N}\Big| w = \text{magic}\right)$$

We have a quotient map $A \to C(S_N)$, given by $w_{ij} \to v_{ij}$. On the other hand, by using the Gelfand theorem we can write $A = C(X)$, with X being a compact space, and by using the coordinates w_{ij} we have $X \subset O_N$, and then $X \subset S_N$. Thus we have as well a quotient map $C(S_N) \to A$ given by $v_{ij} \to w_{ij}$, and this gives (3). See Wang [142]. □

We are led in this way to the following result:

Theorem 13.14. *The following is a Woronowicz algebra,*

$$C(S_N^+) = C^*\left((u_{ij})_{i,j=1,\ldots,N}\Big| u = \text{magic}\right)$$

and the underlying compact quantum group S_N^+ is called quantum permutation group.

Proof. As a first remark, the algebra $C(S_N^+)$ is indeed well-defined, because the magic condition forces $||u_{ij}|| \leq 1$, for any C^*-norm. Our claim now is that we can define maps Δ, ε, S as in Definition 13.6. Consider indeed the following matrix:

$$U_{ij} = \sum_k u_{ik} \otimes u_{kj}$$

As a first observation, we have $U_{ij} = U_{ij}^*$. In fact the entries U_{ij} are orthogonal projections, because we have as well:

$$U_{ij}^2 = \sum_{kl} u_{ik}u_{il} \otimes u_{kj}u_{lj} = \sum_k u_{ik} \otimes u_{kj} = U_{ij}$$

In order to prove now that the matrix $U = (U_{ij})$ is magic, it remains to verify that the sums on the rows and columns are 1. For the rows, this can be checked as follows:

$$\sum_j U_{ij} = \sum_{jk} u_{ik} \otimes u_{kj} = \sum_k u_{ik} \otimes 1 = 1 \otimes 1$$

For the columns the computation is similar, as follows:

$$\sum_i U_{ij} = \sum_{ik} u_{ik} \otimes u_{kj} = \sum_k 1 \otimes u_{kj} = 1 \otimes 1$$

Thus the matrix $U = (U_{ij})$ is magic indeed, and so we can define a comultiplication map by setting $\Delta(u_{ij}) = U_{ij}$. By using a similar reasoning, we can define as well a counit map by $\varepsilon(u_{ij}) = \delta_{ij}$, and an antipode map by $S(u_{ij}) = u_{ji}$. Thus the Woronowicz algebra axioms from Definition 13.6 are satisfied, and this finishes the proof. □

The terminology comes from the following result, also from [142]:

Proposition 13.15. *The quantum permutation group S_N^+ acts on the set $X=\{1,\ldots,N\}$, the corresponding coaction map $\Phi:C(X)\to C(X)\otimes C(S_N^+)$ being given by:*

$$\Phi(\delta_i)=\sum_j\delta_j\otimes u_{ji}$$

In fact, S_N^+ is the biggest compact quantum group acting on X, by leaving the counting measure invariant, in the sense that $(tr\otimes id)\Phi=tr(.)1$, where $tr(\delta_i)=\frac{1}{N},\forall i$.

Proof. Our claim is that given a compact quantum group G, the formula $\Phi(\delta_i)=\sum_j\delta_j\otimes u_{ji}$ defines a morphism of algebras, which is a coaction map, leaving the trace invariant, precisely when the matrix $u=(u_{ij})$ is a magic corepresentation of $C(G)$.

Indeed, let us first determine when Φ is multiplicative. We have:

$$\Phi(\delta_i)\Phi(\delta_k)=\sum_{jl}\delta_j\delta_l\otimes u_{ji}u_{lk}=\sum_j\delta_j\otimes u_{ji}u_{jk}$$

On the other hand, we have as well:

$$\Phi(\delta_i\delta_k)=\delta_{ik}\Phi(\delta_i)=\delta_{ik}\sum_j\delta_j\otimes u_{ji}$$

We conclude that the multiplicativity of Φ is equivalent to the following conditions:

$$u_{ji}u_{jk}=\delta_{ik}u_{ji}\quad,\quad\forall i,j,k$$

Regarding now the unitality of Φ, we have the following formula:

$$\Phi(1)=\sum_i\Phi(\delta_i)=\sum_{ij}\delta_j\otimes u_{ji}=\sum_j\delta_j\otimes\left(\sum_i u_{ji}\right)$$

Thus Φ is unital when the following conditions are satisfied:

$$\sum_i u_{ji}=1\quad,\quad\forall i$$

Finally, the fact that Φ is a $*$-morphism translates into:

$$u_{ij}=u_{ij}^*\quad,\quad\forall i,j$$

Summing up, in order for $\Phi(\delta_i)=\sum_j\delta_j\otimes u_{ji}$ to be a morphism of C^*-algebras, the elements u_{ij} must be projections, summing up to 1 on each row of u. Regarding now the preservation of the trace condition, observe that we have:

$$(tr\otimes id)\Phi(\delta_i)=\frac{1}{N}\sum_j u_{ji}$$

Thus the trace is preserved precisely when the elements u_{ij} sum up to 1 on each of the columns of u. We conclude from this that $\Phi(\delta_i)=\sum_j\delta_j\otimes u_{ji}$ is a morphism of C^*-algebras preserving the trace precisely when u is magic, and since the coaction conditions on Φ are equivalent to the fact that u must be a corepresentation, this finishes the proof of our claim. But this claim proves all the assertions in the statement. $\square$

As a quite surprising result now, also from [142], we have:

Theorem 13.16. *We have an embedding $S_N\subset S_N^+$, given at the algebra level by:*

$$u_{ij}\to\chi\left(\sigma\Big|\sigma(j)=i\right)$$

This is an isomorphism at $N\leq 3$, but not at $N\geq 4$, where S_N^+ is not classical, nor finite.

Proof. The fact that we have indeed an embedding as above is clear. Regarding now the second assertion, we can prove this in four steps, as follows:

Case $N=2$. The fact that S_2^+ is indeed classical, and hence collapses to S_2, is trivial, because the 2×2 magic matrices are as follows, with p being a projection:

$$U=\begin{pmatrix}p&1-p\\1-p&p\end{pmatrix}$$

Case $N=3$. It is enough to check that u_{11},u_{22} commute. But this follows from:

$$\begin{aligned}u_{11}u_{22}&=u_{11}u_{22}(u_{11}+u_{12}+u_{13})\\&=u_{11}u_{22}u_{11}+u_{11}u_{22}u_{13}\\&=u_{11}u_{22}u_{11}+u_{11}(1-u_{21}-u_{23})u_{13}\\&=u_{11}u_{22}u_{11}\end{aligned}$$

Indeed, by applying the involution to this formula, we obtain from this that we have $u_{22}u_{11}=u_{11}u_{22}u_{11}$ as well, and so we get $u_{11}u_{22}=u_{22}u_{11}$, as desired.

Case $N=4$. Consider the following matrix, with p,q being projections:

$$U=\begin{pmatrix}p&1-p&0&0\\1-p&p&0&0\\0&0&q&1-q\\0&0&1-q&q\end{pmatrix}$$

This matrix is then magic, and if we choose p,q as for the algebra $<p,q>$ to be infinite dimensional, we conclude that $C(S_4^+)$ is infinite dimensional as well.

Case $N\geq 5$. Here we can use the standard embedding $S_4^+\subset S_N^+$, obtained at the level of the corresponding magic matrices in the following way:

$$u\to\begin{pmatrix}u&0\\0&1_{N-4}\end{pmatrix}$$

Indeed, with this in hand, the fact that S_4^+ is a non-classical, infinite compact quantum group implies that S_N^+ with $N\geq 5$ has these two properties as well. See [142]. $\square$

In order to study S_N^+, we will use the following version of Tannakian duality:

Theorem 13.17. *The following operations are inverse to each other:*

(1) *The construction $A \to C$, which associates to any Woronowicz algebra A the tensor category formed by the intertwiner spaces $C_{kl} = Hom(u^{\otimes k}, u^{\otimes l})$.*
(2) *The construction $C \to A$, which associates to any tensor category C the Woronowicz algebra A presented by the relations $T \in Hom(u^{\otimes k}, u^{\otimes l})$, with $T \in C_{kl}$.*

Proof. This is something quite deep, going back to [150] in a slightly different form, and to [93] in the simplified form presented above. The idea is as follows:

(1) We have indeed a construction $A \to C$ as above, whose output is a tensor C^*-subcategory with duals of the tensor C^*-category of Hilbert spaces.

(2) We have as well a construction $C \to A$ as above, simply by dividing the free $*$-algebra on N^2 variables by the relations in the statement.

Regarding now the bijection claim, some elementary algebra shows that $C = C_{A_C}$ implies $A = A_{C_A}$, and also that $C \subset C_{A_C}$ is automatic. Thus we are left with proving $C_{A_C} \subset C$. But this latter inclusion can be proved indeed, by doing a lot of algebra, and using von Neumann's bicommutant theorem, in finite dimensions. See [93]. $\square$

We will need as well the notion of "easiness", from [32]. Let us start with:

Definition 13.18. *Let $P(k,l)$ be the set of partitions between an upper row of k points, and a lower row of l points. A set $D = \bigsqcup_{k,l} D(k,l)$ with $D(k,l) \subset P(k,l)$ is called a category of partitions when it has the following properties:*

(1) *Stability under the horizontal concatenation, $(\pi,\sigma) \to [\pi\sigma]$.*
(2) *Stability under the vertical concatenation, $(\pi,\sigma) \to [^\sigma_\pi]$.*
(3) *Stability under the upside-down turning, $\pi \to \pi^*$.*
(4) *Each set $P(k,k)$ contains the identity partition $||\ldots||$.*
(5) *The set $P(0,2)$ contains the semicircle partition $\cap$.*

As a basic example, we have the category of all partitions P itself. Other basic examples include the category of pairings P_2, or the categories NC, NC_2 of noncrossing partitions, and pairings. There are many other examples, and we will be back to this.

The relation with the Tannakian categories and duality comes from:

Proposition 13.19. *Each $\pi \in P(k,l)$ produces a linear map $T_\pi : (\mathbb{C}^N)^{\otimes k} \to (\mathbb{C}^N)^{\otimes l}$,*

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \ldots j_l} \delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

with the Kronecker type symbols $\delta_\pi \in \{0,1\}$ depending on whether the indices fit or not. The assignement $\pi \to T_\pi$ is categorical, in the sense that we have

$$T_\pi \otimes T_\sigma = T_{[\pi\sigma]} \quad , \quad T_\pi T_\sigma = N^{c(\pi,\sigma)} T_{[^\sigma_\pi]} \quad , \quad T_\pi^* = T_{\pi^*}$$

where $c(\pi,\sigma)$ are certain integers, coming from the erased components in the middle.

Proof. The concatenation axiom follows from the following computation:

$$\begin{aligned}
&(T_\pi\otimes T_\sigma)(e_{i_1}\otimes\ldots\otimes e_{i_p}\otimes e_{k_1}\otimes\ldots\otimes e_{k_r})\\
=&\sum_{j_1\ldots j_q}\sum_{l_1\ldots l_s}\delta_\pi\begin{pmatrix}i_1&\ldots&i_p\\ j_1&\ldots&j_q\end{pmatrix}\delta_\sigma\begin{pmatrix}k_1&\ldots&k_r\\ l_1&\ldots&l_s\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_q}\otimes e_{l_1}\otimes\ldots\otimes e_{l_s}\\
=&\sum_{j_1\ldots j_q}\sum_{l_1\ldots l_s}\delta_{[\pi\sigma]}\begin{pmatrix}i_1&\ldots&i_p&k_1&\ldots&k_r\\ j_1&\ldots&j_q&l_1&\ldots&l_s\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_q}\otimes e_{l_1}\otimes\ldots\otimes e_{l_s}\\
=&\ T_{[\pi\sigma]}(e_{i_1}\otimes\ldots\otimes e_{i_p}\otimes e_{k_1}\otimes\ldots\otimes e_{k_r})
\end{aligned}$$

The composition axiom follows from the following computation:

$$\begin{aligned}
&T_\pi T_\sigma(e_{i_1}\otimes\ldots\otimes e_{i_p})\\
=&\sum_{j_1\ldots j_q}\delta_\sigma\begin{pmatrix}i_1&\ldots&i_p\\ j_1&\ldots&j_q\end{pmatrix}\sum_{k_1\ldots k_r}\delta_\pi\begin{pmatrix}j_1&\ldots&j_q\\ k_1&\ldots&k_r\end{pmatrix}e_{k_1}\otimes\ldots\otimes e_{k_r}\\
=&\sum_{k_1\ldots k_r}N^{c(\pi,\sigma)}\delta_{[^\sigma_\pi]}\begin{pmatrix}i_1&\ldots&i_p\\ k_1&\ldots&k_r\end{pmatrix}e_{k_1}\otimes\ldots\otimes e_{k_r}\\
=&\ N^{c(\pi,\sigma)}T_{[^\sigma_\pi]}(e_{i_1}\otimes\ldots\otimes e_{i_p})
\end{aligned}$$

Finally, the involution axiom follows from the following computation:

$$\begin{aligned}
&T_\pi^*(e_{j_1}\otimes\ldots\otimes e_{j_q})\\
=&\sum_{i_1\ldots i_p}<T_\pi^*(e_{j_1}\otimes\ldots\otimes e_{j_q}),e_{i_1}\otimes\ldots\otimes e_{i_p}>e_{i_1}\otimes\ldots\otimes e_{i_p}\\
=&\sum_{i_1\ldots i_p}\delta_\pi\begin{pmatrix}i_1&\ldots&i_p\\ j_1&\ldots&j_q\end{pmatrix}e_{i_1}\otimes\ldots\otimes e_{i_p}\\
=&\ T_{\pi^*}(e_{j_1}\otimes\ldots\otimes e_{j_q})
\end{aligned}$$

Summarizing, our correspondence is indeed categorical. □

In relation with the quantum groups, we have the following notion, from [32]:

Definition 13.20. *A compact quantum matrix group G is called easy when we have*

$$Hom(u^{\otimes k},u^{\otimes l})=span\left(T_\pi\Big|\pi\in D(k,l)\right)$$

for any colored integers k,l, for certain sets of partitions $D(k,l)\subset P(k,l)$, where

$$T_\pi(e_{i_1}\otimes\ldots\otimes e_{i_k})=\sum_{j_1\ldots j_l}\delta_\pi\begin{pmatrix}i_1&\ldots&i_k\\ j_1&\ldots&j_l\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_l}$$

with the Kronecker type symbols $\delta_\pi\in\{0,1\}$ depending on whether the indices fit or not.

We can now formulate our main result regarding S_N^+, as follows:

Theorem 13.21. *We have the following results:*

(1) S_N *is easy, coming from the category of all partitions* P.
(2) S_N^+ *is easy, coming from the category of all noncrossing partitions* NC.

Proof. This is something quite fundamental, with the proof, using the above Tannakian results and subsequent easiness theory, being as follows:

(1) S_N^+. We know that this quantum group comes from the magic condition. In order to interpret this magic condition, consider the fork partition:

$$Y \in P(2,1)$$

The linear map associated to this fork partition Y is then given by:

$$T_Y(e_i \otimes e_j) = \delta_{ij} e_i$$

Thus, in usual matrix notation, this linear map is given by:

$$T_Y = (\delta_{ijk})_{i,jk}$$

Now given a corepresentation u, we have the following formula:

$$(T_Y u^{\otimes 2})_{i,jk} = \sum_{lm} (T_Y)_{i,lm} (u^{\otimes 2})_{lm,jk} = u_{ij} u_{ik}$$

We have as well the following formula:

$$(u T_Y)_{i,jk} = \sum_l u_{il} (T_Y)_{l,jk} = \delta_{jk} u_{ij}$$

We conclude that we have the following equivalence:

$$T_Y \in Hom(u^{\otimes 2}, u) \iff u_{ij} u_{ik} = \delta_{jk} u_{ij}, \forall i, j, k$$

The condition on the right being equivalent to the magic condition, we obtain that S_N^+ is indeed easy, the corresponding category of partitions being, as desired:

$$D =< Y >= NC$$

(2) S_N. Here there is no need for new computations, because we have:

$$S_N = S_N^+ \cap O_N$$

At the categorical level means that S_N is easy, coming from:

$$< NC, \slash\!\!\!\backslash >= P$$

Alternatively, we can rewrite the above proof for S_N^+, by adding at each step the basic crossing $\slash\!\!\!\backslash$ next to the fork partition Y. $\square$

Let us discuss now the computation of the law of the main character. This computation is the main problem regarding any compact quantum group, as shown by the following result, which summarizes the various motivations for doing this:

Theorem 13.22. *Given a Woronowicz algebra (A,u), the law of the main character*

$$\chi=\sum_{i=1}^N u_{ii}$$

with respect to the Haar integration has the following properties:

(1) *The moments of χ are the numbers $M_k=\dim(Fix(u^{\otimes k}))$.*
(2) *M_k counts as well the lenght p loops at 1, on the Cayley graph of A.*
(3) *$law(\chi)$ is the Kesten measure of the associated discrete quantum group.*
(4) *When $u\sim\bar{u}$ the law of χ is a usual measure, supported on $[-N,N]$.*
(5) *The algebra A is amenable precisely when $N\in supp(law(Re(\chi)))$.*
(6) *Any morphism $f:(A,u)\to(B,v)$ must increase the numbers M_k.*
(7) *Such a morphism f is an isomorphism when $law(\chi_u)=law(\chi_v)$.*

Proof. All this is quite advanced, the idea being as follows:

(1) This comes from the Peter-Weyl type theory in [149], which tells us the number of fixed points of $v=u^{\otimes k}$ can be recovered by integrating the character $\chi_v=\chi_u^k$.

(2) This is something true, and well-known, for $A=C^*(\Gamma)$, with $\Gamma=<g_1,\ldots,g_N>$ being a discrete group. In general, the proof is quite similar.

(3) This is actually the definition of the Kesten measure, in the case $A=C^*(\Gamma)$, with $\Gamma=<g_1,\ldots,g_N>$ being a discrete group. In general, this follows from (2).

(4) The equivalence $u\sim\bar{u}$ translates into $\chi_u=\chi_u^*$, and this gives the first assertion. As for the support claim, this follows from $uu^*=1\implies||u_{ii}||\leq1$, for any i.

(5) This is the Kesten amenability criterion, which can be established as in the classical case, $A=C^*(\Gamma)$, with $\Gamma=<g_1,\ldots,g_N>$ being a discrete group.

(6) This is something elementary, which follows from (1) above, and from the fact that the morphisms of Woronowicz algebras increase the spaces of fixed points.

(7) This follows by using (6), and the Peter-Weyl type theory from [149], the idea being that if f is not injective, then it must strictly increase one of the spaces $Fix(u^{\otimes k})$. □

All the above was quite short, but details on all this, characters and motivations for computing laws of characters, can be found in any good quantum group book.

In the case of the symmetric group S_N, the character result is as follows:

Theorem 13.23. *For the symmetric group S_N the main character counts the fixed points,*

$$\chi(\sigma)=\#\left\{i\in\{1,\ldots,N\}\Big|\sigma(i)=i\right\}$$

and its law becomes Poisson (1), in the $N\to\infty$ limit.

Proof. This is something very classical, which can be done in 3 steps, as follows:

(1) A straightforward application of the inclusion-exclusion principle shows that the number of permutations $\sigma \in S_N$ having no fixed points is:

$$N_\emptyset = N!\sum_{k=0}^N \frac{(-1)^k}{k!}$$

(2) Thus, when dividing by $N!$, and letting $N \to \infty$, we obtain:

$$P(\chi = 0) \simeq \frac{1}{e}$$

(3) In fact, the same method gives the following formula, valid for any $k \in \mathbb{N}$:

$$P(\chi = k) \simeq \frac{1}{ek!}$$

But this shows that χ becomes Poisson (1) with $N \to \infty$, as claimed. $\square$

In order to include as well S_N^+ in our discussion, we will need the following result, with $*$ being the classical convolution, and $\boxplus$ being Voiculescu's free convolution [138]:

Theorem 13.24. *The following Poisson type limits converge, for any $t > 0$,*

$$p_t = \lim_{n\to\infty}\left(\left(1-\frac{1}{n}\right)\delta_0 + \frac{1}{n}\delta_t\right)^{*n}$$

$$\pi_t = \lim_{n\to\infty}\left(\left(1-\frac{1}{n}\right)\delta_0 + \frac{1}{n}\delta_t\right)^{\boxplus n}$$

the limiting measures being the Poisson law p_t, and the Marchenko-Pastur law π_t,

$$p_t = \frac{1}{e^t}\sum_{k=0}^\infty \frac{t^k\delta_k}{k!}$$

$$\pi_t = \max(1-t,0)\delta_0 + \frac{\sqrt{4t-(x-1-t)^2}}{2\pi x}\,dx$$

whose moments are given by the following formulae:

$$M_k(p_t) = \sum_{\pi\in P(k)} t^{|\pi|}$$

$$M_k(\pi_t) = \sum_{\pi\in NC(k)} t^{|\pi|}$$

The Marchenko-Pastur measure π_t is also called free Poisson law.

Proof. This is something quite advanced, related to probability theory, free probability theory, and random matrices, the idea being as follows:

(1) The first step is that of finding suitable functional transforms, which linearize the convolution operations in the statement. In the classical case this is the logarithm of the Fourier transform $\log F$, and in the free case this is Voiculescu's R-transform.

(2) With these tools in hand, the above limiting theorems can be proved in a standard way, a bit as when proving the Central Limit Theorem. The computations give the moment formulae in the statement, and the density computations are standard as well.

(3) Finally, in order for the discussion to be complete, what still remains to be explained is the precise nature of the "liberation" operation $p_t \to \pi_t$, as well as the random matrix occurrence of π_t. This is more technical, and we refer here to [38], [94], [140]. $\square$

Getting back now to quantum permutations, the results here are as follows:

Theorem 13.25. *The law of the main character, given by*

$$\chi = \sum_i u_{ii}$$

for S_N/S_N^+ becomes p_1/π_1 with $N \to \infty$. As for the truncated character

$$\chi_t = \sum_{i=1}^{[tN]} u_{ii}$$

for S_N/S_N^+, with $t \in (0,1]$, this becomes p_t/π_t with $N \to \infty$.

Proof. This is something quite technical, the idea being as follows:

(1) In the classical case this is well-known, and follows by using the inclusion-exclusion principle, and then letting $N \to \infty$, as in the proof of Theorem 13.23.

(2) In the free case we know from easiness that $Fix(u^{\otimes k}) = span(NC(k))$ at $N \geq 4$, and at the probabilistic level, this leads to the formulae in the statement. See [16]. $\square$

There are many other things known about the quantum permutations. See [16].

14. Hadamard models

We have seen that a free analogue S_N^+ of the usual permutation group S_N can be constructed, as a compact quantum group, according to the following formula, with "magic" meaning formed of projections, which sum up to 1 on each row and each column:

$$C(S_N^+)=C^*\left((u_{ij})_{i,j=1,\ldots,N}\Big|u=\text{magic}\right)$$

We discuss here the construction of the quantum permutation group $G\subset S_N^+$ associated to a complex Hadamard matrix $H\in M_N(\mathbb{C})$. The idea will be that G encodes the "symmetries" of H, a bit in the same way as $\mathbb{Z}_N$ encodes the symmetries of F_N.

As a first observation, the complex Hadamard matrices are related to the quantum permutation groups, via the following simple fact:

Proposition 14.1. *If $H\in M_N(\mathbb{C})$ is Hadamard, the rank one projections*

$$P_{ij}=Proj\left(\frac{H_i}{H_j}\right)$$

where $H_1,\ldots,H_N\in\mathbb{T}^N$ are the rows of H, form a magic unitary.

Proof. This is clear, the verification for the rows being as follows:

$$\left\langle\frac{H_i}{H_j},\frac{H_i}{H_k}\right\rangle=\sum_l\frac{H_{il}}{H_{jl}}\cdot\frac{H_{kl}}{H_{il}}=\sum_l\frac{H_{kl}}{H_{jl}}=N\delta_{jk}$$

As for the verification for the columns, this is similar, as follows:

$$\left\langle\frac{H_i}{H_j},\frac{H_k}{H_j}\right\rangle=\sum_l\frac{H_{il}}{H_{jl}}\cdot\frac{H_{jl}}{H_{kl}}=\sum_l\frac{H_{il}}{H_{kl}}=N\delta_{ik}$$

Thus, we have indeed a magic unitary, as claimed. □

The above result suggests the following definition:

Definition 14.2. *Associated to any Hadamard matrix $H\in M_N(\mathbb{C})$ is the representation*

$$\pi:C(S_N^+)\to M_N(\mathbb{C})$$
$$u_{ij}\to Proj\left(\frac{H_i}{H_j}\right)$$

where $H_1,\ldots,H_N\in\mathbb{T}^N$ are the rows of H.

The representation π constructed above is a "matrix model" for the algebra $C(S_N^+)$, in the sense that the standard generators $u_{ij}\in C(S_N^+)$, and more generally any element $a\in C(S_N^+)$, gets modelled in this way by an explicit matrix $\pi(a)\in M_N(\mathbb{C})$.

The point now is that, given such a model, we have the following notions:

Definition 14.3. *Let G be a compact matrix quantum group, and let $\pi : C(G) \to M_N(\mathbb{C})$ be a matrix model for the associated Woronowicz algebra.*

(1) *The Hopf image of π is the smallest quotient Woronowicz algebra $C(G) \to C(H)$ producing a factorization of type $\pi : C(G) \to C(H) \to M_N(\mathbb{C})$.*
(2) *When the inclusion $H \subset G$ is an isomorphism, i.e. when there is no non-trivial factorization as above, we say that π is inner faithful.*

As a first observation, in the case where the model is faithful, $\pi : C(G) \subset M_N(\mathbb{C})$, the Hopf image is the algebra $C(G)$ itself, and the model is inner faithful as well. However, this is something that will not appear often in practice, because the existence of an embedding $C(G) \subset M_N(\mathbb{C})$ forces the algebra $C(G)$ to be finite dimensional, and so G to be a finite quantum group. At the level of non-trivial examples now, we have:

(1) In the case where $G = \widehat{\Gamma}$ is a group dual, the model $\pi : C(G) = C^*(\Gamma) \to M_N(\mathbb{C})$ must come from a unitary group representation $\rho : \Gamma \to U_N$, the minimal factorization of π is the one obtained by taking the image, $\rho : \Gamma \to \Lambda \subset U_N$, and the model π is inner faithful when $\Gamma \subset U_N$. This is the main example of the construction in Definition 14.3, which provides intuition, and justifies the terminology as well.

(2) In the case where G is a classical compact group, we have a standard construction of a matrix model for $C(G)$, obtained by taking an arbitrary family of elements $g_1, \ldots, g_N \in G$, and then constructing the representation $\pi : C(G) \to M_N(\mathbb{C})$ given by $f \to diag(f(g_1), \ldots, f(g_N))$. The minimal factorization of π is then via the algebra $C(H)$, with $H = \overline{< g_1, \ldots, g_N >} \subset G$, and π is inner faithful when $G = H$.

In general, the existence and uniqueness of the Hopf image follow by dividing $C(G)$ by a suitable ideal. We refer to [14] for more details regarding this construction. In relation now with the complex Hadamard matrices, we can simply combine Definition 14.2 and Definition 14.3, and we are led in this way into the following notion:

Definition 14.4. *To any Hadamard matrix $H \in M_N(\mathbb{C})$ we associate the quantum permutation group $G \subset S_N^+$ given by the following Hopf image factorization,*

$$\begin{tikzcd} C(S_N^+) \arrow[rr, "\pi"] \arrow[dr] & & M_N(\mathbb{C}) \\ & C(G) \arrow[ur] & \end{tikzcd}$$

where $\pi(u_{ij}) = Proj(H_i/H_j)$, with $H_1, \ldots, H_N \in \mathbb{T}^N$ being the rows of H.

Our claim now is that this construction $H \to G$ is something really useful, with G encoding the combinatorics of H, a bit in the same way as $\mathbb{Z}_N$ encodes the combinatorics of F_N. There are several results supporting this, and as a first such result, we have:

Theorem 14.5. *The construction $H \to G$ has the following properties:*

1. *For $H = F_N$ we obtain the group $G = \mathbb{Z}_N$, acting on itself.*
2. *More generally, for $H = F_G$ we obtain the group G itself, acting on itself.*
3. *For a tensor product $H = H' \otimes H''$ we obtain a product, $G = G' \times G''$.*

Proof. All this is standard, and elementary, as follows:

(1) The rows of the Fourier matrix $H = F_N$ are given by $H_i = \rho^i$, where $\rho = (1, w, w^2, \ldots, w^{N-1})$, with $w = e^{2\pi i/N}$. Thus, we have the following formula:

$$\frac{H_i}{H_j} = \rho^{i-j}$$

It follows that the corresponding rank 1 projections $P_{ij} = Proj(H_i/H_j)$ form a circulant matrix, all whose entries commute. Since the entries commute, the corresponding quantum group must satisfy $G \subset S_N$. Now by taking into account the circulant property of $P = (P_{ij})$ as well, we are led to the conclusion that we have $G = \mathbb{Z}_N$.

(2) In the general case now, where $H = F_G$, with G being an arbitrary finite abelian group, the result can be proved either by extending the above proof, of by decomposing $G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$ and using (3) below, whose proof is independent from (1,2).

(3) Assume that we have a tensor product $H = H' \otimes H''$, and let G, G', G'' be the associated quantum permutation groups. We have then a diagram as follows:

$$\begin{tikzcd}
C(S_{N'}^+) \otimes C(S_{N''}^+) \arrow[r] & C(G') \otimes C(G'') \arrow[r] & M_{N'}(\mathbb{C}) \otimes M_{N''}(\mathbb{C}) \arrow[d] \\
C(S_N^+) \arrow[r] \arrow[u] & C(G) \arrow[r] & M_N(\mathbb{C})
\end{tikzcd}$$

Here all the maps are the canonical ones, with those on the left and on the right coming from $N = N'N''$. At the level of standard generators, the diagram is as follows:

$$\begin{tikzcd}
u'_{ij} \otimes u''_{ab} \arrow[r] & w'_{ij} \otimes w''_{ab} \arrow[r] & P'_{ij} \otimes P''_{ab} \arrow[d] \\
u_{ia,jb} \arrow[r] \arrow[u] & w_{ia,jb} \arrow[r] & P_{ia,jb}
\end{tikzcd}$$

Now observe that this diagram commutes. We conclude that the representation associated to H factorizes indeed through $C(G') \otimes C(G'')$, and this gives the result. $\square$

Generally speaking, going beyond Theorem 14.5 is a quite difficult question. There are several computations available here, for the most regarding the deformations of the Fourier matrices, and we will be back to all this later, in section 16 below.

Let us keep discussing what happens at the general level. We will need the following result, valid in the general context of the Hopf image construction:

Theorem 14.6. *Given a matrix model $\pi : C(G) \to M_N(\mathbb{C})$, the fundamental corepresentation v of its Hopf image is subject to the Tannakian conditions*

$$Hom(v^{\otimes k}, v^{\otimes l}) = Hom(U^{\otimes k}, U^{\otimes l})$$

where $U_{ij} = \pi(u_{ij})$, and where the spaces on the right are taken in a formal sense.

Proof. Since the morphisms increase the intertwining spaces, when defined either in a representation theory sense, or just formally, we have inclusions as follows:

$$Hom(u^{\otimes k}, u^{\otimes l}) \subset Hom(U^{\otimes k}, U^{\otimes l})$$

More generally, we have such inclusions when replacing (G, u) with any pair producing a factorization of π. Thus, by Tannakian duality [150], the Hopf image must be given by the fact that the intertwining spaces must be the biggest, subject to these inclusions.

On the other hand, since u is biunitary, so is U, and it follows that the spaces on the right form a Tannakian category. Thus, we have a quantum group (H, v) given by:

$$Hom(v^{\otimes k}, v^{\otimes l}) = Hom(U^{\otimes k}, U^{\otimes l})$$

By the above discussion, $C(H)$ follows to be the Hopf image of π, as claimed. □

With the above result in hand, we can compute the Tannakian category of the Hopf image, in the Hadamard matrix case, and we are led in this way to:

Theorem 14.7. *The Tannakian category of the quantum group $G \subset S_N^+$ associated to a complex Hadamard matrix $H \in M_N(\mathbb{C})$ is given by*

$$T \in Hom(u^{\otimes k}, u^{\otimes l}) \iff T^\circ G^{k+2} = G^{l+2} T^\circ$$

where the objects on the right are constructed as follows:

(1) $T^\circ = id \otimes T \otimes id$.
(2) $G_{ia}^{jb} = \sum_k H_{ik} \bar{H}_{jk} \bar{H}_{ak} H_{bk}$.
(3) $G^k_{i_1 \ldots i_k, j_1 \ldots j_k} = G^{j_k j_{k-1}}_{i_k i_{k-1}} \ldots G^{j_2 j_1}_{i_2 i_1}$.

Proof. With the notations in Theorem 14.6, we have the following formula:

$$Hom(u^{\otimes k}, u^{\otimes l}) = Hom(U^{\otimes k}, U^{\otimes l})$$

The vector space on the right consists by definition of the complex $N^l \times N^k$ matrices T, satisfying the following relation:

$$TU^{\otimes k} = U^{\otimes l} T$$

If we denote this equality by $L = R$, the left term L is given by:

$$\begin{aligned} L_{ij} &= (TU^{\otimes k})_{ij} \\ &= \sum_a T_{ia} U^{\otimes k}_{aj} \\ &= \sum_a T_{ia} U_{a_1 j_1} \ldots U_{a_k j_k} \end{aligned}$$

As for the right term R, this is given by:

$$\begin{aligned} R_{ij} &= (U^{\otimes l} T)_{ij} \\ &= \sum_b U^{\otimes l}_{ib} T_{bj} \\ &= \sum_b U_{i_1 b_1} \ldots U_{i_l b_l} T_{bj} \end{aligned}$$

Consider now the vectors $\xi_{ij} = H_i / H_j$. Since these vectors span the ambient Hilbert space, the equality $L = R$ is equivalent to the following equality:

$$< L_{ij} \xi_{pq}, \xi_{rs} > = < R_{ij} \xi_{pq}, \xi_{rs} >$$

We use now the following well-known formula, expressing a product of rank one projections $P_1, \ldots, P_k$ in terms of the corresponding image vectors $\xi_1, \ldots, \xi_k$:

$$< P_1 \ldots P_k x, y > = < x, \xi_k >< \xi_k, \xi_{k-1} > \ldots\ldots < \xi_2, \xi_1 >< \xi_1, y >$$

This gives the following formula for L:

$$\begin{aligned} < L_{ij} \xi_{pq}, \xi_{rs} > &= \sum_a T_{ia} < P_{a_1 j_1} \ldots P_{a_k j_k} \xi_{pq}, \xi_{rs} > \\ &= \sum_a T_{ia} < \xi_{pq}, \xi_{a_k j_k} > \ldots < \xi_{a_1 j_1}, \xi_{rs} > \\ &= \sum_a T_{ia} G^{q j_k}_{p a_k} G^{j_k j_{k-1}}_{a_k a_{k-1}} \ldots G^{j_2 j_1}_{a_2 a_1} G^{j_1 s}_{a_1 r} \\ &= \sum_a T_{ia} G^{k+2}_{rap, sjq} \\ &= (T^\circ G^{k+2})_{rip, sjq} \end{aligned}$$

As for the right term R, this is given by:

$$\begin{aligned}
< R_{ij}\xi_{pq},\xi_{rs} > &= \sum_b < P_{i_1b_1}\ldots P_{i_lb_l}\xi_{pq},\xi_{rs} > T_{bj}\\
&= \sum_b < \xi_{pq},\xi_{i_lb_l} > \ldots < \xi_{i_1b_1},\xi_{rs} > T_{bj}\\
&= \sum_b G_{pi_l}^{qb_l}G_{i_li_{l-1}}^{b_lb_{l-1}}\ldots G_{i_2i_1}^{b_2b_1}G_{i_1r}^{b_1s}T_{bj}\\
&= \sum_b G_{rip,sbq}^{l+2}T_{bj}\\
&= (G^{l+2}T^\circ)_{rip,sjq}
\end{aligned}$$

Thus, we obtain the formula in the statement. See [17]. □

There is some similarity here with the computations with transfer matrices from statistical mechanics, and we will be back to this.

Let us discuss now the computation of the Haar functional for the quantum permutation group $G\subset S_N^+$ associated to a complex Hadamard matrix $H\in M_N(\mathbb C)$. In the general random matrix model context, we have the following formula for the Haar integration functional of the Hopf image, coming from the work in [22], [143]:

Theorem 14.8. *Given an inner faithful model $\pi:C(G)\to M_N(C(T))$, we have*

$$\int_G=\lim_{k\to\infty}\frac{1}{k}\sum_{r=1}^k\int_G^r$$

with the truncated integrals on the right being given by

$$\int_G^r=(\varphi\circ\pi)^{*r}$$

where $\varphi=tr\otimes\int_T$ is the random matrix trace.

Proof. We must prove that the limit in the statement $\int_G'$ converges, and that we have $\int_G'=\int_G$. It is enough to check this on the coefficients of corepresentations:

$$\left(id\otimes\int_G'\right)v=\left(id\otimes\int_G\right)v$$

We know from section 13 that the matrix on the right is the orthogonal projection onto $Fix(v)$. As for the matrix on the left, this is the orthogonal projection onto the 1-eigenspace of $(id\otimes\varphi\pi)v$. Now observe that, if we set $V_{ij}=\pi(v_{ij})$, we have:

$$(id\otimes\varphi\pi)v=(id\otimes\varphi)V$$

Thus, as in the proof in section 13, we conclude that the 1-eigenspace that we are interested in equals $Fix(V)$. But, according to Theorem 14.6, we have:

$$Fix(V) = Fix(v)$$

Thus, we have proved that we have $\int_G' = \int_G$, as desired. □

In practice now, we are led to the computation of the truncated integrals $\int_G^r$ appearing in the above result, and the formula of these truncated integrals is as follows:

Proposition 14.9. *The truncated integrals in Theorem 14.8, namely*

$$\int_G^r = (\varphi \circ \pi)^{*r}$$

are given by the following formula, in the orthogonal case, where $u = \bar{u}$,

$$\int_G^r u_{a_1 b_1} \ldots u_{a_p b_p} = (T_p^r)_{a_1 \ldots a_p, b_1 \ldots b_p}$$

with the matrix on the right being given by the formula

$$(T_p)_{i_1 \ldots i_p, j_1 \ldots j_p} = \left(tr \otimes \int_T \right) (U_{i_1 j_1} \ldots U_{i_p j_p})$$

where $U_{ij} = \pi(u_{ij})$ are the images of the standard coordinates in the model.

Proof. This is something straightforward, which comes from the definition of the truncated integrals, namely $\int_G^r = (\varphi \circ \pi)^{*r}$, with $\varphi = tr \otimes \int_T$ being the random matrix trace. Let us mention as well that in the general compact quantum group case, where the condition $u = \bar{u}$ does not necessarily hold, an analogue of the above result holds, by adding exponents $e_1, \ldots, e_p \in \{1, *\}$ everywhere. See [15]. □

Regarding now the main character, the result here is as follows:

Theorem 14.10. *In the context of Theorem 14.8, let μ^r be the law of the main character $\chi = Tr(u)$ with respect to the truncated integration $\int_G^r = (\varphi \circ \pi)^{*r}$.*

(1) *The law of the main character is given by the following formula:*

$$\mu = \lim_{k \to \infty} \frac{1}{k} \sum_{r=0}^{k} \mu^r$$

(2) *The moments of the truncated measure μ^r are the following numbers:*

$$c_p^r = Tr(T_p^r)$$

Proof. These results are both elementary, the proof being as follows:

(1) This follows from the general limiting formula in Theorem 14.8.

(2) This follows from the formula in Proposition 14.9, by summing over $a_i = b_i$. □

In connection with the complex Hadamard matrices, we can use the above technology in order to compute the law of the main character, and also to discuss the behavior of the construction $H \to G$ with respect to the operations $H \to H^t, \bar{H}, H^*$.

Following [15], let us first introduce the following abstract duality:

Definition 14.11. *Let $\pi : C(G) \to M_N(\mathbb{C})$ be inner faithful, mapping $u_{ij} \to U_{ij}$.*

(1) *We set $(U'_{kl})_{ij} = (U_{ij})_{kl}$, and define a model as follows:*
$$\widetilde{\rho} : C(U_N^+) \to M_N(\mathbb{C})$$
$$v_{kl} \to U'_{kl}$$

(2) *We perform the Hopf image construction, as to get a model as follows:*
$$\rho : C(G') \to M_N(\mathbb{C})$$

In this definition U_N^+ is Wang's quantum unitary group, whose standard coordinates are subject to the biunitarity condition $u^* = u^{-1}, u^t = \bar{u}^{-1}$. Observe that the matrix U' constructed in (1) is given by $U' = \Sigma U$, where Σ is the flip. Thus this matrix is indeed biunitary, and produces a representation ρ as in (1), and then a factorization as in (2). The operation $A \to A'$ is a duality, in the sense that we have $A'' = A$, and in the Hadamard matrix case, this comes from the operation $H \to H^t$. See [15].

We denote by D the dilation operation for probability measures, or for general $*$-distributions, given by the formula $D_r(law(X)) = law(rX)$. We have then:

Theorem 14.12. *Consider the rescaled measure $\eta^r = D_{1/N}(\mu^r)$.*

(1) *The moments $\gamma_p^r = c_p^r/N^p$ of η^r satisfy the following formula:*
$$\gamma_p^r(G) = \gamma_r^p(G')$$

(2) *η^r has the same moments as the following matrix:*
$$T'_r = T_r(G')$$

(3) *In the orthogonal case, where $u = \bar{u}$, we have:*
$$\eta^r = law(T'_r)$$

Proof. All the results follow from Theorem 14.10, as follows:

(1) We have the following computation:
$$\begin{aligned} c_p^r(A) &= \sum_i (T_p)_{i_1^1\ldots i_p^1, i_1^2\ldots i_p^2} \ldots\ldots (T_p)_{i_1^r\ldots i_p^r, i_1^1\ldots i_p^1} \\ &= \sum_i tr(U_{i_1^1 i_1^2} \ldots U_{i_p^1 i_p^2}) \ldots\ldots tr(U_{i_1^r i_1^1} \ldots U_{i_p^r i_p^1}) \\ &= \frac{1}{N^r} \sum_i \sum_j (U_{i_1^1 i_1^2})_{j_1^1 j_2^1} \ldots (U_{i_p^1 i_p^2})_{j_p^1 j_1^1} \ldots\ldots (U_{i_1^r i_1^1})_{j_1^r j_2^r} \ldots (U_{i_p^r i_p^1})_{j_p^r j_1^r} \end{aligned}$$

In terms of the matrix $(U'_{kl})_{ij} = (U_{ij})_{kl}$, then by permuting the terms in the product on the right, and finally with the changes $i_a^b \leftrightarrow i_b^a, j_a^b \leftrightarrow j_b^a$, we obtain:

$$\begin{aligned}
c_p^r(A) &= \frac{1}{N^r}\sum_i\sum_j (U'_{j_1^1j_2^1})_{i_1^1i_1^2}\ldots(U'_{j_p^1j_1^1})_{i_p^1i_p^2}\ldots\ldots(U'_{j_1^rj_2^r})_{i_1^ri_1^1}\ldots(U'_{j_p^rj_1^r})_{i_p^ri_p^1}\\
&= \frac{1}{N^r}\sum_i\sum_j (U'_{j_1^1j_2^1})_{i_1^1i_1^2}\ldots(U'_{j_1^rj_2^r})_{i_1^ri_1^1}\ldots\ldots(U'_{j_p^1j_1^1})_{i_p^1i_p^2}\ldots(U'_{j_p^rj_1^r})_{i_p^ri_p^1}\\
&= \frac{1}{N^r}\sum_i\sum_j (U'_{j_1^1j_1^2})_{i_1^1i_2^1}\ldots(U'_{j_r^1j_r^2})_{i_r^1i_1^1}\ldots\ldots(U'_{j_1^pj_1^1})_{i_1^pi_2^p}\ldots(U'_{j_r^pj_r^1})_{i_r^pi_1^p}
\end{aligned}$$

On the other hand, if we use again the above formula of $c_p^r(A)$, but this time for the matrix U', and with the changes $r \leftrightarrow p$ and $i \leftrightarrow j$, we obtain:

$$c_r^p(A') = \frac{1}{N^p}\sum_i\sum_j (U'_{j_1^1j_1^2})_{i_1^1i_2^1}\ldots(U'_{j_r^1j_r^2})_{i_r^1i_1^1}\ldots\ldots(U'_{j_1^pj_1^1})_{i_1^pi_2^p}\ldots(U'_{j_r^pj_r^1})_{i_r^pi_1^p}$$

Now by comparing this with the previous formula, we obtain:

$$N^r c_p^r(A) = N^p c_r^p(A')$$

Thus we have the following equalities, which give the result:

$$\frac{c_p^r(A)}{N^p} = \frac{c_r^p(A')}{N^r}$$

(2) By using (1) and the formula in Theorem 14.10, we obtain:

$$\begin{aligned}
\frac{c_p^r(A)}{N^p} &= \frac{c_r^p(A')}{N^r}\\
&= \frac{Tr((T_r')^p)}{N^r}\\
&= tr((T_r')^p)
\end{aligned}$$

But this gives the equality of moments in the statement.

(3) This follows from the moment equality in (2), and from the standard fact that for self-adjoint variables, the moments uniquely determine the distribution. □

We will be back to such computations in section 16 below, in the context of some explicit examples of quantum groups associated to Hadamard matrices.

Let us discuss now some potential applications of the construction $H \to G$, and of the Hadamard matrices in general, to certain questions from mathematical physics. In order to start, we will need some basic von Neumann algebra theory, coming as a complement to the basic C^*-algebra theory explained in section 13 above, as follows:

Theorem 14.13. *The von Neumann algebras, which are the $*$-algebras $A \subset B(H)$ closed under the weak operator topology, making each $T \to Tx$ continuous, are as follows:*

1. *They are exactly the $*$-algebras of operators $A \subset B(H)$ which are equal to their bicommutant, $A = A''$.*
2. *In the commutative case, these are the algebras of type $A = L^\infty(X)$, with X measured space, represented on $H = L^2(X)$, up to a multiplicity.*
3. *If we write the center as $Z(A) = L^\infty(X)$, then we have a decomposition of type $A = \int_X A_x\,dx$, with the fibers A_x having trivial center, $Z(A_x) = \mathbb{C}$.*
4. *The factors, $Z(A) = \mathbb{C}$, can be fully classified in terms of II_1 factors, which are those satisfying $\dim A = \infty$, and having a faithful trace $tr : A \to \mathbb{C}$.*
5. *The II_1 factors enjoy the "continuous dimension geometry" property, in the sense that the traces of their projections can take any values in $[0, 1]$.*
6. *Among the II_1 factors, the most important one is the Murray-von Neumann hyperfinite factor R, obtained as an inductive limit of matrix algebras.*

Proof. This is something quite heavy, the idea being as follows:

(1) This is von Neumann's bicommutant theorem, which is well-known in finite dimensions, and whose proof in general is not that complicated, either.

(2) It is clear, via basic measure theory, that $L^\infty(X)$ is indeed a von Neumann algebra on $H = L^2(X)$. The converse can be proved as well, by using spectral theory.

(3) This is von Neumann's reduction theory main result, whose statement is already quite hard to understand, and whose proof uses advanced functional analysis.

(4) This is something heavy, due to Murray-von Neumann and Connes, the idea being that the other factors can be basically obtained via crossed product constructions.

(5) This is a gem of functional analysis, with the rational traces being relatively easy to obtain, and with the irrational ones coming from limiting arguments.

(6) Once again, heavy results, due to Murray-von Neumann and Connes, the idea being that any finite dimensional construction always leads to the same factor, called R. $\square$

In relation now with our questions, variations of von Neumann's reduction theory idea, basically using the abelian subalgebra $Z(A) \subset A$, include the use of maximal abelian subalgebras $B \subset A$, called MASA. In the finite von Neumann algebra case, where we have a trace, the use of orthogonal MASA is a standard method as well:

Definition 14.14. *A pair of orthogonal MASA is a pair of maximal abelian subalgebras*

$$B, C \subset A$$

which are orthogonal with respect to the trace, in the sense that we have:

$$(B \ominus \mathbb{C}1) \perp (C \ominus \mathbb{C}1)$$

Here the scalar product is by definition $< b,c >= tr(bc^*)$, and by taking into account the multiples of the identity, the orthogonality condition reformulates as follows:

$$tr(bc) = tr(b)tr(c)$$

This notion is potentially useful in the infinite dimensional context, in relation with various structure and classification problems for the II_1 factors.

However, as a "toy example", we can try and see what happens for the simplest factor that we know, namely the matrix algebra $M_N(\mathbb{C})$, endowed with its usual matrix trace. In this context, we have the following surprising observation of Popa [113]:

Theorem 14.15. *Up to a conjugation by a unitary, the pairs of orthogonal MASA in the simplest factor, namely the matrix algebra $M_N(\mathbb{C})$, are as follows,*

$$A = \Delta$$

$$B = H\Delta H^*$$

with $\Delta \subset M_N(\mathbb{C})$ being the diagonal matrices, and with $H \in M_N(\mathbb{C})$ being Hadamard.

Proof. Any MASA in $M_N(\mathbb{C})$ being conjugated to Δ, we can assume, up to conjugation by a unitary, that we have, with $U \in U_N$:

$$A = \Delta$$

$$B = U\Delta U^*$$

Now observe that given two diagonal matrices $D, E \in \Delta$, we have:

$$\begin{aligned} tr(D \cdot UEU^*) &= \frac{1}{N}\sum_i (DUEU^*)_{ii} \\ &= \frac{1}{N}\sum_{ij} D_{ii}U_{ij}E_{jj}\bar{U}_{ij} \\ &= \frac{1}{N}\sum_{ij} D_{ii}E_{jj}|U_{ij}|^2 \end{aligned}$$

Thus, the orthogonality condition $A \perp B$ reformulates as follows:

$$\frac{1}{N}\sum_{ij} D_{ii}E_{jj}|U_{ij}|^2 = \frac{1}{N^2}\sum_{ij} D_{ii}E_{jj}$$

But this tells us precisely that the entries $|U_{ij}|$ must have the same absolute value:

$$|U_{ij}| = \frac{1}{\sqrt{N}}$$

Thus the rescaled matrix $H = \sqrt{N}U$ must be Hadamard. □

Along the same lines, but at a more advanced level, we have the following result:

Theorem 14.16. *Given a complex Hadamard matrix $H\in M_N(\mathbb C)$, the diagram formed by the associated pair of orthogonal MASA, namely*

$$\begin{array}{ccc}\Delta&\longrightarrow&M_N(\mathbb C)\\ \uparrow&&\uparrow\\ \mathbb C&\longrightarrow&H\Delta H^*\end{array}$$

is a commuting square in the sense of subfactor theory, in the sense that the expectations onto $\Delta,H\Delta H^*$ commute, and their product is the expectation onto $\mathbb C$.

Proof. It follows from definitions that the expectation $E_\Delta:M_N(\mathbb C)\to\Delta$ is the operation which consists in keeping the diagonal, and erasing the rest:

$$M\to M_\Delta$$

Consider now the other expectation, namely:

$$E_{H\Delta H^*}:M_N(\mathbb C)\to H\Delta H^*$$

It is better to identify this with the following expectation, with $U=H/\sqrt N$:

$$E_{U\Delta U^*}:M_N(\mathbb C)\to U\Delta U^*$$

This latter expectation must be given by a formula of type $M\to UX_\Delta U^*$, with X satisfying:

$$<M,UDU^*>=<UX_\Delta U^*,UDU^*>\quad,\quad\forall D\in\Delta$$

The scalar products being given by $<a,b>=tr(ab^*)$, this condition reads:

$$tr(MUD^*U^*)=tr(X_\Delta D^*)\quad,\quad\forall D\in\Delta$$

Thus $X=U^*MU$, and the formulae of our two expectations are as follows:

$$\begin{aligned}E_\Delta(M)&=M_\Delta\\ E_{U\Delta U^*}(M)&=U(U^*MU)_\Delta U^*\end{aligned}$$

With these formulae in hand, we have the following computation:

$$\begin{aligned}(E_\Delta E_{U\Delta U^*}M)_{ij}&=\delta_{ij}(U(U^*MU)_\Delta U^*)_{ii}\\ &=\delta_{ij}\sum_kU_{ik}(U^*MU)_{kk}\bar U_{ik}\\ &=\delta_{ij}\sum_k\frac{1}{N}\cdot(U^*MU)_{kk}\\ &=\delta_{ij}tr(U^*MU)\\ &=\delta_{ij}tr(M)\\ &=(E_{\mathbb C}M)_{ij}\end{aligned}$$

As for the other composition, the computation here is similar, as follows:

$$\begin{aligned}(E_{U\Delta U^*}E_\Delta M)_{ij} &= (U(U^*M_\Delta U)_\Delta U^*)_{ij}\\ &= \sum_k U_{ik}(U^*M_\Delta U)_{kk}\bar{U}_{jk}\\ &= \sum_{kl} U_{ik}\bar{U}_{lk}M_{ll}U_{lk}\bar{U}_{jk}\\ &= \frac{1}{N}\sum_{kl} U_{ik}M_{ll}\bar{U}_{jk}\\ &= \delta_{ij}tr(M)\\ &= (E_{\mathbb{C}}M)_{ij}\end{aligned}$$

Thus, we have indeed a commuting square, as claimed. □

As a conclusion, all this leads us into commuting squares and subfactor theory. So, let us explain now the basic theory here. As a first object, which will be central in what follows, we have the Temperley-Lieb algebra [135], constructed as follows:

Definition 14.17. *The Temperley-Lieb algebra of index $N \in [1,\infty)$ is defined as*

$$TL_N(k) = span(NC_2(k,k))$$

with product given by vertical concatenation, with the rule

$$\bigcirc = N$$

for the closed circles that might appear when concatenating.

In other words, the algebra $TL_N(k)$, depending on parameters $k \in \mathbb{N}$ and $N \in [1,\infty)$, is the formal linear span of the pairings $\pi \in NC_2(k,k)$. The product operation is obtained by linearity, for the pairings which span $TL_N(k)$ this being the usual vertical concatenation, with the conventions that things go "from top to bottom", and that each floating circle that might appear when concatenating is replaced by a scalar factor, equal to N.

Observe that there is a connection here with S_N^+, and more specifically with the category of noncrossing partitions NC producing S_N^+, due to the following fact:

Proposition 14.18. *We have bijections $NC(k) \simeq NC_2(2k) \simeq NC_2(k,k)$, constructed by fattening/shrinking and rotating/flattening, as follows:*

1. *The application $NC(k) \to NC_2(2k)$ is the "fattening" one, obtained by doubling all the legs, and doubling all the strings as well.*
2. *Its inverse $NC_2(2k) \to NC(k)$ is the "shrinking" application, obtained by collapsing pairs of consecutive neighbors.*
3. *The bijection $NC_2(2k) \simeq NC_2(k,k)$ is obtained by rotating and flattening the noncrossing pairings, in the obvious way.*

Proof. The fact that the two operations in (1,2) are indeed inverse to each other is clear, by computing the corresponding two compositions, with the remark that the construction of the fattening operation requires the partitions to be noncrossing. □

Following now Jones [78], consider an inclusion of II_1 factors, which is actually something quite natural in quantum physics:

$$A_0\subset A_1$$

We can consider the orthogonal projection $e_1:A_1\to A_0$, and set:

$$A_2=<A_1,e_1>$$

This procedure, called "basic construction", can be iterated, and we obtain in this way a whole tower of II_1 factors, as follows:

$$A_0\subset_{e_1}A_1\subset_{e_2}A_2\subset_{e_3}A_3\subset\ldots\ldots$$

The basic construction is something quite subtle, making deep connections with advanced mathematics and physics. All this was discovered by Jones, and his main result from [78], which came as a big surprise at that time, along with some supplementary fundamental work, done later, in [79], can be summarized as follows:

Theorem 14.19. *Let $A_0\subset A_1$ be an inclusion of II_1 factors.*

(1) *The sequence of projections $e_1,e_2,e_3,\ldots\in B(H)$ produces a representation of the Temperley-Lieb algebra $TL_N\subset B(H)$, where $N=[A_1,A_0]$.*
(2) *The collection $P=(P_k)$ of the linear spaces $P_k=A_0'\cap A_k$, which contains the image of TL_N, has a planar algebra structure.*
(3) *The index $N=[A_1,A_0]$, which is a Murray-von Neumann continuous quantity $N\in[1,\infty]$, must satisfy $N\in\{4\cos^2(\frac{\pi}{n})|n\in\mathbb N\}\cup[4,\infty]$.*

Proof. This is something quite heavy, the idea being as follows:

(1) The idea here is that the functional analytic study of the basic construction leads to the conclusion that the sequence of projections $e_1,e_2,e_3,\ldots\in B(H)$ behaves algebrically exactly as the rescaled sequence of diagrams $\varepsilon_1,\varepsilon_2,\varepsilon_3,\ldots\in TL_N$ given by $\varepsilon_1=\,^{\cup}_{\cap}$, $\varepsilon_2=|^{\cup}_{\cap}$, $\varepsilon_3=||^{\cup}_{\cap}$, and so on, with the parameter being the index, $N=[A_2,A_1]$.

(2) Since the orthogonal projection $e_1:A_1\to A_0$ commutes with A_0 we have $e_1\in P_2'$, and by translation we obtain $e_1,\ldots,e_{k-1}\in P_k$ for any k, and so $TL_N\subset P$. The point now is that the planar algebra structure of TL_N, obtained by composing diagrams, can be shown to extend into an abstract planar algebra structure of P.

(3) This is something quite surprising, which follows from (1), via some clever positivity considerations, involving the Perron-Frobenius theorem. In fact, the subfactors having index $N\in[1,4]$ can be classified by ADE diagrams, and the obstruction $N=4\cos^2(\frac{\pi}{n})$ itself comes from the fact that N must be the squared norm of such a graph. □

As before with other preliminary material, the above was quite quick. We recommend here Jones' papers [78], [79], which are a must-read, when doing Hadamard matrices.

Getting back now to the commuting squares, the idea is that any such square C produces a subfactor of the hyperfinite II_1 factor R. Indeed, under suitable assumptions on the inclusions $C_{00}\subset C_{10}, C_{01}\subset C_{11}$, we can perform the basic construction for them, in finite dimensions, and we obtain a whole array of commuting squares, as follows:

$$\begin{tikzcd}
A_0 & A_1 & A_2 & \\
C_{02} \arrow[r] \arrow[u, dotted] & C_{12} \arrow[r] \arrow[u, dotted] & C_{22} \arrow[r, dotted] \arrow[u, dotted] & B_2 \\
C_{01} \arrow[r] \arrow[u] & C_{11} \arrow[r] \arrow[u] & C_{21} \arrow[r, dotted] \arrow[u] & B_1 \\
C_{00} \arrow[r] \arrow[u] & C_{10} \arrow[r] \arrow[u] & C_{20} \arrow[r, dotted] \arrow[u] & B_0
\end{tikzcd}$$

Here the various A,B letters stand for the von Neumann algebras obtained in the limit, which are all isomorphic to the hyperfinite II_1 factor R, and we have:

Theorem 14.20. *In the context of the above diagram, the following happen:*

(1) *$A_0\subset A_1$ is a subfactor, and $\{A_i\}$ is the Jones tower for it.*
(2) *The corresponding planar algebra is given by $A_0'\cap A_k=C_{01}'\cap C_{k0}$.*
(3) *A similar result holds for the "horizontal" subfactor $B_0\subset B_1$.*

Proof. This is something standard, the idea being as follows:

(1) This is something quite routine.

(2) This is a subtle result, called Ocneanu compactness theorem [108].

(3) This follows from (1,2), by flipping the diagram. □

Getting back now to the Hadamard matrices, we can extend our lineup of results, namely Theorem 14.15 and Theorem 14.16, with an advanced statement, as follows:

Theorem 14.21. *Given a complex Hadamard matrix $H\in M_N(\mathbb C)$, the diagram formed by the associated pair of orthogonal MASA, namely*

$$\begin{array}{ccc}\Delta & \longrightarrow & M_N(\mathbb C)\\ \uparrow & & \uparrow\\ \mathbb C & \longrightarrow & H\Delta H^*\end{array}$$

is a commuting square in the sense of subfactor theory, and the associated planar algebra $P=(P_k)$ is given by the following formula, in terms of H itself,

$$T\in P_k\iff T^\circ G^2=G^{k+2}T^\circ$$

where the objects on the right are constructed as follows:

1. $T^\circ=id\otimes T\otimes id$.
2. $G_{ia}^{jb}=\sum_k H_{ik}\bar{H}_{jk}\bar{H}_{ak}H_{bk}$.
3. $G^k_{i_1\ldots i_k,j_1\ldots j_k}=G^{j_kj_{k-1}}_{i_ki_{k-1}}\ldots G^{j_2j_1}_{i_2i_1}$.

Proof. The fact that we have indeed a commuting square is from Theorem 14.16, and the computation of the associated planar algebra is possible thanks to formula in Theorem 14.20 (2). By doing some computations, which are quite similar to those in the proof of Theorem 14.7 above, we obtain the formula in the statement. See [81]. □

Now by comparing with Theorem 14.7, we are led to the following result:

Theorem 14.22. *Let $H\in M_N(\mathbb C)$ be a complex Hadamard matrix.*

1. *The planar algebra associated to H is given by $P_k=Fix(u^{\otimes k})$, where $G\subset S_N^+$ is the associated quantum permutation group.*
2. *The corresponding Poincaré series $f(z)=\sum_k\dim(P_k)z^k$ equals the Stieltjes transform $\int_G\frac{1}{1-z\chi}$ of the law of the main character $\chi=\sum_i u_{ii}$.*

Proof. This follows by comparing the quantum group and subfactor results:

(1) As already mentioned above, this simply follows by comparing Theorem 14.7 with the subfactor computation in Theorem 14.21. For full details here, we refer to [17].

(2) This is a consequence of (1), and of the Peter-Weyl type results from [149], which tell us that fixed points can be counted by integrating characters. □

Summarizing, we have now a clarification of the various quantum algebraic objects associated to a complex Hadamard matrix $H\in M_N(\mathbb C)$, the idea being that the central object, which best encodes the "symmetries" of the matrix, and which allows the construction of the other objects as well, is the associated quantum permutation group $G\subset S_N^+$.

Regarding now the subfactor itself, the result here is as follows:

Theorem 14.23. *The subfactor associated to $H \in M_N(\mathbb{C})$ is of the form*

$$A^G \subset (\mathbb{C}^N \otimes A)^G$$

with $A = R \rtimes \widehat{G}$, where $G \subset S_N^+$ is the associated quantum permutation group.

Proof. This is something more technical, the idea being that the basic construction procedure for the commuting squares, explained before Theorem 14.20, can be performed in an "equivariant setting", for commuting squares having components as follows:

$$D \otimes_G E = (D \otimes (E \rtimes \widehat{G}))^G$$

To be more precise, starting with a commuting square formed by such algebras, we obtain by basic construction a whole array of commuting squares as follows, with $\{D_i\}, \{E_i\}$ being by definition Jones towers, and with D_∞, E_∞ being their inductive limits:

$$\begin{tikzcd}
D_0 \otimes_G E_\infty & D_1 \otimes_G E_\infty & D_2 \otimes_G E_\infty & \\
D_0 \otimes_G E_2 \arrow[r] \arrow[u, dotted] & D_1 \otimes_G E_2 \arrow[r] \arrow[u, dotted] & D_2 \otimes_G E_2 \arrow[r, dotted] \arrow[u, dotted] & D_\infty \otimes_G E_2 \\
D_0 \otimes_G E_1 \arrow[r] \arrow[u] & D_1 \otimes_G E_1 \arrow[r] \arrow[u] & D_2 \otimes_G E_1 \arrow[r, dotted] \arrow[u] & D_\infty \otimes_G E_1 \\
D_0 \otimes_G E_0 \arrow[r] \arrow[u] & D_1 \otimes_G E_0 \arrow[r] \arrow[u] & D_2 \otimes_G E_0 \arrow[r, dotted] \arrow[u] & D_\infty \otimes_G E_0
\end{tikzcd}$$

The point now is that this quantum group picture works in fact for any commuting square having $\mathbb{C}$ in the lower left corner. In the Hadamard matrix case, that we are interested in here, the corresponding commuting square is as follows:

$$\begin{tikzcd}
\mathbb{C} \otimes_G \mathbb{C}^N \arrow[r] & \mathbb{C}^N \otimes_G \mathbb{C}^N \\
\mathbb{C} \otimes_G \mathbb{C} \arrow[r] \arrow[u] & \mathbb{C}^N \otimes_G \mathbb{C} \arrow[u]
\end{tikzcd}$$

Thus, the subfactor obtained by vertical basic construction appears as follows:

$$\mathbb{C} \otimes_G E_\infty \subset \mathbb{C}^N \otimes_G E_\infty$$

But this gives the conclusion in the statement, with the II_1 factor appearing there being by definition $A = E_\infty \rtimes \widehat{G}$, and with the remark that we have $E_\infty \simeq R$. See [7]. □

All the above is conjecturally related to statistical mechanics. Indeed, the Tannakian category/planar algebra formula from Theorem 14.7/14.21 has many similarities with the transfer matrix computations for the spin models, and this is explained in Jones' paper [81], and known in fact for long before that, from his 1989 paper [79].

However, the precise significance of the Hadamard matrices in statistical mechanics, or in related areas such as knot and link invariants, remains a bit unclear. From a quantum permutation group perspective, the same questions make sense. The idea here, which is old folklore, going back to the 1998 discovery by Wang [142] of the quantum permutation group S_N^+, is that associated to any 2D spin model should be a quantum permutation group $G\subset S_N^+$, which appears by factorizing the flat representation $C(S_N^+)\to M_N(\mathbb C)$ associated to the $N\times N$ matrix of the Boltzmann weights of the model, and whose representation theory computes the partition function of the model.

This is supported on one hand by Jones' theory in [79], [81], via the connecting results presented above, and on the other hand by a number of more recent results, such as those in [24], having similarities with the computations for the Ising and Potts models. However, the whole thing remains not axiomatized, at least for the moment, and in what regards the Hadamard matrices, their precise physical significance remains unclear.

15. Generalizations

We discuss in this section two extensions of the construction $H\to G$ from the previous section, which are both quite interesting. A first idea, from [13], is that of using complex Hadamard matrices with noncommutative entries.

Let A be a C^*-algebra. For most of the applications A will be a commutative algebra, $A=C(X)$ with X being a compact space, or a matrix algebra, $A=M_K(\mathbb C)$ with $K\in\mathbb N$. We will sometimes consider random matrix algebras, $A=M_K(C(X))$, with X being a compact space, and with $K\in\mathbb N$. Two row or column vectors over A, say $a=(a_1,\ldots,a_N)$ and $b=(b_1,\ldots,b_N)$, are called orthogonal when:

$$\sum_i a_ib_i^*=\sum_i a_i^*b_i=0$$

Observe that, by applying the involution, we have as well:

$$\sum_i b_ia_i^*=\sum_i b_i^*a_i=0$$

With this notion in hand, we can formulate:

Definition 15.1. *An Hadamard matrix over A is a square matrix $H\in M_N(A)$ such that:*

1. *All the entries of H are unitaries, $H_{ij}\in U(A)$.*
2. *These entries commute on all rows and all columns of H.*
3. *The rows and columns of H are pairwise orthogonal.*

As a first remark, in the simplest case $A=\mathbb C$ the unitary group is the unit circle in the complex plane, $U(\mathbb C)=\mathbb T$, and we obtain the usual complex Hadamard matrices. In the general commutative case, $A=C(X)$ with X compact space, our Hadamard matrix must be formed of "fibers", one for each point $x\in X$. Therefore, we obtain:

Proposition 15.2. *The Hadamard matrices $H\in M_N(A)$ over a commutative algebra $A=C(X)$ are exactly the families of complex Hadamard matrices of type*

$$H=\{H^x|x\in X\}$$

with H^x depending continuously on the parameter $x\in X$.

Proof. This follows indeed by combining the above two observations. Observe that, when we wrote $A=C(X)$ in the above statement, we used the Gelfand theorem. □

Let us comment now on the above axioms. For $U,V\in U(A)$ the commutation relation $UV=VU$ implies as well the following commutation relations:

$$UV^*=V^*U\quad,\quad U^*V=VU^*\quad,\quad U^*V^*=U^*V^*$$

Thus the axiom (2) tells us that the C^*-algebras $R_1,\ldots,R_N$ and $C_1,\ldots,C_N$ generated by the rows and the columns of A must be all commutative.

We will be particulary interested in the following type of matrices:

Definition 15.3. *An Hadamard matrix $H \in M_N(A)$ is called "non-classical" if the C^*-algebra generated by its coefficients is not commutative.*

Let us comment now on the axiom (3). According to our definition of orthogonality there are 4 sets of relations to be satisfied, namely for any $i \neq k$ we must have:

$$\sum_j H_{ij}H_{kj}^* = \sum_j H_{ij}^*H_{kj} = \sum_j H_{ji}H_{jk}^* = \sum_j H_{ji}^*H_{jk} = 0$$

Now since by axiom (1) all the entries H_{ij} are known to be unitaries, we can replace this formula by the following more general equation, valid for any i, k:

$$\sum_j H_{ij}H_{kj}^* = \sum_j H_{ij}^*H_{kj} = \sum_j H_{ji}H_{jk}^* = \sum_j H_{ji}^*H_{jk} = N\delta_{ik}$$

The point now is that everything simplifies in terms of the matrices:

$$H = (H_{ij}) \quad , \quad H^* = (H_{ji}^*) \quad , \quad H^t = (H_{ji}) \quad , \quad \bar{H} = (H_{ij}^*)$$

Indeed, the above equations simply read:

$$HH^* = H^*H = H^t\bar{H} = \bar{H}H^t = N1_N$$

So, let us recall now that a square matrix $H \in M_N(A)$ is called "biunitary" if both H and H^t are unitaries. In the particular case where A is commutative, $A = C(X)$, we have "H unitary $\implies$ H^t unitary", so in this case biunitary means of course unitary. In terms of this notion, we have the following reformulation of Definition 15.1:

Proposition 15.4. *Assume that $H \in M_N(A)$ has unitary entries, which commute on all rows and all columns of H. Then the following are equivalent:*

1. *H is Hadamard.*
2. *$H/\sqrt{N}$ is biunitary.*
3. *$HH^* = H^t\bar{H} = N1_N$.*

Proof. We know that (1) happens if and only if the axiom (3) in Definition 15.1 is satisfied, and by the above discussion, this axiom (3) is equivalent to (2). Regarding now the equivalence with (3), this follows from the commutation axiom (2) in Definition 15.1. □

Observe that if $H = (H_{ij})$ is Hadamard, so are $\bar{H} = (H_{ij}^*)$, $H^t = (H_{ji})$, $H^* = (H_{ji}^*)$. In addition, we have the following result:

Proposition 15.5. *The class of Hadamard matrices $H \in M_N(A)$ is stable under:*

1. *Permuting the rows or columns.*
2. *Multiplying the rows or columns by central unitaries.*

When successively combining these two operations, we obtain an equivalence relation on the class of Hadamard matrices $H \in M_N(A)$.

Proof. This is clear from definitions. Observe that in the commutative case $A = C(X)$ any unitary is central, so we can multiply the rows or columns by any unitary. In particular in this case we can always "dephase" the matrix, i.e. assume that its first row and column consist of 1 entries. Note that this operation is not allowed in the general case. $\square$

Let us discuss now the tensor product operation:

Proposition 15.6. *Let $H \in M_N(A)$ and $K \in M_M(A)$ be Hadamard matrices, and assume that $< H_{ij} >$ commutes with $< K_{ab} >$. Then the "tensor product"*

$$H \otimes K \in M_{NM}(A)$$

given by $(H \otimes K)_{ia,jb} = H_{ij}K_{ab}$, is an Hadamard matrix.

Proof. This follows from definitions, and is as well a consequence of the more general Theorem 15.7 below, that will be proved with full details. $\square$

Following [62], the deformed tensor products are constructed as follows:

Theorem 15.7. *Let $H \in M_N(A)$ and $K \in M_M(A)$ be Hadamard matrices, and $Q \in M_{N\times M}(U_A)$. Then the "deformed tensor product" $H \otimes_Q K \in M_{NM}(A)$, given by*

$$(H \otimes_Q K)_{ia,jb} = Q_{ib}H_{ij}K_{ab}$$

is an Hadamard matrix as well, provided that the entries of Q commute on rows and columns, and that the algebras $< H_{ij} >$, $< K_{ab} >$, $< Q_{ib} >$ pairwise commute.

Proof. First, the entries of $L = H \otimes_Q K$ are unitaries, and its rows are orthogonal:

$$\begin{aligned}
\sum_{jb} L_{ia,jb}L^*_{kc,jb} &= \sum_{jb} Q_{ib}H_{ij}K_{ab} \cdot Q^*_{kb}K^*_{cb}H^*_{kj}\\
&= N\delta_{ik}\sum_b Q_{ib}K_{ab} \cdot Q^*_{kb}K^*_{cb}\\
&= N\delta_{ik}\sum_j K_{ab}K^*_{cb}\\
&= NM \cdot \delta_{ik}\delta_{ac}
\end{aligned}$$

The orthogonality of columns can be checked as follows:

$$\begin{aligned}
\sum_{ia} L_{ia,jb}L^*_{ia,kc} &= \sum_{ia} Q_{ib}H_{ij}K_{ab} \cdot Q^*_{ic}K^*_{ac}H^*_{ik}\\
&= M\delta_{bc}\sum_i Q_{ib}H_{ij} \cdot Q^*_{ic}H^*_{ik}\\
&= M\delta_{bc}\sum_i H_{ij}H^*_{ik}\\
&= NM \cdot \delta_{jk}\delta_{bc}
\end{aligned}$$

For the commutation on rows we use in addition the commutation on rows for Q:

$$\begin{aligned}
L_{ia,jb}L_{kc,jb} &= Q_{ib}H_{ij}K_{ab}\cdot Q_{kb}H_{kj}K_{cb}\\
&= Q_{ib}Q_{kb}\cdot H_{ij}H_{kj}\cdot K_{ab}K_{cb}\\
&= Q_{kb}Q_{ib}\cdot H_{kj}H_{ij}\cdot K_{cb}K_{ab}\\
&= Q_{kb}H_{kj}K_{cb}\cdot Q_{ib}H_{ij}K_{ab}\\
&= L_{kc,jb}L_{ia,jb}
\end{aligned}$$

The commutation on columns is similar, using the commutation on columns for Q:

$$\begin{aligned}
L_{ia,jb}L_{ia,kc} &= Q_{ib}H_{ij}K_{ab}\cdot q_{ic}H_{ik}K_{ac}\\
&= Q_{ib}Q_{ic}\cdot H_{ij}H_{ik}\cdot K_{ab}K_{ac}\\
&= Q_{ic}Q_{ib}\cdot H_{ik}H_{ij}\cdot K_{ac}K_{ab}\\
&= Q_{ic}H_{ik}K_{ac}\cdot Q_{ib}H_{ij}K_{ab}\\
&= L_{ia,kc}L_{ia,jb}
\end{aligned}$$

Thus all the axioms are satisfied, and L is indeed Hadamard. $\square$

As a basic example, we have the following construction:

Proposition 15.8. *The following matrix is Hadamard,*

$$M=\begin{pmatrix}x&y&x&y\\x&-y&x&-y\\z&t&-z&-t\\z&-t&-z&t\end{pmatrix}$$

for any unitaries x,y,z,t satisfying $[x,y]=[x,z]=[y,t]=[z,t]=0$.

Proof. This follows indeed from Theorem 15.7, because we have:

$$\begin{pmatrix}1&1\\1&-1\end{pmatrix}\otimes_{\begin{pmatrix}x&y\\z&t\end{pmatrix}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}=\begin{pmatrix}x&y&x&y\\x&-y&x&-y\\z&t&-z&-t\\z&-t&-z&t\end{pmatrix}$$

In addition, the commutation relations in Theorem 15.7 are satisfied indeed. $\square$

The usual complex Hadamard matrices were classified in [69] at $N=2,3,4,5$. In this section we investigate the case of the general Hadamard matrices. We use the equivalence relation constructed in Proposition 15.5 above. We first have:

Proposition 15.9. *The 2×2 Hadamard matrices are all classical, and are all equivalent to the Fourier matrix F_2.*

Proof. Consider indeed an arbitrary 2×2 Hadamard matrix:

$$H = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

We already know that A, D each commute with B, C. Also, we have:

$$AB^* + CD^* = 0$$

We deduce that $A = -CD^*B$ commutes with D, and that $C = -AB^*D$ commutes with B. Thus our matrix is classical, any since all unitaries are now central, we can dephase our matrix, which follows therefore to be the Fourier matrix F_2. $\square$

Let us discuss now the case $N = 3$. Here the classification in the classical case uses the key fact that any formula of type $a + b + c = 0$, with $|a| = |b| = |c| = 1$, must be, up to a permutation of terms, a "trivial" formula of type $a + ja + j^2a = 0$, with $j = e^{2\pi i/3}$. Here is the noncommutative analogue of this simple fact:

Proposition 15.10. *Assume that $a + b + c = 0$ is a vanishing sum of unitaries. Then this sum must be of type*

$$a + wa + w^2a = 0$$

with w unitary satisfying $1 + w + w^2 = 0$.

Proof. Since $-c = a + b$ is unitary we have $(a + b)(a + b)^* = 1$. Thus $ab^* + ba^* = -1$, and so $ab^*ba^* + (ba^*)^2 = -ba^*$. With $w = ba^*$ we obtain $1 + w^2 = -w$, and we are done. $\square$

With this result in hand, we can start the $N = 3$ classification. We first have the following technical result, that we will improve later on:

Proposition 15.11. *Any 3×3 Hadamard matrix must be of the form*

$$H = \begin{pmatrix} a & b & c \\ ua & uv^*w^2vb & uv^*wvc \\ va & wvb & w^2vc \end{pmatrix}$$

with w being subject to the equation $1 + w + w^2 = 0$.

Proof. Consider an arbitrary Hadamard matrix $H \in M_3(A)$. We define a, b, c, u, v, w as for that part of the matrix to be exactly as in the statement, as follows:

$$H = \begin{pmatrix} a & b & c \\ ua & x & y \\ va & wvb & z \end{pmatrix}$$

Let us look first at the scalar product between the first and third row:

$$vaa^* + wvbb^* + zc^* = 0$$

By simplifying we obtain $v + wv + zc^* = 0$, and by using Proposition 15.10 we conclude that we have $1 + w + w^2 = 0$, and that $zc^* = w^2v$, and so $z = w^2vc$, as claimed.

The scalar products of the first column with the second and third ones are:

$$a^*b + a^*u^*x + a^*v^*wvb = 0$$

$$a^*c + a^*u^*y + a^*v^*w^2vc = 0$$

By multiplying to the left by va, and to the right by b^*v^* and c^*v^*, we obtain:

$$1 + vu^*xb^*v^* + w = 0$$

$$1 + vu^*yc^*v^* + w^2 = 0$$

Now by using Proposition 15.10 again, we obtain $vu^*xb^*v^* = w^2$ and $vu^*yc^*v^* = w$, and so $x = uv^*w^2vb$ and $y = uv^*wvc$, and we are done. $\square$

We can already deduce now a first classification result, as follows:

Proposition 15.12. *There is no Hadamard matrix $H \in M_3(A)$ with self-adjoint entries.*

Proof. We use Proposition 15.11. Since the entries are idempotents, we have:

$$a^2 = b^2 = c^2 = u^2 = v^2 = (uw)^2 = (vw)^2 = 1$$

It follows that our matrix is in fact of the following form:

$$H = \begin{pmatrix} a & b & c \\ ua & uwb & uw^2c \\ va & wvb & w^2vc \end{pmatrix}$$

The commutation between H_{22}, H_{23} reads:

$$\begin{aligned} [uwb, wvb] = 0 &\implies [uw, wv] = 0 \\ &\implies uwwv = wvuw \\ &\implies uvw = vuw^2 \\ &\implies w = 1 \end{aligned}$$

Thus we have reached to a contradiction, and we are done. $\square$

Let us go back now to the general case. We have the following technical result, which refines Proposition 15.11 above, and which will be in turn further refined, later on:

Proposition 15.13. *Any 3×3 Hadamard matrix must be of the form*

$$H = \begin{pmatrix} a & b & c \\ ua & w^2ub & wuc \\ va & wvb & w^2vc \end{pmatrix}$$

where (a, b, c) and (u, v, w) are triples of commuting unitaries, and:

$$1 + w + w^2 = 0$$

Proof. We use Proposition 15.11. With $e = uv^*$, the matrix there becomes:

$$H = \begin{pmatrix} a & b & c \\ eva & ew^2vb & ewvc \\ va & wvb & w^2vc \end{pmatrix}$$

The commutation relation between H_{22}, H_{32} reads:

$$\begin{aligned} [ew^2vb, wvb] = 0 &\implies [ew^2v, wv] = 0 \\ &\implies ew^2vwv = wvew^2v \\ &\implies ew^2v = wvew \\ &\implies [ew, wv] = 0 \end{aligned}$$

Similarly, the commutation between H_{23}, H_{33} reads:

$$\begin{aligned} [ewvc, w^2vc] = 0 &\implies [ewv, w^2v] = 0 \\ &\implies ewvw^2v = w^2vewv \\ &\implies ewv = w^2vew^2 \\ &\implies [ew^2, w^2v] = 0 \end{aligned}$$

We can rewrite this latter relation by using the formula $w^2 = -1 - w$, and then, by further processing it by using the first relation, we obtain:

$$\begin{aligned} [e(1+w), (1+w)v] = 0 &\implies [e, wv] + [ew, v] = 0 \\ &\implies 2ewv - wve - vew = 0 \\ &\implies ewv = \frac{1}{2}(wve + vew) \end{aligned}$$

We use now the key fact that when an average of two unitaries is unitary, then the three unitaries involved are in fact all equal. This gives:

$$ewv = wve = vew$$

Thus we obtain $[w, e] = [w, v] = 0$, so w, e, v commute. Our matrix becomes:

$$H = \begin{pmatrix} a & b & c \\ eva & w^2evb & wevc \\ va & wvb & w^2vc \end{pmatrix}$$

Now by remembering that $u = ev$, this gives the formula in the statement. $\square$

We can now formulate our main classification result, as follows:

Theorem 15.14. *The 3×3 Hadamard matrices are all classical, and are all equivalent to the Fourier matrix F_3.*

Proof. We know from Proposition 15.13 that we can write our matrix in the following way, where (a,b,c) and (u,v,w) pairwise commute, and where $1+w+w^2=0$:

$$H=\begin{pmatrix}a&b&c\\ au&buw&cuw^*\\ av&bvw^*&cvw\end{pmatrix}$$

We also know that (a,u,v), (b,uw,vw^*), (c,uw^*,vw) and (ab,ac,bc,w) have entries which pairwise commute. We first show that uv is central. Indeed, we have:

$$\begin{aligned}buv&=buvww^*\\ &=b(uw)(vw^*)\\ &=(uw)(vw^*)b\\ &=uvb\end{aligned}$$

Similarly, $cuv=uvc$. It follows that we may in fact suppose that uv is a scalar. But since our relations are homogeneous, we may assume in fact that $u=v^*$.

Let us now show that $[abc,vw^*]=0$. Indeed, we have:

$$\begin{aligned}abc&=a(bc)ww^*\\ &=aw(bc)w^*\\ &=av(wv^*)bcw^*\\ &=avb(wv^*)cw^*\\ &=v(ab)wv^*cw^*\\ &=vw(ab)v^*cw^*\\ &=vw(ab)w(w^*v^*)cw^*\\ &=vw^2(ab)c(w^*v^*)w^*\\ &=vw^*abcv^*w\end{aligned}$$

We know also that $[b,vw^*]=0$. Hence $[ac,vw^*]=0$. But $[ac,w^*]=0$. Hence $[ac,v]=0$. But $[a,v]=0$. Hence $[c,v]=0$. But $[c,vw]=0$. So $[c,w]=0$. But $[bc,w]=0$. So $[b,w]=0$. But $[b,v^*w]=0$ and $[ab,w]=0$, so respectively $[b,v]=0$ and $[a,w]=0$. Thus all operators a,b,c,v,w pairwise commute, and we are done. $\square$

At $N=4$ now, the classical theory uses the fact that an equation of type $a+b+c+d=0$ with $|a|=|b|=|c|=|d|=1$ must be, up to a permutation of the terms, a "trivial" equation of the form $a-a+b-b=0$. In our setting, however, we have for instance:

$$\begin{pmatrix}a&0\\0&x\end{pmatrix}+\begin{pmatrix}-a&0\\0&y\end{pmatrix}+\begin{pmatrix}b&0\\0&-x\end{pmatrix}+\begin{pmatrix}-b&0\\0&-y\end{pmatrix}=0$$

It is probably possible to further complicate this kind of identity, and this makes the $N=4$ classification a quite difficult task.

The generalized Hadamard matrices produce quantum groups, as follows:

Theorem 15.15. *If $H \in M_N(A)$ is Hadamard, the following matrices $P_{ij} \in M_N(A)$ form altogether a magic matrix $P = (P_{ij})$, over the algebra $M_N(A)$:*

$$(P_{ij})_{ab} = \frac{1}{N} H_{ia} H_{ja}^* H_{jb} H_{ib}^*$$

Thus, we can let $\pi : C(S_N^+) \to M_N(A)$ be the representation associated to P, mapping $u_{ij} \to P_{ij}$, and then factorize this representation as follows,

$$\pi : C(S_N^+) \to C(G) \to M_N(A)$$

with the closed subgroup $G \subset S_N^+$ chosen minimal.

Proof. The magic condition can be checked in three steps, as follows:

(1) Let us first check that each P_{ij} is a projection, i.e. that we have $P_{ij} = P_{ij}^* = P_{ij}^2$. Regarding the first condition, namely $P_{ij} = P_{ij}^*$, this simply follows from:

$$(P_{ij})_{ba}^* = \frac{1}{N} (H_{ib} H_{jb}^* H_{ja} H_{ia}^*)^* = \frac{1}{N} H_{ia} H_{ja}^* H_{jb} H_{ib}^* = (P_{ij})_{ab}$$

As for the second condition, $P_{ij} = P_{ij}^2$, this follows from the fact that all the entries H_{ij} are assumed to be unitaries, i.e. follows from axiom (1) in Definition 15.1:

$$\begin{aligned} (P_{ij}^2)_{ab} &= \sum_c (P_{ij})_{ac} (P_{ij})_{cb} \\ &= \frac{1}{N^2} \sum_c H_{ia} H_{ja}^* H_{jc} H_{ic}^* H_{ic} H_{jc}^* H_{jb} H_{ib}^* \\ &= \frac{1}{N} H_{ia} H_{ja}^* H_{jb} H_{ib}^* \\ &= (P_{ij})_{ab} \end{aligned}$$

(2) Let us check now that fact that the entries of P sum up to 1 on each row. For this purpose we use the equality $H^* H = N 1_N$, coming from the axiom (3), which gives:

$$\begin{aligned} (\sum_j P_{ij})_{ab} &= \frac{1}{N} \sum_j H_{ia} H_{ja}^* H_{jb} H_{ib}^* \\ &= \frac{1}{N} H_{ia} (H^* H)_{ab} H_{ib}^* \\ &= \delta_{ab} H_{ia} H_{ib}^* \\ &= \delta_{ab} \end{aligned}$$

(3) Finally, let us check that the entries of P sum up to 1 on each column. This is the tricky check, because it involves, besides axiom (1) and the formula $H^t \bar{H} = N 1_N$ coming

from axiom (3), the commutation on the columns of H, coming from axiom (2):

$$\begin{aligned}
(\sum_i P_{ij})_{ab} &= \frac{1}{N}\sum_i H_{ia}H_{ja}^*H_{jb}H_{ib}^*\\
&= \frac{1}{N}\sum_i H_{ja}^*H_{ia}H_{ib}^*H_{jb}\\
&= \frac{1}{N}H_{ja}^*(H^t\bar{H})_{ab}H_{jb}\\
&= \delta_{ab}H_{ja}^*H_{jb}\\
&= \delta_{ab}
\end{aligned}$$

Thus P is indeed a magic matrix in the above sense, and we are done. □

As an illustration, consider a usual Hadamard matrix $H \in M_N(\mathbb{C})$. If we denote its rows by $H_1,\ldots,H_N$ and we consider the vectors $\xi_{ij} = H_i/H_j$, then we have:

$$\xi_{ij} = \left(\frac{H_{i1}}{H_{j1}},\ldots,\frac{H_{iN}}{H_{jN}}\right)$$

Thus the orthogonal projection on this vector ξ_{ij} is given by:

$$(P_{\xi_{ij}})_{ab} = \frac{1}{||\xi_{ij}||^2}(\xi_{ij})_a\overline{(\xi_{ij})_b} = \frac{1}{N}H_{ia}H_{ja}^*H_{jb}H_{ib}^* = (P_{ij})_{ab}$$

We conclude that we have $P_{ij} = P_{\xi_{ij}}$ for any i,j, so our construction from Theorem 15.15 is compatible with the construction for the usual complex Hadamard matrices.

We discuss now the computation of the quantum permutation groups associated to the deformed tensor products of Hadamard matrices. Let us begin with a study of the associated magic unitary. We have:

Proposition 15.16. *The magic unitary associated to $H \otimes_Q K$ is given by*

$$P_{ia,jb} = R_{ij} \otimes \frac{1}{N}(Q_{ic}Q_{jc}^*Q_{jd}Q_{id}^* \cdot K_{ac}K_{bc}^*K_{bd}K_{ad}^*)_{cd}$$

where R_{ij} is the magic unitary matrix associated to H.

Proof. With standard conventions for deformed tensor products and for double indices, the entries of $L = H \otimes_Q K$ are by definition the following elements:

$$L_{ia,jb} = Q_{ib}H_{ij}K_{ab}$$

Thus the projections $P_{ia,jb}$ constructed in Theorem 15.15 are given by:

$$\begin{aligned}(P_{ia,jb})_{kc,ld} &= \frac{1}{MN}L_{ia,kc}L_{jb,kc}^*L_{jb,ld}L_{ia,ld}^*\\ &= \frac{1}{MN}(Q_{ic}H_{ik}K_{ac})(Q_{jc}H_{jk}K_{bc})^*(Q_{jd}H_{jl}K_{bd})(Q_{id}H_{il}K_{ad})^*\\ &= \frac{1}{MN}(Q_{ic}Q_{jc}^*Q_{jd}Q_{id}^*)(H_{ik}H_{jk}^*H_{jl}H_{il}^*)(K_{ac}K_{bc}^*K_{bd}K_{ad}^*)\end{aligned}$$

In terms now of the standard matrix units e_{kl}, e_{cd}, we have:

$$\begin{aligned}&P_{ia,jb}\\ = &\frac{1}{MN}\sum_{kcld} e_{kl}\otimes e_{cd}\otimes (Q_{ic}Q_{jc}^*Q_{jd}Q_{id}^*)(H_{ik}H_{jk}^*H_{jl}H_{il}^*)(K_{ac}K_{bc}^*K_{bd}K_{ad}^*)\\ = &\frac{1}{MN}\sum_{kcld}\left(e_{kl}\otimes 1\otimes H_{ik}H_{jk}^*H_{jl}H_{il}^*\right)\left(1\otimes e_{cd}\otimes Q_{ic}Q_{jc}^*Q_{jd}Q_{id}^*\cdot K_{ac}K_{bc}^*K_{bd}K_{ad}^*\right)\end{aligned}$$

Since the quantities on the right commute, this gives the formula in the statement. □

In order to investigate the Diţă deformations, we use:

Definition 15.17. *Let $C(S_M^+)\to A$ and $C(S_N^+)\to B$ be Hopf algebra quotients, with fundamental corepresentations denoted u, v. We let*

$$A *_w B = A^{*N} * B / < [u_{ab}^{(i)}, v_{ij}] = 0 >$$

with the Hopf algebra structure making $w_{ia,jb} = u_{ab}^{(i)}v_{ij}$ a corepresentation.

The fact that we have indeed a Hopf algebra follows from the fact that w is magic. In terms of quantum groups, if $A = C(G)$, $B = C(H)$, we write $A *_w B = C(G \wr_* H)$:

$$C(G) *_w C(H) = C(G \wr_* H)$$

The $\wr_*$ operation is the free analogue of $\wr$, the usual wreath product. See [39]. With this convention, we have the following result:

Theorem 15.18. *The representation associated to $L = H \otimes_Q K$ factorizes as*

$$\begin{array}{ccc} C(S_{NM}^+) & \xrightarrow{\pi_L} & M_{NM}(\mathbb{C})\\ & \searrow \qquad \nearrow & \\ & C(S_M^+ \wr_* G_H) & \end{array}$$

and so the quantum group associated to L appears as a subgroup $G_L \subset S_M^+ \wr_* G_H$.

Proof. We use the formula in Proposition 15.16. For simplifying the writing we agree to use fractions of type $\frac{H_{ia}H_{jb}}{H_{ja}H_{ib}}$ instead of expressions of type $H_{ia}H_{ja}^*H_{jb}H_{ib}^*$, by keeping in mind that the variables are only subject to the commutation relations in Definition 15.1. Our claim is that the factorization can be indeed constructed, as follows:

$$U_{ab}^{(i)}=\sum_jP_{ia,jb}\quad,\quad V_{ij}=\sum_aP_{ia,jb}$$

Indeed, we have three verifications to be made, as follows:

(1) We must prove that the elements $V_{ij}=\sum_aP_{ia,jb}$ do not depend on b, and generate a copy of $C(G_H)$. But if we denote by (R_{ij}) the magic for H, we have indeed:

$$\begin{aligned}V_{ij}&=\frac{1}{N}\left(\frac{Q_{ic}Q_{jd}}{Q_{id}Q_{jc}}\cdot\frac{H_{ik}H_{jl}}{H_{il}H_{jk}}\cdot\delta_{cd}\right)_{kc,ld}\\&=((R_{ij})_{kl}\delta_{cd})_{kc,ld}\\&=R_{ij}\otimes 1\end{aligned}$$

(2) We prove now that for any i, the elements $U_{ab}^{(i)}=\sum_jP_{ia,jb}$ form a magic matrix. Since $P=(P_{ia,jb})$ is magic, the elements $U_{ab}^{(i)}=\sum_jP_{ia,jb}$ are self-adjoint, and we have $\sum_bU_{ab}^{(i)}=\sum_{bj}P_{ia,jb}=1$. The fact that each $U_{ab}^{(i)}$ is an idempotent follows from:

$$\begin{aligned}&((U_{ab}^{(i)})^2)_{kc,ld}\\&=\frac{1}{N^2M^2}\sum_{mejn}\frac{Q_{ic}Q_{je}}{Q_{ie}Q_{jc}}\cdot\frac{H_{ik}H_{jm}}{H_{im}H_{jk}}\cdot\frac{K_{ac}K_{be}}{K_{ae}K_{bc}}\cdot\frac{Q_{ie}Q_{nd}}{Q_{id}Q_{ne}}\cdot\frac{H_{im}H_{nl}}{H_{il}H_{nm}}\cdot\frac{K_{ae}K_{bd}}{K_{ad}K_{be}}\\&=\frac{1}{NM^2}\sum_{ejn}\frac{Q_{ic}Q_{je}Q_{nd}}{Q_{jc}Q_{id}Q_{ne}}\cdot\frac{H_{ik}H_{nl}}{H_{jk}H_{il}}\delta_{jn}\cdot\frac{K_{ac}K_{bd}}{K_{bc}K_{ad}}\\&=\frac{1}{NM^2}\sum_{ej}\frac{Q_{ic}Q_{je}Q_{jd}}{Q_{jc}Q_{id}Q_{je}}\cdot\frac{H_{ik}H_{jl}}{H_{jk}H_{il}}\cdot\frac{K_{ac}K_{bd}}{K_{bc}K_{ad}}\\&=\frac{1}{NM}\sum_j\frac{Q_{ic}Q_{jd}}{Q_{jc}Q_{id}}\cdot\frac{H_{ik}H_{jl}}{H_{jk}H_{il}}\cdot\frac{K_{ac}K_{bd}}{K_{bc}K_{ad}}\\&=(U_{ab}^{(i)})_{kc,ld}\end{aligned}$$

Finally, the condition $\sum_aU_{ab}^{(i)}=1$ can be checked as follows:

$$\begin{aligned}\sum_aU_{ab}^{(i)}&=\frac{1}{N}\left(\sum_j\frac{Q_{ic}Q_{jd}}{Q_{id}Q_{jc}}\cdot\frac{H_{ik}H_{jl}}{H_{il}H_{jk}}\cdot\delta_{cd}\right)_{kc,ld}\\&=\frac{1}{N}\left(\sum_j\frac{H_{ik}H_{jl}}{H_{il}H_{jk}}\cdot\delta_{cd}\right)_{kc,ld}\\&=1\end{aligned}$$

(3) It remains to prove that we have $U_{ab}^{(i)}V_{ij}=V_{ij}U_{ab}^{(i)}=P_{ia,jb}$. First, we have:

$$\begin{aligned}
(U_{ab}^{(i)}V_{ij})_{kc,ld} &= \frac{1}{N^2M}\sum_{mn}\frac{Q_{ic}Q_{nd}}{Q_{id}Q_{nc}}\cdot\frac{H_{ik}H_{nm}}{H_{im}H_{nk}}\cdot\frac{K_{ac}K_{bd}}{K_{ad}K_{bc}}\cdot\frac{H_{im}H_{jl}}{H_{il}H_{jm}}\\
&= \frac{1}{NM}\sum_{n}\frac{Q_{ic}Q_{nd}}{Q_{id}Q_{nc}}\cdot\frac{H_{ik}H_{jl}}{H_{nk}H_{il}}\delta_{nj}\cdot\frac{K_{ac}K_{bd}}{K_{ad}K_{bc}}\\
&= \frac{1}{NM}\cdot\frac{Q_{ic}Q_{jd}}{Q_{id}Q_{jc}}\cdot\frac{H_{ik}H_{jl}}{H_{jk}H_{il}}\cdot\frac{K_{ac}K_{bd}}{K_{ad}K_{bc}}\\
&= (P_{ia,jb})_{kc,ld}
\end{aligned}$$

The remaining computation is similar, as follows:

$$\begin{aligned}
(V_{ij}U_{ab}^{(i)})_{kc,ld} &= \frac{1}{N^2M}\sum_{mn}\frac{H_{ik}H_{jm}}{H_{im}H_{jk}}\cdot\frac{Q_{ic}Q_{nd}}{Q_{id}Q_{nc}}\cdot\frac{H_{im}H_{nl}}{H_{il}H_{nm}}\cdot\frac{K_{ac}K_{bd}}{K_{ad}K_{bc}}\\
&= \frac{1}{NM}\sum_{n}\frac{Q_{ic}Q_{nd}}{Q_{id}Q_{nc}}\cdot\frac{H_{ik}H_{nl}}{H_{jk}H_{il}}\delta_{jn}\cdot\frac{K_{ac}K_{bd}}{K_{ad}K_{bc}}\\
&= \frac{1}{NM}\cdot\frac{Q_{ic}Q_{jd}}{Q_{id}Q_{jc}}\cdot\frac{H_{ik}H_{jl}}{H_{jk}H_{il}}\cdot\frac{K_{ac}K_{bd}}{K_{ad}K_{bc}}\\
&= (P_{ia,jb})_{kc,ld}
\end{aligned}$$

Thus we have checked all the relations, and we are done. □

In general, the problem of further factorizing the above representation is a quite difficult one, even in the classical case. For a number of results here, we refer to [15], [40].

Let us discuss now another generalization of the construction $H\to G$, which is independent from the one above. The idea, following [31], will be that of looking at the partial Hadamard matrices (PHM), and their connection with the partial permutations. Let us start with the following standard definition:

Definition 15.19. *A partial permutation of $\{1\ldots,N\}$ is a bijection $\sigma:X\simeq Y$, with:*

$$X,Y\subset\{1,\ldots,N\}$$

We denote by $\widetilde{S}_N$ the set formed by such partial permutations.

We have $S_N\subset\widetilde{S}_N$, and the embedding $u:S_N\subset M_N(0,1)$ given by the standard permutation matrices can be extended to an embedding $u:\widetilde{S}_N\subset M_N(0,1)$, as follows:

$$u_{ij}(\sigma)=\begin{cases}1 & \text{if } \sigma(j)=i\\ 0 & \text{otherwise}\end{cases}$$

By looking at the image of this embedding, we see that $\widetilde{S}_N$ is in bijection with the matrices $M\in M_N(0,1)$ having at most one 1 entry on each row and column.

In analogy with Wang's theory in [142], we have the following definition:

Definition 15.20. *A submagic matrix is a matrix $u\in M_N(A)$ whose entries are projections, which are pairwise orthogonal on rows and columns. We let $C(\widetilde{S}_N^+)$ be the universal C^*-algebra generated by the entries of a $N\times N$ submagic matrix.*

Here the fact that the algebra $C(\widetilde{S}_N^+)$ is indeed well-defined is clear. As a first observation, this algebra has a comultiplication, given by:

$$\Delta(u_{ij})=\sum_k u_{ik}\otimes u_{kj}$$

This algebra has as well a counit, given by:

$$\varepsilon(u_{ij})=\delta_{ij}$$

Thus $\widetilde{S}_N^+$ is a quantum semigroup, and we have maps as follows, with the bialgebras at left corresponding to the quantum semigroups at right:

$$\begin{matrix}C(\widetilde{S}_N^+)&\to&C(S_N^+)\\ \downarrow&&\downarrow\\ C(\widetilde{S}_N)&\to&C(S_N)\end{matrix}\quad:\quad\begin{matrix}\widetilde{S}_N^+&\supset&S_N^+\\ \cup&&\cup\\ \widetilde{S}_N&\supset&S_N\end{matrix}$$

The relation of all this with the PHM is immediate, appearing as follows:

Theorem 15.21. *If $H\in M_{M\times N}(\mathbb{T})$ is a PHM, with rows denoted $H_1,\ldots,H_M\in\mathbb{T}^N$, then the following matrix of rank one projections is submagic:*

$$P_{ij}=Proj\left(\frac{H_i}{H_j}\right)$$

Thus H produces a representation $\pi_H:C(\widetilde{S}_M^+)\to M_N(\mathbb{C})$, given by $u_{ij}\to P_{ij}$, that we can factorize through $C(G)$, with the quantum semigroup $G\subset\widetilde{S}_M^+$ chosen minimal.

Proof. We have indeed the following computation, for the rows:

$$\left\langle\frac{H_i}{H_j},\frac{H_i}{H_k}\right\rangle=\sum_l\frac{H_{il}}{H_{jl}}\cdot\frac{H_{kl}}{H_{il}}=\sum_l\frac{H_{kl}}{H_{jl}}=<H_k,H_j>=\delta_{jk}$$

The verification for the columns is similar, as follows:

$$\left\langle\frac{H_i}{H_j},\frac{H_k}{H_j}\right\rangle=\sum_l\frac{H_{il}}{H_{jl}}\cdot\frac{H_{jl}}{H_{kl}}=\sum_l\frac{H_{il}}{H_{kl}}=N\delta_{ik}$$

Regarding now the last assertion, we can indeed factorize our representation as indicated, with the existence and uniqueness of the bialgebra $C(G)$, with the minimality property as above, being obtained by dividing $C(\widetilde{S}_M^+)$ by a suitable ideal. See [31]. □

Summarizing, we have a generalization of the $H \to G$ construction. The very first problem is that of deciding under which exact assumptions our construction is in fact "classical". In order to explain the answer here, we will need:

Definition 15.22. *A pre-Latin square is a square matrix*

$$L \in M_M(1, \ldots, N)$$

having the property that its entries are distinct, on each row and each column.

Given such a pre-Latin square L, to any $x \in \{1, \ldots, N\}$ we can associate the partial permutation $\sigma_x \in \widetilde{S}_M$ given by:

$$\sigma_x(j) = i \iff L_{ij} = x$$

With this construction in hand, we denote by $G \subset \widetilde{S}_M$ the semigroup generated by these partial permutations $\sigma_1, \ldots, \sigma_N$, and call it semigroup associated to L. Also, given an orthogonal basis $\xi = (\xi_1, \ldots, \xi_N)$ of $\mathbb{C}^N$, we can construct a submagic matrix $P \in M_M(M_N(\mathbb{C}))$, according to the following formula:

$$P_{ij} = Proj(\xi_{L_{ij}})$$

With these notations, we have the following result, from [31]:

Theorem 15.23. *If $H \in M_{N\times M}(\mathbb{C})$ is a PHM, the following are equivalent:*

(1) *The semigroup $G \subset \widetilde{S}_M^+$ is classical, i.e. $G \subset \widetilde{S}_M$.*
(2) *The projections $P_{ij} = Proj(H_i/H_j)$ pairwise commute.*
(3) *The vectors $H_i/H_j \in \mathbb{T}^N$ are pairwise proportional, or orthogonal.*
(4) *The submagic matrix $P = (P_{ij})$ comes for a pre-Latin square L.*

In addition, if so is the case, G is the semigroup associated to L.

Proof. This is something standard, as follows:

(1) $\iff$ (2) is clear.

(2) $\iff$ (3) comes from the fact that two rank 1 projections commute precisely when their images coincide, or are orthogonal.

(3) $\iff$ (4) is clear again.

The last assertion comes from Gelfand duality. See [31]. □

We call "classical" the matrices in Theorem 15.23, that we will study now. Let us begin with a study at $M = 2$. We make the following convention, where τ is the transposition, ij is the partial permutation $i \to j$, and $\emptyset$ is the null map:

$$\widetilde{S}_2 = \{id, \tau, 11, 12, 21, 22, \emptyset\}$$

With this convention, we have the following result:

Proposition 15.24. *A partial Hadamard matrix $H \in M_{2\times N}(\mathbb{T})$, in dephased form*

$$H = \begin{pmatrix} 1 & \ldots & 1 \\ \lambda_1 & \ldots & \lambda_N \end{pmatrix}$$

is of classical type when one of the following happens:

(1) *Either $\lambda_i = \pm w$, for some $w \in \mathbb{T}$, in which case $G = \{id, \tau\}$.*
(2) *Or $\sum_i \lambda_i^2 = 0$, in which case $G = \{id, 11, 12, 21, 22, \emptyset\}$*

Proof. With $1 = (1, \ldots, 1)$ and $\lambda = (\lambda_1, \ldots, \lambda_N)$, the matrix formed by the vectors H_i/H_j is $(\begin{smallmatrix} 1 & \lambda \\ \bar{\lambda} & 1 \end{smallmatrix})$. Since $1 \perp \lambda, \bar{\lambda}$ we just have to compare $\lambda, \bar{\lambda}$, and we have two cases:

(1) Case $\lambda \sim \bar{\lambda}$. This means $\lambda^2 \sim 1$, and so $\lambda_i = \pm w$, for some $w \in \mathbb{T}$. In this case the associated pre-Latin square is $L = (\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix})$, the partial permutations σ_x associated to L are $\sigma_1 = id$ and $\sigma_2 = \tau$, and we have $G =< id, \tau >= \{id, \tau\}$, as claimed.

(2) Case $\lambda \perp \bar{\lambda}$. This means $\sum_i \lambda_i^2 = 0$. In this case the associated pre-Latin square is $L = (\begin{smallmatrix} 1 & 2 \\ 3 & 1 \end{smallmatrix})$, the associated partial permutations σ_x are given by $\sigma_1 = id$, $\sigma_2 = 21$, $\sigma_3 = 12$, and so we obtain $G =< id, 21, 12 >= \{id, 11, 12, 21, 22, \emptyset\}$, as claimed. $\square$

The matrices in (1) are, modulo equivalence, those which are real. As for the matrices in (2), these are parametrized by the solutions $\lambda \in \mathbb{T}^N$ of the following equations:

$$\sum_i \lambda_i = \sum_i \lambda_i^2 = 0$$

In general, it is quite unclear on how to deal with these equations. Observe that, as a basic example here, we have the upper $2 \times N$ submatrix of F_N, with $N \geq 3$.

Let us discuss now in detail the truncated Fourier matrix case. First, we have:

Proposition 15.25. *The Fourier matrix, $F_N = (w^{ij})$ with $w = e^{2\pi i/N}$, is of classical type, and the associated group $G \subset S_N$ is the cyclic group $\mathbb{Z}_N$.*

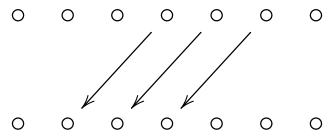
Proof. Since $H = F_N$ is a square matrix, the associated semigroup $G \subset \widetilde{S}_N^+$ must be a quantum group, $G \subset S_N^+$. We must prove that this quantum group is $G = \mathbb{Z}_N$.

With $\rho = (1, w, w^2, \ldots, w^{N-1})$ the rows of H are given by $H_i = \rho^i$, and so we have $H_i/H_j = \rho^{i-j}$. We conclude that H is indeed of classical type, coming from the Latin square $L_{ij} = j - i$ and from the orthogonal basis $\xi = (1, \rho^{-1}, \rho^{-2}, \ldots, \rho^{1-N})$.

We have $G =< \sigma_1, \ldots, \sigma_N >$, where $\sigma_x \in S_N$ is given by $\sigma_x(j) = i \iff L_{ij} = x$. From $L_{ij} = j - i$ we obtain $\sigma_x(j) = j - x$, and so $G = \{\sigma_1, \ldots, \sigma_N\} \simeq \mathbb{Z}_N$, as claimed. $\square$

Let $F_{M,N}$ be the upper $M \times N$ submatrix of F_N, and $G_{M,N} \subset \widetilde{S}_M$ be the associated semigroup. The simplest case is that when M is small, and here we have:

Theorem 15.26. *In the $N > 2M-2$ regime, $G_{M,N} \subset \widetilde{S}_M$ is formed by the maps*

$\sigma =$ 

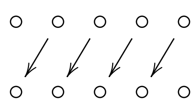
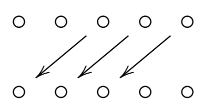
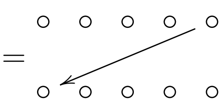
that is, $\sigma : I \simeq J$, $\sigma(j) = j - x$, with $I, J \subset \{1, \ldots, M\}$ intervals, independently of N.

Proof. Since for $\widetilde{H} = F_N$ the associated Latin square is circulant, $\widetilde{L}_{ij} = j - i$, the pre-Latin square that we are interested in is:

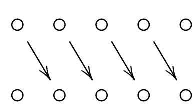
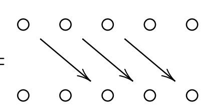
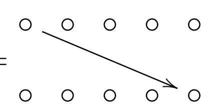
$$L = \begin{pmatrix} 0 & 1 & 2 & \ldots & M-1 \\ N-1 & 0 & 1 & \ldots & M-2 \\ N-2 & N-1 & 0 & \ldots & M-3 \\ \ldots \\ N-M+1 & N-M+2 & N-M+3 & \ldots & 0 \end{pmatrix}$$

Observe that, due to our $N > 2M-2$ assumption, we have $N - M + 1 > M - 1$, and so the entries above the diagonal are distinct from those below the diagonal.

Let us compute now the partial permutations $\sigma_x \in \widetilde{S}_M$ given by $\sigma_x(j) = i \iff L_{ij} = x$. We have $\sigma_0 = id$, and then $\sigma_1, \sigma_2, \ldots, \sigma_{M-1}$ are as follows:

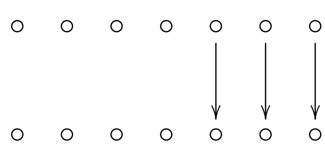
$\sigma_1 =$  $\sigma_2 =$  $\ldots$ $\sigma_{M-1} =$ 

Observe that $\sigma_2 = \sigma_1^2, \sigma_3 = \sigma_1^3, \ldots, \sigma_{M-1} = \sigma_1^{M-1}$. As for the remaining partial permutations, these are given by $\sigma_{N-1} = \sigma_1^{-1}, \sigma_{N-2} = \sigma_2^{-1}, \ldots, \sigma_{N-M+1} = \sigma_{M-1}^{-1}$:

$\sigma_{N-1} =$  $\sigma_{N-2} =$  $\ldots$ $\sigma_{N-M+1} =$ 

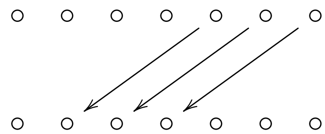
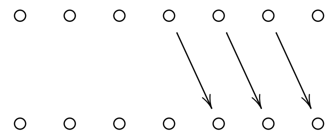
Thus $G_{M,N} =< \sigma_1 >$. Now if we denote by $G'_{M,N}$ the semigroup in the statement, we have $\sigma_1 \in G'_{M,N}$, so $G_{M,N} \subset G'_{M,N}$. The reverse inclusion can be proved as follows:

(1) Assume first that $\sigma \in G'_{M,N}$, $\sigma : I \simeq J$ has the property $M \in I, J$:

$\sigma =$ 

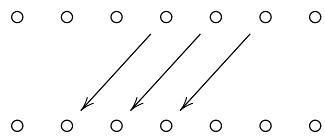
Then we can write $\sigma = \sigma_{N-k}\sigma_k$, with $k = M - |I|$, so we have $\sigma \in G_{M,N}$.

(2) Assume now that $\sigma \in G'_{M,N}$, $\sigma : I \simeq J$ has just the property $M \in I$ or $M \in J$:

$\sigma' =$  $\sigma'' =$ 

In this case we have as well $\sigma \in G_{M,N}$, because σ appears from one of the maps in (1) by adding a "slope", which can be obtained by composing with a suitable map σ_k.

(3) Assume now that $\sigma \in G'_{M,N}$, $\sigma : I \simeq J$ is arbitrary:

$\sigma =$ 

Then we can write $\sigma = \sigma'\sigma''$ with $\sigma' : L \simeq J$, $\sigma'' : I \simeq L$, where L is an interval satisfying $|L| = |I| = |J|$ and $M \in L$, and since $\sigma', \sigma'' \in G_{M,N}$ by (2), we are done. $\square$

Summarizing, we have so far complete results at $N = M$, and at $N > 2M - 2$. In the remaining regime, $M < N \leq 2M - 2$, the semigroup $G_{M,N} \subset \widetilde{S}_M$ looks quite hard to compute, and for the moment we only have some partial results regarding it.

For a partial permutation $\sigma : I \simeq J$ with $|I| = |J| = k$, set $\kappa(\sigma) = k$. We have:

Theorem 15.27. *The components $G_{M,N}^{(k)} = \{\sigma \in G_{M,N} | \kappa(\sigma) = k\}$ with $k > 2M - N$ are, in the $M < N \leq 2M - 2$ regime, the same as those in the $N > 2M - 2$ regime.*

Proof. In the $M < N \leq 2M - 2$ regime the pre-Latin square that we are interested in has as usual 0 on the diagonal, and then takes its entries from the set $S = \{1, \ldots, N - M\} \cup \{N - M + 1, \ldots, M - 1\} \cup \{M, \ldots, N - 1\}$, in a uniform way from each of the 3 components of S. Here is an illustrating example, at $M = 6, N = 8$:

$$L = \begin{pmatrix} \mathbf{0} & 1 & 2 & \mathbf{3} & \mathbf{4} & \mathbf{5} \\ 7 & \mathbf{0} & 1 & 2 & \mathbf{3} & \mathbf{4} \\ 6 & 7 & \mathbf{0} & 1 & 2 & \mathbf{3} \\ \mathbf{5} & 6 & 7 & \mathbf{0} & 1 & 2 \\ \mathbf{4} & \mathbf{5} & 6 & 7 & \mathbf{0} & 1 \\ \mathbf{3} & \mathbf{4} & \mathbf{5} & 6 & 7 & \mathbf{0} \end{pmatrix}$$

The point now is that $\sigma_1, \ldots, \sigma_{N-M}$ are given by the same formulae as those in the proof of Theorem 15.26, then $\sigma_{N-M+1}, \ldots, \sigma_{M-1}$ all satisfy $\kappa(\sigma) = 2M - N$, and finally $\sigma_M, \ldots, \sigma_{N-1}$ are once again given by the formulae in the proof of Theorem 15.26.

Now since we have $\kappa(\sigma\rho) \leq \min(\kappa(\sigma), \kappa(\rho))$, adding the maps $\sigma_{N-M+1}, \ldots, \sigma_{M-1}$ to the semigroup $G_{M,N} \subset \widetilde{S}_M$ computed in the proof of Theorem 15.26 won't change the $G_{M,N}^{(k)}$ components of this semigroup at $k > 2M - N$, and this gives the result. $\square$

16. Fourier models

We have seen that associated to any complex Hadamard matrix $H \in M_N(\mathbb{C})$ is a quantum permutation group $G \subset S_N^+$. The construction $H \to G$ is something very simple, obtained by factorizing the representation $\pi : C(S_N^+) \to M_N(\mathbb{C})$ given by $u_{ij} \to Proj(H_i/H_j)$, where $H_1, \ldots, H_N \in \mathbb{T}^N$ are the rows of H. As a basic example, a Fourier matrix $H = F_G$ produces in this way the group G itself, acting on itself.

Following [15], we discuss here the computation of the quantum permutation groups associated to the Diţă deformations of the tensor products of Fourier matrices. Let us begin by recalling the construction of the Fourier matrix models:

Definition 16.1. *Associated to a finite abelian group G is the matrix model*

$$\pi : C(G) \to M_G(\mathbb{C})$$

coming from the following magic matrix,

$$(U_{ij})_{kl} = \frac{1}{N} F_{i-j,k-l}$$

where $F = F_G$ is the Fourier matrix of G.

According to the formulae in section 13 above, this is precisely the matrix model obtained by taking the minimal factorization of the model $C(S_G^+) \to M_G(\mathbb{C})$ coming from the Fourier matrix F_G, with the algebra $C(G)$ being the Hopf image of this latter model, and with G itself being the quantum permutation group associated to F_G.

Let us recall as well the construction of the deformed Fourier models:

Definition 16.2. *Given two finite abelian groups G, H, we consider the corresponding deformed Fourier matrix, given by the formula*

$$(F_G \otimes_Q F_H)_{ia,jb} = Q_{ib}(F_G)_{ij}(F_H)_{ab}$$

and we factorize the associated representation π_Q of the algebra $C(S_{G\times H}^+)$,

$$\begin{tikzcd} C(S_{G\times H}^+) \arrow[rr, "\pi_Q"] \arrow[dr] & & M_{G\times H}(\mathbb{C}) \\ & C(G_Q) \arrow[ur, "\pi"'] & \end{tikzcd}$$

with $C(G_Q)$ being the Hopf image of this representation π_Q.

Explicitely computing the above quantum permutation group $G_Q \subset S_{G\times H}^+$, as function of the parameter matrix $Q \in M_{G\times H}(\mathbb{T})$, will be our main purpose, in what follows. In order to do so, we will need the following elementary result:

Proposition 16.3. *If G is a finite abelian group then*

$$C(G)=C(S_G^+)\Big/\Big\langle u_{ij}=u_{kl}\Big|\forall i-j=k-l\Big\rangle$$

with all the indices taken inside G.

Proof. As a first observation, the quotient algebra in the statement is commutative, because we have the following relations:

$$u_{ij}u_{kl}=u_{ij}u_{i,l-k+i}=\delta_{j,l-k+i}u_{ij}$$

$$u_{kl}u_{ij}=u_{i,l-k+i}u_{ij}=\delta_{j,l-k+i}u_{ij}$$

Thus if we denote the algebra in the statement by $C(H)$, we have $H\subset S_G$. Now since $u_{ij}(\sigma)=\delta_{i\sigma(j)}$ for any $\sigma\in H$, we obtain:

$$i-j=k-l\implies(\sigma(j)=i\iff\sigma(l)=k)$$

But this condition tells us precisely that $\sigma(i)-i$ must be independent on i, and so, for some $g\in G$, we have $\sigma(i)=i+g$. Thus we have $\sigma\in G$, as desired. $\square$

In order to factorize the representation in Definition 16.2, we will need:

Definition 16.4. *Gives two Hopf algebra quotients, as follows,*

$$C(S_M^+)\to A\quad,\quad C(S_N^+)\to B$$

with fundamental corepresentations denoted u,v, we let

$$A*_w B=A^{*N}*B/<[u_{ab}^{(i)},v_{ij}]=0>$$

with the Hopf algebra structure making $w_{ia,jb}=u_{ab}^{(i)}v_{ij}$ a corepresentation.

The fact that we have indeed a Hopf algebra follows from the fact that w is magic. In terms of quantum groups, let us write $A=C(G)$, $B=C(H)$. We write then:

$$A*_w B=C(G\wr_* H)$$

In other words, we make the following convention:

$$C(G)*_w C(H)=C(G\wr_* H)$$

The $\wr_*$ operation is then the free analogue of $\wr$, the usual wreath product. For details regarding this construction, we refer to [15].

We can now factorize representation π_Q in Definition 16.2, as follows:

Theorem 16.5. *We have a factorization as follows,*

$$\begin{tikzcd}
C(S_{G\times H}^+) \arrow[rr, "\pi_Q"] \arrow[dr] & & M_{G\times H}(\mathbb{C}) \\
& C(H \wr_* G) \arrow[ur, "\pi"'] &
\end{tikzcd}$$

given on the standard generators by the formulae

$$U_{ab}^{(i)}=\sum_j W_{ia,jb}\quad,\quad V_{ij}=\sum_a W_{ia,jb}$$

independently of b, where W is the magic matrix producing π_Q.

Proof. With $K=F_G,L=F_H$ and $M=|G|,N=|H|$, the formula of the magic matrix $W\in M_{G\times H}(M_{G\times H}(\mathbb{C}))$ associated to $H=K\otimes_Q L$ is as follows:

$$\begin{aligned}
(W_{ia,jb})_{kc,ld} &= \frac{1}{MN}\cdot\frac{Q_{ic}Q_{jd}}{Q_{id}Q_{jc}}\cdot\frac{K_{ik}K_{jl}}{K_{il}K_{jk}}\cdot\frac{L_{ac}L_{bd}}{L_{ad}L_{bc}}\\
&= \frac{1}{MN}\cdot\frac{Q_{ic}Q_{jd}}{Q_{id}Q_{jc}}\cdot K_{i-j,k-l}L_{a-b,c-d}
\end{aligned}$$

Our claim now is that the representation π_Q constructed in Definition 16.2 can be factorized in three steps, up to the factorization in the statement, as follows:

$$\begin{tikzcd}
C(S_{G\times H}^+) \arrow[rr, "\pi_Q"] \arrow[d] & & M_{G\times H}(\mathbb{C}) \\
C(S_H^+ \wr_* S_G^+) \arrow[r] \arrow[urr, dotted] & C(S_H^+ \wr_* G) \arrow[r] \arrow[ur, dotted] & C(H \wr_* G) \arrow[u, dotted]
\end{tikzcd}$$

Indeed, these factorizations can be constructed as follows:

(1) The construction of the map on the left is standard, by checking the relations for the free wreath product, and this produces the first factorization.

(2) Regarding the second factorization, the one in the middle, this comes from the fact that since the elements V_{ij} depend on $i-j$, they satisfy the defining relations for the quotient algebra $C(S_G^+)\to C(G)$, coming from Proposition 16.3.

(3) Finally, regarding the third factorization, the one on the right, observe that the above matrix $W_{ia,jb}$ depends only on i,j and on $a-b$. By summing over j we obtain that the elements $U_{ab}^{(i)}$ depend only on $a-b$, and we are done. $\square$

In order to further factorize the above representation, we use:

Definition 16.6. *If $H \curvearrowright \Gamma$ is a finite group acting by automorphisms on a discrete group, the corresponding crossed coproduct Hopf algebra is*

$$C^*(\Gamma) \rtimes C(H) = C^*(\Gamma) \otimes C(H)$$

with comultiplication given by the following formula,

$$\Delta(r \otimes \delta_k) = \sum_{h \in H} (r \otimes \delta_h) \otimes (h^{-1} \cdot r \otimes \delta_{h^{-1}k})$$

for $r \in \Gamma$ and $k \in H$.

Observe that $C(H)$ is a subcoalgebra, and that $C^*(\Gamma)$ is not a subcoalgebra. The quantum group corresponding to $C^*(\Gamma) \rtimes C(H)$ is denoted $\widehat{\Gamma} \rtimes H$.

Now back to the factorization in Theorem 16.5, the point is that we have:

Proposition 16.7. *With $L = F_H, N = |H|$ we have an isomorphism*

$$C(H \wr_* G) \simeq C^*(H)^{*G} \rtimes C(G)$$

given by $v_{ij} \to 1 \otimes v_{ij}$ and by

$$u_{ab}^{(i)} = \frac{1}{N} \sum_c L_{b-a,c} c^{(i)} \otimes 1$$

on the standard generators.

Proof. We know that the algebra $C(H \wr_* G)$ is the quotient of $C(H)^{*G} * C(G)$ by the relations $[u_{ab}^{(i)}, v_{ij}] = 0$. Now since v_{ij} depends only on $j - i$, we obtain:

$$[u_{ab}^{(i)}, v_{kl}] = [u_{ab}^{(i)}, v_{i,l-k+i}] = 0$$

Thus, we are in a usual tensor product situation, and we have:

$$C(H \wr_* G) = C(H)^{*G} \otimes C(G)$$

Let us compose now this identification with $\Phi^{*G} \otimes id$, where $\Phi : C(H) \to C^*(H)$ is the Fourier transform. We obtain an isomorphism as in the statement.

Now observe that we have the following formula:

$$\Phi(u_{ab}) = \frac{1}{N} \sum_c L_{b-a,c} c$$

Thus the formula for the image of $u_{ab}^{(i)}$ is indeed the one in the statement. $\square$

Here is now our key result, which will lead to further factorizations:

Proposition 16.8. *With $c^{(i)} = \sum_a L_{ac} u_{a0}^{(i)}$ and $\varepsilon_{ke} = \sum_i K_{ik} e_{ie}$ we have:*

$$\pi(c^{(i)})(\varepsilon_{ke}) = \frac{Q_{i,e-c} Q_{i-k,e}}{Q_{ie} Q_{i-k,e-c}} \varepsilon_{k,e-c}$$

In particular if $c_1 + \ldots + c_s = 0$ then the matrix

$$\pi(c_1^{(i_1)} \ldots c_s^{(i_s)})$$

is diagonal, for any choice of the indices $i_1, \ldots, i_s$.

Proof. With $c^{(i)}$ as in the statement, we have the following formula:

$$\begin{aligned}
\pi(c^{(i)}) &= \sum_a L_{ac} \pi(u_{a0}^{(i)}) \\
&= \sum_{aj} L_{ac} W_{ia,j0}
\end{aligned}$$

On the other hand, in terms of the basis in the statement, we have:

$$W_{ia,jb}(\varepsilon_{ke}) = \frac{1}{N} \delta_{i-j,k} \sum_d \frac{Q_{id} Q_{je}}{Q_{ie} Q_{jd}} L_{a-b,d-e} \varepsilon_{kd}$$

We therefore obtain, as desired:

$$\begin{aligned}
\pi(c^{(i)})(\varepsilon_{ke}) &= \frac{1}{N} \sum_{ad} L_{ac} \frac{Q_{id} Q_{i-k,e}}{Q_{ie} Q_{i-k,d}} L_{a,d-e} \varepsilon_{kd} \\
&= \frac{1}{N} \sum_d \frac{Q_{id} Q_{i-k,e}}{Q_{ie} Q_{i-k,d}} \varepsilon_{kd} \sum_a L_{a,d-e+c} \\
&= \sum_d \frac{Q_{id} Q_{i-k,e}}{Q_{ie} Q_{i-k,d}} \varepsilon_{kd} \delta_{d,e-c} \\
&= \frac{Q_{i,e-c} Q_{i-k,e}}{Q_{ie} Q_{i-k,e-c}} \varepsilon_{k,e-c}
\end{aligned}$$

Regarding now the last assertion, this follows from the fact that each matrix of type $\pi(c_r^{(i_r)})$ acts on the standard basis elements ε_{ke} by preserving the left index k, and by rotating by c_r the right index e. Thus when we assume $c_1 + \ldots + c_s = 0$ all these rotations compose up to the identity, and we obtain indeed a diagonal matrix. □

We have now all needed ingredients for refining Theorem 16.5, as follows:

Theorem 16.9. *We have a factorization as follows,*

$$\begin{tikzcd}
C(S_{G\times H}^+) \arrow[rr, "\pi_Q"] \arrow[dr] & & M_{G\times H}(\mathbb{C}) \\
& C^*(\Gamma_{G,H})\rtimes C(G) \arrow[ur, "\rho"'] &
\end{tikzcd}$$

where the group on the bottom is given by:

$$\Gamma_{G,H}=H^{*G}\Big/\left\langle[c_1^{(i_1)}\ldots c_s^{(i_s)},d_1^{(j_1)}\ldots d_s^{(j_s)}]=1\Big|\sum_rc_r=\sum_rd_r=0\right\rangle$$

Proof. Assume that we have a representation, as follows:

$$\pi:C^*(\Gamma)\rtimes C(G)\to M_L(\mathbb{C})$$

Let Λ be a G-stable normal subgroup of Γ, so that G acts on Γ/Λ, and we can form the product $C^*(\Gamma/\Lambda)\rtimes C(G)$, and assume that π is trivial on Λ. Then π factorizes as:

$$\begin{tikzcd}
C^*(\Gamma)\rtimes C(G) \arrow[rr, "\pi"] \arrow[dr] & & M_L(\mathbb{C}) \\
& C^*(\Gamma/\Lambda)\rtimes C(G) \arrow[ur, "\rho"'] &
\end{tikzcd}$$

With $\Gamma=H^{*G}$, and by using the above results, this gives the result. $\square$

In what follows we will restrict attention to the case where the parameter matrix Q is generic, and we prove that the representation in Theorem 16.9 is the minimal one.

Our starting point is the group $\Gamma_{G,H}$ found above:

Definition 16.10. *Associated to two finite abelian groups G,H is the discrete group*

$$\Gamma_{G,H}=H^{*G}\Big/\left\langle[c_1^{(i_1)}\ldots c_s^{(i_s)},d_1^{(j_1)}\ldots d_s^{(j_s)}]=1\Big|\sum_rc_r=\sum_rd_r=0\right\rangle$$

where the superscripts refer to the G copies of H, inside the free product.

We will need a more convenient description of this group. The idea here is that the above commutation relations can be realized inside a suitable semidirect product. Given a group acting on another group, $H\curvearrowright G$, we denote as usual by $G\rtimes H$ the semidirect product of G by H, which is the set $G\times H$, with multiplication:

$$(a,s)(b,t)=(as(b),st)$$

Now given a group G, and a finite abelian group H, we can make H act on G^H, and form the product $G^H \rtimes H$. Since the elements of type $(g,\ldots,g)$ are invariant, we can form as well the product $(G^H/G)\rtimes H$. We can identify $G^H/G\simeq G^{|H|-1}$ via the map:

$$(1,g_1,\ldots,g_{|H|-1})\to(g_1,\ldots,g_{|H|-1})$$

Thus, we obtain a product $G^{|H|-1}\rtimes H$. With these notations, we have:

Proposition 16.11. *The group $\Gamma_{G,H}$ has the following properties:*

(1) *We have an isomorphism as follows:*

$$\Gamma_{G,H}\simeq\mathbb{Z}^{(|G|-1)(|H|-1)}\rtimes H$$

(2) *We have as well an isomorphism as follows,*

$$\Gamma_{G,H}\subset\mathbb{Z}^{(|G|-1)|H|}\rtimes H$$

via $c^{(0)}\to(0,c)$ and $c^{(i)}\to(b_{i0}-b_{ic},c)$ for $i\neq 0$, where b_{ic} are the standard generators of $\mathbb{Z}^{(|G|-1)|H|}$.

Proof. We prove these assertions at the same time. We must prove that we have group morphisms, given by the formulae in the statement, as follows:

$$\begin{aligned}\Gamma_{G,H}&\simeq\mathbb{Z}^{(|G|-1)(|H|-1)}\rtimes H\\&\subset\mathbb{Z}^{(|G|-1)|H|}\rtimes H\end{aligned}$$

Our first claim is that the formula in (2) defines a morphism as follows:

$$\Gamma_{G,H}\to\mathbb{Z}^{(|G|-1)|H|}\rtimes H$$

Indeed, the elements $(0,c)$ produce a copy of H, and since we have a group embedding $H\subset\mathbb{Z}^{|H|}\rtimes H$ given by $c\to(b_0-b_c,c)$, the elements $C^{(i)}=(b_{i0}-b_{ic},c)$ produce a copy of H, for any $i\neq 0$. In order to check now the commutation relations, observe that:

$$C_1^{(i_1)}\ldots C_s^{(i_s)}=\left(b_{i_10}-b_{i_1c_1}+b_{i_2c_1}-b_{i_2,c_1+c_2}+\ldots+b_{i_s,c_1+\ldots+c_{s-1}}-b_{i_s,c_1+\ldots+c_s},\sum_r c_r\right)$$

Thus $\sum_r c_r=0$ implies the following condition:

$$C_1^{(i_1)}\ldots C_s^{(i_s)}\in\mathbb{Z}^{(|G|-1)|H|}$$

Since we are now inside an abelian group, we have the commutation relations, and our claim is proved. By using the general crossed product considerations before the statement, it is routine to construct an embedding as follows:

$$\mathbb{Z}^{(|G|-1)(|H|-1)}\rtimes H\subset\mathbb{Z}^{(|G|-1)|H|}\rtimes H$$

To be more precise, we would like this embedding to be such that we have group morphisms whose composition is the group morphism just constructed, as follows:

$$\begin{aligned}\Gamma_{G,H} &\to \mathbb{Z}^{(|G|-1)(|H|-1)} \rtimes H\\ &\subset \mathbb{Z}^{(|G|-1)|H|} \rtimes H\end{aligned}$$

It remains to prove that the map on the left is injective. For this purpose, consider the morphism $\Gamma_{G,H} \to H$ given by $c^{(i)} \to c$, whose kernel T is formed by the elements of type $c_1^{(i_1)} \ldots c_s^{(i_s)}$, with $\sum_r c_r = 0$. We get an exact sequence, as follows:

$$1 \to T \to \Gamma_{G,H} \to H \to 1$$

This sequence splits by $c \to c^{(0)}$, so we have:

$$\Gamma_{G,H} \simeq T \rtimes H$$

Now by the definition of $\Gamma_{G,H}$, the subgroup T constructed above is abelian, and is moreover generated by the following elements:

$$(-c)^{(0)} c^{(i)} \quad , \quad c \neq 0$$

Finally, the fact that T is freely generated by these elements follows from the computation in the proof of Proposition 16.13 below. □

As already mentioned, we will be interested in what follows in the case where the deformation matrix Q is generic. Our genericity assumptions are as follows:

Definition 16.12. *We use the following notions:*

(1) *We call $p_1, \ldots, p_m \in \mathbb{T}$ root independent if for any $r_1, \ldots, r_m \in \mathbb{Z}$ we have:*

$$p_1^{r_1} \ldots p_m^{r_m} = 1 \implies r_1 = \ldots = r_m = 0$$

(2) *A matrix $Q \in M_{G\times H}(\mathbb{T})$, taken to be dephased,*

$$Q_{0c} = Q_{i0} = 1$$

is called generic if the elements Q_{ic}, with $i, c \neq 0$, are root independent.

In what follows we will do the computation for such matrices. We will need:

Proposition 16.13. *Assume that $Q \in M_{G\times H}(\mathbb{T})$ is generic, and set:*

$$\theta_{ic}^{ke} = \frac{Q_{i,e-c} Q_{i-k,e}}{Q_{ie} Q_{i-k,e-c}}$$

For every $k \in G$, we have a representation $\pi^k : \Gamma_{G,H} \to U_{|H|}$ given by:

$$\pi^k(c^{(i)})\epsilon_e = \theta_{ic}^{ke} \epsilon_{e-c}$$

The family of representations $(\pi^k)_{k\in G}$ is projectively faithful, in the sense that if for some $t \in \Gamma_{G,H}$ we have that $\pi^k(t)$ is a scalar matrix for any k, then $t = 1$.

Proof. The representations π^k arise as above. With $\Gamma_{G,H} = T \rtimes H$, as in the proof of Proposition 16.11, we see that for $t \in \Gamma_{G,H}$ such that $\pi^k(t)$ is a scalar matrix for any k, then $t \in T$, since the elements of T are the only ones having their image by π^k formed by diagonal matrices. Now write t as follows, with the generators of T being as in the proof of Proposition 16.11 above, and with $R_{ic} \in \mathbb{Z}$ being certain integers:

$$t = \prod_{i\neq 0, c\neq 0} ((-c)^{(0)}(c)^{(i)})^{R_{ic}}$$

Consider now the following quantities:

$$\begin{aligned} A(k,e) &= \prod_{i\neq 0}\prod_{c\neq 0}(\theta_{ic}^{ke}(\theta_{0c}^{ke})^{-1})^{R_{ic}} \\ &= \prod_{i\neq 0}\prod_{c\neq 0}(\theta_{ic}^{ke})^{R_{ic}}(\theta_{0c}^{ke})^{-R_{ic}} \\ &= \prod_{i\neq 0}\prod_{c\neq 0}(\theta_{ic}^{ke})^{R_{ic}} \cdot \prod_{c\neq 0}(\theta_{0c}^{ke})^{-\sum_{i\neq 0} R_{ic}} \\ &= \prod_{j\neq 0}\prod_{c\neq 0}(\theta_{jc}^{ke})^{R_{jc}} \cdot \prod_{c\neq 0}\prod_{j\neq 0}(\theta_{jc}^{ke})^{\sum_{i\neq 0} R_{ic}} \\ &= \prod_{j\neq 0}\prod_{c\neq 0}(\theta_{jc}^{ke})^{R_{jc}+\sum_{i\neq 0} R_{ic}} \end{aligned}$$

We have $\pi^k(t)(\epsilon_e) = A(k,e)\epsilon_e$, for any k, e. Our assumption is that for any k, we have $A(k,e) = A(k,f)$, for any e, f. Using the root independence of the elements Q_{ic}, $i, c \neq 0$, we see that this implies $R_{ic} = 0$ for any i, c, and this proves our assertion. □

We will need as well the following technical result:

Proposition 16.14. *Let $\pi : C^*(\Gamma) \rtimes C(H) \to L$ be a surjective Hopf algebra map, such that $\pi_{|C(H)}$ is injective, and such that for $r \in \Gamma$ and $f \in C(H)$, we have:*

$$\pi(r \otimes 1) = \pi(1 \otimes f) \implies r = 1$$

Then π is an isomorphism.

Proof. We use here various Hopf algebra tools. Consider the following algebra:

$$A = C^*(\Gamma) \rtimes C(H)$$

We start with the following standard Hopf algebra exact sequence, where $i(f) = 1 \otimes f$, and where $p = \varepsilon \otimes 1$:

$$\mathbb{C} \to C(H) \xrightarrow{i} A \xrightarrow{p} C^*(\Gamma) \to \mathbb{C}$$

Since $\pi \circ i$ is injective, and the Hopf subalgebra $\pi \circ i(C(H))$ is central in L, we can form the following quotient Hopf algebra:

$$\overline{L} = L/(\pi \circ i(C(H))^+ L$$

We obtain in this way another exact sequence, as follows:

$$\mathbb{C}\longrightarrow C(H)\xrightarrow{\pi\circ i}L\xrightarrow{q}\overline{L}\longrightarrow\mathbb{C}$$

Note that this sequence is indeed exact, e.g. by centrality. Thus, we get the following diagram with exact rows, with the Hopf algebra map on the right being surjective:

$$\begin{tikzcd}
\mathbb{C} \arrow[r] & C(H) \arrow[r, "i"] \arrow[d, equal] & A \arrow[r, "p"] \arrow[d, "\pi"] & C^*(\Gamma) \arrow[r] \arrow[d] & \mathbb{C} \\
\mathbb{C} \arrow[r] & C(H) \arrow[r, "\pi\circ i"] & L \arrow[r, "q"] & \overline{L} \arrow[r] & \mathbb{C}
\end{tikzcd}$$

Since a quotient of a group algebra is still a group algebra, we get a commutative diagram with exact rows as follows:

$$\begin{tikzcd}
\mathbb{C} \arrow[r] & C(H) \arrow[r, "i"] \arrow[d, equal] & A \arrow[r, "p"] \arrow[d, "\pi"] & C^*(\Gamma) \arrow[r] \arrow[d] & \mathbb{C} \\
\mathbb{C} \arrow[r] & C(H) \arrow[r, "\pi\circ i"] & L \arrow[r, "q'"] & C^*(\overline{\Gamma}) \arrow[r] & \mathbb{C}
\end{tikzcd}$$

Here the Hopf algebra map on the right is induced by a surjective morphism $u:\Gamma\to\overline{\Gamma}$, $g\mapsto\overline{g}$. By the five lemma we just have to show that u is injective. So, let $g\in\Gamma$ be such that $u(g)=1$. We have then:

$$q'\pi(g\otimes 1)=up(g\otimes 1)=u(g)=\overline{g}=1$$

For $g\in\Gamma$, let us set:

$${}_gA=\left\{a\in A\Big|\,p(a_1)\otimes a_2=g\otimes a\right\}$$

$${}_{\overline{g}}L=\left\{l\in L\Big|\,q'(l_1)\otimes l_2=\overline{g}\otimes l\right\}$$

The commutativity of the square on the right ensures that we have:

$$\pi({}_gA)\subset{}_{\overline{g}}L$$

Then with the previous g, we have, by exactness of the sequence:

$$\pi(g\otimes 1)\in{}_{\overline{1}}L=\pi i(C(H))$$

Thus, for some $f\in C(H)$, we must have:

$$\pi(g\otimes 1)=\pi(1\otimes f)$$

We conclude by our assumption that $g=1$. $\square$

We have now all the needed ingredients for proving a main result, as follows:

Theorem 16.15. *When Q is generic, the minimal factorization for π_Q is*

$$\begin{tikzcd} C(S_{G\times H}^+) \arrow[rr, "\pi_Q"] \arrow[dr] & & M_{G\times H}(\mathbb{C}) \\ & C^*(\Gamma_{G,H}) \rtimes C(G) \arrow[ur, "\pi"'] & \end{tikzcd}$$

where on the bottom

$$\Gamma_{G,H} \simeq \mathbb{Z}^{(|G|-1)(|H|-1)} \rtimes H$$

is the discrete group constructed above.

Proof. We want to apply Proposition 16.13 to the following morphism, arising from the factorization in Theorem 16.9, where L denotes the Hopf image of π_Q:

$$\theta : C^*(\Gamma_{G,H}) \rtimes C(G) \to L$$

To be more precise, this morphism produces the following commutative diagram:

$$\begin{tikzcd} C(S_{G\times H}^+) \arrow[rr, "\pi_Q"] \arrow[dr] \arrow[ddr] & & M_{G\times H}(\mathbb{C}) \\ & L \arrow[ur] & \\ & C^*(\Gamma_{G,H}) \rtimes C(G) \arrow[u, dashed, "\theta"] \arrow[uur, "\pi"'] & \end{tikzcd}$$

The first observation is that the injectivity assumption on $C(G)$ holds by construction, and that for $f \in C(G)$, the matrix $\pi(f)$ is "block scalar", the blocks corresponding to the indices k in the basis ε_{ke} in the basis from Proposition 16.13.

Now for $r \in \Gamma_{G,H}$ with $\theta(r \otimes 1) = \theta(1 \otimes f)$ for some $f \in C(G)$, we see, using the commutative diagram, that we will have that $\pi(r \otimes 1)$ is block scalar. By Proposition 16.11, the family of representations (π^k) of $\Gamma_{G,H}$, corresponding to the blocks k, is projectively faithful, so $r = 1$. We can apply indeed Proposition 16.13, and we are done. □

Summarizing, we have computed the quantum permutation groups associated to the Diţă deformations of the tensor products of Fourier matrices, in the case where the deformation matrix Q is generic. For some further computations, in the case where the deformation matrix Q is no longer generic, we refer to [15] and follow-up papers.

Let us compute now the Kesten measure $\mu = law(\chi)$. Our results here will be a combinatorial moment formula, a geometric interpretation of it, and an asymptotic result.

Let us begin with the moment formula, which is as follows:

Theorem 16.16. *We have the moment formula*

$$\int\chi^p=\frac{1}{|G|\cdot|H|}\#\left\{\begin{matrix}i_1,\ldots,i_p\in G\\ d_1,\ldots,d_p\in H\end{matrix}\Big|\begin{matrix}[(i_1,d_1),(i_2,d_2),\ldots,(i_p,d_p)]\\ =[(i_1,d_p),(i_2,d_1),\ldots,(i_p,d_{p-1})]\end{matrix}\right\}$$

where the sets between square brackets are by definition sets with repetition.

Proof. According to the various formulae above, the factorization found in Theorem 16.15 is, at the level of standard generators, as follows:

$$\begin{matrix}C(S_{G\times H}^+)&\to&C^*(\Gamma_{G,H})\otimes C(G)&\to&M_{G\times H}(\mathbb{C})\\ u_{ia,jb}&\to&\frac{1}{|H|}\sum_cF_{b-a,c}c^{(i)}\otimes v_{ij}&\to&W_{ia,jb}\end{matrix}$$

Thus, the main character of the quantum permutation group that we found in Theorem 16.15 is given by the following formula:

$$\begin{aligned}\chi&=\frac{1}{|H|}\sum_{iac}c^{(i)}\otimes v_{ii}\\ &=\sum_{ic}c^{(i)}\otimes v_{ii}\\ &=\left(\sum_{ic}c^{(i)}\right)\otimes\delta_1\end{aligned}$$

Now since the Haar functional of $C^*(\Gamma)\rtimes C(H)$ is the tensor product of the Haar functionals of $C^*(\Gamma),C(H)$, this gives the following formula, valid for any $p\geq 1$:

$$\int\chi^p=\frac{1}{|G|}\int_{\widehat{\Gamma}_{G,H}}\left(\sum_{ic}c^{(i)}\right)^p$$

Consider the elements $S_i=\sum_c c^{(i)}$. By using the embedding in Proposition 16.11 (2), with the notations there we have:

$$S_i=\sum_c(b_{i0}-b_{ic},c)$$

Now observe that these elements multiply as follows:

$$S_{i_1}\ldots S_{i_p}=\sum_{c_1\ldots c_p}\begin{pmatrix}\begin{matrix}b_{i_10}-b_{i_1c_1}+b_{i_2c_1}-b_{i_2,c_1+c_2}\\ +b_{i_3,c_1+c_2}-b_{i_3,c_1+c_2+c_3}+\ldots\ldots\\ \ldots\ldots+b_{i_p,c_1+\ldots+c_{p-1}}-b_{i_p,c_1+\ldots+c_p}\end{matrix}&,&c_1+\ldots+c_p\end{pmatrix}$$

In terms of the new indices $d_r=c_1+\ldots+c_r$, this formula becomes:

$$S_{i_1}\ldots S_{i_p}=\sum_{d_1\ldots d_p}\begin{pmatrix}\begin{matrix}b_{i_10}-b_{i_1d_1}+b_{i_2d_1}-b_{i_2d_2}\\ +b_{i_3d_2}-b_{i_3d_3}+\ldots\ldots\\ \ldots\ldots+b_{i_pd_{p-1}}-b_{i_pd_p}\end{matrix}&,&d_p\end{pmatrix}$$

Now by integrating, we must have $d_p=0$ on one hand, and on the other hand:

$$[(i_1,0),(i_2,d_1),\ldots,(i_p,d_{p-1})]=[(i_1,d_1),(i_2,d_2),\ldots,(i_p,d_p)]$$

Equivalently, we must have $d_p=0$ on one hand, and on the other hand:

$$[(i_1,d_p),(i_2,d_1),\ldots,(i_p,d_{p-1})]=[(i_1,d_1),(i_2,d_2),\ldots,(i_p,d_p)]$$

Thus, by translation invariance with respect to d_p, we obtain:

$$\int_{\widehat{\Gamma}_{G,H}}S_{i_1}\ldots S_{i_p}=\frac{1}{|H|}\#\left\{d_1,\ldots,d_p\in H\Big|\begin{matrix}[(i_1,d_1),(i_2,d_2),\ldots,(i_p,d_p)]\\=[(i_1,d_p),(i_2,d_1),\ldots,(i_p,d_{p-1})]\end{matrix}\right\}$$

It follows that we have the following moment formula:

$$\int_{\widehat{\Gamma}_{G,H}}\left(\sum_iS_i\right)^p=\frac{1}{|H|}\#\left\{\begin{matrix}i_1,\ldots,i_p\in G\\d_1,\ldots,d_p\in H\end{matrix}\Big|\begin{matrix}[(i_1,d_1),(i_2,d_2),\ldots,(i_p,d_p)]\\=[(i_1,d_p),(i_2,d_1),\ldots,(i_p,d_{p-1})]\end{matrix}\right\}$$

Now by dividing by $|G|$, we obtain the formula in the statement. $\square$

The formula in Theorem 16.16 can be interpreted as follows:

Theorem 16.17. *With $M=|G|,N=|H|$ we have the formula*

$$law(\chi)=\left(1-\frac{1}{N}\right)\delta_0+\frac{1}{N}law(A)$$

where the matrix

$$A\in C(\mathbb{T}^{MN},M_M(\mathbb{C}))$$

is given by $A(q)=$ Gram matrix of the rows of q.

Proof. According to Theorem 16.16, we have the following formula:

$$\begin{aligned}\int\chi^p&=\frac{1}{MN}\sum_{i_1\ldots i_p}\sum_{d_1\ldots d_p}\delta_{[i_1d_1,\ldots,i_pd_p],[i_1d_p,\ldots,i_pd_{p-1}]}\\&=\frac{1}{MN}\int_{\mathbb{T}^{MN}}\sum_{i_1\ldots i_p}\sum_{d_1\ldots d_p}\frac{q_{i_1d_1}\ldots q_{i_pd_p}}{q_{i_1d_p}\ldots q_{i_pd_{p-1}}}\,dq\\&=\frac{1}{MN}\int_{\mathbb{T}^{MN}}\sum_{i_1\ldots i_p}\left(\sum_{d_1}\frac{q_{i_1d_1}}{q_{i_2d_1}}\right)\left(\sum_{d_2}\frac{q_{i_2d_2}}{q_{i_3d_2}}\right)\ldots\left(\sum_{d_p}\frac{q_{i_pd_p}}{q_{i_1d_p}}\right)dq\end{aligned}$$

Consider now the Gram matrix in the statement, namely:

$$A(q)_{ij}=<R_i,R_j>$$

Here $R_1,\ldots,R_M$ are the rows of the following matrix:

$$q\in\mathbb{T}^{MN}\simeq M_{M\times N}(\mathbb{T})$$

We have then the following computation:

$$\begin{aligned}\int\chi^p &= \frac{1}{MN}\int_{\mathbb{T}^{MN}} < R_{i_1},R_{i_2} >< R_{i_2},R_{i_3} > \ldots < R_{i_p},R_{i_1} >\\ &= \frac{1}{MN}\int_{\mathbb{T}^{MN}} A(q)_{i_1i_2}A(q)_{i_2i_3}\ldots A(q)_{i_pi_1}\\ &= \frac{1}{MN}\int_{\mathbb{T}^{MN}} Tr(A(q)^p)dq\\ &= \frac{1}{N}\int_{\mathbb{T}^{MN}} tr(A(q)^p)dq\end{aligned}$$

But this gives the formula in the statement, and we are done. □

In general, the moments of the Gram matrix A are given by a quite complicated formula, and we cannot expect to have a refinement of Theorem 16.17, with A replaced by a plain, non-matricial random variable, say over a compact abelian group. However, this kind of simplification does appear at $M=2$. As a first remark, at $M=2$ we have:

Proposition 16.18. *For $F_2\otimes_Q F_H$, with $Q\in M_{2\times N}(\mathbb{T})$ generic, we have*

$$N\int\left(\frac{\chi}{N}\right)^p=\int_{\mathbb{T}^N}\sum_{k\geq0}\binom{p}{2k}\left|\frac{a_1+\ldots+a_N}{N}\right|^{2k}da$$

where the integral on the right is with respect to the uniform measure on $\mathbb{T}^N$.

Proof. Consider the following quantity, from the proof of Theorem 16.17:

$$\Phi(q)=\sum_{i_1\ldots i_p}\sum_{d_1\ldots d_p}\frac{q_{i_1d_1}\ldots q_{i_pd_p}}{q_{i_1d_p}\ldots q_{i_pd_{p-1}}}$$

We can "half-dephase" the matrix $q\in M_{2\times N}(\mathbb{T})$ if we want to, as follows:

$$q=\begin{pmatrix}1&\ldots&1\\ a_1&\ldots&a_N\end{pmatrix}$$

Let us compute now the above quantity $\Phi(q)$, in terms of the numbers $a_1,\ldots,a_N$. Our claim is that we have the following formula:

$$\Phi(q)=2\sum_{k\geq0}N^{p-2k}\binom{p}{2k}\left|\sum_i a_i\right|^{2k}$$

Indeed, the $2N^k$ contribution will come from $i=(1\ldots1)$ and $i=(2\ldots2)$, then we will have a $p(p-1)N^{k-2}|\sum_i a_i|^2$ contribution coming from indices of type $i=(2\ldots21\ldots1)$, up to cyclic permutations, then a $2\binom{p}{4}N^{p-4}|\sum_i a_i|^4$ contribution coming from indices of type $i=(2\ldots21\ldots12\ldots21\ldots1)$, and so on. More precisely, in order to find the $N^{p-2k}|\sum_i a_i|^{2k}$ contribution, we have to count the circular configurations consisting of p

numbers $1,2$, such that the 1 values are arranged into k non-empty intervals, and the 2 values are arranged into k non-empty intervals as well. Now by looking at the endpoints of these $2k$ intervals, we have $2\binom{p}{2k}$ choices, and this gives the above formula.

Now by integrating, this gives the formula in the statement. $\square$

Observe now that the integrals in Proposition 16.18 can be computed as follows:

$$\begin{aligned}\int_{\mathbb{T}^N}|a_1+\ldots+a_N|^{2k}da &= \int_{\mathbb{T}^N}\sum_{i_1\ldots i_k}\sum_{j_1\ldots j_k}\frac{a_{i_1}\ldots a_{i_k}}{a_{j_1}\ldots a_{j_k}}da\\ &= \#\left\{i_1\ldots i_k,j_1\ldots j_k\Big|[i_1,\ldots,i_k]=[j_1,\ldots,j_k]\right\}\\ &= \sum_{k=\sum r_i}\binom{k}{r_1,\ldots,r_N}^2\end{aligned}$$

We obtain in this way the following "blowup" result, for our measure:

Proposition 16.19. *For $F_2\otimes_Q F_H$, with $Q\in M_{2\times N}(\mathbb{T})$ generic, we have*

$$\mu=\left(1-\frac{1}{N}\right)\delta_0+\frac{1}{2N}\left(\Psi^+_*\varepsilon+\Psi^-_*\varepsilon\right)$$

where ε is the uniform measure on $\mathbb{T}^N$, and where the blowup function is:

$$\Psi^\pm(a)=N\pm\left|\sum_i a_i\right|$$

Proof. We use the formula found in Proposition 16.18 above, along with the following standard identity, coming from the Taylor formula:

$$\sum_{k\geq 0}\binom{p}{2k}x^{2k}=\frac{(1+x)^p+(1-x)^p}{2}$$

By using this identity, Proposition 16.18 reformulates as follows:

$$N\int\left(\frac{\chi}{N}\right)^p=\frac{1}{2}\int_{\mathbb{T}^N}\left(1+\left|\frac{\sum_i a_i}{N}\right|\right)^p+\left(1-\left|\frac{\sum_i a_i}{N}\right|\right)^p da$$

Now by multiplying by N^{p-1}, we obtain the following formula:

$$\int\chi^k=\frac{1}{2N}\int_{\mathbb{T}^N}\left(N+\left|\sum_i a_i\right|\right)^p+\left(N-\left|\sum_i a_i\right|\right)^p da$$

But this gives the formula in the statement, and we are done. $\square$

We can further improve the above result, by reducing the maps $\Psi^\pm$ appearing there to a single one, and we are led to the following statement:

Theorem 16.20. *For $F_2 \otimes_Q F_H$, with $Q \in M_{2\times N}(\mathbb{T})$ generic, we have*

$$\mu = \left(1 - \frac{1}{N}\right)\delta_0 + \frac{1}{N}\Phi_*\varepsilon$$

where ε is the uniform measure on $\mathbb{Z}_2 \times \mathbb{T}^N$, and where the blowup map is:

$$\Phi(e,a) = N + e\left|\sum_i a_i\right|$$

Proof. This is clear indeed from Proposition 16.19 above. □

Let us go back now to the general case, where $M, N \in \mathbb{N}$ are arbitrary. The problem that we would like to solve is that of finding the good regime, $M = f(K), N = g(K), K \to \infty$, where the measure in Theorem 16.16 converges, after some suitable manipulations.

We denote by $NC(p)$ the set of noncrossing partitions of $\{1,\ldots,p\}$, and for $\pi \in P(p)$ we denote by $|\pi| \in \{1,\ldots,p\}$ the number of blocks. We will need:

Proposition 16.21. *With $M = \alpha K, N = \beta K$, $K \to \infty$ we have:*

$$\frac{c_p}{K^{p-1}} \simeq \sum_{r=1}^{p} \#\left\{\pi \in NC(p)\Big||\pi| = r\right\}\alpha^{r-1}\beta^{p-r}$$

In particular, with $\alpha = \beta$ we have:

$$c_p \simeq \frac{1}{p+1}\binom{2p}{p}(\alpha K)^{p-1}$$

Proof. We use the combinatorial formula in Theorem 16.16 above. Our claim is that, with $\pi = \ker(i_1,\ldots,i_p)$, the corresponding contribution to c_p is:

$$C_\pi \simeq \begin{cases} \alpha^{|\pi|-1}\beta^{p-|\pi|}K^{p-1} & \text{if } \pi \in NC(p) \\ O(K^{p-2}) & \text{if } \pi \notin NC(p) \end{cases}$$

As a first observation, the number of choices for a multi-index $(i_1,\ldots,i_p) \in X^p$ satisfying $\ker i = \pi$ is:

$$M(M-1)\ldots(M-|\pi|+1) \simeq M^{|\pi|}$$

Thus, we have the following estimate:

$$C_\pi \simeq M^{|\pi|-1}N^{-1}\#\left\{d_1,\ldots,d_p \in Y\Big|[d_\alpha|\alpha \in b] = [d_{\alpha-1}|\alpha \in b], \forall b \in \pi\right\}$$

Consider now the following partition:

$$\sigma = \ker d$$

The contribution of σ to the above quantity C_π is then given by:

$$\Delta(\pi,\sigma)N(N-1)\ldots(N-|\sigma|+1) \simeq \Delta(\pi,\sigma)N^{|\sigma|}$$

Here the quantities on the right are as follows:

$$\Delta(\pi,\sigma)=\begin{cases}1 & \text{if } |b\cap c|=|(b-1)\cap c|, \forall b\in\pi,\forall c\in\sigma\\ 0 & \text{otherwise}\end{cases}$$

We use now the standard fact that for $\pi,\sigma\in P(p)$ satisfying $\Delta(\pi,\sigma)=1$ we have:

$$|\pi|+|\sigma|\leq p+1$$

In addition, the equality case is well-known to happen when $\pi,\sigma\in NC(p)$ are inverse to each other, via Kreweras complementation. This shows that for $\pi\notin NC(p)$ we have $C_\pi=O(K^{p-2})$, and that for $\pi\in NC(p)$ we have:

$$\begin{aligned}C_\pi &\simeq M^{|\pi|-1}N^{-1}N^{p-|\pi|-1}\\ &= \alpha^{|\pi|-1}\beta^{p-|\pi|}K^{p-1}\end{aligned}$$

Thus, we have obtained the result. □

We denote by D the dilation operation, $D_r(law(X))=law(rX)$. We have:

Theorem 16.22. *With $M=\alpha K, N=\beta K$, $K\to\infty$ we have:*

$$\mu=\left(1-\frac{1}{\alpha\beta K^2}\right)\delta_0+\frac{1}{\alpha\beta K^2}D_{\frac{1}{\beta K}}(\pi_{\alpha/\beta})$$

In particular with $\alpha=\beta$ we have:

$$\mu=\left(1-\frac{1}{\alpha^2 K^2}\right)\delta_0+\frac{1}{\alpha^2 K^2}D_{\frac{1}{\alpha K}}(\pi_1)$$

Proof. At $\alpha=\beta$, this follows from Proposition 16.21. In general now, we have:

$$\begin{aligned}\frac{c_p}{K^{p-1}} &\simeq \sum_{\pi\in NC(p)}\alpha^{|\pi|-1}\beta^{p-|\pi|}\\ &= \frac{\beta^p}{\alpha}\sum_{\pi\in NC(p)}\left(\frac{\alpha}{\beta}\right)^{|\pi|}\\ &= \frac{\beta^p}{\alpha}\int x^p d\pi_{\alpha/\beta}(x)\end{aligned}$$

When $\alpha\geq\beta$, where $d\pi_{\alpha/\beta}(x)=\varphi_{\alpha/\beta}(x)dx$ is continuous, we obtain:

$$\begin{aligned}c_p &= \frac{1}{\alpha K}\int(\beta Kx)^p\varphi_{\alpha/\beta}(x)dx\\ &= \frac{1}{\alpha\beta K^2}\int x^p\varphi_{\alpha/\beta}\left(\frac{x}{\beta K}\right)dx\end{aligned}$$

But this gives the formula in the statement. When $\alpha\leq\beta$ the computation is similar, with a Dirac mass as 0 dissapearing and reappearing, and gives the same result. □

Let us state as well an explicit result, regarding densities:

Theorem 16.23. *With $M=\alpha K,N=\beta K,\ K\to\infty$ we have:*

$$\mu=\left(1-\frac{1}{\alpha\beta K^2}\right)\delta_0+\frac{1}{\alpha\beta K^2}\cdot\frac{\sqrt{4\alpha\beta K^2-(x-\alpha K-\beta K)^2}}{2\pi x}\,dx$$

In particular with $\alpha=\beta$ we have:

$$\mu=\left(1-\frac{1}{\alpha^2K^2}\right)\delta_0+\frac{1}{\alpha^2K^2}\cdot\frac{\sqrt{\frac{4\alpha K}{x}-1}}{2\pi}$$

Proof. According to the formula for the density of the free Poisson law, the density of the continuous part $D_{\frac{1}{\beta K}}(\pi_{\alpha/\beta})$ is indeed given by:

$$\frac{\sqrt{4\frac{\alpha}{\beta}-(\frac{x}{\beta K}-1-\frac{\alpha}{\beta})^2}}{2\pi\cdot\frac{x}{\beta K}}=\frac{\sqrt{4\alpha\beta K^2-(x-\alpha K-\beta K)^2}}{2\pi x}$$

With $\alpha=\beta$ now, we obtain the second formula in the statement, and we are done. $\square$

Observe that at $\alpha=\beta=1$, where $M=N=K\to\infty$, the above measure is:

$$\mu=\left(1-\frac{1}{K^2}\right)\delta_0+\frac{1}{K^2}D_{\frac{1}{K}}(\pi_1)$$

This measure is supported by $[0,4K]$. On the other hand, since the groups $\Gamma_{M,N}$ are all amenable, the corresponding measures are supported on $[0,MN]$, and so on $[0,K^2]$ in the $M=N=K$ situation. The fact that we do not have a convergence of supports is not surprising, because our convergence is in moments.

There are many interesting questions that are still open, regarding the computation of the spectral measure in the case where the parameter matrix Q is not generic, and also regarding the computation for the deformations of the generalized Fourier matrices, which are not necessarily of Diţă type. We refer here to [12], [15], [41] and related papers.

References

[1] S. Agaian, Hadamard matrices and their applications, Springer (1985).

[2] A. Álvarez, J.A. Armario, M.D. Frau, E. Martin and A. Osuna, Error correcting codes from quasi-Hadamard matrices, *Lecture Notes in Comput. Sci.* **4547** (2007), 294–302.

[3] K.T. Arasu, W. de Launey and S.L. Ma, On circulant complex Hadamard matrices, *Des. Codes Cryptogr.* **25** (2002), 123–142.

[4] J. Avan, T. Fonseca, L. Frappat, P. Kulish, E. Ragoucy and G. Rollet, Temperley-Lieb R-matrices from generalized Hadamard matrices, *Theor. Math. Phys.* **178** (2014), 223–240.

[5] J. Backelin, Square multiples n give infinitely many cyclic n-roots (1989).

[6] T. Banica, Symmetries of a generic coaction, *Math. Ann.* **314** (1999), 763–780.

[7] T. Banica, Compact Kac algebras and commuting squares, *J. Funct. Anal.* **176** (2000), 80–99.

[8] T. Banica, The defect of generalized Fourier matrices, *Linear Algebra Appl.* **438** (2013), 3667–3688.

[9] T. Banica, First order deformations of the Fourier matrix, *J. Math. Phys.* **55** (2014), 1–22.

[10] T. Banica, Counting results for thin Butson matrices, *Electron. J. Combin.* **21** (2014), 1–14.

[11] T. Banica, The glow of Fourier matrices: universality and fluctuations, *Oper. Matrices* **9** (2015), 457–474.

[12] T. Banica, Deformed Fourier models with formal parameters, *Studia Math.* **239** (2017), 201–224.

[13] T. Banica, Complex Hadamard matrices with noncommutative entries, *Ann. Funct. Anal.* **9** (2018), 354–368.

[14] T. Banica and J. Bichon, Hopf images and inner faithful representations, *Glasg. Math. J.* **52** (2010), 677–703.

[15] T. Banica and J. Bichon, Random walk questions for linear quantum groups, *Int. Math. Res. Not.* **24** (2015), 13406–13436.

[16] T. Banica, J. Bichon and B. Collins, The hyperoctahedral quantum group, *J. Ramanujan Math. Soc.* **22** (2007), 345–384.

[17] T. Banica, J. Bichon and J.-M. Schlenker, Representations of quantum permutation algebras, *J. Funct. Anal.* **257** (2009), 2864–2910.

[18] T. Banica and B. Collins, Integration over quantum permutation groups, *J. Funct. Anal.* **242** (2007), 641–657.

[19] T. Banica, B. Collins and J.-M. Schlenker, On orthogonal matrices maximizing the 1-norm, *Indiana Univ. Math. J.* **59** (2010), 839–856.

[20] T. Banica, B. Collins and J.-M. Schlenker, On polynomial integrals over the orthogonal group, *J. Combin. Theory Ser. A* **118** (2011), 778–795.

[21] T. Banica and S. Curran, Decomposition results for Gram matrix determinants, *J. Math. Phys.* **51** (2010), 1–14.

[22] T. Banica, U. Franz and A. Skalski, Idempotent states and the inner linearity property, *Bull. Pol. Acad. Sci. Math.* **60** (2012), 123–132.

[23] T. Banica and I. Nechita, Almost Hadamard matrices: the case of arbitrary exponents, *Discrete Appl. Math.* **161** (2013), 2367–2379.

[24] T. Banica and I. Nechita, Flat matrix models for quantum permutation groups, *Adv. Appl. Math.* **83** (2017), 24–46.

[25] T. Banica and I. Nechita, Almost Hadamard matrices with complex entries, *Adv. Oper. Theory* **3** (2018), 149–189.

[26] T. Banica, I. Nechita and J.-M. Schlenker, Analytic aspects of the circulant Hadamard conjecture, *Ann. Math. Blaise Pascal* **21** (2014), 25–59.

[27] T. Banica, I. Nechita and J.-M. Schlenker, Submatrices of Hadamard matrices: complementation results, *Electron. J. Linear Algebra* **27** (2014), 197–212.

[28] T. Banica, I. Nechita and K. Życzkowski, Almost Hadamard matrices: general theory and examples, *Open Syst. Inf. Dyn.* **19** (2012), 1–26.

[29] T. Banica and R. Nicoara, Quantum groups and Hadamard matrices, *Panamer. Math. J.* **17** (2007), 1–24.

[30] T. Banica, D. Özteke and L. Pittau, Isolated partial Hadamard matrices, and related topics, *Open Syst. Inf. Dyn.* **25** (2018), 1–27.

[31] T. Banica and A. Skalski, The quantum algebra of partial Hadamard matrices, *Linear Algebra Appl.* **469** (2015), 364–380.

[32] T. Banica and R. Speicher, Liberation of orthogonal Lie groups, *Adv. Math.* **222** (2009), 1461–1501.

[33] N. Barros e Sá and I. Bengtsson, Families of complex Hadamard matrices, *Linear Algebra Appl.* **438** (2013), 2929–2957.

[34] L.D. Baumert, S.W. Golomb and M. Hall, Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.* **68** (1962), 237–238.

[35] K. Beauchamp and R. Nicoara, Orthogonal maximal abelian $*$-subalgebras of the 6×6 matrices, *Linear Algebra Appl.* **428** (2008), 1833–1853.

[36] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej and K. Życzkowski, Mutually unbiased bases and Hadamard matrices of order six, *J. Math. Phys.* **48** (2007), 1–33.

[37] I. Bengtsson, Å. Ericsson, M. Kuś, W. Tadej, and K. Życzkowski, Birkhoff's polytope and unistochastic matrices, N=3 and N=4, *Comm. Math. Phys.* **259** (2005), 307–324.

[38] H. Bercovici and V. Pata, Stable laws and domains of attraction in free probability theory, *Ann. of Math.* **149** (1999), 1023–1060.

[39] J. Bichon, Free wreath product by the quantum permutation group, *Alg. Rep. Theory* **7** (2004), 343–362.

[40] J. Bichon, Algebraic quantum permutation groups, *Asian-Eur. J. Math.* **1** (2008), 1–13.

[41] J. Bichon, Quotients and Hopf images of a smash coproduct, *Tsukuba J. Math.* **39** (2015), 285–310.

[42] P. Biran, M. Entov and L. Polterovich, Calabi quasimorphisms for the symplectic ball, *Commun. Contemp. Math.* **6** (2004), 793–802.

[43] G. Björck, Functions of modulus 1 on Z_n whose Fourier transforms have constant modulus, and cyclic n-roots, *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.* **315** (1990), 131–140.

[44] G. Björck and R. Fröberg, A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots, *J. Symbolic Comput.* **12** (1991), 329–336.

[45] G. Björck and U. Haagerup, All cyclic p-roots of index 3 found by symmetry-preserving calculations (2008).

[46] R. Burstein, Group-type subfactors and Hadamard matrices, *Trans. Amer. Math. Soc.* **367** (2015), 6783–6807.

[47] A.T. Butson, Generalized Hadamard matrices, *Proc. Amer. Math. Soc.* **13** (1962), 894–898.

[48] C.-H. Cho, Holomorphic discs, spin structures, and Floer cohomology of the Clifford torus, *Int. Math. Res. Not.* **35** (2004), 1803–1843.

[49] C.J. Colbourn and J.H. Dinitz, Handbook of combinatorial designs, CRC Press (2007).

[50] B. Collins and P. Śniady, Integration with respect to the Haar measure on unitary, orthogonal and symplectic groups, *Comm. Math. Phys.* **264** (2006), 773–795.

[51] R. Craigen, The range of the determinant function on the set of $n \times n$ (0,1)-matrices, *J. Combin. Math. Combin. Comput.* **8** (1990) 161–171.

[52] R. Craigen, G. Faucher, R. Low and T. Wares, Circulant partial Hadamard matrices, *Linear Algebra Appl.* **439** (2013), 3307–3317.

[53] R. Craigen and H. Kharaghani, On the nonexistence of Hermitian circulant complex Hadamard matrices, *Australas. J. Combin.* **7** (1993), 225–227.

[54] W. de Launey, On the non-existence of generalized weighing matrices, *Ars Combin.* **17** (1984), 117–132.

[55] W. de Launey and J.E. Dawson, An asymptotic result on the existence of generalised Hadamard matrices, *J. Combin. Theory Ser. A* **65** (1994), 158–163.

[56] W. de Launey, D.L. Flannery and K.J. Horadam, Cocyclic Hadamard matrices and difference sets, *Discrete Appl. Math.* **102** (2000), 47–61.

[57] W. de Launey and D.M. Gordon, A comment on the Hadamard conjecture, *J. Combin. Theory Ser. A* **95** (2001), 180–184.

[58] W. de Launey and D.A. Levin, $(1,-1)$-matrices with near-extremal properties, *SIAM J. Discrete Math.* **23** (2009), 1422–1440.

[59] W. de Launey and D.A. Levin, A Fourier-analytic approach to counting partial Hadamard matrices, *Cryptogr. Commun.* **2** (2010), 307–334.

[60] P. Di Francesco, Meander determinants, *Comm. Math. Phys.* **191** (1998), 543–583.

[61] P. Diaconis and M. Shahshahani, On the eigenvalues of random matrices, *J. Applied Probab.* **31** (1994), 49–62.

[62] P. Diţă, Some results on the parametrization of complex Hadamard matrices, *J. Phys. A* **37** (2004), 5355–5374.

[63] P. Diţă, Separation of unistochastic matrices from the double stochastic ones: recovery of a 3×3 unitary matrix from experimental data, *J. Math. Phys.* **47** (2006), 1–24.

[64] T. Durt, B.-G. Englert, I. Bengtsson and K. Życzkowski, On mutually unbiased bases, *Int. J. Quantum Inf.* **8** (2010), 535–640.

[65] L. Faddeev, Instructive history of the quantum inverse scattering method, *Acta Appl. Math.* **39** (1995), 69–84.

[66] J.-C. Faugère, Finding all the solutions of Cyclic 9 using Gröbner basis techniques, *Lecture Notes Ser. Comput.* **9** (2001), 1–12.

[67] P.C. Fishburn and N.J.A. Sloane, The solution to Berlekamp's switching game, *Discrete Math.* **74** (1989), 263–290.

[68] R.L. Graham and N.J.A. Sloane, On the covering radius of codes, *IEEE Trans. Inform. Theory* **31** (1985), 385–401.

[69] U. Haagerup, Orthogonal maximal abelian $*$-subalgebras of the $n\times n$ matrices and cyclic n-roots, in "Operator algebras and quantum field theory", International Press (1997), 296–323.

[70] U. Haagerup, Cyclic p-roots of prime lengths p and related complex Hadamard matrices (2008).

[71] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. Sci. Math.* **2** (1893), 240–246.

[72] M. Hall, Integral matrices A for which $AA^T=mI$, in "Number Theory and Algebra", Academic Press (1977), 119–134.

[73] G. Hiranandani and J.-M. Schlenker, Small circulant complex Hadamard matrices of Butson type, *European J. Combin.* **51** (2016), 306–314.

[74] K.J. Horadam, Hadamard matrices and their applications, Princeton Univ. Press (2007).

[75] M. Idel and M.M. Wolf, Sinkhorn normal form for unitary matrices, *Linear Algebra Appl.* **471** (2015), 76–84.

[76] N. Ito, Hadamard Graphs I, *Graphs Combin.* **1** (1985), 57–64.

[77] J. Jedwab and S. Lloyd, A note on the nonexistence of Barker sequences, *Des. Codes Cryptogr.* **2** (1992), 93–97.

[78] V.F.R. Jones, Index for subfactors, *Invent. Math.* **72** (1983), 1–25.

[79] V.F.R. Jones, On knot invariants related to some statistical mechanical models, *Pacific J. Math.* **137** (1989), 311–334.
[80] V.F.R. Jones, The Potts model and the symmetric group, in "Subfactors, Kyuzeso 1993" (1994), 259–267.
[81] V.F.R. Jones, Planar algebras I, preprint 1999.
[82] V.F.R. Jones, The annular structure of subfactors, *Monogr. Enseign. Math.* **38** (2001), 401–463.
[83] A. Karabegov, The reconstruction of a unitary matrix from the moduli of its elements and symbols on a finite phase space (1989).
[84] B.R. Karlsson, Three-parameter complex Hadamard matrices of order 6, *Linear Algebra Appl.* **434** (2011), 247–258.
[85] H. Kharaghani and J. Seberry, The excess of complex Hadamard matrices, *Graphs Combin.* **9** (1993), 47–56.
[86] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, *J. Combin. Des.* **13** (2005), 435–440.
[87] H. Kimura, New Hadamard matrix of order 24, *Graphs Combin.* **5** (1989), 235–242.
[88] C. Koukouvinos, M. Mitrouli and J. Seberry, An algorithm to find formulae and values of minors for Hadamard matrices, *Linear Algebra Appl.* **330** (2001), 129–147.
[89] C. Koukouvinos, M. Mitrouli and J. Seberry, An algorithm to find formulae and values of minors for Hadamard matrices. II, *Linear Algebra Appl.* **371** (2003), 111–124.
[90] T.Y. Lam and K.H. Leung, On vanishing sums of roots of unity, *J. Algebra* **224** (2000), 91–109.
[91] K.H. Leung and B. Schmidt, New restrictions on possible orders of circulant Hadamard matrices, *Des. Codes Cryptogr.* **64** (2012), 143–151.
[92] M. Lupini, L. Mančinska and D.E. Roberson, Nonlocal games and quantum permutation groups, *J. Funct. Anal.* **279** (2020), 1–39.
[93] S. Malacarne, Woronowicz's Tannaka-Krein duality and free orthogonal quantum groups, *Math. Scand.* **122** (2018), 151–160.
[94] V.A. Marchenko and L.A. Pastur, Distribution of eigenvalues in certain sets of random matrices, *Mat. Sb.* **72** (1967), 507–536.
[95] M. Matolcsi, J. Réffy and F. Szöllősi, Constructions of complex Hadamard matrices via tiling abelian groups, *Open Syst. Inf. Dyn.* **14** (2007), 247–263.
[96] M. Matolcsi and F. Szöllősi, Towards a classification of 6×6 complex Hadamard matrices, *Open Syst. Inf. Dyn.* **15** (2008), 93–108.
[97] D. McNulty and S. Weigert, Isolated Hadamard matrices from mutually unbiased product bases, *J. Math. Phys.* **53** (2012), 1–21.
[98] M.T. Mohan, On some p-almost Hadamard matrices, *Oper. Matrices* **13** (2019), 253–281.
[99] F.J. Murray and J. von Neumann, On rings of operators, *Ann. of Math.* **37** (1936), 116–229.
[100] F.J. Murray and J. von Neumann, On rings of operators. II, *Trans. Amer. math. Soc.* **41** (1937), 208–248.
[101] F.J. Murray and J. von Neumann, On rings of operators. IV, *Ann. of Math.* **44** (1943), 716–808.
[102] M.G. Neubauer and A.J. Radcliffe, The maximum determinant of ± 1 matrices, *Linear Algebra Appl.* **257** (1997), 289–306.
[103] A. Nica and R. Speicher, Lectures on the combinatorics of free probability, Cambridge Univ. Press (2006).
[104] R. Nicoara, A finiteness result for commuting squares of matrix algebras, *J. Operator Theory* **55** (2006), 295–310.
[105] R. Nicoara and J. White, Analytic deformations of group commuting squares and complex Hadamard matrices, *J. Funct. Anal.* **272** (2017), 3486–3505.

[106] R. Nicoara and J. White, Second order deformations of group commuting squares and Hadamard matrices, *Proce. Amer. Math. Soc.* **148 9** (2020), 3967–3974.

[107] R. Nicoara and J. White, Second order conditions for Hadamard matrices stemming from the Fourier matrix (2020).

[108] A. Ocneanu, Quantum symmetry, differential geometry of finite graphs, and classification of subfactors, Univ. of Tokyo Seminary Notes (1990).

[109] R. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933), 311–320.

[110] K.-H. Park and H.-Y. Song, Quasi-Hadamard matrices, *Proc. ISIT 2010*, Austin, TX (2010).

[111] M. Petrescu, Existence of continuous families of complex Hadamard matrices of certain prime dimensions and related results, Ph.D. Thesis, UCLA (1997).

[112] G. Pólya, Über eine Aufgabe der Wahrscheinlichkeitsrechnung betreffend die Irrfahrt im Strassennetz, *Math. Ann.* **84** (1921), 149–160.

[113] S. Popa, Orthogonal pairs of $*$-subalgebras in finite von Neumann algebras, *J. Operator Theory* **9** (1983), 253–268.

[114] S. Popa, Classification of amenable subfactors of type II, *Acta Math.* **172** (1994), 163–255.

[115] L.B. Richmond and J. Shallit, Counting abelian squares, *Electron. J. Combin.* **16** (2009), 1–9.

[116] R. Roth and K. Viswanathan, On the hardness of decoding the Gale-Berlekamp code, *IEEE Trans. Inform. Theory* **54** (2008), 1050–1060.

[117] H.J. Ryser, Combinatorial mathematics, Wiley (1963).

[118] B. Schmidt, Cyclotomic integers and finite geometry, *J. Amer. Math. Soc.* **12** (1999), 929–952.

[119] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, Wiley (1992).

[120] F.R. Sharpe, The maximum value of a determinant, *Bull. Amer. Math. Soc.* **14** (1907), 121–123.

[121] P.M. Sołtan, Quantum families of maps and quantum semigroups on finite quantum spaces, *J. Geom. Phys.* **59** (2009), 354–368.

[122] P.M. Sołtan, Quantum semigroups from synchronous games, *J. Math. Phys.* **60** (2019), 1–9.

[123] D.R. Stinson, Combinatorial designs: constructions and analysis, Springer-Verlag (2006).

[124] J.J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers, *Phil. Mag.* **34** (1867), 461–475.

[125] F. Szöllősi, Parametrizing complex Hadamard matrices, *European J. Combin.* **29** (2008), 1219–1234.

[126] F. Szöllősi, A two-parameter family of complex Hadamard matrices of order 6 induced by hypocycloids, *Proc. Amer. Math. Soc.* **138** (2010), 921–928.

[127] F. Szöllősi, Exotic complex Hadamard matrices and their equivalence, *Cryptogr. Commun.* **2** (2010), 187–198.

[128] W. Tadej, Defect of a Kronecker product of unitary matrices, *Linear Algebra Appl.* **436** (2012), 1924–1959.

[129] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, *Open Syst. Inf. Dyn.* **13** (2006), 133–177.

[130] W. Tadej and K. Życzkowski, Defect of a unitary matrix, *Linear Algebra Appl.* **429** (2008), 447–481.

[131] T. Tao, Fuglede's conjecture is false in 5 and higher dimensions, *Math. Res. Lett.* **11** (2004), 251–258.

[132] T. Tao, An uncertainty principle for cyclic groups of prime order, *Math. Res. Lett.* **12** (2005), 121–127.

[133] T. Tao and V. Vu, On random ± 1 matrices: singularity and determinant, *Random Structures Algorithms* **28** (2006), 1–23.

[134] T. Tao and V. Vu, On the singularity probability of random Bernoulli matrices, *J. Amer. Math. Soc.* **20** (2007), 603–628.

[135] N.H. Temperley and E.H. Lieb, Relations between the "percolation" and "colouring" problem and other graph-theoretical problems associated with regular planar lattices: some exact results for the "percolation" problem, *Proc. Roy. Soc. London* **322** (1971), 251–280.

[136] R.J. Turyn, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.

[137] E. Verheiden, Integral and rational completions of combinatorial matrices, *J. Combin. Theory Ser. A* **25** (1978) 267–276.

[138] D.V. Voiculescu, Addition of certain noncommuting random variables, *J. Funct. Anal.* **66** (1986), 323–346.

[139] D.V. Voiculescu, Multiplication of certain noncommuting random variables, *J. Operator Theory* **18** (1987), 223–235.

[140] D.V. Voiculescu, K.J. Dykema and A. Nica, Free random variables, AMS (1992).

[141] J. von Neumann, On rings of operators. III, *Ann. of Math.* **41** (1940), 94–161.

[142] S. Wang, Quantum symmetry groups of finite spaces, *Comm. Math. Phys.* **195** (1998), 195–211.

[143] S. Wang, L_p-improving convolution operators on finite quantum groups, *Indiana Univ. Math. J.* **65** (2016), 1609–1637.

[144] A. Wassermann, Coactions and Yang-Baxter equations for ergodic actions and subfactors, *London Math. Soc. Lect. Notes* **136** (1988), 203–236.

[145] D. Weingarten, Asymptotic behavior of group integrals in the limit of infinite rank, *J. Math. Phys.* **19** (1978), 999–1001.

[146] R.F. Werner, All teleportation and dense coding schemes, *J. Phys. A* **34** (2001), 7081–7094.

[147] J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65–81.

[148] A. Winterhof, On the non-existence of generalized Hadamard matrices, *J. Statist. Plann. Inference* **84** (2000), 337–342.

[149] S.L. Woronowicz, Compact matrix pseudogroups, *Comm. Math. Phys.* **111** (1987), 613–665.

[150] S.L. Woronowicz, Tannaka-Krein duality for compact matrix pseudogroups. Twisted SU(N) groups, *Invent. Math.* **93** (1988), 35–76.

T.B.: Department of Mathematics, University of Cergy-Pontoise, F-95000 Cergy-Pontoise, France. teo.banica@gmail.com