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

INTRODUCTION

A complex Hadamard matrix is a square matrix $H \in M_N(\mathbb{C})$ whose entries belong to the unit circle in the complex plane, $H_{ij} \in \mathbb{T}$, and whose rows are pairwise orthogonal with respect to the usual scalar product of $\mathbb{C}^N$, given by $< x, y >= \sum_i x_i \bar{y}_i$.

2010 *Mathematics Subject Classification.* 15B10.

Key words and phrases. Hadamard matrix, Fourier matrix.

The orthogonality condition tells us that the rescaled matrix $U = H/\sqrt{N}$ must be unitary. Thus, these matrices form a real algebraic manifold, given by:

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

The basic example is the Fourier matrix, $F_N = (w^{ij})$ with $w = e^{2\pi i/N}$. In standard matrix form, and with indices $i, j = 0, 1, \ldots, N-1$, this matrix is as follows:

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

More generally, we have as example the Fourier coupling of any finite abelian group G, regarded via the isomorphism $G \simeq \widehat{G}$ as a square matrix, $F_G \in M_G(\mathbb{C})$:

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

Observe that for the cyclic group $G = \mathbb{Z}_N$ we obtain in this way the above standard Fourier matrix F_N. In general, we obtain a tensor product of Fourier matrices F_N.

There are many other examples of such matrices, for the most coming from various combinatorial constructions, basically involving design theory, and roots of unity. In addition, there are several deformation procedures for such matrices, leading to some more complicated constructions as well, or real algebraic geometry flavor.

In general, the complex Hadamard matrices can be thought of as being "generalized Fourier matrices", of somewhat exotic type. Due to their generalized Fourier nature, these matrices appear in a wide array of questions in mathematics and physics:

1. Operator algebras. One important concept in the theory of von Neumann algebras is that of maximal abelian subalgebra (MASA). In the finite case, where the algebra has a trace, one can talk about pairs of orthogonal MASA. In the simplest case, 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.

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 factor R, whose computation a key problem.

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. As a basic example here, the Fourier matrix F_G produces in this way the group G itself. In general, the above-mentioned subfactor can be recovered from G, whose computation is a key problem.

4. Lattice models. According to the work of Jones, the combinatorics of the subfactor associated to an Hadamard matrix $H \in M_N(\mathbb{C})$, which by the above can be recovered from the representation theory of the associated quantum permutation group $G \subset S_N^+$, can be thought of as being the combinatorics of a "spin model", in the context of link invariants, or of statistical mechanics, in an abstract, mathematical sense.

From a more applied point of view, the Hadamard matrices can be used in order to construct mutually unbiased bases (MUB) and other useful objects, which can help in connection with quantum information theory, and other quantum physics questions.

All this is quite recent, basically going back to the 00s. Regarding the known facts about the Hadamard matrices, most of them are in fact of purely mathematical nature. There are indeed many techniques that can be applied, leading to various results:

1. Algebra. In the real case, $H \in M_N(\pm 1)$, the study of such matrices goes back to the beginning of the 20th century, and is quite advanced. The main problems, however, namely the Hadamard conjecture (HC) and the circulant Hadamard conjecture (CHC) are not solved yet, with no efficient idea of approach in sight. Part of the real matrix techniques apply quite well to the root of unity case, $H \in M_N(\mathbb{Z}_s)$, with $s < \infty$.

2. Geometry. As already explained above, the $N \times N$ complex Hadamard matrices form a real algebraic manifold, $X_N = M_N(\mathbb{T}) \cap \sqrt{N} U_N$. This manifold is highly singular, but several interesting geometric results about it have been obtained, notably about the general structure of the singularity at a given point $H \in X_N$, about the neighborhood of the Fourier matrices F_G, and about the various isolated points as well.

3. Analysis. One interesting point of view on the Hadamard matrices, real or complex, comes from the fact that these are precisely the rescaled versions, $H = \sqrt{N} U$, of the matrices which maximize the 1-norm $||U||_1 = \sum_{ij} |U_{ij}|$ on O_N, U_N respectively. When looking more generally at the local maximizers of the 1-norm, one is led into a notion of "almost Hadamard matrices", having interesting algebraic and analytic aspects.

4. Probability. Another speculative approach, this time probabilistic, is by playing a Gale-Berlekamp type game with the matrix, in the hope that the invariants which are obtained in this way are related to the various geometric and quantum algebraic invariants, which are hard to compute. All this is related to the subtle fact that any unitary matrix, and so any complex Hadamard matrix as well, can be put in bistochastic form.

Our aim here is to survey this material, theory and applications. Organizing all this is 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.

The present text is organized in 4 parts, as follows:

(1) Sections 1-3 contain basic definitions and various algebraic results.
(2) Sections 4-6 deal with differential and algebraic geometric aspects.
(3) Sections 7-9 are concerned with various analytic considerations.
(4) Sections 10-12 deal with various mathematical physics aspects.

There are of course many aspects of the theory which are missing from our presentation, but we will provide of course some information here, comments and references.

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 [32], [51], [52].

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 are interested here 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 [85], 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 $\mathbb{R}^N$.

As a first observation, we do not really need real numbers in order to talk about the Hadamard matrices, because the orthogonality condition tells us that, when comparing two rows, the number of matchings should equal the number of mismatchings. 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, 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 a first result:

Proposition 1.2. *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. Let $H \in M_N(\pm 1)$. Since the rows of the rescaled matrix $U = H/\sqrt{N}$ have norm 1, with respect to the usual scalar product on $\mathbb{R}^N$, we conclude that H is Hadamard precisely when U belongs to the orthogonal group O_N, and so when $H \in Y_N$, as claimed. □

As an interesting consequence of the above result, which is not exactly obvious when using the design theory approach, we have the following result:

Proposition 1.3. *Let* $H \in M_N(\pm 1)$ *be an Hadamard matrix.*

1. *The columns of* H *must be pairwise orthogonal.*
2. *The transpose matrix* $H^t \in M_N(\pm 1)$ *is Hadamard as well.*

Proof. Since the orthogonal group O_N is stable under transposition, so is the set Y_N constructed in Proposition 1.2, and this gives both the assertions. □

Let us study now the examples. There are many such matrices, and in order to cut a bit from the complexity, we can use the following notions:

Definition 1.4. *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.*

Also, we say that H is dephased when its first row and column consist of 1 entries.

Observe that we do not include the transposition operation $H \to H^t$ in our list of allowed operations. This is because Proposition 1.3 above, while looking quite elementary, rests however on a deep linear algebra fact, namely that the transpose of an orthogonal matrix is orthogonal as well, and this can produce complications later on.

Regarding the equivalence, there is of course a certain group G acting there, made of two copies of S_N, one for the rows and one for the columns, and of two copies of $\mathbb{Z}_2^N$, once again one for the rows, and one for the columns. The equivalence classes of the Hadamard matrices are then the orbits of the action $G \curvearrowright Y_N$. It is possible to be a bit more explicit here, with a formula for G and so on, but we will not need this.

As for the dephasing, 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 1.4, namely row and column multiplications by -1.

With these notions in hand, we can formulate our first classification result:

Proposition 1.5. *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. □

At $N = 3$ we cannot have examples, due to the orthogonality condition, which forces N to be even. At $N = 4$ now, we have several examples, as for instance:

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

This matrix is a particular case of the following construction:

Proposition 1.6. *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:*

$$H \otimes K \in M_{MN}(\pm 1) \quad , \quad (H \otimes K)_{ia,jb} = H_{ij} K_{ab}$$

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:

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

As for the second assertion, this follows from this, W_2 being Hadamard. □

Before going further, we should perhaps clarify a bit our tensor product notations. In order to write $H \in M_N(\pm 1)$ 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 formula:

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

As an example, by tensoring W_2 with itself, we obtain the above matrix W_4.

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

Proposition 1.7. *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 $H\in M_4(\pm1)$, 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 $\{a,b,c\}=\{-1,-1,1\}$, and so by permuting the last 3 columns, we can further assume that our matrix is as follows:

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

By orthogonality of the first 2 columns we must have $\{m,p\}=\{-1,1\}$, and so by permuting the last 2 rows, we can further assume 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 from the orthogonality of the rows we obtain $x=y=-1$, and then, with these values of x,y plugged in, 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 forces $N\in2\mathbb N$. The point now is that the case $N=6$ is excluded as well, because we have:

Proposition 1.8. *The size of an Hadamard matrix must be $N\in\{2\}\cup4\mathbb N$.*

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:

$$\begin{aligned}(1\perp2)&\quad:\quad x+y=z+t\\(1\perp3)&\quad:\quad x+z=y+t\\(2\perp3)&\quad:\quad x+t=y+z\end{aligned}$$

The solution of this system being $x = y = z = t$, we conclude that the size of our matrix $N = x + y + z + t$ must be a multiple of 4, as claimed. $\square$

As a consequence, we are led to the study of the Hamadard matrices at:

$$N = 8, 12, 16, 20, 24, \ldots$$

This study can be done either abstractly, via various algebraic methods, or with a computer, and this leads to the conclusion that the number of Hadamard matrices of size $N \in 4\mathbb{N}$ grows with N, and this in a rather exponential fashion.

In particular, we are led in this way into the following statement:

Conjecture 1.9 (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 probably 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. At $N = 8$ we have the Walsh matrix W_8. Thus, the next existence problem comes at $N = 12$. And here, we can use the following key construction, due to Paley [75]:

Theorem 1.10. *Let $q = p^r$ be an odd prime power, define $\chi : \mathbb{F}_q \to \{-1, 0, 1\}$ by $\chi(0) = 0$, $\chi(a) = 1$ if $a = b^2$ for some $b \neq 0$, and $\chi(a) = -1$ otherwise, and finally set $Q_{ab} = \chi(a - b)$. 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:*

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

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:

$$QQ^t=q1-\mathbb{I}\quad,\quad Q\mathbb{I}=\mathbb{I}Q=0$$

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. $\square$

These constructions allow us to get well beyond the Walsh matrix level, and we have the following result:

Theorem 1.11. *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) Since $N - 1$ takes the values $q = 11, 19, 23, 27, 43, 47, 59, 67, 71, 79, 83, 87$, all prime powers, we can indeed 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. □

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

Theorem 1.12. *Assuming that $A, B, C, D \in M_K(\pm 1)$ are circulant, symmetric, pairwise commute and satisfy $A^2 + B^2 + C^2 + D^2 = 4K$, 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. The matrix H can be written as follows, where $1, i, j, k \in M_4(0, 1)$, called the quaternion units, are the matrices describing the positions of the A, B, C, D entries:

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

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

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

Thus, if we further assume that A, B, C, D pairwise commute, and satisfy the condition $A^2 + B^2 + C^2 + D^2 = 4K$, 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 [24], [97]. $\square$

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], [41], [43], [56], [64], [84].

As a conceptual finding on this subject, however, we have the recent theory of the cocyclic Hadamard matrices. The basic definition here is as follows:

Definition 1.13. *A cocycle on a finite group G is a matrix $H \in M_G(\pm 1)$ satisfying:*

$$H_{11} = 1 \quad , \quad H_{gh} H_{gh,k} = H_{g,hk} H_{hk}$$

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, the Walsh matrix $H = W_{2^n}$ is cocyclic, coming from the group $G = \mathbb{Z}_2^n$, with cocycle $H_{gh} = (-1)^{<g,h>}$. As explained in [42], many other known examples of Hadamard matrices are cocyclic, and this leads to the following conjecture:

Conjecture 1.14 (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 serious idea here, at least so far.

One potential way of getting away from these questions is that of looking at various special classes of Hadamard matrices. However, this is not really the case, because passed a few trivialities, the existence of special Hadamard matrices is generally subject to an improvement of the HC, as in the cocyclic case, or to difficult non-existence questions.

Illustrating and quite famous here is the situation in the circulant case. Given a vector $\gamma \in (\pm 1)^N$, one can ask whether the matrix $H \in M_N(\pm 1)$ defined by $H_{ij} = \gamma_{j-i}$ is Hadamard or not. Here is a solution to the problem:

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

More generally, any vector $\gamma \in (\pm 1)^4$ satisfying $\sum \gamma_i = \pm 1$ is a solution to the problem. The following conjecture, going back to [84], states that there are no other solutions:

Conjecture 1.15 (Circulant Hadamard Conjecture (CHC)). *There is no circulant Hadamard matrix of size $N \times N$, for any $N \neq 4$.*

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 γ, the Hadamard matrix condition is simply $|S \cap (S+k)| = |S| - N/4$, 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 [83]:

Conjecture 1.16 (Ryser Conjecture). *Given an integer $N > 4$, there is no set $S \subset \{1, \ldots, N\}$ satisfying the condition*

$$|S \cap (S+k)| = |S| - N/4$$

for any $k \neq 0$, taken modulo N.

There has been a lot of work on this conjecture, starting with [83]. However, as it was the case with the HC, all this leads to complicated combinatorics, design theory, algebra and number theory, and so on, and there is no serious idea here, at least so far.

All this might seem a bit depressing, but there are at least two potential exits from the combinatorial and algebraic theory of Hadamard matrices, namely:

(1) Do analysis. There are many things that can be done here, starting with the Hadamard determinant bound [53], and we will discuss this below. Whether all this can help or not in relation with the HC and CHC remains to be seen, but at least we'll have some fun, and do some interesting mathematics.
(2) Do physics. When allowing the entries of H to be complex numbers, both the HC and the CHC dissapear, because the Fourier matrix $F_N = (w^{ij})$ with $w = e^{2\pi i/N}$ is an example of such matrix at any $N \in \mathbb{N}$, which in addition can be put in circulant form. We will discuss this later, starting from section 2 below.

So, let us step now into analytic questions. The first result here, found in 1893 by Hadamard [53], about 25 years after Sylvester's 1867 founding paper [85], and which actually led to such matrices being called Hadamard, is as follows:

Theorem 1.17. *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. $\square$

The above result is quite interesting, philosophically speaking. Let us recall indeed from Proposition 1.2 that the set formed by the $N\times N$ Hadamard matrices is:

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

Thus, what we have in Theorem 1.17 is an analytic method for locating Y_N inside $M_N(\pm 1)$. This suggests doing many geometric and analytic things, as for instance looking at the maximizers of $|\det(H)|$ at values $N\in\mathbb N$ which are not multiples of 4. These latter matrices are called "quasi-Hadamard", and we refer here to [76].

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 [14], is as follows:

Theorem 1.18. *Given a matrix $U\in O_N$ we have*

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

with equality precisely when $H=U/\sqrt{N}$ is Hadamard.

Proof. We have indeed the following estimate, valid for any $U\in O_N$:

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

The equality case holds when $|U_{ij}|=\sqrt{N}$ for any i,j, which amounts in saying that $H=U/\sqrt{N}$ must satisfy $H\in M_N(\pm 1)$, and so that H must be Hadamard. $\square$

As a first comment here, the above Cauchy-Schwarz estimate can be improved with a Hölder estimate, the conclusion being that the rescaled Hadamard matrices maximize the p-norm on O_N at any $p\in[1,2)$, and minimize it at any $p\in(2,\infty]$. We will discuss this in section 9 below, with full details, directly in the complex case.

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, notably with a notion of "almost Hadamard matrix" at stake. We will be back to this in section 9 below.

Let us discuss now, once again as an introduction to analytic topics, yet another such result. We recall that a matrix $H\in M_N(\mathbb R)$ is called row-stochastic when the sums on the rows are all equal, column-stochastic when the same is true for columns, and bistochastic when this is true for both rows and columns, the common sum being the same.

With this terminology, we have the following well-known result:

Theorem 1.19. *For an Hadamard matrix $H \in M_N(\pm 1)$, 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, $H\xi \sim \xi$ is equivalent to $H^t\xi \sim \xi$, and so H must be bistochastic, as claimed. $\square$

There are many known interesting results on the bistochastic Hadamard matrices, and we will be back to this in section 7 below, directly in the complex setting.

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. Let us start with:

Definition 1.20. *The glow of $H \in M_N(\pm 1)$ is the probability measure $\mu \in \mathcal{P}(\mathbb{Z})$ describing the distribution of the excess, $E = \sum_{ij} H_{ij}$, over the 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:

$$\widetilde{H}_{ij} = a_i b_j H_{ij}$$

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 1.21. *Given a matrix $H \in M_N(\pm 1)$, if we define $\varphi : \mathbb{Z}_2^N \times \mathbb{Z}_2^N \to \mathbb{Z}$ by*

$$\varphi(a, b) = \sum_{ij} a_i b_j H_{ij}$$

then the glow μ 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 1.20 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 [50], [82], and this is where our main motivation for studying it comes from.

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 [9]:

Proposition 1.22. *The glow of a matrix $H \in M_N(\pm 1)$ 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 $\beta_r(c) = \left(\frac{\delta_r + \delta_{-r}}{2}\right)^{*c}$, and $c_r = \#\{r \in |S_1|, \ldots, |S_N|\}$, 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 $S = Hb$, the numbers $S_1, \ldots, S_N$ are the sums on the rows of the matrix $\widetilde{H}_{ij} = H_{ij}a_ib_j$. Thus the glow components are given by:

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

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 1.23. *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. (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 $a+d = b+c$, so $a+d = b+c = \frac{N}{2}$. Now since $N/2$ is even, we conclude that $b = c(2)$, and this 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:

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

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 $H\in M_N(\pm1)$ are orthogonal, the total number of these cases is even, and this finishes the proof. □

Observe that Proposition 1.22 and Proposition 1.23 (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 1.24. *Let $H\in M_N(\pm1)$ 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 1.22:

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

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 1.23 (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:

$$\frac{1}{2}(\mu_{+c}+\mu_{-c})=\frac{1}{2}\left(law(\underbrace{\pm0\ldots\pm0}_{N-x}\underbrace{\pm4\ldots\pm4}_{x})+law(\underbrace{\pm2\ldots\pm2}_{N})\right)$$

Now by using Proposition 1.23 (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 $8\mathbb Z,8\mathbb Z+4$. So, 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 measures μ^{even},μ^{odd} don't have further general algebraic properties. Analytically speaking now, we have:

Theorem 1.25. *The glow moments of $H\in M_N(\pm1)$ 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 variable E/N becomes Gaussian in the $N\to\infty$ limit.

Proof. 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 the variable $E=\sum_{ij}a_ib_jH_{ij}$ are then given by:

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

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:

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

Here $K(\pi)=\sum_{\sigma\in P_{even}(r)}\mu(\pi,\sigma)$, where μ is the Möbius function of $P_{even}(r)$, and, with the convention that $H_1,\ldots,H_N\in\mathbb{Z}_2^N$ are the rows of H:

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

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.

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 [8]. □

We will be back to all this in section 8 below, in the complex matrix setting.

Finally, some interesting analytic results can be obtained by exiting the square matrix setting, and looking at the rectangular matrix case. Let us start with:

Definition 1.26. *A partial Hadamard matrix (PHM) is a matrix*

$$H \in M_{M\times N}(\pm 1)$$

having its rows pairwise orthogonal.

These matrices are quite interesting objects, appearing in connection with various questions in combinatorics. The motivating examples are the Hadamard matrices $H \in M_N(\pm 1)$, and their $M \times N$ submatrices, with $M \leq N$. See [54], [58], [84], [94].

In their paper [44], de Launey and Levin were able to count these matrices, in the asymptotic limit $N \in 4\mathbb{N}$, $N \to \infty$. Their method is based on:

Proposition 1.27. *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 $\mathbb{Z}_2^{\binom{M}{2}}$, 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 $T(e_1) + \ldots + T(e_N) = 0$, and this gives the result. □

As explained in [44] the above probability can be indeed computed, and we have:

Theorem 1.28. *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 1.27 above, we have:

$$P_M = \frac{1}{q^{(M-1)N}}\#\left\{\xi_1, \ldots, \xi_N \in E\Big|\sum_i \xi_i = 0\right\} = \frac{1}{q^{(M-1)N}}\sum_{\xi_1,\ldots,\xi_N\in E}\delta_{\Sigma\xi_i,0}$$

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 [44]. □

All this is extremely interesting. Let us mention as well that for the general matrices $H \in M_{M\times N}(\pm 1)$, which are not necessarily PHM, such statistics can be deduced from the work of Tau-Vu [91]. Finally, there is an extension of the notion of PHM in the complex case, and we will be back to this later on, in section 3 below.

2. Complex matrices

We have seen that the Hadamard matrices $H \in M_N(\pm 1)$ are very interesting combinatorial objects. In what follows, we will be interested in their complex versions:

Definition 2.1. *A complex Hadamard matrix is a square complex matrix*

$$H \in M_N(\mathbb{C})$$

whose entries are on the unit circle, $H_{ij} \in \mathbb{T}$, and whose rows are pairwise orthogonal.

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, $H \in M_N(\pm 1)$. We will see that there are many other examples.

Let us start by extending some basic results from the real case. First, we have:

Proposition 2.2. *The set of 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 $H \in Y_N$, as claimed. □

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 of the above result, we have:

Proposition 2.3. *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 operations $U \to U^t, U \to \bar{U}, U \to U^*$, and it follows that the algebraic manifold X_N constructed in Proposition 2.2 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 2.4. *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.

The same remarks as in the real case apply. For instance, we have not taken into account the results in Proposition 2.3 when formulating the above definition, because the operations $H \to H^t, \bar{H}, H^*$ are far more subtle than those in (1,2) above.

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 2.5. *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,*

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

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. □

Thus, there is no analogue of the HC in the complex case. We will see later on, in section 6 below, that the Fourier matrix F_N can be put in circulant form, so there is no analogue of the CHC either, in this setting. This is of course very good news.

We should mention, however, that the HC and CHC do have some complex extensions, which are of technical nature, by restricting the attention to the Hadamard matrices formed by roots of unity of a given order. We will discuss this in section 3 below.

As a first classification result now, in the complex case, we have:

Proposition 2.6. *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 of Proposition 1.5. Regarding now the case $N = 3$, consider an Hadamard matrix $H \in M_3(\mathbb{T})$, 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:

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

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

$$(2 \perp 3) \quad : \quad x\bar{z} + y\bar{t} = -1$$

Now observe that the equation $p+q = -1$ with $p, q \in \mathbb{T}$ tells us that the triangle having vertices at $1, p, q$ must be equilateral, and so that $\{p, q\} = \{w, w^2\}$, with $w = e^{2\pi i/3}$.

By using this fact, for the first two equations, we conclude that we must have $\{x, y\} = \{w, w^2\}$ and $\{z, t\} = \{w, w^2\}$. 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 is 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 2.7. *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*

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

by using the lexicographic order on the double indices.

In order to advance, our first task will be that of tensoring the Fourier matrices. And here, we have the following statement, refining and generalizing Theorem 2.5:

Theorem 2.8. *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 $(i, j) \to w^{ij}$, with $w = e^{2\pi i/N}$.

(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 this result, we have:

Proposition 2.9. *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 have indeed $W_2 = F_2 = F_{K_2}$, and by taking tensor powers we obtain from this that we have $W_N = F_{K_N}$, for any $N = 2^n$. □

By getting back now to our classification work, the possible abelian groups at $N = 4$, that we can use, are the cyclic group $\mathbb{Z}_4$, which produces the Fourier matrix F_4, and the Klein group $K_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$, which produces the Walsh matrix W_4.

The point, however, is that, besides F_4, W_4, there are many other complex Hadamard matrices at $N = 4$. Indeed, we can use here the following version of the tensor product construction, coming from Diţă's paper [47], involving parameters:

Proposition 2.10. *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. The rows R_{ia} of the matrix $H\otimes_Q K$ from (1) are indeed pairwise orthogonal:

$$\begin{aligned}
< R_{ia}, R_{kc} > &= \sum_{jb} Q_{ib}H_{ij}K_{ab}\cdot\bar{Q}_{kb}\bar{H}_{kj}\bar{K}_{cb}\\
&= M\delta_{ik}\sum_b K_{ab}\bar{K}_{cb}\\
&= MN\delta_{ik}\delta_{ac}
\end{aligned}$$

As for the rows L_{ia} of the matrix $H_Q\!\otimes K$ from (2), these are orthogonal as well:

$$\begin{aligned}
< L_{ia}, L_{kc} > &= \sum_{jb} Q_{ja}H_{ij}K_{ab}\cdot\bar{Q}_{jc}\bar{H}_{kj}\bar{K}_{cb}\\
&= N\delta_{ac}\sum_j H_{ij}\bar{H}_{kj}\\
&= MN\delta_{ik}\delta_{ac}
\end{aligned}$$

Thus, both the matrices in the statement are Hadamard, as claimed. $\square$

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, the right deformations of the Walsh matrix $W_4 = F_2\otimes F_2$, with arbitrary parameter matrix $Q = \left(\begin{smallmatrix}p&q\\ r&s\end{smallmatrix}\right)$, are given by:

$$F_2\otimes_Q F_2 = \begin{pmatrix}1&1\\1&-1\end{pmatrix}\underset{\begin{pmatrix}p&q\\r&s\end{pmatrix}}{\otimes}\begin{pmatrix}1&1\\1&-1\end{pmatrix} = \begin{pmatrix}p&q&p&q\\p&-q&p&-q\\r&s&-r&-s\\r&-s&-r&s\end{pmatrix}$$

This follows indeed by carefully working out what happens, by using the lexicographic order on the double indices, as explained after Proposition 1.6 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 $Q = \left(\begin{smallmatrix} p & q\\ r & s\end{smallmatrix}\right)$, these are given by a similar formula, as follows:

$$F_{2Q}\!\otimes F_2 = \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}_{\begin{pmatrix}p & q\\ r & s\end{pmatrix}} \otimes \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \begin{pmatrix}p & p & r & r\\ q & -q & s & -s\\ p & p & -r & -r\\ q & -q & -s & s\end{pmatrix}$$

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 2.11. *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 Proposition 2.10, 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 $Q = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ as above, by dephasing we obtain an equivalence with $F_4^{s'}$, where $s' = ps/qr$:

$$\begin{pmatrix} p & q & p & q \\ p & -q & p & -q \\ r & s & -r & -s \\ r & -s & -r & s \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ r/p & s/q & -r/p & -s/q \\ r/p & -s/q & -r/p & s/q \end{pmatrix}$$
$$\to \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & ps/qr & -1 & -ps/qr \\ 1 & -ps/qr & -1 & ps/qr \end{pmatrix}$$

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 of Proposition 1.7, and from the proof of Proposition 2.6. 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 given by $\{x, y, z, t\} = \{p, q, -p, -q\}$, with $p, q \in \mathbb{T}$.

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 $s=\pm1$, which contradicts our above assumption $s\neq\pm1$.

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 [88]. $\square$

At $N=5$ now, the situation is considerably more complicated, with F_5 being the only known example, but with the proof of its uniqueness being highly nontrivial.

The key technical result here, due to Haagerup [51], is as follows:

Proposition 2.12. *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 $(x-y)(x-ab)(y-ab)=0$.

Proof. This is something quite surprising, and tricky, the proof in [51] 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:

$$\begin{aligned} & (1+a+x)(1+\bar{b}+\bar{y})(1+\bar{a}y+b\bar{x}) \\ = & -(p+q)(r+s)(\bar{p}r+\bar{q}s) \end{aligned}$$

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:

$$\begin{aligned} & (a+x)+(\bar{b}+\bar{y})+(\bar{a}y+b\bar{x})+(a+x)(\bar{b}+\bar{y}) \\ + & (a+x)(\bar{a}y+b\bar{x})+(\bar{b}+\bar{y})(\bar{a}y+b\bar{x})\in\mathbb{R} \end{aligned}$$

By expanding all the products, our formula looks as follows:

$$\begin{aligned} & a+x+\bar{b}+\bar{y}+\bar{a}y+b\bar{x}+a\bar{b}+a\bar{y}+\bar{b}x+x\bar{y} \\ + & 1+ab\bar{x}+\bar{a}xy+b+\bar{a}\bar{b}y+\bar{x}+\bar{a}+b\bar{x}\bar{y}\in\mathbb{R} \end{aligned}$$

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 [51]:

Theorem 2.13. *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 2.12, 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 2.12, applied to H itself, and to its transpose H^t as well, that the entries a,b,x,y must satisfy the following equations:

$$(a-b)(a-xy)(b-xy)=0$$

$$(x-y)(x-ab)(y-ab)=0$$

This is of course something very strong, and these equations are actually valid all across the matrix, by permuting rows and columns. The idea will be that by doing some combinatorics, sometimes combined with a few tricks, this will lead to the result.

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:

$$\begin{aligned} a+b+c+d &= -1 \\ 2Re(a\bar{b}) + 2Re(c\bar{d}) &= -1 \\ 2Re(a\bar{c}) + 2Re(b\bar{d}) &= -1 \\ 2Re(a\bar{d}) + 2Re(b\bar{c}) &= -1 \end{aligned}$$

Since we have $|Re(x)| \leq 1$ for any $x \in \mathbb{T}$, we deduce from the second equation that $Re(a\bar{b}) \leq 1/2$, and so that 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 a, b, c, d are ordered on the circle, and by the above, separated by $\geq \pi/3$ arc lengths. But this implies $\theta(a, c) \geq 2\pi/3$ and $\theta(b, d) \geq 2\pi/3$, which gives $Re(a\bar{c}) \leq -1/2$ and $Re(b\bar{d}) \leq -1/2$, which contradicts 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:

$$\begin{aligned} Re[(a+b)(\bar{c}+\bar{d})] &= -1 \\ Im[(a-b)(\bar{c}-\bar{d})] &= 0 \end{aligned}$$

From $a, b, c, d \in \mathbb{T}$ we obtain $\frac{a+b}{a-b}, \frac{c+d}{c-d} \in i\mathbb{R}$, so 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 $X^2-3X+1=0$, which gives:

$$\Big\{|a+b|\,,\,|c+d|\Big\}=\left\{\frac{\sqrt{5}+1}{2}\,,\,\frac{\sqrt{5}-1}{2}\right\}$$

This is very 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 $b=\bar{a},d=\bar{c}$, and then $Re(a)=\cos(2\pi/5),Re(c)=\cos(\pi/5)$, and so we have $H\sim F_5$.

The second case, with a,b and c,d interchanged, this leads to $H\sim F_5$ as well. $\square$

The above result is of course something quite impressive. However, at the level of practical conclusions, we can only say that the $N=5$ case is something very simple.

At $N=6$ now, the situation becomes considerably complicated, with lots of "exotic" solutions, and with the structure of the Hadamard manifold X_6 being not understood yet. In fact, this manifold X_6 looks as complicated as real algebraic manifolds can get.

The simplest examples of Hadamard matrices at $N=6$ are as follows:

Theorem 2.14. *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:

$$F_6^{(\substack{r\\s})} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ \\ 1 & r & w & wr & w^2 & w^2r \\ 1 & -r & w & -wr & w^2 & -w^2r \\ \\ 1 & s & w^2 & w^2s & w & ws \\ 1 & -s & w^2 & -w^2s & w & -ws \end{pmatrix}$$

(3) The matrix here, from [51], 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 [90], 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. □

The point with the matrices in Theorem 2.14 is that they 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 3 below, with a proof 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, mildly "exotic", found by Björck and Fröberg in [31]:

Proposition 2.15. *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 $a^2+(\sqrt{3}-1)a+1=0$. $\square$

The obvious question here is perhaps on how Björck and Fröberg were able to construct the above matrix (!) This was done via some general theory for the circulant Hadamard matrices, and some computer simulations. We will discuss this in section 6 below.

Further study in the $N=6$ case leads to a number of horrors, of real algebraic geometric flavor, and we have here, as an illustrating example, the following result from [25]:

Theorem 2.16. *The self-adjoint 6×6 Hadamard matrices are, up to equivalence*

$$BN_6^q=\begin{pmatrix}1&1&1&1&1&1\\ 1&-1&\bar{x}&-y&-\bar{x}&y\\ 1&x&-1&t&-t&-x\\ 1&-\bar{y}&\bar{t}&-1&\bar{y}&-\bar{t}\\ 1&-x&-\bar{t}&y&1&\bar{z}\\ 1&\bar{y}&-\bar{x}&-t&z&1\end{pmatrix}$$

with $x,y,z,t\in\mathbb{T}$ depending on a parameter $q\in\mathbb{T}$, in a very complicated way.

Proof. The study here can be done via a lot of work, and tricks, in the spirit of the Haagerup classification result at $N=5$, and the equations are as follows:

$$\begin{aligned}x&=\frac{1+2q+q^2-\sqrt{2}\sqrt{1+2q+2q^3+q^4}}{1+2q-q^2}\\ y&=q\\ z&=\frac{1+2q-q^2}{q(-1+2q+q^2)}\\ t&=\frac{1+2q+q^2-\sqrt{2}\sqrt{1+2q+2q^3+q^4}}{-1+2q+q^2}\end{aligned}$$

All this is very technical, and we refer here to [25]. $\square$

There are many other examples at $N=6$, and no classification known. See [68].

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 [87]:

Theorem 2.17. *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 from the proof of Proposition 1.8 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 [87], the above construction to this matrix:
$$\begin{pmatrix}1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&1&-1&-1&1&1&-1&-1\\1&-1&-1&1&1&-1&-1&1\\1&1&1&1&-1&-1&-1&-1\\1&-1&1&-1&-1&1&-1&1\\1&-1&-1&-1&-1&-1&1&1\\1&-1&-1&1&-1&1&1&-1\end{pmatrix}\to\begin{pmatrix}*&*&*&*&*&*&*&*\\*&-1&1&w&1&w&1&w\\*&1&-1&w&1&1&w&w\\*&w&w&-w&1&w&w&1\\*&1&1&1&-1&w&w&w\\*&w&1&w&w&-w&w&1\\*&1&w&w&w&w&-w&1\\*&w&w&1&w&1&1&-1\end{pmatrix}$$

The matrix on the right is the Petrescu matrix P_7, found in [77]. Thus, we have:

Theorem 2.18. *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*

$$(P_7)_{ijk,abc}=\begin{cases}-w&\text{if }(ijk)=(abc),\ ia+jb+kc=0(2)\\ w&\text{if }(ijk)\neq(abc),\ ia+jb+kc\neq0(2)\\ (-1)^{ia+jb+kc}&\text{otherwise}\end{cases}$$

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 $(F_2)_{ij}=(-1)^{ij}$, we have $(W_8)_{ijk,abc}=(-1)^{ia+jb+kc}$, and this gives the formula in the statement. $\square$

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 [77]:

Theorem 2.19. *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 $N=7$.

3. 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 [34]:

Definition 3.1. *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 by definition 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 in Theorem 2.14, 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 conjecture stating that these obstructions are the only ones. Let us begin with:

Proposition 3.2 (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 [85], being explained in Proposition 1.8 above. □

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 [34], [98]:

Proposition 3.3. *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. 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 $r\in\{1,2,\ldots,l/p\}$ denote by $S_p^r=w^r\cdot S$ the above sum, rotated by w^r. 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 $\ker\Phi$. Indeed, we obviously have $S_p^r\in\ker\Phi$. Also, these elements 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 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:

$$\frac{X^{p^a}-1}{X^{p^{a-1}}-1}=1+X^{p^{a-1}}+X^{2p^{a-1}}+\ldots+X^{(p-1)p^{a-1}}$$

But this shows that $\ker\Phi$ has dimension $p^a-(p^a-p^{a-1})=p^{a-1}$, and 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 3.2, as follows:

Proposition 3.4 (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 3.3, 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 3.5. *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 solid 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 very 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 [93], and called Turyn Conjecture. □

At $l = 3$ the situation is quite complicated, due to the following result, from [40]:

Proposition 3.6 (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

$$5|N \implies H_N(6) = \emptyset$$

and so $H_{15}(3) = \emptyset$, which shows 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 to it, 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:

$$x + y + z = 0 \quad , \quad x^2 + y^2 + z^2 = 0$$

But this system has no solutions. Indeed, let us look at $x^2 + y^2 + z^2 = 0$. If this equality appears as $0 + 0 + 0 = 0$ we can divide x, y, z by 5 and redo the computation, and if not, 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 $H_{15}(3) \subset H_{15}(6) = \emptyset$. □

At $l = 5$ now, things are a bit unclear, with the converse of Theorem 3.5 (4) being something viable, at the conjectural level, at least to our knowledge.

At $l = 6$ the situation becomes again complicated, as follows:

Proposition 3.7 (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 2.13 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 [13] by using a computer, and written in logarithmic form, with k standing for $e^{2k\pi i/6}$:

$$X_{10}^6 = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0\\
0&4&1&5&3&1&3&3&5&1\\
0&1&2&3&5&5&1&3&5&3\\
0&5&3&2&1&5&3&5&3&1\\
0&3&5&1&4&1&1&5&3&3\\
0&3&3&3&3&3&0&0&0&0\\
0&1&1&5&3&4&3&0&2&4\\
0&1&5&3&5&2&4&3&2&0\\
0&5&3&5&1&2&0&2&3&4\\
0&3&5&1&1&4&4&2&0&3
\end{pmatrix}$$

We refer to [13] for more details on this topic. □

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 is something not feasible.

In order to further comment on these difficulties, let us discuss now a generalization of Proposition 3.3 above, and of the related Butson obstruction from Proposition 3.4, which has been our main source of obstructions, so far. Let us start with:

Definition 3.8. *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 3.3 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 [66]:

Theorem 3.9. *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 3.3 above.

(2) This is something that we already know at $k=1$, from Proposition 3.3. At $k=2$ the proof is more technical, along the same lines. See [66].

(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 [66] 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 3.10 (Lam-Leung obstruction)**.** *Assuming $l=p_1^{a_1}\ldots p_k^{a_k}$, 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 3.4 above, comes from Theorem 3.9 (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 3.11 (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, there is probably no way. Indeed, our above conjecture generalizes the HC in the $N >> 0$ regime, which is something beyond reach.

One interesting idea, however, in dealing with such questions, coming from the de Launey-Levin result from [44], explained in section 1, 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, at the end of this section. For a number of related considerations, we refer as well to the papers [40], [43].

Getting away now from all this arithmetic madness, let us discuss now, as a more concrete thing, the classification of the regular complex Hadamard matrices of small order. The definition here, which already appeared in the above, is as follows:

Definition 3.12. *A complex Hadamard matrix $H \in M_N(\mathbb{T})$ is called regular if the scalar products between rows decompose as sums of cycles.*

We should mention that there is some notational clash here, with this notion being sometimes used in order to designate the bistochastic matrices. In this book we use the above notion of regularity, and we call bistochastic the bistochastic matrices.

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 3.13. *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 length 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 3.14. *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 2, and from Proposition 3.13 (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. □

Let us discuss now the classification at $N = 6$. The result here, from [13], states that the above matrices $F_6^{(rs)}, F_6^{(\frac{r}{s})}, H_6^q, T_6$ are the only solutions. The proof of this fact is quite long and technical, but we will present here its main ideas. Let us start with:

Proposition 3.15. *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 3.13 (2). □

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 3.16. *The matrix T_6 is the only one with cycle structure $3+3$.*

Proof. The proof of this fact, from [13], 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 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:

$$B\in M_{4\times 6}(\mathbb Z_3)$$

With this result in hand, we can go now 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 [13]. □

Regarding now the Haagerup matrix, the result is similar, as follows:

Proposition 3.17. *The matrix H_6^q is the only one with cycle structure $2+2+2$.*

Proof. The proof here, from [13], uses the same idea as in the proof of Proposition 3.16. 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 [13]. $\square$

Regarding now the mixed case, where both $2+2+2$ and $3+3$ situations can appear, this is a bit more complicated, and requires some preliminary discussion.

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 3.18. *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 [13], the idea being as follows. Let X be the row graph in the statement. By doing some combinatorics, quite long but of very 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 [13]. □

We can now complete our classification at $N = 6$, as follows:

Proposition 3.19. *The matrices $F_6^{(rs)}, F_6^{(\frac{r}{s})}$ are the only ones with mixed cycle structure.*

Proof. According to Proposition 3.18, 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 [13].

(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 $F_6^{(^r_s)}$, and we are done. See [13]. $\square$

Summing up all the above, we have proved the following theorem:

Theorem 3.20. *The regular complex Hadamard matrices at $N=6$ are:*

(1) *The deformations $F_6^{(rs)},F_6^{(^r_s)}$ 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 3.15, and from the results in Proposition 3.16, Proposition 3.17 and Proposition 3.19. See [13]. $\square$

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 3.21. *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 some more general results from [55]. 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.

As a conclusion to all this, when imposing the regularity condition, things simplify a bit, with respect to the general case, according to a kind of $N \to N+1$ rule. To be more precise, the difficulties in the general case are basically of real algebraic geometry nature, and can be labeled as easy at $N \leq 4$, hard at $N = 5$, and not solved yet at $N = 6$. As for the regular case, here the difficulties are basically of design theory nature, and can be labeled as easy at $N \leq 5$, hard at $N = 6$, and not solved yet at $N = 7$.

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 [13], and then to [22]:

Conjecture 3.22 (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.*

In other words, the first conjecture is that a "tricky vanishing sum" of roots of unity, like the $l = 30$ one given after Definition 3.8 above, cannot be used in order to construct a complex Hadamard matrix. This is a quite difficult question, coming however with substantial computer evidence. We have no idea on how to approach it. See [13].

As for the second conjecture, this simply comes from the known examples of regular Hadamard matrices, which all appear from certain Butson matrices, by inserting parameters, in an affine way. This conjecture is from [22], and we will further discuss the notion of affine deformation, with some general results on the subject, in section 4 below.

We would like to end this section, which was depressingly algebraic and difficult, with no simple and conceptual result in sight, by doing some analysis. As explained after Conjecture 3.11 above (ABC), one way of getting into analysis, in connection with root of unity questions, is that of looking at the partial Butson matrices, at $N >> 0$.

The idea here comes of course from the de Launey-Levin counting result from [44], explained in section 1 above. Let us first discuss the prime power case. We have:

Proposition 3.23. *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. □

Our objective will be to count the matrices in Proposition 3.23. We will need:

Proposition 3.24. *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 [81] 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. By setting $a_i=\frac{n}{s}+x_i\sqrt{n}$ and then by using the various formulae in [81], we obtain:

$$\begin{aligned}
&c_{sp}\\
\simeq\ & s^{pn}(2\pi n)^{\frac{(1-s)p}{2}}s^{\frac{sp}{2}}\exp\left(-\frac{sp}{2}\sum_{i=1}^s x_i^2\right)\\
\simeq\ & s^{pn}(2\pi n)^{\frac{(1-s)p}{2}}s^{\frac{sp}{2}}\underbrace{\int_0^n\ldots\int_0^n}_{s-1}\exp\left(-\frac{sp}{2}\sum_{i=1}^s x_i^2\right)da_1\ldots da_{s-1}\\
=\ & s^{pn}(2\pi n)^{\frac{(1-s)p}{2}}s^{\frac{sp}{2}}n^{\frac{s-1}{2}}\underbrace{\int_0^n\ldots\int_0^n}_{s-1}\exp\left(-\frac{sp}{2}\sum_{i=1}^{s-1}x_i^2-\frac{sp}{2}\left(\sum_{i=1}^{s-1}x_i\right)^2\right)dx_1\ldots dx_{s-1}\\
=\ & s^{pn}(2\pi n)^{\frac{(1-s)p}{2}}s^{\frac{sp}{2}}n^{\frac{s-1}{2}}\times\pi^{\frac{s-1}{2}}s^{-\frac{1}{2}}\left(\frac{sp}{2}\right)^{\frac{1-s}{2}}\\
=\ & s^{pn}(2\pi n)^{\frac{(1-s)p}{2}}s^{\frac{sp}{2}-\frac{1}{2}+\frac{1-s}{2}}\left(\frac{p}{2\pi n}\right)^{\frac{1-s}{2}}\\
=\ & s^{pn}(2\pi n)^{\frac{(1-s)(p-1)}{2}}s^{\frac{sp-s}{2}}p^{\frac{1-s}{2}}
\end{aligned}$$

Thus we have obtained the formula in the statement, and we are done. □

Now with Proposition 3.24 in hand, we can prove:

Theorem 3.25. *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:*

$$P_2\simeq\sqrt{\frac{p^{2-\frac{q}{p}}q^{q-\frac{q}{p}}}{(2\pi N)^{q-\frac{q}{p}}}}$$

In particular, for $q=p$ prime, $P_2\simeq\sqrt{\frac{p^p}{(2\pi N)^{p-1}}}$. Also, for $q=2^k$, $P_2\simeq 2\sqrt{\left(\frac{q/2}{2\pi N}\right)^{q/2}}$.

Proof. First, the probability P_M for a random $M\in M_{M\times N}(\mathbb{Z}_q)$ to be PBM is:

$$P_M=\frac{1}{q^{MN}}\#PBM_{M\times N}$$

Thus, according to Proposition 3.23, we have the following formula:

$$\begin{aligned}
P_2 &= \frac{1}{q^N}\sum_{a_1+\ldots+a_{q/p}=N/p}\binom{N}{\underbrace{a_1\ldots a_1}_p\ldots\ldots\underbrace{a_{q/p}\ldots a_{q/p}}_p}\\
&= \frac{1}{q^N}\binom{N}{\underbrace{N/p\ldots N/p}_p}\sum_{a_1+\ldots+a_{q/p}=N/p}\binom{N/p}{a_1\ldots a_{q/p}}^p\\
&= \frac{1}{p^N}\binom{N}{\underbrace{N/p\ldots N/p}_p}\times\frac{1}{(q/p)^N}\sum_{a_1+\ldots+a_{q/p}=N/p}\binom{N/p}{a_1\ldots a_{q/p}}^p
\end{aligned}$$

Now by using the Stirling formula for the left term, and Proposition 3.24 with $s=q/p$ and $n=N/p$ for the right term, we obtain:

$$\begin{aligned}
P_2 &= \sqrt{\frac{p^p}{(2\pi N)^{p-1}}}\times\sqrt{\frac{(q/p)^{\frac{q}{p}(p-1)}}{p^{\frac{q}{p}-1}(2\pi N/p)^{(\frac{q}{p}-1)(p-1)}}}\\
&= \sqrt{\frac{p^{p-\frac{q}{p}(p-1)-\frac{q}{p}+1+(\frac{q}{p}-1)(p-1)}q^{\frac{q}{p}(p-1)}}{(2\pi N)^{p-1+(\frac{q}{p}-1)(p-1)}}}\\
&= \sqrt{\frac{p^{2-\frac{q}{p}}q^{q-\frac{q}{p}}}{(2\pi N)^{q-\frac{q}{p}}}}
\end{aligned}$$

Thus we have obtained the formula in the statement, and we are done. □

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 3.26. *When $q=p_1p_2$ is a product of distinct primes, the standard form of the dephased partial Butson matrices at $M=2$ is*

$$H=\begin{pmatrix}1&1&\ldots&1&\ldots&\ldots&1&1&\ldots&1\\ \underbrace{1}_{A_{11}}&\underbrace{w}_{A_{12}}&\ldots&\underbrace{w^{p_2-1}}_{A_{1p_2}}&\ldots&\ldots&\underbrace{w^{q-p_2}}_{A_{p_11}}&\underbrace{w^{q-p_2+1}}_{A_{p_12}}&\ldots&\underbrace{w^{q-1}}_{A_{p_1p_2}}\end{pmatrix}$$

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 $q=p_1p_2$ 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 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 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 attention to the case $p_1 = 2$. Here we have:

Theorem 3.27. *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 3.26, 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. $\square$

According to the above result we have $P_2 = \sum_{t \in \mathbb{Z}} P_2^{(t)}$, where $P_2^{(t)}$ with $t \in \mathbb{Z}$ is the probability for a random walk on $\mathbb{Z}^p$ to end up at $(t, \ldots, t)$. Observe that, by using Proposition 3.24 above with s, p, n equal respectively to $p, 2, N/2$, we obtain:

$$\begin{aligned} P_2^{(0)} &= \frac{1}{(2p)^N} \binom{N}{N/2} \sum_{a_1 + \ldots + a_p = N/2} \binom{N/2}{a_1, \ldots, a_p}^2 \\ &\simeq \sqrt{\frac{2}{\pi N}} \times \sqrt{\frac{p^p}{2^{p-1}(\pi N)^{p-1}}} \\ &= 2\sqrt{\left(\frac{p}{2\pi N}\right)^p} \end{aligned}$$

Regarding now the probability $P_2^{(t)}$ of ending up at $(t, \ldots, t)$, in principle for small t this can be estimated by using a modification of the method in [81]. However, it is not clear on how to compute the full diagonal return probability in Theorem 3.27.

It is possible to establish a few more results in this direction, and we refer here to [7]. However, the main question remains that of adapting the methods in [66] to the root of unity case. As a preliminary observation here, also from [7], we have:

Theorem 3.28. *The probability P_M for a random $H\in M_{M\times N}(\mathbb{Z}_q)$ to be partial Butson equals the probability for a length N random walk with increments drawn from*

$$E=\left\{(e_i\bar{e}_j)_{i<j}\Big|e\in\mathbb{Z}_q^M\right\}$$

regarded as a subset $\mathbb{Z}_q^{\binom{M}{2}}$, to return at the origin.

Proof. Indeed, with $T(e)=(e_i\bar{e}_j)_{i<j}$, a matrix $X=[e_1,\ldots,e_N]\in M_{M\times N}(\mathbb{Z}_q)$ is partial Butson if and only if $T(e_1)+\ldots+T(e_N)=0$, and this gives the result. $\square$

Observe now that, according to the above result, we have:

$$\begin{aligned}P_M&=\frac{1}{q^{(M-1)N}}\#\left\{\xi_1,\ldots,\xi_N\in E\Big|\sum_i\xi_i=0\right\}\\&=\frac{1}{q^{(M-1)N}}\sum_{\xi_1,\ldots,\xi_N\in E}\delta_{\Sigma\xi_i,0}\end{aligned}$$

The problem is to continue the computation in the proof of the inversion formula. More precisely, the next step at $q=2$, which is the key one, is as follows:

$$\delta_{\Sigma\xi_i,0}=\frac{1}{(2\pi)^D}\int_{[-\pi,\pi]^D}e^{i<\lambda,\Sigma\xi_i>}d\lambda$$

Here $D=\binom{M}{2}$. The problem is that this formula works when $\Sigma\xi_i$ is real, as is the case in [44], but not when $\Sigma\xi_i$ is complex, as is the case in Theorem 3.28.

4. Geometry, defect

In this section and in the next two ones 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:

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

This intersection is very far from being smooth. Given a point $H \in X_N$, the problem is that of understanding the structure of X_N around H, which is often singular.

There are several ways of discussing this question, a quite straightforward approach, going back to the work in [62], and then in [72], [88], being via the 1-parameter deformations of the complex Hadamard matrices. In what follows we will use an equivalent approach, of more real algebraic geometry flavor, developed in [5], [6].

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 4.1. *For $H \in X_N$ and $A \in M_N(\mathbb{R})$, the following are equivalent:*

1. *$H_{ij}^q = H_{ij} q^{A_{ij}}$ is an Hadamard matrix, for any $q \in \mathbb{T}_1$.*
2. *$\sum_k H_{ik} \bar{H}_{jk} q^{A_{ik}-A_{jk}} = 0$, for any $i \neq j$ and any $q \in \mathbb{T}_1$.*
3. *$\sum_k H_{ik} \bar{H}_{jk} \varphi(A_{ik} - A_{jk}) = 0$, for any $i \neq j$ and any $\varphi : \mathbb{R} \to \mathbb{C}$.*
4. *$\sum_{k \in E_{ij}^r} H_{ik} \bar{H}_{jk} = 0$ for any $i \neq j$ and $r \in \mathbb{R}$, where $E_{ij}^r = \{k | A_{ik} - A_{jk} = r\}$.*

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 $\varphi(r) = q^r$. $\square$

Observe that in the above statement the condition (4) is purely combinatorial.

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, let us introduce the following notions:

Definition 4.2. *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 $F_2 \otimes F_2$:

$$A_l = \begin{pmatrix} a&a&b&b\\ c&c&d&d\\ a&a&b&b\\ c&c&d&d \end{pmatrix} \qquad A_r = \begin{pmatrix} a&b&a&b\\ a&b&a&b\\ c&d&c&d\\ c&d&c&d \end{pmatrix}$$

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 4.3. *Associated to a point $H \in X_N$ are the following objects:*

(1) *The enveloping tangent space: $\widetilde{T}_H X_N = T_H M_N(\mathbb{T}) \cap T_H\sqrt{N}U_N$.*
(2) *The tangent cone $T_H X_N$: 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 $\widetilde{T}_H X_N, T_H^\times X_N$ are real linear spaces, and that $T_H X_N, T_H^\circ X_N$ 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:

$$T_H^\times X_N \subset T_H^\circ X_N \subset T_H X_N \subset \widetilde{T}_H X_N$$

In more algebraic terms now, these various tangent cones are best described by the corresponding matrices, and we have here the following result:

Theorem 4.4. *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 $\sum_kH_{ik}\bar{H}_{jk}(A_{ik}-A_{jk})=0$, for any i,j.*
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 $\sum_kH_{ik}\bar{H}_{jk}e^{i(g_{ik}(t)-g_{jk}(t))}=0$ for any i,j.*
3. *$T_H^\circ X_N$ is formed by the matrices $A\in M_N(\mathbb R)$ satisfying $\sum_kH_{ik}\bar{H}_{jk}q^{A_{ik}-A_{jk}}=0$, for any $i\neq j$ and any $q\in\mathbb T$.*
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:

$$d|H_{ij}|^2=d(X_{ij}^2+Y_{ij}^2)=2(X_{ij}\dot{X}_{ij}+Y_{ij}\dot{Y}_{ij})$$

Now since an arbitrary vector $\xi\in T_HM_N(\mathbb C)$, written as $\xi=\sum_{ij}\alpha_{ij}\dot{X}_{ij}+\beta_{ij}\dot{Y}_{ij}$, belongs to $T_HM_N(\mathbb T)$ if and only if $<\xi,d|H_{ij}|^2>=0$ for any i,j, we obtain:

$$T_HM_N(\mathbb T)=\left\{\sum_{ij}A_{ij}(Y_{ij}\dot{X}_{ij}-X_{ij}\dot{Y}_{ij})\Big|A_{ij}\in\mathbb R\right\}$$

We also know that $\sqrt{N}U_N$ is defined by the algebraic relations $<H_i,H_j>=N\delta_{ij}$, where $H_1,\ldots,H_N$ are the rows of H. 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:

$$\widetilde{T}_HC_N=\left\{\xi\in T_HM_N(\mathbb T)|<\xi,\dot{L}_{ij}>=0,\forall i\neq j\right\}$$

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 $\xi\in T_HM_N(\mathbb T)$, 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 $\widetilde{T}_HX_N$ in the statement.

(2) Pick an arbitrary deformation, and write it as $f_{ij}(e^{it})=H_{ij}e^{ig_{ij}(t)}$. Observe first that the Hadamard condition corresponds to the equations in the statement, namely:

$$\sum_kH_{ik}\bar{H}_{jk}e^{i(g_{ik}(t)-g_{jk}(t))}=0$$

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 $\widetilde{T}_HX_N$, so we obtain in this way a certain map $T_HX_N\to\widetilde{T}_HX_N$. 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 4.1, 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 $T_H^\circ X_N\to\widetilde{T}_HX_N$, 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:

$$\sum_k H_{ik}\bar{H}_{jk}q^{A_{ik}-A_{jk}}=q^{a_i-a_j}\sum_k H_{ik}\bar{H}_{jk}=\delta_{ij}$$

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 4.5. *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 4.4, this gives the result. □

Summarizing, we have so far a number of theoretical results about the tangent cones $T_H X_N$ that we are interested in, and their versions coming from the trivial and affine deformations, and from the intersection formula $X_N = M_N(\mathbb{T}) \cap \sqrt{N} U_N$ as well.

In practice now, passed a few special cases where all these cones collapse to the trivial cone $T_N^\times X_N$, which by Proposition 4.5 means that the image of $H \in X_N$ must be isolated in the dephased manifold $X_N \to Z_N$, things are quite difficult to compute.

However, as a concrete numerical invariant arising from all this, which can be effectively computed in many cases of interest, we have, following [88]:

Definition 4.6. *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 4.5, it is sometimes convenient to replace $d(H)$ by the related quantity $d'(H) = d(H) - 2N + 1$, called dephased defect of H. See [88]. In what follows we will rather use $d(H)$ as defined above, and simply call it "defect" of H.

We already know, from Theorem 4.4, 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 [88]:

Theorem 4.7. *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 4.4 (1), and the second assertion follows either from Theorem 4.4 and its proof, or directly from the definition of the enveloping tangent space $\widetilde{T}_H X_N$, as used in Definition 4.6. $\square$

Here are a few basic properties of the defect:

Proposition 4.8. *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 $T_H^\times X_N\subset T_HX_N\subset\widetilde{T}_HX_N$. 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 $T_HX_N=T_H^\times X_N$, 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. □

Let us discuss now the computation of the defect for the most basic examples of complex Hadamard matrices that we know, namely the real ones, and the Fourier ones.

In order to deal with the real case, it is convenient to modify the general formula from Theorem 4.7 above, via a change of variables, as follows:

Proposition 4.9. *We have a linear space isomorphism as follows,*

$$\widetilde{T}_HX_N\simeq\left\{E\in M_N(\mathbb{C})\Big|E=E^*,(EH)_{ij}\bar{H}_{ij}\in\mathbb{R},\forall i,j\right\}$$

the correspondences $A\to E$ and $E\to A$ being given by the formulae

$$E_{ij}=\sum_kH_{ik}\bar{H}_{jk}A_{ik}\quad,\quad A_{ij}=(EH)_{ij}\bar{H}_{ij}$$

with $A\in\widetilde{T}_HX_N$ being the usual components, from Theorem 4.7 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:

$$E_{ij}=\sum_kH_{ik}\bar{H}_{jk}A_{ik}$$

In terms of these new variables, the equations in Theorem 4.7 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 [86], is as follows:

Theorem 4.10. *For any real Hadamard matrix $H\in M_N(\pm1)$ we have*

$$\widetilde{T}_HX_N\simeq M_N(\mathbb{R})^{symm}$$

and so the corresponding defect is $d(H)=N(N+1)/2$.

Proof. We use Proposition 4.9. 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. □

We should mention that the above result, as well as the whole basic theory of the tangent cones and defect, can be extended in a quite straightforward way to the case of the partial Hadamard matrices [22]. We will be back to this, later on.

Let us discuss now the computation of the defect of the Fourier matrix F_G. The main idea here goes back to [62], with some supplementary contributions from [72], the main formula, in the cyclic group case, was obtained in [88], the extension to the general case was done in [5], and the corresponding deformations were studied in [73].

As a first result on this subject, we have, following [88]:

Theorem 4.11. *For a Fourier matrix $F = F_G$, the matrices $A \in \widetilde{T}_F X_N$, 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 the system of equations in Theorem 4.7, namely:

$$\sum_k F_{ik}\bar{F}_{jk}(A_{ik} - A_{jk}) = 0$$

By decomposing our finite abelian group as $G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_r}$ we can assume $F = F_{N_1} \otimes \ldots \otimes F_{N_r}$, so that with $w_k = e^{2\pi i/k}$ we have:

$$F_{i_1\ldots i_r, j_1\ldots j_r} = (w_{N_1})^{i_1 j_1} \ldots (w_{N_r})^{i_r j_r}$$

With $N = N_1 \ldots N_r$ and $w = e^{2\pi i/N}$, we obtain:

$$F_{i_1\ldots i_r, j_1\ldots j_r} = w^{\left(\frac{i_1 j_1}{N_1} + \ldots + \frac{i_r j_r}{N_r}\right)N}$$

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 4.12. *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 4.11, 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 abstract definition of the Fourier matrix F_G, from Theorem 2.8 above, 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:

$$\begin{aligned}
\delta(\mathbb{Z}_{p^a}) &= 1 + (p-1)p^{-1} + (p^2 - p)p^{-2} + \ldots + (p^a - p^{a-1})p^{-1} \\
&= 1 + a - \frac{a}{p}
\end{aligned}$$

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 4.13. *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:

$$\begin{aligned}\delta(G\times H) &= \sum_{gh}\frac{1}{ord(g,h)}\\ &= \sum_{gh}\frac{1}{[ord(g),ord(h)]}\\ &\geq \sum_{gh}\frac{1}{ord(g)\cdot ord(h)}\\ &= \delta(G)\delta(H)\end{aligned}$$

Now 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. □

We deduce from this that we have the following result:

Proposition 4.14. *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 4.13, because the order of G_p is a power of p. □

As an illustration, we can recover in this way the defect computation in [89]:

Theorem 4.15. *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 cyclic groups $G_{p_i}=\mathbb{Z}_{p_i^{a_i}}$. By applying now Proposition 4.14, and by using the computation for cyclic p-groups performed before Proposition 4.13, 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 4.16. *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. $\square$

Let us compute now δ in the general isotypic case:

Proposition 4.17. *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 by using the notation $[a]_q = 1 + q + q^2 + \ldots + q^{a-1}$.

Proof. First, in terms of the numbers c_k, we have:

$$\delta(G) = 1 + \sum_{k\geq 1} \frac{c_k - c_{k-1}}{p^k}$$

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:

$$c_0 = 1, c_1 = p^r, c_2 = p^{2r}, \ldots, c_{a_1} = p^{ra_1},$$
$$c_{a_1+1} = p^{a_1+(r-1)(a_1+1)}, c_{a_1+2} = p^{a_1+(r-1)(a_1+2)}, \ldots, c_{a_2} = p^{a_1+(r-1)a_2},$$
$$c_{a_2+1} = p^{a_1+a_2+(r-2)(a_2+1)}, c_{a_2+2} = p^{a_1+a_2+(r-2)(a_2+2)}, \ldots, c_{a_3} = p^{a_1+a_2+(r-2)a_3},$$
$$\ldots\ldots\ldots$$
$$c_{a_{r-1}+1} = p^{a_1+\ldots+a_{r-1}+(a_{r-1}+1)}, c_{a_{r-1}+2} = p^{a_1+\ldots+a_{r-1}+(a_{r-1}+2)}, \ldots, c_{a_r} = p^{a_1+\ldots+a_r}$$

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:

$$\begin{aligned}
\delta(G) &= 1+(p^{r-1}+p^{2r-2}+p^{3r-3}+\ldots+p^{a_1r-a_1})\\
&\quad -(p^{-1}+p^{r-2}+p^{2r-3}+\ldots+p^{(a_1-1)r-a_1})\\
&\quad +(p^{(r-1)(a_1+1)-1}+p^{(r-1)(a_1+2)-2}+\ldots+p^{a_1+(r-2)a_2})\\
&\quad -(p^{a_1r-a_1-1}+p^{(r-1)(a_1+1)-2}+\ldots+p^{a_1+(r-1)(a_2-1)-a_2})\\
&\quad +\ldots\\
&\quad +(p^{a_1+\ldots+a_{r-1}}+p^{a_1+\ldots+a_{r-1}}+\ldots+p^{a_1+\ldots+a_{r-1}})\\
&\quad -(p^{a_1+\ldots+a_{r-1}-1}+p^{a_1+\ldots+a_{r-1}-1}+\ldots+p^{a_1+\ldots+a_{r-1}-1})
\end{aligned}$$

Now by performing all the sums, we obtain:

$$\begin{aligned}
\delta(G) &= 1+p^{-1}(p^r-1)\frac{p^{(r-1)a_1}-1}{p^{r-1}-1}\\
&\quad +p^{(r-2)a_1+(a_1-1)}(p^{r-1}-1)\frac{p^{(r-2)(a_2-a_1)}-1}{p^{r-2}-1}\\
&\quad +p^{(r-3)a_2+(a_1+a_2-1)}(p^{r-2}-1)\frac{p^{(r-3)(a_3-a_2)}-1}{p^{r-3}-1}\\
&\quad +\ldots\\
&\quad +p^{a_1+\ldots+a_{r-1}-1}(p-1)(a_r-a_{r-1})
\end{aligned}$$

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 4.12. By putting it together with the various results above, we obtain:

Theorem 4.18. *For a finite abelian group G, decomposed as $G=\times_pG_p$, 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 4.12 that we have $d(F_G)=|G|\delta(G)$, and the result follows from Proposition 4.14 and Proposition 4.17. □

As a first illustration, we can recover in this way the formula in Theorem 4.15. Assuming that $N = p_1^{a_1} \ldots p_s^{a_s}$ is the decomposition of N into prime factors, we have:

$$\begin{aligned} d(F_N) &= N \prod_{i=1}^{s} \left(1 + p_i^{-1}(p_i - 1)a_i\right) \\ &= N \prod_{i=1}^{s} \left(1 + a_i - \frac{a_i}{p_i}\right) \end{aligned}$$

As a second illustration, for the group $G = \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}}$ with $a_1 \leq a_2$ we obtain:

$$\begin{aligned} d(F_G) &= p^{a_1+a_2}(1 + p^{-1}(p^2 - 1)[a_1]_p + p^{a_1-1}(p-1)(a_2 - a_1)) \\ &= p^{a_1+a_2-1}(p + (p^2-1)\frac{p^{a_1}-1}{p-1} + p^{a_1}(p-1)(a_2 - a_1)) \\ &= p^{a_1+a_2-1}(p + (p+1)(p^{a_1} - 1) + p^{a_1}(p-1)(a_2 - a_1)) \end{aligned}$$

Finally, let us mention that for general non-abelian groups, there does not seem to be any reasonable algebraic formula for the quantity $\delta(G)$. As an example, consider the dihedral group D_N, consisting of N symmetries and N rotations. We have:

$$\delta(D_N) = \frac{N}{2} + \delta(\mathbb{Z}_N)$$

Now by remembering the formula for $\mathbb{Z}_N$, namely $\delta(\mathbb{Z}_N) = \prod(1 + p_i^{-1}(p_i - 1)a_i)$, it is quite clear that the $N/2$ factor can not be incorporated in any nice way. See [5].

Let us prove now, following the paper of Nicoara and White [73], 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 4.19. *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 $t \to U_t H$. First, we have:

Theorem 4.20. *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 $|\sum_{rs} H_{rq}\bar{H}_{sq}(e^{tA})_{pr}(e^{-tA})_{sp}| = 1$, for any p, q.*
2. *UH is Hadamard at order 0 when $|(AH)_{pq}| = 1$, for any p, q.*

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 obtain the conclusion in the statement. □

In the Fourier matrix case we can go beyond this, and we have:

Proposition 4.21. *Given a Fourier matrix $F_G \in M_G(\mathbb{C})$, and an antihermitian matrix $A \in M_G(\mathbb{C})$, the matrix 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 4.20 (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 obtain the conclusion in the statement. $\square$

Following [73], let us construct now the deformations. The result is as follows:

Theorem 4.22. *Let G be a finite abelian group, and for any $g, h \in G$, let us set:*

$$B_{pq} = \begin{cases} 1 & \text{if } \exists k \in \mathbb{N}, p = h^k g, q = h^{k+1} g \\ 0 & \text{otherwise} \end{cases}$$

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 [73], is quite long and technical, based on the Fourier computation from Proposition 4.21 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 4.12, 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 4.21. 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 [73]. With this last ingredient in hand, a comparison with Theorem 4.12 shows that the defect of F_G is indeed attained, in the sense that all order 0 deformations are actually true deformations. See [73]. □

The above result is something quite surprising, which came a long time after the original defect paper [88], and even more time after the early computations in [62].

Let us also mention that [73] 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 section 11 below.

5. Special matrices

We have seen in the previous section that the defect theory from [88] can be successfully applied to the real Hadamard matrices, and to the Fourier matrices.

We discuss here a number of more specialized aspects, regarding the tensor products, the Diţă deformations of such tensor products, the Butson and the regular matrices, the master Hadamard matrices, the McNulty-Weigert matrices, and finally the partial Hadamard matrix case, following [2], [5], [6], [22], [69], [88], [89].

Let us begin with some generalities. The standard defect equations are those in Theorem 4.7, naturally coming from the computations in the proof of Theorem 4.4:

$$d(H)=\dim_{\mathbb R}\left\{A\in M_N(\mathbb R)\Big|\sum_kH_{ik}\bar{H}_{jk}(A_{ik}-A_{jk})=0,\forall i,j\right\}$$

However, we have seen that for various concrete questions, some manipulations on these equations are needed. To be more precise, the study in the real case was based on the transformation $E_{ij}=\sum_kH_{ik}\bar{H}_{jk}A_{ik}$ from Proposition 4.9, the study in the Fourier matrix case was based on the transformation $P=AF_G$ from Theorem 4.11, and the fine study in the Fourier matrix case was based on the $t\to e^{tA}H$ method from Proposition 4.21.

In short, each type of complex Hadamard matrix seems to require its own general theory, and defect manipulations, and there is no way of escaping from this.

In view of this phenomenon, let us first present some further manipulations on the defect equations, which are all quite natural, and potentially useful. First, we have:

Proposition 5.1. *The defect $d(H)$ is the corank of the matrix*

$$Y_{ij,ab}=(\delta_{ia}-\delta_{ja})\begin{cases}Re(H_{ib}\bar{H}_{jb})&\text{if } i<j\\ Im(H_{ib}\bar{H}_{jb})&\text{if } i>j\\ *&\text{if } i=j\end{cases}$$

where $*$ can be any quantity, its coefficient being 0 anyway.

Proof. The matrix of the system defining the enveloping tangent space is:

$$X_{ij,ab}=(\delta_{ia}-\delta_{ja})H_{ib}\bar{H}_{jb}$$

However, since we are only looking for real solutions $A\in M_N(\mathbb R)$, we have to take into account the real and imaginary parts. But this is not a problem, because the (ij) equation coincides with the (ji) one, that we can cut. More precisely, if we set Y as above, then we obtain precisely the original system. Thus the defect of H is the corank of Y. $\square$

As an illustration, for the Fourier matrix F_N we have the following formula, where $e(i,j) \in \{-1,0,1\}$ is negative if $i<j$, null for $i=j$, and positive for $i>j$:

$$Y_{ij,ab} = \frac{1}{2}(\delta_{ia} - \delta_{ja})(w^{(i-j)b} + e(i,j)w^{(j-i)b})$$

Observe in particular that for the Fourier matrix F_2 we have:

$$Y = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Here the corank is 3, but, unfortunately, this cannot be seen on the characteristic polynomial, which is $P(\lambda) = \lambda^4$. The problem is that our matrix, and more precisely its middle 2×2 block, is not diagonalizable. This phenomenon seems to hold in general.

A second possible manipulation, which is of interest in connection with quantum groups and subfactor theory, concerns the reformulation of the defect in terms of the profile matrix of H. Indeed, it is known that both the quantum group and subfactor associated to H depend only on this profile matrix, and this will be explained in sections 10-11 below.

We do not have an answer here, but our conjecture is as follows:

Conjecture 5.2. *The profile matrix of H, namely*

$$M_{ia}^{jb} = \sum_k H_{ik}\bar{H}_{jk}\bar{H}_{ak}H_{bk}$$

determines the enveloping tangent space $\widetilde{T}_H X_N$, or at least the defect $d(H)$.

All this is of course related to the general question on whether the associated quantum group or subfactor can "see" the defect, via various representation theory invariants. For a number of further speculations on all this, and on some related glow questions as well, in relation with the general theory in [45], [46], we refer to [5], [6], [8].

Let us get back now to our original goal here, namely computing the defect for various classes of special matrices. For the tensor products, we have the following result:

Proposition 5.3. *For a tensor product $L = H\otimes K$ we have*

$$d(L) \geq d(H)d(K)$$

coming from an inclusion of linear spaces $\widetilde{T}_H X_M \otimes \widetilde{T}_K X_N \subset \widetilde{T}_L X_{MN}$.

Proof. For a matrix $A = B \otimes C$, we have the following formulae:

$$\begin{aligned}\sum_{kc}(H\otimes K)_{ia,kc}\overline{(H\otimes K)}_{jb,kc}A_{ia,kc} &= \sum_k H_{ik}\bar{H}_{jk}B_{ik}\sum_c K_{ac}\bar{K}_{bc}C_{ac}\\ \sum_{kc}(H\otimes K)_{ia,kc}\overline{(H\otimes K)}_{jb,kc}A_{jb,kc} &= \sum_k H_{ik}\bar{H}_{jk}B_{jk}\sum_c K_{ac}\bar{K}_{bc}C_{bc}\end{aligned}$$

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 4 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 5.6 below, with a slight advance on all this.

Let us discuss now the Diţă deformations. Here the study is even more difficult, and we basically have just one result, when the deformation matrix is as follows:

Definition 5.4. *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:

Theorem 5.5. *If $H \in X_M, K \in X_N$ are dephased, of Butson type, and $Q \in M_{M\times N}(\mathbb{T})$ is dephased and elsewhere generic, then $A = (A_{ia,kc})$ belongs to $\widetilde{T}_{H\otimes_Q K} X_{MN}$ iff*

$$A^{ij}_{ac} = A^{ij}_{bc} \quad , \quad A^{ij}_{ac} = \overline{A^{ji}_{ac}} \quad , \quad (A^{ii}_{xy})_{xy} \in \widetilde{T}_K X_N$$

hold 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 system for the enveloping tangent space, 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 $(H \otimes_Q K)_{ia,jb} = q_{ib}H_{ij}K_{ab}$, and so our system 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 $A_{ac}^{ij}=\sum_k H_{ik}\bar{H}_{jk}A_{ia,kc}$ in the statement. We have:

$$\overline{A_{ac}^{ij}}=\sum_k \bar{H}_{ik}H_{jk}A_{ia,kc}=\sum_k H_{jk}\bar{H}_{ik}A_{ia,kc}$$

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 $A_{ac}^{ij}=\overline{A_{bc}^{ji}}$, for any a,b,c and any $i\neq j$. 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 parameters cancel, and our equations become:

$$\sum_c K_{ac}\bar{K}_{bc}(A_{ac}^{ii}-\overline{A_{bc}^{ii}})=0,\quad \forall a,b,c,i$$

On the other hand, we have $A_{ac}^{ii}=\sum_k A_{ia,kc}$, and so 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. □

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 $T_{H\otimes K}^\circ X_{MN}$, obtained by gluing $T_H^\circ X_M,T_K^\circ X_N$. Our answer here, which takes into account the two "semi-trivial" cones coming from the left and right Diţă deformations, is as follows:

Theorem 5.6. *The cones $T_H^\circ X_M=\{B\}$ and $T_K^\circ X_N=\{C\}$ glue via the formulae*

$$A_{ia,jb}=\lambda B_{ij}+\psi_j C_{ab}+X_{ia}+Y_{jb}+F_{aj}$$

$$A_{ia,jb}=\phi_b B_{ij}+\mu C_{ab}+X_{ia}+Y_{jb}+E_{ib}$$

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. In order to prove the result, we use the criterion in Theorem 4.4 (3) above. So, 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:

$$A_{ia,kc} = \lambda B_{ik} + \psi_k C_{ac} + X_{ia} + Y_{kc} + F_{ak}$$
$$A_{jb,kc} = \lambda B_{jk} + \psi_k C_{bc} + X_{jb} + Y_{kc} + F_{bk}$$

Now by substracting, 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:

$$\begin{aligned}
P &= \sum_{kc} H_{ik}\bar{H}_{jk}K_{ac}\bar{K}_{bc}q^{\lambda(B_{ik}-B_{jk})+\psi_k(C_{ac}-C_{bc})+(X_{ia}-X_{jb})+(F_{ak}-F_{bk})}\\
&= q^{X_{ia}-X_{jb}}\sum_k H_{ik}\bar{H}_{jk}q^{F_{ak}-F_{bk}}q^{\lambda(B_{ik}-B_{jk})}\sum_c K_{ac}\bar{K}_{bc}(q^{\psi_k})^{C_{ac}-C_{bc}}\\
&= \delta_{ab}q^{X_{ia}-X_{ja}}\sum_k H_{ik}\bar{H}_{jk}(q^\lambda)^{B_{ik}-B_{jk}}\\
&= \delta_{ab}\delta_{ij}
\end{aligned}$$

Thus Theorem 4.4 (3) applies and tells us that we have $A \in T_{H\otimes K}^\circ X_{MN}$, as claimed. In the second case now, the proof is similar. First, we have:

$$A_{ia,kc} = \phi_c B_{ik} + \mu C_{ac} + X_{ia} + Y_{kc} + E_{ic}$$
$$A_{jb,kc} = \phi_c B_{jk} + \mu C_{bc} + X_{jb} + Y_{kc} + E_{jc}$$

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 Theorem 4.4 (3) applies again, and gives the result. □

We believe Theorem 5.6 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 [6].

Let us discuss now some rationality questions, in relation with:

Definition 5.7. *The rational enveloping tangent space at $H\in X_N$ is*

$$[\widetilde{T}_HX_N]_\mathbb{Q}=\widetilde{T}_HX_N\cap M_N(\mathbb{Q})$$

and the dimension $d_\mathbb{Q}(H)$ of this space is called rational defect of H.

Observe that the first 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 5.7. It follows from definitions that $d_\mathbb{Q}(H)\leq d(H)$, and we have:

Conjecture 5.8. *For a regular Hadamard matrix $H\in M_N(\mathbb{C})$ we have*

$$\widetilde{T}_HC_N=\mathbb{C}\cdot[\widetilde{T}_HC_N]_\mathbb{Q}$$

and so the defect equals the rational defect, $d_\mathbb{Q}(H)=d(H)$.

For the usual Fourier matrices F_N, this definitely holds at $N=p$ prime, because the minimal polynomial of w over $\mathbb{Q}$ is simply $P=1+w+\ldots+w^{p-1}$. The case $N=p^2$ has also a simple solution, coming from the fact that all the $p\times p$ blocks of our matrix A can be shown to coincide. In general, this method should probably work for $N=p^k$, or even for any $N\in\mathbb{N}$. So, our conjecture would be that this holds indeed for the Fourier matrices, usual or general, and more generally for the Butson matrices, and even more generally, modulo Conjecture 3.22 above, for the regular matrices. See [6].

Let us discuss now defect computations for a very interesting class of Hadamard matrices, namely the "master" ones, introduced in [2]:

Definition 5.9. *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 $f(z)=\sum_jz^{n_j}$.

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 [2], the motivating remark there being the fact that the following operator defines a representation of the Temperley-Lieb algebra [92]:

$$R = \sum_{ij} e_{ij} \otimes \Lambda^{n_i - n_j}$$

At the level of examples, the first observation, from [2], is that the standard 4×4 complex Hadamard matrices are, with 2 exceptions, master Hadamard matrices:

Proposition 5.10. *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 $q^2 \neq 1$, we can find $k \in \mathbb{R}$ such that $q^{2k} = -1$, and so 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 if we pick $\lambda \neq 1$ and write $1 = \lambda^x, -1 = \lambda^y, q = \lambda^z, -q = \lambda^t$, we are done. $\square$

We have the following generalization of Proposition 5.10, once again from [2]:

Theorem 5.11. *$F_M \otimes_Q F_N$ is 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 [2] 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:

$$f_M(z) = \sum_i z^{Mr_i + i} \quad , \quad f_N(z) = \sum_a z^{Np_a + a}$$

We use the eigenvalues $\lambda_{ia} = q^i w^a$, where $w = e^{2\pi i/N}$, and where $q^{Nk} = \nu$, where $\nu^M = 1$. Observe that, according to $f(z) = f_M(z^{Nk}) f_N(z)$, the exponents are:

$$n_{jb} = Nk(Mr_j + j) + Np_b + b$$

Thus the associated master Hadamard matrix is given by:

$$\begin{aligned}
H_{ia,jb} &= (q^i w^a)^{Nk(Mr_j+j)+Np_b+b} \\
&= \nu^{ij} q^{i(Np_b+b)} w^{a(Np_b+b)} \\
&= \nu^{ij} w^{ab} q^{i(Np_b+b)}
\end{aligned}$$

Now since $(F_M \otimes F_N)_{ia,jb} = \nu^{ij} w^{ab}$, we get $H = F_M \otimes_Q F_N$ with $Q_{ib} = q^{i(Np_b+b)}$, as claimed. 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 [2]:

Conjecture 5.12 (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 5.13. *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 $L_{ij} = f(\frac{1}{\lambda_i \lambda_j})$ and $R_{i,jk} = f(\frac{\lambda_j}{\lambda_i \lambda_k})$, f being the master function.

Proof. The first order deformation equations are:

$$\sum_k H_{ik} \bar{H}_{jk} (A_{ik} - A_{jk}) = 0$$

With $H_{ij} = \lambda_i^{n_j}$ we have $H_{ij}\bar{H}_{jk} = (\lambda_i/\lambda_j)^{n_k}$, and so the defect is given by:

$$d(H) = \dim_{\mathbb{R}} \left\{ A \in M_N(\mathbb{R}) \Big| \sum_k A_{ik} \left(\frac{\lambda_i}{\lambda_j}\right)^{n_k} = \sum_k A_{jk} \left(\frac{\lambda_i}{\lambda_j}\right)^{n_k}\ \forall i,j \right\}$$

Now, pick $A \in M_N(\mathbb{C})$ and set $B = AH^t$, so that $A = \frac{1}{N} B\bar{H}$. First, we have:

$$\begin{aligned}
A \in M_N(\mathbb{R}) &\iff B\bar{H} = \bar{B}H \\
&\iff \bar{B} = \frac{1}{N} B\bar{H}H^*
\end{aligned}$$

On the other hand, the matrix on the right is given by:

$$(\bar{H}H^*)_{ij} = \sum_k \bar{H}_{ik}\bar{H}_{jk} = \sum_k (\lambda_i\lambda_j)^{-n_k} = L_{ij}$$

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:

$$\begin{aligned}\sum_k A_{ik}\left(\frac{\lambda_i}{\lambda_j}\right)^{n_k} &= \frac{1}{N}\sum_{ks} B_{is}\left(\frac{\lambda_i}{\lambda_j\lambda_s}\right)^{n_k}\\ &= \frac{1}{N}\sum_s B_{is}R_{s,ij}\\ &= \frac{1}{N}(BR)_{i,ij}\end{aligned}$$

Thus the second condition on A reads $(BR)_{i,ij} = (BR)_{j,ij}$, and we are done. □

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. See [22].

Let us discuss now yet another interesting construction of complex Hadamard matrices, due to McNulty and Weigert [69]. The matrices constructed there generalize the Tao matrix T_6, and usually have the interesting feature of being isolated.

The construction in [69] uses the theory of MUB, as developed in [26], [48], but we will follow here a more direct approach, using basic Gauss sums, from [22].

The starting observation from [69] is as follows:

Theorem 5.14. *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 each of the matrices $\frac{1}{\sqrt{Q}}L_i^*R_j \in \sqrt{Q}U_Q$, with $i,j = 1,\ldots,N$, is Hadamard.

Proof. The check of the unitarity is done as follows:

$$\begin{aligned}< H_{ia}, H_{kc} > &= \frac{1}{Q}\sum_{jb} K_{ij}(L_i^*R_j)_{ab}\bar{K}_{kj}\overline{(L_k^*R_j)}_{cb}\\ &= \sum_j K_{ij}\bar{K}_{kj}(L_i^*L_k)_{ac}\\ &= N\delta_{ik}(L_i^*L_k)_{ac}\\ &= NQ\delta_{ik}\delta_{ac}\end{aligned}$$

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 5.15. *For $q\geq 3$ prime, the matrices $\{F_q, DF_q, \ldots, D^{q-1}F_q\}$, 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:

$$\frac{1}{\sqrt{q}}(E_i^*E_j)_{ab}=\frac{1}{\sqrt{q}}(F_q^*D^kF_q)_{ab}=\frac{1}{\sqrt{q}}\sum_c w^{c(b-a)}D_c^k$$

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. $\square$

We recall that the Legendre symbol is defined as follows:

$$\left(\frac{s}{q}\right)=\begin{cases}0 & \text{if } s=0\\ 1 & \text{if } \exists\,\alpha, s=\alpha^2\\ -1 & \text{if } \nexists\,\alpha, s=\alpha^2\end{cases}$$

Here, and in what follows, all the numbers are taken modulo q. We have:

Proposition 5.16. *The matrices $G_k = \frac{1}{\sqrt{q}} F_q^* D^k F_q$, with $D = diag(w^{\frac{c(c-1)}{2}})$ being as above, 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 $k \neq 0$ 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. $\square$

Let us combine now all the above results. We obtain the following statement:

Theorem 5.17. *Let $q \geq 3$ be prime, consider two subsets $S, T \subset \{0, 1, \ldots, q-1\}$ satisfying $|S| = |T|$ and $S \cap T = \emptyset$, and write $S = \{s_1, \ldots, s_N\}$ and $T = \{t_1, \ldots, t_N\}$. Then*

$$H_{ia,jb} = K_{ij} V_{b-a}^{t_j - s_i}$$

where V is as above, is Hadamard, provided that $K \in M_N(\mathbb{C})$ is.

Proof. This follows indeed by using the general construction in Theorem 5.14 above, with input coming from Proposition 5.15 and Proposition 5.16. $\square$

As explained in [69], the above construction covers many interesting examples of Hadamard matrices, known from [88], [89] 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 [69] 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 5.18. *The complex Hadamard matrix constructed in Theorem 5.17 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 [69]. For further details on all this, we refer to [69], and to [22].

As a final topic now, we would like to discuss an extension of a part of the above results, to the case of the partial Hadamard matrices. The extension, done in [22], 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 5.19. *Let $H \in X_{M,N}$ be a partial complex Hadamard matrix.*

1. *A deformation of H is a smooth function $f : \mathbb{T}_1 \to (X_{M,N})_H$.*
2. *The deformation is called "affine" if $f_{ij}(q) = H_{ij} q^{A_{ij}}$, with $A \in M_{M \times N}(\mathbb{R})$.*
3. *We call "trivial" the deformations $f_{ij}(q) = H_{ij} q^{a_i + b_j}$, with $a \in \mathbb{R}^M, b \in \mathbb{R}^N$.*

We have $X_{M,N} = M_{M \times N}(\mathbb{T}) \cap \sqrt{N} U_{M,N}$, 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. This remark leads us to:

Definition 5.20. *Associated to a point $H \in X_{M,N}$ are:*

(1) *The enveloping tangent space: $\widetilde{T}_H X_{M,N} = T_H M_{M\times N}(\mathbb{T}) \cap T_H \sqrt{N} U_{M,N}$.*
(2) *The tangent cone $T_H X_{M,N}$: the set of tangent vectors to the deformations of H.*
(3) *The affine tangent cone $T_H^\circ X_{M,N}$: same as above, using affine deformations only.*
(4) *The trivial tangent cone $T_H^\times X_{M,N}$: as above, using trivial deformations only.*

Observe that $\widetilde{T}_H X_{M,N}, T_H X_{M,N}$ are real vector spaces, and that $T_H X_{M,N}, T_H^\circ X_{M,N}$ are two-sided cones, $\lambda \in \mathbb{R}, A \in T \implies \lambda A \in T$. Also, we have inclusions as follows:

$$T_H^\times X_{M,N} \subset T_H^\circ X_{M,N} \subset T_H X_{M,N} \subset \widetilde{T}_H X_{M,N}$$

Since $\widetilde{T}_H X_{M,N}$ is a real vector space, of particular interest is the computation of its dimension $d(H) = \dim(\widetilde{T}_H X_{M,N})$, called defect of H. We have:

Theorem 5.21. *Let $H \in X_{M,N}$, and pick $K \in \sqrt{N} U_N$ extending H.*

(1) $\widetilde{T}_H X_{M,N} \simeq \{A \in M_{M\times N}(\mathbb{R}) | \sum_k H_{ik}\bar{H}_{jk}(A_{ik} - A_{jk}) = 0, \forall i,j\}$.
(2) $\widetilde{T}_H X_{M,N} \simeq \{E = (X\ Y) \in M_{M\times N}(\mathbb{C}) | X = X^*, (EK)_{ij}\bar{H}_{ij} \in \mathbb{R}, \forall i,j\}$.

The correspondence $A \to E$ is given by $E_{ij} = \sum_k H_{ik}\bar{K}_{jk}A_{ik}$, $A_{ij} = (EK)_{ij}\bar{H}_{ij}$.

Proof. The proofs here go as in the square case, as follows:

(1) In the square case this was done in the proof of Theorem 4.4 above, and the extension of the computations there to the rectangular case is straightforward.

(2) 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 (1) 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 5.22. *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

$$d(H) = N(N+1)/2 + M(N-M)$$

independently of the precise value of H.

Proof. We use Theorem 5.21 (2). 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:

$$\widetilde{T}_H X_{M,N} \simeq \{E = (X\ Y) \in M_{M\times N}(\mathbb{R}) | X = X^*\}$$

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 5.23. *Let $d(H) = \dim(\widetilde{T}_H X_{M,N})$.*

(1) *This number, called undephased defect of H, satisfies $d(H) \geq M + N - 1$.*
(2) *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 result.

(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 5.24. *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 [88], [89].

Let us discuss now some examples of isolated partial Hadamard matrices, and provide some evidence for Conjecture 5.24. We are interested in the following matrices:

Definition 5.25. *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 5.21, and we obtain:

Theorem 5.26. *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 5.21 (1). The defect equations there are as follows:

$$\sum_k F_{ik}\bar{F}_{jk}(A_{ik} - A_{jk}) = 0$$

Since for $F = F_{S,G}$ we have $F_{ik}\bar{F}_{jk} = (F^t)_{k,i-j}$, we obtain:

$$\widetilde{T}_F X_{M,N} = \left\{ A \in M_{M\times N}(\mathbb{R}) \Big| (AF^t)_{i,i-j} = (AF^t)_{j,i-j}, \forall i,j \right\}$$

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:

$$\widetilde{T}_F X_{M,N} = \left\{ A \in M_{M\times N}(\mathbb{R}) \Big| P = AF^t \text{ satisfies } P_{ij} = P_{i+j,j}, \forall i,j \right\}$$

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 5.26:

Theorem 5.27. *The defect of $F = F_{S,G}$ is the number* $\dim(K) + \dim(I)$*, where*

$$\begin{aligned} K &= \left\{ A \in M_{M\times N}(\mathbb{R}) \Big| AF^t = 0 \right\} \\ I &= \left\{ P \in L_M \Big| \exists A \in M_{M\times N}(\mathbb{R}), P = AF^t \right\} \end{aligned}$$

where L_M is the following linear space

$$L_M = \left\{ P \in M_M(\mathbb{C}) \big| P_{ij} = P_{i+j,j} = \bar{P}_{i,-j}, \forall i,j \right\}$$

with all the indices belonging by definition to the group G.

Proof. We use the general formula in Theorem 5.26. With the notations there, and with the linear space L_M being as above, we have a linear map as follows:

$$\Phi : \widetilde{T}_F X_{M,N} \to L_M \quad , \quad \Phi(A) = AF^t$$

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 5.26 we obtain the result. $\square$

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 5.28. *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 5.27, 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 [22].

6. Circulant matrices

We discuss in this section yet 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 6.1. *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.

Here is a basic, and very fundamental example of a circulant Hadamard matrix, which in addition has real entries, and is symmetric:

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

According to the CHC, explained in section 1, this matrix is, up to equivalence, the only circulant Hadamard matrix $H \in M_N(\pm 1)$, regardless of the value of $N \in \mathbb{N}$.

Our first purpose 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 6.2. *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 $s=8$:

$$\begin{bmatrix}0&0&0&0\\0&2&4&6\\0&4&0&4\\0&6&4&2\end{bmatrix}_8\sim\begin{bmatrix}0&1&4&1\\1&4&1&0\\4&1&0&1\\1&0&1&4\end{bmatrix}_8\sim\begin{bmatrix}4&1&0&1\\1&4&1&0\\0&1&4&1\\1&0&1&4\end{bmatrix}_8$$

We will explain later the reasons for denoting this matrix F_4'', instead of F_4'. $\square$

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 6.3. *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. $\square$

As a first conclusion, coming from the above considerations, we have:

Theorem 6.4. *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 2 above, according to the result of Haagerup [51], the Hadamard matrices at $N=2,3,4,5$ are, up to equivalence, those in the statement.

At $N=2,3$ the problem is solved by Proposition 6.2 above.

At $N=4$ now, our claim is that we have $K_4^q \sim F_4^s$, with $s=q^{-2}$. Indeed, 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 6.3.

At $N=5$, 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 [51]. □

Let us prove now that any Fourier matrix F_N can be put in circulant and symmetric form. We use Björck's cyclic root formalism [30], which is as follows:

Theorem 6.5. *Assume that $H \in M_N(\mathbb{T})$ is circulant, $H_{ij} = \gamma_{j-i}$. Then H is Hadamard if and only if the vector $(z_0, z_1, \ldots, z_{N-1})$ given by $z_i = \gamma_i/\gamma_{i-1}$ satisfies:*

$$\begin{aligned} z_0 + z_1 + \ldots + z_{N-1} &= 0 \\ z_0 z_1 + z_1 z_2 + \ldots + z_{N-1} z_0 &= 0 \\ &\ldots \\ z_0 z_1 \ldots z_{N-2} + \ldots + z_{N-1} z_0 \ldots z_{N-3} &= 0 \\ z_0 z_1 \ldots z_{N-1} &= 1 \end{aligned}$$

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 [30]. □

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:

$$\gamma = (z_0, z_0 z_1, z_0 z_1 z_2, \ldots\ldots, z_0 z_1 \ldots z_{N-1})$$

Now back to the Fourier matrices, we have the following result:

Theorem 6.6. *Given $N \in \mathbb{N}$, set $\nu = e^{\pi i/N}$ and $q = \nu^{N-1}, w = \nu^2$. Then*

$$(q, qw, qw^2, \ldots, qw^{N-1})$$

is a cyclic N-root, 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 6.5 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 6.5, this states in our case that we must have $q^N w^{\frac{N(N-1)}{2}} = 1$, and so that we must have $q^N = (-1)^{N-1}$.

We conclude that 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 6.5. We have:

$$\begin{aligned}
\gamma_k = \gamma_{-k}, \forall k \quad &\iff \quad q^{k+1} w^{\frac{k(k+1)}{2}} = q^{-k+1} w^{\frac{k(k-1)}{2}}, \forall k \\
&\iff \quad q^{2k} w^k = 1, \forall k \\
&\iff \quad q^2 = w^{-1}
\end{aligned}$$

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 $H \sim F_N$. 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 matrix $H' = (H_{-i,j})$. Now regarding 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 H' is equivalent to the matrix H'' obtained 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 6.7. *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 6.6, 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 $w = \nu^2 = e^{2\pi i/5}$, 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. $\square$

Regarding the above matrix F'_4, observe that this is equivalent to the matrix F''_4 from Proposition 6.2, 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 6.8. *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 6.6 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 6.6, coming from Backelin's work in [3], and remaining in the circulant and symmetric setting:

Theorem 6.9. *Let $M|N$, and set $w=e^{2\pi i/N}$. We have a cyclic root as follows,*

$$(\underbrace{q_1,\ldots,q_M}_M,\underbrace{q_1w,\ldots,q_Mw}_M,\ldots\ldots,\underbrace{q_1w^{N-1},\ldots,q_Mw^{N-1}}_M)$$

provided that $q_1,\ldots,q_M\in\mathbb{T}$ satisfy $(q_1\ldots q_M)^N=(-1)^{M(N-1)}$. Moreover, assuming

$$q_1q_2=1\quad,\quad q_3q_M=q_4q_{M-1}=\ldots=w$$

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:

$$\begin{aligned}\sum_i z_{i+1}\ldots z_{i+K}&=\begin{pmatrix}q_1\ldots q_K+q_2\ldots q_{K+1}+\ldots\ldots+q_{M-K+1}\ldots q_M\\+q_{M-K+2}\ldots q_Mq_1w+\ldots\ldots+q_Mq_1\ldots q_{K-1}w^{K-1}\end{pmatrix}\\&\quad\times(1+w^K+w^{2K}+\ldots+w^{(N-1)K})\end{aligned}$$

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:

$$\prod_i z_i=(q_1\ldots q_M)^N(1\cdot w\cdot w^2\ldots w^{N-1})^M=(q_1\ldots q_M)^Nw^{\frac{MN(N-1)}{2}}$$

By using $w=e^{2\pi i/N}$ we obtain that the coefficient on the right is:

$$w^{\frac{MN(N-1)}{2}}=e^{\frac{2\pi i}{N}\cdot\frac{MN(N-1)}{2}}=e^{\pi iM(N-1)}=(-1)^{M(N-1)}$$

Thus, if $(q_1\ldots q_M)^N=(-1)^{M(N-1)}$, we obtain a cyclic root, as stated. See [3], [49].

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:

$$H=\begin{pmatrix}
q_1 & q_1q_2 & q_1q_2q_3 & q_1q_2q_3q_4 & q_1q_2q_3q_4q_5 & \ldots\\
1 & q_1 & q_1q_2 & q_1q_2q_3 & q_1q_2q_3q_4 & \ldots\\
\frac{w}{q_M} & 1 & q_1 & q_1q_2 & q_1q_2q_3 & \ldots\\
\frac{w^2}{q_{M-1}q_M} & \frac{w}{q_M} & 1 & q_1 & q_1q_2 & \ldots\\
\frac{w^3}{q_{M-2}q_{M-1}q_M} & \frac{w^2}{q_{M-1}q_M} & \frac{w}{q_M} & 1 & q_1 & \ldots\\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots
\end{pmatrix}$$

We are therefore led to the symmetry conditions in the statement, and we are done. □

Observe that Theorem 6.9 generalizes both Proposition 6.3, and the construction in Theorem 6.6. Thus, we have here a full generalization of Theorem 6.4. Of course, things do not stop here, and the problem of unifying Theorem 6.8 and Theorem 6.9 remains.

As a conclusion to what we have so far, there is definitely no analogue of the CHC in the general complex setting, due to the fact that F_N can be put in circulant form, and this latter result gives rise to a number of interesting generalizations and questions.

However, still in relation with the CHC, but at a more technical level, the problem of investigating the existence of the circulant Butson matrices appears.

The first result in this direction, due to Turyn [93], is as follows:

Proposition 6.10. *The size of a circulant Hadamard matrix*

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

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, the quantity on the left is $<H_0,H_0>=N$. Thus N is a square, and together with the fact that $N\in 2\mathbb{N}$, this gives $N=4n^2$, with $n\in\mathbb{N}$. □

Also found by Turyn in [93] 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 6.11. *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:*

$$\sum_{ik}w^ka_ia_{i+k}=N$$

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 6.12. *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 Proposition 3.3 above, that when l is prime, the vanishing sums of l-roots of unity are exactly the sums of the following type, with $c \in \mathbb{N}$:

$$S = c + cw + \ldots + cw^{l-1}$$

Thus the Turyn obstruction is equivalent to the following 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:

$$(a_0^2 + a_1^2 + a_2^2 + a_3^2) + i \sum a_i a_{i+1} - 2(a_0 a_2 + a_1 a_3) - i \sum a_i a_{i+1} = N$$

Thus the imaginary terms cancel, and we obtain the formula in the statement. □

The above results are of course just some basic, elementary 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 [18], [39].

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. Observe that $F_N = \sqrt{N}F$ is the usual Fourier Hadamard matrix.

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, the above-mentioned linear algebra result is as follows:

Theorem 6.13. *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:

$$Q_{ij} = \frac{1}{N}\sum_{kl} w^{jl-ik}\xi_{l-k} = \delta_{ij}\sum_r w^{jr}\xi_r$$

Also, if $Q = diag(q)$ is diagonal then $H = FQF^*$ is circulant, given by:

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

Observe that this latter formula proves as well the last assertion, $\xi = Fq/\sqrt{N}$. □

In relation now with the orthogonal and unitary matrices, we have:

Proposition 6.14. *The various sets of circulant matrices are as follows:*

(1) $M_N(\mathbb{C})^{circ} = \{FQF^* | q \in \mathbb{C}^N\}$.
(2) $U_N^{circ} = \{FQF^* | q \in \mathbb{T}^N\}$.
(3) $O_N^{circ} = \{FQF^* | q \in \mathbb{T}^N, \bar{q}_i = q_{-i}, \forall i\}$.

In addition, the first row vector of FQF^* is given by $\xi = Fq/\sqrt{N}$.

Proof. All this follows from Theorem 6.13, as follows:
(1) This assertion, along with the last one, is Theorem 6.13 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 6.15. *The sets of complex and real circulant Hadamard matrices are:*

$$X_N^{circ} = \{\sqrt{N}FQF^* | q \in \mathbb{T}^N\} \cap M_N(\mathbb{T})$$

$$Y_N^{circ} = \{\sqrt{N}FQF^* | q \in \mathbb{T}^N, \bar{q}_i = q_{-i}\} \cap M_N(\pm 1)$$

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 6.14 above. □

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 [52]:

Theorem 6.16. *When N is prime, the number of circulant $N\times N$ complex Hadamard matrices, counted with certain multiplicities, is exactly $\binom{2N-2}{N-1}$.*

Proof. This is something advanced, using a variety of techiques from Fourier analysis, number theory, complex analysis and algebraic geometry. The idea in [52] is that, when N is prime, Björck's cyclic root formalism can be further manipulated, by using Fourier transforms, and we are eventually led to a simpler system of equations.

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.

With this finiteness result in hand, the precise count can be done as well, by using various techniques from classical algebraic geometry. See [52]. □

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 [30], [31], [32], [52].

Our belief is that useful here would be an adaptation of the notion of defect, to the circulant case, in the context of the manifolds from Proposition 6.14 and Theorem 6.15. There are some preliminary differential geometry computations to be done here.

We would like to discuss now an alternative take on these questions, based on the estimate $||U||_1\leq N\sqrt{N}$ from Theorem 1.18. This shows that the real Hadamard matrices are the rescaled versions of the maximizers of the 1-norm on O_N, and the same proof shows that the complex Hadamard matrices are the rescaled versions of the maximizers of the 1-norm on U_N. Following [18], we will apply this philosophy to the circulant case.

We will need in fact more general p-norms as well, so let us start with the following result, in the complex case, which is the most general one on the subject:

Proposition 6.17. *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 precisely by the rescaled Hadamard matrices.

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

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

For ψ concave the reverse inequality holds. Also, the equality case holds either when ψ is linear, or when the numbers $x_1,\ldots,x_n$ are all equal.

In our case, with $n=N^2$ and with $\{x_1,\ldots,x_n\}=\{|U_{ij}|^2|i,j=1,\ldots,N\}$, 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 $F(U)\geq N^2\psi(1/N)$, and 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 lead to:

Theorem 6.18. *The rescaled versions $U=H/\sqrt{N}$ of the complex Hadamard matrices $H\in M_N(\mathbb{C})$ can be characterized as being:*

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

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 $\psi(x)=x^{p/2}$, Proposition 6.17 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. □

As explained in [18], the most adapted exponent for the circulant case is $p=4$, due to a number of simplifications which appear in the Fourier manipulations. So, before discussing this, let us record the $p=4$ particular case of Theorem 6.18:

Proposition 6.19. *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 Theorem 6.18, or directly from Cauchy-Schwarz, as follows:

$$||U||_4^4=\sum_{ij}|U_{ij}|^4\geq\frac{1}{N^2}\left(\sum_{ij}|U_{ij}|^2\right)^2=1$$

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 6.20. *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:*

$$\Phi=\sum_{i+k=j+l}\frac{q_iq_k}{q_jq_l}$$

Then Φ is real, and we have $\Phi\geq N^2$, with equality if and only if $\sqrt{N}q$ 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 6.13 and Proposition 6.14, and the formula $\xi=Fq/\sqrt{N}$ there, we have:

$$\begin{aligned}
||U||_4^4&=N\sum_s|\xi_s|^4\\
&=\frac{1}{N^3}\sum_s|\sum_i w^{si}q_i|^4\\
&=\frac{1}{N^3}\sum_s\sum_i w^{si}q_i\sum_j w^{-sj}\bar{q}_j\sum_k w^{sk}q_k\sum_l w^{-sl}\bar{q}_l\\
&=\frac{1}{N^3}\sum_s\sum_{ijkl}w^{(i-j+k-l)s}\frac{q_iq_k}{q_jq_l}\\
&=\frac{1}{N^2}\sum_{i+k=j+l}\frac{q_iq_k}{q_jq_l}
\end{aligned}$$

Thus Proposition 6.19 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. □

We have the following more direct explanation of the above result:

Proposition 6.21. *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. □

All this is quite interesting. As an application, in the real Hadamard matrix case, we have the following analytic reformulation of the CHC, from [18]:

Theorem 6.22. *For $q \in \mathbb{T}^N$ 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 $\Phi \geq N^2$. The CHC states that we cannot have equality at $N > 4$.

Proof. This follows indeed from Theorem 6.20, via the identifications from Theorem 6.15, the parameter space in the real case being $\{q \in \mathbb{T}^N | \bar{q}_i = q_{-i}\}$. □

This is certainly quite nice, and the analytic problem might look quite elementary. However, this is not the case. In fact, we already know from section 1 that the CHC is equivalent to Ryser's conjecture, which looks elementary as well, and is not.

Following [18], let us further discuss all this. We first have:

Theorem 6.23. *Write $\Phi = \Phi_0 + \ldots + \Phi_{N-1}$, 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 6.20 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:

$$\Phi_i = N\sum_s w^{si} q_i \bar{\xi}_s = N\sqrt{N} q_i \overline{(F^*\xi)}_i = N q_i \bar{q}_i = N$$

Thus, we have obtained the conclusion in the statement. □

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 the result is:

Proposition 6.24. *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. $\square$

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 6.25. *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 [19]. $\square$

Regarding now the real case, an analogue of Proposition 6.25 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 $\tilde{\Phi} = |\sum_i q_i|^4$.

We will be back to this a bit later. For the moment, let us do some combinatorics:

Proposition 6.26. *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 $\binom{2p}{\pi}=\binom{2p}{b_1,\ldots,b_{|\pi|}}$, 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 $\pi=\ker\big(i_1k_1\ldots i_pk_p\big)$, and this gives the formula in the statement. $\square$

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 6.27. *We have the moment formula*

$$\int_{\mathbb{T}^N}|\sum_i q_i|^{2p}\,dq=\sum_k C_{pk}\frac{N!}{(N-k)!}$$

where $C_{pk}=\sum_{\pi\in P(p),|\pi|=k}\binom{p}{b_1,\ldots,b_{|\pi|}}$*, with* $b_1,\ldots,b_{|\pi|}$ *being the lengths of the blocks of* π*.*

Proof. This follows indeed exactly as Proposition 6.26 above, by replacing the exponent p by the exponent $p/2$, and by splitting the resulting sum as in the statement. □

Observe that the above formula basically gives the moments of $\tilde{\Phi}$, in the real case. Indeed, let us restrict attention to the case $N=2m$. Then, for the purposes of our minimization problem we can assume that our vector is of the following form:

$$q=(1,q_1,\ldots,q_{m-1},1,\bar{q}_{m-1},\ldots,\bar{q}_1)$$

So, we are led to the following conclusion, relating the real and complex cases:

Proposition 6.28. *Consider the variable* $X=q_1+\ldots+q_{m-1}$ *over the torus* $\mathbb{T}^{m-1}$*.*

1. *For the complex problem at* $N=m-1$*, we have* $\widetilde{\Phi}=|X|^4$
2. *For the real problem at* $N=2m$*, we have* $\widetilde{\Phi}=|2+X+\bar{X}|^4$*.*

Proof. This is indeed clear from the definition of the enveloping sum $\widetilde{\Phi}$. □

Finally, here is a random walk formulation of the problem:

Proposition 6.29. *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 6.27, and the second assertion follows from the formula in Proposition 6.25. □

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.

7. Bistochastic matrices

In this section and the next two ones we discuss certain analytic aspects of the complex Hadamard matrices, based on the various inequalities obtained in section 1. We will extend these inequalities to the complex case, and discuss them in detail.

As a first, fundamental result, we have:

Theorem 7.1. *The complex Hadamard matrices, which form the manifold*

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

can be analytically detected in two ways, as follows:

(1) *Given $H \in M_N(\mathbb{T})$ we have $|\det(H)| \leq N^{N/2}$, with equality when $H \in \sqrt{N} U_N$.*
(2) *Given $H \in \sqrt{N} U_N$ we have $||H||_1 \leq N^2$, with equality when $H \in M_N(\mathbb{T})$.*

Proof. This is something that we already know in the real case, from Theorem 1.17 and Theorem 1.18 above, and the proof in the general case is similar:

(1) This follows indeed as in the real case, because if we denote by $H_1, \ldots, H_N \in \mathbb{T}^N$ the rows of H, then we have, according to the definition of the determinant:

$$\begin{aligned} |\det(H)| &= vol < H_1, \ldots, H_N > \\ &\leq ||H_1|| \times \ldots \times ||H_N|| \\ &= (\sqrt{N})^N \end{aligned}$$

The equality holds when $H_1, \ldots, H_N$ are pairwise orthogonal, as claimed.

(2) This is something that we discussed in much detail in Proposition 6.17, Theorem 6.18 and Proposition 6.19, and which follows from Cauchy-Schwarz:

$$||H||_1 = \sum_{ij} |H_{ij}| \leq N \left(\sum_{ij} |H_{ij}|^2 \right)^{1/2} = N^2$$

The equality case holds when $|H_{ij}| = 1$ for any i, j, as claimed. $\square$

We will further discuss all this in section 9 below, with a few comments on (1), and with a detailed study of the condition (2), which is something quite fruitful.

Regarding now the third and last basic inequality from the real case, namely the excess estimate from Theorem 1.19, this is something of a different nature, that we will discuss in this section, and in the next one. Let us begin with the following definition:

Definition 7.2. *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 6. Indeed, assuming that $H_{ij}=\xi_{j-i}$ is circulant, all rows and columns sum up to:

$$\lambda=\sum_i\xi_i$$

So, let us first review the material in section 6, from this perspective. As a first and trivial remark, the Fourier matrix F_2 looks better in bistochastic form:

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

This is something quite interesting, philosophically speaking. Indeed, we have here a new idea, namely that of studying the 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.

We will see later on that, while certainly being viable, this idea is quite difficult to develop in practice, and is in need of some considerable preliminary work.

Let us keep now reviewing the material in section 6. According to the results there, and to the above-mentioned fact that circulant implies bistochastic, we have:

Theorem 7.3. *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:

$$\sum_{ia}(H\otimes K)_{ia,jb}=\sum_{ia}H_{ij}K_{ab}=\sum_iH_{ij}\sum_aK_{ab}=\lambda\mu$$

$$\sum_{jb}(H\otimes K)_{ia,jb}=\sum_{jb}H_{ij}K_{ab}=\sum_jH_{ij}\sum_bK_{ab}=\lambda\mu$$

Thus, the matrix $H\otimes K$ is bistochastic as well. As for the assertions (1,2,3), we already know all this, from Theorem 6.6, Theorem 6.8 and Theorem 6.9 above. $\square$

In the above list of examples, (2) is the key entry. Indeed, while many interesting 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, when using a decomposition of type $G=\mathbb Z_{N_1}\times\ldots\times\mathbb Z_{N_k}$, and setting $F_G'=F_{N_1}'\otimes\ldots\otimes F_{N_k}'$, we can only say that 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 7.4. *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:

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

(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, respectively column-stochastic with sums λ, reads:

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

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. □

Here is another basic result, that we will need as well in what follows:

Proposition 7.5. *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 7.4, we obtain the result. $\square$

Finally, here is an extension of the excess inequality from Theorem 1.19 above:

Theorem 7.6. *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. Moreover, if we assume $H\xi = \lambda\xi$, the above computation gives $|\lambda|^2 = N$, and by Proposition 7.4, we obtain the result. $\square$

The above estimate is potentially quite useful, because it allows us to analytically locate the bistochastic Hadamard manifold X_N^{bis} inside the whole Hadamard manifold X_N, a bit in the spirit of the two analytic methods in Theorem 7.1. We will be back to this later, with a number of probabilistic results on the subject.

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 7.7. *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 7.4 and Proposition 7.5 above. □

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 [57].

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 [57]:

Proposition 7.8. *For a unitary matrix $U \in U_N$, the following are equivalent:*

1. *There exist $L, R \in U_N$ diagonal such that $U' = LUR$ is bistochastic.*
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) $\implies$ (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:

$$R = diag(g_1, \ldots, g_N) \quad , \quad \bar{L} = diag((Ug)_1, \ldots, (Ug)_N)$$

We have then $R\xi = g$ and $\bar{L}\xi = Ug$, and so $U' = LUR$ 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 [57], we have:

Theorem 7.9. *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 7.8 (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 [29], [35] states that $\mathbb{T}^{N-1}$ cannot be displaced from itself via a Hamiltonian isotopy.

Thus, the results in [29], [35] 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 7.8. See [57]. □

In relation now with our Hadamard matrix questions, we have:

Theorem 7.10. *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 7.9, 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 $\mathbb{T}$. □

All this is extremely interesting, but unfortunately, not explicit. As explained in [57], the various technical results from [29], [35] 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 $|z|=1$.

Summarizing, 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 [29], [35].

Regarding this latter question, a possible approach comes from the excess result from Theorem 7.6 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 7.11. *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 $E=\sum_{ij}H_{ij}$, 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 7.11.

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 [50], [82], 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 7.12. *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 7.13. *The glow of any Hadamard matrix $H\in M_N(\mathbb C)$, or more generally of any $H\in\sqrt NU_N$, 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 7.6 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 7.9 that H can be put in bistochastic form. According to Proposition 7.7, 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 7.12, we obtain from this $N\sqrt{N}\,\mathbb{T}\subset supp(\mu)$, as claimed. $\square$

The challenging question is that of obtaining a proof of the above result by using probabilistic techniques. Indeed, as explained at the end of section 6 above, the support of a measure can be recaptured from the moments, simply by computing a limit. Thus, knowing the moments of the glow well enough would solve the problem.

Regarding the moments of the glow, the formula is as follows:

Proposition 7.14. *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 7.15. *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 7.13, this upper bound is known to be $\leq N^3$ by Cauchy-Schwarz, and the equality holds by [57]. □

To conclude now, the challenging question is that of finding a direct proof for Theorem 7.15. All this would provide an alternative aproach to the results in [57], 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 9 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 7.3, coming from the circulant matrix considerations in section 6. 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, extending the finding from Proposition 7.4 above:

Proposition 7.16. *Assuming that $H_N(l)$ contains a bistochastic matrix, the equations*

$$\begin{aligned} a_0 + a_1 + \ldots + a_{l-1} &= N \\ |a_0 + a_1 w + \ldots + a_{l-1}w^{l-1}|^2 &= N \end{aligned}$$

must have solutions, over the positive integers.

Proof. This is a reformulation of the equality $|\lambda|^2 = N$, from Proposition 7.4 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:

$$\lambda = a_0 + a_1 w + \ldots + a_{l-1}w^{l-1}$$

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 6 above. At very small values of l, the obstructions are as follows:

Theorem 7.17. *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 7.16.

(2) This is best viewed by using Proposition 7.16, and the following formula, that we already know, from section 3 above:

$$|a+bw+cw^2|^2=\frac{1}{2}[(a-b)^2+(b-c)^2+(c-a)^2]$$

At the level of the concrete obstructions, we must have for instance $5\not|N$. 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 7.16, and from $|a+ib|^2=a^2+b^2$. $\square$

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 [63].

In order to reach, however, to a number of positive results, beyond those in Theorem 7.3, 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 7.18. *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 7.19. *The deformations of $F_2\otimes F_2$, with parameter matrix $Q=\left(\begin{smallmatrix}p&q\\r&s\end{smallmatrix}\right)$,*

$$F_2\otimes_Q F_2=\begin{pmatrix}p&q&p&q\\p&-q&p&-q\\r&s&-r&-s\\r&-s&-r&s\end{pmatrix}$$

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. $\square$

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 7.20. *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 $L_{ia,jb} = Q_{ib} H_{ij} K_{ab}$. 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:

$$\begin{aligned}
S'_{ia} &= \sum_{jb} R_{jb} Q_{ib} H_{ij} K_{ab} \\
&= \sum_b K_{ab} Q_{ib} \sum_j H_{ij} R_{jb} \\
&= \sum_b K_{ab} Q_{ib} (HR)_{ib}
\end{aligned}$$

In terms of the variables $C_b^i = Q_{ib}(HR)_{ib}$, these 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 $KC^i = \sqrt{MN} x^i$ for any i, and by multiplying to the left by the adjoint matrix 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:

$$\sqrt{N} Q_{ib} (HR)_{ib} = \sqrt{M} (K^* x^i)_b \quad , \quad \forall i, b$$

With $G_{ib} = (K^* x^i)_b / Q_{ib}$ as in the statement, this condition reads:

$$\sqrt{N} (HR)_{ib} = \sqrt{M} G_{ib} \quad , \quad \forall i, b$$

But this condition is equivalent to $\sqrt{N}HR=\sqrt{M}G$, and by multiplying to the left by the adjoint matrix H^*, we are led to the following condition:

$$\sqrt{MN}R=H^*G$$

Thus, we have obtained the condition in the statement. □

As an illustration for this 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 $x_a^i=y_iz_a$, with $Q=1$ we have:

$$G_{ib}=(K^*x^i)_b=[K^*(y_iz)]_b=y_i(K^*z)_b$$

We therefore obtain the following formula:

$$\begin{aligned}(H^*G)_{ib}&=\sum_j(H^*)_{ij}G_{jb}\\&=\sum_j(H^*)_{ij}y_j(K^*z)_b\\&=(H^*y)_i(K^*z)_b\end{aligned}$$

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 7.21. *A deformed tensor product $F_M\otimes_QK$ 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:

$$\sum_jG_{jb}\bar{G}_{j+l,b}=MN\delta_{l,0}\quad,\quad\forall l,b$$

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 7.20, and with $w=e^{2\pi i/M}$, we have:

$$(H^*G)_{ib}=\sum_jw^{-ij}G_{jb}$$

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 7.20 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:

$$v^b = NF_M^*\xi = \begin{pmatrix} MN\\ 0\\ \vdots\\ 0\end{pmatrix} \quad , \quad \forall b$$

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 7.20 that we have $G_{jb} = (K^* x^j)_b / Q_{jb}$, for certain numbers $x_b^j \in \mathbb{T}$. Since we have $Q_{jb} \in \mathbb{T}$ and $K^*/\sqrt{N} \in U_N$, we obtain:

$$\begin{aligned}\sum_b |G_{jb}|^2 &= \sum_b |(K^* x^j)_b|^2\\ &= ||K^* x^j||_2^2\\ &= N||x^j||_2^2\\ &= N^2\end{aligned}$$

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. □

As an illustration for this result, let us go back to the $Q = 1$ situation, explained after Theorem 7.20. 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 7.19 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 entries of G:

$$G_{0b} = \frac{\left[\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}q\\ -q\end{pmatrix}\right]_b}{Q_{0b}} = \frac{\begin{pmatrix}0\\ 2q\end{pmatrix}_b}{Q_{0b}}$$

$$G_{1b} = \frac{\left[\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}r\\ r\end{pmatrix}\right]_b}{Q_{1b}} = \frac{\begin{pmatrix}2r\\ 0\end{pmatrix}_b}{Q_{1b}}$$

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 7.21 are satisfied.

As a main application now, we have the following result:

Theorem 7.22. *The Diţă deformations $F_N \otimes_Q F_N$ can be put in almost bistochastic form, independently of the value of the parameter matrix $Q \in M_N(\mathbb{T})$.*

Proof. We use Proposition 7.21 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 7.21 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:

$$\sum_j G_{jb}\bar{G}_{jb} = N^2 \sum_j \delta_{j-1,b} = N^2$$

Thus, the conditions in Proposition 7.21 are satisfied, and we obtain the result. □

Here is an equivalent formulation of the above result:

Theorem 7.23. *The matrix $F_N \otimes'_Q F_N$, with $Q \in M_N(\mathbb{T})$, defined by*

$$(F_N \otimes'_Q F_N)_{ia,jb} = \frac{w^{ij+ab}}{w^{bj+j}} \cdot \frac{Q_{ib}}{Q_{b+1,b}}$$

where $w = e^{2\pi i/N}$ is almost bistochastic, and equivalent to $F_N \otimes_Q F_N$.

Proof. Our claim is that this is the matrix constructed in the proof of Theorem 7.22. Indeed, let us first go back to the proof of Theorem 7.20. In the case $M = N$ and $H = K = F_N$, the Diţă deformation $L = H \otimes_Q K$ 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 7.22, 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 7.21 that the choice of G which makes work Theorem 7.22 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:

$$\begin{aligned}
R_{jb} &= \frac{1}{N}(H^*G)_{jb}\\
&= \frac{1}{N}\sum_i w^{-ij}G_{ib}\\
&= \sum_i w^{ij}\cdot\frac{\delta_{i-1,b}}{Q_{ib}}\\
&= \frac{w^{-(b+1)j}}{Q_{b+1,b}}
\end{aligned}$$

Thus, the modified version of $F_N\otimes_Q F_N$ 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. $\square$

As an illustration, let us work out the case $N=2$. Here we have $w=-1$, and with $Q=\left(\begin{smallmatrix}p&q\\ r&s\end{smallmatrix}\right)$, and then with $u=\frac{p}{r},v=\frac{s}{q}$, we obtain the following matrix:

$$F_2\otimes_Q F_2=\begin{pmatrix}\frac{p}{r}&\frac{q}{q}&-\frac{p}{r}&\frac{q}{q}\\ \frac{p}{r}&-\frac{q}{q}&-\frac{p}{r}&-\frac{q}{q}\\ \frac{r}{r}&\frac{s}{q}&\frac{r}{r}&-\frac{s}{q}\\ \frac{r}{r}&-\frac{s}{q}&\frac{r}{r}&\frac{s}{q}\end{pmatrix}=\begin{pmatrix}u&1&-u&1\\ u&-1&-u&-1\\ 1&v&1&-v\\ 1&-v&1&v\end{pmatrix}$$

Observe that this matrix is indeed almost bistochastic, with row sums $2,-2,2,2$.

It is quite unclear on how to get beyond these results. An interesting question here would be probably that of focusing on the real case, and see if the Hadamard matrices there, $H\in M_N(\pm 1)$, 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.

8. Glow computations

We discuss here the computation of the glow, in the $N \to \infty$ limit. We have seen in section 1 that, in what concerns the real glow of the real Hadamard matrices, with $N \to \infty$ we obtain a real Gaussian measure. Our main purpose here will be that of establishing a similar result in the complex case, stating that for the complex glow of the complex Hadamard matrices, with $N \to \infty$ we obtain a complex Gaussian measure.

The computations in the complex case are considerably more involved than those in the real case, and will require a lot of combinatorics. Also, we will investigate the problem of getting beyond the $N \to \infty$ limiting result, with formulae at order $1, 2, 3, 4$.

As a first motivation for all this, we have the Gale-Berlekamp game [50], [82]. Another motivation comes from the questions regarding the bistochastic matrices, in relation with [57], explained in section 7. Finally, we have the question of connecting and computing the defect, and other invariants of the Hadamard matrices, in terms of the glow.

Let us begin by reviewing the few theoretical things that we know about the glow, from section 7 above. The main results there can be summarized as follows:

Theorem 8.1. *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 7, the idea being as follows:
(1) This follows by using $H \to zH$ with $|z| = 1$, as explained in Proposition 7.12.
(2) This follows from (1), the convolution with ε bringing the invariance.
(3) This folllows from Cauchy-Schwarz, as explained in Theorem 7.13.
(4) This is something highly non-trivial, coming from [57]. □

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 value $||H||_2 = N$. Note that this is always the case with the Hadamard matrices, and more generally with the matrices $H \in \sqrt{N} U_N$.

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 well-known formula $\mathbb{E}(|z|^{2p}) = p!$.

Finally, we use the symbol $\sim$ to denote an equality of distributions. We have:

Proposition 8.2. *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 8.1, and the moment method:

(1) Here we have $E=\sqrt{N}\sum_i a_ib_i$, with $a,b\in\mathbb{T}^N$ random, and 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 $E=\sum_{ij}a_ib_j=\sum_i a_i\sum_j b_j$, and this gives the first assertion. Now since $a,b\in\mathbb{T}^N$ are independent, so are the quantities $\sum_i a_i,\sum_j b_j$, 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. $\square$

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 [78]. Also, as explained for instance in section 6, 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 8.3. *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:

$$|E|^2 = |ac + ad + bc - bd|^2 = 4 + \frac{ad}{bc} + \frac{bc}{ad} - \frac{bd}{ac} - \frac{ac}{bd}$$

For proving that $\alpha = \frac{ad}{bc}$ and $\beta = \frac{bd}{ac}$ are independent, we use the moment method:

$$\int_{\mathbb{T}^4} \left(\frac{ad}{bc}\right)^p \left(\frac{bd}{ac}\right)^q = \int_{\mathbb{T}} a^{p-q} \int_{\mathbb{T}} b^{q-p} \int_{\mathbb{T}} c^{-p-q} \int_{\mathbb{T}} d^{p+q} = \delta_{p,q,0}$$

Thus α, β are indeed independent, and we are done. $\square$

Observe that $law(|E|^2)$, and hence $law(E)$, is uniquely determined by the above result. 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 $|E|^2 = 9 + C_0 + C_1 w + C_2 w^2$, where 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 in the real case. We have here the following result:

Theorem 8.4. *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 $B(c_1, \ldots, c_N) = law(\sum_i \lambda_i c_i)$, with $\lambda \in \mathbb{T}^N$ random.

Proof. This is indeed clear from the formula $E = < a, Hb >$, because when $a \in \mathbb{T}^N$ is fixed, E follows the law $B((Ha)_1, \ldots, (Ha)_N)$ in the statement. $\square$

Observe that we can write $B(c_1, \ldots, c_N) = \varepsilon \times \beta(|c_1|, \ldots, |c_N|)$, where the measure $\beta(r_1, \ldots, r_N) \in \mathcal{P}(\mathbb{R}_+)$ with $r_1, \ldots, r_N \geq 0$ is given by $\beta(r_1, \ldots, r_N) = law|\sum_i \lambda_i r_i|$. Regarding now the computation of β, we have:

$$\beta(r_1, \ldots, r_N) = law\sqrt{\sum_{ij} \frac{\lambda_i}{\lambda_j} \cdot r_i r_j}$$

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:

$$\beta(r_1, \ldots, r_N) = law\sqrt{\sum_{ij} \mu_i \mu_{i+1} \ldots \mu_j \cdot r_i r_j}$$

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 8.4.

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 [50], [82] and with the work in section 1. We have the following unifying formalism:

Definition 8.5. *Given $H \in M_N(\mathbb{C})$ and $s \in \mathbb{N} \cup \{\infty\}$, we define $\mu_s \in \mathcal{P}(\mathbb{C})$ by*

$$\int_{\mathbb{C}} \varphi(x) d\mu_s(x) = \int_{\mathbb{Z}_s^N \times \mathbb{Z}_s^N} \varphi\left(\sum_{ij} a_i b_j H_{ij}\right) d(a,b)$$

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 8.1. Also, at $s = 2$ and for a usual Hadamard matrix, $H \in M_N(\pm 1)$, we obtain the measure from section 1.

Observe that for $H \in M_N(\pm 1)$, 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 8.6. *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:

$$V = (\underbrace{1 \ldots 1}_{a_0} \underbrace{w \ldots w}_{a_1} \ldots\ldots \underbrace{w^{s-1} \ldots w^{s-1}}_{a_{s-1}})$$

We have then $|1 \in V| = a_0$ and $\sum V_i = a_0 + a_1 w + \ldots + a_{s-1} w^{s-1}$, and 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 $a_0 + a_1 w + \ldots + a_{s-1} w^{s-1}$ 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. $\square$

As an illustration, at $s = 3$ we can write $E = a + bw + cw^2$, and we have:

$$Re(E) = a - \frac{b+c}{2} = a - \frac{n-a}{2} = \frac{3a-n}{2}$$

At $s = 5$, however, is it now clear how to explicitely solve the problem. In fact, the problem of finding an explicit formula is related to the question of relating the complex probability measures $\mu_s = law(E)$ for a given matrix $H \in M_N(\mathbb{T})$, at various values of $s \in \mathbb{N} \cup \{\infty\}$. Note that Theorem 8.6 tells us that for a matrix $H \in M_N(\mathbb{Z}_s)$ with s prime, the measure μ_2 can be recaptured from the knowledge of μ_s.

Let us investigate now the glow of the complex Hadamard matrices, by using the moment method. We use the moment formula from section 7, namely:

Proposition 8.7. *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 7, 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. □

As a first application, let us investigate the tensor products. We have:

Proposition 8.8. *The even moments of $|E|$ for $L = H \otimes K$ are given by*

$$\int_{\mathbb{T}^{NM} \times \mathbb{T}^{NM}} |E|^{2p} = \sum_{[ia]=[kc],[jb]=[ld]} \frac{H_{i_1j_1}\ldots H_{i_pj_p}}{H_{k_1l_1}\ldots H_{k_pl_p}} \cdot \frac{K_{a_1b_1}\ldots K_{a_pb_p}}{K_{c_1d_1}\ldots K_{c_pd_p}}$$

where the sets between brackets are as usual sets with repetition.

Proof. With $L = H \otimes K$, the formula in Proposition 8.7 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. □

The above result is quite bad news. Indeed, we cannot reconstruct the glow of $H \otimes K$ from that of H, K, because the indices "get mixed".

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 $\sqcap\!\sqcap \ldots \leq \pi \leq |\,|\ldots|$, for any $\pi \in P(p)$. 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 set $\binom{p}{\pi} = \binom{p}{b_1 \ldots b_{|\pi|}} = \frac{p!}{b_1! \ldots b_{|\pi|}!}$, where $b_1, \ldots, b_{|\pi|}$ are the block lenghts. 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 8.9. *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 $I(\pi) = \frac{1}{N^{|\pi|}} \sum_{[i]=[j]} < H_\pi(i), H_\pi(j) >$.

Proof. We know from Proposition 8.7 that the moments are given by:

$$\int_{\mathbb{T}^N \times \mathbb{T}^N} |E|^{2p} = \sum_{[i]=[j],[x]=[y]} \frac{H_{i_1 x_1} \ldots H_{i_p x_p}}{H_{j_1 y_1} \ldots H_{j_p y_p}}$$

With $\sigma = \ker x, \rho = \ker y$, we deduce that the moments of $|E|^2$ decompose over partitions, $\int_{\mathbb{T}^N \times \mathbb{T}^N} |E|^{2p} = \int_{\mathbb{T}^N} \sum_{\sigma, \rho \in P(p)} C(\sigma, \rho)$, with the contributions being 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 8.9. We have here the following result:

Proposition 8.10. $K(\pi)=\sum_{\pi\leq\sigma}\mu(\pi,\sigma)\binom{p}{\sigma}$ *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. (1) We use the fact that $\mu(\pi\pi',\sigma\sigma')=\mu(\pi,\sigma)\mu(\pi',\sigma')$, 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 use here the formula $\mu(\sqcap\sqcap\ldots\sqcap,\sigma)=(-1)^{|\sigma|-1}(|\sigma|-1)!$, which once again is well-known, and can be proved by recurrence on $|\sigma|$. We obtain, as claimed:

$$K(\sqcap\sqcap\ldots\sqcap)=\sum_{\sigma\in P(p)}\mu(\sqcap\sqcap\ldots\sqcap,\sigma)\binom{p}{\sigma}=\sum_{\sigma\in P(p)}(-1)^{|\sigma|-1}(|\sigma|-1)!\binom{p}{\sigma}$$

(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 $a_i\geq1$ the block lengths of σ, then $\binom{p}{\sigma}=\binom{p}{a_1,\ldots,a_r}$. On the other hand, given $a_1,\ldots,a_r\geq1$ 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. □

Now let us take a closer look at the integrals $I(\pi)$. We have here:

Proposition 8.11. *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. (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 8.12. *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. (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:

$$|I(\pi)|\leq\sum_{[i]=[j]}\prod_{\beta\in\pi}1=\sum_{[i]=[j]}1=\#\left\{i,j\in\{1,\ldots,N\}\Big|[i]=[j]\right\}\simeq p!N^p$$

Thus we have obtained the formula in the statement, and we are done. □

We have now all needed ingredients for a universality result:

Theorem 8.13. *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 8.9. By using Proposition 8.12 (3), we conclude that only the p-block and $(p-1)$-block partitions contribute at order 2, so:

$$\int_{\mathbb{T}^N\times\mathbb{T}^N}|E|^{2p}=K(|\,|\ldots|)N^pI(|\,|\ldots|)+\binom{p}{2}K(\sqcap|\ldots|)N^{p-1}I(\sqcap|\ldots|)+O(N^{2p-2})$$

Now by dividing by N^{2p} and then by using the various formulae in Proposition 8.10, Proposition 8.11 and Proposition 8.12 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 standard formulae $F_{ix}F_{iy}=F_{i,x+y}$, $\overline{F}_{ix}=F_{i,-x}$ and $\sum_xF_{ix}=N\delta_{i0}$. We first have:

Proposition 8.14. *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:

$$\frac{1}{N}\left\langle\prod_{r\in\beta}F_{i_r},\prod_{r\in\beta}F_{j_r}\right\rangle=\frac{1}{N}\left\langle F_{\sum_{r\in\beta}i_r},F_{\sum_{r\in\beta}i_r}\right\rangle=\delta_{\sum_{r\in\beta}i_r,\sum_{r\in\beta}j_r}$$

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

We have the following interpretation of the above integrals:

Proposition 8.15. *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. □

Regarding now the glow estimates, we first have the following result:

Proposition 8.16. *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:

$$I(\pi)=\sum_{\sigma\in P(p)}\#\left\{i,j\Big|\ker i=\sigma,[i]=[j],\sum_{r\in\beta}i_r=\sum_{r\in\beta}j_r,\forall\beta\in\pi\right\}$$

Since there are $\frac{N!}{(N-|\sigma|)!}\simeq N^{|\sigma|}$ choices for i satisfying $\ker i=\sigma$, and then there are $\binom{p}{\sigma}=O(1)$ choices for j satisfying $[i]=[j]$, we conclude that the main contribution comes from $\sigma=||\ldots|$, and so we have:

$$I(\pi)=\#\left\{i,j\Big|\ker i=||\ldots|,[i]=[j],\sum_{r\in\beta}i_r=\sum_{r\in\beta}j_r,\forall\beta\in\pi\right\}+O(N^{p-1})$$

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 8.17. *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 8.16 shows that we have the following estimate:

$$I(\pi)=I^\circ(\pi)+O(N^{p-1})$$

Our claim now is that we have the folowing 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 8.16, 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 $\sum_{r\in\beta}i_r=\sum_{j\in\beta}j_r$, with $[i_r|r\in\beta]\neq[j_r|r\in\beta]$. 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:

$$\begin{matrix}i_1\ldots i_c & k_1\ldots k_{a-c} & & j_1\ldots j_c & l_1\ldots l_{a-c}\\ \underbrace{j_1\ldots j_c}_{c} & \underbrace{k_1\ldots k_{a-c}}_{a-c} & & \underbrace{i_1\ldots i_c}_{c} & \underbrace{l_1\ldots l_{a-c}}_{b-c}\end{matrix}$$

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:

$$I^1(a,b)=a!b!\sum_{c\geq 2}\binom{a}{c}\binom{b}{c}N^{p-1}+O(N^{p-2})$$

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 by using the formula $I^\circ(\pi) = \prod_{\beta \in \pi} I(\beta)$, we 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 8.18. *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. We use the fact that, when dealing with the conditions $\sum_{r\in\beta} i_r = \sum_{r\in\beta} j_r$ defining the quantities $I(\pi)$, one can always erase some of the variables i_r, j_r, as to reduce to the "purely arithmetic" case, $\{i_r | r \in \beta\} \cap \{j_r | r \in \beta\} = \emptyset$. 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) Case $\binom{iijj}{jjii}$, 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:

$$\begin{aligned} I_1^{ari}(\sqcap\sqcap) &= \#\{i \neq j | 2i = 2j\} \\ &= \#\{i, j | 2i = 2j\} - \#\{i, j | i = j\} \\ &= 2^e N - N \\ &= (2^e - 1)N \end{aligned}$$

(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:

Theorem 8.19. *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 $K_1=\binom{p}{2}$, $K_2=\binom{p}{2}\frac{3p^2+p-8}{12}$, $K_3=\binom{p}{3}\frac{p^3+4p^2+p-18}{8}$.

Proof. We use the quantities $\widetilde{K}(\pi)=\frac{K(\pi)}{p!}$, $\widetilde{I}(\pi)=\frac{I(\pi)}{N^p}$, which are such that $\widetilde{K}(\pi|\ldots|)=\widetilde{K}(\pi)$, $\widetilde{I}(\pi|\ldots|)=\widetilde{I}(\pi)$. In terms of $J(\sigma)=\binom{p}{\sigma}\widetilde{K}(\sigma)\widetilde{I}(\sigma)$, 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 $\widetilde{K}_0=\widetilde{K}_1=1$, $\widetilde{K}_2=\frac{1}{2}-1=-\frac{1}{2}$, $\widetilde{K}_3=\frac{1}{6}-\frac{3}{2}+2=\frac{2}{3}$ and:

$$\widetilde{K}_4=\frac{1}{24}-\frac{4}{6}-\frac{3}{4}+\frac{12}{2}-6=-\frac{11}{8}$$

Regarding now the numbers C_{pr} in Proposition 8.16, these are given by:

$$C_{p1}=1,C_{p2}=\frac{1}{2}\binom{2p}{p}-1,\ldots\ldots,C_{p,p-1}=\frac{p!}{2}\binom{p}{2},C_{pp}=p!$$

We deduce that $I(|)=N$, $I(\sqcap)=N(2N-1)$, $I(\sqcap\!\!\sqcap)=N(6N^2-9N+4)$ and:

$$I(\sqcap\!\!\sqcap\!\!\sqcap)=N(24N^3-72N^2+82N-33)$$

By using Proposition 8.17 and Proposition 8.18, 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. $\square$

It is possible to compute the next term as well, the result being:

Theorem 8.20. *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. Skipping the technical details here, we obtain the formula for K_4 in the statement. $\square$

The passage from Theorem 8.19 to Theorem 8.20 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. For such a matrix W_N, with $N=2^n$, the underlying group is $G=\mathbb Z_2^n$, and the numbers $C_I(J_1,\ldots,J_r)=\#\left\{(a_i)_{i\in I}\in G\text{ distinct}\Big|\sum_{j\in J_s}a_j=0,\forall s\right\}$ are polynomial in $N=2^n$. This suggests that the integrals $I(\pi)$, and hence the glow, should be polynomial in N.

There are many interesting questions in relation with the glow. As already mentioned in the beginning of this section, a motivation for all this comes from [57]. Also, we have as well the question of connecting the various invariants of the Hadamard matrices, such as the defect, or the algebraic invariants from sections 10-12 below, to the glow.

9. Norm maximizers

We discuss here some further analytic questions. We know from Theorem 7.1 above that the Hadamard manifold $X_N = M_N(\mathbb{T}) \cap \sqrt{N}U_N$ can be analytically computed in two possible ways. The first method is via the Hadamard determinant bound:

$$X_N = \left\{ H \in M_N(\mathbb{T}) \Big| \, |\det(H)| = N^{N/2} \right\}$$

This method, going back to Hadamard's 1893 paper [53] is of course something well-known, and we will not further comment on this. We will focus instead on the second possible method, which is something more recent [14], via the 1-norm bound:

$$X_N = \left\{ H \in \sqrt{N}U_N \Big| \, ||H||_1 = N^2 \right\}$$

This formula suggests a systematic study of the 1-norm on U_N, with results about critical points, and local maximizers. In addition, in connection with the real Hadamard matrix problematics, we would like to study as well the 1-norm on O_N, where the critical points and local maximizers might be different from the real ones over U_N.

We have already met such questions, in sections 1,6,7 above, in various technical contexts. Let us begin with a short summary of the results that we already have:

Theorem 9.1. *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. As explained in section 6 above, all this follows from the Hölder inequality, with the remark that at $p = 1, 4$ we just need the Cauchy-Schwarz inequality. □

We have chosen here to talk about p-norms instead of just the 1-norm, and this, for two reasons. First, we have seen in section 6 that for certain technical questions regarding the circulant matrices, the natural norm to be used is in fact the 4-norm. And second, we will formulate in what follows certain conjectures regarding the 1-norm, and these conjectures are probably easier to investigate first in the p-norm setting, with p arbitrary.

The above result suggests the following definition:

Definition 9.2. *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 mentioned above, 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 $p = 1$. In the real case, following [14], we have:

Theorem 9.3. *If $U \in O_N$ locally maximizes the 1-norm, then $U_{ij} \neq 0$ 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:

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

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. □

In the complex case, following [17], we have a similar result:

Theorem 9.4. *If $U \in U_N$ locally maximizes the 1-norm, then $U_{ij} \neq 0$ 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:

$$\begin{aligned}\frac{\partial||U^t||_1}{\partial t}\Big|_{t=0^-} &= \frac{\partial}{\partial t}\Big|_{t=0^-}(|\cos t|+|\sin t|)(||X||_1+||Y||_1)+C\\ &= (-\sin t-\cos t)\Big|_{t=0}(||X||_1+||Y||_1)+C\\ &= -||X||_1-||Y||_1+C\end{aligned}$$

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 [17], we have:

Theorem 9.5. *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 condition $dF\in span(dA_{ij})$ is satisfied.

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

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

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

$$d|U_{ij}|=d\sqrt{U_{ij}\bar{U}_{ij}}=\frac{U_{ij}d\bar{U}_{ij}+\bar{U}_{ij}dU_{ij}}{2|U_{ij}|}=\frac{1}{2}(S_{ij}d\bar{U}_{ij}+\bar{S}_{ij}dU_{ij})$$

We therefore obtain, with $W_{ij}=sgn(U_{ij})\varphi'(|U_{ij}|)$ as in the statement:

$$dF=\sum_{ij}d\left(\varphi(|U_{ij}|)\right)=\sum_{ij}\varphi'(|U_{ij}|)d|U_{ij}|=\frac{1}{2}\sum_{ij}W_{ij}d\bar{U}_{ij}+\bar{W}_{ij}dU_{ij}$$

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:

$$W=2M^tU\quad,\quad\bar{W}=2M\bar{U}$$

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

$$M^t=\frac{1}{2}WU^*\quad,\quad M^t=\frac{1}{2}UW^*$$

Summing up, the critical point condition on $U\in U_N$ simply reads $WU^*=UW^*$, which means that the matrix WU^* must be self-adjoint, as claimed. □

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

Definition 9.6. *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 9.7. *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 9.5 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 $WU^* = \sum_{r>0} \varphi'(r) U_r U^*$, and when $\varphi : [0, \infty) \to \mathbb{R}$ varies, either as an arbitrary differentiable function, or as a power function $\varphi(x) = x^p$ wirh $p \in [1, \infty)$, the individual components of this sum must be all 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 9.8. *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:

$$U^t = \sum_{r>0} rU_r^t \quad , \quad \bar{U} = \sum_{r>0} r\bar{U}_r \quad , \quad U^* = \sum_{r>0} rU_r^*$$

(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:

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

Thus the color components of $W = U \otimes V$ are the matrices $W_p = \sum_{p=rs} U_r \otimes V_s$, and 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 $U_r U_s^*, U_r^* U_s$, we obtain the result.

(5) The matrix in the statement, which goes back to [20], 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 [20], 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 [20], 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 9.8 (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 9.8 (5):

Theorem 9.9. *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 [20], 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 $\bar{\gamma}_i=\gamma_{-i}$:

$$\begin{aligned}(U_rU_s^*)_{ij} &= \sum_{m\in(-D_r+j)\cap(-D_s+i)}\operatorname{sgn}(\gamma_{j-m})\operatorname{sgn}(\bar{\gamma}_{i-m})\\ &= \sum_{m\in(D_r+i)\cap(D_r+j)}\operatorname{sgn}(\gamma_{j-m})\operatorname{sgn}(\bar{\gamma}_{i-m})\\ &= \sum_{m\in(D_r+i)\cap(D_r+j)}\operatorname{sgn}(\bar{\gamma}_{m-j})\operatorname{sgn}(\gamma_{m-i})\end{aligned}$$

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

$$(U_rU_s^*)_{ji}=\sum_{k\in(D_r+i)\cap(D_r+j)}\operatorname{sgn}(\bar{\gamma}_{k-i})\operatorname{sgn}(\gamma_{k-j})$$

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. □

Summarizing, the study of the critical points alone leads to some interesting combinatorics. There are of course many questions regarding the balanced and semi-balanced matrices, for instance in connection with design theory. See [17].

Let us compute now derivatives. As in Theorem 9.5, 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 an arbitrary unitary matrix, and $A\in M_N(\mathbb{C})$ is assumed to be anti-hermitian, $A^*=-A$, with this latter assumption needed for having $e^A\in U_N$.

Let us first compute the derivative of f. We have:

Proposition 9.10. *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 $f'(0)$. In terms of the color decomposition $U = \sum_{r>0} rU_r$ of our matrix, the result is as follows:

Proposition 9.11. *We have the following formula,*

$$f'(0) = 2\sum_{r>0} r\psi'(r^2) Re\left[Tr(U_r^*UA)\right]$$

where $U_r \in M_N(\mathbb{T} \cup \{0\})$ are the color components of U.

Proof. We use the formula in Proposition 9.10 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 9.12. *We have the following formula,*

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

valid for any $U \in U_N$, and any $A \in M_N(\mathbb{C})$ anti-hermitian.

Proof. We use the formula in Proposition 9.10 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:

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

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 the functional $F(U)=||U||_1$, there are some simplifications, that we will work out now in detail. First, we have:

Proposition 9.13. *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 9.12 above, with $\psi(x)=\sqrt{x}$. The derivatives are here $\psi'(x)=\frac{1}{2\sqrt{x}}$ and $\psi''(x)=-\frac{1}{4x\sqrt{x}}$, and we obtain:

$$\begin{aligned} f''(0) &= -\sum_{ij}\frac{Re\left[(UA)_{ij}\overline{U}_{ij}\right]^2}{|U_{ij}|^3}+\sum_{ij}\frac{Re\left[(UA^2)_{ij}\overline{U}_{ij}\right]}{|U_{ij}|}+\sum_{ij}\frac{|(UA)_{ij}|^2}{|U_{ij}|} \\ &= -\sum_{ij}\frac{Re\left[(UA)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|}+\sum_{ij}Re\left[(UA^2)_{ij}\overline{S}_{ij}\right]+\sum_{ij}\frac{|(UA)_{ij}|^2}{|U_{ij}|} \\ &= Re\left[Tr(S^*UA^2)\right]+\sum_{ij}\frac{|(UA)_{ij}|^2-Re\left[(UA)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|} \end{aligned}$$

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 9.14. *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 9.5 and Proposition 9.13, 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:

$$Re\left[Tr(XA^2)\right] = \frac{1}{2}\left[Tr(XA^2) + Tr(A^2X)\right] = Tr(XA^2)$$

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 9.15. *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:

$$Tr(XA^2) = Tr(Y^2A^2) = Tr(YA^2Y) = -Tr((YA)(YA)^*) \leq 0$$

Thus, the above four conditions are indeed equivalent. □

We would like to discuss as well the real case, and we will need here:

Proposition 9.16. *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 $a = \sum_{ij} A_{ij} e_i \otimes e_j$, which is antisymmetric, we have:

$$Tr(XA^2) =< X, A^2 >= - < AX, A >= - < a, (1 \otimes X)a >$$

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 [17], we can now formulate a final result on the subject, as follows:

Theorem 9.17. *Given $U\in U_N$, set $S_{ij}=\mathrm{sgn}(U_{ij})$, and $X=S^*U$.*

1. *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 $B\in M_N(\mathbb C)$.
2. *If $U\in O_N$, this matrix locally maximizes the 1-norm on O_N precisely when X is self-adjoint, and the sum of its two smallest eigenvalues is positive.*

Proof. Here (1) follows from Theorem 9.14, by setting $A=iB$, and by using Proposition 9.15, which shows that we must have indeed $X\geq 0$. As for (2), this follows from (1), with the remark that the right term vanishes, and from Proposition 9.16. $\square$

In practice now, let us first discuss the real case. The following result, involving the notion of (a,b,c) pattern appearing in Theorem 9.9, was proved in [20]:

Theorem 9.18. *If $U=U(x,y)$ is orthogonal, coming from an (a,b,c) pattern, with*
$$(N(a-b)+2b)|x|+(N(c-b)+2b)|y|\geq 0$$
the matrix $H=\sqrt{N}U$ is almost Hadamard, in a real sense.

Proof. Since any row of U consists of $a+b$ copies of x and $b+c$ copies of y, we have:
$$(SU^t)_{ij}=\begin{cases}(a+b)|x|+(b+c)|y|&(i=j)\\(a-b)|x|+(c-b)|y|&(i\neq j)\end{cases}$$

Now observe that we can write the matrix SU^t as follows:
$$\begin{aligned}SU^t&=2b(|x|+|y|)1_N+((a-b)|x|+(c-b)|y|)NJ_N\\&=2b(|x|+|y|)(1_N-J_N)+((N(a-b)+2b)|x|+(N(c-b)+2b)|y|))J_N\end{aligned}$$

Since $1_N-J_N,J_N$ are orthogonal projections, we have $SU^t>0$ if and only if the coefficients of these matrices are both positive, and this gives the result. $\square$

As a basic example for the above construction, we have the following matrix:
$$K_N=\frac{1}{\sqrt{N}}\begin{pmatrix}2-N&2&\ldots&2\\2&2-N&\ldots&2\\\ldots&\ldots&\ldots&\ldots\\2&2&\ldots&2-N\end{pmatrix}$$

We should mention that this matrix is in fact absolute almost Hadamard, in the real sense, as explained in [70]. There are many other interesting examples, coming from various block design constructions, and we refer here to [20].

Observe now that our basic example, namely the above matrix K_N, is at the same time circulant and symmetric. We have in fact the following result, also from [20]:

Theorem 9.19. *Consider a circulant matrix $H \in M_N(\mathbb{R}^*)$, written $H_{ij} = \gamma_{j-i}$. If the following conditions are satisfied, H is almost Hadamard, in a real sense:*

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

Proof. We use the Fourier transform theory from Theorem 6.13 above. As a first observation, 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:

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

Thus S^tU is circulant, with $\rho/\sqrt{N}$ as first row. We therefore have $S^tU = FLF^*$ with $L = diag(\nu)$ and $\nu = F^*\rho$, so $S^tU > 0$ iff $\nu > 0$, and we are done. See [20]. $\square$

As an example here, consider the following vector, having length $N = 2n+1$:

$$q = (-1)^n(1, -1, 1, \ldots, -1, 1, 1, -1, \ldots, 1, -1)$$

This vector satisfies the conditions of Theorem 9.19, and produces the following circulant $N \times N$ real almost Hadamard matrix, from [20]:

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

We refer to the paper [20] for further details on all this, and for some other basic facts regarding the almost Hadamard matrices, in the real case. Some further analytic facts are available from [14], [15], [18], [70]. There is as well a concrete application of all this, to the minors of the Hadamard matrices, in the spirit of [65], available from [19].

Following now [17], let us discuss the complex case. Quite surprisingly, the above "basic" 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 various matrices coming from Theorem 9.18 and Theorem 9.19 above. And, in addition to this, various complex matrices which can be constructed via straightforward complex extensions of the constructions in Theorem 9.18 and Theorem 9.19 fail to be almost Hadamard as well, in the complex sense.

We are therefore led to the following statement, from [17]:

Conjecture 9.20 (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 of course something very useful.

Regarding now the known verifications of the AHC, as already mentioned above, these basically concern the natural "candidates" coming from Theorem 9.18 and Theorem 9.19, as well as some straightforward complex generalizations of these candidates.

All this is quite technical, and generally speaking, we refer here to [17]. Let us mention, however, that the main idea that emerges from [17] is that of using a method based on a random derivative, pointing towards a suitable homogeneous space coset.

In order to explain this, let $OSC_N \subset USC_N$ be the orthogonal symmetric circulant matrices, and unitary self-adjoint circulant matrices. Via the Fourier transform indentifications from Theorem 6.13, the inclusion $OSC_N \subset USC_N$ corresponds then to the following inclusion, with $\mathbb{Z}_2^{(N+e)/2}$ with $e = 0, 1$ being $\{p \in \mathbb{Z}_2^N | p_k = p_{-k}\}$:

$$\mathbb{Z}_2^{(N+e)/2} \subset \mathbb{Z}_2^N$$

Let us consider as well the set USB_N consisting of unitary bistochastic self-adjoint matrices. The various results in [17] suggest the following statement:

Conjecture 9.21. *Given $U \in USB_N$ satisfying $S^*U \geq 0$, there exists a simple function $B \to B^U$, probably either the identity or the passage to another coset, such that*

$$\int_{OSC_N} \Phi(U, B^U) dB \leq 0$$

and such that the equality can only be attained when $H = \sqrt{N}U$ is Hadamard.

Observe that, in view of Theorem 9.17 above, this would more or less prove the AHC, modulo a remaining extension from USB_N to the group U_N itself.

As already mentioned, this latter conjecture is supported by the computations in [17], which either use this idea, or can be reformulated in this spirit.

Regarding the applications, the situation is of course very different from the one in the real case. Assuming that the AHC holds indeed, we would have here a new approach to the complex Hadamard matrices, which is by construction analytic and local. This would be of course something quite powerful, potentially reshaping the whole subject.

10. Quantum groups

We discuss in what follows the relation between the Hadamard matrices $H \in M_N(\mathbb{C})$ and the quantum permutation groups $G \subset S_N^+$, and its potential applications to certain mathematical physics questions. There is a lot of material to be surveyed here, and we will insist on mathematical aspects, regarding the correspondence $H \to G$.

We will need many preliminaries, first concerning the operator algebras, then the compact quantum groups in the sense of Woronowicz [99], [100], and then the matrix modelling questions for such quantum groups. Once done with this, we will be able to talk about quantum permutations, and their relation with the Hadamard matrices.

Let H be a Hilbert space. We denote by $B(H)$ the algebra of bounded operators $T : H \to H$, with usual norm and involution. The algebra $B(H)$, as well as any of its unital subalgebras $A \subset B(H)$ which are complete, and stable under $*$, fit into:

Definition 10.1. *A unital 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 $a \in A$.*

In what follows we will often omit the adjective "unital", because the passage to the non-unital case would bring nothing interesting, in connection with our questions.

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:

Proposition 10.2. *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. All this is standard, by using $\sigma(f(a)) = f(\sigma(a))$ for any $f \in \mathbb{C}[X]$, and more generally for any $f \in \mathbb{C}(X)$ having poles outside $\sigma(a)$, which is elementary:

(1) This simply comes from $\frac{1}{1-a} = 1 + a + a^2 + \ldots$ for any $||a|| < 1$.

(2) This follows from $\sigma(a)^{-1} = \sigma(a^{-1}) = \sigma(a^*) = \overline{\sigma(a)}$.

(3) This follows from (2), by using $f(z) = (z + it)/(z - it)$, with $t \in \mathbb{R}$.

(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 $\rho \geq \lim_{n\to\infty} ||a^n||^{1/n}$, and then by using $||aa^*|| = ||a||^2$ we obtain $\rho \geq ||a||$, and so $\rho(a) \geq ||a||$, as desired. □

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 10.3. *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 Proposition 10.2 (3) shows that ev is a $*$-morphism, Proposition 10.2 (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 is of course quite brief, but details on all this can be found in any book on operator algebras. For a slightly longer proof of (1), called Gelfand theorem, and which is the key result that we will need here, we refer for instance to [12].

As a conclusion to all this, given a C^*-algebra A, we can think of it as being of the form $A = C(X)$, with X being a "compact quantum space". We will be interested here in the case where X is a "compact quantum group". The axioms for the corresponding C^*-algebras, found by Woronowicz in [99], are, in a soft form, as follows:

Definition 10.4. *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*

$$\Delta(u_{ij}) = \sum_k u_{ik} \otimes u_{kj} \quad , \quad \varepsilon(u_{ij}) = \delta_{ij} \quad , \quad S(u_{ij}) = u_{ji}^*$$

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 10.5. *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. In both cases, we have to exhibit a certain matrix u. For the first assertion, we can use the matrix $u = (u_{ij})$ formed by matrix coordinates of G, given by:

$$g = \begin{pmatrix} u_{11}(g) & \dots & u_{1N}(g) \\ \vdots & & \vdots \\ u_{N1}(g) & \dots & u_{NN}(g) \end{pmatrix}$$

For the second assertion, we can use the diagonal matrix formed by generators:

$$u = \begin{pmatrix} g_1 & & 0 \\ & \ddots & \\ 0 & & g_N \end{pmatrix}$$

Finally, the last assertion follows from the Gelfand theorem, in the commutative case, and in the cocommutative case, this follows from the results of Woronowicz in [99]. □

In general now, the structural maps Δ, ε, S have the following properties:

Proposition 10.6. *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 very nice properties. In view of Proposition 10.5 above, we can now formulate the following definition:

Definition 10.7. *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 $G=\widehat{\Gamma},\Gamma=\widehat{G}$, but in a formal sense.

With this in mind, let us call now corepresentation of A any unitary matrix $v\in M_n(A)$ satisfying the same conditions are 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 [99]:

Theorem 10.8. *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 [99], 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 [99]. □

The above result is something quite fundamental, and as a main application, one can develop a Peter-Weyl type theory for the corepresentations of A. See [99].

Finally, we will need some general theory regarding the random matrix models for the Woronowicz algebras. The idea here is very simple, namely that of modelling the coordinates $u_{ij}\in A$ by certain concrete variables $U_{ij}\in B$. Our favorite type of algebras being the random matrix ones, $B=M_K(C(T))$, we are led into:

Definition 10.9. *A matrix model for $A=C(G)$ is a morphism of C^*-algebras*

$$\pi:C(G)\to M_K(C(T))$$

where T is a compact space, and $K\geq 1$ is an integer.

The "best" models are of course the faithful ones, $\pi:C(G)\subset M_K(C(T))$. However, this formalism is quite restrictive, not covering many interesting examples.

In order to fix this, let us look at the group dual case, $A=C^*(\Gamma)$, with Γ being a usual discrete group. We know that a model $\pi:C^*(\Gamma)\to M_K(C(T))$ must come from a group representation $\rho:\Gamma\to C(T,U_K)$. Now observe that when ρ is faithful, the representation π is in general not faithful, for instance because when $T=\{.\}$ its target algebra is finite dimensional. On the other hand, this representation "reminds" Γ, and so can be used in order to fully understand Γ. This leads to the following definition:

Definition 10.10. *Let $\pi : C(G) \to M_K(C(T))$ be a matrix model.*

(1) *The Hopf image of π is the smallest quotient Hopf C^*-algebra $C(G) \to C(H)$ producing a factorization of type $\pi : C(G) \to C(H) \to M_K(C(T))$.*
(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.*

In the case where $G = \widehat{\Gamma}$ is a group dual, π must come from a group representation $\rho : \Gamma \to C(T, U_K)$, and the above factorization is simply the one obtained by taking the image, $\rho : \Gamma \to \Lambda \subset C(T, U_K)$. Thus π is inner faithful when $\Gamma \subset C(T, U_K)$.

Also, given a compact group G, and elements $g_1, \ldots, g_K \in G$, we have a representation $\pi : C(G) \to \mathbb{C}^K$, given by $f \to (f(g_1), \ldots, f(g_K))$. The minimal factorization of π is then via $C(H)$, with $H = \overline{< g_1, \ldots, g_K >}$, and π is inner faithful when $G = H$.

In general, the existence and uniqueness of the Hopf image comes from dividing $C(G)$ by a suitable ideal. We refer to [11] for more details regarding this construction.

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 [96]:

Proposition 10.11. *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:

$$u_{ij} = \chi\left(\sigma \in G \middle| \sigma(j) = i\right)$$

This leads us into the following key definition, due to Wang [96] as well:

Definition 10.12. *$C(S_N^+)$ is the universal C^*-algebra generated by the entries of a $N \times N$ magic unitary matrix $u = (u_{ij})$, with the morphisms given by*

$$\Delta(u_{ij}) = \sum_k u_{ik} \otimes u_{kj} \quad , \quad \varepsilon(u_{ij}) = \delta_{ij} \quad , \quad S(u_{ij}) = u_{ji}$$

as comultiplication, counit and antipode.

This algebra satisfies the axioms in Definition 10.4, and the underlying compact quantum group S_N^+ is called quantum permutation group. Quite surprisingly, we have:

Theorem 10.13. *We have an embedding $S_N \subset S_N^+$, given at the algebra level by:*

$$u_{ij} \to \chi\left(\sigma \middle| \sigma(j) = i\right)$$

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 [96]. $\square$

At a more advanced level, one can prove that $S_4^+ \simeq SO_3^{-1}$. At $N \geq 5$ the quantum group S_N^+ still has the same fusion rules as SO_3, but is not coamenable. See [12].

In relation now with the complex Hadamard matrices, the connection with the quantum permutations is immediate, coming from the following observation:

Proposition 10.14. *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:

$$\left\langle\frac{H_i}{H_j},\frac{H_i}{H_k}\right\rangle=\sum_l\frac{H_{il}}{H_{jl}}\cdot\frac{H_{kl}}{H_{il}}=\sum_l\frac{H_{kl}}{H_{jl}}=N\delta_{jk}$$

The verification for the columns is similar, we 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. □

Summarizing, any complex Hadamard matrix produces a representation of the quantum permutation algebra $C(S_N^+)$. Thus, we can apply the Hopf image construction from Definition 10.10, and we are led in this way into the following notion:

Definition 10.15. *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. To be more precise, philosophically speaking, the idea will be that "H can be thought of as being a kind of Fourier matrix for G".

There are several results supporting this, with the main evidence coming from the following result, which collects the basic known results regarding the construction:

Theorem 10.16. *The construction $H\to G$ has the following properties:*

1. *For a Fourier matrix $H=F_G$ we obtain the group G itself, acting on itself.*
2. *For $H\notin\{F_G\}$, the quantum group G is not classical, nor a group dual.*
3. *For a tensor product $H=H'\otimes H''$ we obtain a product, $G=G'\times G''$.*

Proof. All this material is standard, and elementary, as follows:

(1) Let us first discuss the cyclic group case, $H=F_N$. Here the rows of H are given by $H_i=\rho^i$, where $\rho=(1,w,w^2,\ldots,w^{N-1})$. 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 $G = \mathbb{Z}_N$.

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 the rest.

(2) This is something more tricky, needing some general study of the representations whose Hopf images are commutative, or cocommutative. For details here, along with a number of supplementary facts on the construction $H \to G$, we refer to [13], [21].

(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:

$$\begin{array}{ccccc} C(S_{N'}^+) \otimes C(S_{N''}^+) & \longrightarrow & C(G') \otimes C(G'') & \longrightarrow & M_{N'}(\mathbb{C}) \otimes M_{N''}(\mathbb{C}) \\ \uparrow & & & & \downarrow \\ C(S_N^+) & \longrightarrow & C(G) & \longrightarrow & M_N(\mathbb{C}) \end{array}$$

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:

$$\begin{array}{ccccc} u'_{ij} \otimes u''_{ab} & \longrightarrow & w'_{ij} \otimes w''_{ab} & \longrightarrow & P'_{ij} \otimes P''_{ab} \\ \uparrow & & & & \downarrow \\ u_{ia,jb} & \longrightarrow & w_{ia,jb} & \longrightarrow & P_{ia,jb} \end{array}$$

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. □

Generally speaking, going beyond Theorem 10.16 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 on, in section 12 below.

We would like to end this section with two theoretical extensions of the construction $H \to G$ from Definition 10.15, which are both quite interesting. A first idea, from [10], is that of using complex Hadamard matrices with noncommutative entries.

Consider an arbitrary unital C^*-algebra A. Two row or column vectors over this algebra, say $a = (a_1, \ldots, a_N)$ and $b = (b_1, \ldots, b_N)$, are called orthogonal when:

$$\sum_i a_i b_i^* = \sum_i a_i^* b_i = 0$$

Observe that by applying the involution, we have as well $\sum_i b_i a_i^* = \sum_i b_i^* a_i = 0$.

With this notion in hand, we can formulate:

Definition 10.17. *An Hadamard matrix over a unital C^*-algebra A is a square matrix $H \in M_N(A)$ satisfying the following conditions:*

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, $A = C(X)$, our Hadamard matrix must be made of "fibers", one for each point $x \in X$. Thus, we must have $H = \{H^x | x \in X\}$, with H^x being complex Hadamard matrices, depending continuously on $x \in X$.

When A is not commutative, we can have many interesting examples, which can be quite far away from the usual Hadamard matrices. We will be back to this later.

In general now, observe that if $H = (H_{ij})$ is Hadamard, then so are the matrices $\bar{H} = (H_{ij}^*)$, $H^t = (H_{ji})$ and $H^* = (H_{ji}^*)$. In addition, we have the following result:

Proposition 10.18. *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.

Proof. This is clear indeed 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.

Let us discuss now the tensor products, and their deformations. Following [47], the deformed tensor products are constructed as follows:

Theorem 10.19. *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. □

As a basic example, we have the following construction:

Proposition 10.20. *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 10.19, 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 10.19 are satisfied indeed. □

The generalized Hadamard matrices produce quantum groups, as follows:

Theorem 10.21. *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, and then factorize $\pi:C(S_N^+)\to C(G)\to M_N(A)$, with $G\subset S_N^+$ 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:

$$\begin{aligned}(P_{ij})_{ba}^*&=\frac{1}{N}(H_{ib}H_{jb}^*H_{ja}H_{ia}^*)^*\\ &=\frac{1}{N}H_{ia}H_{ja}^*H_{jb}H_{ib}^*\\ &=(P_{ij})_{ab}\end{aligned}$$

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 10.17:

$$\begin{aligned}(P_{ij}^2)_{ab} &= \sum_c (P_{ij})_{ac}(P_{ij})_{cb}\\ &= \frac{1}{N^2}\sum_c H_{ia}H_{ja}^*H_{jc}H_{ic}^*H_{ic}H_{jc}^*H_{jb}H_{ib}^*\\ &= \frac{1}{N}H_{ia}H_{ja}^*H_{jb}H_{ib}^*\\ &= (P_{ij})_{ab}\end{aligned}$$

(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 $H^*H = N1_N$, 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 trickiest check, because it involves, besides axiom (1) and the formula $H^t\bar{H} = N1_N$ 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 10.21 is compatible with the construction for the usual complex Hadamard matrices.

In general, computing G is a quite difficult question, and the answer for instance for the matrices in Proposition 10.20 is not known. We refer to [10] for more on this.

Let us discuss now another generalization of the construction $H \to G$. The idea, following [23], will be that of looking at the partial Hadamard matrices (PHM), and their connection with the partial permutations. Let us start with:

Definition 10.22. *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.*

Observe that we have $S_N \subset \widetilde{S}_N$. The embedding $u : S_N \subset M_N(0,1)$ given by 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 [96], we have the following definition:

Definition 10.23. *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.*

The algebra $C(\widetilde{S}_N^+)$ has a comultiplication given by $\Delta(u_{ij}) = \sum_k u_{ik} \otimes u_{kj}$, and 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 10.24. *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, we 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 [23]. □

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 10.25. *A pre-Latin square is a 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 matrix L, to any $x \in \{1,\ldots,N\}$ we can associate the partial permutation $\sigma_x \in \widetilde{S}_M$ given by $\sigma_x(j) = i \iff L_{ij} = x$. We denote by $G \subset \widetilde{S}_M$ the semigroup generated by $\sigma_1,\ldots,\sigma_N$, 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 formula $P_{ij} = Proj(\xi_{L_{ij}})$.

With these notations, we have the following result, from [23]:

Theorem 10.26. *If $H \in M_{N\times M}(\mathbb{C})$ is a PHM, the following are equivalent:*

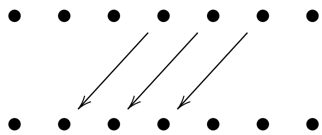
1. *The semigroup $G \subset \widetilde{S}_M^+$ is classical, i.e. $G \subset \widetilde{S}_M$.*
2. *The projections $P_{ij} = Proj(H_i/H_j)$ pairwise commute.*
3. *The vectors $H_i/H_j \in \mathbb{T}^N$ are pairwise proportional, or orthogonal.*
4. *The submagic matrix $P = (P_{ij})$ comes for a pre-Latin square L.*

In addition, if so is the case, G is the semigroup associated to L.

Proof. Here (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, and the last assertion comes from Gelfand duality. See [23]. □

We call "classical" the matrices in Theorem 10.26. There are many examples here, the most basic ones being the upper $M \times N$ submatrices of the Fourier matrices F_N, denoted $F_{M,N}$. If we denote by $G_{M,N} \subset \widetilde{S}_M$ the associated semigroups, we have:

Theorem 10.27. *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.

With this remark in hand, the computation is quite standard. See [22]. □

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 10.28. *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. 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.

With this remark in hand, the proof is quite standard. See [22]. □

There are many interesting questions regarding the construction $H \to G$, in this generalized PHM/partial permutation setting, and we refer here to [22], [23].

11. Subfactor theory

We discuss here some potential applications of the construction $H \to G$, and of the Hadamard matrices in general, to certain questions from mathematical physics.

Generally speaking, all this is related to statistical mechanics. The idea indeed, which is old folklore, 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.

All this comes from the work of Jones in subfactor theory [59], [60], [61], and from various general correspondences between quantum groups and subfactors. There are some direct computations as well, supporting this idea, as those in [16].

However, all this is not axiomatized yet. So, as a more modest goal here, we will explain the relation between the Hadamard matrices and the von Neumann algebras, the commuting squares, the subfactor theory, and Jones' planar algebra work in [61], and then we will comment on some further possible developments of all this.

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 10 above:

Theorem 11.1. *The von Neumann algebras, which are the C^*-algebras $A \subset B(H)$ closed under the weak 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 jewel 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. □

All the above is of course very brief. We recommend here the original papers of von Neumann and Connes, starting for instance with [71], and then [37].

As a philosophical comment, observe the huge technical difference between the basic C^*-algebra theory, more or less explained in section 10 above, and the basic von Neumann algebra theory, barely discussed above. Some theories are much more advanced than others, perhaps because they are more interesting, or more beautiful, or both.

As a side remark here, in view of all this, it would have been of course desirable to introduce the compact quantum groups G by talking directly about the associated von Neumann algebras $L^\infty(G)$. Unfortunately this is not possible, because the underlying Hilbert spaces $H = L^2(G)$ do not come "by definition", but by theorem. In addition, we cannot really talk about von Neumann algebras with generators and relations.

In short, there is some philosophical clash here, between C^*-algebra theory and von Neumann algebra theory. This is a bit like a dispute between topology and probability. You don't really need open and closed sets in order to do interesting mathematics, but if you have the occasion of learning some, why not having them in your bag of tricks.

From a more relaxed perspective, all this can be traced back to the Bohr-Einstein debates, the main question being whether God plays dice or not.

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 11.2. *A pair of orthogonal MASA is a pair of maximal abelian subalgebras*

$$B, C \subset A$$

which are orthogonal with respect to the trace, $(B \ominus \mathbb{C}1) \perp (C \ominus \mathbb{C}1)$.

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:

$$tr(bc) = tr(b)tr(c) \quad , \quad \forall b \in B, c \in C$$

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 $M_N(\mathbb{C})$, with $N\in\mathbb{N}$, endowed with its usual matrix trace.

In this context, we have the following surprising observation of Popa [79]:

Theorem 11.3. *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,*

$$A=\Delta\quad,\quad B=H\Delta H^*$$

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 $A=\Delta$ and $B=U\Delta U^*$, with $U\in U_N$.

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, namely $\frac{1}{\sqrt{N}}$, and so that the rescaled matrix $H=\sqrt{N}U$ must be Hadamard. □

The above result is something quite fascinating, and in stark contrast with the mathematical solidity and beauty of Theorem 11.1. Bluntly put, there is a "black hole" in the foundations of modern von Neumann algebra theory, produced by their complex Hadamard matrices, and their wild structure, geometry and combinatorics.

Whether this black hole must be studied a bit, run away from, or simply ignored, is one of the main philosophical questions in modern von Neumann algebra theory. Generally speaking, subfactor theory and related areas are in favor of the "study a bit" direction, while free probability and related areas opt for the "run away from" solution.

In relation with this, the present text is based on a bit of a hybrid philosophy, namely study the complex Hadamard matrices, of course and definitely, but with the idea in mind of eventually reaching to tools coming from Voiculescu's free probability theory.

Getting back now to work, and to Theorem 11.3 above, as it is, along the same lines, but at a more advanced level, we have the following result:

Theorem 11.4. *Given a complex Hadamard matrix $H\in M_N(\mathbb C)$, the diagram formed by the associated pair of orthogonal MASA, namely*

$$\begin{tikzcd}
\Delta \arrow[r] & M_N(\mathbb{C}) \\
\mathbb{C} \arrow[u] \arrow[r] & H\Delta H^* \arrow[u]
\end{tikzcd}$$

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 $M\to M_\Delta$ which consists in keeping the diagonal, and erasing the rest.

Regarding now the other expectation, $E_{H\Delta H^*}:M_N(\mathbb C)\to H\Delta H^*$, it is better to identify it with the expectation $E_{U\Delta U^*}:M_N(\mathbb C)\to U\Delta U^*$, with $U=H/\sqrt N$. 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. □

We should mention that the notion of commuting square, which was heavily used by Popa in his classification work for the subfactors [80], is a bit more complicated that what was said above. However, the other axioms are trivially satisfied for the class of commuting squares from Theorem 11.4, so we will not get into this. See [80].

As a conclusion, all this leads us into subfactor theory. So, let us explain now, following Jones [59], the basic theory here. Given an inclusion of II_1 factors $A_0\subset A_1$, which is actually something quite natural in physics, 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 in 1983, and his main result from [59], which came as a big surprise at that time, along with some supplementary fundamental work, done later, in [61], can be summarized as follows:

Theorem 11.5. *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 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. $\square$

As it was the case with Theorem 11.1 above, our explanations here were very brief. For all this, and more, we recommend Jones' papers [59], [60], [61], and [92].

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 11.6. *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. Here (1) is something quite routine, (2) is a subtle result, called Ocneanu compactness theorem [74], and (3) follows from (1,2), by flipping the diagram. $\square$

Getting back now to the Hadamard matrices, we can extend our lineup of results, namely Theorem 11.3 and Theorem 11.4, with an advanced statement, as follows:

Theorem 11.7. *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 planar algebra $P = (P_k)$ of the corresponding subfactor can be explicitely computed in terms of H.

Proof. The fact that we have a commuting square is from Theorem 11.4, and the computation of the planar algebra is possible thanks to formula in Theorem 11.6.

As for the precise formula of the planar algebra, which is something quite complicated, this can be found in [61], and we will be back to it later, in Theorem 11.9 below. □

Let us discuss now the relation with the quantum groups. We will need the following result, valid in the general context of the Hopf image construction:

Theorem 11.8. *Given a matrix model $\pi : C(G) \to M_K(C(T))$, the fundamental corepresentation v of its Hopf 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 [100], 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 11.9. *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) $G_{ia}^{jb}=\sum_kH_{ik}\bar{H}_{jk}\bar{H}_{ak}H_{bk}$.
(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. With the notations in Theorem 11.8, 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:

$$\begin{aligned}L_{ij}&=(TU^{\otimes k})_{ij}\\&=\sum_aT_{ia}U^{\otimes k}_{aj}\\&=\sum_aT_{ia}U_{a_1j_1}\ldots U_{a_kj_k}\end{aligned}$$

As for the right term R, this is given by:

$$\begin{aligned}R_{ij}&=(U^{\otimes l}T)_{ij}\\&=\sum_bU^{\otimes l}_{ib}T_{bj}\\&=\sum_bU_{i_1b_1}\ldots U_{i_lb_l}T_{bj}\end{aligned}$$

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 $\xi_1,\ldots,\xi_k$:

$$<P_1\ldots P_kx,y>=<x,\xi_k><\xi_k,\xi_{k-1}>\ldots\ldots<\xi_2,\xi_1><\xi_1,y>$$

This gives the following formula for L:

$$\begin{aligned}
< L_{ij}\xi_{pq}, \xi_{rs} > &= \sum_a T_{ia} < P_{a_1j_1} \ldots P_{a_kj_k}\xi_{pq}, \xi_{rs} > \\
&= \sum_a T_{ia} < \xi_{pq}, \xi_{a_kj_k} > \ldots < \xi_{a_1j_1}, \xi_{rs} > \\
&= \sum_a T_{ia} G^{qj_k}_{pa_k} G^{j_kj_{k-1}}_{a_ka_{k-1}} \ldots G^{j_2j_1}_{a_2a_1} G^{j_1s}_{a_1r} \\
&= \sum_a T_{ia} G^{k+2}_{rap,sjq} \\
&= (T^\circ G^{k+2})_{rip,sjq}
\end{aligned}$$

As for the right term R, this is given by:

$$\begin{aligned}
< R_{ij}\xi_{pq}, \xi_{rs} > &= \sum_b < P_{i_1b_1} \ldots P_{i_lb_l}\xi_{pq}, \xi_{rs} > T_{bj} \\
&= \sum_b < \xi_{pq}, \xi_{i_lb_l} > \ldots < \xi_{i_1b_1}, \xi_{rs} > T_{bj} \\
&= \sum_b G^{qb_l}_{pi_l} G^{b_lb_{l-1}}_{i_li_{l-1}} \ldots G^{b_2b_1}_{i_2i_1} G^{b_1s}_{i_1r} T_{bj} \\
&= \sum_b G^{l+2}_{rip,sbq} T_{bj} \\
&= (G^{l+2}T^\circ)_{rip,sjq}
\end{aligned}$$

Thus, we obtain the formula in the statement. See [13]. $\square$

The point now is that, with $k = 0$, we obtain in this way precisely the spaces P_l computed by Jones in [61]. Thus, we are led to the following result:

Theorem 11.10. *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 11.9 with the subfactor computation in [61]. For full details here, we refer to [13].

(2) This is a consequence of (1), and of the Peter-Weyl type results from [99], which tell us that fixed points can be counted by integrating characters. $\square$

Regarding now the subfactor itself, the result here is as follows:

Theorem 11.11. *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 11.6, can be performed in an "equivariant setting", for commuting squares having components as follows:

$$D\otimes_GE=(D\otimes(E\rtimes\widehat{G}))^G$$

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:

$$\begin{tikzcd}
D_0\otimes_GE_\infty & D_1\otimes_GE_\infty & D_2\otimes_GE_\infty & \\
D_0\otimes_GE_2 \arrow[r] \arrow[u, dotted] & D_1\otimes_GE_2 \arrow[r] \arrow[u, dotted] & D_2\otimes_GE_2 \arrow[r, dotted] \arrow[u, dotted] & D_\infty\otimes_GE_2 \\
D_0\otimes_GE_1 \arrow[r] \arrow[u] & D_1\otimes_GE_1 \arrow[r] \arrow[u] & D_2\otimes_GE_1 \arrow[r, dotted] \arrow[u] & D_\infty\otimes_GE_1 \\
D_0\otimes_GE_0 \arrow[r] \arrow[u] & D_1\otimes_GE_0 \arrow[r] \arrow[u] & D_2\otimes_GE_0 \arrow[r, dotted] \arrow[u] & D_\infty\otimes_GE_0
\end{tikzcd}$$

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:

$$\mathbb C\otimes_GE_\infty\subset\mathbb C^N\otimes_GE_\infty$$

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 [4]. $\square$

All this is of course quite heavy, with the above results being subject to several extensions, and with all this involving several general correspondences between quantum groups, planar algebras, commuting squares and subfactors, that we will not get into.

As a technical comment here, it is possible to deduce Theorem 11.10 directly from Theorem 11.11, via some quantum group computations. However, Theorem 11.11 and its proof involve some heavy algebra and functional analysis, coming on top of the heavy algebra and functional analysis required for the general theory of the commuting squares, and this makes the whole thing quite unusable, in practice. Thus, while being technically weaker, Theorem 11.10 above remains the main result on the subject.

We refer to [4], [13], [21] and related papers for the full story of all this.

As already mentioned in the beginning of this section, all this is conjecturally related to statistical mechanics. Indeed, the Tannakian category/planar algebra formula from Theorem 11.9 has many similarities with the transfer matrix computations for the spin models, and this is explained in Jones' paper [61], and known for long before that, from his 1989 paper [60]. However, the precise significance of the Hadamard matrices in statistical mechanics, or in related areas such as link invariants, remains a bit unclear.

From a quantum group perspective, the same questions make sense. The idea here, which is old folklore, going back to the 1998 discovery by Wang [96] 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 [60], [61], via the connecting results presented above, and on the other hand by a number of more recent results, such as those in [16], 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.

Getting back to work now, the above discussion suggests heavily investing time and energy into the computation of integrals over Hopf images, because it is via such integrals that the mathematics of the corresponding lattice model is supposed to appear.

To be more precise, we would like for instance to have advanced representation theory results, of probabilistic flavor, in the spirit of [36], [45], [46].

Let us begin with some generalities. Our claim is that the "good" problem, about any compact quantum group, is that of computing the law of the main character.

This claim, which is something well-known, and generally agreed upon, is supported by a wealth of interesting results, which can be summarized as follows:

Theorem 11.12. *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 [99], 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 $uu^*=1\implies||u_{ii}||\leq 1$, 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 [99], the idea being that if f is not injective, then it must strictly increase one of the spaces $Fix(u^{\otimes k})$. $\square$

As a conclusion, computing $\mu=law(\chi)$ is indeed the main question to be solved, from a massive number of mathematical viewpoints. In addition to all this, in view of the above, the measure $\mu=law(\chi)$ is expected to have an interesting physical meaning.

More concretely now, let us first investigate the quantum groups S_N,S_N^+. For the symmetric group S_N that the standard coordinates are given by $u_{ij}=\chi(\sigma|\sigma(j)=i)$, and so the main character counts the number of fixed points:

$$\chi(\sigma)=\sum_i\delta_{\sigma(i),i}=\#\left\{i\in\{1,\ldots,N\}\Big|\sigma(i)=i\right\}$$

A well-known computation, based on the inclusion-exclusion principle, shows that with $N\to\infty$ the probability for a random permutation $\sigma\in S_N$ to have no fixed points is $\simeq\frac{1}{e}$.

More generally, one can show that the probability for $\sigma \in S_N$ to have exactly k fixed points is $\simeq \frac{1}{k!e}$. Thus, $\mu = law(\chi)$ becomes with $N \to \infty$ a Poisson variable.

Regarding now S_N^+, the computation here is a bit more complicated, leading to a "free version" of the Poisson law. In order to explain this, we will need the following result, with $*$ being the classical convolution, and $\boxplus$ being Voiculescu's free convolution:

Theorem 11.13. *The following Poisson type limits converge, for any $t > 0$,*

$$p_t = \lim_{n \to \infty} \left(\left(1 - \frac{1}{n}\right) \delta_0 + \frac{1}{n}\delta_t \right)^{*n} \quad , \quad \pi_t = \lim_{n \to \infty} \left(\left(1 - \frac{1}{n}\right) \delta_0 + \frac{1}{n}\delta_t \right)^{\boxplus n}$$

the limiting measures being the Poisson law p_t, and the Marchenko-Pastur law π_t,

$$p_t = \frac{1}{e^t} \sum_{k=0}^{\infty} \frac{t^k \delta_k}{k!} \quad , \quad \pi_t = \max(1-t, 0)\delta_0 + \frac{\sqrt{4t - (x-1-t)^2}}{2\pi x} \, dx$$

whose moments are given by the following formulae:

$$M_k(p_t) = \sum_{\pi \in P(k)} t^{|\pi|} \quad , \quad M_k(\pi_t) = \sum_{\pi \in NC(k)} t^{|\pi|}$$

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 [27], [67], [95]. □

Getting back now to quantum groups, the results here are as follows:

Theorem 11.14. *The law of $\chi = \sum_i u_{ii}$ is as follows:*

(1) *For S_N with $N \to \infty$ we obtain the Poisson law p_1.*
(2) *For S_N^+ with $N \geq 4$ we obtain the free Poisson law π_1.*

Also, the law of $\chi_t = \sum_{i=1}^{[tN]} u_{ii}$ for S_N/S_N^+, with $t \in (0, 1]$, 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 for instance by using the inclusion-exclusion principle, and then letting $N \to \infty$, as explained above.

(2) In the free case it is known that $P_k = Fix(u^{\otimes k})$ equals $TL_N(k)$ at $N \geq 4$, and at the probabilistic level, this leads to the formulae in the statement. See [12]. $\square$

Let us go back now to the Hadamard matrices, and do some computations here. In the general matrix model context, from Definition 10.9 above, we have the following formula for the Haar integration functional of the Hopf image, coming from [99]:

Theorem 11.15. *Given an inner faithful model $\pi : C(G) \to M_K(C(T))$, we have*

$$\int_G = \lim_{k\to\infty} \frac{1}{k} \sum_{r=1}^k \int_G^r$$

where $\int_G^r = (\varphi \circ \pi)^{*r}$, with $\varphi = tr \otimes \int_T$ being 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 Theorem 10.8 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 of Theorem 10.8, we conclude that the 1-eigenspace that we are interested in equals $Fix(V)$. But, according to Theorem 11.8, we have:

$$Fix(V) = Fix(v)$$

Thus, we have proved that we have $\int_G' = \int_G$, as desired. $\square$

In practice, 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 11.16. *The truncated integrals $\int_G^r = (\varphi \circ \pi)^{*r}$ are given by*

$$\int_G^r u_{a_1b_1}^{\varepsilon_1} \ldots u_{a_pb_p}^{\varepsilon_p} = (T_\varepsilon^r)_{a_1\ldots a_p, b_1\ldots b_p}$$

for any exponents $\varepsilon_i \in \{1, *\}$, with the matrix on the right being given by

$$(T_\varepsilon)_{i_1\ldots i_p, j_1\ldots j_p} = \left(tr \otimes \int_T\right) (U_{i_1j_1}^{\varepsilon_1} \ldots U_{i_pj_p}^{\varepsilon_p})$$

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. $\square$

Regarding now the main character, the result here is as follows:

Theorem 11.17. *Let μ^r be the law of $\chi = Tr(u)$ with respect to $\int_G^r = (\varphi \circ \pi)^{*r}$.*

(1) *We have the convergence formula $\mu = \lim_{k\to\infty} \frac{1}{k}\sum_{r=0}^k \mu^r$, in moments.*
(2) *The $*$-moments of the truncated measure μ^r are the numbers $c_\varepsilon^r = Tr(T_\varepsilon^r)$.*

Proof. These results are both elementary, the proof being as follows:
(1) This follows from the general limiting formula in Theorem 11.15.
(2) This follows from the formula in Proposition 11.16, by summing over $a_i = b_i$. $\square$

In connection with the complex Hadamard matrices, we can use this technology in order to discuss the behavior of the construction $H \to G$ with respect to the operations $H \to H^t, \bar{H}, H^*$. Let us first introduce the following abstract duality:

Definition 11.18. *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 $\widetilde{\rho} : C(U_N^+) \to M_N(\mathbb{C})$ by $v_{kl} \to U'_{kl}$.*
(2) *We perform the Hopf image construction, as to get a model $\rho : C(G') \to M_N(\mathbb{C})$.*

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 [11].

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 11.19. *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 $\gamma_p^r(G) = \gamma_r^p(G')$.*
(2) *η^r has the same moments as the matrix $T'_r = T_r(G')$.*
(3) *In the real case $u = \bar{u}$ we have $\eta^r = law(T'_r)$.*

Proof. All the results follow from Theorem 11.17, 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 $N^rc_p^r(A)=N^pc_r^p(A')$. Thus we have $c_p^r(A)/N^p=c_r^p(A')/N^r$, and this gives the result.

(2) By using (1) and the formula in Theorem 11.17, we obtain:

$$\frac{c_p^r(A)}{N^p}=\frac{c_r^p(A')}{N^r}=\frac{Tr((T'_r)^p)}{N^r}=tr((T'_r)^p)$$

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. □

All this is interesting in connection with the transposition operation $H\to H^t$ for the complex Hadamard matrices, and its relation with the lattice model problematics. Indeed, in the context of the classical spin models, the matrix of Boltzmann weights must be symmetric, and the precise meaning of the "Hadamard matrix models" depends on this. For more on this, and other related issues, we refer to [11] and related papers.

12. Fourier models

We have seen that associated to any 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.

Generally speaking, the quantum group $G \subset S_N^+$ is expected to capture the mathematics and physics of the Hadamard matrix $H \in M_N(\mathbb{C})$, via its representation theory.

All this is, unfortunately, a bit conjectural for the moment. In what concerns von Neumann algebra, orthogonal MASA, commuting square, subfactor and planar algebra aspects, this is definitely the case, thanks to the results explained in section 11.

Getting beyond this level, however, as to reach to some clear statistical mechanical results, in the spirit of [59], [60], [61] and beyond, remains an open problem.

From a purely mathematical perspective, there are many interesting questions which are open as well. We would like for instance to know if the defect, and the other geometric invariants of H, are captured or not by the representation theory of G. Similar questions make sense for the glow. Nothing much is known here, and for some comments and speculations on this subject, we refer to [4], [5], [6], [7], [8], [9].

In the lack of an answer to these questions, let us go back to the construction $H \to G$, as it is, and try to have more examples worked out. Generally speaking, going beyond Theorem 10.16 is a difficult task, and only one computation is available so far.

This computation, performed in [33] by using the subfactor formalism, and in [11] by using the quantum group formalism, regards the Diţă deformations of the tensor products $F_{G\times H} = F_G \otimes F_H$ of Fourier matrices. Besides [11], [33], some further results on all this are available from [9] and from [28]. We will follow here the approach in [11].

Before starting, we should mention that, in view of the results from section 4 above, the natural question regarding the deformed Fourier matrices would be that of computing the quantum groups associated to the Nicoara-White deformations of F_G.

However, no result is available here so far, the point being that the above-mentioned papers [9], [11], [28], [33] were all written before the Nicoara-White discovery in [73].

In short, we have to be modest here as well. In what follows we will explain the material from the paper [11], which is somehow central to the subject. This will consist in the computation for the Diţă deformations of the tensor products $F_{G\times H} = F_G \otimes F_H$, at generic values of the parameters, and of some related probabilistic work.

Let us begin by recalling, following [47], the definition of the deformations:

Proposition 12.1. *The matrix $\mathcal{F}_{G\times H}\in M_{G\times H}(\mathbb{T}^{G\times H})$ given by*

$$(\mathcal{F}_{G\times H})_{ia,jb}(Q)=Q_{ib}(F_G)_{ij}(F_H)_{ab}$$

is complex Hadamard, and its fiber at $Q=(1_{ib})$ is the Fourier matrix $F_{G\times H}$.

Proof. The fact that the rows of $F_G\otimes_Q F_H=\mathcal{F}_{G\times H}(Q)$ are pairwise orthogonal follows from definitions. With $1=(1_{ij})$ we have $(F_G\otimes_1 F_H)_{ia,jb}=(F_G)_{ij}(F_H)_{ab}$, and we recognize here the formula of $F_{G\times H}=F_G\otimes F_H$, in double index notation. $\square$

As in [11], it is convenient to take an abstract approach to all this:

Definition 12.2. *Associated to a finite abelian group X is the Fourier model*

$$\pi:C(X)\to M_{|X|}(\mathbb{C})$$

coming from the matrix $(U_{ij})_{kl}=\frac{1}{N}F_{i-j,k-l}$, where $F=F_X$.

Now let X,Y be finite abelian groups, and let us try to understand the model constructed by deforming the tensor product of the corresponded Fourier models:

Definition 12.3. *Given two finite abelian groups X,Y, we consider the corresponding Fourier models U,V, we construct the deformation $W=U\otimes_Q V$, and we factorize*

$$\begin{tikzcd} C(S^+_{X\times Y}) \arrow[rr, "\pi_Q"] \arrow[dr] & & M_{X\times Y}(\mathbb{C}) \\ & C(G_Q) \arrow[ur, "\pi"'] & \end{tikzcd}$$

with $C(G_Q)$ being the Hopf image of π_Q.

Explicitely computing the compact quantum group G_Q, as function of the parameter matrix $Q\in M_{X\times Y}(\mathbb{T})$, will be our main purpose, in what follows.

In order to do so, we use the following notion:

Definition 12.4. *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 then the free analogue of $\wr$, the usual wreath product. See [11].

We will need as well the following elementary result:

Proposition 12.5. *If X is a finite abelian group then*

$$C(X)=C(S_X^+)/<u_{ij}=u_{kl}|\forall i-j=k-l>$$

with all the indices taken inside X.

Proof. Observe first that $C(Y)=C(S_X^+)/<u_{ij}=u_{kl}|\forall i-j=k-l>$ is commutative, because $u_{ij}u_{kl}=u_{ij}u_{i,l-k+i}=\delta_{j,l-k+i}u_{ij}$ and $u_{kl}u_{ij}=u_{i,l-k+i}u_{ij}=\delta_{j,l-k+i}u_{ij}$. Thus we have $Y\subset S_X$, and since $u_{ij}(\sigma)=\delta_{i\sigma(j)}$ for any $\sigma\in Y$, 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 $\sigma(i)=i+x$ for some $x\in X$, and so $\sigma\in X$, as desired. $\square$

We can now factorize representation π_Q in Definition 12.3, as follows:

Theorem 12.6. *We have a factorization*

$$\begin{tikzcd}
C(S_{X\times Y}^+) \arrow[rr, "\pi_Q"] \arrow[dr] & & M_{X\times Y}(\mathbb{C}) \\
& C(Y\wr_* X) \arrow[ur, "\pi"'] &
\end{tikzcd}$$

given by $U_{ab}^{(i)}=\sum_j W_{ia,jb}$ and by $V_{ij}=\sum_a W_{ia,jb}$, independently of b.

Proof. With $K=F_X,L=F_Y$ and $M=|X|,N=|Y|$, the formula of the magic matrix $W\in M_{X\times Y}(M_{X\times Y}(\mathbb{C}))$ associated to $H=K\otimes_Q L$ is:

$$\begin{aligned}
(W_{ia,jb})_{kc,ld} &= \frac{1}{MN}\cdot\frac{Q_{ic}Q_{jd}}{Q_{id}Q_{jc}}\cdot\frac{K_{ik}K_{jl}}{K_{il}K_{jk}}\cdot\frac{L_{ac}L_{bd}}{L_{ad}L_{bc}}\\
&= \frac{1}{MN}\cdot\frac{Q_{ic}Q_{jd}}{Q_{id}Q_{jc}}\cdot K_{i-j,k-l}L_{a-b,c-d}
\end{aligned}$$

Our claim that the representation π_Q constructed in Definition 12.3 can be factorized in three steps, up to the factorization in the statement, as follows:

$$\begin{tikzcd}
C(S_{X\times Y}^+) \arrow[rr, "\pi_Q"] \arrow[d] & & M_{X\times Y}(\mathbb{C}) \\
C(S_Y^+\wr_* S_X^+) \arrow[r] \arrow[urr, dotted] & C(S_Y^+\wr_* X) \arrow[r] \arrow[ur, dotted] & C(Y\wr_* X) \arrow[u, dotted]
\end{tikzcd}$$

Indeed, the construction of the map on the left is standard, and this produces the first factorization. Regarding the second factorization, this comes from the fact that since the elements V_{ij} depend on $i-j$, they satisfy the defining relations for the quotient algebra $C(S_X^+)\to C(X)$, coming from Proposition 12.5. Finally, regarding the third factorization, observe that the above matrix $W_{ia,jb}$ depends only on $a-b$. By summing over j we obtain that $U^{(i)}_{ab}$ depends only on $a-b$, and we are done. □

In order to further factorize the above representation, we use:

Definition 12.7. *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 12.6, the point is that we have:

Proposition 12.8. *With $L = F_Y, N = |Y|$ we have an isomorphism*

$$C(Y \wr_* X) \simeq C^*(Y)^{*X} \rtimes C(X)$$

given by $v_{ij} \to 1 \otimes v_{ij}$ and $u^{(i)}_{ab} = \frac{1}{N} \sum_c L_{b-a,c} c^{(i)} \otimes 1$.

Proof. We know that $C(Y \wr_* X)$ is the quotient of $C(Y)^{*X} * C(X)$ by the relations $[u^{(i)}_{ab}, v_{ij}] = 0$. Now since v_{ij} depends only on $j-i$, we obtain:

$$[u^{(i)}_{ab}, v_{kl}] = [u^{(i)}_{ab}, v_{i,l-k+i}] = 0$$

Thus, we are in a usual tensor product situation, and we have:

$$C(Y \wr_* X) = C(Y)^{*X} \otimes C(X)$$

Let us compose now this identification with $\Phi^{*X} \otimes id$, where $\Phi : C(Y) \to C^*(Y)$ is the Fourier transform. We obtain an isomorphism as in the statement, and since $\Phi(u_{ab}) = \frac{1}{N} \sum_c L_{b-a,c} c$, the formula for the image of $u^{(i)}_{ab}$ is indeed the one in the statement. □

Here is now our key result, which will lead to further factorizations:

Proposition 12.9. *With $c^{(i)} = \sum_a L_{ac} u^{(i)}_{a0}$ 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 $\pi(c_1^{(i_1)} \ldots c_s^{(i_s)})$ is diagonal, for any $i_1, \ldots, i_s$.

Proof. We have the following formula:

$$\pi(c^{(i)})=\sum_a L_{ac}\pi(u_{a0}^{(i)})=\sum_{aj}L_{ac}W_{ia,j0}$$

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 12.6, as follows:

Theorem 12.10. *We have a factorization as follows,*

$$\begin{tikzcd} C(S^+_{X\times Y}) \arrow[rr, "\pi_Q"] \arrow[dr] & & M_{X\times Y}(\mathbb{C}) \\ & C^*(\Gamma_{X,Y})\rtimes C(X) \arrow[ur, "\rho"'] & \end{tikzcd}$$

where $\Gamma_{X,Y}=Y^{*X}/<[c_1^{(i_1)}\ldots c_s^{(i_s)},d_1^{(j_1)}\ldots d_s^{(j_s)}]=1|\sum_r c_r=\sum_r d_r=0>$.

Proof. Assume that we have a representation $\pi:C^*(\Gamma)\rtimes C(X)\to M_L(\mathbb{C})$, let Λ be a X-stable normal subgroup of Γ, so that X acts on Γ/Λ and that we can form the crossed coproduct $C^*(\Gamma/\Lambda)\rtimes C(X)$, and assume that π is trivial on Λ. Then π factorizes as:

$$\begin{tikzcd} C^*(\Gamma)\rtimes C(X) \arrow[rr, "\pi"] \arrow[dr] & & M_L(\mathbb{C}) \\ & C^*(\Gamma/\Lambda)\rtimes C(X) \arrow[ur, "\rho"'] & \end{tikzcd}$$

With $\Gamma=Y^{*X}$, and by using the above results, this gives the result. □

In general, further factorizing the representation found in Theorem 12.10 is a quite complicated task. In what follows we restrict attention to the case where the parameter matrix Q is generic, in the sense that its entries are as algebrically independent as possible, and we prove that the representation in Theorem 12.10 is the minimal one.

Our starting point is the group $\Gamma_{X,Y}$ found above:

Definition 12.11. *Associated to two finite abelian groups X,Y is the discrete group*

$$\Gamma_{X,Y}=Y^{*X}\Big/\left\langle [c_1^{(i_1)}\ldots c_s^{(i_s)},d_1^{(j_1)}\ldots d_s^{(j_s)}]=1\Big|\sum_r c_r=\sum_r d_r=0\right\rangle$$

where the superscripts refer to the X copies of Y, 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 Y, we can make Y act on G^Y, and form the product $G^Y\rtimes Y$.

Since the elements of type $(g,\ldots,g)$ are invariant, we can form as well the product $(G^Y/G)\rtimes Y$, and by identifying $G^Y/G\simeq G^{|Y|-1}$ via the map $(1,g_1,\ldots,g_{|Y|-1})\to(g_1,\ldots,g_{|Y|-1})$, we obtain a product $G^{|Y|-1}\rtimes Y$.

With these notations, we have the following result:

Proposition 12.12. *The group $\Gamma_{X,Y}$ has the following properties:*

1. $\Gamma_{X,Y}\simeq\mathbb{Z}^{(|X|-1)(|Y|-1)}\rtimes Y$.
2. $\Gamma_{X,Y}\subset\mathbb{Z}^{(|X|-1)|Y|}\rtimes Y$ *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* $\mathbb{Z}^{(|X|-1)|Y|}$.

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:

$$\Gamma_{X,Y}\simeq\mathbb{Z}^{(|X|-1)(|Y|-1)}\rtimes Y\subset\mathbb{Z}^{(|X|-1)|Y|}\rtimes Y$$

Our first claim is that the formula in (2) defines a morphism as follows:

$$\Gamma_{X,Y}\to\mathbb{Z}^{(|X|-1)|Y|}\rtimes Y$$

Indeed, the elements $(0,c)$ produce a copy of Y, and since we have a group embedding $Y\subset\mathbb{Z}^{|Y|}\rtimes Y$ given by $c\to(b_0-b_c,c)$, the elements $C^{(i)}=(b_{i0}-b_{ic},c)$ produce a copy of Y, for any $i \neq 0$. In order to check now the commutation relations, observe that:

$$C_1^{(i_1)} \ldots C_s^{(i_s)} = \left(b_{i_1 0} - b_{i_1 c_1} + b_{i_2 c_1} - b_{i_2, c_1+c_2} + \ldots + b_{i_s, c_1+\ldots+c_{s-1}} - b_{i_s, c_1+\ldots+c_s}, \sum_r c_r \right)$$

Thus $\sum_r c_r = 0$ implies $C_1^{(i_1)} \ldots C_s^{(i_s)} \in \mathbb{Z}^{(|X|-1)|Y|}$, and since we are now inside an abelian group, we have the commutation relations, and our claim is proved.

Using the considerations before the statement of the proposition, it is routine to construct an embedding $\mathbb{Z}^{(|X|-1)(|Y|-1)} \rtimes Y \subset \mathbb{Z}^{(|X|-1)|Y|} \rtimes Y$ such that we have group morphisms whose composition is the group morphism just constructed, as follows:

$$\Gamma_{X,Y} \to \mathbb{Z}^{(|X|-1)(|Y|-1)} \rtimes Y \subset \mathbb{Z}^{(|X|-1)|Y|} \rtimes Y$$

It remains to prove that the map on the left is injective. For this purpose, consider the morphism $\Gamma_{X,Y} \to Y$ 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:

$$1 \to T \to \Gamma_{X,Y} \to Y \to 1$$

This sequence splits by $c \to c^{(0)}$, so we have $\Gamma_{X,Y} \simeq T \rtimes Y$. Now by the definition of $\Gamma_{X,Y}$, the subgroup T constructed above is abelian, and is moreover generated by the elements $(-c)^{(0)} c^{(i)}$, $i, c \neq 0$.

Finally, the fact that T is freely generated by these elements follows from the computation in the proof of Proposition 12.14 below. □

Let us specify now what our genericity assumptions are:

Definition 12.13. *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 $Q \in M_{X \times Y}(\mathbb{T})$, 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.*

We will need the following technical result:

Proposition 12.14. *Assume that $Q \in M_{X \times Y}(\mathbb{T})$ is generic, and put*

$$\theta_{ic}^{ke} = \frac{Q_{i,e-c} Q_{i-k,e}}{Q_{ie} Q_{i-k,e-c}}$$

For every $k \in X$, we have a representation $\pi^k : \Gamma_{X,Y} \to U_{|Y|}$ given by:

$$\pi^k(c^{(i)}) \epsilon_e = \theta_{ic}^{ke} \epsilon_{e-c}$$

The family of representations $(\pi^k)_{k \in X}$ is projectively faithful in the sense that if for some $t \in \Gamma_{X,Y}$, we have that $\pi^k(t)$ is a scalar matrix for any k, then $t = 1$.

Proof. The representations π^k arise from above. With $\Gamma_{X,Y} = T \rtimes Y$, as in the proof of Proposition 12.12, we see that for $t \in \Gamma_{X,Y}$ 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 12.12 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 result, technical as well:

Proposition 12.15. *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. Put $A = C^*(\Gamma) \rtimes C(H)$. We start with the following Hopf algebra exact sequence, where $i(f) = 1 \otimes f$ and $p = \varepsilon \otimes 1$:

$$\mathbb{C} \to C(H) \xrightarrow{i} A \xrightarrow{p} C^*(\Gamma) \to \mathbb{C}$$

Since $\pi \circ i$ is injective, and Hopf subalgebra $\pi \circ i(C(H))$ is central in L, we can form the quotient Hopf algebra $\overline{L} = L/(\pi \circ i(C(H))^+ L$, and we get another exact sequence:

$$\mathbb{C} \to C(H) \xrightarrow{\pi\circ i} L \xrightarrow{q} \overline{L} \to \mathbb{C}$$

Note that this sequence is indeed exact, e.g. by centrality. So we get the following diagram with exact rows, with the Hopf algebra map on the right 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 $u(g) = 1$. Then $q'\pi(g \otimes 1) = up(g \otimes 1) = u(g) = \overline{g} = 1$. For $g \in \Gamma$, put:

$$_gA = \{a \in A \mid p(a_1) \otimes a_2 = g \otimes a\}$$

$$_{\overline{g}}L = \{l \in L \mid q'(l_1) \otimes l_2 = \overline{g} \otimes l\}$$

The commutativity of the right square ensures that $\pi(_gA) \subset {}_{\overline{g}}L$. Then with the previous g, we have $\pi(g \otimes 1) \in {}_{\overline{1}}L = \pi i(C(H))$ (exactness of the sequence), so $\pi(g \otimes 1) = \pi(1 \otimes f)$ for some $f \in C(H)$. We conclude by our assumption that $g = 1$. □

We have now all the needed ingredients for proving a main result, as follows:

Theorem 12.16. *When Q is generic, the minimal factorization for π_Q is*

$$\begin{tikzcd}
C(S^+_{X\times Y}) \arrow[rr, "\pi_Q"] \arrow[dr] & & M_{X\times Y}(\mathbb{C}) \\
& C^*(\Gamma_{X,Y}) \rtimes C(X) \arrow[ur, "\pi"'] &
\end{tikzcd}$$

where $\Gamma_{X,Y} \simeq \mathbb{Z}^{(|X|-1)(|Y|-1)} \rtimes Y$ is the discrete group constructed above.

Proof. We want to apply Proposition 12.14 to the morphism $\theta : C^*(\Gamma_{X,Y}) \rtimes C(X) \to L$ arising from the factorization in Theorem 12.10, where L denotes the Hopf image of π_Q, which produces the following commutative diagram:

$$\begin{tikzcd}
C(S_{X\times Y}^+) \arrow[rr, "\pi_Q"] \arrow[dr] \arrow[ddr] & & M_{X\times Y}(\mathbb{C}) \\
& L \arrow[ur] & \\
& C^*(\Gamma_{X,Y}) \rtimes C(X) \arrow[u, dashed, "\theta"'] \arrow[uur, "\pi"'] &
\end{tikzcd}$$

The first observation is that the injectivity assumption on $C(X)$ holds by construction, and that for $f \in C(X)$, the matrix $\pi(f)$ is "block scalar", the blocks corresponding to the indices k in the basis ε_{ke} in the basis from Proposition 12.14.

Now for $r \in \Gamma_{X,Y}$ with $\theta(r \otimes 1) = \theta(1 \otimes f)$ for some $f \in C(X)$, we see, using the commutative diagram, that we will have that $\pi(r \otimes 1)$ is block scalar.

By Proposition 12.12, the family of representations (π^k) of $\Gamma_{X,Y}$, corresponding to the blocks k, is projectively faithful, so $r = 1$.

We can apply indeed Proposition 12.14, and we are done. $\square$

Let us try now to compute 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 12.17. *We have the moment formula*

$$\int_G \chi^p = \frac{1}{|X| \cdot |Y|} \# \left\{ \begin{matrix} i_1, \ldots, i_p \in X \\ d_1, \ldots, d_p \in Y \end{matrix} \middle| \begin{matrix} [(i_1, d_1), (i_2, d_2), \ldots, (i_p, d_p)] \\ = [(i_1, d_p), (i_2, d_1), \ldots, (i_p, d_{p-1})] \end{matrix} \right\}$$

where the sets between square brackets are by definition sets with repetition.

Proof. According to the various formulae above, the factorization found in Theorem 12.16 is, at the level of standard generators, as follows:

$$\begin{matrix} C(S_{X\times Y}^+) & \to & C^*(\Gamma_{X,Y}) \otimes C(X) & \to & M_{X\times Y}(\mathbb{C}) \\ u_{ia,jb} & \to & \frac{1}{|Y|}\sum_c F_{b-a,c} c^{(i)} \otimes v_{ij} & \to & W_{ia,jb} \end{matrix}$$

Thus, the main character is given by:

$$\chi = \frac{1}{|Y|} \sum_{iac} c^{(i)} \otimes v_{ii} = \sum_{ic} c^{(i)} \otimes v_{ii} = \left(\sum_{ic} c^{(i)} \right) \otimes \delta_1$$

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 $p \geq 1$:

$$\int_G \chi^p = \frac{1}{|X|} \int_{\widehat{\Gamma}_{X,Y}} \left(\sum_{ic} c^{(i)} \right)^p$$

Let $S_i = \sum_c c^{(i)}$. By using the embedding in Proposition 12.12 (2), with the notations there we have $S_i = \sum_c (b_{i0} - b_{ic}, c)$, and these elements multiply as follows:

$$S_{i_1} \ldots S_{i_p} = \sum_{c_1 \ldots c_p} \begin{pmatrix} \begin{matrix} b_{i_1 0} - b_{i_1 c_1} + b_{i_2 c_1} - b_{i_2, c_1 + c_2} \\ + b_{i_3, c_1 + c_2} - b_{i_3, c_1 + c_2 + c_3} + \ldots\ldots \\ \ldots\ldots + b_{i_p, c_1 + \ldots + c_{p-1}} - b_{i_p, c_1 + \ldots + c_p} \end{matrix} & , & c_1 + \ldots + c_p \end{pmatrix}$$

In terms of the new indices $d_r = c_1 + \ldots + c_r$, this formula becomes:

$$S_{i_1} \ldots S_{i_p} = \sum_{d_1 \ldots d_p} \begin{pmatrix} \begin{matrix} b_{i_1 0} - b_{i_1 d_1} + b_{i_2 d_1} - b_{i_2 d_2} \\ + b_{i_3 d_2} - b_{i_3 d_3} + \ldots\ldots \\ \ldots\ldots + b_{i_p d_{p-1}} - b_{i_p d_p} \end{matrix} & , & d_p \end{pmatrix}$$

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:

$$\int_{\widehat{\Gamma}_{X,Y}} S_{i_1} \ldots S_{i_p} = \frac{1}{|Y|} \# \left\{ d_1, \ldots, d_p \in Y \middle| \begin{matrix} [(i_1, d_1), (i_2, d_2), \ldots, (i_p, d_p)] \\ = [(i_1, d_p), (i_2, d_1), \ldots, (i_p, d_{p-1})] \end{matrix} \right\}$$

It follows that we have the following moment formula:

$$\int_{\widehat{\Gamma}_{X,Y}} \left(\sum_i S_i \right)^p = \frac{1}{|Y|} \# \left\{ \begin{matrix} i_1, \ldots, i_p \in X \\ d_1, \ldots, d_p \in Y \end{matrix} \middle| \begin{matrix} [(i_1, d_1), (i_2, d_2), \ldots, (i_p, d_p)] \\ = [(i_1, d_p), (i_2, d_1), \ldots, (i_p, d_{p-1})] \end{matrix} \right\}$$

Now by dividing by $|X|$, we obtain the formula in the statement. □

The formula in Theorem 12.17 can be interpreted as follows:

Theorem 12.18. *With $M = |X|, N = |Y|$ we have the formula*

$$law(\chi) = \left(1 - \frac{1}{N}\right) \delta_0 + \frac{1}{N} law(A)$$

where $A \in C(\mathbb{T}^{MN}, M_M(\mathbb{C}))$ is given by $A(q) =$ Gram matrix of the rows of q.

Proof. According to Theorem 12.17, we have the following formula:

$$\begin{aligned}\int_G\chi^p &= \frac{1}{MN}\sum_{i_1\ldots i_p}\sum_{d_1\ldots d_p}\delta_{[i_1d_1,\ldots,i_pd_p],[i_1d_p,\ldots,i_pd_{p-1}]}\\ &= \frac{1}{MN}\int_{\mathbb{T}^{MN}}\sum_{i_1\ldots i_p}\sum_{d_1\ldots d_p}\frac{q_{i_1d_1}\ldots q_{i_pd_p}}{q_{i_1d_p}\ldots q_{i_pd_{p-1}}}\,dq\\ &= \frac{1}{MN}\int_{\mathbb{T}^{MN}}\sum_{i_1\ldots i_p}\left(\sum_{d_1}\frac{q_{i_1d_1}}{q_{i_2d_1}}\right)\left(\sum_{d_2}\frac{q_{i_2d_2}}{q_{i_3d_2}}\right)\ldots\left(\sum_{d_p}\frac{q_{i_pd_p}}{q_{i_1d_p}}\right)dq\end{aligned}$$

Consider now the Gram matrix in the statement, $A(q)_{ij}=<R_i,R_j>$, where $R_1,\ldots,R_M$ are the rows of $q\in\mathbb{T}^{MN}\simeq M_{M\times N}(\mathbb{T})$. We have then:

$$\begin{aligned}\int_G\chi^p &= \frac{1}{MN}\int_{\mathbb{T}^{MN}}<R_{i_1},R_{i_2}><R_{i_2},R_{i_3}>\ldots<R_{i_p},R_{i_1}>\\ &= \frac{1}{MN}\int_{\mathbb{T}^{MN}}A(q)_{i_1i_2}A(q)_{i_2i_3}\ldots A(q)_{i_pi_1}\\ &= \frac{1}{MN}\int_{\mathbb{T}^{MN}}Tr(A(q)^p)dq\\ &= \frac{1}{N}\int_{\mathbb{T}^{MN}}tr(A(q)^p)dq\end{aligned}$$

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

The problem now is that of finding the good regime, $M=f(K),N=g(K),K\to\infty$, where the measure in Theorem 12.18 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 12.19. *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 12.17 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, since there are $M(M-1)\ldots(M-|\pi|+1)\simeq M^{|\pi|}$ choices for a multi-index $(i_1,\ldots,i_p)\in X^p$ satisfying $\ker i=\pi$, we have:

$$C_\pi\simeq M^{|\pi|-1}N^{-1}\#\left\{d_1,\ldots,d_p\in Y\Big|[d_\alpha|\alpha\in b]=[d_{\alpha-1}|\alpha\in b],\forall b\in\pi\right\}$$

Consider now the partition $\sigma=\ker d$. The contribution of σ to the above quantity C_π is then given by $\Delta(\pi,\sigma)N(N-1)\ldots(N-|\sigma|+1)\simeq\Delta(\pi,\sigma)N^{|\sigma|}$, where:

$$\Delta(\pi,\sigma)=\begin{cases}1&\text{if }|b\cap c|=|(b-1)\cap c|,\forall b\in\pi,\forall c\in\sigma\\0&\text{otherwise}\end{cases}$$

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 happens 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 12.20. *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 $\mu=\left(1-\frac{1}{\alpha^2K^2}\right)\delta_0+\frac{1}{\alpha^2K^2}D_{\frac{1}{\alpha K}}(\pi_1)$.

Proof. At $\alpha=\beta$, this follows from Proposition 12.19. In general now, we have:

$$\begin{aligned}\frac{c_p}{K^{p-1}}&\simeq\sum_{\pi\in NC(p)}\alpha^{|\pi|-1}\beta^{p-|\pi|}\\&=\frac{\beta^p}{\alpha}\sum_{\pi\in NC(p)}\left(\frac{\alpha}{\beta}\right)^{|\pi|}\\&=\frac{\beta^p}{\alpha}\int x^pd\pi_{\alpha/\beta}(x)\end{aligned}$$

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. □

As a first comment, when interchanging α, β we obtain $D_{\frac{1}{\beta K}}(\pi_{\alpha/\beta}) = D_{\frac{1}{\alpha K}}(\pi_{\beta/\alpha})$, which is a consequence of the well-known formula $\pi_{t^{-1}} = D_t(\pi_t)$. This latter formula is best understood by using Kreweras complementation, which gives indeed:

$$\begin{aligned} \int x^p d\pi_t(x) &= \sum_{\pi\in NC(p)} t^{|\pi|} \\ &= t^{p+1}\sum_{\pi\in NC(p)} t^{-|\pi|} \\ &= t\int(tx)^p d\pi_{t^{-1}}(x) \end{aligned}$$

Let us state as well an explicit result, regarding densities:

Theorem 12.21. *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. □

Observe that at $\alpha = \beta = 1$, where $M = N = K \to \infty$, the measure in Theorem 12.21, namely $\mu = \left(1 - \frac{1}{K^2}\right)\delta_0 + \frac{1}{K^2}D_{\frac{1}{K}}(\pi_1)$, 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 don't have a convergence of supports is not surprising, because our convergence is in moments.

We have as well the following result, which includes computations from [9]:

Theorem 12.22. *Given two finite abelian groups G, H, with $|G| = M, |H| = N$, consider the main character χ of the quantum group associated to $\mathcal{F}_{G\times H}$. We have then*

$$law\left(\frac{\chi}{N}\right) = \left(1 - \frac{1}{M}\right)\delta_0 + \frac{1}{M}\pi_t$$

in moments, with $M = tN \to \infty$, where π_t is the free Poisson law of parameter $t > 0$. In addition, this formula holds for any generic fiber of $\mathcal{F}_{G\times H}$.

Proof. We already know that the second assertion holds, as explained in Theorem 12.21.

Regarding now the first assertion, which is from [9], our first claim is that for the representation coming from the parametric matrix $\mathcal{F}_{G\times H}$ we have the following formula, where $M = |G|, N = |H|$, and the sets between brackets are sets with repetitions:

$$c_p^r = \frac{1}{M^{r+1}N}\#\left\{\begin{matrix} i_1,\ldots,i_r,a_1,\ldots,a_p \in \{0,\ldots,M-1\}, \\ b_1,\ldots,b_p \in \{0,\ldots,N-1\}, \\ [(i_x+a_y,b_y),(i_{x+1}+a_y,b_{y+1})|y=1,\ldots,p] \\ = [(i_x+a_y,b_{y+1}),(i_{x+1}+a_y,b_y)|y=1,\ldots,p],\forall x \end{matrix}\right\}$$

Indeed, by using the general moment formula with $K = F_G$, $L = F_H$, we have:

$$\begin{aligned} c_p^r \;=\; & \frac{1}{(MN)^r}\int_{T^r}\sum_{i_1^1\ldots i_p^r}\sum_{b_1^1\ldots b_p^r}\frac{Q^1_{i_1^1b_1^1}Q^1_{i_1^2b_2^1}}{Q^1_{i_1^1b_2^1}Q^1_{i_1^2b_1^1}}\cdots\frac{Q^1_{i_p^1b_p^1}Q^1_{i_p^2b_1^1}}{Q^1_{i_p^1b_1^1}Q^1_{i_p^2b_p^1}}\cdots\cdots\frac{Q^r_{i_1^rb_1^r}Q^r_{i_1^1b_2^r}}{Q^r_{i_1^rb_2^r}Q^r_{i_1^1b_1^r}}\cdots\frac{Q^r_{i_p^rb_p^r}Q^r_{i_p^1b_1^r}}{Q^r_{i_p^rb_1^r}Q^r_{i_p^1b_p^r}} \\ & \frac{1}{M^{pr}}\sum_{j_1^1\ldots j_p^r}\frac{K_{i_1^1j_1^1}K_{i_1^2j_2^1}}{K_{i_1^1j_2^1}K_{i_1^2j_1^1}}\cdots\frac{K_{i_p^1j_p^1}K_{i_p^2j_1^1}}{K_{i_p^1j_1^1}K_{i_p^2j_p^1}}\cdots\cdots\frac{K_{i_1^rj_1^r}K_{i_1^1j_2^r}}{K_{i_1^rj_2^r}K_{i_1^1j_1^r}}\cdots\frac{K_{i_p^rj_p^r}K_{i_p^1j_1^r}}{K_{i_p^rj_1^r}K_{i_p^1j_p^r}} \\ & \frac{1}{N^{pr}}\sum_{a_1^1\ldots a_p^r}\frac{L_{a_1^1b_1^1}L_{a_1^2b_2^1}}{L_{a_1^1b_2^1}L_{a_1^2b_1^1}}\cdots\frac{L_{a_p^1b_p^1}L_{a_p^2b_1^1}}{L_{a_p^1b_1^1}L_{a_p^2b_p^1}}\cdots\cdots\frac{L_{a_1^rb_1^r}L_{a_1^1b_2^r}}{L_{a_1^rb_2^r}L_{a_1^1b_1^r}}\cdots\frac{L_{a_p^rb_p^r}L_{a_p^1b_1^r}}{L_{a_p^rb_1^r}L_{a_p^1b_p^r}}\,dQ \end{aligned}$$

Since we are in the Fourier matrix case, $K = F_G, L = F_H$, we can perform the sums over j, a. To be more precise, the last two averages appearing above are respectively:

$$\begin{aligned} \Delta(i) &= \prod_x\prod_y \delta(i_y^x + i_{y-1}^{x+1}, i_y^{x+1} + i_{y-1}^x) \\ \Delta(b) &= \prod_x\prod_y \delta(b_y^x + b_{y-1}^{x+1}, b_y^{x+1} + b_{y-1}^x) \end{aligned}$$

We therefore obtain the following formula for the truncated moments of the main character, where Δ is the product of Kronecker symbols constructed above:

$$c_p^r = \frac{1}{(MN)^r}\int_{T^r}\sum_{\Delta(i)=\Delta(b)=1}\frac{Q^1_{i_1^1b_1^1}Q^1_{i_1^2b_2^1}}{Q^1_{i_1^1b_2^1}Q^1_{i_1^2b_1^1}}\cdots\frac{Q^1_{i_p^1b_p^1}Q^1_{i_p^2b_1^1}}{Q^1_{i_p^1b_1^1}Q^1_{i_p^2b_p^1}}\cdots\cdots\frac{Q^r_{i_1^rb_1^r}Q^r_{i_1^1b_2^r}}{Q^r_{i_1^rb_2^r}Q^r_{i_1^1b_1^r}}\cdots\frac{Q^r_{i_p^rb_p^r}Q^r_{i_p^1b_1^r}}{Q^r_{i_p^rb_1^r}Q^r_{i_p^1b_p^r}}\,dQ$$

Now by integrating with respect to $Q \in (\mathbb{T}^{G\times H})^r$, we are led to counting the multi-indices i, b satisfying the condition $\Delta(i) = \Delta(b) = 1$, along with the following conditions, where the sets between brackets are by definition sets with repetitions:

$$\begin{bmatrix} i_1^1 b_1^1 & \ldots & i_p^1 b_p^1 & i_1^2 b_2^1 & \ldots & i_p^2 b_1^1 \end{bmatrix} = \begin{bmatrix} i_1^1 b_2^1 & \ldots & i_p^1 b_1^1 & i_1^2 b_1^1 & \ldots & i_p^2 b_p^1 \end{bmatrix}$$

$$\vdots$$

$$\begin{bmatrix} i_1^r b_1^r & \ldots & i_p^r b_p^r & i_1^1 b_2^r & \ldots & i_p^1 b_1^r \end{bmatrix} = \begin{bmatrix} i_1^r b_2^r & \ldots & i_p^r b_1^r & i_1^1 b_1^r & \ldots & i_p^1 b_p^r \end{bmatrix}$$

In a more compact notation, the moment formula is therefore as follows:

$$c_p^r = \frac{1}{(MN)^r} \# \left\{ i, b \Big| \Delta(i) = \Delta(b) = 1,\ [i_y^x b_y^x, i_y^{x+1} b_{y+1}^x] = [i_y^x b_{y+1}^x, i_y^{x+1} b_y^x], \forall x \right\}$$

Now observe that the above Kronecker type conditions $\Delta(i) = \Delta(b) = 1$ tell us that the arrays of indices $i = (i_y^x), b = (b_y^x)$ must be of the following special form:

$$\begin{pmatrix} i_1^1 & \ldots & i_p^1 \\ & \ldots & \\ i_r^1 & \ldots & i_p^r \end{pmatrix} = \begin{pmatrix} i_1 + a_1 & \ldots & i_1 + a_p \\ & \ldots & \\ i_r + a_1 & \ldots & i_r + a_p \end{pmatrix} , \begin{pmatrix} b_1^1 & \ldots & b_p^1 \\ & \ldots & \\ b_r^1 & \ldots & b_p^r \end{pmatrix} = \begin{pmatrix} j_1 + b_1 & \ldots & j_1 + b_p \\ & \ldots & \\ j_r + b_1 & \ldots & j_r + b_p \end{pmatrix}$$

Here all the new indices i_x, j_x, a_y, b_y are uniquely determined, up to a choice of i_1, j_1. Now by replacing i_y^x, b_y^x with these new indices i_x, j_x, a_y, b_y, with a MN factor added, which accounts for the choice of i_1, j_1, we obtain the following formula:

$$c_p^r = \frac{1}{(MN)^{r+1}} \# \left\{ i, j, a, b \Big|_{=\, [(i_x + a_y, j_x + b_{y+1}), (i_{x+1} + a_y, j_x + b_y)], \forall x}^{[(i_x + a_y, j_x + b_y), (i_{x+1} + a_y, j_x + b_{y+1})]} \right\}$$

Now observe that we can delete if we want the j_x indices, which are irrelevant. Thus, we obtain the announced formula. The continuation is via combinatorics, see [9]. $\square$

As already mentioned, on several occasions, such computations are expected to have some applications in statistical mechanics, but this remains to be worked out.

There are many other possible applications of the complex Hadamard matrices. Let us mention for instance some potential relations with noncommutative geometry, particle physics, and CKM type matrices, in the spirit of the paper of Connes [38].

Some other well-known applications of the Hadamard matrices concern questions in quantum information theory. We refer here to the MUB literature [26], [48], [89], with the remark that the relation of this with the above still remains to be understood.

This list, which adds to the previous considerations in this book, is certainly incomplete, the Fourier type matrices being potentially useful a bit everywhere.

References

[1] S. Agaian, Hadamard matrices and their applications, Springer (1985).

[2] 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.

[3] J. Backelin, Square multiples n give infinitely many cyclic n-roots, preprint 1989.

[4] T. Banica, Compact Kac algebras and commuting squares, *J. Funct. Anal.* **176** (2000), 80–99.

[5] T. Banica, The defect of generalized Fourier matrices, *Linear Algebra Appl.* **438** (2013), 3667–3688.

[6] T. Banica, First order deformations of the Fourier matrix, *J. Math. Phys.* **55** (2014), 1–22.

[7] T. Banica, Counting results for thin Butson matrices, *Electron. J. Combin.* **21** (2014), 1–14.

[8] T. Banica, The glow of Fourier matrices: universality and fluctuations, *Oper. Matrices* **9** (2015), 457–474.

[9] T. Banica, Deformed Fourier models with formal parameters, *Studia Math.* **239** (2017), 201–224.

[10] T. Banica, Complex Hadamard matrices with noncommutative entries, *Ann. Funct. Anal.* **9** (2018), 354–368.

[11] T. Banica and J. Bichon, Random walk questions for linear quantum groups, *Int. Math. Res. Not.* **24** (2015), 13406–13436.

[12] T. Banica, J. Bichon and B. Collins, Quantum permutation groups: a survey, *Banach Center Publ.* **78** (2007), 13–34.

[13] T. Banica, J. Bichon and J.-M. Schlenker, Representations of quantum permutation algebras, *J. Funct. Anal.* **257** (2009), 2864–2910.

[14] T. Banica, B. Collins and J.-M. Schlenker, On orthogonal matrices maximizing the 1-norm, *Indiana Univ. Math. J.* **59** (2010), 839–856.

[15] T. Banica and I. Nechita, Almost Hadamard matrices: the case of arbitrary exponents, *Discrete Appl. Math.* **161** (2013), 2367–2379.

[16] T. Banica and I. Nechita, Flat matrix models for quantum permutation groups, *Adv. Appl. Math.* **83** (2017), 24–46.

[17] T. Banica and I. Nechita, Almost Hadamard matrices with complex entries, *Adv. Oper. Theory* **3** (2018), 149–189.

[18] T. Banica, I. Nechita and J.-M. Schlenker, Analytic aspects of the circulant Hadamard conjecture, *Ann. Math. Blaise Pascal* **21** (2014), 25–59.

[19] T. Banica, I. Nechita and J.-M. Schlenker, Submatrices of Hadamard matrices: complementation results, *Electron. J. Linear Algebra* **27** (2014), 197–212.

[20] T. Banica, I. Nechita and K. Życzkowski, Almost Hadamard matrices: general theory and examples, *Open Syst. Inf. Dyn.* **19** (2012), 1–26.

[21] T. Banica and R. Nicoara, Quantum groups and Hadamard matrices, *Panamer. Math. J.* **17** (2007), 1–24.

[22] T. Banica, D. Özteke and L. Pittau, Isolated partial Hadamard matrices, and related topics, *Open Syst. Inf. Dyn.* **25** (2018), 1–27.

[23] T. Banica and A. Skalski, The quantum algebra of partial Hadamard matrices, *Linear Algebra Appl.* **469** (2015), 364–380.

[24] 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.

[25] K. Beauchamp and R. Nicoara, Orthogonal maximal abelian $*$-subalgebras of the 6×6 matrices, *Linear Algebra Appl.* **428** (2008), 1833–1853.

[26] 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.

[27] H. Bercovici and V. Pata, Stable laws and domains of attraction in free probability theory, *Ann. of Math.* **149** (1999), 1023–1060.

[28] J. Bichon, Quotients and Hopf images of a smash coproduct, *Tsukuba J. Math.* **39** (2015), 285–310.

[29] P. Biran, M. Entov and L. Polterovich, Calabi quasimorphisms for the symplectic ball, *Commun. Contemp. Math.* **6** (2004), 793–802.

[30] 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.

[31] 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.

[32] G. Björck and U. Haagerup, All cyclic p-roots of index 3 found by symmetry-preserving calculations, preprint 2008.

[33] R. Burstein, Group-type subfactors and Hadamard matrices, *Trans. Amer. Math. Soc.* **367** (2015), 6783–6807.

[34] A.T. Butson, Generalized Hadamard matrices, *Proc. Amer. Math. Soc.* **13** (1962), 894–898.

[35] C.-H. Cho, Holomorphic discs, spin structures, and Floer cohomology of the Clifford torus, *Int. Math. Res. Not.* **35** (2004), 1803–1843.

[36] 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.

[37] A. Connes, Une classification des facteurs de type III, *Ann. Sci. Ec. Norm. Sup.* **6** (1973), 133–252.

[38] A. Connes, A unitary invariant in Riemannian geometry, *Int. J. Geom. Methods Mod. Phys.* **5** (2008), 1215–1242.

[39] R. Craigen and H. Kharaghani, On the nonexistence of Hermitian circulant complex Hadamard matrices, *Australas. J. Combin.* **7** (1993), 225–227.

[40] W. de Launey, On the non-existence of generalized weighing matrices, *Ars Combin.* **17** (1984), 117–132.

[41] 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.

[42] W. de Launey, D.L. Flannery and K.J. Horadam, Cocyclic Hadamard matrices and difference sets, *Discrete Appl. Math.* **102** (2000), 47–61.

[43] W. de Launey and D.M. Gordon, A comment on the Hadamard conjecture, *J. Combin. Theory Ser. A* **95** (2001), 180–184.

[44] W. de Launey and D.A. Levin, A Fourier-analytic approach to counting partial Hadamard matrices, *Cryptogr. Commun.* **2** (2010), 307–334.

[45] P. Di Francesco, Meander determinants, *Comm. Math. Phys.* **191** (1998), 543–583.

[46] P. Diaconis and M. Shahshahani, On the eigenvalues of random matrices, *J. Applied Probab.* **31** (1994), 49–62.

[47] P. Diţă, Some results on the parametrization of complex Hadamard matrices, *J. Phys. A* **37** (2004), 5355–5374.

[48] T. Durt, B.-G. Englert, I. Bengtsson and K. Życzkowski, On mutually unbiased bases, *Int. J. Quantum Inf.* **8** (2010), 535–640.

[49] J.-C. Faugère, Finding all the solutions of Cyclic 9 using Gröbner basis techniques, *Lecture Notes Ser. Comput.* **9** (2001), 1–12.

[50] P.C. Fishburn and N.J.A. Sloane, The solution to Berlekamp's switching game, *Discrete Math.* **74** (1989), 263–290.

[51] 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.

[52] U. Haagerup, Cyclic p-roots of prime lengths p and related complex Hadamard matrices, preprint 2008.
[53] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. Sci. Math.* **2** (1893), 240–246.
[54] M. Hall, Integral matrices A for which $AA^T = mI$, in "Number Theory and Algebra", Academic Press (1977), 119–134.
[55] G. Hiranandani and J.-M. Schlenker, Small circulant complex Hadamard matrices of Butson type, *European J. Combin.* **51** (2016), 306–314.
[56] K.J. Horadam, Hadamard matrices and their applications, Princeton Univ. Press (2007).
[57] M. Idel and M.M. Wolf, Sinkhorn normal form for unitary matrices, *Linear Algebra Appl.* **471** (2015), 76–84.
[58] N. Ito, Hadamard Graphs I, *Graphs Combin.* **1** (1985), 57–64.
[59] V.F.R. Jones, Index for subfactors, *Invent. Math.* **72** (1983), 1–25.
[60] V.F.R. Jones, On knot invariants related to some statistical mechanical models, *Pacific J. Math.* **137** (1989), 311–334.
[61] V.F.R. Jones, Planar algebras I, preprint 1999.
[62] A. Karabegov, The reconstruction of a unitary matrix from the moduli of its elements and symbols on a finite phase space, preprint 1989.
[63] H. Kharaghani and J. Seberry, The excess of complex Hadamard matrices, *Graphs Combin.* **9** (1993), 47–56.
[64] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, *J. Combin. Des.* **13** (2005), 435–440.
[65] 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.
[66] T.Y. Lam and K.H. Leung, On vanishing sums of roots of unity, *J. Algebra* **224** (2000), 91–109.
[67] V.A. Marchenko and L.A. Pastur, Distribution of eigenvalues in certain sets of random matrices, *Mat. Sb.* **72** (1967), 507–536.
[68] M. Matolcsi, J. Réffy and F. Szöllősi, Constructions of complex Hadamard matrices via tiling abelian groups, *Open Syst. Inf. Dyn.* **14** (2007), 247–263.
[69] D. McNulty and S. Weigert, Isolated Hadamard matrices from mutually unbiased product bases, *J. Math. Phys.* **53** (2012), 1–21.
[70] M.T. Mohan, On some p-almost Hadamard matrices, *Oper. Matrices* **13** (2019), 253–281.
[71] F.J. Murray and J. von Neumann, On rings of operators. IV, *Ann. of Math.* **44** (1943), 716–808.
[72] R. Nicoara, A finiteness result for commuting squares of matrix algebras, *J. Operator Theory* **55** (2006), 295–310.
[73] R. Nicoara and J. White, Analytic deformations of group commuting squares and complex Hadamard matrices, *J. Funct. Anal.* **272** (2017), 3486–3505.
[74] A. Ocneanu, Quantum symmetry, differential geometry of finite graphs, and classification of subfactors, Univ. of Tokyo Seminary Notes (1990).
[75] R. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933), 311–320.
[76] K.-H. Park and H.-Y. Song, Quasi-Hadamard matrices, *Proc. ISIT 2010*, Austin, TX (2010).
[77] M. Petrescu, Existence of continuous families of complex Hadamard matrices of certain prime dimensions and related results, Ph.D. Thesis, UCLA (1997).
[78] G. Pólya, Über eine Aufgabe der Wahrscheinlichkeitsrechnung betreffend die Irrfahrt im Strassennetz, *Math. Ann.* **84** (1921), 149–160.
[79] S. Popa, Orthogonal pairs of $*$-subalgebras in finite von Neumann algebras, *J. Operator Theory* **9** (1983), 253–268.

[80] S. Popa, Classification of amenable subfactors of type II, *Acta Math.* **172** (1994), 163–255.
[81] L.B. Richmond and J. Shallit, Counting abelian squares, *Electron. J. Combin.* **16** (2009), 1–9.
[82] R. Roth and K. Viswanathan, On the hardness of decoding the Gale-Berlekamp code, *IEEE Trans. Inform. Theory* **54** (2008), 1050–1060.
[83] H.J. Ryser, Combinatorial mathematics, Wiley (1963).
[84] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, Wiley (1992).
[85] 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.
[86] F. Szöllősi, Parametrizing complex Hadamard matrices, *European J. Combin.* **29** (2008), 1219–1234.
[87] F. Szöllősi, Exotic complex Hadamard matrices and their equivalence, *Cryptogr. Commun.* **2** (2010), 187–198.
[88] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, *Open Syst. Inf. Dyn.* **13** (2006), 133–177.
[89] W. Tadej and K. Życzkowski, Defect of a unitary matrix, *Linear Algebra Appl.* **429** (2008), 447–481.
[90] T. Tao, Fuglede's conjecture is false in 5 and higher dimensions, *Math. Res. Lett.* **11** (2004), 251–258.
[91] T. Tao and V. Vu, On random ± 1 matrices: singularity and determinant, *Random Structures Algorithms* **28** (2006), 1–23.
[92] 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.
[93] R.J. Turyn, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.
[94] E. Verheiden, Integral and rational completions of combinatorial matrices, *J. Combin. Theory Ser. A* **25** (1978) 267–276.
[95] D.V. Voiculescu, K.J. Dykema and A. Nica, Free random variables, AMS (1992).
[96] S. Wang, Quantum symmetry groups of finite spaces, *Comm. Math. Phys.* **195** (1998), 195–211.
[97] J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65–81.
[98] A. Winterhof, On the non-existence of generalized Hadamard matrices, *J. Statist. Plann. Inference* **84** (2000), 337–342.
[99] S.L. Woronowicz, Compact matrix pseudogroups, *Comm. Math. Phys.* **111** (1987), 613–665.
[100] 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`