Introduction to Hadamard matrices

Teo Banica

Hadamard matrices, Complex matrices, Deformed matrices, Bistochastic matrices, Almost Hadamard matrices, Hadamard models

07/20

Foreword

This is an introduction to the Hadamard matrices, focusing on the complex case, and geometric and analytic aspects.

We discuss the Hadamard conjecture, and then the complex case, basic theory, and more specialized topics as well.

These lecture notes consist of slides written in the Summer 2020. Presentations available at my Youtube channel.

Contents 1/2

Contents 2/2

The Hadamard conjecture

Teo Banica

"Introduction to Hadamard matrices", 1/6

07/20

Hadamard matrices

Sylvester. Arrays having the property that when comparing 2 rows, the number of matchings equals the number of mismatchings:

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

Definition. An Hadamard matrix is a square binary matrix $H \in M_N(\pm 1)$ whose rows are pairwise orthogonal.

Remark. We must have $H \in M_N(\pm 1) \cap \sqrt{N} O_N$, and so the columns must be pairwise orthogonal too.

Walsh matrices

The simplest example of an Hadamard matrix is:

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

Tensor product operation, using double indices:

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

We can tensor W_2 with itself. With lexicographic order:

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

$\Longrightarrow$ Walsh matrices $W_N = W_2^{\otimes n}$, of size $N = 2^n$. Radio, coding.

General theory

Theorem. The Hadamard matrices are stable under:

(1) Permuting rows, or permuting columns.

(2) Switching signs on rows, or on columns.

(3) Taking the transpose.

(4) Making tensor products.

Proof. All this is clear from $H \in M_N(\pm 1) \cap \sqrt{N} O_N$, because all operations preserve both $M_N(\pm 1)$ and $\sqrt{N} O_N$.

Convention. Two Hadamard matrices are called equivalent, $H \sim K$, when we can pass from one to the other via (1,2).

Hadamard bound

Theorem. 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. The determinant of a system of N vectors in $\mathbb{R}^N$ is:

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

In our case, ± 1 entries, we have the following inequality,

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

with equality when our vectors are pairwise orthogonal.

Norm estimates

Theorem. 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 the following Cauchy-Schwarz estimate:

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

The equality case holds when $|U_{ij}| = \sqrt{N}$ for any i, j, and so when the rescaled matrix $H = U/\sqrt{N}$ satisfies $H \in M_N(\pm 1)$.

Size restriction

Theorem. The size of an Hadamard matrix is $N \in \{2\} \cup 4\mathbb{N}$.

Proof. Permute rows/columns, multiply them by -1:

$$H = \begin{pmatrix} 1\ldots\ldots1 & 1\ldots\ldots1 & 1\ldots\ldots1 & 1\ldots\ldots1 \\ 1\ldots\ldots1 & 1\ldots\ldots1 & -1\ldots-1 & -1\ldots-1 \\ 1\ldots\ldots1 & -1\ldots-1 & 1\ldots\ldots1 & -1\ldots-1 \\ \underbrace{\ldots\ldots\ldots}_{x} & \underbrace{\ldots\ldots\ldots}_{y} & \underbrace{\ldots\ldots\ldots}_{z} & \underbrace{\ldots\ldots\ldots}_{t} \end{pmatrix}$$

The orthogonality conditions between the first 3 rows read:

$$x + y = z + t \quad , \quad x + z = y + t \quad , \quad x + t = y + z$$

Solution $x = y = z = t \implies 4|N$.

Case $N \notin 4\mathbb{N}$

What to do? There are two possible choices here:

Definition 1. A quasi-Hadamard matrix is a matrix

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

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

Definition 2. An almost Hadamard matrix is a matrix

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

which maximizes the quantity $||H||_1$.

Hadamard conjecture

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

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

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

(1) OK for $N = 4, 8, 16, 32, 64, \ldots$ (Walsh)

(2) Many other constructions (human, computer)

(3) $\#\{Hadamard\}$ grows exponentially with N. We just need one!

Verification as of 2020 goes up to the number of the beast:

$$\mathfrak{N} = 666$$

(That is, $N \leq 664$ known, $N = 668$ unknown. No joke here!)

Paley matrices

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

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

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

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

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

Skew-symmetric ($H + H^t = 2$), respectively symmetric ($H = H^t$).

Proof 1/3

We denote by 1 all identity matrices, of any size, and by $\mathbb{I}$ all rectangular all-one matrices, of any size as well. We have:

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

In addition, we have the following formulae, 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:

Proof 2/3

(1) With our conventions, the matrix in the statement is:

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

The Hadamard matrix condition follows from:

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

The fact that our matrix is skew-symmetric is clear as well.

Proof 3/3

If we denote by G, F the matrices in the statement, which replace respectively the $0, 1$ entries, our matrix is given by:

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

The Hadamard matrix condition follows from:

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

The fact that our matrix is symmetric is clear as well.

Applications

<u>Theorem</u>. 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.

At $N = 92$ these constructions (Walsh, Paley, $\otimes$) don't work.

Williamson matrices

Theorem. 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 is Hadamard:

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

Moreover, such a matrix exists at $K = 23$, and so at $N = 92$.

Proof

With $1, i, j, k \in M_4(0,1)$ being the quaternion units, we have:

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

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

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

Thus, if we further assume that A, B, C, D commute, and satisfy $A^2 + B^2 + C^2 + D^2 = 4K$, we obtain an Hadamard matrix.

Circulant A, B, C, D were found at $K = 23$ by a computer search.

Cocyclic matrices

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

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

When rows are orthogonal, we say that H is cocyclic Hadamard.

Example. The Walsh matrix $H = W_{2^n}$ is cocyclic, coming from the group $G = \mathbb{Z}_2^n$, with cocycle $H_{gh} = (-1)^{<g,h>}$.

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

Circulant matrices

Conjecture (CHC). The only circulant Hadamard matrices are

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

and its conjugates. In other words, no circulants at $N > 4$.

If we denote by $S \subset \{1, \ldots, N\}$ the set of positions of the -1 entries in the first row, we are led to:

Conjecture (Ryser). At $N > 4$, there is no set $S \subset \{1, \ldots, N\}$,

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

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

De Launey-Levin

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

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

having its rows pairwise orthogonal.

Theorem. The probability for $H \in M_{M\times N}(\pm 1)$ 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 (idea)

The probability for $H \in M_{M\times N}(\pm 1)$ to be PHM is the probability for a length N random walk with increments drawn from

$$E = \left\{ (e_i \bar{e}_j)_{i<j} \middle| e \in \mathbb{Z}_2^M \right\}$$

regarded as subset $\mathbb{Z}_2^{\binom{M}{2}}$, to return at the origin. This gives:

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

By Fourier inversion 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 computations, this leads to the result.

Complex Hadamard matrices

Teo Banica

"Introduction to Hadamard matrices", 2/6

07/20

Hadamard matrices

Definition. A complex Hadamard matrix is a square matrix

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

over the unit circle $\mathbb{T}$, whose rows are pairwise orthogonal.

Here the scalar product is the usual one on $\mathbb{C}^N$:

$$< x, y >= \sum_i x_i \bar{y}_i$$

Examples. The real Hadamard matrices, $H \in M_N(\pm 1)$. There are many other interesting examples, to be discussed here.

Basic properties

<u>Theorem</u>. The set formed by the $N \times N$ complex Hadamard matrices is the real algebraic manifold

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

where U_N is the unitary group, and with the intersection being taken inside $M_N(\mathbb{C})$.

<u>Theorem</u>. The Hadamard matrices are stable under:

(1) Permuting rows and columns, or multiplying rows and columns by numbers in $\mathbb{T}$ ("equivalence").

(2) Conjugating/transposing/taking adjoints $(H, \bar{H}, H^t, H^*)$ and also making tensor products, $(H \otimes K)_{ia,jb} = H_{ij} K_{ab}$.

Fourier matrices 1/2

<u>Theorem</u>. 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

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

is a complex Hadamard matrix, in dephased form.

<u>Proof</u>. The scalar products between distinct rows, rescaled by $1/N$, are barycenters of regular polygons, and so they vanish.

Fourier matrices 2/2

Theorem. Given G finite abelian, with dual $\widehat{G} = \{\chi : G \to \mathbb{T}\}$, consider the Fourier coupling $\mathcal{F}_G : G \times \widehat{G} \to \mathbb{T}$:

$$(i, \chi) \to \chi(i)$$

(1) Via the standard isomorphism $G \simeq \widehat{G}$, this Fourier coupling is a square matrix, $F_G \in M_G(\mathbb{T})$, which is complex Hadamard.

(2) For a 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 $F_G = F_{N_1} \otimes \ldots \otimes F_{N_k}$.

Proof. All this is elementary group theory.

Examples. The Walsh matrices W_{2^n} come from the groups $\mathbb{Z}_2^n$.

Diță deformations

Theorem. 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 $Q\in M_{M\times N}(\mathbb T)$:

(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 Diță deformations of $H\otimes K$.

Proof. Follows by computing the scalar products between rows.

Case N=2,3,4

Theorem. The complex Hadamard matrices at $N=2,3,4$ are, up to the equivalence relation, F_2, F_3 and 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 are right Diță deformations of $W_4=F_2\otimes F_2$.

Proof. Follows from basic geometry in the complex plane.

Case N=5

Theorem. Given an Hadamard matrix $H \in M_5(\mathbb{T})$, dephased,

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & a & x & * & * \\ 1 & y & b & * & * \\ 1 & * & * & * & * \\ 1 & * & * & * & * \end{pmatrix}$$

the numbers a, b, x, y must satisfy the following equation:

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

Proof. Very tricky. The orthogonality of the first 3 rows gives

$$(1+a+x)(1+\bar{b}+\bar{y})(1+\bar{a}y+b\bar{x}) \in \mathbb{R}$$

and then a number of further manipulations give the result.

Haagerup

Theorem. The only complex 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.

Proof. Follows from $(x - y)(x - ab)(y - ab) = 0$, used all across the matrix, which eventually leads to 5th roots of unity.

Case N=6

<u>Theorem</u>. The self-adjoint 6×6 Hadamard matrices are

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

with $x,y,z,t\in\mathbb{T}$ depending on a parameter $q\in\mathbb{T}$ as follows:

$$x=\frac{1+2q+q^2-\sqrt{2}\sqrt{1+2q+2q^3+q^4}}{1+2q-q^2}$$

$$y=q\quad,\quad z=\frac{1+2q-q^2}{q(-1+2q+q^2)}$$

$$t=\frac{1+2q+q^2-\sqrt{2}\sqrt{1+2q+2q^3+q^4}}{-1+2q+q^2}$$

<u>Proof</u>. Due to Beauchamp-Nicoara, technical.

Butson matrices

Definition. An Hadamard matrix is called of Butson type if its entries are roots of unity of finite order. Also:

(1) 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 l-th roots of unity.

(2) The level of a given Butson matrix $H \in M_N(\mathbb{T})$ is the smallest integer $l \in \mathbb{N}$ such that $H \in H_N(l)$.

Examples. The real Hadamard matrices form by definition the Butson class $H_N(2)$. Many other examples, including:

(1) The Fourier matrices, $F_N \in H_N(N)$.

(2) The generalized Fourier matrices, F_G with G abelian.

Obstructions

What are the analogues of the HC in this setting?

Basic obstructions:

(1) Butson (2 rows): $H_N(p^a) \neq \emptyset \implies N \in p\mathbb{N}$.

(2) Sylvester (3 rows): $H_N(2) \neq \emptyset \implies N \in \{2\} \cup 4\mathbb{N}$.

(3) de Launey: $H_N(l) \neq \emptyset \implies \exists\, d \in \mathbb{Z}[e^{2\pi i/l}],\ |d|^2 = N^N$.

(4) Haagerup: $H_5(l) \neq \emptyset \implies 5|l$

Lam-Leung

Theorem. Assuming $l = p_1^{a_1} \dots p_k^{a_k}$, the following must hold, due to the orthogonality of the first 2 rows:

$$H_N(l) \neq \emptyset \implies N \in p_1\mathbb{N} + \dots + p_k\mathbb{N}$$

In the case $k \geq 2$, the latter condition is automatic at $N >> 0$.

Proof. This is the Butson obstruction at $k = 1$, is elementary too at $k = 2$, and is something advanced at $k \geq 3$.

$\implies$ Suggests finding analogues of the HC with $N >> 0$.

$\implies$ Interesting questions in relation with the CHC as well.

Regularity 1/2

Definition. A cycle is a full sum of roots of unity, rotated,

$$C = q\sum_{k=1}^{l} w^k \quad , \quad w = e^{2\pi i/l} \quad , \quad q \in \mathbb{T}$$

and a sum of cycles is a formal sum of such cycles.

Example. With $w = e^{2\pi i/6}$, and with $|q| = 1$:

$$1 + w^2 + w^4 + qw + qw^4 = 0$$

Counterexample. With $w = e^{2\pi i/30}$:

$$w^5 + w^6 + w^{12} + w^{18} + w^{24} + w^{25} = 0$$

(note that this has the same length as a sum of cycles, cf. LL)

Regularity 2/2

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

Theorem. The regular complex Hadamard matrices at $N = 6$ are the Diță deformations of F_6, plus the following two matrices,

$$H_6^q = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & i & i & -i & -i \\ 1 & i & -1 & -i & q & -q \\ 1 & i & -i & -1 & -q & q \\ 1 & -i & \bar{q} & -\bar{q} & i & -1 \\ 1 & -i & -\bar{q} & \bar{q} & -1 & i \end{pmatrix} \ , \ T_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & w & w & w^2 & w^2 \\ 1 & w & 1 & w^2 & w^2 & w \\ 1 & w & w^2 & 1 & w & w^2 \\ 1 & w^2 & w^2 & w & 1 & w \\ 1 & w^2 & w & w^2 & w & 1 \end{pmatrix}$$

due to Haagerup and Tao, with $|q| = 1$, and with $w = e^{2\pi i/3}$.

Proof. Three cases, $2+2+2$, $3+3$ and $2+2+2/3+3$ mixed.

Szöllősi

Theorem. Assuming that $H \in M_N(\pm 1)$ with $N \geq 8$ is dephased symmetric Hadamard, if we set

$$w = \frac{(1 \pm i\sqrt{N-5})^2}{N-4}$$

the following procedure yields an 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. This is a standard design theory computation.

Case N=7

Theorem. The Petrescu matrix, with $w = e^{2\pi i/3}$, is Hadamard,

$$P_7^q = \begin{pmatrix} -q & q & w & 1 & w & 1 & w \\ q & -q & w & 1 & 1 & w & w \\ w & w & -w & 1 & w & w & 1 \\ 1 & 1 & 1 & -1 & w & w & w \\ w & 1 & w & w & -\bar{q}w & \bar{q}w & 1 \\ 1 & w & w & w & \bar{q}w & -\bar{q}w & 1 \\ w & w & 1 & w & 1 & 1 & -1 \end{pmatrix}$$

for any $q \in \mathbb{T}$. At $q = 1$ this appears as above, from W_8.

Conjecture. The only regular matrices at $N = 7$ are F_7, P_7^q.

Circulant matrices

Theorem. Assume that $H \in M_N(\mathbb{T})$ is circulant, $H_{ij} = \gamma_{j-i}$. Then H is Hadamard precisely when vector $(z_0, z_1, \ldots, z_{N-1})$ given by

$$z_i = \gamma_i / \gamma_{i-1}$$

satisfies the following equations of Björck:

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

In this case, we say that $z = (z_0, \ldots, z_{N-1})$ is a cyclic N-root.

Fourier matrices

Theorem. Given $N \in \mathbb{N}$, with $\nu = e^{\pi i/N}$, $q = \nu^{N-1}, w = \nu^2$,

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

is a cyclic N-root, and the corresponding complex Hadamard matrix F_N' is circulant and symmetric, and equivalent to F_N.

At $N = 5$ for instance, we have, with $w = e^{2\pi i/5}$:

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

Further work in this direction (deformations) by Backelin.

Haagerup count

Theorem. When N is prime, the number of circulant $N \times N$ Hadamard matrices, counted with certain multiplicities, is:

$$X = \binom{2N-2}{N-1}$$

Proof. (1) When N is prime, Björck's cyclic root formalism can be further manipulated, by using Fourier transforms.

(2) Finite number of solutions, using a theorem of Chebotarev, which states that all the minors of F_N are nonzero.

(3) The precise count can be done as well, by using various techniques from classical algebraic geometry.

Deformed Hadamard matrices

Teo Banica

"Introduction to Hadamard matrices", 3/6

07/20

Hadamard matrices

The complex Hadamard matrix manifold appears by definition as an intersection of smooth real algebraic manifolds:

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

This intersection is far from being smooth. Given a point $H \in X_N$, the problem is that of understanding the singularity at H.

Affine deformations

Notation. We denote by X_p an unspecified neighborhood of a point in a manifold, $p \in X$.

Theorem. For $H \in X_N, A \in M_N(\mathbb{R})$, 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) $\sum_{k \in E_{ij}^r} H_{ik} \bar{H}_{jk} = 0$, $\forall i \neq j, r \in \mathbb{R}$, with $E_{ij}^r = \{k | A_{ik} - A_{jk} = r\}$.

Proof. (1) $\iff$ (2) $\implies$ (4) $\implies$ (3) $\implies$ (2).

General deformations

<u>Notation</u>. We consider functions of type $f : X_p \to Y_q$, which by definition satisfy $f(p) = q$.

<u>Definition</u>. 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) Called "affine" if $f_{ij}(q) = H_{ij} q^{A_{ij}}$, with $A \in M_N(\mathbb{R})$.

(3) Called "trivial" when $f_{ij}(q) = H_{ij} q^{a_i + b_j}$, with $a, b \in \mathbb{R}^N$.

<u>Examples</u>. The Diţă deformations, with $Q_{ij} = q^{A_{ij}}$, are affine.

Tangent cones

Definition. Associated to a point $H \in X_N$ are:

(1) The enveloping tangent space: obtained as intersection of tangent spaces, $\widetilde{T}_H X_N = T_H M_N(\mathbb{T}) \cap T_H \sqrt{N} U_N$.

(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 $T_H^\times X_N$: same as above, using trivial deformations only.

$\implies$ We have $T_H^\times X_N \subset T_H^\circ X_N \subset T_H X_N \subset \widetilde{T}_H X_N$.

Basic geometry

Theorem. The cones $T_H^\times X_N \subset T_H^\circ X_N \subset T_H X_N \subset \widetilde{T}_H X_N$ can be computed as follows:

(1) $\widetilde{T}_H X_N$ is the linear space formed by the matrices $A \in M_N(\mathbb{R})$ satisfying $\sum_k H_{ik}\bar{H}_{jk}(A_{ik} - A_{jk}) = 0$, for any i, j.

(2) $T_H X_N$ consists of matrices of the form $A_{ij} = g_{ij}'(0)$, with $g : M_N(\mathbb{R})_0 \to M_N(\mathbb{R})_0$, $\sum_k H_{ik}\bar{H}_{jk} e^{i(g_{ik}(t) - g_{jk}(t))} = 0$.

(3) $T_H^\circ X_N$ consists of the matrices $A \in M_N(\mathbb{R})$ satisfying $\sum_k H_{ik}\bar{H}_{jk} q^{A_{ik} - A_{jk}} = 0$, for any $i \neq j$ and any $q \in \mathbb{T}$.

(4) $T_H^\times X_N$ consists of the matrices $A \in M_N(\mathbb{R})$ which are of the form $A_{ij} = a_i + b_j$, for certain vectors $a, b \in \mathbb{R}^N$.

Summary, defect

Definition. The defect of an Hadamard matrix $H \in X_N$ is the real dimension $d(H)$ of the associated enveloping tangent space,

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

which can be computed according to the formula

$$\widetilde{T}_H X_N = \left\{ A \in M_N(\mathbb{R}) \Big| \sum_k H_{ik} \bar{H}_{jk} (A_{ik} - A_{jk}) = 0, \forall i, j \right\}$$

and whose elements are those making the matrix

$$H_{ij}^q = H_{ij} q^{A_{ij}}$$

"complex Hadamard at order 1", with respect to $q \in \mathbb{T}$.

Basic properties

Theorem. 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 dephased image of H is isolated.

Proof. (1) The equations at $K_{ij} = a_i b_j H_{ij}$, $|a_i| = |b_j| = 1$ 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, as desired.

(2) This follows from $T_H^\times X_N \subset T_H X_N \subset \widetilde{T}_H X_N$.

(3) If $d(H) = 2N - 1$ then $T_H X_N = T_H^\times X_N$, as needed.

Real matrices 1/2

<u>Theorem</u>. We have a linear space isomorphism

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

with $A \to E$ and $E \to A$ being constructed as follows:

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

<u>Proof</u>. Given $A \in M_N(\mathbb{C})$, if we set $R_{ij} = A_{ij}H_{ij}$ and $E = RH^*$, then $A \to R \to E$ is bijective onto $M_N(\mathbb{C})$, and we have:

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

The equations become $E_{ij} = \bar{E}_{ji}$, and we are left with $A_{ij} \in \mathbb{R}$.

Real matrices 2/2

Theorem. For any real Hadamard matrix $H \in M_N(\pm 1)$ we have

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

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

Proof. We use the previous result. Since H is real the condition

$$(EH)_{ij} \bar{H}_{ij} \in \mathbb{R}$$

simply tells us that E must be real, and this gives the result.

Fourier 1/4

Theorem. For $F = F_G$, 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. By decomposing G, with $w_k = e^{2\pi i/k}$ we have:

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

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

$$(AF)_{i_1 \ldots i_r, i_1 - j_1 \ldots i_r - j_r} - (AF)_{j_1 \ldots j_r, i_1 - j_1 \ldots i_r - j_r} = 0$$

Thus with $P = AF$ our system is simply $P_{i,i-j} = P_{j,i-j}$.

Fourier 2/4

Theorem. 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. The first assertion follows by counting the solutions of $P_{ij} = P_{i+j,j} = \bar{P}_{i,-j}$. Also, we have

$$\begin{aligned} \#(1 \in F_G) &= \# \left\{ (g,\chi) \in G \times \widehat{G} \middle| \chi(g) = 1 \right\} \\ &= \sum_{g \in G} \frac{|G|}{ord(g)} \end{aligned}$$

so the second assertion follows from the first one.

Fourier 3/4

Theorem. 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. This follows by counting, either from

$$d(F_G) = \sum_{g \in G} \frac{|G|}{ord(g)}$$

or from $d(F_G) = \#(1 \in F_G)$.

Fourier 4/4

Theorem. Given a finite abelian group G, the quantity

$$\delta(G) = \sum_{g \in G} \frac{1}{ord(g)}$$

decomposes as follows, over the isotypic components:

$$\delta(G) = \prod_{p} \delta(G_p)$$

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

$$c_k = \# \left\{ g \in G \middle| ord(g) \leq p^k \right\}$$

and these quantities satisfy $c_k(G \times H) = c_k(G) c_k(H)$.

$\implies$ Thus, we can compute $d(F_G)$ for any G.

Exponential writing

Theorem. Assume that $H \in M_N(\mathbb{C})$ is Hadamard, let $A \in M_N(\mathbb{C})$ be antihermitian, and consider the matrix

$$H^{(t)} = e^{tA}H$$

with $t \in \mathbb{R}$. We have then:

(1) $H^{(t)}$ is Hadamard when $|\sum_{rs} H_{rq}\bar{H}_{sq}(e^{tA})_{pr}(e^{-tA})_{sp}| = 1$.

(2) $H^{(t)}$ is Hadamard at order 0 when $|(AH)_{pq}| = 1$.

Proof. Here (1) follows by computing the quantities $|H_{pq}^{(t)}|^2$, and (2) follows from (1) by differentiating at 0.

Nicoara-White

Theorem. Let G be a finite abelian group, and for $g,h\in G$, set:

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

When $(g,h)\in G^2$ range in suitable cosets, the unitary matrices

$$e^{it(B+B^t)}F_G \quad , \quad e^{t(B-B^t)}F_G$$

are both Hadamard, and make the defect of F_G be attained.

Proof. The previous equations simplify, in the case of a Fourier matrix, and we are led into linear algebra and group theory.

Master Hadamard

Definition. The MHM are the Hadamard matrices of type

$$H_{ij} = \lambda_i^{n_j}$$

with $\lambda_i \in \mathbb{T}, n_j \in \mathbb{R}$. $f(z) = \sum_j z^{n_j}$ is called "master function".

Theorem. $F_M \otimes_Q F_N$ is master Hadamard, in the case

$$Q_{ib} = q^{i(Np_b+b)}$$

with $q = e^{2\pi i/MNk}$ and $k \in \mathbb{N}$, and $p_0, \ldots, p_{N-1} \in \mathbb{R}$.

Conjecture. The MHM appear as Diță deformations of F_N.

Defect

Theorem. The defect of a master Hadamard matrix is given by

$$d(H) = \dim_{\mathbb{R}} \left\{ B \in M_N(\mathbb{C}) \Big| \bar{B} = \frac{1}{N} BL, (BR)_{i,ij} = (BR)_{j,ij} \ \forall i,j \right\}$$

where the matrices L, R on the right are given by

$$L_{ij} = f\left(\frac{1}{\lambda_i \lambda_j}\right) \quad , \quad R_{i,jk} = f\left(\frac{\lambda_j}{\lambda_i \lambda_k}\right)$$

with f being the associated master function.

Proof. This is a standard computation, with $B = AH^t$.

Conjecture. The only isolated master Hadamard matrices are the Fourier matrices F_p, with p prime.

McNulty-Weigert

Theorem 1. Assuming that $K \in M_N(\mathbb{C})$ is Hadamard, so is

$$H_{ia,jb} = \frac{1}{\sqrt{Q}} K_{ij} (L_i^* R_j)_{ab}$$

when $\{L_1, \ldots, L_N\} \subset \sqrt{Q} U_Q$ and $\{R_1, \ldots, R_N\} \subset \sqrt{Q} U_Q$ are such that each of the matrices $\frac{1}{\sqrt{Q}} L_i^* R_j \in \sqrt{Q} U_Q$ is Hadamard.

Theorem 2. For $q \geq 3$ prime, $\{F_q, DF_q, \ldots, D^{q-1} F_q\}$, 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 Hadamard, for any $i \neq j$.

Isolation

By combining the above results, we are led to complex Hadamard matrices which are often isolated, such as the Tao matrix:

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

As an interesting consequence, T_6 is not "exceptional". Also, most of the known isolated matrices are of McNulty-Weigert type.

Bistochastic Hadamard matrices

Teo Banica

"Introduction to Hadamard matrices", 4/6

07/20

Bistochastic matrices

A complex Hadamard matrix $H \in M_N(\mathbb{T})$ is called bistochastic when the sums on all rows and all columns are equal.

It is known that any complex Hadamard matrix can be put in bistochastic form, up to the equivalence relation.

As a motivating remark, 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 suggests studying the Hadamard matrices $H \in M_N(\pm 1)$ by putting them in complex bistochastic form, $H' \in M_N(\mathbb{T})$.

Basic examples

Theorem. The class of bistochastic complex Hadamard matrices is stable under permuting rows and columns, and under taking tensor products. As basic examples, we have:

(1) The circulant and symmetric form F_N' of F_N.
(2) The bistochastic and symmetric form F_G' of F_G.
(3) The circulant Backelin matrices, having size MN with $M|N$.

Proof. Assuming that H,K are bistochastic, with sums λ,μ:

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

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

As for the other assertions, we already know all this.

Theory 1/4

Theorem. For $H \in M_N(\mathbb{T})$ Hadamard, the following are equivalent:

(1) H is bistochastic, with sums λ.

(2) H is row-stochastic, with sums λ, and $|\lambda|^2 = N$.

Proof. (1) $\implies$ (2) With $H_1, \ldots, H_N \in \mathbb{T}^N$ being the rows:

$$N = \sum_i < H_1, H_i >= \sum_j H_{1j} \cdot \bar{\lambda} = |\lambda|^2$$

(2) $\implies$ (1) With ξ being the all-one vector, we have:

$$\begin{aligned} H\xi = \lambda\xi \quad &\implies \quad H^*H\xi = \lambda H^*\xi \implies N^2\xi = \lambda H^*\xi \\ &\implies \quad N^2\xi = \bar{\lambda} H^t\xi \implies H^t\xi = \lambda\xi \end{aligned}$$

Thus row-stochastic with $|\lambda|^2 = N$ implies column-stochastic.

Theory 2/4

Theorem. For an Hadamard matrix $H\in M_N(\mathbb{T})$, the excess,

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

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

Proof. In terms of the all-one vector ξ, we have:

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

By Cauchy-Schwarz we obtain, using $H/\sqrt{N}\in U_N$:

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

For equality we must have $H\xi\sim\xi$. But with $H\xi=\lambda\xi$, the above computation gives $|\lambda|^2=N$, so the previous result applies.

Theory 3/4

Notations. The complex projective space appears as follows:

$$P^{N-1}_{\mathbb{C}} = (\mathbb{C}^N - \{0\}) / < x = \lambda y >$$

Inside this projective space, we have the Clifford torus:

$$\mathbb{T}^{N-1} = \left\{ (z_1, \ldots, z_N) \in P^{N-1}_{\mathbb{C}} \Big| |z_1| = \ldots = |z_N| \right\}$$

Theorem. For $U \in U_N$, the following are equivalent:

(1) $U' = LUR$ is bistochastic, with $L, R \in U_N$ diagonal.

(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 $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$.

Theory 4/4

Theorem. Any $U \in U_N$ can be put in bistochastic form,

$$U' = LUR$$

with $L, R \in U_N$ diagonal, via a certain non-explicit method.

Proof. It is known that $\mathbb{T}^{N-1} \subset P_{\mathbb{C}}^{N-1}$ is a Lagrangian submanifold, that $\mathbb{T}^{N-1} \to U\mathbb{T}^{N-1}$ is a Hamiltonian isotopy, and that $\mathbb{T}^{N-1}$ cannot be displaced from itself via a Hamiltonian isotopy (..)

Theorem. Any complex Hadamard matrix $H \in M_N(\mathbb{T})$ can be put in bistochastic form, modulo the equivalence relation.

Proof. Follows from Idel-Wolf, $U = H/\sqrt{N}$ being unitary.

Butson 1/2

Theorem. Assuming that $H_N(l)$ contains a bistochastic matrix,

$$\begin{aligned} a_0+a_1+\ldots+a_{l-1} &= N \\ |a_0+a_1w+\ldots+a_{l-1}w^{l-1}|^2 &= N \end{aligned}$$

with $w=e^{2\pi i/l}$ must have solutions, over the positive integers.

Proof. This comes from the formula $|\lambda|^2=N$, established before. Indeed, if we denote by $a_i\in\mathbb{N}$ the number of w^i entries appearing in the first row of our matrix, the row sum is:

$$\lambda=a_0+a_1w+\ldots+a_{l-1}w^{l-1}$$

Thus, we obtain the system of equations in the statement.

Butson 2/2

Theorem. 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. (1) This follows from the previous result.
(2) This follows by using the following identity:

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

(3) This follows by using $|a + ib|^2 = a^2 + b^2$.

Fourier 1/2

Definition. We say that $H \in M_N(\mathbb{T})$ Hadamard is in "almost bistochastic form" when all row sums belong to $\sqrt{N} \cdot \mathbb{T}$.

Theorem. The matrix $F_N \otimes'_Q F_N$, with $Q \in M_N(\mathbb{T})$, given 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 $\sim F_N \otimes_Q F_N$.

Proof. Direct computation, using roots of unity.

Fourier 2/2

As an illustration, at $N = 2$ we have $w = -1$, and with $Q = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$, and $u = \frac{p}{r}, v = \frac{s}{q}$, 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 $2, -2, 2, 2$.

Questions

We know from Idel-Wolf that any Hadamard matrix $H \in M_N(\mathbb{T})$ can be put in bistochastic form, at least in theory.

The problem is that of doing this explicitly, for instance for:

(1) $F_N \otimes_Q F_M$, with $N \neq M$.

(2) The Paley matrices.

(3) The Williamson matrices.

(4) Other known real Hadamard matrices.

These questions are interesting, because all this might lead to a "complex bistochastic formulation" of the HC, and the CHC.

The glow, 1/4

Definition. 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 real Hadamard equivalence class of H.

In other words, 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 μ is the measure on $\mathbb{Z}$ given by $\mu(\{k\}) = P(\varphi = k)$.

The glow, 2/4

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. All this is related to the Gale-Berlekamp game.

The glow, 3/4

Theorem. Let $H \in M_N(\pm 1)$ be an Hadamard matrix of order $N \geq 4$, and denote by

$$\mu^{even}, \mu^{odd}$$

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. This follows by using the formula

$$\mu = \frac{1}{2^N} \sum_{b \in \mathbb{Z}_2^N} \beta_1(c_1) * \ldots * \beta_N(c_N)$$

with $\beta_r(c) = \left(\frac{\delta_r + \delta_{-r}}{2}\right)^{*c}$, $c_r = \#\{r \in |S_1|, \ldots, |S_N|\}$, $S = Hb$.

The glow, 4/4

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

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

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

Proof. The moments of $E = \sum_{ij} a_i b_j H_{ij}$ are given by

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

and after some computations, this gives the result.

Complex glow, 1/4

Definition. The glow of a complex matrix $H \in M_N(\mathbb{C})$ is the probability measure $\mu \in \mathcal{P}(\mathbb{C})$ given by:

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

In other words, the glow is the law of the excess

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

over the complex Hadamard equivalence class of H.

Complex glow, 2/4

Theorem. The glow 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. (1) Follows by using $H \to zH$ with $|z| = 1$.

(2) Follows from (1), the convolution with ε bringing the invariance.

(3) This folllows from Cauchy-Schwarz, cf. excess theory.

(4) This is something highly non-trivial, coming from Idel-Wolf.

Complex glow, 3/4

Theorem. 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. This uses the moment method, and combinatorics.

Complex glow, 4/4

Theorem. 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. Once again moment method, and combinatorics.

Remark. The next term depends on $G = \mathbb{Z}_{N_1}\times\ldots\times\mathbb{Z}_{N_k}$,
$K_4 = \frac{8}{3}\binom{p}{3} + \frac{3}{4}\left(121 + \frac{2^e}{N}\right)\binom{p}{4} + 416\binom{p}{5} + \frac{2915}{2}\binom{p}{6} + 40\binom{p}{7} + 105\binom{p}{8}$
$e \in \mathbb{N}$ being the number of even numbers among $N_1, \ldots, N_k$.

Almost Hadamard matrices

Teo Banica

"Introduction to Hadamard matrices", 5/6

07/20

Hadamard matrices

The set formed by the $N \times N$ real Hadamard matrices is:

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

(1) How to locate analytically these matrices?

(2) What to do when $N \notin 4\mathbb{N}$?

(3) What about the complex case?

Hadamard bound

Theorem. 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. The determinant of a system of N vectors in $\mathbb{R}^N$ is:

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

In our case, ± 1 entries, we have the following inequality,

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

with equality when our vectors are pairwise orthogonal.

$\implies$ "quasi-Hadamard matrices", at $N \notin 4\mathbb{N}$

Norm estimates

Theorem. 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 the following Cauchy-Schwarz estimate:

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

The equality case holds when $|U_{ij}| = \sqrt{N}$ for any i, j, and so when the rescaled matrix $H = U/\sqrt{N}$ satisfies $H \in M_N(\pm 1)$.

$\implies$ "almost Hadamard matrices", at $N \notin 4\mathbb{N}$

Jensen, Hölder

Theorem. Given $\psi : [0,\infty) \to \mathbb{R}$, define $F : U_N \to \mathbb{R}$ by:

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

(1) ψ concave $\implies$ F maximized when $H = \sqrt{N}U$ Hadamard.

(2) ψ convex $\implies$ F minimized when $H = \sqrt{N}U$ Hadamard.

Theorem. Let $U \in U_N$, and set $H = \sqrt{N}U$.

(1) At $p < 2$, $||U||_p \leq N^{2/p-1/2}$, equality when H Hadamard.

(2) At $p > 2$, $||U||_p \geq N^{2/p-1/2}$, equality when H Hadamard.

Almost Hadamard

Definition. 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 $p \neq 2$.

Also: real versions of these notions, with U_N replaced by O_N.

Rotation trick

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

$$U_{ij} \neq 0$$

for any i, j. We write $U \in O_N^*$.

Proof. This uses a rotation trick (BCS), as follows:

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

By differentiating $||.||_1$ with respect to t, we obtain the result.

Complex case

Theorem. If $U \in U_N$ locally maximizes the 1-norm, then

$$U_{ij} \neq 0$$

for any i, j. We write $U \in U_N^*$.

Proof. As in the real case, this follows from a rotation trick. The computations however are more complicated (BN).

Problem. Find such results at any $p \in [1, \infty] - \{2\}$.

Critical points 1/4

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

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

when WU^* is self-adjoint, where $W_{ij} = \mathrm{sgn}(U_{ij})\varphi'(|U_{ij}|)$.

Proof. Lagrange multipliers. We have the following formula:

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

We are led to $W = 2M^tU$, $\bar{W} = 2M\bar{U}$, and so to $WU^* = UW^*$.

Critical points 2/4

Definition. 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 phases, and we call U:

(1) Semi-balanced, if $U_r U^*$, $U^* U_r$ are all self-adjoint.

(2) Balanced, if $U_r U_s^*$, $U_r^* U_s$ are all self-adjoint.

Theorem. 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 φ.

(2) U is a critical point of all p-norms, with $p \in [1, \infty)$.

(3) U is semi-balanced, in the above sense.

Critical points 3/4

Theorem. The class of balanced matrices is as follows:

(1) It contains $U = H/\sqrt{N}$, with $H \in M_N(\mathbb{C})$ Hadamard.

(2) It is stable under transposition.

(3) It is stable under complex conjugation.

(4) It is stable under and taking adjoints.

(5) It is stable under taking tensor products.

(6) It is stable under the Hadamard equivalence relation.

(7) It contains $V_N = \frac{1}{N}(2\mathbb{I}_N - N1_N)$, where $\mathbb{I}_N$ is the all-1 matrix.

Critical points 4/4

We call (a,b,c) pattern any $M \in M_N(0,1)$, with $N = a + 2b + c$, such that any two rows look as follows, up to a permutation:

$$\begin{matrix} 0\ldots0 & 0\ldots0 & 1\ldots1 & 1\ldots1 \\ \underbrace{0\ldots0}_{a} & \underbrace{1\ldots1}_{b} & \underbrace{0\ldots0}_{b} & \underbrace{1\ldots1}_{c} \end{matrix}$$

Examples from BIBD. These produce two-entry unitary matrices, by replacing the $0,1$ entries with suitable numbers x,y.

<u>Theorem</u>. 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.

Hessians 1/2

Theorem. 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 when $X \geq 0$, and

$$\Phi(U,B) = Tr(XB^2) - \sum_{ij} \frac{Re\left[(UB)_{ij}\overline{S}_{ij}\right]^2}{|U_{ij}|}$$

is positive, for any hermitian matrix $B \in M_N(\mathbb{C})$.

(2) In the real case, $U \in O_N$, this matrix locally maximizes the 1-norm on O_N when the matrix $X = S^*U$ is self-adjoint, and the sum of its two smallest eigenvalues is positive.

Hessians 2/2

The difference between the real and complex cases comes from:

Theorem. For $X \in M_N(\mathbb{C})$ self-adjoint, 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) $X \geq 0$.

Theorem. For $X \in M_N(\mathbb{R})$ symmetric, 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.

Real AHM, 1/4

Theorem. 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 the real sense.

Proof. Since any row of U consists of $a+b$ copies of x and $b+c$ copies of y, we have:

$$(SU^t)_{ij} = \begin{cases} (a+b)|x| + (b+c)|y| & (i = j) \\ (a-b)|x| + (c-b)|y| & (i \neq j) \end{cases}$$

After come computations, this gives the result.

Real AHM, 2/4

As a basic example for the above construction, we have the following matrix:

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

This is absolute almost Hadamard, in the real sense (Mohan).

Other interesting examples, coming from block designs (BNZ).

Real AHM, 3/4

Theorem. Consider a circulant matrix $H \in M_N(\mathbb{R}^*)$, $H_{ij} = \gamma_{j-i}$. If the following conditions are satisfied, H is almost Hadamard:

(1) The vector $q = F^*\gamma$ satisfies $q \in \mathbb{T}^N$.

(2) With $\varepsilon = \mathrm{sgn}(\gamma)$, $\rho_i = \sum_r \varepsilon_r \gamma_{i+r}$, $\nu = F^*\rho$, we have $\nu > 0$.

Proof. We have the following computation:

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

Thus $S^t U$ is circulant, with $\rho/\sqrt{N}$ as first row.

Real AHM, 4/4

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 produces the following circulant $N \times N$ real AHM:

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

$\implies$ many other interesting examples (BNZ)

$\implies$ applications to submatrices of Hadamard matrices (BNS)

Complex AHM

The complex AHM are conjectured to be all Hadamard (!)

Conjecture. Any local maximizer of the 1-norm on U_N must be a global maximizer, i.e. must be a rescaled Hadamard matrix.

$\Longrightarrow$ Verified for real AHM and their complex versions (BN).

$\Longrightarrow$ Potential powerful analytic characterization of the CHM.

Random derivatives

Let $OSC_N \subset USC_N$ be the orthogonal symmetric circulant matrices, and unitary self-adjoint circulant matrices, and USB_N be the unitary bistochastic self-adjoint matrices. We have:

Conjecture. Given $U \in USB_N$ satisfying $S^*U \geq 0$, there exists a simple function $B \to B^U$ (passage to another coset?), such that

$$\int_{OSC_N} \Phi(U, B^U) dB \leq 0$$

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

Hadamard matrix models

Teo Banica

"Introduction to Hadamard matrices", 6/6

07/20

Fourier 1/4

Theorem. 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

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

is a complex Hadamard matrix, in dephased form.

Proof. The scalar products between distinct rows, rescaled by $1/N$, are barycenters of regular polygons, and so they vanish.

Fourier 2/4

Theorem. Given G finite abelian, with dual $\widehat{G} = \{\chi : G \to \mathbb{T}\}$, consider the Fourier coupling $\mathcal{F}_G : G \times \widehat{G} \to \mathbb{T}$:

$$(i, \chi) \to \chi(i)$$

(1) Via the standard isomorphism $G \simeq \widehat{G}$, this Fourier coupling is a square matrix, $F_G \in M_G(\mathbb{T})$, which is complex Hadamard.

(2) For a 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 $F_G = F_{N_1} \otimes \ldots \otimes F_{N_k}$.

Proof. All this is elementary group theory.

Fourier 3/4

Results about the Fourier matrices:

(1) They exist at any $N \in \mathbb{N}$! (no complex HC)

(2) Circulants: Björck F_N' circulant (no CHC), Backelin..

(3) Geometry/Defect: K,N,TZ,BB,T,B + Nicoara-White..

(4) Isolation, versions: McNulty-Weigert, Master Hadamard..

(5) Analysis: $F_N \otimes' F_N$ bistochastic, glow up to order 4

Fourier 4/4

Question. Given a complex Hadamard matrix $H \in M_N(\mathbb{T})$, is it the "Fourier matrix" of something?

Answer. YES, in a certain sense, the relevant group-type object being a quantum permutation group $G \subset S_N^+$.

Bonus. The construction $H \to G$ makes the link with von Neumann algebras, subfactors, planar algebras, spin models.

Quantum groups 1/4

<u>C^*-algebra</u>: complex algebra A, with norm $||.||$ making it a Banach algebra, and involution $*$ satisfying $||aa^*|| = ||a||^2$.

<u>Basic examples</u>: $A \subset B(H)$ closed $*$-algebra ("generic"), also $A = C(X)$ with X compact space, $||.|| = $ sup norm.

<u>Gelfand theorem</u>: the commutative C^*-algebras are those of the form $C(X)$, with X compact space [proof: $X = Spec(A)$].

$\Longrightarrow$ in general, write $A = C(X)$, with X = "<u>NC space</u>".

Quantum groups 2/4

Let G be a compact Lie group. Then $G \subset U_N$. Multiplication:

$$(UV)_{ij} = \sum_k U_{ik} V_{kj}$$

By Stone-Weierstrass we have $C(G) = < u_{ij} >$, where:

$$u_{ij}(U) = U_{ij}$$

The multiplication $G \times G \to G$ transposes as:

$$u_{ij} \to \sum_k u_{ik} \otimes u_{kj}$$

Thus G is well described by $C(G)$, together with $u = (u_{ij})$.

Quantum groups 3/4

Definition. Let A be a C^*-algebra, with $u \in M_N(A)$ biunitary (u, u^t unitaries), whose entries generate A, such that:

– $\Delta(u_{ij}) = \sum_k u_{ik} \otimes u_{kj}$ defines a morphism $\Delta : A \to A \otimes A$.

– $\varepsilon(u_{ij}) = \delta_{ij}$ defines a morphism $\varepsilon : A \to \mathbb{C}$.

– $S(u_{ij}) = u_{ji}^*$ defines a morphism $S : A \to A^{opp}$.

We write $A = C(G)$, and call G a compact quantum group.

[axioms due to Woronowicz, 1987, slightly modified]

Quantum groups 4/4

Theorem 1. Haar integration functional:

$$\left(\int_G \otimes id\right)\Delta = \left(id \otimes \int_G\right)\Delta = \int_G (.)1$$

Theorem 2. Peter-Weyl theory, and in particular:

$$C^\infty(G) \simeq \bigoplus_{r \in Irr(G)} B(H_r)$$

Theorem 3. Tannaka-Krein duality, between G and:

$$C_{kl} = Hom(u^{\otimes k}, u^{\otimes l})$$

[refs: Woronowicz's CMP and TKD papers, late 80s]

Quantum permutations

Permutation matrices $S_N \subset O_N$. Coordinates of S_N are:

$$u_{ij} = \chi\left(\sigma \in S_N \middle| \sigma(j) = i\right)$$

Magic (entries are projections, sum 1 on each row/column)

<u>Definition</u>. The quantum permutation group S_N^+ is defined via:

$$C(S_N^+) = C^*\left((u_{ij}) \middle| u = N \times N \text{ magic}\right)$$

[it's compact (!) verification of the axioms is routine: Wang 98]

The construction

Given an Hadamard matrix $H \in M_N(\mathbb{T})$, the rank 1 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.

Definition. We associate to H the quantum permutation group $G \subset S_N^+$ given by the following "Hopf image" factorization,

$$\begin{array}{ccc} C(S_N^+) & \xrightarrow{\pi} & M_N(\mathbb{C}) \\ & \searrow \quad \nearrow & \\ & C(G) & \end{array}$$

where $\pi(u_{ij}) = Proj(H_i/H_j)$ are the above rank 1 projections.

Results 1/4

Theorem. For a Fourier matrix F_G we obtain in this way the finite abelian group G itself, acting on itself.

Proof. Assume first $H = F_N$. 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:

$$\frac{H_i}{H_j} = \rho^{i-j}$$

Thus the rank 1 projections $P_{ij} = Proj(H_i/H_j)$ form a circulant matrix, all whose entries commute, and we obtain $G = \mathbb{Z}_N$.

In the general case, $H = F_G$ with G arbitrary, the proof is similar. Alternatively, we can use $G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$.

Results 2/4

Theorem. For a tensor product of Hadamard matrices $H = H' \otimes H''$ we obtain a product of quantum groups, $G = G' \times G''$.

Proof. We have a diagram as follows:

$$\begin{array}{ccccc}
C(S_{N'}^+) \otimes C(S_{N''}^+) & \longrightarrow & C(G') \otimes C(G'') & \longrightarrow & M_{N'}(\mathbb{C}) \otimes M_{N''}(\mathbb{C}) \\
\uparrow & & & & \downarrow \\
C(S_N^+) & \longrightarrow & C(G) & \longrightarrow & M_N(\mathbb{C})
\end{array}$$

Thus the representation factorizes through $C(G') \otimes C(G'')$.

Results 3/4

The idea is that the inner faithful models $\pi : C(G) \to M_K(C(T))$ "remind" the quantum group. We have indeed:

Theorem. The Tannakian category of G is given by

$$C_{kl} = Hom(U^{\otimes k}, U^{\otimes l})$$

where $U_{ij} = \pi(u_{ij})$, and with the formal Hom-spaces at right.

Theorem. The integration over G is given by

$$\int_G = \lim_{k \to \infty} \frac{1}{k} \sum_{r=1}^{k} \int_G^r$$

where $\int_G^r = (\varphi \circ \pi)^{*r}$, with $\varphi = tr \otimes \int_T$.

Results 4/4

Theorem. Given two finite abelian groups G, H, with $|G| = M$, $|H| = N$, consider the main character χ of the quantum group associated to the Diță deformation $\mathcal{F}_{G\times H}$. 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 holds for any generic fiber.

Proof. Long story here (B, BB, B, B).

Versions 1/2

Definition. 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.

Theorem. If $H \in M_N(A)$ is Hadamard, the following matrices $P_{ij} \in M_N(A)$ form a magic matrix $P = (P_{ij})$, over $M_N(A)$:

$$(P_{ij})_{ab} = \frac{1}{N} H_{ia} H_{ja}^* H_{jb} H_{ib}^*$$

Thus, we have a representation $\pi : C(S_N^+) \to M_N(A)$, that we can factorize $\pi : C(S_N^+) \to C(G) \to M_N(A)$, with $G \subset S_N^+$ minimal.

Versions 2/2

Definition. The quantum partial permutation semigroup $\widetilde{S}_N^+$ is defined via the formula

$$C(S_N^+)=C^*\left((u_{ij})\Big|u=N\times N\text{ submagic}\right)$$

where "submagic" means that the entries are projections, pairwise orthogonal on rows and columns.

Theorem. Assuming that $H\in M_{M\times N}(\mathbb{T})$ is partial Hadamard, with rows $H_1,\ldots,H_M\in\mathbb{T}^N$, the following matrix is submagic:

$$P_{ij}=Proj\left(\frac{H_i}{H_j}\right)$$

Thus H produces a representation $\pi_H:C(\widetilde{S}_M^+)\to M_N(\mathbb{C})$, that we can factorize through $C(G)$, with $G\subset\widetilde{S}_M^+$ minimal.

Von Neumann

Von Neumann algebras: $A \subset B(H)$, involution $*$, weakly closed.

Theorem 1. The commutative von Neumann algebras are those of the form $L^\infty(X)$, with X being a measured space.

Theorem 2. When writing the center as $Z(A) = L^\infty(X)$, the whole algebra decomposes as $A = \int_X A_x dx$.

Theorem 3. The theory of factors, $Z(A) = \mathbb{C}$, reduces to that of the II_1 factors ($\dim A = \infty$, trace $tr : A \to \mathbb{C}$).

[this is heavy: Murrray-von Neumann, Tomita-Takeaski, Connes..]

Popa

A pair of orthogonal MASA is a pair of maximal abelian subalgebras

$$B, C \subset A$$

which are orthogonal: $tr(bc) = tr(b)tr(c)$, for any $b \in B, c \in C$.

<u>Theorem</u>. Up to a unitary, the pairs of orthogonal MASA in the simplest von Neumann factor, namely $M_N(\mathbb{C})$, are

$$A = \Delta \quad , \quad B = H\Delta H^*$$

with $\Delta =$ diagonal matrices, and $H \in M_N(\mathbb{T})$ Hadamard.

<u>Proof.</u> Write the orthogonality condition, then conclude.

Jones

(1) Given $H \in M_N(\mathbb{T})$ Hadamard, the associated pair of MASA fit into a "commuting square" in the sense of subfactor theory:

$$\begin{array}{ccc} \Delta & \longrightarrow & M_N(\mathbb{C}) \\ \uparrow & & \uparrow \\ \mathbb{C} & \longrightarrow & H\Delta H^* \end{array}$$

(2) By "basic construction" we obtain a subfactor $Q \subset R$, whose invariants can be computed using "Ocneanu compactness".

(3) The factor Q appears as fixed point algebra under the action of the corresponding quantum permutation group $G \subset S_N^+$.

$\implies$ spin models?

References 1/4

[1] 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.

[2] J. Backelin, Square multiples n give infinitely many cyclic n-roots, preprint 1989.

[3] T. Banica, The defect of generalized Fourier matrices, *Linear Algebra Appl.* **438** (2013), 3667–3688.

[4] T. Banica, The glow of Fourier matrices: universality and fluctuations, *Oper. Matrices* **9** (2015), 457–474.

[5] T. Banica and J. Bichon, Random walk questions for linear quantum groups, *Int. Math. Res. Not.* **24** (2015), 13406–13436.

[6] T. Banica and I. Nechita, Almost Hadamard matrices with complex entries, *Adv. Oper. Theory* **3** (2018), 149–189.

[7] T. Banica, I. Nechita and J.-M. Schlenker, Submatrices of Hadamard matrices: complementation results, *Electron. J. Linear Algebra* **27** (2014), 197–212.

[8] T. Banica, I. Nechita and K. Życzkowski, Almost Hadamard matrices: general theory and examples, *Open Syst. Inf. Dyn.* **19** (2012), 1–26.

References 2/4

[9] 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.

[10] K. Beauchamp and R. Nicoara, Orthogonal maximal abelian $*$-subalgebras of the 6×6 matrices, *Linear Algebra Appl.* **428** (2008), 1833–1853.

[11] 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.

[12] J. Bichon, Quotients and Hopf images of a smash coproduct, *Tsukuba J. Math.* **39** (2015), 285–310.

[13] G. Björck, Functions of modulus 1 on $\mathbb{Z}_n$ whose Fourier transforms have constant modulus, and cyclic n-roots, *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.* **315** (1990), 131–140.

[14] R. Burstein, Group-type subfactors and Hadamard matrices, *Trans. Amer. Math. Soc.* **367** (2015), 6783–6807.

[15] A.T. Butson, Generalized Hadamard matrices, *Proc. Amer. Math. Soc.* **13** (1962), 894–898.

[16] W. de Launey, D.L. Flannery and K.J. Horadam, Cocyclic Hadamard matrices and difference sets, *Discrete Appl. Math.* **102** (2000), 47–61.

References 3/4

[17] W. de Launey and D.A. Levin, A Fourier-analytic approach to counting partial Hadamard matrices, *Cryptogr. Commun.* **2** (2010), 307–334.

[18] P. Diţă, Some results on the parametrization of complex Hadamard matrices, *J. Phys. A* **37** (2004), 5355–5374.

[19] 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.

[20] U. Haagerup, Cyclic p-roots of prime lengths p and related complex Hadamard matrices, preprint 2008.

[21] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. Sci. Math.* **2** (1893), 240–246.

[22] M. Idel and M.M. Wolf, Sinkhorn normal form for unitary matrices, *Linear Algebra Appl.* **471** (2015), 76–84.

[23] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, *J. Combin. Des.* **13** (2005), 435–440.

[24] T.Y. Lam and K.H. Leung, On vanishing sums of roots of unity, *J. Algebra* **224** (2000), 91–109.

References 4/4

[25] D. McNulty and S. Weigert, Isolated Hadamard matrices from mutually unbiased product bases, *J. Math. Phys.* **53** (2012), 1–21.

[26] R. Nicoara and J. White, Analytic deformations of group commuting squares and complex Hadamard matrices, *J. Funct. Anal.* **272** (2017), 3486–3505.

[27] R. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933), 311–320.

[28] 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.

[29] F. Szöllősi, Exotic complex Hadamard matrices and their equivalence, *Cryptogr. Commun.* **2** (2010), 187–198.

[30] W. Tadej and K. Życzkowski, Defect of a unitary matrix, *Linear Algebra Appl.* **429** (2008), 447–481.

[31] J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65–81.

[32] S.L. Woronowicz, Compact matrix pseudogroups, *Comm. Math. Phys.* **111** (1987), 613–665.