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

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 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 Diţă 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

Theorem. 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:

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

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

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

Proof. 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 $l = p_1^{a_1} \ldots p_k^{a_k}$, 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 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

<u>Theorem</u>. 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.

<u>Conjecture</u>. 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.