Minimal polynomials of complex Hadamard matrices

Padraig Ó Catháin
joint work with
Ronan Egan, Eric Swartz

Worcester Polytechnic Institute

30 September 2019

Hadamard's Determinant Theorem

Theorem (Hadamard, 1893)

If H is a (complex) matrix of order n and every entry h_{ij} of H satisfies

$$|h_{ij}|^2 \leq 1$$

then

$$|\det(H)| \leq \sqrt{n}^n .$$

Hadamard's Determinant Theorem

Theorem (Hadamard, 1893)

If H is a (complex) matrix of order n and every entry h_{ij} of H satisfies

$$|h_{ij}|^2 \leq 1$$

then

$$|\det(H)| \leq \sqrt{n}^n.$$

- H is Hadamard if $h_{ij}h_{ij}^* = 1$ for all $1 \leq i, j \leq n$ and $|\det(H)| = n^{\frac{n}{2}}$.
- Equivalent to $H^*H = nI_n$ or $HH^* = nI_n$.
- Eigenvalues are of modulus $\sqrt{n}$.

Hadamard's Determinant Theorem

Theorem (Hadamard, 1893)

If H is a (complex) matrix of order n and every entry h_{ij} of H satisfies

$$|h_{ij}|^2 \leq 1$$

then

$$|\det(H)| \leq \sqrt{n}^n .$$

- H is Hadamard if $h_{ij}h_{ij}^* = 1$ for all $1 \leq i, j \leq n$ and $|\det(H)| = n^{\frac{n}{2}}$.
- Equivalent to $H^*H = nI_n$ or $HH^* = nI_n$.
- Eigenvalues are of modulus $\sqrt{n}$.
- Hadamard property is preserved under permutation of rows and columns, and multiplication of rows/columns by complex numbers of modulus 1.
- Eigenvalues are not preserved under equivalence.

E.g.

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & a & -1 & -a \\ 1 & -1 & 1 & -1 \\ 1 & -a & -1 & a \end{vmatrix} \quad (a = e^{i\theta})$$

E.g.

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & a & -1 & -a \\ 1 & -1 & 1 & -1 \\ 1 & -a & -1 & a \end{vmatrix} \quad (a = e^{i\theta})$$

- The character table of any abelian group gives a Hadamard matrix. So there exist $n \times n$ (complex) Hadamard matrices for any $n \in \mathbb{N}$.

E.g.

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & a & -1 & -a \\ 1 & -1 & 1 & -1 \\ 1 & -a & -1 & a \end{vmatrix} \quad (a = e^{i\theta})$$

- The character table of any abelian group gives a Hadamard matrix. So there exist $n \times n$ (complex) Hadamard matrices for any $n \in \mathbb{N}$.
- Restricting to real entries $\{1, -1\}$, we must have $n = 1, 2$ or $n \equiv 0$ mod 4. The (real) Hadamard conjecture is that matrices exist at all these orders.
- The smallest open case of the (real) Hadamard conjecture is 668.

Hadamard's Determinant Theorem

Definition

If H is a (complex) matrix of order n, every entry of H satisfies $|h_{ij}|^2 \leq 1$ and $HH^* = nI_n$ then H is Hadamard.

Hadamard's Determinant Theorem

Definition

If H is a (complex) matrix of order n, every entry of H satisfies $|h_{ij}|^2 \leq 1$ and $HH^* = nI_n$ then H is Hadamard.

- H is **real** if entries are in $\{\pm 1\}$
- H is **Butson** if entries are in $\langle \omega_k \rangle$
- H is **QUH** if entries are in $\{\frac{\pm 1 \pm \sqrt{-k}}{\sqrt{k+1}}\}$

Existence

$k \backslash n$	2	3	4	5	6	7	8	9	10	11	12
2	Y	–	Y	–	–	–	Y	–	–	–	Y
3	–	Y	–	–	Y	–	–	Y	–	–	Y
4	Y	–	Y	–	Y	–	Y	–	Y	–	Y
5	–	–	–	Y	–	–	–	–	Y	–	–
6	Y	Y	Y	–	Y	Y	Y	Y	–	–	Y

Existence

$k \backslash n$	2	3	4	5	6	7	8	9	10	11	12
2	Y	–	Y	–	–	–	Y	–	–	–	Y
3	–	Y	–	–	Y	–	–	Y	–	–	Y
4	Y	–	Y	–	Y	–	Y	–	Y	–	Y
5	–	–	–	Y	–	–	–	–	Y	–	–
6	Y	Y	Y	–	Y	Y	Y	Y	–	–	Y

- The (real) Hadamard conjecture is that matrices exist at orders $1, 2, 4t$ for $t \in \mathbb{N}$.

Existence

$k\backslash n$	2	3	4	5	6	7	8	9	10	11	12
2	Y	–	Y	–	–	–	Y	–	–	–	Y
3	–	Y	–	–	Y	–	–	Y	–	–	Y
4	Y	–	Y	–	Y	–	Y	–	Y	–	Y
5	–	–	–	Y	–	–	–	–	Y	–	–
6	Y	Y	Y	–	Y	Y	Y	Y	–	–	Y

- The (real) Hadamard conjecture is that matrices exist at orders $1, 2, 4t$ for $t \in \mathbb{N}$.
- The complex Hadamard conjecture is that there exist matrices $\mathrm{BH}(2n, 4)$ for all $n, k \in \mathbb{N}$.

Existence

$k\backslash n$	2	3	4	5	6	7	8	9	10	11	12
2	Y	–	Y	–	–	–	Y	–	–	–	Y
3	–	Y	–	–	Y	–	–	Y	–	–	Y
4	Y	–	Y	–	Y	–	Y	–	Y	–	Y
5	–	–	–	Y	–	–	–	–	Y	–	–
6	Y	Y	Y	–	Y	Y	Y	Y	–	–	Y

- The (real) Hadamard conjecture is that matrices exist at orders $1, 2, 4t$ for $t \in \mathbb{N}$.
- The complex Hadamard conjecture is that there exist matrices $\mathrm{BH}(2n, 4)$ for all $n, k \in \mathbb{N}$.
- A $QUH(n, q)$ exists whenever a real Hadamard matrix exists, and whenever $n = q^t$. Is there an existence conjecture?

Existence

$k\backslash n$	2	3	4	5	6	7	8	9	10	11	12
2	Y	–	Y	–	–	–	Y	–	–	–	Y
3	–	Y	–	–	Y	–	–	Y	–	–	Y
4	Y	–	Y	–	Y	–	Y	–	Y	–	Y
5	–	–	–	Y	–	–	–	–	Y	–	–
6	Y	Y	Y	–	Y	Y	Y	Y	–	–	Y

- The (real) Hadamard conjecture is that matrices exist at orders $1, 2, 4t$ for $t \in \mathbb{N}$.
- The complex Hadamard conjecture is that there exist matrices $\mathrm{BH}(2n, 4)$ for all $n, k \in \mathbb{N}$.
- A $QUH(n, q)$ exists whenever a real Hadamard matrix exists, and whenever $n = q^t$. Is there an existence conjecture?
- Suppose that $\mathfrak{m}(x) \in \mathbb{Q}[x]$ has all roots of unit norm. When is there a Hadamard matrix with roots of $\mathfrak{m}(x)$ as entries?

Necessary conditions

- If $H \in \mathcal{BH}(n,k)$, then $\det(H) \in \mathbb{Q}(\zeta_k)$.
- Solvability of norm equations in $\mathbb{Q}(\zeta_k)$ and $\mathbb{Q}(\sqrt{-k})$ can lead to restrictions.

Theorem (de Launey 1984, Winterhof 2000)

Let $k \equiv 3 \mod 4$, $k = q^a$ a prime power, n_0 be the square-free part of n. Then $\mathcal{BH}(n,k)$ is empty if there exists some $p \mid n_0$ with $\left(\frac{p}{q}\right) = 1$.

Necessary conditions

- If $H \in \mathcal{BH}(n,k)$, then $\det(H) \in \mathbb{Q}(\zeta_k)$.
- Solvability of norm equations in $\mathbb{Q}(\zeta_k)$ and $\mathbb{Q}(\sqrt{-k})$ can lead to restrictions.

Theorem (de Launey 1984, Winterhof 2000)

Let $k \equiv 3 \mod 4$, $k = q^a$ a prime power, n_0 be the square-free part of n. Then $\mathcal{BH}(n,k)$ is empty if there exists some $p \mid n_0$ with $\left(\frac{p}{q}\right) = 1$.

- Suppose $k = 3^{2i+1}$. If there exists $p \mid n_0$ with $p \equiv 5 \mod 6$, then $\mathcal{BH}(n,k)$ is empty. E.g. $\mathcal{BH}(15,3)$ is empty.
- Suppose $k = 7^{2i+1}$. If there exists $p \mid n_0$ with $p \equiv 3,5,13 \mod 14$, then $\mathcal{BH}(n,k)$ is empty. E.g. $\mathcal{BH}(21,7)$ is empty.

Existence

Lemma (Sylvester, 1867?)

If there exists an abelian group of order n and exponent k then there exists a $\mathcal{BH}(n,k)$.

Theorem (Butson, 1962)

$\mathcal{BH}(2p,p)$ is non-empty for any odd prime p.

Lemma

If $H_1 \in \mathcal{BH}(n_1,k_1)$ and $H_2 \in \mathcal{BH}(n_2,k_2)$ then

$$H_1 \otimes H_2 \in \mathcal{BH}(n_1 n_2,\ lcm(k_1,k_2))\,.$$

Morphisms

- $\mathcal{BH}(n, k_0) \subseteq \mathcal{BH}(n, k)$ for all $k_0 \mid k$.
- Turyn (1969): If $\mathcal{BH}(n, 4)$ is non-empty, so is $\mathcal{BH}(2n, 2)$.
- Compton, Craigen, de Launey (2015): If there exists $H \in \mathcal{BH}(n, 6)$ with no purely real entries, $\mathcal{BH}(4n, 2)$ is nonempty.

Definition

An (X, Y)-*morphism* of Hadamard matrices is a homomorphism of matrix algebras $\mathrm{M}_n(\mathbb{C}) \to \mathrm{M}_{nt}(\mathbb{C})$ which carries Hadamard matrices with entries in $X \subseteq \mathbb{C}$ to Hadamard matrices with entries in Y.

Turyn's morphism

$$M = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad 2^{-1}M^3 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}, \quad M^{i+4} = -4M^i$$

Define the following map:

$$\phi(1) = M, \ \ \phi(i) = 2^{-1}M^3, \ \ \phi(-1) = 2^{-2}M^5, \ \ \phi(-i) = 2^{-3}M^7 .$$

$$\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^{\phi} = \left(\begin{array}{cc|cc} 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & -1 \\ \hline 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \end{array}\right)$$

Turyn's morphism

$$M = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad 2^{-1}M^3 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}, \quad M^{i+4} = -4M^i$$

Define the following map:

$$\phi(1) = M, \ \ \phi(i) = 2^{-1}M^3, \ \ \phi(-1) = 2^{-2}M^5, \ \ \phi(-i) = 2^{-3}M^7 .$$

$$\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^{\phi} = \left(\begin{array}{cc|cc} 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & -1 \\ \hline 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \end{array}\right)$$

Theorem (Turyn)

If $H \in \mathcal{BH}(n, 4)$, then $H^{\phi} \in \mathcal{BH}(2n, 2)$.

Proving a matrix is Hadamard

To show that an $n \times n$ matrix is (complex) Hadamard we must:

- check every entry has absolute value 1.
- check that every eigenvalue has absolute value $\sqrt{n}$.

Turyn's morphism

Observe that

$$\begin{aligned} AMA^* &= \frac{1}{2}\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \\ &= \begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix} = \sqrt{2}\begin{pmatrix} \zeta_8 & 0 \\ 0 & \zeta_8^7 \end{pmatrix} \end{aligned}$$

- The eigenvalues of $\sqrt{2}^{-1}M$ are primitive eighth roots of unity.
- For any odd integer i, the scaled matrix $\sqrt{2}^{1-i}M^i$ is Hadamard.

Turyn's morphism

Observe that

$$\begin{aligned} AMA^* &= \frac{1}{2}\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \\ &= \begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix} = \sqrt{2}\begin{pmatrix} \zeta_8 & 0 \\ 0 & \zeta_8^7 \end{pmatrix} \end{aligned}$$

- The eigenvalues of $\sqrt{2}^{-1}M$ are primitive eighth roots of unity.
- For any odd integer i, the scaled matrix $\sqrt{2}^{1-i}M^i$ is Hadamard.
- The map $\psi : \mathbb{Q}(\omega_8) \to M_2\left(\mathbb{Q}(\sqrt{2})\right)$ given by

$$\psi(\omega_8^i) \to \sqrt{2}^{1-i}M^i$$

is a homomorphism $\mathbb{Q}$-algebras, and the image of $\sqrt{2}\omega_8^{2i+1}$ is Hadamard.

Turyn's morphism

$$AM^iA^{-1} = \sqrt{2}\begin{pmatrix} \zeta_8^i & 0 \\ 0 & \zeta_8^{8-i} \end{pmatrix}$$

The matrix $(I_n \otimes A)H^\phi(I_n \otimes A^{-1})$ has diagonal blocks. So the **Kronecker shuffle** of this matrix is block diagonal. That is

$$P(I_n \otimes A)H^\phi(I_n \otimes A^{-1})P^{-1} = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}.$$

Via some computation:

$$B_1[i,j] = \sqrt{2}\omega_8 h_{i,j}, \quad B_2[i,j] = \sqrt{2}\omega_8^* h_{i,j}^*.$$

So H^ϕ is similar to a block diagonal matrix where the blocks are scaled Hadamard matrices. So all eigenvalues have modulus $\sqrt{2n}$ and hence H^ϕ is Hadamard!

Hypotheses

- $\mathfrak{m}(x) \in \mathbb{Q}[x]$, and $\mathfrak{m}(x)$ splits in $K = \mathbb{Q}[x]/(\mathfrak{m}(x))$, and K has an embedding in $\mathbb{C}$ such that all roots of $\mathfrak{m}(x)$ have modulus 1.

Hypotheses

- $\mathfrak{m}(x) \in \mathbb{Q}[x]$, and $\mathfrak{m}(x)$ splits in $K = \mathbb{Q}[x]/(\mathfrak{m}(x))$, and K has an embedding in $\mathbb{C}$ such that all roots of $\mathfrak{m}(x)$ have modulus 1.
- There exists a complex Hadamard matrix H with minimal polynomial $\mathfrak{m}(x)$.

Hypotheses

- $\mathfrak{m}(x) \in \mathbb{Q}[x]$, and $\mathfrak{m}(x)$ splits in $K = \mathbb{Q}[x]/(\mathfrak{m}(x))$, and K has an embedding in $\mathbb{C}$ such that all roots of $\mathfrak{m}(x)$ have modulus 1.
- There exists a complex Hadamard matrix H with minimal polynomial $\mathfrak{m}(x)$.
- In the field $\mathbb{Q}[H]$, isomorphic to K, the Galois conjugates of H are all Hadamard.

Hypotheses

- $\mathfrak{m}(x) \in \mathbb{Q}[x]$, and $\mathfrak{m}(x)$ splits in $K = \mathbb{Q}[x]/(\mathfrak{m}(x))$, and K has an embedding in $\mathbb{C}$ such that all roots of $\mathfrak{m}(x)$ have modulus 1.
- There exists a complex Hadamard matrix H with minimal polynomial $\mathfrak{m}(x)$.
- In the field $\mathbb{Q}[H]$, isomorphic to K, the Galois conjugates of H are all Hadamard.

Cyclotomic: $M = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ is associated to $\Phi_8(x) = x^4 + 1$.

Condition (3) requires that normalised odd powers of H are Hadamard.

Hypotheses

- $\mathfrak{m}(x) \in \mathbb{Q}[x]$, and $\mathfrak{m}(x)$ splits in $K = \mathbb{Q}[x]/(\mathfrak{m}(x))$, and K has an embedding in $\mathbb{C}$ such that all roots of $\mathfrak{m}(x)$ have modulus 1.
- There exists a complex Hadamard matrix H with minimal polynomial $\mathfrak{m}(x)$.
- In the field $\mathbb{Q}[H]$, isomorphic to K, the Galois conjugates of H are all Hadamard.

Cyclotomic: $M = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ is associated to $\Phi_8(x) = x^4 + 1$.
Condition (3) requires that normalised odd powers of H are Hadamard.

Imaginary Quadratic: If M is skew of order n then $\mathfrak{m}(x) = x^4 + \frac{2n-4}{n}x^2 + 1$. Condition (3) requires that $M^\top$ and $M - 2I$ and $(M - 2I)^\top$ are Hadamard.

Main Theorem

Hypotheses: H is $k \times k$ complex Hadamard, has minimal polynomial $\mathfrak{m}(x)$, and for any field automorphism σ the matrix H^σ is Hadamard.

Main Theorem

Hypotheses: H is $k \times k$ complex Hadamard, has minimal polynomial $\mathfrak{m}(x)$, and for any field automorphism σ the matrix H^σ is Hadamard.

Theorem

Suppose that M is $n \times n$ complex Hadamard, and all entries are roots of $\mathfrak{m}(x)$. Then substituting $x^\sigma \to H^\sigma$ gives a $kn \times kn$ Hadamard matrix.

Main Theorem

Hypotheses: H is $k \times k$ complex Hadamard, has minimal polynomial $\mathfrak{m}(x)$, and for any field automorphism σ the matrix H^σ is Hadamard.

Theorem

Suppose that M is $n \times n$ complex Hadamard, and all entries are roots of $\mathfrak{m}(x)$. Then substituting $x^\sigma \to H^\sigma$ gives a $kn \times kn$ Hadamard matrix.

Proof.

Since the H^σ are Hadamard, all entries in the image have unit norm. The function $\phi : x \mapsto H$ induces an isomorphism of fields, so orthogonality of rows is preserved. □

Main Theorem

Hypotheses: H is $k \times k$ complex Hadamard, has minimal polynomial $\mathfrak{m}(x)$, and for any field automorphism σ the matrix H^σ is Hadamard.

Theorem

Suppose that M is $n \times n$ complex Hadamard, and all entries are roots of $\mathfrak{m}(x)$. Then substituting $x^\sigma \to H^\sigma$ gives a $kn \times kn$ Hadamard matrix.

Proof.

Since the H^σ are Hadamard, all entries in the image have unit norm. The function $\phi : x \mapsto H$ induces an isomorphism of fields, so orthogonality of rows is preserved. □

Cyclotomic: Egan, Ó C., 2019
Imaginary Quadratic: Heikoop, Nunez Ponasso, Ó C., Pugmire.

Compton-Craigen-de Launey

$$M_4 = \begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{bmatrix}.$$

Compton-Craigen-de Launey

$$M_4 = \begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{bmatrix}.$$

- $X = \{\zeta_6, \zeta_6^2, \zeta_6^4, \zeta_6^5\}$ and $Y = \{\chi_6, \chi_6^5\}$.
- The eigenvalues of $2^{-1}M_4$ are the primitive sixth roots of unity, each with multiplicity 2.

Compton-Craigen-de Launey

$$M_4 = \begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{bmatrix}.$$

- $X = \{\zeta_6, \zeta_6^2, \zeta_6^4, \zeta_6^5\}$ and $Y = \{\chi_6, \chi_6^5\}$.
- The eigenvalues of $2^{-1}M_4$ are the primitive sixth roots of unity, each with multiplicity 2.
- Since χ is the identity map on $\langle\zeta_6\rangle$ and χ_5 is complex conjugation, the restrictions placed on H by Y are vacuous.
- One can check that $2^{-1}M_4^2$ is Hadamard and that $M_4^3 = -8I_4$. As a result, $2^{-3}M_4^4$ and $2^{-4}M_4^5$ are Hadamard.

Compton-Craigen-de Launey

$$M_4 = \begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{bmatrix}.$$

- $X = \{\zeta_6, \zeta_6^2, \zeta_6^4, \zeta_6^5\}$ and $Y = \{\chi_6, \chi_6^5\}$.
- The eigenvalues of $2^{-1}M_4$ are the primitive sixth roots of unity, each with multiplicity 2.
- Since χ is the identity map on $\langle\zeta_6\rangle$ and χ_5 is complex conjugation, the restrictions placed on H by Y are vacuous.
- One can check that $2^{-1}M_4^2$ is Hadamard and that $M_4^3 = -8I_4$. As a result, $2^{-3}M_4^4$ and $2^{-4}M_4^5$ are Hadamard.
- Since M_4^3 and M_4^6 contain zero entries, we have chosen a maximal set X, and the *unreal* condition on H is necessary.

Sound pairs: Compton-Craigen-de Launey

$$M_4 = \begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{bmatrix}.$$

Definition

$H \in \mathcal{BH}(n, 6)$ is *unreal* if no entry is ± 1.

Theorem (Compton-Craigen-de Launey)

If $H \in \mathcal{BH}(n, 6)$ is unreal, then the pair (H, M_4) is sound. If the set of unreal $\mathcal{BH}(n, 6)$ is non-empty, the set of $\mathcal{BH}(4n, 2)$ is non-empty.

MUBS

Definition

A set of orthonormal bases in a d-dimensional inner product space is *mutually unbiased* if

$$|\langle \phi_i, \psi_j \rangle| = \frac{1}{\sqrt{d}},$$

whenever ϕ_i and ψ_j belong to disjoint orthonormal bases.

MUBS

Definition

A set of orthonormal bases in a d-dimensional inner product space is *mutually unbiased* if

$$|\langle \phi_i, \psi_j \rangle| = \frac{1}{\sqrt{d}},$$

whenever ϕ_i and ψ_j belong to disjoint orthonormal bases.

- Without loss of generality, one basis in a set of MUBS may be chosen to be the standard normal basis. Every other basis is then $\frac{1}{\sqrt{d}} H_i$ where H_i is Hadamard.

MUBS

Definition

A set of orthonormal bases in a d-dimensional inner product space is *mutually unbiased* if

$$|\langle \phi_i, \psi_j \rangle| = \frac{1}{\sqrt{d}},$$

whenever ϕ_i and ψ_j belong to disjoint orthonormal bases.

- Without loss of generality, one basis in a set of MUBS may be chosen to be the standard normal basis. Every other basis is then $\frac{1}{\sqrt{d}} H_i$ where H_i is Hadamard.
- Via finite geometry: if $n = p^k$ there exists a complete set of $n + 1$ MUBS.
- Do there exist 4 MUBS in dimension 6?
- Correspond to maximally entangled quantum states.

New morphisms from MUBS

Definition

A set $\{B_0, B_1, \ldots B_m\}$ of orthonormal bases in a d-dimensional inner product space is *mutually unbiased* if

$$|\langle \phi_i, \psi_j \rangle| = \frac{1}{\sqrt{d}},$$

whenever ϕ_i and ψ_j belong to disjoint orthonormal bases.

New morphisms from MUBS

Definition

A set $\{B_0, B_1, \ldots B_m\}$ of orthonormal bases in a d-dimensional inner product space is *mutually unbiased* if

$$|\langle \phi_i, \psi_j \rangle| = \frac{1}{\sqrt{d}},$$

whenever ϕ_i and ψ_j belong to disjoint orthonormal bases.

- If $B_0 = I_d$ then $\sqrt{d}B_i$ is a CHM.
- If $B_0 = I_d$ then $B_i B_j^*$ is a CHM for $i \neq j$.

Sound pairs from MUBS

Theorem (Gow, 2007/2017)

There exists a complete set of $2^n + 1$ MUBs in $\mathbb{C}^{2^n}$ which can be written as powers of a single matrix B. All entries of $\sqrt{2^n}B$ are fourth roots of unity.

Sound pairs from MUBS

Theorem (Gow, 2007/2017)

There exists a complete set of $2^n + 1$ MUBs in $\mathbb{C}^{2^n}$ which can be written as powers of a single matrix B. All entries of $\sqrt{2^n}B$ are fourth roots of unity.

- Now $B^j(B^i)^* = B^{j-i}$.
- Can we use $\langle B \rangle$ to build new morphisms?

Sound pairs from MUBS

Theorem (Gow, 2007/2017)

There exists a complete set of $2^n + 1$ MUBs in $\mathbb{C}^{2^n}$ which can be written as powers of a single matrix B. All entries of $\sqrt{2^n}B$ are fourth roots of unity.

- Now $B^j(B^i)^* = B^{j-i}$.
- Can we use $\langle B \rangle$ to build new morphisms?
- Yes, **if** the eigenvalues of B are all roots of unity of the same order: if $2^n + 1$ is a Fermat prime.

Sound pairs from MUBS

Theorem

Say $H \in \mathcal{BH}(n, 10)$ *is unreal if it has no entries* ± 1*. Then, taking*

$$M_5 = \begin{bmatrix} -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ i & i & -i & -i \\ i & -i & -i & i \end{bmatrix},$$

the pair (H, M_5) *is sound.*

Sound pairs from MUBS

Theorem

Say $H \in \mathcal{BH}(n, 10)$ is unreal if it has no entries ± 1. Then, taking

$$M_5 = \begin{bmatrix} -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ i & i & -i & -i \\ i & -i & -i & i \end{bmatrix},$$

the pair (H, M_5) is sound.

- If there exists an unreal $H \in \mathcal{BH}(n, 10)$ here exists $H' \in \mathcal{BH}(4n, 4)$.

Sound pairs from MUBS

Theorem

Say $H \in \mathcal{BH}(n, 10)$ is unreal if it has no entries ± 1. Then, taking

$$M_5 = \begin{bmatrix} -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ i & i & -i & -i \\ i & -i & -i & i \end{bmatrix},$$

the pair (H, M_5) is sound.

- If there exists an unreal $H \in \mathcal{BH}(n, 10)$ here exists $H' \in \mathcal{BH}(4n, 4)$.
- Composing with the Turyn morphism, there exists $H'' \in \mathcal{BH}(8n, 2)$.

Sound pairs from MUBS

Theorem

Say $H \in \mathcal{BH}(n, 10)$ is unreal if it has no entries ± 1. Then, taking

$$M_5 = \begin{bmatrix} -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ i & i & -i & -i \\ i & -i & -i & i \end{bmatrix},$$

the pair (H, M_5) is sound.

- If there exists an unreal $H \in \mathcal{BH}(n, 10)$ here exists $H' \in \mathcal{BH}(4n, 4)$.
- Composing with the Turyn morphism, there exists $H'' \in \mathcal{BH}(8n, 2)$.
- Generalises to any Fermat prime; if there exists an unreal $H \in \mathcal{BH}(n, p)$ there exists $H' \in \mathcal{BH}(n(p-1), 4)$, and $H'' \in \mathcal{BH}(2n(p-1), 2)$.

- Suppose that H is real, symmetric Hadamard of order $4n$.

- Suppose that H is real, symmetric Hadamard of order $4n$.
- Eigenvalues are $\pm 2\sqrt{n}$.

- Suppose that H is real, symmetric Hadamard of order $4n$.
- Eigenvalues are $\pm 2\sqrt{n}$.
- Multiplicities from the trace: if $n \neq k^2$ then multiplicities are $2n$.

Theorem (Egan-Ó C.- Swartz, 2019)

For each $t \in \mathbb{Z}$, there exists a real Hadamard matrix with minimal polynomial $\Phi_{2^t}(x)$.

- Suppose that H is a real symmetric Hadamard matrix, and P, Q are monomial matrices such that $PHQ^\top = H$.

Theorem (Egan-Ó C.- Swartz, 2019)

For each $t \in \mathbb{Z}$, there exists a real Hadamard matrix with minimal polynomial $\Phi_{2^t}(x)$.

- Suppose that H is a real symmetric Hadamard matrix, and P, Q are monomial matrices such that $PHQ^\top = H$.
- Then $PH = HQ$. So

$$(PH)^2 = (PH)(HQ) = nPQ\,.$$

Theorem (Egan-Ó C.- Swartz, 2019)

For each $t \in \mathbb{Z}$, there exists a real Hadamard matrix with minimal polynomial $\Phi_{2^t}(x)$.

- Suppose that H is a real symmetric Hadamard matrix, and P, Q are monomial matrices such that $PHQ^\top = H$.
- Then $PH = HQ$. So

$$(PH)^2 = (PH)(HQ) = nPQ\,.$$

- Matrices P and Q are monomial (signed permutation). We can compute their eigenvalues.

Theorem (Egan-Ó C.- Swartz, 2019)

For each $t \in \mathbb{Z}$, there exists a real Hadamard matrix with minimal polynomial $\Phi_{2^t}(x)$.

- Suppose that H is a real symmetric Hadamard matrix, and P, Q are monomial matrices such that $PHQ^\top = H$.
- Then $PH = HQ$. So

$$(PH)^2 = (PH)(HQ) = nPQ\,.$$

- Matrices P and Q are monomial (signed permutation). We can compute their eigenvalues.
- We require a matrix PQ in which all cycles have equal length k, and the number of negative entries in each cycle is odd.

Theorem (Egan-Ó C.- Swartz, 2019)

For each $t \in \mathbb{Z}$, there exists a real Hadamard matrix with minimal polynomial $\Phi_{2^t}(x)$.

- Suppose that H is a real symmetric Hadamard matrix, and P, Q are monomial matrices such that $PHQ^\top = H$.
- Then $PH = HQ$. So

$$(PH)^2 = (PH)(HQ) = nPQ\,.$$

- Matrices P and Q are monomial (signed permutation). We can compute their eigenvalues.
- We require a matrix PQ in which all cycles have equal length k, and the number of negative entries in each cycle is odd.
- Minimal polynomial $x^k + 1$.

Theorem (Egan-Ó C.- Swartz, 2019)

For each $t \in \mathbb{Z}$, there exists a real Hadamard matrix with minimal polynomial $\Phi_{2^t}(x)$.

- Let V be n-dimensional over $\mathbb{F}_2$, and let $\mathcal{S}_n = \left[(-1)^{\langle a,b\rangle}\right]_{a,b,\in V}$. Character orthogonality implies that $\mathcal{S}_n$ is symmetric Hadamard.

Theorem (Egan-Ó C.- Swartz, 2019)

For each $t \in \mathbb{Z}$, there exists a real Hadamard matrix with minimal polynomial $\Phi_{2^t}(x)$.

- Let V be n-dimensional over $\mathbb{F}_2$, and let $\mathcal{S}_n = \left[(-1)^{\langle a,b\rangle}\right]_{a,b,\in V}$. Character orthogonality implies that $\mathcal{S}_n$ is symmetric Hadamard.
- It can be shown that $(V \times V) \rtimes \mathrm{GL}(V)$ acts on $\{\pm\mathcal{S}_n\}$ by monomial matrices (but not by automorphisms!)

Theorem (Egan-Ó C.- Swartz, 2019)

For each $t \in \mathbb{Z}$, there exists a real Hadamard matrix with minimal polynomial $\Phi_{2^t}(x)$.

- Let V be n-dimensional over $\mathbb{F}_2$, and let $\mathcal{S}_n = \left[(-1)^{\langle a,b\rangle}\right]_{a,b,\in V}$. Character orthogonality implies that $\mathcal{S}_n$ is symmetric Hadamard.
- It can be shown that $(V \times V) \rtimes \mathrm{GL}(V)$ acts on $\{\pm\mathcal{S}_n\}$ by monomial matrices (but not by automorphisms!)
- We study the orbits of maximal Jordan blocks of $\mathrm{GL}_n(V)$ on vectors. It is crucial that these blocks factor as $M(M^{-1})^\top$ – Fulman-Guralnick.

Theorem (Egan-Ó C.- Swartz, 2019)

For each $t \in \mathbb{Z}$, there exists a real Hadamard matrix with minimal polynomial $\Phi_{2^t}(x)$.

- Let V be n-dimensional over $\mathbb{F}_2$, and let $\mathcal{S}_n = \left[(-1)^{\langle a,b\rangle}\right]_{a,b,\in V}$. Character orthogonality implies that $\mathcal{S}_n$ is symmetric Hadamard.
- It can be shown that $(V \times V) \rtimes \mathrm{GL}(V)$ acts on $\{\pm\mathcal{S}_n\}$ by monomial matrices (but not by automorphisms!)
- We study the orbits of maximal Jordan blocks of $\mathrm{GL}_n(V)$ on vectors. It is crucial that these blocks factor as $M(M^{-1})^\top$ – Fulman-Guralnick.
- From careful analysis of orbit structures, we construct the required automorphism.

Theorem (Egan-Ó C.- Swartz, 2019)

For each $t \in \mathbb{Z}$, there exists a real Hadamard matrix with minimal polynomial $\Phi_{2^t}(x)$.

- This theorem generalises, provided the minimal polynomial we seek has two non-zero terms.
- Irreducible such polynomials are characterised by Lang: such extensions are of the form $\mathbb{Q}[\zeta_{p^a}]$ over $\mathbb{Q}[\zeta_{p^b}]$ for $b < a$.
- Hadamard matrices exist in all these cases: Ostergard-Paavola, Ó C-Swartz.

Theorem (Heikoop-Ó C.-Nunez Ponasso-Pugmire, 2019?)

Let H be an $n \times n$ CHM with entries in $\frac{1}{\sqrt{4t}}\left(\pm 1 \pm \sqrt{1-4t}\right)$, and M a skew-Hadamard matrix of order $4t$. The pair (H, M) is sound, and there exists a real Hadamard matrix of order $4tn$.

Theorem (Fender, Kharaghani, Suda, 2017)

Let $q \equiv 3 \mod 4$ be a prime power. There exists a CHM of order q^α with entries in $\frac{1}{\sqrt{q+1}}(\pm 1 \pm \sqrt{-q})$, for all $\alpha \in \mathbb{N}$.

Corollary

There exist Hadamard matrices of order $q^\alpha(q+1)$ whenever there exists a skew-Hadamard matrix H of order $q+1$.

New examples of sound pairs: partial morphisms

We have found the following matrices computationally.

- $M \in \mathcal{BH}(4,2)$, eigenvalues are primitive 12^{th} roots
- $M \in \mathcal{BH}(6,4)$ eigenvalues are odd powers of ζ_{12}
- $M \in \mathcal{BH}(4,4)$ eigenvalues are primitive 5^{th} roots
- $M \in \mathcal{BH}(8,2)$ eigenvalues are primitive 24^{th} roots
- $M \in \mathcal{BH}(8,2)$ eigenvalues are primitive 16^{th} roots
- $M \in \mathcal{BH}(12,2)$ eigenvalues are all primitive 8^{th} roots
- $M \in \mathcal{BH}(16,2)$ eigenvalues are all fifth roots and all eleventh roots
- ...

New examples of sound pairs: partial morphisms

We have found the following matrices computationally.

- $M \in \mathcal{BH}(4,2)$, eigenvalues are primitive 12^{th} roots
- $M \in \mathcal{BH}(6,4)$ eigenvalues are odd powers of ζ_{12}
- $M \in \mathcal{BH}(4,4)$ eigenvalues are primitive 5^{th} roots
- $M \in \mathcal{BH}(8,2)$ eigenvalues are primitive 24^{th} roots
- $M \in \mathcal{BH}(8,2)$ eigenvalues are primitive 16^{th} roots
- $M \in \mathcal{BH}(12,2)$ eigenvalues are all primitive 8^{th} roots
- $M \in \mathcal{BH}(16,2)$ eigenvalues are all fifth roots and all eleventh roots
- ...
- **Question:** What are necessary or sufficient conditions for an irreducible polynomial $\mathfrak{m}(x)$ to be the minimal polynomial of a complex Hadamard matrix?

Future work/Open questions

- Which irreducible polynomials are minimal polynomials of a real Hadamard matrix?

Future work/Open questions

- Which irreducible polynomials are minimal polynomials of a real Hadamard matrix?
- For which field extensions K/k does K have a basis of Hadamard matrices over k?

Future work/Open questions

- Which irreducible polynomials are minimal polynomials of a real Hadamard matrix?
- For which field extensions K/k does K have a basis of Hadamard matrices over k?
- Progress appears to require techniques from field theory, algebraic number theory and Galois theory over $\mathbb{Q}$. And geometry over finite fields (e.g. polar spaces) and knowledge of classical groups...

Future work/Open questions

- Which irreducible polynomials are minimal polynomials of a real Hadamard matrix?
- For which field extensions K/k does K have a basis of Hadamard matrices over k?
- Progress appears to require techniques from field theory, algebraic number theory and Galois theory over $\mathbb{Q}$. And geometry over finite fields (e.g. polar spaces) and knowledge of classical groups...
- **Thank you for your attention.**