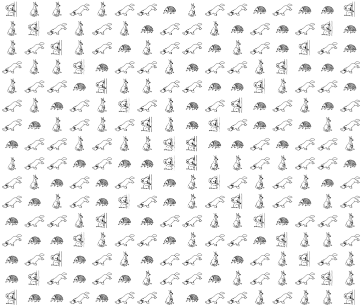
Complex Hadamard matrices and 3-class association schemes

Akihiro Munemasa[1]
(joint work with Takuya Ikuta)

[1]Graduate School of Information Sciences
Tohoku University

June 27, 2014
Algebraic Combinatorics:
Spectral Graph Theory, Erdős-Ko-Rado Theorems and
Quantum Information Theory
A Conference to celebrate the work of Chris Godsil
Unversity of Waterloo

Algebraic Combinatorics:
Spectral Graph Theory, Erdös-Ko-Rado Theorems and Quantum Information Theory



A conference to celebrate the work of Chris Godsil

June 23-27 2014

Department of Combinatorics & Optimization
University of Waterloo

Algebraic Combinatorics:
Spectral Graph Theory, Erdös-Ko-Rado Theorems and
Quantum Information Theory

and Association Schemes   and Complex Hadamard Matrices

```
0 1 1 2 1 2 2 3 1 2 2 3 2 3 3 0
1 0 2 1 2 1 3 2 2 1 3 2 3 2 0 3
1 2 0 1 2 3 1 2 2 3 1 2 3 0 2 3
2 1 1 0 3 2 2 1 3 2 2 1 0 3 3 2
1 2 2 3 0 1 1 2 2 3 3 0 1 2 2 3
2 1 3 2 1 0 2 1 3 2 0 3 2 1 3 2
2 3 1 2 1 2 0 1 3 0 2 3 2 3 1 2
3 2 2 1 2 1 1 0 0 3 3 2 3 2 2 1
1 2 2 3 2 3 3 0 0 1 1 2 1 2 2 3
2 1 3 2 3 2 0 3 1 0 2 1 2 1 3 2
2 3 1 2 3 0 2 3 1 2 0 1 2 3 1 2
3 2 2 1 0 3 3 2 2 1 1 0 3 2 2 1
2 3 3 0 1 2 2 3 1 2 2 3 0 1 1 2
3 2 0 3 2 1 3 2 2 1 3 2 1 0 2 1
3 0 2 3 2 3 1 2 2 3 1 2 1 2 0 1
0 3 3 2 3 2 2 1 3 2 2 1 2 1 1 0
```

$$= 0 \cdot A_0 + 1 \cdot A_1 + 2 \cdot A_2 + 3 \cdot A_3 + 0 \cdot A_4$$

$$= 1 \cdot A_0 + \xi \cdot A_1 + (-1) \cdot A_2 - \xi \cdot A_3 + 1 \cdot A_4 = H$$

Then $HH^* = 16I$, where $|\xi| = 1$

Hadamard matrices and generalizations

- A (real) Hadamard matrix of order n is an $n \times n$ matrix H with entries ± 1, satisfying $HH^\top = nI$.
- A complex Hadamard matrix of order n is an $n \times n$ matrix H with entries in $\{\xi \in \mathbb{C} \mid |\xi| = 1\}$, satisfying $HH^* = nI$, where $*$ means the conjugate transpose.

We propose a strategy to construct infinite families of complex Hadamard matrices using association schemes, and demonstrate a successful case.

Outline

- A problem in algebraic geometry
- Strategy to find complex Hadamard matrices
- A family of 3-class association scheme giving complex Hadamard matrices
- Equivalence and decomposability

References:

- A. Chan and C. Godsil, *Type-II matrices and combinatorial structures*, Combinatorica, **30** (2010), 1–24.
- A. Chan, *Complex Hadamard matrices and strongly regular graphs*, arXiv:1102.5601.
- T. Ikuta and A. Munemasa, *Complex Hadamard matrices contained in a Bose–Mesner algebra*, in preparation

- Describe the image of the map

$$\begin{aligned} f : (\mathbb{C}^\times)^n &\to \mathbb{C}^{n(n-1)/2}, \\ (x_1, \ldots, x_n) &\mapsto \left(\frac{x_i}{x_j} + \frac{x_j}{x_i} \right)_{1 \le i < j \le n} \end{aligned}$$

An easier (linear) problem is

- Describe the image of the map

$$\begin{aligned} f : \mathbb{C}^n &\to \mathbb{C}^{n(n-1)/2}, \\ (x_1, \ldots, x_n) &\mapsto (x_i + x_j)_{1 \le i < j \le n} \end{aligned}$$

The image is

$$(-2 \text{ eigenspace of } T(n) = J(n,2))^\perp.$$

$$\mathbb{C}^{n(n-1)/2} = \langle \mathbf{1} \rangle \oplus V_1 \oplus V_2 \quad \text{as } \mathrm{Sym}(n)\text{-rep.}$$

$$\dim = 1 + (n-1) + \binom{n}{2} - n$$

$$
\begin{aligned}
f : (\mathbb{C}^\times)^n &\to \mathbb{C}^{n(n-1)/2}, \\
(x_1, \ldots, x_n) &\mapsto \left(\frac{x_i}{x_j} + \frac{x_j}{x_i} \right)_{1 \le i < j \le n}
\end{aligned}
$$

Theorem

The image of f coincides with the set of zeros of the ideal I in the polynomial ring $\mathbb{C}[X_{ij} : 1 \le i < j \le n]$ generated by

$$
\begin{aligned}
& g(X_{ij}, X_{ik}, X_{jk}) \\
& h(X_{ij}, X_{ik}, X_{il}, X_{jk}, X_{jl}, X_{kl})
\end{aligned}
$$

where i, j, k, l are distinct, $X_{ij} = X_{ji}$, and

$$
\begin{aligned}
g &= X^2 + Y^2 + Z^2 - XYZ - 4, \\
h &= (Z^2 - 4)U - Z(XW + YV) + 2(XY + VW).
\end{aligned}
$$

Let me know if you know any references.

D. Leonard pointed out this week:

$$
\begin{aligned}
& h(X_{0,1}, X_{0,2}, X_{0,3}, X_{1,2}, X_{1,3}, X_{2,3}) \\
& = (X_{0,3}^2 - 4)X_{1,2} - X_{0,3}(X_{0,1}X_{2,3} + X_{0,2}X_{1,3}) \\
& \quad + 2(X_{0,1}X_{0,2} + X_{1,3}X_{2,3}) \\
& = \det \begin{bmatrix} 2 & X_{0,3} & X_{0,2} \\ X_{0,3} & 2 & X_{2,3} \\ X_{0,1} & X_{1,3} & X_{1,2} \end{bmatrix}
\end{aligned}
$$

Why is the image of the map

$$\begin{aligned} f : (\mathbb{C}^\times)^n &\rightarrow \mathbb{C}^{n(n-1)/2}, \\ (x_1, \dots, x_n) &\mapsto \left(\frac{x_i}{x_j} + \frac{x_j}{x_i} \right)_{1 \le i < j \le n} \end{aligned}$$

relevant to complex Hadamard matrices?

Goethals–Seidel (1970) symmetric regular (real) Hadamard matrix necessarily comes from a strongly regular graph (SRG) on $4s^2$ vertices

de la Harpe–Jones (1990) SRG n: prime $\equiv 1 \pmod 4$ $\rightarrow$ symmetric circulant complex Hadamard

Godsil–Chan (2010), and Chan (2011) classified complex Hadamard matrices of the form:

$$
\begin{aligned}
H &= I + xA_1 + yA_2, \\
A_1 &= \text{adjacency matrix of a SRG } \Gamma, \\
A_2 &= \text{adjacency matrix of } \overline{\Gamma}.
\end{aligned}
$$

and also considered those of the form

$$H = I + xA_1 + yA_2 + zA_3$$

Unifying principle: symmetric association schemes.
(strongly regular graphs is a special case)

A. Chan (2011) found a complex Hadamard matrix of the form

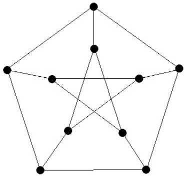
$$H = I + xA_1 + yA_2 + zA_3$$

of order 15 from the line graph $L(O_3)$ of the Petersen graph O_3.

$$x = 1, \quad y = \frac{-7 \pm \sqrt{-15}}{8}, \quad z = 1 \quad \text{(Szöllősi 2010)}$$

$$x = \frac{5 \pm \sqrt{-11}}{6}, \quad y = -1, \quad z = x \quad \text{(Szöllősi 2010)}$$

$$x = \frac{-1 \pm \sqrt{-15}}{4}, \quad y = x^{-1}, \quad z = 1$$



$I + xA + y\overline{A}$ is a type II matrix if and only if

$$\begin{aligned} nI &= (I + xA + y\overline{A})(I + x^{-1}A + y^{-1}\overline{A}) \\ &= I + (x + x^{-1})A + (y + y^{-1})\overline{A} + (xy^{-1} + x^{-1}y)A\overline{A}. \end{aligned}$$

More generally. . . .

If $H = \alpha_0 A_0 + \alpha_1 A_1 + \alpha_2 A_2 + \cdots$ is a type II matrix, where $A_0 = I, A_1, A_2, \ldots$ are the adjacency matrices of a symmetric association scheme, then

$$\begin{aligned} nI = HH^* &= \cdots \alpha_i \alpha_j^{-1} A_i A_j^* + \cdots \\ &= \cdots \frac{\alpha_i}{\alpha_j} A_i A_j + \cdots \\ &= \cdots (\frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i}) A_i A_j + \cdots \\ &= \cdots (\frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i}) A_i A_j + \cdots + \sum_i A_i^2 \end{aligned}$$

Diagonalize to get linear equations

$$n = \sum_{i<j} (\frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i}) P_{hi} P_{hj} + 2 \sum_i P_{hi}^2 \quad (\forall h) x_{ij} P_{hi} P_{hj} + 2 \sum_i P_{hi}^2 \quad (\forall h)$$

where $A_i = \sum_h P_{hi} E_h$: spectral decomposition.
Given x_{ij}, $\exists ? (\alpha_i)$ such that

$$x_{ij} = \frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i}$$

$$
\begin{aligned}
f : (\mathbb{C}^\times)^n &\to \mathbb{C}^{n(n-1)/2}, \\
(x_1, \ldots, x_n) &\mapsto \left(\frac{x_i}{x_j} + \frac{x_j}{x_i} \right)_{1 \le i < j \le n}
\end{aligned}
$$

Theorem

The image of f coincides with the set of zeros of the ideal I in the polynomial ring $\mathbb{C}[X_{ij} : 1 \le i < j \le n]$ generated by

$$
\begin{aligned}
&g(X_{ij}, X_{ik}, X_{jk}) \\
&h(X_{ij}, X_{ik}, X_{il}, X_{jk}, X_{jl}, X_{kl})
\end{aligned}
$$

where i, j, k, l are distinct, $X_{ij} = X_{ji}$, and

$$
\begin{aligned}
g &= X^2 + Y^2 + Z^2 - XYZ - 4, \\
h &= (Z^2 - 4)U - Z(XW + YV) + 2(XY + VW).
\end{aligned}
$$

$$x_{ij} = \frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i} \quad (0 \le i < j \le d). \tag{1}$$

$$\sum_{0 \le i < j \le d} x_{ij} P_{hi} P_{hj} = n - \sum_{i=0}^{d} P_{hi}^2 \quad (\forall h) \tag{2}$$

Step 1 Solve the system of linear equations (2) in $\{x_{ij}\}$

Step 2 Find $\{\alpha_i\}$ from $\{x_{ij}\}$ by (1) using Theorem?.

The theorem only gives a criterion for a given (x_{ij}) to be in the image of the rational map. It does not give how to find preimages.

Given a zero (x_{ij}) of the ideal I, we know that there exists $(\alpha_i) \in (\mathbb{C}^\times)^{d+1}$ such that

$$x_{ij} = \frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i} \quad (0 \le i < j \le d). \tag{1}$$

How do we find (α_i), and when does $(\alpha_i) \in (S^1)^{d+1}$ hold?
Observe, for $\alpha \in \mathbb{C}$,

$$|\alpha| = 1 \iff -2 \le \alpha + \frac{1}{\alpha} \le 2.$$

So we need $-2 \le x_{ij} \le 2$.
Moreover, if $x_{ij} \in \{\pm 2\}$ for all i, j, then $\alpha_i = \pm\alpha_j$ so the resulting matrix is a scalar multiple of a real Hadamard matrix $\to$ Goethals–Seidel (1970).

$$\begin{aligned} f : (\mathbb{C}^\times)^n &\to \mathbb{C}^{n(n-1)/2}, \\ (x_1, \ldots, x_n) &\mapsto \left(\tfrac{x_i}{x_j} + \tfrac{x_j}{x_i}\right)_{1 \le i < j \le n} \end{aligned}$$

Theorem

Suppose $(x_{ij}) \in$ the image of f, $x_{ij} \in \mathbb{R}$, and $-2 < x_{0,1} < 2$. Fix $\alpha_0, \alpha_1 \in S^1$ in such a way that

$$x_{0,1} = \frac{\alpha_0}{\alpha_1} + \frac{\alpha_1}{\alpha_0}.$$

Define α_i $(2 \le i \le n)$ by

$$\alpha_i = \frac{\alpha_0(x_{0,1}\alpha_1 - 2\alpha_0)}{x_{1,i}\alpha_1 - x_{0,i}\alpha_0}.$$

Then $|\alpha_i| = |\alpha_j|$ and

$$\frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i} = x_{ij} \quad (0 \le i < j \le d). \tag{1}$$

and every (α_i) satisfying (1) is obtained in this way.

The procedure

Step 1 Set up the system of equations

$$g(X_{ij}, X_{ik}, X_{jk}) = 0,$$
$$h(X_{ij}, X_{ik}, X_{il}, X_{jk}, X_{jl}, X_{kl}) = 0,$$

$$\sum_{0 \le i < j \le d} X_{ij} P_{hi} P_{hj} = n - \sum_{i=0}^{d} P_{hi}^2$$

Step 2 Eliminate all but one variable X_{01}, and list all solutions $X_{01} = x_{01}$ with $-2 \le x_{01} \le 2$.

Step 3 Without loss of generality we may assume $\alpha_0 = 1$. Determine α_1 by

$$\frac{\alpha_0}{\alpha_1} + \frac{\alpha_1}{\alpha_0} = x_{0,1}.$$

Step 4 Determine (α_i) by

$$\alpha_i = \frac{\alpha_0(x_{0,1}\alpha_1 - 2\alpha_0)}{x_{1,i}\alpha_1 - x_{0,i}\alpha_0}.$$

Step 1 Set up the system of equations

Step 2 Eliminate all but one variable X_{01}, and list all solutions $X_{01} = a_{01}$ with $-2 \leq a_{01} \leq 2$.

In many known examples of association schemes with $d = 3$, Step 2 failed.

Theorem (Chan)

There are only finitely many antipodal distance-regular graphs of diameter 3 whose Bose–Mesner algebra contains a complex Hadamard matrix.

But Chan did find an example. $L(O_3)$: the line graph of the Petersen graph.
Our systematic search through the table of Van Dam (1999) revealed the infinite family starting with $L(O_3)$.

An infinite family

Let A be an association scheme having the eigenmatrix

$$P = \begin{bmatrix} 1 & \frac{q^2}{2} - q & \frac{q^2}{2} & q-2 \\ 1 & \frac{q}{2} & -\frac{q}{2} & -1 \\ 1 & -\frac{q}{2}+1 & -\frac{q}{2} & q-2 \\ 1 & -\frac{q}{2} & \frac{q}{2} & -1 \end{bmatrix}.$$

Such an association scheme arises from (twisted) symplectic polar graph. $V = V(2,q)$, $q = 2^n$, f: symplectic form on V. Define an association scheme on $V \setminus \{0\}$ by

$$R_1 = \{(x,y) \mid f(x,y) \neq 0,\ \mathrm{Tr}\, f(x,y)^e = 0\}, \qquad (e, q-1) = 1$$
$$R_2 = \{(x,y) \mid \mathrm{Tr}\, f(x,y)^e \neq 0\}, \qquad \text{(with Frédéric Vanhove)}$$
$$R_3 = \{(x,y) \mid \langle x\rangle_{\mathrm{GF}(q)} = \langle y\rangle_{\mathrm{GF}(q)}\},$$

$\exists$ a complex Hadamard matrix in its Bose–Mesner algebra.
$q = 4 \iff L(O_3)$.

For the previous family of association schemes, one has

Theorem

The matrix $H = I + \alpha_1 A_1 + \alpha_2 A_2 + \alpha_3 A_3$ is a complex Hadamard matrix if and only if

(i) H belongs to the subalgebra ($\alpha_1 = \alpha_3$) forming the Bose–Mesner algebra of a strongly regular graph (already done by Chan–Godsil),

(ii)
$$\alpha_1 + \frac{1}{\alpha_1} = -\frac{2}{q}, \quad \alpha_2 = \frac{1}{\alpha_1}, \quad \alpha_3 = 1,$$

(iii)
$$\alpha_1 + \frac{1}{\alpha_1} = \frac{(q-1)(q-2) - (q+2)r}{q},$$
where $r = \sqrt{(q-1)(17q-1)} > 0$.

The case (ii) with $q = 4$ was found by Chan.

Equivalence and decomposability

Two complex Hadamard matrices are said to be equivalent if one is obtained from the other by multiplication by monomial matrices. (We do not allow taking transposition or complex conjugation.)

The three families of complex Hadamard matrices obtained are

1. pairwise inequivalent?
2. decomposable into generalized tensor product?

We use Haagerup sets for the first, and Nomura algebras for the second.

The Haagerup set Haag(H) is

$$\mathrm{Haag}(H) = \{H_{i_1,j_1} H_{i_2,j_2} \overline{H_{i_1,j_2} H_{i_2,j_1}} \mid 1 \leq i_1, i_2, j_1, j_2 \leq n\}.$$

For a complex Hadamard matrix H, we define a vector Y_{j_1,j_2} whose i-th entry is given by

$$Y_{j_1,j_2}(i) = H_{i,j_1} \overline{H_{i,j_2}}$$

The Nomura algebra $N(H)$ is

$$N(H) = \{M \in \mathrm{Mat}_n(\mathbb{C}) \mid Y_{j_1,j_2} \text{ is an eigenvector of } M \text{ for all } j_1, j_2\}.$$

Both Haag(H) and $N(H)$ are invariant under equivalence.

(i) $\alpha_1 = \alpha_3$

(ii)

$$\alpha_1 + \frac{1}{\alpha_1} = -\frac{2}{q}, \quad \alpha_2 = \frac{1}{\alpha_1}, \quad \alpha_3 = 1,$$

(iii)

$$\alpha_1 + \frac{1}{\alpha_1} = \frac{(q-1)(q-2) - (q+2)r}{q},$$

where $r = \sqrt{(q-1)(17q-1)} > 0$.

Computing Haag(H), we see that the complex Hadamard matrices in (i), (ii) and (iii) are pairwise inequivalent.

Problem In each of the cases (i), (ii) and (iii), $H \cong \overline{H}$?

(i) $\alpha_1 = \alpha_3$

(ii)

$$\alpha_1 + \frac{1}{\alpha_1} = -\frac{2}{q}, \quad \alpha_2 = \frac{1}{\alpha_1}, \quad \alpha_3 = 1,$$

(iii)

$$\alpha_1 + \frac{1}{\alpha_1} = \frac{(q-1)(q-2) - (q+2)r}{q},$$

where $r = \sqrt{(q-1)(17q-1)} > 0$.

Computing $N(H)$, we see that the complex Hadamard matrices in (iii) are not equivalent to generalized tensor product.

$$\dim N(H) = 2 \implies N(H) \text{ primitive} \iff \text{not gen. tensor}$$

by Hosoya–Suzuki 2003.

Problems

- Equivalence of H and $\bar{H}$?
- Are there any other families?
- Are those complex Hadamard matrices belonging to a Bose–Mesner algebra isolated? Craigen 1991 showed that $\exists$ uncountably many inequivalent complex Hadamard matrices of composite order.

Thank you very much for your attention!

Happy birthday, Chris!