Butson-Hadamard matrices in association schemes of class 6 on Galois rings of characteristic 4

Akihiro Munemasa
Tohoku University
(joint work with Takuya Ikuta)

November 17, 2017
Combinatorics Seminar
Shanghai Jiao Tong University

Hadamard matrices and association schemes

- Goethals-Seidel (1970), regular symmetric Hadamard matrices with constant diagonal are equivalent to certain strongly regular graphs (symmetric association schemes of class 2).

From real ($HH^\top = nI$) to complex ($HH^* = nI$):

$$\begin{aligned} \text{real Hadamard } (\pm 1) &\subset \text{Butson-Hadamard (roots of unity)} \\ &\subset \text{Complex Hadamard (absolute value } 1) \\ &\subset \text{Inverse-orthogonal} = \text{type II} \end{aligned}$$

- Jaeger-Matsumoto-Nomura (1998): type II matrices
- Chan-Godsil (2010): complex Hadamard
- Ikuta-Munemasa (2015): complex Hadamard

Complex Hadamard matrices

An $n \times n$ matrix $H = (h_{ij})$ is called a complex Hadamard matrix if

$$HH^* = nI \text{ and } |h_{ij}| = 1 \quad (\forall i, j).$$

It is called a Butson-Hadamard matrix if all h_{ij} are roots of unity.
It is called a (real) Hadamard matrix if all h_{ij} are ± 1.
The 5th workshop on Real and Complex Hadamard Matrices and Applications, July, 2017, Budapest, aimed at

1. The Hadamard conjecture: a (real) Hadamard matrix exists for every order which is a multiple of 4 (yes for order ≤ 664).
2. Complete set of mutually unbiased bases (MUB) exists for non-prime power dimension? For example, 6.
3. Understand the space of complex Hadamard matrices of order 6.

Coherent Algebras and Coherent Configuration

Let G be a finite permutation group acting on a finite set X. From the set of orbits of $X \times X$, one defines adjacency matrices

$$A_0, A_1, \ldots, A_d \text{ with } \sum_{i=0}^{d} A_i = J \text{ (all-one matrix).}$$

Then the linear span $\langle A_0, A_1, \ldots, A_d \rangle$ is closed under multiplication and transposition ($\longrightarrow$ coherent algebra, coherent configuration).

If G acts transitively, we may assume $A_0 = I$ ($\longrightarrow$ Bose-Mesner algebra of an association scheme).

If G contains a regular subgroup N, we may identify X with N, $A_i \leftrightarrow T_i \subseteq N$, and

$$N = \bigcup_{i=0}^{d} T_i,\ T_0 = \{1_N\}, \quad \mathbb{C}[N] \supseteq \langle \sum_{g \in T_i} g \mid 0 \leq i \leq d \rangle.$$

Schur rings

$$N = \bigcup_{i=0}^{d} T_i, \quad T_0 = \{1_N\},$$

$$\mathbb{C}[N] \supseteq \mathcal{A} = \langle \sum_{g \in T_i} g \mid 0 \le i \le d \rangle \quad \text{(subalgebra)}.$$

$\mathcal{A}$ is called a Schur ring if, in addition

$$\{T_i^{-1} \mid 0 \le i \le d\} = \{T_i \mid 0 \le i \le d\},$$

where

$$T^{-1} = \{t^{-1} \mid t \in T\} \quad \text{for } T \subseteq N.$$

Examples: $AGL(1,q) > G > N = GF(q)$ (cyclotomic).

$AGL(1,q) > G > N = GF(q)$ (cyclotomic)

More generally,

$$R : R^\times > G > N = R : \text{ a ring.}$$

In Ito-Munemasa-Yamada (1991), we wanted to construct an association scheme with eigenvalue a multiple of $i = \sqrt{-1}$. Not possible with $R = GF(q)$.

$$\begin{array}{rcl} GF(p) & \hookrightarrow & GF(p^e) \\ \mathbb{Z}_{p^n} & \hookrightarrow & GR(p^n, e) \end{array}$$

A Galois ring $R = GR(p^n, e)$ is a commutative local ring with characteristic p^n, whose quotient by the maximal ideal pR is $GF(p^e)$.

Structure of $GR(p^n, e)$

Let $R = GR(p^n, e)$ be a Galois ring. Then

$$\begin{aligned} |R| &= p^{ne}, \\ pR &\text{ is the unique maximal ideal,} \\ |R^\times| = |R \setminus pR| &= p^{ne} - p^{(n-1)e} = (p^e - 1)p^{(n-1)e}, \\ R^\times = \mathcal{T} \times \mathcal{U}, &\quad \mathcal{T} \cong \mathbb{Z}_{p^e-1}, \quad |\mathcal{U}| = p^{(n-1)e}. \end{aligned}$$

Now specialize $p^n = 4$, consider $GR(4, e)$.

Structure of $GR(4, e)$

Let $R = GR(4, e)$ be a Galois ring of characteristic 4. Then

$$\begin{aligned} |R| &= 4^e, \\ 2R &\text{ is the unique maximal ideal}, \\ |R^\times| &= |R \setminus 2R| = 4^e - 2^e = (2^e - 1)2^e, \\ R^\times &= \mathcal{T} \times \mathcal{U}, \quad \mathcal{T} \cong \mathbb{Z}_{2^e-1}, \\ \mathcal{U} &= 1 + 2R \cong \mathbb{Z}_2^e. \end{aligned}$$

To construct a Schur ring, we need to partition

$$R = R^\times \cup 2R$$

(into even smaller parts). In Ito-Munemasa-Yamada (1991), the orbits of a subgroup of the form $\mathcal{T} \times \mathcal{U}_0 < R^\times$ were used. Ma (2007) also considered orbits of a subgroup containing $\mathcal{T}$.

$\mathcal{U}_0$ as a subgroup of $\mathcal{U}$ of index 2

$$R = GR(4,e),$$

$2R$ is the unique maximal ideal,

$$R^\times = \mathcal{T} \times \mathcal{U}, \quad \mathcal{T} \cong \mathbb{Z}_{2^e-1},$$

$$\mathcal{U} = 1 + 2R \cong \mathbb{Z}_2^e \quad \text{the principal unit group.}$$

There is a bijection

$$\begin{aligned} GF(2^e) = R/2R \leftarrow \mathcal{T} \cup \{0\} &\to 2R \to \mathcal{U}, \\ a + 2R \leftarrow\!\shortmid a \qquad &\mapsto 2a \mapsto 1 + 2a. \end{aligned}$$

So the "trace-0" additive subgroup of $GF(2^e)$ is mapped to $\mathcal{P}_0$ and $\mathcal{U}_0$ with $|2R : \mathcal{P}_0| = |\mathcal{U} : \mathcal{U}_0| = 2$.
Assume e is odd. Then $1 \notin$ "trace-0" subgroup, so $2 \notin \mathcal{P}_0$ and $-1 = 3 \notin \mathcal{U}_0$.

Partition of $R = GR(4, e)$

Assume e is odd. Then $\mathbf{2} \notin \mathcal{P}_0$, $\mathbf{-1} \notin \mathcal{U}_0$.

$$R^\times = \mathcal{T} \times \mathcal{U}, \quad \mathcal{T} \cong \mathbb{Z}_{2^e-1},$$
$$2R = \mathcal{P}_0 \cup (2 + \mathcal{P}_0),$$
$$\mathcal{U} = \mathcal{U}_0 \cup (-\mathcal{U}_0).$$

Then $\mathcal{U}_0$ acts on R, and the orbit decomposition is

$$R = \left(\bigcup_{t \in \mathcal{T}} t\mathcal{U}_0 \cup (-t\mathcal{U}_0) \right) \cup \left(\bigcup_{a \in 2R} \{a\} \right)$$
$$= \mathcal{U}_0 \cup (-\mathcal{U}_0) \cup \left(\bigcup_{t \in \mathcal{T} \setminus \{1\}} t\mathcal{U}_0 \right) \cup \left(\bigcup_{t \in \mathcal{T} \setminus \{1\}} (-t\mathcal{U}_0) \right)$$
$$\cup \{0\} \cup (\mathcal{P}_0 \setminus \{0\}) \cup (2 + \mathcal{P}_0).$$

$R \setminus \{0\}$ is partitioned into 6 parts

$$\begin{aligned} T_0 &= \{0\}, \\ T_1 &= \bigcup_{t \in \mathcal{T} \setminus \{1\}} t\mathcal{U}_0, \\ T_2 &= \bigcup_{t \in \mathcal{T} \setminus \{1\}} (-t\mathcal{U}_0), \end{aligned} \qquad \begin{aligned} T_3 &= \mathcal{U}_0, \\ T_4 &= -\mathcal{U}_0, \\ T_5 &= \mathcal{P}_0 \setminus \{0\}, \\ T_6 &= 2 + \mathcal{P}_0. \end{aligned}$$

Theorem (Ikuta-M., 2017+)

1. $\{T_0, T_1, \ldots, T_6\}$ *defines a Schur ring on* $GR(4, e)$,
2. *The matrices*

$$A_0 + \epsilon_1 i(A_1 - A_2) + \epsilon_2 i(A_3 - A_4) + A_5 + A_6,$$
$$A_0 + \epsilon_1 i(A_1 - A_2) + \epsilon_2 (A_3 + A_4) + A_5 - A_6$$

are the only hermitian complex Hadamard matrices in its Bose-Mesner algebra, where $\epsilon_1, \epsilon_2 \in \{\pm 1\}$.

Proof

$$T_0 = \{0\},$$
$$T_1 = \bigcup_{t\in\mathcal{T}\setminus\{1\}} t\mathcal{U}_0,$$
$$T_2 = \bigcup_{t\in\mathcal{T}\setminus\{1\}}(-t\mathcal{U}_0),$$
$$T_3 = \mathcal{U}_0,$$
$$T_4 = -\mathcal{U}_0,$$
$$T_5 = \mathcal{P}_0 \setminus \{0\},$$
$$T_6 = 2 + \mathcal{P}_0.$$

Theorem (Ikuta-M., 2017+)

1. $\{T_0, T_1, \ldots, T_6\}$ *defines a Schur ring on* $GR(4, e)$.

Proof.

Compute the character sums ($\chi = \chi_b$: additive character of R)

$$\sum_{\alpha\in T_j} \chi(a) = \sum_{\alpha\in T_j} \sqrt{-1}^{\mathrm{tr}(ab)} \quad (b \in T_i),$$

show that this is independent of $b \in T_i$, depends only on i. □

Proof

Theorem (Ikuta-M., 2017+)

2. *The matrices*
   $A_0 + \epsilon_1 i(A_1 - A_2) + \epsilon_2 i(A_3 - A_4) + A_5 + A_6$,
   $A_0 + \epsilon_1 i(A_1 - A_2) + \epsilon_2 (A_3 + A_4) + A_5 - A_6$
   are the only hermitian complex Hadamard matrices in its Bose-Mesner algebra, where $\epsilon_1, \epsilon_2 \in \{\pm 1\}$.

Proof.

Suppose $H = \sum_{i=0}^{6} w_i A_i$ is a hermitian complex Hadamard matrix. Since the Bose-Mesner algebra is isomorphic to a subalgebra of the group ring of R, the relation $HH^* = nI$ can be translated in terms of additive characters of R. Then one obtains a system of quadratic equations in w_i's. □

Example

$$H = A_0 + i(A_1 + A_3) - i(A_2 + A_4) + (A_5 + A_6)$$
$$\in \langle A_0, A_1 + A_3, A_2 + A_4, A_5 + A_6 \rangle.$$

Smaller Schur ring defined by

$$T_0 = \{0\},$$
$$T_1 \cup T_3 = \bigcup_{t \in \mathcal{T}} t\mathcal{U}_0,$$
$$T_2 \cup T_4 = \bigcup_{t \in \mathcal{T}} (-t\mathcal{U}_0),$$
$$T_5 \cup T_6 = 2R \setminus \{0\}.$$

This defines a nonsymmetric amorphous association scheme of Latin square type $L_{2^e,1}(2^e)$ in the sense of Ito-Munemasa-Yamada (1991).

Theorem (Ikuta-M. (2017+))

Let

$$A_0 + w_1 A_1 + \overline{w_1} A_1^\top + w_3 A_3$$

be a hermitian complex Hadamard matrix contained in the Bose-Mesner algebra $\mathcal{A} = \langle A_0, A_1, A_2 = A_1^\top, A_3 \rangle$ *of a* 3*-class nonsymmetric association scheme. Then* $\mathcal{A}$ *is amorphous of Latin square type* $L_{a,1}(a)$*, and* $w_1 = \pm i$*,* $w_3 = 1$*.*

This can be regarded as a nonsymmetric analogue of

Theorem (Goethals-Seidel (1970))

Let

$$H = A_0 + A_1 - A_2$$

be a (real) Hadamard matrix contained in the Bose-Mesner algebra $\mathcal{A} = \langle A_0, A_1, A_2 \rangle$ *of a* 2*-class symmetric association scheme. Then* $\mathcal{A}$ *is (amorphous) of Latin or negative Latin square type.*