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

Akihiro Munemasa
Tohoku University
(joint work with Takuya Ikuta)

July 17, 2017
Workshop on Group Theory
and Algebraic Combinatorics
Novosibirsk State University

About this talk

Coherent Configuration	$\leftarrow$	Permutation Group
Association Scheme	$\leftarrow$	Transitive Permutation Group
Schur Ring	$\leftarrow$	Transitive Permutation Group with Regular Subgroup

- This is a continuation of my talk

  "Amorphous association schemes over Galois rings of characteristic 4"

  at Vladimir, Russia in August 1991.
- Common theme: Construction of an association scheme from Galois rings of characteristic 4, in terms of a Schur ring.
- Related work: Evdokimov-Ponomarenko: Schur rings over a Galois ring

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, 10–14 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?

Mutually unbiased bases

Given a positive integer n, does there exist complex Hadamard matrices $H_1, \dots, H_n$ of order n such that

$$\frac{1}{\sqrt{n}} H_i H_j^*$$

is a complex Hadamard matrix for all $i \neq j$?
Yes for $n =$ prime power. Unknown for all other n.
An equivalent problem is orthogonal decomposition of the Lie algebra $\mathfrak{sl}(n, \mathbb{C})$ by Cartan subalgebras, as formulated independently by Kostrikin-Kostrikin-Ufnarowskii (1981).

Hadamard matrices and association schemes

For real Hadamard matrices:

- Goethals-Seidel (1970), regular symmetric Hadamard matrices with constant diagonal are equivalent to certain strongly regular graphs (symmetric association schemes of class $\mathbf{2}$).
- Delsarte (1973), skew Hadamard matrices are equivalent to nonsymmetric association schemes of class $\mathbf{2}$.

For complex Hadamard matrices (or more generally "inverse-orthogonal", or "Type II" matrices),

- Jaeger-Matsumoto-Nomura (1998)
- Chan-Godsil (2010)
- Ikuta-Munemasa (2015)

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 H, we may identify X with H, $A_i \leftrightarrow T_i \subseteq H$, and

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

Schur rings

$$H = \bigcup_{i=0}^{d} T_i, \quad T_0 = \{1_H\},$$

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

$\mathcal{A}$ 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

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

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

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

More generally,

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

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

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

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

$$|R| = p^{ne},$$

pR is the unique maximal ideal,

$$|R^\times| = |R \setminus pR| = p^{ne} - p^{(n-1)e} = (p^e - 1)p^{(n-1)e},$$

$$R^\times = \mathcal{T} \times \mathcal{U}, \quad \mathcal{T} \cong \mathbb{Z}_{p^e-1}, \quad |\mathcal{U}| = p^{(n-1)e}.$$

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.

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

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

There is a bijection

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

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 $\mathbf{2} \notin \mathcal{P}_0$, $\mathbf{-1} \notin \mathcal{U}_0$.

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

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

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

$R \setminus \{0\}$ 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. $\{T_0, T_1, \dots, T_6\}$ *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 $\epsilon_1, \epsilon_2 \in \{\pm 1\}$.

Example

$$
\begin{aligned}
H &= A_0 + i(A_1 + A_3) - i(A_2 + A_4) + (A_5 + A_6) \\
&\in \langle A_0, A_1 + A_3, A_2 + A_4, A_5 + A_6 \rangle.
\end{aligned}
$$

Smaller Schur ring defined by

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

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.*