

Happy 25+75=100



Generalized Hadamard matrices and applications

H. Kharaghani

University of Lethbridge
Canada

The First IPM-Isfahan Workshop on Combinatorics

University of Isfahan

May 20-22, 2014

▶ Difference matrices

- ▶ Difference matrices
- ▶ Generalized Hadamard (GH) matrices

- ▶ Difference matrices
- ▶ Generalized Hadamard (GH) matrices
- ▶ Existence and examples

- ▶ Difference matrices
- ▶ Generalized Hadamard (GH) matrices
- ▶ Existence and examples
- ▶ The auxiliary matrices corresponding to GH matrices

- ▶ Difference matrices
- ▶ Generalized Hadamard (GH) matrices
- ▶ Existence and examples
- ▶ The auxiliary matrices corresponding to GH matrices
- ▶ **Association Schemes**

- ▶ Difference matrices
- ▶ Generalized Hadamard (GH) matrices
- ▶ Existence and examples
- ▶ The auxiliary matrices corresponding to GH matrices
- ▶ Association Schemes
- ▶ Some application of GH matrices

Difference matrices

Difference matrices

Let (G, \odot) be a group of order g .

Difference matrices

Let (G, \odot) be a group of order g . A $(g, k; \lambda)$ -*difference matrix* over (G, \odot) is a $k \times g$ matrix $D = (d_{ij})$

Difference matrices

Let (G, \odot) be a group of order g . A $(g, k; \lambda)$ -*difference matrix* over (G, \odot) is a $k \times g$ matrix $D = (d_{ij})$ with entries from G ,

Difference matrices

Let (G, \odot) be a group of order g . A $(g, k; \lambda)$ -*difference matrix* over (G, \odot) is a $k \times g\lambda$ matrix $D = (d_{ij})$ with entries from G , so that for each $1 \leq i < j \leq k$, the multiset

$$\{d_{i\ell} \odot d_{j\ell}^{-1} : 1 \leq \ell \leq g\lambda\}$$

Difference matrices

Let (G, \odot) be a group of order g . A $(g, k; \lambda)$ -*difference matrix* over (G, \odot) is a $k \times g\lambda$ matrix $D = (d_{ij})$ with entries from G , so that for each $1 \leq i < j \leq k$, the multiset

$$\{d_{i\ell} \odot d_{j\ell}^{-1} : 1 \leq \ell \leq g\lambda\}$$

(the *difference list*) contains every element of G λ times.

Difference matrices

Let (G, \odot) be a group of order g . A $(g, k; \lambda)$ -*difference matrix* over (G, \odot) is a $k \times g\lambda$ matrix $D = (d_{ij})$ with entries from G , so that for each $1 \leq i < j \leq k$, the multiset

$$\{d_{i\ell} \odot d_{j\ell}^{-1} : 1 \leq \ell \leq g\lambda\}$$

(the *difference list*) contains every element of G λ times.

Example: A $(3, 6; 2)$ -difference matrix over $(\mathbb{Z}_3, +)$

Difference matrices

Let (G, \odot) be a group of order g . A $(g, k; \lambda)$ -*difference matrix* over (G, \odot) is a $k \times g\lambda$ matrix $D = (d_{ij})$ with entries from G , so that for each $1 \leq i < j \leq k$, the multiset

$$\{d_{i\ell} \odot d_{j\ell}^{-1} : 1 \leq \ell \leq g\lambda\}$$

(the *difference list*) contains every element of G λ times.

Example: A $(3, 6; 2)$ -difference matrix over $(\mathbb{Z}_3, +)$

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 2 & 0 & 1 \\ 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 2 & 2 & 0 & 1 & 1 \\ 2 & 2 & 0 & 1 & 1 & 0 \\ 2 & 0 & 2 & 1 & 0 & 1 \end{pmatrix}$$

Example:

A $(5, 5; 1)$ -difference matrix over $(\mathbb{Z}_5, +)$

Example:

A $(5, 5; 1)$ -difference matrix over $(\mathbb{Z}_5, +)$

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 0 & 3 & 1 & 4 & 2 \\ 0 & 4 & 3 & 2 & 1 \end{pmatrix}$$

Example:

A $(5, 5; 1)$ -difference matrix over $(\mathbb{Z}_5, +)$

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 0 & 3 & 1 & 4 & 2 \\ 0 & 4 & 3 & 2 & 1 \end{pmatrix}$$

A $(5, 5; 1)$ -difference matrix over (\mathbb{Z}_5, \times)

Example:

A $(5, 5; 1)$ -difference matrix over $(\mathbb{Z}_5, +)$

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 0 & 3 & 1 & 4 & 2 \\ 0 & 4 & 3 & 2 & 1 \end{pmatrix}$$

A $(5, 5; 1)$ -difference matrix over (\mathbb{Z}_5, \times)

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}$$

A $(15, 5; 1)$ -difference matrix over $(\mathbb{Z}_{15}, +)$:

$$\text{Take } B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 9 & 12 & 4 & 1 \\ 6 & 3 & 14 & 10 & 7 & 13 & 4 \\ 10 & 6 & 1 & 11 & 2 & 7 & 12 \end{pmatrix},$$

A $(15, 5; 1)$ -difference matrix over $(\mathbb{Z}_{15}, +)$:

$$\text{Take } B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 9 & 12 & 4 & 1 \\ 6 & 3 & 14 & 10 & 7 & 13 & 4 \\ 10 & 6 & 1 & 11 & 2 & 7 & 12 \end{pmatrix},$$

Let $C = \begin{pmatrix} 0 & B & -B \end{pmatrix}$.

A $(15, 5; 1)$ -difference matrix over $(\mathbb{Z}_{15}, +)$:

$$\text{Take } B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 9 & 12 & 4 & 1 \\ 6 & 3 & 14 & 10 & 7 & 13 & 4 \\ 10 & 6 & 1 & 11 & 2 & 7 & 12 \end{pmatrix},$$

Let $C = \begin{pmatrix} 0 & B & -B \end{pmatrix}$.

A $(4, 4; 1)$ -difference matrix over $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

A $(15, 5; 1)$ -difference matrix over $(\mathbb{Z}_{15}, +)$:

$$\text{Take } B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 9 & 12 & 4 & 1 \\ 6 & 3 & 14 & 10 & 7 & 13 & 4 \\ 10 & 6 & 1 & 11 & 2 & 7 & 12 \end{pmatrix},$$

Let $C = \begin{pmatrix} 0 & B & -B \end{pmatrix}$.

A $(4, 4; 1)$ -difference matrix over $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

$$B = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \end{pmatrix},$$

where $2 + 3 = 1$.

A necessary condition for the existence:

A $(g, k; \lambda)$ -difference matrix does not exist if $k > \lambda g$.

A necessary condition for the existence:

A $(g, k; \lambda)$ -difference matrix does not exist if $k > \lambda g$.

Existence:

A necessary condition for the existence:

A $(g, k; \lambda)$ -difference matrix does not exist if $k > \lambda g$.

Existence: The multiplication table for the finite field $\mathbf{GF}(q)$ is a $(q, q; 1)$ -difference matrix over $\mathbf{EA}(q)$,

A necessary condition for the existence:

A $(g, k; \lambda)$ -difference matrix does not exist if $k > \lambda g$.

Existence: The multiplication table for the finite field $\mathbf{GF}(q)$ is a $(q, q; 1)$ -difference matrix over $EA(q)$, where $EA(q)$ denote the order q direct product of prime order cyclic groups.

A necessary condition for the existence:

A $(g, k; \lambda)$ -difference matrix does not exist if $k > \lambda g$.

Existence: The multiplication table for the finite field $\mathbf{GF}(q)$ is a $(q, q; 1)$ -difference matrix over $EA(q)$, where $EA(q)$ denote the order q direct product of prime order cyclic groups.

Conjecture: There is no $(q, q; 1)$ -difference matrix for any non-prime power q .

Auxiliary matrices corresponding to difference matrices:

Let (G, \odot) be a group of order g

Auxiliary matrices corresponding to difference matrices:

Let (G, \odot) be a group of order g and D a normalized $(g, k; \lambda)$ -difference matrix over (G, \odot) .

Auxiliary matrices corresponding to difference matrices:

Let (G, \odot) be a group of order g and D a normalized $(g, k; \lambda)$ -difference matrix over (G, \odot) . Let $r_i, i = 1, 2, \dots, k$ be the i -th row of D .

Auxiliary matrices corresponding to difference matrices:

Let (G, \odot) be a group of order g and D a normalized $(g, k; \lambda)$ -difference matrix over (G, \odot) . Let $r_i, i = 1, 2, \dots, k$ be the i -th row of D .

Let $C_i = r_i^* r_i, i = 1, 2, \dots, k$.

Auxiliary matrices corresponding to difference matrices:

Let (G, \odot) be a group of order g and D a normalized $(g, k; \lambda)$ -difference matrix over (G, \odot) . Let $r_i, i = 1, 2, \dots, k$ be the i -th row of D .

Let $C_i = r_i^* r_i, i = 1, 2, \dots, k$.

Example: Let $D_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$. Then,

Auxiliary matrices corresponding to difference matrices:

Let (G, \odot) be a group of order g and D a normalized $(g, k; \lambda)$ -difference matrix over (G, \odot) . Let $r_i, i = 1, 2, \dots, k$ be the i -th row of D .

Let $C_i = r_i^* r_i, i = 1, 2, \dots, k$.

Example: Let $D_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$. Then,

$$C_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

Auxiliary matrices corresponding to difference matrices:

Let (G, \odot) be a group of order g and D a normalized $(g, k; \lambda)$ -difference matrix over (G, \odot) . Let $r_i, i = 1, 2, \dots, k$ be the i -th row of D .

Let $C_i = r_i^* r_i, i = 1, 2, \dots, k$.

Example: Let $D_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$. Then,

$$C_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, C_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix},$$

Auxiliary matrices corresponding to difference matrices:

Let (G, \odot) be a group of order g and D a normalized $(g, k; \lambda)$ -difference matrix over (G, \odot) . Let $r_i, i = 1, 2, \dots, k$ be the i -th row of D .

Let $C_i = r_i^* r_i, i = 1, 2, \dots, k$.

Example: Let $D_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$. Then,

$$C_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, C_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}, \text{ and } C_3 = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}.$$

Mutually Suitable Latin Squares

Mutually Suitable Latin Squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0, 1, 2, \dots, n-1\}$

Mutually Suitable Latin Squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0, 1, 2, \dots, n-1\}$ are called *suitable*

Mutually Suitable Latin Squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0, 1, 2, \dots, n-1\}$ are called *suitable* if every superimposition of each row of L_1 on each row of L_2 results in only one element of the form (a, a) .

Mutually Suitable Latin Squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0, 1, 2, \dots, n-1\}$ are called *suitable* if every superimposition of each row of L_1 on each row of L_2 results in only one element of the form (a, a) .

Example:

Mutually Suitable Latin Squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0, 1, 2, \dots, n-1\}$ are called *suitable* if every superimposition of each row of L_1 on each row of L_2 results in only one element of the form (a, a) .

Example: Two mutually suitable Latin squares of size 3:

$$\begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

Mutually Suitable Latin Squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0, 1, 2, \dots, n-1\}$ are called *suitable* if every superimposition of each row of L_1 on each row of L_2 results in only one element of the form (a, a) .

Example: Two mutually suitable Latin squares of size 3:

$$\begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$

Mutually Suitable Latin Squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0, 1, 2, \dots, n-1\}$ are called *suitable* if every superimposition of each row of L_1 on each row of L_2 results in only one element of the form (a, a) .

Example: Two mutually suitable Latin squares of size 3:

$$\begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$

If there is a $(g, k; 1)$ -difference matrix, then there is a set of $k-1$ Mutually Suitable Latin Squares of size g .

Generalized Hadamard matrices

Generalized Hadamard matrices

A $(g, g\lambda; \lambda)$ -difference matrix over the group G is said to be a *generalized Hadamard matrix*, over the group G , denoted $\text{GH}(g, \lambda)$.

Generalized Hadamard matrices

A $(g, g\lambda; \lambda)$ -difference matrix over the group G is said to be a *generalized Hadamard matrix*, over the group G , denoted $\text{GH}(g, \lambda)$.

Example: A $\text{GH}(3, 2)$ generalized Hadamard matrix over the cyclic group \mathbb{Z}_3

Generalized Hadamard matrices

A $(g, g\lambda; \lambda)$ -difference matrix over the group G is said to be a *generalized Hadamard matrix*, over the group G , denoted $\text{GH}(g, \lambda)$.

Example: A $\text{GH}(3, 2)$ generalized Hadamard matrix over the cyclic group \mathbb{Z}_3

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\ \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ 1 & \omega^2 & \omega^2 & 1 & \omega & \omega \\ \omega^2 & \omega^2 & 1 & \omega & \omega & 1 \\ \omega^2 & 1 & \omega^2 & \omega & 1 & \omega \end{pmatrix}$$

Example: A *normalized* $\text{GH}(4, 1)$ over $\mathbb{Z}_2 \times \mathbb{Z}_2$

Example: A *normalized* GH(4, 1) over $\mathbb{Z}_2 \times \mathbb{Z}_2$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & c & a & b \\ 1 & b & c & a \\ 1 & a & b & c \end{pmatrix}$$

Example: A *normalized* $\text{GH}(4, 1)$ over $\mathbb{Z}_2 \times \mathbb{Z}_2$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & c & a & b \\ 1 & b & c & a \\ 1 & a & b & c \end{pmatrix}$$

$$c = ab.$$

Example: A *normalized* $\text{GH}(4, 1)$ over $\mathbb{Z}_2 \times \mathbb{Z}_2$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & c & a & b \\ 1 & b & c & a \\ 1 & a & b & c \end{pmatrix}$$

$$c = ab.$$

Existence of generalized Hadamard matrices

Existence of generalized Hadamard matrices

The multiplication table for the finite field $\mathbf{GF}(q)$ is a $(q, q; 1)$ -difference matrix

Existence of generalized Hadamard matrices

The multiplication table for the finite field $\mathbf{GF}(q)$ is a $(q, q; 1)$ -difference matrix and so a generalized Hadamard matrix over $\mathbf{EA}(q)$.

Existence of generalized Hadamard matrices

The multiplication table for the finite field $\mathbf{GF}(q)$ is a $(q, q; 1)$ -difference matrix and so a generalized Hadamard matrix over $EA(q)$.

For any Group G of prime power order q and any integer $t > 0$, there is a $\text{GH}(q, q^{2^t-1})$.

An application

An application

Consider the normalized $\text{GH}(4, 1) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & c & a & b \\ 1 & b & c & a \\ 1 & a & b & c \end{pmatrix}$, $c = ab$, over $\mathbb{Z}_2 \times \mathbb{Z}_2$.

An application

Consider the normalized $\text{GH}(4, 1) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & c & a & b \\ 1 & b & c & a \\ 1 & a & b & c \end{pmatrix}$, $c = ab$, over

$\mathbb{Z}_2 \times \mathbb{Z}_2$.

Let

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

An application

Consider the normalized $\text{GH}(4, 1) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & c & a & b \\ 1 & b & c & a \\ 1 & a & b & c \end{pmatrix}$, $c = ab$, over

$\mathbb{Z}_2 \times \mathbb{Z}_2$.

Let

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & c & a & b \\ 1 & c & -a & -b \\ 1 & -c & a & -b \\ 1 & -c & -a & b \end{pmatrix}$$

An application

Consider the normalized $\text{GH}(4, 1) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & c & a & b \\ 1 & b & c & a \\ 1 & a & b & c \end{pmatrix}$, $c = ab$, over

$\mathbb{Z}_2 \times \mathbb{Z}_2$.

Let

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & c & a & b \\ 1 & c & -a & -b \\ 1 & -c & a & -b \\ 1 & -c & -a & b \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & b & c & a \\ 1 & b & -c & -a \\ 1 & -b & c & -a \\ 1 & -b & -c & a \end{pmatrix}$$

An application

Consider the normalized $\text{GH}(4, 1) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & c & a & b \\ 1 & b & c & a \\ 1 & a & b & c \end{pmatrix}$, $c = ab$, over

$\mathbb{Z}_2 \times \mathbb{Z}_2$.

Let

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & c & a & b \\ 1 & c & -a & -b \\ 1 & -c & a & -b \\ 1 & -c & -a & b \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & b & c & a \\ 1 & b & -c & -a \\ 1 & -b & c & -a \\ 1 & -b & -c & a \end{pmatrix} \quad D = \begin{pmatrix} 1 & a & b & c \\ 1 & a & -b & -c \\ 1 & -a & b & -c \\ 1 & -a & -b & c \end{pmatrix}$$

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $l = i \otimes i$,

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $l = i \otimes i$, $a = i \otimes r$,

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $l = i \otimes i$, $a = i \otimes r$, $b = r \otimes i$,

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $l = i \otimes i$, $a = i \otimes r$, $b = r \otimes i$, and $c = ab = r \otimes r$.

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $l = i \otimes i$, $a = i \otimes r$, $b = r \otimes i$, and $c = ab = r \otimes r$. Then

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $l = i \otimes i$, $a = i \otimes r$, $b = r \otimes i$, and $c = ab = r \otimes r$. Then

$$l = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $l = i \otimes i$, $a = i \otimes r$, $b = r \otimes i$, and $c = ab = r \otimes r$. Then

$$l = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $l = i \otimes i$, $a = i \otimes r$, $b = r \otimes i$, and $c = ab = r \otimes r$. Then

$$l = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $l = i \otimes i$, $a = i \otimes r$, $b = r \otimes i$, and $c = ab = r \otimes r$. Then

$$l = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad c = ab = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $l = i \otimes i$, $a = i \otimes r$, $b = r \otimes i$, and $c = ab = r \otimes r$. Then

$$l = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad c = ab = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Note $l + a + b + c = J$, J is the 4×4 matrix of all ones.

The following holds:

The following holds:

▶ $XX^t = 4I_{16}$, $X \in \{A, B, C, D\}$.

The following holds:

- ▶ $XX^t = 4I_{16}$, $X \in \{A, B, C, D\}$.
- ▶ $H_{XY} = XY^t$ is a **Bush-type Hadamard matrix** of order 16,
 $X \neq Y \in \{A, B, C, D\}$

The following holds:

- ▶ $XX^t = 4I_{16}$, $X \in \{A, B, C, D\}$.
- ▶ $H_{XY} = XY^t$ is a **Bush-type Hadamard matrix** of order 16, $X \neq Y \in \{A, B, C, D\}$ (the 4×4 diagonal blocks are all ones matrices and off-diagonal blocks have zero row and column sums).

The following holds:

- ▶ $XX^t = 4I_{16}$, $X \in \{A, B, C, D\}$.
- ▶ $H_{XY} = XY^t$ is a **Bush-type Hadamard matrix** of order 16, $X \neq Y \in \{A, B, C, D\}$ (the 4×4 diagonal blocks are all ones matrices and off-diagonal blocks have zero row and column sums).
- ▶ Let

$$O = \begin{pmatrix} d & e & f & g \\ -e & d & -g & f \\ -f & g & d & -e \\ -g & -f & e & d \end{pmatrix}.$$

The following holds:

- ▶ $XX^t = 4I_{16}$, $X \in \{A, B, C, D\}$.
- ▶ $H_{XY} = XY^t$ is a **Bush-type Hadamard matrix** of order 16, $X \neq Y \in \{A, B, C, D\}$ (the 4×4 diagonal blocks are all ones matrices and off-diagonal blocks have zero row and column sums).
- ▶ Let

$$O = \begin{pmatrix} d & e & f & g \\ -e & d & -g & f \\ -f & g & d & -e \\ -g & -f & e & d \end{pmatrix}.$$

Let $A' = A \otimes O$, $B' = B \otimes O$, $C' = C \otimes O$, $D' = D \otimes O$.

The following holds:

- ▶ $XX^t = 4I_{16}$, $X \in \{A, B, C, D\}$.
- ▶ $H_{XY} = XY^t$ is a **Bush-type Hadamard matrix** of order 16, $X \neq Y \in \{A, B, C, D\}$ (the 4×4 diagonal blocks are all ones matrices and off-diagonal blocks have zero row and column sums).
- ▶ Let

$$O = \begin{pmatrix} d & e & f & g \\ -e & d & -g & f \\ -f & g & d & -e \\ -g & -f & e & d \end{pmatrix}.$$

Let $A' = A \otimes O$, $B' = B \otimes O$, $C' = C \otimes O$, $D' = D \otimes O$. Then

$$XY^t = (d^2 + e^2 + f^2 + g^2)H_{XY},$$

$X \neq Y \in \{A', B', C', D'\}$, d, e, f, g commuting indeterminates.

The following holds:

- ▶ $XX^t = 4I_{16}$, $X \in \{A, B, C, D\}$.
- ▶ $H_{XY} = XY^t$ is a **Bush-type Hadamard matrix** of order 16, $X \neq Y \in \{A, B, C, D\}$ (the 4×4 diagonal blocks are all ones matrices and off-diagonal blocks have zero row and column sums).
- ▶ Let

$$O = \begin{pmatrix} d & e & f & g \\ -e & d & -g & f \\ -f & g & d & -e \\ -g & -f & e & d \end{pmatrix}.$$

Let $A' = A \otimes O$, $B' = B \otimes O$, $C' = C \otimes O$, $D' = D \otimes O$. Then

$$XY^t = (d^2 + e^2 + f^2 + g^2)H_{XY},$$

$X \neq Y \in \{A', B', C', D'\}$, d, e, f, g commuting indeterminates.
 $\{A', B', C', D'\}'$ forms a set of **mutually unbiased orthogonal designs**.

The following holds:

- ▶ $XX^t = 4I_{16}$, $X \in \{A, B, C, D\}$.
- ▶ $H_{XY} = XY^t$ is a **Bush-type Hadamard matrix** of order 16, $X \neq Y \in \{A, B, C, D\}$ (the 4×4 diagonal blocks are all ones matrices and off-diagonal blocks have zero row and column sums).
- ▶ Let

$$O = \begin{pmatrix} d & e & f & g \\ -e & d & -g & f \\ -f & g & d & -e \\ -g & -f & e & d \end{pmatrix}.$$

Let $A' = A \otimes O$, $B' = B \otimes O$, $C' = C \otimes O$, $D' = D \otimes O$. Then

$$XY^t = (d^2 + e^2 + f^2 + g^2)H_{XY},$$

$X \neq Y \in \{A', B', C', D'\}$, d, e, f, g commuting indeterminates.
 $\{A', B', C', D'\}'$ forms a set of **mutually unbiased orthogonal designs**.



COMBINATORICS II

Mathematical Combinatorics

INSTITUTE FOR STUDIES IN THEORETICAL PHYSICS AND MATHEMATICS

April 20, 2018

پژوهشگاه مطالعات
فیزیک و ریاضیات



NAUTY



The Institute for Studies in Theoretical Physics and Mathematics (IPM) is a research center in Tehran, Iran, dedicated to the study of theoretical physics and mathematics. It was established in 1974 and is currently headed by Professor Amir H. Jazayerni. The institute has a long history of research and has produced many notable scientists and mathematicians. It is a member of the International Centre for Theoretical Physics (ICTP) and the International Union of Pure and Applied Chemistry (IUPAC). The institute's research is primarily in the areas of quantum field theory, string theory, and mathematical physics. It also has a strong focus on the application of mathematics to physics. The institute's website is www.ipm.ir.

1527

Handwritten mathematical notes on a whiteboard, including the letters 'G' and 'H'.



Summary:

- ▶ Let (G, \odot) be a group of order g .

Summary:

- ▶ Let (G, \odot) be a group of order g . A *generalized Hadamard matrix* over G , or $GH(g, \lambda)$,

Summary:

- ▶ Let (G, \odot) be a group of order g . A *generalized Hadamard matrix* over G , or $GH(g, \lambda)$, is a matrix $H = [\omega_{ij}]$ of order $v = g\lambda$ with entries from the group G

Summary:

- ▶ Let (G, \odot) be a group of order g . A *generalized Hadamard matrix* over G , or $GH(g, \lambda)$, is a matrix $H = [\omega_{ij}]$ of order $v = g\lambda$ with entries from the group G such that

Summary:

- ▶ Let (G, \odot) be a group of order g . A *generalized Hadamard matrix* over G , or $GH(g, \lambda)$, is a matrix $H = [\omega_{ij}]$ of order $v = g\lambda$ with entries from the group G such that for any distinct $i, h \in \{1, 2, \dots, g\lambda\}$, the multiset $\{\omega_{ij} \odot \omega_{hj}^{-1} : 1 \leq j \leq v\}$ contains exactly λ copies of every element of G .

Summary:

- ▶ Let (G, \odot) be a group of order g . A *generalized Hadamard matrix* over G , or $GH(g, \lambda)$, is a matrix $H = [\omega_{ij}]$ of order $v = g\lambda$ with entries from the group G such that for any distinct $i, h \in \{1, 2, \dots, g\lambda\}$, the multiset $\{\omega_{ij} \odot \omega_{hj}^{-1} : 1 \leq j \leq v\}$ contains exactly λ copies of every element of G .
- ▶ The multiplication table for any finite field $GF(q)$ of order q forms a $GH(q, 1)$ over $EA(q)$.

Summary:

- ▶ Let (G, \odot) be a group of order g . A *generalized Hadamard matrix* over G , or $GH(g, \lambda)$, is a matrix $H = [\omega_{ij}]$ of order $v = g\lambda$ with entries from the group G such that for any distinct $i, h \in \{1, 2, \dots, g\lambda\}$, the multiset $\{\omega_{ij} \odot \omega_{hj}^{-1} : 1 \leq j \leq v\}$ contains exactly λ copies of every element of G .
- ▶ The multiplication table for any finite field $GF(q)$ of order q forms a $GH(q, 1)$ over $EA(q)$.
- ▶ Let r_i be the i -th row of a $GH(g, 1)$, $i = 1, 2, \dots, g$. The $g - 1$ rank one matrices

Summary:

- ▶ Let (G, \odot) be a group of order g . A *generalized Hadamard matrix* over G , or $GH(g, \lambda)$, is a matrix $H = [\omega_{ij}]$ of order $v = g\lambda$ with entries from the group G such that for any distinct $i, h \in \{1, 2, \dots, g\lambda\}$, the multiset $\{\omega_{ij} \odot \omega_{hj}^{-1} : 1 \leq j \leq v\}$ contains exactly λ copies of every element of G .
- ▶ The multiplication table for any finite field $GF(q)$ of order q forms a $GH(q, 1)$ over $EA(q)$.
- ▶ Let r_i be the i -th row of a $GH(g, 1)$, $i = 1, 2, \dots, g$. The $g - 1$ rank one matrices $C_i = r_i^* r_i$ form a class of MSLS (MOLS) of size g .

Summary:

- ▶ Let (G, \odot) be a group of order g . A *generalized Hadamard matrix* over G , or $GH(g, \lambda)$, is a matrix $H = [\omega_{ij}]$ of order $v = g\lambda$ with entries from the group G such that for any distinct $i, h \in \{1, 2, \dots, g\lambda\}$, the multiset $\{\omega_{ij} \odot \omega_{hj}^{-1} : 1 \leq j \leq v\}$ contains exactly λ copies of every element of G .
- ▶ The multiplication table for any finite field $GF(q)$ of order q forms a $GH(q, 1)$ over $EA(q)$.
- ▶ Let r_i be the i -th row of a $GH(g, 1)$, $i = 1, 2, \dots, g$. The $g - 1$ rank one matrices $C_i = r_i^* r_i$ form a class of MSLS (MOLS) of size g .
- ▶ Any $GH(q, 1)$ over an $EA(q)$ leads to some very interesting objects.

Association Schemes:

Association Schemes:

Let $\{A_0, A_1, \dots, A_\ell\}$ be a set of $n \times n$ symmetric $(0, 1)$ -matrices which satisfy

Association Schemes:

Let $\{A_0, A_1, \dots, A_\ell\}$ be a set of $n \times n$ symmetric $(0, 1)$ -matrices which satisfy

- ▶ A_0 is the identity matrix of order n .

Association Schemes:

Let $\{A_0, A_1, \dots, A_\ell\}$ be a set of $n \times n$ symmetric $(0, 1)$ -matrices which satisfy

- ▶ A_0 is the identity matrix of order n .
- ▶ $\sum_{i=0}^{\ell} A_i = J$, where J is the matrix of all ones of order n .

Association Schemes:

Let $\{A_0, A_1, \dots, A_\ell\}$ be a set of $n \times n$ symmetric $(0, 1)$ -matrices which satisfy

- ▶ A_0 is the identity matrix of order n .
- ▶ $\sum_{i=0}^{\ell} A_i = J$, where J is the matrix of all ones of order n .
- ▶ $A_k A_j$ is a linear combination of A_i s.

Association Schemes:

Let $\{A_0, A_1, \dots, A_\ell\}$ be a set of $n \times n$ symmetric $(0, 1)$ -matrices which satisfy

- ▶ A_0 is the identity matrix of order n .
- ▶ $\sum_{i=0}^{\ell} A_i = J$, where J is the matrix of all ones of order n .
- ▶ $A_k A_j$ is a linear combination of A_i s.

$\{A_0, A_1, \dots, A_\ell\}$ is said to form an ℓ -class symmetric association scheme of order n .

Association Schemes:

Let $\{A_0, A_1, \dots, A_\ell\}$ be a set of $n \times n$ symmetric $(0, 1)$ -matrices which satisfy

- ▶ A_0 is the identity matrix of order n .
- ▶ $\sum_{i=0}^{\ell} A_i = J$, where J is the matrix of all ones of order n .
- ▶ $A_k A_j$ is a linear combination of A_i s.

$\{A_0, A_1, \dots, A_\ell\}$ is said to form an ℓ -class symmetric association scheme of order n .

Let p be a prime number. Then there is a $p + 1$ -class symmetric association scheme of order p^2 which is often collapsable to smaller classes.

Case of $p = 4$:

Case of $p = 4$:

The multiplication table for $GF(4)$ provides a $GH(4, 1)$ over an additive $EA(4)$ as follows:

Case of $p = 4$:

The multiplication table for $GF(4)$ provides a $GH(4, 1)$ over an additive $EA(4)$ as follows:

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \end{pmatrix}.$$

Case of $p = 4$:

The multiplication table for $GF(4)$ provides a $GH(4, 1)$ over an additive $EA(4)$ as follows:

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \end{pmatrix}. \text{ The auxiliary matrices are:}$$

Case of $p = 4$:

The multiplication table for $GF(4)$ provides a $GH(4, 1)$ over an additive $EA(4)$ as follows:

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \end{pmatrix}. \text{ The auxiliary matrices are:}$$

$$C_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

Case of $p = 4$:

The multiplication table for $GF(4)$ provides a $GH(4, 1)$ over an additive $EA(4)$ as follows:

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \end{pmatrix}. \text{ The auxiliary matrices are:}$$

$$C_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix},$$

Case of $p = 4$:

The multiplication table for $GF(4)$ provides a $GH(4, 1)$ over an additive $EA(4)$ as follows:

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \end{pmatrix}. \text{ The auxiliary matrices are:}$$

$$C_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix},$$

$$C_3 = \begin{pmatrix} 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \end{pmatrix},$$

Case of $p = 4$:

The multiplication table for $GF(4)$ provides a $GH(4, 1)$ over an additive $EA(4)$ as follows:

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \end{pmatrix}. \text{ The auxiliary matrices are:}$$

$$C_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix},$$

$$C_3 = \begin{pmatrix} 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{pmatrix}.$$

Case of $p = 4$:

The multiplication table for $GF(4)$ provides a $GH(4, 1)$ over an additive $EA(4)$ as follows:

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \end{pmatrix}. \text{ The auxiliary matrices are:}$$

$$C_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix},$$

$$C_3 = \begin{pmatrix} 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{pmatrix}.$$

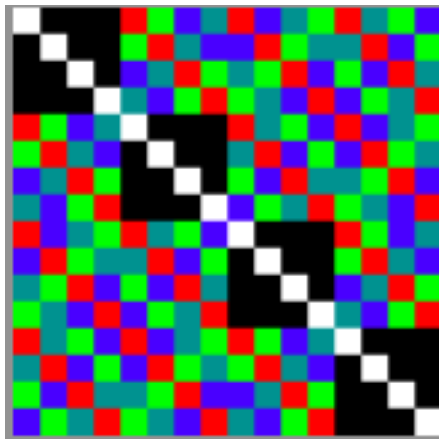
The Generalized Bush-type of order 16 is:

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 & 0 & 2 & 3 & 1 & 0 & 3 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & 2 & 2 & 0 & 1 & 3 & 3 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 & 3 & 0 & 1 & 3 & 1 & 0 & 2 & 1 & 2 & 0 & 3 \\ 0 & 0 & 0 & 0 & 3 & 2 & 1 & 0 & 1 & 3 & 2 & 0 & 2 & 1 & 3 & 0 \\ 0 & 1 & 2 & 3 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 2 & 0 & 2 & 3 & 1 \\ 1 & 0 & 3 & 2 & 0 & 0 & 0 & 0 & 3 & 0 & 2 & 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 3 & 3 & 1 & 0 & 2 \\ 3 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 3 & 0 & 1 & 3 & 2 & 0 \\ 0 & 2 & 3 & 1 & 0 & 3 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 & 3 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 2 \\ 3 & 1 & 0 & 2 & 1 & 2 & 0 & 3 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 1 \\ 1 & 3 & 2 & 0 & 2 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 1 & 0 \\ 0 & 3 & 1 & 2 & 0 & 2 & 3 & 1 & 0 & 1 & 2 & 3 & 0 & 0 & 0 & 0 \\ 3 & 0 & 2 & 1 & 2 & 0 & 1 & 3 & 1 & 0 & 3 & 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 3 & 3 & 1 & 0 & 2 & 2 & 3 & 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 3 & 0 & 1 & 3 & 2 & 0 & 3 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let $H = A_1 + 2A_2 + 3A_3$, where A_1, A_2, A_3 are $(0, 1)$ -matrices.

Let $H = A_1 + 2A_2 + 3A_3$, where A_1, A_2, A_3 are $(0, 1)$ -matrices. Then
There is a 5-class symmetric association scheme collapsable to four
Siamese SRG(16,6,2,2), sharing the cliques of size 4,

Let $H = A_1 + 2A_2 + 3A_3$, where A_1, A_2, A_3 are $(0, 1)$ -matrices. Then
 There is a 5-class symmetric association scheme collapsable to four
 Siamese SRG(16,6,2,2), sharing the cliques of size 4, leading to a
 decomposition of K_{16} to four Siamese SRG(16,6,2,2).



Two open problems

Two open problems

- ▶ There are no GH-matrices $\text{GH}(q, 1)$ over non-prime power order groups.

Two open problems

- ▶ There are no GH-matrices $\text{GH}(q, 1)$ over non-prime power order groups. The first open case is order 12 over $\text{EA}(12)$, where $\text{EA}(q)$ denotes the order q direct product of prime order cyclic groups.

Two open problems

- ▶ There are no GH-matrices $\text{GH}(q, 1)$ over non-prime power order groups. The first open case is order 12 over $\text{EA}(12)$, where $\text{EA}(q)$ denotes the order q direct product of prime order cyclic groups.
- ▶ There is a GH-matrix of order $4k$ over $\text{EA}(4)$ for any positive integer k .

Two open problems

- ▶ There are no GH-matrices $\text{GH}(q, 1)$ over non-prime power order groups. The first open case is order 12 over $\text{EA}(12)$, where $\text{EA}(q)$ denotes the order q direct product of prime order cyclic groups.
- ▶ There is a GH-matrix of order $4k$ over $\text{EA}(4)$ for any positive integer k . This is equivalent to finding a pair of order $4k$ Hadamard matrices whose entrywise product is also Hadamard.

Two open problems

- ▶ There are no GH-matrices $\text{GH}(q, 1)$ over non-prime power order groups. The first open case is order 12 over $\text{EA}(12)$, where $\text{EA}(q)$ denotes the order q direct product of prime order cyclic groups.
- ▶ There is a GH-matrix of order $4k$ over $\text{EA}(4)$ for any positive integer k . This is equivalent to finding a pair of order $4k$ Hadamard matrices whose entrywise product is also Hadamard.

Example:

Two open problems

- ▶ There are no GH-matrices $\text{GH}(q, 1)$ over non-prime power order groups. The first open case is order 12 over $\text{EA}(12)$, where $\text{EA}(q)$ denotes the order q direct product of prime order cyclic groups.
- ▶ There is a GH-matrix of order $4k$ over $\text{EA}(4)$ for any positive integer k . This is equivalent to finding a pair of order $4k$ Hadamard matrices whose entrywise product is also Hadamard.

Example:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix}$$

Two open problems

- ▶ There are no GH-matrices $\text{GH}(q, 1)$ over non-prime power order groups. The first open case is order 12 over $\text{EA}(12)$, where $\text{EA}(q)$ denotes the order q direct product of prime order cyclic groups.
- ▶ There is a GH-matrix of order $4k$ over $\text{EA}(4)$ for any positive integer k . This is equivalent to finding a pair of order $4k$ Hadamard matrices whose entrywise product is also Hadamard.

Example:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \quad K = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

Two open problems

- ▶ There are no GH-matrices $\text{GH}(q, 1)$ over non-prime power order groups. The first open case is order 12 over $\text{EA}(12)$, where $\text{EA}(q)$ denotes the order q direct product of prime order cyclic groups.
- ▶ There is a GH-matrix of order $4k$ over $\text{EA}(4)$ for any positive integer k . This is equivalent to finding a pair of order $4k$ Hadamard matrices whose entrywise product is also Hadamard.

Example:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \quad K = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

The first open case is order 20.

Key words:

Key words:

- ▶ Difference matrices

Key words:

- ▶ Difference matrices
- ▶ Generalized Hadamard matrices

Key words:

- ▶ Difference matrices
- ▶ Generalized Hadamard matrices
- ▶ Auxiliary matrices of rank one

Key words:

- ▶ Difference matrices
- ▶ Generalized Hadamard matrices
- ▶ Auxiliary matrices of rank one
- ▶ Mutually Suitable Latin Squares

Key words:

- ▶ Difference matrices
- ▶ Generalized Hadamard matrices
- ▶ Auxiliary matrices of rank one
- ▶ Mutually Suitable Latin Squares
- ▶ Bush type Hadamard matrices

Key words:

- ▶ Difference matrices
- ▶ Generalized Hadamard matrices
- ▶ Auxiliary matrices of rank one
- ▶ Mutually Suitable Latin Squares
- ▶ Bush type Hadamard matrices
- ▶ Mutually Unbiased Orthogonal Designs

Key words:

- ▶ Difference matrices
- ▶ Generalized Hadamard matrices
- ▶ Auxiliary matrices of rank one
- ▶ Mutually Suitable Latin Squares
- ▶ Bush type Hadamard matrices
- ▶ Mutually Unbiased Orthogonal Designs
- ▶ Bush type Generalized Hadamard matrices

Key words:

- ▶ Difference matrices
- ▶ Generalized Hadamard matrices
- ▶ Auxiliary matrices of rank one
- ▶ Mutually Suitable Latin Squares
- ▶ Bush type Hadamard matrices
- ▶ Mutually Unbiased Orthogonal Designs
- ▶ Bush type Generalized Hadamard matrices
- ▶ Association Schemes

Key words:

- ▶ Difference matrices
- ▶ Generalized Hadamard matrices
- ▶ Auxiliary matrices of rank one
- ▶ Mutually Suitable Latin Squares
- ▶ Bush type Hadamard matrices
- ▶ Mutually Unbiased Orthogonal Designs
- ▶ Bush type Generalized Hadamard matrices
- ▶ Association Schemes
- ▶ Strongly Regular Graphs

Key words:

- ▶ Difference matrices
- ▶ Generalized Hadamard matrices
- ▶ Auxiliary matrices of rank one
- ▶ Mutually Suitable Latin Squares
- ▶ Bush type Hadamard matrices
- ▶ Mutually Unbiased Orthogonal Designs
- ▶ Bush type Generalized Hadamard matrices
- ▶ Association Schemes
- ▶ Strongly Regular Graphs

Main result: For any prime number p there is a $(p + 1)$ -class symmetric association scheme collapsible to smaller class symmetric association scheme of order p^2 .

A BIG **Thank you** to the organizers

Happy Birthday Reza!

