Unbiased weighing matrices

Hadi Kharaghani

University of Lethbridge

ICTP-IPM-WORKSHOP & CONFERENCE IN COMBINATORICS AND GRAPH THEORY

ICTP, Trieste, Italy

September 10, 2012

- Weighing matrices

- Weighing matrices
- Mutually unbiased weighing matrices

- Weighing matrices
- Mutually unbiased weighing matrices
- Quaternary and Binary weighing matrices

- Weighing matrices
- Mutually unbiased weighing matrices
- Quaternary and Binary weighing matrices
- Binary H-matrices from Quaternary H-matrices

- Weighing matrices
- Mutually unbiased weighing matrices
- Quaternary and Binary weighing matrices
- Binary H-matrices from Quaternary H-matrices
- A construction method for mutually unbiased weighing matrices

- Weighing matrices
- Mutually unbiased weighing matrices
- Quaternary and Binary weighing matrices
- Binary H-matrices from Quaternary H-matrices
- A construction method for mutually unbiased weighing matrices
- Mutually unbiased weighing matrices of small weights

- Weighing matrices
- Mutually unbiased weighing matrices
- Quaternary and Binary weighing matrices
- Binary H-matrices from Quaternary H-matrices
- A construction method for mutually unbiased weighing matrices
- Mutually unbiased weighing matrices of small weights
- Some open problems

Weighing matrices

Weighing matrices

Definition

A matrix $W = [w_{ij}]$ of order n and $|w_{ij}| = 0$ or 1 is called a *weighing matrix with weight p* if $WW^* = pI_n$, where I_n is the identity matrix of order n.

Weighing matrices

Definition

A matrix $W = [w_{ij}]$ of order n and $|w_{ij}| = 0$ or 1 is called a *weighing matrix with weight p* if $WW^* = pI_n$, where I_n is the identity matrix of order n.

Example

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 \\ - & 0 & 1 & - \\ - & - & 0 & 1 \\ - & 1 & - & 0 \end{pmatrix},$$

Weighing matrices

Definition

A matrix $W = [w_{ij}]$ of order n and $|w_{ij}| = 0$ or 1 is called a *weighing matrix with weight p* if $WW^* = pI_n$, where I_n is the identity matrix of order n.

Example

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 \\ - & 0 & 1 & - \\ - & - & 0 & 1 \\ - & 1 & - & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

is a *real* $W(4, 3)$ and a *quaternary* $W(2, 2)$, respectively.

More examples

More examples

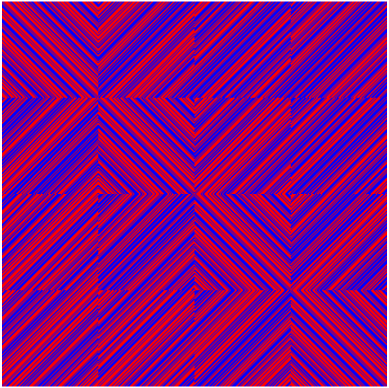

Figure: A binary Hadamard matrix of order 428

Vectors in $\mathbb{C}^n$

Vectors in $\mathbb{C}^n$

Start with a weighing matrix $W(n,p)$ and consider each row as a vector in $\mathbb{C}^n$.

Vectors in $\mathbb{C}^n$

Start with a weighing matrix $W(n, p)$ and consider each row as a vector in $\mathbb{C}^n$.

Normalizing the n vectors we get an orthonormal basis for $\mathbb{C}^n$.

Vectors in $\mathbb{C}^n$

Start with a weighing matrix $W(n, p)$ and consider each row as a vector in $\mathbb{C}^n$.

Normalizing the n vectors we get an orthonormal basis for $\mathbb{C}^n$.

Consider the two orthonormal bases $\mathcal{B}_1$ and $\mathcal{B}_2$ obtained from two given weighing matrices $W_1(n, p)$ and $W_2(n, p)$.

Vectors in $\mathbb{C}^n$

Start with a weighing matrix $W(n,p)$ and consider each row as a vector in $\mathbb{C}^n$.

Normalizing the n vectors we get an orthonormal basis for $\mathbb{C}^n$.

Consider the two orthonormal bases $\mathcal{B}_1$ and $\mathcal{B}_2$ obtained from two given weighing matrices $W_1(n,p)$ and $W_2(n,p)$.

It is of great interest to have the

$$|<u,v>| \in \{0, \frac{1}{\sqrt{p}}\},$$

for all $u \in \mathcal{B}_1$ and $v \in \mathcal{B}_2$.

Mutually unbiased weighing matrices

Mutually unbiased weighing matrices

Definition

Two weighing matrices W_1, W_2 of order n and weight p are called *unbiased* if $W_1 W_2^* = \sqrt{p}\, W$, where W is a weighing matrix of order n and weight p.

Mutually unbiased weighing matrices

Definition

Two weighing matrices W_1, W_2 of order n and weight p are called *unbiased* if $W_1 W_2^* = \sqrt{p}\, W$, where W is a weighing matrix of order n and weight p.

A set of weighing matrices is called *mutually unbiased (MU)* if every pair of matrices are unbiased.

Mutually unbiased weighing matrices

Definition

Two weighing matrices W_1, W_2 of order n and weight p are called *unbiased* if $W_1 W_2^* = \sqrt{p}\, W$, where W is a weighing matrix of order n and weight p.

A set of weighing matrices is called *mutually unbiased (MU)* if every pair of matrices are unbiased.

Example

Let

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

Mutually unbiased weighing matrices

Definition

Two weighing matrices W_1, W_2 of order n and weight p are called *unbiased* if $W_1 W_2^* = \sqrt{p}\, W$, where W is a weighing matrix of order n and weight p.

A set of weighing matrices is called *mutually unbiased (MU)* if every pair of matrices are unbiased.

Example

Let

$$H = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}, K = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \text{ then } HK^* = \sqrt{2} \begin{pmatrix} \frac{1-i}{\sqrt{2}} & \frac{1-i}{\sqrt{2}} \\ \frac{1+i}{\sqrt{2}} & \frac{-1-i}{\sqrt{2}} \end{pmatrix}.$$

Mutually unbiased weighing matrices

Definition

Two weighing matrices W_1, W_2 of order n and weight p are called *unbiased* if $W_1 W_2^* = \sqrt{p}\,W$, where W is a weighing matrix of order n and weight p.

A set of weighing matrices is called *mutually unbiased (MU)* if every pair of matrices are unbiased.

Example

Let

$$H = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}, K = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \text{ then } HK^* = \sqrt{2}\begin{pmatrix} \frac{1-i}{\sqrt{2}} & \frac{1-i}{\sqrt{2}} \\ \frac{1+i}{\sqrt{2}} & \frac{-1-i}{\sqrt{2}} \end{pmatrix}.$$

$\{H, K\}$ forms a set of two unbiased $W(2,2)$.

The [DGS 1975] upper bound; real matrices

The [DGS 1975] upper bound; real matrices

Let V be a set of unit vectors in $\mathbb{R}^n$ in such a way that for all different vectors u, v in V, $| < u, v > | \in \{0, \frac{1}{\sqrt{p}}\}$.

The [DGS 1975] upper bound; real matrices

Let V be a set of unit vectors in $\mathbb{R}^n$ in such a way that for all different vectors u, v in V, $| < u, v > | \in \{0, \frac{1}{\sqrt{p}}\}$. Delsarte, Geothals and Seidel [DGS1975] used an analytic argument related to the orthogonal polynomials and found an upper bound for the number of vectors in V.

The [DGS 1975] upper bound; real matrices

Let V be a set of unit vectors in $\mathbb{R}^n$ in such a way that for all different vectors u, v in V, $| < u, v > | \in \{0, \frac{1}{\sqrt{p}}\}$. Delsarte, Geothals and Seidel [DGS1975] used an analytic argument related to the orthogonal polynomials and found an upper bound for the number of vectors in V. Calderbank, Cameron, Kantor and Seidel [CCKS 1997] found a version of the upper bound as a corollary to one of their many important results.

The [DGS 1975] upper bound; real matrices

Let V be a set of unit vectors in $\mathbb{R}^n$ in such a way that for all different vectors u, v in V, $| < u, v > | \in \{0, \frac{1}{\sqrt{p}}\}$. Delsarte, Geothals and Seidel [DGS1975] used an analytic argument related to the orthogonal polynomials and found an upper bound for the number of vectors in V. Calderbank, Cameron, Kantor and Seidel [CCKS 1997] found a version of the upper bound as a corollary to one of their many important results.

Corollary I [DGS 1975 - CCKS 1997]: Let m be the number of MU weighing matrices of order n and weight p in $\mathbb{R}^n$.

The [DGS 1975] upper bound; real matrices

Let V be a set of unit vectors in $\mathbb{R}^n$ in such a way that for all different vectors u, v in V, $|<u, v>| \in \{0, \frac{1}{\sqrt{p}}\}$. Delsarte, Geothals and Seidel [DGS1975] used an analytic argument related to the orthogonal polynomials and found an upper bound for the number of vectors in V. Calderbank, Cameron, Kantor and Seidel [CCKS 1997] found a version of the upper bound as a corollary to one of their many important results.

Corollary I [DGS 1975 - CCKS 1997]: Let m be the number of MU weighing matrices of order n and weight p in $\mathbb{R}^n$.

Then

$$m \leq \begin{cases} \frac{p(n-1)}{3p-(n+2)} & \text{if } 3p-(n+2) > 0, \\ \frac{(n-1)(n+4)}{6} & \text{otherwise.} \end{cases}$$

The [DGS 1975] upper bound; real matrices

Let V be a set of unit vectors in $\mathbb{R}^n$ in such a way that for all different vectors u, v in V, $|<u,v>| \in \{0, \frac{1}{\sqrt{p}}\}$. Delsarte, Geothals and Seidel [DGS1975] used an analytic argument related to the orthogonal polynomials and found an upper bound for the number of vectors in V. Calderbank, Cameron, Kantor and Seidel [CCKS 1997] found a version of the upper bound as a corollary to one of their many important results.

Corollary I [DGS 1975 - CCKS 1997]: Let m be the number of MU weighing matrices of order n and weight p in $\mathbb{R}^n$.

Then

$$m \leq \begin{cases} \frac{p(n-1)}{3p-(n+2)} & \text{if } \; 3p-(n+2) > 0, \\ \frac{(n-1)(n+4)}{6} & \text{otherwise.} \end{cases}$$

Examples

Example: Let $n = p = 4$, then $3p - (n + 2) = 6$. So $m \leq 2$.

Examples

Example: Let $n = p = 4$, then $3p - (n+2) = 6$. So $m \leq 2$.

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

Examples

Example: Let $n = p = 4$, then $3p-(n+2) = 6$. So $m \leq 2$.

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix}, \; K = \begin{pmatrix} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ 1 & - & 1 & 1 \\ - & 1 & 1 & 1 \end{pmatrix}, \; HK^t = 2\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ - & 1 & 1 & - \end{pmatrix}.$$

Examples

Example: Let $n = p = 4$, then $3p - (n+2) = 6$. So $m \leq 2$.

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix}, \ K = \begin{pmatrix} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ 1 & - & 1 & 1 \\ - & 1 & 1 & 1 \end{pmatrix}, \ HK^t = 2 \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ - & 1 & 1 & - \end{pmatrix}.$$

So, $\{H, K\}$ forms set of unbiased Hadamard matrices of order 4 meeting DGS upper bound.

Examples

Example: Let $n = p = 4$, then $3p - (n+2) = 6$. So $m \leq 2$.

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix}, \; K = \begin{pmatrix} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ 1 & - & 1 & 1 \\ - & 1 & 1 & 1 \end{pmatrix}, \; HK^t = 2 \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ - & 1 & 1 & - \end{pmatrix}.$$

So, $\{H, K\}$ forms set of unbiased Hadamard matrices of order 4 meeting DGS upper bound.

Example: Let $n = 7$ and $p = 4$, then $3p - (n+2) = 3$. So, $m \leq 8$. A computer search turned in eight MU weighing matrices.

Examples

Example: Let $n = p = 4$, then $3p - (n+2) = 6$. So $m \leq 2$.

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix}, \ K = \begin{pmatrix} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ 1 & - & 1 & 1 \\ - & 1 & 1 & 1 \end{pmatrix}, \ HK^t = 2 \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ - & 1 & 1 & - \end{pmatrix}.$$

So, $\{H, K\}$ forms set of unbiased Hadamard matrices of order 4 meeting DGS upper bound.

Example: Let $n = 7$ and $p = 4$, then $3p - (n+2) = 3$. So, $m \leq 8$. A computer search turned in eight MU weighing matrices.

By selecting 28 vectors from the 56 vectors in $\mathbb{R}^7$ we had a Deza graph with two Strongly Regular Graphs (SRG) as children.

Examples

Example: Let $n = p = 4$, then $3p - (n+2) = 6$. So $m \leq 2$.

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix}, \; K = \begin{pmatrix} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ 1 & - & 1 & 1 \\ - & 1 & 1 & 1 \end{pmatrix}, \; HK^t = 2 \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ - & 1 & 1 & - \end{pmatrix}.$$

So, $\{H, K\}$ forms set of unbiased Hadamard matrices of order 4 meeting DGS upper bound.

Example: Let $n = 7$ and $p = 4$, then $3p - (n+2) = 3$. So, $m \leq 8$. A computer search turned in eight MU weighing matrices.

By selecting 28 vectors from the 56 vectors in $\mathbb{R}^7$ we had a Deza graph with two Strongly Regular Graphs (SRG) as children.

Another choice of 21 vectors were used to construct the unique SRG on 21 vertices.

Examples

Example: Let $n = p = 4$, then $3p - (n+2) = 6$. So $m \leq 2$.

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix}, \ K = \begin{pmatrix} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ 1 & - & 1 & 1 \\ - & 1 & 1 & 1 \end{pmatrix}, \ HK^t = 2\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ - & 1 & 1 & - \end{pmatrix}.$$

So, $\{H, K\}$ forms set of unbiased Hadamard matrices of order 4 meeting DGS upper bound.

Example: Let $n = 7$ and $p = 4$, then $3p - (n+2) = 3$. So, $m \leq 8$. A computer search turned in eight MU weighing matrices.

By selecting 28 vectors from the 56 vectors in $\mathbb{R}^7$ we had a Deza graph with two Strongly Regular Graphs (SRG) as children.

Another choice of 21 vectors were used to construct the unique SRG on 21 vertices.

Finally, by adding the seven vectors from the standard basis for $\mathbb{R}^7$, the Gramian provided a new SRG on 63 vertices.

Quaternary and Binary weighing matrices

Quaternary and Binary weighing matrices

The number of MU weighing matrices $W(n, p)$ is a function of n and p and the nature of the entries of the matrices.

Quaternary and Binary weighing matrices

The number of MU weighing matrices $W(n, p)$ is a function of n and p and the nature of the entries of the matrices. The first case to talk about is when **n=p and entries belong to** $\{-1, 1, i, -i\}$.

Quaternary and Binary weighing matrices

The number of MU weighing matrices $W(n, p)$ is a function of n and p and the nature of the entries of the matrices. The first case to talk about is when **n=p and entries belong to** $\{-1, 1, i, -i\}$.

Two quaternary Hadamard matrices H and K of order n are called unbiased if $HK^* = L$, where K^* denotes the Hermitian transpose of K

Quaternary and Binary weighing matrices

The number of MU weighing matrices $W(n, p)$ is a function of n and p and the nature of the entries of the matrices. The first case to talk about is when **n=p and entries belong to** $\{-1, 1, i, -i\}$.

Two quaternary Hadamard matrices H and K of order n are called unbiased if $HK^* = L$, where K^* denotes the Hermitian transpose of K and all the entries of the matrix L are of the absolute value $\sqrt{n}$.

Quaternary and Binary weighing matrices

The number of MU weighing matrices $W(n, p)$ is a function of n and p and the nature of the entries of the matrices. The first case to talk about is when **n=p and entries belong to** $\{-1, 1, i, -i\}$.

Two quaternary Hadamard matrices H and K of order n are called unbiased if $HK^* = L$, where K^* denotes the Hermitian transpose of K and all the entries of the matrix L are of the absolute value $\sqrt{n}$. In this case, it follows that $n = a^2 + b^2$ $(n = a^2)$, where a, b are some nonnegative integers.

Quaternary and Binary weighing matrices

The number of MU weighing matrices $W(n, p)$ is a function of n and p and the nature of the entries of the matrices. The first case to talk about is when **n=p and entries belong to** $\{-1, 1, i, -i\}$.

Two quaternary Hadamard matrices H and K of order n are called unbiased if $HK^* = L$, where K^* denotes the Hermitian transpose of K and all the entries of the matrix L are of the absolute value $\sqrt{n}$. In this case, it follows that $n = a^2 + b^2$ $(n = a^2)$, where a, b are some nonnegative integers.

Theorem [Best, K 2010]: Let m be the number of matrices in a set of MU quaternary Hadamard matrices of order $2n$, n odd. Then $m \leq 2$. Equality occurs for $n = 1, 5, 9$.

Quaternary and Binary weighing matrices

The number of MU weighing matrices $W(n, p)$ is a function of n and p and the nature of the entries of the matrices. The first case to talk about is when **n=p and entries belong to** $\{-1, 1, i, -i\}$.

Two quaternary Hadamard matrices H and K of order n are called unbiased if $HK^* = L$, where K^* denotes the Hermitian transpose of K and all the entries of the matrix L are of the absolute value $\sqrt{n}$. In this case, it follows that $n = a^2 + b^2$ ($n = a^2$), where a, b are some nonnegative integers.

Theorem [Best, K 2010]: Let m be the number of matrices in a set of MU quaternary Hadamard matrices of order $2n$, n odd. Then $m \leq 2$. Equality occurs for $n = 1, 5, 9$.

Binary H-matrices from Quaternary H-matrices

Binary H-matrices from Quaternary H-matrices

Example

Let

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

Then

$$HK^* = \begin{pmatrix} 1-i & 1-i \\ i+1 & -i-1 \end{pmatrix} = (1-i)\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} = (1-i)L.$$

Binary H-matrices from Quaternary H-matrices

Example

Let

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

Then

$$HK^* = \begin{pmatrix} 1-i & 1-i \\ i+1 & -i-1 \end{pmatrix} = (1-i)\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} = (1-i)L.$$

So, the set $\{H, K\}$ forms a set of U quaternary H-matrices of order 2, meeting the DGS upper bound,

Binary H-matrices from Quaternary H-matrices

Example

Let

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

Then

$$HK^* = \begin{pmatrix} 1-i & 1-i \\ i+1 & -i-1 \end{pmatrix} = (1-i)\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} = (1-i)L.$$

So, the set $\{H, K\}$ forms a set of U quaternary H-matrices of order 2, meeting the DGS upper bound, and a little more.

Binary H-matrices from Quaternary H-matrices

Example

Let

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

Then

$$HK^* = \begin{pmatrix} 1-i & 1-i \\ i+1 & -i-1 \end{pmatrix} = (1-i)\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} = (1-i)L.$$

So, the set $\{H, K\}$ forms a set of U quaternary H-matrices of order 2, meeting the DGS upper bound, and a little more.

The property that $HK^* = \alpha L$, where α is a Gaussian complex number and L is a quaternary H-matrix doesn't happen for all orders.

Binary H-matrices from Quaternary H-matrices

Example

Let

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

Then

$$HK^* = \begin{pmatrix} 1-i & 1-i \\ i+1 & -i-1 \end{pmatrix} = (1-i)\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} = (1-i)L.$$

So, the set $\{H, K\}$ forms a set of U quaternary H-matrices of order 2, meeting the DGS upper bound, and a little more.

The property that $HK^* = \alpha L$, where α is a Gaussian complex number and L is a quaternary H-matrix doesn't happen for all orders. For example, there are none of order 10.

Binary H-matrices from Quaternary H-matrices

Example

Let

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

Then

$$HK^* = \begin{pmatrix} 1-i & 1-i \\ i+1 & -i-1 \end{pmatrix} = (1-i)\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} = (1-i)L.$$

So, the set $\{H, K\}$ forms a set of U quaternary H-matrices of order 2, meeting the DGS upper bound, and a little more.

The property that $HK^* = \alpha L$, where α is a Gaussian complex number and L is a quaternary H-matrix doesn't happen for all orders. For example, there are none of order 10. However, if such a pair of U quaternary matrices exist, then by a doubling process one can get a pair of U binary H-matrices.

Binary from Quaternary

Theorem [Best, K 2010]: Let H, K be a pair of U quaternary H-matrices of order $2n$, where $n = a^2$, for which $HK^* = \alpha L$, where α is a Gaussian complex number and L is a quaternary H-matrix.

Binary from Quaternary

Theorem [Best, K 2010]: Let H, K be a pair of U quaternary H-matrices of order $2n$, where $n = a^2$, for which $HK^* = \alpha L$, where α is a Gaussian complex number and L is a quaternary H-matrix.Then there is a pair of unbiased binary H-matrices of order $4n = 4a^2$.

Binary from Quaternary

Theorem [Best, K 2010]: Let H, K be a pair of U quaternary H-matrices of order $2n$, where $n = a^2$, for which $HK^* = \alpha L$, where α is a Gaussian complex number and L is a quaternary H-matrix.Then there is a pair of unbiased binary H-matrices of order $4n = 4a^2$. There are pairs of U quaternary H-matrices for $n = 1, 9$.

Binary from Quaternary

Theorem [Best, K 2010]: Let H, K be a pair of U quaternary H-matrices of order $2n$, where $n = a^2$, for which $HK^* = \alpha L$, where α is a Gaussian complex number and L is a quaternary H-matrix.Then there is a pair of unbiased binary H-matrices of order $4n = 4a^2$. There are pairs of U quaternary H-matrices for $n = 1, 9$.

Corollary: There is a pair of U binary H-matrices of order 36.

Binary from Quaternary

Theorem [Best, K 2010]: Let H, K be a pair of U quaternary H-matrices of order $2n$, where $n = a^2$, for which $HK^* = \alpha L$, where α is a Gaussian complex number and L is a quaternary H-matrix.Then there is a pair of unbiased binary H-matrices of order $4n = 4a^2$. There are pairs of U quaternary H-matrices for $n = 1, 9$.

Corollary: There is a pair of U binary H-matrices of order 36.

Theorem [CCKS 1997]: There is a MU set of quaternary H-matrices of order 2^{2k+1} consisting of 2^{2k+1} matrices in such a way that for each pair H, K, $HK^* = \alpha L$, where α is some Gaussian complex number and L is some quaternary H-matrix.

Weighing matrices; $p = n$

Weighing matrices; $p = n$

Assuming the entries of the matrices are all unit complex numbers, we have one of most studied classes of weighing matrices.

Weighing matrices; $p = n$

Assuming the entries of the matrices are all unit complex numbers, we have one of most studied classes of weighing matrices. There is a huge literature on these matrices for the case where $p = n$, i.e., matrices have no zero entries, and so we are dealing with unit Hadamard matrices.

Weighing matrices; $p = n$

Assuming the entries of the matrices are all unit complex numbers, we have one of most studied classes of weighing matrices. There is a huge literature on these matrices for the case where $p = n$, i.e., matrices have no zero entries, and so we are dealing with unit Hadamard matrices. We begin with a corollary to a result of DGS [1971], CCKS[1997].

Weighing matrices; $p = n$

Assuming the entries of the matrices are all unit complex numbers, we have one of most studied classes of weighing matrices. There is a huge literature on these matrices for the case where $p = n$, i.e., matrices have no zero entries, and so we are dealing with unit Hadamard matrices. We begin with a corollary to a result of DGS [1971], CCKS[1997].

Corollary II : Let m be the number of MU weighing matrices of order n and weight p in $\mathbb{C}^n$.

Weighing matrices; $p = n$

Assuming the entries of the matrices are all unit complex numbers, we have one of most studied classes of weighing matrices. There is a huge literature on these matrices for the case where $p = n$, i.e., matrices have no zero entries, and so we are dealing with unit Hadamard matrices. We begin with a corollary to a result of DGS [1971], CCKS[1997].

Corollary II : Let m be the number of MU weighing matrices of order n and weight p in $\mathbb{C}^n$. Then

$$m \leq \begin{cases} \frac{p(n-1)}{2p-(n+1)} & \text{if } 2p-(n+1) > 0, \\ \frac{(n-1)(n+2)}{2} & \text{otherwise.} \end{cases}$$

Weighing matrices; $p = n$

Assuming the entries of the matrices are all unit complex numbers, we have one of most studied classes of weighing matrices. There is a huge literature on these matrices for the case where $p = n$, i.e., matrices have no zero entries, and so we are dealing with unit Hadamard matrices. We begin with a corollary to a result of DGS [1971], CCKS[1997].

Corollary II : Let m be the number of MU weighing matrices of order n and weight p in $\mathbb{C}^n$. Then

$$m \leq \begin{cases} \frac{p(n-1)}{2p-(n+1)} & \text{if } 2p-(n+1) > 0, \\ \frac{(n-1)(n+2)}{2} & \text{otherwise.} \end{cases}$$

Recall: Two unit Hadamard matrices H and K of order n are *unbiased* if all the entries of HK^* have modulus $\sqrt{n}$.

Weighing matrices; $p = n$

Assuming the entries of the matrices are all unit complex numbers, we have one of most studied classes of weighing matrices. There is a huge literature on these matrices for the case where $p = n$, i.e., matrices have no zero entries, and so we are dealing with unit Hadamard matrices. We begin with a corollary to a result of DGS [1971], CCKS[1997].

Corollary II : Let m be the number of MU weighing matrices of order n and weight p in $\mathbb{C}^n$. Then

$$m \leq \begin{cases} \frac{p(n-1)}{2p-(n+1)} & \text{if } 2p-(n+1) > 0, \\ \frac{(n-1)(n+2)}{2} & \text{otherwise.} \end{cases}$$

Recall: Two unit Hadamard matrices H and K of order n are *unbiased* if all the entries of HK^* have modulus $\sqrt{n}$.

Unbiased unit Hadamard matrices

Unbiased unit Hadamard matrices

Working out the DGS upper bound for p=n, we get:

Lemma

Let m be the number of unbiased unit Hadamard matrices of order n. Then

$$m \leq n.$$

Unbiased unit Hadamard matrices

Working out the DGS upper bound for p=n, we get:

Lemma

Let m be the number of unbiased unit Hadamard matrices of order n. Then

$$m \leq n.$$

Theorem [Hesse 1844, Segre 1868 and others: There is a complete set of unbiased unit Hadamard matrices of order p for each prime power p.

Unbiased unit Hadamard matrices

Working out the DGS upper bound for p=n, we get:

Lemma

Let m be the number of unbiased unit Hadamard matrices of order n. Then

$$m \leq n.$$

Theorem [Hesse 1844, Segre 1868 and others: There is a complete set of unbiased unit Hadamard matrices of order p for each prime power p.

References: Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, Karol Życzkowski, ON MUTUALLY UNBIASED BASES, arXiv:1004.3348v2 [quant-ph].

Unbiased unit Hadamard matrices

Working out the DGS upper bound for p=n, we get:

Lemma

Let m be the number of unbiased unit Hadamard matrices of order n. Then

$$m \leq n.$$

Theorem [Hesse 1844, Segre 1868 and others: There is a complete set of unbiased unit Hadamard matrices of order p for each prime power p.

References: Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, Karol Życzkowski, ON MUTUALLY UNBIASED BASES, arXiv:1004.3348v2 [quant-ph].
Chris Godsil, Aidan Roy, Equiangular lines, mutually unbiased bases, and spin models. European J. Combin. 30 (2009), no. 1, 246–262.

Unbiased unit Hadamard matrices

Unbiased unit Hadamard matrices

Not much known about the unbiased unit Hadamard matrices of order a composite number.

Unbiased unit Hadamard matrices

Not much known about the unbiased unit Hadamard matrices of order a composite number.

For example, the theoretical upper bound for the number of mutually unbiased unit Hadamard matrices (MUUHM) of order 6 is 6, but no class of MUUHM of order 6 is known containing more then two matrices.

Unbiased unit Hadamard matrices

Not much known about the unbiased unit Hadamard matrices of order a composite number.

For example, the theoretical upper bound for the number of mutually unbiased unit Hadamard matrices (MUUHM) of order 6 is 6, but no class of MUUHM of order 6 is known containing more then two matrices.

A characterization of weighing matrices

A characterization of weighing matrices

A characterization of weighing matrices

Theorem

There is a weighing matrix $W(n,p)$ W *of order n and weight p if and only if there are n* $(0,\pm 1)$- *matrices*

A characterization of weighing matrices

Theorem

There is a weighing matrix $W(n,p)$ W of order n and weight p if and only if there are n $(0,\pm1)$- matrices $C_1, C_1, C_2, \ldots, C_n$ of order n such that:

- $C_i^* = C_i$

A characterization of weighing matrices

Theorem

There is a weighing matrix $W(n,p)$ W of order n and weight p if and only if there are n $(0,\pm 1)$- matrices $C_1, C_1, C_2, \ldots, C_n$ of order n such that:

- $C_i^* = C_i$
- $C_i C_j^* = 0$, $i \neq j$

A characterization of weighing matrices

Theorem

There is a weighing matrix $W(n,p)$ W *of order n and weight p if and only if there are n* $(0,\pm 1)$*- matrices* $C_1, C_1, C_2, \ldots, C_n$ *of order n such that:*

- $C_i^* = C_i$
- $C_i C_j^* = 0$, $i \neq j$
- $C_i C_i^* = pC_i$

A characterization of weighing matrices

Theorem

There is a weighing matrix $W(n,p)$ W of order n and weight p if and only if there are n $(0,\pm 1)$- matrices $C_1, C_1, C_2, \ldots, C_n$ of order n such that:

- $C_i^* = C_i$
- $C_i C_j^* = 0$, $i \neq j$
- $C_i C_i^* = pC_i$
- $C_1 + C_1 + C_2 + \cdots + C_n = p^2 I_n$

A characterization of weighing matrices

Theorem

There is a weighing matrix $W(n,p)$ W of order n and weight p if and only if there are n $(0,\pm1)$- matrices $C_1, C_1, C_2, \ldots, C_n$ of order n such that:

- $C_i^* = C_i$
- $C_i C_j^* = 0$, $i \neq j$
- $C_i C_i^* = pC_i$
- $C_1 + C_1 + C_2 + \cdots + C_n = p^2 I_n$

Proof.

A characterization of weighing matrices

Theorem

There is a weighing matrix $W(n,p)$ W of order n and weight p if and only if there are n $(0,\pm 1)$- matrices $C_1, C_1, C_2, \ldots, C_n$ of order n such that:

- $C_i^* = C_i$
- $C_i C_j^* = 0$, $i \neq j$
- $C_i C_i^* = pC_i$
- $C_1 + C_1 + C_2 + \cdots + C_n = p^2 I_n$

Proof.

Let r_i be the i-th row of W and
let $C_i = r_i^* r_i$, $i = 1, \ldots, n$. □

Mutually suitable Latin squares

Mutually suitable Latin squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0, 1, 2, \ldots, n-1\}$ 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 (aa).

Mutually suitable Latin squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0, 1, 2, \ldots, n-1\}$ 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 (aa).

Example:

$$\begin{pmatrix} 0231 \\ 2013 \\ 3102 \\ 1320 \end{pmatrix}, \quad \begin{pmatrix} 0312 \\ 3021 \\ 1203 \\ 2130 \end{pmatrix}, \quad \begin{pmatrix} 0123 \\ 1032 \\ 2301 \\ 3210 \end{pmatrix}.$$

Mutually suitable Latin squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0, 1, 2, \ldots, n-1\}$ 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 (aa).

Example: $\begin{pmatrix} 0231 \\ 2013 \\ 3102 \\ 1320 \end{pmatrix}, \begin{pmatrix} 0312 \\ 3021 \\ 1203 \\ 2130 \end{pmatrix}, \begin{pmatrix} 0123 \\ 1032 \\ 2301 \\ 3210 \end{pmatrix}.$

Lemma

There are m MOLS (Mutually Orthogonal Latin Squares) of order n if and only if there are m MSLS (Mutually Suitable Latin Squares) of order n.

Mutually suitable Latin squares

Two Latin squares L_1 and L_2 of size n on symbol set $\{0,1,2,\ldots,n-1\}$ 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 (aa).

Example: $\begin{pmatrix} 0231 \\ 2013 \\ 3102 \\ 1320 \end{pmatrix}, \quad \begin{pmatrix} 0312 \\ 3021 \\ 1203 \\ 2130 \end{pmatrix}, \quad \begin{pmatrix} 0123 \\ 1032 \\ 2301 \\ 3210 \end{pmatrix}.$

Lemma

There are m MOLS (Mutually Orthogonal Latin Squares) of order n if and only if there are m MSLS (Mutually Suitable Latin Squares) of order n.

Corollary

Let ℓ be the number of MSLS of order n. Then $\ell \leq n-1$, and equality occurs for $n = p$ for each prime power p.

A construction for MUWM

A construction for MUWM

Starting with a $W(n, p)$ we do the following:

A construction for MUWM

Starting with a $W(n, p)$ we do the following:

- Construct the n matrices $C_1, C_2, \ldots, C_n$.

A construction for MUWM

Starting with a $W(n,p)$ we do the following:

- Construct the n matrices $C_1, C_2, \ldots, C_n$.
- For the prime power $q \geq n$, let $L_1, L_2, \ldots, L_{q-1}$ be a complete set of MSLS on the set $\{1, 2, \ldots, q\}$.

A construction for MUWM

Starting with a $W(n,p)$ we do the following:

- Construct the n matrices $C_1, C_2, \ldots, C_n$.
- For the prime power $q \geq n$, let $L_1, L_2, \ldots, L_{q-1}$ be a complete set of MSLS on the set $\{1, 2, \ldots, q\}$.
- Replace each integer i in L_i with C_i, $i = 1, 2, \ldots, n$ and the rest of the entries with all 0-blocks of order n.

A construction for MUWM

Starting with a $W(n, p)$ we do the following:

- Construct the n matrices $C_1, C_2, \ldots, C_n$.
- For the prime power $q \geq n$, let $L_1, L_2, \ldots, L_{q-1}$ be a complete set of MSLS on the set $\{1, 2, \ldots, q\}$.
- Replace each integer i in L_i with C_i, $i = 1, 2, \ldots, n$ and the rest of the entries with all 0-blocks of order n.

A construction for MUWM

Starting with a $W(n, p)$ we do the following:

- Construct the n matrices $C_1, C_2, \ldots, C_n$.
- For the prime power $q \geq n$, let $L_1, L_2, \ldots, L_{q-1}$ be a complete set of MSLS on the set $\{1, 2, \ldots, q\}$.
- Replace each integer i in L_i with C_i, $i = 1, 2, \ldots, n$ and the rest of the entries with all 0-blocks of order n.

Lemma: There are q mutually unbiased weighing matrices (MUWM), $W(nq, p^2)$, for each prime power q, $q \geq n$.

Mutually unbiased Hadamard matrices of order $16n^2$

Mutually unbiased Hadamard matrices of order $16n^2$

Theorem

Let m be the number of MUHM of order $16n^2$ and ℓ the number of MSLS of order $4n$. Then

$$\ell + 1 \leq m \leq 8n^2.$$

Mutually unbiased Hadamard matrices of order $16n^2$

Theorem

Let m be the number of MUHM of order $16n^2$ and ℓ the number of MSLS of order $4n$. Then

$$\ell + 1 \leq m \leq 8n^2.$$

Not much is known on the exact value of m in general.

Mutually unbiased Hadamard matrices of order $16n^2$

Theorem

Let m be the number of MUHM of order $16n^2$ and ℓ the number of MSLS of order $4n$. Then

$$\ell + 1 \leq m \leq 8n^2.$$

Not much is known on the exact value of m in general. The following theorem is the best known result on the values of m attaining the DGS upper bound.

Mutually unbiased Hadamard matrices of order $16n^2$

Theorem

Let m be the number of MUHM of order $16n^2$ and ℓ the number of MSLS of order $4n$. Then

$$\ell + 1 \leq m \leq 8n^2.$$

Not much is known on the exact value of m in general. The following theorem is the best known result on the values of m attaining the DGS upper bound.

Theorem

There are 2^{2k-1} MU Hadamard matrices of order 2^{2k}, for each integer $k \geq 1$.

Mutually unbiased Hadamard matrices of order $16n^2$

Theorem

Let m be the number of MUHM of order $16n^2$ and ℓ the number of MSLS of order $4n$. Then

$$\ell + 1 \leq m \leq 8n^2.$$

Not much is known on the exact value of m in general. The following theorem is the best known result on the values of m attaining the DGS upper bound.

Theorem

There are 2^{2k-1} MU Hadamard matrices of order 2^{2k}, for each integer $k \geq 1$.

Theorem

There is a maximal set of MU Hadamard matrices of order 2^{2k} consisting of 2^k matrices for each integer $k \geq 1$.

MU weighing matrices with weight 2

MU weighing matrices with weight 2

Theorem [Best, K, Ramp 2012]:

MU weighing matrices with weight 2

Theorem [Best, K, Ramp 2012]:
A $W(n,2)$ exists if and only if n is even. Moreover, there is exactly one inequivalent class of $UW(n,2)$ for each even n.

MU weighing matrices with weight 2

Theorem [Best, K, Ramp 2012]:
A $W(n,2)$ exists if and only if n is even. Moreover, there is exactly one inequivalent class of $UW(n,2)$ for each even n.

Theorem [Best, K, Ramp 2012]:

MU weighing matrices with weight 2

Theorem [Best, K, Ramp 2012]:
A $W(n,2)$ exists if and only if n is even. Moreover, there is exactly one inequivalent class of $UW(n,2)$ for each even n.

Theorem [Best, K, Ramp 2012]:
Let n be even. Then there are at most 2 mutually unbiased weighing matrices of order n and weight 2.

MU weighing matrices with small weight

MU weighing matrices with small weight

Lemma [Best, K, Ramp 2012]:

MU weighing matrices with small weight

Lemma [Best, K, Ramp 2012]:
There is a $UW(n,3)$ if and only if $n \neq 5$.

MU weighing matrices with small weight

Lemma [Best, K, Ramp 2012]:
There is a $UW(n,3)$ if and only if $n \neq 5$.

Theorem [Best, K, Ramp 2012]:

MU weighing matrices with small weight

Lemma [Best, K, Ramp 2012]:
There is a $UW(n,3)$ if and only if $n \neq 5$.

Theorem [Best, K, Ramp 2012]: The upper bound on the number of MUWM of the form $W(n,3)$ is:

$$\begin{cases} 3 & \text{if } n \not\equiv 0 \mod 4 \\ 9 & \text{if } n \equiv 0 \mod 4 \end{cases}$$

where $n \in \{3,4\} \cup \{k : k \geq 6\}$,

MU weighing matrices with small weight

Lemma [Best, K, Ramp 2012]:
There is a $UW(n,3)$ if and only if $n \neq 5$.

Theorem [Best, K, Ramp 2012]: The upper bound on the number of MUWM of the form $W(n,3)$ is:

$$\begin{cases} 3 & \text{if } n \not\equiv 0 \mod 4 \\ 9 & \text{if } n \equiv 0 \mod 4 \end{cases}$$

where $n \in \{3,4\} \cup \{k : k \geq 6\}$, and the upper bound is tight.

Type	DGS UB	Number Found	Root of Unity
W(2,2)	2	2	4
W(3,2)	5	0	–
W(3,3)	3	3	3
W(4,2)	2	2	4
W(4,3)	9	9	6
W(4,4)	4	4	4
W(5,2)	14	0	–
W(5,3)	14	0	–
W(5,4)	5	5	6
W(5,5)	5	5	5
W(6,2)	2	2	4
W(6,3)	3	3	3
W(6,4)	20	20	6
W(6,5)	8	2	12
W(6,6)	6	2	12
W(7,2)	27	0	–
W(7,3)	3	3	6
W(7,4)	8	8	2
W(7,5)	15	0	–
W(7,6)	9	0	–
W(7,7)	7	7	7

Some open problems

Some open problems

Open Problem 1: Show that there are two unbiased quaternary Hadamard matrices of order $2n$, $n = 13, 17, 25$.

Some open problems

Open Problem 1: Show that there are two unbiased quaternary Hadamard matrices of order $2n$, $n = 13, 17, 25$.

Open Problem 2: Show that there are two unbiased Hadamard matrices of order 100.

Some open problems

Open Problem 1: Show that there are two unbiased quaternary Hadamard matrices of order $2n$, $n = 13, 17, 25$.

Open Problem 2: Show that there are two unbiased Hadamard matrices of order 100.

Open Problem 3: Let m be the number of MU Hadamard matrices of order $16n^2$, $n \neq 4$ and ℓ the number of MSLS of order $4n$. Show that $m = \ell + 1$.

Some open problems

Open Problem 1: Show that there are two unbiased quaternary Hadamard matrices of order $2n$, $n = 13, 17, 25$.

Open Problem 2: Show that there are two unbiased Hadamard matrices of order 100.

Open Problem 3: Let m be the number of MU Hadamard matrices of order $16n^2$, $n \neq 4$ and ℓ the number of MSLS of order $4n$. Show that $m = \ell + 1$.

Open Problem 4: Find a class of MUHM of order 6 consisting of more than two matrices.

Some open problems

Open Problem 1: Show that there are two unbiased quaternary Hadamard matrices of order $2n$, $n = 13, 17, 25$.

Open Problem 2: Show that there are two unbiased Hadamard matrices of order 100.

Open Problem 3: Let m be the number of MU Hadamard matrices of order $16n^2$, $n \neq 4$ and ℓ the number of MSLS of order $4n$. Show that $m = \ell + 1$.

Open Problem 4: Find a class of MUHM of order 6 consisting of more than two matrices.

Open Problem 5: Prove that no maximal set of MUHM of order 6 contains more than two matrices.

thank you