Biangular Lines

Darcy Best

March 24, 2014

Joint work with:
Hadi Kharaghani (University of Lethbridge)

Hadamard Matrices

A Hadamard matrix, H, is a square matrix (of order n) with entires in $\{\pm 1\}$ such that

$$HH^T = nI.$$

Example of a Hadamard Matrix:

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

Note: $-$ denotes -1.

Constructing Hadamard Matrices

We can easily construct a 2×2 Hadamard matrix as follows:

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}.$$

We can use this matrix to generate H_4 (on the previous slide):

$$H_4 = \begin{pmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{pmatrix}.$$

Constructing Hadamard Matrices

Sylvester noticed that H_{2^k} could be created for any $k \in \mathbb{N}$ by continuing the same procedure.

$$H_{2^k} = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \otimes H_{2^{k-1}} = \begin{pmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{pmatrix}$$

This observation can be extended to arbitrarily large matrices: If we have two Hadamard matrices of order p and q, then we can construct another Hadamard matrix of order pq in the following way:

$$H_{pq} = H_p \otimes H_q$$

Hadamard Conjecture

It is easily proven that if H is a Hadamard matrix of order n, then $n = 1, 2$ or $4k$. The converse, though, is known as the Hadamard conjecture.

Conjecture

A Hadamard matrix exists for every order $n = 4k$.

(True for $n < 668$)

Unbiased Hadamard Matrices

We call two Hadamard matrices (say H and K) *unbiased* if

$$HK^T = \sqrt{n}L$$

where L is a Hadamard matrix.

Example:

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

$$HK^T = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 2 & 2 & -2 & -2 \\ 2 & -2 & 2 & -2 \\ -2 & 2 & 2 & -2 \end{pmatrix} = 2 \underbrace{\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ - & 1 & 1 & - \end{pmatrix}}_{L}$$

Unbiased Hadamard Matrices

If we have a set of Hadamard matrices that are pairwise unbiased, then we have a set of mutually unbiased Hadamard matrices.

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

Can we find any more Hadamard matrices that are unbiased with both H and K? **No.**

Unbiased Hadamard Matrices

There are larger sets of mutually unbiased Hadamard matrices of order 4 if we allow complex entries.

Two differences between the real and complex case:

- Entries must lie on the unit circle.
- Use the conjugate transpose, H^*, instead of the transpose.

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix}, H_2 = \begin{pmatrix} 1 & - & j & j \\ 1 & - & i & i \\ 1 & 1 & i & j \\ 1 & 1 & j & i \end{pmatrix},$$

$$H_3 = \begin{pmatrix} 1 & j & j & - \\ 1 & j & i & i \\ 1 & i & i & 1 \\ 1 & i & j & j \end{pmatrix}, H_4 = \begin{pmatrix} 1 & j & - & j \\ 1 & j & 1 & i \\ 1 & i & - & i \\ 1 & i & 1 & j \end{pmatrix}$$

Note: j denotes $-i$.

Deconstruct the Hadamard Matrices

Take the rows of the Hadamard matrices and place them into a set.

$$\begin{pmatrix} 1\,1\,1\,1 \\ 1\,1\,-\,- \\ 1\,-\,1\,- \\ 1\,-\,-\,1 \end{pmatrix}, \begin{pmatrix} 1\,-\,j\,j \\ 1\,-\,i\,i \\ 1\,1\,i\,j \\ 1\,1\,j\,i \end{pmatrix}, \begin{pmatrix} 1\,j\,j\,- \\ 1\,j\,i\,i \\ 1\,i\,i\,1 \\ 1\,i\,j\,j \end{pmatrix}, \begin{pmatrix} 1\,j\,-\,j \\ 1\,j\,1\,i \\ 1\,i\,-\,i \\ 1\,i\,1\,j \end{pmatrix}$$

$$\downarrow$$

$$V = \left\{ \begin{array}{l} \frac{1}{2}(\,1\,1\,1\,1\,), \frac{1}{2}(\,1\,1\,-\,-\,), \frac{1}{2}(\,1\,-\,1\,-\,), \frac{1}{2}(\,1\,-\,-\,1\,), \\ \frac{1}{2}(\,1\,-\,j\,j\,), \frac{1}{2}(\,1\,-\,i\,i\,), \frac{1}{2}(\,1\,1\,i\,j\,), \frac{1}{2}(\,1\,1\,j\,i\,), \\ \frac{1}{2}(\,1\,j\,j\,-\,), \frac{1}{2}(\,1\,j\,i\,i\,), \frac{1}{2}(\,1\,i\,i\,1\,), \frac{1}{2}(\,1\,i\,j\,j\,), \\ \frac{1}{2}(\,1\,j\,-\,j\,), \frac{1}{2}(\,1\,j\,1\,i\,), \frac{1}{2}(\,1\,i\,-\,i\,), \frac{1}{2}(\,1\,i\,1\,j\,) \end{array} \right\}$$

Deconstruct the Hadamard Matrices

$$V = \left\{ \begin{array}{l} \frac{1}{2}\left(\begin{array}{cccc} 1 & 1 & 1 & 1 \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & 1 & - & - \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & - & 1 & - \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & - & - & 1 \end{array} \right), \\ \frac{1}{2}\left(\begin{array}{cccc} 1 & - & j & j \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & - & i & i \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & 1 & i & j \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & 1 & j & i \end{array} \right), \\ \frac{1}{2}\left(\begin{array}{cccc} 1 & j & j & - \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & j & i & i \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & i & i & 1 \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & i & j & j \end{array} \right), \\ \frac{1}{2}\left(\begin{array}{cccc} 1 & j & - & j \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & j & 1 & i \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & i & - & i \end{array} \right), \frac{1}{2}\left(\begin{array}{cccc} 1 & i & 1 & j \end{array} \right) \end{array} \right\}$$

Properties:

- Take any two vectors from the same matrix, inner product is 0.
- Take any two vectors from different matrices, the inner product has absolute value $\frac{1}{2}$.

$$\left(\frac{1}{2}H\right)\left(\frac{1}{2}K\right)^* = \frac{1}{4}HK^* = \frac{1}{4}\left(\sqrt{4}L\right) = \frac{1}{2}L$$

Biangular Lines

Definition

A set of unit vectors V is called biangular if for any (distinct) pair of vectors, $u, v \in V$,

$$|\langle u, v\rangle| \in \{0, \alpha\},$$

where $0 < \alpha < 1$.

Question

Given n (the dimension) and α, what is the maximum size of a set of biangular vectors?

Bounds on the Size of Sets

Theorem

Let $V \subset \mathbb{R}^n$ *be a set of unit vectors. If* $|\langle v, w\rangle| \in \{0, \alpha\}$ *for all* $v, w \in V$, $v \neq w$, *where* $0 < \alpha < 1$, *then*

$$|V| \leq \binom{n+2}{3}.$$

Proof

We can show that $A = \{X_v := v \otimes v \otimes v \mid v \in V\} \subset S^3(\mathbb{R}^n)$ *is a set of linearly independent vectors in* $S^3(\mathbb{R}^n)$ *which has dimension* $\binom{n+2}{3}$.

Bounds on the Size of Sets

Theorem

Let $V \subset \mathbb{R}^n$ be a set of unit vectors. If $|\langle v, w\rangle| \in \{0, \alpha\}$ for all $v, w \in V$, $v \neq w$, where $0 < \alpha < 1$, then

$$|V| \leq \binom{n+2}{3}.$$

Theorem

Let $V \subset \mathbb{C}^n$ be a set of unit vectors. If $|\langle v, w\rangle| \in \{0, \alpha\}$ for all $v, w \in V$, $v \neq w$, where $0 < \alpha < 1$, then

$$|V| \leq n\binom{n+1}{2}.$$

Bounds on the Size of Sets – Now with α!

Theorem

Let $V \subset \mathbb{R}^n$ be a set of unit vectors. If $|\langle v, w\rangle| \in \{0, \alpha\}$ for all $v, w \in V$, $v \neq w$, where $0 < \alpha < 1$, then

$$|V| \leq \frac{n(n+2)(1-\alpha^2)}{3-(n+2)\alpha^2}$$

if the denominator is positive.

Theorem

Let $V \subset \mathbb{C}^n$ be a set of unit vectors. If $|\langle v, w\rangle| \in \{0, \alpha\}$ for all $v, w \in V$, $v \neq w$, where $0 < \alpha < 1$, then

$$|V| \leq \frac{n(n+1)(1-\alpha^2)}{2-(n+1)\alpha^2}$$

if the denominator is positive.

Comparisons

- AUB (Absolute Upper Bound) – Bound without α
- SUB (Special Upper Bound) – Bound with α

		$\mathbb{R}^n$		$\mathbb{C}^n$	
n	α	AUB	SUB	AUB	SUB
2	1/2	4	3	6	18/5
3	1/2	10	45/7	18	9
4	1/2	20	12	40	20
5	1/2	35	21	75	45
6	1/2	56	36	126	126
7	1/2	84	63	196	N/A
8	1/2	120	120	288	N/A
9	1/2	165	297	405	N/A
10	1/2	220	N/A	550	N/A

Old Example

$$V = \left\{ \begin{array}{l} \frac{1}{2}(\ 1\,1\,1\,1\ ), \frac{1}{2}(\ 1\,1 - -\ ), \frac{1}{2}(\ 1 - 1 -\ ), \frac{1}{2}(\ 1 - - 1\ ), \\ \frac{1}{2}(\ 1 - j\ j\ ), \frac{1}{2}(\ 1 - i\ i\ ), \frac{1}{2}(\ 1\,1\ i\ j\ ), \frac{1}{2}(\ 1\,1\ j\ i\ ), \\ \frac{1}{2}(\ 1\ j\ j -\ ), \frac{1}{2}(\ 1\ j\ i\ i\ ), \frac{1}{2}(\ 1\ i\ i\ 1\ ), \frac{1}{2}(\ 1\ i\ j\ j\ ), \\ \frac{1}{2}(\ 1\ j - j\ ), \frac{1}{2}(\ 1\ j\ 1\ i\ ), \frac{1}{2}(\ 1\ i - i\ ), \frac{1}{2}(\ 1\ i\ 1\ j\ ) \end{array} \right\}$$

V has 16 vectors, but the special upper bound is 20, can we attain this amount? **Yes.**

$$V \cup \left\{ (1\ \ 0\ \ 0\ \ 0), (0\ \ 1\ \ 0\ \ 0), (0\ \ 0\ \ 1\ \ 0), (0\ \ 0\ \ 0\ \ 1) \right\}$$

Unbiased Hadamard Matrices

When you have m mutually unbiased Hadamard matrices (in $\mathbb{C}$) of order n, then we can deconstruct the matrices into mn biangular vectors with $\alpha = \frac{1}{\sqrt{n}}$. We can always add the rows of the identity to the set of vectors and preserve biangularity.

$$(m+1)n = mn + n \leq \frac{n(n+1)(1-\alpha^2)}{2-(n+1)\alpha^2} = (n+1)n$$

So...

$$m \leq n.$$

When you have m mutually unbiased Hadamard matrices (in $\mathbb{R}$), then

$$m \leq \frac{n}{2}.$$

Unbiased Hadamard Matrices

When $n = 4$, this bound is attained (seen above). When else is the bound attained?

Theorem

If n is a prime power, then there are n mutually unbiased Hadamard matrices. (Constructive proof)

Conjecture

No other value of n attains this upper bound.

In the first non-prime power case ($n = 6$), the upper bound is conjectured to be only 2. (Strong computational evidence to support)

Orthogonality Between Matrices

So far, the examples we have given always have an inner product of zero within a matrix, and nonzero between different matrices.

We will loosen that slightly to allow the inner product between matrices to be zero as well.

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

The inner product between vectors from H and K are in $\{0, \pm 4\}$.

Orthogonality Between Matrices

In fact, we can find 8 Hadamard matrices that satisfy this property!

11111111	111–1–11	11–––1–1	1––––1––
11–1––1–	1–11111–	1–––111–	111–––1–
1––11––1	1––1––11	1–1–––11	11––1111
1––––111	11–11–––	1111–11–	1–11–111
11––11––	11–––11–	111–1–––	1–1–1––1
111––––1	1–1–––––	1–1111–1	111111––
1–11–1––	1–––11–1	1––1––––	11–1–––1
1–1–1–1–	1111–1–1	11–11–11	1––11–1–
1–1––1–1	1––1–1–1	111––1––	11––1–1–
111–111–	1–––1–11	1–1–1111	1–11––1–
11––––11	11–1111–	1–––––1–	1––11111
1––1–11–	1111––11	11–1–111	11111––1
1–––1–––	1–111–––	11––1––1	111––111
1111––––	1–1––11–	1––111––	1–1–11––
11–111–1	111–11–1	1–11–––1	1––––––1
1–111–11	11––––––	11111–1–	11–1–1––

Orthogonality Between Matrices

But we introduced a problem...

- Inner product between the 8 Hadamard matrices:

$$\alpha = \frac{1}{2}$$

- Inner product between a Hadamard matrix and the identity:

$$\alpha = \frac{1}{\sqrt{8}}$$

So we **cannot** add the identity in this case.

Orthogonality Between Matrices

We can fix it! There are 7 weighing matrices, $W(8,2)$, who have pairwise inner products that fall in $\left\{0, \pm\frac{1}{2}\right\}$.

So we have

$$\underbrace{8 \cdot 8}_{\textit{Hadamard}} + \underbrace{7 \cdot 8}_{\textit{Weighing}} = 120$$

vectors. This attains the special upper bound!

Orthogonality Between Matrices

We were able to construct 32 Hadamard matrices whose pairwise multiplication are in $\{0, \pm 8\}$.

We found a set of $128 \cdot 128$ vectors that had the correct inner products, but could not partition them into Hadamard matrices.

These two (and a half) cases led us to the following conjecture.

Orthogonality Between Matrices

Conjecture (B., Kharaghani, Ramp (2013))

Let $n = 2^{2k+1}$. Then there exists a set of n real Hadamard matrices, $\{H_1, H_2, \ldots, H_n\}$, so that the entries of $H_i H_j^t$ $(i \neq j)$ contain exactly two elements, 0 and 2^{k+1} (up to absolute value).

Theorem (Nozaki, Suda (2013))

Let $n = 2^{2k+1}$. Then there exists a set of n real Hadamard matrices, $\{H_1, H_2, \ldots, H_n\}$, so that the entries of $H_i H_j^t$ $(i \neq j)$ contain exactly two elements, 0 and 2^{k+1} (up to absolute value).

Proof.

Detailed coding theory techniques. □

Weighing Matrices

So far, we have only used Hadamard matrices to construct sets of biangular vectors. But this is not needed. We will now examine a slightly different type of matrices, weighing matrices:

Definition

A weighing matrix, W, is an $n \times n$ matrix with entries in $\{0, \pm 1\}$ such that $WW^T = wI$ for some w. They are denoted $W(n, w)$.

Example:

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

is a $W(7, 4)$.

Unbiased Weighing Matrices

Two weighing matrices are unbiased if $HK^T = \sqrt{w}L$, where L is a weighing matrix of the same weight as both H and K.

Example:

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

Unbiased Weighing Matrices

By viewing the rows of the matrices as vectors again, we can use the special bound to give us a maximal number of mutually unbiased weighing matrices. (Note that $\alpha = \frac{1}{\sqrt{w}}$ and that we may add the rows of the identity to this set)

If we have a set of m mutually unbiased weighing matrices of order n and weight w (with all real entries), then

$$m \leq \frac{w(n-1)}{3w-(n+2)}.$$

If we have a set of m mutually unbiased weighing matrices of order n and weight w (with complex entries), then

$$m \leq \frac{w(n-1)}{2w-(n+1)}.$$

Unbiased Weighing Matrices

The bounds for unbiased weighing matrices are quite a bit higher than for Hadamard matrices.

For example, for $W(6,4)$ in the complex setting, the special upper bound is 20 weighing matrices. (In fact, this is also the absolute upper bound for $n = 6$.) This bound is attained using weighing matrices with entries consisting solely of sixth roots of unity.

Unbiased Weighing Matrices

List of sets that attain the special upper bound:

Type	$\mathbb{R}^n$ or $\mathbb{C}^n$	SUB
$W(2,2)$	$\mathbb{C}^n$	2
$W(3,3)$	$\mathbb{C}^n$	3
$W(4,3)$	$\mathbb{C}^n$	9
$W(4,4)$	$\mathbb{C}^n$	4
$W(5,5)$	$\mathbb{C}^n$	5
$W(6,4)$	$\mathbb{C}^n$	20
$W(7,4)$	$\mathbb{R}^n$	8
$W(7,7)$	$\mathbb{C}^n$	7
$W(8,4)$	$\mathbb{R}^n$	14

For (almost) every type of weighing matrix with $n \leq 7$ that is missing from this list, we can prove that you cannot attain the SUB with mutually unbiased weighing matrices.

When We Meet the Special Upper Bound

Some nice objects come from this, including

Strongly Regular Graphs (SRGs).

An $SRG(v, k, \lambda, \mu)$ is an undirected graph that satisfies the following:

1. v nodes.
2. Every node has degree k.
3. Every adjacent pair of nodes has λ common neighbours.
4. Every non-adjacent pair of nodes has μ common neighbours.

When We Meet the Special Upper Bound

If V is a biangular set of vectors that attains the special upper bound, then 'perpendicularity' defines an SRG.

Moreover, if the vectors come from a set of mutually unbiased weighing matrices, then the graph will be either geometric or pseudogeometric.

Table of Generated SRGs

Type	$\mathbb{R}^n$ or $\mathbb{C}^n$	SUB	SRG
$W(2,2)$	$\mathbb{C}^n$	2	$SRG(6,4,2,4)$
$W(3,3)$	$\mathbb{C}^n$	3	$SRG(12,9,6,9)$
$W(4,3)$	$\mathbb{C}^n$	9	$SRG(40,27,18,18)$
$W(4,4)$	$\mathbb{C}^n$	4	$SRG(20,16,12,16)$
$W(5,5)$	$\mathbb{C}^n$	5	$SRG(30,25,20,25)$
$W(6,4)$	$\mathbb{C}^n$	20	$SRG(126,80,52,48)$
$W(7,4)$	$\mathbb{R}^n$	8	$SRG(63,32,16,16)$
$W(7,7)$	$\mathbb{C}^n$	7	$SRG(56,49,42,49)$
$W(8,4)$	$\mathbb{R}^n$	14	$SRG(120,56,28,24)$

Other Constructions

- Hadamard Matrices (the $8, 32, 128, \ldots$ case)
  $\longrightarrow$ 3-Association Schemes
- Weighing Matrices + MSLS
  $\longrightarrow$ 3-Association Scheme
- Hadamard Matrices + MSLS + MSLS (multi-angular)
  $\longrightarrow$ 6-Association Scheme
  $\longrightarrow$ 5-Association Scheme
  $\longrightarrow$ 4-Association Scheme
  $\longrightarrow$ 3-Association Scheme
  $\longrightarrow$ 2-Association Scheme = SRG

Open Questions

- Is there a better upper bound when the vectors are flat?
- Is there an infinite family of weighing matrices that meet the special upper bound? (Other than Hadamards of prime power order)
- If a set is *maximal* (in some sense), does it always form an SRG or association scheme?
- Is there a one-to-one relationship between mutually unbiased Hadamard matrices and mutually orthogonal Latin squares (MOLS)?

Thank you!

=)