

# A Maximal Set of Unbiased Butson Hadamard Matrices

Caleb Van't Land

University of Lethbridge

# Hadamard Matrices

A **Hadamard Matrix** of order  $n$  is an  $n \times n$  matrix  $H$  with elements drawn from the set  $\{1, -1\}$  that satisfies  $HH^t = nI$ .

# Hadamard Matrices

A **Hadamard Matrix** of order  $n$  is an  $n \times n$  matrix  $H$  with elements drawn from the set  $\{1, -1\}$  that satisfies  $HH^t = nI$ . For example, the following is a Hadamard Matrix of order 4,

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

# Bush-Type Hadamard Matrices

A Hadamard Matrix of order  $n^2$  is called **Bush-type** if it can be subdivided into  $n^2$  blocks of order  $n$  such that blocks on the main diagonal consist entirely of 1s, and all other blocks have row and columns sums of 0.

# Bush-Type Hadamard Matrices

A Hadamard Matrix of order  $n^2$  is called **Bush-type** if it can be subdivided into  $n^2$  blocks of order  $n$  such that blocks on the main diagonal consist entirely of 1s, and all other blocks have row and columns sums of 0.

For example, the following is a Bush-type Hadamard Matrix of order 4,

$$\left[ \begin{array}{cc|cc} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ \hline - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \end{array} \right]$$

# Bush-Type Hadamard Matrices

A Hadamard Matrix of order  $n^2$  is called **Bush-type** if it can be subdivided into  $n^2$  blocks of order  $n$  such that blocks on the main diagonal consist entirely of 1s, and all other blocks have row and column sums of 0.

For example, the following is a Bush-type Hadamard Matrix of order 4,

$$\left[ \begin{array}{cc|cc} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ \hline - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \end{array} \right]$$

In a paper published to the Journal of Combinatorial Theory in 2002, Kharaghani and Janko presented a Bush-type Hadamard Matrix of order 36 and used it to construct a  $SRG(936, 375, 150, 150)$ .

# Unbiased Hadamard Matrices

A pair of Hadamard matrices of order  $n^2$ ,  $H_1$  and  $H_2$ , are said to be **Unbiased** if  $n^{-1}H_1H_2^t$  is also a Hadamard matrix.

# Unbiased Hadamard Matrices

A pair of Hadamard matrices of order  $n^2$ ,  $H_1$  and  $H_2$ , are said to be **Unbiased** if  $n^{-1}H_1H_2^t$  is also a Hadamard matrix.

For example, the following two Hadamard matrices are unbiased,

$$\begin{bmatrix} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{bmatrix}$$



# Unbiased Hadamard Matrices

$$\frac{1}{2} \left( \begin{bmatrix} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ 1 & - & - & - \\ 1 & - & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ 1 & - & - & - \\ 1 & - & 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & - & 1 \\ - & 1 & - & 1 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

# Unbiased Hadamard Matrices

A set of Hadamard matrices is said to be **Mutually Unbiased** if each pair of distinct matrices from the set is unbiased.

# Unbiased Hadamard Matrices

A set of Hadamard matrices is said to be **Mutually Unbiased** if each pair of distinct matrices from the set is unbiased.

In an Electronic Journal of Combinatorics article published in 2015, Kharaghani, Sasani, and Suda showed that the number of Mutually Unbiased Hadamard matrices of order  $n^2$  is at most  $n - 1$ .

# Butson Hadamard Matrices

A **Butson Hadamard Matrix** of order  $n$  is a matrix  $H$  with elements drawn from the  $m$ -th roots of unity which satisfies  $HH^* = nI$ . We denote such a matrix  $BH(n, m)$ .

# Butson Hadamard Matrices

A **Butson Hadamard Matrix** of order  $n$  is a matrix  $H$  with elements drawn from the  $m$ -th roots of unity which satisfies  $HH^* = nI$ . We denote such a matrix  $BH(n, m)$ .

Let  $\zeta$  be a primitive fifth root of unity, then the following is a  $BH(5, 5)$ ,

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 \\ 1 & \zeta^2 & \zeta^4 & \zeta & \zeta^3 \\ 1 & \zeta^3 & \zeta & \zeta^4 & \zeta^2 \\ 1 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta \end{bmatrix}$$

# Butson Hadamard Matrices

A **Butson Hadamard Matrix** of order  $n$  is a matrix  $H$  with elements drawn from the  $m$ -th roots of unity which satisfies  $HH^* = nI$ . We denote such a matrix  $BH(n, m)$ .

Let  $\zeta$  be a primitive fifth root of unity, then the following is a  $BH(5, 5)$ ,

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 \\ 1 & \zeta^2 & \zeta^4 & \zeta & \zeta^3 \\ 1 & \zeta^3 & \zeta & \zeta^4 & \zeta^2 \\ 1 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta \end{bmatrix}$$

There exists a  $BH(n, n)$  for every order  $n$ .

# Butson Hadamard Matrices

A **Butson Hadamard Matrix** of order  $n$  is a matrix  $H$  with elements drawn from the  $m$ -th roots of unity which satisfies  $HH^* = nI$ . We denote such a matrix  $BH(n, m)$ .

Let  $\zeta$  be a primitive fifth root of unity, then the following is a  $BH(5, 5)$ ,

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 \\ 1 & \zeta^2 & \zeta^4 & \zeta & \zeta^3 \\ 1 & \zeta^3 & \zeta & \zeta^4 & \zeta^2 \\ 1 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta \end{bmatrix}$$

There exists a  $BH(n, n)$  for every order  $n$ .

A Butson Hadamard Matrix is said to be **Normalized** if the first row and column consist entirely of 1s.

# Bush-type Butson Hadamard Matrices

A Butson Hadamard Matrix of order  $n^2$  is called **Bush-type** if it can be subdivided into  $n^2$  blocks of order  $n$  such that blocks on the main diagonal consist entirely of 1s, and all other blocks have row and columns sums of 0.



Let  $\zeta$  be a primitive fifth root of unity, then the following is a Bush-type  $BH(5^2, 5)$ ,

1	1	1	1	1	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^3$	1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^4$	$\zeta^3$	$\zeta^2$	$\zeta$
1	1	1	1	1	$\zeta^4$	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^3$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^2$	1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta$	1	$\zeta^4$	$\zeta^3$	$\zeta^2$
1	1	1	1	1	$\zeta^3$	$\zeta^4$	1	$\zeta$	$\zeta^2$	$\zeta$	$\zeta^3$	1	$\zeta^2$	$\zeta^4$	$\zeta^4$	$\zeta^2$	1	$\zeta^3$	$\zeta$	$\zeta^2$	$\zeta$	1	$\zeta^4$	$\zeta^3$
1	1	1	1	1	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta$	$\zeta^4$	$\zeta$	$\zeta^3$	1	$\zeta^2$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^3$	$\zeta^3$	$\zeta^2$	$\zeta$	1	$\zeta^4$
1	1	1	1	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^3$	1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^4$	$\zeta^3$	$\zeta^2$	$\zeta$	1
$\zeta$	1	$\zeta^4$	$\zeta^3$	$\zeta^2$	1	1	1	1	1	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^3$	1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^2$
$\zeta^2$	$\zeta$	1	$\zeta^4$	$\zeta^3$	1	1	1	1	1	$\zeta^4$	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^3$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^2$	1	$\zeta^3$	$\zeta$	$\zeta^4$
$\zeta^3$	$\zeta^2$	$\zeta$	1	$\zeta^4$	1	1	1	1	1	$\zeta^3$	$\zeta^4$	1	$\zeta$	$\zeta^2$	$\zeta$	$\zeta^3$	1	$\zeta^2$	$\zeta^4$	$\zeta^4$	$\zeta^2$	1	$\zeta^3$	$\zeta$
$\zeta^4$	$\zeta^3$	$\zeta^2$	$\zeta$	1	1	1	1	1	1	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta$	$\zeta^4$	$\zeta$	$\zeta^3$	1	$\zeta^2$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^3$
1	$\zeta^4$	$\zeta^3$	$\zeta^2$	$\zeta$	1	1	1	1	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^3$	1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^2$	1
$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^3$	$\zeta$	1	$\zeta^4$	$\zeta^3$	$\zeta^2$	1	1	1	1	1	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^3$
$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^2$	$\zeta$	1	$\zeta^4$	$\zeta^3$	1	1	1	1	1	$\zeta^4$	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^3$	1	$\zeta^2$	$\zeta^4$	$\zeta$
1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^2$	$\zeta^3$	$\zeta^2$	$\zeta$	1	$\zeta^4$	1	1	1	1	1	$\zeta^3$	$\zeta^4$	1	$\zeta$	$\zeta^2$	$\zeta$	$\zeta^3$	1	$\zeta^2$	$\zeta^4$
$\zeta^2$	1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^4$	$\zeta^3$	$\zeta^2$	$\zeta$	1	1	1	1	1	1	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta$	$\zeta^4$	$\zeta^3$	1	$\zeta^2$	$\zeta^4$
$\zeta^4$	$\zeta^2$	1	$\zeta^3$	$\zeta$	1	$\zeta^4$	$\zeta^3$	$\zeta^2$	$\zeta$	1	1	1	1	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^3$	1
$\zeta$	$\zeta^3$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^3$	$\zeta^2$	1	$\zeta^4$	$\zeta^3$	$\zeta^2$	1	1	1	1	1	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^4$
$\zeta^2$	$\zeta$	$\zeta^3$	1	$\zeta^4$	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^3$	$\zeta^2$	$\zeta$	1	$\zeta^4$	1	1	1	1	1	$\zeta^4$	1	$\zeta$	$\zeta^2$	$\zeta^3$
$\zeta^3$	$\zeta^4$	$\zeta$	$\zeta^3$	1	1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^2$	$\zeta^3$	$\zeta^2$	$\zeta$	1	$\zeta^4$	1	1	1	1	1	$\zeta^3$	$\zeta^4$	1	$\zeta$	$\zeta^2$
1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^3$	$\zeta^2$	1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^4$	$\zeta^3$	$\zeta^2$	$\zeta$	1	1	1	1	1	1	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta$
$\zeta^3$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^3$	$\zeta$	1	$\zeta^4$	$\zeta^3$	$\zeta^2$	$\zeta$	1	1	1	1	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^4$	1
$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta$	$\zeta^3$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^3$	$\zeta$	1	$\zeta^4$	$\zeta^3$	$\zeta^2$	1	1	1	1	1
1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^4$	$\zeta^4$	$\zeta$	$\zeta^3$	1	$\zeta^2$	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^2$	$\zeta$	1	$\zeta^4$	$\zeta^3$	1	1	1	1	1
$\zeta^4$	1	$\zeta$	$\zeta^2$	$\zeta^3$	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^3$	1	1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^2$	$\zeta^3$	$\zeta$	1	$\zeta^4$	1	1	1	1	1	
$\zeta^3$	$\zeta^4$	1	$\zeta$	$\zeta^2$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^3$	$\zeta^2$	1	$\zeta^3$	$\zeta$	$\zeta^4$	$\zeta^4$	$\zeta^3$	$\zeta^2$	$\zeta$	1	1	1	1	1	1
$\zeta^2$	$\zeta^3$	$\zeta^4$	1	$\zeta$	$\zeta^3$	1	$\zeta^2$	$\zeta^4$	$\zeta$	$\zeta^4$	$\zeta^2$	1	$\zeta^3$	$\zeta$	1	$\zeta^4$	$\zeta^3$	$\zeta^2$	$\zeta$	1	1	1	1	1

# Unbiased Butson Hadamard Matrices

A pair of  $BH(n^2, m)$ s,  $H_1$  and  $H_2$ , are said to be **Unbiased** if  $n^{-1}H_1H_2^*$  is also a  $BH(n^2, m)$ .

# Unbiased Butson Hadamard Matrices

A pair of  $BH(n^2, m)$ s,  $H_1$  and  $H_2$ , are said to be **Unbiased** if  $n^{-1}H_1H_2^*$  is also a  $BH(n^2, m)$ .

Let  $\zeta$  be a primitive third root of unity. Then the following are a pair of unbiased  $BH(9, 3)$ s,

$$\left[ \begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & 1 & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta \\ 1 & 1 & 1 & \zeta^2 & 1 & \zeta & \zeta & 1 & \zeta^2 \\ 1 & 1 & 1 & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta & 1 \\ \hline 1 & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta & 1 & 1 & 1 \\ \zeta^2 & 1 & \zeta & \zeta & 1 & \zeta^2 & 1 & 1 & 1 \\ \zeta & \zeta^2 & 1 & \zeta^2 & \zeta & 1 & 1 & 1 & 1 \\ \hline 1 & \zeta^2 & \zeta & 1 & 1 & 1 & 1 & \zeta & \zeta^2 \\ \zeta & 1 & \zeta^2 & 1 & 1 & 1 & \zeta^2 & 1 & \zeta \\ \zeta^2 & \zeta & 1 & 1 & 1 & 1 & \zeta & \zeta^2 & 1 \end{array} \right], \quad \left[ \begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & 1 & \zeta^2 & \zeta & 1 & \zeta & \zeta^2 \\ 1 & 1 & 1 & \zeta & 1 & \zeta^2 & \zeta^2 & 1 & \zeta \\ 1 & 1 & 1 & \zeta^2 & \zeta & 1 & \zeta & \zeta^2 & 1 \\ \hline 1 & \zeta^2 & \zeta & 1 & \zeta & \zeta^2 & 1 & 1 & 1 \\ \zeta & 1 & \zeta^2 & \zeta^2 & 1 & \zeta & 1 & 1 & 1 \\ \zeta^2 & \zeta & 1 & \zeta & \zeta^2 & 1 & 1 & 1 & 1 \\ \hline 1 & \zeta & \zeta^2 & 1 & 1 & 1 & 1 & \zeta^2 & \zeta \\ \zeta^2 & 1 & \zeta & 1 & 1 & 1 & \zeta & 1 & \zeta^2 \\ \zeta & \zeta^2 & 1 & 1 & 1 & 1 & \zeta^2 & \zeta & 1 \end{array} \right]$$



# Mutually Unbiased Butson Hadamard Matrices

A set of  $BH(n^2, m)$ s is said to be **mutually unbiased** if every pair of matrices from the set is unbiased.

# Mutually Unbiased Butson Hadamard Matrices

A set of  $BH(n^2, m)$ s is said to be **mutually unbiased** if every pair of matrices from the set is unbiased.

Continuing to let  $\zeta$  be a primitive third root of unity, the following set of 3  $BH(9, 3)$ s is mutually unbiased.

$$\left\{ \left[ \begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & 1 & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta \\ 1 & 1 & 1 & \zeta^2 & 1 & \zeta & \zeta & 1 & \zeta^2 \\ 1 & 1 & 1 & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta & 1 \\ \hline 1 & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta & 1 & 1 & 1 \\ \zeta^2 & 1 & \zeta & \zeta & 1 & \zeta^2 & 1 & 1 & 1 \\ \zeta & \zeta^2 & 1 & \zeta^2 & \zeta & 1 & 1 & 1 & 1 \\ \hline 1 & \zeta^2 & \zeta & 1 & 1 & 1 & 1 & \zeta & \zeta^2 \\ \zeta & 1 & \zeta^2 & 1 & 1 & 1 & \zeta^2 & 1 & \zeta \\ \zeta^2 & \zeta & 1 & 1 & 1 & 1 & \zeta & \zeta^2 & 1 \end{array} \right], \left[ \begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & 1 & \zeta^2 & \zeta & 1 & \zeta & \zeta^2 \\ 1 & 1 & 1 & \zeta & 1 & \zeta^2 & \zeta^2 & 1 & \zeta \\ 1 & 1 & 1 & \zeta^2 & \zeta & 1 & \zeta & \zeta^2 & 1 \\ \hline 1 & \zeta^2 & \zeta & 1 & \zeta & \zeta^2 & 1 & 1 & 1 \\ \zeta & 1 & \zeta^2 & \zeta^2 & 1 & \zeta & 1 & 1 & 1 \\ \zeta^2 & \zeta & 1 & \zeta & \zeta^2 & 1 & 1 & 1 & 1 \\ \hline 1 & \zeta & \zeta^2 & 1 & 1 & 1 & 1 & 1 & \zeta^2 \\ \zeta^2 & 1 & \zeta & 1 & 1 & 1 & \zeta & 1 & \zeta^2 \\ \zeta & \zeta^2 & 1 & 1 & 1 & 1 & \zeta^2 & \zeta & 1 \end{array} \right], \left[ \begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & \zeta^2 & \zeta^2 & \zeta^2 & \zeta & \zeta & \zeta \\ 1 & 1 & 1 & \zeta & \zeta & \zeta & \zeta^2 & \zeta^2 & \zeta^2 \\ \hline 1 & \zeta & \zeta^2 & 1 & \zeta & \zeta^2 & 1 & \zeta & \zeta^2 \\ 1 & \zeta & \zeta^2 & \zeta^2 & 1 & \zeta & \zeta & \zeta^2 & 1 \\ 1 & \zeta & \zeta^2 & \zeta & \zeta^2 & 1 & \zeta^2 & 1 & \zeta \\ \hline 1 & \zeta^2 & \zeta & 1 & \zeta^2 & \zeta & 1 & \zeta^2 & \zeta \\ 1 & \zeta^2 & \zeta & \zeta^2 & \zeta & 1 & \zeta & 1 & \zeta^2 \\ 1 & \zeta^2 & \zeta & \zeta & 1 & \zeta^2 & \zeta^2 & \zeta & 1 \end{array} \right] \right\}$$

# Latin Squares

A **Latin Square** over a set of  $n$  elements is an  $n \times n$  matrix where every element in the set occurs exactly once in each row and column.

# Latin Squares

A **Latin Square** over a set of  $n$  elements is an  $n \times n$  matrix where every element in the set occurs exactly once in each row and column.

For example, the following is a Latin Square on  $\{0, 1, 2, 3\}$

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}$$



# Suitable Latin Squares

A pair of Latin Squares are called **Suitable** in the event that comparing any row from the first square with any row from the second shows that they share an element in exactly one position.

# Suitable Latin Squares

A pair of Latin Squares are called **Suitable** in the event that comparing any row from the first square with any row from the second shows that they share an element in exactly one position. The following pair of Latin Squares is suitable,

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{bmatrix}$$

# Suitable Latin Squares

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{bmatrix}$$

# Suitable Latin Squares

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{bmatrix}$$

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 3 \end{array}$$

# Suitable Latin Squares

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{bmatrix}$$

# Suitable Latin Squares

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{bmatrix}$$

$$\begin{array}{cccc} 3 & 2 & 1 & 0 \\ 0 & 3 & 1 & 2 \end{array}$$

# The Product of Suitable Latin Squares

If  $L_1$  and  $L_2$  are suitable latin squares, then we can define  $L_1 \circ L_2$  to be a matrix whose  $(i, j)$ -th entry is the point of agreement between row  $i$  of  $L_1$  and row  $j$  of  $L_2$ .

# The Product of Suitable Latin Squares

If  $L_1$  and  $L_2$  are suitable latin squares, then we can define  $L_1 \circ L_2$  to be a matrix whose  $(i, j)$ -th entry is the point of agreement between row  $i$  of  $L_1$  and row  $j$  of  $L_2$ . For example,

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \circ \begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \end{bmatrix}$$



# The Product of Suitable Latin Squares

If  $L_1$  and  $L_2$  are suitable latin squares, then we can define  $L_1 \circ L_2$  to be a matrix whose  $(i, j)$ -th entry is the point of agreement between row  $i$  of  $L_1$  and row  $j$  of  $L_2$ . For example,

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \circ \begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \end{bmatrix}$$

The product of two Latin Squares is itself a Latin Square.

# Mutually Suitable Latin Squares (MSLS)

A set of Latin Squares is called **Mutually Suitable** if every pair of Latin Squares in the set is Suitable.

# Mutually Suitable Latin Squares (MSLS)

A set of Latin Squares is called **Mutually Suitable** if every pair of Latin Squares in the set is Suitable.

The following set of Latin Squares is mutually suitable,

$$\left\{ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \end{bmatrix} \right\}$$

# Mutually Suitable Latin Squares (MSLS)

A set of Latin Squares is called **Mutually Suitable** if every pair of Latin Squares in the set is Suitable.

The following set of Latin Squares is mutually suitable,

$$\left\{ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \end{bmatrix} \right\}$$

If  $q$  is a prime power, then there is a set of  $q - 1$  MSLS of size  $q$ .

# The Construction

Let  $q$  be a prime power, and let  $H$  be a normalized  $BH(q, q)$ .

# The Construction

Let  $q$  be a prime power, and let  $H$  be a normalized  $BH(q, q)$ . As an example, we will performing the construction using  $q = 4$  and the following  $BH(4, 4)$ . Here  $\zeta$  is a primitive fourth root of unity,

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 \\ 1 & \zeta^2 & 1 & \zeta^2 \\ 1 & \zeta^3 & \zeta^2 & \zeta \end{bmatrix}$$

# The Construction

Label the rows of  $H$  as  $r_0, \dots, r_{q-1}$ . The **Auxiliary Matrices** of  $H$  are  $c_i = r_i^* r_i$  for  $i = 0, \dots, q - 1$ .

# The Construction

Label the rows of  $H$  as  $r_0, \dots, r_{q-1}$ . The **Auxiliary Matrices** of  $H$  are  $c_i = r_i^* r_i$  for  $i = 0, \dots, q - 1$ .

In our example, the auxiliary matrices are the following,

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \zeta & \zeta^2 & \zeta^3 \\ \zeta^3 & 1 & \zeta & \zeta^2 \\ \zeta^2 & \zeta^3 & 1 & \zeta \\ \zeta & \zeta^2 & \zeta^3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \zeta^2 & 1 & \zeta^2 \\ \zeta^2 & 1 & \zeta^2 & 1 \\ 1 & \zeta^2 & 1 & \zeta^2 \\ \zeta^2 & 1 & \zeta^2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \zeta^3 & \zeta^2 & \zeta \\ \zeta & 1 & \zeta^3 & \zeta^2 \\ \zeta^2 & \zeta & 1 & \zeta^3 \\ \zeta^3 & \zeta^2 & \zeta & 1 \end{bmatrix}$$



# The Construction

Label the rows of  $H$  as  $r_0, \dots, r_{q-1}$ . The **Auxiliary Matrices** of  $H$  are  $c_i = r_i^* r_i$  for  $i = 0, \dots, q - 1$ .

In our example, the auxiliary matrices are the following,

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \zeta & \zeta^2 & \zeta^3 \\ \zeta^3 & 1 & \zeta & \zeta^2 \\ \zeta^2 & \zeta^3 & 1 & \zeta \\ \zeta & \zeta^2 & \zeta^3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \zeta^2 & 1 & \zeta^2 \\ \zeta^2 & 1 & \zeta^2 & 1 \\ 1 & \zeta^2 & 1 & \zeta^2 \\ \zeta^2 & 1 & \zeta^2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \zeta^3 & \zeta^2 & \zeta \\ \zeta & 1 & \zeta^3 & \zeta^2 \\ \zeta^2 & \zeta & 1 & \zeta^3 \\ \zeta^3 & \zeta^2 & \zeta & 1 \end{bmatrix}$$

Auxiliary Matrices have the following properties,

- 1  $c_i^* = c_i$
- 2  $c_i c_j = \mathbf{0}$  if  $i \neq j$
- 3  $c_i c_i = q * c_i$
- 4  $\sum_i c_i = q * I$





# The Construction

The set constructed by this method is also maximal in the sense that it is not a proper subset of any set of mutually unbiased  $BH(q^2, q)$ s.

# Proof of Maximality

Select the first row from each matrix in our set. Call these rows  $l_1, \dots, l_{q-1}$  and  $k$ .

$$\begin{array}{l} l_1 \\ l_2 \\ l_3 \\ k \end{array} = \begin{array}{cccc|cccc|cccc|cccc} 1 & 1 & 1 & 1 & 1 & \zeta^2 & 1 & \zeta^2 & 1 & \zeta^3 & \zeta^2 & \zeta & 1 & \zeta & \zeta^2 & \zeta^3 \\ 1 & 1 & 1 & 1 & 1 & \zeta^3 & \zeta^2 & \zeta & 1 & \zeta & \zeta^2 & \zeta^3 & 1 & \zeta^2 & 1 & \zeta^2 \\ 1 & 1 & 1 & 1 & 1 & \zeta & \zeta^2 & \zeta^3 & 1 & \zeta^2 & 1 & \zeta^2 & 1 & \zeta^3 & \zeta^2 & \zeta \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

# Proof of Maximality

Select the first row from each matrix in our set. Call these rows  $l_1, \dots, l_{q-1}$  and  $k$ .

$$\begin{array}{l} l_1 = 1 \ 1 \ 1 \ 1 \mid 1 \ \zeta^2 \ 1 \ \zeta^2 \mid 1 \ \zeta^3 \ \zeta^2 \ \zeta \mid 1 \ \zeta \ \zeta^2 \ \zeta^3 \\ l_2 = 1 \ 1 \ 1 \ 1 \mid 1 \ \zeta^3 \ \zeta^2 \ \zeta \mid 1 \ \zeta \ \zeta^2 \ \zeta^3 \mid 1 \ \zeta^2 \ 1 \ \zeta^2 \\ l_3 = 1 \ 1 \ 1 \ 1 \mid 1 \ \zeta \ \zeta^2 \ \zeta^3 \mid 1 \ \zeta^2 \ 1 \ \zeta^2 \mid 1 \ \zeta^3 \ \zeta^2 \ \zeta \\ k = 1 \ 1 \ 1 \ 1 \mid 1 \ 1 \ 1 \ 1 \mid 1 \ 1 \ 1 \ 1 \mid 1 \ 1 \ 1 \ 1 \end{array}$$

Note that when the rows are arranged into blocks of size  $q$ , the first block consists entirely of 1s and the first column of each block consists entirely of 1s.

# Proof of Maximality

Select the first row from each matrix in our set. Call these rows  $l_1, \dots, l_{q-1}$  and  $k$ .

$$\begin{array}{l} l_1 = 1 \ 1 \ 1 \ 1 \mid 1 \ \zeta^2 \ 1 \ \zeta^2 \mid 1 \ \zeta^3 \ \zeta^2 \ \zeta \mid 1 \ \zeta \ \zeta^2 \ \zeta^3 \\ l_2 = 1 \ 1 \ 1 \ 1 \mid 1 \ \zeta^3 \ \zeta^2 \ \zeta \mid 1 \ \zeta \ \zeta^2 \ \zeta^3 \mid 1 \ \zeta^2 \ 1 \ \zeta^2 \\ l_3 = 1 \ 1 \ 1 \ 1 \mid 1 \ \zeta \ \zeta^2 \ \zeta^3 \mid 1 \ \zeta^2 \ 1 \ \zeta^2 \mid 1 \ \zeta^3 \ \zeta^2 \ \zeta \\ k = 1 \ 1 \ 1 \ 1 \mid 1 \ 1 \ 1 \ 1 \mid 1 \ 1 \ 1 \ 1 \mid 1 \ 1 \ 1 \ 1 \end{array}$$

Note that when the rows are arranged into blocks of size  $q$ , the first block consists entirely of 1s and the first column of each block consists entirely of 1s. Also note that the sum of the elements in columns which don't consist entirely of 1s is 0.

# Proof of Maximality

Let  $Q = \{x \in \mathbb{C} : x^q = 1\}$ .

Since these rows come from mutually unbiased Butson Hadamard Matrices, we have  $|\langle x, y \rangle| = q$  for any distinct  $x, y \in \{l_1, \dots, l_{q-1}, k\}$ .



# Proof of Maximality

Let  $Q = \{x \in \mathbb{C} : x^q = 1\}$ .

Since these rows come from mutually unbiased Butson Hadamard Matrices, we have  $|\langle x, y \rangle| = q$  for any distinct  $x, y \in \{l_1, \dots, l_{q-1}, k\}$ . If our set is not maximal then there exists another  $BH(q^2, q)$  which is unbiased with each matrix in our set.

# Proof of Maximality

Let  $Q = \{x \in \mathbb{C} : x^q = 1\}$ .

Since these rows come from mutually unbiased Butson Hadamard Matrices, we have  $|\langle x, y \rangle| = q$  for any distinct

$x, y \in \{l_1, \dots, l_{q-1}, k\}$ . If our set is not maximal then there exists another  $BH(q^2, q)$  which is unbiased with each matrix in our set.

This means that there must exist some vector  $v$  over  $Q$  such that  $|\langle x, v \rangle| = q$  for all  $x \in \{l_1, \dots, l_{q-1}, k\}$ .

# Proof of Maximality

Let  $Q = \{x \in \mathbb{C} : x^q = 1\}$ .

Since these rows come from mutually unbiased Butson Hadamard Matrices, we have  $|\langle x, y \rangle| = q$  for any distinct

$x, y \in \{l_1, \dots, l_{q-1}, k\}$ . If our set is not maximal then there exists another  $BH(q^2, q)$  which is unbiased with each matrix in our set.

This means that there must exist some vector  $v$  over  $Q$  such that  $|\langle x, v \rangle| = q$  for all  $x \in \{l_1, \dots, l_{q-1}, k\}$ . Assume that such a vector exists, and write  $v = (r_1, \dots, r_q)$  where each  $r_i = (y_{i1}, \dots, y_{iq})$  is a block of length  $q$ .



# Proof of Maximality

Since we've assumed that  $|\langle x, v \rangle| = q$  for all  $x \in \{l_1, \dots, l_{q-1}, k\}$ , the sum of all these dot products has the form  $q(z_1 + \dots + z_q)$  for some  $z_1, \dots, z_q \in \mathbb{Q}$ .

# Proof of Maximality

Since we've assumed that  $|\langle x, v \rangle| = q$  for all  $x \in \{l_1, \dots, l_{q-1}, k\}$ , the sum of all these dot products has the form  $q(z_1 + \dots + z_q)$  for some  $z_1, \dots, z_q \in \mathbb{Q}$ .

We can calculate this sum in another way by performing the multiplication as shown below, summing the columns, then summing the column sums.

$$\begin{array}{cccc|cccc|cccc} (1)y_{11} & \dots & (1)y_{1q} & (1)y_{21} & (*)y_{22} & \dots & (*)y_{2q} & \dots & (1)y_{q1} & (*)y_{q2} & \dots & (*)y_{qq} \\ (1)y_{11} & \dots & (1)y_{1q} & (1)y_{21} & (*)y_{22} & \dots & (*)y_{2q} & \dots & (1)y_{q1} & (*)y_{q2} & \dots & (*)y_{qq} \\ & & \vdots & & & & & & & & & \\ (1)y_{11} & \dots & (1)y_{1q} & (1)y_{21} & (1)y_{22} & \dots & (1)y_{2q} & \dots & (1)y_{q1} & (1)y_{q2} & \dots & (1)y_{qq} \end{array}$$

# Proof of Maximality

Since we've assumed that  $|\langle x, v \rangle| = q$  for all  $x \in \{l_1, \dots, l_{q-1}, k\}$ , the sum of all these dot products has the form  $q(z_1 + \dots + z_q)$  for some  $z_1, \dots, z_q \in \mathbb{Q}$ .

We can calculate this sum in another way by performing the multiplication as shown below, summing the columns, then summing the column sums.

$$\begin{array}{cccc|cccc|cccc} (1)y_{11} & \dots & (1)y_{1q} & (1)y_{21} & (*)y_{22} & \dots & (*)y_{2q} & \dots & (1)y_{q1} & (*)y_{q2} & \dots & (*)y_{qq} \\ (1)y_{11} & \dots & (1)y_{1q} & (1)y_{21} & (*)y_{22} & \dots & (*)y_{2q} & \dots & (1)y_{q1} & (*)y_{q2} & \dots & (*)y_{qq} \\ & & \vdots & & & & & & & & & \\ (1)y_{11} & \dots & (1)y_{1q} & (1)y_{21} & (1)y_{22} & \dots & (1)y_{2q} & \dots & (1)y_{q1} & (1)y_{q2} & \dots & (1)y_{qq} \end{array}$$

Every column either consists entirely of 1s or sums to 0, so calculating the sum using this method gives us the result  $q(y_{11} + \dots + y_{1q} + y_{21} + y_{31} + \dots + y_{q1})$ .

# Proof of Maximality

We now have the following equation,

$$y_{11} + \dots + y_{1q} + y_{21} + y_{31} + \dots + y_{q1} = z_1 + \dots + z_q$$

The left side is a sum of  $2q - 1$  roots of unity, and the right side is a sum of  $q$  roots of unity.



# Proof of Maximality

In a paper published to the Journal of Algebra in 2000, Lam and Leung proved the following theorem,

## Theorem

*For any  $m \in \mathbb{N}$ , a sum of  $n$   $m$ -th roots of unity can only be 0 if  $n$  can be expressed as a linear combination of the prime factors of  $m$ .*

# Proof of Maximality

In a paper published to the Journal of Algebra in 2000, Lam and Leung proved the following theorem,

## Theorem

*For any  $m \in \mathbb{N}$ , a sum of  $n$   $m$ -th roots of unity can only be 0 if  $n$  can be expressed as a linear combination of the prime factors of  $m$ .*

## Corollary

*For any  $q = p^k$  a sum of  $n$   $q$ -th roots of unity can only be 0 if  $n$  is a multiple of  $p$ .*

# Proof of Maximality

This corollary can be used to prove the following lemma,

## Lemma

*For a prime power  $q = p^k$ , if  $S$  and  $T$  are two multisets of  $q$ -th roots of unity then the sum of the elements of  $S$  can only equal the sum of the elements of  $T$  if  $|S|^2 \equiv |T|^2 \pmod{p}$ .*

# Proof of Maximality

Returning to our equation,

$$y_{11} + \dots + y_{1q} + y_{21} + y_{31} + \dots + y_{q1} = z_1 + \dots + z_q$$

The multiset on the left side has  $2q - 1$  elements, and the multiset on the right has  $q$  elements, so the equation can only be satisfied if  $(2q - 1)^2 \equiv q^2 \pmod{p}$ .

# Proof of Maximality

Returning to our equation,

$$y_{11} + \dots + y_{1q} + y_{21} + y_{31} + \dots + y_{q1} = z_1 + \dots + z_q$$

The multiset on the left side has  $2q - 1$  elements, and the multiset on the right has  $q$  elements, so the equation can only be satisfied if  $(2q - 1)^2 \equiv q^2 \pmod{p}$ .

Since  $(2q - 1)^2 \equiv q^2 \pmod{p}$  is false for all  $q = p^n$ , it follows that our equation cannot be satisfied and there is no vector  $v$  such that  $|\langle x, v \rangle| = q$  for all  $x \in \{l_1, \dots, l_{q-1}, k\}$ .

# Proof of Maximality

Returning to our equation,

$$y_{11} + \dots + y_{1q} + y_{21} + y_{31} + \dots + y_{q1} = z_1 + \dots + z_q$$

The multiset on the left side has  $2q - 1$  elements, and the multiset on the right has  $q$  elements, so the equation can only be satisfied if  $(2q - 1)^2 \equiv q^2 \pmod{p}$ .

Since  $(2q - 1)^2 \equiv q^2 \pmod{p}$  is false for all  $q = p^n$ , it follows that our equation cannot be satisfied and there is no vector  $v$  such that  $|\langle x, v \rangle| = q$  for all  $x \in \{l_1, \dots, l_{q-1}, k\}$ .

Therefore our set of unbiased Butson Hadamard matrices is maximal.

# An Open Question

We saw earlier that the number of Mutually Unbiased Hadamard Matrices of order  $n^2$  is at most  $n - 1$ , and in fact one can meet this bound using Bush-type Hadamard matrices. In the construction we've just covered, a set of  $n$  Mutually Unbiased Butson Hadamard matrices of order  $n^2$  are constructed, but only  $n - 1$  of them are Bush-type.

# An Open Question

We saw earlier that the number of Mutually Unbiased Hadamard Matrices of order  $n^2$  is at most  $n - 1$ , and in fact one can meet this bound using Bush-type Hadamard matrices. In the construction we've just covered, a set of  $n$  Mutually Unbiased Butson Hadamard matrices of order  $n^2$  are constructed, but only  $n - 1$  of them are Bush-type.

## Open Question

Is the number of Mutually Unbiased Bush-type Butson Hadamard Matrices of order  $n^2$  at most  $n - 1$ , or can larger sets be constructed?