### Balancedly Splittable Orthogonal Designs

Thomas Pender
\*\*\*Joint work with Hadi Kharaghani, Sho Suda

Department of Mathematics and Computer Science University of Lethbridge

Alberta-Montana Combinatorics & Algorithms Days at BIRS June 2022



# Summary

- balancedly splittable Hadamard matrices
- balancedly splittable orthogonal designs
- construction
- related configurations

#### Definition: Hadmard Matrix

- A square matrix with entries from  $\{-1,1\}$  with pairwise orthogonal rows.
- Equiv.  $HH^t = nI_n$ , with H an  $n \times n$  (-1,1)-matrix of order n.

• a Hadamard matrix of order 16

#### Definition: Hadmard Matrix

- A square matrix with entries from  $\{-1,1\}$  with pairwise orthogonal rows.
- Equiv.  $HH^t = nI_n$ , with H an  $n \times n$  (-1,1)-matrix of order n.

#### Definition: Hadmard Matrix

- A square matrix with entries from  $\{-1,1\}$  with pairwise orthogonal rows.
- Equiv.  $HH^t = nI_n$ , with H an  $n \times n$  (-1, 1)-matrix of order n.

### Definition: Balancedly Splittable (Kharaghani and Suda, 2019)

- ullet A Hadamard matrix H of order n with  $n imes \ell$  submatrix  $H_1$  .
- H is  $(n, \ell, a, b)$  balancedly splittable, a < b, if

$$H_1H_1^t=\ell I_n+aA+b(J_n-I_n-A),$$

for symmetric (0,1)-matrix A with zero diagonal.

↓□▶ ↓□▶ ↓□▶ ↓□▶ □ ♥Q♥

• a Hadamard matrix of order 16

• a balancedly splittable Hadamard matrix of order 16

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

```
2222222222222
 222222222222
```

• The rows of the split are equiangular.

• There are four splits.

#### Definition: Orthogonal Designs

• A square  $\{\pm z_1, \dots, \pm z_u\}$ -matriz X of order n such that

$$XX^t = \sigma I_n, \quad s_i \in \mathbb{N},$$

where 
$$\sigma = \sum_{i} s_{i} z_{i}^{2}$$
.

• Write  $OD(n; s_1, \ldots, s_u)$ .

ababababābābāb ababābabābabābab abababābābābabab ababābābababāb bābāabbābāabbāba bābāabbabaabbabā abābbāabbābaabbā abābbaabbabāabba bā bā bā bā a bbā bā a a b bā ba ba ba ab ba bā ab БаБааbbāБааbbābā БаБааbБаbāabБаБа b̄ a b b̄ a a b b ā b ā a b b ā БаbbāаbБаБааbБа abābābaabbābāab abābabāabbabaab

abab<mark>abab</mark>ābābāb ababābabābab abababābābābabab ababā bā bababā b ābāabbābāabbāba bābāabbababā bābbāabbābaabbā bābbaabbabāabba bābabābāabbābaab ā b a b a b a a b b a b a a b a b̄ a a b b ā b̄ a a b b ā b ā a b̄ a a b b̄ a b ā a b b̄ a b̄ a babbaabbābāabbā babbaabbaabaa a b ā b ā b a a b b ā b ā a b abābabāabbabaab

13 / 48

◄□▶◀圖▶◀불▶◀불▶ 불 ∽٩

ababababābābāb ababābabābabābab abababābābābabab ababābābababāb bābāabbābāabbāba bābāabbabaabbabā abābbāabbābaabbā abābbaabbabāabba bābabābaabbābaab bābababaabbabāab БаБааbbāБааbbābā abaabbabāabbaba babbaabbābā abbā abbāabbabaabba abābābaabbābāab abābabāabbabaab

#### Definition: Orthogonal Designs

• A square  $\{\pm z_1, \dots, \pm z_u\}$ -matrix X of order n such that  $XX^t = \sigma I_n, s_i \in \mathbb{N}$ , where  $\sigma = \sum_i s_i z_i^2$ .

#### Definition: Orthogonal Designs

• A square  $\{\pm z_1, \dots, \pm z_u\}$ -matrix X of order n such that  $XX^t = \sigma I_n, s_i \in \mathbb{N}$ , where  $\sigma = \sum_i s_i z_i^2$ .

#### Definition: Balancedly Splittable (Kharaghani et al., 2021)

• An OD X with  $n \times \ell$  submatrix  $X_1$  admits a stable  $(n, \ell, a, b)$  split if

$$X_1X_1^t = \sigma(cI_n + aA + b(J_n - I_n - A)),$$

where  $c \mid \ell$ .

• The split is unstable if it is not stable and

$$X_1X_1^t = \ell I_n + aA + b(J_n - I_n - A)$$

after replacing each variable with 1.

# **Auxiliary Matrices**

#### Definition: Auxiliary Matrices

- X a full  $OD(n; s_1, ..., s_u)$  and H the Hadamard matrix obtained by replacing each variable with 1.
- Label rows of X and H by  $x_0, \ldots, x_{n-1}$ , and  $h_0, \ldots, h_{n-1}$ .
- ullet The auxiliary matrices of X are given by

$$c_i = h_i^t x_i, \qquad i = 0, \ldots, n-1.$$

• An OD(2; 1, 1):

$$\begin{pmatrix} a & b \\ b & -a \end{pmatrix}$$

Auxiliary matrices:

$$c_0 = \begin{pmatrix} a & b \\ a & b \end{pmatrix}, \qquad c_1 = \begin{pmatrix} b & -a \\ -b & a \end{pmatrix}$$

Form the sequences

$$\alpha = (c_0, c_1, c_1), \qquad \beta = (c_0, c_1, -c_1).$$

• The sum of the periodic correlations of  $\alpha$  and  $\beta$  satisfy

$$\sum_{i} \alpha_{i} \alpha_{i+j}^{t} + \sum_{i} \beta_{i} \beta_{i+j}^{t} = 0, \qquad j = 1, 2.$$

Sums of cross-correlations

$$\sum_{i} \alpha_{i} \beta_{i+j}^{t} + \sum_{i} \beta_{i} \alpha_{i+j}^{t} = 0, \qquad j = 1, 2.$$

◆ロト ◆個ト ◆差ト ◆差ト 差 めるぐ

Form the matrices

$$A = circ(\alpha), \qquad B = circ(\beta),$$

• Then the matrix

$$\Theta = \begin{pmatrix} A & B \\ B & A \end{pmatrix}.$$



20 / 48

$$\Theta = \begin{pmatrix} a & b & b & \bar{a} & b & \bar{a} & a & b & b & \bar{a} & \bar{b} & a \\ a & b & \bar{b} & a & \bar{b} & a & a & b & \bar{b} & a & b & \bar{a} \\ b & \bar{a} & a & b & \bar{b} & \bar{a} & \bar{b} & a & a & b & \bar{b} & \bar{a} \\ \bar{b} & a & a & b & \bar{b} & a & b & \bar{a} & a & b & \bar{b} & a \\ b & \bar{a} & b & \bar{a} & a & b & \bar{b} & \bar{a} & \bar{b} & a & a & b \\ \bar{b} & a & \bar{b} & \bar{a} & a & b & \bar{b} & \bar{a} & \bar{b} & \bar{a} & a & b \\ \bar{a} & b & \bar{b} & \bar{a} & \bar{b} & \bar{a} & a & b & \bar{b} & \bar{a} & \bar{b} & \bar{a} \\ \bar{a} & b & \bar{b} & \bar{a} & \bar{b} & \bar{a} & \bar{a} & b & \bar{b} & \bar{a} & \bar{b} & \bar{a} \\ \bar{b} & \bar{a} & \bar{b} \\ \bar{b} & \bar{a} & \bar{b} & \bar{a} & \bar{b} & \bar{b} & \bar{a} & \bar{b} & \bar{a} & \bar{b} & \bar{a} \\ \bar{b} & \bar{a} & \bar{b} & \bar{a} & \bar{b} & \bar{b} & \bar{a} & \bar{b} & \bar{a} & \bar{b} \\ \bar{b} & \bar{a} & \bar{b} & \bar{a} & \bar{b} & \bar{b} & \bar{a} & \bar{b} & \bar{a} & \bar{b} \end{pmatrix}$$

◆ロト ◆個ト ◆重ト ◆重ト ■ める(\*)

$$\Theta\Theta^{t} = \begin{pmatrix} AA^{t} + BB^{t} & AB^{t} + BA^{t} \\ AB^{t} + BA^{t} & AA^{t} + BB^{t} \end{pmatrix}.$$



< ロト < 個 ト < 重 ト < 重 ト ■ ■ の < @

```
abbabā
  abbābaabbā
  a b b a b a a b b a
 ābāabbābaab
 abaabbabāab
abbābaabbābā
      āabbaba
     bābāabbā
 ā a b b̄ a b̄ a a b b̄ a
bābaab<u>b</u>ābāab
 abāabbabaab
```

• Define:

$$Y = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \otimes X,$$
  
 $K = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \otimes H.$ 

• Index rows as  $y_0, \ldots, y_{2n-1}$ , and  $k_0, \ldots, k_{2n-1}$ .

25 / 48

$$Y = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \otimes X$$
  $K = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \otimes H$   
Rows:  $y_0, \dots, y_{2n-1}$  Rows:  $k_0, \dots, k_{2n-1}$ 

#### Form

$$F = \begin{pmatrix} k_1^t x_0 & k_2^t x_0 & k_3^t x_0 \end{pmatrix},$$

$$E = \begin{pmatrix} h_0^t y_1 \\ h_0^t y_2 \\ h_0^t y_3 \end{pmatrix},$$

$$G = k_0^t y_0.$$



/ G	1	F							− <i>F</i>						
		а	b	b	ā	b	ā		а	b	b	ā	b	а	
E		a	b	Б	a	b	a		a	b	Б	a	b	ā	
		Ь	ā	a	b	b	ā		Б	a	a	b	b	ā	
		$\bar{b}$	a	a	b	$\bar{b}$	а		b	ā	a	b	$\bar{b}$	a	
<b>\</b>		Ь	ā	b	ā	a	b		b	ā	$\bar{b}$	a	a	b	
	\	$\bar{b}$	а	$\bar{b}$	a	a	b		Б	a	b	ā	a	b	
		a	Ь	b	ā	b	а		a	b	b	ā	b	ā	
		a	b	Б	a	b	ā		a	b	$\bar{b}$	a	b	a	
	9	$\bar{b}$	a	a	b	b	ā		b	ā	a	b	b	ā	
		b	ā	a	Ь	$\bar{b}$	а		Б	a	a	b	$\bar{b}$	a	
		b	ā	b	a	a	b		b	ā	b	ā	a	b	
		$\bar{b}$	a	b	ā	a	b		b	a	$\bar{b}$	a	a	b	/

◄□▶◀圖▶◀불▶◀불▶ 불 ∽٩

ababababābābāb ababābabābabābab bababābābababababāb ābāabbābāabbāba bābāabbababā bābbāabbābaabbā bā b̄ b̄ a a b b̄ a bā a b b̄ a ā b a b ā b ā a b b ā b a a b bā ba ba ba ab ba bā ab babaabbābaabbābā baabbabaabaaba babbaabbabaabba abbāabbabaabba abābābaabbābāab abābabāabbab

ababababābābāb ababābabābabābab abababābābābabab ababābābababāb ābāabbābāabbāba bābāabbabaabbabā abābbāabbābaabbā abābbaabbabāabba bābabābāabbābaab bā ba ba baab babā ab a b̄aabbā b̄aabbābā abaabbabaabbaba babbaabbabaabba БаbbāаbБаБааbБа abābābaabbābāab abābabāabbabaab

## Complex and Quaternion Elements

• The following is a OD(2; 1, 1) of quaternions.

$$\begin{pmatrix} \bar{a} & bi \\ \bar{b}j & ak \end{pmatrix},$$

• where a and b are real variables.

## Complex and Quaternion Elements

bi a bi bj <mark>āk ā bi bj āk</mark> bj ak ā bi bj āk ak bi āk bi ak bi ak ā bi bi ak bi āk ā bi ak bj āk bj āk bj āk ā bi bj āk bj ak ā bj āk bj āk ā bi bj ak bj āk ā bi bj ak bj ak āk bj āk ā bi bj āk bj ak ā bi bj āk bj āk bi ā bi bj āk ā bi bj ak bj ak ā bi bj ak bi ā bi bj ak ā bi bj āk bj āk ā bi bj āk āk b̄j ak b̄j ak b̄j āk ā bi b̄j ak b̄j ak ā bjāk bjak bjāk bjak ā bi bjāk bjāk ā

### Equiangular Lines and Unbiased Hadamard Matrices

#### Definition: Equiangular Lines

A collection  $\mathcal{L} \subset \mathbb{R}^{\ell}$  of lines (vectors) are equiangular if there is a constant a such that  $|\langle u, v \rangle| = a$  for every  $u, v \in L$ .

#### Definition: Unbiased Hadamard Matrices

Hadamard matrices H and K are unbiased if

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

for some Hadamard matrix L.



### Equiangular Lines and Unbiased Hadamard Matrices

• a Hadamard matrix of order 16

◆ロト ◆問 ト ◆ 意 ト ◆ 意 ・ 夕 Q ②

# Equiangular Lines and Unbiased Hadamard Matrices

• a balanced split

- a collection of equiangular lines
- products are the same in absolute value

H and K are unbiased

◆□▶ ◆□▶ ◆□▶ ◆□▶ ○■ のQ@

#### Proposition (Kharaghani and Suda, 2019)

 $H = (H_1 H_2)$  a Hadamard matrix of order n with

$$H_1H_1^t = \ell I_n + aS$$

where S is a (-1,0,1)-matrix. The following are equivalent:

- $K = (-H_1 H_2)$  is unbiased with H, and
- ②  $(\ell, a) = ((n \pm \sqrt{n})/2, \sqrt{n}/2).$



T. Pender (U of L)

$$\begin{pmatrix}
G & F & -F \\
E & A & B \\
-E & B & A
\end{pmatrix}$$



$$\begin{pmatrix}
G & F & -F \\
E & A & B \\
-E & B & A
\end{pmatrix}$$



$$\begin{pmatrix}
G & F & -F \\
E & A & B \\
-E & B & A
\end{pmatrix}$$



$$\begin{pmatrix}
G & F & -F \\
E & A & B \\
-E & B & A
\end{pmatrix}$$



## Equiangular Lines and Hadamard Matrices

- each split gives equiangular lines
- parametric conditions of the proposition are satisfied
- we can always construct unbiased Hadamard matrices

#### Definition: Unbiased ODs (Kharaghani and Suda, 2018)

- $X_1$  and  $X_2$  be two  $OD(n, s_1, \ldots, s_u)$  in  $\{\pm z_1, \ldots, \pm z_u\}$ .
- ullet  $X_1$  and  $X_2$  are unbiased if there is a Hadamard matrix H such that

$$X_1 X_2^t = \left(\alpha^{-\frac{1}{2}} \sum_i s_i z_i^2\right) H.$$

for some  $\alpha \in \mathbb{R}^+$ .



#### Definition: Unbiased ODs (Kharaghani and Suda, 2018)

- $X_1$  and  $X_2$  be two  $OD(n, s_1, \ldots, s_u)$  in  $\{\pm z_1, \ldots, \pm z_u\}$ .
- $X_1$  and  $X_2$  are unbiased if there is a Hadamard matrix H such that

$$X_1 X_2^t = \left(\alpha^{-\frac{1}{2}} \sum_i s_i z_i^2\right) H.$$

for some  $\alpha \in \mathbb{R}^+$ .

stable split equiangular lines  $\Rightarrow$  unbiased ODs param. cond.

Recall:

$$X = \begin{pmatrix} G & F & -F \\ E & A & B \\ -E & B & A \end{pmatrix}.$$

Take

$$Y = \begin{pmatrix} G & F & F \\ E & A & -B \\ -E & B & -A \end{pmatrix}.$$

• Then  $XY^t = 2\left(\sum_i s_i z_i^2\right) H$ , where H is Hadamard.



(a a a a b b a a b b b b b a a b b a a b b a a b b a a b b a a b b a a b a a b b a a b a a b a a b a a b a a b a a b a a b a a b a a b a a b a a b a a b a a b a a b a a b a a b a a b a a b a a a b a b b b b a a a a b a b b b b a a a b a b b b b a a a b a b b b b a a a b a b b b b a a a b a b b b b a a a b a b a a b b b b a a a b a b a a a b a b b b b a a a b a b a a a b a a b a a a b a a b a a a b a a b a a a b a a b a a a b a a a b a a a b a a a b a a b b b b a a a b b b b a a a b b b a a a b b b a a a b b a a a b b a a a b b a a a b b a a a b b a b a b a b b a b a b a b b a b a a a b b a a a b b a a a b b b a a a a b a b b b a b a a a b b a

◆ロト ◆個ト ◆差ト ◆差ト 差 めるぐ

# The End!!

Thank You!

#### References

- Kharaghani, H., Pender, T., and Suda, S. (2021). Balancedly splittable orthogonal designs and equiangular tight frames. *Des. Codes Cryptogr.*, 89(9):2033–2050.
- Kharaghani, H. and Suda, S. (2018). Unbiased orthogonal designs. *Des. Codes Cryptogr.*, 86(7):1573–1588.
- Kharaghani, H. and Suda, S. (2019). Balancedly splittable Hadamard matrices. *Discrete Math.*, 342(2):546–561.