# Phased unitary Golay pairs, Butson Hadamard matrices and a conjecture of Ito's

Ronan Egan

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

This work has been fully supported by Croatian Science Foundation under the project 1637.

# Butson Hadamard matrices

Let $k$ be a positive integer and let $\zeta_k = e^{\frac{2\pi\sqrt{-1}}{k}}$.

A *Butson Hadamard matrix* $\mathrm{BH}(n,k)$ of order $n$ is an $n \times n$ matrix $H = [h_{ij}]$ whose entries $h_{ij}$ lie in $\langle \zeta_k \rangle$ and such that $HH^* = nI_n$, where $H^* = [\overline{h_{ji}}]$.

# Butson Hadamard matrices

Let $k$ be a positive integer and let $\zeta_k = e^{\frac{2\pi\sqrt{-1}}{k}}$.

A *Butson Hadamard matrix* $\mathrm{BH}(n,k)$ of order $n$ is an $n \times n$ matrix $H = [h_{ij}]$ whose entries $h_{ij}$ lie in $\langle \zeta_k \rangle$ and such that $HH^* = nI_n$, where $H^* = [\overline{h_{ji}}]$.

## Example

The matrix $H$ is a $\mathrm{BH}(3,3)$ where

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \zeta_3 & \zeta_3^2 \\ 1 & \zeta_3^2 & \zeta_3 \end{bmatrix}.$$

# Sequences and notation

- A sequence $a = [a_i]_{0 \le i \le v-1}$ of length $v$ with entries in $\langle \zeta_k \rangle$ is called a $k$-ary sequence.
- $\overline{a} = [\overline{a_i}]_{0 \le i \le v-1}$.
- $\hat{a} = [a_{v-1-i}]_{0 \le i \le v-1}$.
- $a^* = \hat{\overline{a}} = \overline{\hat{a}}$.
- To ease notation we write $k$-ary arrays in log form. That is, we replace $[\zeta_k^{\eta_{i,j}}]$ with $[\eta_{i,j}]$ (or $[\eta_{i,j}]_k$ if necessary).

# Golay pairs

Let $a$ and $b$ be 2-ary (binary) sequences of length $v$. The *aperiodic autocorrelation function* of $a$ with shift $s$ is defined to be

$$\mathrm{AF}_s(a) = \sum_{i=0}^{v-s-1} a_i a_{i+s}.$$

The pair $(a, b)$ is a *Golay pair* of length $v$ if $\mathrm{AF}_s(a) + \mathrm{AF}_s(b) = 0$ for all $1 \leq s \leq v-1$. The set of all Golay pairs of length $v$ is denoted by $\mathrm{GP}(v)$.

# Golay pairs

Let $a$ and $b$ be 2-ary (binary) sequences of length $v$. The *aperiodic autocorrelation function* of $a$ with shift $s$ is defined to be

$$\mathrm{AF}_s(a) = \sum_{i=0}^{v-s-1} a_i a_{i+s}.$$

The pair $(a, b)$ is a *Golay pair* of length $v$ if $\mathrm{AF}_s(a) + \mathrm{AF}_s(b) = 0$ for all $1 \leq s \leq v - 1$. The set of all Golay pairs of length $v$ is denoted by $\mathrm{GP}(v)$.

**Theorem (Turyn)**

$\mathrm{GP}(v)$ *is non-empty for* $v = 2^x 10^y 26^z$ *for all* $x, y, z \geq 0$.

# Golay pairs and Hadamard matrices

Let $(a, b) \in \mathrm{GP}(v)$ and let $A$ and $B$ be the circulant matrices with first rows $a$ and $b$ respectively. Then

$$H = \begin{bmatrix} A & B \\ -B^\top & A^\top \end{bmatrix}$$

is a Hadamard matrix of order $2v$.

# Golay pairs and Hadamard matrices

Let $(a, b) \in \mathrm{GP}(v)$ and let $A$ and $B$ be the circulant matrices with first rows $a$ and $b$ respectively. Then

$$H = \begin{bmatrix} A & B \\ -B^\top & A^\top \end{bmatrix}$$

is a Hadamard matrix of order $2v$.

## Example

Let $(a, b) = ([1, 1, -, 1], [1, 1, 1, -])$. Then

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

is a Hadamard matrix of order 8.

# Periodic Golay pairs

The *periodic autocorrelation function* of $a$ with shift $s$ is defined to be

$$\mathrm{PAF}_s(a) = \sum_{i=0}^{v-1} a_i a_{i+s},$$

where the sequences indices are read modulo $v$.

# Periodic Golay pairs

The *periodic autocorrelation function* of $a$ with shift $s$ is defined to be

$$\mathrm{PAF}_s(a) = \sum_{i=0}^{v-1} a_i a_{i+s},$$

where the sequences indices are read modulo $v$. Equivalently, if $C$ is the $v \times v$ circulant matrix with first row $[0, 1, 0, 0, \ldots, 0]$, then

$$\mathrm{PAF}_s(a) = a \cdot aC^s.$$

# Periodic Golay pairs

The *periodic autocorrelation function* of $a$ with shift $s$ is defined to be

$$\mathrm{PAF}_s(a) = \sum_{i=0}^{v-1} a_i a_{i+s},$$

where the sequences indices are read modulo $v$. Equivalently, if $C$ is the $v \times v$ circulant matrix with first row $[0, 1, 0, 0, \ldots, 0]$, then

$$\mathrm{PAF}_s(a) = a \cdot aC^s.$$

The pair $(a, b)$ is a *periodic Golay pair* of length $v$ if $\mathrm{PAF}_s(a) + \mathrm{PAF}_s(b) = 0$ for all $1 \leq s \leq v - 1$. The set of all periodic Golay pairs of length $v$ is denoted by $\mathrm{PGP}(v)$.

Every $\mathrm{GP}(v)$ is a $\mathrm{PGP}(v)$. Hadamard matrices of order $2v$ are constructed in exactly the same way.

# Negaperiodic Golay pairs

Let $N = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & & 0 & 1 \\ -1 & 0 & 0 & & 0 & 0 \end{bmatrix}$.

The *negaperiodic autocorrelation function* of $a$ with shift $s$ is defined to be

$$\mathrm{NAF}_s(a) = a \cdot aN^s.$$

The pair $(a, b)$ is a *negaperiodic Golay pair* of length $v$ if $\mathrm{NAF}_s(a) + \mathrm{NAF}_s(b) = 0$ for all $1 \leq s \leq v - 1$. The set of all negaperiodic Golay pairs of length $v$ is denoted by $\mathrm{NGP}(v)$.

Let $(a, b) \in \mathrm{NGP}(v)$ and let $A$ and $B$ be the negacirculant matrices with first row $a$ and $b$ respectively. That is, $A_1 = a$ and $A_i = aN^{i-1}$ for all $2 \leq i \leq v$, and $B$ is similar. Then as before

$$H = \begin{bmatrix} A & B \\ -B^\top & A^\top \end{bmatrix}$$

is a Hadamard matrix of order $2v$.

# Constructing Hadamard matrices

Let $(a, b) \in \mathrm{NGP}(v)$ and let $A$ and $B$ be the negacirculant matrices with first row $a$ and $b$ respectively. That is, $A_1 = a$ and $A_i = aN^{i-1}$ for all $2 \leq i \leq v$, and $B$ is similar. Then as before

$$H = \begin{bmatrix} A & B \\ -B^\top & A^\top \end{bmatrix}$$

is a Hadamard matrix of order $2v$.

Every $\mathrm{GP}(v)$ is a $\mathrm{NGP}(v)$.

**Theorem (Balonin & Đoković)**

$\mathrm{GP}(v) = \mathrm{PGP}(v) \cap \mathrm{NGP}(v)$.

# Complex Golay pairs

Let $a$ and $b$ be 4-ary (quaternary) sequences of length $v$. The *complex aperiodic autocorrelation function* of $a$ with shift $s$ is defined to be

$$\mathrm{CAF}_s(a) = \sum_{i=0}^{v-s-1} a_i \overline{a_{i+s}}.$$

# Complex Golay pairs

Let $a$ and $b$ be 4-ary (quaternary) sequences of length $v$. The *complex aperiodic autocorrelation function* of $a$ with shift $s$ is defined to be

$$\mathrm{CAF}_s(a) = \sum_{i=0}^{v-s-1} a_i \overline{a_{i+s}}.$$

The pair $(a, b)$ is a *complex Golay pair* of length $v$ if $\mathrm{CAF}_s(a) + \mathrm{CAF}_s(b) = 0$ for all $1 \leq s \leq v-1$. The set of all complex Golay pairs of length $v$ is denoted by $\mathrm{CGP}(v)$.

# Complex Golay pairs

Let $a$ and $b$ be 4-ary (quaternary) sequences of length $v$. The *complex aperiodic autocorrelation function* of $a$ with shift $s$ is defined to be

$$\mathrm{CAF}_s(a) = \sum_{i=0}^{v-s-1} a_i \overline{a_{i+s}}.$$

The pair $(a, b)$ is a *complex Golay pair* of length $v$ if $\mathrm{CAF}_s(a) + \mathrm{CAF}_s(b) = 0$ for all $1 \leq s \leq v-1$. The set of all complex Golay pairs of length $v$ is denoted by $\mathrm{CGP}(v)$.

**Theorem (Craigen, Holzmann & Kharaghani)**

$\mathrm{CGP}(v)$ *is non-empty for all* $v = 2^{x+u}3^y5^c11^d13^e$ *where* $x, y, c, d, e, u \geq 0$, $y + c + d + e \leq x + 2u + 1$ *and* $u \leq c + e$.

# Complex Golay pairs and complex Hadamard matrices

Let $(a, b) \in \mathrm{CGP}(v)$ and let $A$ and $B$ be the circulant matrices with first rows $a$ and $b$ respectively. Then

$$H = \begin{bmatrix} A & B \\ -B^* & A^* \end{bmatrix}$$

is a $\mathrm{BH}(2v, 4)$.

Let $(a, b) \in \mathrm{CGP}(v)$ and let $A$ and $B$ be the circulant matrices with first rows $a$ and $b$ respectively. Then

$$H = \begin{bmatrix} A & B \\ -B^* & A^* \end{bmatrix}$$

is a $\mathrm{BH}(2v, 4)$.

## Example

Let $(a, b) = ([1, 1, -], [1, i, 1])$. Then

$$H = \left[\begin{array}{ccc|ccc} 1 & 1 & - & 1 & i & 1 \\ - & 1 & 1 & 1 & 1 & i \\ 1 & - & 1 & i & 1 & 1 \\ \hline - & - & i & 1 & - & 1 \\ i & - & - & 1 & 1 & - \\ - & i & - & - & 1 & 1 \end{array}\right]$$

is a $\mathrm{BH}(6, 4)$.

# Unitary Golay pairs

Let $a$ and $b$ be $k$-ary sequences of length $v$. The pair $(a, b)$ is a *unitary Golay pair* of length $v$ if $\mathrm{CAF}_s(a) + \mathrm{CAF}_s(b) = 0$ for all $1 \leq s \leq v - 1$.

The set of all $k$-ary unitary Golay pairs of length $v$ is denoted by $\mathrm{UGP}(v, k)$.

# Unitary Golay pairs

Let $a$ and $b$ be $k$-ary sequences of length $v$. The pair $(a,b)$ is a *unitary Golay pair* of length $v$ if $\mathrm{CAF}_s(a) + \mathrm{CAF}_s(b) = 0$ for all $1 \leq s \leq v-1$.

The set of all $k$-ary unitary Golay pairs of length $v$ is denoted by $\mathrm{UGP}(v,k)$.

Let $m \in \{0,\ldots,k-1\}$ and let

$$C_{k,m} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & & 0 & 1 \\ \zeta_k^m & 0 & 0 & & 0 & 0 \end{bmatrix}.$$

# Phased unitary Golay pairs

We define the *unitary autocorrelation function* of a $k$-ary sequence $a$ of length $v$ and shift $s$ to be

$$\mathrm{UAF}_{m,s}(a) = a \cdot \overline{aC^s_{k,m}}.$$

We say $(a, b)$ is a *phased unitary Golay pair* if $\mathrm{UAF}_{m,s}(a) + \mathrm{UAF}_{m,s}(b) = 0$ for all $1 \leq s \leq v - 1$.

# Phased unitary Golay pairs

We define the *unitary autocorrelation function* of a $k$-ary sequence $a$ of length $v$ and shift $s$ to be

$$\mathrm{UAF}_{m,s}(a) = a \cdot \overline{aC^s_{k,m}}.$$

We say $(a, b)$ is a *phased unitary Golay pair* if $\mathrm{UAF}_{m,s}(a) + \mathrm{UAF}_{m,s}(b) = 0$ for all $1 \leq s \leq v - 1$.

The set of all $k$-ary phased unitary Golay pairs of length $v$ of phase $m$ is denoted by $\mathrm{PUGP}(v, k, m)$.

**Theorem**

$\mathrm{UGP}(v, k) = \cap_{m=0}^{k-1} \mathrm{PUGP}(v, k, m).$

# Constructing Butson Hadamard matrices

Let $(a, b) \in \mathrm{PUGP}(v, k, m)$, and let $A$ and $B$ be the $\zeta_k^m$-circulant matrices with first row $a$ and $b$ respectively. That is, $A_1 = a$ and $A_i = aC_{k,m}^{i-1}$ for all $2 \leq i \leq v$, and $B$ is similar.

$$H = \begin{bmatrix} A & B \\ -B^* & A^* \end{bmatrix}$$

is a $\mathrm{BH}(2v, k)$ is $k$ is even, or a $\mathrm{BH}(2v, 2k)$ if $k$ is odd.

# Constructing Butson Hadamard matrices

Let $(a, b) \in \mathrm{PUGP}(v, k, m)$, and let $A$ and $B$ be the $\zeta_k^m$-circulant matrices with first row $a$ and $b$ respectively. That is, $A_1 = a$ and $A_i = aC_{k,m}^{i-1}$ for all $2 \leq i \leq v$, and $B$ is similar.

$$H = \begin{bmatrix} A & B \\ -B^* & A^* \end{bmatrix}$$

is a $\mathrm{BH}(2v, k)$ is $k$ is even, or a $\mathrm{BH}(2v, 2k)$ if $k$ is odd.

If $(a, b) \in \mathrm{UGP}(v, k)$, we can use the same construction, with any choice of $m \in \{0, \ldots, k-1\}$. Thus we construct $k$ Butson Hadamard matrices, which are not necessarily equivalent.

# Example

Let $a = [0,4,5,0]_6$ and $b = [0,1,5,3]_6$. Then $(a,b) \in \mathrm{UGP}(4,6)$. Then reading the entries modulo 6,

$$H = \left[\begin{array}{cccc|cccc} 0 & 4 & 5 & 0 & 0 & 1 & 5 & 3 \\ m & 0 & 4 & 5 & 3+m & 0 & 1 & 5 \\ 5+m & m & 0 & 4 & 5+m & 3+m & 0 & 1 \\ 4+m & 5+m & m & 0 & 1+m & 5+m & 3+m & 0 \\ \hline 3 & -m & 4-m & 2-m & 0 & -m & 1-m & 2-m \\ 2 & 3 & -m & 4-m & 2 & 0 & -m & 1-m \\ 4 & 2 & 3 & -m & 1 & 2 & 0 & -m \\ 0 & 4 & 2 & 3 & 0 & 1 & 2 & 0 \end{array}\right]$$

is a $\mathrm{BH}(8,6)$ for any $0 \leq m \leq 5$. The matrices constructed belong to two equivalence classes in $\mathrm{BH}(8,6)$. One class contains the matrices constructed with $m \in \{0,1,3,4\}$, and the other contains the matrices constructed with $m \in \{2,5\}$. One class is obtained from the other by replacing each entry in one matrix with its complex conjugate.

# Some further extensions

- Sequences with zeros:
  - Complex generalized weighing matrices.
- Sequences with entries in a signed group:
  - Signed group Hadamard matrices.
  - Signed group weighing matrices.
- Sets of $n > 2$ complementary sequences:
  - e.g., Williamson type constructions.

# Computing

$|\mathrm{PUGP}(v,2,m)|$

| $v\backslash m$ | 0 | 1 | $\|\mathrm{UGP}(v,2)\|$ |
|---|---|---|---|
| 4 | 64 | 128 | 32 |
| 6 | 0 | 576 | 0 |
| 8 | 1536 | 4096 | 192 |
| 10 | 6400 | 11200 | 128 |

$|\mathrm{PUGP}(v,4,m)|$

| $v\backslash m$ | 0 | 1 | 2 | $\|\mathrm{UGP}(v,4)\|$ |
|---|---|---|---|---|
| 2 | 96 | 128 | 96 | 64 |
| 3 | 576 | 576 | 576 | 128 |
| 4 | 2176 | 4096 | 4096 | 512 |
| 5 | 11200 | 11200 | 11200 | 512 |

$|\mathrm{PUGP}(v,6,m)|$

| $v\backslash m$ | 0 | 1 | 2 | 3 | $\|\mathrm{UGP}(v,6)\|$ |
|---|---|---|---|---|---|
| 2 | 360 | 432 | 360 | 432 | 216 |
| 3 | 1296 | 0 | 0 | 1296 | 0 |
| 4 | 19008 | 26496 | 19008 | 26496 | 2592 |

$(|\mathrm{PUGP}(v,k,m)| = |\mathrm{PUGP}(v,k,k-m)|)$

# Consequences of Ito's conjecture

Let $i = \sqrt{-1}$ and let $j = -i$. Let $X$ be the set of 4-ary sequences of length $v$ and $Y$ be the set of 2-ary sequences of length $2v$. Now let $f : X \to Y$ be the bijective map such that $f(x) = y$ where $y$ is obtained from $x \circ \overline{x}$ by replacing each $i$ with $-1$, and each $j$ with 1.

# Consequences of Ito's conjecture

Let $i = \sqrt{-1}$ and let $j = -i$. Let $X$ be the set of 4-ary sequences of length $v$ and $Y$ be the set of 2-ary sequences of length $2v$. Now let $f : X \to Y$ be the bijective map such that $f(x) = y$ where $y$ is obtained from $x \circ \overline{x}$ by replacing each $i$ with $-1$, and each $j$ with 1.

## Proposition

*Let $a, b \in X$ and let $f : X \to Y$ be the bijection above. Then $\mathrm{UAF}_{1,s}(a) + \mathrm{UAF}_{1,s}(b) = 0$ iff $\mathrm{UAF}_{1,s}(f(a)) + \mathrm{UAF}_{1,s}(f(b)) = 0$ for any $s \in \{1, \ldots, v-1\}$.*

# Consequences of Ito's conjecture

**Theorem**

*Define the bijection* $\phi : X \times X \to Y \times Y$ *where* $\phi(a, b) = (f(a), f(b))$ *for all* $a, b \in X$. *The restriction of* $\phi$ *to* $\mathrm{PUGP}(v, 4, 1)$ *is a bijection from* $\mathrm{PUGP}(v, 4, 1)$ *into* $\mathrm{PUGP}(2v, 2, 1)$.

# Consequences of Ito's conjecture

## Theorem

*Define the bijection* $\phi : X \times X \to Y \times Y$ *where* $\phi(a,b) = (f(a), f(b))$ *for all* $a, b \in X$. *The restriction of* $\phi$ *to* $\mathrm{PUGP}(v,4,1)$ *is a bijection from* $\mathrm{PUGP}(v,4,1)$ *into* $\mathrm{PUGP}(2v,2,1)$.

Ito's conjecture → Complex Hadamard conjecture → Hadamard conjecture.

# Consequences of Ito's conjecture

## Theorem

*Define the bijection* $\phi : X \times X \to Y \times Y$ *where* $\phi(a, b) = (f(a), f(b))$ *for all* $a, b \in X$. *The restriction of* $\phi$ *to* $\mathrm{PUGP}(v, 4, 1)$ *is a bijection from* $\mathrm{PUGP}(v, 4, 1)$ *into* $\mathrm{PUGP}(2v, 2, 1)$.

Ito's conjecture $\to$ Complex Hadamard conjecture $\to$ Hadamard conjecture.

## Theorem

*Let* $m$ *be a positive integer such that* $2m - 1$ *and* $4m - 1$ *is a prime power or* $m$ *is odd and there is a Williamson matrix over* $\mathbb{Z}_m$. *Then there exists a* $\mathrm{BH}(2v, 4)$ *for all* $v = 2^a 10^b 26^c m$ *with* $a, b, c \geq 0$. *In particular there exists a* $\mathrm{BH}(2v, 4)$ *for all* $v \leq 46$.