(Pseudo)-cocyclic (structured) Hadamard matrices over (quasi)groups

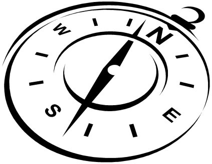
Alvarez, Armario, Falcón, Frau, Gudiel, Güemes and Kotsireas

University of Seville

5th Workshop on Real and Complex Hadamard Matrices and Applications

Outline

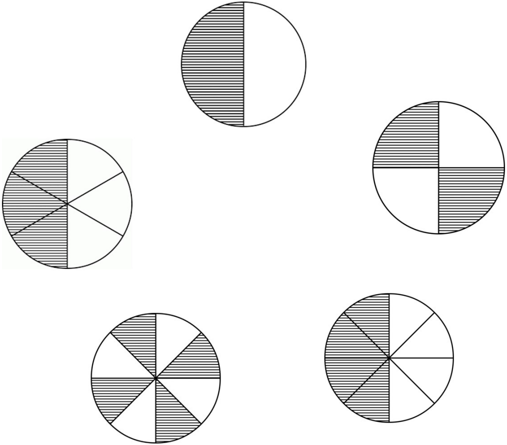
1. Cocyclic constructions for Hadamard matrices
2. (Pseudo)cocyclic Hadamard matrices over quasigroups
3. The Goethals-Seidel arrays are pseudo-cocyclic
4. Searching for large cocyclic Hadamard matrices
5. Future work



The cocyclic framework

$H = \left(\psi(g_i, g_j)\right)$ is a G-cocyclic Hadamard matrix, $|G| = 4t$.

$$\psi(g_i, g_j)\,\psi(g_i g_j, g_k)\psi(g_i, g_j g_k)\,\psi(g_j, g_k) = 1, \quad g_i, g_j, g_k \in G.$$



The cocyclic framework

$H = (\psi(g_i, g_j))$ is a G-cocyclic Hadamard matrix, $|G| = 4t$,

$$\psi(g_i, g_j)\,\psi(g_ig_j, g_k)\psi(g_i, g_jg_k)\,\psi(g_j, g_k) = 1, \;\; g_i, g_j, g_k \in G.$$

	Cocyclic	Non cocyclic
Sylvester	$\mathbb{Z}_2^{\log_2 4t}$	
Williamson	$\mathbb{Z}_2^2 \times \mathbb{Z}_t$	
Paley I	D_{4t}	
Paley II	$\mathbb{Z}_2^2 \times \mathbb{Z}_t$	
Ito	D_{4t}	
1-circulant core	$\mathbb{Z}_{4t-1}$-cocyclic structured	
2-circulant core	D_{4t-2}-cocyclic structured	
Goethals-Seidel		always?
Twin prime power		always?

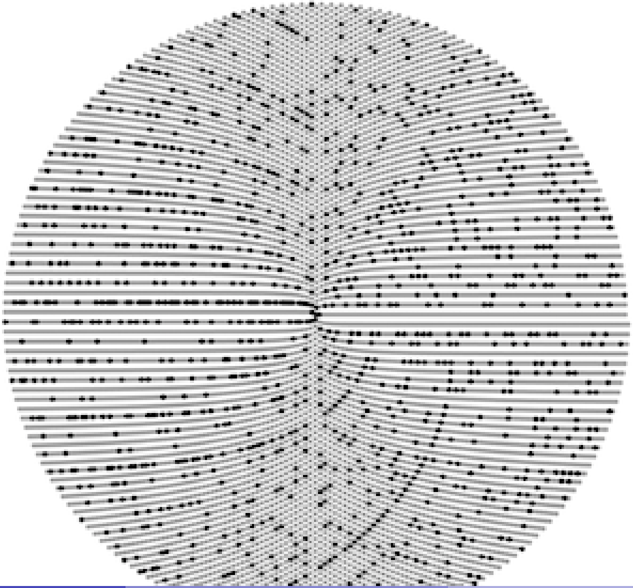
(Dis)advantages

- Faster Hadamard test

$$\sum_{j=1}^{4t} \psi(g_i, g_j) = 0, \text{ for } 2 \leq i \leq 4t.$$

(Dis)advantages

- Search space is reduced 

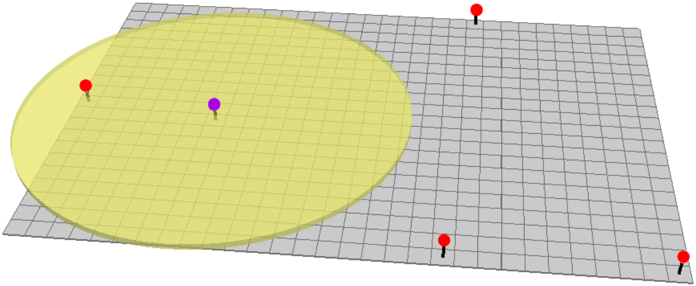


(Dis)advantages

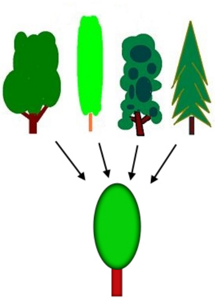
- The proportion of Hadamard matrices is reduced in turn 😳

order	2	4	8	12	16	20	24	28	32	36
$\sim_H$	1	1	1	1	5	3	60	487	13710027	$\geq 3 \cdot 10^6$
$\sim_{H+c}$	1	1	1	1	5	3	**16**	**6**	**100**	**35**

Ó Catháin, Röder 2011



What next? Cocycles over quasigroups...



Cocycles ψ over a *quasigroup* Q (i.e. associativity fails)

$$\forall a, b \in Q,\ \exists! x, y \in Q /\ ax = b, ya = b.$$

$$\psi(g_i, g_j)\ \psi(g_ig_j, g_k)\psi(g_i, g_jg_k)\ \psi(g_j, g_k) = 1,\ \ g_i, g_j, g_k \in Q.$$

What next? Cocycles over quasigroups...

Although the usual Hadamard cocyclic test is available ...

$$\sum_{k=1}^{4t} \psi(g_h, g_k)\psi(g_j, g_k) = 0 \Leftrightarrow \sum_{k=1}^{4t} \psi(g_i, g_k) = 0 \qquad (1)$$

Proposition

...A necessary condition for a Q-cocyclic matrix M_ψ being Hadamard is that Q is actually endowed with a loop structure.

Example: a Q-cocyclic Hadamard matrix of order 8

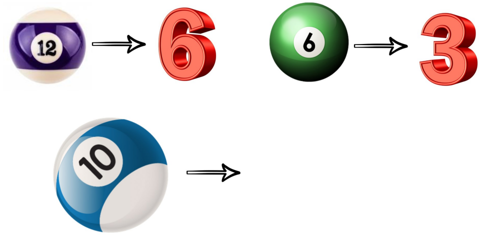
Consider the quasigroup Q of given law $((5 \cdot 6) \cdot 7 = 6 \neq 5 = 5 \cdot (6 \cdot 7))$:

1	2	3	4	5	6	7	8
2	1	4	3	6	5	8	7
3	4	1	2	7	8	5	6
4	3	2	1	8	7	6	5
5	6	8	7	3	4	2	1
6	5	7	8	4	3	1	2
7	8	6	5	1	2	4	3
8	7	5	6	2	1	3	4

$$BN_2 \otimes \mathbf{1}_4, \overset{\partial_2, \partial_3, \partial_4,}{\begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & + & - \\ + & - & - & - \end{pmatrix}} \otimes \mathbf{1}_2$$

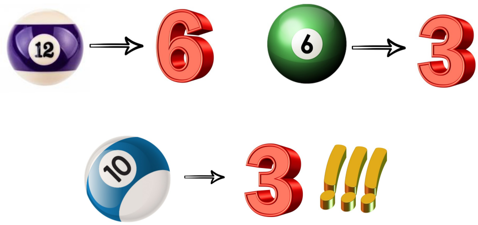
4 out of 32 are Hadamard: $\partial_2\partial_3$, $\partial_2\partial_3\partial_4$, ∂_3, ∂_4.

... Or even pseudo-cocycles over quasigroups!



... Or even pseudo-cocycles over quasigroups!

Formal *coboundaries* **might not** be cocyclic!



Lemma

The elementary map $\partial\delta_h$ actually constitutes a genuine cocycle if and only if

$$g_i(g_jg_k) = g_h \Leftrightarrow (g_ig_j)g_k = g_h, \quad g_i, g_j, g_k \in Q.$$

... Or even pseudo-cocycles over quasigroups!

Those maps which are formally coboundaries but not truly cocycles are called *pseudo-coboundaries*. It is of interest considering *pseudo-cocyclic* matrices $M_{\psi\cdot\phi}$ resulting from the product of a genuine cocycle ψ and a pseudocoboundary ϕ for which the Hadamard test (1) still applies, no matter they are not truly cocyclic.

$\{H: H = M_\psi\} \subset \{H: H = M_{\psi \cdot \phi}\}$

order	2	4	8	12	16	20	24	28	32	36
$\sim_H$	1	1	1	1	5	3	60	487	13710027	$\geq 3 \cdot 10^6$
$\sim_{H+sc}$	1	1	1	1	5	3	??	??	??	??
$\sim_{H+c}$	1	1	1	1	5	3	**16**	**6**	**100**	**35**

	Cocyclic	Non cocyclic
Sylvester	$\mathbb{Z}_2^{\log_2 4t}$	
Williamson	$\mathbb{Z}_2^2 \times \mathbb{Z}_t$	
Paley I	D_{4t}	
Paley II	$\mathbb{Z}_2^2 \times \mathbb{Z}_t$	
Ito	D_{4t}	
1-circulant core	$\mathbb{Z}_{4t-1}$-cocyclic structured	
2-circulant core	D_{4t-2}-cocyclic structured	
Goethals-Seidel	GS_{4t}-pseudo-cocyclic	
Twin prime power		always?

The Goethals-Seidel arrays

$$\begin{pmatrix} A & BR & CR & DR \\ BR & -A & RD & -RC \\ CR & -RD & -A & RB \\ DR & RC & -RB & -A \end{pmatrix} \qquad \begin{array}{l} A, B, C, D \text{ circulants,} \\ R \leftarrow^{b} [0, \ldots, 0, 1] \end{array}$$

It is Hadamard if $AA^T + BB^T + CC^T + DD^T = 4tI_t$.

The Goethals-Seidel arrays

$$GS_{4t} = \langle a, b, c, d : \; a^t = b^2 = c^2 = d^2 = 1, (a^i x)a^j = a^{i+j}x,$$
$$a^i(a^j y) = a^{j-i}y, (a^i y)(a^j y) = a^{j-i}, (a^i y_1)(a^j y_2) = a^{t-2-j-i}y_3\rangle$$

for $x \in \{1, b, c, d\}$, $y \in \{b, c, d\}$, $\{y_1, y_2, y_3\} = \{b, c, d\}$.

$$1, a, \ldots, a^{t-1}, b, ab, \ldots a^{t-1}b, c, ac, \ldots, a^{t-1}c, d, ad, \ldots, a^{t-1}d.$$

The Goethals-Seidel arrays are GS_{4t}-pseudo cocyclic

$$\begin{pmatrix} A & BR & CR & DR \\ BR & -A & RD & -RC \\ CR & -RD & -A & RB \\ DR & RC & -RB & -A \end{pmatrix} \quad \begin{pmatrix} {}^bA & B^c & C^c & D^c \\ {}^bB & A^c & {}^b\bar{D} & {}^b\bar{C} \\ {}^bC & {}^b\bar{D} & A^c & {}^b\bar{B} \\ {}^bD & {}^b\bar{C} & {}^b\bar{B} & A^c \end{pmatrix}$$

Theorem

The Goethals-Seidel array is pseudo-cocyclic over the loop GS_{4t}.

Range	(i,j,k)	$i(jk)$
$2 \le h \le t$	$(t+1, 2t+1, 4t+2-h)$	$1 + (h - 3 \bmod t)$
$t+1 \le h \le 2t$	$(2, 2t+1, 5t+1-h)$	$t + 1 + (h - 3 \bmod t)$
$2t+1 \le h \le 3t$	$(2, t+1, 6t+1-h)$	$2t + 1 + (h - 3 \bmod t)$
$3t+1 \le h \le 4t$	$(2, 2t+1, 7t+1-h)$	$3t + 1 + (h - 3 \bmod t)$

$(ij)k = h \neq i(jk)$ and **none** of the formal coboundaries are cocyclic!

The Goethals-Seidel arrays are GS_{4t}-pseudo cocyclic

$$\begin{pmatrix} A & BR & CR & DR \\ BR & -A & RD & -RC \\ CR & -RD & -A & RB \\ DR & RC & -RB & -A \end{pmatrix} \quad \begin{pmatrix} {}^bA & B^c & C^c & D^c \\ {}^bB & A^c & {}^b\bar{D} & {}^b\bar{C} \\ {}^bC & {}^b\bar{D} & A^c & {}^b\bar{B} \\ {}^bD & {}^b\bar{C} & {}^b\bar{B} & A^c \end{pmatrix}$$

Theorem

The Goethals-Seidel array is pseudo-cocyclic over the loop GS_{4t}.

$$M_\psi = (\prod_{h\in H} M_{\partial_h})R, R = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & - & - & + \\ + & + & - & - \end{pmatrix} \otimes \mathbf{1}_t$$

Permute the pairs of rows $(i, t+2-i)$, for $2 \leq i \leq \frac{t+1}{2}$.

The Goethals-Seidel arrays are GS_{4t}-pseudo cocyclic

Theorem

The Goethals-Seidel array is Hadamard if and only if the related GS_{4t}-pseudococyclic matrix satisfies the usual cocyclic test.

$$\langle Row_{ij}, Row_j \rangle = \sum_{k=1}^{4t} \left(\prod_{h \in H} \delta_{h,i(jk)} \delta_{h,(ij)k} \right) \psi(i,j)\psi(i,jk) =$$

$$\psi(i,j) \sum_{k=1}^{4t} \sigma_k \psi(i,jk) = \psi(i,j) \sum_{k=1}^{4t} \psi(i,k).$$

Furthermore, it suffices to check rows $2 \leq i \leq \frac{t+1}{2}$.

Counting -1s

Counting -1s

$$M_\psi = (\prod_{h \in H} M_{\partial_h})R, \qquad \partial_h(i,j) = \delta_{h,i}\delta_{h,j}\delta_{h,ij}$$

- Every M_{∂_h} contributes two -1s at row k at positions (k,h) (head,) and $(k, k^{-1}h)$ (tail,).

Counting -1s

$$M_\psi = (\prod_{h\in H} M_{\partial_h})R, \qquad \partial_h(i,j) = \delta_{h,i}\delta_{h,j}\delta_{h,ij}$$

- Whenever two different $M_{\partial_{h_1}}$ and $M_{\partial_{h_1}}$ share a tail and a head at row k, they constitute a path at row k.

- Consequently $\prod_{h\in H} M_{\partial_h}$ contributes twice as many -1s as maximal paths there exist at row k.

Counting -1s

$$M_\psi = (\prod_{h \in H} M_{\partial_h})R, \qquad \partial_h(i,j) = \delta_{h,i}\delta_{h,j}\delta_{h,ij}$$

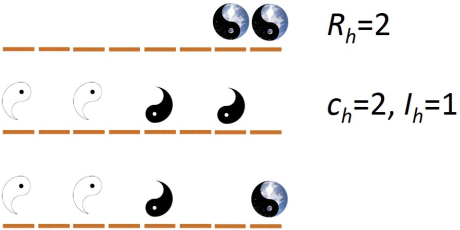
- Following the same principle, whenever a head or a tail of a path is shared by R, an intersection occurs and this tentative -1 is lost.

Counting -1s

$$M_\psi = (\prod_{h \in H} M_{\partial_h})R, \qquad \partial_h(i,j) = \delta_{h,i}\delta_{h,j}\delta_{h,ij}$$

- Consequently, the -1s of M_ψ at row h come from heads, tails and those of R which do not contribute any intersections at all,

$$2c_h + R_h - 2I_h = 2t$$

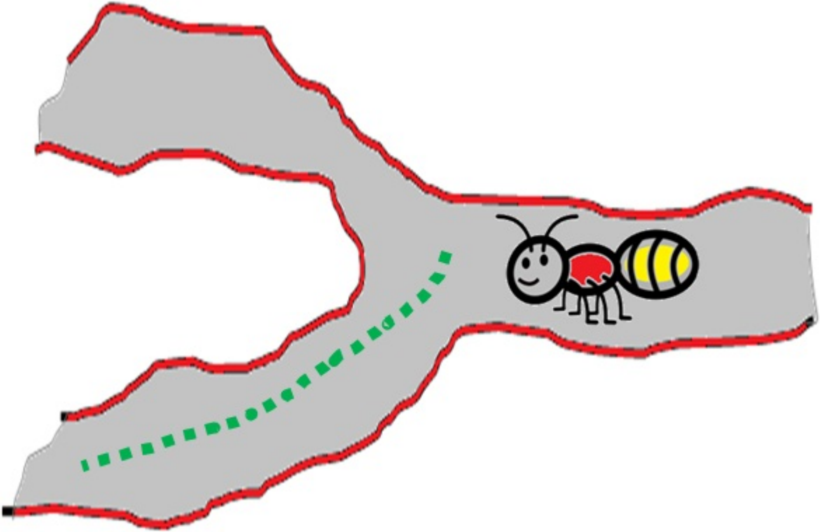


Counting -1s in practise

- Exhaustive search: $t \leq 7$ (2003).

Counting -1s in practise

- Heuristic search: Fitness = number of Hadamard rows (GA 2006, ACS 2009), $t \leq 13$.



Counting -1s in practise

- Exhaustive search via ingredients and recipes (2011), $t \leq 11$, $t \leq 23$.

Counting -1s in practise

- Cocyclic Hadamard ideals (2016), $t \leq 39$.

Counting -1s in practise

- Heuristic search (GA 2017) + local search (CSP), $t = 47$??

Alternative fitness

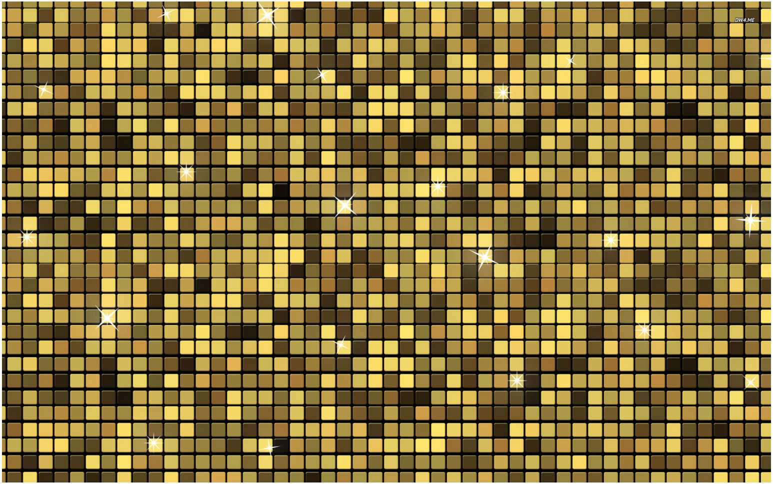
$$F(paths, intersections) = constant \tag{2}$$

Group	$F(p, I)$	$\overrightarrow{\mathbf{k}}$	Rows
$\mathbb{Z}_2^2 \times \mathbb{Z}_t$	p	$(t, \ldots, t)$	$r \equiv 1 \bmod t$
D_{4t}	$p - I$	$(t-1, \ldots, 1)$	$2, \ldots, t$
GS_{4t}	$p_A + p_B + p_C + p_D$	t	$2, \ldots, \frac{t+1}{2}$

IDEA:
$\| \overrightarrow{F}(p, I) - \overrightarrow{\mathbf{k}} \|_\infty$ instead of hamming distance!

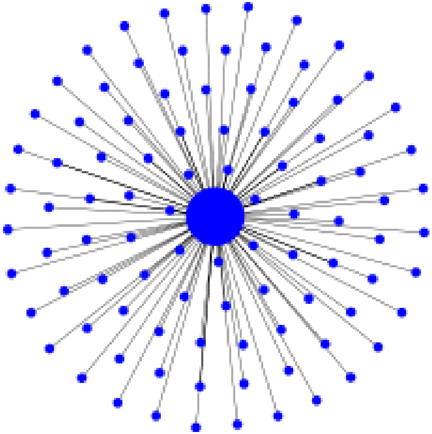
The case $D_{4\cdot 47}$

Fitness of 10000 random individuals runs on $[5, 15]$.



The case $D_{4 \cdot 47}$

Perform a heuristic such that you move to a neighbor as soon as fitness improves.



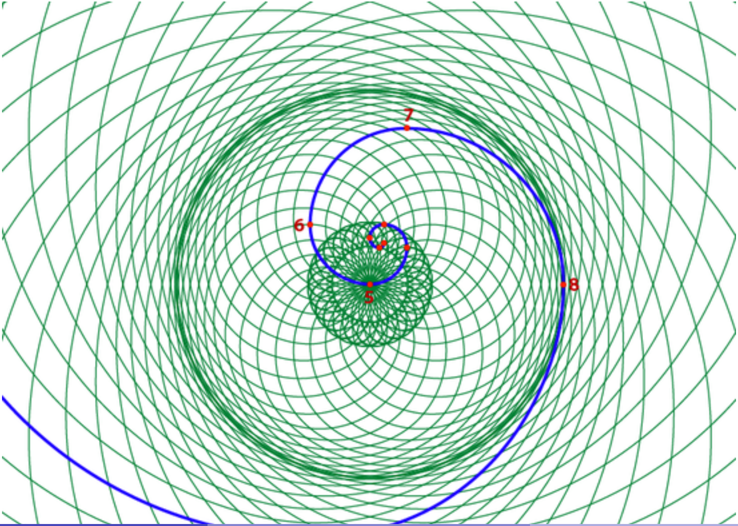
The case $D_{4\cdot 47}$

In case that none of the $4t$ neighbors works, jump to a random individual at a prefixed hamming distance (6 seems to work fine).

The case $D_{4\cdot 47}$

Reaches fitness 2 immediately!

Reaches **fitness 1** almost every run, after no more than 1000 iterations!



The case $D_{4\cdot 47}$

Unfortunately, there are many local minima 😳

The case $D_{4\cdot 47}$

Second step: local search.

Perform a radial search (radius 4 = **51.512.518** instances).

The case $D_{4\cdot 47}$

Faster by means of a Constraint Satisfaction Problem

What to come?

Thank you Mate and Ferenc!