

B. O. & T. Q.

Ilias S. Kotsireas (Ηλιας Σ. Κοτσιρεας)

CARGO Lab, www.cargo.wlu.ca

Wilfrid Laurier University, Waterloo, Ontario, Canada

Hadamard 2025

May 26-30 2025, Sevilla, Spain



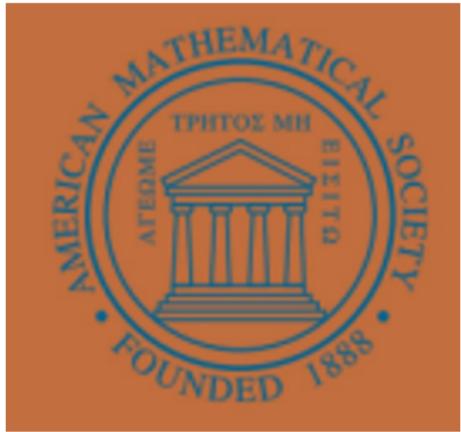
Mathematical
Surveys
and
Monographs
Volume 175

Algebraic Design Theory

Warwick de Launey
Dane Flannery



American Mathematical Society



Undergraduate Research in Orthogonal Matrices*

R. Craigen

Summer 2006

Abstract

Consider the following four (partitioned) 4×4 (± 1)-matrices:

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

They share some properties: in each one, any two rows match in the exactly half the positions. Square (± 1)-matrices with this property are called *Hadamard matrices*—the most celebrated class of *orthogonal matrices* (the more general objects are characterized by various other restrictions on entries and variations on the equation $XX^T = \lambda I$).

In other ways they differ: Look for some interesting structure within and between the blocks formed by the partition lines in our examples. Try building 8×8 Hadamard matrices that exhibit similar structures. Can you see how the last one is self-similar in a certain way? This leads to an important infinite class of Hadamard matrices having many applications.

Hadamard's 1893 conjecture that the matrices named in his honour exist in every order of the form $n = 4k$ remains unresolved today, and is regarded as one of the two most important problems in the field of combinatorics (the other deals with projective planes). Exactly 100 years later I proved an asymptotic existence result that, to this day, is the closest, in one sense, that we have come to settling this question; this summer we will chip away at it a bit more.

We will examine the fascinating inner structure of Hadamard (and other orthogonal) matrices, some of which is hinted at in our examples above. It has long been my conviction that understanding this structure will be the key to solving this and many related open questions. Accordingly I have many small projects in which a microscope is turned on various aspects of structure, including some dandy puzzles for aspiring researchers.

We will also look at some questions regarding the classification of these objects and cook up some great recipes for building them, subject to additional specifications (as demanded by various applications or theoretical considerations).

The matrices we study are used in “error-correction codes” (used for CD’s and DVD’s, wi-fi, etc.), range-finding devices (like GPS), optical filtering, interferometry, discrete Fourier analysis and many other areas. Recently some important questions relating to cutting-edge technological development in quantum computing, quantum information and quantum learning have been reduced to some the very “purely theoretical” questions about orthogonal matrices that we will be addressing.

The footnote!

*Warning: research in this field may be addictive! It involves exposure to dangerous levels of beautiful objects and tantalizing questions.

The footnote!

*Warning: research in this field may be addictive! It involves exposure to dangerous levels of beautiful objects and tantalizing questions.

↝ B. O. & T. Q.

Marco Buratti's motivation theorem

CODESCO 2024, Sevilla



MARIA BRAS-AMORÓS

MATEMÁTICA



"Las matemáticas son un juego: van más allá de los cálculos y la aritmética, tienen un aspecto estético y a la vez son una herramienta muy útil".

www.cientificascasio.com

Ilias S. Kotsireas (CARGO Lab)

B. O. & T. Q.

my Hadamard 2025 talk (based on 7+1 papers)

- ① Periodic Golay pairs **Curtis Bright, Tyler Lumsden** Math. Comp.
- ② Legendre pairs **Christoph Koutschan, Dursun Bulutoglu et al.** JCD + SPMA
Domingo Gómez Pérez, Ana Isabel Gómez Pérez ISSAC 2025
- ③ quaternary Legendre pairs
Christoph Koutschan, Arne Winterhof Stinson66-Fields Inst. Comm. + DM
- ④ weighing matrices
Radel Ben-Av, Giora Dula, Assaf Goldberger, Yossi Strassler DM
- ⑤ Turyn-type sequences ~
Hadamard matrices, T-sequences, Base sequences, Orthogonal Designs
Stephen London submitted

Periodic Golay pairs, PG(n), n EVEN

$$\text{PG}(n) \rightsquigarrow \left\{ \begin{array}{l} A = [a_1, \dots, a_n], a_i \in \{-1, +1\}, i = 1, \dots, n \\ B = [b_1, \dots, b_n], b_i \in \{-1, +1\}, i = 1, \dots, n \\ \text{PAF}(A, s) + \text{PAF}(B, s) = 0, \forall s = 1, \dots, \frac{n}{2} \\ \text{PSD}(A, s) + \text{PSD}(B, s) = 2 \cdot n, \forall s = 1, \dots, \frac{n}{2} \\ a_1 + \dots + a_n = \pm\alpha \\ b_1 + \dots + b_n = \pm\beta \\ \alpha^2 + \beta^2 = 2 \cdot n \end{array} \right.$$

- PAF denotes the Periodic Autocorrelation Function:

$$\text{PAF}(A, s) = \sum_{k=1}^n a_k a_{k+s}, s = 1, \dots, \frac{n}{2}$$

- PSD denotes the Power Spectral Density coefficients, i.e. squared magnitudes of the DFT elements

Periodic Golay pairs, General Properties

- ① $n = 2 \cdot m$ 2-compression $\rightsquigarrow \text{PSD}_A(m), \text{PSD}_B(m)$ being perfect squares
- ② $\omega = \cos\left(\frac{2\pi}{v}\right) + i \sin\left(\frac{2\pi}{v}\right) = \cos\left(\frac{\pi}{m}\right) + i \sin\left(\frac{\pi}{m}\right) \rightsquigarrow \omega^m = -1$
- ③ $\text{DFT}_A(m) = (a_0 + a_2 + \cdots + a_{v-2})\omega^0 + (a_1 + a_3 + \cdots + a_{v-1})\omega^m = A_1 - A_2$
- ④ $\text{PSD}_A(m) = (A_1 - A_2)^2 = \alpha^2 \rightsquigarrow A_1 - A_2 = \pm\alpha$
- ⑤ $\text{DFT}_B(m) = (b_0 + b_2 + \cdots + b_{v-2})\omega^0 + (b_1 + b_3 + \cdots + b_{v-1})\omega^m = B_1 - B_2$
- ⑥ $\text{PSD}_B(m) = (B_1 - B_2)^2 = \beta^2 \rightsquigarrow B_1 - B_2 = \pm\beta$
- ⑦ compatible with $\text{PSD}_A(m) + \text{PSD}_B(m) = 2 \cdot n = \alpha^2 + \beta^2$

Periodic Golay pairs, recent exhaustive searches

- D. Crnković, D. D. Danilović, R. Egan, A. Švob

“Periodic Golay pairs and pairwise balanced designs”

J. Algebraic Combin. 55 (2022), no. 1, pp. 245–257.

- ① conducted exhaustive searches for $PG(n)$ for $n \leq 40$
- ② exploited a relationship between certain pairwise balanced designs with v points and periodic Golay pairs of length v , to classify periodic Golay pairs of length less than 40.
- ③ constructed all pairwise balanced designs with v points under specific block conditions having an assumed cyclic automorphism group, and using isomorph rejection which is compatible with equivalence of corresponding periodic Golay pairs, we complete a classification up to equivalence.
- ④ done using the theory of orbit matrices and some compression techniques which apply to complementary sequences
- ⑤ used similar tools to construct new periodic Golay pairs of lengths greater than 40 where classifications remain incomplete
- ⑥ demonstrate that under some extra conditions on its automorphism group, a periodic Golay pair of length 90 does not exist
- ⑦ Some quasi-cyclic self-orthogonal codes are constructed as an added application

October 2023, Coffee in Koper, Slovenia



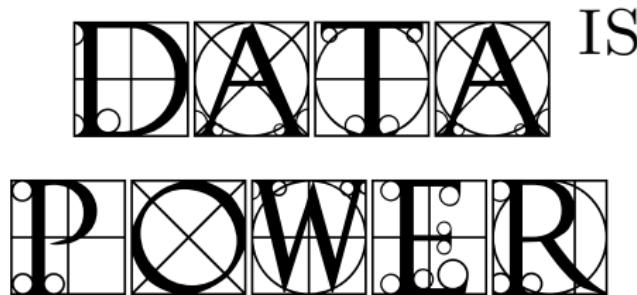
Periodic Golay pairs, recent exhaustive searches

- T. Lumsden, I. Kotsireas, C. Bright
“New results on Periodic Golay pairs”
Math. Comp. (2025), accepted & published on-line
 - ① conducted exhaustive searches for $PG(n)$ for $n \leq 72$
 - ② used isomorph rejection and compression by 2

Periodic Golay pairs, recent exhaustive searches

- T. Lumsden, I. Kotsireas, C. Bright
“New results on Periodic Golay pairs”
Math. Comp. (2025), accepted & published on-line
 - ① conducted exhaustive searches for $PG(n)$ for $n \leq 72$
 - ② used isomorph rejection and compression by 2

DATA IS
POWER



Periodic Golay pairs, conjectural construction

Conjecture: Let n be an even integer s.t. the Diophantine equation $a^2 + b^2 = 2 \cdot n$ has an integer solution (α, β) and w.l.o.g. take $\alpha \leq \beta$. Then a periodic Golay pair $\text{PG}(n)$ can be constructed as follows:

- if $n = 2 \cdot p$, p prime, $p \equiv 1 \pmod{4}$, then (P, Q) p -uncompress to a $\text{PG}(2 \cdot p)$.

$$P = \left[\frac{\alpha + \beta}{2}, \frac{\alpha - \beta}{2} \right], Q = \left[\frac{\alpha + \beta}{2}, -\frac{\alpha - \beta}{2} \right]$$

Moreover, this is a necessary and sufficient condition, i.e. for every $\text{PG}(2 \cdot p)$, the p -compression is given by (P, Q) , up to permuting the sequences and/or their elements.

- if $n \neq 2 \cdot p$, p prime, then there is a (proper) divisor d of n , s.t. the d -compression of $\text{PG}(n)$ is made up from two sequences, each of length $\frac{n}{d}$, with the property that each sequence has ideal autocorrelation 0.

Periodic Golay pairs, $PG(90)$

v	d	sequences of length v/d with zero PAF that d -uncompress to a $PG(v)$
16	2	$[-2, 0, 2, 0, 2, 0, 2, 0]$, $[-2, 0, 2, 0, 2, 0, 2, 0]$ (=)
20	5	$[1, 1, 1, -1]$, $[3, 3, 3, -3]$
32	8	$[0, 0, 0, 0]$, $[4, 4, 4, -4]$
40	4	$[0, 0, 0, 0, 0, 0, 0, 4, 0, 0]$, $[0, -4, 0, 0, 4, 0, 4, 0, 0, 4]$
40	8	$[0, 0, 0, 0, 4]$, $[0, 0, 0, 0, 8]$
50	10	$[0, 0, 0, 0, 0]$, $[0, 0, 0, 0, 10]$
50	10	$[0, 0, 0, 0, 6]$, $[0, 0, 0, 0, 8]$
52	13	$[1, 1, 1, -1]$, $[5, -5, 5, 5]$
64	4	$[-4, 0, 0, 0, 0, 0, 4, 0, 4, 0, 0, 0, 0, 4, 0]$, $[-4, 0, 0, 0, 0, 0, 4, 0, 4, 0, 0, 0, 0, 0, 4, 0]$ (=)
64	8	$[-4, 0, 0, 4, 4, 0, 0, 4]$, $[-4, 0, 0, 4, 4, 0, 0, 4]$ (=)
64	16	$[0, 0, 0, 8]$, $[0, 0, 0, 8]$ (=)
68	17	$[5, -5, -5, -5]$, $[3, -3, -3, -3]$
72	8	$[0, 0, 0, 0, 0, 0, 0, 0, 0]$, $[0, -8, 4, 0, 4, 4, 0, 4, 4]$
72	12	$[0, 0, 0, 0, 0, 0]$, $[0, 0, 0, 0, 0, 12]$
72	24	$[0, 0, 0]$, $[0, 0, 12]$
90	15	$[3, 3, 3, 3, -9, 3]$, $[-3, 3, 3, 3, 3, 3]$
90	18	$[0, 0, 0, 0, 6]$, $[0, 0, 0, 0, 12]$

Periodic Golay pairs, $PG(90)$

PG(90) open problem

Take $v = 90, \alpha = 6, \beta = 12 \rightsquigarrow PSD_A(45) = 36, PSD_B(45) = 144$

PG(106) open problem

Take $v = 106, \alpha = 4, \beta = 14 \rightsquigarrow PSD_A(53) = 16, PSD_B(53) = 196$

These two inequivalent periodic Golay pairs (A_1, B_1) and (A_2, B_2) are given by

$$A_1 = \begin{bmatrix} -----+ + - + + + - + + + + - + + + + + + + + + + - + + + + + \\ + + - - + + + + - + + + + - + + + + + + + + + + + - + + - + + + + + \end{bmatrix},$$

$$B_1 = \begin{bmatrix} - - - + - + + + + + + + + - + + + + + + + + + + + + + + - + + + + + \\ + - + + + + + \end{bmatrix},$$

$$A_2 = \begin{bmatrix} -----+ + - + + + - + + + + - + + + + + + + + + + - + + + + + \\ + + + + + + - + + + + - + + + + + + + + + + + + + + + + + + + - + + + + + \end{bmatrix},$$

$$B_2 = \begin{bmatrix} - - - + - + + + + + + + - + \\ + + - - + \end{bmatrix}.$$

Weighing matrices

- “New weighing matrices via partitioned group actions”

R. Ben-Av, G. Dula, A. Goldberger, I. Kotsireas, Y. Strassler
Discrete Math. 347 (2024)

- ➊ solved the smallest four open cases of weighing matrices, $W(n, 16)$ for $n = 23, 25, 27, 29$, which completes the existence question for weight 16
- ➋ solved the open two-core matrix $W(102, 97)$ (requires supercomputing)
- ➌ identified a common theme for the construction of all such matrices:
partitioned group matrices
- ➍ the study of partitioned group matrices generalizes some well known constructions, namely the one-core and two-core circulant constructions, with or without borders, block circulant matrices, Legendre pairs and many more
- ➎ such constructions generalize to arbitrary groups and carry an algebraic structure which we analyze in some cases
- ➏ our methods here can be made practical for larger weighing matrices
- ➐ analyzed possible location of the zeros (crystal sets) in two-core weighing matrices of co-weight 5, i.e. $W(2n, 2n - 5)$

Turyn/Golay quadruples & Turyn-type sequences

Turyn/Golay quadruples & Turyn-type sequences

- Turyn/Golay quadruples:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths n, n, n, n s.t.

$$NPAF(X, s) + NPAF(Y, s) + NPAF(Z, s) + NPAF(W, s) = 0, s = 1, \dots, n - 1$$

Shalom Eliahou two essays: <https://images.math.cnrs.fr/>

Turyn/Golay quadruples & Turyn-type sequences

- Turyn/Golay quadruples:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths n, n, n, n s.t.

$$NPAF(X, s) + NPAF(Y, s) + NPAF(Z, s) + NPAF(W, s) = 0, s = 1, \dots, n - 1$$

Shalom Eliahou two essays: <https://images.math.cnrs.fr/>

- Turyn-type sequences:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths $n, n, n, n - 1$ s.t.

$$NPAF(X, s) + NPAF(Y, s) + 2 \cdot NPAF(Z, s) + 2 \cdot NPAF(W, s) = 0, s = 1, \dots, n - 1$$

Turyn/Golay quadruples & Turyn-type sequences

- Turyn/Golay quadruples:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths n, n, n, n s.t.

$$NPAF(X, s) + NPAF(Y, s) + NPAF(Z, s) + NPAF(W, s) = 0, s = 1, \dots, n - 1$$

Shalom Eliahou two essays: <https://images.math.cnrs.fr/>

- Turyn-type sequences:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths $n, n, n, n - 1$ s.t.

$$NPAF(X, s) + NPAF(Y, s) + 2 \cdot NPAF(Z, s) + 2 \cdot NPAF(W, s) = 0, s = 1, \dots, n - 1$$

- ➊ Conjecture 1: Turyn/Golay quadruples exist for every n

Turyn/Golay quadruples & Turyn-type sequences

- Turyn/Golay quadruples:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths n, n, n, n s.t.

$$NPAF(X, s) + NPAF(Y, s) + NPAF(Z, s) + NPAF(W, s) = 0, s = 1, \dots, n - 1$$

Shalom Eliahou two essays: <https://images.math.cnrs.fr/>

- Turyn-type sequences:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths $n, n, n, n - 1$ s.t.

$$NPAF(X, s) + NPAF(Y, s) + 2 \cdot NPAF(Z, s) + 2 \cdot NPAF(W, s) = 0, s = 1, \dots, n - 1$$

① Conjecture 1: Turyn/Golay quadruples exist for every n

② Conjecture 2: Turyn-type sequences exist for every even n

Turyn/Golay quadruples & Turyn-type sequences

- Turyn/Golay quadruples:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths n, n, n, n s.t.

$$NPAF(X, s) + NPAF(Y, s) + NPAF(Z, s) + NPAF(W, s) = 0, s = 1, \dots, n - 1$$

Shalom Eliahou two essays: <https://images.math.cnrs.fr/>

- Turyn-type sequences:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths $n, n, n, n - 1$ s.t.

$$NPAF(X, s) + NPAF(Y, s) + 2 \cdot NPAF(Z, s) + 2 \cdot NPAF(W, s) = 0, s = 1, \dots, n - 1$$

① Conjecture 1: Turyn/Golay quadruples exist for every n

② Conjecture 2: Turyn-type sequences exist for every even n

“similar” combinatorial objects can have very different characteristics

Turyn/Golay quadruples & Turyn-type sequences

- Turyn/Golay quadruples:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths n, n, n, n s.t.

$$NPAF(X, s) + NPAF(Y, s) + NPAF(Z, s) + NPAF(W, s) = 0, s = 1, \dots, n - 1$$

Shalom Eliahou two essays: <https://images.math.cnrs.fr/>

- Turyn-type sequences:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths $n, n, n, n - 1$ s.t.

$$NPAF(X, s) + NPAF(Y, s) + 2 \cdot NPAF(Z, s) + 2 \cdot NPAF(W, s) = 0, s = 1, \dots, n - 1$$

① Conjecture 1: Turyn/Golay quadruples exist for every n

② Conjecture 2: Turyn-type sequences exist for every even n

“similar” combinatorial objects can have very different characteristics

▷ 5 known constructions for Turyn/Golay quadruples, smallest open case?

Turyn/Golay quadruples & Turyn-type sequences

- Turyn/Golay quadruples:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths n, n, n, n s.t.

$$NPAF(X, s) + NPAF(Y, s) + NPAF(Z, s) + NPAF(W, s) = 0, s = 1, \dots, n - 1$$

Shalom Eliahou two essays: <https://images.math.cnrs.fr/>

- Turyn-type sequences:

Four $\{-1, +1\}$ -sequences X, Y, Z, W of lengths $n, n, n, n - 1$ s.t.

$$NPAF(X, s) + NPAF(Y, s) + 2 \cdot NPAF(Z, s) + 2 \cdot NPAF(W, s) = 0, s = 1, \dots, n - 1$$

① Conjecture 1: Turyn/Golay quadruples exist for every n

② Conjecture 2: Turyn-type sequences exist for every even n

“similar” combinatorial objects can have very different characteristics

- ▷ 5 known constructions for Turyn/Golay quadruples, smallest open case?
- ▷ no known constructions for Turyn-type sequences, algorithmic ad-hoc methods.

n	$T(n, n, n, n)$	n	$T(n, n, n, n)$	n	$T(n, n, n, n)$	n	$T(n, n, n, n)$
1		51	●	101	$g + g$	151	
2	$g + g$	52	$g + g$	102	$g + g$	152	$g + g$
3	$g + g$	53	$g + g$	103		153	
4	$g + g$	54	$g + g$	104	$g + g$	154	$g + g \text{ } 77 \otimes 2$
5	$g + g$	55	●	105	● $BS(53, 52) \text{ } g + g$	155	
6	$g + g$	56	$g + g$	106	$g + g$	156	$g + g$
7	●	57	●	107	●	157	
8	$g + g$	58	$g + g$	108	$g + g$	158	$79 \otimes 2$
9	$g + g$	59	● ●	109		159	
10	$g + g$ ●	60	$g + g$	110	$g + g$	160	$g + g$
11	$g + g$ ● ●	61	●	111		161	● $BS(81, 80) \text{ } g + g$
12	$g + g$	62	$g + g$	112	$g + g$	162	$g + g$
13	●	63	●	113	●	163	
14	$g + g$ ●	64	$g + g$	114	$g + g$	164	$g + g$
15	● ●	65	$g + g$ ●	115		165	
16	$g + g$	66	$g + g$	116	$g + g$	166	
17	$g + g$	67	●	117		167	
18	$g + g$ ●	68	$g + g$	118	$59 \otimes 2$	168	$g + g$
19	●	69	●	119	●	169	
20	$g + g$	70	$35 \otimes 2$	120	$g + g$	170	$g + g$
21	$g + g$	71	●	121		171	
22	$g + g$	72	$g + g$	122	$61 \otimes 2$	172	$86 \otimes 2$
23	●	73	● $BS(37, 36)$	123		173	
24	$g + g$	74	$g + g$	124	$g + g$	174	
25	●	75	● $BS(35, 37)$	125	●	175	
26	$g + g$	76	$35 \otimes 2$	126	$g + g$	176	$g + g$
27	$g + g$ ●	77	● $BS(29, 38)$	127		177	
28	$g + g$	78	$g + g$	128	$g + g$	178	
29	●	79	● $BS(40, 39)$	129	● $BS(65, 64) \text{ } g + g$	179	
30	$g + g$	80	$g + g$	130	$g + g$	180	$g + g$
31	●	81	● $BS(41, 40) \text{ } g + g$	131		181	
32	$g + g$	82	$g + g$	132	$g + g$	182	
33	$g + g$	83	● $BS(55, 25)$	133		183	
34	$g + g$	84	$g + g$	134	$67 \otimes 2$	184	$g + g$
35	●	85	● $BS(43, 42)$	135		185	
36	$g + g$	86	$43 \otimes 2$	136	$g + g$	186	$g + g$
37	●	87	● $BS(44, 43)$	137		187	
38	$19 \otimes 2$	88	$g + g$	138	$g + g$	188	$94 \otimes 2$
39	●	89	● $BS(59, 30)$	139		189	
40	$g + g$	90	$g + g$	140	$g + g$	190	
41	$g + g$ ●	91	● $BS(45, 45)$	141		191	
42	$g + g$	92	$g + g$	142	$71 \otimes 2$	192	$g + g$
43	●	93	● $BS(47, 46)$	143		193	
44	$g + g$	94	$47 \otimes 2$	144	$g + g$	194	
45	●	95	● $BS(63, 32)$	145		195	
46	$g + g$	96	$g + g$	146	$73 \otimes 2$	196	$98 \otimes 2$
47	●	97	● $BS(49, 48)$	147		197	
48	$g + g$	98	$49 \otimes 2$	148	$g + g$	198	
49	●	99	● $BS(50, 49)$	149		199	
50	$g + g$	100	$g + g$	150	$75 \otimes 2$	200	$g + g$

State-of-the-art result on Turyn-type sequences $TT(n)$

Theorem

Turyn-type sequences $TT(n)$ exist for every even $n = 2, \dots, 40$.

State-of-the-art result on Turyn-type sequences $TT(n)$

Theorem

Turyn-type sequences $TT(n)$ exist for every even $n = 2, \dots, 40$.

Main contributions:

State-of-the-art result on Turyn-type sequences $TT(n)$

Theorem

Turyn-type sequences $TT(n)$ exist for every even $n = 2, \dots, 40$.

Main contributions:

- $TT(36)$ H. Kharaghani + BTR, JCD 2006 $\rightsquigarrow HM(428), 107 = 3 \cdot 36 - 1$

State-of-the-art result on Turyn-type sequences $TT(n)$

Theorem

Turyn-type sequences $TT(n)$ exist for every even $n = 2, \dots, 40$.

Main contributions:

- ▶ $TT(36)$ H. Kharaghani + BTR, JCD 2006 $\rightsquigarrow HM(428), 107 = 3 \cdot 36 - 1$
- ▶ $TT(38)$ D. Djokovic, H. Kharaghani et al. JCD 2012

State-of-the-art result on Turyn-type sequences $TT(n)$

Theorem

Turyn-type sequences $TT(n)$ exist for every even $n = 2, \dots, 40$.

Main contributions:

- ▶ $TT(36)$ H. Kharaghani + BTR, JCD 2006 $\rightsquigarrow HM(428), 107 = 3 \cdot 36 - 1$
- ▶ $TT(38)$ D. Djokovic, H. Kharaghani et al. JCD 2012
- ▶ $TT(40)$ S. London, PhD Thesis, 2012

WR

State-of-the-art result on Turyn-type sequences $TT(n)$

Theorem

Turyn-type sequences $TT(n)$ exist for every even $n = 2, \dots, 40$.

Main contributions:

- ▶ $TT(36)$ H. Kharaghani + BTR, JCD 2006 $\rightsquigarrow HM(428), 107 = 3 \cdot 36 - 1$
- ▶ $TT(38)$ D. Djokovic, H. Kharaghani et al. JCD 2012
- ▶ $TT(40)$ S. London, PhD Thesis, 2012

WR

```
++++--+++++-++-+---+----+---++-+---+-+  
+-++-+----+----+---++-+----+----+---++-+  
+-+--+-++-+---+---++-+---+----+----+---+  
+++-+--++-+---+---++-+---+----+----+---+
```

State-of-the-art result on Turyn-type sequences $TT(n)$

New contributions:

- $TT(42)$ S. London 2018 $\rightsquigarrow HM(500), 125 = 3 \cdot 42 - 1$

State-of-the-art result on Turyn-type sequences $TT(n)$

New contributions:

- $TT(42)$ S. London 2018 $\rightsquigarrow HM(500), 125 = 3 \cdot 42 - 1$
- $TT(44)$ S. London, I. Kotsireas 2025 $\rightsquigarrow HM(524), 131 = 3 \cdot 44 - 1$

State-of-the-art result on Turyn-type sequences $TT(n)$

New contributions:

- $TT(42)$ S. London 2018 $\rightsquigarrow HM(500), 125 = 3 \cdot 42 - 1$
- $TT(44)$ S. London, I. Kotsireas 2025 $\rightsquigarrow HM(524), 131 = 3 \cdot 44 - 1$

Theorem

Turyn-type sequences $TT(n)$ exist for every even $n = 2, \dots, 44$.

State-of-the-art result on Turyn-type sequences $TT(n)$

New contributions:

- $TT(42)$ S. London 2018 $\rightsquigarrow HM(500), 125 = 3 \cdot 42 - 1$
- $TT(44)$ S. London, I. Kotsireas 2025 $\rightsquigarrow HM(524), 131 = 3 \cdot 44 - 1$

Theorem

Turyn-type sequences $TT(n)$ exist for every even $n = 2, \dots, 44$.

Target future contributions:

- $TT(46), TT(48), TT(50), TT(52), TT(54)$

State-of-the-art result on Turyn-type sequences $TT(n)$

New contributions:

- $TT(42)$ S. London 2018 $\rightsquigarrow HM(500), 125 = 3 \cdot 42 - 1$
- $TT(44)$ S. London, I. Kotsireas 2025 $\rightsquigarrow HM(524), 131 = 3 \cdot 44 - 1$

Theorem

Turyn-type sequences $TT(n)$ exist for every even $n = 2, \dots, 44$.

Target future contributions:

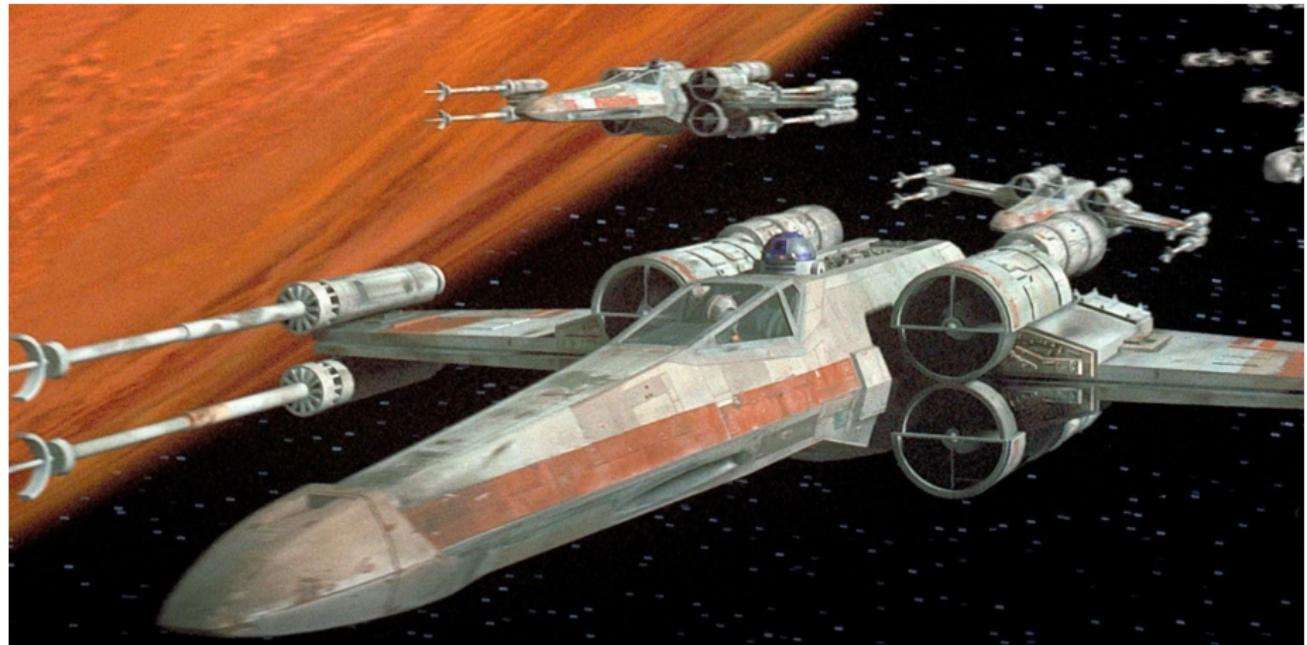
- $TT(46), TT(48), TT(50), TT(52), TT(54)$
- $TT(56) \rightsquigarrow HM(668), 167 = 3 \cdot 56 - 1$

1 Hadamard Matrices and Hadamard Designs

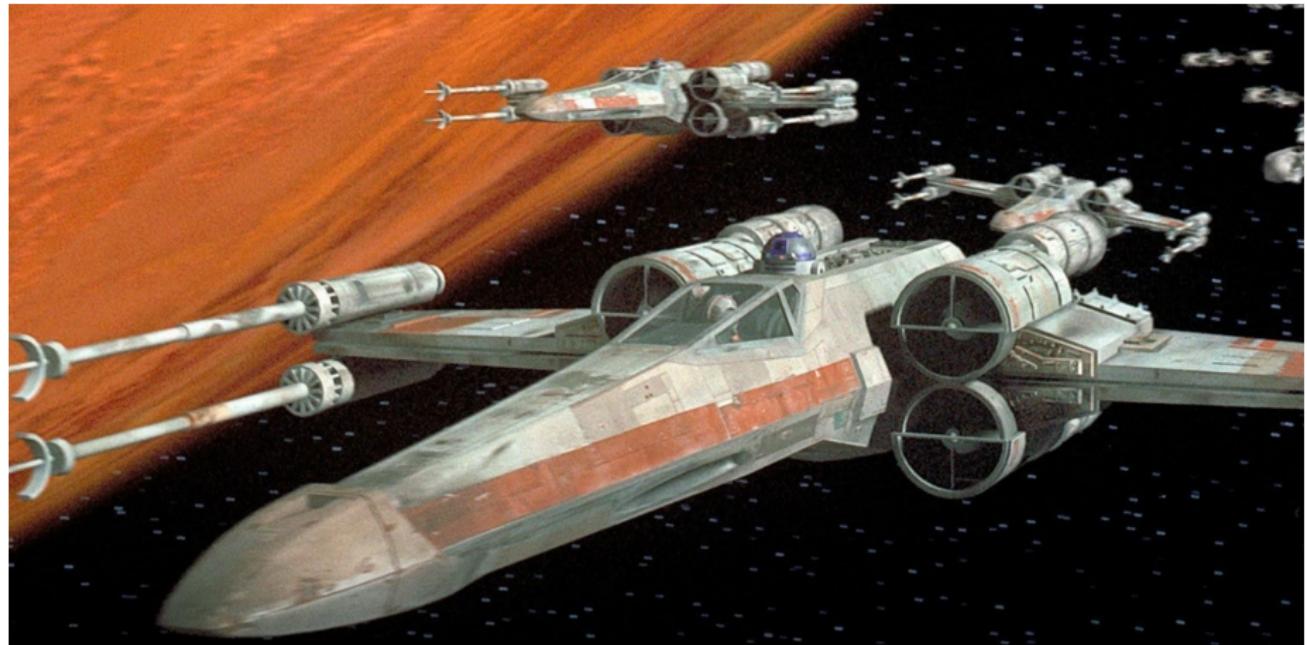
ROBERT CRAIGEN
HADI KHARAGHANI

- 1.41 **Construction** [919] Replacing variables of G (from Examples 1.33) with Goethals–Seidel type matrices A, B, C, D , and R with any type II monomial matrix, gives an $H(4n)$. If $A = I + S$, $S^T = -S$, then the $H(4n)$ is skew-type.
- 1.42 **Remark** Turyn type sequences (see §V.8.4) of lengths 56, 56, 56, 55 would give Goethals–Seidel type matrices of order 167 and so $H(668)$, the first unresolved order. This may be the currently most promising approach to this order, see [1287].

State-of-the-art result on Turyn-type sequences $TT(n)$



State-of-the-art result on Turyn-type sequences $TT(n)$



State-of-the-art result on Turyn-type sequences $TT(n)$



Digital Research
Alliance of Canada

Alliance de recherche
numérique du Canada

*This email contains important information about the results of your resource application.
Please read it carefully.*

Dear Ilias Kotsireas,

Thank you for submitting your application with the title *New World Records on Turyn-type sequences* (RRG no. 5314) to the Resources for Research Groups 2025 competition.

This message is to confirm that your application has been **successful**.

State-of-the-art result on Turyn-type sequences $TT(n)$



Digital Research
Alliance of Canada

Alliance de recherche
numérique du Canada

*This email contains important information about the results of your resource application.
Please read it carefully.*

Dear Ilias Kotsireas,

Thank you for submitting your application with the title *New World Records on Turyn-type sequences* (RRG no. 5314) to the Resources for Research Groups 2025 competition.

This message is to confirm that your application has been **successful**.

Your allocation will be available starting on **Monday, July 7, 2025**, and is valid until **Tuesday, April 7, 2026**. You can find documentation on how to use your resource allocation [here](#).

Providing these resources to your research group costs roughly **\$178,762**. This amount includes all capital (amortized) and operational costs incurred and is an average cost across all facilities.

Legendre Pairs (Seberry, 2001)

Definition

∀ odd n , two sequences $A = [a_0, \dots, a_{n-1}]$ and $B = [b_0, \dots, b_{n-1}]$, with $\{-1, +1\}$ elements, form a **Legendre Pair LP(n)** of order/length n if:

$$PAF(A, s) + PAF(B, s) = -2, s = 1, \dots, \frac{n-1}{2}$$

- Normalization: $a_0 + \dots + a_{n-1} = 1, b_0 + \dots + b_{n-1} = 1$

~~ upper bound on potential A,B seqs: $\binom{n}{\frac{n+1}{2}}$

- Consequence/Property: the PSD constant Wiener–Khinchin

$$PSD(A, s) + PSD(B, s) = 2n + 2, s = 1, \dots, \frac{n-1}{2}$$

- LPs characterized by: constancy of PAF & PSD invariants

Examples of Legendre pairs

Example (1)

$$n = 11, \quad LP(11), \quad PSD = 2 \cdot 11 + 2 = 24$$

$$A = [1, 1, -1, 1, 1, 1, -1, -1, 1, -1]$$

$$B = [1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1]$$

first 5 PAF values for A: -1, -1, -1, -1, -1

first 5 PAF values for B: -1, -1, -1, -1, -1

Example (2)

$$n = 13, \quad LP(13), \quad PSD = 2 \cdot 13 + 2 = 28$$

$$A = [-1, -1, -1, 1, -1, 1, -1, -1, 1, 1, 1, 1, 1],$$

$$B = [-1, -1, 1, -1, 1, -1, -1, 1, 1, -1, 1, 1, 1]$$

first 6 PAF values for A: 1, 1, -3, -3, -3, 1

first 6 PAF values for B: -3, -3, 1, 1, 1, -3

Example (3)

$$n = 37, \quad LP(37), \quad PSD = 2 \cdot 37 + 2 = 76$$

$A = [-1, -1, -1, 1, -1, 1, 1, -1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, -1, 1, 1, 1, -1, 1, 1, 1]$
 $B = [-1, -1, -1, 1, -1, -1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, -1, 1, 1, 1, -1, 1, 1, -1, -1, 1]$

first 18 PAF values for A: -3, 1, -3, -3, 1, 1, -3, 1, -3, -3, -3, 1, 1, 1, -3, 1, 1

first 18 PAF values for B: 1, -3, 1, 1, -3, -3, 1, 1, -3, 1, 1, -3, -3, 1, -3, -3

- 1, 25.83447494, 50.16552507, 76
- 2, 50.16552503, 25.83447496, 76
- 3, 25.83447496, 50.16552506, 76
- 4, 25.83447493, 50.16552505, 76
- 5, 50.16552507, 25.83447493, 76
- 6, 50.16552504, 25.83447494, 76
- 7, 25.83447496, 50.16552505, 76
- 8, 50.16552503, 25.83447494, 76
- 9, 25.83447496, 50.16552504, 76
- 10, 25.83447495, 50.6165525, 76
- 11, 25.83447494, 50.1655250, 76
- 12, 25.83447491, 50.1655250, 76
- 13, 50.16552505, 25.8344749, 76
- 14, 50.16552507, 25.8344749, 76
- 15, 50.16552504, 25.8344749, 76
- 16, 25.83447493, 50.1655250, 76
- 17, 50.16552507, 25.8344749, 76
- 18, 50.16552505, 25.8344749, 76

Example (4)

$$n = 55, \quad LP(55), \quad PSD = 2 \cdot 55 + 2 = 112$$

① $A := [1, -1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1];$

② $B := [1, -1, -1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1];$

③ first 27 PAF values for A:

$-9, 3, 3, -5, -1, 3, 3, 3, -5, 3, -1, -1, 3, -1, -1, 3, -1, 3, -1, -9, -9, -1, -1, -5, 3, -5, -1$

④ first 27 PAF values for B:

$7, -5, -5, 3, -1, -5, -5, -5, 3, -5, -1, -1, -5, -1, -1, -5, -1, -5, -1, 7, 7, -1, -1, 3, -5, 3, -1$

Exhaustive searches for Legendre Pairs

ℓ	order of $H_{2\ell+2}$	total number of $LP(\ell)$	
3	8	9	$= 1 \times 3^2$
5	12	50	$= 2 \times 5^2$
7	16	196	$= 4 \times 7^2$
9	20	972	$= 12 \times 9^2$
11	24	2,904	$= 24 \times 11^2$
13	28	7,098	$= 42 \times 13^2$
15	32	38,700	$= 172 \times 15^2$
17	36	93,058	$= 322 \times 17^2$
19	40	161,728	$= 448 \times 19^2$
21	44	433,944	$= 984 \times 21^2$
23	48	1,235,744	$= 2,336 \times 23^2$
25	52	2,075,000	$= 3,320 \times 25^2$
27	56	5,353,776	$= 7,344 \times 27^2$
29	60	12,401,386	$= 14,746 \times 29^2$
31	64	22,472,024	$= 23,384 \times 31^2$

exhaustive
searches
for $LP(\ell)$

LPs of prime lengths: Legendre symbol construction

For every odd prime p , $\exists \text{ LP}(p)$, via the **Legendre symbol**.

Maple code:

```
with(NumberTheory);
L:=[seq(LegendreSymbol(i,p),i=1..p-1)];
A:=[1,op(L)];
B:=[1,-op(L)];
```

(A, B) is a Legendre pair of length p , for $p = 3, 5, 7, \dots$

An interesting behavior occurs, according to the parity of $p \bmod 4$:

the mod 4 dichotomy

- $p \equiv 3 \pmod{4}$

all the PAF values of (a,b) are equal to -1

all the PSD values are equal to $p + 1$

(so we get the PAF const -2 and the PSD const $2p + 2$)

- $p \equiv 1 \pmod{4}$

all the PAF values of (a,b) belong to $\{1, -3\}$

there are only two different PSD values

Gauss sum interpretation, [Arne Winterhof](#)

(so we get the PAF const -2 and the PSD const $2p + 2$)

LPs twin primes construction

For twin primes $p, p + 2, \exists LP(p \cdot (p + 2))$

TWO CAVEATS:

- ① Twin prime conjecture \rightsquigarrow infinite classes of LPs & HMs
- ② the twin primes must have a common primitive root
turns out this is an open problem in Number Theory
(for which there is no known counter-example)

CONSTRUCTION DETAILS:

- ① $g = \text{common primitive root of } p \text{ and } p + 2,$
- ② $n = p \cdot (p + 2), ub = (p^2 - 3)/2$
- ③ Positions of the $-1's$ are encoded by:
 $[g^i \bmod n, i = 0 \dots ub, i(p + 2) \bmod n, i = 0 \dots p - 1]]$

LPs \rightsquigarrow HMs, Two circulant cores (2cc) construction

From an $LP(n), (A, B)$, form the two circulants $C(A), C(B)$.

Then a **2cc Hadamard matrix** $HM(2n + 2)$ is given by:

$$H_{2n+2} = \left[\begin{array}{cc|ccccc} - & - & + & \cdots & + & + & \cdots & + \\ - & + & + & \cdots & + & - & \cdots & - \\ \hline + & + & & & & & & \\ \vdots & \vdots & C(A) & & & C(B) & & \\ + & + & & & & & & \\ \hline + & - & & & & & & \\ \vdots & \vdots & C(B)^t & & & -C(A)^t & & \\ + & - & & & & & & \end{array} \right] \quad \begin{aligned} LP(p) &\rightsquigarrow HM(2p + 2) \\ LP(p(p + 2)) &\rightsquigarrow \\ HM(2 \cdot p \cdot (p + 2) + 2) & \end{aligned}$$

Legendre pairs \rightsquigarrow “structured” version of the Hadamard conjecture

Djokovic-Kotsireas Compression of Legendre pairs (1)

Definition (Djokovic-Kotsireas, DCC 2015)

Let $A = [a_0, a_1, \dots, a_{v-1}]$ be a sequence of length $v = d \cdot m$.

Set $a_j^{(d)} = a_j + a_{j+d} + \dots + a_{j+(m-1)d}$, for $j = 0, \dots, d-1$.

The sequence $A^{(d)} = [a_0^{(d)}, a_1^{(d)}, \dots, a_{d-1}^{(d)}]$ of length d is the ***m*-compression** of A .

Djokovic-Kotsireas Compression of Legendre pairs (1)

Definition (Djokovic-Kotsireas, DCC 2015)

Let $A = [a_0, a_1, \dots, a_{v-1}]$ be a sequence of length $v = d \cdot m$.

Set $a_j^{(d)} = a_j + a_{j+d} + \dots + a_{j+(m-1)d}$, for $j = 0, \dots, d-1$.

The sequence $A^{(d)} = [a_0^{(d)}, a_1^{(d)}, \dots, a_{d-1}^{(d)}]$ of length d is the ***m*-compression** of A .

- m -compression of $LP(v), (A, B)$, by the same m , yields two sequences $(A^{(d)}, B^{(d)})$ of length d each, $\{-m, \dots, +m\}$.
- $PAF(A^{(d)}, s) + PAF(B^{(d)}, s) = (-2) \cdot m, \quad \forall s = 1, \dots, \frac{d-1}{2}$
- $PSD(A^{(d)}, s) + PSD(B^{(d)}, s) = 2 \cdot v + 2, \quad \forall s = 1, \dots, \frac{d-1}{2}$
- m -compression \rightsquigarrow PAF scales linearly, PSD **remains invariant**

Djokovic-Kotsireas Compression of Legendre pairs (2)

Example

$$LP(15), \quad n = 15 = 3 \cdot 5 = 5 \cdot 3$$

3-compression \rightsquigarrow

$$A^{(5)} = [a_0 + a_5 + a_{10}, a_1 + a_6 + a_{11}, a_2 + a_7 + a_{12}, a_3 + a_8 + a_{13}, a_4 + a_9 + a_{14}]$$

$$B^{(5)} = [b_0 + b_5 + b_{10}, b_1 + b_6 + b_{11}, b_2 + b_7 + b_{12}, b_3 + b_8 + b_{13}, b_4 + b_9 + b_{14}]$$

5-compression \rightsquigarrow

$$A^{(3)} = [a_0 + a_3 + a_6 + a_9 + a_{12}, a_1 + a_4 + a_7 + a_{10} + a_{13}, a_2 + a_5 + a_8 + a_{11} + a_{14}]$$

$$B^{(3)} = [b_0 + b_3 + b_6 + b_9 + b_{12}, b_1 + b_4 + b_7 + b_{10} + b_{13}, b_2 + b_5 + b_8 + b_{11} + b_{14}]$$

Djokovic-Kotsireas Compression of Legendre pairs (3)

Example

$LP(133) = 133 = 7 \cdot 19$ compute its 19-compression:

- ① $A^{(7)} = [1, 1, -3, 1, -3, -3, 7], \quad B^{(7)} = [-5, -5, 5, -5, 5, 5, 1]$
- ② $PAF(A^{(7)}, s) + PAF(B^{(7)}, s) = (-2) \cdot 19 = -38, \quad s = 1, 2, 3$
- ③ $PSD(A^{(7)}, s) + PSD(B^{(7)}, s) = 2 \cdot 133 + 2 = 268, \quad s = 1, 2, 3$

-
- ① Conversely, given $A^{(7)}, B^{(7)}$, recover $LP(133)$ **decompression**
 - ② Compression is **not an one-to-one mapping**, regrettably:

$\tilde{A}^{(7)}, \tilde{B}^{(7)}$ with $PAF = -38$ and $PSD = 268$, it is not guaranteed that decompression will yield $LP(133)$

Legendre pair of length 77, DCC, 2021

Turner/Kotsireas/Bulutoglu/Geyer

- Exploit the idea of **simultaneous decompressions** for LPs of composite length based on generating binary matrices with fixed row and column sums.
- PhD thesis of Jonathan Turner, AFIT, Ohio
- First construction of $LP(77)$, $77 = 7 \times 11$ & the only known example of $LP(77)$, open problem since 2001, i.e. 20+ years

Legendre pair of length 77, DCC, 2021

Turner/Kotsireas/Bulutoglu/Geyer

- Exploit the idea of **simultaneous decompressions** for LPs of composite length based on generating binary matrices with fixed row and column sums.
- PhD thesis of Jonathan Turner, AFIT, Ohio
- First construction of $LP(77)$, $77 = 7 \times 11$ & the only known example of $LP(77)$, open problem since 2001, i.e. 20+ years
- 11-compression of $LP(77)$ reveals **PAF constancy** property:

$$A^{(7)} = [-3, 5, -3, -3, -5, 5, 5] \quad B^{(7)} = [1, -1, 1, -1, -1, 1, 1]$$
$$\begin{array}{c} \downarrow \\ -21, -21, -21 \end{array} \qquad \qquad \qquad \begin{array}{c} \downarrow \\ -1, -1, -1 \end{array}$$

Legendre pair of length 77, DCC, 2021

Turner/Kotsireas/Bulutoglu/Geyer

- Exploit the idea of **simultaneous decompressions** for LPs of composite length based on generating binary matrices with fixed row and column sums.
- PhD thesis of Jonathan Turner, AFIT, Ohio
- First construction of $LP(77)$, $77 = 7 \times 11$ & the only known example of $LP(77)$, open problem since 2001, i.e. 20+ years
- 11-compression of $LP(77)$ reveals **PAF constancy** property:

$$A^{(7)} = [-3, 5, -3, -3, -5, 5, 5] \quad B^{(7)} = [1, -1, 1, -1, -1, 1, 1]$$
$$\begin{matrix} \downarrow \\ -21, -21, -21 \end{matrix} \qquad \qquad \qquad \begin{matrix} \downarrow \\ -1, -1, -1 \end{matrix}$$

~~~ **Legendre Pairs Divisors Conjecture**

$\forall$  odd composite  $\ell$ ,  $\exists$  (at least one) proper divisor  $d$  of  $\ell$  s.t. a constant-PAF pair of sequences of lengths  $\ell/d$  & sum  $(-2)d$ , can be d-uncompressed to  $LP(\ell)$

# Legendre pairs of lengths $\ell \equiv 0 \pmod{3}$ , JCD, 2021, Kotsireas/Koutschan

- elaboration of the PAF constancy property for an arbitrary divisor  $m$  of  $\ell$

Theorem (Kotsireas/Koutschan, 2021)

If the  $m$ -compression of  $(A, B)$ ,  $(\mathcal{A}, \mathcal{B})$  is made up from two constant-PAF sequences of length  $n$ :

$$\text{PAF}(\mathcal{A}, 1) = \dots = \text{PAF}(\mathcal{A}, \frac{n-1}{2}), \text{PAF}(\mathcal{B}, 1) = \dots = \text{PAF}(\mathcal{B}, \frac{n-1}{2})$$

then the PSD values at integer multiples of  $m$  of  $A$  and  $B$  are integers, with the explicit evaluations

$$\text{PSD}(A, m \cdot s) = p_2(\mathcal{A}) - \text{PAF}(\mathcal{A}, 1), \quad s = 1, 2, \dots, \frac{n-1}{2}$$

$$\text{PSD}(B, m \cdot s) = p_2(\mathcal{B}) - \text{PAF}(\mathcal{B}, 1), \quad s = 1, 2, \dots, \frac{n-1}{2}$$

- Determination of the **complete spectrum** of the  $\ell/3$ -rd value of the DFT/PSD for  $LP(\ell)$  s.t.  $\ell \equiv 0 \pmod{3}$ .

**sample result:** for LPs of length  $\ell = 117 = 3 \cdot 39$ :

$$[PSD(A, 39), PSD(B, 39)] \in \{[28, 208], [64, 172], [112, 124]\},$$

- state-of-the-art list of **twelve** integers in the range  $< 200$  for which the question of existence of Legendre pairs remains unresolved.

85, 87, 115, 145, 159, 161, 169, 175, 177, 185, 187, 195.

# Legendre pairs of lengths $\ell \equiv 0 \pmod{5}$ , SPMA 2023, Kotsireas/Koutschan/Bulutoglu/Arquette/Turner/Ryan

- Exploit a conjecture regarding the value of  $PSD(\cdot, \frac{\ell}{5})$   
For every  $\ell \equiv 0 \pmod{5}$ , there exist Legendre pairs  $(A, B)$  of length  $\ell$  s.t.  
for some  $x \geq 0$  we have:

$$PSD(A, \frac{\ell}{5}) = \ell + 1 + \frac{\sqrt{5}}{2} \cdot x$$

$$PSD(B, \frac{\ell}{5}) = \ell + 1 - \frac{\sqrt{5}}{2} \cdot x$$

- state-of-the-art list of **ten** integers ( $< 200$ ) for which the question of  
existence of Legendre pairs remains unresolved.

115, 145, 159, 161, 169, 175, 177, 185, 187, 195.

(**half** of them are multiples of 5)

# Quaternary Legendre pairs, 2023-2024, Kotsireas/Koutschan/Winterhof

- ① "Quaternary Legendre pairs", in New Advances in Designs, Codes and Cryptography, Stinson66, Toronto, Canada, June 13-17, 2022, Eds: Charles J. Colbourn, Jeffrey H. Dinitz, Fields Institute Communications, volume 86
- ② "Quaternary Legendre pairs II", Kotsireas, Ilias S.; Koutschan, Christoph; Winterhof, Arne Quaternary Legendre pairs II. Discrete Math. 348 (2025)

## Definition

Two sequences  $A = [a_0, \dots, a_{\ell-1}]$  and  $B = [b_0, \dots, b_{\ell-1}]$ , of the same length  $\ell$ , with  $\{-1, -i, +1, +i\}$  elements, form a **quaternary Legendre Pair** if:

①  $PAF(A, s) + PAF(B, s) = -2$ , for  $s = 1, \dots, \frac{\ell-1}{2}$

- Pay attention to use complex conjugate in the definition of PAF.
- Note that the parity restriction on the length has been removed
- Algebraic Number Theory provides new restrictions/constraints

Quaternary Legendre pairs are **balanced**

### Lemma

Let  $A = [a_0, a_1, \dots, a_{\ell-1}]$ ,  $B = [b_0, b_1, \dots, b_{\ell-1}]$  be a quaternary Legendre pair of length  $\ell$ . Put

$$\alpha = \sum_{j=0}^{\ell-1} a_j \quad \text{and} \quad \beta = \sum_{j=0}^{\ell-1} b_j.$$

Then we have  $|\alpha|^2 + |\beta|^2 = 2$ ,

$$\alpha, \beta \in \{-1, 1, -i, i\} \quad \text{if } \ell \text{ is odd}$$

and

$$\{\alpha, \beta\} \in \{\{0, 1+i\}, \{0, 1-i\}, \{0, -1+i\}, \{0, -1-i\}\} \quad \text{if } \ell \text{ is even.}$$

↝ Jonathan Jedwab and Thomas Pender,  
Combinatorial Theory, 2025  
“Two constructions of quaternary Legendre pairs of even length”

## Lemma

Let  $(A, B)$  be a quaternary Legendre pair of *odd* length  $\ell$  with  $\alpha = \beta = 1$ . Then

$$\left( \begin{array}{cc|ccccc} -1 & -1 & 1 & \dots & 1 & 1 & \dots & 1 \\ -1 & 1 & 1 & \dots & 1 & -1 & \dots & -1 \\ \hline 1 & 1 & & & & & & \\ \vdots & \vdots & C(A) & & & & C(B) & \\ 1 & 1 & & & & & & \\ \hline 1 & -1 & & & & & & \\ \vdots & \vdots & C(\bar{B})^T & & & & -C(\bar{A})^T & \\ 1 & -1 & & & & & & \end{array} \right)$$

is a quaternary complex Hadamard matrix of order  $2(\ell + 1)$

## Lemma

Let  $(A, B)$  be a quaternary Legendre pair of **even** length  $\ell$  with  $\alpha = 0$  and  $\beta = 1 + i$ . Then

$$\left( \begin{array}{cc|ccccc} -1 & i & 1 & \dots & 1 & 1 & \dots & 1 \\ -i & 1 & 1 & \dots & 1 & -1 & \dots & -1 \\ \hline 1 & 1 & & & & & & \\ \vdots & \vdots & C(A) & & & & C(B) & \\ 1 & 1 & & & & & & \\ \hline 1 & -1 & & & & & & \\ \vdots & \vdots & C(\bar{B})^T & & & & -C(\bar{A})^T & \\ 1 & -1 & & & & & & \end{array} \right)$$

is a quaternary complex Hadamard matrix of order  $2(\ell + 1)$

# qLPs toy examples

- ① even  $n = 2$ ,  $A = (1, -1)$ ,  $B = (1, i)$

$$PAF(A, 1) = -2, \quad PAF(B, 1) = 0$$

- ② odd  $n = 15$ ,

$$A = (1, 1, 1, -1, 1, 1, i, -i, -1, 1, -i, -1, -1, i, -1)$$

$$B = (1, 1, i, 1, i, -i, i, -1, -i, i, 1, -i, -1, -1, -i)$$

|                     |           |      |           |      |      |      |           |
|---------------------|-----------|------|-----------|------|------|------|-----------|
| 7 PAF values for A: | $-1 + 2I$ | $-1$ | $-1 + 4I$ | $1$  | $-1$ | $-3$ | $-1 + 2I$ |
| 7 PAF values for B: | $-1 - 2I$ | $-1$ | $-1 - 4I$ | $-3$ | $-1$ | $1$  | $-1 - 2I$ |
|                     | $-2$      | $-2$ | $-2$      | $-2$ | $-2$ | $-2$ | $-2$      |

# Seed Sequences

## Definition

For a prime  $p > 2$  let two “seed” sequences  $A_p = (a_j^{(p)})$  and  $B_p = (b_j^{(p)})$  be defined by:

$$a_j^{(p)} = \begin{cases} 0, & j \equiv 0 \pmod{p}, \\ 2 \left(\frac{j}{p}\right), & j \not\equiv 0 \pmod{p}, \end{cases} \quad j = 0, 1, \dots$$

and

$$b_j^{(p)} = \begin{cases} 1 + i, & j \equiv 0 \pmod{p}, \\ 0, & j \not\equiv 0 \pmod{p}, \end{cases} \quad j = 0, 1, \dots$$

## Theorem

*The construction of the previous Definition satisfies:*

$$PAF(A_p, 0) = 4(p - 1), \quad PAF(B_p, 0) = 2,$$

$$PAF(A_p, s) = -4, \quad PAF(B_p, s) = 0, \quad s = 1, 2, \dots, p - 1,$$

$$DFT(A_p, s) = \begin{cases} 2 \left( \frac{s}{p} \right) p^{1/2}, & p \equiv 1 \pmod{4}, \\ 2i \left( \frac{s}{p} \right) p^{1/2}, & p \equiv 3 \pmod{4}, \end{cases}$$

$$DFT(B_p, s) = 1 + i, \quad s = 1, 2, \dots, p - 1,$$

$$PSD(A_p, s) = 4p, \quad PSD(B_p, s) = 2, \quad s = 1, 2, \dots, p - 1,$$

$$PSD(A_p, s) + PSD(B_p, s) = 2(2p + 1), \quad s = 1, 2, \dots, p - 1.$$

seed sequences  $A_p, B_p$  provide promising 2-compressions of qLPS

```

> n := 17;
omegal7 := cos(2*Pi/n) + sin(2*Pi/n)*I;
a17:=[2, 0, -1-I, -1+I, 1+I, -1-I, 1-I, 1-I, 0, -1+I, 0, 1+I, -1+I, -1-I, -1+I];
b17:=[-1-I, 0, 0, 1-I, -1+I, -2, 1-I, -1-I, 2*I, 0, 2, -1+I, 2, 2, 1+I, -1-I, -1+I];
convert(a17,'+');
convert(b17,'+');
checkSol(a17,b17);

```

$$\begin{aligned}
n &:= 17 \\
\omega l7 &:= \cos\left(\frac{2\pi}{17}\right) + I \sin\left(\frac{2\pi}{17}\right) \\
a17 &:= [2, 0, 0, -1 - I, -1 + I, 1 + I, -1 - I, 1 - I, 1 - I, 1 - I, 0, -1 + I] \\
b17 &:= [-1 - I, 0, 0, 1 - I, -1 + I, -2, 1 - I, -1 - I, 2I, 0, 2, -1 + I] \\
&\qquad\qquad\qquad 0 \\
&\qquad\qquad\qquad 1 + I
\end{aligned}$$

n = 17, a = 0, b = 1+I

```

1, 11.95435283, 58.04564729, 70.00000012
2, 32.47032693, 37.52967306, 69.99999999
3, 58.38683479, 11.61316519, 69.99999998
4, 42.49851355, 27.50148646, 70.00000001
5, 2.156428559, 67.84357142, 69.99999998
6, 35.65184145, 34.34815858, 70.00000003
7, 65.60881828, 4.391181717, 70.00000000
8, 8.491143941, 61.50885606, 70.00000000
9, 19.88365876, 50.11634125, 70.00000001
10, 13.73338800, 56.26661202, 70.00000002
11, 30.01014793, 39.98985207, 70.00000000
12, 5.987369174, 64.01263085, 70.00000002
13, 67.69143005, 2.308569960, 70.00000001
14, 1.726538051, 68.27346191, 69.99999996
15, 48.17528264, 21.82471734, 69.99999998
16, 31.57392552, 38.42607479, 70.00000031

```

```
for j from 1 to n-1 do
    p1||j := convert(sPSD(sDFT(a17,omega17,j)),exp):
od;
```





# Unified description of combinatorial objects

