130+ Years of the Hadamard Conjecture

Ilias S. Kotsireas (Ηλιας Σ. Κοτσιρεας)

CARGO Lab, www.cargo.wlu.ca

Wilfrid Laurier University, Waterloo, Ontario, Canada

Combinatorial Designs and Codes (CODESCO'24)
Satellite event: 9th European Congress of Mathematics
July 8-12, 2024, Sevilla, Spain

17 YEARS AGO ... SEVILLA 2007 HADAMARD CONF.

17 YEARS AGO ... SEVILLA 2007 HADAMARD CONF.

17 YEARS AGO ... SEVILLA 2007 HADAMARD CONF.

17 YEARS AGO ... SEVILLA 2007 HADAMARD CONF.

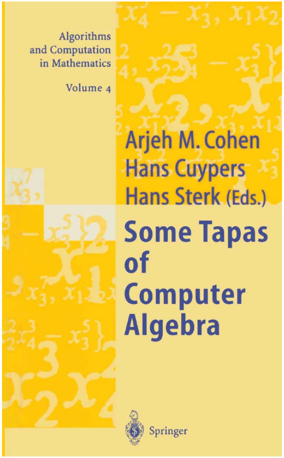
17 YEARS AGO ... SEVILLA 2007 HADAMARD CONF.

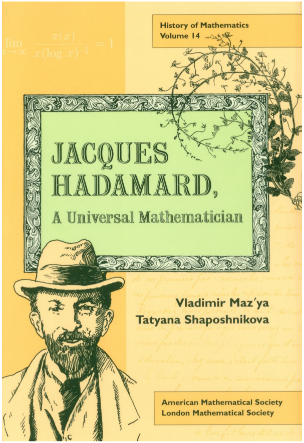
17 YEARS AGO ... SEVILLA 2007 HADAMARD CONF.

17 YEARS AGO ... SEVILLA 2007 HADAMARD CONF.


NO DO


NO8DO


Algorithms
and Computation
in Mathematics
Volume 4
Arjeh M. Cohen
Hans Cuypers
Hans Sterk (Eds.)
Some Tapas
of
Computer
Algebra
Springer



Jacques Salomon Hadamard

8 December 1865 (Versailles) – 17 October 1963 (Paris)

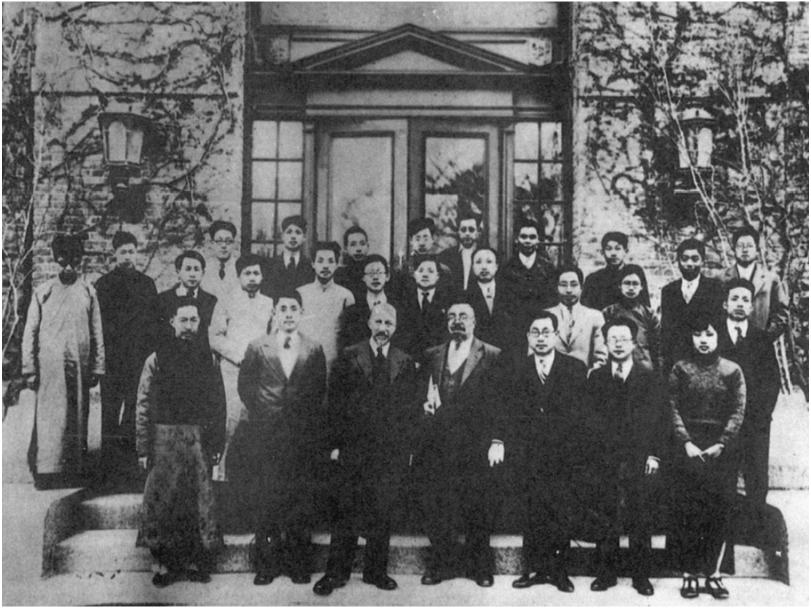
https://www.fondation-hadamard.fr/

A foundation promoting scientific excellence in mathematics

Biographical highlights

https://www.britannica.com/biography/Jacques-Salomon-Hadamard

- 1869: The Hadamard family moves to Paris
- 1884: 1st place in entrance examinations: École Polytechnique & ENS
- 1892: doctorate: ENS
- 1892: Grand Prix des Sciences Mathématiques: "Determination of the Number of Primes Less than a Given Number"
- 1893–1896: University of Bordeaux
- 1896: proof of the prime number theorem
- 1897: Alfred Dreyfus affair
- 1897-1935: professorship: Collège de France, Paris
- 1912–1935: professorship: École Polytechnique, Paris
- Spent WWII in the United States and the United Kingdom
- 1944: Hardy: LMS intro: "mathematics living legend"
- 1945: PUP: "The Psychology of Invention in the Mathematical Field"



Genesis of the Hadamard conjecture

1893

Sur le module maximum que puisse atteindre un déterminant, C. R. Acad. Sci. Paris **116**, 1500.

Résolution d'une question relative aux déterminants, Bull. Sci. Math. (2) **17**, 240–246.

Hadamard matrices are $n \times n$ (square) matrices H with ± 1 elements s.t.

$$H \cdot H^t = nI_n \longrightarrow HM(n)$$

- $\frac{1}{\sqrt{n}} H$ is an orthogonal matrix, $|\det(H)| = n^{n/2}$
- trivial cases: $n = 1, [1]$ and $n = 2$, $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- well-known necessary condition: $n \equiv 0 \pmod 4$
- the sufficiency of this condition is the celebrated Hadamard conjecture
- "There exists a Hadamard matrix of order n, for every $n \equiv 0 \pmod 4$" (1893)

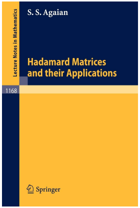
Computational state-of-the-art

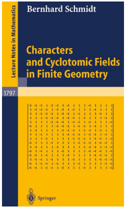
- smallest unresolved order until 1985: 268, K. Sawade, Graphs Combin.
- smallest unresolved order until 2005: 428, H. Kharaghani+BTR, JCD
- $HM(764)$, D. Z. Djokovic, Combinatorica 2008
- **smallest unresolved order until 2024: $\mathbf{668}$**
- 3 unresolved cases < 1000: $668, 716, 892$
- 10 unresolved cases < 2000:
  $1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, 1964$
- 2012: list of integers $v < 500$ for which no Hadamard matrices of order $4v$ are known consisted of 13 integers, all of them primes $\equiv 3 \pmod 4)$

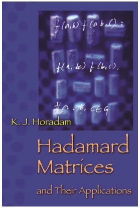
$$\mathbf{167}, \mathbf{179}, \mathbf{223}, \cancel{251}, 283, 311, 347, 359, 419, 443, 479, 487, 491$$

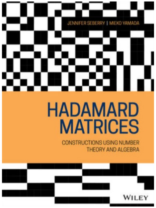
- $HM(4 \cdot 251)$ Djokovic, Golubitsky, Kotsireas, JCD, 2012
  unions of orbits approach + 4 zero-PAF sequences of lengths 251 + GS
- Magma and Sage contain databases of HMs
- N.J.A. Sloane on-line database http://neilsloane.com/hadamard/

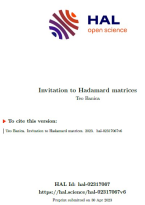
Hadamard Matrices Books & Chapters

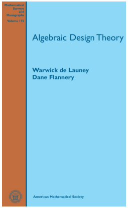


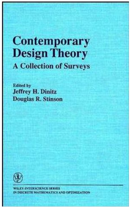


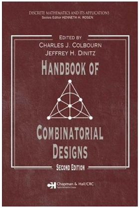


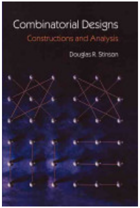


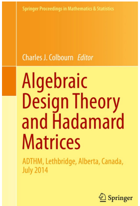


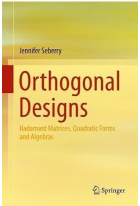












Hadamard Matrices Existence Results

- C. Lam, S. Lam, V. D. Tonchev, Bounds on the number of affine, symmetric, and Hadamard designs and matrices. JCTA 92 (2000), no. 2, 186–196.
- C. Lam, S. Lam, V. D. Tonchev, Bounds on the number of Hadamard designs of even order. JCD 9 (2001), no. 5, 363–378.

The number of inequivalent Hadamard matrices of order 40 is at least 3.66×10^{11}.

- E. Merchant, Exponentially many Hadamard designs. DCC 38 (2006), no. 2, 297–308.

If a Hadamard design of order n exists, then the number of inequivalent Hadamard matrices of size $8n$ is at least $2^{8n-16-11\log n}$.

- https://images.math.cnrs.fr/
- LA CONJECTURE DE HADAMARD (I), par Shalom Eliahou
- LA CONJECTURE DE HADAMARD (II), par Shalom Eliahou

Hadamard Matrices Asymptotic Existence Results

- J. Seberry-Wallis, JCTA 1976, "On the existence of Hadamard matrices"
- R. Craigen, JCTA 1995, "Signed groups, sequences, and the asymptotic existence of Hadamard matrices"
- W. de Launey, JCTA 2009, "Note On the asymptotic existence of Hadamard matrices"

Hadamard Matrices Asymptotic Existence Results

- J. Seberry-Wallis, JCTA 1976, "On the existence of Hadamard matrices"
- R. Craigen, JCTA 1995, "Signed groups, sequences, and the asymptotic existence of Hadamard matrices"
- W. de Launey, JCTA 2009, "Note On the asymptotic existence of Hadamard matrices"

It is conjectured that Hadamard matrices exist for all orders $4t$ ($t > 0$). However, despite a sustained effort over more than five decades, the strongest overall existence results are asymptotic results of the form: for all odd natural numbers k, there is a Hadamard matrix of order $k2^{[a+b\log_2 k]}$, where a and b are fixed non-negative constants. To prove the Hadamard Conjecture, it is sufficient to show that we may take $a = 2$ and $b = 0$. Since Seberry's ground-breaking result, which showed that we may take $a = 0$ and $b = 2$, there have been several improvements where b has been by stages reduced to 3/8. In this paper, we show that for all $\epsilon > 0$, the set of odd numbers k for which there is a Hadamard matrix of order $k2^{2+[\epsilon\log_2 k]}$ has positive density in the set of natural numbers. The proof adapts a number-theoretic argument of Erdos and Odlyzko to show that there are enough Paley Hadamard matrices to give the result.

Important topics

- cocyclic approach:
  K. Horadam, D. Flannery, P. O'Cathain. R. Egan, The Sevilla Group
- cohomology approach: A. Goldberger, G. Dula
- Eliahou Theory, Coding Theory reformulation of the (structured) Hadamard conjecture
- large body of work on complexity/randomness
  A. Winterhof, C. Mauduit, A. Sarkozy, K. Gyarmati etc
- skew HMs symmetris HMs, Butson-Hadamard, complex HMs,

Important topics

- cocyclic approach:
  K. Horadam, D. Flannery, P. O'Cathain. R. Egan, The Sevilla Group
- cohomology approach: A. Goldberger, G. Dula
- Eliahou Theory, Coding Theory reformulation of the (structured) Hadamard conjecture
- large body of work on complexity/randomness
  A. Winterhof, C. Mauduit, A. Sarkozy, K. Gyarmati etc
- skew HMs symmetris HMs, Butson-Hadamard, complex HMs, Bush HMs

Important topics

- cocyclic approach:
  K. Horadam, D. Flannery, P. O'Cathain. R. Egan, The Sevilla Group
- cohomology approach: A. Goldberger, G. Dula
- Eliahou Theory, Coding Theory reformulation of the (structured) Hadamard conjecture
- large body of work on complexity/randomness
  A. Winterhof, C. Mauduit, A. Sarkozy, K. Gyarmati etc
- skew HMs symmetris HMs, Butson-Hadamard, complex HMs, Bush HMs Obama HMs,

Important topics

- cocyclic approach:
  K. Horadam, D. Flannery, P. O'Cathain. R. Egan, The Sevilla Group
- cohomology approach: A. Goldberger, G. Dula
- Eliahou Theory, Coding Theory reformulation of the (structured) Hadamard conjecture
- large body of work on complexity/randomness
  A. Winterhof, C. Mauduit, A. Sarkozy, K. Gyarmati etc
- skew HMs symmetris HMs, Butson-Hadamard, complex HMs, Bush HMs
  Obama HMs, ~~Trump HMs~~,

Important topics

- cocyclic approach:
  K. Horadam, D. Flannery, P. O'Cathain. R. Egan, The Sevilla Group
- cohomology approach: A. Goldberger, G. Dula
- Eliahou Theory, Coding Theory reformulation of the (structured) Hadamard conjecture
- large body of work on complexity/randomness
  A. Winterhof, C. Mauduit, A. Sarkozy, K. Gyarmati etc
- skew HMs symmetris HMs, Butson-Hadamard, complex HMs, Bush HMs
  Obama HMs, ~~Trump HMs~~, ~~Biden HMs~~

Important topics

- cocyclic approach:
  K. Horadam, D. Flannery, P. O'Cathain. R. Egan, The Sevilla Group
- cohomology approach: A. Goldberger, G. Dula
- Eliahou Theory, Coding Theory reformulation of the (structured) Hadamard conjecture
- large body of work on complexity/randomness
  A. Winterhof, C. Mauduit, A. Sarkozy, K. Gyarmati etc
- skew HMs symmetris HMs, Butson-Hadamard, complex HMs, Bush HMs
  Obama HMs, ~~Trump HMs~~, ~~Biden HMs~~ replaced by N. Haley & K. Harris.

Formulae for the number of Hadamard matrices of order n

1. Shalom Eliahou
   Enumerative combinatorics and coding theory
   Enseign. Math. (2), 40(1-2):171–185, 1994.
2. Warwick de Launey and Daniel A. Levin
   A Fourier-analytic approach to counting partial Hadamard matrices
   Cryptogr. Commun., 2(2):307–334, 2010.

- The Eliahou formula uses Coding Theory: binary linear code + weight enumerator
- The de Launey-Levin formula uses multidimensional integrals associated with lattice walks
- Both formulas require a certain amount of technical definitions before they can be stated in a self-contained manner and are very difficult (computationally) to evaluate

It is far from evident why these two formulae (should) agree for all $n \equiv 0 \pmod 4$

Constructions for Hadamard matrices

1. Sylvester Kronecker product construction: $HM(n) \otimes HM(m) \longrightarrow HM(nm)$
2. U. Scarpis, 1898: $HM(n)$ $s.t.$ $(n-1)$ is prime $\longrightarrow HM((n-1)n)$
3. R.E.A.C. Paley, 1933: $n \equiv 0 \pmod 4$ s.t. $n-1$ or $\frac{n}{2}-1$ is p^k $\longrightarrow HM(n)$
4. J. Seberry Wallis, 1976: $\forall\, q$ odd, $\exists\, HM(2^t \cdot q)$, for t large enough.
5. Gruner's theorem: p and $p+2$ are twin primes, $\longrightarrow HM(p(p+2)+1)$
6. Circulant HMs: **Ryser conjecture (1963): CHM(4) is the only one ...**
7. Williamson method: uses the Williamson array $\begin{pmatrix} -A & B & C & D \\ B & A & D & -C \\ C & -D & A & B \\ D & C & -B & A \end{pmatrix}$

   where A, B, C, D are $n \times n$ circulant matrices satisfying certain properties.
8. Miyamoto JCTA 1991:

   requires 32 $(0,-1,1)$-matrices U_{ij}, V_{ij} s.t. $U_{ij} \pm V_{ij}$ are $(-1,1)$-matrices

There are literally $100s$ of HM constructions ...

They all suffer from two kinds of disadvantages:

- they produce a sparse set of orders (e.g twin primes)
- they fail for specific parameter values (e.g. Williamson for $n = 35$)

Opinion: The Hadamard conjecture is too general

The introduction of the **circulant** structure, furnishes two promising candidates and their variants for a proof of the (general) Hadamard conjecture $\rightsquigarrow$

1. Turyn/Golay quadruples conjecture: 4 sequences with **aperiodic autoc.** 0
2. Legendre pairs conjecture: 2 sequences with **periodic autocorrelation** -2

These two conjectures:

- introduce some **structure** into the more general Hadamard Conjecture. This structure is described in terms of four/two circulant matrices whose first rows (seen as binary sequences) have constant aperiodic/periodic autocorrelation $0/-2$
- **do not fail** for any value of the parameter, i.e. cover the full range of multiples of 4

1. I. S. Kotsireas et al. Hadamard ideals and Hadamard matrices with two circulant cores *European J. Combin.*, 27(5):658–668, 2006.
2. I. S. Kotsireas, Structured Hadamard Conjecture, 2013
in: Number Theory and Related Areas Eds: J. M. Borwein, I. Shparlinski, and W. Zudilin

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

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

- Turyn-type sequences:
  Four $\{-1,+1\}$-sequences X, Y, Z, W of lengths $n, n, n, n-1$ s.t.
  $NPAF(X,s) + NPAF(Y,s) + 2 \cdot NPAF(Z,s) + 2 \cdot NPAF(W,s) = 0, s = 1, \ldots n-1$

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

- Turyn-type sequences:
  Four $\{-1,+1\}$-sequences X, Y, Z, W of lengths $n, n, n, n-1$ s.t.
  $NPAF(X,s) + NPAF(Y,s) + 2 \cdot NPAF(Z,s) + 2 \cdot NPAF(W,s) = 0, s = 1, \ldots n-1$

1. 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.
  $NPAF(X,s) + NPAF(Y,s) + NPAF(Z,s) + NPAF(W,s) = 0, s = 1, \ldots n-1$
- Turyn-type sequences:
  Four $\{-1,+1\}$-sequences X, Y, Z, W of lengths $n, n, n, n-1$ s.t.
  $NPAF(X,s) + NPAF(Y,s) + 2 \cdot NPAF(Z,s) + 2 \cdot NPAF(W,s) = 0, s = 1, \ldots n-1$

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

- Turyn-type sequences:
  Four $\{-1,+1\}$-sequences X, Y, Z, W of lengths $n, n, n, n-1$ s.t.
  $NPAF(X,s) + NPAF(Y,s) + 2 \cdot NPAF(Z,s) + 2 \cdot NPAF(W,s) = 0, s = 1, \ldots n-1$

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

- Turyn-type sequences:
  Four $\{-1,+1\}$-sequences X, Y, Z, W of lengths $n, n, n, n-1$ s.t.
  $NPAF(X,s) + NPAF(Y,s) + 2 \cdot NPAF(Z,s) + 2 \cdot NPAF(W,s) = 0, s = 1, \ldots n-1$

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.
  $NPAF(X,s)+NPAF(Y,s)+NPAF(Z,s)+NPAF(W,s)=0, s=1,\dots n-1$
- 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	$T(n,n,n,n)$	n	$T(n,n,n,n)$
1		51	🔴	101	$g+g$	151		201	🟢$BS(101,100)$
2	$g+g$	52	$g+g$	102	$g+g$	152	$g+g$	202	$101\otimes 2$
3	$g+g$	53	$g+g$	103		153		203	
4	$g+g$	54	$g+g$	104	$g+g$	154	$g+g$ $77\otimes 2$	204	$102\otimes 2$
5	$g+g$	55	🟢	105	🟢$BS(53,52)$ $g+g$	155		205	
6	$g+g$	56	$g+g$	106	$g+g$	156	$g+g$	206	
7	🔴	57	🟢	107	🟣	157		207	
8	$g+g$	58	$g+g$	108	$g+g$	158	$79\otimes 2$	208	$104\otimes 2$
9	$g+g$	59	🔴🟢	109		159		209	🟢$BS(105,104)$
10	$g+g$ 🔵	60	$g+g$	110	$g+g$	160	$g+g$	210	$105\otimes 2$
11	$g+g$ 🔴🟢	61	🟢	111		161	🟢$BS(81,80)$ $g+g$	211	
12	$g+g$	62	$g+g$	112	$g+g$	162	$g+g$	212	$106\otimes 2$
13	🟢	63	🟢	113	🟣	163		213	
14	$g+g$ 🔵	64	$g+g$	114	$g+g$	164	$g+g$	214	
15	🔴🟢	65	$g+g$ 🟢	115		165		215	
16	$g+g$	66	$g+g$	116	$g+g$	166		216	$108\otimes 2$
17	$g+g$	67	🟢	117		167		217	
18	$g+g$ 🔵	68	$g+g$	118	$59\otimes 2$	168	$g+g$	218	$10+2\cdot 104DS$
19	🔴	69	🟢	119	🟣	169		219	
20	$g+g$	70	$35\otimes 2$	120	$g+g$	170	$g+g$	220	$110\otimes 2$
21	$g+g$	71	🟢	121		171		221	
22	$g+g$	72	$g+g$	122	$61\otimes 2$	172	$86\otimes 2$	222	
23	🔴	73	🟢$BS(37,36)$	123		173		223	
24	$g+g$	74	$g+g$	124	$g+g$	174		224	$112\otimes 2$
25	🟢	75	🟢 $BS(38,37)$	125	🟣	175		225	
26	$g+g$	76	$38\otimes 2$	126	$g+g$	176	$g+g$	226	
27	$g+g$ 🔴	77	🟢 $BS(39,38)$	127		177		227	
28	$g+g$	78	$g+g$	128	$g+g$	178		228	
29	🟢	79	🟢 $BS(40,39)$	129	🟢$BS(65,64)$ $g+g$	179		229	
30	$g+g$	80	$g+g$	130	$g+g$	180	$g+g$	230	
31	🔴	81	🟢 $BS(41,40)$ $g+g$	131		181		231	
32	$g+g$	82	$g+g$	132	$g+g$	182		232	
33	$g+g$	83	🟣 $BS(55,28)$	133		183		233	
34	$g+g$	84	$g+g$	134	$67\otimes 2$	184	$g+g$	234	
35	🟢	85	🟢?$BS(43,42)$	135		185		235	
36	$g+g$	86	$43\otimes 2$	136	$g+g$	186	$g+g$	236	
37	🟢	87	🟢?$BS(44,43)$	137		187		237	
38	$19\otimes 2$	88	$g+g$	138	$g+g$	188	$94\otimes 2$	238	
39	🟢	89	🟣 $BS(59,30)$	139		189		239	
40	$g+g$	90	$g+g$	140	$g+g$	190		240	
41	$g+g$ 🟢	91	🟢?$BS(46,45)$	141		191		241	
42	$g+g$	92	$g+g$	142	$71\otimes 2$	192	$g+g$	242	
43	🟢	93	🟢?$BS(47,46)$	143		193		243	
44	$g+g$	94	$47\otimes 2$	144	$g+g$	194		244	
45	🟢	95	🟣$BS(63,32)$	145		195		245	
46	$g+g$	96	$g+g$	146	$73\otimes 2$	196	$98\otimes 2$	246	
47	🟢	97	🟢?$BS(49,48)$	147		197		247	
48	$g+g$	98	$49\otimes 2$	148	$g+g$	198		248	
49	🟢	99	🟢?$BS(50,49)$	149		199		249	
50	$g+g$	100	$g+g$	150	$75\otimes 2$	200	$g+g$	250	

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

Theorem

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

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

Theorem

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

Main contributions:

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

Theorem

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

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 $n = 2, \ldots, 40$.

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 $n = 2, \ldots, 40$.

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 $n = 2, \ldots, 40$.

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 $n = 2, \ldots, 40$.

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

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

$HM(668), 167 = 3 \cdot 56 - 1$

Autocorrelation (periodic and aperiodic)

- The **periodic autocorrelation function** associated to a finite sequence $A = [a_0, \dots, a_{n-1}]$ of length n is defined as

$$P_A(s) = \sum_{k=0}^{n-1} a_k a_{k+s}, \; s = 0, \dots, n-1,$$

  where $k + s$ is taken modulo n, when $k + s > n$.
- The **aperiodic autocorrelation function** associated to a finite sequence $A = [a_0, \dots, a_{n-1}]$ of length n is defined as

$$N_A(s) = \sum_{k=0}^{n-1-s} a_k a_{k+s}, \; s = 0, \dots, n-1,$$

We are mostly concerned with binary $\{-1, +1\}$, ternary $\{-1, 0, +1\}$ and quaternary $\{\pm 1, \pm i\}$ sequences.
Note that for sequences with complex elements, a_{k+s} is replaced by $\overline{a_{k+s}}$.

Example: $n = 7$, $A = [a_1, \ldots, a_7]$

$$
\begin{aligned}
P_A(0) &= {a_1}^2 + {a_2}^2 + {a_3}^2 + {a_4}^2 + {a_5}^2 + {a_6}^2 + {a_7}^2 \\
P_A(1) &= a_1a_2 + a_2a_3 + a_3a_4 + a_4a_5 + a_5a_6 + a_6a_7 + a_7a_1 \\
P_A(2) &= a_1a_3 + a_2a_4 + a_3a_5 + a_4a_6 + a_5a_7 + a_6a_1 + a_7a_2 \\
P_A(3) &= a_1a_4 + a_2a_5 + a_3a_6 + a_4a_7 + a_5a_1 + a_6a_2 + a_7a_3 \\
P_A(4) &= a_1a_4 + a_2a_5 + a_3a_6 + a_4a_7 + a_5a_1 + a_6a_2 + a_7a_3 \\
P_A(5) &= a_1a_3 + a_2a_4 + a_3a_5 + a_4a_6 + a_5a_7 + a_6a_1 + a_7a_2 \\
P_A(6) &= a_1a_2 + a_2a_3 + a_3a_4 + a_4a_5 + a_5a_6 + a_6a_7 + a_7a_1
\end{aligned}
$$

$$
\begin{aligned}
N_A(0) &= {a_1}^2 + {a_2}^2 + {a_3}^2 + {a_4}^2 + {a_5}^2 + {a_6}^2 + {a_7}^2 \\
N_A(1) &= a_1a_2 + a_2a_3 + a_3a_4 + a_4a_5 + a_5a_6 + a_6a_7 \\
N_A(2) &= a_1a_3 + a_2a_4 + a_3a_5 + a_4a_6 + a_5a_7 \\
N_A(3) &= a_1a_4 + a_2a_5 + a_3a_6 + a_4a_7 \\
N_A(4) &= a_1a_5 + a_2a_6 + a_3a_7 \\
N_A(5) &= a_1a_6 + a_2a_7 \\
N_A(6) &= a_1a_7
\end{aligned}
$$

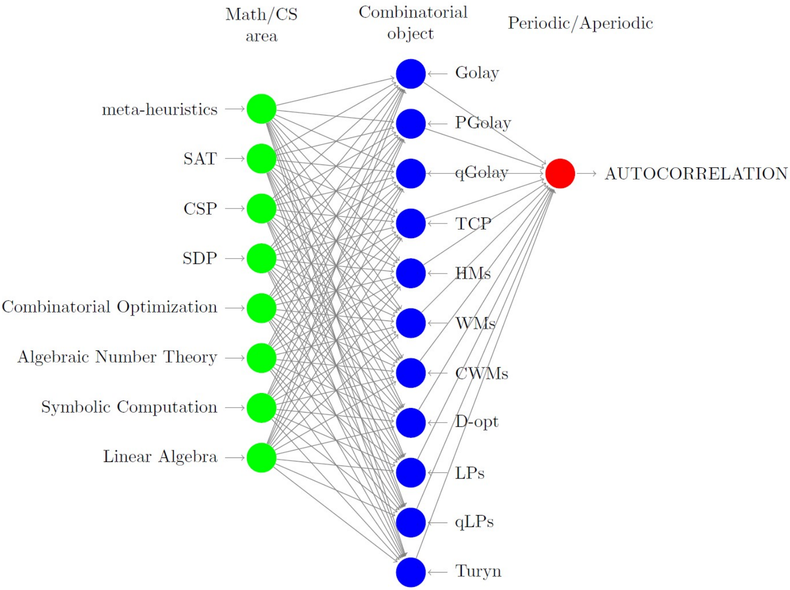
Circulant matrices

A $n \times n$ matrix $C(A)$ is called **circulant** if every row (except the first) is obtained by the previous row by a right cyclic shift by one.

$$C(A) = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_2 & a_3 & \dots & a_0 & a_1 \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{bmatrix}$$

- Consider a finite sequence $A = [a_0, \dots, a_{n-1}]$ of length n and the circulant matrix $C(A)$ whose first row is equal to A. Then $P_A(i)$ is the inner product of the first row of $C(A)$ and the $i+1$ row of $C(A)$.
- **symmetry property** $\rightsquigarrow$ $P_A(s) = P_A(n-s), s = 1, \dots, n-1.$
- 2^{nd} **ESF property** $\rightsquigarrow$ $P_A(1) + P_A(2) + \dots + P_A(n-1) = 2e_2(a_0, \dots, a_{n-1})$
- $\rightsquigarrow$ $N_A(s) + N_A(n-s) = P_A(s), s = 1, \dots, n-1.$

Unified description of combinatorial objects



Constraint Satisfaction Problems (CSP)

- General AI formalism to solve search problems, using V, D, C
- The Sevilla Group DAM 2019, "Generating binary partial HMs"

Constraint Satisfaction Problems (CSP)

- General AI formalism to solve search problems, using V, D, C
- The Sevilla Group DAM 2019, "Generating binary partial HMs"
  V. Alvarez, J.A. Armario, R.M. Falcón, M.D. Frau, F. Gudiel, M.B. Güemes, A. Osuna
- CSPLib: A problem library for constraints https://www.csplib.org/
- **prob084 2cc Hadamard matrix Legendre pairs**

Constraint Satisfaction Problems (CSP)

- General AI formalism to solve search problems, using V, D, C
- The Sevilla Group DAM 2019, "Generating binary partial HMs"
  V. Alvarez, J.A. Armario, R.M. Falcón, M.D. Frau, F. Gudiel, M.B. Güemes, A. Osuna
- CSPLib: A problem library for constraints https://www.csplib.org/
- **prob084 2cc Hadamard matrix Legendre pairs**

```
#
# 2cc Hadamard matrix Legendre pairs CSP, {V,D,C}, for ell = 5
# Created by: Ilias S. Kotsireas, ikotsire@gmail.com, Date Created: December 15, 2020
# 10 variables, 10 {-1,+1} domains, 4 constraints, (2 linear and 2 quadratic)
#

V :=
a1, a2, a3, a4, a5
b1, b2, b3, b4, b5

D :=
Da1 = ... = Da5 = {-1,+1}
Db1 = ... = Db5 = {-1,+1}

C :=
c1 := a1*a2+a2*a3+a3*a4+a4*a5+a5*a1+b1*b2+b2*b3+b3*b4+b4*b5+b5*b1 = -2

c2 := a1*a3+a2*a4+a3*a5+a4*a1+a5*a2+b1*b3+b2*b4+b3*b5+b4*b1+b5*b2 = -2

c3 := a1+a2+a3+a4+a5 = 1

c4 := b1+b2+b3+b4+b5 = 1
```

Legendre Pairs (Seberry, 2001)

Definition

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

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

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

  $\rightsquigarrow$ upper bound on potential A,B seqs: $\binom{n}{\frac{n+1}{2}}$
- Consequence/Property: the PSD constant Wiener–Khinchin

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

- 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, -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,-1,1,1,1,-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,-1,1,-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, -3, 1, 1, 1, -3, 1, 1
first 18 PAF values for B: 1, -3, 1, 1, -3, -3, 1, -3, 1, 1, 1, 1, -3, -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. $A := [1, -1, -1, 1, 1, 1, -1, -1, -1, -1, -1, -1, 1, -1, 1, -1, -1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1,$
   $-1, 1, 1, 1, -1, 1, 1, -1, 1, 1, -1, -1, -1, 1, 1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1];$
2. $B := [1, -1, -1, -1, 1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1,$
   $-1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, 1, -1, -1, -1, -1];$
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 $p, \exists\ LP(p)$, 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 $p = 3, 5, 7, \ldots$

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

the mod 4 dichotomy

- $p \equiv 3 \,(mod\ 4)$
  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 $2p+2$)

- $p \equiv 1 \,(mod\ 4)$
  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. $g =$ common primitive root of p and $p+2$,
2. $n = p \cdot (p+2), ub = (p^2 - 3)/2$
3. Positions of the $-1's$ are encoded by:
   $[g^i \mod n, i = 0 \ldots ub, i(p+2) \mod n, i = 0 \ldots p-1)]$

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:

$$H_{2n+2} = \left[\begin{array}{cc|ccc ccc} - & - & + & \cdots & + & + & \cdots & + \\ - & + & + & \cdots & + & - & \cdots & - \\ \hline + & + & & & & & & \\ \vdots & \vdots & & C(A) & & & C(B) & \\ + & + & & & & & & \\ \hline + & - & & & & & & \\ \vdots & \vdots & & C(B)^t & & & -C(A)^t & \\ + & - & & & & & & \end{array}\right]$$

$LP(p) \rightsquigarrow HM(2p+2)$

$LP(p(p+2)) \rightsquigarrow$
$HM(2 \cdot p \cdot (p+2) + 2)$

Legendre pairs $\rightsquigarrow$ "structured" version of the Hadamard conjecture

Djokovic-Kotsireas Compression of Legendre pairs (1)

Definition (Djokovic-Kotsireas, DCC 2015)

Let $A = [a_0, a_1, \ldots, a_{v-1}]$ be a sequence of length $v = d \cdot m$.
Set $a_j^{(d)} = a_j + a_{j+d} + \ldots + a_{j+(m-1)d}$, for $j = 0, \ldots, d-1$.
The sequence $A^{(d)} = [a_0^{(d)}, a_1^{(d)}, \ldots, a_{d-1}^{(d)}]$ of length d is the m-compression of A.

Djokovic-Kotsireas Compression of Legendre pairs (1)

Definition (Djokovic-Kotsireas, DCC 2015)

Let $A = [a_0, a_1, \ldots, a_{v-1}]$ be a sequence of length $v = d \cdot m$.
Set $a_j^{(d)} = a_j + a_{j+d} + \ldots + a_{j+(m-1)d}$, for $j = 0, \ldots, d-1$.
The sequence $A^{(d)} = [a_0^{(d)}, a_1^{(d)}, \ldots, a_{d-1}^{(d)}]$ 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, $\{-m, \ldots + m\}$.
- $PAF(A^{(d)}, s) + PAF(B^{(d)}, s) = (-2) \cdot m, \quad \forall s = 1, \ldots, \frac{d-1}{2}$
- $PSD(A^{(d)}, s) + PSD(B^{(d)}, s) = 2 \cdot v + 2, \quad \forall s = 1, \ldots, \frac{d-1}{2}$
- 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:

$$A^{(7)} = [-3, 5, -3, -3, -5, 5, 5] \qquad B^{(7)} = [1, -1, 1, -1, -1, 1, 1]$$

$$\downarrow \qquad\qquad\qquad\qquad \downarrow$$

$$-21, -21, -21 \qquad\qquad -1, -1, -1$$

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 ℓ

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:
$\mathrm{PAF}(\mathcal{A}, 1) = \cdots = \mathrm{PAF}(\mathcal{A}, \frac{n-1}{2}), \mathrm{PAF}(\mathcal{B}, 1) = \cdots = \mathrm{PAF}(\mathcal{B}, \frac{n-1}{2})$
then the PSD values at integer multiples of m of A and B are integers, with the explicit evaluations

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

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

- 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 $\ell = 117 = 3 \cdot 39$:

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

- 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 ℓ 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)

Multiplication Theorems

Turyn's multiplication of Golay pairs

1. Hall polynomial: (discrete GF) $[a_0, \ldots, a_{n-1}] \leftrightarrow a_0 + a_1 z + \ldots + a_{n-1} z^{n-1}$
2. (A, B) Golay pair of length g, (C, D) Golay pair of length v
3. The product pair (E, F) is a Golay pair of length gv
4. $E(z) = \frac{1}{2}[A(z) + B(z)]C(z^g) + \frac{1}{2}[A(z) - B(z)]D(z^{-g})z^{gv-g}$
5. $F(z) = \frac{1}{2}[B(z) - A(z)]C(z^{-g})z^{gv-g} + \frac{1}{2}[A(z) + B(z)]D(z^g)$

Multiplication of Golay & periodic Golay pairs (Djokovic-Kotsireas)

Theorem

If (A, B) is a Golay pair of length g and (C, D) is a periodic Golay pair of length v, then Turyn's pair (E, F) is a periodic Golay pair of length gv.

Open Problem: find multiplication theorems for Legendre pairs

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", submitted

Definition

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

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

- Pay attention to use complex conjugate in the definiton 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 $A = [a_0, a_1, \ldots, a_{\ell-1}]$, $B = [b_0, b_1, \ldots, b_{\ell-1}]$ *be a quaternary Legendre pair of length* ℓ. *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

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

Lemma

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

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

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

Lemma

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

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

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:

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

and

$$b_j^{(p)} = \begin{cases} 1 + i, & j \equiv 0 \bmod p, \\ 0, & j \not\equiv 0 \bmod p, \end{cases} \qquad j = 0, 1, \ldots$$

Theorem

The construction of the previous Definition satisfies:

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

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

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

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

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

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

seed sequences A_p, B_p provide promising 2-compressions of qLPs