Cyclic $(v; k_1, k_2, k_3; \lambda)$ difference families with $v \equiv 3 \pmod 4$ a prime

Dragomir Z. Djokovic, Ilias S. Kotsireas

University of Waterloo, Wilfrid Laurier University

Waterloo ON, Canada

djokovic@uwaterloo.ca, ikotsire@wlu.ca

Summary

We construct several new cyclic difference families $(v; k_1, k_2, k_3; \lambda)$ with $v \equiv 3 \pmod 4$ a prime and $\lambda = k_1 + k_2 + k_3 - \dfrac{3v-1}{4}$.

The construction is based on the method of orbits, together with an efficient algorithm to solve a corresponding 3-way matching problem.

Such families can be used in conjunction with the well-known Paley-Todd difference sets to construct Hadamard and skew Hadamard matrices of order $4v$.

In particular, we construct the first example of a skew Hadamard matrix of order $4 \cdot 239$.

Motivation

Hadamard matrices are $n \times n$ matrices H with ± 1 elements such that $H \cdot H^t = nI_n$.

trivial cases: $n = 1$ and $n = 2$.

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)

smallest unresolved order until 1985: 268

smallest unresolved order until 2004: 428

smallest four unresolved orders until 2012:
$668 = 4 \cdot 167, \quad 716 = 4 \cdot 179, \quad 892 = 4 \cdot 223, \quad 1004 = 4 \cdot 251$

Construction of a HM of order 1004, Djokovic, Golubitsky, Kotsireas, JCD, 2012

unions of orbits approach, new matching algorithm based on hashing techniques,
4 complementary sequences of lengths 251, plug them into the Goethals-Seidel array.

Autocorrelation of finite sequences

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

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

  where $k + s$ is taken modulo n, when $k + s > n$.

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

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

We are mostly concerned with binary $\{-1, +1\}$, ternary $\{-1, 0, +1\}$ and 4th roots of unity $\{\pm 1, \pm i\}$ sequences.

Note that for sequences with complex number elements, a_{k+s} is replaced by $\overline{a_{k+s}}$.

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

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

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

$$P_A(s) = N_A(s) + N_A(n - s), s = 1, ..., n - 1$$

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** $\rightsquigarrow$ $P_A(s) = P_A(n-s), s = 1, \dots, n-1.$
- $2^{\mathbf{nd}}$ **ESF property** $\rightsquigarrow$ $P_A(1) + P_A(2) + \dots + P_A(n-1) = 2e_2(a_0, \dots, a_{n-1})$
- $\rightsquigarrow$ $N_A(s) + N_A(n-s) = P_A(s), s = 1, \dots, n-1.$

```
> restart;
> aa:=[-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];

  bb:=[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];
```

$aa := [-1, -1, -1, -1, -1, -1, -1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, 1, 1]$

$bb := [1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, 1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, -1, -1, 1, -1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1]$

```
> nops(aa); nops(bb);
```

50

50

```
> PAF := proc(a,s)
  local i,j,n,paf;
  paf := 0;
  n := nops(a);
  for i from 1 to n do
  paf := paf + a[i]*a[((i+s-1) mod n) + 1];
  od:
  RETURN(paf);
  end proc:
> seq(PAF(aa,s),s=1..25);
```

2, 2, -2, 2, -2, -2, -6, 2, 2, -2, 2, 6, -2, 2, -2, -6, -6, 2, -10, 2, 2, -2, -2, -6, -2

```
> seq(PAF(bb,s),s=1..25);
```

-2, -2, 2, -2, 2, 2, 6, -2, -2, 2, -2, -6, 2, -2, 2, 6, 6, -2, 10, -2, -2, 2, 2, 6, 2

```
> seq(PAF(aa,s)+PAF(bb,s),s=1..25);
```

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0

```
>
```

Complementary Sequences

Definition:

Let $\{A_i\}_{i=1,\ldots,t}$ be t sequences of length v with complex elements. The sequences $\{A_i\}_{i=1,\ldots,t}$ are called complementary, if

$$\sum_{i=1}^{t} PAF_{A_i} = [\alpha_0, \underbrace{\alpha, \ldots, \alpha}_{v-1 \text{ terms}}]$$

with the convention:

$$PAF_{A_i} = [PAF_{A_i}(0), PAF_{A_i}(1), \ldots, PAF_{A_i}(v-1)].$$

Algorithms and Metaheuristics for Combinatorial Matrices,
Ilias S. Kotsireas, in Handbook of Combinatorial Optimization, 2nd edition,
Pardalos, P. M., Du, D.-Z., Graham, R. L. (eds)
pp. 283-309, Springer 2013

Unified description of combinatorial objects

number/type of sequences	defining property	name
1 binary	aper. autoc. $0, \pm 1$	Barker sequences
1 ternary	per. autoc. 0	circulant weighing matrices
2 binary	aper. autoc. 0	Golay sequences
2 binary	per. autoc. 0	Hadamard matrices
2 binary	per. autoc. 2	D-optimal matrices
2 binary	per. autoc. -2	Hadamard matrices
2 ternary	aper. autoc. 0	TCP
2 ternary	per. autoc. 0	Weighing matrices
3 binary	aper. autoc. const.	Normal sequences
4 binary	aper. autoc. 0	Base sequences
4 binary	aper. autoc. 0	Turyn type sequences
4 ternary	aper. autoc. 0	T-sequences
4 ternary	per. autoc. 0	T-matrices
$2 \ldots 12$ binary	per. autoc. zero	PCS

Power Spectral Density, PSD

Seberry & Gysin first introduced the PSD concept in the search for complementary sequences of various kinds.

Definition:

$PSD([a_1, \ldots, a_n], k)$ denotes the k-th element of the power spectral density sequence, i.e. the square magnitude of the k-th element of the discrete Fourier transform (DFT) sequence associated to $[a_1, \ldots, a_n]$.

The DFT sequence associated to $[a_1, \ldots, a_n]$ is defined as

$$DFT_{[a_1,\ldots,a_n]} = [\,\mu_0, \ldots, \mu_{n-1}\,], \text{ with } \mu_k = \sum_{i=0}^{n-1} a_{i+1}\,\omega^{ik}, \; k = 0, \ldots, n-1$$

where $\omega = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ is a primitive n-th root of unity.

An important relationship: **Wiener-Khinchin Theorem**

- The PSD of a sequence is equal to the DFT of its PAF sequence

$$\mid \mu_k \mid^2 = \sum_{j=0}^{n-1} PAF_A(j)\omega^{jk}$$

- The PAF of a sequence is equal to the inverse DFT of its PSD sequence

$$PAF_A(j) = \frac{1}{n} \sum_{j=0}^{n-1} \mid \mu_k \mid^2 \omega^{-jk}$$

The **Parseval Theorem** provides a *horizontal* relationship between the elements of a sequence $[a_1, \ldots, a_n]$ and its DFT sequence:

$$\sum_{i=1}^{n} \mid a_i \mid^2 = \frac{1}{n} \sum_{i=1}^{n} PSD([a_1, \ldots, a_n], i)$$

The **PSD theorem** provides a *vertical* relationship between the elements of two sequences $[a_1, \ldots, a_n]$ and $[b_1, \ldots, b_n]$.

```
> restart; Digits := 30;
```

$$Digits := 30$$

```
> aa:=[-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];

  bb:=[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];
```

$$aa := [-1, -1, -1, -1, -1, -1, -1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, 1, 1]$$

$$bb := [1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, 1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, -1, -1, 1, -1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1]$$

```
1, 87.005424454998786158779794798, 12.994575545001213841220200 5203, 100.000000000000000000000000000
2, 38.300910807301752211033593677 4, 61.690089192698247788966406 3224, 99.999999999999999999999999998
3, 44.633164960844338773349525822 5, 55.366835039155661226650474 1778, 100.000000000000000000000000000
4, 86.036673577623558750539151470 4, 13.963326422376441249460848 5296, 100.000000000000000000000000000
5, 90.249223594996214535365126037 0, 9.750776405003785464634873 96287, 99.999999999999999999999999999
6, 11.465561574321691567300081494 2, 88.534438425678308432699918 5057, 99.999999999999999999999999999
7, 59.717643834157526278178392429 3, 40.282356165842473721821607 5700, 99.999999999999999999999999993
8, 40.395342401612696341396934832 9, 59.604657598387303658603065 1669, 99.999999999999999999999999998
9, 44.299802891932235785134869638 4, 55.700197108067764214865130 3617, 100.000000000000000000000000000
10, 45.527864045000420607181652662 7, 54.472135954999579392818347 3373, 100.000000000000000000000000000
11, 56.452314801804562947805714130 4, 43.547685198195437052194285 8699, 100.000000000000000000000000000
12, 78.373686899517426122358058020 0, 21.626313100482573877641941 9798, 99.999999999999999999999999998
13, 40.952853792542013761762630652 3, 59.047146207457986238237369 3477, 100.000000000000000000000000000
14, 60.387741906400938164144285924 8, 39.612258093599061835855714 0743, 99.999999999999999999999999991
15, 9.750776405003785464634873962 82, 90.249223594996214535365126037 0, 99.999999999999999999999999998
16, 16.108857711569792035701535556 4, 83.891142288430207964298464443 5, 99.999999999999999999999999999
17, 95.552731141157980358591890208 8, 4.447268858842019641408109790 89, 99.999999999999999999999999997
18, 38.208294857454749527604575152 0, 61.791705142545250472395424848 0, 100.000000000000000000000000000
19, 26.541817771928953105441280534 0, 73.458182228071046894558719465 5, 99.999999999999999999999999995
20, 54.472135954999579392818347337 7, 45.527864045000420607181652662 4, 100.000000000000000000000000000
21, 13.339960304337565038746599530 3, 86.660039695662434961253400469 8, 100.000000000000000000000000000
22, 77.082444809111272761698575004 4, 22.917555190888727238301424995 5, 99.999999999999999999999999999
23, 31.504286046296037792209297573 4, 68.495713953703962207790702426 8, 100.000000000000000000000000000
24, 53.640485455086122518223208866 1, 46.359514544913877481776791134 0, 100.000000000000000000000000000
```

```
>
```

PSD criterion

case study: 2 complementary sequences of length n, PAF 0, PSD $2n$, n is even.

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

if for a certain sequence $[a_1, \ldots, a_n]$ there exists $i \in \{1, \ldots, n-1\}$ with the property that $PSD([a_1, \ldots, a_n], i) > \beta$, then this sequence cannot be used to construct 2 such complementary sequences

Important Consequence: we can now **decouple** the PAF equations, roughly corresponding to cutting down the complexity by half.

Consider the ring $\mathbf{Z}_v = \{0, 1, \ldots, v-1\}$ of integers modulo a positive integer v.

Let $k_1, \ldots, k_t$ be positive integers and λ an integer such that

$$\lambda(v-1) = \sum_{i=1}^{t} k_i(k_i - 1), \tag{1}$$

Let $X_1, \ldots, X_t$ be subsets of $\mathbf{Z}_v$ such that

$$|X_i| = k_i, \quad i \in \{1, \ldots, t\}. \tag{2}$$

Definition

We say that $X_1, \ldots, X_t$ are *supplementary difference sets* (SDS) with parameters $(v; k_1, \ldots, k_t; \lambda)$, if for every nonzero element $c \in \mathbf{Z}_v$ there are exactly λ ordered pairs (a, b) such that $a - b = c \pmod{v}$ and $\{a, b\} \subseteq X_i$ for some $i \in \{1, 2, \ldots, t\}$.

The parameter n is defined as: $n = k_1 + \cdots + k_t - \lambda$.

SDSs with $t = 1$ are called cyclic difference sets

SDSs with $t = 2$ are called difference families with two base blocks

References

- Baumert 1971
- Stinson 2004
- D. Jungnickel, A. Pott, K. W. Smith,
  Difference sets
  in
  Handbook of combinatorial designs.
  Edited by C. J. Colbourn and J. H. Dinitz. Second edition. 2007
- Djokovic, Dragomir Z.
  Cyclic (v;r,s;lambda) difference families with two base blocks and v <= 50.
  Ann. Comb. 15 (2011), no. 2, 233--254.

We are interested in the case of difference families (SDSs) with three base blocks, i.e. $t = 3$ and in the special class for which v is equal to a prime $p \equiv 3 \pmod 4$.

These SDSs can be used with the well-known difference sets for primes $p \equiv 3 \pmod 4$, (see the book of van Lint & Wilson) "Paley-Todd difference sets".

For SDSs $(v; k_1, k_2, k_3; \lambda)$ with three base blocks we have that $n = k_1 + k_2 + k_3 - \lambda$ and if we denote the $\{\pm 1\}$-sequences associated to it by A, B, C, then using the general formulae from

Djokovic, Dragomir Z. and Kotsireas, Ilias S.
Compression of periodic complementary sequences and applications.
Des. Codes Cryptogr. 74 (2015), no. 2, 365-377

$$\mathrm{PSD}(A, i) + \mathrm{PSD}(B, i) + \mathrm{PSD}(C, i) = 4n, \ i = 1, \ldots, v-1, \tag{3}$$

and

$$\mathrm{PAF}(A, i) + \mathrm{PAF}(B, i) + \mathrm{PAF}(C, i) = 3v - 4n = 1, \ i = 1, \ldots, v-1. \tag{4}$$

because $4n = 3v - 1$.

Examples

$\mathrm{SDS}(67; 39, 39, 36; 64), \quad n = 50$

{6, 8, 9, 10, 16, 17, 18, 21, 22, 23, 24, 25, 26, 27, 28, 30, 31, 35, 36, 38, 39, 40, 41, 43, 46, 47, 50, 53, 54, 55, 56, 59, 60, 61, 62, 63, 64, 65, 66}

{1, 6, 9, 12, 13, 15, 16, 17, 19, 21, 24, 25, 26, 27, 29, 32, 33, 34, 36, 37, 39, 40, 41, 42, 43, 45, 46, 48, 50, 52, 54, 55, 56, 57, 59, 60, 61, 62, 65}

{2, 3, 7, 9, 12, 13, 15, 17, 19, 20, 24, 25, 26, 30, 32, 33, 34, 36, 38, 39, 41, 42, 43, 44, 45, 48, 50, 52, 54, 55, 57, 58, 59, 60, 65, 66}

$\mathrm{SDS}(67; 30, 30, 27; 37), \quad n = 50$

{8, 12, 13, 15, 16, 17, 19, 24, 25, 26, 27, 28, 31, 32, 33, 34, 41, 42, 43, 45, 46, 48, 50, 52, 54, 55, 56, 57, 61, 62}

{1, 3, 9, 12, 13, 15, 19, 20, 23, 25, 29, 32, 33, 34, 36, 37, 39, 42, 44, 45, 47, 48, 52, 54, 55, 57, 59, 60, 64, 65}

{1, 4, 6, 8, 10, 14, 18, 21, 22, 23, 25, 28, 29, 31, 34, 35, 37, 40, 47, 48, 49, 52, 53, 54, 55, 63, 64}

Searching for SDSs $(v; k_1, k_2, k_3; \lambda)$

1998

2015 http://top500.org/

TIANHE-2	(MILKYWAY-2)
Site:	National Super Computer Center in Guangzhou
Cores:	3,120,000
Linpack Performance (Rmax)	33,862.7 TFlop/s
Theoretical Peak (Rpeak)	54,902.4 TFlop/s
Memory:	1,024,000 GB
Processor:	Intel Xeon E5-2692v2 12C 2.2GHz
Compiler:	icc

2007: open problem, 2^{50} ops $\rightsquigarrow$ 2015: ex. search in 10 minutes

The Epiphany

The sequences D of length v arising from Paley-Todd difference sets for v a prime $v \equiv 3 \pmod 4$ satisfy:

$$\mathrm{PAF}(D, i) = -1, \ i = 1, \ldots, v-1.$$

Therefore:

if for a prime $v \equiv 3 \pmod 4$ we can find SDSs $(v; k_1, k_2, k_3; \lambda)$, with $\lambda = k_1 + k_2 + k_3 - \dfrac{3v-1}{4}$

then the sequences A, B, C, D will satisfy

$$\mathrm{PAF}(A, i) + \mathrm{PAF}(B, i) + \mathrm{PAF}(C, i) + \mathrm{PAF}(D, i) = 0, \ i = 1, \ldots, v-1.$$

i.e. they are **complementary sequences** and can be used in the G-S array, to yield HMs of order $4 \cdot v$.

$\mathrm{SDS}(223; 111, 102, 123; 169), n = 167 \quad \rightsquigarrow \quad$ HM of order $4 \cdot 223$

3-way matching

INPUT

- a positive integer constant λ
- three text files A, B, C with k columns and n_A, n_B, n_C rows (resp.), containing positive integers

OUTPUT

- match
- three line numbers L_A, L_B, L_C in files A, B, C (resp.) s.t.

$$\begin{cases} L_A[1] + L_B[1] + L_C[1] = \lambda \\ \dots \\ L_A[k] + L_B[k] + L_C[k] = \lambda \end{cases}$$

EXAMPLE

$\lambda = 120$, $k = 3$, $n_A = n_B = n_C = 4$

file A	file B	file C
10 20 30	60 70 40	20 20 20
20 40 50	50 80 20	30 50 10
50 60 70	80 60 50	60 40 80
30 80 10	90 40 30	30 40 50

A match is given by $L_A = 2, L_B = 3, L_C = 1$

For problems of interest:

Typically, $\lambda < 1000$, elements < 100,

$k \in [40 - 50]$, sizes of n_A, n_B, n_C: Billions, size of A, B, C: Terabytes

Additional Property:

The line sums in files A, B, C are (all) constant.

$\rightsquigarrow$ geometric interpretations

Applications of 3-way matching:

- solution of extremely hard combinatorial problems, such as construction of D-optimal matrices, Hadamard matrices, weighing matrices etc.
- construction of cyclic $(v; k_1, k_2, k_3; \lambda)$ difference families with $v \equiv 3 \pmod 4$ a prime

Compression of complementary sequences

Definition:

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

PhD thesis of Yoseph Strassler, (1997), Bar Ilan University, Israel.

Example:

$$A = CW(24, 9) = [0, 0, 0, -1, -1, 0, 0, 0, 0, 0, 1, -1, 0, 0, 0, -1, 1, 0, 0, 1, 0, 0, -1, -1]$$

$$m = 2, \quad d = 12, \quad \rightsquigarrow \quad A^{(12)} = [0, 0, 0, -2, 0, 0, 0, 1, 0, 0, 0, -2]$$

$$m = 3, \quad d = 8, \quad \rightsquigarrow \quad A^{(8)} = [1, 0, 1, -1, -1, 0, -1, -2]$$

Theorem: Djokovic-Kotsireas (2012)

Let $\{A_i\}_{i=1,\ldots,t}$ be t complementary sequences, of length v each, with complex elements $A_i = [a_{i0}, a_{i1}, \ldots, a_{i,v-1}]$, for $i = 1, \ldots, t$ and $\sum_{i=1}^{t} PAF_{A_i} = [\alpha_0, \underbrace{\alpha, \ldots, \alpha}_{v-1 \text{ terms}}]$.

Assume that $v = dm$ and set $a_{ij}^{(d)} = a_{i,j} + a_{i,j+d} + \cdots + a_{i,j+(m-1)d}$ for $i = 1, \ldots, t$ and $j = 0, \ldots, d-1$.

Let $A_i^{(d)}$ be the t sequences $A_i^{(d)} = [a_{i0}^{(d)}, \ldots, a_{i,d-1}^{(d)}]$, for $i = 1, \ldots, t$.

Then the t sequences $\{A_i^{(d)}\}_{i=1,\ldots,t}$, of length d each, are also complementary and we have:

$$\sum_{i=1}^{t} PAF_{A_i^{(d)}} = [\alpha_0 + (m-1)\alpha, \underbrace{m\alpha, \ldots, m\alpha}_{d-1 \text{ terms}}] \tag{5}$$

$$\sum_{i=1}^{t} PSD_{A_i^{(d)}} = [\beta_0, \underbrace{\beta, \ldots, \beta}_{d-1 \text{ terms}}] \tag{6}$$

Optimization formalism

The search for complementary sequences can be formulated as an optimization problem, via the concept of the PAF.

There are optimization algorithms that deal with problems with $20K$ (discrete) variables.

We need **symmetric matrices** and certain vector/matrix products

$$\min_{x \in \{0,1\}^n} x^T A x$$

Let $a = [a_1, a_2, \ldots, a_n]^T$ be a column $n \times 1$ vector, where $a_1, a_2, \ldots, a_n \in \{-1, +1\}$ and consider the elements of the PAF vector $P_A(1), \ldots, P_A(m)$. Define the following $m = [n/2]$ symmetric matrices (which are independent of the sequence a)

$$M_i = (m_{jk}), \text{ s.t. } \begin{cases} m_{jk} = m_{kj} = \frac{1}{2}, & \text{when } a_j a_k \in P_A(i),\ j,k \in \{1,\ldots,n\} \\ 0, & \text{otherwise} \end{cases}, i = 1, \ldots, m$$

Lemma

The matrices M_i can be used to write the PAF equations in a matrix form:

- for n odd:

$$a^T M_i a = P_A(i), \;\; i = 1, \ldots, m.$$

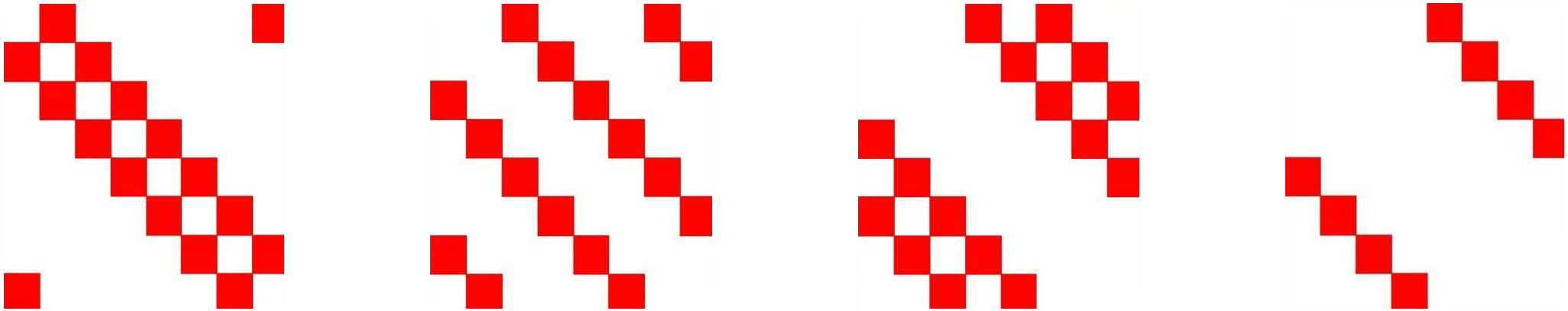
- for n even:

$$a^T M_i a = P_A(i), \;\; i = 1, \ldots, m-1 \text{ and } a^T M_m a = \frac{1}{2} P_A(m).$$

Example

Let $n = 8$, $a = [a_1, \ldots, a_8]$. Then we have that $m = 4$ and

$$a^T M_i a = P_A(i), \;\; i = 1, 2, 3 \text{ and } a^T M_4 a = \frac{1}{2} P_A(4)$$



Graphical representations of the four symmetric matrices M_1, M_2, M_3, M_4

Problem I Now suppose that we are looking for two $\{-1, +1\}$ sequences A and B of lengths n, such that

$$P_A(i) + P_B(i) = 2, \;\; i = 1, \ldots, m.$$

Via the previous lemma we can reformulate this problem as follows:

Problem II Find two binary sequences a, b, (viewed as $n \times 1$ column vectors) such that

$$a^T M_i a + b^T M_i b = 2, \;\; i = 1, \ldots, m.$$

Explicit DFT/PSD evaluations

The elements of the DFT/PSD vectors associated to a $\{-1,+1\}$-sequence are usually complex numbers with floating point real and imaginary parts.

However, for $n \equiv 0\,(mod\ 3)$

LEMMA

v odd integer, $v \equiv 0\,(mod\ 3)$, $m = \dfrac{v}{3}$, $[a_1,\ldots,a_v]$ $\{-1,+1\}$-sequence. Then we have the explicit evaluations:

$$DFT([a_1,\ldots,a_v],m) = \left(A_1 - \frac{1}{2}A_2 - \frac{1}{2}A_3\right) + \left(\frac{\sqrt{3}}{2}A_2 - \frac{\sqrt{3}}{2}A_3\right)i$$

$$PSD([a_1,\ldots,a_v],m) = A_1^2 + A_2^2 + A_3^2 - A_1A_2 - A_1A_3 - A_2A_3$$

where

$$A_1 = \sum_{i=0}^{m-1} a_{3i+1},\quad A_2 = \sum_{i=0}^{m-1} a_{3i+2},\quad A_3 = \sum_{i=0}^{m-1} a_{3i+3}.$$

COROLLARY $PSD([a_1,\ldots,a_n],m)$ is a non-negative integer.

Necklaces, Bracelets, Charm bracelets

One of the most natural groups acting on k-ary strings $a_0a_1 \cdots a_{n-1}$ of length n is the group of rotations.

The generator of this group acts on the indices by sending $i \to i+1 \pmod{n}$: $a_0a_1 \cdots a_{n-1} \rightsquigarrow a_1 \cdots a_{n-1}a_0$.

Applying this action partitions the set of k-ary strings into equivalence classes that are called necklaces.

When the action of reversal is composed with rotations, the resulting dihedral groups partition k-ary strings into equivalence classes called bracelets.

We refer only to the lexicographically smallest element in each respective equivalence class as a necklace or a bracelet.

Example: consider the bracelet equivalence class for the string 12003:

	12003	30021	
	20031	00213	$\leftarrow$ *bracelet (necklace)*
necklace $\rightarrow$	00312	02130	
	03120	21300	
	31200	13002	

Observe that this class contains two necklaces 00312 and 00213, the lexicographically smallest being the bracelet representative.

An efficient algorithm to list bracelets is given in:

`Joe Sawada. Generating bracelets in constant amortized time.`
`SIAM J. Comput., 31(1), 259-268, 2001.`

Our study of charm bracelets was motivated by the search for **periodic Golay pairs of length 68 and 72**.

Periodic Golay pairs of length 68

Consider the following two sequences of length 34 each, with $\{-2, 0, +2\}$ elements:

$$A^{(34)} = [0,0,0,2,0,0,-2,0,0,0,2,-2,0,0,-2,0,0,2,0,0,0,2,2,-2,0,0,-2,0,0,2,0,2,0,2]$$
$$B^{(34)} = [0,0,-2,2,0,2,0,-2,-2,0,2,2,0,2,-2,0,2,0,-2,2,0,2,2,0,2,0,2,2,0,-2,2,0,-2,-2]$$

These two sequences satisfy the following properties:

1. $\mathrm{PAF}(A^{(34)}, s) + \mathrm{PAF}(B^{(34)}, s) = 0, s = 0, 1, \ldots, 33;$
2. $\mathrm{PSD}(A^{(34)}, s) + \mathrm{PSD}(B^{(34)}, s) = 2 \cdot 68 = 136, \ s = 0, 1, \ldots, 33;$
3. $\mathrm{PSD}(A^{(34)}, 17) = 100$ and $\mathrm{PSD}(B^{(34)}, 17) = 36;$
4. $\sum_{i=1}^{34} A_i^{(34)} = 6$ and $\sum_{i=1}^{34} B_i^{(34)} = 10;$
5. The total number of 0 elements in $A^{(34)}$ and $B^{(34)}$ is equal to 34;
6. The total number of ± 2 elements in $A^{(34)}$ and $B^{(34)}$ is equal to 34;
7. $A^{(34)}$ contains 21 zeros and $B^{(34)}$ contains 13 zeros.

$A^{(34)}$ and $B^{(34)}$ are the 2-compressed sequences of two $\{-1,+1\}$ sequences of length 68 each, that form a particular **periodic Golay pair of length** 68:

$$A = \begin{array}{l} --+-+-+-+-++--+--++--+---+--+-+++ \\ ++-++--+-+-+--+-++++++-++-++++++-+ \end{array}$$

$$B = \begin{array}{l} ---+++---+++++--+-+-++++++++--+-- \\ ++-+-++--+-+-++--++++-+-++++-+-- \end{array}$$

$\rightsquigarrow$ Hadamard matrices of order $2 \cdot 68$

Djokovic, Dragomir; Kotsireas, Ilias; Recoskie, Daniel; Sawada, Joe
Charm bracelets and their application to the
construction of periodic Golay pairs.
Discrete Appl. Math. 188 (2015), 32-40.

Periodic Golay pairs of length 72

Using the same machinery, we also found **periodic Golay pairs of length** 72

Dragomir Djokovic and Ilias Kotsireas, Periodic Golay pairs of length 72 in:
Springer Proceedings in Mathematics & Statistics, Vol. 133
Algebraic Design Theory and Hadamard Matrices
ADTHM, Lethbridge, Alberta, Canada, July 2014
Colbourn, Charles J. (Ed.) 2015

Only known example of a length of a periodic Golay pair that is divisible by 3

SDS$(72; 36, 30; 30)$

10M lines of C code, meta-programming with Maple & bash shell

next open case: order 90

Power spectral density constancy over orbits

Let Z_v be the ring of integers $\mod v$, i.e $Z_v = \{0, 1, \ldots, v-1\}$. Let $Z_v^\star$ be the group of invertible elements of Z_v, i.e. $Z_v^\star = \{k \in Z_v : \gcd(k, v) = 1\}$.

The order of $Z_v^\star$ is equal to $\phi(v)$.

Let $H \leqslant Z_v^\star$ be a subgroup of $Z_v^\star$. Then H acts on Z_v and we denote the orbits of this action by

$$\mathcal{O}_1 = \{0\}, \mathcal{O}_2, \ldots \mathcal{O}_m.$$

Thus we have the disjoint union relationship $Z_v = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_m$.

Djokovic, Gysin, Seberry, 1991,1997,1998 constructed solutions for circulant type D-optimal matrices by expressing the corresponding SDSs as unions of certain orbits associated to a suitable subgroup of $Z_v^\star$.

The special structure of these solutions implies certain constraints on the possible range of values of the PSDs of the sequences associated to the SDS.

The power spectral densities remain constant over the orbits.

Let (X, Y) be an SDS of Z_v with parameters $(v; r, s; \lambda)$, with v odd and $\lambda = r + s - \frac{v-1}{2}$, corresponding to a circulant D-optimal matrix.

Assume that

$$X = \bigcup_{j \in J} \mathcal{O}_j, \quad Y = \bigcup_{k \in K} \mathcal{O}_k$$

for some subsets J, K of $\{1, 2, \ldots, m\}$.

By abuse of notation, let X also denote the sequence $x_0, x_1, \ldots, x_{v-1}$ where

$$x_i = \begin{cases} 1 & \text{if} \quad i \notin X \\ -1 & \text{if} \quad i \in X \end{cases}$$

and define similarly the sequence $Y = y_0, y_1, \ldots, y_{v-1}$.

THEOREM (Djokovic-Kotsireas 2012)

If k and k' belong to the same orbit $\mathcal{O}_r \subseteq Z_v$ and the sequence X is as defined above, then

$$PSD_X(k) = PSD_X(k').$$

New D-optimal matrix for $v = 241$ (order 482) Consider the subgroup

$H = \{1, 15, 24, 54, 87, 91, 94, 98, 100, 119, 160, 183, 205, 225, 231\}$ of order 15, of $Z^{\star}_{241}$.
Enumerate the 16 orbits. Find $SDS(241; 120, 105; 105)$

$$X = \bigcup_{j \in J} H \cdot j, \quad Y = \bigcup_{k \in K} H \cdot k$$

$$J = \{3, 4, 5, 6, 7, 10, 13, 38\}, \quad K = \{3, 5, 7, 11, 19, 35, 38\}$$

Acknowledgement: This work was made possible by the facilities of the Shared Hierarchical Academic Research Computing Network, SHARCNET, `www.sharcnet.ca` and Compute/Calcul Canada.

Interactions with Coding Theory

- **Gröbner Bases, Coding, and Cryptography**
  M. Sala, T. Mora, L. Perret, S. Sakata, C. Traverso (Editors)

  Open problem: Does there exists a binary linear $[72, 36, 16]$ code?
  The answer lies in being able to construct an ample supply of skew-Hadamard matrices of order 72.

- **Information security, coding theory and related combinatorics. Information coding and combinatorics**
  Dean Crnkovic and Vladimir Tonchev (Editors)
  NATO Science for Peace and Security Series D:
  Information and Communication Security, 29.
  IOS Press, Amsterdam, 2011.

Interactions with Quantum Computing

Weighing matrices are generalizations of Hadamard matrices.

$$W \cdot W^t = kI_n$$

- "Weighing matrices and optical quantum computing" S. Flammia and S. Severini, J. Phys. A: Math. Theor. 42 (2009) 065302
- "Quantum Algorithms for Weighing Matrices and Quadratic Residues" W. van Dam, Algorithmica 34, (2002) pp. 413428.

Future work

- achieve further progress on the algebraic front, especially exploiting symmetries
- explore the applicability of new HPC paradigms: FPGA, GPU etc
- improve and further optimize algorithms implementations
- intensify our study of connections with Coding Theory and Quantum Computing
- deepen our understanding of meta-heuristic methods, especially using landscape theory
- systematize the use of compression, both at the theoretical and practical levels