Title: Recent advances in the search for complementary sequences

Date: May 07, 2014 09:45 AM

URL: http://pirsa.org/14050040

Abstract: We will present recent developments in the search for complementary sequences namely new theoretical and algorithmic progress. SHARCNET resources are used quite heavily in this project.

Recent advances in the search for complementary sequences

Dragomir Z. Djokovic, Ilias S. Kotsireas

University of Waterloo, Wilfrid Laurier University
Waterloo ON, Canada

djokovic@uwaterloo.ca, ikotsire@wlu.ca

co-authors: Oleg Golubitsky, Daniel Recoskie, Joe Sawada

Outline of the talk

- Periodic and aperiodic autocorrelation of finite sequences
- Complementary sequences
- Compression of complementary sequences
- Unified description of combinatorial objects (Hadamard matrices, D-optimal matrices, weighing matrices)
- Alternative formulations (matrix, polynomial, algebraic, combinatorial optimization)
- New D-optimal matrices, new Hadamard and skew-Hadamard matrices

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 quaternionic $\{\pm 1, \pm i\}$ 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^{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

number/type of sequences	defining property	name
1 ternary	aper. autoc. 0	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
2...12 binary	per. autoc. zero	PCS

```
> 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]
 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:

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

Applications of low off-peak autocorrelation sequences

(1) communication engineering problems

- Schroeder M R, 1984, Number Theory in Science and Communication, Springer, Berlin.

(2) wireless telecommunications protocols

- S. Golomb, G. Gong, Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar Application, 2005, Cambridge University Press

(3) high-precision interplanetary radar measurements to check out space-time curvature

- Shapiro I I, Pettengill G H, Ash M E, Stone M L, Smith W B, Ingalls R P, Brockelman R A, 1968, Fourth test of general relativity, Phys. Rev. Lett. 20 1265-9

Searching for Complementary Sequences

Theorem:

Let $\{A_i\}_{i=1,\ldots,t}$ be t complementary sequences, of length v each, with complex elements. If

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

then

$$\sum_{i=1}^{t} PSD_{A_i} = [\beta_0, \underbrace{\beta, \ldots, \beta}_{v-1 \text{ terms}}] \tag{2}$$

and the following relationships hold:

$$\beta_0 = \alpha_0 + \alpha(v-1), \quad \beta = \alpha_0 - \alpha \tag{3}$$

$$\alpha_0 = (\beta_0 - \beta)\frac{1}{v} + \beta, \quad \alpha = \frac{\beta_0 - \beta}{v}. \tag{4}$$

Conversely, (2) implies (1).

Power Spectral Density, PSD

J. Seberry 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

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

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];

  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];
```

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

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

```
1, 87.005424454998786158779799479 8, 12.994575545001213841220200520 3, 100.000000000000000000000000000
2, 38.300910807301752211033593677 4, 61.699089192698247788966406322 4, 99.999999999999999999999999998
3, 44.633164960844338773349525822 5, 55.366835039155661226650474177 8, 100.000000000000000000000000000
4, 86.036673577623558750539151470 4, 13.963326422376441249460848529 6, 100.000000000000000000000000000
5, 90.249223594996214535365126037 0, 9.750776405003785464634873962 87, 99.999999999999999999999999999
6, 11.465561574321691567300081494 2, 88.534438425678308432699918505 7, 99.999999999999999999999999999
7, 59.717643834157526278178392429 3, 40.282356165842473721821607570 0, 99.999999999999999999999999993
8, 40.395342401612696341396934832 9, 59.604657598387303658603065166 9, 99.999999999999999999999999998
9, 44.299802891932235785134869638 4, 55.700197108067764214865130361 7, 100.000000000000000000000000000
10, 45.527864045000420607181652662 7, 54.472135954999579392818347337 3, 100.000000000000000000000000000
11, 56.452314801804562947805714130 4, 43.547685198195437052194285869 9, 100.000000000000000000000000000
12, 78.373686899517426122358058020 0, 21.626313100482573877641941979 8, 99.999999999999999999999999998
13, 40.952853792542013761762630652 3, 59.047146207457986238237369347 7, 100.000000000000000000000000000
14, 60.387741906400938164144285924 8, 39.612258093599061835855714074 3, 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
> 
```

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.

Example:

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

$$m = 2, \quad d = 12, \quad \rightsquigarrow \quad [0, 0, 0, -2, 0, 0, 0, 1, 0, 0, 0, -2]$$

$$m = 3, \quad d = 8, \quad \rightsquigarrow \quad [1, 0, 1, -1, -1, 0, -1, -2]$$

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:

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

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

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, $v \equiv 0\,(mod\ 3)$, $m = \frac{v}{3}$, $[a_1,\ldots,a_v]$ $\{-1,+1\}$-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.

Algorithms (deterministic, randomized, metaheuristic)

Classified in 4 main categories:

- Union of orbits approach
- String sorting
- Randomized string sorting
- Genetic Algorithms, Tabu Search, Simulated Annealing, Ant Colony Optimization

Make heavy use of theoretical results and practical optimizations to **prune** the (exponentially large) search spaces.

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.

Objective functions

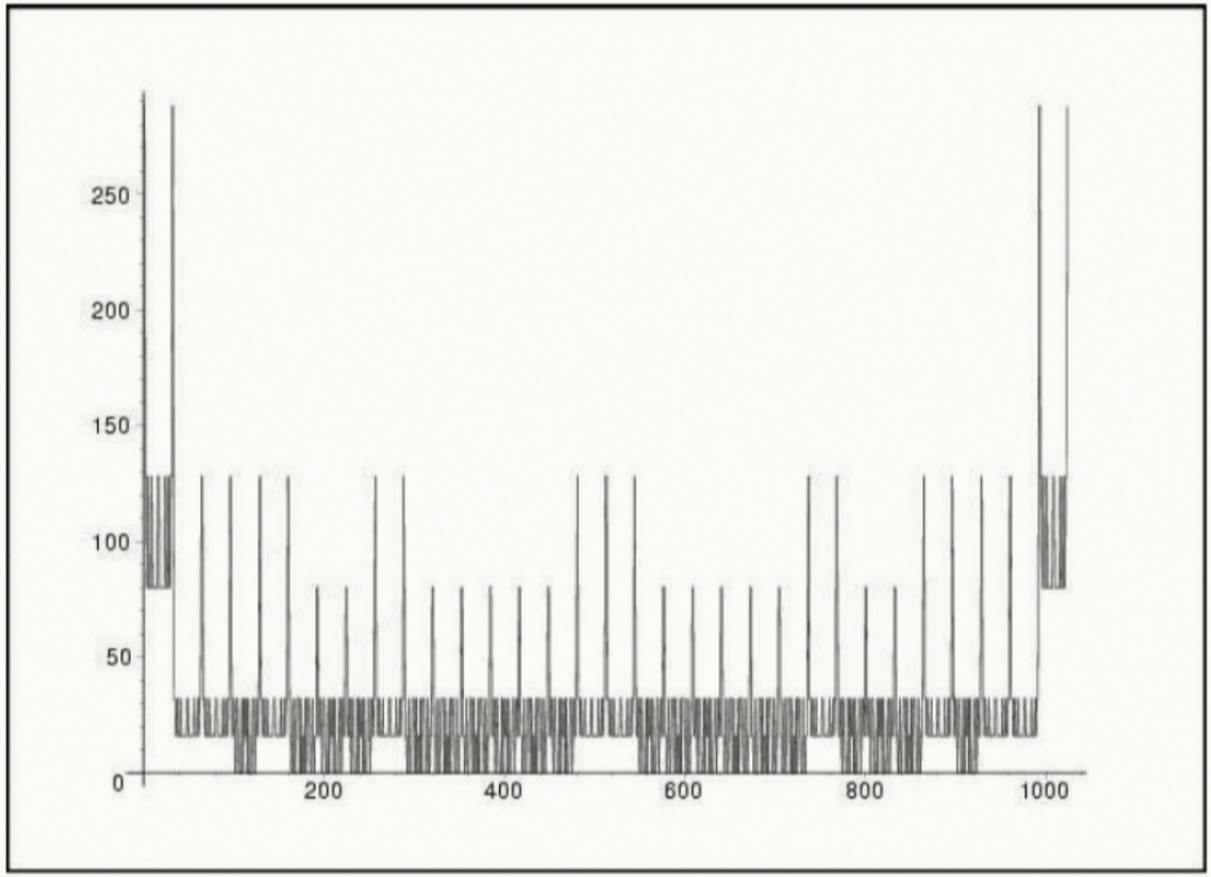
$$OF_1 = (P_A(1) + P_B(1) + c)^2 + \ldots + (P_A(m) + P_B(m) + c)^2$$

$$OF_2 = \mid P_A(1) + P_B(1) + c \mid + \ldots + \mid P_A(m) + P_B(m) + c \mid$$

All meta-heuristic techniques for complementary sequences suffer from the same disadvantage:

$\exists$ several trillions of local minima

Objective functions landscapes


250
200
150
100
50
0
200
400
600
800
1000

Interactions with Coding Theory

Gröbner Bases, Coding, and Cryptography
Edited by: M. Sala, T. Mora, L. Perret, S. Sakata, C. Traverso

Open problem: Does there exists a binary linear $[72, 36, 16]$ code?

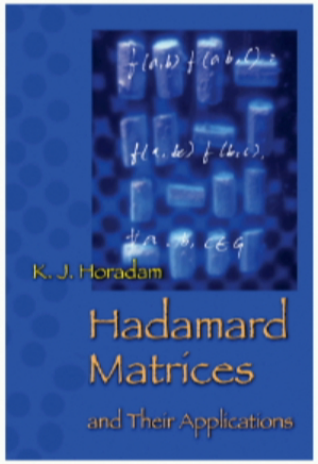
The answer lies in being able to construct skew-Hadamard matrices of order 32.

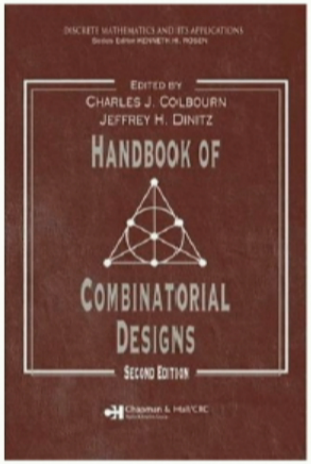
Interactions with Coding Theory

Gröbner Bases, Coding, and Cryptography
Edited by: M. Sala, T. Mora, L. Perret, S. Sakata, C. Traverso

Open problem: Does there exists a binary linear $[72, 36, 16]$ code?

The answer lies in being able to construct skew-Hadamard matrices of order 32.





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

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

Is this now the limit of what we can do? it may very well be, but certainly advances will not be made by people who think they cannot succeed.

– Carl Pomerance