Combinatorial Designs: constructions, algorithms and new results

Ilias S. Kotsireas

Wilfrid Laurier University

ikotsire@wlu.ca

Combinatorial Design Theory

Is it possible to arrange elements of a finite set into subsets so that certain properties are satisfied?

Existence and non-existence results. Infinite classes.

Tools & concepts from: linear algerbra, algebra, group theory, number theory, combinatorics, symbolic computation, numerical analysis.

Applications to: cryptography, optical communications, wireless communications, coding theory.

- W. D. Wallis, A. P. Street, J. Seberry, *Combinatorics: Room squares, sum-free sets, Hadamard matrices.* Springer-Verlag, 1972.
- A. V. Geramita, J. Seberry, *Orthogonal designs. Quadratic forms and Hadamard matrices.* Marcel Dekker Inc. 1979.
- C. J. Colbourn, J. H. Dinitz, *The CRC handbook of combinatorial designs.* CRC Press, 1996.
- V. D. Tonchev, *Combinatorial configurations: designs, codes, graphs.* Longman Scientific & Technical, John Wiley & Sons, Inc., 1988.
- T. Beth, D. Jungnickel, H. Lenz, *Design theory.* Vols. I, II. Second edition. Cambridge University Press, Cambridge, 1999.
- A. S. Hedayat, N. J. A. Sloane, J. Stufken *Orthogonal arrays. Theory and applications.* Springer-Verlag, 1999.
- D. R. Stinson, *Combinatorial designs, Constructions and analysis.* Springer-Verlag, 2004.
- C. J. Colbourn, J. H. Dinitz, *Handbook of Combinatorial Designs.* Second Edition, Chapman and Hall/CRC Press, 2006.
- K. J. Horadam, *Hadamard Matrices and Their Applications.* Princeton University Press, 2006.

Weighing Matrices

A **weighing matrix** $W = W(n,k)$ of weight k, is a square $n \times n$ matrix with entries $-1, 0, +1$ having k non-zero entries per row and column and inner product of distinct rows zero.

$$W \cdot W^t = k\, I_n$$

Fact:
If there is a $W(2n,k)$, n odd, then $k \leq 2n-1$ and k is the sum of two squares.

Theorem:
If there exist two circulant matrices A, B of order n each, satisfying $A \cdot A^t + B \cdot B^t = k\, I_n$, then there exists a $W(2n,k)$.

$$W(2n,k) = \begin{pmatrix} A & B \\ -B^t & A^t \end{pmatrix}$$

$W(2n, 2n-1)$ constructed from two circulants: infinite class

$W(2n, 2n-3)$ constructed from two circulants: do not exist

Ten Open Problems: [C. Koukouvinos, J. Seberry, JSPI (81), 1999]

Do there exist

$$W(2\cdot 23, 41),\ W(2\cdot 25, 45),\ W(2\cdot 27, 49),\ W(2\cdot 29, 53),\ W(2\cdot 33, 61),$$

$$W(2\cdot 35, 65),\ W(2\cdot 39, 73),\ W(2\cdot 43, 81),\ W(2\cdot 45, 85),\ W(2\cdot 47, 89)$$

constructed from two circulants?

Common feature: $W(2n, 2n-5)$, for $n = 23, \ldots, 47$.

Odd large weights.

R. Craigen, The structure of weighing matrices having large weights.

Des. Codes Cryptogr. (5) 1995

Plan of attack:

Establish potential patterns for the locations of the 5 zeros in solutions.

$$\text{From } 3^{2n} \sim 2^{3.17n} \text{ ops, down to } 2^{2n-5} \text{ ops.}$$

Idea:

Analyze the solutions sets for $W(2n, 2n-5)$ for all odd n up to $n = 15$.
(bash/Maple meta-program, C code generation, supercomputing)

First observation: (4 zeros)

$$\begin{array}{ccccc@{\qquad}ccccc} \star & \dots & \star & 0 & 0 & 0 & 0 & \star & \dots & \star \\ a_1 & \dots & a_{n-2} & a_{n-1} & a_n & b_1 & b_2 & b_3 & \dots & b_n \end{array}$$

Second observation: (the remaining fifth zero)

$$\underbrace{a_1 \star \ldots \star}_{\frac{n-3}{2}\text{ terms}} \quad 0 \quad \underbrace{\star \ldots \star a_{n-2}}_{\frac{n-3}{2}\text{ terms}} \quad 0 \quad 0 \quad 0 \quad 0 \quad \underbrace{b_3 \star \ldots \star b_n}_{n-2\text{ terms}}$$

$$\underbrace{a_1 \star \ldots \star a_{n-2}}_{n-2\text{ terms}} \quad 0 \quad 0 \quad 0 \quad 0 \quad \underbrace{b_3 \star \ldots \star}_{\frac{n-3}{2}\text{ terms}} \quad 0 \quad \underbrace{\star \ldots \star b_n}_{\frac{n-3}{2}\text{ terms}}$$

CRYSTALIZATION When we fix the 4 zeros as indicated above, then the fifth zero can only appear in exactly two possible places, in a $W(2n, 2n-5)$ solution.

A proof will probably use **Hall polynomials, PAF equations**

Implication: Infinite Class of $W(2n, 2n-5)$

Results:

```
W(2*23,41) solution
-1 -1 -1 -1 -1 1  1 -1 1 -1 0  1  1  1 -1 -1  1 -1 -1 1 -1 0  0
0  0 -1 -1  1 1 -1 -1 1  1 1 -1 -1 -1 -1 -1 -1  1 -1 1 -1 1 -1

W(2*25,45) solution
1 1  1  1 1 -1 -1 1 1 -1 1  0 1 -1  1 -1 -1 -1 -1 1 1  1  1 0 0
0 0 -1 -1 1 -1 -1 1 1  1 1 -1 1  1 -1  1 -1  1 -1 1 1 -1 -1 1 1

W(2*27,49) solution
1 1  1  1  1 1 -1 -1 -1 1 -1 -1  0 -1 -1 1  1 -1 -1  1 -1  1 -1 1 -1 0 0
0 0 -1 -1 -1 1  1 -1  1 1 -1 -1 -1 -1 1 1 -1 -1 -1 -1  1 -1 -1 1 -1 1 -1
```

$W(2 \cdot 29, 53)$ is still out of reach, as it still requires 2^{53} ops.

Periodic & non-periodic autocorrelation function

The 2nd elementary symmetric function in n variables $a_1, \ldots, a_n$

$$\sigma_2 = a_1 a_2 + \cdots a_{n-1} a_n = \sum_{1 \leq i < j \leq n} a_i a_j$$

plays a pivotal role in building $W(2n, k)$.

PAF and NPAF concepts

σ_2 is made up of $\displaystyle\sum_{i=1}^{n-1} n - i = \frac{n(n-1)}{2} = \binom{n}{2}$

(pairwise different) quadratic monomials:

$$
\left\{
\begin{array}{ccccc}
a_1a_2 & a_2a_3 & a_3a_4 & \vdots & a_{n-1}a_n \\
a_1a_3 & a_2a_4 & \vdots & \vdots & \bullet \\
\vdots & \vdots & a_3a_n & \vdots & \bullet \\
a_1a_{n-1} & a_2a_n & \bullet & \vdots & \bullet \\
a_1a_n & \bullet & \bullet & \vdots & \bullet \\
\underbrace{\hspace{2cm}}_{n-1 \text{ terms}} & \underbrace{\hspace{2cm}}_{n-2 \text{ terms}} & \underbrace{\hspace{2cm}}_{n-3 \text{ terms}} & \underbrace{\hspace{2cm}}_{n-i \text{ terms}} & \underbrace{\hspace{2cm}}_{1 \text{ term}}
\end{array}
\right.
$$

$$
\left\{
\begin{array}{ccccccc}
a_1a_2 & a_2a_3 & a_3a_4 & \vdots & a_{n-1}a_n & \leftarrow & N_A(1) \\
a_1a_3 & a_2a_4 & \vdots & \vdots & \bullet & \leftarrow & N_A(2) \\
\vdots & \vdots & a_3a_n & \vdots & \bullet & \leftarrow & N_A(3) \\
a_1a_{n-1} & a_2a_n & \bullet & \vdots & \bullet & \vdots & \vdots \\
a_1a_n & \bullet & \bullet & \vdots & \bullet & \leftarrow & N_A(n-1)
\end{array}
\right.
$$

Lemma:

$$N_A(1) + N_A(2) + \ldots + N_A(n-1) = \sigma_2$$

Fact:

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

Lemma:

$$P_A(1) + P_A(2) + \ldots + P_A(n-1) = 2\sigma_2$$

Fact:

$$NPAF = 0 \Longrightarrow PAF = 0$$

The converse is not always true.

Definition:

Two sequences $A = [a_1, \ldots, a_n]$ and $B = [b_1, \ldots, b_n]$ are said to have zero PAF (resp. NPAF) if

$$P_A(s) + P_B(s) = 0, \;\; i = 1, \ldots, n-1$$

$$\text{resp. } N_A(s) + N_B(s) = 0, \;\; i = 1, \ldots, n-1.$$

Weighing matrices come from sequences with zero PAF.

Fact:

If we can construct two sequences A and B with zero PAF, then we can construct $W(2 \cdot n, k)$ from two circulants.

Power Spectral Density, PSD

PSD Theorem

[Fletcher, Gysin, Seberry, Australas. J. Combin., 23, 2001]

Two sequences $[a_1, \ldots, a_n]$, $[b_1, \ldots, b_n]$ can be used to make up circulant matrices A and B that will give $W(2n, k)$ weighing matrices if and only if

$$PSD([a_1, \ldots, a_n], i) + PSD([b_1, \ldots, b_n], i) = k, \ \forall\ i = 0, \ldots, \frac{n-1}{2}$$

where $PSD([a_1, \ldots, a_n], k)$ 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.

The proof is based on the **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 $[b_1, \ldots, b_n]$.

The **PSD criterion** for $W(2n, k)$ states that:

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

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

Algorithm: String Sorting

Begin with

$$PSD([b_1,\dots,b_n],i) = k - PSD([a_1,\dots,a_n],i),\ \forall\ i=0,\dots,\frac{n-1}{2}$$

and take integer parts

$$[PSD([b_1,\dots,b_n],i)] = \begin{cases} k-1-[PSD([a_1,\dots,a_n],i)], & \text{is not an integer} \\ k-[PSD([a_1,\dots,a_n],i)], & \text{is an integer} \end{cases}$$

A pair of vectors $[a_1,\dots,a_n]$ and $[b_1,\dots,b_n]$ can be **encoded** as the concatenation of the integer parts of the first $\frac{n-1}{2}$ components of their PSD vectors:

$$[b_1,\dots,b_n] \longrightarrow [PSD([b_1,\dots,b_n],1)]\dots$$

$$[a_1,\dots,a_n] \longrightarrow k-1-[PSD([a_1,\dots,a_n],1)]\dots$$

Using the above encoding, the condition that a pair of sequences $[a_1, \ldots, a_n]$ and $[b_1, \ldots, b_n]$ can be used as the first rows of circulants to construct $W(2n, k)$ weighing matrices, can be simply phrased by saying that their corresponding string encodings are equal.

Therefore we see that the search for weighing matrices is essentially a string sorting problem.

A solution for $W(2 \cdot 29, 53)$ can now be found within a day, with serial programs.

However: A solution for $W(2 \cdot 33, 61)$ was still not found.

Is it possible that $[\mathbf{PSD}([\mathbf{a_1}, \ldots, \mathbf{a_n}], \mathbf{i})]$ can be an integer?

Rounding Error Treatment

LEMMA Let n be an odd integer such that $n \equiv 0\,(mod\ 3)$ and let $m = \frac{n}{3}$. Let $\omega = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ the principal n-th root of unity. Let $[a_1, \ldots, a_n]$ be a sequence with elements from $\{-1, 0, +1\}$. Then we have that $DFT([a_1, \ldots, a_n], m)$ can be evaluated explicitly in closed form and $PSD([a_1, \ldots, a_n], m)$ is a non-negative integer. The explicit evaluations are given by

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

$$PSD([a_1, \ldots, a_n], m) = A_1^2 + A_2^2 + A_3^2 - A_1 A_2 - A_1 A_3 - A_2 A_3$$

where

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

Sketch of proof: Acknowledgement: Doron Zeilberger

$DFT([a_1,\ldots,a_n],m)$ is a linear combination of $\omega^0,\omega^m,\omega^{2m}$

$$DFT([a_1,\ldots,a_n],m)=\sum_{i=0}^{n-1}a_{i+1}\,\omega^{im}=$$
$$=\left(\sum_{i=0}^{m-1}a_{3i+1}\right)\omega^0+\left(\sum_{i=0}^{m-1}a_{3i+2}\right)\omega^m+\left(\sum_{i=0}^{m-1}a_{3i+3}\right)\omega^{2m}$$
$$A_1\omega^0+A_2\omega^m+A_3\omega^{2m}.$$

$\omega^m=e^{\frac{2\pi i}{3}}$ and $\omega^{2m}=e^{\frac{4\pi i}{3}}$ are the roots of the cyclotomic polynomial $\Phi_3(x)=x^2+x+1$ and can be evaluated explicitly as:

$$\omega^m=-\frac{1}{2}+\frac{\sqrt{3}}{2}i,\;\;\omega^{2m}=-\frac{1}{2}-\frac{\sqrt{3}}{2}i.$$

Solutions for $W(2\cdot 33,61)$ were found. `http://www.cargo.wlu.ca/weighing/`

Lemma 11. *Let* $k = a^2 + b^2$, $k \leqslant 2n - 1$. *Then there exist* $W(2n, k)$ *constructed from two circulants except for*

1. $n = 23$, $k \in \{41, 45\}$;
2. $n = 25$, $k \in \{41, 45\}$;
3. $n = 27$, $k \in \{9, 18, 29, 36, 37, 41, 45, 49, 50\}$;
4. $n = 29$, $k \in \{9, 18, 29, 36, 37, 41, 45, 49, 50, 53\}$;
5. $n = 31$, $k \in \{9, 18, 29, 45, 49, 53, 58\}$;
6. $n = 33$, $k \in \{29, 37, 41, 49, 53, 58, 61, 65\}$;
7. $n = 35$, $k \in \{9, 18, 29, 37, 41, 45, 49, 53, 58, 61, 65, 68\}$;
8. $n = 39$, $k \in \{29, 41, 49, 53, 58, 61, 68, 71, 72\}$.

In addtion there exist $W(2n, k)$ *not constructed from two circulants for*

1. $n = 23$, $k \in \{45\}$;
2. $n = 27, 29, 31$, $k \in \{9, 18\}$;
3. $n = 31, 33, 35, 39$, $k \in \{29\}$.