J Comb Optim (2011) 22:873–881
DOI 10.1007/s10878-010-9335-5

A modified power spectral density test applied to weighing matrices with small weight

Ilias S. Kotsireas · Christos Koukouvinos · Panos M. Pardalos

Published online: 17 June 2010

Abstract The power spectral density test has been used for at least a decade in the search for many kinds of combinatorial matrices, such as weighing matrices for instance. In this paper we establish a modified power spectral density test that we apply to the search for weighing matrices of small weights constructed from two circulants. The main novelty of our approach is to define the Discrete Fourier Transform on the support of the first rows of the two circulants, thus exploiting the inherent sparsity of the problem. This new formalism turns out to be very efficient for small weights 9, 18, 36 and we find 10 new weighing matrices $W(2 \cdot p, 18)$ for prime $p \in \{37, 47, 53, 59, 61, 67, 73, 79, 83, 97\}$. These matrices are given here for the first time. We also discuss briefly a connection with Combinatorial Optimization.

Keywords Weighing matrices · Algorithm · Sparsity · Support

1 Introduction

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

I.S. Kotsireas is supported by an NSERC grant. P.M. Pardalos is supported by an Air Force grant.

I.S. Kotsireas
Department of Physics and Computer Science, Wilfrid Laurier University, 75 University Avenue West, Waterloo, Ontario N2L 3C5, Canada

C. Koukouvinos
Department of Mathematics, National Technical University of Athens, Zografou, 15773 Athens, Greece

P.M. Pardalos (✉)
Department of Industrial and Systems Engineering, University of Florida, Gainesville, FL, USA
e-mail: pardalos@ufl.edu

to zero. Therefore, W satisfies $WW^t = wI_n$. The number w is called the weight of W. Weighing matrices have been studied extensively, see (Koukouvinos and Seberry 1999) and references therein.

There are numerous applications of weighing matrices in Statistics, Coding Theory and elsewhere, see (Koukouvinos and Seberry 1997) for more details.

A well-known necessary condition for the existence of $W(2\cdot n, w)$ matrices states that if there exists a $W(2\cdot n, w)$ matrix with n odd, then $w < 2n$ and w is the sum of two squares, see (Koukouvinos and Seberry 1999). The two circulants construction for weighing matrices is described in the theorem below, taken from (Geramita and Seberry 1979).

Theorem 1 *If there exist two circulant matrices A, B of order n, with $0, \pm 1$ elements, satisfying $AA^t + BB^t = wI_n$, then there exists a $W(2\cdot n, w)$, given as*

$$W(2\cdot n, w) = \begin{pmatrix} A & B \\ -B^t & A^t \end{pmatrix} \quad or \quad W(2\cdot n, w) = \begin{pmatrix} A & BR \\ -BR & A \end{pmatrix}$$

where R is the square matrix of order n with $r_{ij} = 1$ if $i + j - 1 = n$ and 0 otherwise.

Definition 1 The periodic autocorrelation function, PAF, of a sequence $[a_1, \dots, a_n]$ of length n is defined as

$$PAF_A(i) = \sum_{k=1}^{n} a_k a_{k+i}, \quad i = 0, \dots, n-1,$$

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

It is well-known, see (Koukouvinos and Seberry 1999), that $W(2\cdot n, w)$ weighing matrices constructed from two circulants come from sequences with PAF equal to 0, i.e.

$$PAF_A(i) + PAF_B(i) = 0, \quad i = 1, \dots, n-1. \tag{1}$$

In this paper we use property (1) to search for such weighing matrices, typically with $w = 18$, even though our algorithm can be used efficiently with other small weights as well.

We now define some notations that we use in the rest of this paper to specify the first rows of two circulant matrices A and B that make up a weighing matrix $W(2\cdot n, w)$ constructed from two circulants, as per Theorem 1.

Definition 2 The following four sets are associated with a weighing matrix $W(2\cdot n, w)$ constructed from two circulants A, B:

$$posA = \text{the list of locations of } +1\text{'s in the first row of } A,$$
$$negA = \text{the list of locations of } -1\text{'s in the first row of } A,$$
$$posB = \text{the list of locations of } +1\text{'s in the first row of } B,$$
$$negB = \text{the list of locations of } -1\text{'s in the first row of } B.$$

We also denote by pA, nA, pB, nB the cardinalities of the sets *posA*, *negA*, *posB*, *negB* respectively.

Definition 3 The support of a weighing matrix $W(2 \cdot n, w)$ constructed from two circulants A, B is the multiset:

$$S_{W(2\cdot n,w)} = posA \cup negA \cup posB \cup negB.$$

Clearly, we have that $|S_{W(2\cdot n,w)}| = w$ and we denote the elements of the support (possibly with repetitions) by s_i:

$$S_{W(2\cdot n,w)} = \{s_1, \dots, s_w\}.$$

2 Two infinite classes of weighing matrices constructed from two circulants

We now describe some infinite classes of weighing matrices constructed from two circulants, given in (Koukouvinos and Seberry 1999).

Lemma 1 *If there exists a weighing matrix* $W(2 \cdot n, w)$ *constructed from two circulants, then there exist*:

- *a weighing matrix* $W(2 \cdot pn, w)$ *constructed from two circulants, for every integer* $p > 1$,
- *a weighing matrix* $W(2 \cdot pn, 2w)$ *constructed from two circulants, for every integer* $p > 1$.

Proof The proof of the first assertion in Lemma 1 is as follows: Let $\{x_1, \dots, x_n\}$ and $\{y_1, \dots, y_n\}$ be the two first rows of the circulants that make up a $W(2 \cdot n, w)$. Let 0_{p-1} denote the sequence of $p-1$ zero elements. Then the sequences $\{x_1, 0_{p-1}, x_2, 0_{p-1}, \dots, x_n, 0_{p-1}\}$ and $\{y_1, 0_{p-1}, y_2, 0_{p-1}, \dots, y_n, 0_{p-1}\}$ can be used as the first rows of circulants that make up a $W(2 \cdot pn, w)$, for every integer $p > 1$.

The proof of the second assertion is similar, see (Koukouvinos and Seberry 1999). □

Example 1 Consider a weighing matrix $W(2 \cdot 5, 9)$ given by the first rows of the two circulants as:

$$A = [-1, 1, 1, 1, 1], \qquad B = [1, 1, -1, 0, -1].$$

Then the sequences

$$C = [-1, 0_{p-1}, 1, 0_{p-1}, 1, 0_{p-1}, 1, 0_{p-1}, 1, 0_{p-1}],$$
$$D = [1, 0_{p-1}, 1, 0_{p-1}, -1, 0_{p-1}, 0, 0_{p-1}, -1, 0_{p-1}]$$

can be used as the first rows of circulants that make up a $W(10 \cdot p, 9)$, for every integer $p > 1$.

In terms of the supports we have:

$$
\begin{aligned}
&posA := [2, 3, 4, 5],\\
&negA := [1],\\
&posB := [1, 2],\\
&negB := [3, 5],\\
&S_{W(2\cdot 5,9)} := \{1, 1, 2, 2, 3, 3, 4, 5, 5\},
\end{aligned}
$$

$$
\begin{aligned}
&posC := [p + 1, 2p + 1, 3p + 1, 4p + 1],\\
&negC := [1],\\
&posD := [1, p + 1],\\
&negD := [2p + 1, 4p + 1],\\
&S_{W(10\cdot p,9)} := \{1, 1, p + 1, p + 1, 2p + 1, 2p + 1, 3p + 1, 4p + 1, 4p + 1\}.
\end{aligned}
$$

Coming back to the proof of the first assertion in Lemma 1, we see that in general the supports of $W(2 \cdot n, w)$ and $W(2 \cdot pn, w)$ are related by:

$$
\begin{aligned}
&S_{W(2\cdot n,w)} = \{s_1, \dots, s_w\}, \qquad S_{W(2\cdot pn,w)} = \{t_1, \dots, t_w\},\\
&t_i = (s_i - 1)p + 1, \text{ for } i = 1, \dots, w.
\end{aligned}
\tag{2}
$$

Remark 1 Another interpretation of the infinite class presented in Lemma 1 is that one blows up the support of a $W(2\cdot n, w)$ into the support of a $W(2\cdot pn, w)$, for every integer $p > 1$, exclusively using numbers that are $\equiv 1 \pmod p$ and more precisely as specified in (2).

3 Description of the algorithm

The Discrete Fourier Transform (DFT) and the Power Spectral Density (PSD) criterion have been traditionally used to devise algorithms to search for weighing matrices and other similar combinatorial matrices. The main computational advantage of these two concepts lies in the fact that they are used to decouple equations (1), so that the algorithm operates on the candidate sequences for the first rows of the circulant matrices A and B separately. Typically, sequences that have a value of an element of the PSD vector $> w$, can safely be discarded from the search.

The main computational overhead of DFT/PSD-based algorithms to search for weighing matrices constructed from two circulants is the computation of the DFT and the PSD of candidate sequences. Even though the DFT/PSD computation is performed incrementally, it is still a highly laborious computation, especially for large values of n and small values of the weight. In this case, the sequences A and B, i.e. the first rows of the two circulants, exhibit significant sparsity and so it would be desirable to formulate the concepts of DFT/PSD not on the entire sequences, but on the support of the two sequences, as per Definition 3. This would result in a drastic reduction of the number of operations it takes to compute the DFT.

3.1 A motivating example: weight 9

We present a generic motivating example, based on weighing matrices $W(2\cdot n, 9)$ of weight 9, constructed from two circulants. Let

$$\omega = \cos\left(\frac{2\pi}{n}\right) + I\sin\left(\frac{2\pi}{n}\right).$$

It can easily be seen (using the definition of the DFT) that the exponents of the powers of ω in $DFT_A(1), DFT_B(1)$ are specified by the locations of elements in the support, i.e. we have:

$$DFT_A(1) = \sum_{i=1}^{pA} \omega^{(posA[i]-1)} - \sum_{i=1}^{nA} \omega^{(negA[i]-1)}, \tag{3}$$

$$DFT_B(1) = \sum_{i=1}^{pB} \omega^{(posB[i]-1)} - \sum_{i=1}^{nB} \omega^{(negB[i]-1)}. \tag{4}$$

Further, suppose that there exists a positive integer m, which is a (the smallest) common solution $(\bmod n)$ of the following system of w linear congruences (build on the support):

$$x_1(s_1 - 1) \equiv 0 \ (\bmod n),$$
$$\vdots$$
$$x_w(s_w - 1) \equiv 0 \ (\bmod n).$$

Note that there may actually be less than w different congruences, in case there are repeated elements in the support.

Also note that if $1 \in S_{W(2\cdot n,w)}$ then the corresponding congruence can be omitted from the system, since it is trivially satisfied.

Further, when the value of m is known, it is easy to see that

$$DFT_A(m) = |posA| - |negA|,$$
$$DFT_B(m) = |posB| - |negB|$$

and therefore

$$PSD(A,m) + PSD(B,m) = (|posA| - |negA|)^2 + (|posB| - |negB|)^2 = w$$

as one would expect.

Moreover, for every integer multiple of m, i.e. km with $k > 1$, which is smaller than n we will also have

$$DFT_A(km) = |posA| - |negA|,$$
$$DFT_B(km) = |posB| - |negB|,$$
$$PSD(A,km) + PSD(B,km) = w$$

which implies that the existence of m establishes a certain periodicity w.r.t. the values of the DFT vector. More specifically, it suffices to compute the first $m-1$ values of the DFT vectors

$$DFT_A(1),\dots,DFT_A(m-1) \quad \text{and} \quad DFT_B(1),\dots,DFT_B(m-1),$$

since the remaining values will be repeated, with period m.

Example 2 We illustrate with a specific example of a $W(2\cdot 350, 9)$ taken from (Kotsireas et al. 2010a).

$$\begin{aligned}
&n := 350,\\
&w := 9,\\
&posA := [15, 99, 169, 197],\\
&negA := [1],\\
&posB := [1, 15],\\
&negB := [43, 85],\\
&S_{W(2\cdot 350,9)} := \{1, 1, 15, 15, 43, 85, 99, 169, 197\},\\
&\omega = \cos\left(\frac{2\pi}{350}\right) + I\sin\left(\frac{2\pi}{350}\right),\\
&DFT_A(1) = \omega^{196} + \omega^{168} + \omega^{98} + \omega^{14} - 1,\\
&DFT_B(1) = -\omega^{84} - \omega^{42} + \omega^{14} + 1.
\end{aligned}$$

It turns out that the smallest common solution of the system of 6 linear congruences build on the support $S_{W(2\cdot 350,9)}$

$$\begin{aligned}
14x_1 &\equiv 0 \pmod{350},\\
42x_2 &\equiv 0 \pmod{350},\\
84x_3 &\equiv 0 \pmod{350},\\
98x_4 &\equiv 0 \pmod{350},\\
168x_5 &\equiv 0 \pmod{350},\\
196x_6 &\equiv 0 \pmod{350},
\end{aligned}$$

is $m = 25$, which implies that

$$\begin{aligned}
DFT_A(25) &= |posA| - |negA| = 4 - 1 = 3,\\
DFT_B(25) &= |posB| - |negB| = 2 - 2 = 0
\end{aligned}$$

and therefore

$$PSD(A,25) + PSD(B,25) = 3^2 + 0^2 = 9.$$

We also have that

$$DFT_A(25) = DFT_A(50) = DFT_A(75) = DFT_A(100) = \cdots = DFT_A(350) = 3,$$
$$DFT_B(25) = DFT_B(50) = DFT_B(75) = DFT_B(100) = \cdots = DFT_B(350) = 0.$$

3.2 Algorithm

We describe the algorithm that incorporates the idea of defining the DFT on the support of the first rows of the two circulants that make up the weighing matrix $W(2 \cdot n, w)$ as per Theorem 1. In this context, a structural pattern (k_1, k_2) is a statement of the form: there are k_1 non-zero elements in the first row of A and k_2 non-zero elements in the first row of B. Clearly, we must have $k_1 + k_2 = w$.

This is a DFT/PSD & string sorting type of algorithm, see (Kotsireas et al. 2009, 2010a).

INPUT: integers n (order) and w (weight), such that the Diophantine equation $x^2 + y^2 = w$ is solvable

OUTPUT: two $\{0, \pm 1\}$ sequences $a = [a_1, \dots, a_n]$ and $b = [b_1, \dots, b_n]$ of length n each, described by their supports, that can be used as the first rows of circulant matrices to construct a weighing matrix $W(2 \cdot n, w)$.

(1) Choose a structural pattern (k_1, k_2) for the distribution of the w non-zero elements in the two sequences $[a_1, \dots, a_n]$ and $[b_1, \dots, b_n]$. If w is even, then a frequently used structural pattern is $(\frac{w}{2}, \frac{w}{2})$. If w is odd, then a frequently used structural pattern is $(\frac{w-1}{2}, \frac{w+1}{2})$.

(2) Generate the $\binom{n}{k_1}$ possible supports for $posA \cup negA$ (that pass the PSD test) and their corresponding (see Kotsireas et al. 2009 for details) string encodings, using the generalizations of formula (3):

$$DFT_A(j) = \sum_{i=1}^{pA} \omega^{(posA[i]-1)j \bmod n} - \sum_{i=1}^{nA} \omega^{(negA[i]-1)j \bmod n}, \quad j = 1, \dots, n-1. \tag{5}$$

(3) Generate the $\binom{n}{k_2}$ possible supports for $posB \cup negB$ (that pass the PSD test) and their corresponding (see Kotsireas et al. 2009 for details) string encodings, using the generalizations of formula (4):

$$DFT_B(j) = \sum_{i=1}^{pB} \omega^{(posB[i]-1)j \bmod n} - \sum_{i=1}^{nB} \omega^{(negB[i]-1)j \bmod n}, \quad j = 1, \dots, n-1. \tag{6}$$

(4) If any common strings (see Kotsireas et al. 2010a for details) are detected, then return the corresponding support $S_{W(2 \cdot n, w)} = posA \cup negA \cup posB \cup negB$.

3.3 Practical considerations

Steps (2) and (3) of the algorithm can be prohibitively computationally expensive when n is large. We take this opportunity to elaborate somewhat on some practical considerations regarding our algorithm. What happens in practice is that only about

1% of the entire space of combinations needs to be generated before a pair of matching strings can be found. More specifically, steps (2) and (3) are independent and are executed in parallel. Also, the combinatorial generation proceeds incrementally and for each generated combination the corresponding string encoding is generated immediately. In addition, step (4) is also independent of steps (2) and (3) and can be executed periodically on the result files produced by steps (2) and (3). When a pair of matching strings is found, the computationally expensive combinatorial generation and string encoding generation of steps (2) and (3) is stopped.

Another important point to emphasize is that this algorithm works well for small weights, e.g. $w = 9$, 18 for instance. The reason is that the idea of defining the DFT on the support of the two sequences, carries an actual computational benefit only when there are lots of zero elements in the two sequences, i.e. only when the weight is small.

4 New results

In this section we mention a few results that we obtained using the ideas and the algorithm in the previous sections. In particular we were able to compute 10 new weighing matrices

$$W(2\cdot p, 18) \quad \text{for prime } p \in \{37, 47, 53, 59, 61, 67, 73, 79, 83, 97\}$$

which are (computationally) way beyond the reach of almost any currently known algorithm:

	posA	*negA*	*posB*	*negB*
$W(2\cdot 37, 18)$	[19, 24, 28, 29, 30, 37]	[18, 21, 33]	[18, 24, 27, 31, 32, 34]	[19, 25, 37]
$W(2\cdot 47, 18)$	[21, 22, 28, 32, 34, 44]	[20, 38, 41]	[20, 22, 33, 34, 39, 42]	[21, 44, 45]
$W(2\cdot 53, 18)$	[26, 35, 36, 40, 51, 53]	[25, 34, 44]	[29, 30, 34, 37, 38, 41]	[25, 27, 33]
$W(2\cdot 59, 18)$	[24, 25, 43, 45, 51, 58]	[27, 30, 32]	[25, 28, 39, 41, 56, 57]	[24, 55, 59]
$W(2\cdot 61, 18)$	[24, 25, 34, 40, 45, 47]	[38, 46, 50]	[24, 25, 36, 37, 46, 60]	[45, 47, 48]
$W(2\cdot 67, 18)$	[24, 25, 28, 38, 47, 53]	[34, 46, 67]	[25, 43, 45, 46, 51, 65]	[24, 31, 48]
$W(2\cdot 73, 18)$	[25, 47, 48, 49, 52, 73]	[24, 27, 43]	[25, 31, 40, 43, 63, 70]	[24, 28, 66]
$W(2\cdot 79, 18)$	[24, 36, 38, 43, 46, 52]	[26, 30, 57]	[26, 36, 38, 49, 55, 75]	[24, 45, 78]
$W(2\cdot 83, 18)$	[23, 24, 26, 44, 51, 56]	[31, 69, 77]	[24, 38, 39, 51, 64, 79]	[23, 36, 52]
$W(2\cdot 97, 18)$	[23, 47, 56, 60, 73, 90]	[26, 36, 64]	[26, 37, 45, 48, 51, 53]	[23, 43, 64]

Note that using Lemma 1 and our results, we obtain the following 20 infinite classes:

Proposition 1 *For every integer $N > 1$ and every prime $p \in \{37, 47, 53, 59, 61, 67, 73, 79, 83, 97\}$,*

- *There exists a weighing matrix $W(2\cdot Np, 18)$ constructed from two circulants,*
- *There exists a weighing matrix $W(2\cdot Np, 36)$ constructed from two circulants.*

5 The connection with Combinatorial Optimization

The problem of searching for weighing matrices constructed from two circulant submatrices can be phrased as a Combinatorial Optimization problem on ternary variables. We note that in (Kotsireas et al. 2010b) we gave a Combinatorial Optimization formalism for the periodic complementary binary sequences problem and used it to solve all remaining open cases regarding periodic complementary binary sequences in the Bömer and Antweiler diagram. We now describe how our formalism from (Kotsireas et al. 2010b) readily extends to the case of weighing matrices constructed from two circulant submatrices. Let $m = [\frac{n}{2}]$, where $[x]$ denotes the integer part of x.

Problem 1 Suppose that we are looking for two $\{-1, 0, +1\}$ sequences A and B of lengths n, such that

$$PAF_A(i) + PAF_B(i) = 0, \quad i = 1, \ldots, m.$$

Using Lemma 2 of (Kotsireas et al. 2010b) we can reformulate this problem as follows:

Problem 2 Find two ternary sequences a, b, (viewed as $n \times 1$ column vectors) such that

$$a^T M_i a + b^T M_i b = 0, \quad i = 1, \ldots, m.$$

where $a = [a_1, \ldots, a_n]$ and $b = [b_1, \ldots, b_n]$ and $a_i, b_i \in \{-1, 0, +1\}$.

The matrices $M_1, \ldots, M_m$ are symmetric and are defined in (Kotsireas et al. 2010b). They basically correspond to the matrices associated to the periodic autocorrelation function elements viewed as quadratic forms.

Evidently, Problem 1 is simply property (1) and its equivalent reformulation as Problem 2 allows one to employ Combinatorial Optimization methods to solve it.

Acknowledgements We wish to thank the Editor and the Referees for their constructive comments and suggestions that led to an improved presentation of this paper.

References

Geramita AV, Seberry J (1979) Orthogonal designs. Quadratic forms and Hadamard matrices. Lecture notes in pure and applied mathematics, vol 45. Marcel Dekker, New York

Kotsireas IS, Koukouvinos C, Seberry J (2009) Weighing matrices and string sorting. Ann Comb 13(3):305–313

Kotsireas IS, Koukouvinos C, Pardalos PM (2010a) An efficient string sorting algorithm for weighing matrices of small weight. Optim Lett 4:29–36

Kotsireas IS, Koukouvinos C, Pardalos PM, Shylo OV (2010b) Periodic complementary binary sequences and combinatorial optimization algorithms. J Comb Optim (to appear)

Koukouvinos C, Seberry J (1997) Weighing matrices and their applications. J Stat Plan Inference 62:91–101

Koukouvinos C, Seberry J (1999) New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function-a review. J Stat Plan Inference 81(1):153–182