New weighing matrices of order $2n$ and weight $2n - 9$

Ilias S. Kotsireas
Department of Phys. and Comp. Sci.
Wilfrid Laurier University
Waterloo ON, N2L 3C5, Canada

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

Jennifer Seberry
Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong, NSW 2522, Australia

Abstract

In this paper we find six new weighing matrices of order $2n$ and weight $2n-9$ constructed from two circulants, by establishing various patterns on the locations of the nine zeros in a potential solution.

Keywords: Weighing matrices, algorithm, patterns, locations of zeros.

MSC classification: 05B20, 62K05.

1 Introduction

A weighing matrix $W = W(n, k)$ is a square matrix with entries $0, \pm 1$ having k non-zero entries per row and column and inner product of distinct rows equal to zero. Therefore W satisfies $WW^t = kI_n$. The number k is called the weight of W. Weighing matrices have been studied extensively, see [8] and references therein. Weighing matrices are important in Coding Theory, for instance they can be used [1] to construct self-dual codes.

A well-known necessary condition for the existence of $W(2n,k)$ matrices states that if there exists a $W(2n,k)$ matrix with n odd, then $k < 2n$ and k is the sum of two squares. In this paper we are focusing on $W(2n,k)$ constructed from two circulants. The two circulants construction for weighing matrices is described in the theorem below, taken from [6].

Theorem 1 *If there exist two circulant matrices A_1, A_2 of order n, with $0, \pm 1$ elements, satisfying $A_1 A_1^t + A_2 A_2^t = f I_n$ and f is an integer, then there exists a $W(2n, f)$, given as*

$$W(2n,f) = \begin{pmatrix} A_1 & A_2 \\ -A_2^t & A_1^t \end{pmatrix} \quad or \quad W(2n,f) = \begin{pmatrix} A_1 & A_2 R \\ -A_2 R & A_1 \end{pmatrix}$$

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

A number of conjectures on weighing matrices, as well as a comprehensive list of open cases for $W(2n,k)$ constructed from two circulants, are contained in [8]. Here we focus on $W(2n, 2n-9)$ i.e. weighing matrices of weight $2n-9$, constructed from two circulants. Results on the structure of weighing matrices $W(n, n-2)$, $W(n, n-3)$, $W(n, n-4)$ (not necessarily constructed from two circulants) are given in [3].

2 Patterns for the location of the nine zeros

In [7] the authors constructed new weighing matrices of order $2n$ and weight $2n-5$ constructed from two circulants, by establishing the following pattern for the locations of the five zeros

$$\underbrace{a_1 \star \dots \star}_{\frac{n-3}{2}\text{ terms}} \quad 0 \quad \underbrace{\star \dots \star a_{n-2}}_{\frac{n-3}{2}\text{ terms}} \quad 0 \quad 0 \quad 0 \quad 0 \quad \underbrace{b_3 \star \dots \star b_n}_{n-2\text{ terms}} \tag{1}$$

where the asterisk symbol $\star$ denotes a binary $\{-1, +1\}$ variable.
Keeping the order fixed to $2n$ but decreasing the weight and using an analogous pattern to see whether we will still obtain solutions, leads us to consider weighing matrices of order $2n$ and weight $2n-9$ constructed from two circulants. For n odd, $2n - 9 \equiv 1 \pmod 4$.
We note here that for n odd, the weights $2n - 7$ and $2n - 11$ are excluded from similar considerations, due to the diophantine constraints $a^2 + b^2 = 2n-7$ and $a^2+b^2 = 2n-11$. A number is a sum of two squares if and only if all its prime factors of the form $3 \pmod 4$ appear with an even exponent in

the prime factorization of the number. Therefore, a number is not a sum of two squares if and only if there exists a prime factor of the form $3 \pmod 4$ appearing with an odd exponent in the prime factorization of the number. Now, we have that $2n - 7 \equiv 3 \pmod 4$ and $2n - 11 \equiv 3 \pmod 4$ when n is odd, which means that there exist a $3 \pmod 4$ prime factor of $2n - 7$ and $2n - 11$ that will occur with an odd exponent, in the prime factorizations of $2n - 7$ and $2n - 11$ (if all prime factors of the form $3 \pmod 4$ appeared with an even exponent, then $2n - 7$ and $2n - 11$ would be $\equiv 1 \pmod 4$). Therefore the diophantine equations $a^2 + b^2 = 2n - 7$ and $a^2 + b^2 = 2n - 11$ do not have solutions for odd n.
We wrote a bash shell script metaprogram to generate via the Maple `CodeGeneration` package the C programs to perform exhaustive searches for $W(2n, 2n-9)$ constructed from two circulants whose first rows are given by $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ and that follow the patterns

$$\underbrace{a_1 * \ldots *}_{\frac{n-5}{2}\text{ terms}} \quad 0 \quad \underbrace{* \ldots * a_{n-4}}_{\frac{n-5}{2}\text{ terms}} \quad 0 \quad 0 \quad 0 \quad 0 \;\mid\; 0 \quad 0 \quad 0 \quad 0 \quad \underbrace{b_5 * \ldots * b_n}_{n-4\text{ terms}} \qquad \text{1-4-4} \tag{2}$$

and

$$\underbrace{a_1 * \ldots * a_{n-5}}_{n-5\text{ terms}} \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \;\mid\; 0 \quad 0 \quad * \quad 0 \quad 0 \quad \underbrace{b_6 * \ldots * b_n}_{n-5\text{ terms}} \qquad \text{5-2-2} \tag{3}$$

where the vertical bar symbol | separates the a's from the b's.

Using these patterns, we transform the problem of looking for a weighing matrix $W(2n, 2n - 9)$ constructed from two circulants, from a problem in $2n$ triadic variables into a problem in $2n - 9$ binary variables. The computational gain is expressed by the ratio $\frac{3^{2n}}{2^{2n-9}}$ which is equal to $512(2.25)^n$. This allows us to tackle previously computationally intractable values of n, see [3, 8].

3 Results

We used the power spectral density criterion [5], to search for $W(2n, 2n-9)$ weighing matrices for $n = 25, 27, 29, 31, 35, 37, 41$, in conjunction with the patterns 1-4-4 and 5-2-2. We found a number of $W(2n, 2n - 9)$ weighing matrices, which are given here for the first time. Lists of known and unknown weighing matrices can be found in [2, 3, 4, 8]. A permissible value of n is a value such that the Diophantine equation $a^2 + b^2 = 2n - 9$ has solutions. In the next table, we summarize the results of the searches, omitting the non-permissible values of n. The prototype C programs have been generated at the CARGO Lab of Wilfrid Laurier University and the computations have been performed remotely at SHARCnet high-performance computing clusters. All the results described in the next table are given on the on-line appendix of the paper http://www.cargo.wlu.ca/weighing/

$W(2n, 2n-9)$	pattern 1-4-4	pattern 5-2-2
$W(2\cdot 7, 5)$	8	8
$W(2\cdot 9, 9)$	0	0
$W(2\cdot 11, 13)$	0	16
$W(2\cdot 13, 17)$	32	16
$W(2\cdot 17, 25)$	64	32
$W(2\cdot 19, 29)$	112	32
$W(2\cdot 23, 37)$	48	32
$W(2\cdot 25, 41)$	80	48
$W(2\cdot 27, 45)$	0	0
$W(2\cdot 29, 49)$	0	16
$W(2\cdot 31, 53)$	20	8
$W(2\cdot 35, 61)$	32	44
$W(2\cdot 37, 65)$	2	0
$W(2\cdot 41, 73)$	2	0

We now give the first rows for some $W(2n, 2n-9)$ weighing matrices constructed from two circulants, for $n = 25, 29, 31, 35, 37, 41$, in the format $a_1, \ldots, a_n, b_1, \ldots, b_n$.

```
W(2*25,41) solution with pattern 1-4-4

- - - - - + + - + + 0 - + - + - + + - - - 0 0 0 0
0 0 0 0 - + - + + - + + - - - + + + - + + + + + -

W(2*25,41) solution with pattern 5-2-2

- - - - + + - - - + - - + - - + - + + + 0 0 0 0 0
0 0 - 0 0 - - - - + - + + - - - + - + - + + + - -

W(2*29,49) solution with pattern 5-2-2

- - - - - + + - - + + - + - + + - + - - + + + + 0 0 0 0 0
0 0 - 0 0 + - - + + + - + - + + + + + + - - + - + + + - +

W(2*31,53) solution with pattern 1-4-4

- - - + - + - - + - + + - 0 + - - + + + - + + + - - - 0 0 0 0
0 0 0 0 - - - - + - + - - - + - - + + - - - - - + - + + + + -

W(2*35,61) solution with pattern 1-4-4

+ - + - - - - + + + - + + - - 0 - + - - + + + + + + + + + - + 0 0 0 0
0 0 0 0 - + + - - + + - + + - + - + + + - + - + - - + + + + - - - + +

W(2*37,65) solution with pattern 1-4-4

+ + + + - - + - + - - + - - + + 0 - - - + + + + + + - + - - - + + 0 0 0 0
0 0 0 0 - - + - - - + + + + - + + - + - + + + - + + + - + + - + + + - + -
```

```
W(2*41,73) solution with pattern 1-4-4

+ + + + + + + - - + + + - - + - - + 0 + + + - + - - + + - - - + + - + - + 0 0 0 0
0 0 0 0 - + + + + - + - + + + + + - + - - - + - - + + - + + + - - - - + - + - - +
```

We give a summary of the results for weighing matrices $W(2n, 2n-9)$ constructed from two circulants in the following table, omitting the non-permissible values of n.

n	$2n$	2n-9	Reference for W(2n,2n-9)
7	14	5	[8], solutions with patterns (2) and (3)
9	18	9	[8], no solutions with patterns (2), (3)
11	22	13	[8], no solutions with pattern (2), solutions with pattern (3)
13	26	17	[8], solutions with patterns (2) and (3)
17	34	25	[8], solutions with patterns (2) and (3)
19	38	29	[8], solutions with patterns (2) and (3)
23	46	37	[8], solutions with patterns (2) and (3)
25	50	41	New, solutions with patterns (2) and (3)
27	54	45	Undecided
29	58	49	New, solutions with pattern (3)
31	62	53	New, solutions with pattern (2)
35	70	61	New, solutions with pattern (2)
37	74	65	New, solutions with pattern (2)
41	82	73	New, solutions with pattern (2)
45	90	81	Undecided

References

[1] K. T. Arasu and T. A. Gulliver, Self-dual codes over $\mathbb{F}_p$ and weighing matrices, *IEEE Trans. Inform. Theory*, 47, 2001, No 5, pp. 2051-2055.

[2] R. Craigen, Weighing matrices and conference matrices, in The CRC Handbook of Combinatorial Designs, (Eds. C. J. Colbourn and J. H. Dinitz), CRC Press, Boca Raton, Fla., 1996, pp. 496-504.

[3] R. Craigen, The structure of weighing matrices having large weights, *Des. Codes Cryptogr.* 5, 1995, No 3, pp. 199-216.

[4] R. Craigen and H. Kharaghani, Orthogonal designs, in Handbook of Combinatorial Designs, (Eds. C.J. Colbourn and J.H. Dinitz), 2nd ed. Chapman and Hall/CRC Press, Boca Raton, Fla., 2006, pp. 280-295.

[5] R. J. Fletcher, M. Gysin and J. Seberry, Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices, *Australas. J. Combin.*, 23, 2001, pp. 75-86.

[6] A. V. Geramita and J. Seberry, *Orthogonal designs. Quadratic forms and Hadamard matrices*, Lecture Notes in Pure and Applied Mathematics, 45, Marcel Dekker Inc. New York, 1979.

[7] I. S. Kotsireas and C. Koukouvinos, New weighing matrices of order $2n$ and weight $2n-5$, *J. Combin. Math. Combin. Comput.*, to appear.

[8] C. Koukouvinos and J. Seberry, New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function-a review, *J. Statist. Plann. Inference*, 81, No 1, 1999, pp. 153–182.