Note on Williamson Matrices of Orders 25 and 37

Dragomir Ž. Đoković*
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1

ABSTRACT. All Williamson matrices in this Note are symmetric circulants. Eight non-equivalent sets of Williamson matrices of order 25 are known. They were discovered by Williamson (2 sets), Baumert and Hall (2 sets), and Sawade (4 sets). Sawade carried out a complete search and reported that there are exactly eight non-equivalent such sets of matrices. Subsequently this was confirmed by Koukouvinos and Kounias. It is surprising that we have found two more such sets. Hence there are ten non-equivalent sets of Williamson matrices of order 25.

Only three non-equivalent sets of Williamson matrices of order 37 were known so far. One of them was discovered by each of Williamson, Turyn, and Yamada. We have found one more such set.

1.

Let $n = 2k + 1 > 0$ be an odd integer and $S = \{1, 2, \ldots, k\}$. Let S_i, S_{-i} $(i = 1, 2, 3, 4)$ form a partition of S into 8 subsets (possibly void). Denote by R the group ring $\mathbf{Z}C_n$ where $C_n = \langle x \rangle$ is a cyclic group of order n with generator x. Set $w_j = x^j + x^{n-j} \in R$. We shall refer to the equation

$$\sum_{i=1}^{4} (1 + 2 \sum_{j \in S_i} w_j - 2 \sum_{j \in S_{-i}} w_j)^2 = 4n \qquad (1)$$

as the *Williamson equation*. Two solutions of this equation are said to be equivalent if one can be obtained from another by applying an automorphism of the group C_n and/or by permuting the indices i of the sets $S_{\pm i}$.

*Supported in part by the NSERC Grant A-5285.

By applying the ring homomorphism $R \to \mathbf{Z}$, $x \mapsto 1$, to Eq. (1) we obtain

$$\sum_{i=1}^{4} (1 + 4|S_i| - 4|S_{-i}|)^2 = 4n. \tag{2}$$

While it is well known that $4n$ is a sum of four odd squares, and so Eq. (2) has a solution, it was an open question (until recently) whether Eq. (1) has a solution for every odd $n > 0$. It appears now that it has none for $n = 35$ (see [3]).

2.

An m by m matrix A whose entries are ± 1 and satisfies $AA^T = mI_m$ (A^T is the transpose of A and I_m is the identity matrix) is called a *Hadamard matrix*. Every solution of Eq. (1) gives rise to a Hadamard matrix W of size $4n$. Indeed, such a solution can be used to construct four symmetric circulant matrices A, B, C, D of order n satisfying $A^2 + B^2 + C^2 + D^2 = 4nI_n$, known as *Williamson matrices*. For details we refer the reader to [4]. By inserting such four matrices in the *Williamson array*:

$$W = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}, \tag{3}$$

one obtains a Hadamard matrix of order $4n$.

R.J. Turyn [8] has found a solution of the Williamson equation when $4n = 2(q + 1)$ where q is a prime power $\equiv 1 \pmod 4$. Another proof of the same result was given by A.L. Whiteman [9]. Furthermore Whiteman discovered another infinite class of solutions of Eq. (1) [10], namely for $n = p(p + 1)/2$ where p is a prime $\equiv 1 \pmod 4$.

3.

In this section $n = 25$. Two non-equivalent sets of Williamson matrices of order 25 (No. 1 and 8 in Table 1) were found by J. Williamson himself [11]. Two additional such sets (No. 5 and 6 in Table 1) were discovered later by L. D. Baumert and M. Hall Jr. [1]. Subsequently K. Sawade [7] carried out a complete search for Williamson matrices of order 25 and found four new sets (No. 4, 7, 9, 10 in Table 1). C. Koukouvinos and S. Kounias claimed in [5] that they also carried out an exhaustive search for these matrices and confirmed the findings of K. Sawade that there are only eight non-equivalent sets of Williamson matrices of order 25. While testing one of our programs we found, to our surprise, two additional non-equivalent sets

of Williamson matrices of order 25. Then we carried out a complete search for these matrices. Our result is that there are exactly ten non-equivalent sets of Williamson matrices of order 25. For the sake of completness, we give in Table 1 below all ten solutions of Eq. (1). The new solutions are No. 2 and 3.

#	S_1	S_{-1}	S_2	S_{-2}	S_3	S_{-3}	S_4	S_{-4}
1	1,9	6	7,12	8	2,5	4	10,11	3
2	1,9	6	7,12	8	3,5	11	4,10	2
3	1,2	3	6,9	10	7,11	4	8,12	5
4	5	10	6,11	2	4,9,12	7,8		1,3
5					6,12	2,3,5,7	8,9	1,4,10,11
6	3	7	4	1	8	9,10,11	6	2,5,12
7	3	9	4	12		1,7	6,8	2,5,10,11
8	6	11	3	1,12	4	7,9	2,5,10	8
9	2,10	1,8		5	9,11	3,4,7	6,12	
10			1,2	3,8,9	7,11	4,6,12	5,10	

Table 1: Solutions of Eq. (1) for $n = 25$

There are four different decompositions of 100 as a sum of four odd squares. The first three solutions in Table 1 are associated via (2) with the decomposition $5^2+5^2+5^2+5^2$, the fourth with $1^2+5^2+5^2+7^2$, the next three with $1^2+1^2+7^2+7^2$, and the last three with $1^2+3^2+3^2+9^2$.

4.

In this section $n = 37$. J. Williamson [11] found the first set of Williamson matrices of order 37 (No. 1 in Table 2). There is also a set of Williamson matrices of this order (No. 2 in Table 2) that belongs to the infinite series discovered by Turyn [8]. In 1979, Yamada [12] carried out a complete search for a special class of Williamson matrices of order 37 and found one more set of Williamson matrices of this order (No. 3 in Table 2). We have recently found a fourth such set (No. 4 in Table 2).

#	S_1	S_{-1}	S_2	S_{-2}	S_3	S_{-3}	S_4	S_{-4}
1			5,7	1,2,6,12	4,13	9,10,14,17	3,18	8,11,15,16
2					1,3,5,10,17,18	4,9,12,15,16	11,14	2,6,7,8,13
3	16	2,9,10	5,13,18	6,8	15	12,14,17	3,4,7	1,11
4		3,18	2,15,17	13,14	9,12,16	4,10	8,11	1,5,6,7

Table 2: Known solutions of Eq. (1) for $n = 37$

The first solution is associated with the decomposition $1^2+7^2+7^2+7^2$ of 148, the second with $1^2+1^2+5^2+11^2$, and the last two with $5^2+5^2+7^2+7^2$. There are two more decompositions of 148 as a sum of four odd squares namely, $3^2+3^2+3^2+11^2$ and $3^2+3^2+7^2+9^2$. We have carried out a complete search for the former and did not find any solutions.

5.

An exhaustive computer search for non-equivalent solutions of Eq. (1) had been carried out by Baumert and Hall [1] for odd $n \leq 23$, by Sawade [7] for $n = 25$ and 27, by Koukouvinos and Kounias for $n = 9$, 15, 21, 25, 27, 33, and 39 [5, 6], and by the author for all the values mentioned above and for n= 29, 31, and 35 [2, 3]. We have reported elsewhere [3] about the discrepancies that we encountered in the cases $n = 33$ and 39.

Our computer program is straightforward : we essentially generate all possible partitions satisfying Eq. (2), and then test whether we have a solution or not. Some shortcuts are possible due to the fact that two solutions of Eq. (2) may differ only in the ordering of $|S_{\pm i}|$'s. As we have tested our program on many cases, we are confident that our results are complete as stated. On the other hand, it is very difficult to claim that any computer program, consisting of several hundred lines of code, is bug-free, and so there is still a small probability of error.

6.

We thank the referee for her/his comments, and in particular for the suggestion to conform to the current usage of the term *Williamson matrices.* As we have adopted this suggestion, we should point out that in all of our references, except [6] and the original paper of Williamson [11], this term is used in the older sense, i.e., it refers to the Hadamard matrix (3).

References

[1] L.D. Baumert and M. Hall Jr., Hadamard Matrices of the Williamson Type, *Math. Computation* **19** (1965), 442–447.

[2] D. Ž. Đoković, Williamson Matrices of Orders $4 \cdot 29$ and $4 \cdot 31$, *J. Combin. Theory* Ser. A **61** (1992), 319–321.

[3] D. Ž. Đoković, Williamson Matrices of Orders $4n$ for n=33, 35, 39, *Discrete Math.* **115** (1993), 267–271.

[4] M. Hall Jr., *Combinatorial Theory*, Blaisdell, Waltham MA, 1967.

[5] C. Koukouvinos and S. Kounias, Hadamard Matrices of the Williamson Type of Order $4 \cdot m$, $m = p \cdot q$. An Exhaustive Search for $m = 33$, *Discrete Math.* **68** (1988), 45–57.

[6] C. Koukouvinos and S. Kounias, There Are No Circulant Symmetric Williamson Matrices of Order 39, *J. Comb. Math. Comb. Comput.* **7** (1990), 161–169.

[7] K. Sawade, Hadamard Matrices of Order 100 and 108, *Bull. Nagoya Inst. Technol.* **29** (1977), 147–153.

[8] R.J. Turyn, An Infinite Class of Williamson Matrices, *J. Combin. Theory* Ser. A **12** (1972), 319–321.

[9] A.L. Whiteman, An Infinite Family of Hadamard Matrices of Williamson Type, *J. Combin. Theory* Ser. A **14** (1973), 334–340.

[10] A.L. Whiteman, Hadamard Matrices of Williamson Type, *J. Austral. Math. Soc.*, Ser. A **21** (1976), 481–486.

[11] J. Williamson, Hadamard's Determinant Theorem and the Sum of Four Squares, *Duke Math. J.* **11** (1944), 65–81.

[12] M. Yamada, On the Williamson Type j Matrices of Orders $4 \cdot 29$, $4 \cdot 41$, and $4 \cdot 37$, *J. Combin. Theory* Ser. A **27** (1979), 378–381.