Good Matrices of Orders 33, 35 and 127 Exist *

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

Abstract. Four $\{\pm 1\}$-matrices A, B, C, D of order n are called good matrices if $A - I_n$ is skew-symmetric, B, C and D are symmetric, $AA^T + BB^T + CC^T + DD^T = 4nI_n$, and, pairwise, they satisfy $XY^T = YX^T$. It is known that they exist for odd $n \leq 31$. We construct four sets of good matrices of order 33 and one set for each of the orders 35 and 127.

Consequently, there exist 4-Williamson type matrices of order 35, and a complex Hadamard matrix of order 70. Such matrices are constructed here for the first time. We also deduce that there exists a Hadamard matrix of order 1524 with maximal excess.

1 Statement of the Result

A $\{\pm 1\}$-matrix A of order n is called a *Hadamard matrix* if $AA^T = I_n$, where A^T is the transpose of A and I_n is the identity matrix of order n. A $\{\pm 1\}$-matrix A is said to be of *skew type* if $A - I_n$ is skew-symmetric. Two $\{\pm 1\}$-matrices A, B of order n are said to be *amicable* if $AB^T = BA^T$.

Definition 1. Four $\{\pm 1\}$-matrices A, B, C, D of order n are called 4–*Williamson type matrices* if A, B, C, D are pairwise amicable and satisfy

$$AA^T + BB^T + CC^T + DD^T = 4nI_n.$$

Definition 2. 4–Williamson type matrices A, B, C, D of order n are called *good matrices* if A is of skew type and B, C, D are symmetric.

* 1980 *Mathematics Subject Classification.* Primary 05B20, Secondary 05B30.
† This work was supported by NSERC of Canada Grants A-5285 and EQP0107539.

Williamson type matrices are of paramount importance in modern constructions of Hadamard matrices, see [Se1], [Se2], [Co]. Given 4–Williamson type matrices of order n one can construct a Hadamard matrix of order $4nt$ for infinitely many odd values of t. The permissible values of t are those for which there exist Baumert–Hall arrays of order $4t$, see [Co] or [Se2] for details. Good matrices can be used to construct new 4–Williamson type matrices. We mention only the following result of J. Seberry [Se1].

Theorem 1. *Assume that there exist good matrices of order n. Then*
(i) there exist 4–Williamson type matrices of order $n(4n-1)$;
(ii) if there exists a symmetric Hadamard matrix of order $4n+4$ then there exist 4–Williamson type matrices of order $n(4n+3)$.

So far only finitely many sets of good matrices of odd order are known. These orders are the odd integers ≤ 31. For the listing of known good matrices of odd order see [Sze]. The object of this note is to construct good matrices of orders 33, 35 and 127.

Theorem 2. *There exist good matrices of orders 33, 35 and 127.*

The proof of this theorem will be given in the next two sections. Recall that a $\{\pm 1, \pm i\}$-matrix A of order n is called a *complex Hadamard matrix* if $AA^* = nI_n$, where i is the imaginary unit, and A^* denotes the conjugate transpose of the matrix A.

Corollary 1. *There exist 4-Williamson type matrices of order 35, and a complex Hadamard matrix of order 70.*

Proof. The first assertion is obvious from Definition 2. The second follows from the first and an observation of Kharaghani and Seberry in [Kha]. For the convenience of the reader we give the details. If A, B, C, D are 4-Williamson type matrices of order n, and if we set

$$X = (A+B)/2,\ Y = (A-B)/2,\ V = (C+D)/2,\ W = (C-D)/2,$$

then

$$\begin{pmatrix} X+iY & V+iW \\ -V+iW & X-iY \end{pmatrix}$$

is a complex Hadamard matrix of order $2n$.

2 Method of Construction

In order to describe our construction of good matrices announced above, we need a few more definitions. Let n be a postive integer.

Definition 3. A matrix $A = (a_{ij}),\ i,j = 0,1,\dots,n-1$, is said to be *circulant* resp. *back-circulant* if $a_{i,j} = a_{i+1,j+1}$ resp. $a_{i,j} = a_{i-1,j+1}$ for all i,j (indices should be reduced modulo n).

Definition 4. Four subsets S_0, S_1, S_2, S_3 of $\{1,2,\dots,n-1\}$ are called 4-$(n; n_0, n_1, n_2, n_3; \lambda)$ *supplementary difference sets (sds)* modulo n if $|S_k| = n_k$ for $k = 0,1,2,3$ and for each $m \in \{1,2,\dots,n-1\}$ we have $\lambda_0(m) + \cdots + \lambda_3(m) = \lambda$, where $\lambda_k(m)$ is the number of solutions (i,j) of the congruence $i - j \equiv m \pmod n$ with $i,j \in S_k$.

Suppose that S_k are $4-(n; n_0, n_1, n_2, n_3; \lambda)$ sds modulo n having the following additional properties:

$$n + \lambda = n_0 + n_1 + n_2 + n_3, \tag{1}$$

$$i \in S_0 \Longleftrightarrow n - i \notin S_0, \tag{2}$$

$$i \in S_k \Longleftrightarrow n - i \in S_k,\ \ k = 1,2,3, \tag{3}$$

where in (2) and (3) it is assumed that $i \in \{1,2,\dots,n-1\}$.

Let $a_k = (a_{k0}, a_{k1}, \dots, a_{k,n-1}),\ k = 0,1,2,3$, be the row vector defined by

$$a_{ki} = \begin{cases} -1 & \text{if } i \in S_k; \\ 1 & \text{otherwise.} \end{cases}$$

Furthermore let A_0 be the circulant matrix with first row a_0, and let $A_k,\ k = 1,2,3$, be the back-circulant matrix with first row a_k. Then it is well-known (and can be easily verified) that A_0, A_1, A_2, A_3 are good matrices of order n.

The good matrices listed in [Sze] are all of the type described above. The good matrices that we have constructed are also of this type. In order to prove Theorem 2 it suffices to exhibit the sds's modulo $n = 33, 35$ and 127 satisfying the additional conditions (1), (2) and (3).

Let r be an integer relatively prime to n, and set

$$S_k' = \{ri \pmod n : i \in S_k\} \subset \{1,2,\dots,n-1\}$$

for $k = 0,1,2,3$. These sets are also $4-(n;n_0,n_1,n_2,n_3;\lambda)$ sds modulo n satisfying the conditions (1), (2) and (3). We shall say that such quadruples S_0,S_1,S_2,S_3 and S_0',S_1',S_2',S_3' are *equivalent.*

We now give a brief description of the method of computation used to find the necessary sds's. The numbers n_i are easy to determine (cf. [Sze]). We first generate a number of subsets of size n_i of $\{1,2,\dots,n\}$, having the required symmetry properties (2) or (3), and at the same time compute the corresponding set of differences. We store the multiplicities of these differences in a file, say f_i. In the case $n = 127$ the sets used were not arbitrary, but only those which can be built up from cosets of the subgroup H given in the next section. After creating these files for each of the sizes $n_0,\dots,n_3$, we try to match the items in the four files to produce an sds. This is done by examining items in two files only, say f_0 and f_1 and creating a new file in which we record the pairs which produce relatively small variation in total multiplicities of the differences. The procedure is repeated with the remaining two files f_2 and f_3. Finally the resulting two files are examined in order to find a perfect match.

3 Supplementary Difference Sets

We consider separately the three cases $n = 33, 35$ and 127.

Case $n = 33$. In this case we exhibit 4 non-equivalent sds's satisfying the conditions (1), (2), (3). The first two are $4-(33;16,16,18,22;39)$ sds:

$S_0 = \{3,10,13,14,15,16,21,22,24,25,26,27,28,29,31,32\}$,
$S_1 = \{1,6,7,9,11,12,13,15,18,20,21,22,24,26,27,32\}$,
$S_2 = \{1,3,4,5,6,10,13,14,16,17,19,20,23,27,28,29,30,32\}$,
$S_3 = \{1,2,3,5,6,7,10,11,12,13,15,18,20,21,22,23,26,27,$
$28,30,31,32\}$;

$S_0' = \{1,7,9,11,14,15,16,20,21,23,25,27,28,29,30,31\}$,
$S_1' = \{3,4,6,8,9,11,14,15,18,19,22,24,25,27,29,30\}$,
$S_2' = \{2,3,4,5,6,8,10,14,15,18,19,23,25,27,28,29,30,31\}$,

$S_3' = \{3,4,6,7,9,10,11,12,13,14,15,18,19,20,21,22,23,24,$
$26,27,29,30\}.$

The third is a $4-(33;16,12,14,14;23)$ sds :

$S_0=\{3,5,6,7,9,11,14,15,16,20,21,23,25,29,31,32\},$
$S_1=\{2,3,5,8,10,11,22,23,25,28,30,31\},$
$S_2=\{1,2,6,10,11,13,16,17,20,22,23,27,31,32\},$
$S_3=\{2,4,5,6,7,8,12,21,25,26,27,28,29,31\}.$

The fourth is a $4-(33;16,12,16,20;31)$ sds :

$S_0=\{1,3,4,6,9,13,17,18,19,21,22,23,25,26,28,31\},$
$S_1=\{1,3,5,6,9,10,23,24,27,28,30,32\},$
$S_2=\{3,4,5,6,7,10,11,16,17,22,23,26,27,28,29,30\},$
$S_3=\{1,3,4,5,8,10,11,12,13,15,18,20,21,22,23,25,28,29,$
$30,32\}.$

The row sums of the good matrices which correspond to these sds's are $1,1,-3,-11$ in the first two cases, $1,9,5,5$ in the third case, and $1,9,1,-7$ in the last case.

Case $n=35$. In this case we have found one set of $4-(35;17,12,16,16;26)$ sds satisfying the conditions (1), (2) and (3) :

$S_0=\{4,6,9,10,11,12,15,18,19,21,22,27,28,30,32,33,34\},$
$S_1=\{1,9,10,11,14,17,18,21,24,25,26,34\},$
$S_2=\{1,3,6,7,8,11,13,16,19,22,24,27,28,29,32,34\},$
$S_3=\{1,3,10,11,14,15,16,17,18,19,20,21,24,25,32,34\}.$

The row sums of the corresponding good matrices are 1,11,3,3.

Case $n=127$. Let G be the group of nonzero residues modulo 127 and let $H=<2>=\{1,2,4,8,16,32,64\}$ be its subgroup of order 7. We enumerate the 18 cosets α_i, $0\le i\le 17$, of H in G as follows:

$$\alpha_0=H,\ \alpha_2=3H,\ \alpha_4=5H,\ \alpha_6=7H,\ \alpha_8=9H,$$

$$\alpha_{10} = 11H,\ \alpha_{12} = 13H,\ \alpha_{14} = 19H,\ \alpha_{16} = 21H,$$

and $\alpha_{2i+1} = -1 \cdot \alpha_{2i}$ for $0 \le i \le 8$.

We have found a $4-(127; 63, 70, 70, 70; 146)$ sds modulo 127, S_0, S_1, S_2, S_3, where each S_k is a union of certain cosets α_i, namely

$$\begin{aligned} S_0 &= \cup\alpha_i,\ i \in \{0,2,5,6,8,10,13,14,16\}, \\ S_1 &= \cup\alpha_i,\ i \in \{0,1,2,3,4,5,10,11,14,15\}, \\ S_2 &= \cup\alpha_i,\ i \in \{0,1,4,5,6,7,8,9,14,15\}, \\ S_3 &= \cup\alpha_i,\ i \in \{0,1,4,5,12,13,14,15,16,17\}. \end{aligned}$$

These sets satisfy the conditions (1), (2), (3). Let us remark that this sds can be used, as in [Đo], to construct a new Hadamard matrix of skew type of order $4 \cdot 127$.

4 Comments

1) 4–Williamson type matrices of order 127 were constructed by Miyamoto [Mi]. Our good matrices of order 127 give another such set.

2) Our computer search for good matrices of orders 33, 35 and 127 was incomplete. Hence there may exist additional solutions not equivalent to those listed in Section 3.

3) If S_0, S_1, S_2, S_3 are $4-(n; n_0, n_1, n_2, n_3; \lambda)$ sds satisfying the conditions (1), (2) and (3), then the row sums of the corresponding good matrices are $r_i = n - 2n_i$, with $r_0 = 1$ and $4n = r_0^2 + r_1^2 + r_2^2 + r_3^2$. Thus we obtain a representation of $4n-1$ as a sum of 3 odd squares. In the case $n = 33$ there are three such decompositions, namely

$$131 = 11^2 + 3^2 + 1^2 = 9^2 + 7^2 + 1^2 = 9^2 + 5^2 + 5^2.$$

For each of these decompositions we have found at least one set of good matrices.

4) From Theorem 1 (i) we infer that there exist 4–Williamson type matrices of orders 4323, 4865 and 64389. Since there exist symmetric Hadamard matrices of order $4 \cdot 34$, $4 \cdot 36$ and $4 \cdot 128$, Theorem 1 (ii) implies that there exist 4–Williamson type matrices of order 4455, 5005 and 64897. We believe that all these orders are new.

5) The row sums of the good matrices of order 127 exhibited above are $1, -13, -13, -13$. This implies that there exists a Hadamard matrix of order 1524 and maximal excess 1524·39, see [Kou, p. 146].

6) The claim made in [Je, p. 163] that the sds's constructed in [Wh] give rise to good matrices is in error. These sds's satisfy (1) and (2), while (3) is satisfied only by one of the sets S_1, S_2, S_3.

Acknowledgment :

The author is grateful to a referee for her/his suggestions and remarks.

References :

[Co] G. Cohen, D. Rubie, J. Seberry, C. Koukouvinos, S. Kounias, and M. Yamada, A Survey of Base Sequences, Disjoint Complementary Sequences and $OD(4t; t, t, t, t)$, *J. Comb. Math. Comb. Comput.* 5 (1989), pp. 69–104.

[Đo] D. Ž. Đoković, Construction of Some New Hadamard Matrices, *Bull. Australian Math. Soc.* 45 (1992), pp. 327–332.

[Je] B. A. Jenkins, C. Koukouvinos, S. Kounias, J. Seberry, and R. Seberry, Some Results on the Excesses of Hadamard Matrices, *J. Comb. Math. Comb. Comput.* 4 (1988), pp. 155–158.

[Kha] H. Kharaghani, and J. Seberry, Regular Complex Hadamard Matrices, *Congr. Numer.* 75 (1990), pp. 187–201.

[Kou] C. Koukouvinos, S. Kounias, and J. Seberry, Further Hadamard Matrices with Maximal Excess and New SBIBD $(4k^2, 2k^2 + k, k^2 + k)$, *Utilitas Math.* 36 (1989), pp. 135–150.

[Mi] M. Miyamoto, A Construction of Hadamard Matrices, *J. Combinatorial Theory*, Ser. A 57 (1991), pp. 86–108.

[Se1] J. Seberry Wallis, Construction of Williamson Type Matrices, *Linear and Multilinear Algebra* 3 (1975), pp. 197–207.

[Se2] J. Seberry Wallis, On Hadamard Matrices, *J. Combinatorial Theory*, Ser. A 18 (1975), pp. 149–164.

[Sze] G. Szekeres, A Note on Skew Type Orthogonal ±1 Matrices, in "Combinatorics," Colloquia Mathematica Societatis János Bolyai, No. 52, North Holland 1988, Ed. by A. Hajnal, L. Lovász, and V.T. Sós, pp. 489–498.

[Wh] A. L. Whiteman, Skew–Hadamard Matrices of Goethals–Seidel Type, *Discrete Math.* 2 (1975), pp. 397–405.