Five New Orders for Hadamard Matrices of Skew Type

Dragomir Ž. Đoković*

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1

Abstract

By using the (generalized) Goethals–Seidel array, we construct Hadamard matrices of skew type of order $4n$ for $n = 81, 103, 151, 169,$ and 463. Hadamard matrices of skew type for these orders are constructed here for the first time. Consequently the list of odd integers $n < 300$ for which no Hadamard matrix of skew type of order $4n$ is presently known is reduced to 45 numbers (see the comments after the statement of Theorem 1).

1 Introduction

Let G be a finite abelian group of order n. For $S \subset G$ and $a \in G$ let $\nu(S,a)$ be the number of ordered pairs $(x,y) \in S \times S$ such that $x - y = a$. We say that subsets $S_1, \ldots, S_k \subset G$ are *supplementary difference sets* (abbreviated as *SDS*) with parameters $(n; n_1, \ldots, n_k; \lambda)$ if $|S_i| = n_i$ for all i and

$$\sum_{i=1}^{k} \nu(S_i, a) = \lambda, \quad \forall a \in G \setminus \{0\}.$$

We are especially interested in supplementary difference sets S_1, S_2, S_3, S_4 whose parameters $(n; n_1, n_2, n_3, n_4; \lambda)$ satisfy the condition

$$n + \lambda = n_1 + n_2 + n_3 + n_4. \tag{1}$$

Such SDS's give rise to Hadamard matrices M of order $4n$.

In order to explain the construction of M we need some more notations (see also [7, Theorem 7.2] or [8]). Given any subset $S \subset G$, let A_S be the matrix of order n whose rows and columns are indexed by elements of G and whose (x,y)-entry is -1

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

if $y - x \in S$, and $+1$ otherwise. For the sake of simplicity let us write A_i for A_{S_i}. If $S_1, \ldots, S_4$ are $(n; n_1, \ldots, n_4; \lambda)$-SDS such that (1) holds, then it is easy to check that

$$\sum_{i=1}^{4} A_i A_i^T = 4nI_n, \tag{2}$$

where the superscript T denotes the transposition of matrices. Let J be the matrix of order n all of whose entries are 1. By pre-multiplying and post-multiplying (2) by J we obtain

$$\sum_{i=1}^{4} (n - 2n_i)^2 = 4n. \tag{3}$$

In practice, (3) is used to find, for a given n, the possible parameters n_i.

Let R be the matrix of order n whose (x, y)-entry is 1 if $x + y = 0$, and 0 otherwise. Thus $R = (\delta_{x,-y})$, where $\delta_{x,y} = 1$ if $x = y$ and 0 otherwise. It is easy to see that $R^2 = I_n$ and $R^T = R$. Then the desired Hadamard matrix M is given by the following formula :

$$M = \begin{pmatrix} A_1 & A_2R & A_3R & A_4R \\ -A_2R & A_1 & -A_4^TR & A_3^TR \\ -A_3R & A_4^TR & A_1 & -A_2^TR \\ -A_4R & -A_3^TR & A_2^TR & A_1 \end{pmatrix}. \tag{4}$$

This construction was discovered by Goethals and Seidel in the case when G is cyclic (see [6]). For the generalization to arbitrary finite abelian groups see [8]. We shall refer to the array (4) as the (generalized) *GS-array.*

The GS-array is also a very powerful tool for constructing Hadamard matrices of skew type. Let us say that a subset $S \subset G$ is of *skew type* if $S \cap (-S) = \emptyset$ and $S \cup (-S) = G \setminus \{0\}$. Clearly such S exists iff n is odd.

Now assume that n is odd, that $S_1, S_2, S_3, S_4 \subset G$ are SDS whose parameters satisfy (1), and that S_1 is of skew type. Then the Hadamard matrix M given by (4) is of skew type. This follows from the observation that each of the matrices A_iR and A_i^TR $(i = 2, 3, 4)$ is symmetric, while $A_1 - I_n$ is skew symmetric. In order to verify the former assertion, let $A = (a_{x,y})$ be any matrix satisfying $a_{x+z,y+z} = a_{x,y}$ for all $x, y, z \in G$. (All the matrices A_S, $S \subset G$, satisfy this condition.) Then the (x, z)-entry of AR is

$$\sum_{y \in G} a_{x,y}\delta_{y,-z} = a_{x,-z} = a_{x+z,0},$$

which is obviously symmetric in x and z. Similarly, RA is symmetric, i.e., $RA = A^TR$.

We have used this method successfully to construct Hadamard matrices of skew type of order $4n$ for prime $n =$ 37, 43, 67, 113, 127, 157, 163, 181, and 241, see [1] and [2], and for composite $n =$ 39, 49, 65, 93, 121, 129, 133, 217, 219, and 267 in [3]. In all these cases G was a cyclic group of order n. When n is big, say $n > 35$, the search for required SDS's is beyond the power of the machines available to us. Consequently, in practically all cases we had to restrict the search for the S_i's to some special class of subsets. For a brief description of our method of computation see our recent article [5].

We use this opportunity to correct three misprints in [3]. The number 16 should be deleted from J_4 of case (h) on p. 52. The quadruple J_1, J_2, J_3, J_4 just above the quadruple (l) on p. 57 should carry the label (k). The integer 24 in the bottom line of p. 57 should be replaced by 25.

2 Some new supplementary difference sets

We state our main result.

Theorem 1. *There exists Hadamard matrices of skew type of order* $4n$ *for* $n = 81,\ 103,\ 151,\ 169$ *and* 463.

For the list of Hadamard matrices of skew type of order $4n$, $n \leq 1000$, see [7]. By taking into account all known facts, the above theorem implies that the list of odd integers $n < 300$, for which no Hadamard matrix of skew type of order $4n$ is presently known, is now reduced to the following list of 45 integers :

$$n = \begin{array}{l} 47,59,69,89,97,101,107,109,119,145,149,153,167,177,179,191,\\ 193,201,205,209,213,223,225,229,233,235,239,245,247,249,251,\\ 253,257,259,261,265,269,275,277,283,285,287,289,295,299. \end{array}$$

As explained in Section 1, Theorem 1 is a consequence of the following existence result for supplementary difference sets.

Theorem 2. *An elementary abelian group* G *of order* $n = 81,\ 103,\ 151,\ 169$ *or* 463 *contains supplementary difference sets* $S_1,\ S_2,\ S_3,\ S_4$, *with* S_1 *of skew type, and with parameters* $(n; n_1, n_2, n_3, n_4; \lambda)$ *given in Table* 1 *below.*

Table 1

n	n_1	n_2	n_3	n_4	λ
81	40	35	35	45	74
103	51	51	57	60	116
151	75	65	80	80	149
169	84	77	77	77	146
463	231	231	231	210	440

We shall now give explicit construction of the required SDS's. The five cases will be treated separately. In each case, G will be the additive group of a Galois field F of order $n = p^k$, H will be a subgroup of F^*, the order of H will be odd, and so the index $[F^* : H]$ will be even, say $2s$. We enumerate the $2s$ cosets α_i, $0 \leq i < 2s$, of

H so that $\alpha_0 = H$ and $\alpha_{2i+1} = -\alpha_{2i}$ for $0 \le i < s$. It suffices to list only the even cosets α_{2i}. Each S_i $(i = 1, 2, 3, 4)$ will be of the form

$$S_i = \bigcup_{j \in J_i} \alpha_j$$

for some index set $J_i \subset \{0, 1, \ldots, 2s-1\}$. Instead of listing the sets S_i we shall only list their index sets J_i. Unless stated otherwise, the set S_1 will be always of skew type. This is easy to verify by checking that for each i, $0 \le i < s$, exactly one of the integers $2i$ and $2i+1$ belongs to J_1.

Case $n = 81$: We construct the Galois field F of order $81 = 3^4$ by adjoining to $\mathbf{Z}_3$ a root x of the polynomial $t^4 - t^3 - 1$ (which is irreducible and primitive over $\mathbf{Z}_3$). Thus $F = \mathbf{Z}_3[x]$ where $x^4 = 1 + x^3$. The group $F^* = \langle x \rangle$ is cyclic of order 80. Let $H = \langle x^{16} \rangle$ be its subgroup of order 5. We enumerate the 16 cosets of H in F^* as follows : $\alpha_{2i} = x^i H$ and $\alpha_{2i+1} = -x^i H$ for $0 \le i < 8$.

We have found seven non-equivalent SDS's S_1, S_2, S_3, S_4, with S_1 of skew type, having parameters (81; 40, 35, 35, 45; 74), but we shall only list two of them :

$$(a)\quad J_1 = \{1,2,4,6,8,10,12,14\},\quad J_2 = \{1,2,3,4,10,11,13\},$$
$$J_3 = \{4,5,6,8,12,13,14\},\quad J_4 = \{2,4,5,6,7,11,12,13,15\};$$

$$(b)\quad J_1 = \{0,2,5,7,8,11,13,14\},\quad J_2 = \{0,2,4,6,13,14,15\},$$
$$J_3 = \{5,6,7,8,11,12,15\},\quad J_4 = \{0,1,4,6,8,12,13,14,15\}.$$

For both SDS's the sum of squares (3) is $11^2 + 11^2 + 9^2 + 1^2$.

In the remaining cases we shall only list the essential information.

Case $n = 103$: $F = \mathbf{Z}_{103}$, $H = \{1, 46, 56\}$, $s = 17$. Even cosets :

$$\alpha_0 = H,\quad \alpha_2 = 2H,\quad \alpha_4 = 3H,\quad \alpha_6 = 4H,\quad \alpha_8 = 5H,\quad \alpha_{10} = 6H,$$
$$\alpha_{12} = 7H,\quad \alpha_{14} = 8H,\quad \alpha_{16} = 10H,\quad \alpha_{18} = 12H,\quad \alpha_{20} = 14H,\quad \alpha_{22} = 15H,$$
$$\alpha_{24} = 17H,\quad \alpha_{26} = 19H,\quad \alpha_{28} = 21H,\quad \alpha_{30} = 23H,\quad \alpha_{32} = 30H.$$

(103; 51, 51, 57, 60; 116)-SDS :

$$(c)\quad J_1 = \{1,3,4,6,8,11,12,14,17,18,20,22,25,27,28,30,32\},$$
$$J_2 = \{2,9,10,12,13,14,15,16,20,21,22,23,24,26,28,29,30\},$$
$$J_3 = \{0,1,2,3,4,11,12,13,16,17,19,20,21,24,25,26,28,30,31\},$$
$$J_4 = \{0,1,2,3,4,5,6,13,15,18,19,20,23,24,25,26,27,28,29,31\}.$$

Sum of squares : $17^2 + 11^2 + 1^2 + 1^2$.

Case $n = 151$: $F = \mathbf{Z}_{151}$, $H = \{1, 8, 19, 59, 64\}$, $s = 15$. Even cosets :

$$\alpha_0 = H,\quad \alpha_2 = 2H,\quad \alpha_4 = 3H,\quad \alpha_6 = 4H,\quad \alpha_8 = 5H,$$
$$\alpha_{10} = 6H,\quad \alpha_{12} = 9H,\quad \alpha_{14} = 10H,\quad \alpha_{16} = 11H,\quad \alpha_{18} = 12H,$$
$$\alpha_{20} = 15H,\quad \alpha_{22} = 22H,\quad \alpha_{24} = 27H,\quad \alpha_{26} = 29H,\quad \alpha_{28} = 30H.$$

(151; 65, 75, 80, 80; 149)-SDS :

$$
\begin{aligned}
(d)\quad J_1 &= \{0,3,5,6,8,11,13,14,16,19,21,23,25,27,28\},\\
J_2 &= \{2,3,6,13,16,17,20,23,25,26,27,28,29\},\\
J_3 &= \{0,1,2,3,4,6,7,8,9,10,11,12,23,24,27,28\},\\
J_4 &= \{1,4,5,10,11,12,13,14,16,18,19,22,25,26,27,28\}.
\end{aligned}
$$

(151: 80, 80, 80, 85; 174)-SDS :

$$
\begin{aligned}
(e)\quad J_1 &= \{0,1,2,4,5,6,7,8,13,14,16,18,19,20,26,29\},\\
J_2 &= \{2,3,4,8,10,11,14,15,16,18,19,22,25,27,28,29\},\\
J_3 &= \{2,7,8,9,11,12,15,19,21,23,24,25,26,27,28,29\},\\
J_4 &= \{0,2,3,5,6,7,8,9,11,16,17,18,20,22,23,25,27\}.
\end{aligned}
$$

(151; 70, 70, 75, 85; 149)-SDS :

$$
\begin{aligned}
(f)\quad J_1 &= \{0,8,10,11,12,14,16,20,21,22,23,27,28,29\},\\
J_2 &= \{2,9,10,13,14,15,16,18,24,25,26,27,28,29\},\\
J_3 &= \{0,3,4,5,10,11,12,13,14,18,19,20,21,23,24\},\\
J_4 &= \{0,1,2,4,5,6,7,12,15,16,17,18,19,23,24,27,29\}.
\end{aligned}
$$

In the cases (e) and (f) the sets S_1 are not of skew type. The sums of squares for (d), (e), (f) are $21^2+9^2+9^2+1^2$, $19^2+9^2+9^2+9^2$, $19^2+11^2+11^2+1^2$, respectively.

Case $n = 169$: $F = \mathbf{Z}_{13}[x]$, $x^2 = 4x - 6$, $F^* = \langle x \rangle$, $H = \langle x^{24} \rangle$, $|H| = 7$, and $s = 12$. All cosets : $\alpha_{2i} = x^i H$ and $\alpha_{2i+1} = -x^i H$ for $0 \le i < 12$.

(169; 84, 77, 77, 77; 146)-SDS's :

$$
\begin{aligned}
(g)\quad J_1 &= \{0,2,5,7,9,10,12,15,16,18,21,22\},\\
J_2 &= \{0,1,2,7,8,9,13,14,18,20,23\},\\
J_3 &= \{1,4,6,7,9,14,16,17,20,21,23\},\\
J_4 &= \{3,5,6,9,10,12,13,14,15,17,20\};
\end{aligned}
$$

$$
\begin{aligned}
(h)\quad J_1 &= \{1,3,4,6,8,10,13,15,16,19,21,22\},\\
J_2 &= \{1,2,3,4,5,6,8,10,11,17,18\},\\
J_3 &= \{1,2,5,8,9,12,14,15,16,18,19\},\\
J_4 &= \{2,3,4,5,6,7,8,9,17,18,23\}.
\end{aligned}
$$

In both cases the sum of squares is $15^2 + 15^2 + 15^2 + 1^2$.

Case $n = 463$: $F = \mathbf{Z}_{463}$, $H = \langle 251 \rangle$, $|H| = 21$, and $s = 11$. Even cosets :

$$
\begin{aligned}
&\alpha_0 = H,\quad \alpha_2 = 2H,\quad \alpha_4 = 4H,\quad \alpha_6 = 5H,\quad \alpha_8 = 7H,\quad \alpha_{10} = 8H,\\
&\alpha_{12} = 10H,\quad \alpha_{14} = 19H,\quad \alpha_{16} = 25H,\quad \alpha_{18} = 29H,\quad \alpha_{20} = 49H.
\end{aligned}
$$

(463; 231, 231, 231, 210; 440)-SDS :

$$
\begin{aligned}
(i)\quad J_1 &= \{0,2,4,7,9,10,13,15,16,18,20\},\\
J_2 &= \{0,4,5,7,8,14,15,16,17,19,21\},\\
J_3 &= \{0,4,5,7,9,12,14,15,18,19,21\},\\
J_4 &= \{0,6,7,8,9,12,13,14,16,21\}.
\end{aligned}
$$

Sum of squares : $43^2 + 1^2 + 1^2 + 1^2$. Note that S_1 is the set of squares of F^*, and so it is the well known (463, 231, 115) cyclic difference set. Hence the sets S_2, S_3, S_4 are (463; 231, 231, 210; 325)-SDS. We mention that 10 non-equivalent SDS's with the parameters (463; 231, 231, 231, 210; 440) were constructed in [4] but none of them contained a set of skew type.

References

[1] D. Ž. Đoković, Skew Hadamard matrices of order 4 × 37 and 4 × 43, *J. Combinatorial Theory*, Ser. A **61** (1992), 319-321.

[2] D. Ž. Đoković, Construction of some new Hadamard matrices, *Bull. Austral. Math. Soc.* **45** (1992), 327-332.

[3] D. Ž. Đoković, Ten new orders for Hadamard matrices of skew type, *Publ. Elektrotehničkog Fak.*, Ser. Matematika, Univ. of Belgrade, **3** (1992), 47-59.

[4] D. Ž. Đoković, Ten Hadamard matrices of order 1852 of Goethals-Seidel type, *Europ. J. Combinatorics* **13** (1992), 245-248.

[5] D. Ž. Đoković, Good matrices of orders 33, 35 and 127 exist, *J. Comb. Math. Comb. Comput.* **14** (1993), 145-152.

[6] J. M. Goethals and J. J. Seidel, A skew-Hadamard matrix of order 36, *J. Austral. Math. Soc.* A **11** (1970), 343-344.

[7] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, in *Contemporary Design Theory : A Collection of Surveys*, pp. 431-560, J. H. Dinitz and D. R. Stinson Eds., Wiley, New York, 1992.

[8] J. Wallis and A. L. Whiteman, Some classes of Hadamard matrices with constant diagonal, *Bull. Austral. Math. Soc.* **7** (1972), 233-249.

(Received 13/12/93)