UDC 519.614
doi:10.31799/1684-8853-2018-4-2-8

Articles

SYMMETRIC HADAMARD MATRICES OF ORDERS 268, 412, 436 AND 604

N. A. Balonin[a], *Dr. Sc., Tech., Professor, korbendfs@mail.ru*
D. Ž. Đoković[b], *PhD, Distinguished Professor Emeritus, djokovic@uwaterloo.ca*
[a]*Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation*
[b]*University of Waterloo, Department of Pure Mathematics and Institute for Quantum Computing, Waterloo, Ontario, N2L 3G1, Canada*

Purpose: *To investigate more fully, than what was done in the past, certain families of symmetric Hadamard matrices of small orders by using the so called propus construction.* ***Methods:*** *Orbit method for the search of three cyclic blocks to construct Hadamard matrices of propus type. This method speeds up the classical search of required sequences by distributing them into different bins using a hash-function.* ***Results:*** *Our main result is that we have constructed, for the first time, symmetric Hadamard matrices of order 268, 412, 436 and 604. The necessary difference families are constructed by restricting the search to the families which admit a nontrivial multiplier. A wide collection of new symmetric Hadamard matrices was obtained and tabulated, according to the feasible sets of parameters.* ***Practical relevance:*** *Hadamard matrices are used extensively in the problems of error-free coding, compression and masking of video information. Programs for search of symmetric Hadamard matrices and a library of constructed matrices are used in the mathematical network “Internet” together with executable on-line algorithms.*

Keywords *— Propus Construction, Difference Families, Symmetric Hadamard Matrices, Optimal Binary Sequences.*

2010 Mathematics Subject Classification: 05B10, 05B20.

Citation: Balonin N. A., Đoković D. Ž. Symmetric Hadamard Matrices of Orders 268, 412, 436 and 604. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 4, pp. 2–8. doi:10.31799/1684-8853-2018-4-2-8

Introduction

The construction of symmetric Hadamard matrices was stagnating for long time while that of skew-Hadamard matrices advanced rapidly. The reason for this discrepancy was the fact that for the latter we had a very versatile tool, namely the Goethals — Seidel (GS) array, while for the former such tool was missing. The new tool for the construction of the symmetric Hadamard matrices, so called propus array, was discovered recently [1] by J. Seberry and the first author. It was already used in [2–4] to construct many propus Hadamard matrices (such matrices are always symmetric) including some having new orders.

The authors of [1] observed that the well known Turyn series of Williamson quadruples (of symmetric circulant blocks) gives the first infinite series of propus Hadamard matrices. They also give a variation of the propus array in which they plug symmetric and commuting Williamson type quadruples to construct another infinite series of symmetric Hadamard matrices. Yet another infinite series of propus Hadamard matrices was identified in [4, Theorem 5].

In this paper we continue our previous work [2, 3] where we used the propus construction to find new symmetric Hadamard matrices. We refer to these papers and [5] for the more comprehensive description of this construction and the definitions of the GS-array and GS-difference families. As the propus difference families play a crucial role in the paper, we shall define them precisely in the next section and specify the propus array that we use.

The first Hadamard matrix of order $4 \cdot 67 = 268$ was constructed by Sawade in 1985 [6]. The first skew-Hadamard matrix of the same order was constructed in 1992 by one of the authors [7]. However a symmetric Hadamard matrix of order 268 was not discoverd so far. We present in Sect. 3 six propus difference families in the cyclic group $\mathbf{Z}_{67}$ which we use to construct six symmetric Hadamard matrices of order 268. Moreover, in the same section we also construct the first examples of symmetric Hadamard matrices of orders 412, 436 and 604. Examples of symmetric Hadamard matrices of order $4v$ are now known [2–4, 8] for all odd positive integers $v < 200$ except for

$$59, 65, 81, 89, 93, 101, 107, 119, 127, 133, 149,$$
$$153, 163, 167, 179, 183, 189, 191, 193.$$

The binary sequences, i.e., $\{\pm 1\}$-sequences, of length $v \equiv 1 \pmod 4$ are called *optimal* if the off-peak values of its periodic autocorrelation function are +1 or −3. Such sequence is *balanced* if its sum is ±1. A computer generated list of binary balanced optimal sequences of length $v \equiv 1 \pmod 4$ is given in [9] for $v \leq 47$. As a byproduct of our computations of propus difference families we have obtained binary balanced optimal sequences of lengths 49 and 61. They are presented in Sect. 4.

In addition to the propus difference families used in Sect. 3, we give a more extensive list of such families in Sect. 5.

While trying to verify the proof of [1, Corollary 1] we observed that this corollary is stated incorrectly. The second sentence of the corollary should read: "Then there exist symmetric Williamson type matrices of order $q+2$ and a symmetric propus-type Hadamard matrix of order $4(q+2)$". Consequently, $4(2q+1)$ should be replaced with $4(q+2)$ in the abstract as well as in line 3 on p. 351. Further, the two lists, one on p. 352 and the other on p. 356 should be corrected. The integers 59, 67, 81, 89, 105, 111, 119, 127 should be removed from the former, while 97, 99 should be removed from and 59, 67, 89, 119, 127 inserted into the latter. (The cases 59, 89, 119, 127 are still unresolved.)

Preliminaries

Let G be a finite abelian group of order $v > 1$. Let (X_i), $i = 1, 2, \dots, m$, be a difference family in G. We fix its parameter set

$$(v;\, k_1, k_2, \dots, k_m;\, \lambda),\ k_i = |X_i|. \tag{1}$$

Recall that these parameters satisfy the equation

$$\sum_{i=1}^{t} k_i\left(k_i - 1\right) = \lambda\left(v - 1\right). \tag{2}$$

The set of diference families in G having this parameter set is invariant under the following elementary transformations:

a) for some i replace X_i by a translate $g + X_i$, $g \in G$;

b) for some i replace X_i by $-X_i$;

c) for all i replace X_i by its image $\alpha(X_i)$ under an automorphism α of G;

d) exchange X_i and X_j provided that $|X_i| = |X_j|$.

Definition 1. *We say that two difference families with the same parameter set are equivalent if one can be transformed to the other by a finite sequence of elementary transformations.*

Definition 2. *Let (X_i) be a difference family in G. We say that an automprphism α of G is a multiplier of this family if each set $\alpha(X_i)$ is a translate of X_i.*

If a positive integer m is relatively prime to v then the multiplication by m is an automorphism of G. If this automorphism is a multiplier of a difference family, then we also say that the integer m is a *multiplier* or a *numeric multiplier* of that family.

The multipliers of a difference family in G form a subgroup of the automorphism group of G. All difference families that we construct in this paper have nontrivial multipliers. This follows from the fact that we use only the base blocks X_i which are union of orbits of a fixed nontrivial subgroup H of the automorphism group of G. We refer to this method of constructing difference families as the *orbit method*.

We are only interested in GS-difference families formally introduced in [5] and [10]. They consist of four base blocks (X_1, X_2, X_3, X_4) and their parameter sets, also known as the GS-*parameter sets*, satisfy besides the obvious condition (2) (with $m = 4$) also the condition

$$\sum_{i=1}^{4} k_i = \lambda + v. \tag{3}$$

By eliminating the parameter λ from the equations (2) and (3), we obtain that

$$\sum_{i=1}^{4}\left(v - 2k_i\right)^2 = 4v. \tag{4}$$

If $k_i = k_j$ for some $i \neq j$ in a GS-parameter set $(v;\, k_1, k_2, k_3, k_4;\, \lambda)$ then we say that this parameter set is a *propus parameter set*.

In fact we shall use only a very special class of GS-difference families known as *propus difference families*. We adopt here the following definiton of these families.

Definition 3. *A propus difference family is a GS-difference family (X_i), $i = 1, 2, 3, 4$, subject to two additional conditions*:

a) *two of the base blocks are equal, say $X_i = X_j$ for some $i < j$, which implies that $k_i = k_j$*;

b) *at least one of the other two base blocks is symmetric.*

(We say that a subset $X \subseteq G$ is symmetric if $-X = X$.)

Unless stated otherwise, we shall assume from now on that G is cyclic. We identify G with the additive group of the ring $\mathbf{Z}_v$ of integers modulo v. We denote by $\mathbf{Z}_v^*$ the group of units (invertible elements) of $\mathbf{Z}_v$. We identify the automorphism group of G with $\mathbf{Z}_v^*$. Thus, every automorphism α of $\mathbf{Z}_v$ is just the multiplication modulo v by some integer k relatively prime to v.

To any subset $X \subseteq \mathbf{Z}_v$ we associate the binary sequence (i.e., a sequence with entries +1 and –1) of length v, say $(x_0, x_1, \dots, x_{v-1})$, where $x_i = -1$ if and only if $i \in X$. By abuse of language, we shall use the symbol X to denote also the binary sequence associated to the subset X.

Let (X_i) be a GS-diference family in $\mathbf{Z}_v$. Further, let $\mathbf{A}_i$ be the circulant matrix having the sequence X_i as its first row. Then the $\mathbf{A}_i$ satisfy the equation

$$\sum_{i=1}^{4} \mathbf{A}_i^{\mathrm{T}} \mathbf{A}_i = 4v\mathbf{I}_v, \tag{5}$$

where $\mathbf{I}_v$ is the identity matrix of order v. This equation guarantees that, after plugging the $(\mathbf{A}_i)$ into the GS-array, we obtain a Hadamard matrix.

If (X_i) is a propus difference family, we say that the corresponding matrices $(\mathbf{A}_i)$ are *propus matrices*. By plugging these $(\mathbf{A}_i)$, in suitable order, into the *propus array*

$$\begin{bmatrix} -\mathbf{A}_1 & \mathbf{A}_2\mathbf{R} & \mathbf{A}_3\mathbf{R} & \mathbf{A}_4\mathbf{R} \\ \mathbf{A}_3\mathbf{R} & \mathbf{R}\mathbf{A}_4 & \mathbf{A}_1 & -\mathbf{R}\mathbf{A}_2 \\ \mathbf{A}_2\mathbf{R} & \mathbf{A}_1 & -\mathbf{R}\mathbf{A}_4 & \mathbf{R}\mathbf{A}_3 \\ \mathbf{A}_4\mathbf{R} & -\mathbf{R}\mathbf{A}_3 & \mathbf{R}\mathbf{A}_2 & \mathbf{A}_1 \end{bmatrix}, \qquad (6)$$

where $\mathbf{R}$ is the back-diagonal permutation matrix, we obtain a symmetric Hadamard matrix of order $4v$. The ordering should be chosen so that $\mathbf{A}_1$ is symmetric and $\mathbf{A}_2 = \mathbf{A}_3$.

We construct the base blocks X_i as unions of certain orbits of a small nontrivial subgroup $H \subseteq \mathbf{Z}_v^*$ (mostly of order 3 or 5). When recording a base block, to save space, we just list the representatives of the orbits which occur in the block. As a representative, we always choose the smallest integer of the orbit.

The Cases $v = 67, 103, 109, 151$

In this section we list six non-equivalent examples of propus difference families in $\mathbf{Z}_{67}$, three such families in $\mathbf{Z}_{103}$, two in $\mathbf{Z}_{109}$, and a single one in $\mathbf{Z}_{151}$. By using the propus array, they provide the first examples of symmetric Hadamard matrices of orders 268, 412, 436 and 604, respectively.

In the case $v = 67$, up to a permutation of the k_is, there are three feasible propus parameter sets for the subgroup $H = \{1, 29, 37\} \subseteq \mathbf{Z}_{67}^*$. For each of them we have found several propus difference families. We list only two families per parameter set. The block X_4 is symmetric in the first two families while X_1 is symmetric in the remaining four families.

Let us explain how we record the base blocks. As an example, we take the block X_2 of the first family in Table 1. It is the union of ten H-orbits whose representatives are the integers 0, 2, 4, 6, 16, 17, 25, 27, 30, 41. As each nontrivial orbit has size 3, the block X_2 has the size $1 + 9 \cdot 3 = 28$. The blocks X_1 and X_4 are given similarly. In all difference families listed in this and the next section we have $X_2 = X_3$ and we record only the blocks X_1, X_2 and X_4 in that order. The families having the same parameter set are separated by a semicolon.

■ ***Table 1**.* Propus difference families in $\mathbf{Z}_{67}$, $\mathbf{Z}_{103}$, $\mathbf{Z}_{109}$ and $\mathbf{Z}_{151}$

(67; 33, 28, 28, 31; 53), $H = \{1, 29, 37\}$
[1, 3, 4, 10, 12, 15, 17, 30, 34, 36, 41], [0, 2, 4, 6, 16, 17, 25, 27, 30, 41], [0, 1, 4, 5, 8, 10, 16, 18, 30, 32, 36];
[1, 2, 8, 15, 16, 18, 25, 30, 32, 34, 36], [0, 2, 3, 6, 8, 9, 17, 18, 34, 36], [0, 1, 2, 4, 5, 9, 16, 17, 18, 30, 41]

(67; 30, 31, 31, 27; 52), $H = \{1, 29, 37\}$
[1, 5, 6, 15, 16, 17, 27, 30, 34, 41], [0, 2, 4, 9, 10, 12, 16, 23, 30, 36, 41], [5, 8, 9, 12, 16, 17, 23, 25, 41];
[3, 5, 8, 10, 12, 16, 23, 25, 32, 36], [0, 5, 6, 9, 12, 15, 16, 17, 23, 27, 30], [1, 2, 3, 4, 8, 27, 30, 32, 36]

(67; 30, 30, 30, 28; 51), $H = \{1, 29, 37\}$
[3, 4, 5, 8, 10, 16, 18, 23, 32, 36], [3, 6, 9, 10, 12, 15, 17, 23, 25, 41], [0, 5, 9, 10, 12, 15, 17, 27, 30, 41];
[2, 3, 4, 9, 10, 17, 18, 23, 32, 41], [1, 2, 9, 16, 17, 23, 27, 32, 34, 41], [0, 3, 10, 15, 16, 17, 23, 27, 32, 34]

(103; 48, 51, 51, 42; 89), $H = \{1, 46, 56\}$
[3, 4, 14, 17, 19, 21, 29, 30, 31, 33, 38, 40, 49, 51, 55, 62], [2, 3, 4, 6, 7, 14, 15, 22, 29, 30, 31, 38, 42, 44, 47, 49, 62],
[3, 6, 8, 10, 15, 17, 21, 31, 33, 38, 42, 44, 55, 60];
[1, 3, 6, 8, 10, 11, 21, 30, 33, 40, 44, 47, 49, 51, 55, 62], [5, 6, 7, 11, 12, 14, 19, 23, 29, 30, 38, 40, 47, 51, 55, 60, 62],
[4, 6, 7, 8, 10, 12, 17, 20, 22, 33, 42, 44, 49, 55]

(109; 52, 49, 49, 48; 89), $H = \{1, 45, 63\}$
[0, 3, 4, 6, 9, 10, 11, 12, 18, 19, 20, 24, 31, 36, 43, 48, 50, 60], [0, 1, 2, 3, 5, 9, 10, 16, 19, 20, 23, 25, 41, 46, 55, 57, 62],
[1, 2, 4, 6, 9, 10, 15, 19, 20, 24, 31, 36, 38, 46, 48, 57];
[0, 3, 5, 8, 11, 12, 13, 15, 18, 20, 30, 31, 41, 43, 46, 53, 55, 57], [0, 1, 2, 3, 5, 8, 11, 12, 13, 16, 29, 31, 38, 41, 48, 50, 57],
[3, 6, 8, 10, 18, 20, 23, 24, 25, 29, 41, 48, 55, 57, 60, 62];
[0, 1, 2, 3, 6, 9, 10, 12, 15, 18, 24, 25, 36, 41, 43, 48, 53, 57], [0, 1, 3, 6, 8, 9, 11, 12, 13, 18, 23, 29, 31, 36, 41, 43, 57],
[1, 3, 9, 11, 13, 16, 18, 29, 30, 31, 43, 46, 50, 53, 62, 67]

(151; 71, 71, 71, 66; 128), $H = \{1, 8, 19, 59, 64\}$
[0, 2, 5, 6, 7, 11, 15, 17, 23, 27, 30, 34, 37, 51, 68], [0, 1, 2, 3, 4, 14, 17, 23, 27, 28, 34, 47, 51, 68, 87],
[0, 1, 2, 3, 4, 5, 7, 10, 29, 34, 46, 47, 51, 68]

For the cases $v = 103$ and $v = 109$ we use again the subgroups H of order 3, namely $\{1, 46, 56\} \subset \mathbf{Z}^*_{103}$ and $\{1, 45, 63\} \subset \mathbf{Z}^*_{109}$. For $v = 103$ we found two non-equivalent propus difference families having the same parameter set and for $v = 109$ we found three such families. In all six families the block X_4 is symmetric.

For the case $v = 151$ we use the subgroup of order five. Only one propus difference family was found. The symmetric block is X_1.

Some New Balanced Optimal Binary Sequences

In this section we list some balanced optimal binary sequences of lengths 49 and 61. They arose as a byproduct of our search for propus difference families. We say that a binary sequence of length v has *three-level autocorrelation function* if this function takes exactly three distinct values, including the value v at shift 0.

Up to a permutation of the k_is, there are three feasible propus parameter sets for the subgroup $H = \{1, 18, 30\}$ of $\mathbf{Z}^*_{49}$. We discard the one with all $k_i = 21$ as it probably does not admit any propus difference family, see [3]. In Table 2 we list five propus difference families for $v = 49$ and a single family for $v = 61$.

The block X_2, of cardinality 24, in the first example is

$$X_2 = \{3, 5, 7, 8, 9, 13, 14, 15, 16, 21, 25, 28, 29, 32, 35, 37, 38, 39, 41, 42, 43, 44, 46, 47\}.$$

The values of the periodic autocorrelation function of the corresponding sequence X_2, for the shifts in the range 0, 1, ..., 24, are:

$$49, 1, -3, -3, 1, -3, 1, 1, -3, -3, 1, -3, -3, 1, -3, 1, -3, 1, 1, -3, 1, 1, 1, -3.$$

Thus the correlation values of X_2 occupy just three levels 49, 1 and −3. In the terminology of [9, p. 144] (see also [11]) the sequence X_2 is a balanced optimal binary sequence of length 49. Such sequences of lengths $v \equiv 1 \pmod 4$ are listed there on the same page for $v \le 45$. Our sequence X_2 extends that list one step further. The meaning of the word 'balanced' in this context is that the sum of the sequence is 1 or −1.

The sequences X_2 in the second and third example also have only 3 correlation values but this time these values are 49, 1 and −7 and so they are not optimal.

The block X_2 in the fourth example

$$X_2 = \{0, 1, 6, 7, 9, 10, 12, 14, 15, 16, 17, 18, 20, 25, 28, 29, 30, 32, 33, 37, 39, 43\}$$

has cardinality 22. Consequently, its binary sequence is not balanced. The correlation values of the sequence X_2, for the shifts in the range 0, 1, ..., 24 are:

$$49, 1, 1, 1, 1, 1, 1, -3, 1, -3, 1, 1, -3, 1, -3, -3, 1, -3, 1, 1, -3, -3, 1, 1, -3.$$

Thus the correlation values of X_2 occupy only three levels, 49, 1 and −3. Hence, this sequence is optimal but not balanced. The same is true for the fifth example.

The block X_2 in the last example

$$X_2 = \{1, 2, 3, 9, 12, 13, 15, 19, 22, 26, 27, 28, 31, 33, 34, 35, 36, 37, 39, 41, 42, 45, 46, 47, 49, 54, 56, 57, 58, 59\}$$

has cardinality 30 and so its binary sequence X_2 is balanced. The correlation values of the sequence X_2, for the shifts in the range 0, 1, ..., 30 are:

$$61, 1, -3, -3, -3, -3, 1, 1, 1, -3, 1, -3, 1, 1, 1, 1, -3, 1,1, -3, -3, -3, -3, 1, 1, -3, -3, 1, -3, -3, 1.$$

Hence, X_2 is a balanced optimal binary sequence of length 61.

■ ***Table 2.*** Three-level autocorrelation functions from propus difference families

(49; 22, 24, 24, 18; 39), $H = \{1, 18, 30\}$
[0, 1, 6, 7, 8, 9, 13, 16], [3, 7, 8, 9, 13, 16, 21, 29], [3, 6, 8, 12, 16, 29];
[0, 2, 7, 8, 13, 16, 19, 26], [2, 6, 9, 12, 16, 24, 26, 29], [1, 3, 7, 8, 19, 21];
[0, 1, 3, 4, 12, 13, 16, 24], [1, 6, 8, 13, 16, 19, 24, 29], [1, 4, 6, 16, 19, 26]

(49; 22, 22, 22, 19; 36), $H = \{1, 18, 30\}$
[0, 4, 6, 7, 9, 13, 19, 26], [0, 1, 6, 7, 9, 12, 16, 29], [0, 1, 6, 7, 16, 19, 21];
[0, 3, 4, 6, 7, 12, 19, 29], [0, 1, 2, 4, 7, 8, 13, 19], [0, 1, 3, 7, 8, 19, 21]

(61; 25, 30, 30, 25; 49), $H = \{1, 13, 47\}$
[0, 6, 8, 11, 16, 18, 23, 32, 36], [1, 2, 3, 9, 12, 22, 27, 28, 31, 36],
[0, 4, 7, 8, 9, 11, 16, 27, 28]

Table 3. Propus difference families with $v \equiv 1 \pmod 6$ a prime

(7; 3, 3, 3, 1; 3), $H = \{1, 2, 4\}$
[3], [3], [0]

(13; 6, 6, 6, 3; 8), $H = \{1, 3, 9\}$
[1, 4], [4, 7], [4]

(13; 6, 4, 4, 6; 7), $H = \{1, 3, 9\}$
[2, 7], [0, 4], [1, 7]

(19; 7, 9, 9, 6; 12), $H = \{1, 7, 11\}$
[0, 4, 10], [2, 4, 5], [1, 10]; [0, 1, 8], [1, 4, 10], [1, 8]

(19; 9, 7, 7, 7; 11), $H = \{1, 7, 11\}$
[2, 4, 8], [0, 5, 10], [0, 1, 8]

(31; 15, 15, 15, 10; 24), $H = \{1, 2, 4, 8, 16\}$
[3, 7, 15], [1, 3, 15], [1, 15]

(31; 15, 12, 12, 13; 21), $H = \{1, 5, 25\}$
[1, 2, 4, 8, 12], [2, 4, 8, 11], [0, 2, 4, 11, 12]

(31; 13, 13, 13, 12; 20), $H = \{1, 5, 25\}$
[0, 1, 2, 6, 12], [0, 2, 6, 8, 11], [2, 4, 12, 16];
[0, 2, 4, 11, 17], [0, 3, 8, 11, 17], [1, 4, 6, 11]

(37; 18, 15, 15, 15; 26), $H = \{1, 10, 26\}$
[2, 3, 5, 7, 17, 18], [1, 3, 7, 17, 21], [6, 7, 14, 17, 21]

(37; 16, 18, 18, 13; 28), $H = \{1, 10, 26\}$
[0, 1, 7, 14, 17, 21], [1, 2, 6, 9, 14, 21], [0, 1, 2, 11, 17]

(43; 21, 21, 21, 15; 35), $H = \{1, 4, 11, 16, 21, 35, 41\}$
[6, 7, 9], [1, 6, 9], [0, 3, 6]

(43; 19, 18, 18, 18; 30), $H = \{1, 6, 36\}$
[0, 2, 4, 9, 14, 19, 20], [2, 3, 10, 13, 20, 26],
[3, 4, 10, 13, 20, 21];
[0, 5, 7, 9, 10, 20, 21], [1, 3, 4, 10, 14, 21], [1, 3, 5, 7, 13, 21]

(43; 18, 21, 21, 16; 33), $H = \{1, 6, 36\}$
[1, 5, 7, 10, 13, 26], [2, 3, 5, 13, 14, 20, 26],
[0, 1, 7, 9, 19, 20]

(49; 22, 24, 24, 18; 39), $H = \{1, 18, 30\}$
[0, 1, 6, 7, 8, 9, 13, 16], [3, 7, 8, 9, 13, 16, 21, 29],
[3, 6, 8, 12, 16, 29];
[0, 2, 7, 8, 13, 16, 19, 26], [2, 6, 9, 12, 16, 24, 26, 29],
[1, 3, 7, 8, 19, 21];
[0, 1, 3, 4, 12, 13, 16, 24], [1, 6, 8, 13, 16, 19, 24, 29],
[1, 4, 6, 16, 19, 26]

(49; 22, 22, 22, 19; 36), $H = \{1, 18, 30\}$
[0, 4, 6, 7, 9, 13, 19, 26], [0, 1, 6, 7, 9, 12, 16, 29],
[0, 1, 6, 7, 16, 19, 21];
[0, 3, 4, 6, 7, 12, 19, 29], [0, 1, 2, 4, 7, 8, 13, 19],
[0, 1, 3, 7, 8, 19, 21]

(61; 30, 26, 26, 26; 47), $H = \{1, 9, 20, 34, 58\}$
[2, 6, 8, 10, 23, 26], [0, 1, 4, 5, 6, 8], [0, 3, 5, 6, 10, 12]

(61; 30, 25, 25, 30; 49), $H = \{1, 9, 20, 34, 58\}$
[4, 5, 10, 12, 13, 26], [1, 5, 6, 8, 26], [2, 4, 10, 12, 13, 26]

(61; 30, 25, 25, 30; 49), $H = \{1, 13, 47\}$
[1, 4, 6, 8, 9, 11, 14, 18, 23, 32],
[0, 6, 7, 8, 14, 22, 23, 27, 28], [1, 3, 4, 6, 7, 8, 9, 11, 28, 36]

(61; 25, 30, 30, 25; 49), $H = \{1, 13, 47\}$
[0, 3, 6, 7, 8, 18, 22, 23, 31],
[1, 2, 9, 14, 16, 18, 22, 23, 31, 36],
[0, 1, 8, 9, 18, 27, 28, 31, 36]

(61; 28, 28, 28, 24; 47), $H = \{1, 13, 47\}$
[0, 1, 3, 4, 14, 16, 18, 23, 31, 32],
[0, 3, 4, 9, 14, 16, 18, 22, 28, 32][1],
[2, 6, 8, 11, 18, 23, 28, 32]

(61; 28, 27, 27, 25; 49), $H = \{1, 13, 47\}$
[0, 1, 2, 4, 7, 8, 16, 28, 32, 36], [1, 2, 7, 8, 9, 12, 16, 27, 36],
[0, 2, 7, 12, 16, 27, 28, 31, 36]

(73; 36, 36, 36, 28; 63), $H = \{1, 8, 64\}$
[3, 5, 6, 11, 12, 21, 25, 26, 27, 33, 35, 43],
[3, 4, 9, 14, 17, 18, 21, 26, 34, 35, 42, 43],
[0, 1, 7, 13, 18, 21, 25, 33, 35, 42]

(73; 36, 31, 31, 33; 58), $H = \{1, 8, 64\}$
[3, 4, 5, 6, 13, 14, 25, 27, 33, 34, 36, 42],
[0, 2, 3, 5, 9, 18, 21, 26, 27, 35, 42],
[1, 5, 7, 11, 18, 21, 27, 33, 34, 42, 43]

(73; 31, 36, 36, 30; 60), $H = \{1, 8, 64\}$
[0, 2, 7, 11, 12, 13, 17, 18, 26, 35, 42],
[3, 5, 6, 12, 14, 18, 21, 26, 27, 33, 34, 35],
[1, 2, 5, 6, 9, 12, 26, 34, 36, 42]

(73; 31, 34, 34, 31; 55), $H = \{1, 8, 64\}$
[0, 1, 3, 5, 7, 9, 12, 17, 27, 33, 35],
[0, 1, 2, 5, 9, 11, 12, 18, 21, 27, 36, 43],
[0, 1, 3, 9, 18, 21, 26, 27, 35, 36, 42]

(73; 31, 36, 36, 30; 60), $H = \{1, 8, 64\}$
[0, 1, 4, 14, 17, 21, 26, 34, 36, 42, 43],
[2, 3, 4, 7, 12, 14, 25, 27, 35, 36, 42, 43],
[1, 4, 9, 11, 12, 13, 26, 35, 36, 42]

(73; 34, 33, 33, 30; 57), $H = \{1, 8, 64\}$
[0, 2, 3, 4, 6, 7, 9, 12, 13, 26, 27, 35], [1, 2, 5, 6, 7, 12, 17, 21, 25, 26, 35], [2, 4, 6, 7, 11, 17, 18, 25, 26, 36]

(157; 78, 78, 78, 66; 143), $H = \{1, 14, 16, 39, 46, 67, 75, 93, 99, 101, 108, 130, 153\}$
[2, 3, 7, 9, 11, 13], [3, 5, 6, 11, 13, 15], [0, 3, 4, 5, 7, 13]

(307; 153, 153, 153, 136; 288), $H = \{1, 9, 81, 115, 114, 105, 24, 216, 102, 304, 280, 64, 269, 272, 299, 235, 273\}$
[2, 3, 4, 5, 6, 7, 14, 20, 30], [4, 5, 7, 12, 14, 28, 30, 31, 49],
[2, 6, 7, 10, 21, 28, 30, 31]

---

[1]The binary sequence of this block has only four correlation values 61, 1, −3, and −11.

Propus Difference Families

In Table 3 we list propus difference families that we constructed by using the method of orbits. We only consider the cases where the subgroup H is nontrivial. If each of the k_i is the size of an H-invariant subset of $\mathbf{Z}_v$, then we say that the parameter set is *H-feasible* (or just *feasible* when H is known from the context). The case $v = 67$ is omitted as it was treated separately in section 3.

We can permute the X_i and replace any X_i with its complement. When listing the propus difference families it is convenient to introduce some additional restrictions on the propus parameter sets (1). We shall assume that each $k_i \leq v/2$, $k_2 = k_3$ and that $k_1 \geq k_4$.

In Table 3 below we first record the propus parameter set, and the subgroup H of the multiplicative group of the finite field $\mathbf{Z}_v$. Each of the three blocks X_1, $X_2 = X_3$, X_4 is a union of orbits of H acting on the additive group of $\mathbf{Z}_v$. In order to specify which orbits constitute a block we just list the representatives of these orbits. As representative we choose the smallest integer in the orbit. For instance, 0 is the unique representative of the trivial orbit {0}, and 1 is the representative of the orbit H.

When two or more difference families are listed for the same parameter set, they are separated by a semicolon. When $k_1 > k_4$ we have tried to find propus difference families with X_1 symmetric as well as those with X_4 symmetric. However, in some cases we did not succeed.

The last two families have the same parameter sets as the corresponding Turyn propus families of the same lengths but they are not equivalent to them.

Acknowledgements

The authors are indebted to an anonymous referee for his comments and to Tamara Balonina for converting the manuscript into the printing format. The research of the first author leading to these results has received funding from the Ministry of Education and Science of the Russian Federation according to the project part of the state funding assignment No 2.2200.2017/4.6. The second author acknowledges generous support by NSERC. His work was enabled in part by support provided by the Shared Hierarchical Academic Research Computing Network (www.sharcnet.ca) and Compute/Calcul Canada (www.computecanada.ca).

References

1. **Seberry J., and Balonin N. A.** Two Infinite Families of Symmetric Hadamard Matrices. *Australasian Journal of Combinatorics*, 2017, no. 69(3), pp. 349–357.
2. **Balonin N. A., Balonin Y. N., Đoković D. Ž., Karbovskiy D. A., Sergeev M. B.** Construction of Symmetric Hadamard Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2017, no. 5, pp. 2–11 (In Russian). doi:10.15217/issn1684-8853.2017.5.2
3. **Balonin N. A., Đoković D. Ž., and Karbovskiy D. A.** Construction of Symmetric Hadamard Matrices of Order 4v for $v = 47$; 73; 113. *Spec. Matrices*, 2018, vol. 6, pp. 11–22. doi:https://doi.org/10.1515/spma-2018–0002
4. **Di Mateo O., Đoković D. Ž., Kotsireas I. S.** Symmetric Hadamard Matrices of Order 116 and 172 Exist. *Special Matrices*, 2015, vol. 3, pp. 227–234.
5. **Đoković D. Ž., and Kotsireas I. S.** Goethals-Seidel Difference Families with Symmetric or Skew Base Blocks. *Math. Comput. Sci.* https:/doi.org/10.1007/S11786-018-0381-1
6. **Sawade K.** A Hadamard Matrix of Order 268. *Graphs and Combinatorics*, 1985, vol. 1, iss. 1, pp. 185–187.
7. **Đoković D. Ž.** Construction of Some New Hadamard Matrices. *Bull. Austral. Math. Soc.*, 1992, vol. 45, pp. 327–332.
8. **Craigen R., and Kharaghani H.** Hadamard Matrices and Hadamard Designs. In: *Handbook of Combinatorial Designs*. 2nd ed. C. J. Colbourn, J. H. Dinitz (eds.). Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall, 2007. Pp. 273–280.
9. **Arasu K. T.** Sequences and Arrays with Desirable Correlation Properties. *Information Security, Coding Theory and Related Combinatorics*, IOS Press, 2011, vol. 29, pp. 136–171. doi:10.3233/978-1-60750-663-8-136
10. **Đoković D. Ž., and Kotsireas I. S.** Algorithms for Difference Families in Finite Abelian Groups. *arXiv*: 1801.07627 [math.CO], 23 Jan 2018.
11. **Mertens S., and Bessenrodt C.** On the Ground States of the Bernasconi Model. *Journal of Physics A: Mathematical and General*, 1998, vol. 31, iss. 16, pp. 3731–3749. doi:10.1088/0305-4470/31/16/004

УДК 519.614
doi:10.31799/1684-8853-2018-4-2-8

Симметричные матрицы Адамара порядков 268, 412, 436 и 604

Балонин Н. А.[а], доктор техн. наук, профессор, korbendfs@mail.ru
Джокович Д. Ж.[б], PhD, профессор, djokovic@uwaterloo.ca
[а]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ
[б]Университет Ватерлоо, Ватерлоо, Онтарио, N2L 3G1, Канада

Цель: исследовать более полно, чем это было известно ранее, выделенные семейства симметричных матриц Адамара малых порядков, используя так называемую пропус-конструкцию. **Методы:** метод орбит поиска трех циклических блоков, составляющих матрицу Адамара типа пропус. Этот метод ускоряет классический поиск требуемых последовательностей с предварительной сортировкой их на непересекающиеся сомножества потенциальных решений с помощью хэш-функции. **Результаты:** основной результат состоит в том, что впервые удалось сконструировать симметричные матрицы Адамара порядков 268, 412, 436 и 604. Необходимые разностные семейства сконструированы посредством выделения тех из них, которые содержат заданный нетривиальный множитель. Получено и классифицировано в таблицы обширное множество новых симметричных матриц Адамара, отличающихся между собой индивидуальными наборами параметров. **Практическое значение:** матрицы Адамара имеют непосредственное практическое значение для задач помехоустойчивого кодирования, сжатия и маскирования видеоинформации. Программное обеспечение нахождения симметричных матриц Адамара и библиотека найденных матриц используются в математической сети Интернет с исполняемыми онлайн алгоритмами.

Ключевые слова — пропус-конструкция, разностные семейства, симметричные матрицы Адамара, оптимальные бинарные последовательности.

Цитирование: Balonin N. A., Đoković D. Ž. Symmetric Hadamard Matrices of Orders 268, 412, 436 and 604 // Информационно-управляющие системы. 2018. № 4. С. 2–8. doi:10.31799/1684-8853-2018-4-2-8
Citation: Balonin N. A., Đoković D. Ž. Symmetric Hadamard Matrices of Orders 268, 412, 436 and 604. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 4, pp. 2–8. doi:10.31799/1684-8853-2018-4-2-8

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию. Рукописи не возвращаются.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.