UDC 519.614
doi:10.31799/1684-8853-2019-5-2-9

Hadamard matrices from Goethals — Seidel difference families with a repeated block

***L. V. Abuzin*[a]**, *Master Student, orcid.org/0000-0003-0759-7930*
***N. A. Balonin*[a]**, *Dr. Sc., Professor, orcid.org/0000-0001-7338-4920*
***D. Ž. Đoković*[b]**, *Dr. Sc., Distinguished Professor Emeritus, orcid.org/0000-0002-0176-2395, djokovic@uwaterloo.ca*
***I. S. Kotsireas*[c]**, *Dr. Sc., Professor, orcid.org/0000-0003-2126-8383, ikotsire@wlu.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
[c]Wilfrid Laurier University, Department of Physics & Computer Science, Waterloo, Ontario, N2L 3C5, Canada

Purpose: *To construct Hadamard matrices by using Goethals — Seidel difference families having a repeated block, generalizing the so called propus construction. In particular we construct the first examples of symmetric Hadamard matrices of order 236.* ***Methods:*** *The main ingredient of the propus construction is a difference family in a finite abelian group of order v consisting of four blocks (X_1, X_2, X_3, X_4) where X_1 is symmetric and $X_2 = X_3$. The parameters (v; k_1, k_2, k_3, k_4; λ) of such family must satisfy the additional condition $\sum k_i = \lambda + v$. We modify this construction by imposing different symmetry conditions on some of the blocks and construct many examples of Hadamard matrices of this kind. In this paper we work with the cyclic group Z_v of order v. For larger values of v we build the blocks X_i by using the orbits of a suitable small cyclic subgroup of the automorphism group of Z_v.* ***Results:*** *We continue the systematic search for symmetric Hadamard matrices of order $4v$ by using the propus construction. Such searches were carried out previously for odd $v \leq 51$. We extend it to cover the case $v = 53$. Moreover we construct the first examples of symmetric Hadamard matrices of order 236. A wide collection of symmetric and skew-symmetric Hadamard matrices was obtained and the corresponding difference families tabulated by using the symmetry properties of their blocks.* ***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 — *symmetric and skew-Hadamard matrices, Goethals — Seidel array, propus array, cyclic difference families.*

For citation: Abuzin L. V., Balonin N. A., Đoković D. Ž., Kotsireas I. S. Hadamard matrices from Goethals — Seidel difference families with a repeated block. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 5, pp. 2–9. doi:10.31799/1684-8853-2019-5-2-9

Introduction

A *Hadamard matrix* is a $\{\pm 1\}$-matrix $\mathbf{H}$ of order m whose rows are mutually orthogonal, i. e. $\mathbf{H}\mathbf{H}^{\mathrm{T}} = m\mathbf{I}_m$, where $\mathbf{I}_m$ is the identity matrix of order m and $\mathbf{T}$ denotes the transposition. We say that $\mathbf{H}$ is a *skew-Hadamard matrix* if also $\mathbf{H} + \mathbf{H}^{\mathrm{T}} = 2\mathbf{I}_m$. The smallest orders $4v$ for which skew-Hadamard matrices have not been constructed is 276. Since the size of a Hadamard, skew-Hadamard or symmetric Hadamard matrix can always be doubled, while preserving its type, we are interested mainly in the case where these matrices have order $4v$ with v odd.

One of the powerful constructions of Hadamard matrices is based on the well-known Goethals — Seidel (GS) array. For this construction we need a difference family (X_1, X_2, X_3, X_4) consisting of four subsets X_i of a finite abelian group G of order v. In addition to the basic condition $\sum k_i(k_i - 1) = \lambda(v - 1)$, $k_i = |X_i|$, which the parameters (v; k_1, k_2, k_3, k_4; λ) of all difference families must satisfy, it is also required that $\sum k_i = \lambda + v$. Following [1], we shall refer to the parameter sets and the difference families satisfying this additional condition as *GS-parameter sets* and *GS-difference families*, respectively. By eliminating λ from these two conditions, one obtains that

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

If v is odd and one of the blocks X_i, say X_1, is skew then we have $k_1 = (v - 1)/2$. The meaning of X_1 being *skew* is that G is a disjoint union of X_1, $-X_1$ and $\{0\}$. Given such a difference family we can construct skew-Hadamard matrix by plugging the matrices A_i associated with the blocks X_i into the GS-array. In the case when $G = \mathbf{Z}_v$, a cyclic group of order v, the $\mathbf{A}_i$ are circulant matrices. For instance the first row of $\mathbf{A}_1$ is the $\{\pm 1\}$-sequence (a_0, a_1, … , a_{v-1}) where $a_i = -1$ if and only if $i \in X_1$.

Constructing GS-difference families may be a very hard computational problem. For instance no such family is known when $v = 167$. However, the problem can be simplified to some extent by selecting a suitable subclass of GS-difference families which possess more structure. One of such subclasses, known as *propus difference families* has been introduced recently [2] in order to construct symmetric Hadamard matrices. A GS-difference family (X_1, X_2, X_3, X_4) is a *propus difference family* if one of the blocks is repeated, say $X_2 = X_3$, and at least one of the other two blocks, say X_1, is symmetric. Recall that X_1 is *symmetric* if $-X_1 = X_1$.

In this paper we focus on a larger subclass of GS-difference families, namely the families having one repeated block. We shall assume that $X_2 = X_3$, and consequently $k_2 = k_3$. For convenience we may also assume that all $k_i \leq v/2$. This is justified because replacing a block with its complement in $\mathbf{Z}_v$ preserves the property of being a GS-difference family. One can impose further additional symmetry restrictions on some of the blocks in order to make the search easier. For instance we may ask that the block X_1 be symmetric or skew, or that the repeated block X_2 be symmetric or skew.

The existence question of propus difference families for odd sizes $v \leq 51$ and all relevant parameter sets was addressed and resolved in the papers [3, 4]. The cases where all four k_i's are equal are exceptional and no propus difference families are known except when the k_i's are equal to 3 [4]. In the first section we extend these results to the case $v = 53$. The cases $v = 55$ and $v = 57$ have not been explored so far systematically. However, in both cases one propus difference family is known.

In the case $v = 59$ we have constructed six propus difference families. One of them has the parameter set (59; 23, 28, 28, 26; 46) and the other five nonnequivalent solutions have the parameter set (59; 27, 25, 25, 26; 44). These solutions are presented in the next section. They are important because they provide the first examples of symmetric Hadamard matrices of order 236. The smallest order $4v$ for which symmetric Hadamard matrices are not yet known is now 260 (see [2]).

After that, in the subsequent three sections we consider the cases where the block X_1 is skew, X_2 is skew, X_2 is symmetric, respectively.

Propus difference families for $v = 53$

The class of cyclic propus difference families contains an infinite series to which, for simplicity, we refer as the *X-series*. It is based on the main result of the paper [6] of Xia M., Xia T., Seberry J., and Wu J. These families exist when $4v - 1 \equiv 3 \pmod 8$ is a prime power. The four circulants $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3 = \mathbf{A}_2$, $\mathbf{A}_4$ associated with blocks X_1, X_2, $X_3 = X_2$, X_4 of the X-series can be plugged into the so called propus array, see (2), to obtain a symmetric Hadamard matrix of order $4v$ [2, 3, 7]. On the other hand, after a suitable permutation of the blocks, they can be also plugged into the GS-array to obtain a skew-Hadamard matrix of the same order.

For $v = 53$ there are three propus parameter sets, but there are six essentially different choices for selecting the symmetric and the repeated blocks. Below we list the solutions (i. e., propus difference families) for each of these six choices. In all cases the block X_1 is symmetric and $X_2 = X_3$, and so we list only the three blocks X_1, X_2, X_4 in that order. The first solution belongs to the X-series.

(53; 23, 22, 22, 26; 40)
{0, ±1, ±3, ±9, ±10, ±12, ±14, ±16, ±17, ±20, ±23, ±25}
{0, 1, 2, 3, 9, 11, 18, 21, 24, 25, 29, 33, 34, 35, 36, 41, 44, 46, 48, 49, 50, 52}
{1, 5, 6, 10, 11, 12, 15, 18, 22, 27, 28, 29, 30, 32, 33, 34, 36, 37, 39, 40, 44, 45, 46, 49, 50, 51}

(53; 26, 22, 22, 23; 40)
{±1, ±7, ±9, ±10, ±12, ±14, ±17, ±18, ±19, ±20, ±21, ±24, ±25}
{7, 11, 13, 14, 16, 18, 19, 20, 24, 26, 27, 28, 30, 31, 36, 41, 42, 44, 45, 48, 50, 51}
{0, 5, 9, 11, 12, 13, 18, 22, 23, 25, 31, 32, 33, 36, 37, 38, 41, 43, 45, 48, 49, 50, 52}

(53; 24, 25, 25, 20; 41)
{±4, ±7, ±9, ±10, ±13, ±14, ±15, ±16, ±19, ±22, ±24, ±26}
{1, 6, 7, 8, 9, 16, 17, 21, 22, 23, 25, 27, 30, 33, 34, 35, 37, 38, 39, 40, 41, 44, 48, 50, 52}
{1, 2, 9, 10, 13, 17, 18, 22, 23, 29, 36, 39, 42, 43, 45, 47, 48, 50, 51, 52}

(53; 20, 25, 25, 24; 41)
{±2, ±4, ±6, ±10, ±13, ±16, ±19, ±20, ±21, ±23}
{0, 1, 3, 4, 5, 9, 15, 16, 17, 18, 23, 24, 25, 28, 31, 33, 36, 37, 42, 45, 46, 47, 49, 51, 52}
{1, 3, 4, 8, 11, 12, 14, 15, 16, 24, 27, 29, 34, 39, 40, 42, 43, 45, 46, 47, 49, 50, 51, 52}

(53; 24, 22, 22, 24; 39)
{±2, ±6, ±8, ±10, ±11, ±12, ±14, ±15, ±17, ±21, ±22, ±24}
{0, 3, 10, 11, 19, 20, 21, 22, 23, 24, 26, 28, 31, 34, 35, 37, 39, 40, 41, 45, 46, 50}
{6, 7, 10, 11, 12, 14, 16, 17, 19, 22, 24, 27, 28, 31, 36, 37, 39, 43, 44, 45, 49, 50, 51, 52}

(53; 22, 24, 24, 22; 39)
{±7, ±8, ±10, ±12, ±14, ±15, ±17, ±18, ±23, ±24, ±26}
{1, 2, 3, 8, 10, 12, 13, 14, 15, 16, 17, 19, 22, 23, 29, 31, 32, 33, 37, 39, 42, 43, 47, 50}
{2, 6, 7, 12, 14, 19, 23, 25, 26, 29, 31, 34, 37, 38, 39, 41, 42, 46, 49, 50, 51, 52}

Six symmetric Hadamard matrices of order 236

As $236 = 4 \cdot 59$ we set $v = 59$. Define the subsets X_1, X_2, X_3, X_4 of $\mathbf{Z}_v$ by:

$X_1 = \{0, \pm1, \pm4, \pm5, \pm7, \pm8, \pm11, \pm14, \pm20, \pm25, \pm28, \pm29\}$,
$X_2 = X_3 = \{4, 5, 7, 11, 12, 16, 17, 24, 25, 26, 27, 28, 29, 33, 34, 37, 39, 40, 42,43, 44, 45, 47, 49, 51, 53, 56, 58\}$,
$X_4 = \{2, 3, 10, 12, 13, 14, 16, 18, 19, 26, 28, 29, 36, 38, 39, 40, 42, 44, 46, 47, 49,50, 53, 54, 55, 57\}$.

One can easily verify that these four blocks form a difference family in $\mathbf{Z}_v$ with parameters (59; 23, 28, 28, 26; 46). The four circulants $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, $\mathbf{A}_4$ of order 59 associated with the blocks X_1, X_2, X_3, X_4 respectively can be plugged into the propus array

$$\begin{bmatrix} -\mathbf{A}_1 & \mathbf{A}_2\mathbf{R} & \mathbf{A}_3\mathbf{R} & \mathbf{A}_4\mathbf{R} \\ \mathbf{A}_3\mathbf{R} & \mathbf{R}\mathbf{A}_4 & \mathbf{A}_1 & -\mathbf{R}\mathbf{A}_2 \\ \mathbf{A}_2\mathbf{R} & \mathbf{A}_1 & -\mathbf{R}\mathbf{A}_4 & \mathbf{R}\mathbf{A}_3 \\ \mathbf{A}_4\mathbf{R} & -\mathbf{R}\mathbf{A}_3 & \mathbf{R}\mathbf{A}_2 & \mathbf{A}_1 \end{bmatrix}, \tag{2}$$

where

$$\mathbf{R} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & & 1 & 0 \\ \vdots & & & & \\ 0 & 1 & & 0 & 0 \\ 1 & 0 & & 0 & 0 \end{bmatrix},$$

to obtain the desired symmetric Hadamard matrix of order 236.

For the parameter set (59; 27, 25, 25, 26; 44) we have constructed the following five nonequivalent difference families. As in the previous section we list only the blocks X_1, X_2, X_4. In each case the block X_1 is obviously symmetric.

{0, ±2, ±4, ±7, ±8, ±12, ±13, ±15, ±16, ±17, ±18, ±20, ±23, ±29}
{1, 2, 4, 5, 12, 13, 17, 19, 20, 21, 22, 23, 26, 27, 31, 35, 37, 38, 40, 44, 47, 49, 50, 55, 57}
{3, 7, 12, 13, 14, 16, 18, 19, 20, 22, 23, 24, 25, 26, 31, 32, 33, 34, 36, 38, 43, 45, 46, 50, 51, 53}

{0, ±2, ±4, ±5, ±6, ±7, ±9, ±10, ±11, ±12, ±20, ±21, ±26, ±29}
{1, 4, 5, 8, 9, 11, 15, 18, 19, 20, 21, 23, 26, 29, 31, 35, 36, 38, 41, 42, 43, 44, 49, 51, 55}
{1, 2, 4, 5, 7, 9, 11, 13, 14, 15, 21, 23, 28, 32, 33, 34, 35, 36, 37, 39, 44, 45, 49, 50, 53, 57}

{0, ±1, ±5, ±8, ±11, ±12, ±13, ±17, ±21, ±22, ±23, ±27, ±28, ±29}
{1, 2, 3, 5, 6, 9, 10, 12, 14, 15, 17, 20, 27, 30, 34, 41, 42, 43, 45, 46, 47, 48, 50, 52, 54}
{2, 4, 5, 6, 8, 12, 15, 17, 20, 23, 25, 28, 29, 31, 35, 40, 41, 42, 43, 44, 49, 51, 52, 54, 57, 58}

{0, ±4, ±6, ±7, ±10, ±12, ±13, ±15, ±16, ±18, ±20, ±25, ±26, ±29}
{2, 4, 6, 10, 11, 15, 16, 17, 18, 19, 21, 26, 27, 28, 29, 30, 33, 35, 36, 42, 53, 54, 56, 57, 58}
{3, 6, 7, 8, 9, 13, 18, 19, 21, 23, 24, 26, 28, 29, 33, 34, 36, 37, 41, 43, 47, 50, 51, 54, 56, 58}

$\{0, \pm1, \pm2, \pm7, \pm12, \pm17, \pm18, \pm19, \pm21, \pm23, \pm25, \pm26, \pm27, \pm29\}$
$\{2, 5, 7, 13, 14, 15, 17, 23, 24, 25, 28, 29, 32, 35, 39, 41, 44, 45, 46, 48, 49, 51, 52, 53, 58\}$
$\{1, 2, 4, 6, 7, 15, 20, 21, 23, 25, 31, 32, 34, 35, 37, 38, 39, 43, 46, 47, 48, 50, 52, 53, 57, 58\}$

As in the first example of this section, these propus difference families give five symmetric Hadamard matrices of order 236.

Difference families with X_1 skew

In the case when X_1 is skew v must be odd, $k_1 = (v - 1)/2$ and the parameter set will be written as

$$(v;\ k_1 = (v - 1)/2,\ k_2,\ k_3 = k_2,\ k_4;\ \lambda). \tag{3}$$

Further we have

$$2k_2 + k_4 = \lambda + (v + 1)/2 \tag{4}$$

and

$$(v - 2k_4)^2 + 2(v - 2k_2)^2 = 4v - 1. \tag{5}$$

Without any loss of generality, we impose the following additional restriction:

$$v/2 \geq k_2,\ k_4. \tag{6}$$

We conjecture that for each parameter set (3) there exists at least one difference family (X_1, X_2, $X_3 = X_2$, X_4) in $\mathbf{Z}_v$ with these parameters and with X_1 skew.

There exist positive odd integers v for which there is no parameter set of the form (3). For instance, this is the case for $v = 9, 23, 29, 39, 49, 51, 59$. More precisely, it was proved by Gauss [8] that the Diophantine equation $a^2 + 2b^2 = m$, where m is a positive integer, has a solution with a and b relatively prime if and only if -2 is a square in $\mathbf{Z}_m$.

For odd $v < 50$, we list in Tables 1–3 all parameter sets (3) which satisfy the conditions (4) and (6). There are in total 27 such parameter sets (12 of them arise from the X-series). For each of them we have recorded in Tables 1–3 at least one difference family with X_1 skew and $X_2 = X_3$. Thus our conjecture has been verified for $v < 50$. The block X_4 is symmetric in Table 1, skew in Table 2, and neither symmetric nor skew in Table 3. In Table 1 the symbol X indicates that the parameter set belongs to the X-series.

In some cases we build the base blocks X_i from the orbits of a subgroup, H, of the group of the invertible elements, $\mathbf{Z}_v^*$, of the ring $\mathbf{Z}_v$. In such cases our choice for H is always a cyclic subgroup $\langle s \rangle$, with generator s, and we show it below the corresponding parameter set. In these cases, instead of listing all elements of the X_i we list (in square brackets) only the representatives of the orbits of H contained in X_i.

One of the blocks of difference families in the X-series is symmetric and we have endevoured to find such solutions in other cases as well. In some cases, exaustive computer searches showed that such solutions do not exist.

The second solution given above for the case $v = 7$ gives a positive answer to a question raised in [6, p. 503]. Indeed the polynomials

$$f_1(\zeta) = \zeta - \zeta^2 - \zeta^3 + \zeta^4 + \zeta^5 - \zeta^6;$$
$$f_2(\zeta) = 1 + \zeta + \zeta^2 - \zeta^3 - \zeta^4 + \zeta^5 + \zeta^6;$$
$$f_3(\zeta) = -1 + \zeta - \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6;$$
$$f_4(\zeta) = f_3(\zeta)$$

satisfy the conditions (16) and (17) of the cited paper [6] as well as

$$f(1)^2 = 0,\ f_2(1)^2 = f_3(1)^2 = f_4(1)^2 = 9.$$

If both $X_2 = X_3$ and X_4 are skew then the parameter set must have the form

$$(v = 2s^2 + 2s + 1;\ s^2 + s,\ s^2,\ s^2,\ s^2 + s;\ \lambda = 2s^2 - 1);\ s = 1, 2, 3, \ldots$$

■ ***Table 1.*** X_1 skew, $X_2 = X_3$, and X_4 symmetric

(3; 1, 1, 1, 0; 0)	X	{1} {0} ∅
(5; 2, 1, 1, 2; 1)	X	{1, 2} {0} {±2}
(7; 3, 3, 3, 1; 3)	X	{1, 2, 4} {0, 1, 3} {0}
(7; 3, 2, 2, 2; 2)		{2, 3, 6} {0, 2} {±3}
(11; 5, 4, 4, 3; 5)	X	{1, 2, 4, 6, 8} {0, 1, 2, 5} {0, ±3}
(13; 6, 6, 6, 3; 8)		{1, 2, 3, 4, 7, 8} {0, 1, 2, 6, 9, 11} {0, ±3}
(13; 6, 4, 4, 6; 7)		{1, 2, 3, 5, 6, 9} {0, 1, 3, 9} {±1, ±3, ±4}
(15; 7, 5, 5, 6; 8)	X	{2, 4, 5, 6, 7, 12, 14} {2, 5, 6, 9, 11} {±2, ±6, ±7}
(17; 8, 7, 7, 5; 10)	X	{1, 2, 3, 5, 9, 10, 11, 13} {0, 3, 7, 9, 12, 13, 14} {0, ±2, ±3}
(19; 9, 7, 7, 7; 11)		{1, 2, 3, 7, 10, 11, 13, 14, 15} {4, 5, 9, 11, 13, 14, 17} {0, ±2, ±3, ±5}
(21; 10, 10, 10, 6; 15)	X	{1, 3, 4, 6, 7, 8, 9, 10, 16, 19} {0, 4, 5, 7, 8, 9, 11, 13, 18, 19} {±3, ±4, ±8}
(25; 12, 11, 11, 8; 17)		{1, 2, 3, 5, 7, 8, 10, 11, 12, 16, 19, 21} {1, 3, 9, 10, 11, 13, 14, 15, 16, 20, 23} {±1, ±5, ±8, ±9}
(27; 13, 10, 10, 12; 18)	X	{2, 3, 5, 6, 8, 13, 15, 16, 17, 18, 20, 23, 26} {3, 4, 9, 11, 14, 18, 20, 22, 23, 24} {±3, ±7, ±8, ±11, ±12, ±13}
(31; 15, 12, 12, 13; 21) ⟨5⟩		[6, 8, 11, 12, 16] [2, 8, 16, 17] [0, 3, 4, 11, 16]
(33; 16, 14, 14, 12; 23)	X	{1, 4, 8, 12, 14, 17, 18, 20, 22, 23, 24, 26, 27, 28, 30, 31} {3, 5, 6, 9, 10, 11, 12, 14, 17, 22, 23, 24, 27, 32} {±3, ±4, ±5, ±12, ±14, ±16}
(35; 17, 16, 16, 12; 26)	X	{2, 3, 5, 7, 8, 9, 10, 11, 13, 14, 15, 18, 19, 23, 29, 31, 34} {0, 1, 3, 5, 8, 9, 16, 17, 18, 19, 23, 25, 28, 30, 31, 34} {±5, ±6, ±7, ±9, ±12, ±16}
(41; 20, 16, 16, 20; 31)		{1, 4, 6, 7, 9, 11, 13, 14, 18, 19, 20, 24, 25, 26, 29, 31, 33, 36, 38, 39} {4, 6, 9, 12, 13, 14, 17, 18, 25, 26, 28, 29, 30, 32, 35, 39} {5, 7 ,8, 9, 13, 15, 16, 17, 18, 19, 22, 23, 24, 25, 26, 28, 32, 33, 34, 36}
(45; 22, 19, 19, 18; 33)	X	{3, 4, 8, 11, 13, 14, 15, 17, 18, 20, 21, 23, 26, 29, 33, 35, 36, 38, 39, 40, 43, 44} {2, 4, 6, 7, 8, 9, 12, 15, 18, 19, 20, 22, 23, 24, 26, 31, 32, 33, 41} {±1, ±4, ±5, ±6, ±12, ±13, ±16, ±18, ±20}

■ ***Table 2.*** X_1 and X_4 skew and $X_2 = X_3$

s	v	Subgroup	$X_1\ X_2\ X_4$
1	5	⟨1⟩	{1, 2} {0} {1, 3}
2	13	⟨3⟩	[2, 4] [0, 2] [1, 2]
3	25	⟨1⟩	{1, 2, 3, 5, 6, 7, 12, 14, 15, 16, 17, 21} {1, 5, 9, 12, 13, 15, 18, 19, 21} {2, 3, 4, 5, 7, 9, 10, 11, 12, 17, 19, 24}
4	41	⟨10⟩	[1, 2, 11, 15] [0, 1, 4, 11] [1, 5, 6, 11]
5	61	⟨9⟩	[1, 2, 4, 10, 13, 23] [1, 5, 8, 12, 13] [1, 4, 6, 8, 13, 26]
6	85	?	?
7	113	?	?

■ ***Table 3.*** X_1 skew and $X_2 = X_3$

(25; 12, 10, 10, 9; 16)	{1, 3, 4, 5, 7, 8, 9, 13, 14, 15, 19, 23} {1, 3, 5, 8, 10, 11, 13, 14, 21, 22}
	{5, 6, 7, 8, 11, 14, 15, 18, 20}

(31; 15, 15, 15, 10; 24) ⟨5⟩	[2, 6, 8, 11, 16] [1, 2, 3, 4, 6] [0, 2, 4, 11]
(37; 18, 15, 15, 15; 26) ⟨10⟩	[3, 6, 11, 17, 18, 21] [1, 3, 11, 14, 18] [6, 7, 11, 14, 17]
(43; 21, 21, 21, 15; 35) ⟨6⟩	[1, 3, 4, 13, 14, 20, 26] [1, 2, 5, 10, 13, 19, 20] [1, 14, 19, 20, 26]
(43; 21, 19, 19, 16; 32) ⟨6⟩	[1, 5, 9, 10, 14, 19, 21] [0, 1, 7, 9, 10, 13, 19] [0, 3, 4, 7, 13, 20]

(43; 21, 17, 17, 20; 32)	{1, 4, 5, 6, 7, 11, 14, 15, 19, 21, 23, 25, 26, 27, 30, 31, 33, 34, 35, 40, 41}
	{2, 4, 7, 9, 10, 13, 15, 20, 21, 22, 24, 25, 29, 32, 34, 35, 41}
	{0, 5, 6, 8, 10, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 30, 34, 35, 41}

(47; 23, 22, 22, 17; 37)	{1, 4, 5, 9, 10, 12, 17, 18, 19, 21, 22, 24, 27, 31, 32, 33, 34, 36, 39, 40, 41, 44, 45}
	{4, 5, 6, 9, 12, 20, 21, 22, 23, 25, 28, 30, 31, 32, 34, 36, 38, 40, 41, 42, 45, 46}
	{0, 2, 4, 5, 9, 16, 18, 19, 21, 22, 23, 24, 25, 28, 31, 38, 43}

(47; 23, 19, 19, 21; 35)	{2, 3, 4, 6, 7, 9, 14, 17, 18, 19, 23, 25, 26, 27, 31, 32, 34, 35, 36, 37, 39, 42, 46}
	{0, 2, 4, 12, 14, 17, 20, 21, 25, 27, 28, 34, 37, 38, 39, 40, 43, 45, 46}
	{1, 3, 4, 5, 7, 8, 10, 11, 12, 14, 19, 20, 24, 25, 34, 35, 39, 40, 41, 43, 45}

For the first five values of s, difference families with these parameters exist. They are shown in Table 2.

Table 3 covers the cases where we could not find solutions with X_4 symmetric or skew.

Difference families with $X_2 = X_3$ skew

We list here the difference families with the repeated block $X_2 = X_3$ skew. A necessary condition for the existence of such families is that $2v - 1$ must be a sum of two squares. This follows from the equation (1). We assume that $k_1 \geq k_4$. In the second column we indicate the symmetry types of the blocks X_1, X_2 and X_4. The letter "s" means that the block is symmetric and "k" means that it is skew. The letter "x" means that, in the given solution, the corresponding block is neither symmetric nor skew. The question mark indicates that the existence question remains undecided.

If v is a prime number $\equiv 3 \pmod 4$ and if there exists a D-optimal design (X_1, X_4) with parameters $(v;\ k_1,\ k_4;\ \lambda = k_1 + k_4 - (v - 1)/2)$ then we can take $X_2 = X_3$ to be the Legendre difference set to obtain the desired difference family (X_1, X_2, X_3, X_4). For an example see the difference family for (43; 21, 21, 21, 15; 35) in Table 4. Solutions where (X_1, X_4) is not a

■ ***Table 4.*** X_2 skew and $X_2 = X_3$

(3; 1, 1, 1, 0; 0)	(kks)	{1} {1} $\emptyset$
(5; 1, 2, 2, 1; 1)	(xkx)	No
(7; 3, 3, 3, 1; 3)	(kks)	{3, 5, 6} {3, 5, 6} {0}
(9; 3, 4, 4, 2; 4)	(xkx)	No

(13; 6, 6, 6, 3; 8)	(skx)	{±2, ±5, ±6} {2, 4, 5, 6, 10, 12} {0, 1, 4}
		{4, 7, 8, 10, 11, 12} {1, 3, 7, 8, 9, 11} {0, 3, 12}

(13; 4, 6, 6, 4; 7)	(skx)	{±1, ±2} {1, 3, 7, 8, 9, 11} {0, 1, 6, 10}
(15; 6, 7, 7, 4; 9)	(xkx)	No

■ ***Table 4 (compl.)***

(19; 7, 9, 9, 6; 12)	(xks)	{0, 5, 8, 10, 11, 12, 14} {2, 3, 8, 10, 12, 13, 14, 15, 18}
		{±1, ±7, ±8}

(21; 10, 10, 10, 6; 15)	(xkx)	{1, 3, 7, 9, 13, 14, 15, 16, 19, 20} {1, 7, 8, 10, 12, 15, 16, 17, 18, 19}
		{0, 4, 7, 12, 17, 20}

(23; 10, 11, 11, 7; 16)	(xkx)	{0, 1, 4, 5, 6, 8, 11, 12, 14, 22} {5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22}
		{7, 8, 11, 15, 17, 20, 22}

(25; 9, 12, 12, 9; 17)	(xkx)	{4, 7, 9, 11, 15, 16, 17, 21, 22} {1, 2, 3, 4, 5, 7, 9, 10, 13, 14, 17, 19}
		{1, 4, 7, 8, 10, 15, 18, 19, 24}

(27; 11, 13, 13, 9; 19)	(xkx)	{0, 1, 4, 8, 10, 13, 14, 15, 21, 23, 25}
		{4, 5, 8, 13, 15, 16, 17, 18, 20, 21, 24, 25, 26}
		{0, 2, 8, 11, 13, 14, 15, 17, 20}

(31; 15, 15, 15, 10; 24) ⟨5⟩	(kkx)	[1, 3, 8, 11, 12] [1, 2, 3, 8, 11] [0, 4, 11, 17]
(33; 15, 16, 16, 11; 25)	(xkx)	No
(33; 13, 16, 16, 12; 24)	(xkx)	No
(37; 16, 18, 18, 13; 28)	(xkx)	?
(41; 16, 20, 20, 16; 31)	(xkx)	?

(43; 21, 21, 21, 15; 35)	(xkx)	{0, 1, 2, 3, 4, 5, 6, 7, 11, 12, 13, 14, 17, 20, 24, 25, 28, 30, 31, 34, 39}
		{2, 3, 5, 7, 8, 12, 18, 19, 20, 22, 26, 27, 28, 29, 30, 32, 33, 34, 37, 39, 42}
		{0, 2, 3, 4, 7, 9, 12, 14, 16, 22, 24, 30, 31, 34, 39}

(43; 18, 21, 21, 16; 33) ⟨6⟩	(xkx)	[2, 7, 10, 14, 20, 26] [1, 4, 9, 10, 13, 14, 21] [0, 4, 13, 14, 20, 26]
(45; 21, 22, 22, 16; 36)	(xkx)	?
(49; 22, 24, 24, 18; 39)	(xkx)	?

DO-design may also exist, as an example see the difference family for (43; 18, 21, 21, 16; 33) in Table 4.

Difference families with $X_2 = X_3$ symmetric

The difference families (X_1, X_2, X_3, X_4) in $\mathbf{Z}_v$, v odd, associated with the Williamson matrices in the well-known Turyn series [9] have the following properties. After a suitable permutation of the X_i, we have $X_1 = \{0\} \cup X_4$, $X_2 = X_3$ and all X_i are symmetric. They exist whenever $q = 2v - 1 \equiv 1 \pmod 4$ is a prime power. Apart from this series, for odd $v < 30$ we found only three additional cyclic GS-difference families (X_1, X_2, X_3, X_4) having a repeated block $X_2 = X_3$ which is symmetric (see Table 5).

■ ***Table 5.*** X_2 symmetric and $X_2 = X_3$

(13; 6, 6, 6, 3; 8)	(xsx)	{0, 2, 3, 6, 11, 12} {1, ±3, ±4}
		{0, 1, 4}

(13; 4, 6, 6, 4; 7)	(ssx)	{±3, ±5} {±2, ±5, ±6} {0, 1, 5, 7}

(23; 10, 11, 11, 7; 16)	(xsx)	{0, 1, 3, 5, 8, 12, 14, 15, 17, 20}
		{0, ±1, ±2, ±4, ±8, ±9}
		{0, 2, 4, 5, 9, 12, 13}

Acknowledgements

The research of the second 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 research of the last two authors was enabled in part by SHARCNET (http://www.sharcnet.ca) and Compute Canada (http://computecanada.ca).

References

1. Đoković D. Ž., Kotsireas I. S. Goethals — Seidel difference families with symmetric or skew base blocks. *Mathematics in Computer Science*, 2018, vol. 12(4), pp. 373–388.
2. Seberry J., Balonin N. A. The propus construction for symmetric Hadamard matrices. *Australasian Journal of Combinatorics*, 2017, no. 69(3), pp. 349–357.
3. 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. doi:10.15217/issn1684-8853.2017.5.2
4. Balonin N. A., Đoković D. Ž., Karbovskiy D. A. Construction of symmetric Hadamard matrices of order $4v$ for $v=47$, 73, 113. *Spec. Matrices*, 2018, vol. 6, iss. 1, pp. 11–22.
5. 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
6. Xia M., Xia T., Seberry J. and Wu J. An infinite series of Goethals — Seidel arrays. *Discrete Applied Mathematics*, 2005, no. 145, pp. 498–504.
7. Di Mateo O., Đoković D. Ž., Kotsireas I. S. Symmetric Hadamard matrices of order 116 and 172 exist. *Spec. Matrices*, 2015, no. 3, pp. 227–234.
8. Gauss Carl Friedrich. *Trudy po teorii chisel* [Proceedings in Number Theory]. Ed. of I. M. Vinogradov, Moscow, AN SSSR Publ., 1959. 979 p. (In Russian).
9. Turyn R. J. An infinite class of Williamson matrices. *Journal Combinatorial Theory*, Ser. A, 1972, no. 12, pp. 319–321.

УДК 519.614
doi:10.31799/1684-8853-2019-5-2-9

Матрицы Адамара разностного семейства Гетхальса — Зейделя с повторяющимся блоком

Л. В. Абузин[а], магистрант, orcid.org/0000-0003-0759-7930
Н. А. Балонин[а], доктор наук, профессор, orcid.org/0000-0001-7338-4920
Д. Ж. Джокович[б], доктор наук, профессор, orcid.org/0000-0002-0176-2395, djokovic@uwaterloo.ca
И. С. Котсирис[в], доктор наук, профессор, orcid.org/0000-0003-2126-8383, ikotsire@wlu.ca
[а]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, 190000, Санкт-Петербург, РФ
[б]Университет Ватерлоо, Ватерлоо, Онтарио, N2L 3G1, Канада
[в]Университет Уилфрида Лорье, Ватерлоо, Онтарио, N2L 3C5, Канада

Цель: построить матрицы Адамара, описываемые разностными семействами Гетхальса — Зейделя с повторяющимися блоками, посредством обобщения так называемой пропус-конструкции. **Методы:** основная составляющая конструкции пропусов — разностное семейство конечной абелевой группы порядка v, содержащее четыре блока (X_1, X_2, X_3, X_4), где X_1 симметричен и $X_2=X_3$. Параметры (v; k_1, k_2, k_3, k_4; λ) такого семейства должны удовлетворять дополнительному условию $\sum k_i=\lambda+v$. Эта конструкция модифицирована использованием различных типов симметрий выбираемых блоков и конструированием разнообразных примеров матриц Адамара такого сорта. В этой статье работа велась с циклической группой $\mathbf{Z}_v$ порядка v. Для больших значений v построены блоки X_i посредством орбит подходящих малых циклических подгрупп группы автоморфизмов $\mathbf{Z}_v$. **Результаты:** продолжен систематический поиск симметричных матриц Адамара порядка $4v$, использующий пропус-конструкцию. Аналогичные исследования проведены ранее для нечетных значений $v \leq 51$. Мы расширяем итог, закрывая случай $v=53$. Кроме того, сконструированы первые примеры симметричных матриц Адамара порядка 236. Получена обширная коллекция симметричных и кососимметричных матриц Адамара, и соответствующие разностные семейства классифицированы на основе видов симметрий их блоков. **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 — симметричные и кососимметричные матрицы Адамара, массив Гетхальса — Зейделя, массив пропус, циклические разностные семейства.

Для цитирования: Abuzin L. V., Balonin N. A., Đoković D. Ž., Kotsireas I. S. Hadamard matrices from Goethals — Seidel difference families with a repeated block. *Информационно-управляющие системы*, 2019, № 5, с. 2–9. doi:10.31799/1684-8853-2019-5-2-9
For citation: Abuzin L. V., Balonin N. A., Đoković D. Ž., Kotsireas I. S. Hadamard matrices from Goethals — Seidel difference families with a repeated block. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 5, pp. 2–9. doi:10.31799/1684-8853-2019-5-2-9