

TWO CLASSES OF HADAMARD MATRICES OF GOETHALS-SEIDEL TYPE

DRAGOMIR Ž. ĐOKOVIĆ

ABSTRACT. We introduce two classes of Hadamard matrices of Goethals-Seidel type and construct many matrices in these classes. The largest one among them has order $4 \cdot 631 = 2524$. We do not know whether these classes are infinite. In the appendix we pose three questions about prime numbers. These questions arose naturally from the difficulties we encounter while trying to construct Hadamard matrices of small unknown orders.

1. INTRODUCTION

The Goethals-Seidel (GS) array

$$\begin{bmatrix} A_0 & A_1 R & A_2 R & A_3 R \\ -A_1 R & A_0 & -R A_3 & R A_2 \\ -A_2 R & R A_3 & A_0 & -R A_1 \\ -A_3 R & -R A_2 & R A_1 & A_0 \end{bmatrix}$$

is a powerful tool for constructing Hadamard matrices [4, 5, 10] and in particular skew-Hadamard matrices.

In order to use this tool we need a special kind of difference families over a finite abelian group G consisting of four blocks

$$(1) \quad \mathbf{X} = (X_0, X_1, X_2, X_3)$$

Let the parameter set of this family be

$$(2) \quad (v; k_0, k_1, k_2, k_3; \lambda).$$

Thus we have $v = |G|$, $k_i = |X_i|$ for $0 \leq i \leq 3$, and

$$(3) \quad \sum_{i=0}^3 k_i(k_i - 1) = \lambda(v - 1).$$

An additional parameter, called *order*, is defined by

$$(4) \quad n = \sum_{i=0}^3 k_i - \lambda.$$

If $n = v$ we say that the difference family $\mathbf{X}$ and its parameter set are of *Goethals-Seidel (GS) type*.

Given such a family, there is a simple procedure which uses the GS-array to produce a Hadamard matrix of order $4v$. We say that such Hadamard matrix has *GS-type*. If the group G is cyclic then the matrix blocks A_i are circulants of order v and R is the back-circulant identity matrix, for more details see [4, 10].

It is an open question whether for each GS-parameter set (2) there exists a GS-difference family (over some abelian group G of order v) having these parameters.

A positive answer would imply that the well known Hadamard matrix conjecture is true. It is a folklore conjecture that the answer to the above question is positive. There is also a stronger conjecture which requires G to be a cyclic group.

Assume now that $\mathbf{X}$ is a GS-difference family and let $i \in \{0, 1, 2, 3\}$. If we replace the block X_i with its complement $G \setminus X_i$ we get again a GS-difference family but now its parameter set is changed: we have to replace k_i with $v - k_i$ and replace λ with $\lambda + v - 2k_i$. Thus, in order to avoid redundancy, we may and we shall assume that each $k_i \leq v/2$.

Since the size of a Hadamard matrix can easily be doubled, we consider only the cases with v odd. Moreover, we shall assume that G is cyclic and we identify G with the additive group of the ring $\mathbf{Z}_v$ (integers modulo v).

We say that a GS-parameter set (2) is *special* if $k_1 = k_2 = k_3$. By using the equations (3), (4) and $n = v$, one can easily show that if a parameter set $(v; k_0, k, k, k; \lambda)$ is special then the integer $1 + 2(k_0 + 3k) - 3(k_0 - k)^2$ must be a square.

Our objective is to construct pairs $(\mathbf{X}, \mu)$ where X is a GS-difference family and $\mu \in \mathbf{Z}_v^*$ (a *multiplier*) sends X_1 to X_2 and X_2 to X_3 , i.e., $\mu X_1 = X_2$ and $\mu X_2 = X_3$. There are two cases: $\mu X_3 = X_1$ and $\mu X_3 \neq X_1$. In the first case we say that $(\mathbf{X}, \mu)$ and the associated Hadamard matrix have a *spin structure* and in the second case a *slide structure*.

Note that if $(\mathbf{X}, \mu)$ is such a pair then so is the pair $(\mathbf{X}', \mu^{-1})$ where $\mathbf{X}'$ is obtained from $\mathbf{X}$ by interchanging the blocks X_1 and X_3 .

Note also that if $(\mathbf{X}, \mu)$ has spin structure then $\mathbf{Z}_v^*$ must have an element of order 3. For convenience we say that a special parameter set is of *spin type* if $\mathbf{Z}_v^*$ has an element of order 3.

We point out that there exist pairs $(\mathbf{X}, \mu_1)$ and $(\mathbf{X}, \mu_2)$ with $\mu_1 \neq \mu_2$ such that $(\mathbf{X}, \mu_1)$ has spin structure while $(\mathbf{X}, \mu_2)$ has slide structure. We shall give an example at the end of section 3.

A subset X of $\mathbf{Z}_v$ is *symmetric* if $-X = X$. It is *skew* if $\mathbf{Z}_v$ is a disjoint union of X , $-X$ and $\{0\}$. If the block X_0 of a GS-difference family $\mathbf{X}$ is skew then the associated Hadamard matrix is of skew type. We say that a GS-difference family $\mathbf{X}$ is *good* if X_0 is skew and the other three blocks are symmetric. On the other hand, if X_0 is symmetric and the other X_i are skew then we say that $\mathbf{X}$ is a *best* family. (The corresponding matrix blocks A_i in the GS-array have the same symmetry type as the corresponding X_i .)

From now on we assume that $\mathbf{X}$ is a GS-difference family whose parameter set is special. Hence the blocks X_1, X_2, X_3 have the same size and the same symmetry type.

We indicate the symmetry types of X_0 and X_1 by letters, s for symmetric and k for skew. For instance the symmetry symbol (sk) means that X_0 is symmetric and X_1 is skew (and so are X_2 and X_3). The meaning of $(s*)$ is that X_0 is symmetric and that we make no claim about the symmetry type of X_1 . The symmetry symbol $(**)$ is usually omitted. GS-type Hadamard matrices having special parameter sets and symmetry type (ss) , (sk) , (ks) are special cases of Williamson, good and best matrices, respectively. For the list of known Williamson matrices with v odd and $v \leq 59$ see [7].

2. PARAMETERS AND HADAMARD MATRICES OF SPIN TYPE FOR $v < 100$

In this section we list all parameter sets of spin type with $v < 100$. We give examples of spin difference families whenever we succeeded to find one. In some cases we found many solutions but we list only a few. The question mark after the parameter set means that we failed to find an associated spin difference family. In such cases we searched for the slide difference families (and if found, they are given in section 4). Beside the blocks X_0 and X_1 we also specify the multiplier μ . In general μ does not have to fix the block X_0 . If it does, we point it out by saying that X_0 is fixed.

A few examples in our list below are extracted from other papers or some well known lists of special Hadamard matrices such as Williamson matrices, good matrices and best matrices. We point out explicitly such cases.

(7; 3, 2, 2, 2; 2) (ks) , $\mu = 2$, X_0 fixed,
 $X_0 = [1, 2, 4]$, $X_1 = [1, 6]$
 Good matrices.

(7; 1, 3, 3, 3; 3) (ss) , $\mu = 2$, X_0 fixed,
 $X_0 = [0]$, $X_1 = [0, 1, 6]$
 Williamson matrices.

(9; 3, 3, 3, 3; 3) (ss) , $\mu = 4$, X_0 fixed,
 $X_0 = [0, 3, 6]$, $X_1 = [0, 1, 8]$
 Williamson matrices.

(13; 4, 5, 5, 5; 6) $(*s)$, $\mu = 3$,
 $X_0 = [0, 1, 4, 6]$ $X_1 = [0, 4, 6, 7, 9]$.

(13; 3, 6, 6, 6; 8) $(*k)$, $\mu = 3$,
 $X_0 = [6, 7, 10]$ $X_1 = [1, 2, 3, 4, 6, 8]$.

(19; 9, 7, 7, 7; 11) (ks) , $\mu = -2$, X_0 fixed,
 $X_0 = [1, 4, 5, 6, 7, 9, 11, 16, 17]$ $X_1 = [0, 1, 7, 8, 11, 12, 18]$.
 Good matrices.

In the next two examples the block X_0 can be combined with each of the listed choices for X_1 .

(19; 9, 7, 7, 7; 11) $(k*)$, $\mu = 7$, X_0 fixed,
 $X_0 = [2, 3, 4, 6, 8, 9, 12, 14, 18]$
 $X_1 = [0, 1, 6, 8, 13, 15, 16]$, $X_1 = [0, 2, 8, 9, 10, 11, 13]$,
 $X_1 = [0, 2, 8, 9, 10, 11, 14]$, $X_1 = [0, 1, 4, 5, 12, 15, 18]$.

(19; 6, 8, 8, 8; 11), $(s*)$, $\mu = 7$, X_0 fixed,
 $X_0 = [4, 6, 9, 10, 13, 15]$ $X_1 = [0, 1, 5, 8, 9, 10, 11, 13]$,
 $X_1 = [0, 1, 8, 9, 10, 11, 13, 14]$, $X_1 = [0, 1, 8, 9, 10, 11, 14, 17]$,
 $X_1 = [0, 4, 7, 9, 10, 11, 14, 18]$, $X_1 = [0, 4, 8, 9, 10, 11, 12, 13]$,
 $X_1 = [0, 6, 9, 10, 11, 12, 14, 18]$, $X_1 = [0, 6, 9, 10, 11, 12, 16, 17]$.

(21; 9, 8, 8, 8; 12) $(*s)$, $\mu = 4$,
 $X_0 = [1, 4, 5, 8, 10, 11, 12, 17, 19]$ $X_1 = [1, 3, 8, 9, 12, 13, 18, 20]$.

$$(21; 6, 10, 10, 10; 15) \quad \mu = 4, \\ X_0 = [0, 8, 10, 11, 12, 16] \quad X_1 = [0, 1, 2, 5, 6, 7, 13, 15, 16, 19].$$

Although the next parameter set is of spin type, our exhaustive search did not find any (cyclic) spin difference family having these parameters.

$$(27; 9, 12, 12, 12; 18).$$

$$(31; 12, 13, 13, 13; 20), (*s), \mu = 5, \\ X_0 = [2, 4, 6, 12, 14, 16, 17, 19, 25, 26, 28, 29], \\ X_1 = [0, 3, 9, 11, 13, 14, 15, 16, 17, 18, 20, 22, 28].$$

$$(31; 10, 15, 15, 15; 24), (*k), \mu = 5, \\ X_0 = [0, 2, 10, 13, 16, 17, 20, 26, 28, 29], \\ X_1 = [1, 4, 12, 13, 14, 15, 20, 21, 22, 23, 24, 25, 26, 28, 29].$$

$$(37; 18, 15, 15, 15; 26), (ks), \mu = 10, X_0 \text{ fixed}, \\ X_0 = [2, 3, 4, 6, 8, 11, 15, 18, 20, 21, 23, 24, 25, 27, 28, 30, 32, 36], \\ X_1 = [0, 1, 2, 5, 9, 13, 14, 15, 22, 23, 24, 28, 32, 35, 36]. \\ \text{Good matrices.}$$

$$(37; 13, 17, 17, 17; 27), (ss), \mu = 10, X_0 \text{ fixed}, \\ X_0 = [0, 3, 4, 5, 7, 13, 18, 19, 24, 30, 32, 33, 34], \\ X_1 = [0, 1, 2, 3, 4, 6, 12, 13, 18, 19, 24, 25, 31, 33, 34, 35, 36]. \\ \text{Williamson matrices.}$$

$$(39; 18, 16, 16, 16; 27), (s*), \mu = 16, X_0 \text{ fixed}, \\ X_0 = [1, 4, 6, 10, 14, 15, 16, 17, 18, 21, 22, 23, 24, 25, 29, 33, 35, 38], \\ X_1 = [0, 2, 4, 6, 7, 10, 11, 14, 16, 19, 20, 22, 26, 32, 33, 38].$$

$$(39; 15, 17, 17, 17; 27), (ss), \mu = 16, X_0 \text{ fixed}, \\ X_0 = [0, 4, 8, 10, 11, 13, 14, 19, 20, 25, 26, 28, 29, 31, 35], \\ X_1 = [0, 1, 4, 5, 6, 8, 11, 12, 14, 25, 27, 28, 31, 33, 34, 35, 38]. \\ \text{Williamson matrices.}$$

$$(43; 19, 18, 18, 18; 30) ? \\ (43; 15, 21, 21, 21; 35) ? \\ (49; 21, 21, 21, 21; 35) ? \\ (49; 19, 22, 22, 22; 36) ? \\ (57; 24, 25, 25, 25; 42) ?$$

An exhaustive search for best matrices of order 57 has been carried out in [1]. Three solutions were found. It turned out that two of them have spin structure:

$$(57; 21, 28, 28, 28; 48), (sk), \mu = 7, X_0 \text{ is fixed in both cases.} \\ 1) X_0 = [0, 4, 11, 12, 18, 19, 20, 25, 26, 27, 28, 29, 30, 31, 32, 37, 38, 39, 45, 46, 53], \\ X_1 = [1, 2, 5, 6, 7, 8, 9, 10, 12, 17, 19, 21, 22, 24, 25, 28, 30, 31, 34, \\ 37, 39, 41, 42, 43, 44, 46, 53, 54], \\ 2) X_0 = [0, 4, 5, 12, 17, 18, 19, 22, 25, 27, 28, 29, 30, 32, 35, 38, 39, 40, 45, 52, 53], \\ X_1 = [2, 4, 6, 7, 8, 10, 13, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 28, \\ 36, 42, 43, 45, 46, 48, 52, 54, 56]. \\ \text{Best matrices.}$$

When all blocks X_i are H -invariant for some subgroup H of $\mathbf{Z}_v^*$ then it suffices to list only the representatives of the H -orbits contained in X_0 (rep. 0) and X_1 (rep. 1).

(61; 30, 26, 26, 26; 47), $(k*)$, $\mu = 13$, $H = [1, 9, 20, 34, 58]$,
 rep. 0 : [3, 4, 5, 6, 8, 10], rep. 1 : [0, 8, 10, 13, 23, 26].
 X_0 fixed.

(61; 24, 28, 28, 28; 47) ?
 (63; 30, 27, 27, 27; 48) ?
 (63; 24, 30, 30, 30; 51) ?
 (67; 31, 29, 29, 29; 51) ?
 (67; 28, 30, 30, 30; 51) ?
 (73; 33, 32, 32, 32; 56) ?

(73; 28, 36, 36, 36; 63), $(*s)$, $\mu = 4$, $H = [1, 8, 64]$,
 1) rep. 0 : [0, 9, 13, 18, 25, 26, 27, 35, 36, 43],
 rep. 1 : [1, 2, 4, 9, 11, 14, 18, 21, 26, 34, 36, 43].
 2) rep. 0 : [0, 5, 7, 9, 14, 17, 18, 33, 34, 36],
 rep. 1 : [4, 5, 7, 12, 14, 17, 21, 33, 34, 35, 36, 43].
 X_0 is fixed in both cases.

(79; 33, 36, 36, 36; 62) ?
 (81; 36, 36, 36, 36; 63) ?

(91; 45, 40, 40, 40; 74), $(**)$, $\mu = 9$, $H = [1, 16, 74]$,
 rep. 0 : [1, 5, 6, 7, 13, 14, 16, 19, 20, 24, 28, 29, 39, 47, 49],
 rep. 1 : [0, 3, 8, 13, 16, 23, 24, 38, 40, 46, 47, 48, 49, 57].

(91; 37, 43, 43, 43; 75),
 1) $(s*)$, $H = [1, 16, 74]$, $\mu = 9$,
 rep. 0 : [0, 3, 4, 5, 8, 11, 19, 25, 27, 43, 45, 50, 55],
 rep. 1 : [0, 1, 4, 5, 13, 14, 15, 25, 28, 33, 38, 43, 44, 49, 55].
 2) $H = [1, 9, 81]$, $\mu = 16$,
 rep. 0 : [0, 6, 8, 12, 13, 19, 20, 24, 38, 39, 40, 48, 57],
 rep. 1 : [0, 2, 15, 16, 19, 23, 24, 28, 30, 38, 40, 47, 48, 49, 57].

(91; 40, 41, 41, 41; 72) ?
 (91; 36, 45, 45, 45; 80) ?

(93; 45, 41, 41, 41; 75), $\mu = 25$, $H = [1, 4, 16, 64, 70]$,
 rep. 0 : [3, 10, 11, 14, 21, 23, 33, 34, 46],
 rep. 1 : [3, 9, 11, 17, 23, 33, 34, 46, 62].

(93; 39, 43, 43, 43; 75) ?
 (97; 46, 43, 43, 43; 78) ?
 (97; 39, 47, 47, 47; 83) ?

3. ADDITIONAL CASES

There are only finitely many known good matrices. Their orders are ≤ 127 . We constructed those of order 127 long ago in [2]. Much later we observed that the GS-difference family used in that construction has very special properties to which

we now refer as spin structure. Here is that example where we replaced the three blocks of size 70 by their complements (of size 57):

$$\begin{aligned} & (127; 63, 57, 57, 57; 107), \quad (ks), \quad \mu = 19, \\ & H = [1, 2, 4, 8, 16, 32, 64], \\ & \text{rep. } 0 : [1, 3, 7, 9, 11, 19, 21, 23, 47], \\ & \text{rep. } 1 : [0, 3, 7, 9, 11, 15, 29, 31, 55]. \\ & \text{Good matrices.} \end{aligned}$$

The H above is the subgroup of $\mathbf{Z}_{127}^*$ of order 7. All four blocks are H -invariant, and so each of them is a union of some H -orbits. The representatives of the H -orbits contained in X_0 and those in X_1 are listed above. The block X_0 is skew and X_1 is symmetric. The multiplier $\mu = 19$ (of order 3) fixes the block X_0 and permutes cyclically the other three blocks.

As v grows the search for spin Hadamard matrices becomes harder and harder. The search may be feasible only for difference families invariant under relatively large subgroup say H of $\mathbf{Z}_v^*$. In the following three examples we used subgroups of order 7, 9 and 11.

$$\begin{aligned} & (129; 63, 58, 58, 58; 108), \quad \mu = 13, \\ & H = [1, 4, 16, 64, 97, 121, 127], \\ & \text{rep. } 0 : [1, 9, 10, 14, 19, 21, 23, 26, 27], \\ & \text{rep. } 1 : [2, 5, 9, 10, 13, 18, 22, 27, 43, 86]. \end{aligned}$$

$$\begin{aligned} & (271; 135, 126, 126, 126; 242), \quad (k*), \quad \mu = 5, \\ & H = [1, 28, 106, 125, 169, 178, 242, 248, 258], \\ & 1) \text{ rep. } 0 : [1, 4, 5, 7, 8, 11, 14, 16, 19, 21, 22, 25, 31, 43, 44], \\ & \quad \text{rep. } 1 : [1, 2, 3, 5, 7, 8, 12, 19, 22, 27, 38, 42, 44, 51], \\ & 2) \text{ rep. } 0 : [1, 2, 4, 5, 7, 8, 9, 11, 14, 16, 17, 22, 25, 31, 44], \\ & \quad \text{rep. } 1 : [1, 3, 5, 9, 12, 14, 17, 19, 21, 22, 33, 44, 71, 86]. \end{aligned}$$

$$\begin{aligned} & (331; 165, 155, 155, 155; 299), \quad (k*), \quad \mu = 31, \\ & H = [1, 74, 80, 85, 111, 120, 167, 180, 270, 274, 293], \\ & 1) \text{ rep. } 0 : [5, 10, 11, 13, 16, 19, 20, 22, 32, 38, 53, 56, 64, 76, 101], \\ & \quad \text{rep. } 1 : [0, 4, 11, 16, 20, 28, 31, 37, 41, 49, 53, 56, 73, 88, 101]. \\ & 2) \text{ rep. } 0 : [4, 5, 13, 14, 16, 19, 20, 22, 32, 38, 49, 53, 56, 64, 76], \\ & \quad \text{rep. } 1 : [0, 11, 13, 14, 19, 22, 31, 37, 44, 49, 56, 62, 73, 76, 88]. \end{aligned}$$

So far no spin type GS-difference families with $v > 631$ are known. For that reason we list below all five solutions that we constructed for $v = 631$. The first two are just minor modifications of the two GS-difference families used in [3] to construct two skew-Hadamard matrices of order $4v$. Surprisingly, it turned out that these two families indeed have spin structure. In all five solutions, H is the subgroup of order 15 and the block X_0 is skew and fixed by μ .

- (631; 315, 301, 301, 301; 587), $(k*)$, $\mu = 2$,
 $H = [1, 8, 43, 64, 79, 188, 228, 242, 279, 310, 339, 344, 512, 562, 587]$,
 1) rep. 0 : $[1, 2, 3, 4, 6, 7, 12, 13, 14, 17, 19, 21, 26, 27, 31, 38,$
 $42, 52, 62, 76, 124]$,
 rep. 1 : $[0, 11, 13, 14, 18, 19, 21, 22, 29, 35, 39, 46, 62, 63,$
 $65, 66, 67, 92, 117, 124, 187]$,
 2) rep. 0 : $[11, 13, 19, 22, 26, 29, 31, 33, 38, 39, 44, 52, 62, 65,$
 $66, 67, 76, 78, 117, 124, 187]$,
 rep. 1 : $[0, 2, 6, 7, 12, 13, 19, 21, 27, 31, 35, 44, 52, 63, 66,$
 $76, 78, 92, 124, 126, 187]$,
 3) rep. 0 : $[1, 2, 4, 5, 7, 9, 14, 17, 18, 21, 23, 27, 31, 33, 42, 46,$
 $62, 66, 67, 92, 124]$,
 rep. 1 : $[0, 4, 5, 9, 13, 14, 19, 21, 22, 27, 29, 31, 33, 35, 44,$
 $63, 76, 92, 124, 126, 187]$,
 4) rep. 0 : $[1, 2, 4, 7, 13, 14, 23, 26, 27, 31, 33, 46, 52, 62, 65,$
 $66, 67, 92, 117, 124, 187]$,
 rep. 1 : $[0, 3, 4, 6, 12, 13, 17, 18, 19, 23, 26, 27, 29, 31, 35,$
 $46, 62, 65, 67, 76, 92]$,
 5) rep. 0 : $[1, 2, 3, 4, 6, 7, 12, 13, 14, 17, 19, 21, 26, 27, 31, 38,$
 $42, 52, 62, 76, 124]$,
 rep. 1 : $[0, 2, 5, 6, 7, 13, 18, 19, 21, 27, 33, 39, 44, 52, 62,$
 $63, 76, 78, 92, 117, 126]$.

If we replace the multiplier $\mu = 2$ with $\mu = 4$, then all five pairs $(\mathbf{X}, \mu)$ above will loose the spin structure and acquire the slide structure.

4. HADAMARD MATRICES WITH SLIDE STRUCTURE

In this section we give examples of pairs $(\mathbf{X}, \mu)$ having slide structure. In three of these examples we have indicated that $X_3 = -X_1$. Hence we can replace X_3 with X_1 to obtain a GS-difference family with a repeated block.

- (25; 10, 10, 10, 10; 15), $\mu = 7$,
 $X_0 = [1, 5, 7, 9, 12, 13, 15, 16, 19, 21]$,
 $X_1 = [2, 4, 5, 6, 7, 11, 19, 20, 21, 24]$,
 $X_3 = -X_1$.
 (27; 9, 12, 12, 12; 18), $\mu = 7$, $H = [1, 10, 19]$,
 1) $X_0 = [2, 6, 8, 10, 13, 14, 16, 18, 21]$,
 $X_1 = [2, 3, 8, 11, 12, 13, 14, 15, 16, 17, 22, 26]$.
 2) $X_0 = [2, 6, 8, 9, 13, 14, 16, 19, 21]$,
 $X_1 = [1, 5, 7, 10, 12, 13, 14, 15, 16, 17, 21, 25]$.
 (31; 10, 15, 15, 15; 24), $\mu = 4$, $H = [1, 5, 25]$,
 rep. 0 : $[0, 3, 11, 12]$, rep. 1 : $[1, 3, 8, 16, 17]$.
 (43; 19, 18, 18, 18; 30), $\mu = 3$, $H = [1, 6, 36]$,
 rep. 0 : $[0, 1, 3, 9, 19, 20, 21]$, rep. 1 : $[1, 5, 13, 19, 20, 26]$.
 (43; 15, 21, 21, 21; 35), $H = [1, 6, 36]$,
 1) rep. 0 : $[1, 4, 9, 20, 26]$, rep. 1 : $[1, 9, 10, 13, 20, 21, 26]$, $\mu = 3$,
 2) rep. 0 : $[1, 2, 3, 20, 21]$, rep. 1 : $[3, 4, 5, 10, 20, 21, 26]$, $\mu = 9$.

- (49; 21, 21, 21, 21; 35), $\mu = 9$, $H = [1, 18, 30]$,
rep. 0 : $[1, 2, 8, 9, 21, 24, 29]$, rep. 1 : $[2, 6, 12, 19, 24, 26, 29]$.
- (49; 19, 22, 22, 22; 36), $\mu = 4$, $H = [1, 18, 30]$,
rep. 0 : $[0, 2, 4, 7, 8, 16, 29]$, rep. 1 : $[0, 2, 7, 8, 12, 13, 26, 29]$.
- (61; 30, 26, 26, 26; 47), $(s*)$, $\mu = 2$, $H = [1, 9, 20, 34, 58]$,
rep. 0 : $[1, 3, 4, 5, 12, 13]$, rep. 1 : $[0, 8, 12, 13, 23, 26]$.
- (61; 24, 28, 28, 28; 47), $\mu = 11$, $H = [1, 13, 47]$,
rep. 0 : $[1, 8, 9, 11, 12, 18, 27, 36]$,
rep. 1 : $[0, 1, 7, 8, 9, 18, 22, 27, 31, 32]$.
 $X_3 = -X_1$.
- (67; 28, 30, 30, 30; 51), $\mu = 15$, $H = [1, 29, 37]$,
rep. 0 : $[0, 1, 4, 5, 7, 11, 12, 16, 17, 19]$,
rep. 1 : $[2, 3, 4, 9, 12, 15, 16, 17, 19, 21]$.
- (73; 28, 36, 36, 36; 63), $\mu = 3$, $H = \langle 2 \rangle$ subgroup of order 9,
rep. 0 : $[0, 1, 3, 13]$, rep. 1 : $[3, 11, 13, 17]$,
 $X_3 = -X_1$.
- (79; 33, 36, 36, 36; 62), $H = [1, 23, 55]$, $\mu = 12$,
rep. 0 : $[4, 5, 6, 10, 17, 22, 27, 30, 33, 44, 47]$,
rep. 1 : $[1, 5, 8, 17, 18, 20, 22, 34, 37, 40, 44, 47]$.
- (129; 63, 58, 58, 58; 108), $H = [1, 4, 16, 64, 97, 121, 127]$,
rep. 0 : $[1, 6, 9, 11, 13, 19, 23, 26, 27]$, $\mu = 19$,
rep. 1 : $[2, 7, 9, 14, 21, 22, 23, 27, 43, 86]$.
- (211; 91, 105, 105, 105; 195), $H = \langle 19 \rangle$ subgroup of order 15,
1) rep. 0 : $[0, 1, 2, 10, 22, 26, 43]$, $\mu = 25$,
rep. 1 : $[1, 4, 10, 11, 22, 29, 43]$.
2) rep. 0 : $[5, 10, 11, 22, 26, 29]$, $\mu = 13$,
rep. 1 : $[2, 5, 7, 10, 22, 29, 43]$.

5. APPENDIX: PRIME CHAINS

While trying to construct Hadamard matrices of unknown small orders $4v$, we noticed that the hardest cases are often those where v is a prime congruent to 3 mod 4 and $(v - 1)/2$ is also a prime. Let us mention three of them. For about 30 years (1932-1962) it was not known how to construct a Hadamard matrix of order $92 = 4 \cdot 23$, see [11, p. 177]. This was the smallest order (multiple of 4) for which no Hadamard matrix was known. Such matrix was constructed in 1962 when the computers became available. For about 20 years (1985-2005) the smallest unknown order was $428 = 4 \cdot 107$. The first Hadamard matrix of that order was constructed by H. Kharaghani and B. Tayfeh-Rezaie [8]. Presently, for $v < 250$ there are only 3 values, namely $v = 167, 179, 223$ for which no Hadamard matrix of order $4v$ is known. All three are primes congruent to 3 mod 4 and in the first two cases the number $(v - 1)/2$ is a prime. These observations led us to raise several questions below concerning the prime numbers.

Let Π denote the set of all prime numbers and define the function $\sigma : \Pi \rightarrow \Pi$ by

$$\sigma(p) = \begin{cases} 2p+1 & \text{if } 2p+1 \in \Pi \\ p & \text{otherwise.} \end{cases}$$

Let $\Pi' = \{p \in \Pi : (p-1)/2 \notin \Pi\}$ and $\Pi'' = \{p \in \Pi' : 2p+1 \notin \Pi\}$. It is easy to show that the set Π' is infinite. Indeed if $p \in \Pi$ is congruent to 1 modulo 4 then the integer $(p-1)/2$ is even and so it is a prime only if $p = 5$. In all other cases $p \in \Pi'$. For $p \in \Pi'$ we set $\Sigma_p = \{\sigma^i(p) : i \geq 0\}$ and we note that $\Pi' \cap \Sigma_p = \{p\}$. Evidently the sets Σ_p with $p \in \Pi'$ form a partition of Π . We shall refer to the sets Σ_p with $p \in \Pi'$ as *prime chains* and we say that p is the *head* of Σ_p . A prime chain Σ_p is *trivial* if $\Sigma_p = \{p\}$.

If $p \in \Pi'$ and $d > 0$ does not exceed the size of Σ_p then for $0 \leq i < d$ we have

$$(5) \quad \sigma^i(p) = 2^i(p+1) - 1.$$

Hence the sequence $(\sigma^i(p), i = 0, 1, \dots, d-1)$ is just a shifted geometric progression with ratio 2. In particular, the set of Mersenne primes is a union of prime chains. However all prime chains of Mersenne primes are trivial except the first, namely $\{3, 7\}$.

Let us look at a few examples of prime chains. We can order the set of prime chains by saying that $\Sigma_p < \Sigma_q$ if $p < q$. By using this ordering, we computed for each $s \in \{1, 2, \dots, 9\}$ the smallest prime chain of cardinality s :

s	prime chain
1	$\{13\}$,
2	$\{3, 7\}$,
3	$\{41, 83, 167\}$,
4	$\{509, 1019, 2039, 4079\}$,
5	$\{2, 5, 11, 23, 47\}$,
6	$\{89, 179, 359, 719, 1439, 2879\}$,
7	$\{1122659, 2245319, 4490639, 8981279, 17962559, 35925119, 71850239\}$,
8	$\{19099919, 38199839, 76399679, 152799359, 305598719, 611197439,$ $1222394879, 2444789759\}$,
9	$\{85864769, 171729539, 343459079, 686918159, 1373836319, 2747672639,$ $5495345279, 10990690559, 21981381119\}$.

We now state our questions.

Question 1: Are all prime chains finite?

The answer is expected to be affirmative. Let us recall a very special case of Artin's primitive root conjecture (which is still open). It asserts that 2 is a primitive root of q for infinitely many primes q , see e.g. [6]. Assuming that this is true, we can show that the answer to Question 1 is affirmative. Indeed, suppose that a prime chain Σ_p is infinite for some $p \in \Pi'$. We can choose $q \in \Pi$ such that 2 is a primitive root of q and $q > p+1$. As Σ_p is infinite, the equation (5) is valid for all integers $i \geq 0$. Since 2 is a primitive root of q we can choose i so that $2^i(p+1) \equiv 1 \pmod{q}$ and $2^i(p+1) > q+1$. Hence we have a contradiction because $\sigma^i(p)$ is divisible by q and greater than q .

Question 2: Are the sizes of finite prime chains bounded?

We tried to find at least one prime chain of size larger than 9. Our computer computation failed. The conclusion was that if such a chain Σ_p exists then $p > 6119789909$.

We need some more notation. Let π_N be the number of primes $\leq N$, π'_N the number of prime chains with head $\leq N$, and π''_N the number of these chains which are also trivial. The table below summarizes the results of our computations. For each value of the exponent $e = 1, 2, \dots, 8$, the number N is the smallest prime larger than 10^e . The timings in seconds are given just for computing the data for the primes not covered by the previous cases (smaller values of e).

e	N	π_N	π'_N	π''_N	π''_N/π'_N	seconds
1	11	5	2	0	0	0.075
2	101	26	19	13	0.6842105263	0.074
3	1009	169	144	114	0.7916666667	0.072
4	10007	1230	1114	952	0.8545780969	0.135
5	100003	9593	8923	7878	0.8828869214	0.616
6	1000003	78499	74175	67135	0.9050893158	5.016
7	10000019	664580	633923	582143	0.9183181554	52.412
8	100000007	5761456	5531888	5136716	0.9285647143	569.637

In view of the steady growth of the numbers in the penultimate column, we state our last question.

Question 3: Is it true that almost all prime chains are trivial, i.e. that

$$\lim_{N \rightarrow \infty} \frac{\pi''_N}{\pi'_N} = 1?$$

6. ACKNOWLEDGEMENTS

This research was enabled in part by support provided by SHARCNET (<http://www.sharcnet.ca>) and the Digital Research Alliance of Canada (alliancecan.ca).

REFERENCES

- [1] C. Bright, D. Ž. Đoković, I. Kotsireas, V. Ganesh, The SAT+CAS method for combinatorial search with applications to best matrices, *Annals of Mathematics and Artificial Intelligence* (2019) 87:321–342.
- [2] D. Ž. Đoković, Good Matrices of Orders 33,35 and 127. *JCMCC* 14 (1993), 145–152.
- [3] D. Ž. Đoković, O. Golubitsky and I. S. Kotsireas, Some new orders of Hadamard and skew-Hadamard matrices. *J. Combin. Designs*, 22 (2014), 270–277.
- [4] D. Ž. Đoković, I. S. Kotsireas, Goethals-Seidel difference families with symmetric or skew base blocks. *Math. Comput. Sci.* (2018) 12: 373–388.
- [5] J. M. Goethals and J. J. Seidel, A skew-Hadamard matrix of order 36, *J. Austral. Math. Soc. A* 11 (1970), 343–344.
- [6] D. R. Heath-Brown, Artin’s conjecture for primitive roots, *The Quarterly Journal of Mathematics*, vol. 37, issue 1, 1986.
- [7] W. H. Holzmann, H. Kharaghani and B. Tayfeh-Rezaie, Williamson matrices up to order 59, *Designs, Codes and Cryptography*, 46 (2008), 343–352.
- [8] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, *J. Combin. Des.* 13 (6): 435–440, 2005.
- [9] Maple 2023 (X86 64 LINUX) Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.
- [10] J. Seberry, M. Yamada, Hadamard matrices, sequences, and block designs. In *Contemporary design theory*, 431–560, Wiley-Intersci. Ser. Discrete Math. Optim., Wiley, New York, 1992.
- [11] J. H. van Lint & R. M. Wilson, *A course in Combinatorics*, Cambridge University Press, 1992

UNIVERSITY OF WATERLOO, DEPARTMENT OF PURE MATHEMATICS, WATERLOO, ONTARIO, N2L
3G1, CANADA
Email address: `dragomir@rogers.com`