Hadamard ideals and Hadamard matrices from two circulant submatrices

Ilias S. Kotsireas[1] and Christos Koukouvinos[2]

Abstract

We apply Computational Algebra methods to the construction of Hadamard matrices from two circulant submatrices, given by C. H. Yang. We associate Hadamard ideals to this construction, to systematize the application of Computational Algebra methods. Our approach yields an exhaustive search for Hadamard matrices from two circulant submatrices for this construction, for the first eight admissible values 2, 4, 8, 10, 16, 18, 20, 26 and partial searches for the next three admissible values 32, 34 and 40. From the solutions we found, for the admissible values 26 and 34, we located new inequivalent Hadamard matrices of orders 52 and 68 with two circulant submatrices, thus improving the lower bounds for the numbers of inequivalent Hadamard matrices of orders 52 and 68. We also propose a heuristic decoupling of one of the equations arising from this construction, which can be used together with the PSD test to search for solutions more efficiently.

Keywords: Hadamard Matrices, Computational Algebra, Hadamard ideal, Hadamard equivalence, algorithm.

MSC: 05B20, 13P10.

1 Introduction

In [26] the author describes a construction of Hadamard matrices of order 2ν from two circulant submatrices of order ν each. In this paper we associate Hadamard ideals to this construction with two circulant submatrices, as a means of applying computational algebra techniques.

The problem of enumerating Hadamard matrices constructed from two circulant submatrices is equivalent to the problem of enumerating pairs of $\{-1, 1\}$ sequences with complementary periodic autocorrelation functions. Golay pairs, since they have complementary aperiodic autocorrelation functions, are a very special case, and have been very well studied [8]. Up to order 100, the enumeration of Golay pairs is nearly complete [4].

[1] Wilfrid Laurier University, Department of Physics and Computer Science, 75 University Avenue West, Waterloo, Ontario N2L 3C5, Canada, ikotsire@wlu.ca, Supported in part by a grant from the Natural Sciences and Engineering Research Council of Canada.

[2] Department of Mathematics, National Technical University of Athens, Zografou 15773, Athens, Greece, ckoukouv@math.ntua.gr

The more general periodic case has only much more recently attracted attention, see for instance [3, 2, 7, 10]. In particular, the existence of a periodic complementary pair of sequences of length 34 (which is excluded for Golay pairs) was first established in [7] and the non-existence of a pair of length 36 is a consequence of a theorem proved in [2, 9]. The non-existence of a pair of length 18, that we have also verified independently, was already ruled out by exhaustive search in [27], and also follows from the aforementioned theorem.

2 Hadamard matrices from two circulant submatrices

A Hadamard matrix of order n is an $n \times n$ matrix with elements ± 1 such that $HH^T = H^T H = nI_n$, where I_n is the $n \times n$ identity matrix and T stands for transposition. For more details see the books of Jennifer Seberry cited in the bibliography. An Hadamard matrix of order 2ν which can be written in the form

$$H_{2\nu} = \left[\begin{array}{c|c} A & B \\ \hline -B^T & A^T \end{array} \right] \tag{1}$$

where $A = (a_{ij})$, $B = (b_{ij})$ are two circulant matrices of order ν i.e. $a_{ij} = a_{1,j-i+1(\text{mod } \nu)}$, $b_{ij} = b_{1,j-i+1(\text{mod } \nu)}$, is said to be constructible from two circulant submatrices, see [26]. The following matrix is an example of a Hadamard matrix of order 8 constructible from two circulant submatrices of order $\nu = 4$ each:

$$\left[\begin{array}{cccc|cccc} 1 & 1 & 1 & - & 1 & 1 & - & 1 \\ - & 1 & 1 & 1 & 1 & 1 & 1 & - \\ 1 & - & 1 & 1 & - & 1 & 1 & 1 \\ 1 & 1 & - & 1 & 1 & - & 1 & 1 \\ \hline - & - & 1 & - & 1 & - & 1 & 1 \\ - & - & - & 1 & 1 & 1 & - & 1 \\ 1 & - & - & - & 1 & 1 & 1 & - \\ - & 1 & - & - & - & 1 & 1 & 1 \end{array} \right]$$

where $-$ stands for -1 to conform with the customary notation for Hadamard matrices.

The two circulant submatrices A and B satisfy the matrix equation

$$AA^T + BB^T = (2\nu)I_\nu \tag{2}$$

where I_ν is the identity matrix or order ν.

Since 2ν must be equal to a multiple of 4 we have that ν must be an even integer for this construction to yield a Hadamard matrix.

2.1 Equivalent Hadamard matrices

Two Hadamard matrices H_1 and H_2 are called equivalent (or Hadamard equivalent, or H-equivalent) if one can be obtained from the other by a sequence of row negations, row permutations, column negations and column permutations. More specifically, two Hadamard matrices are equivalent if one can be obtained by the other by a sequence of the following transformations:

- Multiply rows and/or columns by -1.
- Interchange rows and/or columns.

For a detailed presentation of Hadamard matrices and their constructions see [15], [25], [23], [16] and for inequivalent Hadamard matrices see [14] and [13].

Remark 1 *For a given set X of Hadamard matrices of arbitrary but fixed dimension n, the relation of H-equivalence (noted $\overset{H}{\sim}$ here) is an equivalence relation. Indeed, H-equivalence is reflexive ($H \overset{H}{\sim} H, \forall H \in X$) symmetric ($H_1 \overset{H}{\sim} H_2$ implies $H_2 \overset{H}{\sim} H_1$,$\forall H_1, H_2 \in X$) and transitive ($H_1 \overset{H}{\sim} H_2$ and $H_2 \overset{H}{\sim} H_3$ imply $H_1 \overset{H}{\sim} H_3$, $\forall H_1, H_2, H_3 \in X$). Therefore, one can study the equivalence classes and define representatives for each class.*

To define $\overset{H}{\sim}$ more formally, suppose P and Q are two monomial matrices of order n (monomial means elements $0, +1, -1$ and only one non-zero entry in each row and column) where $PP^T = QQ^T = I_n$. Then two Hadamard matrices A and B of order n are said to be equivalent if $A = PBQ$.

3 Hadamard ideals

We detail the construction of Hadamard matrices from two circulant submatrices with an eye to producing a set of nonlinear polynomial equations and study the structure of the associated ideal which we will call a **Hadamard Ideal.**

Consider two vectors of ν unknowns each $(a_1, \ldots, a_\nu)$ and $(b_1, \ldots, b_\nu)$. These two vectors generate two circulant $\nu \times \nu$ matrices A_ν and B_ν:

$$A_\nu = \begin{bmatrix} a_1 & a_2 & \ldots & a_\nu \\ a_\nu & a_1 & \ldots & a_{\nu-1} \\ \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & \ldots & a_1 \end{bmatrix}, \quad B_\nu = \begin{bmatrix} b_1 & b_2 & \ldots & b_\nu \\ b_\nu & b_1 & \ldots & b_{\nu-1} \\ \vdots & \vdots & \vdots & \vdots \\ b_2 & b_3 & \ldots & b_1 \end{bmatrix}$$

Once we have constructed the two circulant matrices A_ν and B_ν, the C. H. Yang construction of Hadamard matrices from two circulant submatrices (see [26]) stipulates that an Hadamard matrix of order 2ν is obtained by arranging these matrices and their transposes as in (1):

$$H_{2\nu} = \left[\begin{array}{ccc|ccc} a_1 & \ldots & a_\nu & b_1 & \ldots & b_\nu \\ a_\nu & \ldots & a_{\nu-1} & b_\nu & \ldots & b_{\nu-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_2 & \ldots & a_1 & b_2 & \ldots & b_1 \\ \hline -b_1 & \ldots & -b_2 & a_1 & \ldots & a_2 \\ -b_2 & \ldots & -b_3 & a_2 & \ldots & a_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -b_\nu & \ldots & -b_1 & a_\nu & \ldots & a_1 \end{array}\right].$$

The additional constraints $\{a_1, \ldots, a_\nu, b_1, \ldots, b_\nu\} \subset \{-1, +1\}^{2\nu}$ arise from the fact that the elements of a Hadamard matrix are required to be ± 1. A succinct algebraic description of these quadratic constraints given above is provided by the following set of 2ν algebraic equations:

$$a_1^2 - 1 = 0, \ldots, a_\nu^2 - 1 = 0, b_1^2 - 1 = 0, \ldots, b_\nu^2 - 1 = 0.$$

Another way to express this, is to say that we want to target some elements of the variety which are located inside the subvariety defined by

$$\underbrace{\{-1, +1\} \times \ldots \times \{-1, +1\}}_{2\nu \text{ terms}}.$$

The matrix equation $H_{2\nu} H_{2\nu}^T = (2\nu) I_{2\nu}$ gives rise to the following categories of equations:

- a set of quadratic equations whose precise structure will be detailed in the forthcoming definition of Hadamard ideals;
- a quadratic equation of a different structure than the quadratic equations mentioned above;
- the equation of the form

  $$a_1^2 + \ldots + a_\nu^2 + b_1^2 + \ldots + b_\nu^2 = 2\nu$$

  which is satisfied trivially, since $a_1^2 = \ldots = a_\nu^2 = b_1^2 = \ldots = b_\nu^2 = 1$;

To systematize the study of the systems of polynomial equations that arise in the C. H. Yang construction for Hadamard matrices from two circulant submatrices, we associate to them some **Hadamard Ideals**. This allows us to apply numerous tools of computational algebra [5, 24] such as Gröbner bases to the study of Hadamard matrices from two circulant submatrices. Similar Hadamard Ideals have been associated to other constructions for Hadamard matrices, see [18], [19]. The ideals that arise in all of these constructions share numerous similar characteristics and this justifies using the term Hadamard Ideal to describe all of them. When it is not clear which construction we are referring to, the name of the construction may be mentioned explicitly, to remove any potential ambiguities.

Definition 1 *For any even natural number $\nu = 2, 4, 6, \ldots$ set $m = \frac{\nu}{2}$. Then the ν-th* **Hadamard ideal** *$\mathcal{H}_\nu$ (associated with the two circulant submatrices construction C. H. Yang) is defined by:*

$$\mathcal{H}_\nu = \langle q_1, \ldots, q_{m-1}, Q_\nu, a_1^2 - 1, \ldots, a_\nu^2 - 1, b_1^2 - 1, \ldots, b_\nu^2 - 1 \rangle$$

where $q_1, \ldots q_{m-1}$ are quadratic equations defined by:

$$q_j = \sum_{i=1}^{\nu} \left(a_i a_{(i+j) \bmod \nu} + b_i b_{(i+j) \bmod \nu} \right) = 0 \; for \; j = 1, \ldots, m-1.$$

(with the convention that for $\nu = 2$ there are no such equations) and Q_ν is a quadratic equation defined by:

$$Q_\nu = \sum_{i=1}^{m} \left(a_i a_{(i+m)} + b_i b_{(i+m)} \right) = 0. \tag{3}$$

The ideal $\mathcal{H}_\nu$ is generated by $m + 2\nu$ polynomials. Moreover, the ideal $\mathcal{H}_\nu$ is zero-dimensional (This is evident, because all elements of the variety $\mid V(\mathcal{H}_\nu) \mid$ are also elements of $\{-1, +1\}^{2\nu}$ which is in turn, a finite set).

4 Diophantine constraints, Gröbner bases and PSD test

In this section we mention necessary (but not sufficient) conditions for the existence of solutions in the two circulant submatrices construction. First we describe a Diophantine constraint that is satisfied by all solutions of. Then we describe the power spectral density (PSD) test.

4.1 Diophantine constraints

We multiply the matrix equation (2) from the left with the row vector e^t and from the right with the column vector $e = (1, 1, \ldots, 1)^t$. This gives rise to the Diophantine constraint

$$a^2 + b^2 = 2\,\nu \tag{4}$$

where $a = a_1 + \ldots + a_\nu$ and $b = b_1 + \ldots + b_\nu$. A derivation of the above Diophantine constraint can be found in [27].

The condition that 2ν can be written as a sum of two squares is a necessary condition for the existence of solutions in the two circulant submatrices construction. For example, for $\nu = 26$,we have that $a = \pm 4$ and $b = \pm 6$. We can also have $a = \pm 6$ and $b = \pm 4$.

The fact that this condition is not sufficient can be illustrated by the case $\nu = 18$. In this case, the equation (4) has the solutions $a = 0$ and $b = \pm 6$ (or $a = \pm 6$ and $b = 0$) but the exhaustive search using the Hadamard ideal $\mathcal{H}_{18}$

shows that there are no solutions, i.e. there are no Hadamard matrices or order 36, with two circulant submatrices or order 18 each.

Another Diophantine constraint on the elements of the first rows of A and B is obtained by pre-multiplying and post-multiplying (2) by the row vector $p^T = [1, -1, \ldots, 1, -1]$. This constraint is:

$$a_\alpha^2 + b_\alpha^2 = 2\nu \tag{5}$$

where $a_\alpha = a_1 - a_2 + \cdots + a_{\nu-1} - a_\nu$ and $b_\alpha = b_1 - b_2 + \cdots + b_{\nu-1} - b_\nu$ are the alternating sums of the $a_i's$ and $b_i's$.

Indeed we have that $p^T AA^T p + p^T BB^T p = p^T I_n p$ implies

$$\nu(a_1 - a_2 + \cdots + a_{\nu-1} - a_\nu)^2 + \nu(b_1 - b_2 + \cdots + b_{\nu-1} - b_\nu)^2 = \nu(2\nu)$$

which gives $a_\alpha^2 + b_\alpha^2 = 2\nu$.

The fact that the sums and the alternating sums of the $a_i's$ and $b_i's$ satisfy the same Diophantine constraint can be used to reduce the number of candidate solutions at an early stage, namely before applying the PSD test. From numerical experiments for $\nu = 10$ and $\nu = 16$ we see that by using alternating sums we can eliminate more than 70% of the candidate solutions that satisfy (4).

Definition 2 *An even value of the parameter ν is called* admissible, *if the Diophantine equation $a^2 + b^2 = 2\,\nu$ has solutions.*

Therefore, the first ten admissible values of the parameter ν are: 2, 4, 8, 10, 16, 18, 20, 26, 32, 34.

The Diophantine constraint (4) can be used to accelerate the exhaustive and partial search programs by extracting linear equations that can be added to the Hadamard ideal. If (α, β) is a solution of the equation (4), then we obtain the linear equations

$$|a_1 + \ldots + a_\nu| = \alpha, \qquad |b_1 + \ldots + b_\nu| = \beta.$$

We note here that the methods of [20, 12] can be readily adapted to this problem, so that running times would be drastically shorter and more complete data could be obtained as well as higher orders could be reached.

4.2 Gröbner bases

Gröbner bases [5, 24] computations and analysis of the results of the exhaustive searches, reveal an interesting fact about how equation (3) is realized in solutions of the problem. In particular, we propose a heuristic decoupling of equation (3) based on the observation that if we assume that equation (3) is realized as

$$\sum_{i=1}^{m} \left(a_i a_{(i+m)}\right) = k, \text{ and } \sum_{i=1}^{m} \left(b_i b_{(i+m)}\right) = -k \tag{6}$$

where k is an integer, for all solutions for a fixed value of ν, then Gröbner bases computations reveal that

- for $\nu = 4$, we have that $k = 0$, by computing the reduced Gröbner basis of the ideal $\mathcal{H}_4$ augmented with two equations that come from the solutions of the Diophantine constraint $a^2 + b^2 = 8$

```
a1*a4+a1*a2+a2*a3+a3*a4+b1*b4+b1*b2+b2*b3+b3*b4,
a1 * a3 + a2 * a4 -k,
b1 * b3 + b2 * b4 +k,
a1 + a2 + a3 + a4 -2,
b1 + b2 + b3 + b4 -2,
a1^2-1, a2^2-1, a3^2-1, a4^2-1, b1^2-1, b2^2-1, b3^2-1, b4^2-1
```

  for an elimination ordering that eliminates k. We note that the Gröbner basis has 15 elements and was computed in Magma.

- for $\nu = 8$, we have that $k = 0$, by computing the reduced Gröbner basis of the ideal $\mathcal{H}_8$ augmented with two equations that come from the solutions of the Diophantine constraint $a^2 + b^2 = 16$

```
a1*a8+a1*a2+a2*a3+a3*a4+a4*a5+a5*a6+a6*a7+a7*a8+b1*b8+b1*b2
+b2*b3+b3*b4+b4*b5+b5*b6+b6*b7+b7*b8,
a1*a7+a2*a8+a1*a3+a2*a4+a3*a5+a4*a6+a5*a7+a6*a8+b1*b7+b2*b8
+b1*b3+b2*b4+b3*b5+b4*b6+b5*b7+b6*b8,
a1*a6+a2*a7+a3*a8+a1*a4+a2*a5+a3*a6+a4*a7+a5*a8+b1*b6+b2*b7
+b3*b8+b1*b4+b2*b5+b3*b6+b4*b7+b5*b8,
a1 * a5 + a2 * a6 + a3 * a7 + a4 * a8 -k,
b1 * b5 + b2 * b6 + b3 * b7 + b4 * b8 +k,
a1 + a2 + a3 + a4 + a5 + a6 + a7 + a8 ,
b1 + b2 + b3 + b4 + b5 + b6 + b7 + b8 -4,
a1^2-1, a2^2-1, a3^2-1, a4^2-1, a5^2-1, a6^2-1, a7^2-1, a8^2-1,
b1^2-1, b2^2-1, b3^2-1, b4^2-1, b5^2-1, b6^2-1, b7^2-1, b8^2-1
```

  for an elimination ordering that eliminates k. We note that the Gröbner basis has 237 elements and was computed in Magma.

Based on the assumption that for each admissible value of ν there is a value of k so that equation (3) is realized as described in (6), for all solutions for this fixed value of ν we can carry out an analysis for any admissible value of ν, in order to establish reasonable estimates for the value of k. We make use of the well-known fact that if x, y are ± 1 elements then we have

$$xy \equiv x + y - 1 (\bmod 4).$$

Upon reducing $\sum_{i=1}^{m} \left(a_i a_{(i+m)}\right) = k$ and $\sum_{i=1}^{m} \left(b_i b_{(i+m)}\right) = -k$ modulo 4 we obtain

$$a_1 + \ldots + a_\nu - m \equiv k \, (\bmod 4) \text{ and } b_1 + \ldots + b_\nu - m \equiv -k \, (\bmod 4)$$

(we remind here that $m = \frac{\nu}{2}$) which can be rewritten as:

$$k \equiv a - m (\bmod 4) \text{ and } k \equiv m - b (\bmod 4)$$

where a, b are solutions of $a^2 + b^2 = 2\nu$. Here are the solutions mod 4 of the first congruence above, for all admissible values of ν (except $\nu = 18, 36$), for $\nu \leq 50$.

ν	a	m	k
4	± 2	2	$\equiv 0(\bmod 4)$
8	$0, \pm 4$	4	$\equiv 0(\bmod 4)$
10	$\pm 2, \pm 4$	5	$\equiv 1(\bmod 4), \equiv 3(\bmod 4)$
16	± 4	8	$\equiv 0(\bmod 4)$
20	$\pm 2, \pm 6$	10	$\equiv 0(\bmod 4)$
26	$\pm 4, \pm 6$	13	$\equiv 1(\bmod 4), \equiv 3(\bmod 4)$
32	$0, \pm 8$	16	$\equiv 0(\bmod 4)$
34	$\pm 2, \pm 8$	17	$\equiv 1(\bmod 4), \equiv 3(\bmod 4)$
40	$\pm 4, \pm 8$	20	$\equiv 0(\bmod 4)$
50	$0, \pm 6, \pm 8, \pm 10,$	25	$\equiv 1(\bmod 4), \equiv 3(\bmod 4)$

These considerations on the possible values of k can be used to eliminate sequences that cannot give solutions.

4.3 PSD test

The PSD test [11] furnishes another necessary condition for the existence of solutions in the two circulant submatrices construction.

Definition 3 *The* Discrete Fourier Transform *sequence (DFT) of the sequence of length n, $A = [a_0, \ldots, a_{n-1}]$ is the sequence of length n:*

$$DFT_A = [\mu_0, \ldots, \mu_{n-1}], \text{ where } \mu_k = \sum_{i=0}^{n-1} a_i \omega^{ik}, \; k = 0, \ldots, n-1, \tag{7}$$

and where $\omega = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ is a primitive n-th root of unity (also called the principal n-th root of unity).

Definition 4 *The* Power Spectral Density *sequence (PSD) sequence of the sequence A is the sequence of length n:*

$$PSD_A = [\mid \mu_0^2 \mid, \ldots, \mid \mu_{n-1}^2 \mid]$$

i.e. the sequence of squared magnitudes of the elements of the sequence DFT_A.

We note that all elements of the PSD sequence of A are non-negative.

The following theorem is a direct consequence of the discussion in [11].

Theorem 1 *If the sequences $[a_1, \ldots, a_\nu]$ and $[b_1, \ldots, b_\nu]$ are solutions of the two circulant submatrices construction, then the corresponding components of their PSDs sum to the constant*

$$c = \frac{\nu \sum_{i=1}^{\nu} a_i^2 - \left(\sum_{i=1}^{\nu} a_i\right)^2}{\nu - 1} + \frac{\nu \sum_{i=1}^{\nu} b_i^2 - \left(\sum_{i=1}^{\nu} b_i\right)^2}{\nu - 1}.$$

In view of the Diophantine constraint (4), it is easy to see that we have $c = 2\nu$.

Taking into account the non-negativity of the terms of the PSD sequence, the PSD test for the two circulant submatrices construction can be expressed by saying that if a term of the PSD sequence of the sequence $[a_1, \ldots, a_\nu]$ (corresp. $[b_1, \ldots, b_\nu]$) exceeds 2ν then this sequence cannot yield a solution to the problem.

The importance of the PSD test lies in the fact that it can be applied to the sequences $[a_1, \ldots, a_\nu]$ and $[b_1, \ldots, b_\nu]$ separately.

5 Structure of the variety $V(\mathcal{H}_\nu)$

We summarize in the following table the computational results of exhaustive and partial searches obtained using the Hadamard ideals $\mathcal{H}_2$, ..., $\mathcal{H}_{34}$: (the symbol $\mid V(\mathcal{H}_\nu) \mid$ stands for the number of solutions of the system corresponding to the Hadamard ideal $\mathcal{H}_\nu$).

ν	$\mid V(\mathcal{H}_\nu) \mid$	
2	8	$= 2 \times 2^2$ exhaustive search
4	64	$= 4 \times 4^2$ exhaustive search
6	0	
8	1,536	$= 24 \times 8^2$ exhaustive search
10	6,400	$= 64 \times 10^2$ exhaustive search
12	0	
14	0	
16	229,376	$= 896 \times 16^2$ exhaustive search
18	0	
20	2,867,200	$= 7,168 \times 20^2$ exhaustive search
22	0	
24	0	
26	13,152,256	$= 19,456 \times 26^2$ exhaustive search
28	0	
30	0	
32	$\geq$ 723,901	partial search
34	$\geq$ 18,465	partial search
36	0	
40	$\geq$ 320	partial search

(8)

The value $\nu = 36$ is contained in the above table for completeness. We didn't perform computer searches for $\nu = 36$, because it is well-known that there are no Golay pairs for $\nu = 36$ [1] and that there are no sequences with zero periodic autocorrelation function [7].

The values $\nu = 42, 44, 46, 48$ are not admissible. The value $\nu = 50$ is admissible but no solutions are known, it is an open problem.
Examining table (8) our computational results can be stated concisely as:

Theorem 2 *For the first thirteen values $\nu = 2, \ldots, 26$, the resolution of the system corresponding to the Hadamard ideal $\mathcal{H}_\nu$ (Hadamard matrices constructible from 2 circulant submatrices by the method of C. H. Yang) indicates that*

$$| V(\mathcal{H}_\nu) | = h_\nu \cdot \nu^2$$

and that the proportionality constants are given by the sequence

ν	2	4	6	8	10	12	14	16	18	20	22	24	26
h_ν	2	4	0	24	64	0	0	896	0	7,168	0	0	19,456

6 Inequivalent Hadamard matrices

In this section we locate inequivalent Hadamard matrices, within the sets of Hadamard matrices we have computed. Due to the large amounts of matrices coming out of the exhaustive searches for $\nu = 16$ and $\nu = 20$, we work in two phases. First we use the 4-profile criterion [6] (as implemented in Magma 2.11) to identify inequivalent matrices within these sets. The 4-profile criterion is a necessary but not sufficient condition for Hadamard equivalence. This means that matrices with different 4-profiles are inequivalent, but matrices with equal 4-profiles may or may not be inequivalent. However, the profile criterion is extremely efficient and can be seen as a means of partitioning a set of matrices according to their 4-profiles. Then we use the graph isomorphism criterion [21, 22] (as implemented in Magma 2.11) to search for inequivalent matrices within the sets of matrices with equal profiles. The graph isomorphism criterion is a necessary and sufficient condition for Hadamard equivalence.

6.1 Inequivalent matrices via the 4-profile criterion

Using the 4-profile criterion (as implemented in Magma 2.11) to search for inequivalent Hadamard matrices made up from two circulant submatrices, we obtain the results in the table below.

ν	2	4	8	10	16	20	26	32	34	40
matrix order	4	8	16	20	32	40	52	64	68	80
ineq. matrices	1	1	2	1	10	56	99	857	167	4

(9)

It should be noted that the paper [11] contains many matrices of some of the above orders and even if these matrices are Hadamard equivalent to the matrices reported in the above table, that can only increase the numbers of inequivalent matrices.

In particular, we establish two new constructive lower bounds for the numbers of inequivalent Hadamard matrices of orders 52 and 68.

6.1.1 Two new constructive lower bounds for the numbers of inequivalent Hadamard matrices of orders 52 and 68

In this section we establish constructively two new lower bounds for the numbers of inequivalent Hadamard matrices of orders 52 and 68, by combining the inequivalent Hadamard matrices with two circulant submatrices, with inequivalent Hadamard matrices coming from other constructions. Denote by N_k the number of inequivalent Hadamard matrices of order k. We establish the inequalities

$$N_{52} \geq 743, \quad N_{68} \geq 515.$$

All the inequivalent Hadamard matrices constructed in this paper are available in the web page `http://www.cargo.wlu.ca/circulantSubmatrices` .

6.1.2 Order 52

Inequivalent sets of Hadamard matrices of order 52, are available from the following five sources:

1. 638 matrices, web page of Christos Koukouvinos;
2. 76 matrices, see [19]; (these are included in the 638 matrices mentioned above)
3. 4 matrices, 4 Williamson array construction;
4. 11 matrices, skew 4 Williamson array construction;
5. 99 matrices, see table (9) above.

Using the 4-profile criterion in the above 752 Hadamard matrices of order 52, we establish constructively a new lower bound for the number of inequivalent Hadamard matrices of order 52, i.e. $N_{52} \geq 743$.

6.1.3 Order 68

Inequivalent sets of Hadamard matrices of order 68, are available from the following five sources:

1. 2 matrices, web page of Christos Koukouvinos;
2. 338 matrices, see [19];
3. 5 matrices, 4 Williamson array construction;
4. 4 matrices, skew 4 Williamson array construction;
5. 167 matrices, see table (9) above.

Using the 4-profile criterion in the above 516 Hadamard matrices of order 68, we establish constructively a new lower bound for the number of inequivalent Hadamard matrices of order 68, i.e. $N_{68} \geq 515$.

6.2 Inequivalent matrices via the graph isomorphism criterion

Using the graph isomorphism criterion (as implemented in Magma 2.11) to search for inequivalent Hadamard matrices made up from two circulant submatrices for $\nu = 16$ and $\nu = 20$, we obtain the following refined results.

- for $\nu = 16$, there are 10 inequivalent Hadamard matrices of order 32 made up from two circulant submatrices. This result was obtained by applying the buckets algorithm [17] in the 8 sets corresponding to the 8 inequivalent matrices located with the 4-profile criterion. It may be interesting to remark that the set of 229,376 matrices of order 32 is separated in 10 subsets with respect to Hadamard equivalence and that six of these subsets are of cardinality $16,384 = 2^{14}$ and four of these subsets are of cardinality $32,768 = 2^{15}$.

- for $\nu = 20$, there are 56 inequivalent Hadamard matrices of order 40 made up from two circulant submatrices. This result was obtained by applying the buckets algorithm [17] in the 48 sets corresponding to the 48 inequivalent matrices located with the 4-profile criterion. It may be interesting to remark that the set of 2,867,200 matrices of order 40 is separated in 56 subsets with respect to Hadamard equivalence and that all of these subsets are of cardinality $51,200 = 2^{11}5^2$.

All the new inequivalent Hadamard matrices constructed in this section are available in the web page `http://www.cargo.wlu.ca/circulantSubmatrices` .

7 Acknowledgments

We thank the anonymous referee for their detailed comments and constructive suggestions that resulted in a substantially improved version of our paper. This work is supported in part by a grant from the National Sciences and Engineering Research Council of Canada, NSERC. All computations in Magma have been performed remotely at the *Centre de calcul formel MEDICIS, École Polytechnique, Paris, France.* All computations in Maple have been performed at the *Computer Algebra Research Group, CARGO, Wilfrid Laurier University, Waterloo, ON, Canada.* All computations in C have been performed remotely at *SHARCnet* and *WestGrid* high performance computing clusters.

8 Conclusion

In this paper we introduce the concept of Hadamard ideals to the study of Hadamard matrices constructible from two circulant submatrices for the construction of C. H. Yang. Hadamard ideals are used to perform exhaustive searches for the first seven admissible values 2, 4, 8, 10, 16, 18, 20 and partial searches for the next three admissible values 26, 32 and 34. From the solutions we found, for the admissible values 26 and 34, we located new inequivalent Hadamard matrices of orders 52 and 68 with two circulant submatrices, thus improving the lower bounds for the numbers of inequivalent Hadamard matrices of orders 52 and 68.

References

[1] T. H. Andres and R. G. Stanton, Golay sequences, *Combinatorial mathematics V*, (Proc. Fifth Austral. Conf., Roy. Melbourne Inst. Tech., Melbourne, 1976), Lecture Notes in Math., Vol. 622 (1977), 44-54.

[2] K. T. Arasu and Q. Xiang, On the existence of periodic complementary binary sequences, *Des. Codes Cryptogr.*, 2 (1992), Number 3, 257-262.

[3] L. Bömer and M. Antweiler, Periodic complementary binary sequences, *IEEE Trans. Inform. Theory*, 36, (1990), Number 6, 1487-1494.

[4] P. B. Borwein and R. A. Ferguson, A complete description of Golay pairs for lengths up to 100, *Math. Comp.*, 73 (2004) Number 246, 967-985.

[5] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms : an Introduction to Computational Algebraic Geometry and Commutative Algebra* UTM, Springer-Verlag, New York, 1992.

[6] J. Cooper, J. Milas, and W. D. Wallis, Hadamard equivalence, in Combinatorial Mathematics, Lecture Notes in Mathematics, Vol. 686, Springer-Verlag, Berlin, Heidelberg, New York, 1978, 126-135.

[7] D. Ž. Đoković, Note on periodic complementary sets of binary sequences, *Des. Codes Cryptogr.*, 13, (1998), Number 3, 251-256.

[8] D. Ž. Đoković, Equivalence classes and representatives of Golay sequences, *Discrete Math.*, 189, (1998), Number 1-3, 79-93.

[9] S. Eliahou, M. Kervaire, and B. Saffari, A new restriction on the lengths of Golay complementary sequences, *J. Combin. Theory Ser. A*, 55, (1990), Number 1, 49-59.

[10] K. Feng, P. J. Shiue and Q. Xiang, On aperiodic and periodic complementary binary sequences, *IEEE Trans. Inform. Theory*, 45, (1999), Number 1, 296-303.

[11] R. J. Fletcher, M. Gysin, and J. Seberry, Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices, *Australas. J. Combin.*, 23, (2001), 75-86.

[12] R. J. Fletcher, C. Koukouvinos and J. Seberry, New skew-Hadamard matrices of order $4 \cdot 59$ and new D-optimal designs of order $2 \cdot 59$, Discrete Math., 286, (2004), Number 3, 251-253.

[13] S. Georgiou and C. Koukouvinos, On equivalence of Hadamard matrices and projection properties, *Ars Combinatorica*, 69 (2003), 79-95.

[14] S. Georgiou, C. Koukouvinos and J. Seberry, Hadamard matrices, orthogonal designs and construction algorithms, Chapter 7, in *Designs 2002: Further Computational and Constructive Design Theory*, ed. W.D. Wallis, Kluwer Academic Publishers, Norwell, Massachusetts, 2003, 133-205.

[15] A.V. Geramita, and J. Seberry, *Orthogonal designs: Quadratic forms and Hadamard matrices*, Marcel Dekker, New York-Basel, 1979.

[16] M. Hall Jr, *Combinatorial Theory*, 2nd Ed., Wiley, 1998

[17] I. S. Kotsireas, C. Koukouvinos, Inequivalent Hadamard matrices with buckets, *J. Discrete Math. Sci. Cryptogr.* 7 (2004), Number 3, pp. 307-317.

[18] I. S. Kotsireas, C. Koukouvinos and J. Seberry, Hadamard ideals and Hadamard matrices with circulant core, *J. Combin. Math. Combin. Comput.* 57 (2006), 47-63.

[19] I. S. Kotsireas, C. Koukouvinos and J. Seberry, Hadamard ideals and Hadamard matrices with two circulant cores, *Europ. J. Combin.* 27 (2006), no. 5, 658-668.

[20] S. Kounias, C. Koukouvinos, N. Nikolaou, A. Kakos, The nonequivalent circulant D-optimal designs for $n \equiv 2 \bmod 4$, $n \leq 54$, $n = 66$, *J. Combin. Theory Ser. A*, 65, (1994), Number 1, 26-38.

[21] J. S. Leon, An algorithm for computing the automorphism group of a Hadamard matrix, *J. Combin. Theory Ser. A* 27 (1979) 289306.

[22] B. D. McKay, Hadamard equivalence via graph isomorphism, *Discrete Math.*, 27 (1979) 213 214.

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

[24] B. Sturmfels, *Solving Systems of Polynomial Equations*, American Mathematical Society, CBMS Regional Conference Series in Mathematics, 97, 2002.

[25] W. D. Wallis, A. P. Street and Jennifer Seberry Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard matrices*, Lecture Notes in Mathematics, Springer-Verlag, Vol. 292, 1972.

[26] C. H. Yang, On Hadamard matrices constructible by circulant submatrices, *Math. Comp.*, 25 (1971), 181-186.

[27] C. H. Yang, Maximal binary matrices and sum of two squares, *Math. Comput.*, 30, (1976), Number 133, 148-153.