Constructions for Hadamard matrices of Williamson type

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

Abstract: In this paper we examine the classical Williamson construction for Hadamard matrices, from the point of view of a striking analogy with isomorphisms of division algebras. By interpreting the 4 Williamson array as a matrix arising from the real quaternion division algebra, we construct Williamson arrays with 8 matrices, based on the real octonion division algebra. Using a Computational Algebra formalism we perform exhaustive searches for even-order 4-Williamson matrices up to 18 and odd- and even-order 8-Williamson matrices up to 9 and partial searches for even-order 4-Williamson matrices up to 22 and odd- and even-order 8-Williamson matrices for orders $10-13$. Using Magma, we conduct searches for inequivalent Hadamard matrices within all the sets of matrices obtained by exhaustive and partial searches. In particular, we establish constructively ten new lower bounds for the number of inequivalent Hadamard matrices of the consecutive orders 72, 76, 80, 84, 88, 92, 96, 100, 104 and 108.

1 Introduction

Hadamard matrices arise in Statistics, Combinatorics, Cryptography and other areas and have been studied extensively. It is well known that the order of an Hadamard matrix must be 1, 2 or a multiple of 4. An 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 [12, 15]. An important class of Hadamard matrices can be constructed based on the 4 Williamson array. We propose a Computational Algebra formalism to tackle the problem of constructing Hadamard matrices from a 4 Williamson array. We use our construction to construct Hadamard matrices from an 8 Williamson array.

[1]Wilfrid Laurier University, Department of Physics and Computer Science, 75 University Avenue West, Waterloo, Ontario N2L 3C5, Canada. Supported in part by a grant from NSERC.

[2]Department of Mathematics, National Technical University of Athens, Zografou 15773, Athens, Greece

2 Hadamard matrices from a 4 Williamson array

The classical Williamson construction for Hadamard matrices is based on the 4×4 array

$$H = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

where A, B, C, D are square matrices of order n, where n is a positive integer. When the matrices A, B, C, D are circulant and symmetric, with ± 1 elements, then H turns out to be an Hadamard matrix of order $4n$, i.e. we have $HH^T = 4nI_{4n}$. Let U be the matrix of order n

$$U = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} \tag{1}$$

which has the property $U^n = I_n$. Following Williamson, [9], we will use the matrix U to define the block matrices of order n in the four Williamson array, as polynomials in U with ± 1 coefficients. Then the block matrices will commute with each other. Moreover, by imposing symmetry conditions on the coefficients, the block matrices will be symmetric, in view of the fact that $U^T = U^{-1}$. The four matrices A, B, C, D are defined by polynomials in U as follows:

$$\begin{array}{rcccccccc} A & = & a_0 I_n & + & a_1 U & + & \cdots & + & a_{n-1} U^{n-1} \\ B & = & b_0 I_n & + & b_1 U & + & \cdots & + & b_{n-1} U^{n-1} \\ C & = & c_0 I_n & + & c_1 U & + & \cdots & + & c_{n-1} U^{n-1} \\ D & = & d_0 I_n & + & d_1 U & + & \cdots & + & d_{n-1} U^{n-1} \end{array} \tag{2}$$

where the $4n$ coefficients $a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1}, c_0, \dots, c_{n-1}, d_0, \dots, d_{n-1}$ satisfy the additional symmetry conditions

$$a_{n-i} = a_i, b_{n-i} = b_i, c_{n-i} = c_i, d_{n-i} = d_i, \ i = 1, \dots, n-1. \tag{3}$$

See [9] for more details.

If we decompose (conceptually) the matrix H into an Hadamard product[3] of a matrix $H_{(A,B,C,D)}$ and the matrix of signs H_s:

$$H = H_{(A,B,C,D)} \bullet H_s = \begin{pmatrix} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{pmatrix} \bullet \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{pmatrix}$$

[3] element-wise product, which we denote by $\bullet$

then we see that the matrix of signs H_s is itself an Hadamard matrix of order 4. This prompts us to consider what happens when we replace the H_s (which is a particular Hadamard matrix of order 4) with an arbitrary Hadamard matrix of order 4. It turns out that from the 768 possible Hadamard matrices of order 4, only 256 matrices (one third of all possible Hadamard matrices of order 4) are appropriate to be used as sign matrices H_s, in the sense that they preserve the property $HH^T = 4nI_{4n}$.
An example of an Hadamard matrix of order 4 that cannot be used as a sign matrix H_s (because the property $HH^T = 4nI_{4n}$ is violated) is:

$$\begin{pmatrix} 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 \end{pmatrix}.$$

The matrix H appears in the context of quaternions, which can be thought of as an extension of complex numbers and the first number system in the hierarchy of hypercomplex numbers. See [6, 16] for general background on quaternions. The next number system in the hierarchy of hypercomplex numbers is given by octonions. See [6, 13] for general background on octonions.

The real quaternion division algebra $\mathbb{H}$ is algebraically isomorphic to a certain 4-dimensional real matrix algebra given by the matrix H. This striking similarity raises the question whether it is possible to use similar isomorphisms of the real octonion division algebra $\mathbb{O}$ to construct Hadamard matrices via a Williamson array with 8 matrices. In this paper we show that this is indeed possible. The resulting construction of Hadamard matrices of orders $8n$ is illustrated with examples and solidified with exhaustive searches using Computational Algebra techniques.

3 Hadamard matrices from a 8 Williamson array

3.1 Left matrix representation of octonions

Consider the 8×8 matrix

$$W = \begin{pmatrix} A & -B & -C & -D & -E & -F & -G & -H \\ B & A & -D & C & -F & E & H & -G \\ C & D & A & -B & -G & -H & E & F \\ D & -C & B & A & -H & G & -F & E \\ E & F & G & H & A & -B & -C & -D \\ F & -E & H & -G & B & A & D & -C \\ G & -H & -E & F & C & -D & A & B \\ H & G & -F & -E & D & C & -B & A \end{pmatrix}$$

which specifies the left matrix representation of an octonion $\alpha \in \mathbb{O}$ over the set of real numbers. See [14] for a complete derivation of this matrix.
Following the classical Williamson construction we first view A, B, C, D, E, F, G, H as numbers and we obtain:

$$WW^T = (A^2 + B^2 + C^2 + D^2 + E^2 + F^2 + G^2 + H^2) \times I_8.$$

Moreover, when A, B, C, D, E, F, G, H, are symmetric square matrices of order n that commute with each other, then we will have

$$WW^T = 8nI_{8n}$$

which says that W is an Hadamard matrix of order I_{8n} (provided these eight matrices have ± 1 elements). In [8] eight matrices that satisfy these conditions are called Williamson matrices.
For completeness we mention here an exact construction guaranteeing that the eight matrices A, B, C, D, E, F, G, H are symmetric and commute with each other, mimicking the construction for the matrices A, B, C, D appearing in the classical Williamson construction, see [9].
Let U be the matrix (1) and take the eight matrices A, B, C, D, E, F, G, H to be polynomials in U as in (2). Since $U^T = U^{-1}$, the eight matrices A, B, C, D, E, F, G, H will be symmetric if

$$a_{n-i} = a_i, b_{n-i} = b_i, c_{n-i} = c_i, d_{n-i} = d_i,$$

$$e_{n-i} = e_i, f_{n-i} = f_i, g_{n-i} = g_i, h_{n-i} = h_i,$$

for $i = 1, \ldots, n-1$.

When the coefficients $a_0, \ldots,, h_{n-1}$ are all ± 1 then W will be a matrix with $\pm$ entries satisfying the equation $WW^T = 8nI_{8n}$, i.e. W will be an Hadamard matrix of order $8n$.

3.2 Right matrix representation of octonions

Consider the 8×8 matrix

$$W = \begin{pmatrix} A & -B & -C & -D & -E & -F & -G & -H \\ B & A & D & -C & F & -E & -H & G \\ C & -D & A & B & G & H & -E & -F \\ D & C & -B & A & H & -G & F & -E \\ E & -F & -G & -H & A & B & C & D \\ F & E & -H & G & -B & A & -D & C \\ G & H & E & -F & -C & D & A & -B \\ H & -G & F & E & -D & -C & B & A \end{pmatrix}$$

which specifies the right matrix representation of an octonion $\alpha \in \mathbb{O}$ over the set of real numbers. See [14] for a complete derivation of this matrix.
Following the classical Williamson construction we first view A, B, C, D, E, F, G, H as numbers and we obtain:

$$WW^T = (A^2 + B^2 + C^2 + D^2 + E^2 + F^2 + G^2 + H^2) \times I_8.$$

From this point on, using the conditions of the last paragraph on the matrices A, B, C, D, E, F, G, H, we obtain another construction for Hadamard matrices.
Note: The 4 Williamson arrays of section 2 and the 8 Williamson arrays of section 3 are in essence orthogonal designs described in [8]. The facts that these arrays can be interpreted via isomorphisms of division algebras and that the sign matrices are Hadamard matrices seem to be new.

4 Williamson matrices via Computational Algebra

In this section we analyze Hadamard matrices of the Williamson type with 4 and 8 matrices, using Computational Algebra. The analogies between the two constructions are preserved at the ideals/varieties level. We use our Computational Algebra formalism to perform exhaustive and partial searches and thus obtain several Hadamard matrices of orders $4n$ and $8n$. Our Computational Algebra formalism and techniques are applied here for the first time, to the problem of searching for Hadamard matrices of the Williamson type from the 4 and 8 Williamson arrays. Several optimizations and vast improvements for this kind of search are still possible, see [11] for instance, but we postpone the application of optimized techniques in a future work. We were unable to find any previous work in the literature pertaining to exhaustive and partial searches for even-order Williamson matrices and exhaustive and partial searches for the

8 Williamson array. The motivation for undertaking these searches for all orders from the beginning, lies in the belief that the sequence of the numbers of solutions for all values of the parameters, should be studied as an indivisible entity. For each construction separately, properties of the associated sequence such as lacunarity, monotonicity and rate of growth, provide useful insights in the structure of the sets of solutions, whether or not symmetries are taken into account.

The exhaustive and partial searches reported below, have been performed with automatically generated serial C programs at the Computer Algebra Research Group, CARGO, Wilfrid Laurier University and remotely at the *Centre de calcul formel MEDICIS, École Polytechnique, Paris, France*, SHARCnet high-performance computing clusters (University of Western Ontario) and WestGrid high-performance computing clusters (Simon Fraser University, University of British Columbia, University of Calgary).

The automatic generation of C code was performed using the `CodeGeneration` package of Maple. Using this tool offers the advantage that any modifications and optimizations in the original Maple code, are reflected automatically in the generated C code. Two such optimizations are to take into account the decoupled structure of the equations and the diophantine constraints on the generators of the cyclic submatrices.

the search for inequivalent Hadamard matrices in each order, has been performed with Magma V2.11-2 running on machines at the *Centre de calcul formel MEDICIS, École Polytechnique, Paris, France.* In particular we used the Magma command `HadamardInvariant` which computes the 4-profile of an Hadamard matrix.

4.1 4 Williamson array via Computational Algebra

4.1.1 $n = 3$

Taking four square matrices of order $n = 3$ satisfying the conditions of the classical Williamson construction, we see that the coefficients of the polynomials must satisfy the algebraic equation

$$2 + a_0a_1 + b_0b_1 + c_0c_1 + d_0d_1 = 0 \tag{4}$$

where the eight unknowns a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 can only take ± 1 values. An exhaustive search shows that there are precisely 64 solutions with ± 1 elements to equation (4). These solutions are given in the table below in the format [solution number,$a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1$].

[1, −1, −1, −1, 1, −1, 1, −1, 1]
[3, −1, −1, −1, 1, 1, −1, −1, 1]
[5, −1, −1, 1, −1, −1, 1, −1, 1]
[7, −1, −1, 1, −1, 1, −1, −1, 1]
[9, −1, 1, −1, −1, −1, 1, −1, 1]
[11, −1, 1, −1, −1, 1, −1, −1, 1]
[13, −1, 1, −1, 1, −1, −1, −1, 1]
[15, −1, 1, −1, 1, −1, 1, −1, −1]
[17, −1, 1, −1, 1, 1, −1, −1, −1]
[19, −1, 1, −1, 1, 1, 1, −1, 1]
[21, −1, 1, 1, −1, −1, −1, −1, 1]
[23, −1, 1, 1, −1, −1, 1, −1, −1]
[25, −1, 1, 1, −1, 1, −1, −1, −1]
[27, −1, 1, 1, −1, 1, 1, −1, 1]
[29, −1, 1, 1, 1, −1, 1, −1, 1]
[31, −1, 1, 1, 1, 1, 1, −1, −1, 1]
[33, 1, −1, −1, −1, −1, 1, −1, −1, 1]
[35, 1, −1, −1, −1, 1, −1, −1, 1]
[37, 1, −1, −1, 1, −1, −1, −1, 1]
[39, 1, −1, −1, 1, −1, 1, −1, −1]
[41, 1, −1, −1, 1, 1, −1, −1, −1]
[43, 1, −1, −1, 1, 1, 1, −1, 1]
[45, 1, −1, 1, −1, −1, −1, −1, 1]
[47, 1, −1, 1, −1, −1, 1, −1, −1]
[49, 1, −1, 1, −1, 1, −1, −1, −1]
[51, 1, −1, 1, −1, 1, 1, −1, 1]
[53, 1, −1, 1, 1, −1, 1, −1, 1]
[55, 1, −1, 1, 1, 1, −1, −1, 1]
[57, 1, 1, −1, 1, −1, 1, −1, 1]
[59, 1, 1, −1, 1, 1, −1, −1, 1]
[61, 1, 1, 1, −1, −1, 1, −1, 1]
[63, 1, 1, 1, −1, 1, −1, −1, 1]

[2, −1, −1, −1, 1, −1, 1, 1, −1]
[4, −1, −1, −1, 1, 1, −1, 1, −1]
[6, −1, −1, 1, −1, −1, 1, 1, −1]
[8, −1, −1, 1, −1, 1, −1, 1, −1]
[10, −1, 1, −1, −1, −1, 1, 1, −1]
[12, −1, 1, −1, −1, 1, −1, 1, −1]
[14, −1, 1, −1, 1, −1, −1, 1, −1]
[16, −1, 1, −1, 1, −1, 1, 1, 1]
[18, −1, 1, −1, 1, 1, −1, 1, 1]
[20, −1, 1, −1, 1, 1, 1, 1, −1]
[22, −1, 1, 1, −1, −1, −1, 1, −1]
[24, −1, 1, 1, −1, −1, 1, 1, 1]
[26, −1, 1, 1, −1, 1, −1, 1, 1]
[28, −1, 1, 1, −1, 1, 1, 1, −1]
[30, −1, 1, 1, 1, −1, 1, 1, −1]
[32, −1, 1, 1, 1, 1, −1, 1, −1]
[34, 1, −1, −1, −1, −1, 1, 1, −1]
[36, 1, −1, −1, −1, 1, −1, 1, −1]
[38, 1, −1, −1, 1, −1, −1, 1, −1]
[40, 1, −1, −1, 1, −1, 1, 1, 1]
[42, 1, −1, −1, 1, 1, −1, 1, 1]
[44, 1, −1, −1, 1, 1, 1, 1, −1]
[46, 1, −1, 1, −1, −1, −1, 1, −1]
[48, 1, −1, 1, −1, −1, 1, 1, 1]
[50, 1, −1, 1, −1, 1, −1, 1, 1]
[52, 1, −1, 1, −1, 1, 1, 1, −1]
[54, 1, −1, 1, 1, −1, 1, 1, −1]
[56, 1, −1, 1, 1, 1, −1, 1, −1]
[58, 1, 1, −1, 1, −1, 1, 1, −1]
[60, 1, 1, −1, 1, 1, −1, 1, −1]
[62, 1, 1, 1, −1, −1, 1, 1, −1]
[64, 1, 1, 1, −1, 1, −1, 1, −1]

Note: The last of the solutions (the one numbered 64) given above, is the same as the solution in the example given in page 253 of [9]. This exhaustive search documents the fact that there are exactly 64 Hadamard matrices of order 12 coming out of the classical Williamson construction.

4.1.2 $n = 5$

Taking four square matrices of order $n = 5$ satisfying the conditions of the classical Williamson construction, we see that the coefficients of the polynomials must satisfy the system of two algebraic equations

$$\begin{aligned} 2 + a_0a_2 + a_2a_1 + b_0b_2 + b_2b_1 + c_0c_2 + c_2c_1 + d_0d_2 + d_2d_1 &= 0 \\ 2 + a_0a_1 + a_2a_1 + b_0b_1 + b_2b_1 + c_0c_1 + c_2c_1 + d_0d_1 + d_2d_1 &= 0 \end{aligned} \tag{5}$$

where the twelve unknowns a_0, a_1, a_2, b_0, b_1, b_2, c_0, c_1, c_2, d_0, d_1, d_2 can only take ± 1 values. An exhaustive search shows that there are precisely 192 solutions with ± 1 elements to equations (5). The last solution found is:

$$a_0 = 1,\ a_1 = 1,\ a_2 = -1,\ b_0 = 1,\ b_1 = 1,\ b_2 = -1,$$

$$c_0 = 1,\ c_1 = -1,\ c_2 = 1,\ d_0 = 1,\ d_1 = -1,\ d_2 = 1.$$

These solutions give rise to 192 Hadamard matrices or order 20 coming out of the classical Williamson construction.

4.1.3 Synopsis of the results

In this paragraph, we present a synopsis of the results of exhaustive and partial searches for $(n = 3, \ldots, 27)$ we have obtained using our algebraic formalism for the 4 Williamson array.

n	matrix order $4n$	number of unknowns $2n+2, n$ odd $2n+4, n$ even	number of solutions	$\mid V(\mathcal{W}_n^4) \mid$	number of inequivalent matrices
3	12	8	$64 =$	1×2^6	1
4	16	12	$256 =$	4×2^6	2
5	20	12	$192 =$	3×2^6	1
6	24	16	$1,536 =$	24×2^6	1
7	28	16	$960 =$	15×2^6	2
8	32	20	$1,536 =$	24×2^6	2
9	36	20	$2,112 =$	33×2^6	3
10	40	24	$7,680 =$	120×2^6	2
11	44	24	$1,920 =$	30×2^6	1
12	48	28	$16,384 =$	256×2^6	4
13	52	28	$5,184 =$	81×2^6	4
14	56	32	$87,552 =$	$1,368 \times 2^6$	9
15	60	32	$4,608 =$	72×2^6	6
16	64	36	$24,576 =$	384×2^6	5
17	68	36	$6,144 =$	96×2^6	5
18	72	40	$622,080 =$	$9,720 \times 2^6$	64
19	76	40	$14,400 =$	225×2^6	10
20	80	44	$\geq 403,046$	partial search	49
21	84	44	$11,904 =$	186×2^6	12
22	88	48	≥ 152744	partial search	52
23	92	48	$4,224 =$	66×2^6	2
25	100	52	$\geq 9,077$	partial search	17
27	108	56	≥ 610	partial search	11

Remark:
In the table above, despite the fluctuations of the size of the numbers, we remark a certain divisibility property satisfied by all the elements of the sequence of numbers $\mid V(\mathcal{W}_n^4) \mid$, namely:

$$\mid V(\mathcal{W}_n^4) \mid \equiv 0 \pmod{64}.$$

Moreover, it is known that there are no Hadamard matrices of the Williamson type for the 4 Williamson array for $n = 35$, i.e. $\mid V(\mathcal{W}_{35}^4) \mid = 0$. However, the divisibility property is still (trivially) satisfied even in such cases. The fact that there are no Williamson matrices of order 35 was first proved in [7], by an exhaustive computer search. This was also confirmed by an independent search in [10]. A table with values $n < 1000$ for which Williamson type matrices of order n are not known is given in [5].

4.2 8 Williamson array via Computational Algebra

4.2.1 $n = 3$

Taking eight square matrices of order $n = 3$ satisfying the conditions of the 8 Williamson array construction, we see that the coefficients of the polynomials

must satisfy the algebraic equation

$$4 + a_0a_1 + b_0b_1 + c_0c_1 + d_0d_1 + e_0e_1 + f_0f_1 + g_0g_1 + h_0h_1 = 0 \qquad (6)$$

where the sixteen unknowns a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1, e_0, e_1, f_0, f_1, g_0, g_1, h_0, h_1 can only take ± 1 values. An exhaustive search shows that there are precisely 7168 solutions with ± 1 elements to equations (6). Solutions are presented used the order of variables: a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1, e_0, e_1, f_0, f_1, g_0, g_1, h_0, h_1. The first solution found is:

$$- - - - - + - + - + - + - + - +$$

The last solution found is:

$$+ + + + + - + - + - + - + - + -$$

Note that the last solution is exactly the first solution, multiplied by -1. These solutions give rise to 7,168 Hadamard matrices of order 24 coming out of the 8 Williamson array construction.

4.2.2 $n = 5$

Taking eight square matrices of order $n = 5$, subject to the conditions described at the end of paragraph 3.1, in the 8 Williamson array, we see that the coefficients of the polynomials must satisfy the system of two algebraic equations

$$\begin{aligned} &4 + a_0a_1 + a_1a_2 + b_0b_1 + b_1b_2 + c_0c_1 + c_1c_2 + d_0d_1 + d_1d_2 + \\ &+e_0e_1 + e_1e_2 + f_0f_1 + f_1f_2 + g_0g_1 + g_1g_2 + h_0h_1 + h_1h_2 = 0 \\ &4 + a_0a_2 + a_1a_2 + b_0b_2 + b_1b_2 + c_0c_2 + c_1c_2 + d_0d_2 + d_1d_2 + \\ &+e_0e_2 + e_1e_2 + f_0f_2 + f_1f_2 + g_0g_2 + g_1g_2 + h_0h_2 + h_1h_2 = 0 \end{aligned} \qquad (7)$$

where the twenty four unknowns a_0, ..., h_2, can only take ± 1 values as usual. An exhaustive search shows that there are precisely 394,240 solutions with ± 1 elements to equations (7). The first solution found is:

$$- - - - - + - - + - - + - + - - + - - + - - - + +$$

The last solution found is:

$$+ + + + + - + + - + + - + - + + - + + - + + - -$$

Note that the last solution is exactly the first solution, multiplied by -1. These solutions give rise to 394,240 Hadamard matrices or order 40 coming out of the 8 Williamson array.

4.2.3 $n = 7$

Taking eight square matrices of order $n = 7$, subject to the conditions described at the end of paragraph 3.1, in the 8 Williamson array, we obtain a system of three equations in the thirty two binary unknowns $a_0, \ldots, h_3$. An exhaustive search shows that there are precisely 11,289.600 solutions with ± 1 elements to these equations.
The first solution found is:

$$- - - + - - - + - - - + - - - + - - + - - - + - - + - + - + - +$$

The last solution found is:

$$+ + + - + + + - + + + - + + + - + + - + + + - + + - + - + - + -$$

Note that the last solution is exactly the first solution, multiplied by -1. These solutions give rise to 11,289,600 Hadamard matrices or order 56 coming out of the 8 Williamson array construction.

4.2.4 $n = 9$

Taking eight square matrices of order $n = 9$, subject to the conditions described at the end of paragraph 3.1, in the 8 Williamson array, we obtain a system of four equations in the forty binary unknowns $a_0, \ldots, h_4$. An exhaustive search shows that there are precisely 241,597,440 solutions with ± 1 elements to these equations.
The first solution found is:

$$- - - - + - - - - + - - - + + - - + + - - + - - + - + - + - - + -$$
$$+ + - + + - +$$

The last solution found is:

$$+ + + + - + + + + - + + + - - + + - - + + - + + - + - + - + + - +$$
$$- - + - - + -$$

Note that the last solution is exactly the first solution, multiplied by -1. The solutions give rise to 241,597,440 Hadamard matrices of order 72 coming out of the 8 Williamson array construction.

4.2.5 Synopsis of the results

In this paragraph, we present a synopsis of the results of exhaustive ($n = 3, \ldots, 9$) and partial ($n = 10, 11, 12, 13$) searches we have obtained using our algebraic formalism for the 8 Williamson array.

n	matrix order $8n$	number of unknowns $4n+4$ n odd $4n+8$ n even	number of solutions	$\mid V(\mathcal{W}_n^8) \mid$	number of inequivalent matrices
3	24	16	$7,168 =$	7×2^{10}	2
4	32	24	$65,536 =$	64×2^{10}	3
5	40	24	$394,240 =$	385×2^{10}	8
6	48	32	$10,608,640 =$	$10,360 \times 2^{10}$	17
7	56	32	$11,289,600 =$	$11,025 \times 2^{10}$	30
8	64	40	$775,290,880 =$	$757,120 \times 2^{10}$	60
9	72	40	$241,597,440 =$	$235,935 \times 2^{10}$	418
10	80	48	$\geq 1,137,151,116$	partial search	76
11	88	48	$\geq 129,902,861$	partial search	1,074
12	96	56	$\geq 100,055,428$	partial search	2,664
13	104	56	$\geq 1,854,318$	partial search	1,714

Remark 1:
In the table above, we remark an exponentially increasing sequence of numbers of solutions, contrary to the 4 Williamson array case;

Remark 2:
In the table above, we also remark an analogous divisibility property satisfied by all the elements of the sequence of numbers $\mid V(\mathcal{W}_n^8) \mid$, namely:

$$\mid V(\mathcal{W}_n^8) \mid \equiv 0 \pmod{1024}.$$

5 Inequivalence of solutions

We describe three different concepts of inequivalence of solutions for Williamson matrices constructed via the 4 and 8 Williamson arrays.

- `Naive definition`: two solutions are inequivalent if they consist of different sequences of plus signs and minus signs;
- `Hadamard inequivalence`: two solutions are inequivalent if they give rise to inequivalent Hadamard matrices;
- `Williamson equivalence`: suppose that we have a solution specified by a quadruple of Williamson matrices of order m, $A = circ(a_0, \ldots, a_{m-1})$, $B = circ(b_0, \ldots, b_{m-1})$, $C = circ(c_0, \ldots, c_{m-1})$, $D = circ(d_0, \ldots, d_{m-1})$. Then applying the transformation $j \to js(\mod m)$, $(s, m) = 1$, we obtain another quadruple of Williamson matrices. These quadruples are called equivalent and we need to know only one quadruple from each equivalence class. In each equivalence class there are at most $\frac{\phi(m)}{2}$ such quadruples

where $\phi(m)$ is the number of integers s such that $(s,m) = 1, 0 < s < m$ (Euler totient function). This is because some quadruples may be transformed into themselves and the transformations $j \rightarrow js(\mod m)$ and $j \rightarrow j(m-s)(\mod m)$ are identical due to the symmetry of A, B, C, D.

These three different concepts of inequivalence of solutions, give rise to three different counts for the solutions respectively. The naive definition gives rise to the raw count (exhaustive searches). The Hadamard inequivalence definition accounts for the numbers of inequivalent Hadamard matrices that are also Williamson matrices from the 4 or 8 Williamson arrays. The Williamson equivalence definition is the only one of these three concepts that accounts satisfactorily for the many symmetries that Williamson matrices have.

Remark 1: The distinction between Hadamard and Williamson equivalence is further clarified by the fact that negation of D in the Williamson array produces a matrix that is Hadamard equivalent to the transpose of the Williamson array. This fact, combined with the fact that some Williamson matrices are not self-dual presumably explains all discrepancies between the numbers of Hadamard inequivalent matrices and the numbers of Williamson inequivalent matrices.

Remark 2: It is important to point out that two solutions may be Williamson equivalent, but at the same time giving rise to Hadamard matrices of the Williamson type, which are Hadamard inequivalent. For example, it is well-known (see [3]) that the number of distinct (Williamson inequivalent) solutions of the Williamson equations for $n = 23$ (order $4 \times 23 = 92$) is 1. There is only one solution of the Williamson equations for $n = 23$ (order $4 \times 23 = 92$) up to Williamson equivalence. In [3], this unique solution is given as:

```
1-11-11--111111--11-11-  (a0, ..., a23)
--111-111-1--1-111-111-  (b0, ..., b23)
111---11-1-11-1-11---11  (c0, ..., c23)
111-111-1------1-111-11  (d0, ..., d23)
```

However, we computed 2 inequivalent Hadamard matrices of order 92 from the 4 Williamson array for $n = 23$. These two inequivalent Hadamard matrices of order 92 are specified via the two solutions given below.

(1)

```
1--1--111------111--1--  (a0, ..., a23)
---111--11----11--111--  (b0, ..., b23)
-11--1-1-1----1-1-1--11  (c0, ..., c23)
-11-1-1----------1-1-11  (d0, ..., d23)
```

(2)

```
1--1--111------111--1--  (a0, ..., a23)
```

```
---111--11----11--111--  (b0, ..., b23)
-11--1-1-1----1-1-1--11  (c0, ..., c23)
1--1-1-1111111111-1-1--  (d0, ..., d23)
```

These two solutions are Williamson equivalent, because their a, b, c components are exactly the same and the d components of the second solution is equal to the d component of the first solution multiplied by -1. However, these two solutions give rise to two inequivalent Hadamard matrices, because the corresponding Hadamard matrices have different 4-profiles

```
[ 1687556, 855692, 217120, 30452, 3036, 184, 0, 92, 0, 0, 23, 0 ]
[ 1691972, 845756, 225400, 27508, 3036, 368, 0, 92, 0, 0, 23, 0 ]
```

as computed with Magma's `HadamardInvariant` command. As an additional consistency check, we also used the graph isomorphism criterion, as implemented in Magma's `IsHadamardEquivalent` command to check the inequivalence of these two Hadamard matrices. In summary, equivalent Williamson solutions give rise to equivalent or inequivalent Hadamard matrices. This is a subtle distinction between Hadamard equivalence and Williamson equivalence. A nice survey on the (Williamson) inequivalent 4-Williamson matrices for each order up to $4 \times 37 = 148$ is presented in [10]. In the present paper, we are interested in Hadamard inequivalent matrices of the Williamson type, constructed from the 4 and 8 Williamson arrays.

5.1 Inequivalent Hadamard matrices from the 4 and 8 Williamson arrays

In this section we summarize the computational results on locating inequivalent Hadamard matrices within the sets of Hadamard matrices computed in the previous section. We analyzed the corresponding solution sets with Magma V2.11 to search for inequivalent Hadamard matrices. See [1] for a full description of Magma V2.11 available functionality for Hadamard matrices. We used the profile criterion to distinguish between inequivalent Hadamard matrices. The profile criterion is a necessary (but not sufficient) condition for Hadamard inequivalence. Hadamard matrices with unequal 4-profiles are inequivalent. However, Hadamard matrices with equal profiles may or may not be inequivalent. The profile criterion has been implemented in Magma's `HadamardInvariant` command. See [4] for more details on the profile criterion.

All the inequivalent matrices we located in this paper, are given in the web page `http://www.cargo.wlu.ca/hi48` in Magma format, together with programs to convert them to other formats.

Remark: The graph isomorphism criterion is a necessary and sufficient condition for Hadamard inequivalence. The graph isomorphism criterion has been implemented in Magma's `IsHadamardEquivalent` command. Because we are

using the profile criterion to locate inequivalent Hadamard matrices, it is possible that the actual numbers of the inequivalent Hadamard matrices within the solution sets we computed, are somewhat larger. This is why in the result tables below, we only give lower bounds for the number of inequivalent Hadamard matrices.

Notation: Let N_n denote the number of inequivalent Hadamard matrices of order n.

Our computations using the 4 Williamson array and the 8 Williamson array, establish ten new lower bounds for N_n, summarized in the following tables: (we mention that no 4-Williamson matrix is Hadamard equivalent to any 8-Williamson matrix of the same order)

n	72	76	80
N_n	$\geq 482\ (= 64 + 418)$	≥ 10	$\geq 125\ (= 49 + 76)$
	$4W, n = 18$ $8W, n = 9$	$4W, n = 19$	$4W, n = 20$ $8W, n = 10$

n	84	88
N_n	≥ 12	$\geq 1,126\ (= 52 + 1,074)$
	$4W, n = 21$	$4W, n = 22$ $8W, n = 11$

n	92	96	100	104	108
N_n	≥ 2	$\geq 2,664$	≥ 17	$\geq 1,714$	≥ 11
	$4W, n = 23$	$8W, n = 12$	$4W, n = 25$	$8W, n = 13$	$4W, n = 27$

6 Acknowledgments

The authors thank the anonymous referee for many constructive comments. insightful suggestions and positive criticisms, as well as Remark 1 on the distinction between Hadamard and Williamson equivalence. This work is supported in part by a grant from the National Sciences and Engineering Research Council of Canada, NSERC. The prototype C programs were generated via Maple at the *Computer Algebra Research Group, CARGO, Wilfrid Laurier University*, Waterloo ON, Canada. All computations in Magma have been performed remotely at the *Centre de calcul formel MEDICIS, École Polytechnique* Paris, France. All computations in C have been performed remotely at *SHARCnet high performance computing clusters, University of Western Ontario*, London ON, Canada and *WestGrid high performance computing clusters, University of British Columbia, Simon Fraser University*, Vancouver BC, Canada, *University of Calgary*, Calgary AB, Canada.

7 Conclusion

In this paper we study constructions of Hadamard matrices from 4 and 8 Williamson arrays, by exploiting a noticeable similarity between the classical

Williamson construction and a matrix representation of the algebra of quaternions. We establish a Computational Algebra formalism for Hadamard matrices from 4 and 8 Williamson arrays. Using this formalism we search for inequivalent Hadamard matrices of various orders using the Computational Algebra system Magma and High-performance computing. We establish constructively ten new lower bounds for the number of inequivalent Hadamard matrices of the consecutive orders 72, 76, 80, 84, 88, 92, 96, 100, 104 and 108.

References

[1] G. Bailey, *Hadamard matrices* in J. Cannon and W. Bosma, *Handbook of Magma functions*, Version 2.11, Sydney, 2004, Chapter 112, 3456-3462.

[2] L. D. Baumert, S.W. Golomb and M. Hall Jr., Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.*, 68 (1962), 237-238.

[3] L. D. Baumert and M. Hall Jr., Hadamard matrices of the Williamson type, *Math. Comput.*, 19 (1965), 442-447.

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

[5] R. Craigen, Hadamard Matrices and Designs, in *The CRC Handbook of Combinatorial Designs*, (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, Fla., 1996, pp. 370-377.

[6] G. M. Dixon, *Division algebras: octonions, quaternions, complex numbers and the algebraic design of physics*, Mathematics and its Applications, 290, Kluwer Academic Publishers Group, Dordrecht, 1994.

[7] D. Z. Djokovic, Williamson matrices of order 4n for n=33,35,39, *Discrete Math.*, 115 (1993), pp. 267-271.

[8] A. V. Geramita and J. Seberry, *Orthogonal designs. Quadratic forms and Hadamard matrices*, Lecture Notes in Pure and Applied Mathematics, 45. Marcel Dekker, Inc., New York, 1979.

[9] M. Hall, Jr. *Combinatorial theory*, Reprint of the 1986 second edition, Wiley Classics Library, 1998. Wiley, New York.

[10] J. Horton, C. Koukouvinos and J. Seberry, A search for Hadamard matrices constructed from Williamson matrices, *Bull. Inst. Combin. Appl.* 35, 2002, pp. 75–88.

[11] C. Koukouvinos and S. Kounias, Hadamard matrices of the Williamson type of order 4m, m=pq. An exhaustive search for m=33, *Discrete Math.*, 68 (1988), 45-57.

[12] 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.

[13] T. A. Springer and F. D. Veldkamp, *Octonions, Jordan algebras and exceptional groups*, Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[14] Y. Tian, Matrix representations of octonions and their applications, *Advances in Applied Clifford Algebras*, 10 (2000), no. 1, pp. 61-90.

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

[16] J. P. Ward, *Quaternions and Cayley numbers. Algebra and applications*, Mathematics and its Applications, 403. Kluwer Academic Publishers Group, Dordrecht, 1997.