July 2006

Hadamard ideals and Hadamard matrices with two circulant cores

I. S. Kotsireas
Wilfrid Laurier University, Ontario, Canada

C. Koukouvinos
National Technical University of Athens, Greece

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Hadamard ideals and Hadamard matrices with two circulant cores

Abstract

We apply Computational Algebra methods to the construction of Hadamard matrices with two circulant cores, given by Fletcher, Gysin and Seberry. We introduce the concept of Hadamard ideal, to systematize the application of Computational Algebra methods for this construction. We use the Hadamard ideal formalism to perform exhaustive search constructions of Hadamard matrices with two circulant cores for the twelve orders 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52. The total number of such Hadamard matrices is proportional to the square of the parameter. We use the Hadamard ideal formalism to compute the proportionality constants for the twelve orders listed above. Finally, we use the Hadamard ideal formalism to improve the lower bounds for the number of inequivalent Hadamard matrices for the seven orders 44, 48, 52, 56, 60, 64, 68.

Keywords

Hadamard Matrices, Computational Algebra, Hadamard ideal, Hadamard equivalence, algorithm, 1991 MSC: 05B20, 13P10

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as: Kotsireas, IS, Koukouvinos, C & Seberry, J, Hadamard ideals and Hadamard matrices with two circulant cores, European Journal of Combinatorics, 2006, 27(5), 658-668. The original journal can be found here.

Hadamard ideals and Hadamard matrices with two circulant cores

Ilias S. Kotsireas [a,1,*] , Christos Koukouvinos [b] and Jennifer Seberry [c]

[a] *Wilfrid Laurier University, Department of Physics and Computer Science, 75 University Avenue West, Waterloo, Ontario N2L 3C5, Canada*

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

[c] *Centre for Computer Security Research, School of Information Technology and Computer Science, University of Wollongong, Wollongong, NSW 2522, Australia*

Abstract

We apply Computational Algebra methods to the construction of Hadamard matrices with two circulant cores, given by Fletcher, Gysin and Seberry. We introduce the concept of Hadamard ideal, to systematize the application of Computational Algebra methods for this construction. We use the Hadamard ideal formalism to perform exhaustive search constructions of Hadamard matrices with two circulant cores for the twelve orders 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52. The total number of such Hadamard matrices is proportional to the square of the parameter. We use the Hadamard ideal formalism to compute the proportionality constants for the twelve orders listed above. Finally, we use the Hadamard ideal formalism to improve the lower bounds for the number of inequivalent Hadamard matrices for the seven orders 44, 48, 52, 56, 60, 64, 68.

Key words: Hadamard Matrices, Computational Algebra, Hadamard ideal, Hadamard equivalence, algorithm.
1991 MSC: 05B20, 13P10.

* Corresponding author. Address: Wilfrid Laurier University, Waterloo, ON N2L 3C5, Canada

Email address: ikotsire@wlu.ca (Ilias S. Kotsireas).

[1] Supported in part by a grant from the Research Office of Wilfrid Laurier University and a grant from the Natural Sciences and Engineering Research Council of Canada.

1 Introduction

In [3] the authors introduce Legendre sequences and generalised Legendre pairs (GL–pairs). They show how to construct an Hadamard matrix of order $2\ell+2$ from a GL–pair of length ℓ. This Hadamard matrix is constructed via two circulant matrices. The authors review the known constructions for GL–pairs and use the discrete Fourier transform (DFT) and power spectral density (PSD) to complete an exhaustive search for GL–pairs for lengths $\ell \leq 45$ and partial results for other ℓ. In this paper we introduce Hadamard ideals for two circulant cores as a means of applying computational algebra techniques in the aforementioned Hadamard matrix construction.

2 Hadamard matrices with two circulant cores

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 of Jennifer Seberry cited in the bibliography. An Hadamard matrix of order $2\ell+2$ which can be written in one of the two equivalent forms

$$H_{2\ell+2} = \left[\begin{array}{cc|ccc} - & - & + & \cdots & + \\ - & + & + & \cdots & - \\ \hline + & + & & & \\ \vdots & \vdots & & A & \\ + & + & & & \\ \hline + & - & & & \\ \vdots & \vdots & & B^T & \\ + & - & & & \end{array}\right] \quad \text{or} \quad \left[\begin{array}{cc|ccc} 1 & 1 & & & \\ \vdots & & & A & \\ 1 & 1 & & & \\ \hline 1 & - & & & \\ \vdots & & & B^T & \\ 1 & - & & & \\ \hline - & - & 1 & \cdots & 1 \\ - & 1 & 1 & \cdots & 1 \end{array}\right. \left.\begin{array}{ccc} & & \\ & B & \\ & & \\ \hline & & \\ & -A^T & \\ & & \\ \hline 1 & \cdots & 1 \\ - & \cdots & - \end{array}\right] \tag{1}$$

where $A = (a_{ij})$, $B = (b_{ij})$ are two circulant matrices of order ℓ i.e. $a_{ij} = a_{1,j-i+1(\text{mod } \ell)}$, $b_{ij} = b_{1,j-i+1(\text{mod } \ell)}$, is said to have two circulant cores, see [3]. The following matrix is an example of a Hadamard matrix of order 8 with two

circulant cores of order $\ell = 3$ each:

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

where $-$ stands for -1 to conform with the customary notation for Hadamard matrices. The two forms are equivalent as described in section 2.1. In this paper we use the first form as described in section 3.

The two circulant matrices A and B satisfy the matrix equation

$$AA^T + BB^T = (2\ell + 2)I_\ell - 2J_\ell \tag{2}$$

where I_ℓ is the identity matrix or order ℓ and J_ℓ is a matrix of order ℓ whose elements are all equal to 1.

Since $2\ell + 2$ must be equal to a multiple of 4 we have that ℓ must be an odd integer for this construction to yield a Hadamard matrix.

Georgiou, Koukouvinos and Seberry [6] point out that GL-pairs, which can be used to construct Hadamard matrices of order $2\ell + 2$ with two circulant cores, exist for many cases. We group these results as a theorem

Theorem 1 (Two Circulant Cores Hadamard Construction Theorem)

An Hadamard matrix of order $2\ell + 2$ with with two circulant cores can be constructed if

(1) ℓ is a prime (see for example [3]);
(2) $2\ell + 1$ is a prime power (these arise from Szekeres difference sets, see for example [3] or [7]);
(3) $\ell = 2^k - 1$, $k \geq 2$ (two Galois sequences are a GL-pair, see for example [12]);
(4) $\ell = p(p + 2)$ where p and $p + 2$ are both primes (two such sequences are a GL-pair,see for example, [14,17]);
(5) $\ell = 49, 57$ (these have been found by a non-exhaustive computer search that uses generalized cyclotomy and master-switch techniques, see [7,8]);

(6) $\ell = 3, 5, \ldots, 45$ *(these have been found and classified by exhaustive computer searches, see [3]);*
(7) $\ell = 47, 49, 51, 53$ *and* 55 *(these have been found and classified by partial computer searches, see [3]);*
(8) $\ell = 143$ *(also verified the results for* $\ell = 3, 5, 7, 11, 13, 15, 17, 19, 23, 25, 31, 35, 37, 41, 43, 53, 59, 61, 63$ *see [5]).*

GL-pairs do not exist for even lengths. It is indicated in [3] that the following lengths $\ell \leq 200$ are unresolved: 77, 85, 87, 91, 93, 115, 117, 121, 123, 129, 133, 145, 147, 159, 161, 169, 171, 175, 177, 185, 187 and 195.

We note here that a *GL*-pair for length $\ell = 143$ is constructed easily since $143 = 11 \cdot 13$ is a product of twin primes.

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 [7], [16], [13] and for inequivalent Hadamard matrices see [6] and [4].

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 of order* n *are said to be equivalent if* $A = PBQ$*.*

3 Hadamard ideals

We detail the construction of Hadamard matrices with circulant core 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**. See [2], [15] for detailed presentations of the concepts of an ideal in a polynomial ring, the corresponding system of polynomial equations and the associated variety.

Consider two vectors of ℓ unknowns each $(a_1, \ldots, a_\ell)$ and $(b_1, \ldots, b_\ell)$. These two vectors generate two circulant $\ell \times \ell$ matrices A_ℓ and B_ℓ:

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

Once we have constructed the two circulant matrices A_ℓ and B_ℓ, the Fletcher-Gysin-Seberry construction of Hadamard matrices with two circulant cores (see [3], [11]) stipulates that an Hadamard matrix of order $2\ell + 2$ is obtained by supplementing these matrices and their transposes by rows and columns of $1s$ and half $1s$ and $-1s$, as in (1):

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

The additional constraints $\{a_1, \ldots, a_\ell, b_1, \ldots, b_\ell\} \subset \{-1, +1\}^{2\ell}$ 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 2ℓ algebraic equations:

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

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

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

Let $a = a_1 + \ldots + a_\ell$ and $b = b_1 + \ldots + b_\ell$. Then the matrix equation (2) implies the equation

$$a^2 + b^2 = 2,$$

which has the 4 integer solutions: $(a, b) = (1, 1)$, $(a, b) = (1, -1)$, $(a, b) = (-1, 1)$, $(a, b) = (-1, -1)$.

The matrix equation $H_{2\ell+2} = (2\ell+2)I_{2\ell+2}$ 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;
- the equation of the form

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

  which is satisfied trivially, since $a_1^2 = \ldots = a_\ell^2 = b_1^2 = \ldots = b_\ell^2 = 1$;
- the two equations

  $$\sum_{i=1}^{\ell} a_i = \sum_{i=1}^{\ell} b_i \quad \text{and} \quad \sum_{i=1}^{\ell} a_i + \sum_{i=1}^{\ell} b_i = 2$$

  which imply the simpler equations:

  $$\sum_{i=1}^{\ell} a_i = 1 \quad \text{and} \quad \sum_{i=1}^{\ell} b_i = 1.$$

To systematize the study of the system of polynomial equations that arise in the Fletcher-Gysin-Seberry construction of Hadamard matrices with two circulant cores, we introduce the notion of **Hadamard Ideal**. This allows us to apply numerous tools of computational algebra to the study of Hadamard matrices with two circulant cores. This connection between an important combinatorial problem and ideals in multivariate polynomial rings is exploited in this paper from both the theoretical and the computational points of view.

Hadamard Ideals are also defined for other constructions of Hadamard matrices based on the concept of circulant core [9]. 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 odd natural number $\ell = 3, 5, 7, \ldots$ set $m = (\ell - 1)/2$. Then the ℓ-**th Hadamard ideal** $\mathcal{H}_\ell$ (associated with the two circulant cores construction by Fletcher, Gysin and Seberry) is defined by:*

$$\mathcal{H}_\ell = \langle s_1, \ldots s_m, a_1 + \ldots + a_\ell - 1, b_1 + \ldots + b_\ell - 1, a_1^2 - 1, \ldots, a_\ell^2 - 1, b_1^2 - 1, \ldots, b_\ell^2 - 1 \rangle$$

where $s_1, \ldots s_m$ are quadratic equations defined by:

$$\begin{array}{rcl} s_1 & = & 2 + \sum_{i=1}^{\ell} \left(a_i a_{(i+1) \bmod \ell} + b_i b_{(i+1) \bmod \ell} \right) \\ \vdots & \vdots & \vdots \\ s_m & = & 2 + \sum_{i=1}^{\ell} \left(a_i a_{(i+m) \bmod \ell} + b_i b_{(i+m) \bmod \ell} \right) \end{array} \tag{3}$$

Remark 2 *$\mathcal{H}_\ell$ is generated by $m + 2 + 2\ell$ polynomials.*

Remark 3 *From the 4 solutions in (a, b) of the equation $a^2 + b^2 = 1$, we have elected to include in the definition of the Hadamard ideal only the two linear equations corresponding to the solution $(a, b) = (1, 1)$. There are three reasons that justify this choice:*

- *Once we know a solution of the system corresponding to the Hadamard ideal as defined above with $(a, b) = (1, 1)$ then we can generate a solution corresponding to the case $(a, b) = (1, -1)$ simply by multiplying the unknowns $b_1, \ldots, b_\ell$ by -1. Similarly, we can generate two more solutions corresponding to the cases $(a, b) = (-1, 1)$, $(a, b) = (-1, -1)$.*
- *The presence of the two linear equations is useful in applying combinatorial optimization techniques such as pruning in binary trees.*
- *The presence of the two linear equations allows us to establish un upper bound on the number of solutions of the system corresponding to the Hadamard ideal.*

The symbol $V(\mathcal{H}_\ell)$ will denote the affine algebraic variety corresponding to the Hadamard ideal $\mathcal{H}_\ell$, that is the set of solutions of the system of polynomial equations corresponding to the Hadamard ideal $\mathcal{H}_\ell$.

Property 1 *$\mathcal{H}_\ell$ is a zero-dimensional ideal. (This is evident, because all points in $\mathcal{H}_\ell$ are also points of $\{-1, +1\}^{2\ell}$ which is in turn, a finite set). In particular the number of solutions of the system corresponding to the Hadamard ideal $\mathcal{H}_\ell$*

is bounded by above by $2^{2\ell}$,

$$\mid V(\mathcal{H}_\ell) \mid \leq 2^{2\ell}.$$

A better upper bound for the number of solutions is given in the lemma below, using the two linear equations in the definition of the Hadamard ideal.

Lemma 1 *The number of solutions of the system corresponding to the Hadamard ideal* $\mathcal{H}_\ell$ *is bounded by above from the square of a binomial coefficient,*

$$\mid V(\mathcal{H}_\ell) \mid \leq \binom{\ell}{\frac{\ell+1}{2}}^2.$$

Proof
Consider a specific solution $a_1, \ldots, a_\ell, b_1, \ldots, b_\ell$. This solutions must satisfy the linear equations $a_1 + \ldots + a_\ell = 1$, $b_1 + \ldots + b_\ell = 1$ and since $a_i, b_i \in \{-1, +1\}$, we see that we must have exactly $\frac{\ell+1}{2}$ of the a_i being equal to 1 (the remaining $\frac{\ell-1}{2}$ of the a_i being equal to -1) and exactly $\frac{\ell+1}{2}$ of the b_i being equal to 1 (the remaining $\frac{\ell-1}{2}$ of the b_i being equal to -1). There are $\binom{\ell}{\frac{\ell+1}{2}}$ possible ways to choose $\frac{\ell+1}{2}$ out of the ℓ a_i to be equal to 1 and similarly for b_i. Each such configuration of the a_i is combined with each such configuration of the b_i and therefore an upper bound on the number of solutions is given by the square of this binomial coefficient. □

Remark 4 *The binomial coefficient* $\binom{\ell}{\frac{\ell+1}{2}}$ *(and therefore the upper bound in the above lemma) can be expressed is terms of* **Catalan numbers***:*

$$\binom{\ell}{\frac{\ell+1}{2}} = \ell C_{\frac{\ell-1}{2}}$$

where the Catalan numbers C_n *are defined by:*

$$C_n = \frac{1}{n+1}\binom{2n}{n}, n = 0, 1, 2, \ldots.$$

Remark 5 *Since* $1 + 1 \mod \ell = 2$ *and* $\ell + 1 \mod \ell = 1$, *equation* s_1 *starts with the term* $a_1 a_2$ *and finishes with the term* $a_\ell a_1$ *(and the analogous* b*-terms).*

Remark 6 *The quadratic equations* $s_1, \ldots, s_m$ *are composed from* 2ℓ *terms plus the constant term* 2. *The* 2ℓ *quadratic terms are divided into two decoupled classes with* ℓ *terms each. One class contains quadratic monomials in the* a_i *alone and the other class contains quadratic monomials in the* b_i *alone. The decoupled form of these equations, is exploited to yield an important optimization in the exhaustive search computations in the sequel.*

Denote by e_2^a the second elementary symmetric function in the unknowns $a_1, \ldots, a_\ell$. Denote by e_2^b the second elementary symmetric function in the unknowns $b_1, \ldots, b_\ell$. In general, the second elementary symmetric function e_2 in ℓ variables contains $\binom{\ell}{2} = \frac{\ell(\ell-1)}{2}$ terms and therefore the sum $e_2^a + e_2^b$ will contain $2\binom{\ell}{2} = \ell(\ell-1)$ terms.

The m equations (3) (resp. some of the the generators of the ℓ-th Hadamard ideal $\mathcal{H}_\ell$) are not algebraically independent. A particular syzygy is given in the next lemma, whose proof is trivial.

Lemma 2 *For any odd natural number $\ell = 3, 5, 7, \ldots$ set $m = (\ell-1)/2$. Then we have that*

$$s_1 + \ldots + s_m = e_2^a + e_2^b + 2m.$$

4 Structure of the variety $V(\mathcal{H}_\ell)$

We summarize in the following table the computational results obtained using the Hadamard ideals $\mathcal{H}_3, \ldots, \mathcal{H}_{25}$: (the symbol $\mid V(\mathcal{H}_\ell) \mid$ stands for the number of solutions of the system corresponding to the Hadamard ideal $\mathcal{H}_\ell$).

ℓ	matrix order	$\mid V(\mathcal{H}_\ell) \mid$			
3	8	9	$=$	1×3^2	exhaustive searches
5	12	50	$=$	2×5^2	
7	16	196	$=$	4×7^2	
9	20	972	$=$	12×9^2	
11	24	2,904	$=$	24×11^2	
13	28	7,098	$=$	42×13^2	
15	32	38,700	$=$	172×15^2	
17	36	93,058	$=$	322×17^2	
19	40	161,728	$=$	448×19^2	
21	44	433,944	$=$	984×21^2	
23	48	1,235,744	$=$	2336×23^2	
25	52	2,075,000	$=$	3320×25^2	

(4)

It is worthwhile to point out that the above tables contain exhaustive search results for Hadamard matrices with two circulant cores for the twelve orders 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48 and 52.

Moreover, the fact that the sequence of the integer proportionality constants (for $\ell = 3, \ldots, 23$) is strictly increasing, suggests the following:

Conjecture 1 (Kotsireas-Koukouvinos-Seberry, 2003) *For every odd* $\ell = 3, \ldots$ *there exists a Hadamard matrix of order* $2\ell+2$ *with two cicrculant cores.*

Since the set $\{2\ell + 2, \ell \text{ odd}\}$ covers the full range of multiples of 4, a solution to the above conjecture would settle the general Hadamard conjecture.

The next theorem clarifies a basic fact about the number of solutions of the system corresponding to the Hadamard ideal $\mathcal{H}_\ell$:

Theorem 2 *For any odd* $\ell \geq 3$*, the total number of solutions of the system corresponding to the Hadamard ideal* $\mathcal{H}_\ell$ *is proportional to* ℓ^2*. In symbols*

$$\mid V(\mathcal{H}_\ell) \mid = h_\ell \cdot \ell^2,$$

where h_ℓ *is an integer proportionality constant.*

Proof
Consider a specific solution a_1, ..., a_ℓ, b_1, ..., b_ℓ and decompose it as two finite sequences, the $a_i s$ and the $b_i s$, of lengths ℓ each. Consider the ℓ cyclic permutations of the a_1, ..., a_ℓ and the ℓ cyclic permutations of the b_1, ..., b_ℓ. Combining each of the ℓ permutations of the a_i with each of the ℓ permutations of the b_i, gives a solution of the system. Therefore, each solution gives rise to ℓ^2 solutions, which implies that the total number of solutions of the system is proportional to ℓ^2. $\square$

In view of lemma (1) and remark (4) we deduce immediately the following upper bound on the integer proportionality constant h_ℓ:

Lemma 3 *For every odd* $\ell = 3, \ldots,$ *we have*

$$h_\ell \leq C^2_{\frac{\ell-1}{2}}.$$

In light of theorem (2) and since Hadamard ideals provide a means of performing exhaustive searches for the associated Hadamard matrices, the computational results of table 4 can be stated concisely as:

Theorem 3 *For the first twelve values* $\ell = 3, \ldots, 25$*, the resolution of the polynomial system arising from the Hadamard ideal* $\mathcal{H}_\ell$ *indicates that the corresponding proportionality constants* h_ℓ *are given by the sequence of integers* 1, 2, 4, 12, 24, 42, 172, 322, 448, 984, 2336, 3320.

5 Inequivalent Hadamard matrices with two circulant cores

Based on the exhaustive searches for Hadamard matrices with two circulant cores, performed using the Hadamard ideals $\mathcal{H}_3$, ..., $\mathcal{H}_{25}$ and on partial searches performed using the Hadamard ideals $\mathcal{H}_{27}$, $\mathcal{H}_{29}$, $\mathcal{H}_{31}$, $\mathcal{H}_{33}$ 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 sufficient (but not necessary) condition for Hadamard inequivalence. Hadamard matrices with unequal profiles are inequivalent. However, Hadamard matrices with equal profiles may or may not be inequivalent. See [10] for mode details on the profile criterion. In this section we report on search results for inequivalent Hadamard matrices with two circulant cores of orders 44, 48, 52, 56, 60, 64, 68. Based on our searches for new inequivalent Hadamard matrices of these seven orders we established new lower bounds for the number of inequivalent Hadamard matrices for the seven orders 44, 48, 52, 56, 60, 64, 68. All the inequivalent Hadamard matrices described below are available in the web page `http://www.cargo.wlu.ca/hi`.

5.1 Inequivalent Hadamard matrices with two circulant cores of orders 44*,* 48*,* 52*,* 56*,* 60*,* 64*,* 68

Lower bounds for the number of inequivalent Hadamard matrices of orders up to (and including) 40 have been established by various authors. Using our algebraic formalism we were able to locate many new inequivalent Hadamard matrices of orders 44, 48, 52, 56, 60, 64 and 68. We contributed (and continue to contribute) these matrices to the Magma Hadamard Database, which is integrated into Magma V2.11, see [1].

The Hadamard ideals $\mathcal{H}_{21}$, $\mathcal{H}_{23}$, and $\mathcal{H}_{25}$ indicate that there are $433,944$, $1,235,744$ and $2,075,000$ Hadamard matrices (exhaustive searches) with two circulant cores of orders 44, 48 and 52 respectively. Using Magma V2.11 we were able to process all these matrices for inequivalence check using the profile criterion and identify:

- 37 inequivalent Hadamard matrices of order 44. This raised the lower bound of inequivalent Hadamard matrices of order 44 to 500;
- 53 inequivalent Hadamard matrices of order 48. This raised the lower bound of inequivalent Hadamard matrices of order 48 to 55;
- 76 inequivalent Hadamard matrices of order 52. This raised the lower bound of inequivalent Hadamard matrices of order 52 to 638.

The Hadamard ideals $\mathcal{H}_{27}$, $\mathcal{H}_{29}$, $\mathcal{H}_{31}$ and $\mathcal{H}_{33}$ produce Hadamard matrices (partial searches) with two circulant cores of orders 56, 60, 64 and 68 respectively. Using Magma V2.11 we were able to process all these matrices for inequivalence check using the profile criterion and identify:

- 203 inequivalent Hadamard matrices of order 56. This raised the lower bound of inequivalent Hadamard matrices of order 56 to 205;
- 253 inequivalent Hadamard matrices of order 60. This raised the lower bound of inequivalent Hadamard matrices of order 60 to 256;
- 394 inequivalent Hadamard matrices of order 64. This raised the lower bound of inequivalent Hadamard matrices of order 64 to 395;
- 338 inequivalent Hadamard matrices of order 68. This raised the lower bound of inequivalent Hadamard matrices of order 68 to 340;

The inequivalent Hadamard matrices with two circulant cores that we computed, are inequivalent with the Hadamard matrices of the corresponding orders in the Magma database. This is taken into account, in the improvement of lower bounds above.

6 Acknowledgments

This work is supported in part by a grant from the National Sciences and Engineering Research Council of Canada, NSERC and a grant from the Research Office of Wilfrid Laurier University. 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, Wilfrid Laurier University, Waterloo, Ontario, Canada*. 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*

7 Conclusion

In this paper we introduce the concept of Hadamard ideals to the study of Hadamard matrices with two circulant cores for the construction of Fletcher, Gysin and Seberry. Hadamard ideals are used to perform exhaustive searches for Hadamard matrices with two circulant cores, for the first twelve orders $8, \ldots, 52$. Finally, we use the Hadamard ideal formalism to improve the lower bounds for the number of inequivalent Hadamard matrices for the seven orders 44, 48, 52, 56, 60, 64, 68.

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] 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.

[3] 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.

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

[5] S. Georgiou and C. Koukouvinos, On generalized Legendre pairs and multipliers of the corresponding supplementary difference sets, *Utilitas Math.*, 61 (2002), 47-63.

[6] 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.

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

[8] M. Gysin and J. Seberry, An experimental search and new combinatorial designs via a generalization of cyclotomy, *J. Combin. Math. Combin. Comput.*, 27 (1998), 143-160.

[9] I. S. Kotsireas, C. Koukouvinos and J. Seberry, Hadamard ideals and Hadamard matrices with circulant core. *J. Combin. Math. Combin. Comput.*, (2005) (to appear).

[10] 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.

[11] R.E.A.C. Paley, On orthogonal matrices, *J. Math. Phys.*, 12 (1933), 311-320.

[12] M. R. Schroeder, *Number Theory in Science and Communication*, Springer–Verlag, New York, 1984.

[13] 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.

[14] R.G. Stanton and D.A. Sprott, A family of difference sets, *Canad. J. Math.*, 10 (1958), 73-77.

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

[16] 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.

[17] A.L. Whiteman, A family of difference sets, *Illinois Journal of Mathematics*, 6 (1962), 107-121.