Hadamard ideals and Hadamard matrices with circulant core

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

Computational Algebra methods have been used successfully in various problems in many fields of Mathematics. Computational Algebra encompasses a set of powerful algorithms for studying ideals in polynomial rings and solving systems of nonlinear polynomial equations efficiently. The theory of Gröbner bases is a cornerstone of Computational Algebra, since it provides us with a constructive way of computing a kind of a particular basis of an ideal which enjoys some important properties. In this paper we introduce the concept of Hadamard ideals in order to establish a new approach to the construction of Hadamard matrices with circulant core. Hadamard ideals reveal the rich interplay between Hadamard matrices with circulant core and ideals in multivariate polynomial rings. Our approach yields an exhaustive list of Hadamard matrices with circulant core for any specific dimension.

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

Hadamard matrices arise in Statistics, Combinatorics, Cryptography and other areas and have been studied extensively. It is well known that the order of a Hadamard matrix must be 1, 2 or a multiple of 4. A particularly important class of $n \times n$ Hadamard matrices can be constructed based on $n-1 \times n-1$ circulant matrices. These are called Hadamard matrices with circulant core. Four categories of Hadamard matrices with circulant core have been identified, essentially using techniques from Combinatorics and Number Theory. We propose a Computational Algebra formalism to tackle the problem of constructing Hadamard matrices with circulant core of any fixed dimension, or prove that such matrices do not exist. Our formalism is based on the concept of the Hadamard ideal, which exemplifies the algebraic structure of the problem as well as a group-theoretic interpretation of the structure of the corresponding variety. The concept of the Hadamard ideal is shown to be a valuable tool for computation, since it allows us to apply directly a lot of the available machinery for ideals in multivariate polynomial rings, as it has been developed in the realm of Computational Algebra.

2 Hadamard matrices with 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 J. Seberry cited in the bibliography. An Hadamard matrix of order $p+1$ which can be written in one of the two equivalent forms

$$\left(\begin{array}{c|c} 1 & 1 \cdots 1 \\ \hline 1 & \\ \vdots & C \\ 1 & \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c} 1 & \\ \vdots & C \\ 1 & \\ \hline 1 & -1 \cdots -1 \end{array}\right)$$

where $C = (c_{ij})$ is a circulant matrix of order p i.e. $c_{ij} = c_{1,j-i+1(\text{mod p})}$, is said to have a circulant core. The following matrices are examples for order 12.

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	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	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	-	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	-	-	-	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	-	1
1	1	-	-	-	1	1	1	-	1	1	-
1	-	1	-	-	-	1	1	1	-	1	1
1	-	-	-	-	-	-	-	-	-	-	-

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 second form as described in section 2.2.

Four families of these kinds of Hadamard matrices have been found by Paley [10], Stanton, Sprott and Whiteman [16,20], Singer [14] and Marshall Hall Jr. [6]. We group these results as a theorem

Theorem 1 (Circulant Core Hadamard Construction Theorem) *An Hadamard matrix of order $p+1$ with circulant core can be constructed if*

(1) $p \equiv 3 (\mathrm{mod}\ 4)$ *is a prime [10];*
(2) $p = q(q+2)$ *where q and $q+2$ are both primes [16,20];*
(3) $p = 2^t - 1$ *where t is a positive integer [14];*
(4) $p = 4x^2 + 27$ *where p is a prime and x a positive integer [6].*

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 columns 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 [5], [19], [13] and for inequivalent Hadamard matrices see [4] and [3].

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 none 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 $A = PBQ$.

2.2 Construction of Hadamard matrices with circulant core

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**.

Let $n = 4k$, for $k = 1, 2, \ldots$ and consider the vector of $n-1$ unknowns $(a_1, \ldots, a_{n-1})$. This vector generates the cyclic $n \times n-1$ matrix (supplemented from underneath by a row of $-1s$)

$$B_{n-1} = \begin{bmatrix} a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_1 & \ldots & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & \ldots & a_1 \\ -1 & -1 & \ldots & -1 \end{bmatrix}.$$

The Plackett-Burman construction of Hadamard matrices (see [11]) stipulates that we must have $B_{n-1}^t \cdot B_{n-1} = nI_{n-1}$ with the additional constraints:

- $\{a_1, \ldots, a_{n-1}\} \subset \{-1, +1\}^{n-1}$ (amounts to a set of $n-1$ quadratic constraints);
- $a_1 + a_2 + \ldots + a_{n-1} = 1$ (linear constraint).

Once we have constructed the matrix B_{n-1}, an $n \times n$ Hadamard matrix is

obtained by supplementing it with a column of 1s from the left

$$H_n = \begin{bmatrix} 1 & a_1 & a_2 & \dots & a_{n-1} \\ 1 & a_{n-1} & a_1 & \dots & a_{n-2} \\ 1 & \vdots & \vdots & \vdots & \vdots \\ 1 & a_2 & a_3 & \dots & a_1 \\ 1 & -1 & -1 & \dots & -1 \end{bmatrix}.$$

3 Hadamard Ideals

The matrix equation $B_{n-1}^t \cdot B_{n-1} = nI_{n-1}$ gives rise to a set of $2k-1$ equations $s_1 = 0, \ldots, s_{2k-1} = 0$ where each s_i is a quadratic homogeneous polynomial with $4k-1$ terms plus the constant term 1.

Notice that the equations corresponding to the diagonal of the matrix equation $B_{n-1}^t \cdot B_{n-1} = nI_{n-1}$, boil down to the one equation

$$a_1^2 + \ldots + a_{n-1}^2 + 1 = n$$

which is satisfied trivially, since $a_1^2 = \ldots = a_{n-1}^2 = 1$.

Moreover, a succinct algebraic description of the quadratic constraints given above is provided by the following set of $n-1$ algebraic equations:

$$a_1^2 - 1 = 0, \ldots, a_{n-1}^2 - 1 = 0.$$

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

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

To systematize the study of the system of polynomial equations that arises from considering Hadamard matrices with circular core, we introduce the notion of **Hadamard Ideal**. This allows us to apply numerous tools of computational algebra to the study of Hadamard matrices with circular core. 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. The interpretation of the **Circulant Core Hadamard Construction Theorem** in terms of Hadamard ideals is also of interest because it implies some non-trivial algebraic statements. The algebraic

ramifications entailed by the **Circulant Core Hadamard Construction Theorem** are important because the theorem is of number-theoretic nature and a priori there are no direct dependencies between number-theoretic conditions on the form of an ideal in a multivariate polynomial ring and the structure of the ideal.

Definition 1 *For $k = 1, 2, \ldots$ the* **k-th Hadamard ideal** *is defined by:*

$$\mathcal{H}_k = \langle s_1, \ldots s_{2k-1}, a_1 + \ldots + a_{n-1} - 1, a_1^2 - 1, \ldots, a_{n-1}^2 - 1 \rangle.$$

Notation 1 *We will also use the notation*

$$\mathcal{H}_k = \langle h_1, \ldots h_{2k-1}, h_{2k}, h_{2k+1}, \ldots, h_{6k-1} \rangle$$

in direct one-to-one correspondence with the definition of $\mathcal{H}_k$ given above.

Remark 2 *$\mathcal{H}_k$ is generated by $2k - 1 + 1 + 4k - 1 = 6k - 1$ polynomials.*

Property 1 *$\mathcal{H}_k$ is a zero-dimensional ideal. (This is evident, because all points in $\mathcal{H}_k$ are also points of $\{-1, +1\}^{n-1}$ which is in turn, a finite set).*

Property 2 *$s_1 + \ldots + s_{2k-1} = e_2 + (2k-1)$ where e_2 is the second elementary symmetric function in the unknowns $a_1, \ldots, a_{n-1}$.*

The second elementary symmetric function e_2 in the unknowns $a_1, \ldots, a_{n-1}$ contains $\binom{n-1}{2} = (2k-1)(4k-1)$ terms.

Lemma 1 *For any $k = 1, 2, \ldots$, the $6k - 1$ generators of the Hadamard ideal $\mathcal{H}_k$ are not algebraically independent. More specifically we have the syzygy:*

$$h_1 + \ldots + h_{6k-1} = 0.$$

Proof Consider the general syzygy (linear combination)

$$H = \alpha(h_1 + \ldots + h_{2k-1}) + \beta h_{2k} + \gamma(h_{2k+1} + \ldots + h_{6k-1}) \tag{1}$$

for scalar (constant polynomials) α, β, γ. We will use the properties $h_1 + \ldots + h_{2k-1} = e_2 + (2k-1)$ and $h_{2k} = e_1 - 1$. Moreover, notice that we have

$$h_{2k+1} + \ldots + h_{6k-1} = a_1^2 + \ldots + a_{4k-1}^2 - (4k-1) = e_1^2 - 2e_2 - (4k-1)$$

where e_1, e_2 denote the first and second elementary symmetric functions in the variables $a_1, \ldots, a_{4k-1}$ respectively. By construction of the Hadamard ideal $\mathcal{H}_k$ we have that $e_1 = p_1 = a_1 + \ldots + a_{n-1} = 1$ and to evaluate e_2 we use the expression of the elementary symmetric functions in the power-sum basis (an instance of what is generally referred to as the Jacobi-Trudi formula in

Combinatorics, see [9] and [17])

$$e_2 = \frac{1}{2!}\begin{vmatrix} p_1 & 1 \\ p_2 & p_1 \end{vmatrix} = \frac{p_1^2}{2} - \frac{p_2}{2} \quad \text{and dually} \quad p_2 = \frac{1}{2!}\begin{vmatrix} e_1 & 1 \\ 2e_2 & e_1 \end{vmatrix} = e_1^2 - 2e_2.$$

By construction of the Hadamard ideal $\mathcal{H}_k$ we have that $p_2 = a_1^2 + \ldots + a_{n-1}^2 = n - 1 = 4k - 1$. Combining the expressions for the three separate parts of the linear combination (1) we obtain:

$$H = \alpha\ (e_2 + 2\,k - 1) + \beta\ (e_1 - 1) + \gamma\ \left({e_1}^2 - 2\,e_2 - 4\,k + 1\right) =$$

$$= \alpha\ \left(\frac{p_1^2}{2} - \frac{p_2}{2} + 2\,k - 1\right) + \beta\ (p_1 - 1) + \gamma\ (p_2 - 4\,k + 1)$$

$$= \alpha\ \left(\frac{1}{2} - \frac{4k-1}{2} + 2\,k - 1\right) + \gamma\,(4k - 1 - 4\,k + 1) = 0.$$

□

The above lemma reveals some of the structure of the $6k-1$ generators of the Hadamard Ideal. It could possibly be used in proofs of non-existence of solutions via Hilbert's (weak) Nullstellensatz, which provides us with a necessary and sufficient condition for solvability of a system of polynomial equations. In particular: **a system of polynomial equations does not have a common solution in C^n if and only if 1 belongs to the ideal defined by these polynomials**. See [2] and [18] for a detailed exposition of these and related ideas.

If we can exhibit a linear combination (with scalar or polynomial coefficients) of the 41 generators (or some of them) of the Hadamard Ideal $\mathcal{H}_7$, which is equal to 1, then this furnishes a proof that the ideal $\mathcal{H}_7$ is equal to the whole polynomial ring in 27 variables and that the corresponding variety (set of solutions) is empty.

Fact: $\mathcal{H}_k$ is a radical ideal for $k = 1, 2, 3, 4, 5$, (computations in Magma and Macaulay).

Could this be true for every $k \geq 1$?

Remark 3 *Two solutions of the system corresponding to the Hadamard ideal $\mathcal{H}_k$ will be termed* **equivalent**, *if the corresponding Hadamard matrices are equivalent in the sense defined in 2.1.*

4 Computational results

In this section we present the computational results we obtained via Hadamard ideals and some computational algebra techniques. This section contains:

(1) a complete description of all Hadamard matrices with circular core for $k = 1, \ldots, 8$ up to equivalence,
(2) combinatorial and algebraic constructions that detail how the concept of H-equivalence can be used to generate all equivalent Hadamard matrices and distinguish between them,
(3) some heuristic arguments that we used to produce solutions in early stages of our investigations,
(4) a combinatorial technique that allows us to sieve out many equivalent solutions and therefore compute the inequivalent solutions faster.

We want to emphasize that the importance of these computational results lies not in the biggest value of k that we can currently solve, but in the insight we gain and in the general results that can be established, see for example the analysis of H-equivalence.

4.1 k=1 (n=4)

Form the matrices B_3 and B_3^t and their product $B_3^t \cdot B_3$:

$$B_3 = \begin{bmatrix} a1 & a2 & a3 \\ a3 & a1 & a2 \\ a2 & a3 & a1 \\ -1 & -1 & -1 \end{bmatrix} \quad B_3^t = \begin{bmatrix} a1 & a3 & a2 & -1 \\ a2 & a1 & a3 & -1 \\ a3 & a2 & a1 & -1 \end{bmatrix}$$

The Hadamard Ideal $\mathcal{H}_1$ is then given by:

$$\mathcal{H}_1 = \langle a1\ a2 + a3\ a1 + a2\ a3 + 1, a1 + a2 + a3 - 1, {a1}^2 - 1, {a2}^2 - 1, {a3}^2 - 1 \rangle$$

and there are 3 solutions to the corresponding system of equations:$[a1 = -1, a2 = 1, a3 = 1]$,, $[a1 = 1, a2 = 1, a3 = -1]$, and $[a1 = 1, a3 = 1, a2 = -1]$. Each one of these 3 solutions gives rise to a a Hadamard matrix of order 4

with cyclic core:

$$\begin{bmatrix} 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix}.$$

All three of the above matrices are H-equivalent.

4.2 Exhaustive solution for $k \leq 5$

For reference purposes we explicit here the definition of the Hadamard Ideal $\mathcal{H}_2$:

$$\begin{aligned} \mathcal{H}_2 = \langle\ & a1\ a4 + a7\ a3 + a6\ a2 + a5\ a1 + a4\ a7 + a3\ a6 + a2\ a5 + 1, \\ & a1\ a2 + a7\ a1 + a6\ a7 + a5\ a6 + a4\ a5 + a3\ a4 + a2\ a3 + 1, \\ & a3\ a1 + a7\ a2 + a6\ a1 + a5\ a7 + a4\ a6 + a3\ a5 + a2\ a4 + 1, \\ & a1 + a2 + a3 + a4 + a5 + a6 + a7 - 1, \\ & a1^2 - 1, a2^2 - 1, a3^2 - 1, a4^2 - 1, a5^2 - 1, a6^2 - 1, a7^2 - 1\ \rangle \end{aligned}$$

A synopsis of the computational results for $k = 2, 3, 4, 5$ is in the table below. For each value of k we computed all solutions, but since all solutions give rise to equivalent Hadamard matrices, we give only one solution for each k.

k	# solutions	one solution
2	14	$a1 = 1\ \ a2 = 1\ \ a3 = 1\ \ a4 = -1\ \ a5 = 1\ \ a6 = -1\ \ a7 = -1$
3	22	$a1 = -1\ \ a2 = 1\ \ \ a3 = 1\ \ \ a4 = 1\ \ a5 = -1\ \ a6 = 1\ \ a7 = 1\ \ a8 = -1$ $a9 = 1\ \ \ a10 = -1\ \ a11 = -1$
4	30	$a1 = -1\ \ a2 = -1\ \ a3 = -1\ \ \ a4 = 1\ \ \ a5 = -1\ \ a6 = -1\ \ a7 = 1\ \ \ a8 = 1$ $a9 = -1\ \ a10 = 1\ \ \ a11 = -1\ \ a12 = 1\ \ a13 = 1\ \ \ a14 = 1\ \ \ a15 = 1$
5	38	$a1 = 1\ \ \ a2 = 1\ \ \ a3 = -1\ \ \ a4 = -1\ \ a5 = 1\ \ \ \ a6 = 1\ \ \ \ a7 = 1\ \ \ \ a8 = 1$ $a9 = -1\ \ a10 = 1\ \ a11 = -1\ \ a12 = 1\ \ \ a13 = -1\ \ a14 = -1\ \ a15 = -1\ \ a16 = -1$ $a17 = 1\ \ \ a18 = 1\ \ a19 = -1$

4.3 Exhaustive solution for $k = 6, 7, 8$

In this section we group the computational results for $k = 6, 7, 8$ using the Hadamard ideal formalism and some additional algebraic techniques.

4.3.1 $k = 6$

The system is too big to be solved directly by Maple. However, two approaches based on the Hadamard ideal formalism, allow us to find some solutions quickly and to state conclusively that the system has $46 = 8 \cdot 6 - 2$ solutions.

(A) **Heuristics with prescribed values**

Observing properties of the complete solution sets for $k = 2, 3, 4, 5$ we discover that:

- Examining the sets of solutions for $k = 2, 3$ we see that there are exactly 2 solutions with $a_1 = a_2 = a_3 = 1$.
- Examining the sets of solutions for $k = 4, 5$ we see that there are exactly 2 solutions with $a_1 = a_2 = a_3 = a_4 = 1$.

We are thus led to assume that for $k = 6$ there could be exactly 2 solutions with $a_1 = a_2 = a_3 = a_4 = a_5 = 1$. Incorporating this heuristic argument in algebraic form in the definition of the Hadamard Ideal $\mathcal{H}_6$ we do indeed obtain the two solutions listed below:

- $$[a1 = 1, a2 = 1, a3 = 1, a4 = 1, a5 = 1, a6 = -1, a7 = -1, a8 = -1, a9 = -1, a10 = 1, a11 = -1, a12 = 1,$$
  $$a13 = -1, a14 = -1, a15 = 1, a16 = 1, a17 = -1, a18 = -1, a19 = 1, a20 = 1, a21 = -1, a22 = 1, a23 = -1]$$
- $$[a1 = 1, a2 = 1, a3 = 1, a4 = 1, a5 = 1, a6 = -1, a7 = 1, a8 = -1, a9 = 1, a10 = 1, a11 = -1, a12 = -1,$$
  $$a13 = 1, a14 = 1, a15 = -1, a16 = -1, a17 = 1, a18 = -1, a19 = 1, a20 = -1, a21 = -1, a22 = -1, a23 = -1]$$

These two solutions give rise to two (equivalent) Hadamard matrices of order 24.

(B) **Computer search**

The Hadamard Ideal $\mathcal{H}_6$ is defined over 23 variables. An exhaustive computer search would need to check for all $2^{23} = 8388608$ possible cases to detect solutions. The linear equation $a_1 + \ldots + a_{23} = 1$ could serve to sieve out non-solutions quickly. But this approach has the disadvantage that it would still require a lot of computing time and it would be entirely impractical for bigger values of k.

Using the Hadamard Ideal $\mathcal{H}_6$ we can detect a reasonable cut-off point in the number or variables that we can bound with a series of nested ± 1 loops. For each of the possible cases that arise, we can then solve the system corresponding to the associated restriction of the Hadamard Ideal $\mathcal{H}_6$. It turns out that a good cut-off point is 13. More specifically, we solve the $2^{13} = 8192$ systems arising from the restriction of the Hadamard Ideal $\mathcal{H}_6$ when the first 13 variables $a_1, \cdots, a_{13}$ take all possible ± 1 combinations. We obtain exactly 46 solutions, two of which have been given above, using a heuristic argument.

4.3.2 k=7 (n=28)

The system is again too big to be solved directly by Maple. The heuristic argument employed in the case $k = 6$ does not produce any solutions. The Hadamard Ideal $\mathcal{H}_7$ is defined over 27 variables. An exhaustive computer search would need to check for all $2^{27} = 134217728$ possible cases to detect solutions. Using the Hadamard Ideal $\mathcal{H}_7$ we see that a good cut-off point is again 13. More specifically, we solve the $2^{13} = 8192$ systems arising from the restriction of the Hadamard Ideal $\mathcal{H}_7$ when the first 13 variables $a_1, \cdots, a_{13}$ take all possible ± 1 combinations. No solutions were found. Therefore we can conclude that:

The variety of the Hadamard Ideal $\mathcal{H}_7$ is empty.
This assertion can be stated equivalently as:

- The Hadamard Ideal $\mathcal{H}_7$ generates the whole space $K[a_1, \cdots, a_{27}]$;
- 1 belongs to the Hadamard Ideal $\mathcal{H}_7$;

These results constitute another proof of the following theorem (see [1])

Theorem 2 *There are no* 28×28 *Hadamard matrices with circulant core.*

Two independent proofs of this theorem can be furnished using the Hadamard ideal $\mathcal{H}_7$ by:

- computing a minimal reduced Gröbner basis for a degree order for $\mathcal{H}_7$. The result will be equal to the singleton $\{1\}$ and this means that the system does not have any solutions.
- exhibiting a linear combination of (some of) the 41 generators of $\mathcal{H}_7$ which is equal to 1. This means that $\mathcal{H}_7 = K[a_1, \ldots, a_{27}]$ and that $V(\mathcal{H}_7) = \emptyset$.

4.3.3 k=8 (n=32)

For $k = 8 (n = 32)$ the following two solutions produce 32×32 Hadamard Matrices with circulant core:

- \- - - - 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 - 1 1 - 1 1

These two solutions are not equivalent. This can be checked easily in Magma (instruction `IsHadamardEquivalent`). This constitutes another proof of the following theorem (see [8])

Theorem 3 *There are only* 2 *inequivalent* 32×32 *Hadamard matrices with*

circulant core.

5 Combinatorial reductions

In this section we establish a combinatorial reduction that takes into account the fact that for a fixed value of k, each solution generates $8k-2$ equivalent solutions. One wants to be able to compute as less out of these $8k-2$ equivalent solutions as possible. This would reduce computation times drastically and would make the approach applicable to higher values of k.

Theorem 4 *We stipulate that we can fix the first three values a_1, a_2, a_3, without missing any inequivalent solutions, according to the pattern*

$$a_1 = 1, \quad a_2 = 1, \quad a_3 = -1.$$

Proof

Every solution starts with either $+1$ or -1. We may suppose that it starts with a $+1$ (if not, we multiply by -1). A solution cannot have all of its elements alternate from 1 to -1 or vice-versa, because the inner product of two rows of the core matrix C is equal to -1. Moreover, a solution cannot have all of its elements equal to 1 because it must contain $2k$ 1^s and $2k-1$ -1^s. Therefore the pattern $11-$ always exists. $\square$

The combinatorial reduction specified above possesses a direct algebraic interpretation in terms of Hadamard ideals. When we fix $a_1 = 1$, $a_2 = 1$, $a_3 = -1$, this amounts to enlarging the Hadamard ideal and at the same time shrinking its variety. This ideal-variety correspondence reaches its climax when the ideal is equal to the whole polynomial ring and the corresponding variety is empty. In the framework of Hadamard ideals, this is what happens in the case of $\mathcal{H}_7$. the See [2] for material on the ideal-variety correspondence.

6 Additional algebraic techniques

For $k \geq 7$, the solution of the system corresponding to the Hadamard Ideal $\mathcal{H}_k$ cannot be obtained in a reasonable amount of time in Maple. To increase the efficiency of our approach and thus be able to treat bigger values of k, we can proceed in three ways:

- *Use modular (p-adic) techniques to compute the solution with a lexicographical Gröbner bases computations.* When we compute a Gröbner basis mod-

ulo a prime p, we avoid the well-known problem of intermediate expression swell. Therefore, the computation is always much faster that the conventional computation over the integers or over the rationals. Moreover, if we choose the prime p carefully we obtain viable indications for the number of solutions of the system.

- *Use FGLM and Gröbner Walk algorithms to speed up the Gröbner bases computations.* These are essentially change of basis algorithms, in the sense that we first compute a Gröbner basis for an easy monomial order and then we use this basis to compute the lexicographical Gröbner basis.
- *Use total degree Gröbner bases computations to compute the dimension of the quotient ring $K[a_1, \ldots, a_{n-1}]/\mathcal{H}_k$.* A classical technique in Gröbner bases theory is the determination of the dimension as well as a basis of the quotient ring $K[x_1, \ldots, x_m]/I$ for an ideal I, by means of a total degree Gröbner basis computation. Total degree computations are in general much faster that the corresponding lexicographical computations but they encapsulate nevertheless the information on the dimension of the quotient ring (as a vector space) which is equal to the number of solutions. Notice that this time the approach is not constructive. We compute the number and thus the existence, of solutions, but we don't find them explicitly. This approach yields a basis of the quotient ring as a vector space.

We illustrate the third option above, in the case $k = 3$. The Hadamard Ideal $\mathcal{H}_3$ is defined as follows:

$$\begin{aligned}\mathcal{H}_3 = \langle & a1\ a2 + a11\ a1 + a10\ a11 + a9\ a10 + a8\ a9 + a7\ a8 + a6\ a7 + a5\ a6 + a4\ a5 + a3\ a4 + a2\ a3 + 1,\\ & a1\ a3 + a11\ a2 + a10\ a1 + a9\ a11 + a8\ a10 + a7\ a9 + a6\ a8 + a5\ a7 + a4\ a6 + a3\ a5 + a2\ a4 + 1,\\ & a1\ a4 + a11\ a3 + a10\ a2 + a9\ a1 + a8\ a11 + a7\ a10 + a6\ a9 + a5\ a8 + a4\ a7 + a3\ a6 + a2\ a5 + 1,\\ & a5\ a1 + a11\ a4 + a10\ a3 + a9\ a2 + a8\ a1 + a7\ a11 + a6\ a10 + a5\ a9 + a4\ a8 + a7\ a3 + a6\ a2 + 1,\\ & a6\ a1 + a11\ a5 + a10\ a4 + a9\ a3 + a8\ a2 + a7\ a1 + a6\ a11 + a5\ a10 + a4\ a9 + a3\ a8 + a7\ a2 + 1,\\ & a1 + a2 + a3 + a4 + a5 + a6 + a7 + a8 + a9 + a10 + a11 - 1,\\ & a1^2 - 1, a2^2 - 1, a3^2 - 1, a4^2 - 1, a5^2 - 1, a6^2 - 1, a7^2 - 1, a8^2 - 1, a9^2 - 1, a10^2 - 1, a11^2 - 1\rangle\end{aligned}$$

Upon computing a total degree Gröbner basis for $\mathcal{H}_3$ with Magma, we obtain the following list of 28 initial monomials:

$$\begin{aligned}I_3 = [& a1, a2, a3, a4, a5^2, a5\ a6, a5\ a7, a5\ a8, a5\ a9, a5\ a10, a11\ a5, a6^2, a6\ a7,\\ & a6\ a8\ a10, a6\ a8\ a11, a6\ a9, a6\ a10\ a11, a7^2, a7\ a8, a7\ a9\ a10,\\ & a7\ a9\ a11, a7\ a10\ a11, a8^2, a8\ a9\ a10, a8\ a9\ a11, a9^2, a10^2, a11^2]\end{aligned}$$

Incidentally, at this point we can also verify that the system is of dimension 0 (has a finite number of solutions) because the separation property is satisfied: for each variable a_i there is an element of the form a_i^j for some power j in I_3 .

To compute a vector space basis (and at the same time the dimension) of the quotient ring $K[a_1, \ldots, a_{11}]/\mathcal{H}_3$ we need to compute the set of monomials u such that no monomial in I_3 divides them.

$$U = \{u : u \text{ is a monomial such that } \nexists\ g \in I_3 \text{ with } g|u\}.$$

One way (not the fastest one) to compute this set U in this particular example, is to build the list of all products of the 11 variables $a_1, \ldots, a_{11}$, by 1, by 2, by 3 and by 4 and check the divisibility condition. We need to consider only squarefree monomials, because in I_3 there are either linear or quadratic terms in the variables. We build this list in Maple

```
c:=[
 op(choose([a1,a2,a3,a4,a5,a6,a7,a8,a9,a10,a11], 1)),
 op(choose([a1,a2,a3,a4,a5,a6,a7,a8,a9,a10,a11], 2)),
 op(choose([a1,a2,a3,a4,a5,a6,a7,a8,a9,a10,a11], 3)),
 op(choose([a1,a2,a3,a4,a5,a6,a7,a8,a9,a10,a11], 4))
]; cc:=map(convert,c,`*`); nops(cc);
```

and it turns out that it contains 561 elements. After filtering out those monomials which are divided by some monomial in I_3 we get a list of 21 monomials which make up U, together with 1 which always belongs to U

$$U = [1, a10, a11, a5, a6, a7, a8, a9, a10\ a11, a6\ a10, a7\ a10, a8\ a10, a9\ a10,$$

$$a6\ a11, a7\ a11, a8\ a11, a9\ a11, a6\ a8, a7\ a9, a8\ a9, a10\ a11\ a8, a10\ a11\ a9].$$

Therefore there are 22 solutions to the system, which agrees with the number of solutions found by Maple.

7 Structure of the variety $V(\mathcal{H}_k)$

In this section we describe the structure of the variety $V(\mathcal{H}_k)$ from a combinatorial/algebraic and a group-theoretic point of view. The computational results of the previous paragraph are summarized below for easy reference:

k	1	2	3	4	5	6	7	8
$\#V(\mathcal{H}_k)$	3	14	22	30	38	46	0	124

Table of the number of solutions for the Hadamard Ideal $\mathcal{H}_k$ for $k = 1, \ldots, 8$.

7.1 A combinatorial/algebraic interpretation

The number $\#V(\mathcal{H}_k)$ (number of elements of the variety $V(\mathcal{H}_k)$) is equal to:

- the number of solutions of the system of equations corresponding to the $6k-1$ generators of $\mathcal{H}_k$;

- the dimension of the quotient $K[a_1, \ldots, a_{n-1}]/\mathcal{H}_k$ as a vector space.

We notice that for $k = 2, 3, 4, 5, 6$ we obtain $8k - 2$ solutions and that for $k = 8$ we obtain $2(8k - 2)$ solutions. A combinatorial interpretation of these quantities can be given by considering a specific solution $a_1, \ldots, a_{n-1}$ as a finite sequence of length $n - 1 = 4k - 1$. Two sequences such that one is the reverse of the other are considered to be equivalent. Two sequences such that one is a cyclic permutation of the other are considered to be equivalent. If we reverse this specific solution, then we obtain the equivalent solution $a_{n-1}, \ldots, a_1$, which produces $4k - 1$ cyclic permutations as well. Therefore, from one solution, we find $2 \times (4k - 1) = 8k - 2$ equivalent solutions. These $8k - 2$ equivalent solutions belong to the same equivalence class with respect to the equivalence relation $\overset{H}{\sim}$ defined in remark 1. For $k = 2, 3, 4, 5, 6$ there is only one equivalence class with respect to the equivalence relation $\overset{H}{\sim}$.

For $k = 8$, there are two inequivalent solutions (the ones mentioned in § 4.3.3) and each one produces $8 \cdot 8 - 2 = 62$ solutions, so that we get a total of 124 solutions. Equivalently, for $k = 8$ there are two equivalence classes with respect to the equivalence relation $\overset{H}{\sim}$.

In general, there are $h(8k-2)$ solutions for $\mathcal{H}_k$, where h is given in the following table:

k	1	2	3	4	5	6	7	8
h	$\frac{1}{2}$	1	1	1	1	1	0	2

Table of values of h for $\mathcal{H}_k$ for $k = 1, \ldots, 8$.

The discussion above can be stated as:

Theorem 5 *If for a specific $n = 4k$ there are $n \times n$ Hadamard matrices with circulant core, then there are h inequivalent such matrices.*

or equivalently

Theorem 6 *If for a specific $n = 4k$ the number of equivalence classes of the equivalence relation $\overset{H}{\sim}$ is non-zero, then it is equal to h.*

7.2 A group theoretic interpretation

7.2.1 The dihedral group formalism

The *dihedral group* of order $2n$ is denoted D_{2n} and is defined via the two generators ρ (the rotation) and ϵ (the reflection) and the relations

$$\rho^n = 1 = \epsilon^2 \text{ and } \epsilon\rho = \rho^{-1}\epsilon \tag{2}$$

among them. Then the $2n$ distinct elements of D_{2n} are

$$1, \rho, \rho^2, \ldots, \rho^{n-1}, \epsilon, \rho\epsilon, \rho^2\epsilon, \ldots, \rho^{n-1}\epsilon.$$

The geometric interpretation of the group generators ρ and ϵ is usually given in terms a regular polygon with n sides. ρ denotes the rotation about the center of the polygon through angle $2\pi/n$ and ϵ denotes any of the reflection. See [12] for more details.

7.2.2 Dihedral group structure of $V(\mathcal{H}_k)$

For a fixed k (resp. n), suppose that we choose an element $[a_1, a_2, \ldots, a_{n-1}]$ of the variety $V(\mathcal{H}_k)$ and we define it to be the unit element:

$$1 = [a_1, a_2, \ldots, a_{n-1}].$$

Now mimic the definition of the dihedral group D_{2n} and define

(1) the "rotation" ρ, such that

$$\rho([a_1, a_2, \ldots, a_{n-1}]) = [a_2, \ldots, a_{n-1}, a_1]$$

this is actually a left shift by one operation.

(2) the "reflection" ϵ such that

$$\epsilon([a_1, a_2, \ldots, a_{n-1}]) = [a_{n-1}, \ldots, a_2, a_1]$$

It is easy to see that the relations (2) are satisfied. Moreover, the solutions constructed by the solution we started with, according to the elements of the dihedral group D_{2n} are exactly the $8k-2$ solutions constructed in the previous paragraph.

The discussion above can be stated as:

Theorem 7 *If for a specific $n = 4k$ we can find an $n \times n$ Hadamard matrix with circulant core, then using the $D_{2(n-1)}$ dihedral group formalism we can write down $2(n-1) = 8k-2$ equivalent Hadamard matrices.*

The above theorem is important because it can be used to speed up considerably the detection of inequivalent solutions and correspondingly of inequivalent Hadamard matrices for fixed values of n.

8 Expanded Hadamard Ideals

The realization that the structure of the variety $V(\mathcal{H}_k)$ is determined by equivalence classes with respect to $\overset{H}{\sim}$ or alternatively, by the dihedral group formalism, has an important impact on the acceleration of the computation of $V(\mathcal{H}_k)$. This is accomplished by considering a fixed solution $[b_1, \ldots, b_n]$ and using this solution to extract from the variety all its equivalent solutions. This amounts to shrinking the variety and thus expanding the Hadamard ideal. These expanded Hadamard ideals are specified by adjoining one more generator in the definition of Hadamard ideals.

Definition 2 *For $k = 1, 2, \ldots$ the* **k-th expanded Hadamard ideal** *with respect to the solution $[b_1, \ldots, b_n]$ is defined by:*

$$\mathcal{H}_k^{[b_1,\ldots,b_{n-1}]} =$$
$$= \langle s_1, \ldots s_{2k-1}, a_1 + \ldots + a_{n-1} - 1, a_1^2 - 1, \ldots, a_{n-1}^2 - 1, \lambda \left(\prod_{i=1}^{n-1} (a_i - b_i) \right) + 1 \rangle$$

where λ is a new variable and $n = 4k$ as before.

The equation

$$\lambda(a_1 - b_1) \ldots (a_{n-1} - b_{n-1}) + 1 = 0$$

codifies in a compact manner the fact that neither $[b_1, \ldots, b_n]$ nor any of its equivalent solutions (to the total of $8k - 2$ solutions) belongs to the variety of the expanded Hadamard ideal $V(\mathcal{H}_k^{[b_1,\ldots,b_{n-1}]})$. Therefore the variety $V(\mathcal{H}_k^{[b_1,\ldots,b_{n-1}]})$ of the expanded Hadamard ideal , contains only those solutions of the variety of the Hadamard ideal $V(\mathcal{H}_k)$ that are not equivalent to the solution $[b_1, \ldots, b_{n-1}]$. In case where there is only one solution (up to H-equivalence), the variety $V(\mathcal{H}_k^{[b_1,\ldots,b_{n-1}]})$ will be empty. Thus, when we know one solution, it is usually simpler to compute the variety of the expanded Hadamard ideal with respect to this solution, than to compute the entire variety.

We illustrate the utility of expanded Hadamard ideals by revisiting the case $k = 4$. Consider the Hadamard ideal $\mathcal{H}_4$ and the solution (element of the variety $V(\mathcal{H}_4)$)

$$[-1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1].$$

The expanded 4-th Hadamard ideal with respect to this solution, denoted $\mathcal{H}_4^{[-1,-1,-1,1,-1,-1,1,1,-1,1,-1,1,1,1,1]}$, is obtained by adjoining the generator

$$\lambda(a_1+1)(a_2+1)(a_3+1)(a_4-1)(a_5+1)(a_6+1)(a_7-1)(a_8-1)(a_9+1)(a_{10}-1)(a_{11}+1)(a_{12}-1)(a+13-1)(a_{14}-1)(a15-1)+1$$

to the generators of the 4-th Hadamard ideal $\mathcal{H}_4$. An important feature of the variety $V(\mathcal{H}_4^{[-1,-1,-1,1,-1,-1,1,1,-1,1,-1,1,1,1,1]})$ is that its computation is much easier than the computation of the whole variety $V(\mathcal{H}_4)$. The variety $V(\mathcal{H}_4^{[-1,-1,-1,1,-1,-1,1,1,-1,1,-1,1,1,1,1]})$ is empty as expected, since there is only one solution (up to H-equivalence) for $k = 4$.

9 Conclusion

In this paper we introduce the concept of Hadamard ideals to the study of Hadamard matrices with circulant core. Hadamard ideals establish a rich and fruitful connection between Hadamard matrices with circulant core and ideals in multivariate polynomial rings. This connection allows us to apply much of the machinery of computational algebra to investigations concerning Hadamard matrices with circulant core. We show that this new approach is suitable for proving in a unified manner many results about Hadamard matrices with circulant core.

References

[1] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Vol. 182, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[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] S. Georgiou and C. Koukouvinos, On equivalence of Hadamard matrices and projection properties, *Ars Combinatorica*, (to appear)

[4] S. Georgiou, C. Koukouvinos and J. Seberry, Hadamard Matrices, Orthogonal designs and construction algorithms, in *Designs 2002: Further Combinatorial and Constructive Design Theory*, (W.D.Wallis, ed.), Kluwer Academic Publishers, Norwell, Ma, 2002, 133-205.

[5] A.V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York-Basel, 1979.

[6] M. Hall Jr, A survey of difference sets, *Proc. Amer. Math. Soc.*, 7 (1956), 975-986.

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

[8] J.-H. Kim and H.-Y. Song, Existence of cyclic Hadamard difference dets and its relation to binary sequences with ideal autocorrelation, *J. of Comm. and Networks*, 1 (1999), 14-18.

[9] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Clarendon Press, Oxford, 1979.

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

[11] R.L. Plackett and J.P. Burman, The design of optimum multifactorial experiments, *Biometrika*, 33 (1946), 305-325.

[12] J. S. Rose, *A Course on Group Theory*, Cambridge University Press, Cambridge; New York, 1978.

[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] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, 43 (1938) 377-385.

[15] N. J. A. Sloane, AT&T on-line encyclopedia of integer sequences, `http://www.research.att.com/ njas/sequences/`

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

[17] B. Sturmfels, *Algorithms in Invariant Theory*, Texts and monographs in symbolic computation, Springer-Verlag, Wien; New York, 1993.

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

[19] 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.

[20] A.L. Whiteman, A family of difference sets, *Illinois J. Math.*, 6 (1962), 107-121.