Department of Mathematics and Computer Science
University of Southern Denmark, Odense

August 31, 2008
Marco Chiarandini

DM811 - Heuristics for Combinatorial Optimization

Laboratory Assignment, Fall 2008

1 Introduction

Hadamard matrices are square matrices with entries $+1$ and -1 whose row vectors are mutually orthogonal, that is, their scalar products is equal to zero.

It follows from the definition that a Hadamard matrix H of order n satisfies

$$H^T H = nI_n$$

where the superscript T indicates the matrix transpose and I_n the $n \times n$ identity matrix. Thus, $\det H = \pm n^{n/2}$. An example of Hadamard matrix of order 12 is given in Figure 1.

Hadamard matrices of order n were introduced by Jacques Hadamard in 1893 as solution to the maximum determinant problem, that is, the $n \times n$ complex matrix M with elements $|M_{ij}| \leq 1$ that have the maximum possible determinant in absolute value is a real matrix M with the properties of a Hadamard matrix.

The Hadamard conjecture, one of the most interesting open problems in combinatorics, states that there are Hadamard matrices with every size $n = 4k$ (and for $n > 2$ no other sizes are possible). The smallest unsolved case is 668. The previous smallest unsolved case was 428 and was solved in 2004 by [3].

1.1 Applications

Hadamard matrices have a few interesting applications. They can almost directly be used as error-correcting code (generalized in ReedMuller codes) [7]. Moreover, they can be used in statistics in balanced repeated replication (BRR) to estimate the variance of a parameter estimator.

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - \\
1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 \\
1 & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - \\
1 & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - \\
1 & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - \\
1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 \\
1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 \\
1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 \\
1 & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - \\
1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 \\
1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & -
\end{bmatrix}$$

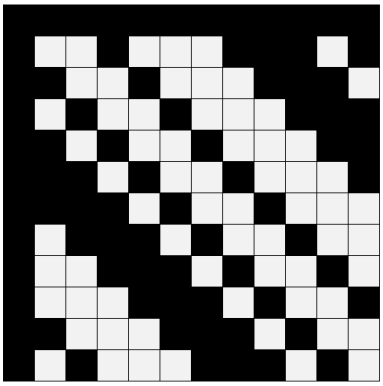

Figure 1: Two common representations of Hadamard matrix of order 12.

1.2 Equivalence of Hadamard matrices

There are some trivial transformations that applied to an Hadamard matrix return another Hadamard matrix. These are row negation, column negation, row interchange, and column interchange. Two Hadamard matrices are considered *equivalent* if one can be obtained from the other by any combination of these transformation.

Every Hadamard matrix has an equivalent *normalized* Hadamard matrix, in which every element of the first row and column are $+1$. If a Hadamard matrix of order $4k$ is in its normalized form then every row (column), except the first, has $2k$ minus ones and $2k$ plus ones. The example in Figure 1 is in normalized form.

The number of inequivalent Hadamard matrices of order n is known only for $n \leq 28$ and is:

Order	1	2	4	8	12	16	20	24	28
Inequivalent matrices	1	1	1	1	1	5	3	60	487

Millions of inequivalent matrices are known in orders 32, 36, and 40.

1.3 Constructions of Hadamard matrices

There are several methods for constructing Hadamard matrices. The first has been introduced by Sylvester in 1867, before Hadamard matrices became known with their name. Sylvester's construction shows that there is a Hadamard matrix of order 2^k for every non-negative integer k. Let H be a Hadamard matrix of order n. Then the partitioned matrix

$$\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

is a Hadamard matrix of order $2n$. This observation can be applied repeatedly and leads to the following sequence of matrices, also called Walsh matrices.

$$H_1 = \begin{bmatrix} 1 \end{bmatrix},$$

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

and

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}$$

for $k \geq 2$. This construction is equivalent to say that the Kronecker product of two Hadamard matrices is an Hadamard matrix.

The Hadamard matrices obtained in this way have some further special properties: they are symmetric and with null trace. Moreover the elements in the first row are all positive. These properties make this kind of construction particularly suitable for engineering applications such as communication systems and digital image processing.

Several others methods for constructing Hadamard matrices have been found. A list with explanation and further references of some of these methods can be found at [2]. A repository of Hadamard matrices of order up to 1000 is also available at the same web site and at [6, 8].

In this assignment, we focus on a special construction method: the *construction of Hadamards with two circulant cores via Hadamard ideals*. In [1] the authors introduce *generalized Legendre pairs* of length ℓ and show that they can be used to generate Hadamard matrices with two circulant cores of order $2\ell + 2$. Later, in [5], the authors made this construction more systematic through the notion of *Hadamard ideal*. This allowed to perform an exhaustive search of all Hadamard matrices with two circulant cores for orders up to 52 corresponding to $\ell = 25$. However, exhaustive search failed to yield results beyond Hadamards of order 68, that is $\ell = 33$. Other techniques from computational algebra and genetic algorithms increased the number of Hadamard matrices constructed in this way [4].

The task of the assignment is to design and implement heuristic algorithms for the the construction of Hadamard matrices via Hadamards ideals.

In the next section we give the details of how the construction of Hadamard matrices with two circulant cores can be reduced to the problem of finding Hadamard ideals.

2 Hadamard matrices with two circulant cores

A matrix $A = [a_{ij}]$ is a circulant matrix if $a_{ij} = a_{1,1+(j-i \pmod{\ell})}$. Let $a = (a_1, \ldots, a_\ell)$ and $b = (b_1, \ldots, b_\ell)$ be two vectors of ℓ elements and A_ℓ and B_ℓ the two circulant $\ell \times \ell$ matrices that they generate:

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

The Fletcher-Gynsin-Seberry construction of Hadamard matrices with two circulant cores [1] states that a Hadamard matrix of order $2\ell + 2$ is obtained by two circulant matrices A_ℓ and B_ℓ in the following way:

$$H_{2\ell+2} = \left[\begin{array}{cc|c|c} - & - & 1 \cdots 1 & 1 \cdots 1 \\ - & 1 & 1 \cdots 1 & - \cdots - \\ \hline 1 & 1 & & \\ \vdots & \vdots & A_l & B_l \\ 1 & 1 & & \\ \hline 1 & - & & \\ \vdots & \vdots & B_l^T & -A_l^T \\ 1 & - & & \end{array}\right], \tag{1}$$

where $-$ stands for -1, and the following further restrictions on ℓ and the vectors a and b.

- Since $2\ell + 2$ must be a multiple of 4, ℓ must be an odd integer.
- All elements of Hadamard matrices are required to be ± 1 and hence, for example,

$$a_1^2 - 1 = 0, \ldots, a_\ell^2 - 1 = 0 \qquad b_1^2 - 1 = 0, \ldots, b_\ell^2 - 1 = 0 \tag{2}$$

- Moreover, the following categories of constraints derive from the definition of Hadamard matrices of order $2\ell + 2$, that is, $H_{2\ell+2}^T H_{2\ell+2} = (2\ell + 2) I_{2\ell+2}$.

- The two circulant core matrix must satisfy the matrix equation:

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

where I_ℓ is the identity matrix of order ℓ and J_ℓ is a matrix of order ℓ with all elements equal to one.
This entails (the Diophantine constraint):

$$\left(\sum_{i=1}^{\ell} a_i\right)^2 + \left(\sum_{i=1}^{\ell} b_i\right)^2 = 2$$

and we might restrict to consider only one of the solutions of this equation (see [5] for a detailed treatment) which imposes:

$$a_1 + \ldots + a_\ell = 1, \qquad b_1 + \ldots + b_\ell = 1 \tag{3}$$

- Let $P_a(s)$ be the *periodic autocorrelation function* defined on a (finite) sequence of ℓ real numbers $\{a_0, a_1, ..., a_{\ell-1}\}$ by

$$P_a(s) = \sum_{i=0}^{\ell-1} a_i a_{(i+s) \bmod \ell}, \quad s = 0, 1, \ldots, \ell - 1 \tag{4}$$

Then the Hadamard condition imposes the following further constraints on the elements of the vectors a and b:

$$P_a(s) + P_b(s) = -2, \qquad s = 1, \ldots, \ell - 1 \tag{5}$$

Vectors a and b which are solutions to this system of equations are also called *generalized Legendre pairs*.

The system of constraints (2), (3) and (5) defines the *l-th Hadamard ideal* $\mathcal{H}_\updownarrow$ [5] and is used to generate Hadamard matrices with two circulant cores.

Note that since ℓ must be odd, we have the following *symmetry property*:

$$P_A(s) = P_A(\ell - s), \qquad s = 1, \ldots, \frac{\ell - 1}{2} \tag{6}$$

and the system of equations can be reduced from $2\ell + 2 + (l - 1)$ to $2\ell + 2 + m$ equations, with $m = \frac{l-1}{2}$.

3 Known Results

It is known that for some ℓ a Hadamard matrix of order $2\ell + 2$ with two circulant cores exists. We refer to [5] for a most up-to-date list of results which appeared in several different publications. For these values of $\ell \leq 200$ the existence of generalized Legendre pairs is instead unresolved: 77, 85, 87, 91, 93, 115, 117, 121, 123, 129, 133, 145, 147, 159, 161, 169, 171, 175, 177, 185, 187 and 195.

Similarly there are values of ℓ for which solutions have been found.

- exhaustive search $\ell \leq 25$ [5]

- truncated exhaustive search $\ell \leq 47$ [1]
- incomplete search for $49 \leq \ell \leq 55$ [1]

The progression of the number of solutions $|V(\mathcal{H}_l)|$ for each ℓ up to 25 is summarized in the following table copied from [5]:

Matrix	*order*	$\vert V(H)\vert$		
3	8	9	=	1×3^2
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

To illustrate the difficulty of finding solutions to the system of polynomial equations of the Hadamard ideal we mention that the size of the discrete search space $\{-1,+1\}^{2\ell}$ (also called the boolean hypercube) is equal to $2^{2\ell}$. The size of the subspace of solutions $V(\mathcal{H}_\updownarrow)$ defined by equations (2), (3) and (5) is upper bounded by the following lemma [5].

Lemma 1 *For every odd $\ell = 3, \ldots$, we have*

$$|V(\mathcal{H}_l)| \leq C^2_{\frac{l-1}{l}} \cdot \ell^2$$

where Catalan numbers C_n are defined by:

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

References

[1] R.J. Fletcher, M. Gysin, and J. Seberry. Application of the discrete fourier transform to the search for generalised legendre pairs and hadamard matrices. *Australasian Journal of Combinatorics*, 23:75–86, 2001.

[2] V.K. Gupta, Rajender Parsad, and A. Dhandapani. Hadamard matrix. http://www.iasri.res.in/webhadamard/, Created: July, 2007, Visited: September, 2007.

[3] H. Kharaghani and B. Tayfeh-Rezaie. A hadamard matrix of order 428. *Journal of Combinatorial Designs*, 13:435–440, 2005.

[4] I. S. Kotsireas and C. Koukouvinos. Genetic algorithms for the construction of Hadamard matrices with two circulant cores. *Journal of Discrete Mathematical Sciences and Cryptography*, 8(2):658–668, 2005.

[5] Ilias S. Kotsireas, Christos Koukouvinos, and Jennifer Seberry. Hadamard ideals and Hadamard matrices with two circulant cores. *European J. Combin.*, 27(5):658–668, 2006.

[6] Jennifer Seberry. http://www.uow.edu.au/˜jennie/hadamard.html, 2001.

[7] Jennifer Seberry, Beata J Wysocki, and Tadeusz A Wysocki. On some applications of hadamard matrices. *Metrika*, pages 221–239, 2005.

[8] N. J. A. Sloane. A library of hadamard matrices. http://www.research.att.com/˜njas/hadamard/.