University of Wollongong
Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

2010

Some remarks on Hadamard matrices

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

Marilena Mitrouli
University of Athens, Greece

Publication Details

Seberry, J and Mitrouli, M, Some remarks on Hadamard matrices, Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences, Published on line 7th July 2010 *Cryptography and Communications,* 2(2): 293-306 (2010) 293-306.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Some remarks on Hadamard matrices

Abstract

In this note we use combinatorial methods to show that the unique, up to equivalence, 5×5 $(1, -1)$-matrix with determinant 48, the unique, up to equivalence, 6×6 $(1,-1)$-matrix with determinant 160, and the unique, up to equivalence, 7×7 $(1,-1)$-matrix with determinant 576, all cannot be embedded in the Hadamard matrix of order 8. We also review some properties of Sylvester Hadamard matrices, their Smith Normal Forms, and pivot patterns of Hadamard matrices when Gaussian Elimination with complete pivoting is applied on them. The pivot values which appear reconfirm the above non-embedding results.

Disciplines

Physical Sciences and Mathematics

Publication Details

Seberry, J and Mitrouli, M, Some remarks on Hadamard matrices, Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences, Published on line 7th July 2010 *Cryptography and Communications,* 2(2): 293-306 (2010) 293-306.

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/852

Some remarks on Hadamard matrices

Jennifer Seberry
CCISR, SCSSE
University of Wollongong
NSW, 2522
Australia

Marilena Mitrouli
Department of Mathematics
University of Athens
Panepistemiopolis 15784
Greece

June 8, 2010

Dedicated with great respect to Warwick de Launey

Abstract

In this note we use combinatorial methods to show that the unique, up to equivalence, 5×5 $(1, -1)$-matrix with determinant 48, the unique, up to equivalence, 6×6 $(1, -1)$-matrix with determinant 160, and the unique, up to equivalence, 7×7 $(1, -1)$-matrix with determinant 576, all cannot be embedded in the Hadamard matrix of order 8.

We also review some properties of Sylvester Hadamard matrices, their Smith Normal Forms, and pivot patterns of Hadamard matrices when Gaussian Elimination with complete pivoting is applied on them. The pivot values which appear reconfirm the above non-embedding results.

Key words and phrases: Hadamard matrices, Smith Normal Form, embedding matrices, completely pivoted, determinant, Gaussian elimination

AMS Subject Classification: 05B20, 15A15, 65F40, 62K05

1 Matrices with $(1, -1)$ entries and maximal determinant

An n-dimensional Hadamard matrix is an $n \times n$ matrix of $1s$ and $-1s$ with $HH^T = nI_n$. A Hadamard matrix is said to be *normalized* if it has its first row and column all $1s$. We can always normalize a Hadamard matrix by multiplying rows and columns by -1 where needed. In these matrices, n is necessarily 2 or a multiple of 4 [**?**]. We recall that although orthogonal $(1, -1)$-matrices are known as Hadamard matrices, they were in fact first reported by Sylvester in 1867 [**?**]. Sylvester had noted that if one took a $(1, -1)$-matrix, S, of order t whose rows are mutually orthogonal, then

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

is an orthogonal $(1,-1)$-matrix of order $2t$. Matrices of this form are called *Sylvester Hadamard matrices*, and are defined for all powers of 2.

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 and/or column interchanges and row and/or column negations.

We recall that the original interest in Hadamard matrices stemmed from the fact that a Hadamard matrix $H = (h_{ij})$ of order n satisfies equality in Hadamard's inequality

$$(det\ H)^2 \leq \prod_{j=1}^{n} \sum_{i=1}^{n} |h_{ij}|^2$$

for elements in the unit circle.

This has led to further study of the maximum determinant problem for $(1,-1)$-matrices of any order. This problem was first brought to the attention of one of us by a 1970 report for the USAF [**?**] by Stanley Payne at Dayton, Ohio.

A *D-optimal design of order* n is an $n \times n$ $(1,-1)$-matrix having maximum determinant. Like Hadamard matrices, we can always put a D-optimal design into normalized form. It is well known that Hadamard matrices of order n have absolute value of determinant $n^{n/2}$, and thus are D-optimal designs for $n \equiv 0\ (mod\ 4)$.

It is a simple exercise to show that the matrices

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

have maximum determinant for n= 2, 3, 4. We call these matrices (or their Hadamard equivalents) D_2, D_3, and D_4. The following result specifies the existence of the D-optimal design of order 4 with determinant 16 in every Hadamard matrix.

Theorem 1 ([?], [?]) *Every Hadamard matrix of order* ≥ 4 *contains a submatrix equivalent to*

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

Remark 1 Since D_2 and D_3 are embedded in D_4, Theorem **??** implies that every Hadamard matrix of order ≥ 4 contains submatrices equivalent to D_2 and D_3.

In this paper we are interested in embedding D-optimal designs of orders $m = 5, 6, 7$ and 8 in Hadamard matrices of order n. We also study some interesting properties of Sylvester Hadamard matrices, such as their sign changes and

their Smith Normal Form. We present some results concerning the pivot values that appear when Gaussian Elimination with complete pivoting is applied to Hadamard matrices. Using the pivot patterns which have been evaluated, we prove the existence or non existence of specific D-optimal designs.

Notation. Throughout this paper we use $-$ for -1 and 1 for $+1$. We write H_j for a Hadamard matrix of order j, S_j for the Sylvester Hadamard matrix of order j, and D_j for a D-optimal design of order j. The notation $D_j \in H_n$ means "D_j is embedded in some H_n". Whenever a determinant or minor is mentioned in this work, we mean its absolute value.

2 D-optimal designs embedded in Hadamard matrices

The unique, under Hadamard equivalence operations, D-optimal designs are given by H. Kharaghani and W. Orrick [**?**]. We note here:

the 5×5 $(1, -1)$-matrix with maximal determinant 48

$$D_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & - \\ 1 & 1 & - & - & - \\ 1 & - & - & 1 & - \\ 1 & - & - & - & 1 \end{bmatrix};$$

the 6×6 $(1, -1)$-matrix with maximal determinant 160

$$D_6 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & - & 1 \\ 1 & 1 & - & - & - & 1 \\ 1 & - & - & 1 & - & 1 \\ 1 & 1 & 1 & 1 & - & - \\ 1 & - & - & - & 1 & - \end{bmatrix};$$

and the 7×7 $(1, -1)$-matrix with maximal determinant 576

$$D_7 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & - & - & - & 1 & 1 \\ 1 & - & 1 & - & - & 1 & 1 \\ 1 & - & - & 1 & 1 & - & 1 \\ 1 & - & - & 1 & 1 & 1 & - \\ 1 & 1 & 1 & - & 1 & - & - \\ 1 & 1 & 1 & 1 & - & - & - \end{bmatrix}.$$

The $(1, -1)$-matrix with maximal determinant 4096 is the Hadamard matrix of order 8. Indeed the Hadamard matrix of order n always has maximal determinant $n^{\frac{n}{2}}$.

2.1 Embedding D_5 in H_8

Lemma 1 *The D-optimal design of order* 5 *(D_5) is not embedded in a Hadamard matrix of order* 8 *(H_8).*

Proof. We attempt to extend

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

to H_8. Without loss of generality we choose $(1,6) = (1,7) = (1,8) = 1$. We note that rows $2,3,4,5$ each contain three $-1s$ and two $1s$, so for them to be orthogonal with the first row each needs to be extended by one -1 and two $1s$. We also note the mutual inner product of rows 2, 3, 4, 5 is $+1$. It is not possible to extend them by choosing the single -1 in individual columns, as there are 4 rows and 3 columns. Hence by the pigeonhole principle this is impossible. Hence D_5 does not exist embedded in a Hadamard matrix of order 8.

We note that Edelman and Mascarenhas [**?**] and Seberry, Xia, Koukouvinos and Mitrouli [**?**] have shown that D_5 is embedded in H_{12}.

2.2 Embedding D_6 in H_8

Lemma 2 *The D-optimal design of order* 6 *(D_6) is not embedded in a Hadamard matrix of order* 8 *(H_8).*

Proof. We extend partially the 6×6 matrix, D_6, by adding two columns. Without loss of generality we may choose $h_{17} = h_{18} = h_{27} = -h_{28} = 1 = h_{67} = h_{68}$, so we have

$$H_8^{partial} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & - & 1 & 1 & - \\ 1 & 1 & - & - & - & 1 & h_{37} & h_{38} \\ 1 & - & - & 1 & - & 1 & h_{47} & h_{48} \\ 1 & 1 & 1 & 1 & - & - & h_{57} & h_{58} \\ 1 & - & - & - & 1 & - & 1 & 1 \end{bmatrix}.$$

Now the inner product of row 5 with row 1 gives $h_{57} + h_{58} = -2$, while the inner product of row 5 and row 2 gives $h_{57} - h_{58} = 0$. So $h_{57} = h_{58} = -1$. But now the inner product of rows 5 and 6 cannot be zero, so D_6 cannot be extended to H_8.

2.3 Embedding D_7 in H_8

Lemma 3 *The D-optimal design of order* 7 *(D_7) is not embedded in a Hadamard matrix of order* 8 *(H_8).*

Proof. To embed D_7 in H_8 it is merely necessary to note that for H_8 we can choose $h_{18} = 1$. Every other row of H_8 must have 4 $1s$ and 4 $-1s$, so we extend D_7 thus:

$$D_7^{extended} = \left[\begin{array}{ccccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & - & - & - & 1 & 1 & - \\ 1 & - & 1 & - & - & 1 & 1 & - \\ 1 & - & - & 1 & 1 & - & 1 & - \\ 1 & - & - & 1 & 1 & 1 & - & - \\ 1 & 1 & 1 & - & 1 & - & - & - \\ 1 & 1 & 1 & 1 & - & - & - & - \end{array}\right].$$

But rows 2 and 3 are not orthogonal, so the embedding is not possible.

Remark 2 One of the referees has also pointed out that since all the 7×7 minors of the 8×8 Hadamard matrix are equal to 512 (an immediate consequence of the definition of Hadamard matrix), this also proves Lemma 3.

2.4 Other embeddings

We searched for D-optimal designs of orders $m = 5, 6, 7$ and 8 embedded in classes of Hadamard matrices. By selecting m rows and columns of the Hadamard matrices tested, we checked if the determinants of the $m \times m$ submatrices were equal to $\det(D_m)$. More specifically, we searched the full list of Hadamard matrices of orders $n = 12$, 16, 20, 24 and 28 for this purpose. There are exactly 1, 5, 3, 60 and 487 inequivalent Hadamard matrices respectively, at each order. Our findings are summarized in Table **??**.

	n				
m	12	16	20	24	28
5	1	5	3	60	487
6	1	4	3	60	487
7	1	3	3	60	487
8	0	5	3	60	487

Table 1: Number of Hadamard matrices of order n in which the D-optimal design of order m embeds

By examining Table 1, one notices that

- The D-optimal design of order $m = 5$ is embedded in all Hadamard matrices of the specific orders we study.
- The D-optimal design of order $m = 6$ is embedded in almost all Hadamard matrices of the specific orders we study. It is not embedded in one Hadamard matrix of order $n = 16$: the Sylvester Hadamard matrix.

- The D-optimal design of order $m = 7$ is embedded in all Hadamard matrices we study, except for two Hadamard matrices of order $n = 16$, one of which is the Sylvester Hadamard matrix.
- The D-optimal design of order $m = 8$ (i.e., the Hadamard matrix of order 8) is embedded in all Hadamard matrices we study except for the Hadamard matrix of order $n = 12$.

In Table **??** we summarize the above results, with some extensions and conjectures added in the last column.

$D_2 \in D_4$				$D_2 \in H_{4t} \ \ \forall \ \ t$
$D_3 \in D_4$				$D_3 \in H_{4t} \ \ \forall \ \ t$
$D_4 \in H_8$	$D_4 \in H_{12}$	$D_4 \in H_{16}$	$D_4 \in H_{20}, H_{24}, H_{28}$	$D_4 \in H_{4t} \ \ \forall \ \ t$
$D_5 \notin H_8$	$D_5 \in H_{12}$	$D_5 \in H_{16}$	$D_5 \in H_{20}, H_{24}, H_{28}$	$D_5 \in H_{4t} \ \ \forall \ \ t > 2$
$D_6 \notin H_8$	$D_6 \in H_{12}$	$D_6 \in H_{16}$	$D_6 \in H_{20}, H_{24}, H_{28}$	$D_6 \in H_{4t} \ \ \forall \ \ t > 2$
		$D_6 \notin S_{16}$		$D_6 \in S_{32}, S_{64}$
$D_7 \notin H_8$	$D_7 \in H_{12}$	$D_7 \in H_{16}$	$D_7 \in H_{20}, H_{24}, H_{28}$	$D_7 \in H_{4t} \ \ \forall \ \ t > 2$
		$D_7 \notin S_{16}$		$D_7 \notin S_{32}$, $D_7 \in S_{64}$
$D_8 = H_8$	$D_8 \notin H_{12}$	$D_8 \in H_{16}$	$D_8 \in H_{20}, H_{24}, H_{28}$	

Table 2: Existence and non existence of D-optimal designs in Hadamard matrices

The above results and conjectures posed are indicative of the following theorem of Warwick de Launey's [**?**].

Theorem 2 *For every $(1, -1)$-submatrix there exists an n_0, large enough, such that the submatrix is embedded in H_{n_0}.*

One of the referees provided a proof for a slightly stronger result than this, concerning the existence of any $(1, -1)$-matrix in S_N, for large enough N.

Remark 3 Using the same combinatorial methods as used to show that $D_7 \notin H_8$, we can show that $H_n \notin H_{n+4}, \ldots, H_{2n-4}$.

Question 1. Can we give a bound on the size of D_m that will embed into an S_n? (Note that $D_6 \notin S_{16}$ but $D_6 \in S_{32}, S_{64}$.)

3 Remarks on Sylvester Hadamard matrices

The first few Sylvester-Hadamard matrices of orders 2^p, $p = 1, 2, 3$, are given below. We augment each matrix with an additional last column which states the number of times the sign changes as we proceed from left to right across the row.

$$S_2 = \left[\begin{array}{cc|c} 1 & 1 & 0 \\ 1 & - & 1 \end{array}\right], \quad S_4 = \left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 1 & - & 1 & - & 3 \\ 1 & 1 & - & - & 1 \\ 1 & - & - & 1 & 2 \end{array}\right], \quad S_8 = \left[\begin{array}{cccccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & - & 1 & - & 1 & - & 1 & - & 7 \\ 1 & 1 & - & - & 1 & 1 & - & - & 3 \\ 1 & - & - & 1 & 1 & - & - & 1 & 4 \\ 1 & 1 & 1 & 1 & - & - & - & - & 1 \\ 1 & - & 1 & - & - & 1 & - & 1 & 6 \\ 1 & 1 & - & - & - & - & 1 & 1 & 2 \\ 1 & - & - & 1 & - & 1 & 1 & - & 5 \end{array}\right]$$

In fact we have

Lemma 4 *If a $(1,-1)$-matrix S_m of order m has all the sign changes $0, 1, \ldots, m-1$, then its Sylvester matrix S_{2m} of order $2m$, constructed from (**??**), will have all the sign changes $0, 1, \ldots, 2m-1$. The same is true for the columns.*

This is also observed in

$$S_{16} = \left[\begin{array}{cccccccccccccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 15 \\ \\ 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 7 \\ 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 & 8 \\ \\ 1 & 1 & 1 & 1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - & - & 3 \\ 1 & - & 1 & - & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - & 1 & 12 \\ \\ 1 & 1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - & - & 1 & 1 & 4 \\ 1 & - & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - & 1 & 1 & - & 11 \\ \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - & - & 1 & - & 1 & - & 1 & - & 1 & 14 \\ \\ 1 & 1 & - & - & 1 & 1 & - & - & - & - & 1 & 1 & - & - & 1 & 1 & 6 \\ 1 & - & - & 1 & 1 & - & - & 1 & - & 1 & 1 & - & - & 1 & 1 & - & 9 \\ \\ 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - & 1 & 1 & 1 & 1 & 2 \\ 1 & - & 1 & - & - & 1 & - & 1 & - & 1 & - & 1 & 1 & - & 1 & - & 13 \\ \\ 1 & 1 & - & - & - & - & 1 & 1 & - & - & 1 & 1 & 1 & 1 & - & - & 5 \\ 1 & - & - & 1 & - & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - & 1 & 10 \end{array}\right].$$

This property is well known to users of the Walsh functions, but has not been emphasized in the mathematical literature. This has prompted us to mention it explicitly here.

3.1 Smith Normal Form

The following theorem due to Smith [**?**] has been reworded from the theorem and proofs in MacDuffee [**?**, p41] and Marcus and Minc [**?**, p44].

Theorem 3 *If $A = (a_{ij})$ is any integer matrix of order n and rank r, then there is a unique integer matrix*

$$D = \mathrm{diag}(a_1, a_2, \ldots, a_r, 0, \ldots, 0)$$

where $a_i | a_{i+1}$ are non-negative invariant integers, such that A can be diagonalized to D. The greatest common divisor of the $i \times i$ sub-determinants of A is

$$a_1, a_2, \ldots, a_i.$$

These invariants are called the *invariants of* A, and the diagonal matrix D is called *the Smith Normal Form* (SNF).

A SNF is said to be in *standard form* [**?**, p. 411] for all Hadamard matrices of order $4t$, if it is in the form

$$\mathrm{diag}(1, \underbrace{2, 2, \ldots, 2}_{2t-1}, \underbrace{2t, 2t, \ldots, 2t}_{2t-1}, 4t).$$

We note that the SNF of the inverse of a Hadamard matrix is the same (up to a constant) as that of a Hadamard matrix. In the proof they appear in reverse order, but to satisfy the divisibility property they must be reordered. This was observed by Spence [**?**]. W. D. Wallis and Jennifer Seberry (Wallis) [**?**] showed that for a Hadamard matrix, H, of order $4t$, where t is square free, the SNF of H is in standard form. More recently T. S. Michael and W. D. Wallis [**?**] have shown that all skew Hadamard matrices have SNF in standard form.

However the powers of 2 are different. Marshall Hall, Jr. [**?**] gave five inequivalent classes of Hadamard matrices of order 16: HI, HII, $HIII$, HIV, $HV = HIV^T$. These have SNFs

$$\mathrm{diag}(1, \underbrace{2, 2, \ldots, 2}_{4}, \underbrace{4, 4, \ldots, 4}_{6}, \underbrace{8, 8, \ldots, 8}_{4}, 16),$$

$$\mathrm{diag}(1, \underbrace{2, 2, \ldots, 2}_{5}, \underbrace{4, 4, \ldots, 4}_{4}, \underbrace{8, 8, \ldots, 8}_{5}, 16),$$

$$\mathrm{diag}(1, \underbrace{2, 2, \ldots, 2}_{6}, \underbrace{4, 4, \ldots, 4}_{2}, \underbrace{8, 8, \ldots, 8}_{6}, 16),$$

and, for HIV and HV,

$$\mathrm{diag}(1, \underbrace{2, 2, \ldots, 2}_{7}, \underbrace{8, 8, \ldots, 8}_{7}, 16).$$

The Sylvester Hadamard matrix of order 16 belongs to Marshall Hall, Jr.'s class HI. It is known that the number of $2s$ in the SNF of a Hadamard matrix of order $4t$ is $\geq \log_2 4t$.

In fact the Sylvester Hadamard matrix of order 2^t always has exactly t $2s$ in its SNF.

Lemma 5 *If the SNF of any matrix, A, is*

$$D = \mathrm{diag}(a_1, a_2, \ldots, a_r, 0, \ldots 0)$$

then the SNF of $\begin{bmatrix} A & A \\ A & -A \end{bmatrix}$ *is comprised of*

$$(a_1, a_2, \ldots, a_r, 2a_1, 2a_2, \ldots, 2a_r, 0, \ldots 0).$$

(These may have to be reordered.)

Remark 4 The number of occurrences of 2^r in the SNF of the Sylvester matrix of order 2^k is $\binom{k}{r}$ for $0 \leq r \leq k$.

4 The Growth Problem for Hadamard matrices

During the process of Gaussian Elimination to solve linear equations or to invert a matrix, the pivots can become very large and so, with rounding errors included, unstable. This is the origin of the "growth problem".

Hadamard matrices are related to the well known growth problem. Traditionally, backward error analysis for Gaussian Elimination (GE), see e.g. [**?**], on a matrix $A = (a_{ij}^{(1)})$ is expressed in terms of the *growth factor*

$$g(n, A) = \frac{max_{i,j,k}|a_{ij}^{(k)}|}{max_{i,j}|a_{ij}^{(1)}|},$$

which involves all the elements $a_{ij}^{(k)}$, $k = 1, 2, \ldots, n$, that occur during the elimination. Matrices with the property that no row and column exchanges are needed during GE with complete pivoting are called *completely pivoted* (CP). In other words, at each step of the elimination the element of largest magnitude (the "pivot") is located at the top left position of every submatrix appearing during the process. For a CP matrix A we have

$$g(n, A) = \frac{max\{p_1, p_2, \ldots, p_n\}}{|a_{11}^{(1)}|},$$

where $p_1, p_2, \ldots, p_n$ are the pivots of A.

The following lemma gives a useful relation between pivots and minors and a characteristic property for CP matrices.

Lemma 6 ([?]) *Let A be a CP matrix.*

(i) *The magnitude of the pivots which appear after application of GE operations to A is given by*

$$p_j = \frac{A(j)}{A(j-1)}, \quad j = 1, 2, \ldots, n, \quad A(0) = 1.$$

where $A(j)$ denotes the absolute value of the $j \times j$ principal minor.

(ii) *The maximum $j \times j$ leading principal minor of A, when the first $j-1$ rows and columns are fixed, is $A(j)$.*

From Lemma **??** we see that the calculation of minors is important in studying pivot structures. Moreover, the maximum $j \times j$ minor appears in the upper left $j \times j$ corner of A. So, if the existence of a matrix with maximal determinant, i.e., a D-optimal design, is proved for a CP matrix A, we can indeed assume that it always appears in its upper left corner.

H-equivalence operations do not preserve pivots, i.e., the pivot pattern is not invariant under H-equivalence, and many pivot patterns can be observed. So H-equivalent matrices do not necessarily have the same pivot pattern.

Pivots can also be given from the relation in [**?**]:

$$p_{n+1-k} = \frac{nA[k-1]}{A[k]}, \quad k = 1, 2, \ldots, n, \quad A[0] = 1.$$

where $A[k]$ denotes the absolute value of the determinant of the lower right $k \times k$ principal submatrix.

In 1968 Cryer [**?**] conjectured that the maximum growth at each stage of Gaussian Elimination is less than or equal to the order of the matrix, and equals the order only if the matrix is Hadamard.

Gould [**?**] proved that the first part of the conjecture is not true. He found matrices as follows

n	growth
13	13.02
18	20.45
20	24.25
25	32.99

Thus, the following remains open.

Conjecture [Cryer]. The growth of a Hadamard matrix is its order.

Concerning progress on this conjecture, the pivot patterns of Sylvester Hadamard matrices are specified in [**?**], and the pivot patterns of Hadamard matrices of orders 12 and 16 are specified in [**?**, **?**]. Next, we connect, for the first time, the values of the pivots appearing to the existence or not of D-optimal designs in these Hadamard matrices. This will provide another proof of Lemmas 1, 2, 3, and a reconfirmation of the results in Table 1.

The pivot structure of H_8
The growth of H_8 is 8 [**?**] and its unique pattern is

$$1 \quad 2 \quad 2 \quad 4 \quad 2 \quad 4 \quad 4 \quad 8$$

Day and Peterson [**?**] specify that $H_8(5) = 32$, $H_8(6) = 128$ and $H_8(7) = 512$. From this we can reconfirm Lemmas 1,2 and 3, i.e., $D_5, D_6, D_7 \notin H_8$.

The pivot structure of H_{12}
In [**?**] it was proved that the growth of H_{12} is 12 and its unique pattern was determined to be

$$1 \quad 2 \quad 2 \quad 4 \quad 3 \quad \tfrac{10}{3} \quad \tfrac{18}{5} \quad 4 \quad 3 \quad 6 \quad 6 \quad 12$$

Lemma 7 *The D-optimal design of order* 5 *appears in the Hadamard matrix of order* 12.

Proof. From the unique pivot pattern of H_{12} we see that p_5 is 3. From Lemma 6 we have that

$$p_5 = \frac{H_{12}(5)}{H_{12}(4)}.$$

According to Theorem 1 and Lemma 6, $H_{12}(4)$ always takes the value 16. Thus the value of $H_{12}(5)$ will be 48. This means that the D-optimal design of order 5 always appears in the Hadamard matrix of order 12.

Lemma 8 *The D-optimal design of order* 6 *appears in the Hadamard matrix of order* 12.

Proof. From the unique pivot pattern of H_{12} we see that p_6 is $\frac{10}{3}$. From Lemma 6 we have that

$$p_6 = \frac{H_{12}(6)}{H_{12}(5)}.$$

According to Lemmas 6 and **??**, $H_{12}(5)$ takes the value 48; thus the value of $H_{12}(6)$ will be 160. This means that the D-optimal design of order 6 always appears in the Hadamard matrix of order 12.

Lemma 9 *The D-optimal design of order* 7 *appears in the Hadamard matrix of order* 12.

Proof. From the unique pivot pattern of H_{12} we see that p_7 is $\frac{18}{5}$. From Lemma 6 we have that

$$p_7 = \frac{H_{12}(7)}{H_{12}(6)}.$$

According to Lemmas 6 and **??**, $H_{12}(6)$ takes the value 160; thus the value of $H_{12}(7)$ will be 576. This means that the D-optimal design of order 7 always appears in the Hadamard matrix of order 12.

Lemma 10 *The D-optimal design of order* 8 *does not appear in the Hadamard matrix of order* 12.

Proof. From the unique pivot pattern of H_{12} we see that p_8 is 4. From Lemma 6 we have that

$$p_8 = \frac{H_{12}(8)}{H_{12}(7)}.$$

According to Lemmas 6 and **??**, $H_{12}(7)$ takes the value 576. Thus the value of $H_{12}(8)$ will be 2309 and not 4096, which is the value of the D-optimal case. This means that the D-optimal design of order 8 does not appear in the Hadamard matrix of order 12.

The pivot structure of H_{16}

In [**?**] it was proved that the growth of H_{16} is 16, and it was determined that there are exactly 34 pivot patterns up to H-equivalence as given in Table **??**.

Pivot	1st Class (Sylvester Hadamard)	2nd Class	3rd Class	4th Class
1	1	1	1	1
2	2	2	2	2
3	2	2	2	2
4	4	4	4	4
5	2,3	2,3	2,3	2,3
6	4,$\frac{8}{3}$	4,$\frac{10}{3}$	4,$\frac{8}{3}$,$\frac{10}{3}$	4,$\frac{10}{3}$
7	2,4	4,$\frac{8}{10/3}$,$\frac{16}{5}$	4,$\frac{18}{5}$	4,$\frac{18}{5}$
8	4,6,8	4,5,6,8	4,$\frac{9}{2}$,5,6,8	4,5,6,8
9	2,4,$\frac{8}{3}$	2,4,$\frac{8}{3}$,$\frac{16}{3}$,$\frac{16}{5}$	2,4,$\frac{9}{2}$,$\frac{8}{3}$,$\frac{16}{5}$	2,4,$\frac{9}{2}$,$\frac{8}{3}$ $\frac{16}{5}$
10	4,8	4,5	4,5,$\frac{16}{18/5}$	4,5,$\frac{16}{18/5}$
11	4,6,8	4,6,$\frac{16}{10/3}$	4,6,$\frac{16}{10/3}$	4,6,$\frac{16}{10/3}$
12	8,$\frac{16}{3}$	8,$\frac{16}{3}$	8,$\frac{16}{3}$	8,$\frac{16}{3}$
13	4,8	4	4	4
14	8	8	8	8
15	8	8	8	8
16	16	16	16	16

Table 3: The 34 pivot patterns of the Hadamard matrix of order 16

An interesting fact is that 8 occurs as pivot p_{13} only in the Sylvester Hadamard matrices. Since $p_{13} = \frac{nH_{16}[3]}{H_{16}[4]}$, and since $H_{16}[3]$ equals 4 (the only possible nonzero value for the determinant of a 3×3 matrix with entries in $(1, -1)$), in order $p_{13} = 8$ we must have that $H_{16}[4]$ takes the value 8 (possible nonzero values for the determinants of a 4×4 matrix with entries in $(1, -1)$ are 8 and 16). This raises the following question.

Question 2. For a CP Hadamard matrix of order 16, can the determinant of its lower right 4×4 principal submatrix only take the value 8 if the matrix is in the Sylvester Hadamard equivalence class?

The next open case is the specification of the growth factor of the Hadamard matrix of order 20.

5 Summary and Conclusions

While we have given some results that are known, it is clear that pushing the boundaries is generally rewarding. During the talk given by Prof. Seberry at the 'International Conference on Design Theory and Applications' in Galway in 2009 (which was the motivation for this paper), discussion of open questions was very exciting. A recent abstract of Kharaghani and Tayfeh-Rezaie [**?**] shows that there are very nearly 13,680,757 inequivalent matrices of order 32 (and perhaps a very few more of other types). It was observed that 20 million inequivalent Hadamard matrices of order 36 are known. All are regular. It was emphasized that this work was ongoing and much of it seems to be being carried out in Iran. It was conjectured in Bouyukliev, Fack and Winne [**?**] that all Hadamard matrices of order 36 are regular. So we raise four further questions.

Question 3. Although many regular symmetric Hadamard matrices of order 36 are known, not all are: many are not equivalent to their own transposes. How many regular symmetric Hadamard matrices exist?

Question 4. How many regular symmetric Hadamard matrices of order 36 with constant diagonal, i.e., a nice graph, can be found?

Question 5. We have excellent asymptotic results for the existence of Hadamard matrices. Indeed, Warwick de Launey [**?**] makes exciting new claims. He believes that the full power of the multiplication results of Agaian type has not yet been exploited [**?**]. We have asymptotic results for existence of symmetric Hadamard matrices. Is there an asymptotic result for the existence of skew Hadamard matrices?

Question 6. Show that Hadamard matrices exist with positive density in the integers $4t$.

Note added in proof. Warwick de Launey [**?**] indicated that he has found an asymptotic existence theorem for skew Hadamard matrices.

Acknowledgement. We thank the referees for their thoughtful and thought provoking comments, the references they gave, and the inspiration they provided.

References

[1] I. Bouyukliev, V. Fack and J. Winne, 2-(31,15,7), 2-(35,17,8) and 2-(36,15,6) designs with automorphisms of odd prime order, and their related Hadamard matrices and codes, *Designs Codes and Cryptography*, 51 (2009) 105.

[2] C.W. Cryer, Pivot size in Gaussian elimination, *Numer. Math.*, 12 (1968), 335-345.

[3] J. Day and B. Peterson, Growth in Gaussian elimination, *Amer. Math. Monthly*, 95 (1988), 489-513.

[4] Warwick de Launey, private conversation, Sevilla, Spain, 2007.

[5] Warwick de Launey, private conversation, Galway, Ireland, 2009.

[6] Warwick de Launey, private email to Jennifer Seberry, February 2010.

[7] Warwick de Launey, On the asymptotic existence of Hadamard matrices.

`http://arxiv.org/abs/1003.4001`

[8] A. Edelman and W. Mascarenhas, On the complete pivoting conjecture for a Hadamard matrix of order 12, *Linear and Multilinear Algebra*, 38 (1995), 181-187.

[9] N. Gould, On growth in Gaussian elimination with pivoting, *SIAM J. Matrix Anal. Appl.*, 12 (1991), 354-361.

[10] Marshall Hall Jr., Hadamard matrices of order 16, J.P.L. Research Summary No.36-10, 1 (1961), 21-26.

[11] H. Kharaghani and W. Orrick, D-optimal Matrices, in *Handbook of Combinatorial Designs*, eds. C.J. Colbourn and J.H. Dinitz, Second Edition, Chapman and Hall, CRC, Boca Racon Fla., 2007, pp. 296-298.

[12] H. Kharaghani and B. Tayfeh-Rezaie, On the classification of Hadamard matrices of order 32.

`http://www3.interscience.wiley.com/journal/123249643/abstract`

[13] C. Kravvaritis and M. Mitrouli, The growth factor of a Hadamard matrix of order 16 is 16, *Numerical Linear Algebra and its Appl.*, 16, (7-9), (2009), 715-743.

[14] C. C. Macduffee, *The Theory of Matrices*, Reprint of First Ed., Chelsea, NY, 1964.

[15] M. Marcus and H. Minc, *A Survey of Matrix Theory and Matrix Inequalities,* Allyn and Bacon, Boston, 1964.

[16] T.S. Michael and W.D. Wallis, Skew Hadamard matrices and the Smith normal form, *Designs, Codes and Cryptography*, 13 (1998), 173-176.

[17] Verbal conversation between Stanley Payne and Jennifer Seberry (Wallis) circa 1972.

[18] J. Seberry, T. Xia, C. Koukouvinos, and M. Mitrouli, The maximal determinant and subdeterminants of ± 1 matrices, *Linear Algebra and its Appl.*, 373 (2003), 297-310.

[19] Jennifer Seberry (Wallis), Hadamard matrices, Part IV, of W.D.Wallis, Anne Penfold Street and Jennifer Seberry (Wallis), *Combinatorics: Room Squares, Sum-Free Sets and Hadamard Matrices*, LNM, Springer Verlag, Berlin, 1972.

[20] H. J. S. Smith, Arithmetical notes, *Proc. London Math. Soc.*, 4 (1873), 236-253.

[21] E. Spence, A note on the equivalence of Hadamard matrices, *Notices of the American Mathematical Society,* 18 (1971) 624.

[22] J. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile work, and the theory of numbers, *Phil. Mag.* (4) 34, (1867), 461-475.

[23] W. D. Wallis and Jennifer Seberry Wallis, Equivalence of Hadamard matrices, *Israel J. Math.,* 7, (1969), 122-128.