On the real unbiased Hadamard matrices

W. H. Holzmann, H. Kharaghani^{*} Department of Mathematics & Computer Science University of Lethbridge Lethbridge, Alberta, T1K 3M4 Canada email: holzmann@uleth.ca, kharaghani@uleth.ca W. Orrick Department of Mathematics Indiana University Bloomington, Indiana 47405 USA email: worrick@indina.edu

February 8, 2010

Abstract

The class of mutually unbiased Hadamard (**MUH**) matrices is studied. We show that the number of **MUH** matrices of order $4n^2$, *n* odd is at most 2 and that the bound is attained for n = 1, 3. Furthermore, we find a lower bound for the number of **MUH** matrices of order $16n^2$, assuming the existence of a Hadamard matrix of order 4n. An extension to unbiased weighing matrices is also presented.

AMS Subject Classification: Primary 05B20.

Keywords: Hadamard matrix, unbiased Hadamard matrices, unbiased bases, Latin Square, MOLS, Mutually Suitable Latin Squares.

1 Preliminaries

A *Hadamard* matrix is a matrix H of order n with entries in $\{-1,1\}$ and orthogonal rows in the usual inner product on \mathbb{R}^n . Such matrices exist only if n is a multiple of 4, $n \ge 3$. It is

^{*}Both authors supported by an NSERC Discovery Grant - Group.

conjectured that for each natural number k, there is a Hadamard matrix of order 4k. The first order for which the existence of a Hadamard matrix is not known is 668. We refer the reader to [6, 8] for more information. Two Hadamard matrices H and K of order n are called *unbiased* if $HK^t = \sqrt{nL}$, where K^t denotes the transpose of the matrix H and L is a Hadamard matrix of order n. While there is considerable interest in unbiased unit Hadamard matrices, matrices where the entries of the matrices are complex numbers of absolute value one, [2, 4, 9], it is only recently that some attention has been given to unbiased Hadamard matrices subsequent to which interesting applications have emerged [7]. In this paper we concentrate only on unbiased Hadamard matrices.

2 Unbiased Hadamard matrices of order $4n^2$, *n* odd

We start this section with a characterization of Hadamard matrices.

Theorem 1 (Kharaghani 1985 [5]). *There is a Hadamard matrix H of order 2n if and only if there are 2n(-1,1)-matrices C*₀, C₁, C₂,..., C_{2n-1} *of order 2n such that:*

- 1. $C_i^t = C_i$,
- 2. $C_i C_j = 0, i \neq j,$
- 3. $C_i^2 = 2nC_i$,
- 4. $C_0 + C_1 + C_2 + \dots + C_{2n-1} = 2nI_{2n}$,
- 5. C_0 may be chosen to be the matrix of all ones.

Proof. Let r_i be the *i*-th row of H, and let $C_i = r_i^t r_i$, for i = 0, 1, ..., 2n - 1.

Theorem 2. Let $U = \{H_1, H_2, \dots, H_m\}$ be a set of mutually unbiased real (respectively complex) Hadamard matrices of order 2n. Then $m \le n$.

Proof. For $1 \le j \le m$, let $C_{1j}, C_{2j}, \ldots, C_{(2n)j}$, be the matrices corresponding to the Hadamard matrix H_j . Let $S_j = \{C_{ij} - I_{2n} \mid 1 \le i \le 2n - 1\}$. Then $\{S_j \mid 1 \le j \le 2n\}$ forms a set of linearly independent matrices. To see this, one needs to consider the matrices as a subset of all matrices of order 2n, say M_{2n} , equipped with the inner product defined by $\langle A, B \rangle = \text{trace}(AB^*)$, for A and B in M_{2n} . The span of all S_l 's is contained in the set of all symmetric (respectively Hermitian) matrices with zero diagonal. So $m(2n-1) \le (1+2+\dots+2n-1) = n(2n-1)$ (respectively $m(2n-1) \le 2(1+2+\dots+2n-1) = 2n(2n-1)$).

The upper bound in previous theorem is attained for Hadamard matrices of order 4^k , see [3].

Lemma 3. If H and K are two regularly unbiased Hadamard matrices of order $4n^2$, n odd, then at least one of the two matrices is not regular.

Proof. Suppose on the contrary both *H* and *K* are regular and $HK^t = 2nL$, where *L* is a Hadamard matrix. Then *L* is regular and (1/2)(J+H) and (1/2)(J-K) are integer valued matrices. However, $(1/4)(J+H)(J-K) = (1/4)(4n^2J - HK^t) = n^2J - (n/2)L$ is only integer valued if *n* is even.

Corollary 4. Let m be the number of regularly mutually unbiased Hadamard matrices of order $4n^2$, n odd, then $m \le 2$.

Theorem 5. There are two regularly unbiased Hadamard matrices of order 36, consequently the upper bound of the preceding Corollary is attained for n = 3.

Proof. A pair *H* and *K* of unbiased Hadamard matrices of order 36 are given in Tables 1 and 2. \Box

To search for the unbiased Hadamard matrices of order 36, we examined over 3,000,000 Hadamard matrices of order 36, looking for unbiased mates. Only a small percentage of matrices had unbiased mates. The interesting part was that most of those admitting unbiased mates had many mates and most of the mates were not included in the library of known Hadamard matrices of order 36.

Conjecture 6. Let *m* be the number of elements in a set of regularly mutually unbiased Hadamard matrices (RMUH) of order $4n^2$, *n* odd, then m = 2.

3 Unbiased Hadamard matrices of order $16n^2$

Definition 7. Two Latin squares L_1 and L_2 of size n on the symbol set $\{0, 1, 2, ..., n-1\}$ are called suitable if every superimposition of each row of L_1 on each row of L_2 results in only one element of the form (a, a).

Example 8. The following are three mutually suitable Latin squares of size 4:

(0 2 3)	1	$(0 \ 3 \ 1 \ 2$	()	1	$2 \ 3 \$
2 0 1	3	3 0 2 1		0	3 2
3 1 0	2 ,	1 2 0 3	, 2	3	0 1
$\begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$	0/	$\begin{pmatrix} 2 & 1 & 3 & 0 \end{pmatrix}$	$) / \langle 3$	2	1 0 /

Next we show that given a pair of mutually orthogonal Latin squares (see [1]), one can construct a pair of mutually suitable Latin square and vice versa.

Lemma 9. There are m MOLS (Mutually Orthogonal Latin Squares) of size n if and only if there are m MSLS (Mutually Suitable Latin Squares) of size n.

Proof. Let L_1, L_2 be two orthogonal Latin squares on $\{1, 2, \dots, n\}$ both having their row and columns labeled by the set. Let ((i, j), k) denote the entry at (i, j) position of a Latin square. Then the transformation $((i, j), k) \Longrightarrow ((k, j), i)$ results in a pair of suitable Latin squares. Reversing the transformation would imply the reverse implication.

Table 1: H, the first of a pair of unbiased Hadamard matrices of order 36

1111111111111111111------11111111111-----111111----11111-----111111-------111-----11-111-11-1-1-1111----11----1 1 - - - - 1 1 1 - 1 1 1 - 1 1 - 1 1 - 1 1 1 1 1 - - 1 - - - 1 1 - - - 111 - 11 - 1 - - 1 - - - 111 - 1 - 11 - - 11 - - 111 $---1\,1-1-1\,1-1\,1-1-1-1\,1\,1-1-1-1-1\,1\,1\\$ -111---1-11-11-11-11-11-11-11-1 ----1111111-1-1-1-----1-111-1-1 --1-11-1-1-1-1-11111-11--1-111---1111---1--111--1-11--1-11--1-11--1-11 -11-1--1111-1-1------11-1-1-111 --11-11-11111-----11-1111-----111 11-11--1-1-11---1-11-1-11 -111-1--1--11-11---11--11--111---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 - 11 - 1 1 - 1 - - - 1 1 - 1 - - - 1 1 - 1 - - 1 - 1 1 1 -

$$H =$$

Table 2: K, the second of a pair of unbiased Hadamard matrices of order 36

--11111111-111-1--111-11--1-11111-----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 - 1-11---111111111-11--1111---1-111---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 - - 11 - - 1 1 - - 1 - 1 1 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 1 1--11-1-11-11-1111111--11-11111----1-111-111--11---111-1111----1-111 -11-11-1--1-1-1-1111111-11-11--11-111 -1-11-1-1-1-1-1111111-1-11111-1-1-111 --111-1-11-1-1-1-1-1-1-1-1-11111111--11-11-111-111-1-111-111-111--111----1 - 1 1 1 - 1 1 - 1 1 1 - 1 - - - 1 1 1 1 1 1 1 1 - 1 1 - 1 - 1 - 1--11111-1---11----11111111111

Lemma 10. Let q be a prime power. Then there are q - 1 mutually suitable Latin squares of size q.

Definition 11. A Bush-type Hadamard matrix is a block matrix $H = [H_{ij}]$ of order $4n^2$ with block size 2n, $H_{ii} = J_{2n}$ and $H_{ij}J_{2n} = J_{2n}H_{ij} = 0$, $i \neq j$, $1 \le i \le 2n$, $1 \le j \le 2n$ where J_{2n} is the 2n by 2n matrix of all 1 entries.

Example 12. Let

$$H_4 = \left(\begin{array}{rrrrr} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{array}\right).$$

The matrices corresponding to this Hadamard matrix are:

The matrix

$$L = \begin{pmatrix} C_0 & C_1 & C_2 & C_3 \\ C_1 & C_0 & C_3 & C_2 \\ C_2 & C_3 & C_0 & C_1 \\ C_3 & C_2 & C_1 & C_0 \end{pmatrix}$$

is a Bush-type Hadamard matrix of order 16.

Theorem 13. If there are m mutually suitable Latin squares of size 2n, where 2n is the order of a Hadamard matrix, then there are m mutually unbiased Bush-type Hadamard matrices of order $4n^2$.

Proof. Let $C_0, C_1, \ldots, C_{2n-1}$, be the matrices corresponding to the normalized Hadamard matrix of order 2*n*. We can assume that all Latin squares are on the set $\{0, 1, \cdots, 2n-1\}$ and their row and columns are all labeled by the set. Replace the entry *i* in each of the Latin squares by the matrix C_i , $0 \le i \le 2n-1$ would result in *m* mutually unbiased Bush-type Hadamard matrices of order $4n^2$.

Example 14. Let

$$H_{1} = \begin{pmatrix} C_{0} & C_{2} & C_{3} & C_{1} \\ C_{2} & C_{0} & C_{1} & C_{3} \\ C_{3} & C_{1} & C_{0} & C_{2} \\ C_{1} & C_{3} & C_{2} & C_{0} \end{pmatrix}, \quad H_{2} = \begin{pmatrix} C_{0} & C_{3} & C_{1} & C_{2} \\ C_{3} & C_{0} & C_{2} & C_{1} \\ C_{1} & C_{2} & C_{0} & C_{3} \\ C_{2} & C_{1} & C_{3} & C_{0} \end{pmatrix}, \quad and$$

$$H_3 = \begin{pmatrix} C_0 & C_1 & C_2 & C_3 \\ C_1 & C_0 & C_3 & C_2 \\ C_2 & C_3 & C_0 & C_1 \\ C_3 & C_2 & C_1 & C_0 \end{pmatrix}$$

These are remarkable matrices. The three matrices are symmetric and

$$\left\{\frac{1}{4}H_1, \frac{1}{4}H_2, \frac{1}{4}H_3, I_{16}\right\}$$

forms a group under matrix multiplication. The blocks are not sign sensitive, i.e., one can change the block signs without changing the unbiasedness of the matrices.

Corollary 15. There are $4^n - 1$ mutually unbiased Bush-type Hadamard matrices of order 4^{2n} , *n* any positive integer.

Next we give a lower bound for the number of MUH matrices.

Theorem 16. Let *m* be the number of mutually suitable Latin squares of size 2n, where 2n is the order of a Hadamard matrix H, then there are m + 1 mutually unbiased Hadamard matrices of order $4n^2$.

Proof. Let r_i be the *i*-th row of H, and let K be the block matrix defined by $K = [k_{ij}] = [r_j^t r_i]$, $i, j = 0, 1, \dots, 2n - 1$. It is easy to see that K is a Hadamard matrix of order $4n^2$ which is unbiased with all the Bush-type Hadamard matrices constructed in Theorem 13.

The lower bound in Theorem 16 has appeared in a number of papers, see for example [2, 7]. Next we show that our method above extends to weighing matrices.

Definition 17. A matrix $W = [w_{ij}]$ of order n and $w_{ij} \in \{-1, 0, 1\}$ is called a weighing matrix with weight p, if $WW^t = pI_n$, where I_n is the identity matrix of order n, see [8]. Two weighing matrices W_1, W_2 of order n and weight p are called unbiased, if $W_1W_2^t = \sqrt{p}W$, where W is a weighing matrix of order n and weight p.

Theorem 18. Let *m* be the number of mutually suitable Latin squares of size *n*, where *n* is the order of a weighing matrix W with weight *p*, then there are m + 1 mutually unbiased weighing matrices of order n^2 with weight p^2 .

Proof. The construction and the proof of Theorem 16 works here too.

Example 19. Let

$$W = \left(\begin{array}{rrrrr} 0 & 1 & 1 & 1 \\ - & 0 & 1 & - \\ - & - & 0 & 1 \\ - & 1 & - & 0 \end{array}\right).$$

The matrices corresponding to this weighing matrix are:

$$C_{0} = r_{0}^{t} r_{0} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \quad C_{1} = r_{1}^{t} r_{1} = \begin{pmatrix} 1 & 0 & - & 1 \\ 0 & 0 & 0 & 0 \\ - & 0 & 1 & - \\ 1 & 0 & - & 1 \end{pmatrix},$$
$$C_{2} = r_{2}^{t} r_{2} = \begin{pmatrix} 1 & 1 & 0 & - \\ 1 & 1 & 0 & - \\ 0 & 0 & 0 & 0 \\ - & - & 0 & 1 \end{pmatrix}, \quad C_{3} = r_{3}^{t} r_{3} = \begin{pmatrix} 1 & - & 1 & 0 \\ - & 1 & - & 0 \\ 1 & - & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Substituting these in the matrices of Example 8 gives

and

$$W_{3} = \begin{pmatrix} 0 0 0 0 1 0 - 1 1 1 0 - 1 - 1 0 \\ 0 1 1 1 0 0 0 0 1 1 0 - - 1 - 0 \\ 0 1 1 1 - 0 1 - 0 0 0 0 1 - 1 0 \\ 0 1 1 1 1 0 - 1 - - 0 1 0 0 0 0 \\ 1 0 - 1 0 0 0 0 1 - 1 0 1 1 0 - \\ 0 0 0 0 0 1 1 1 - 1 - 0 1 1 0 - \\ - 0 1 - 0 1 1 1 1 - 1 - 0 0 0 0 0 \\ 1 0 - 1 0 1 1 1 0 0 0 0 - - 0 1 \\ 1 1 0 - 1 - 1 0 0 0 0 0 1 0 - 1 \\ 1 1 0 - 1 - 1 0 0 1 1 1 0 0 0 0 \\ 0 0 0 0 1 - 1 0 0 1 1 1 0 0 0 0 \\ 0 0 0 0 1 - 1 0 0 1 1 1 - 0 1 - \\ - - 0 1 0 0 0 0 0 0 1 1 1 1 0 - 1 \\ 1 - 1 0 1 1 0 - 1 0 - 1 0 0 0 0 \\ - 1 - 0 1 1 0 - 0 0 0 0 0 1 1 1 \\ 1 - 1 0 0 0 0 - 0 1 - 0 1 1 1 \end{pmatrix}$$

A construction akin of the one used in the proof of Theorem 16 applied to W gives:

$$K = \begin{pmatrix} 0 0 0 0 0 - - - 0 - - - 0 - - - 0 \\ 0 1 1 1 0 0 0 0 0 - - - 0 1 1 1 \\ 0 1 1 1 0 1 1 1 0 0 0 0 0 - - - \\ 0 1 1 1 0 - - - 0 1 1 1 0 0 0 0 \\ 0 0 0 0 1 0 - 1 1 0 - 1 1 0 - 1 \\ - 0 1 - 0 0 0 0 0 1 0 - 1 - 0 1 - \\ - 0 1 - - 0 1 - 0 0 0 0 0 1 0 - 1 \\ - 0 1 - 1 0 - 1 - 0 1 - 0 0 0 0 \\ 0 0 0 0 1 1 0 - 1 1 0 - 1 1 0 - \\ - - 0 1 0 0 0 0 1 1 0 - - 0 1 \\ - - 0 1 - 0 1 0 0 0 0 1 1 0 - - 0 1 \\ - - 0 1 1 1 0 - - - 0 1 0 0 0 0 \\ 0 0 0 0 1 - 1 0 1 - 1 0 1 - 1 0 \\ - 1 - 0 0 0 0 0 1 - 1 0 - 1 - 0 \\ - 1 - 0 1 - 0 0 0 0 0 1 - 1 0 \\ - 1 - 0 1 - 0 0 0 0 0 0 - 0 \\ \end{pmatrix}$$

Then W₁, W₂, W₃ and K are mutually unbiased weighing matrices of order 16 and weight 9.

Remark 20. (a) The most interesting application of Theorem 18 is that it can be applied to weighing matrices of odd order. For example, it is known that a weighing matrix of order 13 and weight 9 exists. Theorem 18 applies and 13 unbiased weighing matrices of order 169 and weight 81 can be constructed.

(b) Theorem 18 is an extension of Theorem 16 in one direction. We could have obtained Theorem 16 as a corollary to Theorem 18, but we chose not to, due to the fact that there is much interest in unbiased Hadamard matrices. However, there is an obvious advantage in our method, since

it works for all matrices enjoying an orthogonality property.

(c) Another way to extend Theorem 16 is to apply it to partial Hadamard matrices. These are $m \times n$, $m \le n$, matrices with orthogonal rows. The method used in this paper extends to these matrices.

References

- R. Julian R. Abel, Charles Colbourn, Jeffrey Dinitz, Mutually Orthogonal Latin Squares (MOLS), in *Handbook of Combinatorial Designs* (C. J. Colbourn and J. H. Dinitz, eds.), Second Edition, pp. 160–193, Chapman & Hall/CRC Press, Boca Raton, FL, 2007.
- [2] P. O. Boykin, M. Sitharam, M. Tarifi and P. Wocjan, Real mutually unbiased bases. Preprint. arXiv:quant-ph/0502024v2 [math.CO], (revised version dated Feb. 1, 2008).
- [3] P. J. Cameron and J. J. Seidel, Quadratic forms over GF(2), *Nederl. Akad. Wetensch. Proc. Ser. A 76=Indag. Math* **35** (1973), 1–8.
- [4] Chris Godsil, Aidan Roy, Equiangular lines, mutually unbiased bases, and spin models *European J. Combin.*, **30** (2009), 246–262.
- [5] H. Kharaghani, New class of weighing matrices, Ars Combin. 19 (1985), 69–72.
- [6] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, J. Combin. Designs 13 (2005), 435–440.
- [7] Nicholas LeCompte, William J. Martin, William Owens, On the equivalence between real mutually unbiased bases and a certain class of association schemes, preprint.
- [8] J. Seberry and M. Yamada, *Hadamard matrices, sequences, and block designs*, in Contemporary Design Theory: A Collection of Surveys, J. H. Dinitz and D. R. Stinson, eds., John Wiley Sons, Inc., 1992, pp. 431–560.
- [9] P. Wocjan and T. Beth, New construction of mutually unbiased bases in square dimensions, *Quantum Inf. Comput.* **5** (2005), 93–101.