A New Family of Amicable Hadamard Matrices

Jennifer Seberry

Centre for Computer and Information Security Research, SCSSE,
University of Wollongong, NSW 2522, Australia
Email: [j.seberry]@uow.edu.au

May 12, 2012

In Memory of Professor J D Srivastava

Abstract

We study constructions for amicable Hadamard matrices. The family for orders 2^t, t a positive integer is explicitly exhibited. We also show that there are amicable Hadamard matrices of order $(2^t-1)^r+1$ for any odd integer $r>1$. Now we have orders 15^r+1, 63^r+1, 255^r+1, 511^r+1, ... $r>1$ an odd integer, for the first time.

Key words: Hadamard matrices, amicable Hadamard matrices, amicable Hadamard cores
MSC: Primary 05B20,

1 Introduction

The papers by Tarokh, Jafarkhani and Calderbank [22], and Belevitch [2, 3], showing possible connections between amicable Hadamard matrices and communications has motivated their further study. A delightful introduction to this topic has been written by Adams [1].

An *Hadamard matrix*, H, of order n is a square ±1 matrix whose rows (and columns) are pairwise orthogonal, that is $HH^T = nI_n$. Hadamard matrices of order n are conjectured to exist for all orders $n \equiv 0 (\mathrm{mod}\ 4)$. A weighing matrix, $W = W(n,k)$, of order n and weight k has elements 0, ±1 and satisfies $WW^T = kI_n$. If an Hadamard matrix M, can be written in the form $M = I + S$ where $S^T = -S$, then M is said to be a *skew-Hadamard matrix.* Skew Hadamard matrices are also conjectured to exist for all orders $n \equiv 0 (\mathrm{mod}\ 4)$.

If $M = I + S$ is a skew Hadamard matrix, of order n, $N = N^T$, is an Hadamard matrix also of order n and $MN^T = NM^T$, then M and N will be said to be *amicable Hadamard matrices.* If $MN^T = -NM^T$, then M and N will be said to be special or anti-amicable Hadamard matrices [25, p296]. Seberry and Yamada [20, p535] give amicable and skew Hadamard matrices which were known in 1992. Since then new skew-Hadamard matrices have been found for a few orders by extensive computer searches [4, 5, 6, 7].

However, compared with the knowledge regarding the existence of Hadamard matrices very little is known regarding the existence of amicable and skew-Hadamard matrices.

2 Some Basic Results

Most of the results of this section are not new but we group them together here for future reference. We refer the interested reader to Geramita and Seberry [10] for information about orthogonal designs and amicable orthogonal designs.

Definition 1 [Amicable Matrices] Two square matrices of order n, A and B, are said to be *amicable* if $AB^T = BA^T$.

Notation 1 [Back Diagonal Matrix] We use

$$R = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & & & & \vdots \\ 0 & 1 & & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

for the *back-diagonal matrix of order* n and and also for type 2 back-diagonal matrix.

Remark 1 Let A and B be circulant matrices of order n. Then $C = BR$ is symmetric and $AC^T = CA^T$ so A and C are amicable. If A and B are type 1 matrices (see [25]), and $C = BR$ where R is the type 2 back diagonal matrix then A and C will be amicable (see [10, 4.13] for the definition of type 2).

Proposition 1 *The following are equivalent for orders $n \equiv 0 (\text{mod } 4)$:*

1. *a $W(n, n-1)$;*
2. *a skew-Hadamard matrix of order n;*
3. *an $OD(n; 1, n-1)$.*

Proposition 2 *The following are equivalent for orders $n \equiv 0 (\text{mod } 4)$:*

1. *amicable Hadamard matrices of order n; and*
2. *$AOD(n : 1, n-1; n)$.*

Proof. See [10, Lemma 5.43] for the proof.

3 Amicable Cores

To make our next result clear we first define what we mean by different types of cores.

Definition 2 [Amicable Hadamard Cores] Let $A = I + S$ and B be amicable Hadamard matrices of order n which can be written in the form

$$A = \begin{bmatrix} 1 & e \\ -e^T & I + W \end{bmatrix}$$

and

$$B = \begin{bmatrix} -1 & e \\ e^T & R + V \end{bmatrix},$$

where e is a $1 \times n - 1$ vector of all $+1$s. Let R be the back-diagonal matrix, W and V have row sum $+1$ and

$$V^T = V, \; VW^T = WV, \text{ and } RW^T = WR. \tag{1}$$

Then $I + W$ and $R + V$ will be said to be *amicable cores* of amicable Hadamard matrices. We call W and V *amicable Hadamard cores* when the properties of Equation 1 are satisfied. We call W the skew-symmetric core and V the symmetric (partner) core.

Now $C = I + W$ or $C = R + V$ are said to be *amicable cores* of the Hadamard matrix, and

$$CC^T = nI_{n-1} - J_{n-1}, \; CJ = JC = J.$$

Example 1 Amicable Hadamard Matrices and Their Cores
The following two Hadamard matrices are amicable Hadamard matrices.

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \end{bmatrix}$$

with the following two matrices

$$I + W = \begin{bmatrix} 1 & 1 & -1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{bmatrix} \quad \text{and} \quad R + V = \begin{bmatrix} -1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{bmatrix}$$

as amicable cores of the amicable Hadamard matrices. Note they satisfy all the properties of Equation 1.

The following theorem is quoted from Geramita and Seberry [10, Theorem 5.52]

Theorem 1 *Let* $p \equiv 3 \pmod 4$ *be a prime power. Then there exist amicable Hadamard matrices of order* $p + 1$.

Example 2 [Amicable Paley Cores]First we note that Paley cores apply to prime power orders only.

To illustrate we use Paley's original construction [19, 25] to form a skew-symmetric matrix, Q, with zero diagonal and other entries ± 1 satisfying $QJ = 0$, $QQ^T = pI - J$, $Q^T = -Q$. This matrix Q is called the *Paley core.*

We now Write W for Q to be consistent with the remainder of this paper. Let R be the back-diagonal matrix of order p, when p is prime, and the type 2 (see [25] for definitions) equivalent when p is a prime power. Write $V = QR$. Then W and V are amicable Hadamard cores. We also (loosely) call them *amicable Paley cores.* From Remark 1 V is symmetric.

Writing W and V for the amicable Paley cores we see that we can write the amicable Hadamard matrices as

$$M_{p+1} = \begin{bmatrix} 1 & e \\ -e^T & I + W \end{bmatrix}$$

and

$$N_{p+1} = \begin{bmatrix} -1 & e \\ e^T & R + V \end{bmatrix}.$$

where e is a $1 \times p$ vector of all $+1$s. □

$I + W$ and $R + V$ are amicable Hadamard cores of amicable Hadamard matrices. W and V are amicable Hadamard cores.

4 Construction for Amicable Hadamard Matrices of order 2^t

Seberry and Yamada [20, p535] give amicable Hadamard matrices which were known in 1992.

Unfortunately the very first family of amicable Hadamard designs (and indeed amicable orthogonal designs) which were foreshadowed in Geramita, Pullman and Seberry Wallis [9], has never been explicitly cited. We give a more general theorem which has this family as a corollary.

Theorem 2 [Multiplication Theorem for Amicable Hadamard Matrices] *If there are amicable Hadamard matrices of order n_1 and n_2 there are amicable Hadamard matrices of order $n_1 n_2$.*

Proof. See [10, Theorem 5.77].

Corollary 1 *Let t be a positive integer. Then there exist $AOD(2^t; 1, 2^t - 1; 2^t)$ or amicable Hadamard matrices for every 2^t.*

Proof. We write this proof in some detail to ensure we have the symmetric and skew-symmetric cores for Theorem 3. We note the amicable Hadamard matrices of order 2:

$$M_2 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \quad \text{and} \quad N_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Applying Theorem 2 once gives us the 4×4 matrices

$$M_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix} \quad \text{and} \quad N_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Here all the properties of Equations 1 hold except $RJ = -J$.

We note that M_4 is Hadamard of skew-type, a skew Hadamard matrix and N_4 is symmetric. This example is not yet in the form we need for Theorem 3 but multiplying column 1 and then rows 2 to 4 of N_4, to give N_4', which does not alter the symmetry of amicable Hadamard property of M_4 and N_4' gives the desired form.

Then iterative use of Theorem 2 gives Hadamard matrices of order $q = 2^t$ where M_{2^t} is skew-type and $N_{2^t} = (n_{ij})$ is symmetric and the elements

$$(2, 2^t), \ (3, 2^t - 1), \ \cdots, (2^t, 2)$$

of N_{2^t} are all -1. This is R for N_{2^t}. That is, using induction, we can write the amicable Hadamard matrices $M_{2^t} = I + S$ and N_{2^t} as

$$M_{2^t} = \begin{bmatrix} 1 & e \\ -e^T & I + W \end{bmatrix}$$

and

$$N_{2^t}' = \begin{bmatrix} -1 & e \\ e^T & R + V \end{bmatrix},$$

where e is a $1 \times 2^t - 1$ vector of all $+1$s and W and V are amicable Hadamard cores. R is the back diagonal matrix of order $2^t - 1$.

We note M_{2^t} and N_{2^t}' satisfy all the properties of Equations 1. □

5 Construction of Amicable Hadamard Matrices using Cores

In early papers Belevitch [2, 3] and Goldberg [14] showed that the core of a skew-Hadamard matrix, of order $n+1$, could be used to generate a core of a skew-Hadamard matrix of order $n^3 + 1$. Seberry Wallis [24] realized that this construction could be extended to orders n^5+1 and n^7+1. These were further generalized by Turyn [23] to orders $n^r + 1$, where $r > 0$ is an odd integer. We now give the results in considerable detail to try to make the constructions as clear as possible.

Theorem 3 [Belevitch - Goldberg Theorem] *Suppose W is a skew-symmetric core of size $n \equiv 3 \pmod 4$ then*

$$I \times J \times W + W \times I \times J + J \times W \times I + W \times W \times W$$

is a core of order n^3.

Remark 2 If $I + W$ and $R + V$ are amicable Hadamard cores then the symmetric companion of the above skew-symmetric core is

$$R \times J \times V + V \times R \times J + J \times V \times R + V \times V \times V$$

We now use part of Corollary 3.12 of [25] which shows that is W is a skew-symmetric (symmetric) core of size $n \equiv 3 \pmod 4$ then there exists a skew-symmetric (symmetric) of size n^r for all odd $r > 1$.

Example 3 The skew-symmetric core of order n^5 from a skew-symmetric core of order n is the sum of

$$I \times J \times I \times J \times W; \text{ and } I \times J \times W \times W \times W;$$

plus

$$W \times W \times W \times W \times W,$$

plus their circulants

$$W \times I \times J \times I \times J; \; W \times I \times J \times W \times W;$$

$$J \times W \times I \times J \times I; \; W \times W \times I \times J \times W;$$

$$I \times J \times W \times I \times J; \; W \times W \times W \times I \times J;$$

$$J \times I \times J \times W \times I; \; J \times W \times W \times W \times I.$$

The symmetric core will have the same form with I replaced by R and W replaced by V. So it becomes the sum of

$$R \times J \times R \times J \times V; \text{ and } R \times J \times V \times V \times V; V \times V \times V \times V \times V,$$

plus their circulants

$$V \times R \times J \times R \times J; \; V \times R \times J \times V \times V; J \times V \times R \times J \times R; \; V \times V \times R \times J \times V;$$

$$R \times J \times V \times R \times J; \; V \times V \times V \times R \times J; J \times R \times J \times V \times R; \; J \times V \times V \times V \times R.$$

These amicable cores, that is the skew-symmetric and the symmetric cores, are amicable term by term.

□

We now use this to construct amicable Hadamard matrices of order $n^r + 1$ from amicable Hadamard matrix cores of order $n + 1$. This is illustrated by the Belevitch-Goldberg construction Theorem 3 for $n = 3$ and by Example 3 for $n = 5$.

Theorem 4 [Construction] *Suppose W is a skew-symmetric core of size $n \equiv 3 \pmod 4$ and V $(V^T = V)$ is an amicable symmetric core. Let $\mathcal{M}$ and $\mathcal{N}$ given by*

$$I \times I \times I \cdots \times I + B_r$$

and

$$R \times R \times R \cdots \times R + D_r$$

where each single term is comprised of the sum of the Kronecker product of n terms as described below. Then $\mathcal{M}$ and $\mathcal{N}$ are cores of amicable Hadamard matrices of order n^r for any odd $r > 0$.

Proof. Let I, J, W of order n be as above. The proof consists of taking the sum of the Kronecker product of all the possible basic terms A of the form $I \times J \times W \times \cdots \times W$, $I \times J \times I \times J \times W \times \cdots \times W$, $I \times J \times W \times I \times J \times \cdots \times W$ and so on and all their circulants. That is, if a new term is introduced to make a larger power, the newly introduced terms will have $I \times J$ or $W \times W$ inserted at the beginning of each term of the smaller order A_{r-2}. Call this matrix $B = B_r$. Then B will satisfy $BB^T = n^r I_{n^r} - J_{n^r}$, $BJ = JB = 0$.

Because $WJ = JW = 0$ it becomes easy to see that the terms of BB^T are actually each individual term of A each multiplied by its transpose.

It is a little more difficult to see that B will be a skew-symmetric core, that is that all the off diagonal elements are ± 1. However this can be shown from the careful placements of the elements and that J and W (and J and V) occur in the same position in each distinct pair of terms for the higher power construction (note $JW = WJ = 0$) and each pair of terms is disjoint.

Carrying out the same procedure but with A_r and B_r, with elements I, J and W replaced by C_r and D_r which have elements R, J and V gives the symmetric partner. □

Corollary 2 *Suppose there exist amicable Hadamard matrices of order n with amicable cores of order $n-1$. Then there exist amicable Hadamard matrices of order $(n-1)^r + 1$, for all odd $r \geq 1$.*

From Seberry and Yamada [20, p535], Geramita, Pullman and Seberry Wallis [9] and this paper, amicable Hadamard matrices exist for the following orders, x_0, x_3 and x_4 are given explicitly here for the first time.

Key	Order	Method
x_0	2^t	t a non $-$ negative integer. See [10, p224].
x_1	$p^r + 1$	$p^r \equiv 3 \pmod 4$ is a prime power. See [20, p110].
x_2	$2(q+1)$	$2q+1$ is a prime power, $q \equiv 1 \pmod 4$ is a prime. See [20, p114].
x_3	$(4t-1)^r + 1$	when circulant (or type 1) Hadamard cores of order $4t-1$ exist.
x_4	nh	$n, h,$ are orders of amicable Hadamard matrices. See [10, p255].

Seberry and Yamada [20, p541-542] give a list of constructions for skew-Hadamard matrices known in 1992. There are very few further constructions known (see [4, 5, 6, 7]).

Since amicable Hadamard matrices exist for 15+1, 63 +1, 255 +1, 511 +1, ... we have amicable Hadamard matrices for the new orders 15^r+1, 63^r+1, 255^r+1, 511^r+1, ... $r>1$ an odd integer, for the first time.

Further research is needed to extend our knowledge of amicable Hadamard matrices.

References

[1] Sarah Spence Adams, A journey of discovery: orthogonal matrices and communications, *AMS Contemporary Mathematics Series* 479, (2009), 1-9.

[2] V. Belevitch, Conference networks and Hadamard matrices, *Ann. Soc. Scientifique Brux.* T82, (1968), 13-32.

[3] V. Belevitch, Theory of $2n$-terminal networks with applications to conference telephony, *Electr. Commun.*, 27, 3 (1950), 231-244.

[4] Dragomir Djokovic, Skew Hadamard matrices of order 4×37 and 4×43. *J. Combin. Theory Ser. A*, 61 (1992), no. 2, 319-321.

[5] Dragomir Djokovic, Skew-Hadamard matrices of orders 188 and 388 exist. *Int. Math. Forum*, 3 (2008), no. 21-24, 1063-1068.

[6] Dragomir Djokovic, Skew-Hadamard matrices of orders 436, 580, and 988 exist. *J. Combin. Des.* 16 (2008), no. 6, 493-498.

[7] Roderick J Fletcher, Christos Koukouvinos, and Jennifer Seberry, New skew-Hadamard matrices of order $4\cdot 59$ and new D-optimal designs of order $2\cdot 59$. *Discrete Math.*, 286 (2004), no. 3, 251-253.

[8] P. Delsarte, J. M. Goethals and J. J. Seidel, Orthogonal matrices with zero diagonal, *Canad, J, Math.*, 23 (1971), 816-832.

[9] Anthony V. Geramita, Norman J Pullman and Jennifer Seberry Wallis, Families of weighing matrices, *Bull. Aust. Math. Soc.*, 10 (1974), 119-122.

[10] Anthony V. Geramita and Jennifer Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices,* Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, Inc., New York and Basel, 1979.

[11] Anthony V. Geramita and J. H. Verner, Orthogonal designs with zero diagonal, *Canad. J. Math.*, 28 (1976), 215-225.

[12] J. M. Goethals and J. J. Seidel, Orthogonal matrices with zero diagonal, *Canad, J, Math.*, 19 (1967), 1001-1010.

[13] J. M. Goethals and J. J. Seidel, A skew-Hadamard matrix of order 36, *J. Austral. Math. Soc.* 11 (1970), 343-344.

[14] K. Goldberg, Hadamard matrices of order cube plus one, *Proc. Amer. Math, Soc.* 17, (1966) 744-746.

[15] M. Hall, Jr., *Combinatorial Theory*, 2nd ed., John Wiley & Sons, New York, 1986.

[16] H. Kharaghani, New classes of orthogonal designs, *Ars Combin.*, 29, (1990), 187-192.

[17] I. S. Kotsireas and C Koukouvinos, New skew-Hadamard matrices via computational algebra. *Australas. J. Combin.* 41 (2008), 235.248,

[18] A C Mukopadhyay, Some infinite classes of Hadamard matrices, *J Combin. Theory, Ser A.*, 25, no 2, (1978), 128-141.

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

[20] Jennifer Seberry and Mieko Yamada, Hadamard matrices, sequences, and block designs, *Contemporary Design Theory: A Collection of Surveys*, J. H. Dinitz and D. R. Stinson, eds., John Wiley and Sons, Inc., 431-560, 1992.

[21] Jennifer Seberry and R. Craigen, Orthogonal designs, *Chapter in CRC Handbook of Combinatorial Designs*, Editors Charles J. Colbourn and Jeffrey H. Dinitz, CRC Press, 1996, 400-406.

[22] V. Tarokh, H. Jafarkhani and A.R. Calderbank, Space-time codes from orthogonal designs, *IEEE Trans. Inform. Theory*, 45, (1999), 1456-1467.

[23] R. J. Turyn, C-matrices of arbitrary powers, *Bull. Canad. Math. Soc.*, 23, (1971), 531-535.

[24] Jennifer Seberry Wallis, *Combinatorial Matrices*, Ph.D. Thesis, La Trobe University, 1971.

[25] Jennifer Seberry Wallis, Hadamard matrices, in W. D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, *Combinatorics: Room Squares, Sum-Free Sets and Hadamard Matrices,* Lecture Notes in Mathematics, Springer Verlag, Berlin, 1972.