AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **69(3)** (2017), Pages 349–357

Two infinite families of symmetric Hadamard matrices

Jennifer Seberry

Centre for Computer Security Research
School of Computing and Information Technology, EIS
University of Wollongong, NSW 2522
Australia
jennifer_seberry@uow.edu.au

N. A. Balonin

Saint Petersburg State University of Aerospace Instrumentation
67, B. Morskaia St.
190000, St. Petersburg
Russian Federation
korbendfs@mail.ru

Dedicated to the unforgettable Mirka Miller

Abstract

A construction method for orthogonal ±1 matrices based on a variation of the Williamson array, first described by N. A. Balonin, on his web page mathscinet.ru/catalogue/propus/ where he called it the *propus array*, gives symmetric propus-Hadamard matrices using

$$\begin{matrix} A & B & B & D \\ B & D & -A & -B \\ B & -A & -D & B \\ D & -B & B & -A \end{matrix}$$

We show that: for $q \equiv 1 \pmod 4$, a prime power, symmetric propus-Hadamard matrices exist for order $2(q+1)$; and for $q \equiv 1 \pmod 4$, a prime power, and $\frac{1}{2}(q+1)$ a prime power or the order of the core of a symmetric conference matrix (this happens for $q = 89$), symmetric propus-type Hadamard matrices of order $4(2q+1)$ exist.

We give constructions to find symmetric propus-Hadamard matrices for 57 orders $4n$, $n < 200$ odd.

1 Introduction

Hadamard matrices arise in statistics, signal processing, masking, compression, combinatorics, weaving, spectroscopy and other areas. They been studied extensively. Hadamard showed [7] the order of an Hadamard matrix must be 1, 2 or a multiple of 4. Many constructions for ±1 matrices and similar matrices such as Hadamard matrices, weighing matrices, conference matrices and D-optimal designs use skew and symmetric Hadamard matrices in their construction. For more details see Seberry and Yamada [12].

An Hadamard matrix of order n is an $n \times n$ matrix with elements ±1 such that $HH^\top = H^\top H = nI_n$, where I_n is the $n \times n$ identity matrix and $\top$ stands for transposition. A skew Hadamard matrix $H = I + S$ has $S^\top = -S$. For more details see the books and surveys of Jennifer Seberry (Wallis) and others [12, 16] cited in the bibliography.

Theorems of the type *for every odd integer n there exists a t_0 dependent on n so that Hadamard, regular Hadamard, co-cyclic Hadamard and some full orthogonal designs exist for all orders $2^t n$, $t > t_0$, t integer* are known [3, 4, 9, 13]. A similar result for symmetric Hadamard and skew-Hadamard matrices is conjectured.

Suppose $n \equiv 3 \pmod 4$ and X and Y are amicable ±1 matrices of order n, that is $XY^\top = YX^\top$ which satisfy $XX^\top + YY^\top = (2n-2)I + 2J$ then D-optimal designs use

$$\begin{bmatrix} X & Y \\ Y^\top & -X^\top \end{bmatrix}$$

to form matrices with maximal determinant.

The propus construction was first introduced by the authors in an ArXiv paper of the same name but has not appeared in any other paper. It uses four orthogonal ±1 matrices, A, B, C, and D, where $C = B$ of order n, where

$$AA^\top + 2BB^\top + DD^\top = 4nI,$$

I the identity matrix, called *propus matrices*, based on the array

$$\begin{matrix} A & B & B & D \\ B & D & -A & -B \\ B & -A & -D & B \\ D & -B & B & -A \end{matrix}$$

to construct symmetric Hadamard matrices.

We give methods to find propus-Hadamard matrices: using Williamson matrices and D-optimal designs. These are then generalized to allow non-circulant symmetric matrices with the same aim to give symmetric Hadamard matrices.

We show that for

- $q \equiv 1 \pmod 4$, a prime power, the required matrices exist for order $t = \frac{1}{2}(q+1)$, and thus symmetric Hadamard matrices of order $2(q+1)$;

- $q \equiv 1 \pmod 4$, a prime power, and $\frac{1}{2}(q+1)$ a prime power or the order of the core of a symmetric conference matrix (this happens for $q = 89$) the required symmetric propus-type Hadamard matrices of order $4(2q+1)$ exist;

- $t \equiv 3 \pmod 4$, a prime, such that D-optimal designs, constructed using two circulant matrices, one of which must be circulant and symmetric, exist of order $2t$, then such symmetric Hadamard matrices exist for order $4t$.

We note that appropriate *Williamson type* matrices may also be used to give propus-Hadamard matrices but do not pursue this avenue in this paper. There is also the possibility that this propus construction may lead to some insight into the existence or non-existence of symmetric conference matrices for some orders. We refer the interested reader to [1].

1.1 Definitions and Basics

Two matrices X and Y of order n are said to be *amicable* if $XY^\top = YX^\top$.

We define the following classes of propus like matrices. We note that there are slight variations in the matrices which allow variant arrays and non-circulant matrices to be used to give symmetric Hadamard matrices, All propus like matrices A, B, C, D where $B = C$ are (± 1) matrices of order n satisfy the *additive property*

$$AA^\top + 2BB^\top + DD^\top = 4nI_n, \tag{1}$$

I the identity matrix, J the matrix of all ones. We recall that Williamson matrices are defined to be circulant and symmetric, however Williamson-type matrices are defined to be amicable.

We consider the following kinds of ± 1 of order n which give symmetric Hadamard matrices:

- *propus matrices*: four circulant symmetric ± 1 matrices, A, B, $C = B$, D of order n, satisfying the additive property (use P) (this uses Williamson matrices);

- *propus-type matrices*: four pairwise amicable ± 1 matrices, A, B, $C = B$, D of order n, $A^\top = A$, satisfying the additive property (use P) (this includes Williamson-type matrices);

- *generalized-propus matrices*: four pairwise commutative ± 1 matrices, A, B, $C = B$, D of order n, $A^\top = A$, which satisfy the additive property (use GP) (this uses circulant and/or type 1 matrices which are appropriate).

We use two types of arrays into which to plug the propus like matrices: the propus array, P (see below), or the generalized-propus array, GP (see below). These can also be used with generalized matrices ([15]). R is the back-diagonal matrix.

$$P = \begin{bmatrix} A & B & B & D \\ B & D & -A & -B \\ B & -A & -D & B \\ D & -B & B & -A \end{bmatrix} \quad \text{and} \quad GP = \begin{bmatrix} A & BR & BR & DR \\ BR & D^\top R & -A & -B^\top R \\ BR & -A & -D^\top R & B^\top R \\ DR & -B^\top R & B^\top R & -A. \end{bmatrix}.$$

2 Symmetric Propus-Hadamard Matrices

We first give the explicit statements of two well known theorem, Paley's Theorem [11], for the Legendre core Q, and Turyn's Theorem [14], in the form in which we will use them.

Theorem 1. [**Paley's Legendre Core** [11]] *Let $p \neq 2$ be a prime power, then there exists a matrix, Q, of order p with zero diagonal and other elements ± 1 satisfying $QQ^\top = (q+1)I - J$, Q is symmetric or skew-symmetric according as $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.*

Theorem 2. [**Turyn's Theorem** [14]] *Let $q \equiv 1 \pmod 4$ be a prime power then there are two symmetric matrices, P and S of order $\frac{1}{2}(q+1)$, satisfying $PP^\top + SS^\top = qI$ such that P has zero diagonal and other elements ± 1 and S elements ± 1.*

2.1 Propus-Hadamard Matrices from Williamson Matrices

Lemma 1. *Let $q \equiv 1 \pmod 4$, be a prime power, then propus matrices exist for orders $n = \frac{1}{2}(q+1)$ which give symmetric propus-Hadamard matrices of order $2(q+1)$.*

Proof. We note that for $q \equiv 1 \pmod 4$, a prime power, Turyn (Theorem 2 [14]) gave Williamson matrices, $X + I$, $X - I$, Y, Y, which are circulant and symmetric for orders $n = \frac{1}{2}(q+1)$. Then choosing

$$A = X + I, \; B = C = Y, \; D = X - I$$

gives the required propus-Hadamard matrices. □

We now have propus-Hadamard matrices for orders $4n$ where n is in

$$\{1, 3, [5], 7, 9, [13], 15, 19, 21, [25], 27, 31, 37, [41], 45, 49, 51, 55, 57, 59,$$
$$[61], [63], 67, 69, 75, 79, 81, [85], 87, 89, 91, 97, 99, 105, 111, 115, 117, 119, 121,$$
$$127, 129, 135, 139, 141, [145], 147, 157, 159, 169, 175, 177, [181], 187, 195, 199.\}$$

Some cases written in square brackets arise when q is a prime power; howeveri, the combined results of Delsarte, Goethals, Seidel and Turyn means the required circulant matrices also exist for these prime powers.

2.1.1 Propus matrices of small order and from q prime power

There are two easily obtained propus-Hadamard matrices of orders 12 and 20 based on $A = J$, $B = C = D = J - 2I$, for $n = 3$, and $A = Q + I$, $B = C = J - 2I$, $D = Q - I$ (Q constructed using Legendre symbols) for $n = 5$.

2.2 Propus-Hadamard matrices from D-optimal designs

Lemma 2. *Let $n \equiv 3 \pmod 4$ be a prime, such that D-optimal designs, constructed using two circulant matrices, $X^\top = X$ and Y, exist for order $2n$. Then propus-Hadamard matrices exist for order $4n$.*

Proof. We choose $A = X$, $B = C = (Q+I)$ and $D = Y$ in the GP array (Q constructed using Legendre symbols). □

Djoković and Kotsireas in [8, 6] give D-optimal designs, constructed using two circulant matrices, for $n \in \{3, 5, 7, 9, 13, 15, 19, 21, 23, 25, 27, 31, 33, 37, 41, 43, 45, 49, 51, 55, 57, 59, 61, 63, 69, 73, 75, 77, 79, 85, 87, 91, 93, 97, 103, 113, 121, 131, 133, 145, 157, 181, 183\}$, $n < 200$. We are interested in those cases where the D-optimal design is constructed from two circulant matrices one of which must be symmetric.

Suppose D-optimal designs for orders $n \equiv 3 \pmod 4$, a prime, are constructed using two circulant matrices, X and Y. Suppose X is symmetric. Let $Q + I$ be the Paley matrix of order n. Then choosing

$$A = X, \quad B = C = Q + I, \quad D = Y,$$

to put in the array GP gives the required propus-Hadamard matrices.

Hence, as one of the constiutents of the D-optimal design is known to be symmetric for orders n in $\{3, 7, 19, 31\}$, we have propus-Hadamard matrices, constructed using D-optimal designs, for orders $4n$. The results for $n = 19$ and 31 were given to us by Dragomir Djokovič.

2.3 A Variation of a Theorem of Miyamoto

In Seberry and Yamada [12] one of Miyamoto's results [10] was reformulated so that symmetric Williamson-type matrices can be obtained. The results given here are due to Miyamoto, Seberry and Yamada [10, 12].

Theorem 3 (Propus Variation)**.** *Let U_i, V_j, $i, j = 1, 2, 3, 4$ be $(0, +1, -1)$ matrices of order n which satisfy*

(i) U_i, U_j, $i \neq j$ are pairwise amicable,

(ii) V_i, V_j, $i \neq j$ are pairwise amicable,

(iii) $U_i \pm V_i$, $(+1, -1)$ matrices, $i = 1, 2, 3, 4$,

(iv) the row sum of U_1 is 1, and the row sum of U_j, $i = 2, 3, 4$ is zero,

(v) $\sum_{i=1}^{4} U_i U_i^T = (2n + 1)I - 2J$, $\sum_{i=1}^{4} V_i V_i^T = (2n + 1)I$,

(vi) $U_2 = U_3$ and $V_2 = V_3$.

Let S_1, S_2, S_3, S_4 be four $(+1,-1)$-matrices of order $2n$ defined by

$$S_j = U_j \times \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + V_j \times \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix},$$

where $S_2 = S_3$.

Then S_1, $S_2 = S_3$, S_4 are propus-Williamson type matrices of order $2n+1$. If U_i and V_i are symmetric, $i = 1,2,3,4$ then the Williamson-type matrices are symmetric. Hence there is a symmetric propus-type Hadamard matrix of order $4(2n+1)$.

Proof. With S_1, S_2, S_3, S_4, as in the lemma enunciation the row sum of $S_1 = 2$ and of $S_i = 0$, $i = 2,3,4$. Now define

$$X_1 = \begin{bmatrix} 1 & -e_{2n} \\ -e_{2n}^T & S_1 \end{bmatrix} \quad \text{and} \quad X_i = \begin{bmatrix} 1 & e_{2n} \\ e_{2n}^T & S_i \end{bmatrix}, \quad i = 2,3,4.$$

First note that since U_i, U_j, $i \neq j$ and V_i, V_j, $i \neq j$ are pairwise amicable,

$$\begin{aligned} S_i S_j^T &= \left(U_i \times \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + V_i \times \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\right)\left(U_j^T \times \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + V_j^T \times \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\right) \\ &= U_i U_j^T \times \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} + V_i V_j^T \times \begin{bmatrix} 2 & -2 \\ -2 & 2 \end{bmatrix} \\ &= S_j S_i^T. \end{aligned}$$

(Note this relationship is valid if and only if conditions (i) and (ii) of the theorem are valid.)

$$\begin{aligned} \sum_{i=1}^{4} S_i S_i^T &= \sum_{i=1}^{4} U_i U_i^T \times \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} + \sum_{i=1}^{4} V_i V_i^T \times \begin{bmatrix} 2 & -2 \\ -2 & 2 \end{bmatrix} \\ &= 2\begin{bmatrix} 2(2n+1)I - 2J & -2J \\ -2J & 2(2n+1)I - 2J \end{bmatrix} \\ &= 4(2n+1)I_{2n} - 4J_{2n} \end{aligned}$$

Next we observe

$$X_1 X_i^T = \begin{bmatrix} 1-2n & e_{2n} \\ e_{2n}^T & -J + S_1 S_i^T \end{bmatrix} = X_i X_1^T \qquad i = 2,3,4,$$

and

$$X_i X_j^T = \begin{bmatrix} 1+2n & e_{2n} \\ e_{2n}^T & J + S_i S_j^T \end{bmatrix} = X_j X_i^T \qquad i \neq j, \quad i,j = 2,3,4.$$

Further

$$\sum_{i=1}^{4} X_i X_i^T = \begin{bmatrix} 1+2n & -3e_{2n} \\ -3e_{2n}^T & J + S_1 S_1^T \end{bmatrix} + \sum_{i=2}^{4} \begin{bmatrix} 1+2n & e_{2n} \\ e_{2n}^T & J + S_i S_i^T \end{bmatrix}$$
$$= \begin{bmatrix} 4(2n+1) & 0 \\ 0 & 4J + 4(2n+1)I - 4J \end{bmatrix}.$$

Thus we have shown that X_1, X_2, X_3, X_4 are pairwise amicable, symmetric Williamson type matrices of order $2n+1$, where $X_2 = X_3$. These can be used as in (ii) of Theorem using the additive property to obtain the required symmetric propus Hadamard matrix of order $4(2n+1)$. □

Many powerful corollaries arose and new results were obtained by making suitable choices in the theorem. We choose X_1, X_2, X_3, X_4 to ensure that the propus construction can be used to form symmetric Hadamard matrices of order $4(2n+1)$.

From Paley's theorem (Corollary 1) for $p \equiv 3 \pmod 4$ we use the backcirculant or type 1, symmetric matrices QR and R instead of Q and I; whereas for $p \equiv 1 \pmod 4$ we use the symmetric Paley core Q. If p is a prime power $\equiv 3 \pmod 4$ we set $U_1 = I$, $U_2 = U_3 = QR$, $U_4 = 0$ of order p, and if p is a prime power $\equiv 1 \pmod 4$, we set $U_1 = I$, $U_2 = U_3 = Q$, $U_4 = 0$ of order p. Hence $\sum_{k=1}^{4} U_k U_k^\top = (q+2)I - 2J$.

From Turyn's result (Corollary 2) we set, for $p \equiv 1 \pmod 4$ $V_1 = P$, $V_2 = V_3 = I$ and $V_4 = S$, and for $p \equiv 3 \pmod 4$, $V_1 = P$, $V_2 = V_3 = R$ and $V_4 = S$, so $\sum_{k=1}^{4} V_k V_k^\top = (q+2)I$.

Hence we have:

Corollary 1. *Let $q \equiv 1 \pmod 4$ be a prime power and $\frac{1}{2}(q+1)$ be a prime power or the order of the core of a symmetric conference matrix (this happens for $q = 89$). Then there exist symmetric Williamson type matrices of order $2q+1$ and a symmetric propus-type Hadamard matrix of order $4(2q+1)$.*

Using $q = 5$ and $q = 41$ gives the previously unresolved cases for orders 11 and 83.

2.3.1 Three Equal Ingredients

The two starting Hadamard matrices of orders 12 and 28 are based on the skew Paley core $B = C = D = Q + I$ (constructed using Legendre symbols). They are unique because $12 = 3^2 + 1^2 + 1^2 + 1^2$ and $28 = 5^2 + 1^2 + 1^2 + 1^2$ are the only orders for which a symmetric circulant A can exist with $B = C = D$.

3 Propus-Hadamard matrices from conference matrices: even order matrices

A powerful method to construct propus-Hadamard matrices for n even is using conference matrices.

Lemma 3. *Suppose M is a conference matrix of order $n \equiv 2 \pmod 4$. Then $MM^\top = M^\top M = (n-1)I$, where I is the identity matrix and $M^\top = M$. Then using $A = M + I$, $B = C = M - I$, $D = M + I$ gives a propus-Hadamard matrix of order $4n$.*

We use the conference matrix orders from [2] and so have propus-Hadamard matrices of orders $4n$ where $n \in$

$$\{6, 10, 14, 18, 26, 30, 38, 42, 46, 50, 54, 62, 74, 82, 90, 98\}.$$

Conference matrices can be constructed using two circulant matrices A and B of order n where both A and B are symmetric.

Then using the matrices $A + I$, $B = C$ and $D = A - I$ in P gives the required construction.

The conference matrices can also be made from two circulant matrices A and B of order n where both A and B are symmetric. However here we use $A+I$, $BR = CR$ and $D = A - I$ in P to obtain the required construction. There is another variant of this family which uses the symmetric Paley cores $A = Q + I$, $D = Q - I$ (constructed using Legendre symbols) and one circulant matrix of maximal determinant $B = C = Y$.

4 Conclusion and Future Work

Using the results of Lemma 1 and Corollary 1 and the symmetric propus-Hadamard matrices of Di Matteo, Djoković, and Kotsireas given in [5], we see that the unresolved cases for symmetric propus-Hadamard matrices for orders $4n$, $n < 200$ odd, are where n is in:

$$\{17, 23, 29, 33, 35, 39, 47, 53, 65, 71, 73, 77, 93, 95, 97, 99,$$
$$101, 103, 107, 109, 113, 125, 131, 133, 137, 143, 149, 151, 153, 155,$$
$$161, 163, 165, 167, 171, 173, 179, 183, 185, 189, 191, 193, 197.\}$$

There are many constructions and variations of the propus theme to be explored in future research. Visualizing the propus construction gives aesthetically pleasing examples of propus-Hadamard matrices. The visualization also makes the construction method clearer; see Balonin [1].

References

[1] N. A. Balonin, Propus matrices, mathscinet.ru/catalogue/propus/.

[2] N. A. Balonin and J. Seberry, A review and new symmetric conference matrices, *Informatsionno-upravliaiushchie sistemy*, no. 4, 71 (2014), 2-7.

[3] R. Craigen, Signed groups, sequences and the asymptotic existence of Hadamard matrices, *J. Combin. Theory Ser. A* 71 (1995), 241–254.

[4] W. de Launey and H. Kharaghani, On the asymptotic existence of cocyclic Hadamard matrices, *J. Combin. Theory Ser. A* 116 (no. 6) (2009), 1140–1153.

[5] O. Di Matteo, D. Djoković and I. S. Kotsireas, Symmetric Hadamard matrices of order 116 and 172 exist, *Special Matrices* 3 (2015), 227–234.

[6] D. Z. Djoković and I. S. Kotsireas, New results on D-optimal matrices, *J. Combin. Des.* 20 (2012), 278–289.

[7] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. des Sciences Math.* 17 (1893), 240–246.

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

[9] E. Ghaderpour and H. Kharaghani, The asymptotic existence of orthogonal designs, *Australas. J. Combin.* 58 (2014), 333–346.

[10] M. Miyamoto, A construction for Hadamard matrices, *J. Combin. Theory Ser. A* 57 (1991), 86–108.

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

[12] 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.

[13] J. Seberry Wallis, On the existence of Hadamard matrices, *J. Combin. Theory Ser. A* 21 (1976), 186–195.

[14] R. J. Turyn, An infinite class of Williamson matrices, *J. Combin. Theory Ser A.* 12 (1972), 319–321.

[15] J. (Seberry) Wallis, Williamson matrices of even order, Combinatorial Mathematics: Proc. Second Australian Conference, (Ed.: D.A. Holton), Lec. Notes in Math. 403, SpringerVerlag, Berlin-Heidelberg-New York, (1974), 132–142.

[16] W. D. Wallis, A. P. Street and J. Seberry Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Lec. Notes in Math., Springer-Verlag, Vol. 292, 1972.

(Received 27 Sep 2016; revised 22 Sep 2017)