2018

A construction for {0,1,-1} orthogonal matrices visualized

N A. Balonin
Saint-Petersburg State University of Aerospace Instrumentation, korbendfs@mail.ru

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

A construction for {0,1,-1} orthogonal matrices visualized

Disciplines

Engineering | Science and Technology Studies

Publication Details

Balonin, N. & Seberry, J. (2018). A construction for {0,1,-1} orthogonal matrices visualized. Lecture Notes in Computer Science, 10765 47-57. Newcastle 17-21 July, 2017 28th International Workshop, IWOCA 2017

A Construction for {0,1,-1} Orthogonal Matrices Visualized

N. A. Balonin *and Jennifer Seberry †

Dedicated to the Unforgettable Mirka Miller

Abstract

Propus is a construction for orthogonal ±1 matrices, which is based on a variation of the Williamson array, called the *propus array*

$$\begin{bmatrix} A & B & B & D \\ B & D & -A & -B \\ B & -A & -D & B \\ D & -B & B & -A \end{bmatrix}.$$

This array showed how a picture made is easy to see the construction method. We have explored further how a picture is worth ten thousand words.

We give variations of the above array to allow for more general matrices than symmetric Williamson propus matrices. One such is the *Generalized Propus Array (GP)*.

Keywords: Hadamard Matrices, D-optimal designs, conference matrices, propus construction, Williamson matrices; visualization; 05B20.

1 Introduction

Hadamard matrices arise in statistics, signal processing, masking, compression, combinatorics, error correction, coil winding, weaving, spectroscopy and other areas. They been studied extensively. Hadamard showed [14] 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 [30]. Different constructions are most useful

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

†School of Computing and Information Technology, EIS, University of Wollongong, NSW 2522, Australia. Email: jennifer_seberry@uow.edu.au

in different cases. For example the Paley I construction for spectroscopy and the Sylvester construction for Walsh functions (discrete Fourier transforms) for signal processing.

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 [30, 34] cited in the bibliography.

Propus is a construction method for symmetric orthogonal ± 1 matrices, using four matrices A, $B = C$, and D, where

$$AA^\top + 2BB^\top + DD^\top = \text{ constant } I,$$

based on the array

$$\begin{bmatrix} A & B & B & D \\ B & D & -A & -B \\ B & -A & -D & B \\ D & -B & B & -A \end{bmatrix}.$$

It gives aesthetically pleasing visual images (pictures) when converted using MATLAB (we show some below).

We show how finding propus-Hadamard matrices using Williamson matrices and D-optimal designs can be easily seen through their pictures. These can be generalized to allow non-circulant and/or non-symmetric matrices with the same aim to give symmetric Hadamard matrices.

We illustrate two constructions to show the construction method (these are proved in [2])

- $q \equiv 1 \pmod 4$, a prime power, such matrices exist for order $t = \frac{1}{2}(q+1)$, and thus propus-Hadamard matrices of order $2(q+1)$ (this uses the Paley II construction) ;
- $t \equiv 3 \pmod 4$, 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 propus-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 mathscinet.ru/catalogue/propus/.

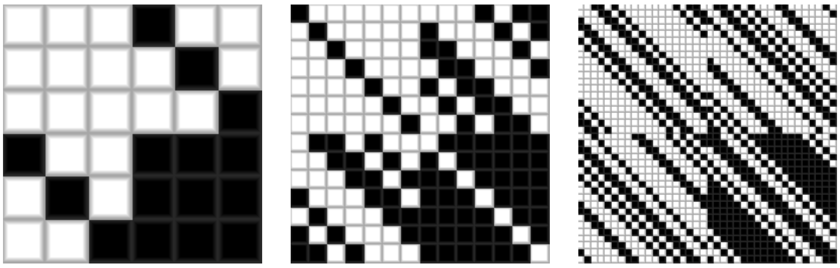
1.1 Definitions and Basics

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

A *D-optimal design* of order $2n$ is formed from two commuting or amicable (±1) matrices, A and B, satisfying $AA^\top + BB^\top = (2n-2)I + 2J$, J the matrix of all ones, written in the form

$$DC = \begin{bmatrix} A & B \\ B^\top & -A^\top \end{bmatrix} \quad \text{and} \quad DA = \begin{bmatrix} A & B \\ B & -A \end{bmatrix}.$$

respectively. In figure 1 the structure is clear to see.



(a) D6 ($n = 3$) **(b)** D14 ($n = 7$) **(c)** D38 ($n = 19$)

Figure 1: D-optimal designs for orders $2n$

Symmetric Hadamard matrices made using propus like matrices will be called *symmetric propus-Hadamard matrices.*

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 are ±1 matrices of order n satisfy the *additive property*

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

We make the definitions following [2]:

- *propus matrices*: four circulant symmetric ±1 matrices, A, B, B, D of order n, satisfying the additive property (use P);
- *propus-type matrices*: four pairwise amicable ±1 matrices, A, B, B, D of order n, $A^\top = A$, satisfying the additive property (use P);
- *generalized-propus matrices*: four pairwise commutative ±1 matrices, A, B, B, D of order n, $A^\top = A$, which satisfy the additive property (use GP).

We use two types of arrays into which to plug the propus like matrices: the Propus array, P, or the generalized-propus array, GP. These can also be used with generalized matrices ([33]).

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

Symmetric Hadamard matrices made using propus like matrices will be called *symmetric propus-Hadamard matrices.*

2 Symmetric Propus-Hadamard Matrices

We first give the explicit statements of two well known theorem, Paley's Theorem [28], for the Legendre core Q, and Turyn's Theorem [31], in the form in which we will use them.

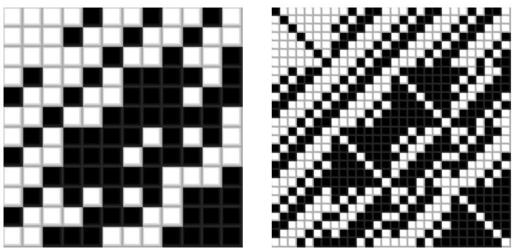
Theorem 1. **[Paley's Legendre Core [28]]** *Let p be a prime power, either $\equiv 1 \pmod 4$ or $\equiv 3 \pmod 4$ then there exists a matrix, Q, of order p with zero diagonal and other elements ± 1 satisfying $QQ^\top = (q+1)I - J$, Q is or symmetric or skew-symmetric according as $p \equiv 1 \pmod 4$ (Paley I) or $p \equiv 3 \pmod 4$ (Paley II).*

Theorem 2. **[Turyn's Theorem [31]]** *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 $PP^\top + SS^\top = qI$: P has zero diagonal and other elements ± 1 and S elements ± 1.*

2.1 Simple Propus-Hadamard Matrices of 12 and 20

2.2 $B = C = D$

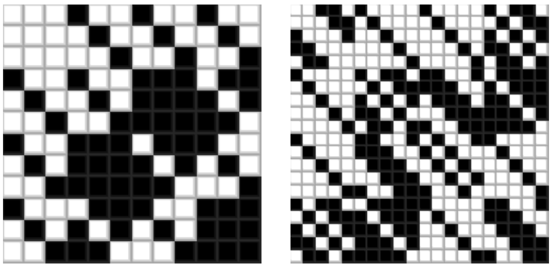
There are only two starting Hadamard matrices, of orders 12 and 28, based on skew Paley core $B = C = D = Q + I$ (constructed using Legendre symbols). This special set is finite because $12 = 3^2 + 1^2 + 1^2 + 1^2$ and $28 = 5^2 + 1^2 + 1^2 + 1^2$ and these are the only orders for which a symmetric circulant A can exist with $B = C = D$. Figure 2 clearly shows the structure.



(a) P12 ($n = 3$) **(b)** P28 ($n = 7$)

Figure 2: Propus-Hadamard matrices using three back circulants $B = C = D$

There are two simple propus-Hadamard matrices of orders 12 and 20 based on symmetric Paley cores $A = J$, $B = C = J - 2I$, $D = J = 2I$ for $n = 3$, and $A = Q + I$, $B = C = J - 2I$, $D = Q - I$ (constructed using Legendre symbols) for $n = 5$. This second construction can be continued with back-circulant matrices $C = B$ which allows the symmetry property of A to be conserved.



(a) P12 ($q = 5; n = 3$) **(b)** P20 ($q = 3^2; n = 5$)

Figure 3: Simple Propus-Hadamard matrices for orders 12 and 20

Note how the slightly different construction of $P12$ in Figures 2 and 3 can be easily seen.

2.3 Order $4n$ from Williamson Matrices using q a Prime Power

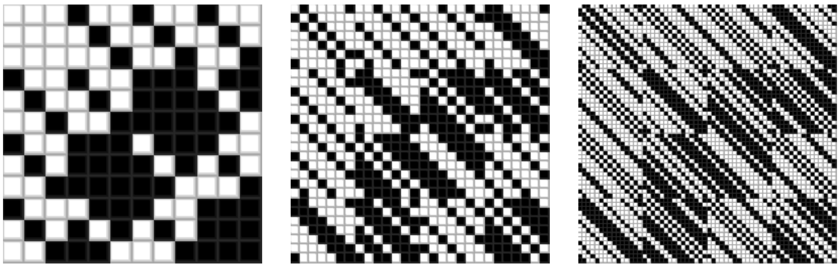
Lemma 1. *Let $q \equiv 1 \pmod 4$, be a prime power, then propus matrices exist for orders $n = \frac{1}{2}(q+1)$ which give symmetric propus-Hadamard matrices of order $2(q+1)$.*

Proof. We note that for $q \equiv 1 \pmod 4$, a prime power, Turyn (Theorem 2 [31]) gave Williamson matrices, $X + I$, $X - I$, Y, Y, which are circulant and symmetric for orders $n = \frac{1}{2}(q+1)$. Then choosing

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

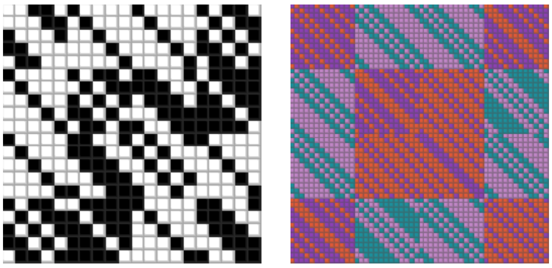
gives the required propus-Hadamard matrices. □

This gives propus-Hadamard matrices for 45 orders $4n$ where $n \leq 200$ [2]. Some of these cases arise when q is a prime power, however the Delsarte-Goethals-Seidel-Turyn construction means the required circulant matrices also exist for these prime powers (see Figures 4 and 5).



(a) P12 ($q = 5; n = 3$) **(b)** P28 ($q = 13; n = 7$) **(c)** P60 ($q = 29; n = 15$)

Figure 4: Propus-Hadamard matrices for orders $4q$ for q prime, $q \equiv 1 \pmod 4$



(a) P20 ($q = 3^2; n = 5$) **(b)** P52 ($q = 5^2; n = 13$)

Figure 5: Propus-Hadamard matrices for orders $4q$, q a prime power.

2.4 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, one of which is symmetric, exist for order $2n$. Then propus-Hadamard matrices exist for order $4n$.*

Djoković and Kotsireas in [23, 9] give 43 D-optimal designs, constructed using two circulant matrices, for $n < 200$. We are interested in those cases where the D-optimal design is constructed from two circulant matrices one of which must be symmetric.

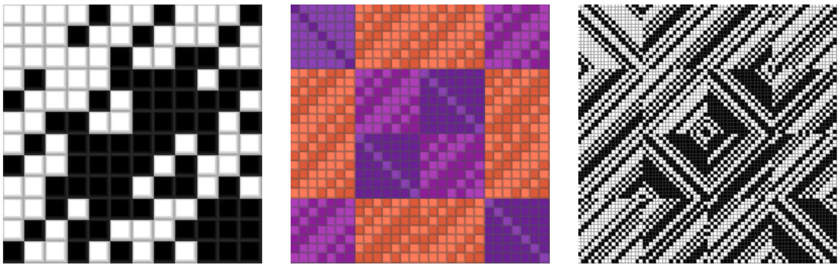
Suppose D-optimal designs for orders $n \equiv 3 \pmod 4$, a prime, are constructed using two circulant matrices, X and Y. Suppose X is symmetric. Let $Q + I$ be the Paley matrix of order n. Then choosing

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

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

Hence we have propus-Hadamard matrices, constructed using D-optimal designs, for orders $4n$ where n is in $\{3, 7, 19, 31\}$. The results for $n = 19$ and 31 were given to us by Dragomir Djokovič.

We see clearly, looking first at $GP28$ in Figure 6 where the D-optimal design is highlighted in purple, the construction method. Now the method will also be clear in $GP12$ and $GP76$.



(a) GP12 ($n = 3$) **(b)** GP28 ($n = 7$) **(c)** GP76 ($n = 19$)

Figure 6: Order $4n$ propus-Hadamard matrices constructed using D-optimal Designs

2.5 The Propus Construction

We have shown [2] that if $X_1 = A$, $X_2 = B$, $X_3 = B$, $X_4 = D$ are pairwise amicable, symmetric Williamson type matrices of order $2n+1$, where $X_2 = X_3 = B$, and satisfy the additive property, they can be used as in the appropriate array, G or GP, to form symmetric propus Hadamard matrix of order $(4(2n+1)$. For example 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.

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

From Turyn's result (Corollary 2) we set, for $p \equiv 1 \pmod 4$ $X_1 = P + I$, $X_2 = X_3 = S$ and $X_4 = P - I$.

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 $4(2q+1)$.*

This gives the previously unresolved cases for $2q+1 = 11$, and 83.

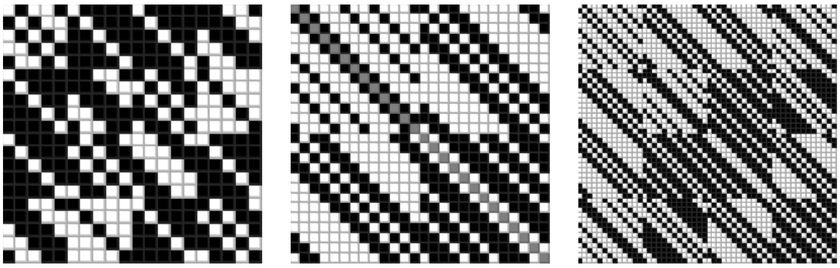
3 Propus-Hadamard Matrices from Conference matrices: even order matrices

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 sixteen conference matrix orders of even order $n \leq 100$ from [1] to give propus-Hadamard matrices of orders $4n$. The conference matrices in Figure 7 are made two circulant matrices A and B of order n where both A and B are symmetric.

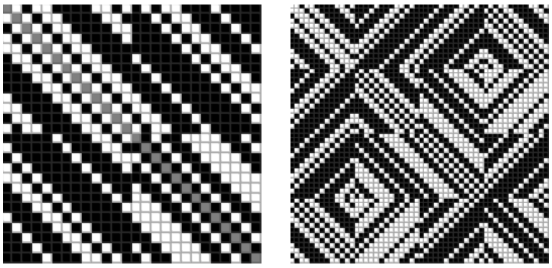
Then using the matrices $A + I$, $B = C$ and $D = A - I$ in P gives the required construction.



(a) CP20 ($n = 3$) **(b)** C26 ($n = 13$) **(c)** CP52 ($n = 13$)

Figure 7: Conference matrices for orders $2n$ using two circulants: propus-Hadamard matrices for orders $4n$

The conference matrices in Figure 8 are 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.



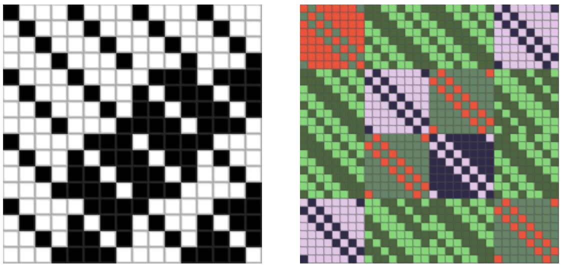
(a) C26G ($n = 13$) **(b)** CP52G ($n = 13$)

Figure 8: Conference matrices for orders $2n$ using two circulant and back-circulants: propus-Hadamard matrices for orders $4n$

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 $B = C = Y$.

3.1 Propus-Hadamard matrices for n even

Figure 9 gives visualizations (images/pictures) of propus-Hadamard matrices orders 16, 32. These have even n.



(a) P16 ($n = 4$) **(b)** P32 ($n = 8$)

Figure 9: Matrices P16 and P32

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 $n \in$

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

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. There is the possibility that these visualizations may be used for quilting.

References

[1] N. A. Balonin and Jennifer Seberry, A review and new symmetric conference matrices, *Informatsionno-upravliaiushchie sistemy*, no 4, 71 (2014) 27.

[2] N. A. Balonin and Jennifer Seberry, Two infinite families of symmetric Hadamard matrices, *Austral. Comb*,Vol.69(3) (2017), 349-357.

[3] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Vol. 182, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[4] J.H.E. Cohn, A D-optimal design of order 102, *Discrete Mathematics*, 1, 102 (1992) 61-65.

[5] Olivia Di Matteo, Dragomir Djoković, and Ilias S. Kotsireas, Symmetric Hadamard matrices of order 116 and 172 exist. *Special Matrices*, 3 (2015), pp. 227-234.

[6] D. Z. Djoković, On maximal $(1, -1)$-matrices of order $2n$, n odd, *Radovi Matematicki*, 7 no 2 (1991),371-378.

[7] D.Z. Djoković, Some new D-optimal designs, *Australasian Journal of Combinatorics*, 15 (1997), 221-231.

[8] D.Z. Djoković, Cyclic $(v; r, s; \lambda)$ difference families with two base blocks and $v \leq 50$ *Annals of Combinatorics*, 15, no2 (2011), 233-254.

[9] Dragomir Z. Djoković and Ilias S. Kotsireas, New results on D-optimal matrices, *Journal of Combinatorial Designs*, 20 (2012), 278-289.

[10] Dragomir Z. Djoković and Ilias S. Kotsireas, email communication from I. Kotsireas 3 August 2014 1:13 pm.

[11] Roderick J. Fletcher, Marc Gysin and Jennifer Seberry, Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices, *Australasian J. Combinatorics*, 23 (2001) 75-86.

[12] Roderick J. Fletcher, Christos Koukouvinos and Jennifer Seberry, New skew-Hadamard matrices of order and new D-optimal designs of order $2 \cdot 59$, *Discrete Mathematics* , volume = 286, no3 (2004) 251-253.

[13] Roderick J. Fletcher and Jennifer Seberry, New D-optimal designs of order 110,*Australasian J. Combinatorics*, 23 (2001) 49-52.

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

[15] Marc Gysin, New D-optimal designs via cyclotomy and generalised cyclotomy, *Australasian Journal of Combinatorics*, 15 (1997) 247-255.

[16] Marc Gysin, *Combinatorial Designs, Sequences and Cryptography*, PhD Thesis, University of Wollongong, 1997.

[17] Marc Gysin and Jennifer Seberry, An experimental search and new combinatorial designs via a generalisation of cyclotomy, *J. Combin. Math. Combin. Comput.*, 27 (1998) 143-160.

[18] Wolf H. Holzmann and Hadi Kharaghani, A D-optimal design of order 150, *Discrete Mathematics*, 190 no 1 (1998) 265-269.

[19] Ilias S. Kotsireas and Panos M. Pardalos, D-optimal matrices via quadratic integer optimization, *J. Heuristics*, 19 no 4 (2013) 617-627.

[20] C. Koukouvinos, S. Kounias and Jennifer Seberry, Supplementary difference sets and optimal designs, *Discrete Math.*, 88 no 1 (1991) 49-58.

[21] C.Koukouvinos, Jennifer Seberry, A. L. Whiteman and M. Xia, Optimal designs, supplementary difference sets and multipliers, *Journal of Statistical Planning and Inference*, 62 no 1 (1997) 81-90.

[22] S. Georgiou, C. Koukouvinos and J. Seberry, Hadamard matrices, orthogonal designs and construction algorithms, in *Designs 2002: Further Combinatorial and Constructive Design Theory*, (W.D.Wallis, ed.), Kluwer Academic Publishers, Norwell, Ma, 2002, 133-205.

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

[24] M. Hall Jr, A survey of difference sets, *Proc. Amer. Math. Soc.*, 7 (1956), 975-986.

[25] M. Hall Jr, *Combinatorial Theory*, 2nd Ed., Wiley, 1998.

[26] M. Miyamoto, A construction for Hadamard matrices, *J. Comb. Th. Ser A.* 57 (1991) 86-108.

[27] Marilena Mitrouli, D-optimal designs embedded in Hadamard matrices and their effect on the pivot patterns, *Linear Algebra and its Applications*, 434 (2011) 1751-1772.

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

[29] R.L. Plackett and J.P. Burman, The design of optimum multifactorial experiments, *Biometrika*, 33 (1946), 305-325.

[30] Jennifer Seberry and Mieko 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.

[31] Richard J Turyn, An infinite class of Williamson matrices, *J. Combinatorial Theory Ser A.* 12 (1972) 319-321.

[32] N. J. A. Sloane, AT&T on-line encyclopedia of integer sequences, http://www.research.att.com/ njas/sequences/.

[33] Jennifer (Seberry) Wallis, Williamson matrices of even order, Combinatorial Mathematics: Proceedings of the Second Australian Conference, (D.A. Holton, (Ed.)), Lecture Notes in Mathematics, 403, SpringerVerlag, BerlinHeidelbergNew York, (1974), 132-142.

[34] W.D. Wallis, A.P. Street and Jennifer Seberry Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Lecture Notes in Mathematics, Springer-Verlag, Vol. 292, 1972.

[35] A. L. Whiteman, A family of D-optimal designs, *Ars Combin.*, 30 (1990) 23-26.

[36] Mieko Yamada, On the Williamson type j matrices of order 4.29, 4.41, and 4.37, *J. Combin. Theory, Ser A*, 27 (1979) 378-381.

[37] Jennifer Seberry Wallis, On the existence of Hadamard matrices, *J. Combin. Th. (Ser. A)*, 21 (1976), 186-195.

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

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

[40] Warwick de Launey and H. Kharaghani, On the asymptotic existence of cocyclic Hadamard matrices, *J. Combin. Th. (Ser. A)*, 116 no 6 (2009), 1140-1153.