Vizualizing Hadamard Matrices: the Propus Construction

N. A. Balonin [*]and Jennifer Seberry [†]

September 5, 2014

Abstract

Propus (which means twins) is a construction method for orthogonal ±1 matrices based on the *propus array*

$$\begin{array}{rrrr} A & B & C & D \\ C & D & -A & -B \\ B & -A & -D & C \\ D & -C & B & -A. \end{array}$$

This construction, based on circulant symmetric ±1 matrices, called *propus matrices*, is aimed to give aesthetically pleasing visual images (pictures) when converted using MATLAB. It gives symmetric Hadamard matrices.

We give two constructions and note that using these results, we are able to find images (pictures) for propus-Hadamard matrices for orders $4n$, $n < 100$ odd, where n is not in

$$\{11, 17, 23, 29, 33, 35, 39, 43, 47, 53, 65, 71, 73, 77, 83, 85, 93,$$
$$101, 103, 107, 109, 113, 123, 125, ...\}.$$

A computer algorithm seems to be needed to find further results.

We give variations of the above array to allow for more general matrices than propus matrices, including the *Goethals-Seidel-Propus matrices.*

We show how conference matrices can be used to find propus-Hadamard for n even.

We refer the interested reader to mathscinet.ru/catalogue/propus/.

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

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

[†] Centre for Computer Security Research, School of Computer Science and Software Engineering, EIS, University of Wollongong, NSW 2522, Australia. Email: jennifer_seberry@uow.edu.au

1 Introduction

Hadamard matrices arise in Statistics, Signal Processing, Combinatorics, Cryptography, Weaving, Spectroscopy and other areas. They been studied extensively. Hadamard showed [12] the order of an Hadamard matrix must be 1, 2 or a multiple of 4.

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. For more details see the books and surveys of Jennifer Seberry (Wallis) and others [27, 31] cited in the bibliography.

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

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

I the identity matrix, based on the array

$$\begin{array}{cccc} A & B & C & D \\ C & D & -A & -B \\ B & -A & -D & C \\ D & -C & B & -A. \end{array}$$

This construction, based on circulant symmetric ± 1 matrices, called *propus matrices*, is aimed to give aesthetically pleasing visual images (pictures) when converted using MATLAB. It gives symmetric Hadamard matrices.

We give methods to find propus-Hadamard matrices: using Williamson matrices and D-optimal designs. Many delightful visual images are included. These are then generalized to allow non-circulant and/or non-symmetric matrices with the same aim to give aesthetically pleasing visual images (pictures) and symmetric Hadamard matrices.

We show that for

- $q \equiv 1 (\text{mod } 4)$, a prime power, such matrices exist for order $t = \frac{q+1}{2}$, and thus propus-Hadamard matrices of order $2(q+1)$;
- $t \equiv 3 (\text{mod } 4)$, 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 persue 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 $XY^\top = YX^\top$.

We define the following classes of propus like matrices. All propus like matrices A, $B = C$, D are ± 1 matrices of order n satisfy the *additive property*

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

I the identity matrix.

We make the following definitions:

- *propus matrices*: four circulant symmetric ± 1 matrices satisfying the additive property (use P);
- *propus-type matrices*: four symmetric ± 1 matrices satisfying the additive property and which are pairwise amicable (use P);
- *good-propus matrices*: four circulant ± 1 matrices, one of which must be symmetric, which satisfy the additive property (use GP);
- *Goethals-Seidel-propus-type matrices*: four ± 1 matrices satisfying the additive property, one of the four must be symmetric, and be pairwise amicable with the other three; the other three pairwise commute (use GSP).

We use three types of arrays into which to plug the propus like matrices: the Propus array, P, the good-propus array, GP, the Goethals-Seidel-Propus (GSP) arrays. These are

$$P = \begin{array}{rrrr} A & B & C & D \\ C & D & -A & -B \\ B & -A & -D & C \\ D & -C & B & -A \end{array}$$

and as with good matrices ([30])

$$GP = \begin{array}{rrrr} A & BR & CR & DR \\ CR & D^\top R & -A & -B^\top R \\ BR & -A & -D^\top R & C^\top R \\ DR & -C^\top R & B^\top R & -A. \end{array} \quad \text{or} \quad GSP = \begin{array}{rrrr} A & B & C & D \\ C & D^\top & -A & -B^\top \\ B & -A & -D^\top & C^\top \\ D & -C^\top & B^\top & -A. \end{array}$$

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

1.2 Propus-Hadamard matrices from Williamson matrices

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

We note that for $q \equiv 1 \pmod 4$, a prime power, Turyn [28] gave Williamson matrices, $X+I$, $X-I$, Y, Y, which are circulant and symmetric for orders $n = \frac{q+1}{2}$. Then choosing

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

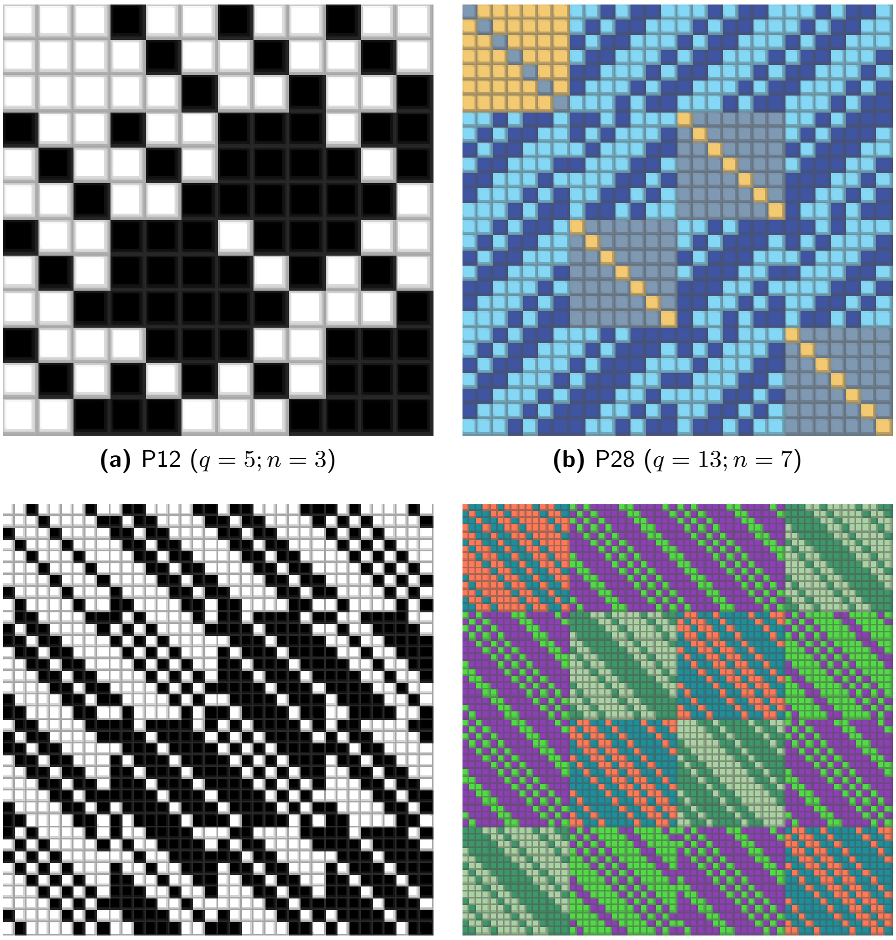
gives the required propus-Hadamard matrices.
We now have propus-Hadamard matrices for orders $4n$ where n is in

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

This means we do not yet have the cases

$$\{11, 17, 23, 29, 33, 35, 39, 43, 47, 53, 65, 71, 73, 77, 83, 93, 99, 101, 103, 107, 109, 113, 123, 125, ...\}.$$

The cases written in square brackets [5],[13],[25],[41],[61],[63],[85],[113],[145], [181] arise when q is a prime power, $q = 9$, 25, 49, 81, 121, 125, 169, 225, 289 and 361 respectively, may need to be investigated further for inequivalent results.



(a) P12 $(q = 5; n = 3)$

(b) P28 $(q = 13; n = 7)$

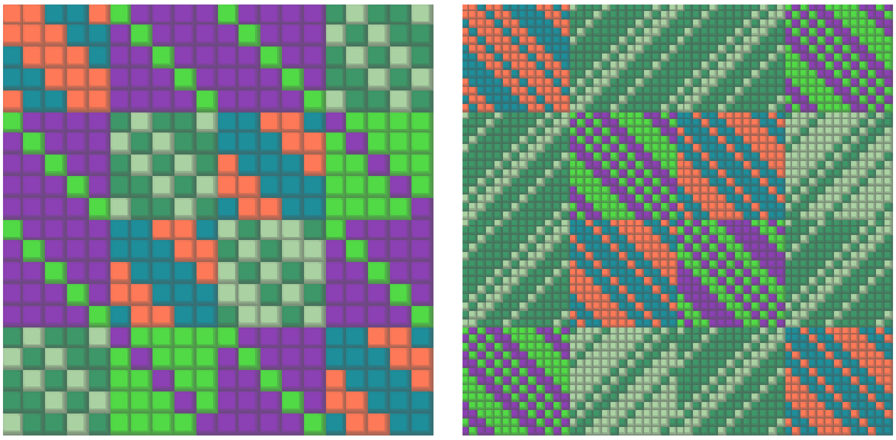
(c) P36 $(q = 17; n = 9)$

(d) P60 $(q = 29; n = 15)$

Figure 1: Propus-Hadamard matrices for orders $4n$

1.2.1 Propus matrices of small order and from q prime power

The cases 5, 13, 25, 41, 61, 63 and 85 have arisen from prime powers and while they exist, we may need investigate further to establish inequivalent results. In fact we have results by computer search for $q = 5$, 13 and 25 with circulant matrices.



(a) P20 ($q = 9; n = 5$) **(b)** P52 ($q = 25; n = 13$)

Figure 2: Propus-Hadamard matrices for orders $4n$

This family is considered to contain two propus-Hadamard matrices of orders 4 and 20 based on symmetric Paley cells $A = Q + I$, $D = Q - I$ (constructed using Legendre symbols) and two symmetric circulant matrices $C = B$. $C = B = J$ for n=5. This special set can be continued with back-circulant matrices $C = B$ which allows the symmetry property of A to be conserved.

1.3 Propus-Hadamard matrices from D-optimal designs

Lemma 2 *Let $n \equiv 3 (\mathrm{mod}\ 4)$, 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 $4n$.*

Djokovic and Kotsireas in [8] give D-optimal designs for n =69, 75, 77 and 87 constructed using two circulant matrices. From Djokovic and Kotsireas [7] we have that D-optimal designs exist for $n \in \{3, 5, 7, 9, 13, 15, 19, 21, ...27, 31, 33, 37, 41, 43, 45, 49, 51, 55...63, 69, 73, 75, 77, 79, 85, 87, 91, 93, 97, 103, 113, 121, 131, 133, 145, 157, 181, 183\}$. 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 $n \equiv 3 (\mathrm{mod}\ 4)$, 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

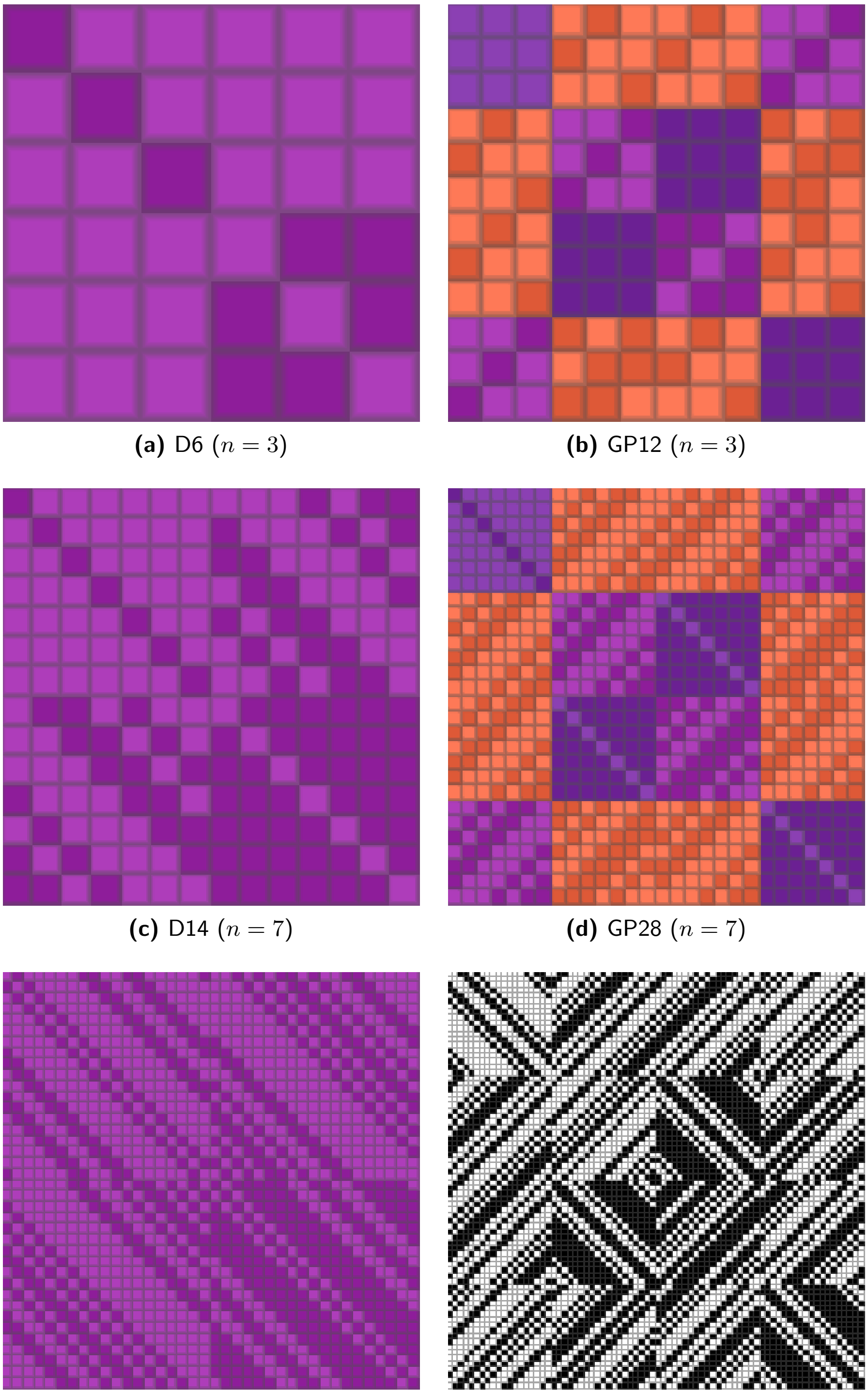
$$A = X,\ B = C = Q + I,\ D = Y,$$

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 Djokovic.



(a) D6 ($n = 3$)

(b) GP12 ($n = 3$)

(c) D14 ($n = 7$)

(d) GP28 ($n = 7$)

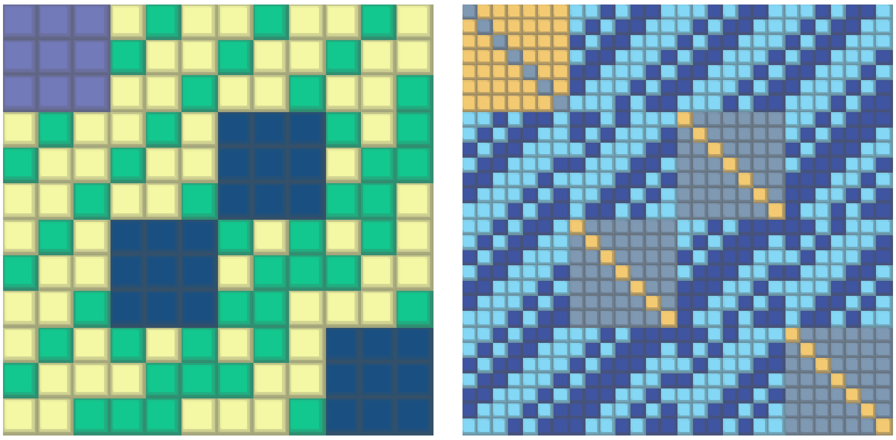
(e) D38 ($n = 19$)

(f) GP76 ($n = 19$)

Figure 3: D-optimal designs for orders $2n$ propus-Hadamard matrices for orders $4n$

1.3.1 Three Equal

The family given above included two starting Hadamard matrices of orders 12 and 28 based on skew Paley cells $B = C = D = Q + I$ (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 $B = C = D$.



(a) P12 ($n = 3$)

(b) P28 ($n = 7$)

Figure 4: Propus-Hadamard matrices using D-optimal designs

2 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 $n \equiv 2 (\mathrm{mod}\ 4)$. 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 $4n$.*

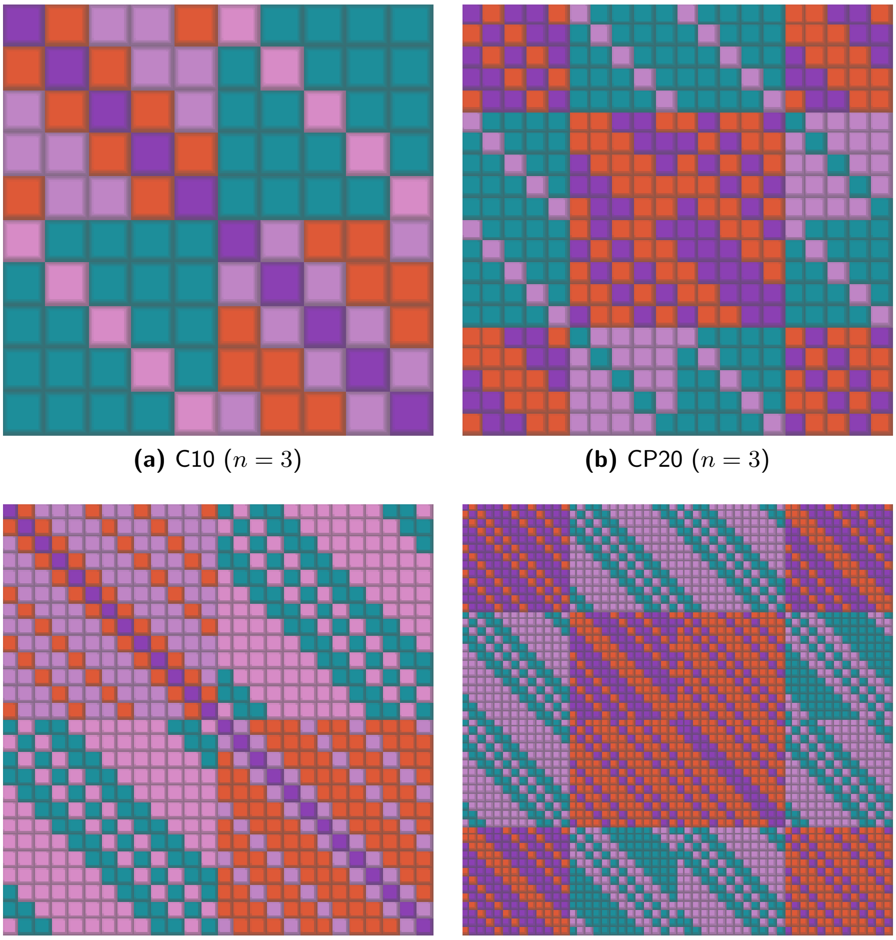
We use the conference matrix orders from [1] and so have propus-Hadamard matrices of orders $4n$ where $n \in$

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

The conference matrices in Figure 5 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.

See http://mathscinet.ru/catalogue/propus/twocirculant/.



(a) C10 ($n = 3$)

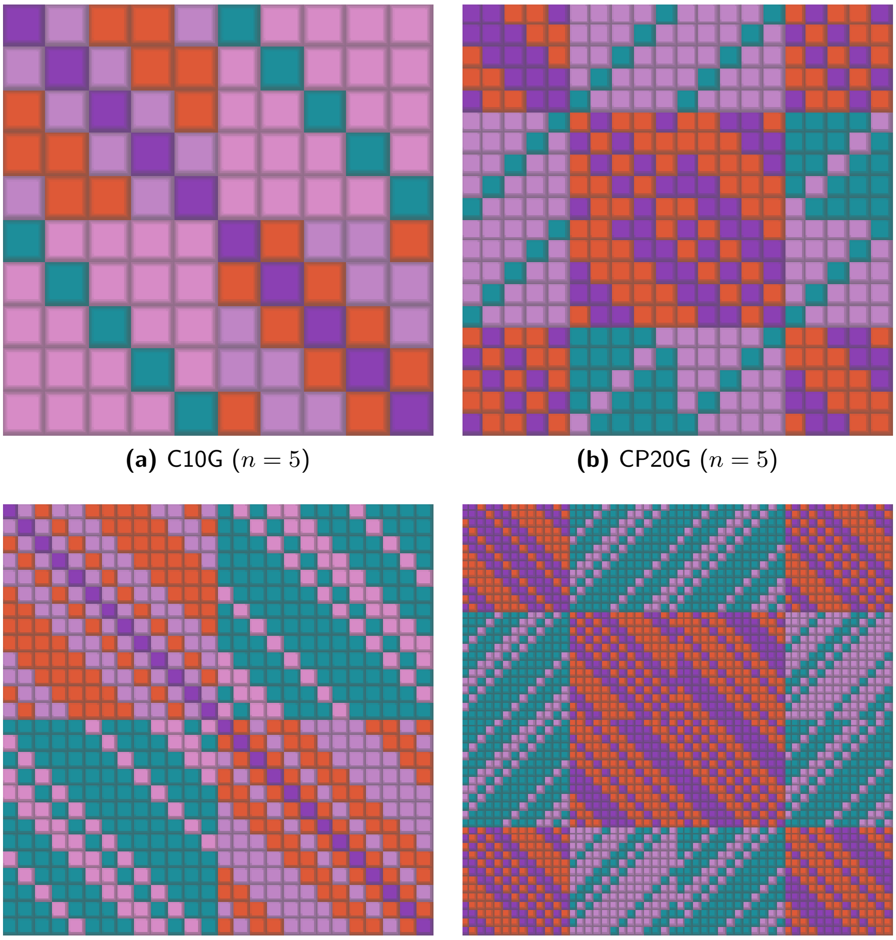
(b) CP20 ($n = 3$)

(c) C26 ($n = 13$)

(d) CP52 ($n = 13$)

Figure 5: Conference matrices for orders $2n$ using two circulants: poor propus-Hadamard matrices for orders $4n$

The conference matrices in Figure 6 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) C10G ($n = 5$)

(b) CP20G ($n = 5$)

(c) C26G ($n = 13$)

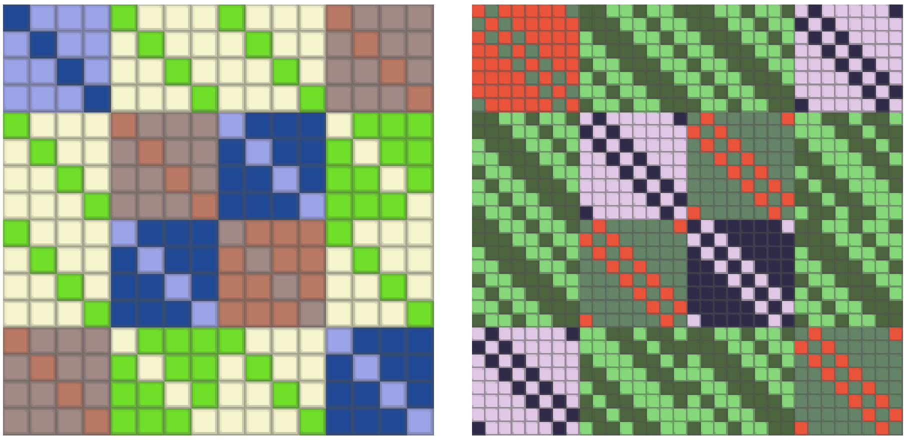
(d) CP52G ($n = 13$)

Figure 6: Conference matrices for orders $2n$ using two circulants: rich propus-Hadamard matrices for orders $4n$

There is another variant of this family which uses the symmetric Paley cells $A = Q + I$, $D = Q - I$ (constructed using Legendre symbols) and one circulant matrix of maximal determinant $B = C = Y$.

2.1 Propus-Hadamard matrices for n even

We have given visualizations (images/pictures) of propus-Hadamard matrices for Hadamard matrices of orders 8, 16, 24, 32 in Figure 7. These have even n.



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

Figure 7: Matrices P16 and P32

2.2 Summary

The above constructions mean we have propus-Hadamard matrices for orders $4n$, $n < 200$ odd, where $n \in$

So we do not yet know of propus-Hadamard matrices for orders $4n$, $n < 125$ odd, where $n \in$

$$\{11, 17, 23, 29, 33, 35, 39, 43, 47, 53, 65, 71, 73, 77, 83, 93,$$
$$101, 103, 107, 109, 113, 123, 125, ...\}.$$

3 Conclusion and Future Work

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.

We can also consider other patterns for the matrices A, B, B, D for example $A^\top = A$, BR, BR, DR with B and D skew or $A^\top = A$, BR, BR, DR with B skew. These are dependent on how $4n = a^2 + b^2 + c^2 + d^2$ can be written as the sum of four squares; the skew matrices yielding $b^2 = c^2 = 1^2$.

References

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

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

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

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

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

[6] D.Z. Djoković, Cyclic $(v; r, s; \lambda)$ difference families with two base blocks and $v \leq 50$ *Annals of Combinatorics*, 15, no 2 (2011), 233-254.

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

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

[9] 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.

[10] 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* , 286, no 3 (2004) 251-253.

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

[12] Jacques Hadamard, Resolution d'une question relative aux determinants, *Bull. des Sciences Math.*, 17 (1893) 240-246.

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

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

[15] 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.

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

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

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

[19] 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.

[20] 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.

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

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

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

[24] 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.

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

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

[27] 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.

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

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

[30] 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.

[31] 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.

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

[33] 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.