**Communications in Mathematics and Applications**
Vol. 14, No. 1, pp. 81–88, 2023
ISSN 0975-8607 (online); 0976-5905 (print)
Published by RGN Publications
DOI: 10.26713/cma.v14i1.2225
http://www.rgnpublications.com

Research Article

# On Some Examples of Williamson Matrices

Pankaj Kumar Manjhi*[1] and Ninian Nauneet Kujur[2]

[1] *University Department of Mathematics, Vinoba Bhave University, Hazaribag, India*
[2] *Department of Mathematics, Sri Venkateswara College, University of Delhi, New Delhi, India*
***Corresponding author:** 19pankaj81@gmail.com

**Received:** February 7, 2023 **Accepted:** April 3, 2023

**Abstract.** This article deals with some special cases of Williamson Hadamard matrices, which are generated by block symmetric circulant matrices. In these cases, the patterns of the obtained examples have been analyzed for insight into the nature of the Williamson matrices.

**Keywords.** Hadamard matrix, Williamson matrix

**Mathematics Subject Classification (2020).** 05B15, 05B20, 05B30



## 1. Introduction

A square matrix $H$ of order $n$ is called a Hadamard matrix if $HH' = nI_n$. It is known that the order of a Hadamard matrix will be $1,2$ or some integral multiple of 4. According to the Hadamard conjecture, there exists a Hadamard matrix of every order of the form $4t$, $t$ being some integer (for more details see [5, 7, 10, 14, 15]). Despite the availability of a large number of methods for constructing Hadamard matrices, the Hadamard matrix conjecture has still remained an open problem in mathematics for the past 100 years. 668, 716, 892 and 956 are some of the orders for which the Hadamard matrix is not yet known. Hadamard matrices are used in error-correcting code and communication systems (for more details see [7]). Holzmann *et al*. [6] are credited with the construction of a new Hadamard matrix of order 448 in the year 2005 which is the last new construction.

The Hadamard matrices were first given by J. J. Sylvester in 1867 [15]. Sylvester's method enabled us to construct a Hadamard matrix of order $2^k$ where $k$ is a positive integer.

In 1893, Hadamard [5] proved one of the famous theorems of Hadamard's inequality and this led to the popularity of Hadamard matrices in the mathematical community. R. Paley [11] discovered a new method of constructing Hadamard matrices in 1933, using finite fields. Paley's method gives Hadamard matrices of order $(q+1),(2(q+1))$ for $q \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$ respectively where $q$ is an odd prime power. The Williamson method of constructing Hadamard matrices was given by Williamson in 1944 [16]. The modern computational era in the construction of Hadamard matrices can be attributed to Williamson's method.

Symmetric and circulant matrices $A,B,C,D$ of order $n$, are known as Williamson matrices if $A^2+B^2+C^2+D^2=4nI_n$. These matrices are named after J. Williamson who introduced these matrices [16] while developing a method for the construction of Hadamard matrices. He showed that if $A,B,C,D$ are Williamson matrices of order $n$, then

$$H=\begin{pmatrix} A & B & C & D \\ -B & A & D & -C \\ -C & -D & A & B \\ -D & C & -B & A \end{pmatrix} \tag{1}$$

is a Hadamard matrix of order $4n$ ([12, 16]). He conjectured that Williamson matrices exist for all positive integers $n$. This was proved false by Đoković, by exhaustive computer search showing that for $n=35$, no Williamson matrix exists (for more details see [4]). The majority of work in Williamson matrices has been done for odd orders. Williamson matrices of odd order exist for all orders $n<65$ except for $n=35,47,53,59$. A complete enumeration for $n<60$ has been done so far [6]. For $n=61$ it was done by Lang and Schneider in 2012 [8]. For even orders, a complete enumeration up to $n=64$ has been done so far by Bright *et al*. in 2018 [1]. Later in 2019, a complete enumeration for $n=63,66,68,70$ have been by Bright *et al*. [2], and thereby they have conjectured that Williamson matrices exist in every even order. By taking $B=C$ in the above matrix $H$ (see (1)) three block construction of Hadamard matrices have been specified by Sergeev and Vostrikov [13].

In 2018, Manjhi and Kumar [10] introduced a method of construction of Hadamard matrices which is of the type (1) with $A=J_n$ and $B=C=D$, where $J_n$ is all 1*s* matrix and $A$ is a $\pm 1$ matrix, each of order $n$, as given below:

$$H=\begin{pmatrix} J_n & A & A & A \\ -A & J_n & A & -A \\ -A & -A & J_n & A \\ -A & A & -A & J_n \end{pmatrix}. \tag{2}$$

Manjhi and Kumar [10] showed that $H$ given in (2) is a Hadamard matrix if $n$ is a multiple of 3. In addition, some other properties of this type of Hadamard matrices have been discussed with one illustration.

In this article, some examples of small orders of Williamson matrices of particular types have been obtained. Furthermore, the patterns of obtained examples have been analyzed. Meanwhile, some non-existence results have been obtained for some particular orders.

## 2. Main Work

In eq. (1) the four symmetric circulant matrices $A,B,C,D$ with entries $\pm1$ will give a Hadamard matrix if and only if $A^2+B^2+C^2+D^2=4nI_n$. This article brings all exhaustive search results on the special cases up to $n=10$ with the first entry 1. The results are given below:

(i) $A=B=C=D$

| Sl. No. | Value of $n$ | Existence of $A,B,C$ and $D$ |
|---|---|---|
| 1 | 2,3,5,6,7,8,9,10 | Does not exist |
| 2 | 4 | (i) $A=\text{circ}(1,-1,-1,-1)$ |
| | | (ii) $A=\text{circ}(1,1,-1,1)$ |

(ii) $A,B$ are distinct; $B=C=D$

| Sl. No. | Value of $n$ | Existence of $A,B,C$ and $D$ |
|---|---|---|
| 1 | 2,5,6,7,8,9,10 | Does not exist |
| 2 | 3 | (i) $A=\text{circ}(1,1,1)$, $B=\text{circ}(1,-1,-1)$ |
| 3 | 4 | (i) $A=\text{circ}(1,-1,-1,-1)$, $B=\text{circ}(1,1,-1,1)$ |
| | | (ii) $A=\text{circ}(1,1,-1,1)$, $B=\text{circ}(1,-1,-1,-1)$ |

(iii) $A,C$ are distinct; $A=B$ and $C=D$

| Sl. No. | Value of $n$ | Existence of $A,B,C$ and $D$ |
|---|---|---|
| 1 | 2 | $A=\text{circ}(1,-1)$, $C=\text{circ}(1,1)$ |
| 2 | 3,5,6,7,9,10 | Does not exist |
| 3 | 4 | $A=\text{circ}(1,-1,-1,-1)$, $C=\text{circ}(1,1,-1,1)$ |
| 4 | 8 | (i) $A=\text{circ}(1,-1,-1,1,1,1,-1,-1)$, $C=\text{circ}(1,-1,1,1,1,1,1,-1)$ |
| | | (ii) $A=\text{circ}(1,-1,-1,1,1,1,-1,-1)$, $C=\text{circ}(1,1,1,-1,1,-1,1,1)$ |
| | | (iii) $A=\text{circ}(1,-1,1,1,1,1,1,-1)$, $C=\text{circ}(1,1,-1,-1,1,-1,-1,1)$ |
| | | (iv) $A=\text{circ}(1,1,-1,-1,1,-1,-1,1)$, $C=\text{circ}(1,1,1,-1,1,-1,1,1)$ |

(iv) $A,B,C$ are distinct; $C = D$

| Sl. No. | Value of $n$ | Existence of $A,B,C$ and $D$ |
|---|---|---|
| 1 | $2,3,4,6,9,10$ | Does not exist |
| 2 | 5 | $A = \text{circ}(1,-1,1,-1,-1)$, $B = \text{circ}(1,1,-1,-1,1)$, $C = \text{circ}(1,-1,-1,-1,-1)$ |
| 3 | 7 | (i) $A = \text{circ}(1,-1,-1,1,1,-1,-1)$, $B = \text{circ}(1,1,1,-1,-1,1,1)$, $C = \text{circ}(1,-1,1,1,1,1,-1)$ |
| | | (ii) $A = \text{circ}(1,-1,1,-1,-1,1,-1)$, $B = \text{circ}(1,1,-1,1,1,-1,1)$, $C = \text{circ}(1,1,1,-1,-1,1,1)$ |
| | | (iii) $A = \text{circ}(1,-1,1,-1,-1,1,-1)$, $B = \text{circ}(1,1,-1,-1,-1,-1,1)$, $C = \text{circ}(1,1,-1,1,1,-1,1)$ |
| 4 | 8 | (i) $A = \text{circ}(1,-1,-1,1,1,1,-1,-1)$, $B = \text{circ}(1,1,-1,-1,1,-1,-1,1)$, $C = \text{circ}(1,-1,1,1,1,1,1,-1)$ |
| | | (ii) $A = \text{circ}(1,-1,-1,1,1,1,-1,-1)$, $B = \text{circ}(1,1,-1,-1,1,-1,-1,1)$, $C = \text{circ}(1,1,1,-1,1,-1,1,1)$ |
| | | (iii) $A = \text{circ}(1,-1,1,1,1,1,1,-1)$, $B = \text{circ}(1,1,1,-1,1,-1,1,1)$, $C = \text{circ}(1,-1,-1,1,1,1,-1,-1)$ |
| | | (iv) $A = \text{circ}(1,-1,1,1,1,1,1,-1)$, $B = \text{circ}(1,1,1,-1,1,-1,1,1)$, $C = \text{circ}(1,1,-1,-1,1,-1,-1,1)$ |

(v) $A, B, C$, and $D$ all are distinct.

| Sl. No. | Value of $n$ | Existence of $A, B, C$ and $D$ |
|---|---|---|
| 1 | 2,3,4,5,8,9,10 | Does not exist |
| 2 | 6 | (i) $A = \text{circ}(1,-1,-1,-1,-1,-1)$,<br>$B = \text{circ}(1,-1,-1,1,-1,-1)$,<br>$C = \text{circ}(1,-1,1,1,1,-1)$,<br>$D = \text{circ}(1,1,-1,-1,-1,1)$ |
| | | (ii) $A = \text{circ}(1,-1,-1,-1,-1,-1)$,<br>$B = \text{circ}(1,-1,-1,1,-1,-1)$,<br>$C = \text{circ}(1,1,-1,-1,-1,1)$,<br>$D = \text{circ}(1,1,-1,1,-1,1)$ |
| | | (iii) $A = \text{circ}(1,-1,-1,-1,-1,-1)$,<br>$B = \text{circ}(1,-1,1,1,1,-1)$,<br>$C = \text{circ}(1,1,-1,-1,-1,1)$,<br>$D = \text{circ}(1,1,1,-1,1,1)$ |
| | | (iv) $A = \text{circ}(1,-1,-1,1,-1,-1)$,<br>$B = \text{circ}(1,1,-1,-1,-1,1)$,<br>$C = \text{circ}(1,1,-1,1,-1,1)$,<br>$D = \text{circ}(1,1,1,-1,1,1)$ |
| 3 | 7 | (i) $A = \text{circ}(1,-1,-1,-1,-1,-1,-1)$,<br>$B = \text{circ}(1,-1,-1,1,1,-1,-1)$,<br>$C = \text{circ}(1,-1,1,-1,-1,1,-1)$,<br>$D = \text{circ}(1,1,-1,-1,-1,-1,1)$ |

In the construction of Hadamard matrix of the form (2), Manjhi and Kumar [10] illustrated the methodology by considering $A = J_3 - 2I_3$ for order 12. However, no more illustrations have been forwarded by them. We note that in the illustration Manjhi and Kumar [10], the matrix $A$ is taken as a linear combination of $I_n$ and $J_n$. Herewith we forward some non-existence theorems for the Hadamard matrices of higher order by adopting the same process of selecting the matrix $A$.

**Theorem 2.1.** *The matrix $H$* (2) *is a Hadamard matrix with $A = J_n - 2I_n$ if and only if $n = 3$.*

*Proof.* $H$ will be a Hadamard matrix if and only if $J_n^2 + 3(J_n - 2I_n)^2 = 4nI_n$

if and only if $J_n^2 + 3(J_n^2 + 4I_n - 4J_n) = 4nI_n$

if and only if $nJ_n + 3(nJ_n + 4I_n - 4J_n) = 4nI_n$

if and only if $4(n-3)J_n + 12I_n = 4I_n$

if and only if $n = 3$. □

**Remark 2.1.** The method of construction of Hadamard matrix of the form (2) is a tedious job for the next possible order 24, the above theorem only suggests the non-existence of higher order Hadamard matrices in a particular approach of selecting matrix $A$.

In the particular case of the Williamson Hadamard matrix when $A, B$ are distinct and $A = B$, $C = D$, the obtained results show that the order of Williamson matrices must be 2, 4 or 8 up to order 10. However, when Williamson matrices are itself Hadamard then we will get a Hadamard matrix of the form (1). The conclusion is shown in the form of a theorem below:

**Theorem 2.2.** *If $A$ and $C$ are symmetric circulant Hadamard matrices, then* (1) *will be a Hadamard matrix for $A, B$ distinct and $A = B$, $C = D$.*

*Proof.* The matrix $H$ given in (1) will be a Hadamard matrix if and only if $A^2 + C^2 = 4nI_n$ where $A, C$ are distinct and $A = B$, $C = D$. If $A$ and $C$ are symmetric circulant Hadamard matrices, then $A = A'$ and $B = B'$. This implies that $A^2 + C^2 = A \cdot A + C \cdot C = A \cdot A' + C \cdot C' = nI_n + nI_n = 2nI_n$. Thus, $A^2 + B^2 + C^2 + D^2 = 4nI_n$. This proves the theorem. □

**Remark 2.2.** The above result may not be continued for the construction of Hadamard matrices for $n > 4$ due to the conjecture of Ryser on circulant Hadamard matrices ([3, 7]). However, the selection of non-symmetric circulant matrices $A, B, C, D$ may be found beyond our search domain (up to $n = 10$) so that $H$ given in (1) will become a Hadamard matrix.

## 3. Discussions and Conclusion

We note that in the searching process, we have taken symmetric circulant Williamson matrices, and the searching chain is limited up to order 10. From the search results for all the above-mentioned cases, it may be observed that Williamson matrices do not exist for orders 9 and 10. The distinct symmetric circulant matrices have been found only for orders 6 and 7. The Williamson matrices have been found for the orders 5, 7, and 8 in the case when $C = D$. Seberry and Bolonin [1] showed that such type of Williamson matrices exist for the order $\frac{q+1}{2}$ where $q$ is a prime power such that $q \equiv 1 \pmod 4$; the results obtained satisfy the conditions. The symmetric circulant Williamson matrices have been obtained only for the orders 2, 4, and 8 when $A = B$, $C = D$, indicating that this type of symmetric circulant Williamson matrices have an order of the form $2^n$, this case has been discussed in theorem 2 and the subsequent remark. Williamson Hadamard matrices with two distinct symmetric circulants have been obtained only for orders 3 and 4, it seems that there does not exist any symmetric circulant Williamson matrices of higher orders. In the case when $A = B = C = D$, we must have $A^2 = mI_m$ with symmetric circulant matrix $A$. So, $A$ will be a circulant Hadamard matrix, and, as per Ryser's conjecture [3, 9], there does not exist any circulant Hadamard matrix of order greater than 4, the reported outputs are supportive results for Ryser's conjecture.

[1] J. Seberry and N.A. Balonin, The Propus construction for symmetric Hadamard matrices, *arXiv: Combinatorics* (2015), DOI: 10.48550/arXiv.1512.01732.

In addition, the examples are clearly arranged on a platform for orders up to 10, the data will help researchers with multi-purpose applications in various disciplines.

## Competing Interests

The authors declare that they have no competing interests.

## Authors' Contributions

All the authors contributed significantly in writing this article. The authors read and approved the final manuscript.

## References


[1] C. Bright, I. Kotsireas and V. Ganesh, A SAT + CAS method for enumerating Williamson matrices of even order, in: *Proceedings of the AAAI Conference on Artificial Intelligence* **32** (2018), 6573 – 6580, DOI: 10.1609/aaai.v32i1.12203.

[2] C. Bright, I. Kotsireas and V. Ganesh, Applying computer algebra systems with SAT solvers to the Williamson conjecture, *Journal of Symbolic Computation* **100** (2020), 187 – 209, DOI: 10.1016/j.jsc.2019.07.024.

[3] R. Craigen, G. Faucher, R. Low and T. Wares, Circulant partial Hadamard matrices, *Linear Algebra and its Applications* **439** (2013), 3307 – 3317, DOI: 10.1016/j.laa.2013.09.004.

[4] D.Ž. Đoković, Williamson matrices of order $4n$ for $n = 33, 35, 39$, *Discrete Mathematics* **115**(1-3) (1993), 267 – 271, DOI: DOI: 10.1016/0012-365X(93)90495-F.

[5] J.S. Hadamard, Resolution d'une question relative aux determinants, *Bulletin des Sciences Mathematiques* **17**(1893), 240 – 246.

[6] W.H. Holzmann, H. Kharaghani and B. Tayfeh-Rezaie, Williamson matrices up to order 59, *Designs, Codes and Cryptography* **46** (2008), 343 – 352, DOI: 10.1007/s10623-007-9163-5.

[7] K.J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, Princeton, (2007), https://www.jstor.org/stable/j.ctt7t6pw.

[8] W. Lang and E. Schneider, Turyn type Williamson matrices up to order 99, *Designs, Codes and Cryptography* **62** (2012), 79 – 84, DOI: 10.1007/s10623-011-9492-2.

[9] P.K. Manjhi, Some results on the parameters of the general difference sets correspond to circulant partial Hadamard matrices, *Research in Mathematics* **9** (2022), Article number 2152961, DOI: 10.1080/27684830.2022.2152961.

[10] P.K. Manjhi and A. Kumar, On the construction of Hadamard matrices, *International Journal of Pure and Applied Mathematics* **120** (2018), 51 – 58.

[11] R. E. A. C. Paley, On orthogonal matrices, *Journal of Mathematics and Physics* **12**(1-4) (1933), 311 – 320, DOI: 10.1002/sapm1933121311.

[12] J. Seberry and M. Yamada, *Hadamard Matrices: Constructions using Number Theory and Algebra*, 1st edition, John Wiley and Sons, (2020), DOI: 10.1002/9781119520252.

[13] A. Sergeeva and A. Vostrikova, Calculating symmetrical Hadamard matrices of Balonin-Seberry construction for coding and masking, *Procedia Computer Science* **176** (2020), 1722 – 1728, DOI: 10.1016/j.procs.2020.09.197.

**[14]** M.K. Singh and P.K. Manjhi, Construction of Hadamard matrices from certain Frobenius groups, *Global Journal of Computer Science and Technology* **11** (2011), 45 – 50, https://computerresearch.org/index.php/computer/article/view/753.

**[15]** J. Sylvester, LX. Thoughts on inverse orthogonal matrices, simultaneous signsuccessions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers, *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* **34**(232) (1867), 461 – 475, DOI: 10.1080/14786446708639914.

**[16]** J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Mathematical Journal* **11** (1944), 65 – 81, DOI: 10.1215/S0012-7094-44-01108-7.