On the asymptotic existence of complex Williamson Hadamard matrices

H. Kharaghani
Department of Mathematics & Computer Science
University of Lethbridge
Lethbridge, Alberta, T1K 3M4
Canada

Abstract

It is shown that for each odd integer q, there is a complex Williamson-Hadamard matrix of order $2^{2^{n(q)+1}} \cdot 2^{n(q)+1} \cdot q$.

In a recent paper Craigen, Holzmann and Kharaghani [1] showed that for every odd integer q, there is an integer $N(q)$ which does not exceed twice the number of nonzero digits in the binary expansion of q, such that the existence of an Orthogonal Design (OD) of order $2^{N(q)-1}$ implies the existence of a Complex Orthogonal Design (COD) of the same number of variables and of order $2^{N(q)}q$. Although ODs of order 2^m for small values of m are known, not much is known when m is 7 or more. We first give a method of constructing some crucial ODs of order 2^m, for $m \geq 7$. Then we use these ODs and present a simple method of extending a classical method of Williamson [3] to any class of 2^m circulant ±1-matrices, leading to an asymptotic existence theorem for complex Williamson matrices.

A (Complex) Orthogonal Design of order n and type $(s_1, s_2, \ldots, s_k)$, s_i positive integers, denoted (C)OD$(n; s_1, s_2, \ldots, s_k)$, is a matrix X of order n, with entries in $\{0, \varepsilon x_1, \varepsilon x_2, \ldots, \varepsilon x_k\}$, $\varepsilon \in \{\pm1\}$ $(\varepsilon \in \{\pm1, \pm i\})$, satisfying $XX^* = \sum_{i=1}^{k} (s_i x_i^2) I_n$. A (complex) Hadamard matrix is a special (C)OD with $x_i = 1$, for all i and no zero entries. A set $\{A_1, A_2, \ldots, A_m\}$ of $(0, \pm1, \pm i)$-matrices of order n is called m-supplementary of weight w if $\sum_{i=1}^{m} A_i A_i^* = wI_n$. An m-supplementary set of circulant matrices of weight nm is called a set of m-complex Williamson matrices if $A_i = A_i^*$ for all i. A pair of matrices X, Y is called amicable (antiamicable) if $XY^* = YX^*$ $(XY^* = -YX^*)$. For integer $n = 2^c q$, q odd, write $c = 4a + b$, $0 \leq b < 4$. $\rho(n) = 8a + 2^b$ is called the Radon number of n. It is easy to see that $\rho(2^{2^{n+1}-1}q) = 2^{n+2}$, for any odd integer q.

Our main reference is [2] and we refer the reader to this reference for terminology not defined here.

We begin with a well known result.

Theorem 1 *For every positive integer n, there is an* $\mathrm{OD}(n; 1, 1, \ldots, 1)$ *in $\rho(n)$-variables. Equivalently, there are $\rho(n)$ $(0, \pm 1)$-matrices, $P_1, P_2, \ldots, P_{\rho(n)}$, of order n such that:*

(i) $P_i * P_j = 0, \quad i \neq j$

(ii) $P_i P_i^t = I$

(iii) $P_i P_j^t = -P_j P_i^t, \quad i \neq j$.

PROOF. See page 2 of [2]. ∎

Following Craigen, $(0, \pm 1)$-matrices satisfying (ii) above are called signed permutations. For matrices A_1, A_2, let $L_2(A_1, A_2) = \begin{pmatrix} A_1 & A_2 \\ A_2 & A_1 \end{pmatrix}$. Inductively, for $k > 1$ and matrices $A_1, A_2, \ldots, A_{2^k}$, let

$$L_{2^k}(A_1, A_2, \ldots, A_{2^k}) = L_2(L_{2^{k-1}}(A_1, A_2, \ldots, A_{2^{k-1}}), L_{2^{k-1}}(A_{2^{k-1}+1}, \ldots, A_{2^k})).$$

For example,

$$L_{2^2}(A_1, A_2, A_3, A_{2^2}) = L_2(L_2(A_1, A_2), L_2(A_3, A_{2^2})) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2 & A_1 & A_4 & A_3 \\ A_3 & A_4 & A_1 & A_2 \\ A_4 & A_3 & A_2 & A_1 \end{pmatrix}.$$

We call such a matrix an L_{2^k}-matrix constructed from 2^k matrices $A_1, A_2, \ldots, A_{2^k}$. Obviously, different ordering of A_i's give different L_{2^k}-matrices.

Lemma 2 *Let $\{P_1, P_2, \ldots, P_{2^k}\}$, k a positive integer, be a set of mutually anti-amicable signed permutations of order n. Let H be an Hadamard matrix of order n. Then any L_{2^k}-matrix constructed from 2^k matrices $x_1P_1H, x_2P_2H, \ldots, x_{2^k}P_{2^k}H$, is an* $\mathrm{OD}(2^k n; n, n, \ldots, n)$ *in 2^k-variables.*

PROOF. We use induction on k. For $k = 1$, note that $(x_iP_iH)(x_iP_iH)^t = nx_i^2 I_n$, so x_iP_iH is an $\mathrm{OD}(n; n)$ for all i. P_1, P_2 are antiamicable, so are x_1P_1H, x_2P_2H. Hence $L_2(x_1P_1H, x_2P_2H)$ is an $\mathrm{OD}(2n; n, n)$.

Assume that $X = L_{2^\ell}(x_1P_1H, x_2P_2H, \ldots, x_{2^\ell}P_{2^\ell}H)$ and $Y = L_{2^\ell}(x_{2^\ell+1}P_{2^\ell+1}H, \ldots, x_{2^{\ell+1}}P_{2^{\ell+1}}H)$ are $\mathrm{OD}(2^\ell n; n, n, \ldots, n)$. It follows now from the assumption on the P_i's that X and Y are antiamicable ODs. So $L_{2^{\ell+1}}(x_1P_1H, \ldots, x_{2^{\ell+1}}P_{2^{\ell+1}}H)$ is an $\mathrm{OD}(2^{\ell+1}n; n, n, \ldots, n)$ in $2^{\ell+1}$-variables. ∎

Theorem 3 *Let the P_i's and H be as in Lemma 2. Assume further that $P_{2i} * P_{2i-1} = 0$, $i = 1, 2, \ldots, 2^{k-1}$. Then any L_{2^k}-matrix constructed from 2^{k-1} matrices $\{A_i = \frac{1}{2}a_{2i}(P_{2i} + P_{2i-1})H + \frac{1}{2}a_{2i-1}(P_{2i} - P_{2i-1})H\}_{i=1}^{2^{k-1}}$ is an $\mathrm{OD}(2^{k-1}n; \frac{n}{2}, \frac{n}{2}, \ldots, \frac{n}{2})$ in 2^k-variables.*

PROOF. Note that the set $\{P_{2i} + P_{2i-1}, P_{2i} - P_{2i-1}\}_{i=1}^{2^{k-1}}$ is a mutually antiamicable set of $(0, \pm 1)$-matrices and $(\frac{a}{2}(P_{2i}+P_{2i-1})H + \frac{b}{2}(P_{2i} - P_{2i-1})H)\ (\frac{a}{2}(P_{2i}+P_{2i-1})H + \frac{b}{2}(P_{2i} - P_{2i-1})H)^t = \frac{1}{2}(a^2 + b^2)nI_n$, $i = 1, 2, \ldots, 2^{k-1}$. The rest follows from Lemma 2. ∎

Theorem 4 *For each positive integer n, there is an $\mathrm{OD}(2^{2^{n+1}-1} \cdot 2^{n+1}; a, a, \ldots, a)$ in 2^{n+2}-variables, which is an $L_{2^{n+1}}$-matrix constructed from 2^{n+1} antiamicable matrices.*

PROOF. Apply Theorem 3 to any Hadamard matrix of order $2^{2^{n+1}-1}$ and signed permutation matrices of order $2^{2^{n+1}-1}$ obtained from Theorem 1. ∎

REMARKS. (i) While Theorem 4 does not give ODs of new order for $n = 1$, all ODs obtained have special structures. All the ODs, for $n > 1$, obtained from Theorem 3 are new.

(ii) The existence of $\mathrm{OD}(2; 1, 1)$, $\mathrm{OD}(4; 1, 1, 1, 1)$ and $\mathrm{OD}(8; 1, 1, 1, 1, 1, 1, 1, 1)$ leads one to the following conjecture.

Conjecture *All full (no zero entries) $\mathrm{OD}(2^{2^{n+1}-1}; a, a, \ldots, a)$ in 2^{n+2}-variables exist, $n \geq 1$.*

The conjecture is only known for $n = 1$. It is easy to see that any OD of the above type will not be constructible from antiamicable ODs as in Theorem 4.

Next we show a method to "replace" every ± 1-circulant matrix with two Hermitian $(\pm 1, \pm i)$-circulant ones. Let A be a normal ± 1-matrix. Let $B = \frac{1}{2}(A + A^t)$, $C = \frac{i}{2}(A - A^t)$. Then B, C are disjoint Hermitian $(0, \pm 1, \pm i)$-matrices of the same order as A. Furthermore, $BB^* + CC^* = AA^t$, $BC = CB$. Let $B_1 = B + C$, $C_1 = B - C$, then B_1, C_1 are commuting $(\pm 1, \pm i)$-matrices and $B_1 B_1^* + C_1 C_1^* = 2AA^t$.

Noting that every circulant matrix is normal, we have the following.

Lemma 5 *Given m-supplementary circulant ± 1-matrices of order n, there are $2m$-supplementary circulant $(\pm 1, \pm i)$-Hermitian matrices of order n.*

PROOF. Let $\{A_1, A_2, \ldots, A_m\}$ be a supplementary set of circulant ± 1-matrices of order n. Let B_i, C_i be the matrices corresponding to A_i as above for each $1 \leq i \leq m$. The lemma is now immediate. ∎

$(0, \pm 1)$-matrices with zero non-periodic autocorrelations are called complementary matrices. There are plenty of such matrices, see [2] for details. Complementary matrices are special cases of supplementary matrices. The most elementary method of constructing complementary matrices is to use Golay sequences of length 2^n. In order to show the asymptotic existence of complex Williamson matrices we need the following simple lemma.

Lemma 6 *Let q be an odd integer. Let $n(q)$ be the smallest integer such that the number of nonzero terms in the binary expansion of q does not exceed $2^{n(q)}$. Then*

$$q = \sum_{i=1}^{2^{n(q)}} 2^{\alpha_i}, \quad \alpha_i \geq 0.$$

PROOF. Let $q = 1 + \sum_{i=1}^{k} 2^{\beta_i}, \quad 0 < \beta_1 < \beta_2 < \ldots < \beta_k$. Then by the choice of $n(q)$ $2^{n(q)-1} < k+1 \leq 2^{n(q)}$. Let $j = 2^{n(q)} - k - 1$, and write $2^{\beta_k} = 2^{\beta_k - 1} + 2^{\beta_k - 2} + \ldots + 2^{\beta_k - j} + 2^{\beta_k - j}$. Then $q = 1 + 2^{\beta_1} + 2^{\beta_2} + \ldots + 2^{\beta_{k-1}} + \ldots + 2^{\beta_k - 1} + \ldots + 2^{\beta_k - j} =$ a sum of $2^{n(q)}$ terms. ∎

For ± 1-sequences $A, B, C, \ldots$, as usual, let $ABC\ldots$ denote the longer sequence A followed by B, C and so on. Let $\bar{A}$ be the negative of all elements of A.

Lemma 7 *For odd integer q, let $n(q)$ be as in Lemma 5. Then there is a $2^{n(q)+1}$-complementary sequence of ± 1-circulant matrices of order q, constructed from Golay sequences of length 2^k, $k \geq 0$.*

PROOF. Let $q = \sum_{i=1}^{2^{n(q)}} 2^{\alpha_i}, \quad \alpha_1 = 0, \ \alpha_i > 0$. Let A_k, B_k be a Golay sequence of length 2^{α_k}, taking $A_1 = (1)$, $B_1 = (1)$. Let e be the $2^{n(q)}$-dimensional column vector of ones, H an Hadamard matrix of order $2^{n(q)}$ and $A = (A_1, A_2, \ldots, A_{2^{n(q)}})$, $B = (B_1, B_2, \ldots, B_{2^{n(q)}})$ the $2^{n(q)}$-dimensional row vectors. Consider the matrices $(eA) * H$ and $(eB) * H$, where $*$ is the Hadamard product. Consider a circulant ± 1-matrix whose first row is one row from either of $(eA) * H$ or $(eB) * H$. There are $2^{n(q)+1}$ such matrices of order q. This gives the desired matrices. ∎

Lemma 8 *Let q be an odd integer. Then there is a set of $2^{n(q)+2}$-complex Williamson matrices of order q.*

PROOF. By Lemma 7, there is a $2^{n(q)+1}$-complementary sequence of ± 1-circulant matrices of order q. By applying Lemma 5, we thus get $2^{n(q)+2}$-supplementary $(\pm 1, \pm i)$-circulant Hermitian matrices of order q. ∎

Theorem 9 *Let q be an odd integer. Then there is a complex Williamson-Hadamard matrix of order $2^{2^{n(q)+1}} \cdot 2^{n(q)+1} \cdot q$.*

PROOF. By Theorem 4, there is an $OD(2^{2^{n(q)+1}-1} \cdot 2^{n(q)+1}; a, \ldots, a)$ in $2^{n(q)+2}$-variables. Replace the variables by the Williamson matrices obtained in Lemma 8, to get the desired Hadamard matrix. ∎

Let $q = 11$, and write $+ = 1$, $- = -1$. Note $11 = 1 + 2 + 2^3 = 1 + 2 + 2^2 + 2^2$, so $n(11) = 2$. Now,

$$A_1 = (+), \quad B_1 = (+),$$
$$A_2 = (++), \quad B_2 = (+-),$$
$$A_3 = A_4 = (+++-), \quad B_3 = B_4 = (++-+),$$
$$A = (A_1, A_2, A_3, A_4), \quad B = (B_1, B_2, B_3, B_4),$$

$$H = \begin{pmatrix} + & + & + & + \\ + & - & - & + \\ + & - & + & - \\ + & + & - & - \end{pmatrix},$$

$$(eA) * H = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_1 & \bar{A}_2 & \bar{A}_3 & A_4 \\ A_1 & \bar{A}_2 & A_3 & \bar{A}_4 \\ A_1 & A_2 & \bar{A}_3 & \bar{A}_4 \end{pmatrix}, \quad (eB) * H = \begin{pmatrix} B_1 & B_2 & B_3 & B_4 \\ B_1 & \bar{B}_2 & \bar{B}_3 & B_4 \\ B_1 & \bar{B}_2 & B_3 & \bar{B}_4 \\ B_1 & B_2 & \bar{B}_3 & \bar{B}_4 \end{pmatrix}.$$

$$\begin{aligned}
A_1A_2A_3A_4 &= (++++++-+++-) = a_1 \\
A_1\bar{A}_2\bar{A}_3A_4 &= (+-----++++-) = a_2 \\
A_1\bar{A}_2A_3\bar{A}_4 &= (+--+++----+) = a_3 \\
A_1A_2\bar{A}_3\bar{A}_4 &= (+++---+---+) = a_4 \\
B_1B_2B_3B_4 &= (++-++-+++-+) = a_5 \\
B_1\bar{B}_2\bar{B}_3B_4 &= (+-+--+-++-+) = a_6 \\
B_1\bar{B}_2B_3\bar{B}_4 &= (+-+++-+--+-) = a_7 \\
B_1B_2\bar{B}_3\bar{B}_4 &= (++---+---+-) = a_8.
\end{aligned}$$

From each of the a_i we get two Hermitian circulant matrices, but we show only the first two.

$$\tfrac{1}{2}(a_1 + a_1^t) = (+0+++00+++0), \quad \tfrac{1}{2}(a_1 - a_1^t) = (0+000+-000-).$$

So, $(+i+++i\bar{i}+++\bar{i})$ and $(+\bar{i}+++\bar{i}i+++i)$ are the two $(\pm 1, \pm i)$-Hermitian matrices corresponding to a_1.

Continuing this process we get 16 $(\pm 1, \pm i)$-circulant Hermitian matrices. Replacing the variables in $OD(2^{10}; 2^6, \ldots, 2^6)$ in 2^4-variables by these Hermitian matrices, we get a complex Williamson matrix of order $2^{10} \cdot 11$. If the conjecture in this paper was correct, then we would have had a complex Williamson matrix of order $2^7 \cdot 11$. ∎

The following result shows a great advantage of the construction method used in this paper.

Theorem 10 *Let p, q be odd integers with $n(p) = n(q)$. If $2^{2^{n(p)+1}-1} \cdot p$ is the order of an Hadamard matrix, then there is a complex Williamson Hadamard matrix of order $2^{2^{n(p)+1}-1} \cdot 2^{n(p)+1} \cdot pq$.*

PROOF. Apply Theorem 3 to the Hadamard matrix of order $2^{2^{n(p)+1}-1} \cdot p$ and the signed permutation matrices of order $2^{2^{n(p)+1}-1} \cdot p$ obtained from Theorem 1, to get an $OD(2^{2^{n(p)+1}-1} \cdot 2^{n(p)+1} \cdot p;\ a, a, \ldots, a)$ in $2^{n(p)+2}$-variables. Now, replace the variables by the complex Williamson matrices of Lemma 8. ∎

Acknowledgements. This work is supported by an NSERC grant. The author wishes to thank Rob Craigen for useful discussions.

References

[1] R. Craigen, W. H. Holzmann and H. Kharaghani, On the asymptotic existence of complex Hadamard matrices, in preparation.

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

[3] J. Williamson, Hadamard's determinant theorem and sum of four squares, *Duke. Math. J.* **11** (1944), 65–81.

(Received 1/3/94)