On the multiplication theorems of Hadamard matrices of generalized quaternion type using M-structures[1]

Jennifer Seberry
Department of Computer Science
The University of Wollongong
Wollongong, NSW, 2500
Australia

and

Mieko Yamada
Department of Mathematics
Kyushu University
Fukuoka 812
Japan

Abstract. We show that M-structures can be extended to Hadamard matrices of *generalized quaternion type* and obtain multiplication type theorems which preserve the structure.

1. Introduction

The concept of M-structures generalizes a number of concepts in Hadamard matrices, including Williamson matrices, Goethals-Seidel matrices, Wallis-Whiteman matrices and generalized quaternion matrices. We found many symmetric Williamson matrices and many Hadamard matrices using the concept of M-structures [4], [5], [6]. Furthermore, the concept of M-structures leads to the new concept of strong Kronecker products introduced by Jennifer Seberry and Xian-mo Zhang [8]. This was used by Craigen, Seberry and Zhang [1] to prove that if there exist Hadamard matrices of orders $4p$, $4q$, $4r$, and $4s$, then we have an Hadamard matrix of order $16pqrs$.

An orthogonal matrix of order $4t$ can be divided into sixteen $t \times t$ blocks M_{ij}. This partitioned matrix is said to be an *M-structure*. If the orthogonal matrix can be partitioned into sixty-four blocks M_{ij}, it will be called a 64 block M-structure.

First we give some definitions.

Definition 1: The matrices X and Y are said to be *amicable matrices* if

$$XY^t = YX^t,$$

where X^t and Y^t are the transpose matrices of X and Y respectively.

Definition 2: *Williamson matrices* of order w are four circulant symmetric matrices A, B, C, D which have entries 1 or -1 and which satisfy

$$AA^t + BB^t + CC^t + DD^t = 4wI_w$$

where I_w is a unit matrix of order w.

[1] Written while Professor Seberry was on faculty at the Center for Communication and Information Science, the Department of Electrical Engineering and the Department of Computer Science and Engineering, University of Nebraska-Lincoln, NE 68588-0502, U.S.A. This research was funded by Telecom grant 7027, ARC grant A48830241 and an ATERB grant.

Definition 3: *Williamson-type matrices* of order w are four pairwise amicable matrices A, B, C, D which have entries 1 or -1 and which satisfy

$$AA^t + BB^t + CC^t + DD^t = 4wI_w.$$

A generalized quaternion group Q_s, of order 2^{s+2} is a group generated by the two elements ρ, j such that

$$\rho^{2^{s+1}} = 1,\ j^2 = \rho^{2^s},\ j\rho j^{-1} = \rho^{-1}.$$

Let G be a semi-direct product of a cyclic group of an odd order n by the generalized quaternion group Q_s of order 2^{s+2}. That is, G is generated by ρ, ξ and j with the relations

$$\rho^{2^s} = -1,\ j^2 = -1,\ j\rho j^{-1} = \rho^{-1},\ \rho\zeta\rho^{-1} = \zeta,\ j\zeta j^{-1} = \zeta^{-1},\ \zeta^n = 1.$$

We consider the ring $\mathcal{R}$ obtained from the group ring $\mathbf{Z}G$ by identifying the elements ± 1 in the center of Q_s with ± 1 of the rational integer ring $\mathbf{Z}$. Put $\mathcal{H} = \{p^k\zeta^l : 0 \leq k \leq 2^s - 1, 0 \leq l \leq n-1\}$ and choose the basis $\mathcal{L} = \mathcal{H} \cup \mathcal{H}j$ of $\mathcal{R}$. An element ξ in $\mathcal{R}$ takes the fo]lowing form.

$$\xi = \sum_{k=0}^{2N-1}\sum_{l=0}^{n-1} a_{k,l}\zeta^l\rho^k + \sum_{k=0}^{2N-1}\sum_{l=0}^{n-1} b_{k,l}\zeta^l\rho^k j = \alpha + \beta j,\ N = 2^{s-1}, \qquad (1)$$

where

$$\alpha = \sum_{k=0}^{2N-1}\sum_{l=0}^{n-1} a_{k,l}\zeta^l\rho^k \text{ and } \beta = \sum_{k=0}^{2N-1}\sum_{l=0}^{n-1} b_{k,l}\zeta^l\rho^k.$$

We define the conjugate $\xi = \overline{\alpha} - \beta j$ of $\xi = \alpha + \beta j$ based on the automorphism $\tau : \rho \to \rho^{-1}, \zeta \to \zeta^{-1}$ of G. Furthermore, we define the norm $\mathcal{N}(\xi) = \xi\overline{\xi}$ so that:

$$\mathcal{N}(\xi) = \alpha\overline{\alpha} + \beta\overline{\beta}$$
$$\mathcal{N}(\xi\eta) = \mathcal{N}(\xi)\mathcal{N}(\eta) \text{ for } \xi, \eta \in \mathcal{R}.$$

For an arbitrary element $\xi \in \mathcal{R}$ we construct the right regular representation matrix $R(\xi)$, defined by

$$(\rho^k\zeta^l\xi) = R(\xi)(\rho^k\zeta^l).$$

More precisely, for an element ξ of $\mathcal{R}$ with the form (1) the right regular representation matrix $R(\xi)$ is given by

$$R(\xi) = \begin{pmatrix} \mathcal{A} & \mathcal{B} \\ -\mathcal{B}^t & \mathcal{A}^t \end{pmatrix}$$

$$A = \begin{pmatrix} A_0 & A_1 & \cdots & A_{2N-1} \\ -A_{2N-1} & A_0 & \cdots & A_{2N-2} \\ \vdots & \vdots & & \vdots \\ -A_1 & -A_2 & \cdots & A_0 \end{pmatrix}$$

$$B = \begin{pmatrix} B_0 & B_1 & \cdots & B_{2N-1} \\ -B_{2N-1} & B_0 & \cdots & B_{2N-2} \\ -B_{2N-2} & B_{2N-1} & \cdots & B_{2N-3} \\ \vdots & \vdots & & \vdots \\ -B_1 & -B_2 & \cdots & B_0 \end{pmatrix}$$

where $A_k = \sum_{l=0}^{n-1} a_{k,l}T^l$ and $B_k = \sum_{l=0}^{n-1} a_{k,l}T^l$ are the circulant matrices of order n where T denotes the basic circulant matrix of order n

$$T = \begin{pmatrix} 0 & 1 & 0 & & & & 0 \\ 0 & 0 & 1 & & & & 0 \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Since $R(\xi) = R(\xi)^t$, we have

$$R(\xi)R(\xi) = R(\xi)R(\bar{\xi}) = R(\xi\bar{\xi}) = \begin{pmatrix} AA^t + BB^t & 0 \\ 0 & AA^t + BB^t \end{pmatrix}$$

Definition 4: If an element in $\mathcal{R}$ which is given by the equation (1) above satisfies

(i) all the coefficients $a_{k,l}, b_{k,l}$ are from $\{1, -1\}$ and

(ii) $\mathcal{N}(\xi) = 2^{s+1}n = 4nN$,

then the right regular representation matrix $R(\xi)$ becomes an Hadamard matrix of order $2^{s+1}n = 4nN$, which is called an *Hadamard matrix of generalized quaternion type.*

Similarly, if the following conditions are satisfied:

(iii) $a_{k,k} = 0$ and all other coefficients $a_{k,l}, b_{k,l}$ are from $\{1, -1\}$ and

(iv) $\mathcal{N}(\xi) = 2^{s+1}n - 1 = 4nN - 1$,

then $R(\xi)$ is a C-matrix of order $2^{s+1}n = 4nN$, which we call a *C-matrix of generalized quaternion type.*

We abbreviate *generalized quaternion type* as GQ *type* for convenience sake.

Let us express the conditions (i), (ii) in terms of the component matrices A_k, and B_k:

$$\sum_{k=0}^{2N-1} A_k A_k^t + \sum_{k=0}^{2N-1} B_k B_k^t = 4nNI,$$

$$\sum_{k=0}^{t-1}(A_k A_{2N-t+k}^t + B_{2N-t+k}^t) - \sum_{k=0}^{2N-t-1} (A_k^t A_{k+t} + B_k^t B_{k+t}) = 0 \text{ for } 1 \le t \le 2N-1.$$

In particular, in the case $N = 1$ the conditions will become

$$A_0A_0^t + A_1A_1^t + B_0B_0^t + B_1B_1^t = 4nI,$$
$$A_0A_1^t - A_1A_0^t + B_0B_1^t + B_1B_0^t = 0.$$

Moreover, suppose that A_0, A_1, B_0 and B_1 are symmetric, that is, Williamson matrices, or suppose they are pairwise amicable, that is, Williamson-type matrices, then the second condition is trivial.

2. M-structure Hadamard matrices

We consider Hadamard matrices of GQ type as an M-structure. Namely, an Hadamard matrix H of GQ type is partitioned into sixteen blocks,

$$H = \begin{pmatrix} A & B \\ -B^t & A^t \end{pmatrix} = \begin{pmatrix} C_0 & C_1 & D_0 & D_1 \\ -C_1 & C_0 & -D_1 & D_0 \\ -D_0^t & D_1^t & C_0^t & -C_1^t \\ -D_1^t & -D_0^t & C_1^t & C_0^t \end{pmatrix} \tag{3}$$

where

$$C_0 = \begin{pmatrix} A_0 & A_1 & \cdots & A_{N-1} \\ -A_{2N-1} & A_0 & \cdots & A_{N-2} \\ -A_{N+1} & -A_{N+2} & \cdots & A_0 \end{pmatrix}, \quad C_1 = \begin{pmatrix} A_N & A_{N+1} & \cdots & A_{2N-1} \\ -A_{N-1} & A_N & \cdots & A_{2N-2} \\ -A_1 & -A_2 & \cdots & A_N \end{pmatrix},$$
$$D_0 = \begin{pmatrix} B_0 & B_1 & \cdots & B_{N-1} \\ -B_{2N-1} & B_0 & \cdots & B_{N-2} \\ -B_{N+1} & -B_{N+2} & \cdots & B_0 \end{pmatrix}, \quad D_1 = \begin{pmatrix} B_N & B_{N+1} & \cdots & B_{2N-1} \\ -B_{N-1} & B_N & \cdots & B_{2N-2} \\ -B_1 & -B_2 & \cdots & B_N \end{pmatrix},$$

Since H is an Hadamard matrix, the component matrices C_0, C_1, D_0, D_1 satisfy the following equations,

$$\begin{cases} C_0C_0^t + C_1C_1^t + D_0D_0^t + D_1D_1^t = C_0^tC_0 + C_1^tC_1 + D_0^tD + 0 + D_1^tD_1 = 4nNI \\ C_0C_1^t - C_1C_0^t + D_1D_1^t - D_1D_0^t = C_0^tC_1 - C_1^tC_0 + D_0^tD_1 - D_1^tD_0 = 0 \\ C_0D_0 - C_1D_1 - D_0C_0 + D_1C_1 = 0 \\ C_0D_1 + C_1D_0 - D_0C_1 - D_1C_0 = 0 \end{cases} \tag{4}$$

An Hadamard matrix having the form (3) will be called an *M-structure Hadamard matrix of* GQ *type*.

3. Paley type 1 matrix

The Paley type 1 matrix can be changed into the form of a C-matrix of GQ type and is defined as follows (see [3]).

Definition 5: Let q be a prime power, $q \equiv 3 \pmod 4$, $F = GF(q)$ the finite field of q elements, $K = GF(q^2)$ a quadratic extension over F, and $K^\times$ and $F^\times$ the multiplicative groups of K and F respectively. Furthermore, let η be a generator of $K^\times$, $\gamma = \eta^{(q+1)/2}$ and let $N_{K/F}$ and $S_{K/F}$ denote the relative norm and relative trace from K to F respectively. Denote by ψ the quadratic character of F. Then the matrix

$$P = (\psi(N_{K/F}\alpha)\psi(S_{K/F}\gamma^{-1}\beta\alpha^{-1}))_{\alpha,\beta\in K^\times/F^\times}$$

is called the *Paley type 1 matrix.*

We recall here the definition of Seidel-equivalence of matrices.

Definition 6: If a square matrix A can be obtained from a square matrix B by a sequence of two kinds of operations:

(i) multiplying the row and the corresponding column by -1 simultaneously,
(ii) interchanging two rows and the corresponding two columns simultaneously,

then A will be said to be *Seidel-equivalent* to B.

Theorem 1. *The Paley type 1 matrix is Seidel equivalent to a C-matrix of* GQ *type with some additional properties:*

(i) *A is skew symmetric;*
(ii) *$B_{2N-m-1} = -B_m^t$ for $m = 0, \ldots, N-1$ where $q+1 = 2^{s+1}n$, $s \geq 1$, n odd, $N = 2^{s+1}$.*

Proof: See [11]. ∎

4. Infinite series of Hadamard matrices of generalized quaternion type

Yamada constructed some infinite series of Hadamard matrices of GQ type [11]. In this section we show these constructions of finite series.

Let q be a power of a prime p, $F = GF(q)$ denote a finite field of q elements, $K = GF(q^t)$ an extension of F of degree t, $t \geq 2$. Let η be a generator of $K^\times$ and let S_K and S_F denote the absolute trace in K and F. Furthermore, let $S_{K/F}$ and $N_{K/F}$ be the relative trace and relative norm from K to F respectively.

Definition 7: Let χ be a character of F and $\zeta_p = e^{2\pi i/p}$, then the Gauss sum $\tau_F(\chi)$ is defined by

$$\tau_f(\chi) = \sum_{\alpha\in F} \chi(\alpha)\zeta_p^{S_F\alpha}.$$

If χ is a nonprincipal character of K, then the ratio

$$\theta_\chi = \frac{\tau_K(\chi)}{\tau_F(\chi)}$$

of two Gauss sums is called the *relative Gauss sum associated with* χ.

The following theorem on the relative Gauss sum is very useful.

Theorem 2. *Suppose that χ is a character of K inducing in F a nonprincipal character. Then the relative Gauss sum associated with χ can be written in the following form*

$$\theta_\chi = \sum_{\alpha \in K^\times / F^\times} \chi(\alpha)\overline{\chi}(S_{K/F}\alpha),$$

and we have the norm relation

$$\theta_\chi \overline{\theta}_\chi = q^{t-1}.$$

Proof: See [11]. ∎

Using Theorem 2 for the case $t = 2$, we give infinite series of Hadamard matrices of GQ type.

Theorem 3. *Let $q + 1 = 2^s n$, $s \geq 2$, n odd, ρ a primitive 2^{s+1} th root of unity and w an arbitrary nth root of unity. Put $\chi = \chi_{2^{s+1}}\chi_n$ where $\chi_{2^{s+1}}(\eta) = \rho$, $\chi_n(\eta) = w$, so that χ induces a quadratic character ψ in F.*

Then for the relatite Gauss sum θ_χ we have

$$\theta_\chi = \alpha + \beta\rho^n \quad \alpha, \beta \in \mathbf{Z}[\rho^2, w],$$

and the right regular representation matrix of

$$\gamma = \alpha \pm i + \beta j$$

gives an Hadamard matrix of GQ type of order $2^s n$ where i is a primitive fourth root of unity.

Proof: See [11]. ∎

Corollary 1. *Let α, β be as in Theorem 3. Then the right regular representation matrix of*

$$\gamma = (\alpha - i + \beta\rho^n j)(1 - j) = (1 - j)(\theta_\chi + ij)$$

is an Hadamard matrix of GQ type of order $2^{s+1} n$. In particular, if $s = 1$ then we get an Hadamard matrix of Turyn's type [9], [10].

Proof: See [11]. ∎

Theorem 4. *Let $q + 1 = 2n$, n odd and ρ a primitive octic root of unity. Let η and w, be as in Theorem 3. Put $\chi = \chi_8\chi_n$, $\chi_8(\eta) = \rho$. So that χ induces a biquadratic character in F.*

The right regular representation matrix of

$$\tau = (\theta_\chi + \rho^t j)(1 + i)(1 + j),\ t = 1, 3, 5, 7,$$

gives an Hadamard matrix of GQ type of order $8n$. We may change the order of factors $\theta_\chi + \rho^t j$, $1 + i$ and $1 + j$ arbitrarily.

Proof: See [11]. ∎

On the other hand, if there exists an Hadamard matrix of GQ type of order $2^s n$, we can double its order.

Theorem 5. *Assume that the right regular representation matrix of* $\xi = \alpha + \beta j$ *in* $\mathcal{R}$ *is an Hadamard matrix of* GQ *type of order* $2^s n$. *Let* ρ *be a primitive* 2^{s+1} *th root of unity. Then*

$$\gamma = (\alpha + \beta j)(1 + \rho^t j) \text{ for } t = 1, 3, 5, \ldots, 2^s - 1,$$

generates an Hadamard matrix of GQ *type of order* $2^{s+1} n$. *We can exchange the order of two factors* $\alpha + \beta j$ *and* $1 + \rho^t j$.

Proof: See [11]. ∎

5. Main theorems

Theorem 6. *Let* H *be an* M*-structure Hadamard matrix of* GQ *type of order* $4n$,

$$H = \begin{pmatrix} C_0 & C_1 & D_0 & D_1 \\ -C_1 & C_0 & -D_1 & D_0 \\ -D_0^t & D_1^t & C_0^t & -C_1^t \\ -D_1^t & -D_0^t & C_1^t & C_0^t \end{pmatrix}.$$

Furthermore, let T_0, T_1, T_2 *and* T_3 *be matrices of order* m *which have entries* $0, 1$ *or* -1 *which satisfy*

(i) $T_i \wedge T_j, i \neq j$ ($\wedge$ *the Hadamard product*);
(ii) $\sum_{i=0}^{3} T_i$ *is a matrix whose entries are* ± 1 *or* -1;
(iii) $\sum_{i=0}^{3} T_i T_i^t = \sum_{i=0}^{3} T_i^t T_i = m I_m$;
(iv) $T_0 T_1^t - T_1 T_0^t + T_2 T_3^t - T_3 T_2^t = T_0^t T_1 - T_1^t T_0 + T_2^t T_3 - T_3^t T_2 = 0$,
$T_0 T_2 - T_2 T_0 - T_1 T_3 + T_3 T_1 = T_0 T_3 - T_3 T_0 + T_1 T_2 - T_2 T_1 = 0$.

Then we have an M*-structure Hadamard matrices of* GQ *type of* $4nm$.

Proof: We define the matrices α, β, γ and δ as follow.

$$\alpha = T_0 \times C_0 - T_1 \times C_1 - T_2 \times D_0^t - T_3 \times D_1^t,$$
$$\beta = T_0 \times C_1 + T_1 \times C_0 + T_2 \times D_1^t - T_3 \times D_0^t,$$
$$\gamma = T_0 \times D_0 - T_1 \times D_1 + T_2 \times C_0^t + T_3 \times C_1^t,$$
$$\delta = T_0 \times D_1 + T_1 \times D_0 - T_2 \times C_1^t + T_3 \times C_0^t,$$

It is easily verified that α, β, γ and δ satisfy the equation (4). Hence

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta \\ -\beta & \alpha & -\delta & \gamma \\ -\gamma^t & \delta^t & \alpha^t & -\beta^t \\ \delta^t & -\gamma^t & \beta^t & \alpha^t \end{pmatrix}$$

is an M-structure Hadamard matrix of GQ type of order $4nm$. ∎

Corollary 2. *Let q be a prime power and $q+1 = 2^s n$, n odd. Let $m_1, \dots, m_r$, be the orders of Williamson matrices or type 1 Williamson type matrices. Then*

(i) *when $s \geq 2$, there exists an M-structure Hadamard matrix of* GQ *type of order $2^r m_1 \dots m_r(q+1) = 2^{r+s} r_1 \dots m_r n$;*

(ii) *when $s = 1$, there exists an M-structure Hadamard matrix of* GQ *type of order $2^{r+1} m_1 \dots m_r(q+1) = 2^{r+2} m_1 \dots m_r n$.*

Proof: From Theorems 1 and 3 there exists an M-structure Hadamard matrix of GQ type of order $2^s n$. From Corollary 1 an M-structure of Hadamard matrix of GQ type of order $4n$ exists. Let W_1, W_2, W_3 and W_4 be Williamson matrices of order m or type 1 Williamson-type matrices of order m. Put

$$X_1 = 2(W_1+W_2), X_2 = \frac{1}{2}(W_1-W_2), Y_1 = \frac{1}{2}(W_3+W_4), Y_2 = \frac{1}{2}(W_3-W_4).$$

Further, put

$$T_0 = \begin{pmatrix} X_1 & \\ & X_1 \end{pmatrix}, T_1 = \begin{pmatrix} X_2 & \\ & X_2 \end{pmatrix}, T_2 = \begin{pmatrix} & Y_1 \\ Y_1 & \end{pmatrix}, T_3 = \begin{pmatrix} & Y_2 \\ Y_2 & \end{pmatrix},$$

then T_0, T_1, T_2, T_3 satisfy the conditions of Theorem 6. ∎

Theorem 7. *Let H be an M-structure Hadamard matrix of* GQ *type of order $4n$,*

$$H = \begin{pmatrix} C_0 & C_1 & D_0 & D_1 \\ -C_1 & C_0 & -D_1 & D_0 \\ -D_0^t & D_1^t & C_0^t & -C_1^t \\ -D_1^t & -D_0^t & C_1^t & C_0^t \end{pmatrix}.$$

Furthermore, let T_0 and T_1 be the matrices of order m which have entries $0, 1$ or -1 and satisfy

(i) $T_0 \wedge T_1 = 0$, *($\wedge$ the Hadamard product);*

(ii) $T_0 + T_1$ *is a matrix which has entries 1 or -1;*

(iii) $T_0 T_0^t + T_1 T_1^t = T_0^t T_0 + T_1^t T_1 = mI$;

(iv) $T_0 T_1^t - T_1 T_0^t = T_0^t T_1 - T_1^t T_0 = 0$.

Then we have an M-structure Hadamard matrix of GQ *type of order $4nm$.*

Proof: We define the matrices $\alpha, \beta \gamma$ and δ as follows.

$$\alpha = T_0 \times C_0 - T_1 \times C_1,$$
$$\beta = T_0 \times C_1 + T_1 \times C_0$$
$$\gamma = T_0 \times D_0 - T_1 \times D_1$$
$$\delta = T_0 \times D_1 + T_1 \times D_0$$

Then, α, β, γ and δ satisfy the equation (4). ∎

Corollary 3. *Let q be a prime power and $q+1 = 2^s n$, n odd. Let p_i be a prime power and $p_i \equiv 1 \pmod 4$ for $1 \le i \le r$. Then*

(i) *when $s \ge 2$ there exists an M-structure Hadamard matrix of* GQ *type of order $(p_1+1)(p_2+1)\ldots(p_r+1)(q+1)$;*

(ii) *when $s = 1$ there exists an M-structure Hadamard matrix of* GQ *type of order $2(p_1+1)(p_2+1)\ldots(q+1)$.*

Proof: An Hadamard matrix of order $2(p_i+1)$ obtained from the Paley type 2 matrix has a form

$$\begin{pmatrix} X & Y \\ Y & -X \end{pmatrix}.$$

Then $T_0 = \frac{1}{2}(X+Y), T_1 = \frac{1}{2}(X-Y)$ satisfy the conditions of Theorem 7. ∎

Corollary 4. *Let q be a prime power and $q+1 = 2^s n$, n odd. Let $m_1, \ldots, m_r$ be the orders of Williamson type (not necessarily circulant or type 1) matrices. Then*

(i) *when $s \ge 2$, there exists an M-structure Hadamard matrix of* GQ *type of order $2^r m_1 \ldots m_r(q+1) = 2^{r+s} r_1 \ldots m_r n$;*

(ii) *when $s = 1$, there exists an M-structue Hadamard matrix of* GQ *type of order $2^{r+1} m_1 \ldots m_r(q+1) = 2^{r+2} m_1 \ldots m_r n$.*

Proof: Let W_1, W_2, W_3 and W_4 be Williamson type matrices of order m. Then

$$\begin{pmatrix} W_1 & W_2 & W_3 & W_4 \\ -W_2 & W_1 & -W_4 & -W_3 \\ -W_3 & W_4 & W_1 & W_2 \\ W_4 & W_3 & -W_2 & W_1 \end{pmatrix}$$

is an Hadamard matrix which has an M-structure

$$\begin{pmatrix} X & Y \\ -Y & X \end{pmatrix}.$$

where

$$X = \begin{pmatrix} W_1 & W_2 \\ -W_2 & W_1 \end{pmatrix}, \quad Y = \begin{pmatrix} W_3 & W_4 \\ -W_4 & W_3 \end{pmatrix}.$$

Then $T_0 = \frac{1}{2}(X+Y), T_1 = \frac{1}{2}(X-Y)$ satisfy the conditions of Theorem 7. ∎

Corollary 5. *Let q be a prime power and $q+1 = 2^s n$, n odd. Suppose there exists a symmetric C-matrix of order p_i+1 and there exists a symmetric Hadamard matrix of order $p_i - 1$ for $1 \le i \le r$. Then*

(i) *when $s \ge 2$ we have an M-structure Hadamard matrix of* GQ *type of order $2^r p_1 \ldots p_r(q+1) = 2^{r+s} p_1 \ldots p_r n$;*

(ii) *when $s = 1$ we have an M=structure Hadamard matrix of* GQ *type of order $2^{r+1} p_1 \ldots p_r(q+1) = 2^{r+2} p_1 \ldots p_r n$.*

Proof: If there exists a symmetric C-matrix of order $p_i + 1$ and there exists a symmetric Hadamard matrix of $p_i - 1$, then there exists a symmetric Hadamard matrix of order $4p_i$ having a form

$$\begin{pmatrix} X & Y \\ Y & -X \end{pmatrix}.$$

for $1 \leq i \leq l$. $T_0 = \frac{1}{2}(X + Y)$ and $T_1 = \frac{1}{2}(X - Y)$ satisfy the conditions of Theorem 7. ∎

References

1. R. Craigen, Jennifer Seberry, and Xian-Mo Zhang, *Product of four Hadamard matrices*, J. Combinatorial Th. (Ser A) 59 (1992). (to appear).
2. W. de Launey and Jennifer Seberry, *The strong Kronecker product*. (to appear).
3. A.V. Geramita and Jennifer Seberry, "Orthogonal Designs: Quadratic Forms and Hadamard Matrices", Marcel Dekker, New York-Basel, 1979.
4. M. Miyamoto, *A construction of Hadamard matrices*, J. Combinatorial Theory, Ser. A 57 (1991), 86–108.
5. Jennifer Seberry and Mieko Yamada, *Products of Hadamard matrices, Williamson matrices and other orthogonal matrices using M-structures*, Proceedings of Combinatorics Conference, Kobe, Japan, November (1989).
6. Jennifer Seberry and Mieko Yamada, *On products of Hadamard matrices Williamson matrices and other orthogonal matrices using M-structures* JCMCC 7 (1990), 97–137.
7. Jennifer Seberry Wallis, *Hadamard matrices, Part IV, Combinatorics: Room Squares, Sum free sets and Hadamard Matrices*, "Lecture Notes in Mathematics, Vol 292, eds. W.D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis", Springer-Verlag, Berlin-Heidelberg-New York, 1972.
8. Jennifer Sebbery and Xian-Mo Zhang, *Some orthogonal matrices constructed by strong Kronecker multiplication*, Austral. J. Comb. (to appear).
9. R.J. Turyn, *An infinite class of Williamson matrices*, J. Combinatorial Theory, Ser. A 12 (1972), 319–321.
10. A.L. Whiteman, *An infinite family of Hadamard matrices of Williamson type*, J. Combinatorial Theory, Ser. A 14 (1973), 334–340.
11. Mieko Yamada, *Hadamard matrices of generalized quaternion type*, Discrete Math 87 (1991), 187–196.
12. K. Yamamoto, *On a generalized Williamson equation*, Colloquia Mathematica Societatis Janos Bolyai 37 (1985), 839–850.