J. Austral. Math. Soc. (*Series A*) **46** (1989), 371–383

SOME NEW SERIES OF HADAMARD MATRICES

MIEKO YAMADA

(Received 23 February 1987)

Communicated by Louis Caccetta

Abstract

The purpose of this paper is to prove (1) if $q \equiv 1 \pmod 8$ is a prime power and there exists a Hadamard matrix of order $(q-1)/2$, then we can construct a Hadamard matrix of order $4q$, (2) if $q \equiv 5 \pmod 8$ is a prime power and there exists a skew-Hadamard matrix of order $(q+3)/2$, then we can construct a Hadamard matrix of order $4(q+2)$, (3) if $q \equiv 1 \pmod 8$ is a prime power and there exists a symmetric C-matrix of order $(q+3)/2$, then we can construct a Hadamard matrix of order $4(q+2)$.

We have 36, 36 and 8 new orders $4n$ for $n \leq 10000$, of Hadamard matrices from the first, the second and third theorem respectively, which were known to the list of Geramita and Seberry. We prove these theorems by using an adaptation of generalized quaternion type array and relative Gauss sums.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 05 B 20.

1. Notations

To begin with, we list notations which will be used frequently in this paper.

q: a power of a prime p,
$F = GF(q)$: a finite field with q elements,
$K = GF(q^t)$: an extension of F of degree $t \geq 2$,
$F^\times$: the multiplicative group of F,
$K^\times$: the multiplicative group of K,
S_K: the absolute trace from K,
S_F: the absolute trace from F,
$S_{K/F}$: the relative trace from K to F,

ξ: a primitive element of K,
A^*: the transpose of a matrix A,
I_m: the unit matrix of order m,
J_m: the matrix of order m with every element $+1$,
$\otimes$: tensor product of matrices,
$J_m(x) = 1 + x + \cdots + x^{m-1}$.

2. An adaptation of generalized quaternion type array with trimming

In the following theorem we give a Hadamard matrix of order $4(n+1)$.

THEOREM 1. *Let*

$$L = \begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix},$$

and

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix},$$

and $K = -LM/2$. *Note that these are Hadamard matrices of order* 4. *Here*

$$H = \begin{pmatrix} A & B & C & D \\ -B^* & A^* & -D^* & C^* \\ -C^* & D & A^* & -B \\ -D^* & -C & B^* & A \end{pmatrix}$$

is a matrix of order $4n$ *if* A, B, C, D *are matrices of order* n. *Moreover suppose that the component matrices* A, B, C, D *satisfy the following conditions*:

(i) A, B, C, D *are normal matrices of order* n *whose elements are from* $\{1, -1\}$;

(ii) $AB = BA$, $AC = CA$, $AD = DA^*$, $BC = C^*B$, $BD^* = DB^*$, $CD = DC$, $A^*B = BA^*$, $A^*D^* = D^*A$, $CB = BC^*$, $B^*D = D^*B$, $C^*D = DC^*$;

(iii) $AA^* + BB^* + CC^* + DD^* = 4(n+1)I_n - 4J_n$;

(iv) $A\mathbf{e} = 2\mathbf{e}$, $B\mathbf{e} = C\mathbf{e} = D\mathbf{e} = 0$ *where* $\mathbf{e}$ *is the column vector of length* n *with every element* $+1$.

https://doi.org/10.1017/S144678870003086X Published online by Cambridge University Press

Then

$$N = \begin{pmatrix} 1 \otimes L & \mathbf{e}^* \otimes K \\ \mathbf{e} \otimes M^* & H \end{pmatrix}$$

is a Hadamard matrix of order $4(n+1)$.

PROOF. See [6].

If A, B, C, D are circulant matrices, then the matrix H is the right regular representation matrix of a particular element in a non-associative quaternion extension ring over the generalized quaternion ring. So we may regard the matrix H as an adaptation of generalized quaternion type array. More precisely see [6].

3. Gauss sums and relative Gauss sums

We define Gauss sums and relative Gauss sums over a finite field.

DEFINITION. Let χ be a character of F and let $\zeta_p = e^{2\pi i/p}$. Then the *Gauss sum* $\tau_F(\chi)$ is defined by

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

When $\chi = 1$, the principal character, then $\tau_F(\chi) = -1$. And if $\chi \neq 1$, then we have $\tau_F(\chi)\overline{\tau_F(\chi)} = q$. If χ is a non-principal character of K, then the ratio

$$\Theta_{K/F}(\chi) = \frac{\tau_K(\chi)}{\tau_F(\chi)}$$

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

The following theorem on relative Gauss sums is very important.

THEOREM 2. *Let* $\chi = \chi_K$ *be a character of* K *and let* χ_F, *the character* χ *restricted to* F, *be non-principal. Let* $\mathscr{L}$ *be a system of representatives of the quotient group* $K^\times/F^\times$. *Then we have*

$$\Theta_{K/F}(\chi) = \sum_{\alpha \in \mathscr{L}} \overline{\chi}_F(S_{K/F}\alpha)\chi(\alpha).$$

Moreover we have the norm relation $\Theta_{K/F}(\chi)\overline{\Theta_{K/F}(\chi)} = q^{t-1}$.

PROOF. See [7, 8].

We need the following corollary concerning a character sum.

COROLLARY TO THEOREM 2. *Let* χ *be a non-principal character of* K *and denote by* χ_F *the character* χ *restricted to* F. *We take an* $\mathscr{L}$ *decomposed in*

https://doi.org/10.1017/S144678870003086X Published online by Cambridge University Press

the two parts

$$\mathscr{L} = \mathscr{L}_0 + \mathscr{L}_1; \quad \mathscr{L}_0 = \{\alpha : S_{K/F}\alpha = 0\}, \quad \mathscr{L}_1 = \{\alpha : S_{K/F}\alpha = 1\}.$$

Then we have

$$\sum_{\beta \in \mathscr{L}_1} \chi(\beta) = \begin{cases} \Theta_{K/F}(\chi) & \text{when } \chi_F \neq 1, \\ -\frac{1}{q}\tau_K(\chi) & \text{when } \chi_F = 1. \end{cases}$$

PROOF. See [7, 8].

4. Lemmas

In the rest of this paper, we suppose $t = 2$. Let χ be the character of K such that $\chi(\xi) = \zeta_{q-1}$ where ζ_{q-1} is a primitive $(q-1)$th root of unity. We define the numbers z_m by

$$\chi\left(\frac{S_{K/F}\xi^m}{2\xi^m}\right) = \zeta_{q-1}^{z_m} \quad \text{for } m \not\equiv \frac{q+1}{2} \pmod{q+1}.$$

Furthermore we define the polynomial

$$f(x) \equiv \sum_{\substack{m=0 \\ m \neq (q+1)/2}}^{q} x^{z_m} \pmod{x^{q-1} - 1}.$$

LEMMA 1. *The polynomial $f(x)$ has the following properties*:

(1) *$f(x)$ contains every x^{z_m} exactly twice except for $x^0 = 1$ which appears only once*;

(2) $f(x)f(x^{-1}) \equiv q + (q+1)J_{q-1}(x) - 2J_{(q-1)/2}(x^2) \pmod{x^{q-1} - 1}$.

PROOF. (1) Since $z_{-m} \equiv z_m \pmod{q-1}$, $f(x)$ contains every x^{z_m} twice except for $x^0 = 1$. We show that $f(x)$ contains x^{z_m} "exactly" twice. Let G be the subgroup of $K^\times$ generated by ξ^{q-1}. This is characterized as the set of elements with the relative norm 1. Assume $z_m \equiv z_{m'} \pmod{q-1}$, that is

$$\frac{S_{K/F}\xi^m}{2\xi^m} \equiv \frac{S_{K/F}\xi^{m'}}{2\xi^{m'}} \pmod{{}^\times G}.$$

This is equivalent to

$$N_{K/F}\left(\frac{S_{K/F}\xi^m}{2\xi^m}\right) = N_{K/F}\left(\frac{S_{K/F}\xi^{m'}}{2\xi^{m'}}\right),$$

$$N_{K/F}(1 + \xi^{(q-1)m}) = N_{K/F}(1 + \xi^{(q-1)m'}),$$

$$(1 + \xi^{(q-1)m})(1 + \xi^{-(q-1)m}) = (1 + \xi^{(q-1)m'})(1 + \xi^{-(q-1)m'}),$$

$$\xi^{(q-1)m} + \xi^{-(q-1)m} = \xi^{(q-1)m'} + \xi^{-(q-1)m'}.$$

https://doi.org/10.1017/S144678870003086X Published online by Cambridge University Press

Putting $\alpha = \xi^{(q-1)m}$, $\beta = \xi^{(q-1)m'}$, the equation above becomes

$$\alpha + \frac{1}{\alpha} = \beta + \frac{1}{\beta}.$$

Thus we have $\alpha = \beta$ or $\alpha = \frac{1}{\beta}$, that is $m \equiv \pm m' \pmod{q+1}$. This implies that there exists no z_m such that $z_m \equiv z_{m'} \pmod{q-1}$, $m \not\equiv \pm m' \pmod{q+1}$.

(2) Now let χ be the character of K such that $\chi(\xi) = \zeta$ where ζ is an arbitrary $(q-1)$th root of unity.

Since

$$f(\zeta) = \sum_{\substack{m=0 \\ m \neq (q+1)/2}}^{q} \zeta^{z_m} = \sum_{\substack{m=0 \\ m \neq (q+1)/2}}^{q} \chi\left(\frac{S_{K/F}\xi^m}{2\xi^m}\right) = \overline{\chi}(2) \sum_{\beta \in \mathscr{S}_1} \overline{\chi}(\beta),$$

it suffices to verify

$$f(\zeta)\overline{f(\zeta)} = \sum_{\beta \in \mathscr{S}_1} \chi(\beta) \overline{\sum_{\beta \in \mathscr{S}_1} \chi(\beta)} = q + (q+1)J_{q-1}(\zeta) - 2J_{(q-1)/2}(\zeta^2).$$

We can do this easily from the corollary to Theorem 2.

LEMMA 2. *Put* $f(x) \equiv f_0(x^2) + xf_1(x^2) \pmod{x^{q-1} - 1}$. *By replacing* x^2 *by* x *in the polynomials* $f_0(x^2)$ *and* $f_1(x^2)$, *we define the polynomials*

$$\varphi_0(x) \equiv f_0(x) - J_{(q-1)/2}(x) \pmod{x^{(q-1)/2} - 1},$$
$$\varphi_1(x) \equiv f_1(x) - J_{(q-1)/2}(x) \pmod{x^{(q-1)/2} - 1}.$$

Then all the coefficients of $\varphi_0(x)$ *and* $\varphi_1(x)$, *except for the constant term of* $\varphi_0(x)$, *are from* $\{1, -1\}$ *and we have*

$$\varphi_0(x)\varphi_0(x^{-1}) + \varphi_1(x)\varphi_1(x^{-1}) \equiv q - 2J_{(q-1)/2}(x) \pmod{x^{(q-1)/2} - 1}.$$

PROOF. We have

$$\begin{aligned}
&\varphi_0(x)\varphi_0(x^{-1}) + \varphi_1(x)\varphi_1(x^{-1}) \\
&\quad \equiv (f_0(x) - J_{(q-1)/2}(x))(f_0(x^{-1}) - J_{(q-1)/2}(x)) \\
&\qquad + (f_1(x) - J_{(q-1)/2}(x))(f_1(x^{-1}) - J_{(q-1)/2}(x)) \\
&\quad \equiv f_0(x)f_0(x^{-1}) + f_1(x)f_1(x^{-1}) \\
&\qquad - (f_0(x) + f_0(x^{-1}) + f_1(x) + f_1(x^{-1}))J_{(q-1)/2}(x) + 2J_{(q-1)/2}^2(x) \\
&\quad \equiv f_0(x)f_0(x^{-1}) + f_1(x)f_1(x^{-1}) - (q+1)J_{(q-1)/2}(x) \pmod{x^{(q-1)/2} - 1}.
\end{aligned}$$

Notice that $f_0(x)f_0(x^{-1}) + f_1(x)f_1(x^{-1})$ is congruent to

$$f(x)f(x^{-1}) \pmod{x^{(q-1)/2} - 1},$$

https://doi.org/10.1017/S144678870003086X Published online by Cambridge University Press

neglecting odd power terms. Thus we obtain from Lemma 1,

$$f_0(x)f_0(x^{-1}) + f_1(x)f_1(x^{-1}) \equiv q + (q-1)J_{(q-1)/2}(x) \pmod{x^{(q-1)/2} - 1},$$

and

$$\varphi_0(x)\varphi_0(x^{-1}) + \varphi_1(x)\varphi_1(x^{-1}) \equiv q - 2J_{(q-1)/2}(x) \pmod{x^{(q-1)/2} - 1}.$$

5. Further lemmas

In this section, we assume that $q \equiv 1 \pmod 4$ and put $n = (q+1)/2$. We let i be a primitive fourth root of unity and ψ be the quadratic character of F. We define the polynomial $g(x)$ by

$$g(x) \equiv \sum_{m=0}^{q} \psi(S_{K/F}\xi^m) i^m x^m \pmod{x^n - 1}.$$

Since n is odd, we can write $g(x)$ in following form,

$$g(x) \equiv \sum_{m=0}^{n-1} \psi(S_{K/F}\xi^{4m})x^m + i^n \sum_{m=0}^{n-1} \psi(S_{K/F}\xi^{4m+n})x^m \pmod{x^n - 1}.$$

Moreover we define the polynomials

$$\alpha(x) \equiv \sum_{m=0}^{n-1} \psi(S_{K/F}\xi^{4m})x^m \pmod{x^n - 1},$$

$$\beta(x) \equiv \sum_{m=0}^{n-1} \psi(S_{K/F}\xi^{4m+n})x^m \pmod{x^n - 1}.$$

Then we have $g(x) \equiv \alpha(x) + i^n\beta(x) \pmod{x^n - 1}$ and $\alpha(x)$ and $\beta(x)$ have the following properties.

LEMMA 3. *For the polynomial $\alpha(x)$ and $\beta(x)$, we have*

(1) $$\alpha(x^{-1}) \equiv \alpha(x), \ \beta(x^{-1}) \equiv \beta(x) \pmod{x^n - 1},$$

(2) $$\alpha(x)\alpha(x^{-1}) + \beta(x)\beta(x^{-1}) \equiv q \pmod{x^n - 1}.$$

PROOF. Let $\chi = \chi_4\chi_n$ be the character of K such that $\chi_4(\xi) = i$ and $\chi_n(\xi) = \zeta_n$ where ζ_n is an arbitrary nth root of unity. The character χ restricted to F becomes the quadratic character ψ of F.

From Theorem 2, we get

$$g(\zeta_n) = \alpha(\zeta_n) + i^n\beta(\zeta_n) = \sum_{m=0}^{n-1} \psi(S_{K/F}\xi^m) i^m \zeta_n^m = \Theta_{K/F}(\chi).$$

https://doi.org/10.1017/S144678870003086X Published online by Cambridge University Press

Since

$$\begin{aligned}\Theta_{K/F}(\chi)\overline{\Theta_{K/F}(\chi)} &= (\alpha(\zeta_n) + i^n\beta(\zeta_n))\left(\overline{\alpha(\zeta_n)} - i^n\overline{\beta(\zeta_n)}\right)\\ &= \alpha(\zeta_n)\overline{\alpha(\zeta_n)} + \beta(\zeta_n)\overline{\beta(\zeta_n)} - i^n\left(\beta(\zeta_n)\overline{\alpha(\zeta_n)} - \alpha(\zeta_n)\overline{\beta(\zeta_n)}\right)\\ &= q,\end{aligned}$$

we have

$$\alpha(\zeta_n)\overline{\alpha(\zeta_n)} + \beta(\zeta_n)\overline{\beta(\zeta_n)} = q,$$

and

$$\beta(\zeta_n)\overline{\alpha(\zeta_n)} - \alpha(\zeta_n)\overline{\beta(\zeta_n)} = 0.$$

Hence

$$\alpha(x)\alpha(x^{-1}) + \beta(x)\beta(x^{-1}) \equiv q \pmod{x^n - 1}.$$

Next we can easily check

$$\psi(S_{K/F}\xi^{-4m}) = \psi(S_{K/F}\xi^{4m}),$$

$$\psi(S_{K/F}\xi^{-4m+n}) = \psi(S_{K/F}\xi^{4m+n}).$$

Therefore it leads to that

$$\alpha(x^{-1}) \equiv \sum_{m=0}^{n-1}\psi(S_{K/F}\xi^{4m})x^{-m} \equiv \sum_{m=0}^{n-1}\psi(S_{K/F}\xi^{4m})x^{m} \equiv \alpha(x) \pmod{x^n - 1},$$

$$\beta(x^{-1}) \equiv \sum_{m=0}^{n-1}\psi(S_{K/F}\xi^{4m+n})x^{-m} \equiv \sum_{m=0}^{n-1}\psi(S_{K/F}\xi^{4m+n})x^{m} \equiv \beta(x) \pmod{x^n - 1}.$$

6. The main theorems

THEOREM 3. *If $q \equiv 1 \pmod 8$ is a prime power and there exists a Hadamard matrix of order $(q-1)/2$, then we can consturct a Hadamard matrix of order $4q$.*

THEOREM 4. *If $q \equiv 5 \pmod 8$ is a prime power and there exists a skew-Hadamard matrix of order $(q+3)/2$, then we can construct a Hadamard matrix of order $4(q+2)$.*

https://doi.org/10.1017/S144678870003086X Published online by Cambridge University Press

THEOREM 5. *If $q \equiv 1 \pmod 8$ is a prime power and there exists a symmetric C-matrix of order $(q+3)/2$, then we can construct a Hadamard matrix of order $4(q+2)$.*

Theorems 4 and 5 were announced and proved in a private communicaton by Z. Kiyasu [3], but he has not published the proof. In particular when $(q+3)/2$ is a prime power, these theorems reduce to Kiyasu's Theorem 9.18 of [2] (without proof). In [3] he used *KSW* array.

In this paper we prove the more general three theorems all by using an adaptation of generalized quaternion type array with a trimming and relative Gauss sums.

We have 36, 36 and 8 new orders $4n$ for $n \leq 10000$, of Hadamard matrices from Theorems 3, 4, and 5 respectively, unknown to the list of Geramita and Seberry [1].

(1) New orders obtained from Theorem 3.

n: 233, 809, 953, 1193, 1889, 2393, 2417, 2441, 2729, 2953, 3209, 3593, 3617, 3881, 4049, 4217, 4721, 4889, 5657, 5849, 6073, 6089, 6257, 6449, 6473, 6569, 6977, 7177, 7417, 7433, 7753, 8297, 8609, 8713, 8761, 9833.

(2) New orders obtained from Theorem 4.

n: 103, 125, 151, 655, 879, 1231, 1951, 1999, 2239, 2271, 2559, 2799, 2839, 2959, 3039, 3183, 3583, 3679, 4359, 4735, 4863, 4911, 5079, 5311, 5503, 5815, 5983, 6199, 6639, 7519, 8119, 8223, 8679, 9279, 9631, 9903.

(3) New orders obtained from Theorem 5.

n: 579, 2019, 3043, 4443, 6339, 7419, 8523, 9819.

7. Proof of Theorem 3

We define the matrices A and B by using the polynomials $\varphi_0(x)$ and $\varphi_1(x)$ in Lemma 2 and let

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \varphi_0(T) + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I_{(q-1)/2}, \qquad B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \varphi_1(T),$$

where T is the basic circulant matrix of order $(q-1)/2$.

Since there exists a Hadamard matrix H_0 of order $(q-1)/2$, by assumption, we define the matrices C and D by

$$C = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes H_0, \qquad D = C \text{ or } D = C^*.$$

https://doi.org/10.1017/S144678870003086X Published online by Cambridge University Press

We can verify that the matrices A, B, C, D satisfy the conditions of Theorem 1. It is obvious that the condition (i) is satisfied. Notice that the product of the matrix $\left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right)$ and the matrix $\left(\begin{smallmatrix}1&-1\\-1&1\end{smallmatrix}\right)$ is equal to the zero matrix. Hence we obtain

$$BC = C^*B, \qquad CB = BC^*, \qquad BD^* = DB^*, \qquad B^*D = D^*B,$$

which are all the zero matrix. From $D = C$ or $D = C^*$, we have

$$CD = DC, \qquad C^*D = DC^*.$$

Since $\varphi_0(T)$ and $\varphi_1(T)$ are circulant matrices,

$$AB = BA, \qquad A^*B = BA^*.$$

Furthermore we get

$$AC = CA = A^*C = CA^* = 2\begin{pmatrix}1&-1\\-1&1\end{pmatrix} \otimes H_0,$$

$$AC^* = C^*A = A^*C^* = C^*A^* = 2\begin{pmatrix}1&-1\\-1&1\end{pmatrix} \otimes H_0,$$

that is,

$$AC = CA, \qquad AD = DA^*, \qquad A^*D^* = D^*A.$$

Therefore A, B, C, D satisfy the condition (ii).

By Lemma 2,

$$\begin{aligned} AA^* + BB^* + CC^* + DD^* &= 2\begin{pmatrix}1&1\\1&1\end{pmatrix} \otimes \varphi_0(T)\varphi_0(T^{-1}) + 2\begin{pmatrix}1&-1\\-1&1\end{pmatrix} \otimes I_{(q-1)/2} \\ &\quad + 2\begin{pmatrix}1&1\\1&1\end{pmatrix} \otimes \varphi_1(T)\varphi_1(T^{-1}) + 4\begin{pmatrix}1&-1\\-1&1\end{pmatrix} \otimes H_0H_0^* \\ &= 2\begin{pmatrix}1&1\\1&1\end{pmatrix} \otimes (qI_{(q-1)/2} - 2J_{(q-1)/2}) + 2\begin{pmatrix}1&-1\\-1&1\end{pmatrix} \\ &\quad \otimes I_{(q-1)/2} + 2\begin{pmatrix}1&-1\\-1&1\end{pmatrix} \otimes (q-1)I_{(q-1)/2} \\ &= 4qI_{q-1} - 4J_{q-1}. \end{aligned}$$

If m is even (odd), then z_m is also even (odd). Hence we have

$$f_0(1) = \frac{q+1}{2}, \qquad f_1(1) = \frac{q-1}{2},$$

$$\varphi_0(1) = f_0(1) - \frac{q-1}{2} = 1, \qquad \varphi_1(1) = f_1(1) - \frac{q-1}{2} = 0.$$

So we obtain $A\mathbf{e} = 2\mathbf{e}$, $B\mathbf{e} = 0$. It is obvious that $C\mathbf{e} = D\mathbf{e} = 0$. Thus we construct a Hadamard matrix of order $4q$ by Theorem 1.

https://doi.org/10.1017/S144678870003086X Published online by Cambridge University Press

8. Proof of Theorem 4

We define the matrices A and B by using the polynomials $\alpha(x)$ and $\beta(x)$ in Lemma 3,

$$A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \beta(T) + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes I_{(q+1)/2}, \qquad B = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \alpha(T),$$

where T is the basic circulant matrix of order $(q+1)/2$.

The matrices C and D are defined as follows:

$$C = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I_{(q+1)/2}, \qquad D = C \text{ or } D = C^*.$$

Let Q denote a skew-Hadamard matrix of order $(q+3)/2$, assumed to exist. We transform Q in a normalized form

$$Q = \begin{pmatrix} 1 & \mathbf{e}^* \\ -\mathbf{e} & S + I_{(q+1)/2} \end{pmatrix},$$

where $\mathbf{e}$ is the column vector of length $(q+1)/2$ with every element 1. Notice that

$$S\mathbf{e} = 0, \quad SS^* = \frac{q+1}{2} I_{(q+1)/2} - J_{(q+1)/2}.$$

Similarly to the proof of Theorem 3, we verify that the matrices A, B, C, D satisfy the conditions of Theorem 1. It is obvious that the condition (i) is satisfied. From Lemma 2 the matrices A and B are symmetric. So that if

$$AB = BA, \qquad AC = CA, \qquad AC^* = C^*A, \qquad BC = C^*B, \qquad CB = BC^*$$

are valid, then the condition (ii) is satisfied. Now since $\alpha(T)$ and $\beta(T)$ are circulant matrices, we obtain $AB = BA$. We have also

$$\begin{aligned} AC &= \left\{ \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \beta(T) + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes I \right\} \\ &\quad \times \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I \right\} \\ &= 2 \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \beta(T) + 2 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S, \end{aligned}$$

https://doi.org/10.1017/S144678870003086X Published online by Cambridge University Press

$$CA = \left\{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I\right\} \times \left\{\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \beta(T) + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes I\right\} = 2\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S + 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \beta(T),$$

$$AC^* = \left\{\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \beta(T) + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes I\right\} \times \left\{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S^* + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I\right\} = 2\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S^* + 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \beta(T),$$

$$C^*A = \left\{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S^* + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I\right\} \times \left\{\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \beta(T) + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes I\right\} = 2\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S^* + 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \beta(T),$$

$$BC = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \alpha(T)\left\{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I\right\} = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \alpha(T),$$

$$C^*B = \left\{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S^* + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I\right\}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \alpha(T) = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \alpha(T),$$

$$CB = \left\{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I\right\}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \alpha(T) = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \alpha(T),$$

$$BC^* = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \alpha(T)\left\{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes S^* + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I\right\} = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \alpha(T),$$

where I is the unit matrix of order $(q+1)/2$.

https://doi.org/10.1017/S144678870003086X Published online by Cambridge University Press

Next from Lemma 3, we get

$$\begin{aligned}
&AA^* + BB^* + CC^* + DD^* \\
&\quad = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \beta(T)\beta(T^{-1}) + 2\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes I_{(q+1)/2} \\
&\qquad + 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \alpha(T)\alpha(T^{-1}) + 4\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes SS^* \\
&\qquad + 4\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I_{(q+1)/2} \\
&\quad = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes qI_{(q+1)/2} + 2\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes I_{(q+1)/2} \\
&\qquad + 4\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \left(\frac{q+1}{2} I_{(q+1)/2} - J_{(q+1)/2}\right) + 4\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I_{(q+1)/2} \\
&\quad = 4(q+2)I_{q+1} - 4J_{q+1}.
\end{aligned}$$

By the definition of A and B, it is easy to check that $A\mathbf{e} = 2\mathbf{e}$, $B\mathbf{e} = 0$. On the other hand, from $S\mathbf{e} = 0$, we have $C\mathbf{e} = D\mathbf{e} = 0$. Hence Theorem 4 is proved.

9. Proof of Theorem 5

Let A, B be the same as in the proof of Theorem 4. Let R be a C-matrix of order $(q+3)/2$, assumed to exist in Theorem 5. We transform R in a normalized form

$$R = \begin{pmatrix} 0 & \mathbf{e}^* \\ \mathbf{e} & U \end{pmatrix}.$$

Similarly we define the matrices C and D:

$$C = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes U + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I_{(q+1)/2}, \qquad D = C \text{ or } D = C^*.$$

Now we proceed in the same way as in the proof of Theorem 4.

Acknowledgement

I am grateful to Professor Z. Kiyasu for his consent to a publication of Theorems 4 and 5 prior to his publication.

References

[1] A. V. Geramita and J. Seberry, *Orthogonal designs* (Lecture Notes in Pure and Applied Math. **45**, Marcel Dekker, New York–Basel, 1979).
[2] Z. Kiyasu, *Hadamard matrices and their applications* (Denshi-Tsushin Gakkai, Tokyo, 1980, in Japanese).
[3] Z. Kiyasu, private communication.
[4] E. Spense, 'Hadamard matrices from relative difference sets', *J. Combin. Theory* Ser. A **19** (1975), 287–300.
[5] A. L. Whiteman, 'Hadamard matrices of order $4(2p + 1)$', *J. Number Theory* **8** (1976), 1–11.
[6] M. Yamada, 'Hadamard matrices generated by an adaptation of generalized quaternion type array', *Graphs and Combinatorics* **2** (1986), 179–187.
[7] K. Yamamoto and M. Yamada, 'Williamson Hadamard matrices and Gauss sums', *J. Math. Soc. Japan* **37** (1985), 703–717.
[8] K. Yamamoto, 'On congruences arising from relative Gauss sums', *Number Theory and Combinatorics, Japan* 1984 (World Scientific Publ., Singapore, 1985).

Department of Mathematics
Tokyo Woman's Christian University
2-6-1 Zempukuji, Suginamiku
Tokyo 167
Japan