Kyushu J. Math.
Vol. **51**, 1997, pp. 369–379

ON HADAMARD GROUPS III

Noboru ITO

(Received 18 March 1996)

1. Introduction

A group $G(n)$ of type Q is defined by $G(n) = \langle a, b \mid a^{4n} = e, a^{2n} = b^2$ and $b^{-1}ab = a^{-1}\rangle$. $G(n)$ is dicyclic, has order $8n$ and a Sylow 2-subgroup of $G(n)$ is a generalized quaternion group. $G(n)$ contains only one involution $a^{2n} = b^2$, which is central in $G(n)$.

Let G be a group of order $8n$ containing a central involution e^*. Let D be a transversal of G with respect to $\langle e^*\rangle$. Then we have that $G = D \cup De^*$ and $D \cap De^* = \emptyset$. If there exists a transversal D such that $|D \cap Da| = 2n$ for any element a of G outside $\langle e^*\rangle$, then D and G are called an Hadamard subset and an Hadamard group respectively. If there exists an Hadamard group G of order $8n$, then there exists an Hadamard matrix H of order $4n$ such that the automorphism group $\mathrm{Aut}(H)$ of H contains G as a 'regular' subgroup [**7**].

Thus Hadamard groups are introduced to show the existence of Hadamard matrices which have an optimal group-theoretical property with the hope that such Hadamard matrices exist for every possible order. On the other hand, de Launey and Horadam [**2**] and Flannery [**3**] are working in a similar manner to show the existence of 'cocyclic' Hadamard matrices of order $4n$ developed over groups of order $4n$, where n is any positive integer, using the cohomology theory of groups. Furthermore, quite recently Flannery [**4**] has obtained a fundamental result which tells us that the existence of an Hadamard group of order $8n$ is equivalent to the existence of a cocyclic Hadamard matrix of order $4n$. He also makes a detailed consideration on dihedral groups which seems to be parallel to our consideration on groups of type Q.

Now let D be a transversal of $G(n)$ with respect to $\langle e^*\rangle$, where $e^* = a^{2n}$. Then we list elements of D as follows:

$$ee_0, ae_1, \ldots, a^{2n-1}e_{2n-1}; bf_0, baf_1, \ldots, ba^{2n-1}f_{2n-1},$$

where e_i and f_i are equal to e or e^* for $i = 0, 1, \ldots, 2n-1$. Now we define the

polynomials $c(x)$ and $d(x)$ associated with D as follows:

$$c(x) = c_0 + c_1 x + \cdots + c_{2n-1} x^{2n-1}$$

and

$$d(x) = d_0 + d_1 x + \cdots + d_{2n-1} x^{2n-1},$$

where c_i and d_j are equal to 1 or -1, according to whether e_i and f_j are equal to e or e^* respectively for i and $j = 0, 1, \ldots, 2n-1$. Moreover, we regard $c(x)$ and $d(x)$ as elements of $Z[x]/(1 + x^{2n})$. Then D is an Hadamard subset if and only if the following equality holds:

$$c(x^{-1})c(x) + d(x^{-1})d(x) = 4n. \tag{1}$$

(For this, see [**9**].)

We would like to conjecture that every $G(n)$ is an Hadamard group.

2. Groups of type Q

If $2n = q + 1$ or $4n = q + 1$, where q is a prime power, then $G(n)$ is an Hadamard group and there exists a special type of an Hadamard subset D which will be called an Hadamard subset of Paley type or quadratic residue type respectively (see [**7**] and [**8**]). There $G(n)$ itself is called an Hadamard group of Paley type or quadratic residue type respectively. This fact can be regarded as a strong support to the conjecture made at the end of Section 1.

We begin with the following proposition.

PROPOSITION 1. *If $G(n)$ is an Hadamard group, then so is $G(2n)$.*

Proof. Assume that $G(n)$ is an Hadamard group and let D be an Hadamard subset. Let $c(x)$ and $d(x)$ be polynomials associated with D. Then $c(x)$ and $d(x)$ satisfy (1). Now put $c_2(x) = c(x^2) + xd(x^2)$ and $d_2(x) = d(x^2) - x^{-1}c(x^2)$. It is easy to see that these are $(-1, 1)$ polynomials in $Z[x]/(1 + x^{4n})$. Now we have that

$$c_2(x^{-1})c_2(x) + d_2(x^{-1})d_2(x) = 2(c(x^{-2})c(x^2) + d(x^{-2})d(x^2)) = 8n$$

by (1). □

The same argument was used earlier by Yamada in [**13–15**]. The following corollary seems to be implicitly given in [**15**].

COROLLARY 1. *All generalized quaternion groups are Hadamard groups.*

Proof. $G(1)$ is a quaternion group, and it is an Hadamard group [**7**]. Thus by Proposition 1 $G(2^m)$ is an Hadamard group for every non-negative integer m. A generalized quaternion group is clearly isomorphic with $G(2^m)$ for some m. □

From now on we assume that n is odd. Hence a Sylow 2-subgroup of $G(n)$ is a quaternion group. Now we recall a fundamental result by Seberry [**11**] which tells us that for any odd integer n there exists a positive integer m such that there exists an Hadamard matrix of order $2^m n$. It seems to be difficult to obtain a similar result in the realm of groups of type Q. However, if $2n-1$ is a prime power, or if there exists a power of 2, say 2^m with $m \geq 2$ such that $2^m n - 1$ is a prime power, then as stated in the beginning of this section $G(n)$ or $G(2^{m-2}n)$ is an Hadamard group. On the other hand, for certain n's, for instance for $n = 659$ and 1013, it seems to be difficult to find such integers m.

3. Transversals of Williamson type

Let $f(x) = f_0 + f_1 x + \cdots + f_{2n-1}x^{2n-1}$ be a polynomial of $Z[x]/(1+x^{2n})$. Then $f(x)$ is called a polynomial of classical Williamson type, if the following conditions are satisfied:

$$|f_i| = 1 \text{ and } f_i = (-1)^{i+1} f_{2n-i} \quad \text{for } i = 1, 2, \ldots, 2n-1. \tag{2}$$

Let $f(x)$ and $g(x) = g_0 + g_1 x + \cdots + g_{2n-1}x^{2n-1}$ be two polynomials of $Z[x]/(1+x^{2n})$. Then the inner product $(f(x), g(x))$ of $f(x)$ and $g(x)$ equals $f_0 g_0 + f_1 g_1 + \cdots + f_{2n-1} g_{2n-1}$.

Now let D be a transversal of $G(n)$ with respect to $\langle e^* \rangle$. If the polynomials $c(x)$ and $d(x)$ associated with D are polynomials of classical Williamson type, then D is called a transversal of classical Williamson type.

LEMMA 1. *Let D be a transversal of $G(n)$ with respect to $\langle e^* \rangle$. If $(c(x), c(x)x^j) = (d(x), d(x)x^j) = 0$, then $|D \cap Da^j| = 2n$.*

Proof. Consider $(c(x), c(x)x^j)$ and $(d(x), d(x)x^j)$. Let $p(c)$ and $p(d)$ be the numbers of terms $c_i c_{i+j} = 1$ and $d_i d_{i+j} = 1$ respectively, where indices are taken modulo $2n$. Then $|D \cap Da^j| = p(c) + p(d)$. Moreover, $(c(x), c(x)x^j) = (d(x), d(x)x^j) = 0$ if and only if $p(c) = p(d) = n$. □

PROPOSITION 2. *If D is a transversal of classical Williamson type of $G(n)$ with respect to $\langle e^* \rangle$, then $|D \cap Da^{2i+1}| = 2n$ for $i = 0, 1, \ldots, n-1$.*

Proof. Let $f(x)$ be a polynomial of classical Williamson type of $Z[x]/(1+x^{2n})$. By Lemma 1 it is enough to show that $(f(x), f(x)x^{2i+1}) = 0$. Now we have that

$$\begin{aligned} f(x)x^{2i+1} &= -f_{2n-2i-1} - f_{2n-2i}x - \cdots - f_{2n-1}x^{2i} + f_0x^{2i+1} \\ &\quad + f_1x^{2i+2} + \cdots + f_{2n-2i-2}x^{2n-1}. \end{aligned}$$

Thus we have that

$$\begin{aligned} (f(x), f(x)x^{2i+1}) &= -f_0f_{2n-2i-1} - f_1f_{2n-2i} - \cdots - f_{2i}f_{2n-1} + f_{2i+1}f_0 \\ &\quad + f_{2i+2}f_1 + \cdots + f_{2n-1}f_{2n-2i-2} \\ &= (-f_0f_{2n-2i-1} + f_{2i+1}f_0) + (-f_1f_{2n-2i} - f_{2i}f_{2n-1}) \\ &\quad + \cdots + (f_{2i+2}f_1 + f_{2n-1}f_{2n-2i-2}) = 0. \end{aligned}$$

□

Let D be a transversal of classical Williamson type. If D is an Hadamard subset, then D is called an Hadamard subset of classical Williamson type. The use of the name 'classical Williamson' is justified as follows. A polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ of $Z[x]/(1-x^n)$ is called symmetric if $c(x) = c(x^{-1})$; namely, if $c_i = c_{n-i}$ for $i = 1, 2, \ldots, n-1$. Moreover, $c(x)$ is called a $(-1, 1)$ polynomial if $|c_i| = 1$ for $i = 0, 1, \ldots, n-1$.

Now an Hadamard matrix of classical Williamson type is defined by a quartet of symmetric $(-1, 1)$ polynomials $c_1(x), c_2(x), c_3(x)$ and $c_4(x)$ of $Z[x]/(1-x^n)$ such that

$$c_1(x^{-1})c_1(x) + c_2(x^{-1})c_2(x) + c_3(x^{-1})c_3(x) + c_4(x^{-1})c_4(x) = 4n \qquad (3)$$

(see [**12**, p. 382]).

LEMMA 2. *If $c_1(x)$ and $c_2(x)$ are symmetric $(-1, 1)$ polynomials of $Z[x]/(1-x^n)$, then $c(x) = c_1(x^4) + x^nc_2(x^4)$ is a polynomial of classical Williamson type of $Z[x]/(1+x^{2n})$. Conversely, if $c(x)$ is a polynomial of classical Williamson type of $Z[x]/(1+x^{2n})$ and if we put $c(x) = c_1(x^4) + x^nc_2(x^4)$, then $c_1(x)$ and $c_2(x)$ are symmetric $(-1, 1)$ polynomials of $Z[x]/(1-x^n)$. Moreover, we have that*

$$c(x^{-1})c(x) = c_1(x^{-4})c_1(x^4) + c_2(x^{-4})c_2(x^4).$$

Proof. Let

$$c_1(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$$

and

$$c_2(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$$

be symmetric $(-1, 1)$ polynomials of $Z[x]/(1 - x^n)$. Then we have that

$$\begin{aligned} c(x) &= c_1(x^4) + x^n c_2(x^4) \\ &= a_0 - a_{(n+1)/2}x^2 + a_1x^4 - a_{(n+3)/2}x^6 + \cdots + a_{(n-3)/2}x^{2n-6} \\ &\quad -a_{n-1}x^{2n-4} + a_{(n-1)/2}x^{2n-2} + u(x). \end{aligned}$$

Then if $n \equiv 1 (\mathrm{mod}\ 4)$, we have that

$$\begin{aligned} u(x) &= b_{(3n+1)/4}x - b_{(n+3)/4}x^3 + b_{(3n+5)/4}x^5 - b_{(n+7)/4}x^7 \\ &\quad + \cdots + b_{n-1}x^{n-4} - b_{(n-1)/2}x^{n-2} + b_0x^n - b_{(n+1)/2}x^{n+2} \\ &\quad + b_1x^{n+4} - \cdots - b_{(3n-3)/4}x^{2n-3} + b_{(n-1)/4}x^{2n-1}. \end{aligned}$$

If $n \equiv 3 (\mathrm{mod}\ 4)$, we have that

$$\begin{aligned} u(x) &= -b_{(n+1)/4}x + b_{(3n+3)/4}x^3 - b_{(n+5)/4}x^5 + b_{(3n+7)/4}x^7 \\ &\quad - \cdots + b_{n-1}x^{n-4} - b_{(n-1)/2}x^{n-2} + b_0x^n - b_{(n+1)/2}x^{n+2} \\ &\quad + b_1x^{n+4} - \cdots + b_{(n-3)/4}x^{2n-3} - b_{(3n-1)/4}x^{2n-1}. \end{aligned}$$

Hence the fact that $c_1(x)$ and $c_2(x)$ are symmetric implies that $c(x)$ is a polynomial of classical Williamson type of $Z[x]/(1 + x^{2n})$. Conversely, let

$$c(x) = c_0 + c_1x + \cdots + c_{2n-1}x^{2n-1}$$

be a polynomial of classical Williamson type of $Z[x]/(1 + x^{2n})$. If we put $c(x) = c_1(x^4) + x^n c_2(x^4)$, then

$$c_1(x^4) = c_0 + c_4x^4 + c_8x^8 + \cdots + c_{2n-2}x^{2n-2} - c_2x^{2n+2} - c_6x^{2n+6} - \cdots - c_{2n-4}x^{4n-4}.$$

Now if $n \equiv 1 (\mathrm{mod}\ 4)$, then

$$\begin{aligned} c_2(x^4) &= c_n + c_{n+4}x^4 + \cdots + c_{2n-1}x^{n-1} - c_3x^{n+3} - c_7x^{n+7} \\ &\quad - \cdots - c_{n-2}x^{2n-2} - c_{n+2}x^{2n+2} - c_{n+6}x^{2n+6} \\ &\quad - \cdots - c_{2n-3}x^{3n-3} + c_1x^{3n+1} + \cdots + c_{n-4}x^{4n-4}. \end{aligned}$$

If $n \equiv 3 (\mathrm{mod}\ 4)$, then

$$\begin{aligned} c_2(x^4) &= c_n + c_{n+4}x^4 + \cdots + c_{2n-3}x^{n-3} - c_1x^{n+1} - c_5x^{n+5} \\ &\quad - \cdots - c_{n-2}x^{2n-2} - c_{n+2}x^{2n+2} - c_{n+6}x^{2n+6} \\ &\quad - \cdots - c_{2n-1}x^{3n-1} + c_3x^{3n+3} + \cdots + c_{n-4}x^{4n-4}. \end{aligned}$$

So (2) implies that $c_1(x)$ and $c_2(x)$ are symmetric. Finally, since $c_1(x)$ and $c_2(x)$ are symmetric and $x^{2n} = -1$, we get the last assertion. □

PROPOSITION 3. *$G(n)$ contains an Hadamard subset of classical Williamson type if and only if there exists an Hadamard matrix of classical Williamson type.*

Proof. Let $c(x)$ and $d(x)$ be polynomials of classical Williamson type associated with an Hadamard subset of classical Williamson type. Then put $c(x) = c_1(x^4) + x^n c_2(x^4)$ and $d(x) = c_3(x^4) + x^n c_4(x^4)$. By Lemma 2, $c_1(x), c_2(x), c_3(x)$ and $c_4(x)$ define an Hadamard matrix of classical Williamson type. Further, by Lemma 2 we can reverse the argument. □

Moreover, we add the following remark. Let D be an Hadamard subset of $G(n)$ with respect to $\langle e^* \rangle$. Let $c(x)$ and $d(x)$ be polynomials associated with D. Put

$$c(x) = c_1(x^4) + x^n c_2(x^4)$$

and

$$d(x) = c_3(x^4) + x^n c_4(x^4).$$

Then $c_i(x)$ belongs to $Z[x]/(1 - x^n)$ for $i = 1, 2, 3$, and 4. Now considering the portion of terms of odd degrees of $c(x^{-1})c(x) + d(x^{-1})d(x) = 4n$, we obtain the following equation:

$$c_1(x^{-1})c_2(x) + c_3(x^{-1})c_4(x) = c_2(x^{-1})c_1(x) + c_4(x^{-1})c_3(x).$$

4. Hadamard subsets of Paley type

Assume that $2n = q + 1$, where q is a prime power. Then $G(n)$ is presented as a factor group of a subgroup of the general linear group $GL(4, q)$ over the field $GF(q)$ of q elements, which is acting on the set of ordered pairs of projective half-points [**8**]. A sketch of the presentation is given as follows.

Let $GF(q^2)$ be the field of q^2 elements and x an element of order $q + 1$ of $GF(q^2)^\times$. Put $y = x + x^q$ and $2b = y$. Then b is an element of $GF(q)$. Moreover,

let r be a generator of $GF(q)^\times$ and s the inverse of r. $Q = \langle r^2 \rangle$ is the subgroup of quadratic residues of $GF(q)^\times$. There exists an element c of $GF(q)$ such that $b^2 - c^2 s = 1$.

The subgroup mentioned above is denoted by L. L is generated by the following two matrices:

$$A = \begin{pmatrix} c & br & 0 & 0 \\ b & c & 0 & 0 \\ 0 & 0 & -cs & b \\ 0 & 0 & b & -cs \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 0 & r & 0 \\ 0 & 0 & 0 & r \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

together with the subgroup M consisting of diagonal matrices

$$\begin{pmatrix} u & 0 & 0 & 0 \\ 0 & u & 0 & 0 \\ 0 & 0 & v & 0 \\ 0 & 0 & 0 & v \end{pmatrix},$$

where u and v run over Q. It holds that $B^{-1}AB = A^{-1}$ modulo M. M acts trivially on the set of ordered pairs of projective half-points.

We put $GF(q)^\times = Q + N$. Projective half-points are the following: for any element a of $GF(q)$, (c, ca), $c \in Q$, $(c, ca), c \in N$, together with $(0, c)$, $c \in Q$ and $(0, c), c \in N$. They will be denoted by a, a^*, t and t^* respectively. Then the ordered pairs of projective half-points are the following: $a_1 = (a, -a)$, $a_1^* = (a^*, -a^*)$, $a_2 = (a, -a^*)$, $a_2^* = (a^*, -a)$, $t_1 = (t, t)$, $t_1^* = (t^*, t^*)$, $t_2 = (t, t^*)$ and $t_2^* = (t^*, t)$. These pairs constitute the set of points of the Hadamard design of Paley type. Moreover, one of the blocks of the design consists of the following points: t_1, a_1 (a runs over $GF(q)$), t_2^* and a_2 (a runs over $GF(q)$). Hence elements of L transferring t_1 into this block forms an Hadamard subset of Paley type.

Let $c(x) = c_0 + c_1 x + \cdots + c_{2n-1} x^{2n-1}$ and $d(x) = d_0 + d_1 x + \cdots + d_{2n-1} x^{2n-1}$ be the pair of polynomials of $Z[x]/(1 + x^{2n})$ associated with the above Hadamard subset.

PROPOSITION 4. *We have that:*

(i) $c_i = (-1)^{i+1} c_{2n-i}$;

(ii) $c_0 + d_0 = 0$ *and* $c_i = d_i$ *for* $i = 1, 2, \ldots, 2n - 1$;

(iii) $c_0 = 1$ *and* $c_n = (-1)^{(n-1)/2}$.

Proof. Elements of the Hadamard subset are essentially determined by a principal submatrix

$$P^i = \begin{pmatrix} c & br \\ b & c \end{pmatrix}^i$$

of A^i, namely A^i and BA^i belong to the Hadamard subset if and only if the (2, 1)-component T of P^i either belong to Q, or $T = 0$ and the (2, 2)-component of P^i belongs to Q. Put

$$P^i = \begin{pmatrix} x & y \\ z & w \end{pmatrix}.$$

Then we have that

$$P^{-i} = \left(\frac{1}{\det P}\right)^i \begin{pmatrix} w & -r \\ -z & x \end{pmatrix}, \quad P^{2n-i} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}.$$

Since $\det P = -r$ belongs to N, we see that A^i belongs to the Hadamard subset if and only if A^{2n-i} belongs to the Hadamard subset if i is odd, and A^i belongs to the Hadamard subset if and only if A^{2n-i} does not belong to the Hadamard subset if i is even. This proves (i).

We have that

$$BA^i = \begin{pmatrix} 0 & 0 & * & * \\ 0 & 0 & * & * \\ x & y & 0 & 0 \\ z & w & 0 & 0 \end{pmatrix}.$$

So (ii) is clear. Moreover, we have that

$$A^n = \begin{pmatrix} 0 & r & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & s & 0 \end{pmatrix}$$

if $n \equiv 1 (\mathrm{mod}\ 4)$, and

$$A^n = \begin{pmatrix} 0 & -1 & 0 & 0 \\ r & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & s & 0 \end{pmatrix}$$

if $n \equiv 3 (\mathrm{mod}\ 4)$. It is obvious that E (= the identity matrix) and BE belong to the Hadamard subset. This completes the proof. □

Remark 1. (i) says that Hadamard subsets of Paley type are Hadamard subsets of classical Williamson type. For this, see [**6**].

Conditions (i)–(iii) of Proposition 6 seem to be very restrictive. They might characterize Paley type: however, it is curiously difficult to proceed in this direction. We only show the following.

PROPOSITION 5. *Assume that* (ii) *of Proposition 6 holds for an Hadamard subset of* $G(n)$. *Then* $2n-1$ *is a sum of two squares.*

Proof. Put $c(\mathbf{i}) = a + b\mathbf{i}$, where $\mathbf{i}$ denotes the imaginary unit. Then we have that $d(\mathbf{i}) = a - 2 + b\mathbf{i}$. Now by (1) we have that $a^2 + b^2 + (a-2)^2 + b^2 = 4n$, which implies that $2n - 1 = (a-1)^2 + b^2$. □

5. Hadamard subset of quadratic residue type

Assume that $4n = q + 1$, where q is a prime power. Then $G(n)$ is presented as a subgroup of the special linear group $SL(2, q)$ over the field $GF(q)$ of q elements which is acting on the set of projective half-points [**7**]. A sketch of the presentation is given as follows.

Let $GF(q^2)$ be the field of q^2 elements and x an element of $GF(q^2)$ of multiplicative order $q+1$. Put $y = x + x^q$. Then y is an element of $GF(q)$. Now $G(n)$ is presented as a subgroup of $SL(2, q)$ generated by the following two matrices:

$$A = \begin{pmatrix} a & b \\ b & d \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

where $a + d = y$. We have that the order of A equals $q+1$, $B^{-1}AB = A^{-1}$ and $A^{(q+1)/2} = B^2 = -E$, where E denotes the identity matrix. It is necessary to specialize A a little more. Since $X^2 - yX + 1$ has no solution in $GF(q)$, $y^2 - 4 = (y+2)(y-2)$ belongs to N. Since $q \equiv 3 (\mathrm{mod}\ 4)$, x can be replaced by $-x$. Hence we may assume that $y - 2$ belongs to Q. So we put $y - 2 = c^2$, $a = c^2 + 1$, $b = c$ and $d = 1$. Thus we have that

$$A = \begin{pmatrix} c^2+1 & c \\ c & 1 \end{pmatrix}.$$

The set of points of an Hadamard design of quadratic residue type is the set of projective half-points (for this see the previous section), and a block of this design consists of projective half-points a (a runs over $GF(q)$), and t. Hence elements of

$G(n)$ transferring t^* into this block form an Hadamard subset of quadratic residue type. Let

$$c(x) = c_0 + c_1 x + \cdots + c_{2n-1} x^{2n-1}$$

and

$$d(v) = d_0 + d_1 x + \cdots + d_{2n-1} x^{2n-1}$$

be the pair of polynomials of $Z[x]/(1 + x^{2n})$ associated with the above Hadamard subset.

PROPOSITION 6.
(i) *It holds that* $c_0 = -1$ *and* $c_i = c_{2n-i}$ *for* $i = 1, 2, , 2n - 1$.
(ii) *It holds that* $d_0 = -1$ *and* $d_i + d_{2n-i-1} = 0$ *for* $i = 0, 1, \ldots, 2n - 1$.

Proof. To show (i) we may put

$$A^i = \begin{pmatrix} a(i) & b(i) \\ b(i) & d(i) \end{pmatrix}.$$

A^i belongs to the above Hadamard subset if and only if either $b(i)$ belongs to N or $b(i) = 0$ and $d(i)$ belongs to N. Now we have that

$$A^{4n-i} = \begin{pmatrix} d(i) & -b(i) \\ -b(i) & a(i) \end{pmatrix} \quad \text{and} \quad A^{2n-i} = \begin{pmatrix} -d(i) & b(i) \\ b(i) & -a(i) \end{pmatrix}.$$

This proves (i).

To show (ii) we may put

$$A^i = \begin{pmatrix} a_i(c) & b_i(c) \\ b_i(c) & d_i(c) \end{pmatrix},$$

where $a_i(x), b_i(x)$ and $d_i(x)$ are polynomials of $GF(q)[x]$ $(i = 0, 1, \ldots, 2n - 1)$.

Equating $(1, 2)$- and $(2, 1)$-components of $A^{i+1} = A^i A$, we obtain that

$$a_i(c) = c b_i(c) + d_i(c). \tag{4}$$

Now we have that

$$A^{2n-i} = \begin{pmatrix} -d_i(c) & b_i(c) \\ b_i(c) & -a_i(c) \end{pmatrix}$$

and that

$$A^{2n-i-1} = \begin{pmatrix} -c b_i(c) - d_i(c) & (c^2 + 1) b_i(c) + c d_i(c) \\ c a_i(c) + b_i(c) & -(c^2 + 1) a_i(c) - c b_i(c) \end{pmatrix}.$$

Hence we have that

$$BA^i = \begin{pmatrix} -b_i(c) & -d_i(c) \\ a_i(c) & b_i(c) \end{pmatrix}$$

and that

$$BA^{2n-i-1} = \begin{pmatrix} -ca_i(c) - b_i(c) & (c^2+1)a_i(c) + cb_i(c) \\ -cb_i(c) - d_i(c) & (c^2+1)b_i(c) - cd_i(c) \end{pmatrix}.$$

Now (4) completes the proof. □

We add a remark that the corresponding Hadamard matrix is skew.

REFERENCES

[1] A. Baliga and K. J. Horadam. Cocyclic Hadamard matrices over $Z_t \times Z_2^2$. Australas. J. Combinatorics **11** (1995), 123–134.

[2] W. de Launey and K. J. Horadam. A weak difference set construction for higher dimensional designs. Designs, Codes and Cryptography **3** (1993), 75–87.

[3] D. L. Flannery. Calculation of cocyclic matrices. J. Pure Appl. Algebra **112** (1996), 181–190.

[4] D. L. Flannery. Cocyclic Hadamard matrices and Hadamard groups are equivalent. Preprint.

[5] K. J. Horadam and W. de Launey. Cocyclic development of designs. J. Algebraic Combinatorics **2** (1993), 267–290.

[6] N. Ito. Note on Hadamard matrices of type Q. Studia Sci. Math. Hungarica **16** (1981), 389–393.

[7] N. Ito. On Hadamard groups. J. of Algebra **168** (1994), 981–987.

[8] N. Ito. On Hadamard groups, II. J. of Algebra **169** (1994), 936–942.

[9] N. Ito. Some results on Hadamard groups. Groups—Korea'94. 149–155. de Gruyter, Berlin and New York, 1995.

[10] R. J. Turyn. An infinite class of Williamson matrices. J. Combinatorial Theory **12** (1972), 319–321.

[11] J. Wallis. On the existence of Hadamard matrices. J. Combinatorial Theory Ser. A **21** (1976), 444–451.

[12] W. D. Wallis, A. P. Street and J. S. Wallis. Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices (Lecture Notes in Mathematics 292). Springer, Berlin-Heidelberg-New York, 1972.

[13] M. Yamada. On a series of Hadamard matrices of order 2^t and the maximal excess of Hadamard matrices of order 2^{2t}. Graphs and Combinatorics **4** (1988), 297–301.

[14] M. Yamada. Supplementary relative difference sets and their applications to Hadamard matrices. Ars Combin. **26A** (1988), 223–238.

[15] M. Yamada. Hadamard matrices of generalized quaternion type. Discrete Math. **87** (1991), 187–196.

Noboru Ito
Department of Mathematics
Meijo University
Nagoya, Tenpaku 468, Japan