

Hadamard matrices constructed by circulant and negacyclic matrices*

TIANBING XIA

*School of ITACS
University of Wollongong
NSW 2522
Australia
txia@uow.edu.au*

MINGYUAN XIA

*School of Mathematics and Statistics
Central China Normal University
Wuhan, Hubei 430079
P.R. China
xiamy@ccnu-1.ccnu.edu.cn*

JENNIFER SEBERRY JING WU

*School of ITACS
University of Wollongong
NSW 2522
Australia
{j.seberry, jw91}@uow.edu.au*

Abstract

In this paper we establish a correspondence between circulant and negacyclic matrices of order n for n odd, give the definition of suitable matrices, and show several new methods for constructing composite suitable negacyclic (circulant) matrices from base sequences and suitable negacyclic (circulant) matrices under some general conditions.

1 Introduction

The existence of Hadamard matrices of order $4n$ for all integers $n > 0$ is an unsolved problem for more than 100 years. In 1944 J. Williamson [6] gave a method called “the

* Research supported by the ARC (No. LX0560185).

sum of four squares” for constructing Hadamard matrices. The obtained matrices by this method are of Williamson type matrices. Generalizing Williamson’s method, then people gave Hadamard matrices of Goethals-Seidel type (or Wallis-Whiteman-type), T -matrices, etc. [3]. The common properties of these methods are:

1. Find 4 suitable matrices, say, A, B, C and D of order n to “plug in” (or “plug into”) for constructing an Hadamard matrix of order $4n$;
2. Every obtained matrix of A, B, C and D has a constant row sum and column sum.

In this paper the construction of Hadamard matrices by negacyclic matrices is a generalization of methods above too, but it keeps only the property 1. Hence, without restriction of 2, some new constructions will be given. Moreover, we establish a correspondence between circulant and negacyclic matrices of order n for n odd, and show several new methods for constructing composite negacyclic matrices from known negacyclic matrices and base sequences under some general conditions. So, lots of new orders of circulant matrices are obtained which can be used to construct Hadamard matrices with Gothals-Seidel type (or Wallis-Whiteman type).

2 Circulant and negacyclic matrices

In this section we establish a correspondence between circulant and negacyclic matrices of order n for n odd.

Let $A = (a_{ij})$ be a matrices of order n . We denote the first row of A by $a = (a_0, a_1, \dots, a_{n-1})$. If

$$a_{ij} = \begin{cases} a_{j-i}, & \text{as } 0 \leq i \leq j \leq n-1, \\ a_{n+j-i}, & \text{as } 0 \leq j < i \leq n-1, \end{cases}$$

we call A circulant. If

$$a_{ij} = \begin{cases} a_{j-i}, & \text{as } 0 \leq i \leq j \leq n-1, \\ -a_{n+j-i}, & \text{as } 0 \leq j < i \leq n-1, \end{cases}$$

we call A negacyclic.

Set $n \times n$ matrices

$$U = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \cdots & 1 \\ -1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

It is well known that

$$U^0 = U^n = I_n, \quad (U^i)^T = U^{n-i} = U^{-i}, \\ U^i U^j = U^j U^i = U^{i+j}, \forall i, j,$$

where A^T is the transpose of A and I_n is the identity matrix of order n . Similarly,

$$\begin{aligned} V^0 &= V^{2n} = I_n, \quad V^n = -I_n, \\ (V^i)^T &= V^{2n-i} = V^{-i}, \quad V^i V^j = V^j V^i = V^{i+j}, \quad \forall i, j. \end{aligned}$$

Let $a = (a_0, a_1, \dots, a_{n-1})$ be the first row of matrix A . If A is circulant, then

$$A = \sum_{i=0}^{n-1} a_i U^i; \tag{1}$$

if A is negacyclic, then

$$A = \sum_{i=0}^{n-1} a_i V^i. \tag{2}$$

Now we define two shift operators s and f for any sequence $a = (a_0, a_1, \dots, a_{n-1})$ as follows:

$$\begin{aligned} s(a) &= (a_{n-1}, a_0, a_1, \dots, a_{n-2}), \\ f(a) &= (-a_{n-1}, a_0, a_1, \dots, a_{n-2}), \end{aligned}$$

It is easy to see that $s^n(a) = a$ and $f^n(a) = -a$.

Let A be a matrix of order n with the first row a . Then the i th row of A would be $s^{i-1}(a)$ or $f^{i-1}(a)$, according as A is circulant or negacyclic, $1 \leq i \leq n$.

Suppose $a = (a_0, a_1, \dots, a_{n-1})$ and $b = (b_0, b_1, \dots, b_{n-1})$ are two sequences of length n . We define the inner production of a and b by

$$\langle a, b \rangle = \sum_{i=0}^{n-1} a_i b_i.$$

If A is given in (1), then

$$AA^T = \sum_{i=0}^{n-1} \langle a, s^i(a) \rangle U^i.$$

If A is given in (2), then

$$AA^T = \sum_{i=0}^{n-1} \langle a, f^i(a) \rangle V^i.$$

For convenience, we define the following terms: The $(1, -1)$ matrices A_1, A_2, A_3 and A_4 of order n are called 4-suitable matrices if

$$\sum_{i=1}^4 A_i A_i^T = 4n I_n. \tag{3}$$

If all of them are circulant (negacyclic) and (3) holds, we call them 4-suitable circulant (negacyclic) matrices.

Similarly, if two $(1, -1)$ matrices A_1 and A_2 of order $2n$ satisfy

$$A_1 A_1^T + A_2 A_2^T = 4n I_{2n}, \tag{4}$$

we call them 2-suitable matrices. If they are circulant (negacyclic) and (4) holds, we call them 2-suitable circulant (negacyclic) matrices.

The following theorem shows the correspondence between suitable circulant matrices and suitable negacyclic matrices.

Theorem 1 *Suppose $n > 0$ is odd. Then there exist 4-suitable circulant matrices of order n if and only if there exist 4-suitable negacyclic matrices of order n .*

Proof. Let A be given in (1). Put

$$x_i = (-1)^i a_i, \quad 0 \leq i < n, \tag{5}$$

$$x = (x_0, \dots, x_{n-1}) \text{ and } X = \sum_{i=0}^{n-1} x_i V^i. \tag{6}$$

Since n is odd, we have

$$\langle x, f^i(x) \rangle = (-1)^i \langle a, s^i(a) \rangle, \quad 0 \leq i < n. \tag{7}$$

Moreover, suppose B, C and D are given as in (1). Similarly, we can take negacyclic matrices Y, Z and W as in (5) and (6). Then A, B, C and D are 4-suitable circulant matrices \iff

$$\langle a, s^i(a) \rangle + \langle b, s^i(b) \rangle + \langle c, s^i(c) \rangle + \langle d, s^i(d) \rangle = 0, \quad 0 < i < n$$

\iff

$$\langle x, f^i(x) \rangle + \langle y, f^i(y) \rangle + \langle z, f^i(z) \rangle + \langle w, f^i(w) \rangle = 0, \quad 0 < i < n$$

$\iff X, Y, Z$ and W are 4-suitable negacyclic matrices. The proof is completed. \square

It is well known that if there exist 4-suitable circulant (negacyclic) matrices of order n , there exists an Hadamard matrix of order $4n$ with Goethals-Seidel (or Wallis-Whiteman) type. Particularly, if A, B, C and D are Williamson type matrix of order n, n odd, X, Y, Z and W are negacyclic matrices constructed from A, B, C and D by (5) and (6) respectively, then X, Y, Z and W are symmetric and the Williamson array is

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

It is well known that for $n \in S_1 \cup S_2 \cup S_3 \cup S_4$ there exist 4-suitable circulant matrices of order n where

$$\begin{aligned} S_1 &= \{2k + 1 : 0 \leq k \leq 36\} \cup \{6m - 1 : 13 \leq m \leq 17\} [2, 7], \\ S_2 &= \{2^i \cdot 10^j \cdot 26^k + 1 : i, j, k \geq 0\} [5], \\ S_3 &= \{n : 2n - 1 \equiv 1 \pmod{4} \text{ is a prime power}\} [4], \\ S_4 &= \{n : 4n - 1 \equiv 3 \pmod{8} \text{ is a prime power}\} [10]. \end{aligned}$$

By theorem 1 for these values of n there are 4-suitable negacyclic matrices of order n .

Example 1 In $GF(73)$ let $C_i = \{5^{8j+i} \pmod{73} : j = 0, 1, \dots, 8\}$, $i = 0, 1, \dots, 7$. Put

$$\begin{aligned} D_1 &= \{0\} \cup C_0 \cup C_1 \cup C_5, & D_2 &= C_0 \cup C_1 \cup C_2 \cup C_5, \\ D_3 &= C_0 \cup C_2 \cup C_4 \cup C_6, & D_4 &= C_1 \cup C_3 \cup C_5 \cup C_7. \end{aligned}$$

The $(1, -1)$ incidence matrices (type 1) of D_1, D_2, D_3 and D_4 are 4-suitable circulant matrices of order 73.

3 2-suitable negacyclic matrices

From [1, 8, 9] we know that there are 2-suitable matrices of order $2n$ for $n \in S_5 \cup S_6 \cup S_7 \cup S_8$ where

$$\begin{aligned} S_5 &= \{1, 5, 13, 17, 37, 41, 61\}[8], \\ S_6 &= \{p^{2r} : r \geq 1 \text{ and } p \equiv 5 \pmod{8} \text{ is a prime}\}[9], \\ S_7 &= \{3^{2a}t^4 : a = 0 \text{ or } 1, t \text{ any integer}\}[1], \\ S_8 &= \{mn : m \in S_5 \cup S_6, n \in S_7\}[9]. \end{aligned}$$

In this section we will extend the results to the case of negacyclic matrices. For this purpose we introduce the following notation and preliminaries.

Let $a_i = (a_{i,0}, \dots, a_{i,n-1})$, $i = 1, \dots, m$ be sequences of length n . We define

$$(/a_1, \dots, a_m) = (a_{1,0}, \dots, a_{m,0}, a_{1,1}, \dots, a_{m,1}, \dots, a_{1,n-1}, \dots, a_{m,n-1}).$$

The resulting sequences $(/a_1, \dots, a_m)$ is of length mn .

Lemma 1 Suppose a, b, c and d are sequences of length n and for some i

$$\langle a, f^i(a) \rangle + \langle b, f^i(b) \rangle + \langle c, f^i(c) \rangle + \langle d, f^i(d) \rangle = 0. \tag{8}$$

Then the following conditions are equivalent:

- (i) (8) holds for all $i \not\equiv 0 \pmod{n}$;
- (ii) (8) is valid for $0 < i \leq \frac{n-1}{2}$.

Proof. Obviously, (i) \implies (ii). Conversely, suppose (ii) is true. We denote the left hand side of (8) by $Q(i)$. For $\frac{n-1}{2} < i < n$, we have $0 < n-i < \frac{n+1}{2}$ and $Q(i) = -Q(n-i)$. If $n-i \leq \frac{n-1}{2}$, then $Q(i) = 0$. If $\frac{n-1}{2} < n-i < \frac{n+1}{2}$, then n is even and $i = \frac{n}{2}$. Hence $Q(\frac{n}{2}) = -Q(\frac{n}{2}) = 0$. For any $i \not\equiv 0 \pmod{n}$, there exist integers k and j such that $i = kn + j$ and $0 < j < n$. In this case $Q(i) = (-1)^k Q(j) = 0$. This means that (i) is true. The proof is completed. \square

Lemma 2 Suppose a, b, c and d are sequences of length n , and for some i ,

$$\langle a, f^i(b) \rangle + \langle b, f^{i-1}(a) \rangle + \langle c, f^i(d) \rangle + \langle d, f^{i-1}(c) \rangle = 0. \tag{9}$$

Then the following conditions are equivalent:

(i) (9) holds for all i ;

(ii) (9) is true for $0 < i \leq \frac{n-1}{2}$.

Proof. Clearly, (i) \implies (ii). Conversely, suppose (ii) is valid. We denote the left hand side of (9) by $R(i)$. Since $R(0) = R(1)$, repeating the discussion similar to that of Lemma 1, we can get that (ii) \implies (i). \square

Lemma 3 Suppose a and b are sequences of length n and for some i ,

$$\langle a, f^i(b) \rangle + \langle b, f^{i-1}(a) \rangle = 0. \tag{10}$$

Then the following conditions are equivalent:

(i) (10) holds for all i ;

(ii) (10) is true for $0 < i \leq \frac{n-1}{2}$.

The proof of Lemma 3 is similar to that of Lemma 2.

Theorem 2 Suppose X and Y are negacyclic matrices of order $2n$ with the first rows $x = (a, b)$ and $y = (c, d)$ respectively. Then X and Y are 2-suitable if and only if the following conditions are satisfied:

(i) (8) is valid for $0 < i \leq \frac{n-1}{2}$,

(ii) (9) is valid for $0 < i \leq \frac{n-1}{2}$.

Proof. We know that X and Y are 2-suitable negacyclic matrices \iff

$$\langle x, f^i(x) \rangle + \langle y, f^i(y) \rangle = 0, \quad 0 < i < 2n. \tag{11}$$

Consider odd and even values of i in (11), it follows that (11) \iff (i) and (ii). The theorem is proved. \square

Remark. Under the assumption of Theorem 2 there is an Hadamard matrix of order $4n$ with the form

$$\begin{pmatrix} X & Y \\ -Y^T & X^T \end{pmatrix},$$

where X and Y are negacyclic matrices.

The following theorem is devoted to compose 2-suitable negacyclic matrices for known negacyclic matrices and Golay sequences.

Two $(1, -1)$ sequences $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ of length n are called Golay sequences if the sums of the nonperiodic autocorrelation functions of x and y satisfy

$$N_j(x) + N_j(y) = \sum_{i=1}^{n-i} (x_i x_{i+j} + y_i y_{i+j}) = 0, \quad 0 < j < n. \tag{12}$$

For Golay sequences see [3].

Theorem 3 *If there are 2-suitable negacyclic matrices of order n and Golay sequences of length m , then there are 2-suitable negacyclic matrices of order mn .*

Proof. Suppose A and B are 2-suitable negacyclic matrices of order n with the first rows a and b respectively. Let $x = (x_1, \dots, x_m)$ and $y = (y_1, \dots, y_m)$ be Golay sequences of length m . Then (12) holds.

Let ε and δ be two symbols and satisfying

$$\varepsilon\delta = \delta\varepsilon = 0, \quad \varepsilon^2 = \delta^2 = 1. \tag{13}$$

(In the real 2-dimensional Euclidean space every pair of orthonormal vectors can be taken as ε and δ in (13) with the notation of inner product of ε and δ by $\varepsilon\delta$).

Put

$$\alpha_i = \frac{1}{2}(x_i + y_i), \quad \beta_i = \frac{1}{2}(x_i - y_i), \quad h_i = h_i(\varepsilon, \delta) = \alpha_i\varepsilon + \beta_i\delta, \quad i = 1, \dots, m,$$

$$h = h(\varepsilon, \delta) = (h_1(\varepsilon, \delta), \dots, h_m(\varepsilon, \delta)).$$

Then the nonperiodic autocorrelation function $N_j(h)$ of $h(\varepsilon, \delta)$ satisfies

$$\begin{aligned} N_j(h) &= \sum_{i=1}^{m-j} h_i(\varepsilon, \delta)h_{i+j}(\varepsilon, \delta) = \sum_{i=1}^{m-j} (\alpha_i\alpha_{i+j} + \beta_i\beta_{i+j}) \\ &= \frac{1}{2}(N_j(x) + N_j(y)) = 0, \quad 0 < j < m. \end{aligned}$$

Set negacyclic matrices C and D of order mn with the first rows c and d respectively, where

$$c = (/h(a, b)), \quad d = (/h^*(-b, a))$$

and $h^*(-b, a)$ is the reverse of $h(-b, a)$.

Now we are going to prove that C and D are 2-suitable negacyclic matrices.

If $i = mj, 0 < j < n$,

$$\langle c, f^i(c) \rangle + \langle d, f^i(d) \rangle = \sum_{k=1}^m (\alpha_k^2 + \beta_k^2) (\langle a, f^j(a) \rangle + \langle b, f^j(b) \rangle) = 0.$$

If $i = mj + k, 0 \leq j < n, 0 < k < m$, then

$$\langle c, f^i(c) \rangle = \sum_{t=1}^k \langle h_t, f^{j+1}(h_{m-k+t}) \rangle + \sum_{t=1}^{m-k} \langle h_{k+t}, f^j(h_t) \rangle, \tag{14}$$

$$\langle d, f^i(d) \rangle = \sum_{t=1}^k \langle h_{t+m-k}, f^{j+1}(h_t) \rangle + \sum_{t=1}^{m-k} \langle h_t, f^j(h_{t+k}) \rangle, \tag{15}$$

Substituting h_t by $\alpha_t a + \beta_t b$ in (14) and by $-\alpha_t b + \beta_t a$ in (15) respectively, we have

$$\begin{aligned} \langle c, f^i(c) \rangle + \langle d, f^i(d) \rangle &= N_k(h) (\langle a, f^{j+1}(a) \rangle + \langle b, f^{j+1}(b) \rangle) \\ &\quad + N_{m-k}(h) (\langle a, f^j(a) \rangle + \langle b, f^j(b) \rangle) = 0. \end{aligned}$$

The proof is completed. □

In the following we consider some special cases in which (10) will be true.

Lemma 4 *Suppose n is odd and a is a sequence of length n . Then (10) is true for a and $b = f^{\frac{n-1}{2}}(a)$.*

Proof. Now

$$\langle a, f^{j+1}(b) \rangle + \langle b, f^j(a) \rangle = \langle a, f^{\frac{n+1}{2}+j}(a) \rangle + \langle a, f^{\frac{n-1}{2}-j}(a) \rangle$$

and

$$\langle a, f^{\frac{n+1}{2}+j}(a) \rangle = -\langle a, f^{\frac{n-1}{2}-j}(a) \rangle.$$

The lemma is proved. □

Lemma 5 *Suppose n is odd, a and b are sequences of length n such that*

$$a_i = -a_{n-i}, \quad b_i = -b_{n-i}, \quad 1 \leq i < n. \tag{16}$$

Then (10) is true for a and $f^{\frac{n-1}{2}}(b)$.

Proof. Since

$$\langle a, f^{j+1}(f^{\frac{n-1}{2}}(b)) \rangle + \langle f^{\frac{n-1}{2}}(b), f^j(a) \rangle = \langle a, f^{\frac{n+1}{2}+j}(b) \rangle + \langle f^{\frac{n-1}{2}-j}(b) \rangle$$

and for $j = \frac{n-1}{2}$,

$$f^n(b) + b = 0,$$

we can consider only the case: $0 \leq j < \frac{n-1}{2}$. Let

$$e(j) = f^{\frac{n+1}{2}+j}(b) + f^{\frac{n-1}{2}-j}(b) = (e_0(j), e_1(j), \dots, e_{n-1}(j)).$$

First, from (16) we have

$$e_0(j) = -b_{\frac{n-1}{2}-j} - b_{\frac{n+1}{2}+j} = 0.$$

Then, for $0 < i \leq \frac{n-1}{2} - j$, we have $n - i \geq \frac{n+1}{2} + j$ and

$$e_i(j) = -b_{\frac{n-1}{2}-j+i} - b_{\frac{n+1}{2}+j+i} = b_{\frac{n+1}{2}+j-i} + b_{\frac{n-1}{2}-j-i} = e_{n-i}(j).$$

Finally, for $\frac{n-1}{2} - j < i \leq \frac{n-1}{2}$, we have $\frac{n+1}{2} \leq n - i < \frac{n+1}{2} + j$ and

$$e_i(j) = -b_{\frac{n-1}{2}-j+i} + b_{i-\frac{n-1}{2}+j} = e_{n-i}(j).$$

Consequently,

$$\langle a, f^{\frac{n+1}{2}+j}(b) \rangle + \langle f^{\frac{n-1}{2}-j}(b) \rangle = \sum_{i=1}^{n-1} a_i e_i(j) = \sum_{i=1}^{\frac{n-1}{2}} (a_i + a_{n-i}) e_i(j) = 0.$$

The proof is completed. □

Corollary 1 *There exist 2-suitable negacyclic matrices of order $2v$ if*

(i) $2v \in \{2^i 10^j 26^k : i, j, k \geq 0\}$, or

(ii) $v \in S_3 \cup S_9$ where $S_9 = \{2k + 1 : 0 \leq k \leq 16\} \cup \{39, 43\}$, or

(iii) $2v = 2mn$ with m satisfying (i) and n satisfying (ii).

Proof. In case (i) there are Golay sequences of length $2v$ [3, 5]. The corollary follows from Theorem 3. In case (ii) there are Williamson matrices of order v with the first rows, say, $a_i = (a_{i,0}, a_{i,1}, \dots, a_{i,v-1})$, $i = 1, 2, 3, 4$, respectively, such that

$$a_{i,0} = 1, \quad a_{i,j} = a_{i,v-j}, \quad 0 < j < v, \quad i = 1, 2, 3, 4.$$

Let

$$b_{i,j} = (-1)^j a_{i,j}, \quad 0 \leq j < v, \quad i = 1, 2, 3, 4.$$

Then $b_i = (b_{i,0}, \dots, b_{i,v-1})$, $i = 1, 2, 3, 4$, satisfy (16). The corollary follows from Theorem 1, Lemma 5 and Theorem 2. (iii) follows from (i), (ii) and Theorem 3. \square

Example 2 In $GF(13)$, let

$$D_1 = D_2 = \{0, 1, 3, 9\}, \quad D_3 = \{1, 3, 4, 9, 10, 12\}, \quad D_4 = \{2, 5, 6, 7, 8, 11\}.$$

Then the $(1, -1)$ incidence matrices (type 1) of D_1, D_2, D_3 and D_4 are suitable circulant matrices with the first rows, say, a, b, c and d respectively, such that

$$\begin{aligned} a &= b = (+ + - + - - - - + - - -), \\ c &= (- + - + + - - - - + + - +), \\ d &= (- - + - - + + + + - - - +). \end{aligned}$$

From Theorem 1 and Theorem 2, Lemma 4 and Lemma 5 we can construct 2-suitable negacyclic matrices of order 26 with the first rows as follows:

$$\begin{aligned} &(+ - - + - + - + - - + + - + + - - - - - - + + - -), \\ &(- + - - - - - + + + + - - + + - + - + + - + - + +), \end{aligned}$$

where we denote 1 and -1 by $+$ and $-$ respectively.

4 4-suitable negacyclic matrices

In this section we give a method for constructing 4 composite suitable negacyclic matrices from 2-suitable negacyclic matrices and base sequences.

Sequences $q = (q_1, \dots, q_{m+p})$, $r = (r_1, \dots, r_{m+p})$, $e = (e_1, \dots, e_m)$ and $t = (t_1, \dots, t_m)$ are called base sequences of lengths $m + p$, $m + p$, m , m respectively (p odd), if

$$N_j(q) + N_j(r) + N_j(e) + N_j(t) = 0, \quad 0 < j < m, \tag{17}$$

and

$$N_j(q) + N_j(r) = 0, \quad m \leq j < m + p. \tag{18}$$

(see [2, 3]).

Theorem 4 *If there are 2–suitable negacyclic matrices of order $2n$ and base sequences of lengths $m+p, m+p, m, m$, respectively (p odd), then there are 4–suitable negacyclic matrices of order $(2m+p)n$.*

Proof. By the assumptions of Theorem 4 and Theorem 2 there are 4 sequences, say, a, b, c and d of length n satisfying (8) and (9). Let q, r, e, t be base sequences of lengths $m+p, m+p, m, m$, respectively, satisfying (17) and (18). Set

$$\begin{aligned} \alpha_i &= \frac{1}{2}(q_i + r_i), \quad \beta_i = \frac{1}{2}(q_i - r_i), \quad i = 1, \dots, m+p, \\ \lambda_i &= \frac{1}{2}(e_i + t_i), \quad \mu_i = \frac{1}{2}(e_i - t_i), \quad i = 1, \dots, m, \\ g_i &= g_i(\varepsilon, \delta) = \alpha_i\varepsilon + \beta_i\delta, \quad i = 1, \dots, m+p, \\ h_i &= h_i(\varepsilon, \delta) = \lambda_i\varepsilon + \mu_i\delta, \quad i = 1, \dots, m, \\ g &= g(\varepsilon, \delta) = (g_1, \dots, g_{m+p}), \quad h = h(\varepsilon, \delta) = (h_1, \dots, h_m), \end{aligned}$$

where ε, δ are 2 symbols satisfying (13). Put

$$\begin{aligned} x &= (/g(a, c), h(b, d)), & y &= (/h(a, c), g(b, d)), \\ z &= (/g^*(c, -a), h^*(d, -b)), & w &= (/h^*(c, -a), g^*(d, -b)), \end{aligned}$$

where g^*, h^* are the reverse of g, h respectively.

We denote $\langle x, f^i(x) \rangle + \langle y, f^i(y) \rangle + \langle z, f^i(z) \rangle + \langle w, f^i(w) \rangle$ by $Q(i)$. Our purpose is to prove that $Q(i) = 0$ for $0 < i < (2m+p)n$.

When $i = (2m+p)j, 0 < j < n$,

$$Q(i) = (N_0(g) + N_0(h))(\langle a, f^j(a) \rangle + \langle b, f^j(b) \rangle + \langle c, f^j(c) \rangle + \langle d, f^j(d) \rangle) = 0.$$

When $i = (2m+p)j + k, 0 \leq j < n, 0 < k \leq m$,

$$\begin{aligned} Q(i) &= (N_{m-k}(g, h) + N_{m+p-k}(h, g))(\langle a, f^{j+1}(b) \rangle + \langle b, f^j(a) \rangle \\ &\quad + \langle c, f^{j+1}(d) \rangle + \langle d, f^j(c) \rangle) \\ &\quad + (N_k(g) + N_k(h))(\langle a, f^j(a) \rangle + \langle b, f^j(b) \rangle + \langle c, f^j(c) \rangle + \langle d, f^j(d) \rangle) \\ &= 0, \end{aligned}$$

where

$$N_{m-k}(g, h) = \sum_{l=1}^k g_l h_{l+m-k}, \quad N_{m+p-k}(h, g) = \sum_{l=1}^k h_l g_{l+m+p-k}.$$

When $i = (2m+p)j + k, 0 \leq j < n, m < k \leq m+p$,

$$\begin{aligned} Q(i) &= (\tilde{N}_{k-m}(h, g) + \tilde{N}_{m+p-k}(h, g))(\langle a, f^{j+1}(b) \rangle + \langle b, f^j(a) \rangle \\ &\quad + \langle c, f^{j+1}(d) \rangle + \langle d, f^j(c) \rangle) \\ &\quad + N_{2m+p-k}(g)(\langle a, f^{j+1}(a) \rangle + \langle b, f^{j+1}(b) \rangle + \langle c, f^{j+1}(c) \rangle + \langle d, f^{j+1}(d) \rangle) \\ &\quad + N_k(g)(\langle a, f^j(a) \rangle + \langle b, f^j(b) \rangle + \langle c, f^j(c) \rangle + \langle d, f^j(d) \rangle) \\ &= 0, \end{aligned}$$

where

$$\bar{N}_{k-m}(h, g) = \sum_{l=1}^m h_l g_{l+k-m}, \quad \bar{N}_{m+p-k}(h, g) = \sum_{l=1}^m h_l g_{l+m+p-k}.$$

When $i = (2m + p)j + k, 0 \leq j < n, \widehat{m} + p < k < 2m + p,$

$$\begin{aligned} Q(i) &= (\widehat{N}_{k-m}(h, g) + \widehat{N}_{k-m-p}(g, h))(\langle a, f^{j+1}(b) \rangle + \langle b, f^j(a) \rangle \\ &\quad + \langle c, f^{j+1}(d) \rangle + \langle d, f^j(c) \rangle) \\ &\quad + (N_{2m+p-k}(g) + N_{2m+p-k}(h))(\langle a, f^{j+1}(a) \rangle + \langle b, f^{j+1}(b) \rangle \\ &\quad + \langle c, f^{j+1}(c) \rangle + \langle d, f^{j+1}(d) \rangle) = 0, \end{aligned}$$

where

$$\widehat{N}_{k-m}(h, g) = \sum_{l=1}^{2m+p-k} h_l g_{l-k-m}, \quad \widehat{N}_{k-m-p}(g, h) = \sum_{l=1}^{2m+p-k} g_l h_{k-m-p+l}.$$

Take negacyclic matrices X, Y, Z and W of order $(2m + p)n$ with the first rows x, y, z and w respectively, as required. The proof is completed. \square

From Theorem 4 we have the following corollary.

Corollary 2 *There are 4-suitable negacyclic matrices of order $(2t + 1)n$ for $n \in S_3 \cup S_9$ and*

- (i) $2t + 1 \in S_2,$ or
- (ii) $1 \leq 2t + 1 \leq 71,$ or
- (iii) $2t + 1 = 6m - 1$ and $13 \leq m \leq 17.$

Proof. For $n \in S_3 \cup S_9,$ there are 2-suitable negacyclic matrices. In case (i) there are Golay sequences of length $2t \in \{2^i 10^j 26^k : i, j, k \geq 0\},$ hence there are base sequences of lengths $m + p, m + p, m, m$ with $m = 1$ and $p = 2t - 1.$ In case (ii) there are base sequences of lengths $t + 1, t + 1, t, t$ and in case (iii) there are base sequences of lengths $4m - 1, 4m - 1, 2m, 2m.$ The conclusion of Corollary 2 follows from Theorem 4. \square

Example 3 *When $2t + 1 = 5, n = 7,$ let*

$$\begin{aligned} a &= (- - + - + - +), & b &= (- + + - + + -), \\ c &= (+ + + + - - -), & d &= (- - + + + - -). \end{aligned}$$

It is easy to verify that a, b, c and d satisfy (8) and (10). Let

$$g(\varepsilon, \delta) = (\varepsilon, \varepsilon, \delta, -\delta), \quad h(\varepsilon, \delta) = \varepsilon.$$

From Theorem 4 we have

$$\begin{aligned}
 x &= (/g(a, c), h(b, d)) = (/a, a, c, -c, b) = \\
 &(- - + - - - - + - + + + + - + - - + - - + + - + + - - - + + + + - + -), \\
 y &= (/h(a, c), g(b, d)) = (/a, b, b, d, -d) = \\
 &(- - - - + - + + - + + + + + - - - - + - + + + + - - + + - + + - - - +), \\
 z &= (/g^*(c, -a), h^*(d, -b)) = (/a, -a, c, c, d) = \\
 &(- + + + - - + + + - + - + + + + - + + + + - - - + - + - - - + - - - -), \\
 w &= (/h^*(c, -a), g^*(d, -b)) = (/c, b, -b, d, d) = \\
 &(+ - + - - + + - - - + + - + + + + - + + + - + - + + - + - - - - + - -).
 \end{aligned}$$

It is easy to check that they satisfy (8).

In general, the composite matrices constructed from base sequences and circulant matrices need not be circulant, but by Theorem 4 and Theorem 1 the resulting matrices would be circulant too.

References

- [1] Y. Q. Chen, On the existence of Abelian Hadamard difference sets and a new family of difference sets, *Finite Fields and their Applications* **3** (1997), 234–256.
- [2] C. Koukouvinos, Base sequence of lengths $m + p$, $m + p$, m , m for $p = 1$ and $0 \leq m \leq 35$, and $p = 2t - 1$, $m = 2t$, $13 \leq t \leq 17$, Personal communication.
- [3] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, In *Contemporary Design Theory*, John Wiley & Sons, New York, pp. 431–560.
- [4] R. J. Turyn, An infinite class of Williamson matrices, *J. Combin. Theory, Ser. A* **12** (1972), 319–321.
- [5] R. J. Turyn, Hadamard matrices, Baumert-Hall units, four symbols sequences, pulse compression and surface wave codings, *J. Combin. Theory, Ser. A* **16** (1974), 313–333.
- [6] J. Williamson, Hadamard’s determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65–81.
- [7] M. Y. Xia, On supplementary difference sets and Hadamard marices, *Acta Math. Sci.* **4** (1984), 81–92 (in Chinese).
- [8] M. Y. Xia and G. Liu, On the class H_1 , *Acta Math. Sci.* **15** (1995), 361–369.
- [9] M. Y. Xia and T. B. Xia, Hadamard matrices constructed from supplementary difference sets in the class H_1 , *J. Combin. Designs* **2** (1994), 325–339.
- [10] M. Y. Xia, T. B. Xia, J. Seberry and J. Wu, An infinite family of Goethals-Seidel arrays, *Discrete Applied Math.* **145** (2005), 498–504.

(Received 19 May 2004)