Available online at www.sciencedirect.com
SCIENCE DIRECT
Discrete Applied Mathematics 145 (2005) 498–504
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

# An infinite family of Goethals–Seidel arrays

Mingyuan Xia[a,1], Tianbing Xia[b], Jennifer Seberry[b], Jing Wu[b]

[a] *Department of Mathematics, Central China Normal University, Wuhan, Hubei 430079, China*
[b] *School of IT and CS, University of Wollongong, Wollongong, NSW 2522, Australia*

Received 15 April 2002; received in revised form 27 May 2003; accepted 23 June 2003

**Abstract**

In this paper we construct an infinite family of Goethals–Seidel arrays and prove the theorem: If $q=4n-1$ is a prime power $\equiv 3 \pmod 8$, then there exists an Hadamard matrix of order $4n$ of Goethals–Seidel type.


*Keywords:* Hadamard matrix; Goethals–Seidel array; Galois fields

## 1. Introduction

An Hadamard matrix is a square matrix of ones and minus ones whose row (and therefore column) vectors are orthogonal. The order $v$ of such a matrix is necessarily 1, 2 or divisible by 4. It is a long standing unsolved conjecture that an Hadamard matrix exists for $v=4n$, $n$ any positive integer. Constructions have been given for particular values of $n$ and even for various infinite classes of values (see [2,3] for background material). Since an Hadamard matrix of order $2v=2(4n)$ can be easily constructed from one of order $v$, the question of the existence for all possible $v$ is reduced to the case where $n$ is odd.

The Goethals–Seidel array is of the form

$$\begin{pmatrix} A & BR & CR & DR \\ -BR & A & D'R & -C'R \\ -CR & -D'R & A & B'R \\ -DR & C'R & -B'R & A \end{pmatrix}, \tag{1}$$

where $R$ is the back-diagonal identity matrix, $A$, $B$, $C$ and $D$ are circulant $(1,-1)$ matrices of order $n$ satisfying

$$AA'+BB'+CC'+DD'=4nI_n. \tag{2}$$

If $A$, $B$, $C$, and $D$ above are symmetric, then one gets a Williamson array

$$W=\begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix} \tag{3}$$

---

[1] The research supported by the NSF of China (No. 10071029).

*E-mail addresses:* xiamy@ccnu.edu.cn (M. Xia), txia@uow.edu.au (T. Xia), j.seberry@uow.edu.au (J. Seberry), jw91@uow.edu.au (J. Wu).

0166-218X/$ - see front matter 
doi:10.1016/j.dam.2003.06.007

with

$$A^2 + B^2 + C^2 + D^2 = 4nI_n. \tag{4}$$

The Goethals–Seidel array is a generalization of Williamson arrays. For detail discussion of more Goethals–Seidel arrays, we recommend Ref. [3,6].

Turyn first found an infinite class of Williamson arrays in [4]. Then Whiteman gave a new proof for Turyn's theorem [5]. Whiteman's method is both elegant and instructive. We will use this method to construct an infinite family of Goethals –Seidel arrays.

The polynomials associated with the matrices $A$, $B$, $C$ and $D$ are

$$\varphi_1(\zeta) = a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1},$$

$$\varphi_2(\zeta) = b_0 + b_1\zeta + \cdots + b_{n-1}\zeta^{n-1},$$

$$\varphi_3(\zeta) = c_0 + c_1\zeta + \cdots + c_{n-1}\zeta^{n-1},$$

$$\varphi_4(\zeta) = d_0 + d_1\zeta + \cdots + d_{n-1}\zeta^{n-1},$$

where $\zeta$ is any $n$th root of unity. The coefficients $a_i$, $b_i$, $c_i$ and $d_i$, $i = 0, 1, \ldots, n-1$, comprise the first rows of $A$, $B$, $C$ and $D$, respectively. One may also associate a finite Parseval relation with each $\varphi_i(\zeta)$, $i = 1, 2, 3, 4$. For example, if the coefficients of $\varphi_1(\zeta)$ are complex numbers, this relation is given for a fixed integer $t$ by

$$\sum_{i=0}^{n-1} a_i\bar{a}_{i+t} = \frac{1}{n}\sum_{j=0}^{n-1} |\varphi_1(\zeta^j)|^2\zeta^{jt}, \tag{5}$$

where $\bar{a}_{i+t}$ is the conjugate of $a_{i+t}$, and $\zeta = exp(2\pi\mathrm{i}/n)$.

If the coefficients $a_i$, $b_i$, $c_i$, $d_i$ $(i = 0, 1, \ldots, n-1)$ are real, then the identity

$$\sum_{i=0}^{n-1}(a_ia_{i+t} + b_ib_{i+t} + c_ic_{i+t} + d_id_{i+t})$$

$$= \frac{1}{n}\sum_{j=0}^{n-1}(|\varphi_1(\zeta^j)|^2 + |\varphi_2(\zeta^j)|^2 + |\varphi_3(\zeta^j)|^2 + |\varphi_4(\zeta^j)|^2)\zeta^{jt}$$

holds for each integer $t$. It follows that the matrix $G$ in (1) is an Hadamard matrix of order $4n$ if the elements of $A$, $B$, $C$ and $D$ are $\pm 1$, and if the identity

$$|\varphi_1(\zeta^j)|^2 + |\varphi_2(\zeta^j)|^2 + |\varphi_3(\zeta^j)|^2 + |\varphi_4(\zeta^j)|^2 = 4n, \tag{6}$$

prevails for each $n$th root of unity $\zeta$ including $\zeta = 1$. The case $\zeta = 1$ of this identity is of particular interest, for it reveals a remarkable connection between Goethals–Seidel array and the representation of $4n$ as the sum of four squares of integers.

The following construction gives an infinite family of Hadamard matrices of Goethals–Seidel type. It is natural to ask if there is an Hadamard matrix of Goethals–Seidel type corresponding to every representation of integers as sum of squares.

## 2. Preliminaries on Galois fields

Let $GF(q)$ denote the Galois field of order $q$, where $q = p^t$ and $p$ is an odd prime. Let $\gamma$ be a non-square element in $GF(q)$. Then the polynomial $P(x) = x^2 - \gamma$ is irreducible in $GF(q)$, and the polynomials $ax + b$ $(a,\ b \in GF(q))$ modulo $P(x)$ form a finite field $GF(q^2)$ of order $q^2$. In what follows we will employ this concrete representation of $GF(q^2)$. If $g$ is a generator of the cyclic group of non-zero elements of $GF(q^2)$, then $g^{q+1} = \delta$ is a generator of the cyclic group of non-zero elements of $GF(q)$. For arbitrary $h \in GF(q^2)$ define

$$tr(h) = h + h^q, \tag{7}$$

so that $tr(h) \in GF(q)$. It follows from this definition that

$$tr(g^k) = g^{(q+1)k}tr(g^{-k}) \tag{8}$$

for an arbitrary integer $k$.

Let $q \equiv 3 \pmod 4$. For $h \in GF(q^2)$, $h \neq 0$, let $ind(h)$ be the least non-negative integer $t$ such that $g^t = h$. Let $\beta$ denote a primitive eighth root of unity. Then

$$\chi(h) = \begin{cases} \beta^{ind(h)}, & h \neq 0, \\ 0, & h = 0, \end{cases} \tag{9}$$

defines an eighth power character $\chi$ of $GF(q^2)$. For $a \in GF(q)$, $a \neq 0$, put $\delta^j = a$. By (9) we have $\chi(a) = \beta^{(q+1)j}$. Consequently $\chi(a) = (-1)^j$ if $q \equiv 3 \pmod 8$ and $\chi(a) = 1$ if $q \equiv 7 \pmod 8$. In the case $q \equiv 3 \pmod 8$ this means that $\chi(a)$ reduces to the Legendre symbol in $GF(q)$ defined by $\chi(a) = 1, -1$ or 0 according as $a$ is a non-zero square, a non-square or 0 in $GF(q)$. In the sequel we will assume that $q \equiv 3 \pmod 8$. Accordingly we obtain from (8) that

$$\chi(tr(g^k))\chi(tr(g^{-k})) = (-1)^k, \quad tr(g^k) \neq 0. \tag{10}$$

For a fixed $\eta \in GF(q^2)$ put $\eta = cx + d$, $c$, $d \in GF(q)$. Then $\eta \in GF(q)$ if $c = 0$ and $\eta \notin GF(q)$ if $c \neq 0$. We require the formula

$$\sum_{\xi} \chi(tr(\xi))\chi(tr(\eta\xi)) = \begin{cases} \chi(d)q(q-1), & c = 0, \\ 0, & c \neq 0, \end{cases} \tag{11}$$

where the summation is over all $\xi \in GF(q^2)$. Put $\xi = ax + b$, $a, b \in GF(q)$. By (7) we have $tr(\xi) = 2b$ and $tr(\eta\xi) = 2(ac\gamma + bd)$. Therefore

$$\sum_{\xi} \chi(tr(\xi))\chi(tr(\eta\xi)) = \sum_{b} \chi(2b) \sum_{a} \chi(2(ac\gamma + bd))$$

and (11) follows at once.

For $\eta \neq 0$ we may put $\eta = g^t$ $(0 \leqslant t \leqslant q^2 - 2)$ so that $c = 0$ if $q + 1 | t$ and $c \neq 0$ if $q + 1 \nmid t$. If $c = 0$, put $t = j(q+1)$ and then $\chi(d) = (-1)^j$. The sum in (11) now becomes

$$\sum_{k=0}^{q^2-2} \chi(tr(g^k))\chi(tr(g^{k+t})) = \sum_{h=0}^{q-2} \sum_{k=h(q+1)}^{h(q+1)+q} \chi(tr(g^k))\chi(tr(g^{k+t})).$$

The double sum on the right has the value 0 if $q + 1 \nmid t$. Since $\chi(tr(g^{k+q+1})) = -\chi(tr(g^k))$ the value of the inner sum is the same for each $h$. For $h = 0$ we get, in particular,

$$\sum_{k=0}^{q} \chi(tr(g^k))\chi(tr(g^{k+t})) = \begin{cases} (-1)^j q, & q + 1 | t, \\ 0, & q + 1 \nmid t, \end{cases} \tag{12}$$

where, in the first case, $t = j(q+1)$.

## 3. Main results

The principal result of this paper is given in the following theorem.

**Theorem 1.** *Let $q$ be a prime power $\equiv 3 \pmod 8$ and put $n = (q+1)/4$. Let $g$ be a primitive element of $GF(q^2)$. Put*

$$g^k = \alpha_k x + \beta_k, \quad \alpha_k, \beta_k \in GF(q) \tag{13}$$

*and define*

$$a_k = \chi(\alpha_k), \quad b_k = \chi(\beta_k). \tag{14}$$

*Then the sums*

$$\begin{aligned} f_1(\zeta) &= a_0 + a_8\zeta + \cdots + a_{8(n-1)}\zeta^{n-1}, \\ f_2(\zeta) &= b_0 + b_8\zeta + \cdots + b_{8(n-1)}\zeta^{n-1}, \\ f_3(\zeta) &= a_1 + a_9\zeta + \cdots + a_{8(n-1)+1}\zeta^{n-1}, \\ f_4(\zeta) &= b_1 + b_9\zeta + \cdots + b_{8(n-1)+1}\zeta^{n-1}, \end{aligned} \tag{15}$$

*satisfy the identity*

$$|f_1(\zeta)|^2 + |f_2(\zeta)|^2 + |f_3(\zeta)|^2 + |f_4(\zeta)|^2 = q \tag{16}$$

*for each nth root of unity* $\zeta$ *including* $\zeta=1$. *Moreover, the following relations hold*:

$$\begin{array}{ll} a_0=0, & a_{8i}=-a_{8(n-i)}, \\ b_0=1, & b_{8i}=b_{8(n-i)}, \end{array} \quad 1\leqslant i<n. \tag{17}$$

**Proof.** Since $g$ is a primitive element of $GF(q^2)$, the integer $k=(q+1)/2=2n$ is the only value of $k$ in the interval $0\leqslant k\leqslant q$ for which $tr(g^k)=0$. Put $g^{2n}=\omega x$, $\omega\in GF(q)$. The numbers $a_k$, $b_k$ in (14) satisfy the relations

$$b_{k+2n}=-\chi(\omega)a_k, \tag{18}$$

$$b_{k+4n}=-b_k, \tag{19}$$

$$b_{k+8n}=b_k. \tag{20}$$

Moreover, from (13) it follows that

$$\begin{aligned} -\alpha_{8i}x+\beta_{8i} &= (g^{8i})^q=g^{8n(4i-1)+8(n-i)} \\ &= \delta^{2(4i-1)}(\alpha_{8(n-i)}x+\beta_{8(n-i)}), \quad 0\leqslant i\leqslant n, \end{aligned} \tag{21}$$

hence

$$\alpha_{8i}=-\delta^{2(4i-1)}\alpha_{8(n-i)}, \quad \beta_{8i}=\delta^{2(4i-1)}\beta_{8(n-i)}, \quad 0\leqslant i\leqslant n. \tag{22}$$

Therefore (17) is valid. Note that the periodicity property (20) implies

$$\sum_{i=0}^{n-1} b_{8i+t}=\sum_{i=0}^{n-1} b_{8i+s}, \quad t\equiv s (\mathrm{mod}\ 8). \tag{23}$$

If we replace $b's$ by $a's$, then (20) and (23) would also be true.

Denote the sum in (12) by $F(t)$. The assumption $q\equiv 3 (\mathrm{mod}\ 8)$ implies that $t=0$ is the only value of $t$ in the interval $0\leqslant t\leqslant n-1$ for which $8t$ is divisible by $q+1$. Thus it follows from (12) that

$$F(8t)=\sum_{k=0}^{q} b_k b_{k+8t}=\begin{cases} q, & t=0, \\ 0, & 1\leqslant t<n. \end{cases} \tag{24}$$

On the other hand from (18), (19) and (24) we have

$$\begin{aligned} F(8t) &= \sum_{k=0}^{3}\sum_{i=0}^{n-1} b_{4i+k}b_{4i+k+8t} \\ &= \sum_{k=0}^{3}\sum_{i=0}^{n-1} b_{8i+kn}b_{8i+kn+8t} \\ &= \sum_{k=0}^{1}\sum_{i=0}^{n-1} (a_{8i+kn}a_{8i+kn+8t}+b_{8i+kn}b_{8i+kn+8t}) \\ &= \sum_{i=0}^{n-1} (a_{8i}a_{8i+8t}+b_{8i}b_{8i+8t}+a_{8i+1}a_{8i+1+8t}+b_{8i+1}b_{8i+1+8t}). \end{aligned} \tag{25}$$

Applying the finite Parseval relation (5) we now obtain

$$\begin{aligned} &\sum_{i=0}^{n-1} (a_{8i}a_{8i+8t}+b_{8i}b_{8i+8t}+a_{8i+1}a_{8i+1+8t}+b_{8i+1}b_{8i+1+8t}) \\ &\quad =\frac{1}{n}\sum_{j=0}^{n-1} (|f_1(\zeta^j)|^2+|f_2(\zeta^j)|^2+|f_3(\zeta^j)|^2+|f_4(\zeta^j)|^2)\zeta^{jt}, \end{aligned} \tag{26}$$

where $\zeta=exp(2\pi\mathrm{i}/n)$.

Combining (25) and (26) we get

$$F(8t) = \frac{1}{n}\sum_{j=0}^{n-1}(|f_1(\zeta^j)|^2 + |f_2(\zeta^j)|^2 + |f_3(\zeta^j)|^2 + |f_4(\zeta^j)|^2)\zeta^{jt}. \tag{27}$$

The inverted form of (27) is given by

$$|f_1(\zeta^j)|^2 + |f_2(\zeta^j)|^2 + |f_3(\zeta_j)|^2 + |f_4(\zeta^j)|^2 = \sum_{t=0}^{n-1} F(8t)\zeta^{-tj}, \quad j = 0, 1, \ldots, n-1.$$

By (24) we have $F(0) = q$ and $F(8t) = 0$ for $1 \leqslant t < n$. Hence the last sum reduces to $q$. This completes the proof of Theorem 1. □

**Theorem 2.** *Let $q$ be a prime power $\equiv 3 (\mathrm{mod}\ 8)$. Then*

$$|f_3(\zeta)|^2 = |f_4(\zeta)|^2 \tag{28}$$

*for each nth root of unity $\zeta$ including $\zeta = 1$, where $n = (q+1)/4$, $f_3(\zeta)$ and $f_4(\zeta)$ are the polynomials defined in (15).*

**Proof.** Since

$$|f_3(\zeta)|^2 = \sum_{t=0}^{n-1}\left(\sum_{i=0}^{n-1} a_{8i+1}a_{8i+1+8t}\right)\zeta^{-t},$$

$$|f_4(\zeta)|^2 = \sum_{t=0}^{n-1}\left(\sum_{i=0}^{n-1} b_{8i+1}b_{8i+1+8t}\right)\zeta^{-t},$$

for the proof of Theorem 2 it is sufficient to show that

$$\sum_{i=0}^{n-1} a_{8i+1}a_{8i+1+8t} = \sum_{i=0}^{n-1} b_{8i+1}b_{8i+1+8t}, \quad 0 \leqslant t < n. \tag{29}$$

To do this it is enough to prove that

$$\sum_{i=0}^{n-1} a_{8i+n}a_{8i+n+8t} = \sum_{i=0}^{n-1} b_{8i+n}b_{8i+n+8t}, \quad 0 <= t < n.$$

Put $g^n = \lambda(x+\varepsilon)$, $\lambda$, $\varepsilon \in GF(q)$. Then from

$$\omega x = (g^n)^2 = \lambda^2(2\varepsilon x + \varepsilon^2 + \gamma)$$

it follows that

$$\gamma = -\varepsilon^2 \quad \text{and} \quad \omega = 2\varepsilon\lambda^2. \tag{30}$$

Now

$$g^{8i+n} = \lambda\{(\beta_{8i} + \varepsilon\alpha_{8i})x + \varepsilon\beta_{8i} + \gamma\alpha_{8i}\}. \tag{31}$$

Using (13), (14), (31), (22), (30) and (23), we have

$$\begin{aligned}\sum_{i=0}^{n-1} b_{8i+n}b_{8i+n+8t} &= \sum_{i=0}^{n-1}\chi(\varepsilon\beta_{8i} + \gamma\alpha_{8i})\chi(\varepsilon\beta_{8(i+t)} + \gamma\alpha_{8(i+t)})\\ &= \sum_{i=0}^{n-1}\chi(\varepsilon\beta_{8(n-i)} - \gamma\alpha_{8(n-i)})\chi(\varepsilon\beta_{8(n-i-t)} - \gamma\alpha_{8(n-i-t)})\\ &= \sum_{i=0}^{n-1}\chi(\beta_{8(n-i)} + \varepsilon\alpha_{8(n-i)})\chi(\beta_{8(n-i-t)} + \varepsilon\alpha_{8(n-i-t)})\\ &= \sum_{i=0}^{n-1}\chi(\beta_{8i} + \varepsilon\alpha_{8i})\chi(\beta_{8i-8t} + \varepsilon\alpha_{8i-8t})\\ &= \sum_{i=0}^{n-1} a_{8i+n}a_{8i+n+8t}, \quad 0 \leqslant t < n. \end{aligned} \tag{32}$$

The proof is completed. □

**Remark 1.** From (17) one sees that $Re f_1(\zeta)=0$ and $f_2(\zeta)$ is real.

The following corollaries are immediate consequences of Theorems 1 and 2.

**Corollary 1.** *Let $q$ be a prime power $\equiv 3 (\mathrm{mod}\ 8)$. Then*

$$q=a^2+2b^2 \tag{33}$$

*for some odd integers a and b.*

**Remark 2.** In general, representation (33) is not unique, and so the values of $a$ and $b$ in (33) are not completely determined by Theorems 1 and 2. In this case there is a problem: Do there exist polynomials $f_1(\zeta)$, $f_2(\zeta)$, $f_3(\zeta)$, $f_4(\zeta)$, corresponding to every pair $(a,b)$, satisfying (33), given as in (15), satisfying (16) and (17), such that

$$f_1(1)=0, \quad f_2(1)^2=a^2, \quad f_3(1)^2=f_4(1)^2=b^2,$$

or not?

**Example 1.** $q=3^3=5^2+2\cdot 1^2=3^2+2\cdot 3^2$. *Take*

$$f_1(\zeta)=\zeta+\zeta^2-\zeta^3+\zeta^4-\zeta^5-\zeta^6,$$

$$f_2(\zeta)=1-\zeta-\zeta^2-\zeta^3-\zeta^4-\zeta^5-\zeta^6,$$

$$f_3(\zeta)=-1-\zeta-\zeta^2+\zeta^3-\zeta^4+\zeta^5+\zeta^6,$$

$$f_4(\zeta)=-1+\zeta+\zeta^2-\zeta^3+\zeta^4-\zeta^5-\zeta^6,$$

Then $f_1(\zeta)$, $f_2(\zeta)$, $f_3(\zeta)$ and $f_4(\zeta)$ satisfy (16) and (17), and

$$f_1(1)=0, \quad f_2(1)^2=5^2, \quad f_3(1)^2=f_4(1)^2=1.$$

**Question.** Do there exist polynomials $f_1(\zeta)$, $f_2(\zeta)$, $f_3(\zeta)$ and $f_4(\zeta)$ in $\zeta$ of order 6, given as in (15), satisfying (16) and (17), such that

$$f_1(1)=0, \quad f_2(1)^2=f_3(1)^2=f_4(1)^2=3^2?$$

**Corollary 2.** *Let $q=4n-1$ be a prime power $\equiv 3 (\mathrm{mod}\ 8)$. Put*

$$\varphi_1(\zeta)=1+f_1(\zeta), \quad \varphi_2(\zeta)=f_2(\zeta), \quad \varphi_3(\zeta)=\varphi_4(\zeta)=f_3(\zeta),$$

*where $f_1(\zeta)$, $f_2(\zeta)$ and $f_3(\zeta)$ are the polynomials defined in (15). Then the identity*

$$|\varphi_1(\zeta)|^2+|\varphi_2(\zeta)|^2+|\varphi_3(\zeta)|^2+|\varphi_4(\zeta)|^2=4n$$

*is satisfied for each nth root of unity $\zeta$ including $\zeta=1$.*

Returning to the Goethals–Seidel matrix in (1) we may now derive the following theorem:

**Theorem 3.** *Let $q=4n-1$ be a prime power $\equiv 3 (\mathrm{mod}\ 8)$. Then there exists an Hadamard matrix of order $4n$ of Goethals–Seidel type in which*

$$(I-A)'=-I+A, \quad B'=B \text{ and } C=D.$$

**Proof.** We employ the construction outlined in the introduction. By (14) and (17) we have $a_0=0$, $b_0=1$, $-a_{8i}=a_{8(n-i)}$, $b_{8i}=b_{8(n-i)}$, $1\leqslant i<n$. The successive elements in the first row of $A$ are $1,a_8,\ldots,a_{8(n-1)}$. The successive elements in the first row of $B$ are $1,b_8,\ldots,b_{8(n-1)}$. The successive elements in the first row of $C$ and $D$ are, say, $a_1,a_9,\ldots,a_{8(n-1)+1}$. The matrices $A$, $B$, $C$ and $D$ are circulant. Theorem 3 now follows readily from the last corollary. □

**Remark 3.** In this case the Hadamard matrix of order $4n$ has the simpler form (the Wallis–Whiteman construction is applicable)

$$G = \begin{pmatrix} A & B & CR & C \\ -B & A' & -C & CR \\ -CR & C' & A & -B \\ -C' & -CR & B & A' \end{pmatrix},$$

where $R$ is the back-diagonal identity matrix, and $G$ is of skew type.

**Remark 4.** While there are no Williamson matrices for order 35 by a complete computer search, and no Williamson type matrices are known for the orders

$$35, 155, 171, 203, 227, 291, 323, 371, 395, 467, 483, 563,$$

$$587, 603, 635, 771, 875, 915, 923, 963, 1131, 1307, 1331,$$

$$1355, 1467, 1523, 1595, 1643, 1691, 1715, 1803, 1923, 1971$$

(see [1,3]) Theorem 3 shows that Goethals–Seidel matrices do exist for all these orders.

**Example 2.** Suppose $n = 35$. Then $q = 4n - 1 = 139$ is a prime $\equiv 3 (\mathrm{mod}\ 8)$. Set

$$a = (+-++++-+-++-+--++-+--++-+--+-+----+)$$

$$b = (++-++-+++-++---++++++---++-+++-++-+)$$

$$c = (++---+-+---+++-+----++--++-+-++++++)$$

where $a$, $b$ and $c$ denote the first row of $n \times n$ circulant matrices $A$, $B$ and $C$, respectively. This gives the desired Goethals –Seidel array.

## Acknowledgements

The authors are grateful to the referees and Prof. P.L. Hammer and Prof. W.C. Shiu for their helpful comments.

## References

[1] D.Z. Djokovic, Williamson matrices of order $4n$ for $n = 33$, 35, 39, Discrete Math. 115 (1993) 267–271.
[2] M. Hall Jr., Combinatorial Theory, 2nd Edition, Wiley, New York, 1986.
[3] J. Seberry, M. Yamada, Hadamard matrices, sequences and block designs, Jeffery H. Dinitz, Douglas R. Stinson (Eds.), in: Contemporary Design Theory: Collection of surveys, Wiley, New York, 1992, pp. 431–560.
[4] R.J. Turyn, An infinite class of Williamson matrices, J. Combin. Theory Ser. A 12 (1972) 319–321.
[5] A.L. Whiteman, An infinite family of Hadamard matrices of Williamson type, J. Combin. Theory Ser. A 14 (1973) 334–340.
[6] M.Y. Xia, Some new families of SDSS and Hadamard matrices, Acta Math. Sci. 16 (1996) 153–161.