AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **54** (2012), Pages 3–11

A class of mutually inequivalent circulant weighing matrices

Goldwyn Millar*

School of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada
goldwynmillar@cmail.carleton.ca

Abstract

It is well-known that for each prime power q and for each $d \in 2\mathbb{N}$, there exists a circulant weighing matrix of order $\frac{q^{d+1}-1}{q-1}$ and weight q^d. We extend this result to show that there exist $\frac{\phi(d+1)}{2}$ inequivalent circulant weighing matrices of order $\frac{q^{d+1}-1}{q-1}$ and weight q^d, where ϕ is the Euler totient function. Further, we obtain a bound on the magnitude of the values taken by the cross-correlation function of any pair of perfect ternary sequences obtained from these matrices.

1 Introduction

Let $\{a_i\}$ and $\{b_i\}$ be periodic complex sequences of period n. Then the function $\gamma_{a,b} : [0, n-1] \to \mathbb{C}$ defined by the rule $\gamma_{a,b}(t) = \sum_{i=0}^{n-1} a_i\overline{b_{i+t}}$ is the *periodic cross-correlation function of* $\{a_i\}$ *and* $\{b_i\}$. The function $\gamma_{a,a}$ is the *periodic auto-correlation function of* $\{a_i\}$. The pair $(\{a_i\}, \{b_i\})$ is said to have *good periodic cross correlation* if for each $t \in [0, n-1]$, $|\gamma_{a,b}(t)|$ is "small" relative to both $\gamma_{a,a}(0)$ and $\gamma_{b,b}(0)$. Similarly, $\{a_i\}$ has *good periodic auto-correlation* if for each $t \in [1, n-1]$, $|\gamma_{a,a}(t)|$ is "small" relative to $\gamma_{a,a}(0)$. If for each $t \in [1, n-1]$, $\gamma_{a,a}(t) = 0$, then we say that $\{a_i\}$ has *perfect periodic auto-correlation*. We refer to $\gamma_{a,a}(0)$ as the in-phase correlation of the sequence.

Sequences of complex units, and in particular binary sequences (sequences each of whose elements are either 1 or -1), with good periodic autocorrelation properties have been used to improve the accuracy of radar and sonar devices ([9] pp. 402–403, 417–418). However, it is known that, for $4 < n < 548,964,900$, there exists no binary sequence of order n with perfect periodic autocorrelation [14].

* This research was conducted while the author was a student at the Department of Mathematics, University of Manitoba, Winnipeg, MB, Canada.

Ternary sequences, each of whose elements is either 0, 1, or -1, could be used for the same purpose (see [11], [12], or [17]). If one does use a ternary sequence, it is desirable [11] that the in-phase correlation of the sequence be as large as possible relative to the period of the sequence. There do, in fact, exist ternary sequences with perfect periodic autocorrelation (i.e. *perfect ternary sequences*). It is known that for each prime power q and for each $d \in 2\mathbb{N}$, there exists a perfect ternary sequence of period $\frac{q^{d+1}-1}{q-1}$ and in-phase correlation q^d. For a proof of this result, consult [2], and see [3], [16], and [7] for some generalizations (several early versions of this result had appeared previously, as in [24]; consult [1] and [8] for histories). Note that as $q \to \infty$,

$$\frac{q^{d+1}-1}{q^d(q-1)} \to 1.$$

For applications in which a single radar or sonar station is used to simultaneously range several objects, it is useful to have sets of sequences with good autocorrelation properties and pairwise good cross-correlation properties [20].

If S is a subset of a group G, then, in the context of the group ring $\mathbb{Z}[G]$, we identify S with $\sum_{y \in S} y$. Further, for

$$T = \sum a_i g_i \in \mathbb{Z}[G]$$

and $t \in \mathbb{Z}$, we stipulate that

$$T^{(t)} = \sum a_i g_i^t.$$

Let $n, k \in \mathbb{N}$ and let α generate the cyclic group G of order n. The existence of a perfect ternary sequence $\{a_i\}$ of period n and in-phase correlation k is equivalent [1] to the existence of an element $\theta(\alpha) \in \mathbb{Z}[G]$ such that

$$\theta(\alpha)\theta(\alpha)^{(-1)} = k.$$

In this case, we refer to $\theta(\alpha)$ as the *group ring polynomial of* $\{a_i\}$. Likewise, the existence of sequences $\{a_i\}$ and $\{b_i\}$ with good periodic cross-correlation is equivalent to the existence of two group ring elements $\theta_1(\alpha)$ and $\theta_2(\alpha)$ such that each of the coefficients of

$$\theta_1(\alpha)\theta_2(\alpha)^{(-1)}$$

is "small" relative to k.

A *circulant weighing matrix of order* n *and weight* k is an $n \times n$ circulant matrix W such that $WW^T = kI$. We refer to a circulant weighing matrix of order n and weight k as a $CW(n,k)$. The existence of a perfect ternary sequence of period n and in-phase correlation k is equivalent to the existence of a $CW(n,k)$ [1]. Two $CW(n,k)$'s with corresponding group ring polynomials $\theta_1(\alpha)$ and $\theta_2(\alpha)$ are equivalent if there exist $s, t \in \mathbb{Z}$ such that $\gcd(n,t) = 1$, and

$$\theta_1(\alpha)^{(t)} = \alpha^s \theta_1(\alpha). \tag{1}$$

The author wrote the present paper while studying circulant weighing matrices under the supervision of Dr. Robert Craigen at the University of Manitoba. A reading of [18] (wherein the present paper is incorrectly cited as "[Mil09] Crosscorrelation of perfect ternary sequences") in concert with [4] and [15] should provide one with a reasonably up to date understanding of the research literature on circulant weighing matrices.

2 Constructing inequivalent circulant weighing matrices

Let q be a prime power, and let $d \in \mathbb{N}$. Let $P\left(GF\left(q^{d+1}\right)\right)$ denote the projective space, of dimension d, developed over $GF\left(q^{d+1}\right)$. Let $F : GF\left(q^{d+1}\right) \to GF(q)$ be a quadratic form. For $x \in GF\left(q^{d+1}\right)$, let $\langle x \rangle$ denote the point of $P\left(GF\left(q^{d+1}\right)\right)$ that contains x. Then

$$\mathcal{Q}' = \{\langle x \rangle | F(x) = 0\}$$

is a *quadric* in $P\left(GF\left(q^{d+1}\right)\right)$. Let α generate the cyclic group

$$G = GF\left(q^{d+1}\right)^* / GF(q)^*.$$

Define $\mathcal{Q} \in \mathbb{Z}[G]$ by the rule that $\mathcal{Q} = \sum \delta_i \alpha^i$, where $\delta_i = 1$ if $\alpha^i \in \mathcal{Q}'$ and $\delta_i = 0$ otherwise.

The synthetic analogue of the notion of a quadric is the notion of a quadratic set (see, for example, [18], Ch. 2). We say that a line ℓ of $P\left(GF\left(q^{d+1}\right)\right)$ is *tangent* to a set of points Q if either ℓ intersects Q in exactly one point or ℓ is contained in Q. For $p \in Q$, the *tangent space* T_p of p relative to Q is the set of all points that lie on tangent lines that pass through p. We say that Q is a quadratic set if the following two conditions hold:

(i) Any line that intersects Q in 3 points is contained in Q.

(ii) For each $p \in Q$, T_p is either a hyperplane or the whole space $P\left(GF\left(q^{d+1}\right)\right)$.

If d is even, then Q is a quadric if and only if Q is a quadratic set (actually, this is always the case, unless $d = 3$; see [6], [21] and [23]). If for each $p \in Q$, T_p is a hyperplane, then Q is a *non-degenerate* quadric.

From here on, let tr denote the usual field trace (with the stipulation that, for $\langle y \rangle = \langle \alpha^i \rangle \in G$, $\mathrm{tr}\left(\alpha^i\right) = \mathrm{tr}(y)$). The following result is well-known (see [7], [11] or [12]).

Theorem 1 *For each i, j,*

$$\left\{\langle x \rangle | \mathrm{tr}\left(x^{q^i+q^j}\right) = 0\right\}$$

is a quadric in $P\left(GF\left(q^{d+1}\right)\right)$.

Let $D' = \{d_1, \ldots, d_k\}$ be a set of k residues (mod v). Then D' is a (v, k, λ) *cyclic difference set* if, for each residue x (mod v), there exist exactly λ pairs (d_i, d_j) such that $d_i - d_j = x$. Let z generate the cyclic group G of order v. The existence of a (v, k, λ) cyclic difference set D' is equivalent to the existence of an element $D \in \mathbb{Z}[G]$ such that

$$DD^{(-1)} = k + \lambda\left(z + \cdots + z^{v-1}\right).$$

The set of non-zero powers of the group ring element $G - D$ is a $(v, v-k, v-2k+\lambda)$ cyclic difference set called the *complement of* D'. The next result, known as Singer's Theorem (see [10] and [22]), establishes the existence of a class of cyclic difference sets.

Theorem 2 *The coefficients of the powers of* α *in the set*

$$E = \left\{\alpha^i | \mathrm{tr}\left(\alpha^i\right) = 0\right\},$$

comprise a (v, k, λ) *cyclic difference set, with*

$$v = \frac{q^{d+1}-1}{q-1},\ k = \frac{q^d-1}{q-1},\ \lambda = \frac{q^{d-1}-1}{q-1}.$$

Further, the map $x \to \alpha x$ *is an automorphism of* $P\left(GF\left(q^{d+1}\right)\right)$ *that preserves subspaces, and each hyperplane of* $P\left(GF\left(q^{d+1}\right)\right)$ *can be written as a coset* $\alpha^j E$ *of* E.

Let $\gcd(v, t) = 1$. We say that t is a *multiplier* of a group ring element T if there exists $\alpha^i \in G$ such that

$$T^{(t)} = \alpha^i T.$$

The next theorem is due to Gordon, Mills and Welch (see [5]).

Theorem 3 *A number* m *is a multiplier of* E *if and only if* m *is a power of* q.

Let $\sum_{i=0}^{v-1} c_i g^i$ be the group ring polynomial corresponding to a cyclic difference set D. Then, following ([2] and [3]), we stipulate that D has a *Waterloo decomposition* if there exists a circulant weighing matrix W with group ring polynomial $\sum_{i=0}^{v-1} a_i g^i$ such that $\sum_{i=0}^{v-1} |a_i| g^i = \sum_{i=0}^{v-1} c_i g^i$. From here on, let $d = 2f$, for some $f \in \mathbb{N}$. For each $t \leq d$, let

$$Q_t = \left\{\langle x\rangle \in P\left(GF\left(q^{d+1}\right)\right) \mid \mathrm{tr}\left(x^{q^t+1}\right) = 0\right\}$$

and let

$$C_t = \frac{1}{q^{f-1}}\left(EQ_t^{(-1)} - \lambda G\right).$$

For $t \in \mathbb{Z}$, let $\mathbb{Z}_t^*$ denote the group of units modulo t and let $\phi(t) = |\mathbb{Z}_t^*|$.

Theorem 4 (below) generalizes Theorem 4.1 from [2] (an exposition of which can be found in Section 3.3 of [19]). As such, Theorem 4 partially addresses a problem raised in ([2], pp. 328–329): namely, that of determining the number of equivalence classes of circulant weighing matrices that arise as Waterloo decompositions of $G - E$.

It turns out that Theorem 4 is similar to some results that have already been proven (see Propositions 2.1 and 2.2 from [16]). The results from [16] are more general in the case that q is an even prime power but do not apply if q is an odd prime power. Further, by Theorem 3.1 from [3], the approach from [16] cannot be extended to cover the case that q is odd.

Theorem 4 *For each $t \in \mathbb{Z}_{d+1}^*$, Q_t is a non-degenerate quadric of $P\left(GF\left(q^{d+1}\right)\right)$, and C_t is a Waterloo decomposition of $G - E$. For $t, s \in \mathbb{Z}_{d+1}^*$, C_t and C_s are equivalent as circulant weighing matrices if and only if there exists $\beta \in P\left(GF\left(q^{d+1}\right)\right)$ such that $Q_t = \beta Q_s$; and $Q_t = \beta Q_s$, for some $\beta \in P\left(GF\left(q^{d+1}\right)\right)$, if and only if $t = (d+1) - s$. So there are at least $\phi(d+1)/2$ inequivalent $CW\left(v, q^d\right)$'s.*

Proof: Let $t \in \mathbb{Z}_{d+1}^*$. Note that the roots of the polynomial

$$\theta_1(y) = y^t + 1$$

are all non-trivial $2t^{\text{th}}$ roots of unity and that the roots of the polynomial

$$\theta_2(y) = \frac{y^{d+1} - 1}{y - 1}$$

are all $(d+1)^{\text{th}}$ roots of unity. It follows, since $(d+1, 2t) = 1$, that $\theta_1(y)$ and $\theta_2(y)$ have no common roots and, consequently, no common factors. Further, since $\theta_1(y)$ and $\theta_2(y)$ are both monic, there exists no $u \in \mathbb{Z} - \{1\}$ such that $u|\theta_1(y)$ and $u|\theta_2(y)$. Therefore, $(q^t + 1, v) = 1$. So, we can write $Q_t = E^{\left(\left(q^t+1\right)^{-1}\right)}$, and it follows that Q_t has the same cardinality as the difference set E.

Let $t \in \mathbb{Z}_{d+1}^*$. By Theorem 1, Q_t is a quadric. If q is even and $t \in \mathbb{Z}_{d+1}^*$, then reasoning similar to the proof of the even case given in the proof of Theorem 4.1 from [2] (or, alternatively, [19] p. 98) suffices to show that Q_t is a non-degenerate quadric and that C_t is a Waterloo decomposition of $G - E$.

The case that q is odd requires somewhat less trivial modifications to the argument from [2]. In order to show that Q_t is non-degenerate, we will show that there exists no $z \in Q_t$ such that

$$x \in Q_t \implies (z + x) \in Q_t.$$

Suppose that there is such a $z \in Q_t$. Then, since $(t, d+1) = 1$, for each $x \in Q_t$,

$$0 = \text{tr}(z + x)^{q^t+1} = \text{tr}\left(z^{q^t}x + zx^{q^t}\right) = \text{tr}\left(x\left(z^{q^t} + z^{q^{-t}}\right)\right).$$

So, since Q_t has the same cardinality as a hyperplane, if $z^{q^t} + z^{q^{-t}} \neq 0$, Q_t is the hyperplane

$$\left\{\langle x\rangle \in P\left(GF\left(q^{d+1}\right)\right) | \text{tr}\left(x\left(z^{q^t} + z^{q^{-t}}\right)\right) = 0\right\}.$$

By Theorem 3, however, this is impossible since the inverses of powers of q are powers of q and, consequently, $\left(q^t + 1\right)^{-1}$ is not a power of q and, hence, not a multiplier of E.

So, $z^{q^t} + z^{q^{-t}} = 0$, and therefore, $(z^2)^{q^{2t}} = z^2$. Since $(d+1, 2t) = 1$, we must have that $(z^2)^q = z^2$. It follows that $z^2 \in GF(q)$, and, consequently, that

$$z^{q^t+1} = \left(z^2\right)^{\left(q^t+1\right)/2} \in GF(q).$$

But then

$$\mathrm{tr}\left(z^{q^t+1}\right) = z^{q^t+1} \neq 0,$$

which contradicts the fact that $z \in Q_t$. This contradiction proves that Q_t is a non-degenerate quadric. At this point, reasoning similar to the proof of Theorem 4.1 from [2] (or from [19] p. 98) suffices to show that C_t is a Waterloo Decomposition of $G - E$.

Let $1 \leq s \neq t \leq d$. Assume C_s is equivalent to C_t. Then there exist m and r such that $C_s^{(m)} = \alpha^r C_t$. Since C_s and C_t are Waterloo Decompositions of $G - E$, m is a multiplier of $G - E$. It follows that m is also a multiplier of E. Thus, there exists r_1 such that

$$\begin{aligned} C_s^{(m)} &= \frac{1}{q^{f-1}}\left(E^{(m)}\left(\left(E^{(m)}\right)^{\left((q^s+1)^{-1}\right)}\right)^{(-1)} - \lambda G\right) \\ &= \alpha^{r_1}\frac{1}{q^{f-1}}\left(E\left(E^{\left((q^s+1)^{-1}\right)}\right)^{(-1)} - \lambda G\right). \end{aligned}$$

Consequently, since $C_s^{(m)} = \alpha^r C_t$, there exists r_2 such that

$$E\left(E^{\left((q^s+1)^{-1}\right)}\right)^{(-1)} = \alpha^{r_2} E\left(E^{\left(\left(q^t+1\right)^{-1}\right)}\right)^{(-1)}.$$

Multiplying both sides by $E^{(-1)}$ and simplifying, we deduce that

$$E^{\left((q^s+1)^{-1}\right)} = \alpha^{-r_2} E^{\left(\left(q^t+1\right)^{-1}\right)},$$

i.e. that

$$E^{\left((q^s+1)^{-1}\left(q^t+1\right)\right)} = \alpha^{-r_2\left(q^t+1\right)} E.$$

By Theorem 3, then, there exists $0 \leq w \leq d$ such that

$$\left(q^s+1\right)^{-1}\left(q^t+1\right) \equiv q^w \pmod{v},$$

i.e. such that

$$q^t + 1 \equiv q^{w+s} + q^w \pmod{v}.$$

This equation cannot hold unless either $q^w \equiv 1 \pmod{v}$ or $q^{w+s} \equiv 1 \pmod{v}$, i.e. unless either $w = 0$ (in which case $s = t$, which is impossible) or $w = (d+1) - s$, in which case $t = (d+1) - s$. Of course, this reasoning can easily be reversed. It follows that C_s and C_t are equivalent if and only if $t = (d+1) - s$. □

3 The cross-correlation bound

The question of determining the values taken by the cross-correlation function of pairs of perfect ternary sequences associated with these circulant weighing matrices reduces to determining the intersection properties of pairs of the quadrics of the form Q_t. The authors of [13] were able to determine upper and lower bounds for the size of such intersections.

Theorem 5 [13] *Let $d+1 \geq 5$ and let Q and Q' be two non-degenerate quadrics in $P\left(GF\left(q^{d+1}\right)\right)$; then*

$$\frac{q^{2f-2}-q^f+q^{f-1}-1}{q-1} \;\leq\; |Q \cap Q'| \;\leq\; \frac{2q^{2f-1}-q^{2f-2}+q^{f+1}-q^f-1}{q-1}.$$

Making use of this result, we obtain the following bound on the size of the values taken by the cross-correlation function of any pair of these perfect ternary sequences.

Theorem 6 *Let $d+1 \geq 5$, let $s,t, \in \mathbb{Z}_{d+1}^*$, and let $s \neq t, (d+1)-t$. Let*

$$C_s C_t^{(-1)} = \sum a_i \alpha^i.$$

Then, for each i,

$$\frac{-q^{2f+2}+3q^{2f+1}-3q^{2f}+q^{2f-1}-q^{f+3}+3q^{f+2}-3q^{f+1}+q^f}{(q-1)^3} \leq a_i$$

and

$$a_i \leq \frac{q^{2f+2}-3q^{2f+1}+3q^{2f}-q^{2f-1}+q^{f+4}-3q^{f+3}+3q^{f+2}-q^{f+1}}{(q-1)^3}.$$

Proof:

$$C_s C_t^{(-1)} = \frac{1}{q^{2f-2}}\left((k-\lambda)Q_s Q_t^{(-1)} - k^2\lambda G + \lambda^2 v G\right).$$

Note that, for each i, the coefficient of α^i in $Q_s Q_t^{(-1)}$ is equal to

$$\left|\alpha^{-i}Q_s \cap Q_t\right|.$$

Suppose that a line ℓ intersects $\alpha^{-i}Q_s$ in 3 points but that it is not contained in $\alpha^{-i}Q_s$. Then $\alpha^i\ell$ intersects Q_s in 3 points and is not contained in it. However, this is impossible since Q_s is a quadric and, by Theorem 2, $\alpha^i\ell$ is a line.

Now let $p \in \alpha^{-i}Q_s$ and let T_p be the set of all points that lie on lines tangent to $\alpha^{-i}Q_s$ at p. Then $\alpha^i T_p$ is the set of all points that lie on lines tangent to Q_s at $\alpha^i p$. But then, since Q_s is non-degenerate, it follows that $\alpha^i T_p$ is a hyperplane and, by Theorem 2, so is T_p.

Therefore, for each i, $\alpha^{-i}Q_s$ is a non-degenerate quadric distinct from Q_t (distinct by Theorem 4).

So, by Theorem 5,

$$\begin{aligned}
&\frac{-q^{2f+2}+3q^{2f+1}-3q^{2f}+q^{2f-1}-q^{f+3}+3q^{f+2}-3q^{f+1}+q^f}{(q-1)^3}\\
&= \frac{1}{q^{2f-2}}\left((k-\lambda)\left(\frac{q^{2f-2}-q^f+q^{f-1}-1}{q-1}\right)-k^2\lambda+\lambda^2 v\right)\\
&\leq a_i\\
&\leq \frac{1}{q^{2f-2}}\left((k-\lambda)\left(\frac{2q^{2f-1}-q^{2f-2}+q^{f+1}-q^f-1}{q-1}\right)-k^2\lambda+\lambda^2 v\right)\\
&= \frac{q^{2f+2}-3q^{2f+1}+3q^{2f}-q^{2f-1}+q^{f+4}-3q^{f+3}+3q^{f+2}-q^{f+1}}{(q-1)^3}.
\end{aligned}$$

□

Note that for each $i \in [1, v-1]$, as $q \to \infty$, $\mathcal{O}\left(\frac{a_i}{q^d}\right) = \frac{1}{q}$.

References

[1] K. T. Arasu and J. F. Dillon, *Perfect Ternary Sequences*, Difference Sets, Sequences, and their Correlation Properties, Eds. A. Pott, P.V. Kumar, T. Helleseth and D. Jungnickel, Springer, 1999, 1–16.

[2] K. T. Arasu, J. F. Dillon, D. Jungnickel and A. Pott, The Solution of the Waterloo Problem, *J. Combin. Theory Ser. A* **17** (1995), 316–331.

[3] K. T. Arasu, J. F. Dillon, Ka Hin Leung and Siu Lun Ma, Cyclic Relative Difference Sets with Classical Parameters, *J. Combin. Theory Ser. A* **94** (2001), 118–126.

[4] K. T. Arasu, Ka Hin Leung, Siu Lun Ma, Ali Nabavi and D. K. Ray-Chaudhuri, Circulant Weighing Matrices of Weight 2^{2t}, *Des. Codes, Crypto.* **41** (2006), 111–123.

[5] L. D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics **182**, Springer-Verlag, 1971.

[6] F. Buekenhout, *Ensembles Quadratiques des Espaces Projectifs*, **110** (1969), 306–318.

[7] Richard A. Games, *The Geometry of Quadrics and Correlations of Sequences*, IEEE Transactions on Information Theory **32** (1986), no. 3, 423–426.

[8] Anthony V. Geramita and Jennifer Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, Inc., 1979.

[9] Solomon W. Golomb and Guang Gong, *Signal Design for Good Correlation*, Cambridge university press, 2005.

[10] Marshall Hall Jr., Combinatorial Theory, John Wiley and Sons, 1998.

[11] Tom Hoholdt and Jorn Justesen, *Ternary Sequences with Perfect Periodic Autocorrelation*, IEEE Transactions on Information Theory **29** (1983), no. 4, 597–600.

[12] W. A. Jackson and P. R. Wild, *Relations Between Two Perfect Ternary Sequence Constructions*, Designs, Codes, and Cryptography **2** (1992), 325–332.

[13] David B. Leep and Laura Mann Schueller, *Zeroes of a Pair of Quadratic Forms Defined Over a Finite Field*, Finite Fields and Their Applications **5** (1999), 157–176.

[14] Ka Hin Leung and Bernhard Schmidt, *The Field Descent Method*, Designs, Codes, and Cryptography **36** (2005), no. 2, 171–188.

[15] Ka Hin Leung and Bernhard Schmidt, *Finiteness of Circulant Weighing Matrices of Fixed Weight*, Journal of Combinatorial Theory (A) **118** (2011), Issue 3, 908–919.

[16] Ka Hin Leung, Siu Lun Ma, and Bernhard Schmidt, *Constructions of Relative Difference Sets with Classical Parameters and Circulant Weighing Matrices*, Journal of Combinatorial Theory (A) **99** (2002), 111–127.

[17] Hans Dieter Luke, *Sequences and Arrays with Perfect Periodic Correlation*, IEEE Transactions on Aerospace and Electronic Systems **24** (1988), No. 3, 287–294.

[18] Goldwyn Millar, *Circulant Weighing Matrices*, M.Sc. Thesis, University of Manitoba, February, 2010.

[19] Alexander Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics, Springer, 1995.

[20] Michael B. Pursley and Dilip V. Sarwate, *Crosscorrelation Properties of Pseudorandom and Related Sequences*, Proceedings of the IEEE **68** (1980), no.5, 593–619.

[21] B. Segre, *Sulle Ovali Nei Piani Finiti*, Atti Accad. Naz. Lincei Rendic. **17** (1954), 141–142.

[22] J. Singer, *A Theorem in Finite Projective Geometry and Some Applications to Number Theory*, Transactions of the American Mathematical Society **43** (1938), no. 3, 377–385.

[23] J. A. Thas, *On Semi-Ovals and Semi-Ovoids*, Geometriae Dedicata **3** (1974), no. 3, 229–231.

[24] Jennifer Seberry Wallis and Albert Leon Whitman, *Some Results on Weighing Matrices*, Bulletin of the Australian Mathematical Society **12** (1975), 433–447.

(Received 13 Apr 2010; revised 18 July 2012)