On infinite families of sequences with one and two valued autocorrelation and two valued crosscorrelation function

Marc Gysin

Bullant Technology,
181 Miller Street,
North Sydney, NSW 2060, Australia.
e-mail: Marc.Gysin@bullant.com

Jennifer Seberry*

Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong, NSW 2500, Australia
e-mail: jennie@uow.edu.au

Abstract

We show how to construct infinite families of sequences that have one and two valued autocorrelation and two valued crosscorrelation function. These sequences are obtained via the discrete Fourier transform of integer sequences. The sequences obtained can be complex valued or having entries $\in \{0, 1, \ldots, p\}$, p prime, depending on the construction used.

1 Introduction

We shall make use of the following notations: (i) $\mathcal{Z}$, $\mathcal{R}$ and $\mathcal{C}$ will denote the integers, real numbers and complex numbers, respectively; (ii) if $a \in \mathcal{C}$ then a^* is its complex conjugate and $Re(a)$ and $Im(a)$ denote its real and imaginary part, respectively; (iii) when talking about a sequence of length ℓ, subscripts are to be taken reduced modulo ℓ.

*Research supported by Large ARC Grants A9803826, A49703117 and a small ARC Grant. This paper has been written while the first author was at the University of Wollongong.

Let $\mathcal{S}$ be a set and let $X = \{x_0, \ldots, x_{\ell-1}\}$ be a sequence where $x_i \in \mathcal{S}$, for $i = 0, \ldots, \ell - 1$. We call X a *binary sequence* or *ternary sequence* if $\mathcal{S} = \{-1, 1\}$ or $\mathcal{S} = \{-1, 0, 1\}$, respectively.

The *periodic autocorrelation function* $P_X(s)$, of a sequence X with shift s is defined as:

$$P_X(s) = \sum_{i=0}^{\ell-1} x_i x_{i+s}.^1$$

We are interested in one or two binary or ternary sequence(s) X or X, Y such that

$$P_X(s) = c \text{ or } P_X(s) + P_Y(s) = c, \quad s = 1, \ldots, \ell - 1. \tag{1}$$

If we let $w = P_X(0)$ or $w = P_X(0) + P_Y(0)$ and $w \neq c$ then we say that the periodic autocorrelation function of X or X and Y is *two valued.* If $w = c$ then we say the periodic autocorrelation function is *one valued.*

The *periodic crosscorrelation function* $C_{X,Y}(s)$ of two sequences X, Y with shift s is defined as:

$$C_{X,Y}(s) = \sum_{i=0}^{\ell-1} x_i y_{i+s}.$$

Note that for $s \neq 0$ generally $C_{X,Y}(s) \neq C_{Y,X}(s)$. If

$$C_{X,Y}(s) = c, \quad s = 1, \ldots, \ell - 1 \tag{2}$$

and $C_{X,Y}(0) = w$, then we say that the periodic crosscorrelation function of X and Y is *one valued* or *two valued*, if $w = c$ or $w \neq c$, respectively.

Binary or ternary sequences satisfying (1) or (2) play an important role in communication and combinatorial design theory, [GavLem94], [GerSeb79], [Paterson98], [SebYam92]. Unfortunately, such sequences are hard to find for larger lengths ℓ.

We generalise and let $\mathcal{S} = \mathcal{C}$, or $\mathcal{S} = \{0, \ldots, p - 1\}$, where p is a prime and show how to construct infinite families of sequences having properties (1) and (2) for any length ℓ. If $\mathcal{S} = \mathcal{C}$, all the calculations are to be done in the field of complex numbers, whereas for $\mathcal{S} = \{0, \ldots, p - 1\}$ all the calculations are in the field $GF(p)$.

2 The Constructions

Let $\mathcal{S}_1 = \mathcal{Z}$, where $\mathcal{Z}$ are the integers and let $\mathcal{S}_2 = \mathcal{C}$. We start with an integer sequence $A = \{a_0, \ldots, a_{\ell-1}\}$, $a_k \in \mathcal{S}_1$ and we let $X = \{x_0, \ldots, x_{\ell-1}\}$, $Y = \{y_0, \ldots, y_{\ell-1}\}$

[1] In the terms of the above sum, the second factor is *not* the complex conjugate as seen in many definitions of the periodic autocorrelation function. The reason why we do not take the complex conjugate is to keep definitions consistent throughout this paper which otherwise would not be possible.

where

$$x_k = \sum_{j=0}^{\ell-1} a_j e^{2\pi ijk/\ell}, \quad y_k = \sum_{j=0}^{\ell-1} a_j e^{-2\pi ijk/\ell} \tag{3}$$

and $i^2 = -1$. Observe that x_k is the k–th element of the discrete Fourier transform of the sequence A and $x_k = x^*_{-k} = y^*_k$. Also $x_k, y_k \in \mathcal{S}_2$.

We first prove:

Lemma 1 *Altering the sign of one element of A does not affect the periodic crosscorrelation function of X and Y. More precisely, let A and $\tilde{A}$ be two integer sequences such that $\tilde{a}_p = -a_p$ for some $p \in \{0, \ldots, \ell-1\}$ and $\tilde{a}_k = a_k$ for all other elements. Let X, Y and $\tilde{X}$, $\tilde{Y}$ be the sequences obtained from A and $\tilde{A}$, respectively according to (3). Then*

$$C_{\tilde{X},\tilde{Y}}(s) = C_{X,Y}(s) \text{ and } C_{\tilde{Y},\tilde{X}}(s) = C_{Y,X}(s) \tag{4}$$

for all $s = 0, \ldots, \ell-1$.

Proof. For symmetry reasons it is sufficient to prove $C_{X,Y}(s) = C_{\tilde{X},\tilde{Y}}(s)$. Consider

$$\Delta_s = C_{\tilde{X},\tilde{Y}}(s) - C_{X,Y}(s).$$

We have

$$\Delta_s = \sum_{k=0}^{\ell-1}\sum_{j=0}^{\ell-1}\sum_{u=0}^{\ell-1} \tilde{a}_j \tilde{a}_u e^{2\pi i(jk-uk-us)/\ell} - \sum_{k=0}^{\ell-1}\sum_{j=0}^{\ell-1}\sum_{u=0}^{\ell-1} a_j a_u e^{2\pi i(jk-uk-us)/\ell}$$

which is

$$-2a_p\Big(\sum_{k=0}^{\ell-1}\sum_{u=0,u\neq p}^{\ell-1} a_u e^{2\pi i(pk-uk-us)/\ell} + \sum_{k=0}^{\ell-1}\sum_{j=0,j\neq p}^{\ell-1} a_j e^{2\pi i(jk-pk-ps)/\ell}\Big)$$

because of the construction of $\tilde{A}$ and A. We exchange the two sum–operators and obtain

$$-2a_p\Big(\sum_{u=0,u\neq p}^{\ell-1}\sum_{k=0}^{\ell-1} a_u e^{2\pi ik(p-u)/\ell} e^{-2\pi ius/\ell} + \sum_{j=0,j\neq p}^{\ell-1}\sum_{k=0}^{\ell-1} a_j e^{2\pi ik(j-p)/\ell} e^{-2\pi ips/\ell}\Big)$$

which can be written as

$$-2a_p\Big(\sum_{u=0,u\neq p}^{\ell-1} a_u e^{-2\pi ius/\ell} \sum_{k=0}^{\ell-1} e^{2\pi ik(p-u)/\ell} + \sum_{j=0,j\neq p}^{\ell-1} a_j e^{-2\pi ips/\ell} \sum_{k=0}^{\ell-1} e^{2\pi ik(j-p)/\ell}\Big).$$

Because $u \neq p \neq j$ the two innermost sums both evaluate to zero. Therefore, all the summations are over zero and $\Delta_s = 0$. Because no specifications have been made about s, $\Delta_s = 0$, for all $s \in \{0, \ldots, \ell-1\}$.

The above lemma allows us to prove the following:

Theorem 2 *Let $A = \{a_0, \ldots, a_{\ell-1}\}$ be any integer sequence such that $a_0 = |a|$ and $|a_1| = |a_2| = \ldots = |a_{\ell-1}| = b$. Then*

$$C_{X,Y}(0) = \ell(a^2 - b^2) + \ell^2 b^2$$
$$C_{X,Y}(s) = \ell(a^2 - b^2), \quad s = 1, \ldots, \ell - 1$$

and the same is true for $C_{Y,X}(s)$.

In other words, the periodic crosscorrelation function of X and Y is two valued with values $\ell(a^2 - b^2) + \ell^2 b^2$ and $\ell(a^2 - b^2)$, respectively.

Proof. Because of Lemma 1 we are allowed to assume that $a_0 = a$, $a_1 = a_2 = \ldots = a_{\ell-1} = b$. Consider now $C_{X,Y}(s)$ for $s \neq 0$. We have

$$\begin{aligned} C_{X,Y}(s) &= \sum_{k=0}^{\ell-1} \sum_{j=0}^{\ell-1} \sum_{u=0}^{\ell-1} a_j a_u e^{2\pi i(jk-uk-us)/\ell} \\ &= \sum_{k=0}^{\ell-1} (\sum_{u=1}^{\ell-1} abe^{-2\pi iu(k+s)/\ell} + \sum_{j=1}^{\ell-1} abe^{2\pi ijk/\ell} + a^2) + \sum_{k=0}^{\ell-1} \sum_{j=1}^{\ell-1} \sum_{u=1}^{\ell-1} b^2 e^{2\pi i(jk-uk-us)/\ell}. \end{aligned}$$

We first evaluate the two leftmost sums.

$$\begin{aligned} &\sum_{k=0}^{\ell-1} (\sum_{u=1}^{\ell-1} abe^{-2\pi iu(k+s)/\ell} + \sum_{j=1}^{\ell-1} abe^{2\pi ijk/\ell} + a^2) \\ &= \ell a^2 - 2\ell ab + \sum_{k=0}^{\ell-1} (\sum_{u=0}^{\ell-1} abe^{-2\pi iu(k+s)/\ell} + \sum_{j=0}^{\ell-1} abe^{2\pi ijk/\ell}). \end{aligned}$$

The two innermost sums of this expressions evaluate to zero, except for the case $k = -s$ and $k = 0$, respectively. In this case both innermost sums evaluate to ℓab. Therefore,

$$\begin{aligned} &\sum_{k=0}^{\ell-1} (\sum_{u=1}^{\ell-1} abe^{-2\pi iu(k+s)/\ell} + \sum_{j=1}^{\ell-1} abe^{2\pi ijk/\ell} + a^2) \\ &= \ell a^2 - 2\ell ab + (\ell - 1)(0 + 0) + \ell ab + \ell ab = \ell a^2. \end{aligned}$$

The rightmost sum is:

$$\begin{aligned} &\sum_{k=0}^{\ell-1} \sum_{j=1}^{\ell-1} \sum_{u=1}^{\ell-1} b^2 e^{2\pi i(jk-uk-us)/\ell} \\ &= \sum_{k=0}^{\ell-1} \sum_{j=0}^{\ell-1} \sum_{u=0}^{\ell-1} b^2 e^{2\pi i(jk-uk-us)/\ell} - \sum_{k=0}^{\ell-1} (\sum_{u=1}^{\ell-1} b^2 e^{-2\pi iu(k+s)/\ell} + \sum_{j=1}^{\ell-1} b^2 e^{2\pi ijk/\ell} + b^2). \end{aligned}$$

Now similarly to the above

$$\sum_{k=0}^{\ell-1} (\sum_{u=1}^{\ell-1} b^2 e^{-2\pi iu(k+s)/\ell} + \sum_{j=1}^{\ell-1} b^2 e^{2\pi ijk/\ell} + b^2) = \ell b^2$$

and it can be shown (using similar techniques) that for $s \neq 0$

$$\sum_{k=0}^{\ell-1}\sum_{j=0}^{\ell-1}\sum_{u=0}^{\ell-1} b^2 e^{2\pi i(jk-uk-us)/\ell} = 0.$$

Therefore, the rightmost sum is $-\ell b^2$ and $C_{X,Y}(s) = \ell(a^2 - b^2)$, $s \neq 0$. It remains to consider $C_{X,Y}(0)$. Since no assumptions have been made about s except for

$$\sum_{k=0}^{\ell-1}\sum_{j=0}^{\ell-1}\sum_{u=0}^{\ell-1} b^2 e^{2\pi i(jk-uk-us)/\ell} = 0$$

we know

$$C_{X,Y}(0) = \ell(a^2 - b^2) + \sum_{k=0}^{\ell-1}\sum_{j=0}^{\ell-1}\sum_{u=0}^{\ell-1} b^2 e^{2\pi i(jk-uk)/\ell}.$$

But

$$\sum_{k=0}^{\ell-1}\sum_{j=0}^{\ell-1}\sum_{u=0}^{\ell-1} b^2 e^{2\pi i(jk-uk)/\ell} = b^2 \sum_{j=0}^{\ell-1}\sum_{u=0}^{\ell-1}\sum_{k=0}^{\ell-1} e^{2\pi ik(j-u)/\ell} = b^2\ell^2$$

because the innermost sum vanishes except for $j = u$ when it assumes the value ℓ. Therefore, $C_{X,Y}(0) = \ell(a^2 - b^2) + \ell^2 b^2$.

Corollary 3 *Let the sequence X be as in Theorem 2 and write $x_k = r_k + iw_k$. Let R, W be the sequences $\{r_0, \ldots, r_{\ell-1}\}$ and $\{w_0, \ldots, w_{\ell-1}\}$, respectively. Then*

$$P_R(s) + P_W(s) = \begin{cases} \ell(a^2 - b^2) + \ell^2 b^2 & s = 0 \\ \ell(a^2 - b^2) & s = 1, \ldots, \ell - 1 \end{cases}$$

and

$$C_{R,W}(s) = C_{W,R}(s),$$

for $s = 0, \ldots, \ell - 1$.

Proof. Consider $C_{X,Y}(s) = \sum_{k=0}^{\ell-1}(r_k + iw_k)(r_{k+s} - iw_{k+s}) = P_R(s) + P_W(s) + i(C_{W,R}(s) - C_{R,W}(s))$.

We now show how to construct sequences with one valued periodic autocorrelation function.

Lemma 4 *Let A be an integer sequence satisfying for $k \neq 0$, $a_k \neq 0 \Longrightarrow a_{-k} = 0$. Then "deleting" one element not at the beginning of A does not affect the periodic autocorrelation function of X and Y. More precisely, let A be as above and let $\tilde{A}$ be an integer sequences such that $\tilde{a}_p = 0$ for some $p \neq 0$ where $a_p \neq 0$ and $\tilde{a}_k = a_k$ for all other elements. Let X, Y and $\tilde{X}$, $\tilde{Y}$ be the sequences obtained from A and $\tilde{A}$, respectively according to (3). Then*

$$P_{\tilde{X}}(s) = P_X(s) \text{ and } P_{\tilde{Y}}(s) = P_Y(s) \tag{5}$$

for all $s = 0, \ldots, \ell - 1$.

Proof. Consider

$$\Delta_s = P_X(s) - P_{\tilde{X}}(s).$$

We have

$$\begin{aligned}
\Delta_s &= \sum_{k=0}^{\ell-1}\sum_{j=0}^{\ell-1}\sum_{u=0}^{\ell-1} a_j a_u e^{2\pi i(jk+uk+us)/\ell} - \sum_{k=0}^{\ell-1}\sum_{j=0}^{\ell-1}\sum_{u=0}^{\ell-1} \tilde{a}_j \tilde{a}_u e^{2\pi i(jk+uk+us)/\ell} \\
&= \sum_{k=0}^{\ell-1}\Big(\sum_{u=0,u\neq p}^{\ell-1} a_p a_u e^{2\pi i(pk+uk+us)/\ell} + \sum_{j=0,j\neq p}^{\ell-1} a_j a_p e^{2\pi i(jk+pk+ps)/\ell} + a_p^2 e^{2\pi ip(2k+s)/\ell}\Big) \\
&= \sum_{u=0,u\neq p}^{\ell-1} a_p a_u \sum_{k=0}^{\ell-1} e^{2\pi i(pk+uk+us)/\ell} + \sum_{j=0,j\neq p}^{\ell-1} a_j a_p \sum_{k=0}^{\ell-1} e^{2\pi i(jk+pk+ps)/\ell} \\
&\qquad + a_p^2 \sum_{k=0}^{\ell-1} e^{2\pi ip(2k+s)/\ell}.
\end{aligned}$$

Consider now the three sums:

$$\begin{aligned}
\sum_{k=0}^{\ell-1} e^{2\pi i(pk+uk+us)/\ell} &= e^{2\pi ius/\ell} \sum_{k=0}^{\ell-1} e^{2\pi i(k(p+u))/\ell} \\
\sum_{k=0}^{\ell-1} e^{2\pi i(jk+pk+ps)/\ell} &= e^{2\pi ips/\ell} \sum_{k=0}^{\ell-1} e^{2\pi i(k(j+p))/\ell} \\
\sum_{k=0}^{\ell-1} e^{2\pi i(p(2k+s))/\ell} &= e^{2\pi ips/\ell} \sum_{k=0}^{\ell-1} e^{2\pi i(k2p)/\ell}.
\end{aligned}$$

The last of the three sums is zero because $p \neq 0$. The first and second sum vanish if and only if $u \neq -p$ and $j \neq -p$, respectively. But if $u = -p$ then either $a_p = 0$ or $a_u = 0$ by the assumption about A. Hence,

$$a_p a_u \sum_{k=0}^{\ell-1} e^{2\pi i(pk+uk+us)/\ell} = 0.$$

Similarly for the second sum we always have

$$a_j a_p \sum_{k=0}^{\ell-1} e^{2\pi i(jk+pk+ps)/\ell} = 0.$$

Therefore $\Delta_s = 0$, for $s = 0, \ldots, \ell - 1$.

The above lemma allows us to prove the following:

Theorem 5 *Let* $A = \{a_0, \ldots, a_{\ell-1}\}$ *be any integer sequence such that for* $k \neq 0$, $a_k \neq 0 \Longrightarrow a_{-k} = 0$. *Then*

$$\begin{aligned}
P_X(s) &= \ell a_0^2 \\
P_Y(s) &= \ell a_0^2
\end{aligned}$$

for $s = 0, \ldots, \ell - 1$.

In other words, the periodic autocorrelation function of X or Y is one valued with value ℓa_0^2.

Proof. Because of Lemma 4 we are allowed to assume $a_1 = a_2 = \ldots = a_{\ell-1} = 0$. Now

$$P_X(s) = \sum_{k=0}^{\ell-1} \sum_{j=0}^{\ell-1} \sum_{u=0}^{\ell-1} a_j a_u e^{2\pi i(jk+uk+us)/\ell} = \sum_{k=0}^{\ell-1} a_0^2 = \ell a_0^2.$$

Corollary 6 *Let the sequence X be as in Theorem 5 and write $x_k = r_k + iw_k$. Let R, W be the sequences $\{r_0, \ldots, r_{\ell-1}\}$ and $\{w_0, \ldots, w_{\ell-1}\}$, respectively. Then*

$$P_R(s) - P_W(s) = \ell a^2$$

and

$$C_{R,W}(s) + C_{W,R}(s) = 0,$$

for $s = 0, \ldots, \ell - 1$.

Proof. Consider $P_X(s) = \sum_{k=0}^{\ell-1}(r_k + iw_k)(r_{k+s} + iw_{k+s}) = P_R(s) - P_W(s) + i(C_{W,R}(s) + C_{R,W}(s))$.

Special Constructions

The first construction can be enhanced by putting additional conditions on the integer sequence A. We describe this in the following lemma.

Lemma 7 *Let A be an integer sequence satisfying the conditions of Theorem 2. Then*

(i) if in addition $a_k = a_{-k}$ we have

$$P_X(0) = P_Y(0) = \ell(a^2 - b^2) + \ell^2 b^2$$
$$P_X(s) = P_Y(s) = \ell(a^2 - b^2), \quad s = 1, \ldots, \ell - 1;$$

(ii) if in addition $a_k = -a_{-k}$ and ℓ is odd then

$$P_X(0) = P_Y(0) = \ell(a^2 + b^2) - \ell^2 b^2$$
$$P_X(s) = P_Y(s) = \ell(a^2 + b^2), \quad s = 1, \ldots, \ell - 1.$$

Observe that we now have sequences X or Y with two valued periodic autocorrelation function.

Proof. The proof of (i) is very simple. Because of $a_k = a_{-k}$, X and Y are both real valued. Also $x_k = y_k = x_{-k} = y_{-k}$. That is, $X = Y$, and so, $C_{X,Y}(s) = C_{Y,X}(s) =$

$P_X(s) = P_Y(s)$, for $s = 0, \ldots, \ell - 1$. For (ii) let $w_k = Im(x_k)$. By construction $x_k = a + iw_k$. From Theorem 2 we know that

$$C_{X,Y}(s) = \sum_{k=0}^{\ell-1} x_k y_{k+s} = \ell a^2 + \sum_{k=0}^{\ell-1} w_k w_{k+s} = \begin{cases} \ell(a^2 - b^2) + \ell^2 b^2 & s = 0 \\ \ell(a^2 - b^2) & s = 1, \ldots, \ell - 1. \end{cases}$$

Hence

$$\sum_{k=0}^{\ell-1} w_k w_{k+s} = \begin{cases} -\ell b^2 + \ell^2 b^2 & s = 0 \\ -\ell b^2 & s = 1, \ldots, \ell - 1. \end{cases}$$

Now

$$P_X(s) = \sum_{k=0}^{\ell-1} x_k x_{k+s} = \ell a^2 - \sum_{k=0}^{\ell-1} w_k w_{k+s} = \begin{cases} \ell(a^2 + b^2) - \ell^2 b^2 & s = 0 \\ \ell(a^2 + b^2) & s = 1, \ldots, \ell - 1. \end{cases}$$

3 Altering $\mathcal{S}_1$ and $\mathcal{S}_2$

All the proofs "go through" if we let $\mathcal{S}_1 = \mathcal{R}$ or $\mathcal{S}_1 = \mathcal{C}$, that is, if A is a real or complex valued sequence. If $\mathcal{S}_1 = \mathcal{Z}$, we can also choose $\mathcal{S}_2 = \{0, \ldots, p^\alpha - 1\}$, p prime. Let us briefly focus on this last case. Assume that we want to construct sequences with the above properties of length ℓ. We then have to choose p and α such that $\ell \mid p^\alpha - 1$. Let g be a primitive root of $GF(p^\alpha)$ and let $\tilde{g} = g^{\frac{p^\alpha - 1}{\ell}}$. The sequences X and Y are then obtained by

$$x_k = \sum_{j=0}^{\ell-1} a_j \tilde{g}^{jk} \text{ and } y_k = \sum_{j=0}^{\ell-1} a_j \tilde{g}^{-jk}$$

where all the calculations are to be done in $GF(p^\alpha)$. Because of $\sum_{j=0}^{\ell-1} \tilde{g}^j = 0$, all the proofs from Section 2 remain valid.

4 Examples

Example 1:
Let $\mathcal{S}_1 = \mathcal{Z}$ and $\mathcal{S}_2 = \mathcal{C}$. Let $\ell = 6$ and $A_1 = \{2, 3, -3, 3, 3, -3\}$ and $A_2 = \{2, -3, 3, -3, -3, -3\}$ then

$$X_1 = \{5, -1, 5 + 10.39i, -1, 5 - 10.39i, -1\}$$
$$Y_1 = \{5, -1, 5 - 10.39i, -1, 5 + 10.39i, -1\}$$

and for X_2, Y_2:

$$X_2 = \{-7, 2 + 5.2i, 2 - 5.2i, 11, 2 + 5.2i, 2 - 5.2i\}$$
$$Y_2 = \{-7, 2 - 5.2i, 2 + 5.2i, 11, 2 - 5.2i, 2 + 5.2i\}$$

and

$$C_{X_1,Y_1}(s) = C_{Y_1,X_1}(s) = C_{X_2,Y_2}(s) = C_{Y_2,X_2}(s) = \begin{cases} 294 & s = 0 \\ -30 & s = 1, \ldots, 5. \end{cases}$$

Example 2:
Let $\mathcal{S}_1 = \mathcal{Z}$ and $\mathcal{S}_2 = \mathcal{C}$. Let $\ell = 9$ and $A_1 = \{1, 5, 0, -3, 4, 0, 0, 0, 0\}$ and $A_2 = \{1, 0, 0, 0, 0, -5, 2, 7, 1\}$ then

$$\begin{aligned} X_1 = \{&7, 2.57 + 1.98i, 6.43 + 4.95i, -6.5 + 7.79i, -1.5 - 4.83i, \\ &-1.5 + 4.83i, -6.5 - 7.79i, 6.43 - 4.95i, 2.57 - 1.98i\} \\ Y_1 = \{&7, 2.57 - 1.98i, 6.43 - 4.95i, -6.5 - 7.79i, -1.5 + 4.83i, \\ &-1.5 - 4.83i, -6.5 + 7.79i, 6.43 + 4.95i, 2.57 + 1.98i\} \end{aligned}$$

and for X_2, Y_2:

$$\begin{aligned} X_2 = \{&6, 6.68 - 7.56i, -10.23 - 4.86i, 1.5 + 9.53i, 3.55 - 2.5i, \\ &3.55 + 2.5i, 1.5 - 9.53i, -10.23 + 4.86i, 6.68 + 7.56i\} \\ Y_2 = \{&6, 6.68 + 7.56i, -10.23 + 4.86i, 1.5 - 9.53i, 3.55 + 2.5i, \\ &3.55 - 2.5i, 1.5 + 9.53i, -10.23 - 4.86i, 6.68 - 7.56i\} \end{aligned}$$

and

$$P_{X_1}(s) = P_{Y_1}(s) = P_{X_2}(s) = P_{Y_2}(s) = 9,$$

for $s = 0, \ldots, 8$.

Example 3:
(As Example 1 but now with $\mathcal{S}_2 = \{0, \ldots, 12\}$, $p = 13$. We let $g = 2$, $\tilde{g} = g^2 = 4$.)

$$\begin{aligned} X_1 &= \{5, 12, 8, 12, 2, 12\} \\ Y_1 &= \{5, 12, 2, 12, 8, 12\} \end{aligned}$$

and for X_2, Y_2:

$$\begin{aligned} X_2 &= \{6, 10, 7, 11, 10, 7\} \\ Y_2 &= \{6, 7, 10, 11, 7, 10\} \end{aligned}$$

and

$$C_{X_1,Y_1}(s) = C_{Y_1,X_1}(s) = C_{X_2,Y_2}(s) = C_{Y_2,X_2}(s) = \begin{cases} 8 & s = 0 \\ 9 & s = 1, \ldots, 5. \end{cases}$$

Example 4:
(As Example 1 but now with $\mathcal{S}_2 = \{0, \ldots, 36\}$, $p = 37$. We let $g = 2$, $\tilde{g} = g^6 = 27$.)

$$\begin{aligned} X_1 &= \{5, 36, 27, 36, 20, 36\} \\ Y_1 &= \{5, 36, 20, 36, 27, 36\} \end{aligned}$$

and for X_2, Y_2:

$$X_2 = \{30, 13, 28, 11, 13, 28\}$$
$$Y_2 = \{30, 28, 13, 11, 28, 13\}$$

and

$$C_{X_1,Y_1}(s) = C_{Y_1,X_1}(s) = C_{X_2,Y_2}(s) = C_{Y_2,X_2}(s) = \begin{cases} 35 & s = 0 \\ 7 & s = 1, \ldots, 5. \end{cases}$$

Example 5:
(As Example 2 but now with $\mathcal{S}_2 = \{0, \ldots, 18\}$, $p = 19$. We let $g = 2$, $\tilde{g} = g^2 = 4$.)

$$X_1 = \{7, 17, 11, 4, 11, 3, 2, 7, 4\}$$
$$Y_1 = \{7, 4, 7, 2, 3, 11, 4, 11, 17\}$$

and for X_2, Y_2:

$$X_2 = \{6, 4, 6, 8, 7, 10, 14, 1, 10\}$$
$$Y_2 = \{6, 10, 1, 14, 10, 7, 8, 6, 4\}$$

and

$$P_{X_1}(s) = P_{Y_1}(s) = P_{X_2}(s) = P_{Y_2}(s) = 9,$$

for $s = 0, \ldots, 8$.

Example 6:
Let $\mathcal{S}_1 = \mathcal{Z}$ and $\mathcal{S}_2 = 0, \ldots, 18$, $p = 19$, $g = 2$, $\tilde{g} = g^2 = 4$. Let $\ell = 9$ and $A = \{2, 1, 1, -1, -1, -1, -1, 1, 1\}$ then

$$X = Y = \{1, 7, 3, 17, 15, 15, 17, 3, 7\}$$

and

$$P_X(s) = P_Y(s) = \begin{cases} 5 & s = 0 \\ 0 & s = 0, \ldots, 8. \end{cases}$$

5 A Computer–Search

We have shown constructions that yield sequences with special periodic autocorrelation function for every length ℓ. We can implement a search–program that searches through all sequences which have special periodic autocorrelation function and then checks which ones have certain additional properties (for example all its elements are in $\{-1, 0, 1\}$). "Traditional searches" for such sequences go precisely the other way round: typically a search–program searches through all sequences which have certain properties (for example all its elements are in $\{-1, 0, 1\}$) *and then* checks for special periodic autocorrelation function.

Length ℓ	Sequences R and W	$P_R(s) + P_W(s)$
8	$R = \{2, 2, 2, 2, -6, 2, 2, 2\}$	$64, \ s = 0$
	$W = \{0, 0, 0, 0, 0, 0, 0, 0\}$	$0, \ s \neq 0$
12	$R = \{6, 2, -4, 2, 0, 2, 2, 2, 0, 2, 4, 2\}$	$144, \ s = 0$
	$W = \{0, 2, 0, 4, 0, 2, 0, -2, 0, -4, 0, 2\}$	$0, \ s \neq 0$

Table 1: Sample sequences R and W obtained via Corollary 3

Length ℓ	Sequences R and W	$P_R(s) - P_W(s)$
8	$R = \{6, 0, -2, 0, 2, 0, -2, 0\}$	0
	$W = \{0, 2, 4, -2, 0, 2, -4, -2\}$	
12	$R = \{1, 0, 2, 0, -2, 0, -1, 0, -2, 0, 2, 0\}$	0
	$W = \{0, 0, 0, 3, 0, 0, 0, 0, 0, -3, 0, 0\}$	

Table 2: Sample sequences R and W obtained via Corollary 6

Computational Results

We let $\mathcal{S}_1 = \{-1, 0, 1\}$ and search through sequences R and W according to Lemma 7, Corollaries 3 and 6 and *hope* that $r_k, w_k \in \mathcal{Z}$. We got many results. Table 1 and 2 show a few examples. A sample search is given in the appendix.

Results obtained are somewhat disappointing since the sequences obtained expose a rather simple pattern. The sequences obtained may be constructed directly rather than via the theory and search in this paper.

References

[GavLem94] A. Gavish and A. Lempel, On ternary complementary sequences, *IEEE Transactions on Information Theory*, 40, 2, 522–526, 1994.

[GerSeb79] A.V. Geramita and J.Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York – Basel, 1979.

[GysSeb97] M. Gysin and J. Seberry, An experimental search and new combinatorial designs via a generalisation of cyclotomy, *Journal of Combinatorial Mathematics and Combinatorial Computing*, 27, 143–160, 1998.

[IreRos82] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer–Verlag, New York, 1982.

[Paterson98] K.G. Paterson, Binary sequence sets with Favorable Correlations from Difference Sets and MDS Codes, *IEEE Transactions on Information Theory*, Vol. 44, 1, 172–180, 1998.

[Schroeder84] M.R. Schroeder, *Number Theory in Science and Communication*, Springer–Verlag, New York, 1984.

[SebYam92] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, *Contemporary Design Theory – a Collection of Surveys*, eds. J.Dinitz and D.R. Stinson, John Wiley and Sons, New York, 431–560, 1992.

[Sloane73] N.J.A. Sloane, *A Handbook of Integer Sequences*, Academic Press, New York, 1973.

A Complete Results from Exhaustive Computer–Searches

Construction Lemma 7 (i) with $\ell = 18$, $a = b = 1$, $r_k \in \mathcal{Z}$

(Some information about the seeding sequence A is also printed immediately after the sequence R. We set $a_0 = a = 1$ and then a_1 to a_9 = "sequence printed out" and a_{10} to a_{17} follow from a_1 to a_8.)

```
R: 018* 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 *
+++++++++
R: 016*002*-02*002*-02*002*-02*002*-02*002*-02*002*-02*002*-02*002*-02*002*-02*002*
++++++++-
R: 014*002*002*-04*002*002*-04*002*002*-04*002*002*-04*002*002*-04*002*002*-04*002*002*
+++++-+++
R: 012*004* 0 *-02* 0 *004*-06*004* 0 *-02* 0 *004*-06*004* 0 *-02* 0 *004*
+++++-++-
R: 014*-02*002*004*002*-02*-04*-02*002*004*002*-02*-04*-02*002*004*002*-02*
++-++++++
R: 012* 0 * 0 *006* 0 * 0 *-06* 0 * 0 *006* 0 * 0 *-06* 0 * 0 *006* 0 * 0 *
++-+++++-
R: 010* 0 *004* 0 *004* 0 *-08* 0 *004* 0 *004* 0 *-08* 0 *004* 0 *004* 0 *
++-++-+++
R: 008*002*002*002*002*002*-10*002*002*002*002*002*-10*002*002*002*002*002*
++-++-++-
R: 006* 0 * 0 *006* 0 * 0 *006* 0 * 0 *-12* 0 * 0 *006* 0 * 0 *006* 0 * 0 *
+-+-+++-+
R: 004*002*-02*008*-02*002*004*002*-02*-10*-02*002*004*002*-02*008*-02*002*
+-+-+++--
R: 002*002*002*002*002*002*002*002*002*-16*002*002*002*002*002*002*002*002*
+-+-+-+-+
R:  0 *004* 0 *004* 0 *004* 0 *004* 0 *-14* 0 *004* 0 *004* 0 *004* 0 *004*
```

```
+-+-+-+--
R: 002*-02*002*010*002*-02*002*-02*002*-08*002*-02*002*-02*002*010*002*-02*
+---+++-+
R:  0 * 0 * 0 *012* 0 * 0 * 0 * 0 * 0 *-06* 0 * 0 * 0 * 0 * 0 *012* 0 * 0 *
+---+++--
R: -02* 0 *004*006*004* 0 *-02* 0 *004*-12*004* 0 *-02* 0 *004*006*004* 0 *
+---+-+-+
R: -04*002*002*008*002*002*-04*002*002*-10*002*002*-04*002*002*008*002*002*
+---+-+--
R: 006* 0 * 0 *-06* 0 * 0 *006* 0 * 0 *012* 0 * 0 *006* 0 * 0 *-06* 0 * 0 *
-+++-+-++
R: 004*002*-02*-04*-02*002*004*002*-02*014*-02*002*004*002*-02*-04*-02*002*
-+++-+-+-
R: 002*002*002*-10*002*002*002*002*002*008*002*002*002*002*002*-10*002*002*
-+++---++
R:  0 *004* 0 *-08* 0 *004* 0 *004* 0 *010* 0 *004* 0 *004* 0 *-08* 0 *004*
-+++---+-
R: 002*-02*002*-02*002*-02*002*-02*002*016*002*-02*002*-02*002*-02*002*-02*
-+-+-+-++
R:  0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 *018* 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 *
-+-+-+-+-
R: -02* 0 *004*-06*004* 0 *-02* 0 *004*012*004* 0 *-02* 0 *004*-06*004* 0 *
-+-+---++
R: -04*002*002*-04*002*002*-04*002*002*014*002*002*-04*002*002*-04*002*002*
-+-+---+-
R: -06* 0 * 0 * 0 * 0 * 0 *012* 0 * 0 * 0 * 0 * 0 *012* 0 * 0 * 0 * 0 * 0 *
--+--+--+
R: -08*002*-02*002*-02*002*010*002*-02*002*-02*002*010*002*-02*002*-02*002*
--+--+---
R: -10*002*002*-04*002*002*008*002*002*-04*002*002*008*002*002*-04*002*002*
--+-----+
R: -12*004* 0 *-02* 0 *004*006*004* 0 *-02* 0 *004*006*004* 0 *-02* 0 *004*
--+------
R: -10*-02*002*004*002*-02*008*-02*002*004*002*-02*008*-02*002*004*002*-02*
-----+--+
R: -12* 0 * 0 *006* 0 * 0 *006* 0 * 0 *006* 0 * 0 *006* 0 * 0 *006* 0 * 0 *
-----+---
R: -14* 0 *004* 0 *004* 0 *004* 0 *004* 0 *004* 0 *004* 0 *004* 0 *004* 0 *
--------+
R: -16*002*002*002*002*002*002*002*002*002*002*002*002*002*002*002*002*002*
---------
```

Nr of sequences found: 00032

(Received 10/4/2000)