Array Correlation and Sequences with Equal Magnitude Correlation

DEDICATED TO DR. S. W. GOLOMB ON HIS 70TH BIRTHDAY.

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1
CANADA
Email. ggong@calliope.uwaterloo.ca

Abstract. In this paper, we will investigate cross correlation of sequences over $\mathbb{R}$ where $\mathbb{R}$ is either the integer residue ring $\mathbb{Z}_q$ or the Galios ring $\mathbb{GR}(p^e, d)$ where q, e and d are positive integers and p is a prime. First, in terms of the interleaved structure of sequences, we will introduce a new type of cross correlation between two periodic sequences over $\mathbb{R}$ with period $v = nm$ where $n > 1$ and $m > 1$ are positive integers, which will be called an *array cross/auto correlation* in this paper. Then, we will construct two families of sequences over $\mathbb{R}$ of period $v = nm$. We will show that for each pair of sequences, each taken from different sets, their cross correlation (as a usual difinition) is equal to their array cross correlation. Moreover, the magnitude of the sum of each correlation value and the constant 1 is equal to the constant $n - 1$.

Keywords: Array correlation, cross correlation, and sequences.

1. Introduction

In this paper, we will investigate cross correlation of sequences over $\mathbb{R}$ where $\mathbb{R}$ is either the integer residue ring of modulo q, $\mathbb{Z}_q$ or the Galios ring $\mathbb{GR}(p^e, d)$ which is is a Galois extension of degree d over Z_{p^e} where q, e and d are positive integers and p is a prime. We will also fix the following notation in this paper: $\mathbb{F}_Q = GF(Q)$ is a finite field with Q elements; $\mathbb{F}_Q^*$, the multiplication group of $\mathbb{F}_Q$; $\mathbb{R}^v = (a_0, a_1, \cdots, a_{v-1})$, a module over $\mathbb{R}$; $\mathbf{a} = \{a_i\}$, a sequence over $\mathbb{R}$ if $a_i \in \mathbb{R}$ and if $\mathbf{a}$ is periodic of period v, we also denote $\mathbf{a}$ as a vector in $\mathbb{R}^v$.

First, we will introduce a new type of cross correlation between two periodic sequences over $\mathbb{R}$ with period $v = nm$ where $n > 1$ and $m > 1$ are positive integers, which will be called an *array cross/auto correlation* in this paper. Then, we will construct two families of sequences over $\mathbb{R}$ of period $v = nm$, say $\mathcal{A}$ and $\mathcal{B}$, where each sequence in these sets can

be regarded as a n by m matrix over $\mathbb{R}$. We will show that for each pair of sequences, each taking from different sets, their cross correlation (as a usual difinition) is equal to their array cross correlation. Moreover, the magnitude of the sum of each correlation value and the constant 1 is the constant $n-1$. We would like to point that for different choices of A, B corresponds to bent function over $\mathbb{R}$ and hyper bent functions $\mathbb{R}$, respectively.

This paper is organized as follows. In Sections 2 and 3, we introduce the concepts of array shift operators and array cross/auto correlation functions for sequences over $\mathbb{R}$. In Section 4, we give a construction for the sets $\mathcal{A}$ and $\mathcal{B}$ and prove their array cross correlation property for the binary case.

2. Array Shift Operators

Recall that the (cyclic left) shift operator L on a periodic sequence $\mathbf{a} \in \mathbb{R}^v$ is defined as $L\mathbf{a} = a_1, a_2, \cdots$. For any $i > 0$, $L^i\mathbf{a} = a_i, a_{i+1}, \cdots$. $L^i\mathbf{a}$ is said to be a *phase shift* of A. Note that L is a linear operator on the n-module $\mathbb{R}^n$. We give the following method to convert the sequence $\mathbf{a}$ in $\mathbb{R}^v$ into a matrix in $\mathbb{R}^{n,m}$ where $v = nm$ for both $n > 1$ and $m > 1$.

Conversion 1. For a given sequence $\mathbf{a}$ in $\mathbb{R}^v$, let

$$A = \begin{bmatrix} a_0 & a_1 & \cdots & a_{m-1} \\ a_m & a_{m+1} & \cdots & a_{2m-1} \\ a_{2m} & a_{2m+1} & \cdots & a_{3m-1} \\ \vdots & & & \\ a_{(n-1)m} & a_{(n-1)m+1} & \cdots & a_{nm-1} \end{bmatrix} \tag{1}$$

We say that A is a matrix form of the sequence $\mathbf{a}$, sometimes we denote it as $A_{\mathbf{a}}$ when it is needed for indicating which sequence.

Conversion 2. Given a matrix A in $\mathbb{R}^{n,m}$, we can obtain a sequence in $\mathbb{R}^v$ by reading out the entries in A row by row starting with the first row from left to right.

Thus the conversions 1 and 2 give a one-to-one correspondence between $\mathbb{R}^v$ and $\mathbb{R}^{n,m}$. In the following, we will introduce a shift operator on the matrix ring $\mathbb{R}^{n,m}$. For $A = (a_{k,l}) \in R^{n,m}$, we may write A in

terms of its row vectors and column vectors into the following forms:

$$A = [\mathbf{c}_0(A), \mathbf{c}_1(A), \cdots, \mathbf{c}_{m-1}(A)] = \begin{bmatrix} \mathbf{r}_0(A) \\ \mathbf{r}_1(A) \\ \vdots \\ \mathbf{r}_{n-1}(A) \end{bmatrix}$$

where $\mathbf{r}_i(A)$ and $\mathbf{c}_j(A)$ are the ith row vector and jth column vector of A, respectively, $0 \le i < n; 0 \le j < m$.
Let $\sigma(i,j)$ be an operator on A, defined as follows:

$$\begin{aligned} \sigma^{i,j}(A) \ &= \ [L^i\mathbf{c}_j(A), L^i\mathbf{c}_{j+1}(A), \cdots, L^i\mathbf{c}_{j-1}(A)], \\ &\quad 0 \le i < n, 0 \le j < m \end{aligned} \tag{2}$$

where the index of $\mathbf{c}_j(A)$ is reduced by modulo m. Or equivalently,

$$\sigma^{i,j}(A) = (a_{k+i,l+j})_{n\times m} \tag{3}$$

where the row index $k+i$ is reduced by modulo n and the column index $l+j$ by modulo m.

Definition 1 *With the above notation, $\sigma^{i,j}$, defined by (2), is called an* array (left-upward) shift operator *on A. We also say that $\sigma^{i,j}$ is an* array (left-upward) shift operator *of the sequence* $\mathbf{a}$ *when it is considered as a matrix in $\mathbb{R}^{n,m}$ in the way of (1).*

For example,

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & \boxed{0} & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \Longrightarrow \sigma^{2,1}(A) = \begin{bmatrix} \boxed{0} & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

where $\sigma^{2,1}(A) = [L^2\mathbf{c}_1(A), L^2\mathbf{c}_2(A), L^2\mathbf{c}_3(A), L^2\mathbf{c}_4(A), L^2\mathbf{c}_0(A)]$.

For any $\mathbf{a} \in \mathbb{R}^v$, let A be its matrix form. We can derive the matrix, say D, converted from $L^{im+j}(\mathbf{a})$ as follows:

$$\begin{aligned} D \ &= \ [L^i\mathbf{c}_j(A), L^i\mathbf{c}_{j+1}(A), \cdots, L^i\mathbf{c}_{m-1}(A), L^{i+1}\mathbf{c}_0(A), \cdots, L^{i+1}\mathbf{c}_{j-1}(A)], \\ &\quad 0 \le i < n; 0 \le j < m. \end{aligned} \tag{4}$$

Compared it with (2), in general, $D \neq \sigma^{i,j}(A)$. Thus, in general, the sequence converted from $\sigma^{i,j}(A)$ is not equal to $L^{im+j}(\mathbf{a})$.

Property 1 *$\sigma^{i,j}$ is a linear transformation on $\mathbb{R}^{n,m}$.*

3. Array Correlation

In this section, we introduce the definition of an array correlation. In the following, we always assume that sequences belong to $\mathbb{R}^v$ and $v = nm$ where $n > 1$ and $m > 1$ and the matrix forms of the sequences belong to $\mathbb{R}^{n,m}$. Before we introduce the definition for the array correlation, we need some preparation for the Galois ring $\mathbb{R} = \mathbb{GR}(p^e, d)$. Let $Q = p^d$ and $\mathcal{T} = \{x \mid x \in R,\ x^Q = x\ \}$. It is known that $\mathcal{T} = \{\ \beta^i \mid 1 \leq i < Q\} \cup \{0\}$ where β is an invertible element of order $Q - 1$ in $\mathbb{R}$. The function

$$\mu(x) = \sum_{i=0}^{e-1} w_i^p p^i, \forall x = \sum_{i=0}^{e-1} w_i p^i,\ w_i \in \mathcal{T}$$

is an isomorphism of $\mathbb{R}$, called an *Frobenius automorphism.* Sometimes it is also denoted as $\mu(x) = x^\mu$. For any $x \in \mathbb{R}$, it is known that $\mu(x) = x$ if and only if $x \in Z_{p^e}$. The trace function from $\mathbb{R}$ to $\mathbb{Z}_{p^e}$ is defined as follows.

$$Tr_{\mathbb{R}}(x) = \sum_{0 \leq i < d} x^{\mu^i}$$

where μ is the Frobenius automorphism of $\mathbb{R}$. If x is written as $x = \sum_{i=0}^{e-1} w_i p^i$, $w_i \in \mathcal{T}$, then

$$Tr_{\mathbb{R}}\left(\sum_{i=0}^{e-1} w_i p^i\right) = \sum_{i=0}^{e-1} \sum_{0 \leq j < d} w_i^{p^j} p^i.$$

It is known that $Tr_{\mathbb{R}}(x) \in \mathbb{Z}_{p^e} \forall x \in \mathbb{R}$ and $Tr_{\mathbb{R}}(x)$ maps exactly $p^{e(d-1)}$ elements in $\mathbb{R}$ into one element in $\mathbb{Z}_{p^e}$. We are now in a position to give a definition of the array correlation.

Definition 2 *For any two sequences* **a** *and* **b** *in $\mathbb{R}^v$, let $A = (a_{k,l})$ and $B = (b_{k,l})$ be their matrix forms, an* array cross correlation function *between A and B is defined by*

$$C_{A,B}(i,j) = \sum_{k=0}^{n-1} \sum_{j=0}^{m-1} \omega^{a_{k,l} - b_{k+i,l+j}}, 0 \leq i < n, 0 \leq l < m. \qquad (5)$$

where ω is a qth primitive root of unity in the complex field if $\mathbb{R} = \mathbb{Z}_q$ and ω is a p^eth primitive root of unity in the complex field if $\mathbb{R} =$

$\mathbb{GR}(p^e, d)$. *In the later case,* $a_{k,l}$ *and* $b_{k+i,l+j}$ *in (5) should be replaced by their trace values from* $\mathbb{GR}(p^e, d)$ *to* $\mathbb{Z}_{p^e}$, *i.e., if* $\mathbb{R} = \mathbb{GR}(p^e, d)$, *then*

$$C_{A,B}(i,j) = \sum_{k=0}^{n-1} \sum_{j=0}^{m-1} \omega^{Tr_{\mathbb{R}}(a_{k,l}) - Tr_K(b_{k+i,l+j})}, 0 \le i < n, 0 \le l < m. \quad (6)$$

In particular, for the later case,

1. *Case 1.* $\mathbb{GR}(p^e, 1) = \mathbb{Z}_{p^e}$, *i.e., if* $d = 1$, *(6) becomes*

$$C_{A,B}(i,j) = \sum_{k=0}^{n-1} \sum_{j=0}^{m-1} \omega^{a_{k,l} - b_{k+i,l+j}}, 0 \le i < n, 0 \le l < m. \quad (7)$$

2. *Case 2.* $\mathbb{GR}(p, d) = \mathbb{F}_{p^d}$, *in this case case, (6) has the same representation as (7), but* ω *is a pth primitive root of unit instead of the* p^e*th one.*

If $A = B$, $C_{A,B}(i,j)$, *shortened as* $C_A(i,j)$, *is called an* array auto correlation function *of the matrix* A.
An array cross correlation *between* $\mathbf{a}$ *and* $\mathbf{b}$, *denoted as* $C^2_{\mathbf{a},\mathbf{b}}(\tau)$, *is defined as the array cross correlation when we consider their matrix forms, i.e.,*

$$C^2_{\mathbf{a},\mathbf{b}}(\tau) = C_{A,B}(i,j), \tau = im + j, 0 \le i < n, 0 \le l < m. \quad (8)$$

Similarly, an array auto correlation *of the sequence* $\mathbf{a}$, *denoted as* $C^2_{\mathbf{a}}(\tau)$, *is defined as*

$$C^2_{\mathbf{a}}(\tau) = C_{A,A}(i,j), \tau = im + j, 0 \le i < n, 0 \le l < m. \quad (9)$$

Note that for $\mathbb{R}$ being the Galios ring $\mathbb{GR}(p^e, d)$, when $d > 1$, all results on sequences over $\mathbb{Z}_{p^e}$ or $\mathbb{F}_p$ where $e = 1$ can be routinely generalized to the case $\mathbb{GR}(p^e, d)$ or $\mathbb{F}_{p^d}$, because the trace function from $\mathbb{GR}(p^e, d)$ to $\mathbb{Z}_{p^e}$ and the trace function from $\mathbb{F}_{p^d}$ to $\mathbb{F}_p$ are balanced, which map $p^{e(d-1)}$ (p^{d-1}) elements in $\mathbb{GR}(p^e, d)$ ($\mathbb{F}_{p^e}$) into into exactly one element in $\mathbb{Z}_{p^e}$ ($\mathbb{F}_p$), respectively. So we omit it in this paper. Thus, what we will discuss in the rest of the paper is the case that elements of sequences taken from the residue integer ring $\mathbb{Z}_q$ where q can be an arbitrary positive integer.

In order to compute the array cross correlation, we will introduce other two notations which are analogue to the computation of the ordinary correlation. The first one is $Im(A)$ where A can be a matrix in $\mathbb{Z}_q^{n,m}$ or A a vector of $\mathbb{Z}_q^r$ where r is a positive integer.

$$Im(A) = \sum_{k=0}^{n-1} \sum_{j=0}^{m-1} \omega^{a_{k,l}}, A = (a_{k,l}) \in \mathbb{Z}_q^{n,m} \text{ or } \quad (10)$$

$$Im(A) = \sum_{k=0}^{r-1} \omega^{a_k}, A = (a_0, a_1, \cdots, a_{r-1}) \in \mathbb{R}^r. \quad (11)$$

Let $\mathbf{a} = (a_0, \cdots, a_r) \in \mathbb{Z}_q^r$. We define

$$N_t(\mathbf{a}) = |\{j | 0 \le j < r, a_j = t\}|, t \in \mathbb{Z}_q. \quad (12)$$

Under these notations, we can derive the following relation.

Property 2 *For $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_q^v$, let $A, B \in \mathbb{Z}_q^{n,m}$ be their matrix forms, the array cross correlation between A and B, or equivalently between $\mathbf{a}$ and $\mathbf{b}$, can be computed in the following ways:*

$$\begin{aligned} C^2_{\mathbf{a},\mathbf{b}}(im + j) &= C_{A,B}(i, j) \\ &= Im(A - \sigma^{i,j}(B)) \quad (13) \\ &= \sum_{k=0}^{m-1} Im(\mathbf{c}_k(A) - L^i(\mathbf{c}_{j+k}(B)) \quad (14) \\ &= \sum_{t=0}^{q-1} \left(\sum_{k=0}^{m-1} N_t(\mathbf{c}_k(A) - L^i(\mathbf{c}_{j+k}(B)) \right) \omega^t. \quad (15) \end{aligned}$$

Proof. Notice that

$$Im(\mathbf{c}_k(A) - L^i(\mathbf{c}_{j+k}(B)) = \sum_{t=0}^{q-1} N_t(\mathbf{c}_k(A) - L^i(\mathbf{c}_{j+k}(B))\omega^t.$$

The results follow immediately.

Under Definition 2, for $\mathbf{a}, \mathbf{b} \in \mathbb{R}^v$, there are two types of correlations. As usual, one is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{v-1} \omega^{a_i - b_{i+\tau}}. \quad (16)$$

According to Definition 2, the array cross correlation between $\mathbf{a}$ and $\mathbf{b}$ is given by (8). In general, these two correlation functions are not equal. In other words, the following two sets are not equal:

$$\begin{aligned} S_1 &= \{C^2_{\mathbf{a},\mathbf{b}}(im + j) \,|\, 0 \le i < n, 0 \le j < m\} \text{ and} \\ S_2 &= \{C_{\mathbf{a},\mathbf{b}}(im + j) \,|\, 0 \le i < n, 0 \le j < m\}. \end{aligned}$$

In order to see correctness of this claim, we first show that

Property 3 *For* $\mathbf{a}, \mathbf{b} \in \mathbb{R}^v$, *and* $\tau = im + j$ *where* $0 \leq i < n, 0 \leq j < m$,

$$C_{\mathbf{a},\mathbf{b}}(im+j) = \sum_{k=0}^{m-j-1} Im(\mathbf{c}_k(A) - L^i(\mathbf{c}_{j+k}(B)) + \sum_{k=m-j}^{m-1} Im(\mathbf{c}_k(A) - L^{i+1}(\mathbf{c}_{j+k}(B)). \quad (17)$$

This result follows directly from (4) and (16).

Comparing (17) with (14), we can conclude that, in general, the cross correlation between the sequences $\mathbf{a}$ and $\mathbf{b}$ is not equal to their array cross correlation. However, in some cases, they are equal. In the next section, we will construct two sets of sequences over $\mathbb{Z}_q$ and show that for any pair of sequences each taken from different sets their cross correlation and their array cross correlation are equal and the maginitude of the cross correlation values are also equal.

Remark 1 *The array correlations are equal for the sequences converted from* $\mathbb{R}^v$ *whenever we consider that it is a matrix in* $\mathbb{R}^{n,m}$ *or in* $\mathbb{R}^{m,n}$ *where* $v = nm$.

4. Constructions

Let $\mathbf{a} \in \mathbb{Z}_q^r$. We say that $\mathbf{a}$ is *balanced* if in every period, the numbers of all elements in $\mathbb{Z}_q$ are nearly equal. (More precisely, the disparity is not to exceed 1.) In particular, when $r = tq - 1$, we say that $\mathbf{a}$ is *balanced* if each non- zero element in $\mathbb{Z}_q$ occurs t times and zero element occurs $t - 1$ times. When $r = sq + 1$, we say that $\mathbf{a}$ is *convex balanced* if each non -zero element in $\mathbb{Z}_q$ occurs s times and zero element occurs $s + 1$ times. When $r = uq$, we say that $\mathbf{a}$ is *strict* balanced if each element in $\mathbb{Z}_q$ occurs exactly u times in $\mathbf{a}$.

Constructions of Sets $\mathcal{A}$ and $\mathcal{B}$

Let $v = nm$ where $n = tq - 1$ and $m = sq + 1$. Let $U_n \subset \mathbb{Z}_q^n$ which contains all balanced sequences in $\mathbb{Z}_q^n$ and $R_m \subset \mathbb{Z}_q^m$ which consists of all convex balanced sequences in $\mathbb{Z}_q^m$. For any positive integer r, if $\mathbf{c} = (c, c, \cdots, c) \in \mathbb{Z}_q^r$, then we say that $\mathbf{c}$ is a constant sequence or a constant vector in $\mathbb{Z}_q^r$. For $\mathbf{a} = (a_0, a_1, \cdots, a_{r-1}) \in \mathbb{Z}_q^r$, sometimes we use the notation $\mathbf{a} + c$ to denote $(a_0, a_1, \cdots, a_{r-1}) + (c, c, \cdots, c)$.

1. $\mathcal{A}$ consists of all matrices in $\mathbb{Z}_q^{n,m}$ with the following form: $m-1$ columns belong to U_n and one column is the zero sequence $\mathbf{0}$.

2. $\mathcal{B}$ consists of all matrices in $\mathbb{Z}_q^{n,m}$ which has identical rows where the row vector $\mathbf{b} = (b_0, b_1, \cdots, b_{m-1}) \in R_m$,, i.e., $\mathbf{b}$ is a convex balanced sequence in $\mathbb{Z}_q^m$.

Notice that from the construction of $\mathcal{B}$, for any matrix B in $\mathcal{B}$, the column vectors of B has the following patterns. For each nonzero c in $\mathbb{Z}_q$, there are s column vectors of B being the constant vector $(c, c, \cdots, c)$, and $s+1$ column vectors of B are the zero vector. In particular, if $q = 2$, then B has s columns are the constant vector $\mathbf{1}$ and $s+1$ column vectors are the zero vector. We list this result as a property.

Property 4 *For any $B \in \mathcal{B}$, let B_j be the jth coloumn vector of B, i.e, $B = [B_0, B_1, \cdots, B_{m-1}]$, then*

$$B_j = [b_j, \cdots, b_j]^T \in \mathbb{Z}_q^n \text{ where } N_c(\mathbf{b}) = s \text{ if } c \neq 0 \text{ and } N_0(\mathbf{b}) = s+1 \tag{18}$$

where v^T is the tranpose of the vector v and $N_t(\mathbf{b})$ is the number of c occurs in $\mathbf{b}$, defined in (12). In particular, if $q = 2$, then $N_1(\mathbf{b}) = s$ and $N_0(\mathbf{b}) = s+1$.

Theorem 1 *Both $\mathcal{A}$ and $\mathcal{B}$ are invarant under the array shift operator $\sigma^{i,j}$. In other word, for any $A = (a_{k,l}) \in \mathcal{A}$ and $B = (b_{k,l}) \in \mathcal{B}$,*

$$\sigma^{i,j}(A) \in \mathcal{A} \text{ and } \sigma^{i,j}(B) \in \mathcal{B}.$$

Proof. Let A_j and B_j be the column vectors of A and B respectively. From the construction, we have

$$A \in \mathcal{A} \Longleftrightarrow A = [A_0, A_1, \cdots, A_{m-1}], \tag{19}$$

for all $A_j \in U_n$ except for the zero sequence. From Property 4, it follows that

$$B \in \mathcal{B} \Longleftrightarrow B = [B_0, B_1, \cdots, B_{m-1}] \tag{20}$$

where $N_c(\mathbf{b}) = s$ if $c \neq 0$ and $N_0(\mathbf{b}) = s+1$ where $\mathbf{b} = (b_0, b_1, \cdots, b_{m-1})$ and $B_j = (b_j, \cdots, b_j)^T$. From (2), we have

$$\sigma^{i,j}(A) = [L^i A_j, L^i A_{j+1}, \cdots, L^i A_{j-1}]$$

and

$$\sigma^{i,j}(B) = [L^i B_j, L^i B_{j+1}, \cdots, L^i B_{j-1}].$$

Note that the shift operator L does not change the balanced property of A_j, namely, $L^i A_{j+k} \in U_n$ if and only if $A_{j+k} \in U_n$. Furthermore, $L^i B_{j+k} = B_{j+k}$ when B_{j+k} is a constant sequence. Thus, $\sigma^{i,j}(A)$ and $\sigma^{i,j}(B)$ satisfy (19) and (20) respectively. Therefore, the results follow.

In the following, we will distinquish the case $q = 2$ from the general case since this gives binary sequences which has many important applications in communications and cryptology. The general case will be given in the full version of this work.

Theorem 2 *Let $q = 2$, n and m be odd. For any pair $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^v$, if their matrix forms $A \in \mathcal{A}$ and $B \in \mathcal{B}$, then $C^2_{\mathbf{a},\mathbf{b}}(im + j)$, the array cross correlation between $\mathbf{a}$ and $\mathbf{b}$ is given by*

$$C_{\mathbf{a},\mathbf{b}}(\tau) + 1 = \pm(n+1), \text{ for any } \tau = im + j, 0 \le i < n, 0 \le j < m.$$

Proof. From the formula (13) in Property 2, we have

$$C^2_{\mathbf{a},\mathbf{b}}(im + j) = C_{A,B}(i, j) = Im(A + \sigma^{i,j}(B)).$$

According to Theorem 1, $\sigma^{i,j}(B) \in \mathcal{B}$. Thus we only need to show that $Im(A+B)+1 = \pm(n+1)$ for any pair $A \in \mathcal{A}$ and $B \in \mathcal{B}$. Again, using Property 2, we have

$$Im(A + B) = \sum_{k=0}^{m-1} (N_0(A_k + B_k) + N_1(A_k + B_k)(-1))$$

where A_k and B_k are column vectors of A and B respectively. Since there is only one k such that $A_k = (0, \cdots, 0)$, without loss of generality, we may assume that $A_0 = (0, \cdots, 0)$. Note that

$$N_1(A_k + b_k) = \begin{cases} \frac{n-1}{2} & \text{if } b_k = 1 \\ \frac{n+1}{2} & \text{if } b_k = 0 \end{cases}$$

Case 1. $b_0 = 0$. In this case, there are $\frac{m-1}{2}$ k's such that $b_k = 1$. Thus

$$\begin{aligned} N_1(A + B) &= \sum_{k=0}^{m-1} N_1(A_k + b_k) \\ &= \frac{m-1}{2}\frac{n-1}{2} + \frac{m-1}{2}\frac{n+1}{2} \\ &= \frac{nm-n}{2}. \end{aligned}$$

Consequently,

$$Im(A + B) = nm - 2\frac{nm-n}{2} = n. \tag{21}$$

Case 2. $b_0 = 1$. In this case, there are $\frac{m-1}{2} - 1$ k's such that $b_k = 1$ for $k > 0$. Thus

$$\begin{aligned} N_1(A+B) &= \sum_{k=0}^{m-1} N_1(A_k + b_k) \\ &= n + \left(\frac{m-1}{2} - 1\right)\frac{n-1}{2} + \left(\frac{m-1}{2} + 1\right)\frac{n+1}{2} \\ &= n + \frac{(m-3)(n-1)}{4} + \frac{(m+3)(n+1)}{4} \\ &= n + \frac{2nm - 2n + 4}{4} = \frac{nm + n + 2}{2} \end{aligned}$$

Thus

$$Im(A+B) = nm - 2\frac{nm+n+2}{2} = -n - 2. \tag{22}$$

The above two cases yield that

$$Im(A+B) + 1 = \pm(n+1)$$

which completes the proof.

Note that this result is independent of the value of m. From the proof of Theorem 2, we have established the following result.

Corollary 1 *If $A \in \mathcal{A}$ and $B \in \mathcal{B}$, then $Im(A+B) = \pm(n+1) - 1$.*

Corollary 2 *With the notation in Theoerm 2, then the cross correlation between* $\mathbf{a}$ *and* $\mathbf{b}$ *is equal to their array cross correlation. Furthermore, they have equal absolutely values when 1 is added to these values, i.e.,*

$$C_{\mathbf{a},\mathbf{b}}(\tau) + 1 = C^2_{\mathbf{a},\mathbf{b}}(\tau) + 1 = \pm(n+1), \tau = im + j, 0 \le i < n, 0 \le j < m$$

and

$$|C_{\mathbf{a},\mathbf{b}}(im+j)+1| = |C^2_{\mathbf{a},\mathbf{b}}(\tau)+1| = n+1, \forall \tau = im+j, 0 \le i < n, 0 \le j < m.$$

Proof. From Theorem 2, we only need to show that $C_{\mathbf{a},\mathbf{b}}(im+j)+1 = \pm(n+1)$. Notice that the column vectors of B, say B_j, is equal to either zero constant vector or a constant vector of 1's for all $0 \le j < m$. Thus any shift of these vectors is unchanged, i.e., $L^k(B_j) = B_j$ for any $0 \le k < n; 0 \le j < m$. Combining with (4) in Section 2, the matrix form, say D, of $L^{im+j}(\mathbf{b})$ is given by

$$\begin{aligned} D &= [L^i(B_j), \cdots, L^i(B_{m-1}), L^{i+1}(B_0), \cdots, L^{i+1}(B_{j-1})] \\ &= [B_j, \cdots, B_{m-1}, B_0, \cdots, B_{j-1}] \in \mathcal{B}. \end{aligned}$$

Consequently, from Property 3, we have

$$C_{\mathbf{a},\mathbf{b}}(im+j) = Im(A+D)$$

where $A \in \mathcal{A}$ and $D \in \mathcal{B}$. Using Corollary 1, we have

$$C_{\mathbf{a},\mathbf{b}}(im+j) + 1 = Im(A+D) + 1 = \pm(n+1).$$

From Theorem 2, the results follows.

Remark. Let $n = 2^r - 1$ and $m = 2^r + 1$.

(a) Assume that $\mathcal{A}$ consists of the matrices converted from one binary m-sequence of period $2^{2r}-1$ together its shifts. Then the sequences converted from $\mathcal{B}$ give bent functions, which correspond to Dillon's $PS^{(-1)}$ set in [1].

(b) Assume that $\mathcal{A}$ consists of the matrices converted from all shift distinct m-sequences together their shifts. In this case, any sequence converted from $\mathcal{B}$ corresponds to a hyper-bent function discussed by Youssef and Gong in [3]. In other words, the authors of [3] established that any sequence converted from $\mathcal{B}$ has the maximal distance from all shift distinct m-sequences. Note that the concept for investigating the distance of a sequence from all shift distinct m-sequences was pioneered by Gong and Golomb in 1999 in [2].

Thus the result of Corollary 2 shows that any sequence converted from $\mathcal{B}$ has the maximal distance from all balanced binary sequences of period $2^{2r} - 1$.

References

1. J. F. Dillon, Elementary Hadamard Difference sets, *Proc. Sixth SE Conf. Comb. Graph Theory and Comp.*, F. Hoffman et al. (Eds), Winnipeg Utilitas Math (1975), pp. 237-249 (or *Elementary Hadamard Difference Sets*, Ph.D. Dissertation, University of Maryland, 1974).
2. G. Gong and S.W. Golomb, Transform Domain Analysis of DES, *IEEE Trans. on Inform. Theory*, vol. 45, No.6, September 1999, pp. 2065-2073.
3. A.M. Youssef and G. Gong, Hyper-Bent Functions, *Advances in Cryptology-Eurocrypto'2001*, Lecture Notes in Computer Science, 2045, Springer, 2001, pp. 406-419.