Correlation Functions of $m-$Sequences of Different Lengths

Zepeng Zhuo[1], Jinfeng Chong[1,2], and Lei Yu[3]
(Corresponding author: Jinfeng Chong)

School of Mathematical Sciences, Huaibei Normal University[1]
Information College, Huaibei Normal Universtiy[2]
School of Computer Science and Technology, Huaibei Normal Universtiy[3]
Huaibei, Anhui 235000, China
(Email: cjf791009@sohu.com)

(Received Oct. 16, 2018; Revised and Accepted Jan. 23, 2019; First Online Mar. 4, 2019)

Abstract

The sequences over a finite field F_p with good correlation properties are important applications in coding, communication, and cryptography. The maximal period sequences($m-$ sequences) and their decimations are widely used to design sequence families with low correlation. In this paper, the correlation functions on $m-$sequences of different lengths are investigated. Two classes of $m-$sequences of different lengths are considered, and some properties of the correlation functions between these $m-$sequences are presented.

Keywords: Autocorrelation Function; Binary Sequence; Cross-correlation Function; $m-$sequence; Perfect Sequence

1 Introduction

Correlation is a measure of the similarity or relatedness. If properly normalized, the correlation measure is a real number between -1 and $+1$. A correlation value of -1 indicates that the two phenomena are diametrically opposite while a correlation value 0 means that they are uncorrelated, and a correlation value $+1$ means that they are identical. In other sources, the correlation between two sets of data is called their covariance. In linear algebra, the correlation between two vectors is their (normalized) dot product [3].

Let $\mathbf{a} = (a_0, a_1, \cdots, a_{N-1})$ and $\mathbf{b} = (b_0, b_1, \cdots, b_{N-1})$ be two binary sequences of period N. The *(periodic) cross-correlation function* between these two sequences at shift τ, where $0 \le \tau \le N-1$, is defined by

$$\mathcal{C}_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{N-1} (-1)^{a_{i+\tau}+b_i}, \tag{1}$$

where the subscripts are reduced modulo N, that is, $\mathcal{C}_{\mathbf{a},\mathbf{b}}(\tau)$ is the dot product of two vectors

$$((-1)^{a_\tau}, (-1)^{a_{\tau+1}}, \cdots, (-1)^{a_{\tau+N-1}}).$$

and

$$((-1)^{b_0}, (-1)^{b_1}, \cdots, (-1)^{b_{N-1}}).$$

If the sequences $\mathbf{a}$ and $\mathbf{b}$ are the same, we call $\mathcal{C}_{\mathbf{a},\mathbf{a}}(\tau)$ the *(periodic) autocorrelation function* of $\mathbf{a}$, denoted by $\mathcal{A}_{\mathbf{a}}(\tau)$. $\mathcal{A}_{\mathbf{a}}(\tau)$ measures the amount of similarity between the sequence and its phase shift. This is always the highest for $\tau = 0$, because

$$\mathcal{A}_{\mathbf{a}}(0) = \sum_{i=0}^{N-1} (-1)^{a_i+a_i} = N.$$

During the last decades, many applications of sequences with low correlation have been found in coding, communication and cryptography [1,4,5,9,13,15,16]. Using sequences with low(auto and cross)correlation values, the interference of different users during the transmission can be reduced. Therefore, sequences with low correlation have been an important research problem enjoying considerable interests. If the autocorrelation properties are optimum, the sequences would been called perfect. Conventional autocorrelation functions have two different definitions: periodic and aperiodic autocorrelations. Traditionally, the studies of the periodic autocorrelation of a binary sequence, especially about the sequences families of code-division multiple access communication (CDMA) system, have attracted more and more attention in the research of this field. However, the aperiodic autocorrelation is considered to better characterize a binary sequence for more realistic communication systems [15].

A well-studied problem is to find the cross-correlation function between two binary $m-$sequences $\{s_t\}$ and $\{s_{dt}\}$ of the same period $2^m - 1$ that differs by a decimation d such that $\mathtt{gcd}(d, 2^m-1) = 1$. A survey of some of the basic researches on the cross-correlation between $m-$sequencs of the same length can be found [5]. Several sequence families with practical applications use $m-$sequencs of different periods, a prime example is the optimal small family of Kasami sequences. The correlation properties of this family depends on the correlation properties of an $m-$sequence of period $2^m - 1$ and an $m-$sequence of period $2^{m/2-1}$ where m is even.

A cross-correlation function between two periodic sequences $\mathbf{a} = \{a_i\}$, of period s, and $\mathbf{b} = \{b_i\}$, of period t, over F_2 can be defined as [3].

$$\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{N-1} (-1)^{a_{i+\tau}+b_i}, \tau = 0, 1, \cdots, \quad (2)$$

where $N = \mathtt{lcm}[s, t]$.

In [10], Ness and Helleseth studied the cross correlation between an $m-$sequencs $\{s_t\}$ of length $n = 2^m - 1$ and an $m-$sequence $\{u_{dt}\}$ of length $2^k - 1$, where $m = 2k$ and $\mathtt{gcd}(d, 2^k - 1) = 1$. Here $\{u_t\}$ denotes the $m-$sequence which used in constructing the small family of Kasami sequence. The cross-correlation functions between $m-$sequences of different lengths were investigated in [2, 6–8, 10–12, 14]. The first infinite family of pairs of $m-$sequences with four-valued cross-correlation was constructed and the complete correlation distribution of this family was also determined [11]. From the above studies, we are motivated by [2,6–8,10–12,14] to study correlation functions of $m-$sequences of different lengths.

2 Preliminaries

Definition 1. *If the autocorrelation function $\mathcal{A}_{\boldsymbol{a}}(\tau)$ is two-valued, given by*

$$\mathcal{A}_{\boldsymbol{a}}(\tau) = \begin{cases} N, & \text{if } \tau \equiv 0 \pmod{N}, \\ K, & \text{if } \tau \not\equiv 0 \pmod{N}, \end{cases} \quad (3)$$

where K is a constant. If $K = -1$, N is an odd and $K = 0$, N is an even, then we say that the sequence $\boldsymbol{a}$ has the (ideal) 2-level autocorrelation function, and $\boldsymbol{a}$ is called the perfect sequence.

If $N = 2^n - 1$, the autocorrelation function $\mathcal{A}_{\mathbf{a}}(\tau)$ is two-valued and is given by

$$\mathcal{A}_{\mathbf{a}}(\tau) = \begin{cases} 2^n - 1, & \text{if } \tau \equiv 0 \pmod{2^n - 1}, \\ -1, & \text{if } \tau \not\equiv 0 \pmod{2^n - 1}. \end{cases} \quad (4)$$

Binary sequences with 2-level autocorrelation have many applications in communication such as radar distance ranging, hardware testing, coding theory, and cryptography. A binary sequence of period $2^n - 1$ with 2-level autocorrelation corresponds to a cyclic Hadamard difference set with parameters $(2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1)$. A sequence $\mathbf{a}$ is called *balanced* if the number of ones and zeros in each period is $n/2$ if n is even or $(n \pm 1)/2$ if n is odd. Balanced sequences with autocorrelation -1 are widely used in communications and cryptography. The $m-$sequences is the first class of binary sequences of period $2^n - 1$ with 2-level autocorrelation for any positive integer n, and it corresponds to the Singer Hamamard difference sets which were discovered by Singer in 1938. Golomb found $m-$sequences from the approach linear feedback shift register sequences in 1954. These sequences have several other common names, e.g., *pseudo-noise(PN) sequences* and *maximal length shift register sequences*. The importance of $m-$sequences is largely due to the part which they called pseudo randomness properties, *i.e.*, properties that make $m-$sequences behave like sequences whose elements are chosen at random.

Let p be any prime, r be a positive integer, $q = p^r$. Let $\omega = e^{2\pi i/p}$ be a primitive pth root of unity. The *(canonical) additive character* of F_{p^r} is defined by

$$\chi(x) = e^{2\pi i Tr(x)/p}, x \in \mathrm{F}_{p^r}, \quad (5)$$

where $Tr(x)$ is the trace function from F_{p^r} to F_p, given by

$$Tr(x) = x + x^p + \cdots + x^{p^{r-1}}, x \in \mathrm{F}_{p^r}.$$

Definition 2. *A cross-correlation function between two periodic sequences $\boldsymbol{a}$, of period s, and $\boldsymbol{b}$, of period t, over F_q can be defined as*

$$\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau) = \sum_{i=0}^{N-1} \chi(a_{i+\tau})\chi^*(b_i), \tau = 0, 1, \cdots, \quad (6)$$

where $\chi^*(x) = (\chi(x))^*$, the complex conjugation of $\chi(x)$, and $N = \mathtt{lcm}[s, t]$. In particular, the cross-correlation function of $\boldsymbol{a}$ and $\boldsymbol{b}$ defined by Equation (6) becomes Equation (2) and the following formulae:

$$\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau) = \sum_{i=0}^{N-1} \omega^{a_{i+\tau}-b_i}, \tau = 0, 1, \cdots, \text{for } \ \mathrm{q = p > 2}. \quad (7)$$

In [3], the basic properties of cross-correlation function which defined as Equation (7) were studied. We list in the following:

Property 1[1]: Let $\mathbf{a}$ and $\mathbf{b}$ be two periodic sequences over F_p with periods $s = p^n - 1$ and t, where $t|s$ respectively. Let L be the left shift operator.

1) $\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) = \mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau + kt), k = 0, 1, \cdots$

2) $\mathcal{CC}_{L^k\mathbf{a},L^k\mathbf{b}}(\tau) = \mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau), 0 \le k < s.$

3) $\mathcal{CC}_{L^i\mathbf{a},L^j\mathbf{b}}(\tau) = \mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau + i - j), 0 \le i, j < s$, where $\tau + i - j$ is reduced modulo s.

4) $\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) = \overline{\mathcal{CC}_{\mathbf{b},\mathbf{a}}(-\tau)}$. In particular, if $p = 2$, then $\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) = \mathcal{CC}_{\mathbf{b},\mathbf{a}}(-\tau)$, where $-\tau$ is reduced modulo s.

5) If $p = 2$, according to the assumption, $t|2^n - 1$. Let $d > 1$ satisfying $\mathtt{gcd}(d, t) = 1$, then

$$\mathcal{CC}_{\mathbf{a},\mathbf{b}^{(d^{-1})}}(\tau) = \mathcal{CC}_{\mathbf{b},\mathbf{a}^{(d)}}(-d^{-1}\tau).$$

3 Main Results

In this section, we mainly discuss the properties of the cross-correlation function $\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau)$ defined as Equation (2).

3.1 The $\mathtt{gcd}(s,t) = 1$ Property

3.1.1 Product Sequences

In [15], Yu and Gong discussed the applications of the perfect binary sequence for binary sequences with optimal (periodic) autocorrelation. Let **a** and **b** be binary sequences of periods N_1 and N_2 respectively, where $\mathtt{gcd}(N_1, N_2) = 1$. Then the product sequence $\mathbf{p{=}a{+}b} = (p_0, p_1, \cdots, p_{N-1})$ of period $N = N_1N_2$ is defined by the component-wise addition of $p_i = a_i + b_i \pmod 2$, $0 \le i \le N-1$. The (periodic) autocorrelation $\mathcal{A}_{\mathbf{p}}(\tau)$ of the product sequence is given by

$$\begin{aligned}
\mathcal{A}_{\mathbf{p}}(\tau) &= \sum_{i=0}^{N-1}(-1)^{p_{i+\tau}+p_i} \\
&= \sum_{i=0}^{N_1N_2-1}(-1)^{a_{i+\tau}+b_{i+\tau}+a_i+b_i} \\
&= \left[\sum_{j=0}^{N_1-1}(-1)^{a_{j+\tau}+a_j}\right]\cdot\left[\sum_{k=0}^{N_2-1}(-1)^{b_{k+\tau}+b_k}\right] \\
&= \mathcal{A}_{\mathbf{a}}(\tau)\cdot\mathcal{A}_{\mathbf{b}}(\tau),
\end{aligned}$$

where $0 \le \tau \le N-1$, and the indices of a sequence are computed modulo its own period.

That is, the (periodic) autocorrelation functions of the products of periodic sequences of relatively prime lengths are themselves the products of the individual autocorrelation functions.

Example 1. *Let* $\boldsymbol{a} = 110, \boldsymbol{b} = 11010$*, then*

$$\boldsymbol{a} : 110110110110110,$$

$$\boldsymbol{b} : 110101101011010,$$

$$\boldsymbol{p} : 000011011101100.$$

We compute their autocorrelation functions as following:

$$\begin{aligned}
&\mathcal{A}_{\mathbf{a}}(0), \mathcal{A}_{\mathbf{a}}(1), \cdots, \mathcal{A}_{\mathbf{a}}(14) \\
= \;& 3, -1, -1, 3, -1, -1, 3, -1, -1, 3, -1, -1, 3, -1, -1, \\
&\mathcal{A}_{\mathbf{b}}(0), \mathcal{A}_{\mathbf{b}}(1), \cdots, \mathcal{A}_{\mathbf{b}}(14) \\
= \;& 5, -3, 1, 1, -3, 5, -3, 1, 1, -3, 5, -3, 1, 1, -3, \\
&\mathcal{A}_{\mathbf{p}}(0), \mathcal{A}_{\mathbf{p}}(1), \cdots, \mathcal{A}_{\mathbf{p}}(14) \\
= \;& 15, 3, -1, 3, 3, -5, -9, -1, -1, -9, -5, 3, 3, -1, 3.
\end{aligned}$$

Obviously, from the above example, we have $\mathcal{A}_{\mathbf{p}}(\tau) = \mathcal{A}_{\mathbf{a}}(\tau)\cdot\mathcal{A}_{\mathbf{b}}(\tau), 0 \le \tau \le 14$.

3.1.2 Cross-Correlation Functions Between $m-$Sequences of Relatively Prime Lengths

In this section, we discuss the cross-correlation function between an arbitrary pair of $m-$sequences whose periods are relatively prime. First, we give the following fact.

Proposition 1. *Let* $\boldsymbol{a}$ *and* $\boldsymbol{b}$ *be binary sequences of periods s and t respectively, where* $\mathtt{gcd}(s,t) = 1$*. Let* $\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau)$ *be the cross-correlation function between* $\boldsymbol{a}$ *and* $\boldsymbol{b}$ *defined by Equation (2). Then the* $\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau)$ *is a periodic function, and the period of* $\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau)$ *is equal to* $\mathtt{min}(s,t)$*.*

In fact, without loss of generality, we assume $s < t$. So, **a** is a short sequence. If the sequence **a** shifts s times later, it will return to the original location again. Hence, the value of $\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau)$ won't change any more.

Example 2. *Let* $\boldsymbol{a} = 011, \boldsymbol{b} = 0010111$*, they are $m-$sequences of length 3 and 7 respectively. By Equation (2), we compute*

$$\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau) = \sum_{i=0}^{20}(-1)^{a_{i+\tau}+b_i}, \tau = 0, 1, \cdots$$

Since,

$$\mathbf{a} : 011011011011011011011,$$

$$\mathbf{b} : 001011100101110010111.$$

Then, we have

$$\mathcal{CC}_{\mathbf{a},\mathbf{b}}(0) = 1, \mathcal{CC}_{\mathbf{a},\mathbf{b}}(1) = 1, \mathcal{CC}_{\mathbf{a},\mathbf{b}}(2) = 1, \mathcal{CC}_{\mathbf{a},\mathbf{b}}(3) = 1, \cdots$$

Before proceeding, we will give a somewhat technical result about $\mathtt{gcd}$'s(*greatest common divisor*) that will be used in the following.

Lemma 1. *Let a, m, n be positive integers, and $a > 1$. Then*

$$\mathtt{gcd}(a^m - 1, a^n - 1) = a^{\mathtt{gcd}(m,n)} - 1.$$

Proof. If $m = n$, the result is trivial. If $m \ne n$, and $m, n > 1$, without loss of generality, we assume $m > n$. Using Division algorithm, then

$$m = qn + r, 0 \le r < n.$$

□

We have

$$\begin{aligned}
a^m - 1 &= a^{qn+r} - 1 \\
&= a^{qn+r} - a^r + a^r - 1 \\
&= a^r(a^{qn} - 1) + (a^r - 1).
\end{aligned}$$

Since $(a^n - 1)|(a^{qn} - 1)$, *i.e.*, $\exists A \in \mathbf{N}, a^{qn} - 1 = A(a^n - 1)$, then $a^m - 1 = Aa^r(a^n - 1) + (a^r - 1)$. Therefore, $\mathtt{gcd}(a^m - 1, a^n - 1) = \mathtt{gcd}(a^n - 1, a^r - 1)$.

Note that $\mathtt{gcd}(m,n) = \mathtt{gcd}(n,r)$. If $r = 0$, then $\mathtt{gcd}(m,n) = n$, the result is true. If $r > 0$, then we discuss $\mathtt{gcd}(a^n - 1, a^r - 1)$ by using the same method. According to Euclid's algorithm, the result is true.

The above result is very powerful. For example, it says that $\mathtt{gcd}(3^9-1,3^8-1)=3^{\mathtt{gcd}(9,8)}-1=2$, a fact which is unobvious if we had written $3^9-1=19682, 3^8-1=6560$. Similarly, using Lemma 1, we can compute many polynomial gcd's effortlessly: $\mathtt{gcd}(x^9-1,x^{12}-1)=x^3-1$.

Theorem 1. *Let **a** and **b** be binary $m-$sequences of periods 2^m-1 and 2^n-1 respectively, where $\mathtt{gcd}(m,n)=1$. Let $\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau)$ be the cross-correlation function between **a** and **b** defined by Equation (2). Then*

$$\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau)=1.$$

Since $\mathtt{gcd}(m,n)=1$, according to Lemma 1, we have $\mathtt{gcd}(2^m-1,2^n-1)=1$. Using the knowledge of probability, we calculate $\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau)$. Let **a** be an $m-$sequence of period P. Hence, the sequence **a** satisfies the balance property, *i.e.*, in every period, 0's occur $(P-1)/2$ times and 1's occur $(P+1)/2$ times. So, in every period,

$$\mathtt{Pr}(0)=(P-1)/2P,\ \ \mathtt{Pr}(1)=(P+1)/2P.$$

Note that for two periodic sequences $\mathbf{a}=\{a_i\},\mathbf{b}=\{b_i\}$ of relatively prime lengths s,t, the cross-correlation function Equation (2) can be defined as

$$\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau)=A(\tau)-D(\tau), 0\le\tau\le st-1,$$

where $A(\tau)$ and $D(\tau)$ denote the number of agreements and disagreements between **a**'s phase shift $\{a_{i+\tau}\}, 0\le i\le st-1$ and $\{b_i\}, 0\le i\le st-1$ respectively. In statistical terms, the cross-correlation function Equation (2) becomes the standard correlation coefficient defined as

$$\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau)=(2^m-1)(2^n-1)(\mathtt{Pr}\{a_{i+\tau}=b_i\}-\mathtt{Pr}\{a_{i+\tau}\ne b_i\}).$$

Proof of Theorem 1: For the sequences **a** and **b**, we have

$$\mathtt{Pr}_{\mathbf{a}}(0)=\frac{2^{m-1}-1}{2^m-1},\ \mathtt{Pr}_{\mathbf{a}}(1)=\frac{2^{m-1}}{2^m-1},$$
$$\mathtt{Pr}_{\mathbf{b}}(0)=\frac{2^{n-1}-1}{2^n-1},\ \mathtt{Pr}_{\mathbf{b}}(1)=\frac{2^{n-1}}{2^n-1}.$$

Since the two sequences **a** and **b** are statistically independent, we get four joint probabilities

$$\mathtt{Pr}(00)=\mathtt{Pr}_{\mathbf{a}}(0)\cdot\mathtt{Pr}_{\mathbf{b}}(0)=\frac{(2^{m-1}-1)(2^{n-1}-1)}{(2^m-1)(2^n-1)},$$
$$\mathtt{Pr}(01)=\mathtt{Pr}_{\mathbf{a}}(0)\cdot\mathtt{Pr}_{\mathbf{b}}(1)=\frac{2^{n-1}(2^{m-1}-1)}{(2^m-1)(2^n-1)},$$
$$\mathtt{Pr}(10)=\mathtt{Pr}_{\mathbf{a}}(1)\cdot\mathtt{Pr}_{\mathbf{b}}(0)=\frac{2^{m-1}(2^{n-1}-1)}{(2^m-1)(2^n-1)},$$
$$\mathtt{Pr}(11)=\mathtt{Pr}_{\mathbf{a}}(1)\cdot\mathtt{Pr}_{\mathbf{b}}(1)=\frac{2^{m-1}\cdot 2^{n-1}}{(2^m-1)(2^n-1)}.$$

Therefore,

$$\begin{aligned}\mathtt{Pr}\{a_{i+\tau}=b_i\} &= \mathtt{Pr}(00)+\mathtt{Pr}(11)\\ &= \frac{(2^{m-1}-1)(2^{n-1}-1)+2^{m-1}\cdot 2^{n-1}}{(2^m-1)(2^n-1)},\end{aligned}$$

$$\begin{aligned}\mathtt{Pr}\{a_{i+\tau}\ne b_i\} &= \mathtt{Pr}(01)+\mathtt{Pr}(10)\\ &= \frac{2^{n-1}(2^{m-1}-1)+2^{m-1}(2^{n-1}-1)}{(2^m-1)(2^n-1)}.\end{aligned}$$

Thus,

$$\begin{aligned}\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) &= (2^m-1)(2^n-1)\\ &\cdot\ (\mathtt{Pr}\{a_{i+\tau}=b_i\}-\mathtt{Pr}\{a_{i+\tau}\ne b_i\})\\ &= 1.\end{aligned}$$

Example 3: With the notation in **Example 2**. We compute $\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau)$ by using Theorem 1. First, we have

$$\mathtt{Pr}_{\mathbf{a}}(0)=1/3,\ \mathtt{Pr}_{\mathbf{a}}(1)=2/3,\ \mathtt{Pr}_{\mathbf{b}}(0)=3/7,\ \mathtt{Pr}_{\mathbf{b}}(1)=4/7,$$

and

$$\begin{aligned}\mathtt{Pr}(00)=\mathtt{Pr}_{\mathbf{a}}(0)\cdot\mathtt{Pr}_{\mathbf{b}}(0)=3/21,\\ \mathtt{Pr}(01)=\mathtt{Pr}_{\mathbf{a}}(0)\cdot\mathtt{Pr}_{\mathbf{b}}(1)=4/21,\\ \mathtt{Pr}(10)=\mathtt{Pr}_{\mathbf{a}}(1)\cdot\mathtt{Pr}_{\mathbf{b}}(0)=6/21,\\ \mathtt{Pr}(11)=\mathtt{Pr}_{\mathbf{a}}(1)\cdot\mathtt{Pr}_{\mathbf{b}}(1)=8/21,\end{aligned}$$

then,

$$\mathtt{Pr}\{a_{i+\tau}=b_i\}=\mathtt{Pr}(00)+\mathtt{Pr}(11)=11/21,$$
$$\mathtt{Pr}\{a_{i+\tau}\ne b_i\}=\mathtt{Pr}(01)+\mathtt{Pr}(10)=10/21.$$

Therefore,

$$\begin{aligned}\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) &= 21(\mathtt{Pr}\{a_{i+\tau}=b_i\}-\mathtt{Pr}\{a_{i+\tau}\ne b_i\})\\ &= 1,\ \tau=0,1,\cdots\end{aligned}$$

3.2 The $t|s$ Property

In Equation (2), if $t|s$, then we have

$$\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau)=\sum_{i=0}^{s-1}(-1)^{a_{i+\tau}+b_i}, \tau=0,1,\cdots, \tag{8}$$

In this section, we mainly study the properties of $\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau)$ defined as Equation (8).

Lemma 2. *Let **a** and **b** be two binary sequences of periods t and s, where $t|s$. Then*

$$\sum_{\tau=0}^{t-1}\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau)\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau+k)=\sum_{l=0}^{s-1}\mathcal{A}_{\boldsymbol{b}}(l)\mathcal{A}_{\boldsymbol{a}}(l+k). \tag{9}$$

Proof. By Equation (8), we obtain

$$\begin{aligned}&\textstyle\sum_{\tau=0}^{t-1}\ \mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau)\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau+k)\\ &= \sum_{\tau=0}^{t-1}\sum_{i=0}^{s-1}(-1)^{a_{i+\tau}+b_i}\sum_{j=0}^{s-1}(-1)^{a_{j+\tau+k}+b_j}\\ &= \sum_{i=0}^{s-1}\sum_{j=0}^{s-1}(-1)^{b_i+b_j}\sum_{\tau=0}^{t-1}(-1)^{a_{i+\tau}+a_{j+\tau+k}}\\ &= \sum_{l=0}^{s-1}\sum_{i=0}^{s-1}(-1)^{b_{i+l}+b_i}\sum_{\theta=0}^{t-1}(-1)^{a_{\theta+l+k}+a_\theta}\\ &= \sum_{l=0}^{s-1}\mathcal{A}_{\mathbf{b}}(l)\mathcal{A}_{\mathbf{a}}(l+k).\end{aligned}$$

□

Theorem 2. *Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be two $m-$sequences of periods t and s, where $t|s$,* i.e., *$\exists d \in Z$ such that $s = dt$. Then the cross-correlation function value $\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(\tau)$ defined as Equation (8) satisfies the following relations.*

(2-1) $\sum_{\tau=0}^{t-1} \mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) = 1.$

(2-2) $\sum_{\tau=0}^{t-1} (\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) + 1) = t + 1.$

(2-3) $\sum_{\tau=0}^{t-1} \mathcal{CC}^2_{\mathbf{a},\mathbf{b}}(\tau) = st + t - d.$

(2-4) $\sum_{\tau=0}^{t-1} \mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau)\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau + k) = -s - d - 1,$ for $k \neq 0$.

(2-5) $\sum_{\tau=0}^{t-1} (\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau) + 1)^2 = st + 2t - d + 2.$

Proof. (2-1) According to Equation (8), then

$$\begin{aligned} \sum_{\tau=0}^{t-1} \mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{\tau=0}^{t-1}\sum_{i=0}^{s-1}(-1)^{a_{i+\tau}+b_i} \\ &= \sum_{i=0}^{s-1}(-1)^{b_i}\sum_{\tau=0}^{t-1}(-1)^{a_{i+\tau}} \\ &= (-1)(-1) = 1. \end{aligned}$$

Since an $m-$sequence is almost balanced in the sense that it contains one more one than a zero during its period. (2-2) Due to (2-1), the assertion (2-2) is clear. (2-3) By using Equation (9) and the 2-level autocorrelation properties of the two $m-$sequences, we have

$$\begin{aligned} \sum_{\tau=0}^{t-1} \mathcal{CC}^2_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{l=0}^{s-1} \mathcal{A}_{\mathbf{b}}(l)\mathcal{A}_{\mathbf{a}}(l) \\ &= \mathcal{A}_{\mathbf{b}}(0)\mathcal{A}_{\mathbf{a}}(0) + \mathcal{A}_{\mathbf{b}}(1)\mathcal{A}_{\mathbf{a}}(1) + \cdots \\ &= st - t(d-1) + (s - 1 - (d-1)) \\ &= st + t - d. \end{aligned}$$

(2-4) According to Equation (8) and the 2-level autocorrelation properties of the two $m-$sequences, then

$$\begin{aligned} \sum_{\tau=0}^{t-1} \mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau)\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau + k) &= -s - td + (s - 1 - d) \\ &= -s - d - 1. \end{aligned}$$

(2-5) By using (2-1)(2-3), the assertion (2-5) is clear. □

Example 3. *Let $\boldsymbol{a} = 011$ and $\boldsymbol{b} = 000100110101111$ be two $m-$sequences with periods 3 and 15, respectively, then by using Equation (8), we compute their cross-correlation functions as following:*

$\mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(0), \mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(1), \cdots, \mathcal{CC}_{\boldsymbol{a},\boldsymbol{b}}(14)$
$= -5, 3, 3, -5, 3, 3, -5, 3, 3, -5, 3, 3, -5, 3, 3.$

Thus, we obtain

$$\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) = \begin{cases} -5, & \text{if } \tau \equiv 0 \pmod{3}, \\ 3, & \text{if } \tau \not\equiv 0 \pmod{3}. \end{cases} \qquad (10)$$

Case 1: Using Equation (10), we have

(1-a) $\sum_{\tau=0}^{2} \mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) = -5 + 3 + 3 = 1.$

(1-b) $\sum_{\tau=0}^{2} (\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) + 1) = (-5+1) + (3+1) + (3+1) = 4.$

(1-c) $\sum_{\tau=0}^{2} \mathcal{CC}^2_{\mathbf{a},\mathbf{b}}(\tau) = \mathcal{CC}^2_{\mathbf{a},\mathbf{b}}(0) + \mathcal{CC}^2_{\mathbf{a},\mathbf{b}}(1) + \mathcal{CC}^2_{\mathbf{a},\mathbf{b}}(2) = 25 + 9 + 9 = 43.$

(1-d) $\sum_{\tau=0}^{2} \mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau)\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau + k)$

$= \mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(0)\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(k) + \mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(1)\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(1+k) + \mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(2)\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(2+k)$

$= -5 \times 3 + 3 \times 3 / -5 \times 3 = -21.$

(1-e) $\sum_{\tau=0}^{2} (\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau) + 1)^2$

$= (\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(0)+1)^2 + (\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(1)+1)^2 + (\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(2)+1)^2$

$= (-5+1)^2 + (3+1)^2 + (3+1)^2 = 48.$

Case 2: Using Theorem 2, where $s = 15, t = 3$ and $d = 5$, we have

(2-a) $\sum_{\tau=0}^{2} \mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) = 1.$

(2-b) $\sum_{\tau=0}^{2} (\mathcal{CC}_{\mathbf{a},\mathbf{b}}(\tau) + 1) = t + 1 = 3 + 1 = 4.$

(2-c) $\sum_{\tau=0}^{2} \mathcal{CC}^2_{\mathbf{a},\mathbf{b}}(\tau) = st + t - d = 15 \times 3 + 3 - 5 = 43.$

(2-d) $\sum_{\tau=0}^{2} \mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau)\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau + k) = -s - d - 1 = -15 - 5 - 1 = -21.$

(2-e) $\sum_{\tau=0}^{2} (\mathcal{CC}_{\mathbf{a},\ \mathbf{b}}(\tau) + 1)^2 = st + 2t - d + 2 = 15 \times 3 + 2 \times 3 - 5 + 2 = 48.$

By comparison, we get that Case 2 is simpler than Case 1.

4 Conclusions

We study the correlation functions on $m-$sequences of different lengths in this paper. Also, we consider two classes of $m-$sequences of different lengths and give some properties of the correlation functions between these $m-$sequences.

Acknowledgments

This study was supported by the Anhui Provincial Natural Science Foundation (Grant No.1608085MF143) and the Natural Science Foundation of Anhui Higher Education Institutions of China(No.KJ2018A0678). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. D. Bugrov, "The cross correlation of linear recurrent sequences," *Discrete Mathematics and Applications*, vol. 28, no. 2, pp. 65-73, 2018.

[2] X. L. Fang, "New binary sequences with different periods," Master's Thesis, Central China Normal University, Wuhan, China, 2017.(in Chinese)

[3] S. W. Golomb and G. Gong, "Signal design for good correlation for wireless communication, cryptography, and radar," *Engineering & Transportation*, 2005. (`https://www.amazon.com/Signal-Design-Good-Correlation-Communication/dp/0521821045`)

[4] G. Gong and S. W. Golomb, "Binary sequences with two-level autocorrelation," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 692-693, 1999.

[5] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Mathematics*, vol. 16, no. 3, pp. 209-232, 1976.

[6] T. Helleseth, A. Kholosha and G. J. Ness, "Characterization of $m-$sequences of lengths $2^{2k}-1$ and 2^k-1 with three-valued cross correlation," *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 2236-2245, 2007.

[7] T. Helleseth, L. Hu, A. Kholosha *et al.*, "Period-different $m-$sequences with at most four-valued cross correlation," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3305-3311, 2009.

[8] T. Helleseth and A. Kholosha, "$m-$sequences of lengths $2^{2k}-1$ and 2^k-1 with at most four-valued cross correlation," in *Proceedings of the 5th International Conference on Sequences and Their Applications (SETA'08)*, pp.106-120, Sep. 2008.

[9] R. F. Meng, T. J. Yan, "New constructions of binary interleaved sequences with low autocorrelation," *International Journal of Network Security*, vol. 19, no. 4, pp. 546-550, 2017.

[10] G. J. Ness and T. Helleseth, "Cross correlation of $m-$sequences of different lengths," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1637-1648, 2006.

[11] G. J. Ness and T. Helleseth, "A new family of four-valued cross correlation between $m-$sequences of different lengths," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4308-4313, 2007.

[12] G. J. Ness and T. Helleseth, "A new three-valued cross correlation of between $m-$sequences of different lengths," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4695-4701, 2006.

[13] W. Su, Y. Yang, Z. C. Zhou, *et al.*, "New quaternary sequences of even length with optimal autocorrelation," *Science China Information Sciences*, vol. 61, no. 2, pp. 022308, 2018.

[14] Y. H. Sun, H. Li, T. J. Yan, "Properties of cross-correlation between two P-ary $m-$sequencs of different periods," *Journal of Xidian University*, vol. 39, no. 5, pp. 30-34, 2012.

[15] N. Y. Yu and G. Gong, "The perfect binary sequence of period 4 for low periodic and aperiodic autocorrelations," in *Sequences, Subsequences, Consequences, International Workshop (SSC'07)*, pp. 37-49, 2007.

[16] T. Zhang, S. X. Li, T. Feng, *et al.*, "Some new results on the cross correlation of $m-$sequences," *IEEE Transactions on Information Theory*, vol. 60, no. 5, pp. 3062-3068, 2014.

Biography

Zepeng Zhuo was born in 1978. He received the M.S. degree from Huaibei Normal University in 2007, and the Ph.D. degree from Xidian University in 2012. Since 2002, he has been with the School of Mathematical Science, Huaibei Normal Universtiy, where he is currently a professor. His research interests include cryptography and information theory.

Jinfeng Chong was born in 1979. She received the M.S. degree from Huaibei Normal University in 2007. Since 2002, she has been with the School of Mathematical Science, Huaibei Normal Universtiy, where she is currently an associate professor. Her research interests include cryptography and information theory.

Lei Yu was born in 1978. He received the M.S. degree from Huaibei Normal University in 2009. Since 2002, he has been with the School of Computer Science and Technology, Huaibei Normal Universtiy, where he is currently an associate professor. His research interests include cryptography and information theory.