Some Observations on Distribution of Cross Correlation of Two Nonbinary Sequences

Ernist Tilenbaev, Hasan Dilek, Zülfükar Saygı and Çetin Ürtiş

***Abstract*—Let p be an odd prime, m an odd integer, $d = \frac{(p^m+1)^2}{2(p+1)}$ and $0 < l < (p^m+1)/2$. In this study we have considered cross correlation distribution of p-ary m-sequence $m(t)$, with period $p^{2m}-1$, and its decimated sequences $m(dt+l)$. In [1] authors had given possible values of cross correlation, as 9 different values for the case $p = 3$ and 11 different values for the case $p > 3$. For the case $p = 3$, $m \leq 5$ and all possible values of l we have given complete distribution table and observed that there are 8 different values in total. Note that it was stated in [1], this distribution has at most 9 values, that is we observe that the candidate $-1 + \frac{1+p}{2}p^m$ does not occur. Furthermore, for the case $p = 3$, $m = 3$ and $l = (p^m+1)/4$ we have observed that there are exactly 6 different values. In this case the distribution is different from the case $l = 0$.**

***Index Terms*—nonbinary sequence, cross correlation, exponential sum, quadratic form, cross correlation distribution**

I. INTRODUCTION

Cross correlation and cross correlation distribution of p-ary m-sequence $m(t)$ and its decimated sequences $m(dt)$ or $m(dt+l)$, where $0 \leq l < (p^m+1)/2$ have been studied in [1], [2], [3], [5], [6], [7], [8] and [9]. In [2] cross correlation distribution of m-sequence $m(t)$ and its decimated sequence $m(dt+l)$ have been studied, where $d = \frac{(p^m+1)^2}{2(p^k+1)}$ and $l = 0$. In this study we have considered the cross correlation distribution of m-sequence $m(t)$ and its decimated sequences $m(dt+l)$, where $d = \frac{(p^m+1)^2}{2(p+1)}$ and $0 < l < (p^m+1)/2$. Using the same techniques in [3] and [2] we have evaluated some moment identities. Also numerical results indicate that there are 8 distinct values for $p = 3$ and 9 distinct values for $p > 3$.

The main goal of this study is to derive to complete distribution of correlation values for all odd primes p and all values of $l \neq 0$.

II. PRELIMINARIES

In this section we will give some notations and useful results which was obtained in [1] and [2]. The following notations will be fixed except for specific statements.

- Let p be an odd prime.
- Let m be an odd integer, $n = 2m$ and $d = \dfrac{(p^m+1)^2}{2(p+1)}$.
- Let $\mathbb{F}_{p^n}$ be finite field of order p^n.
- Let α be a primitive element of $\mathbb{F}_{p^n}$.
- Let $\mathrm{Tr}_j^i : \mathbb{F}_{p^i} \to \mathbb{F}_{p^j}$ be the trace mapping for $j \mid i$.
- Let $\omega = \exp\left(2\pi\sqrt{-1}/p\right)$ be the primitive p^{th} root of unity.
- Let $\chi(x) = \omega^{\mathrm{Tr}_p^{p^n}(x)}$ for $x \in \mathbb{F}_{p^n}$ be an additive character.

From [2] we know the following identities,

- $\gcd(p^n-1, d) = \dfrac{p^m+1}{2}$.
- $d\left(p^{m+1}+1\right) \equiv p^m+1 \pmod{p^n-1}$. (It follows from the fact that $\dfrac{p(p^m+1)+p+1}{p+1}$ is an even integer and $d\left(p^{m+1}+1\right) = (p^n-1)\dfrac{p(p^m+1)+p+1}{p+1} + p^m + 1$).

Lemma 1: [10] Assume that $f \mid p^m+1$ and $a \in \mathbb{F}_{p^n}^*$. Then we have

$$\sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_1^n(ax^f)} = \begin{cases} (f-1)p^m, & \text{if } a = \alpha^{h+jf} \text{ for some integer } j \\ -p^m, & \text{otherwise.} \end{cases}$$

where $h = 0$ if $\dfrac{p^m+1}{f}$ is even and $h = \dfrac{f}{2}$ otherwise.

Definition 2: Let (a_t) and (b_t) be two p-ary sequences of period p^n. The cross correlation between the sequences at shift τ, $0 \leq \tau < p^n-1$, is defined by

$$C_{a,b}(\tau) = \sum_{t=0}^{p^n-2} \omega^{a_{t+\tau}-b_t}.$$

p-ary m-sequence $m(t)$ with the period p^n-1 can be expresed as

$$m(t) = \mathrm{Tr}_1^n\left(\alpha^t\right).$$

Since $\gcd(p^n-1, d) = \dfrac{p^m+1}{2}$, there are $\dfrac{p^m+1}{2}$ distinct decimated sequences $m(dt+l)$ of period $2(p^m-1)$ for $0 \leq l < \dfrac{p^m+1}{2}$, which are defined as

$$m(dt+l) = \mathrm{Tr}_1^n\left(\alpha^{dt+l}\right).$$

E.Tilenbaev, Department of Mathematics, TOBB University of Economics and Technology, Ankara
H.Dilek, Department of Mathematics, TOBB University of Economics and Technology, Ankara
Z.Saygı, Department of Mathematics, TOBB University of Economics and Technology, Ankara
Ç.Ürtiş, Department of Mathematics, TOBB University of Economics and Technology, Ankara

The cross-correlation $C_l(\tau)$ between $m(t)$ and $m(dt+l)$ is

$$\begin{aligned} C_l(\tau) &= \sum_{t=0}^{p^n-2} \omega^{m(t+\tau)-m(dt+l)} \\ &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{Tr}_1^n\left(\alpha^{t+\tau}-\alpha^{dt+l}\right)} \\ &= \sum_{x\in\mathbb{F}_q^*} \omega^{\mathrm{Tr}_1^n\left(ax-bx^d\right)} \\ &= \sum_{x\in\mathbb{F}_{p^n}^*} \chi\left(ax-bx^d\right) \\ &= C(a,b)-1 \end{aligned} \tag{II.1}$$

where $a=\alpha^\tau$, $b=\alpha^l$ and $C(a,b)=\sum_{x\in\mathbb{F}_{p^n}}\chi\left(ax-bx^d\right)$.

We aim to find the distribution of $C_l(\tau)$ as $0\le\tau<p^n-1$ varies, by II.1 finding distribution of $C(a,b)$ as $a\in\mathbb{F}_{p^n}^*$ varies is the same.

Lemma 3: [1] The possible values of $C_l(\tau)$ are given as follows:

1) For $p=3$ there are 9 possible values in total,

$$\left\{-1,-1\pm p^m,\ -1\pm\frac{1+i\sqrt{p}}{2}p^m,\ -1\pm\frac{1-i\sqrt{p}}{2}p^m,-1\pm\frac{1+p}{2}p^m\right\}.$$

2) For $p\equiv 3\,(\mathrm{mod}\,4)\,(\neq 3)$ there are 11 possible values in total,

$$\left\{-1,-1\pm p^m,-1\pm\frac{1+i\sqrt{p}}{2}p^m,-1\pm\frac{1-i\sqrt{p}}{2}p^m,-1\pm\frac{1+p}{2}p^m,-1\pm\frac{1-p}{2}p^m\right\}.$$

3) For $p\equiv 1\,(\mathrm{mod}\,4)$ there are 11 possible values in total,

$$\left\{-1,-1\pm p^m,-1\pm\frac{1+\sqrt{p}}{2}p^m,-1\pm\frac{1-\sqrt{p}}{2}p^m,-1\pm\frac{1+p}{2}p^m,-1\pm\frac{1-p}{2}p^m\right\}.$$

Exactly half of the elements of $\mathbb{F}_{p^n}^*$ are squares and the other half are nonsquares. Using $\gcd\left(p^{m+1}+1,p^m-1\right)=\gcd\left(p^{m+1}+1,p^n-1\right)=2$ and $p^{m+1}+1\equiv 2\,(\mathrm{mod}\,4)$, we have $\gcd\left(p^{m+1}+1,p^n-1\right)=2$. Thus square elements in $\mathbb{F}_{p^n}^*$ can be represented as $x=y^{p^{m+1}+1}$ and nonsquares as $x=ry^{p^{m+1}+1}$, where $y\in\mathbb{F}_{p^n}^*$ and r is a nonsquare in $\mathbb{F}_{p^n}^*$. Note that as y runs through $\mathbb{F}_{p^n}^*$, each $x\in\mathbb{F}_{p^n}^*$, either a square or a nonsquare appears twice. Hence $C(a,b)$ can be expressed as

$$\begin{aligned} 2C(a,b) &= \sum_{y\in\mathbb{F}_{p^n}}\chi\left(ay^{p^{m+1}+1}-by^{d\left(p^{m+1}+1\right)}\right) \\ &\quad+\sum_{y\in\mathbb{F}_{p^n}}\chi\left(ary^{p^{m+1}+1}-br^dy^{d\left(p^{m+1}+1\right)}\right) \\ &= \sum_{y\in\mathbb{F}_{p^n}}\chi\left(ay^{p^{m+1}+1}-by^{p^m+1}\right) \\ &\quad+\sum_{y\in\mathbb{F}_{p^n}}\chi\left(ary^{p^{m+1}+1}-br^dy^{p^m+1}\right) \\ &= T(a,b)+T\left(ar,br^d\right) \end{aligned}$$

where $T(a,b)=\sum_{y\in\mathbb{F}_{p^n}}\chi\left(ay^{p^{m+1}+1}-by^{p^m+1}\right)$.

III. RESULTS

Using similar techniques as in [1], [2] and [3] we have derived the following moment identities.

Lemma 4: The following identities hold:

i) $\sum_{a\in\mathbb{F}_{p^n}}C(a,b)=p^n$.

ii) $\sum_{a\in\mathbb{F}_{p^n}}C^2(a,b)=\begin{cases}p^nN, & \text{if } p\equiv 3\,(\mathrm{mod}\,4)\\ p^{2n}, & \text{if } p\equiv 1\,(\mathrm{mod}\,4).\end{cases}$

where $N=\begin{cases}\frac{(p^n-p^m)}{2}, & \text{if } -2b=\alpha^{\frac{p^m+1}{2}j} \text{ for } j\in\mathbb{Z}\\ -p^m, & \text{otherwise.}\end{cases}$

iii) $\sum_{a\in\mathbb{F}_{p^n}}T(a,b)=q$.

iv) $\sum_{a\in\mathbb{F}_{p^n}}T^2(a,b)=\begin{cases}p^{2n}, & \text{if } p\equiv 1\,(\mathrm{mod}\,4)\\ p^nN_2 & \text{if } p\equiv 3\,(\mathrm{mod}\,4)\end{cases}$

where

$$N_2=\begin{cases}p^n, & \text{if } -2b=\alpha^{\frac{p^m+1}{2}+j(p^m+1)},\ j\in\mathbb{Z}\\ -p^m, & \text{otherwise.}\end{cases}$$

Proof:

i)

$$\begin{aligned}\sum_{a\in\mathbb{F}_{p^n}}C(a,b) &= \sum_{a\in\mathbb{F}_{p^n}}\sum_{x\in\mathbb{F}_{p^n}}\chi\left(ax-bx^d\right) \\ &= \sum_{x\in\mathbb{F}_{p^n}}\chi\left(-bx^d\right)\sum_{a\in\mathbb{F}_{p^n}}\chi(ax) \\ &= p^n\end{aligned}$$

where $\sum_{a\in\mathbb{F}_{p^n}}\chi(ax)=\begin{cases}p^n, & \text{if } x=0\\ 0, & \text{if } x\neq 0.\end{cases}$

ii) Since d is odd when $p\equiv 1\,(\mathrm{mod}\,4)$ and even when $p\equiv 3\,(\mathrm{mod}\,4)$, we have

$$\begin{aligned}&\sum_{a\in\mathbb{F}_{p^n}}C^2(a,b) \\ &= \sum_{a\in\mathbb{F}_{p^n}}\sum_{x\in\mathbb{F}_{p^n}}\chi\left(ax-bx^d\right)\sum_{y\in\mathbb{F}_{p^n}}\chi\left(ay-by^d\right) \\ &= \sum_{x,y\in\mathbb{F}_{p^n}}\chi\left(-b\left(x^d+y^d\right)\right)\sum_{a\in\mathbb{F}_{p^n}}\chi\left(a(x+y)\right) \\ &= p^n\sum_{x\in\mathbb{F}_{p^n}}\chi\left(-b\left(x^d+(-x)^d\right)\right) \\ &= \begin{cases}p^{2n}, & \text{if } p\equiv 1\,(\mathrm{mod}\,4)\\ p^nN & \text{if } p\equiv 3\,(\mathrm{mod}\,4)\end{cases}\end{aligned}$$

where,

$$N = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^{d}\right)$$
$$= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^{\frac{p^m+1}{2}}\right)$$
$$= \frac{1}{2}\sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^{p^m+1}\right) + \frac{1}{2}\sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2br^{\frac{p^m+1}{2}}x^{p^m+1}\right)$$
$$= \begin{cases} \frac{1}{2}\left(p^n-p^m\right) & \text{if } -2b=\alpha^{\frac{p^m+1}{2}j} \text{ for } j\in\mathbb{Z} \\ -p^m & \text{otherwise} \end{cases}$$

with r being nonsquare. Also note that $\sum_{a\in\mathbb{F}_{p^n}} \chi\left(a\left(x+y\right)\right) = \begin{cases} p^n, \text{ if } x+y=0 \\ 0, \text{ if } x+y\neq 0. \end{cases}$

iii) $\sum_{a\in\mathbb{F}_{p^n}} T\left(a,b\right)$

$$= \sum_{a,x\in\mathbb{F}_{p^n}} \chi\left(ax^{p^{m+1}+1} - bx^{p^m+1}\right)$$
$$= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-bx^{p^m+1}\right) \sum_{a\in\mathbb{F}_{p^n}} \chi\left(ax^{p^{m+1}+1}\right)$$
$$= p^n.$$

iv) $\sum_{a\in\mathbb{F}_{p^n}} T^2\left(a,b\right)$

$$= \sum_{a,x,y\in\mathbb{F}_{p^n}} \chi\left(a\cdot g\left(x,y\right) - b\left(x^{p^m+1}+y^{p^m+1}\right)\right)$$
$$= \sum_{x,y\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^{p^m+1}+y^{p^m+1}\right)\right) \cdot \sum_{a\in\mathbb{F}_{p^n}} \chi\left(a\left(g\left(x,y\right)\right)\right)$$
$$= p^n \cdot \left(\sum_{\left\{\substack{x,y\in\mathbb{F}_{p^n},\\ g(x,y)=0}\right\}} \chi\left(-b\left(x^{p^m+1}+y^{p^m+1}\right)\right)\right)$$
$$= p^n \sum_{\left\{\substack{x,y\in\mathbb{F}_{p^n},\\ x^2+y^2=0}\right\}} \chi\left(-b\left(x^{p^m+1}+y^{p^m+1}\right)\right)$$
$$= p^n \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^{p^m+1}+\left(-x^2\right)^{\frac{p^m+1}{2}}\right)\right)$$
$$= p^n \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^{p^m+1}+\left(-1\right)^{\frac{p^m+1}{2}}x^{p^m+1}\right)\right)$$
$$= \begin{cases} p^{2n}, & \text{if } p\equiv 1 \pmod 4 \\ p^n N_2 & \text{if } p\equiv 3 \pmod 4 \end{cases}$$

where $g\left(x,y\right) = x^{p^{m+1}+1} + y^{p^{m+1}+1}$ and

$$N_2 = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^{p^m+1}\right)$$
$$= \begin{cases} p^n, \text{ if } -2b=\alpha^{\frac{p^m+1}{2}+j(p^m+1)}, \; j\in\mathbb{Z} \\ -p^m, \text{ otherwise} \end{cases}$$

by Lemma 1.

■

Note that the above identities will be usefull in finding the cross correlation distribution for all values of $l\neq 0$. But they are not sufficient.

IV. EXPERIMENTAL RESULTS

As we stated before, in [1] all possible values of cross correlation between p-ary m-sequence $m\left(t\right)$ and its decimated sequences $m\left(dt+l\right)$ have been given. Where for the case $p=3$ there are 9 and for the case $p>3$ there are 11 possible values in total. But the exact distribution was not given in [1]. In our numerical results for the case $p=3$, $m\leq 5$ and all possible values of l we have observed that there are at most 8 different values. Here we see that the value $C_l\left(\tau\right) = -1+\frac{1+p}{2}p^m$ that was stated in [1] (which we present in Lemma 3) does not occur. For the general case, i.e. $m>5$ it has to be proved. Furthermore, for the case $p=3$, $m=3$ and $l=\left(p^m+1\right)/4$ we have observed that there are exactly 6 different values with distribution being different from the case $l=0$. Note that the case $l=0$ and $p\equiv 3 \pmod 4$ was proved in [2] and the case $l=0$ and $p\equiv 1 \pmod 4$ was proved in [4].

Computations of this paper were performed in High Performance and Grid Computing Center (TÜBİTAK) by using SAGE program. These codes are partially available online at `www.etilenbaev.etu.edu.tr` . Complexity of a code that computes distribution of $C_l\left(\tau\right)$ for fixed l as τ varies is $O\left(p^{2n}\right)$. Running time for the case $p=3, m=5$ is approximately 2 weeks, while for the case $p=5, m=3$ it took approximately 4 days.

Example 5: When $p=3$, $m=1$ and $0\leq l<\left(p^m+1\right)/2$ complete distribution of cross correlation between m-sequence $m\left(t\right)$ and its decimated sequences $m\left(dt+l\right)$ are given as follows,

	l=0	l=1
$C_l\left(\tau\right)$ values	$\#C_l\left(\tau\right)$	$\#C_l\left(\tau\right)$
$-1+p^m$	4	4
$-1-\frac{1+i\sqrt{p}}{2}p^m$	2	4
$-1-\frac{1-i\sqrt{p}}{2}p^m$	2	-

Example 6: When $p=3$, $m=3$ and $0\leq l<\left(p^m+1\right)/2$ complete distribution of cross correlation between m-sequence $m\left(t\right)$ and its decimated sequences $m\left(dt+l\right)$ are given as follows. Here we point out the case $l=\left(p^m+1\right)/4=7$,

which is 6 valued.

	$l=0$	l=1,2,3,4, 5,6,8,9,10, 11,12,13	$l=7$
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	252	84	-
$-1+p^m$	196	84	168
$-1-p^m$	-	28	56
$-1+\frac{1-i\sqrt{p}}{2}p^m$	-	140	84
$-1+\frac{1+i\sqrt{p}}{2}p^m$	-	140	84
$-1-\frac{1-i\sqrt{p}}{2}p^m$	126	112	168
$-1-\frac{1+i\sqrt{p}}{2}p^m$	126	112	168
$-1-\frac{1+p}{2}p^m$	28	28	-

Example 7: When $p=3$, $m=5$ and $0\le l<(p^m+1)/2$ complete distribution of cross correlation between m-sequence $m(t)$ and its decimated sequences $m(dt+l)$ are given as follows,

	$l=0$	l=1,2,3,5,6,9,10,13, 15,18,20,26,27,30, 32,34,39,40,41,44, 45,52,54,58,60,62, 64,68,70,77,78,81, 82,83,88,90,92,95, 96,102,104,107,109, 112,113,116,117, 119,120,121
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	21960	6588
$-1+p^m$	14884	8052
$-1-p^m$	-	2684
$-1+\frac{1-i\sqrt{p}}{2}p^m$	-	9516
$-1+\frac{1+i\sqrt{p}}{2}p^m$	-	9516
$-1-\frac{1-i\sqrt{p}}{2}p^m$	9882	10248
$-1-\frac{1+i\sqrt{p}}{2}p^m$	9882	10248
$-1-\frac{1+p}{2}p^m$	2440	2196

	l=8,11,17,19,23,24, 25,28,29,31,33,35, 37,38,47,49,50,51, 53,57,65,69,71,73, 75,84,85,87,89,91, 93,94,97,98,99, 103,105,111,114	l=4,7,12,14,16, 21,22,36,42,43, 46,48,55,56,59, 61,63,66,67,74, 76,79,80,86,100, 101,106,108, 110,115,118
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	8052	7320
$-1+p^m$	6588	7320
$-1-p^m$	2196	2440
$-1+\frac{1-i\sqrt{p}}{2}p^m$	10492	10004
$-1+\frac{1+i\sqrt{p}}{2}p^m$	10492	10004
$-1-\frac{1-i\sqrt{p}}{2}p^m$	9272	9760
$-1-\frac{1+i\sqrt{p}}{2}p^m$	9272	9760
$-1-\frac{1+p}{2}p^m$	2684	2440

Example 8: When $p=5$, $m=1$ and $0\le l<(p^m+1)/2$ complete distribution of cross correlation between m-sequence $m(t)$ and its decimated sequences $m(dt+l)$ are given as follows,

	$l=0$	l=1,2
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	6	6
$-1+p^m$	6	$-$
$-1-p^m$	6	6
$-1+\frac{1-\sqrt{p}}{2}p^m$	3	3
$-1+\frac{1+\sqrt{p}}{2}p^m$	3	3
$-1-\frac{1-\sqrt{p}}{2}p^m$	$-$	112
$-1-\frac{1+\sqrt{p}}{2}p^m$	$-$	112
$-1-\frac{1+p}{2}p^m$	$-$	$-$

Example 9: When $p=5$, $m=3$ and $0\le l<(p^m+1)/2$ complete distribution of cross correlation between m-sequence $m(t)$ and its decimated sequences $m(dt+l)$ are given as follows,

	$l=0$	l=1,5,16,17,22, 25,38,41,46,47, 58,62
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	5796	4536
$-1+p^m$	2646	2520
$-1-p^m$	3906	2016
$-1-\frac{1-\sqrt{p}}{2}p^m$	$-$	1449
$-1-\frac{1+\sqrt{p}}{2}p^m$	$-$	1449
$-1+\frac{1-\sqrt{p}}{2}p^m$	1575	1701
$-1+\frac{1+\sqrt{p}}{2}p^m$	1575	1701
$-1+\frac{1-p}{2}p^m$	126	126
$-1-\frac{1+p}{2}p^m$	$-$	126

	l=3,7,12,14,15,28, 35,48,49,51,56,60	l=4,20,26,37, 43,59
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	4536	4536
$-1+p^m$	2772	2898
$-1-p^m$	1764	1638
$-1-\frac{1-\sqrt{p}}{2}p^m$	1701	1827
$-1-\frac{1+\sqrt{p}}{2}p^m$	1701	1827
$-1+\frac{1-\sqrt{p}}{2}p^m$	1449	1323
$-1+\frac{1+\sqrt{p}}{2}p^m$	1449	1323
$-1+\frac{1-p}{2}p^m$	126	126
$-1-\frac{1+p}{2}p^m$	126	126

	l=8,11,23,40,52,55	l=21,42
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	4536	4536
$-1+p^m$	2646	2268
$-1-p^m$	1890	2268
$-1-\frac{1-\sqrt{p}}{2}p^m$	1575	1197
$-1-\frac{1+\sqrt{p}}{2}p^m$	1575	1197
$-1+\frac{1-\sqrt{p}}{2}p^m$	1575	1953
$-1+\frac{1+\sqrt{p}}{2}p^m$	1575	1953
$-1+\frac{1-p}{2}p^m$	126	126
$-1-\frac{1+p}{2}p^m$	126	126

	l=9,18,22,27, 36,45,54	l=19,29,31,32, 34,44
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	5166	5166
$-1+p^m$	2520	2016
$-1-p^m$	1386	1890
$-1-\frac{1-\sqrt{p}}{2}p^m$	1701	1197
$-1-\frac{1+\sqrt{p}}{2}p^m$	1701	1197
$-1+\frac{1-\sqrt{p}}{2}p^m$	1449	1953
$-1+\frac{1+\sqrt{p}}{2}p^m$	1449	1953
$-1+\frac{1-p}{2}p^m$	–	–
$-1-\frac{1+p}{2}p^m$	252	252

	l=6,24,30,33, 39,57	l=2,13,10,50, 53,61
$C_l(\tau)$ values	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	5166	5166
$-1+p^m$	2520	2016
$-1-p^m$	1386	1890
$-1-\frac{1-\sqrt{p}}{2}p^m$	1701	1197
$-1-\frac{1+\sqrt{p}}{2}p^m$	1701	1197
$-1+\frac{1-\sqrt{p}}{2}p^m$	1449	1953
$-1+\frac{1+\sqrt{p}}{2}p^m$	1449	1953
$-1+\frac{1-p}{2}p^m$	–	–
$-1-\frac{1+p}{2}p^m$	252	252

V. CONCLUSION

In conclusion, we have observed from the numerical data that for the case $p = 3$ there are 8 different possible values when $l \neq 0, (p^m+1)/4$, which has to be proved, and 6 different values of cross correlation occurs when $l = (p^m + 1)/4$. Using similar techniques as in [2], [3] we have computed some moment identites. Using additional equations one can compute the distribution of cross correlation for the case $p = 3$, $l = (p^m+1)/4$ and a harder problem which is the case $p = 3$, $l \neq 0, (p^m + 1)/4$, which we leave as a future work.

ACKNOWLEDGMENTS

The authors thank the anonymous referees for their helpful comments. The numerical calculations reported in this paper were performed at TUBITAK ULAKBIM, High Performance and Grid Computing Center (TRUBA Resources). Also the second and the third authors were partially supported by TÜBİTAK under grant no.: TBAG-109T344.

REFERENCES

[1] S.T. Choi, T. Lim, J.S. No and H. Chung, On the cross-correlation of a p-ary m-sequence of period $p^{2m}-1$ and its decimated sequences by $(p^m+1)^2/2(p+1)$, IEEE Trans. Inf. Theory, vol. 58, no. 3, March 2012.

[2] J. Luo, T. Helleseth and A. Kholosha, Two nonbinary sequences with six-valued cross correlation, Proceedings of IWSDA 2011.

[3] E.Y. Seo, Y.S. Kim, J.S. No and D.J. Shin, Cross-correlation distribution of p-ary m-sequences of period p^{4k-1} and its decimated sequences by $\left(\frac{p^{2k}+1}{2}\right)^2$, IEEE Trans. Inf. Theory, vol. 54, no. 7, July 2008.

[4] Y.Sun, H.Li and Z.Wang, The cross-correlation distribution of a p-ary m-sequence of period $p^{2m}-1$ and its decimation by $\frac{(p^m+1)^2}{2(p^e+1)}$ [Online]. Available: http://arxiv.org/abs/1111.3477v1 .

[5] T.Helleseth, L.Hu, A.Kholosha, X.Zeng, N.Li and W.Jiang, Period-different m-sequences with at most four-valued cross correlation, IEEE Trans. Inf. Theory, vol. 55, no. 7, July 2009.

[6] G.J.Ness and T.Helleseth, Cross correlation of m-sequences of different length, IEEE Trans. Inf. Theory, vol. 52, no. 4, April 2006.

[7] T.Helleseth, A.Kholosha and A.Johanssen, m-Sequences of different lengths with four-valued cross correlation, ISIT, July 2008.

[8] A.Johanssen, T.Helleseth and A.Kholosha, Further results on m-sequences with five-valued cross correlation, IEEE Trans. Inf. Theory, vol. 55, no. 12, December 2009.

[9] T.Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Math. 16, 209-232, 1976.

[10] R.Lidl and H.Niederreiter, Finite Fields. Cambridge University Press, 1997.