Evaluation of Cross-Correlation Values of $p$-ary m-Sequence and its Decimated Sequence by

$$\frac{p^n+1}{p+1} + \frac{p^n-1}{2}$$

Sung-Tai Choi, Taehyung Lim, and Jong-Seon No
Department of Electrical Engineering and Computer Science, INMC
Seoul National University
Seoul 151-744, Korea
Email: stchoi@ccl.snu.ac.kr, jayelish@hotmail.com, and jsono@snu.ac.kr

Habong Chung
School of Electronics and Electrical Engineering
Hongik University
Seoul 121-791, Korea
Email: habchung@hongik.ac.kr

Abstract—For a prime $p \equiv 1 \mod 4$, an odd integer $n$, and $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$, we investigate the cross-correlation values of $p$-ary m-sequence $m(t)$ of period $p^n - 1$ and its decimated m-sequence $m(dt)$. It is shown that the cross-correlation function between $m(t)$ and $m(dt)$ takes the values in $\{-1, -1 \pm p^{n/2}, -1 \pm \frac{1+p\sqrt{p}}{2}p^{n/2}, -1 \pm \frac{1-p\sqrt{p}}{2}p^{n/2}, -1 \pm 1\pm p^{n/2} \}$. 

Index Terms—Cross-correlation, m-sequence, decimated sequence, $p$-ary sequence.

I. INTRODUCTION

Evaluation of the cross-correlation function between an m-sequence $m(t)$ and its decimated m-sequence $m(dt)$ has been studied by various researchers. Gold [1] evaluated the cross-correlation function for the case $d = 2^k + 1$ and $n/\gcd(n,k)$ odd. Welch [2] evaluated the cross-correlation function for the case $d = 2^{2k} - 2^k + 1$ and $n/\gcd(n,k)$ odd. Niho [3] found some decimation values for which the cross-correlation of two binary m-sequences has few correlation values and derived the distribution of the cross-correlation values. Trachtenberg [4] extended the results to nonbinary cases. For an odd prime $p$, he evaluated the cross-correlation function for the cases $d = \frac{p^{2k}+1}{2}$ and $d = p^{2k} - p^k + 1$. For an odd prime $p$, Helleseth [5] found some decimation values for which the cross-correlation of two m-sequences has few correlation values and derived the distribution of the cross-correlation values. For the decimation value $d = \frac{p^{2k}+1}{2} + p^{2k-1}$, Muller [7] and Hu et al. [8] derived an upper bound on the magnitudes of the cross-correlations for $p = 3$ and an odd prime $p \equiv 3 \mod 4$, respectively. In their studies, there are two distinct decimated sequences $m(dt)$ and $m(dt+1)$ since $\gcd(d, p^n - 1) = 2$.

In this paper, for the same decimation $d$, but for a prime $p \equiv 1 \mod 4$ and an odd integer $n$ so that $\gcd(d, p^n - 1) = 1$, the possible values of the cross-correlation function between a $p$-ary m-sequence $m(t)$ and its decimated m-sequence $m(dt)$ are determined.

II. PRELIMINARIES AND NOTATIONS

A. Trace Functions and Cross-Correlation Function

Let $p$ be a prime and $F_p^n$, the finite field with $p^n$ elements. Then the trace function $\text{tr}_k(·)$ from $F_p^n$ to $F_p^k$ is defined as

$$\text{tr}_k(x) = \sum_{i=0}^{\frac{p-1}{k}} x^{p^ki}$$

where $x \in F_p^n$ and $k|n$.

Let $\alpha$ be a primitive element of $F_p^n$. Then a $p$-ary m-sequence $m(t)$ of period $p^n - 1$ can be expressed as

$$m(t) = \text{tr}_1^n(\alpha^t).$$

The periodic cross-correlation function between two $p$-ary sequences $s_1(t)$ and $s_2(t)$ of period $N$ at shift $\tau$ is defined as

$$C(\tau) = \sum_{t=0}^{N-1} \omega^{s_1(t+\tau) - s_2(t)}$$

where $\omega$ is a $p$-th root of unity.

B. Quadratic Form

The quadratic character of $F_p^n$ is defined as

$$\eta(x) = \begin{cases} 
1, & \text{if } x \text{ is a square in } F_p^n \setminus \{0\} \\
-1, & \text{if } x \text{ is a nonsquare in } F_p^n \setminus \{0\} \\
0, & \text{if } x = 0.
\end{cases}$$

A quadratic form over $F_p$ in $n$ indeterminates is a homogeneous polynomial in $F_p[x_1, x_2, \cdots, x_n]$ of degree 2 and can be expressed as

$$f(x_1, x_2, \cdots, x_n) = \sum_{i,j \leq n} a_{ij}x_ix_j$$

where $a_{ij} \in F_p$.

Let $(F_p^n)^n$ denote an $n$-dimensional vector space over $F_p$. The number of solutions $(x_1, x_2, \cdots, x_n) \in (F_p^n)^n$ satisfying the quadratic form $f(x_1, x_2, \cdots, x_n) = b$ for any $b \in F_p$ can be determined from the rank of the quadratic form $f(x_1, x_2, \cdots, x_n)$. The following lemma explains how to calculate the rank of a quadratic form.
Lemma 1 ([7]): Let $f \in F_p[x_1, x_2, \cdots, x_n]$ be a quadratic form. Define

$$Z := \{z \in (F_p)^n : f(x + z) - f(x) = 0 \text{ for all } x \in (F_p)^n\}.$$ 

Then $Z$ is a subspace of $(F_p)^n$ and rank$(f) = n - \dim(Z)$. 

A quadratic form $f(x)$ in $n$ indeterminates over $F_p$ can be regarded as a mapping $f(x)$ from $F_p^n$ into $F_p$. Thus, we will also use the term 'quadratic form' for this mapping $f(x)$ in a finite extension field $F_p^n$. In this case, Lemma 1 in a finite field version can be restated as follows.

Corollary 2: The rank $\rho$ of the quadratic form $f(x)$ from $F_p^n$ to $F_p$ can be determined by finding the number of elements of the form $f(x)$ dependent, i.e., $p^n - \rho$ is the number of $z \in F_p^n$ such that $f(x + z) = f(x)$ for all $x \in F_p^n$.

If a nonzero quadratic form $f \in F_p[x_1, x_2, \cdots, x_n]$ has a rank $k \leq n$, it can be rewritten as an equivalent canonical form $a_1x_1^2 + a_2x_2^2 + \cdots + a_kx_k^2$ with all nonzero $a_i$'s. Hence for any $b \in F_p$, the number of solutions of $a_1x_1^2 + a_2x_2^2 + \cdots + a_kx_k^2 = b$ in $(F_p)^n$ is $p^{n-k}$ times the number of solutions of the same equation in $(F_p)_k$. [9]

A quadratic form $f \in F_p[x_1, x_2, \cdots, x_k]$ in $k$ indeterminates over $F_p$ is said to be a nondegenerate quadratic form if $f$ has a rank $k$, i.e., $f$ can be expressed as the canonical form $a_1x_1^2 + a_2x_2^2 + \cdots + a_kx_k^2$ for $a_i \neq 0$. Let $\Delta = a_1a_2\cdots a_k$ denote the determinant of the quadratic form $f$. Then $f$ is a nondegenerate quadratic form of rank $k$, the number of solutions $x$ in $F_p$ satisfying $f(x) = b$ in $F_p$ is determined as the following lemma.

Lemma 3 (Theorem 6.26 and 6.27 [9]): Let $\eta$ be the quadratic character of $F_p$. The number of solutions $N(b)$ of $f(x) = b$ in $(F_p)^k$ when $f(x)$ is a nondegenerate quadratic form of rank $k$ with determinant $\Delta$ and $b \in F_p$, is given as follows:

Case 1) $k$ even;

$$N(b) = \begin{cases} p^{k-1} - \epsilon p^{k-2}, & \text{if } b \neq 0 \\ p^{k-1} + \epsilon(p - 1)p^{k-2}, & \text{if } b = 0 \end{cases}$$

where $\epsilon = \eta((-1)^{k/2}\Delta)$.

Case 2) $k$ odd;

$$N(b) = \begin{cases} p^{k-1} + \epsilon \eta(b)p^{k-2}, & \text{if } b \neq 0 \\ p^{k-1}, & \text{if } b = 0 \end{cases}$$

where $\epsilon = \eta((-1)^{(k-1)/2}\Delta)$.

C. Linearized Polynomial

Let $p$ be a prime. A polynomial of the form

$$L(x) = \sum_{i} \alpha_i x^{p^i}$$

with coefficients in an extension field $F_p^n$ of $F_p$ is called a linearized polynomial over $F_p^n$. If $F$ is an arbitrary extension field of $F_p$, then

$$L(\beta + \gamma) = L(\beta) + L(\gamma), \text{ for all } \beta, \gamma \in F$$

$$L(c\beta) = cL(\beta), \text{ for all } \beta \in F \text{ and } c \in F_p$$

Hence the set of solutions of $L(x) = 0$ in $F$ is considered as a vector subspace over $F_p$.

In the rest of the paper, the following notations are used:

- $p$ is an odd prime such that $p \equiv 1 \mod 4$;
- $n$ is an odd positive integer;
- $d = p^{n+1} + p^{n-1}$;
- $\alpha$ is a primitive element of $F_p^n$;
- $\omega$ is a primitive $p$-th root of unity;
- $F_p^n$ is a multiplicate group of $F_p^n$, i.e., $F_p^n \setminus \{0\}$.

III. Evaluation of Cross-Correlation Values

The periodic cross-correlation $C(\tau)$ between $m(t)$ and $m(dt)$ at shift $\tau$ is given as

$$C(\tau) = \sum_{t=0}^{p^n-2} \omega^{m(t+\tau) - m(dt)}$$

$$= \sum_{t=0}^{p^n-2} \omega^{\text{tr}_1^{\alpha}(\alpha^{t+\tau} - \alpha^{dt})}$$

$$= \sum_{x \in F_p^n} \omega^{\text{tr}_1^{\alpha}(ax - x^d)}$$

where $a = \alpha^\tau$.

Let $S(a)$ be the exponential sum defined by

$$S(a) = \sum_{x \in F_p^n} \omega^{\text{tr}_1^{\alpha}(ax - x^d)}.$$ 

Then the cross-correlation $C(\tau)$ can be expressed as

$$C(\tau) = S(a) - 1.$$ 

Exactly the half of the elements in $F_p^n$ are squares and the other half are nonsquares. Using $\gcd(p+1, p^n-1) = 2$, we can represent each square in $F_p^n$ as $x = y^{p+1}$ for some $y \in F_p^n$. Since a nonsquare in $F_p^n$ is also a nonsquare in $F_p$, we can represent nonsquares in $F_p^n$, as $x = ry^{p+1}$, where $r$ is a nonsquare in $F_p$. Note that as $y$ runs through $F_p^n$, $y^{p+1}$ covers all the squares in $F_p$, exactly twice and so does $ry^{p+1}$ for the nonsquares. Using $y^{p+1} = y^2$ and $y^{p+1} = -r$, we can express $S(a)$ as

$$2S(a) = \sum_{y \in F_p^n} \omega^{\text{tr}_1^{\alpha}(ay^{p+1} - y^2)} + \sum_{y \in F_p^n} \omega^{\text{tr}_1^{\alpha}(ay^{p+1} - y^2)}$$

$$= \sum_{y \in F_p^n} \omega^{\text{tr}_1^{\alpha}(ay^{p+1} - y^2)} + \sum_{y \in F_p^n} \omega^{\text{tr}_1^{\alpha}(ay^{p+1} + y^2)}$$

$$= \sum_{y \in F_p^n} \omega^{g(y)} + \sum_{y \in F_p^n} \omega^{h(y)}$$

where $g(y) = \text{tr}_1^{\alpha}(ay^{p+1} - y^2)$ and $h(y) = \text{tr}_1^{\alpha}(ay^{p+1} + y^2)$.

If $y$ is expressed in terms of a basis $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ of $F_p^n$ over $F_p$ as $y = \sum_{i=1}^n y_i \alpha_i$, where $y_i \in F_p$, then $g(y)$ can
be represented as the quadratic form, that is,
\[ g(y) = \text{tr}_1^a \left( a \left( \sum_{i=1}^n y_i \alpha_i \right)^2 \right) - \left( \sum_{i=1}^n y_i \alpha_i \right)^2 \]
\[ = \text{tr}_1^a \left( a \left( \sum_{i=1}^n y_i \alpha_i \right) \left( \sum_{j=1}^n y_j \alpha_j \right) \right) - \left( \sum_{i=1}^n y_i \alpha_i \right)^2 \]
\[ = \sum_{i=1}^n y_i \alpha_i \left( a \alpha_i \alpha_j - \alpha_i \alpha_j \right) \]
\[ = \sum_{i=1}^n y_i \alpha_i \left( 2a \alpha_i \alpha_j \right) \]
where \( g_{ij} = \text{tr}_1^a \left( a \alpha_i \alpha_j - \alpha_i \alpha_j \right). \)

Similarly, we can show that \( h(y) \) is also a quadratic form. From Lemma 1, Corollary 2, and Lemma 3, in order to evaluate the exponential sum \( S(a) \), we need to know the ranks of the quadratic forms \( g(y) \) and \( h(y) \), i.e., the number of solutions \( z \in F_{p^n} \) of the equations \( g(y + z) = g(y) \) and \( h(y + z) = h(y) \) for all \( y \in F_{p^n} \).

Lemma 4: The number of solutions \( z \in F_{p^n} \) satisfying \( g(y + z) = g(y) \) for all \( y \in F_{p^n} \) equals the number of solutions \( z \in F_{p^n} \) satisfying
\[ L_g(z) = a^p z^p - 2z + a = 0 \]  \hspace{1cm} (6)
and the number of solutions \( z \in F_{p^n} \) satisfying \( h(y + z) = h(y) \) for all \( y \in F_{p^n} \) equals the number of solutions \( z \in F_{p^n} \) satisfying
\[ L_h(z) = a^p z^p + 2z + a = 0. \] \hspace{1cm} (7)

Proof: The equation \( g(y + z) = g(y) \) can be written as
\[ \text{tr}_1^a \left( a(y + z)^{p+1} - (y + z)^2 \right) = \text{tr}_1^a \left( ay^{p+1} - y^2 \right). \] \hspace{1cm} (8)
Then (8) can be rewritten as
\[ \text{tr}_1^a \left( a(y + z)^{p+1} - (y + z)^2 \right) = \text{tr}_1^a \left( ay^{p+1} - y^2 \right). \] \hspace{1cm} (9)
Equation (9) holds for all \( y \in F_{p^n} \) if and only if
\[ \text{tr}_1^a \left( az^{p+1} - z^2 \right) = 0 \] \hspace{1cm} (10)
and (6) are satisfied simultaneously. Hence the number of solutions \( z \in F_{p^n} \) satisfying (8) can be determined by finding the number of solutions \( z \in F_{p^n} \) satisfying (6) and (10) simultaneously.

Now, we will show that all solutions \( z \in F_{p^n} \) satisfying (6) also satisfy (10). From (6) we have
\[ 2z = a^{p^2} + az. \]
Raising to the \( p^i - 1 \) power and multiplying by \( z^p \) gives
\[ 2z^{p^i} = a^{p^i} z^{p^{i+1} + p^i} + a^{p^i - 1} z^{p^{i+1} + p^{i-1}}. \] \hspace{1cm} (11)
Using (11), the left hand side of (10) can be rewritten as
\[ \text{tr}_1^a \left( az^{p+1} - z^2 \right) \]
\[ = \sum_{i=0}^{p^i - 1} \left( a^{p^i} z^{p^{i+1} + p^i} - z^{2p^i} \right) \]
\[ = \sum_{i=0}^{p^i - 1} \left( a^{p^i} z^{p^{i+1} + p^i} - 2^{-1}(a^{p^i} z^{p^{i+1} + p^i} + a^{p^i - 1} z^{p^i + p^{i-1}}) \right) \]
\[ = 0. \]

Hence we only need to calculate the number of solutions for (6) to determine the number of solutions for \( g(y + z) = g(y) \). The case of \( h(y) \) can be proven similarly.

Lemma 5: Let \( n_g \) and \( n_h \) denote the number of solutions in \( F_{p^n} \) of \( L_g(z) = 0 \) and \( L_h(z) = 0 \), respectively. Then either \( n_g \) or \( n_h \) is one.

Proof: Assume that both equations \( L_g(z) = 0 \) and \( L_h(z) = 0 \) have nonzero solutions \( z_1 \) and \( z_2 \), respectively. The possible ranks of the quadratic forms \( L_g(z_1) \) and \( L_h(z_2) \) should be one, which is proved in the following lemma.

Lemma 6: Let \( r_g \) and \( r_h \) denote the ranks of the quadratic forms \( g(y) \) and \( h(y) \), respectively. The possible ranks of \( g(y) \) and \( h(y) \) are \((1,1), (1,p), (1,p^2), (p,1), \) and \((p^2,1)\). It is straightforward to derive the following corollary from the above lemma.

Corollary 6: Let \( r_g \) and \( r_h \) denote the ranks of the quadratic forms \( g(y) \) and \( h(y) \), respectively. The possible ranks of \( g(y) \) and \( h(y) \) are \((n,n), (n,n-1), (n,n-2), (n-1,n), \) and \((n-2,n)\). Next, we will present the upper bound of \(|S(a)|\) given in (5) as Lemma 9. The following theorems are needed for the proof of Lemma 9.
Theorem 7 (Theorem 5.15 [9]): Let \( p \) be an odd prime and \( \eta \) the quadratic character of \( F_p \). Then
\[
\sum_{i=1}^{p-1} \eta(i) \omega^i = \begin{cases} 
\frac{1}{p}, & \text{if } p \equiv 1 \mod 4 \\
\frac{-1}{ip^2}, & \text{if } p \equiv 3 \mod 4
\end{cases}
\]
where \( \omega \) is a primitive \( p \)-th root of unity.

Theorem 8 (Theorem 5.38 [9]): Let \( f \in F_p[x] \) be a polynomial of degree \( s \geq 1 \) with \( \gcd(s, p^n) = 1 \) and let \( \chi \) be a nontrivial additive character of \( F_p^n \). Then
\[
| \sum_{c \in F_p^n} \chi(f(c)) | \leq (s-1)p^{n/2}.
\]

Lemma 9: The magnitude of the exponential sum \( S(a) \) given in (5) is upper-bounded as
\[
| S(a) | \leq \frac{p-1}{2} p^{\frac{n}{2}}.
\]

Proof: We have to show that
\[
\left| \sum_{y \in F_p^n} \omega^{\mu y + \rho} \right| \leq (p-1) p^{\frac{n}{2}}.
\]
Set \( r = \alpha^{\frac{n-1}{2}} \), which is a nonsquare in \( F_p \) and generator of \( F_p \). Define \( C_0 = \{ x^2 \mid x \in F_p^* \} \) and \( C_1 = F_p^* \backslash C_0 \).

The first term in (12) can be written as
\[
\sum_{y \in F_p^n} \omega^{\mu y + \rho} = 1 + \sum_{z \in C_0} \omega^{\mu \frac{z^2}{p} + \rho} - \sum_{z \in C_1} \omega^{\mu \frac{z^2}{p} + \rho}
\]
where \( z = y^2 \).

Clearly, \(-1\) is a square in \( F_p \) and \( \frac{p-1}{2} = -r \). Then we have
\[
\sum_{z \in C_0} \omega^{\mu \frac{z^2}{p} + \rho} = \sum_{u \in C_1} \omega^{\mu (ru) + \rho} = \sum_{u \in C_1} \omega^{\mu (ru) + \rho} - \sum_{u \in C_1} \omega^{\mu (ru) + \rho} - \sum_{u \in C_1} \omega^{\mu (ru) + \rho} + \sum_{v \in C_1} \omega^{\mu \frac{v^2}{p} + \rho}
\]
where \( z = ru \) and \( v = -u \). Hence the first term in (12) can be written as
\[
\sum_{y \in F_p^n} \omega^{\mu y + \rho} = 1 + \sum_{z \in C_0} \omega^{\mu \frac{z^2}{p} + \rho}
\]
Similarly, the second term in (12) can be written as
\[
\sum_{y \in F_p^n} \omega^{\mu y + \rho} = 1 + \sum_{z \in C_0} \omega^{\mu \frac{z^2}{p} + \rho} + \sum_{z \in C_1} \omega^{\mu \frac{z^2}{p} + \rho} + \sum_{z \in C_1} \omega^{\mu \frac{z^2}{p} + \rho}. \tag{13}
\]
where \( z = y^2 \).

Proof: From (5), the correlation function in (3) can be expressed using the function \( S(a) \) as
\[
C(\tau) = -1 + S(a) = -1 + \frac{1}{2} \left( \sum_{y \in F_p^n} \omega^{g(y)} + \sum_{y \in F_p^n} \omega^{h(y)} \right)
\]
where \( g(y) = \omega^{\mu y + \rho} \) and \( h(y) = \omega^{\mu y + \rho} \), and \( g(y) \) and \( h(y) \) are quadratic forms. From Corollary 6, the possible ranks of \( g(y) \) and \( h(y) \) are \( (n,n) \),
(n-1,n), (n-2,n), (n,n-1), and (n,n-2). By using Lemma 3, we can derive the correlation values as follows:

Case 1) Rank of \(g(y) = n-2\) and rank of \(h(y) = n\) (or rank of \(g(y) = n\) and rank of \(h(y) = n-2\));

From Lemma 3 and Theorem 7, we have

\[
2S(a) = \sum_{y \in F_p^n} \omega^g(y) + \sum_{y \in F_p^n} \omega^h(y)
\]

\[
= p^2 \left( p^{n-3} + \sum_{i=1}^{p-1} \left( \left( p^{n-3} + \epsilon_g \eta(i) p^{\frac{n-3}{2}} \right) \omega^i \right) \right) \\
+ \left( p^{n-1} + \sum_{i=1}^{p-1} \left( \left( p^{n-1} + \epsilon_h \eta(i) p^{\frac{n-1}{2}} \right) \omega^i \right) \right)
\]

\[
= p^{\frac{n+1}{2}} \epsilon_g \sum_{i=1}^{p-1} \eta(i) \omega^i + p^{\frac{n-1}{2}} \epsilon_h \sum_{i=1}^{p-1} \eta(i) \omega^i
\]

\[
= p^{\frac{n+1}{2}} (p \epsilon_g + \epsilon_h).
\]

Thus, we obtain

\[
C(\tau) = -1 + \frac{p \epsilon_g + \epsilon_h}{2} p^{\frac{n}{2}}.
\]

Both \(\epsilon_g\) and \(\epsilon_h\) should take values in \([+1,-1]\). However, when \(\epsilon_g = \epsilon_h\), it contradicts to Lemma 9. Hence the possible case is \(\epsilon_g = 1\) and \(\epsilon_h = -1\) or vice versa. Hence the possible values here are

\[
\{ -1 + \frac{p-1}{2} p^{n/2}, -1 + \frac{-p+1}{2} p^{n/2} \}.
\]

Case 2) Rank of \(g(y) = n-1\) and rank of \(h(y) = n\) (or rank of \(g(y) = n\) and rank of \(h(y) = n-1\));

The case for rank \(n\) was dealt with in the previous case. Hence we have

\[
C(\tau) = -1 + \epsilon_g + \epsilon_h p^{\frac{n}{2}}.
\]

Since \(\epsilon_g\) and \(\epsilon_h\) take values in \([+1,-1]\), the number of possible correlation values is 3 in this case. Hence the possible values here are

\[
\{ -1, -1 + p^{n/2}, -1 - p^{n/2} \}.
\]

IV. Concluding Remark

In this paper, we evaluate the values of cross-correlation function between a \(p\)-ary \(m\)-sequence \(m(t)\) and its decimated sequence \(m(dt)\), for \(d = p^n + 1 + p^{n-1} \frac{1}{2}\), a prime \(p \equiv 1 \text{ mod } 4\), and \(n\) odd. In fact, we have derived the distribution of cross-correlation values. Due to the page limit, we did not include them, in this paper. The extended version [10], in which the derivation of the distribution of the cross-correlation values is included, will be soon submitted.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2011-0000328) and the KCC (Korea Communications Commission), Korea, under the R&D program supervised by the KCA (Korea Communications Agency) (KCA-2011-08913-04003).

References


[10] S. T. Choi, T. Lim, J. S. No, and H. Chung, “Cross-Correlation Distribution of \(p\)-ary \(m\)-sequence and its Decimated sequence by \(p^n + 1 + p^{n-1} \frac{1}{2}\) in preparation.