Upper Bound on the Cross-Correlation between Two Decimated Sequences

Chang-Min CHO (a), Wijik LEE (b), Nonmembers, Jong-Seon NO (c), and Young-Sik KIM (d), Members

SUMMARY In this paper, for an odd prime \( p \), two positive integers \( n, m \) with \( n = 2m \) and \( p^m \equiv 1 \pmod{4} \), we derive an upper bound on the magnitude of the cross-correlation function between two decimated sequences of a \( p \)-ary m-sequence. The two decimation factors are 2 and \( 2(p^m + 1) \), and the upper bound is derived as \( \frac{2^{(p^m+1)/2}}{2} \). In fact, those two sequences correspond to the \( p \)-ary sequences used for the construction of Kasami sequences decimated by 2. This result is also used to obtain an upper bound on the cross-correlation magnitude between a \( p \)-ary m-sequence and its decimated sequence with the decimation factor \( d = \frac{2^{(p^m+1)/2}}{2} \).

Key words: cross-correlation, decimated sequences, m-sequences, \( p \)-ary sequences

1. Introduction

In pseudorandom sequence design, finding sequences with low correlation property has been of great interest. Such sequences have various applications in code-division multiple-access (CDMA), radar, cryptography, and so on. To find sequence families with low correlation, lots of studies have attempted to find the cross-correlation between an \( m \)-sequence and its decimated sequences. The readers may refer to [1]–[12] for details on this topic.

Recently, the cross-correlation between two differently decimated sequences has been studied. Kim et al. [13] constructed a \( p \)-ary sequence family with low correlation by using two decimated sequences, where \( p \equiv 3 \pmod{4} \) is an odd prime, \( n \) is an odd integer, and the decimation factors are 2 and \( 2(\frac{p^n-1}{2}-p^{n-1}) \). The results in [13] were generalized in [14], where the decimation factors are \( e \) and \( e(\frac{p^n-1}{2}-p^{n-1}) \) with \( e \) and \( < \sqrt{p^n-1}/\sqrt{p} \). Xia and Chen [15] constructed a \( p \)-ary sequence family by using sequences with decimation factors 2 and \( p^m + 1 \), and derived its correlation distribution. Lee et al. [16] obtained an upper bound on the cross-correlation magnitude of two decimated \( p \)-ary sequences and constructed new sequence families. The maximum correlation bound was derived by using Weil’s bound [20] on exponential sums. In [17] and [18], the cross-correlation between \( p \)-ary sequences with decimation factors 2 and \( 2d = 2d \) was investigated, where the values \( d \) were studied in [1], [7], and [11]. Note that in most cases, one of the two decimation factors is 2 and then the sequence families constructed have period \( \frac{p^n-1}{2} \), which is the half of that of an \( m \)-sequence.

In this paper, an upper bound on the magnitude of the cross-correlation between two decimated \( p \)-ary sequences is determined, where the decimation factors are 2 and \( 2(2(p^m+1)) \) with \( n = 2m \) and \( p^m \equiv 1 \pmod{4} \). In fact, those two sequences correspond to the \( p \)-ary sequences used for the construction of Kasami sequences decimated by 2. The upper bound is derived as \( \frac{2^{(p^m+1)/2}}{2} \), which is the same as that of [16]. It is obtained by showing equivalence to the exponential sum in [16] and applying Weil’s bound.

Also, using the above result of the cross-correlation between two decimated sequences, an upper bound of cross-correlation magnitude between a \( p \)-ary m-sequence and its decimated sequence is derived. The decimation factor is \((p^m+1)/2\) where \( n = 2m \) and \( p^m \equiv 1 \pmod{4} \). Note that this decimation factor was investigated previously in [18] to construct a sequence family of half period.

The remainder of this paper is organized as follows. In Sect. 2, we give some notations and preliminaries for the trace function, sequences, and the character sums. In Sect. 3, we present upper bounds on the cross-correlation between two \( p \)-ary sequences. The concluding remarks are given in Sect. 4.

2. Preliminaries

Let \( p \) be an odd prime, \( m \) be a positive integer satisfying \( p^m \equiv 1 \pmod{4} \), and \( n = 2m \). Let \( F_{p^m} \) denote the finite field with \( p^m \) elements and \( F_{p^m}^* = F_{p^m}\backslash\{0\} \). The trace function \( \text{tr}_n^m(\cdot) \) from \( F_{p^m} \) to its subfield \( F_{p^m}^* \) is defined as

\[
\text{tr}_n^m(x) = \sum_{i=0}^{\frac{m}{n}-1} x^{p^{ni}}.
\]

An element \( x \) in \( F_{p^m} \) can be expressed as

\[
x = \sum_{i=1}^{\frac{m}{n}} c_i \alpha_i
\]

where \( c_i \in F_{p^m} \) and \( \{\alpha_1, \ldots, \alpha_{n/k}\} \) is a basis of \( F_{p^m} \) over \( F_{p^m}^* \).
The basis \( \{ \alpha_1, \ldots, \alpha_n \} \) is said to be \textit{trace-orthogonal} if
\[
\text{tr}_k^n(a_i \alpha_j) = \begin{cases} 
d_i, & \text{if } i = j \\
0, & \text{otherwise}
\end{cases}
\]
where \( d_i \in F_{p^n} \). It is known that for any odd prime \( p \), there exists a trace-orthogonal basis of \( F_{p^n} \) over \( F_p \) [19].

Let \( \sigma \) be a primitive element of \( F_{p^n} \). Then a \( p \)-ary \( m \)-sequence \( s(t) \) of period \( p^n - 1 \) can be written as \( s(t) = \text{tr}_k^n(a^t) \) and its decimated sequences \( s(dt + l) \) are given as \( s(dt + l) = \text{tr}_k^n(a^{dt+l}) \).

The cross-correlation function of two \( p \)-ary sequences \( a(t) \) and \( b(t) \) of period \( N \) is defined as
\[
C_{a,b}(\tau) = \sum_{t=0}^{N-1} \omega^{a(t+\tau)-b(t)}
\]
where \( \omega = e^{2\pi \sqrt{-1}/p} \) is a primitive \( p \)-th root of unity.

For a finite abelian group \( G \), a character \( \chi \) of \( G \) is a homomorphism from \( G \) to the multiplicative group of complex numbers with absolute value 1. For a finite field, there are two kinds of characters, namely, an additive character and a multiplicative character.

The canonical additive character of \( F_{p^n} \) is defined as \( \chi_1(x) = \omega^{pr(x)} \) for all \( x \in F_{p^n} \) and every additive character of \( F_{p^n} \) can be obtained as \( \chi_b(x) = \chi_1(bx) \) for all \( b, x \in F_{p^n} \).

A multiplicative character of \( F_{p^n} \) is defined as \( \psi_j(a^t) = e^{2\pi \sqrt{-1}/p} \) for \( k = 0, 1, \ldots, p^n - 2 \).

If \( j = (p^n - 1)/2 \), then the character \( \eta(x) = \psi((p-1)/2) \) takes the value 1 if \( x \) is the square in \( F_{p^n}^* \) and \(-1\) if \( x \) is the nonsquare. This multiplicative character \( \eta(x) \) is called the quadratic character of \( F_{p^n}^* \).

The following lemma for the character sums, which is needed.

**Lemma 1:** (Weil’s bound [20]) Let \( q = p^n \) be an additive character of the finite field \( F_q \), and \( \psi \) a multiplicative character of \( F_q \) of order \( m \). Let \( f(x) \in F_q[x] \) be of degree \( e \geq 1 \) and \( g(x) \in F_q[x] \) be with \( s \) distinct roots in \( F_q[x] \), where \( \phi \neq c \cdot \text{h}^m \) for some \( c \in F_q \), \( f \neq \text{h}^p - h \) for \( h \in F_q[x] \), and \( F_q \) denotes the algebraic closure of \( F_q \). Then we have
\[
\left| \sum_{x \in F_q} \psi(g(x))\chi(f(x)) \right| \leq (e + s - 1) \sqrt{q}. \]

\[ \Box \]

### 3. Main Results

#### 3.1 The Cross-Correlation between \( s(2t + i) \) and \( s(2(p^n + 1)t + j) \)

The cross-correlation function between \( s(2t + i) \) and \( s(2(p^n + 1)t + j) \) of period \((p^n - 1)/2\) is given as
\[
C_{i,j}(\tau) = \sum_{\tau=0}^{p^n-1} \omega^{\tau(a^{2(i+\tau)+1}-a^{2(p^n+1)\tau+1})} \quad (1)
\]
where \( \text{gcd}(p^n - 1, 2(p^n + 1)) = 2(p^n + 1) \), \( i = 0, 1, \) and \( j = 0, p^n + 1 \). In fact, those two sequences correspond to the \( p \)-ary sequences used for the construction of Kasami sequences decimated by 2. In this subsection, we derive the cross-correlation bound for the above two decimated sequences. It is easy to check that
\[
\sum_{\tau=0}^{p^n-1} \omega^{\tau(a^{2(i+\tau)+1}-a^{2(p^n+1)\tau+1})} = \sum_{\tau=-\frac{p^n}{2}}^{\frac{p^n}{2}-1} \omega^{\tau(a^{2(i+\tau)+1}-a^{2(p^n+1)\tau+1})}
\]
and thus we can express the cross-correlation as
\[
C_{i,j}(\tau) = \sum_{\tau=-\frac{p^n}{2}}^{\frac{p^n}{2}-1} \omega^{\tau(a^{2(i+\tau)+1}-a^{2(p^n+1)\tau+1})}
\]
where \( x = a' \), \( a = \omega^{2+i} \), and \( b = a' \). Let \( y = x^2 \) and \( QR \) denote the set of squares in \( F_{p^n}^* \). Then as \( x \) runs through \( F_{p^n}^* \), \( y \) runs through \( QR \) twice. Therefore, (2) can be rewritten as
\[
C_{i,j}(\tau) = \frac{1}{2} \sum_{y \in QR} \omega^{\tau(a^{2(i+\tau)+1}-a^{2(p^n+1)\tau+1})}
\]
\[
= \frac{1}{2} \sum_{y \in F_{p^n}^*} \omega^{\tau(a^{2(i+\tau)+1})} + \sum_{y \in F_{p^n}^*} \eta(y) \omega^{\tau(a^{2(p^n+1)\tau+1})}. \quad (3)
\]

We want to find the upper bound of the cross-correlation magnitude \( |C_{i,j}(\tau)| \). It is obvious from the correlation property of \( p \)-ary Kasami sequences that [21]
\[
\sum_{y \in F_{p^n}^*} \left| \omega^{\tau(a^{2(i+\tau)+1})} \right| \leq p^n + 1. \quad (4)
\]

In order to prove our main theorem, the following results are needed.
Lemma 2: For an odd prime $p$, two integers $n, m$ with $n = 2m$, and $p^m ≡ 1 \pmod{4}$, there exist $a', b'$, and $z ∈ F_p^*$ satisfying

$$tr_f(ay - by^{p+1}) = tr_f(a'z - b'z^2)$$

(5)

where as $y$ runs through $F_p^*$, $z$ also runs through all elements in $F_p^*$.

Proof: Using the property of the trace function, we have

$$tr_f(by^{p+1}) = tr_f(tr_m(by^{p+1})) = tr_f(2by^{p+1})$$

because $b = 1$ or $a^{p+1} ∈ F_p^*$ and $y^{p+1} ∈ F_p^*$. Let $y = c_1a_1 + c_2a_2$, where $\{a_1, a_2\}$ is a trace-orthogonal basis of $F_p^*$ over $F_p$ and $c_1, c_2 ∈ F_p^*$. Then, we have

$$tr_m(by^{p+1}) = 2b(c_1a_1 + c_2a_2)^{p+1}
= 2b(c_1^2a_1^{p+1} + c_1c_2(a_1a_2 + a_1a_2^{p+1}) + c_2^2a_2^{p+1})
= 2b(c_1^2a_1^{p+1} + c_1c_2(tr_m(a_1a_2) + c_2^2a_2^{p+1}).$$

(6)

It is easy to check that the sequence $tr_f(2by^{p+1})$ is always the same sequence of period $p^m - 1$ with respect to cyclic shift. Therefore, we assume that $b = 1$ and then (6) becomes

$$tr_m(by^{p+1}) = 2(c_1^2a_1^{p+1} + c_1c_2(tr_m(a_1a_2)) + c_2^2a_2^{p+1}).$$

(7)

For $tr_m(b'z^2) = tr_m(tr_m(b'z^2))$ in (5), we can assume that $b' ∈ QR$. Then without loss of generality, we can let $b' = 1$ because we can choose another element $z' ∈ F_p^*$ such that $z^2 = b'z^2$. Now let $z = e_1a_1 + e_2a_2, e_1, e_2 ∈ F_p^*$ and then $tr_m(z^2)$ can be rewritten as

$$tr_m(z^2) = tr_m((e_1a_1 + e_2a_2)^2)
= e_1^2tr_m(a_1^2) + e_1e_2tr_m(a_1a_2) + e_2^2tr_m(a_2^2)
= e_1^2d_1 + e_2^2d_2$$

(8)

where $d_1, d_2 ∈ F_p^*$, and the last equality holds from the property of trace-orthogonal basis.

From (7), we can choose the basis $\{a_1, a_2\}$ such that $tr_m(a_1^{p+1}a_2) = 0$ as follows. From the property of trace-orthogonal basis, we have

$$tr_m(a_1a_2) = a_1a_2 + a_1^{p+1}a_2^{p+1}
= a_1a_2(1 + a_1^{p+1}a_2^{p+1})
= 0$$

and thus we have

$$a_1^{p+1} = -a_2^{p+1}.$$ 

(9)

Suppose that

$$tr_m(a_1^{p+1}a_2) = a_1^{p+1}a_2 + a_1a_2^{p+1}
= a_1a_2(a_1^{p+1} + a_2^{p+1})
= 0.$$ 

Then from (9), we have

$$a_1^{p+1} ≠ 1 \quad \text{or} \quad a_2^{p+1} ≠ 1.$$ 

(10)

From (9) and (10), we have

$$a_1^{p+1} = 1 \quad \text{and} \quad a_2^{p+1} = 1$$

or

$$a_1^{p+1} = -1 \quad \text{and} \quad a_2^{p+1} = -1.$$ 

(11)

Any choice of $(a_1, a_2)$ in (11) satisfies the trace-orthogonal property and the equation $tr_m(a_1^2a_2^2) = 0$. Thus from now on, we simply let

$$a_1 = 1 \quad \text{and} \quad a_2 = a^{p+1}.$$ 

(12)

Then (7) becomes

$$tr_m(by^{p+1}) = 2(c_1^2 + c_2^2a^{p+1})$$

and (8) becomes

$$tr_m(z^2) = 2(c_1^2 + c_2^2a^{p+1}).$$

Then we can choose $c_1, c_2, e_1$, and $e_2$ such that $tr_m(y^{p+1}) = tr_m(z^2)$ holds. One simple choice of $c_1, c_2, e_1$, and $e_2$ is as follows:

$$c_1 = e_1 \quad \text{and} \quad c_2 = a^{p+1}.$$ 

(13)

Next, we find the values $a$ and $a'$ such that the equation $tr_m(ay) = tr_m(a'z)$ holds, where the relationship between $y$ and $z$ is given in (13). Let $a = u_1a_1 + u_2a_2$, and $a' = v_1a_1 + v_2a_2$, where $u_1, u_2, v_1, v_2 ∈ F_p^*$. Then $tr_m(ay)$ can be rewritten as

$$tr_m(ay) = tr_m((u_1a_1 + u_2a_2)(c_1a_1 + c_2a_2))
= tr_m(c_1u_1a_1^2 + (c_1u_2 + c_2u_1)a_1a_2 + c_2u_2a_2^2).$$

By choosing the trace-orthogonal basis as in (12), we have

$$tr_m(ay) = 2(c_1u_1 + c_2u_2a^{p+1})$$

and similarly,

$$tr_m(a'z) = 2(e_1v_1 + e_2v_2a^{p+1}).$$

Suppose that $tr_m(ay) = tr_m(a'z)$, where $c_1, e_1$, and $e_2$ are given in (13). Then we have

$$e_1u_1 + e_2u_2a^{p+1} = e_1v_1 + e_2v_2a^{p+1}.$$ 

(14)

There are many choices of $u_1, u_2, v_1$, and $v_2$ satisfying (14). A straightforward example is given as

$$u_1 = v_1 = 1 \quad \text{and} \quad a^{p+1} = u_2 = v_2.$$ 

(15)

From the discussions above, we have found a condition for the functions $tr_m(ay - by^{p+1})$ and $tr_m(a'z - z^2)$ to be equivalent. Clearly, for fixed $a$ and $a'$ satisfying (15), as $y$ runs through $F_p^*$, $z$ satisfying (13) runs through $F_p^*$. Also note that for $b = a^{p+1}$ and any square $b'$, we can find the
relationship between \((a, y)\) and \((a', z)\) such that (5) holds in the similar way.

**Theorem 3:** For an odd prime \(p\), two integers \(n, m\) with \(n = 2m\), and \(p^m \equiv 1 \pmod 4\), the magnitude of the following ‘mixed’ exponential sum is upper bounded as

\[
\left| \sum_{y \in F_p} \eta(y) \omega_{p^m}(ay - yb^{m+1}) \right| \leq 2p^m.
\]  

**Proof:** Let \(g\) be a function in \(F_{p^m}[x]\) which maps \(z\) to \(y\). It can be proved that such a function \(g\) exists and it has only one root \(0\) as follows. Consider the case \(b = b' = 1\). The basis is given in (12) and the relationship between \(y\) and \(z\) is given in (13). Suppose that \(g(z) = y\). From \(z = e_1 + e_2\alpha^{(p^m+1)/2}\) and the property of the trace function, we have

\[
2^{-1} \text{tr}_{m}^n(z) = c_1
\]

because \(\text{tr}_{m}^n(\alpha^{(p^m+1)/2}) = 0\) and \(e_1, e_2 \in F_{p^m}\). And similarly, we have

\[
2^{-1} \cdot \alpha^{e_2} \text{tr}_{m}^n(z \cdot \alpha^{-e_2}) = e_2.
\]

Therefore, the function \(g\) can be given as

\[
g(z) = 2^{-1}(\text{tr}_{m}^n(z) + \alpha^{e_2} \text{tr}_{m}^n(z \cdot \alpha^{-e_2})).
\]

It is obvious that \(g(z)\) is a 1-to-1 function and has 0 as only one root. For \(b = \alpha^{p^m+1}\) and any \(b' \in QR\), the function \(g : z \rightarrow y\) can also be obtained similarly.

Now from Lemma 1, we have

\[
\left| \sum_{y \in F_p} \eta(y) \omega_{p^m}(ay - yb^{m+1}) \right| \leq 2p^m.
\]

Using Lemma 2 and \(y = g(z)\), we have

\[
\left| \sum_{y \in F_p} \eta(y) \omega_{p^m}(ay - yb^{m+1}) \right| \leq 2p^m
\]

and thus it is proved.

**Theorem 4:** Let \(p\) be an odd prime, \(n, m\) be the positive integers such that \(n = 2m\) with \(p^m \equiv 1 \pmod 4\), \(i = 0, 1\), and \(j = 0, p^m + 1\). Let \(s(t)\) be a \(p\)-ary m-sequence of period \(p^m - 1\). Then the magnitude of the cross-correlation function between its decimated sequences \(s(2t + i)\) and \(s(2(p^m + 1)t + j)\) is upper bounded as

\[
|C_{b}(a)| \leq \frac{3}{2} p^m + \frac{1}{2}.
\]

**Proof:** Combining (4) and (16), the magnitude of the cross-correlation function in (3) can be given as

\[
|C_{b}(a)| \leq \frac{1}{2} \left| \sum_{y \in F_p} \omega_{p^m}(ay - yb^{m+1}) \right| + \frac{1}{2} \left| \sum_{y \in F_p} \eta(y) \omega_{p^m}(ay - yb^{m+1}) \right| \leq \frac{3}{2} p^m + \frac{1}{2}.
\]  

Here are two examples of the above theorem.

**Example 5:** Let \(p = 5, n = 6,\) and \(m = 3\). Then \(2(p^m + 1) = 252\) and by computer experiment, the maximum cross-correlation magnitude is given as 174.045, which is smaller than \(\frac{3}{2} p^m + \frac{1}{2} = 188\). The number of distinct correlation values is given as 80.

**Example 6:** Let \(p = 11, n = 4,\) and \(m = 2\). Then \(2(p^m + 1) = 244\) and by numerical computations, the maximum cross-correlation magnitude is given as 181.83, which is smaller than \(\frac{3}{2} p^m + \frac{1}{2} = 182\). The number of distinct correlation values is given as 130.

Note that for sequences with long period (i.e., large \(n\) or \(p\)), the maximum cross-correlation magnitude becomes close to the upper bound and the number of distinct correlation values increases as \(n\) or \(p\) increases.

From the numerical analysis, we believe that the result in Theorem 4 also holds when \(p^m \equiv 3 \pmod 4\). But that is not easy to prove because it is difficult to find values \(a'\) and \(z\) satisfying (5).

Suppose that \(\text{tr}_{m}^n(ay - yb^{m+1}) = \text{tr}_{m}^n(b'z^2)\) holds. For \(p^m \equiv 3 \pmod 4\) case, it can be shown that no \(b' \in QR\) can satisfy the equation above. Thus we assume that \(b'\) is nonsquare and then without loss of generality, we can let \(b' = \alpha\). Similar to (8), \(\text{tr}_{m}^n(\alpha z^2)\) can be rewritten as

\[
\text{tr}_{m}^n(\alpha z^2) = \text{tr}_{m}^n(\alpha(e_1\alpha_1 + e_2\alpha_2)^2) = c_1^2 \text{tr}_{m}^n(\alpha e_1^2) + e_1 e_2 \text{tr}_{m}^n(e_1\alpha_1\alpha_2) + e_2^2 \text{tr}_{m}^n(e_2^2\alpha_2^2).
\]  

From (7) and (17), finding a condition for \(c_1, c_2, e_1,\) and \(e_2\) to have \(\text{tr}_{m}^n(ay - yb^{m+1}) = \text{tr}_{m}^n(\alpha z^2)\) does not seem to be an easy task. Thus we leave it as a future work and propose a following conjecture.

**Conjecture 7:** Let \(p\) be an odd prime, \(n, m\) be positive integers with \(n = 2m, i = 0, 1,\) and \(j = 0, p^m + 1\). Let \(s(t)\) be a \(p\)-ary m-sequence of period \(p^m - 1\). Then the magnitude of the cross-correlation function between its decimated sequences \(s(2t + i)\) and \(s(2(p^m + 1)t + j)\) is upper bounded as

\[
|C_{b}(a)| \leq \frac{3}{2} p^m + \frac{1}{2}.
\]  

\(\square\)
3.2 The Cross-Correlation between \( s(t) \) and \( s\left(\frac{(p^n+1)^2}{2}\right) \)

In [18], the cross-correlation between two decimated sequences \( s(2t+i) \) and \( s\left(\frac{(p^n+1)^2}{2}t\right) \) is investigated, where \( s(t) \) is a \( p \)-ary m-sequence of period \( p^n - 1 \), \( n = 2m \), and \( p^m \equiv 1 \) (mod 4). In this subsection, we study the cross-correlation function between \( s(t) \) and \( s\left(\frac{(p^n+1)^2}{2}t\right) \), and derive the upper bound of the cross-correlation magnitude.

**Theorem 8:** Let \( p \) be an odd prime and \( n, m \) be the positive integers such that \( n = 2m \) with \( p^m \equiv 1 \) (mod 4). Let \( s(t) \) be a \( p \)-ary m-sequence of period \( p^n - 1 \). Then the magnitude of the cross-correlation function between \( s(t) \) and its decimated sequence \( s_\frac{(p^n+1)^2}{2}t \) is upper bounded as

\[
|C(\tau)| \leq 3p^m + 1.
\]

**Proof:** The cross-correlation function between \( s(t) \) and \( s\left(\frac{(p^n+1)^2}{2}t\right) \) is given as

\[
C(\tau) = \sum_{t=0}^{n^2-2} \omega \left( a^t + a^{p^{n+1}t} \right)
= \sum_{x \in F_{p^n}} \omega \left( \gamma x + x^{p^{n+1}} \right)
= \sum_{x \in F_{p^n}} \omega \left( \gamma x^2 - x^{p^m+1} \right), \tag{18}
\]

where \( \gamma = \alpha' \) and \( \gamma = x^2 \). Let \( x = y^2 \) when \( x \) is a square and \( x = \sigma y^2 \) when \( x \) is a nonsquare, where \( \sigma \) is a fixed nonsquare in \( F_{p^n} \). Then (18) can be rewritten as

\[
C(\tau) = \left[ \sum_{y \in F_{p^n}} \omega \left( y^{p^m+1} - y^{p^m+1} \right) \right] + \sum_{y \in F_{p^n}} \omega \left( \gamma y^2 - \gamma y^{p^m+1} \right), \tag{19}
\]

where \( \gamma' = \gamma^{p^m+1} \). Since \( (p^{n+1})^2 = p^n + 2p^m + 1 \equiv 2(p^n - 1) \), we have

\[
|C(\tau)| \leq \left| \sum_{x \in F_{p^n}} \omega \left( x^{p^m+1} - x^{p^m+1} \right) \right| + \sum_{y \in F_{p^n}} \omega \left( \gamma y^2 - \gamma y^{p^m+1} \right)
\leq \frac{1}{2} \left| \sum_{y \in F_{p^n}} \omega \left( x^{p^m+1} - x^{p^m+1} \right) \right| + \left| \sum_{y \in F_{p^n}} \omega \left( \gamma y^2 - \gamma y^{p^m+1} \right) \right|
\leq 3p^m + 1. \tag{20}
\]

The last inequality comes from (2) and Theorem 4, and the proof is complete. \( \square \)

Some numerical analysis implies that the bound obtained in Theorem 8 may not be tight. For example, for \( p = 11 \) and \( n = 4 \), by computer experiment the maximum cross-correlation magnitude is given as 242.241, which is far smaller than the upper bound \( 3p^m + 1 = 367 \) from Theorem 8. Tighter upper bound may be found by more detailed investigation on the cross-correlation function. We remain this as a further work.

## 4. Conclusion

In this paper, some new results on the cross-correlation between two \( p \)-ary sequences are proposed. First, we derived an upper bound on the magnitude of the cross-correlation function between two decimated sequences of a \( p \)-ary m-sequence. Those sequences are given as \( s(2t+i) \) and \( s(2(p^n+1)+j) \), where \( p \) is an odd prime, \( n, m \) are positive integers with \( n = 2m, p^m \equiv 1 \) (mod 4), and \( s(t) \) is a \( p \)-ary m-sequence of period \( p^n - 1 \). The condition for two functions \( tr_y(a'y - by^{p^m+1}) \) and \( tr_z(a'z - b'z^2) \) to be equivalent is found and then using Weil’s bound, the upper bound \( \frac{3}{2}p^m + \frac{1}{2} \) is obtained.

Additionally, we give an upper bound on the magnitude of the cross-correlation between \( s(t) \) and \( s\left(\frac{(p^n+1)^2}{2}t\right) \). This upper bound is obtained by using the above result and is given as \( 3p^m + 1 \).

From the cross-correlation results given above, new sequence families with good correlation can be considered. Thus as a future work, we will research on the construction of sequence families using the sequences studied in this paper.

## Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (B0717-16-0130, Research on Lightweight Post-Quantum Crypto-systems for IoT and Cloud Computing).

## References


Chang-Min Cho received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2012, where he is currently pursuing the Ph.D. degree in electrical and computer engineering. His area of research interests includes pseudorandom sequences, cryptography, and error-correcting codes.

Wijik Lee received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2012, where he is currently pursuing the Ph.D. degree in electrical and computer engineering. His area of research interests includes pseudorandom sequences, cryptography, and error-correcting codes.

Jong-Seon No received the B.S. and M.S.E.E degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988. He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, Korea, from September 1990 to July 1999. He joined the faculty of the Department of Electrical and Computer Engineering, Seoul National University, in August 1999, where he is currently a Professor. From 1996 to 2008, he served as a Founding Chair of Seoul Chapter, IEEE Information Theory Society. He was a General Chair for Sequence and Their Applications 2004 (SETA2004) in Seoul, Korea. He also served as a General Co-Chair for International Symposium on Information Theory and Its Applications 2006 (ISITA 2006) and International Symposium on Information Theory 2009 (ISIT 2009) in Seoul, Korea. He was a recipient of IEEE Information Theory Society Chapter of the Year Award in 2007. He is elevated to IEEE Fellow in Research Engineer/Scientist through IEEE Information Theory Society, November, 2011. He has become Co-Editor-in-Chief of Journal of Communications and Networks, January, 2012. His area of research interests includes error-correcting codes, sequences, cryptography, LDPC codes, interference alignment and wireless communication systems.

Young-Sik Kim received B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from Seoul National University in 2001, 2003, and 2007, respectively. He joined Semiconductor Division, Samsung Electronics and carried out research and development of secure hardware IPs for various embedded systems, especially for smartcards until the end of August in 2010. He is now an associate professor at Chosun University, Gwangju, Korea. His research interests include post-quantum cryptography, IoT security, physical layer security, data hiding, channel coding, and signal design.