VOL. E98-B NO. 7
JULY 2015

The usage of this PDF file must comply with the IEICE Provisions on Copyright.
The author(s) can distribute this PDF file for research and educational (nonprofit) purposes only.
Distribution by anyone other than the author(s) is prohibited.
New $p$-ary Sequence Families of Period $\frac{p^n-1}{2}$ with Good Correlation Property Using Two Decimated $m$-Sequences

Chang-Min CHO$^{(a)}$, Ji-Youp KIM$^{(b)}$, Nonmembers, and Jong-Seon NO$^{(c)}$, Member

SUMMARY In this paper, for an odd prime $p$ and $i = 0, 1$, we investigate the cross-correlation between two decimated sequences, $s(2i + t)$ and $s(dt)$, where $s(t)$ is a $p$-ary $m$-sequence of period $p^n - 1$. Here we consider two cases of $d, \frac{d}{2} = (\frac{\varphi(p^{n}+1)}{2})^{\frac{k}{2}}$ with $n = 2m$, $p^{m} \equiv 1 \pmod{4}$ and $d = (\frac{\varphi(p^{n}+1)}{2})^{\frac{k}{2}}$ with $n = 2m$ and odd $m/e$. The value distribution of the cross-correlation function for each case is completely determined. Also, by using these decimated sequences, two new $p$-ary sequence families of period $\frac{p^n-1}{2}$ with good correlation property are constructed.

key words: cross-correlation distribution, decimated sequences, $p$-ary sequences, sequence families

1. Introduction

Sequences with good correlation property have various applications in cryptography, radar, and wireless communication system such as code-division multiple-access (CDMA). To construct sequence families with low correlation, the cross-correlation between an $m$-sequence and its decimated sequences has been studied for several decades. For a $p$-ary $m$-sequence of period $p^n - 1$, the decimation values $d$ with $\gcd(d, p^n - 1) = 1$ have been investigated in [1]–[3].

There have also been some researches for decimation factors with $\gcd(d, p^n - 1) > 1$ [4]–[14]. Especially, for an odd prime $p$, a positive integer $k$, $n = 4k$, and a decimation value $d = (\frac{\varphi(p^{n}+1)}{2})^{\frac{k}{2}}$, Seo et al. [9] derived the cross-correlation distribution between a $p$-ary $m$-sequence $s(t)$ of period $p^n - 1$ and its all decimated sequences $s(dt + l)$, $0 \leq l < \frac{p^n - 1}{2}$. This result is later generalized by Luo [10], where $m$ is a positive integer satisfying $p^m \equiv 1 \pmod{4}$, $n = 2m$, and $d = (\frac{\varphi(p^{n}+1)}{2})^{\frac{k}{2}}$. Choi et al. [11] investigated the cross-correlation for the decimation factor $d = (\frac{\varphi(p^{n}+1)}{2})^{\frac{k}{2}}$, where $n = 2m$ and $m$ is an odd integer. Luo et al. [12] and Sun et al. [13] generalized this decimation value by $d = (\frac{\varphi(p^{n}+1)}{2})^{\frac{k}{2}}$, where $e|m$. The results are further generalized by Xia and Chen [14], where $m$ is any positive integer with odd $m/e$. Note that in each case, $\gcd(d, p^n - 1) = \frac{p^n - 1}{2}$.

Recently, there have been some studies for construction of $p$-ary sequence families using two decimated sequences.

Kim, Choi, No, and Chung [15] constructed a new $p$-ary sequence family by shift and addition of two decimated sequences with the decimation factors $2$ and $2(\frac{p^n-1}{2} - p^{m-1})$, where $p \equiv 3 \pmod{4}$ is an odd prime and $n$ is an odd integer. Kim, Chae, and Song [16] generalized the result of [15] using the decimation factors $e$ and $e(\frac{p^n-1}{2} - p^{m-1})$, where $e|p^n - 1$ and $e < \sqrt{p^{m-1}/2}$. Using two decimation factors $2$ and $p^{m} + 1$, Xia and Chen [17] also constructed a new sequence family, where $p$ is an odd prime and $m$ is a positive integer. Lee, Kim, and No [18] constructed new sequence families, where $p \equiv 3 \pmod{4}$, $n$ is odd, one decimation factor is $2$, and the other decimation factor can be either $4$ or $p^{m} + 1$.

In this paper, we study the cross-correlation between two decimated sequences $s(2i + t)$ and $s(dt)$, where $s(t)$ is a $p$-ary $m$-sequence of period $p^n - 1$ and $i = 0, 1$. Here two decimation values $d$ are considered, that is, the first one is $d = (\frac{\varphi(p^{n}+1)}{2})^{\frac{k}{2}}$ with $n = 2m$ and $p^{m} \equiv 1 \pmod{4}$, where $\frac{k}{2} = (\frac{\varphi(p^{n}+1)}{2})^{\frac{k}{2}}$ is studied in [9], [10], and the second one is $d = (\frac{\varphi(p^{n}+1)}{2})^{\frac{k}{2}}$ with $n = 2m$ and odd $m/e$, where $\frac{k}{2} = (\frac{\varphi(p^{n}+1)}{2})^{\frac{k}{2}}$ is investigated in [11]–[14]. For each case, the possible cross-correlation values and the cross-correlation distribution are derived. Also, using these decimated sequences, new $p$-ary sequence families of period $\frac{p^n-1}{2}$ with good correlation property are constructed.

The construction method of the proposed $p$-ary sequence families is similar to that of the $p$-ary Kasami sequence family in [24], that is, $s(t)$ and $s(dt)$ are sequences in the field $F_{p^n}$ and its subfield $F_{p^{m}}$, respectively with $n = 2m$ because $\gcd(p^n - 1, d) = p^{m} + 1$. The period of the proposed sequences is $N_1 = \frac{p^n-1}{2}$ while the period of the Kasami sequences is $N_2 = p^n - 1$. Compared the proposed two sequence families with the Kasami sequence family, the family size of the proposed sequence families is approximately $3 \sqrt{N_1}$ while that of the Kasami sequence family is approximately $\sqrt{N_2}$. The maximum magnitudes of correlation values of the proposed sequence families are approximately $2 \sqrt{N_1}$ and $0.7p^{m} \sqrt{N_2}$ while that of the Kasami sequence family is approximately $\sqrt{N_2}$.

2. Preliminaries

Let $p$ be an odd prime, $n$ be a positive integer, and $F_{p^n}$ be the finite field with $p^n$ elements. Then the trace function $tr_{p^n}^{p^m} (\cdot)$ from $F_{p^n}$ to $F_{p^m}$ is defined as

\[ tr_{p^n}^{p^m} (x) = x + x^{p} + \cdots + x^{p^{m-1}}. \]
\[ \text{tr}_n^m(x) = \sum_{i=0}^{\frac{\delta - 1}{m}} x^{i\omega^m} \]

where \( x \in F_{p^n} \) and \( mn \).

Let \( a \) be a primitive element of \( F_{p^n} \). Then, a \( p \)-ary sequence \( s(t) \) of period \( p^n - 1 \) can be expressed as

\[ s(t) = \text{tr}_n^m(a^t) \]

and its \( d \)-decimated sequence \( s(dt) \) is given as

\[ s(dt) = \text{tr}_n^m(a^{dt}) \]

The cross-correlation function between 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 \( \omega = e^{2\pi i/N} \) is a primitive \( p \)-th root of unity. When \( a(t) = s(2t + i) \) and \( b(t) = s(dt) \) with \( i \in \{0, 1\} \) and \( \gcd(p^n - 1, d) \) is a multiple of 2, the cross-correlation function between these two decimated sequences is given as

\[ C_i(\tau) = \sum_{t=0}^{N-1} \omega^{\text{tr}_n^m(a^{2t+ir}+a^\tau)-\text{tr}_n^m(a^\tau)} \]

where \( N = \frac{p^n - 1}{2} \). Since \( \gcd(p^n - 1, d) \) is a multiple of 2, we have

\[ \sum_{t=0}^{N-1} \omega^{\text{tr}_n^m(a^{2t+ir}+a^\tau)-\text{tr}_n^m(a^\tau)} = \sum_{t=0}^{N/2} \omega^{\text{tr}_n^m(a^{2t+ir}+a^\tau)-\text{tr}_n^m(a^\tau)} \]

and thus \( C_i(\tau) \) can be rewritten as

\[ C_i(\tau) = \frac{1}{2} \sum_{t=0}^{N/2} \omega^{\text{tr}_n^m(a^{2t+ir}+a^\tau)-\text{tr}_n^m(a^\tau)} - \frac{1}{2} \]

where \( x = a^r \) and \( a = \omega^{2^r i} \). Note that \( a \) is a square if \( i = 0 \) and a nonsquare if \( i = 1 \). Then, we express the cross-correlation between \( s(2t + i) \) and \( s(dt) \) as

\[ C(a) = \frac{1}{2} \sum_{x \in F_{p^n}} \omega^{\text{tr}_n^m(x^2-x^\tau)} - \frac{1}{2}. \quad (1) \]

The following two lemmas for exponential sums are introduced in [2], which will be used in this paper.

**Lemma 1:** ([2]) Let \( p \) be an odd prime and \( n \) an even integer. Then, for \( a \in F_{p^n} \), we have

\[ \sum_{x \in F_{p^n}} \omega^{\text{tr}_n^m(ax^{2^{i+1}})} = \begin{cases} \left( \frac{p^n}{2} \right), & \text{if } a + a^{\pm 2} = 0 \\ -p^n, & \text{if } a + a^{\pm 2} \neq 0. \end{cases} \]

**Lemma 2:** ([2]) For an odd prime \( p \), an integer \( n \), and \( a \in F_{p^n} \), we have

\[ \sum_{x \in F_{p^n}} \omega^{\text{tr}_n^m(ax^2)} = \begin{cases} p^n, & \text{if } a = 0 \\ (1-p^n)(1-\omega p^n)^2, & \text{if } a \text{ is a square} \\ (1-p^n)(1-\omega^{-1} p^n)^2, & \text{if } a \text{ is a nonsquare}. \end{cases} \]

**3. Cross-Correlation for the Case of \( d = \frac{(p^n+1)^2}{2} \)**

In this section, we assume that \( n = 2m \), where \( m \) is a positive integer with \( p^m \equiv 1 \pmod{4} \). Also, the following notations will be used throughout this section:

- \( d = \frac{(p^n+1)^2}{2} \)
- \( N = p^{m-1} \)
- \( d' = \frac{d}{2} = \left( \frac{p^m+1}{2} \right)^2 \)
- \( \delta \) is a primitive element of \( F_{p^n} \)
- \( \beta = \delta^{p^m+1} \)
- \( \gamma = \delta^{2(p^m-1)} \)
- \( \alpha = \beta \gamma \)

Then, the following properties hold:

1. \( \gcd(p^n - 1, d) = p^{m+1} + 1 \)
2. \( \gcd((p^m + 1)/2, 2(p^m - 1)) = 1 \)
3. \( \alpha = \beta \gamma \) is a primitive element of \( F_{p^n} \)
4. \( \beta \gamma^p = -\beta \)
5. \( \beta \gamma^p = \beta \), if \( p^m = 5 \pmod{8} \)
6. \( \beta \gamma^p = -\beta \), otherwise
7. \( \gamma^p = \gamma^{-1} \) and \( \gamma^p = 1 \)
8. For any positive integer \( t \), \( \gamma^t \neq 1 \)

These notations and properties are from [9] with some minor changes.

In this section, we derive the cross-correlation distribution between \( s(2t + i) \) and \( s(dt) \), where \( s(t) \) is a \( p \)-ary sequence of period \( p^n - 1 \) and \( i = 0, 1 \). First, we determine the possible cross-correlation values of \( s(2t + i) \) and \( s(dt) \).

**Theorem 3:** Let \( n, m \) be the positive integers such that \( n = 2m \) with \( p^m \equiv 1 \pmod{4} \). Let \( s(t) \) be a \( p \)-ary sequence of period \( p^n - 1 \) and \( d = \frac{(p^n+1)^2}{2} \). Then, the cross-correlation function between its decimated sequences \( s(2t + i) \) with \( i \in \{0, 1\} \) and \( s(dt) \) can take the values in the following sets

\[ \begin{cases} \left( \frac{-1+p^m}{2}, \frac{1+p^m}{2}, \frac{-1+3p^m}{2} \right), & \text{for } i = 0 \\ \left( \frac{-1+p^m}{2}, -1+p^m, \frac{-1+3p^m}{2} \right), & \text{for } i = 1. \end{cases} \]

**Proof:** Using the similar method as in the proof of Theorem 2 in [9], this theorem can be proved. Let \( x = \alpha^y \gamma^{\frac{a^{x+1}}{2}} \), where \( y \in F_{p^n} \) and \( 0 \leq j < \frac{p^n+1}{2} \). Then, as \( y \) runs through \( F_{p^n} \) and \( j \)
takes the values in \(0, 1, \ldots, p^{m-1}\), \(x\) runs through \(F_{p^m}\) \(p^{m+1}\) times and \(y^{p^{m+1}} = y^{p^{m+1}}\). Therefore, (1) can be rewritten as

\[
C(a) + \frac{1}{2} = \frac{1}{m+1} \sum_{a \in \mathbb{F}_{p^m}} \omega_{p^m}(ax^2 - x)
\]

\[
= \frac{1}{p^m + 1} \sum_{y \in \mathbb{F}_{2p^m}} \sum_{j \in \mathbb{F}_{2p^m}} \omega_{p^m}(y^{p^{m+1}} - x^{p^m} y^{p^{m+1}})
\]

\[
= \frac{1}{p^m + 1} \sum_{j \in \mathbb{F}_{2p^m}} \sum_{y \in \mathbb{F}_{2p^m}} \omega_{p^m}(y^{p^{m+1}}(a x^2 - x^2)), \tag{2}
\]

Let \(K(a)\) denote the number of solutions of \(j\) of

\[
(aa^{2j} - a^{2j})^p + (aa^{2j} - a^{2j}) = 0
\]

where \(0 \leq j < p^{m+1}\). Then, by using Lemma 1, (2) becomes

\[
C(a) = \frac{1}{m+1} \left( p^{2m} K(a) + (-1)^{m} \left( \frac{p^m + 1}{2} - K(a) \right) \right)
\]

\[
= p^m (K(a) - \frac{1}{2}). \tag{4}
\]

Therefore, we can determine the possible values of the cross-correlation function by obtaining the possible values of \(K(a)\).

Let \(2 \leq k \leq m\). Then \(d = d'k\) and by using \(a = \beta y\), (3) can be rewritten as

\[
a^{2k} (\beta y)^{p^m k} - (\beta y)^{d' k} + a (\beta y)^k - (\beta y)^{d} k = 0 \tag{5}
\]

where \(0 \leq k < p^m + 1\) and \(k\) is even. Then, by using the properties of \(\beta\) and \(y\), (5) can be rewritten as

\[
a^{2k} \beta^k y^k - \beta^k + \alpha^2 y^k = 0
\]

and by multiplying \(\beta^k y^k\), we have

\[
\alpha y^k - 2 \beta^k + \alpha^2 y^k = 0. \tag{6}
\]

This is a quadratic equation of \(y^k\) and the possible number of solutions is 0, 1, or 2. Suppose that (6) has two distinct solutions \(y^{-1}\) and \(y^2\), where \(s_1\) and \(s_2\) are both even. Also, \(a\) can be represented as \(a = \delta x^{2^{i+1}}\) and by using the quadratic formula, we have

\[
y^{s_1 + s_2} = \delta^{2^{(p^m-1)(s_1+s_2)}} = \delta^{2^{(2^{i+1})(p^m-1)}}.
\]

Therefore, we have

\[
2(s_1 + s_2) = 2 \tau + i \mod p^m + 1.
\]

Note that the left-hand side is always even. When \(i = 1\), the right-hand side is odd and (6) cannot have two distinct solutions. Therefore, the possible values of \(K(a)\) are 0, 1, 2 for \(i = 0\) and 0, 1 for \(i = 1\). Thus the theorem is proved.

In order to derive the cross-correlation distribution, we need two linear equations for \(i = 1\) and three linear equations for \(i = 0\). Let \(N_i\) be the number of occurrences of each possible cross-correlation value as \(\tau\) runs over \(0 \leq \tau \leq N - 1\). For the case of \(i = 1\), by calculating \(\Sigma_{\tau=0}^{N-1} C(a)\) with \(N_1 + N_2 \leq \frac{p^{m-1}}{2}\), the value distribution of \(C(a)\) can be determined, where \(a = \alpha^{2^{i+1}}\). Similarly, when \(i = 0\), by using \(\Sigma_{\tau=0}^{N-1} C(a)\) and \(\Sigma_{\tau=0}^{N-1} C^2(a)\) with \(N_1 + N_2 + N_3 = \frac{p^{m-1}}{2}\), the cross-correlation distribution can also be evaluated.

Now, we compute \(\Sigma_{\tau=0}^{N-1} C(a)\) and \(\Sigma_{\tau=0}^{N-1} C^2(a)\) as in the following lemmas.

**Lemma 4:** For \(C(a)\) in (1), we have

\[
\sum_{\tau=0}^{N-1} C(a) = \begin{cases} \frac{1}{2} (p^m + 2p^m + 1), & \text{for } i = 0 \\ \frac{1}{2} (-p^m + 1), & \text{for } i = 1. \end{cases}
\]

**Proof:**

\[
\sum_{\tau=0}^{N-1} C(a) = \frac{1}{2} \sum_{\tau=0}^{N-1} \sum_{y \in \mathbb{F}_{2p^m}} \omega_{p^m}(x^{2^{i+1}}, y)
\]

\[
= \frac{1}{2} \sum_{x \in \mathbb{F}_{2p^m}} \sum_{a \in \mathbb{F}_{2p^m}} \omega_{p^m}(x^{2^{i+1}}, a) = \sum_{x \in \mathbb{F}_{2p^m}} \omega_{p^m}(x^{2^{i+1}}, a)
\]

where \(a = \alpha^{2^{i+1}}\). Let \(y = \beta^2\). Then by Lemma 2, we have

\[
\sum_{x \in \mathbb{F}_{2p^m}} \omega_{p^m}(x^{2^{i+1}}, y) = \begin{cases} \frac{1}{2} (-p^m + 1), & \text{for } i = 0 \\ \frac{1}{2} (p^m - 1), & \text{for } i = 1. \end{cases} \tag{7}
\]

Next, since \(gcd(p^m - 1, d) = p^m + 1\), \(x^d\) runs through \(F_{p^m}^* \) \(p^m + 1\) times as \(x\) runs through \(F_{p^m}^*\). Then by Lemma 1, we have

\[
\sum_{x \in \mathbb{F}_{2p^m}} \omega_{p^m}(x^d) = \sum_{x \in \mathbb{F}_{2p^m}} \omega_{p^m}(-x^{d+1}) = -p^m - 1. \tag{8}
\]

Combining (7) and (8), the lemma can be proved.

The following lemma will be used to compute \(\Sigma_{\tau=0}^{N-1} C^2(a)\).

**Lemma 5:**

(i) For \(z \in F_{p^m}^*\), the number of solutions of \(1 + z^d = 0\) is \(p^m + 1\).

(ii) For \(z \in F_{p^m}^*\), satisfying \(1 + z^d = 0\), we have

\[
1 + z^2 \in \{0\}, \quad 2\text{ times}
\]

\[
\{QNR\}, \quad p^m - 1\text{ times}
\]

where \(QNR\) is the set of nonsquares in \(F_{p^m}^*\).

(iii) If \(1 + z^d \not\equiv 0\), \(1 + z^d + (1 + z^d)d \not\equiv 0\).

**Proof:** (i) Since \(gcd(p^m - 1, d) = p^m + 1\), the mapping \(z \mapsto z^d\) is a \(p^m + 1\) to 1 mapping from \(F_{p^m}^*\) onto \(F_{p^m}^*\). Thus the number of solutions of \(1 + z^d = 0\) is \(p^m + 1\).
(ii) From (i), the number of \( z \) satisfying \( 1 + z^d = 0 \) is \( p^m + 1 \). There are two values of \( z \) satisfying \( 1 + z^2 = 0 \) and for those \( z, z^d = 2^{2d} = (-1)^d = -1 \) holds since \( d^2 \) is odd. Next, from Case 1-2 of Theorem 8 in [9], it was shown that for a square \( x \) satisfying \( 1 + x^d = 0 \), \( 1 + x \) cannot be a square. Thus we have that for \( z \) satisfying \( 1 + z^d = 1 + (z^d)^d = 0, 1 + z^2 \) can be either 0 or a nonsquare. Since there are two \( z^2 \)'s satisfying \( 1 + z^2 = 0, 1 + z^2 \in \text{QNR} \) holds for other \( p^m - 1 \) values of \( z \).

(iii) For \( 1 + z^d \neq 0 \), we have

\[
1 + z^d + (1 + z^d)^{p^m} = (1 + z^d)^{(1 + (1 + z^d)^{p^m}-1)}.
\]

Since \( z^d \in F_{p^m} \) and \( 1 + z^d \neq 0, 1 + z^d \in F_{p^m} \) and therefore \( (1 + z^d)^{p^m-1} = 1 \). Then the proof is done. \( \square \)

Lemma 6: For \( C(a) \) with \( i = 0 \) in (1), we have

\[
\sum_{\tau=0}^{N-1} C^2(\tau) = \frac{2p^2n - 6p^m - 4p^m - 1}{8}
\]

Proof:

\[
\sum_{\tau=0}^{N-1} C^2(\tau) = \frac{1}{4} \sum_{\tau=0}^{N-1} \sum_{x \in F_{p^m}} \sum_{x' \in F_{p^m}} \omega^{\tau(x^2 - x')} \omega^{\tau(x'^2 - x')} = \frac{1}{4} \sum_{x \in F_{p^m}} \sum_{x' \in F_{p^m}} \sum_{y \in F_{p^m}} \sum_{x'^{2} - x'^{2}} \omega^{\tau(y^2(x^2 - x'))}
\]

(9)

where \( a = \alpha^2 = y^2 \). Let \( z = z_{a} \) and then (10) becomes

\[
\sum_{\tau=0}^{N-1} C^2(\tau) = \frac{1}{8} \sum_{x \in F_{p^m}} \sum_{x' \in F_{p^m}} \sum_{y \in F_{p^m}} \omega^{\tau(y^2(x^2 - x'))}
\]

(10)

Let

\[
X(x_1, y, z) = \omega^{-\tau y^2(x_1^2 + z^2)} \sum_{y \in F_{p^m}} \omega^{\tau y^2(x_1^2 + z^2)}(x_1^2 + z^2)
\]

and \( QR \) denote the set of squares in \( F_{p^m} \). Then (10) can be rewritten as

\[
\sum_{\tau=0}^{N-1} C^2(\tau) = \frac{1}{8} \sum_{x \in F_{p^m}} \sum_{x' \in F_{p^m}} \sum_{z \in \text{QNR}} X(x_1, y, z) + \sum_{z \in \text{QNR}} X(x_1, y, z)
\]

For \( z \in F_{p^m} \), from Theorem 67 of [32], we have

\[1 + z^2 \in \{0, 1, 2 \times \text{QR}, \frac{p^m-1}{2} \text{ times}, \frac{p^m-1}{2} \text{ times}.\]

Then, by using Lemmas 1, 2, and 5, we have

\[
\sum_{x \in F_{p^m}} \sum_{x' \in F_{p^m}} \sum_{z \in \text{QNR}} X(x_1, y, z) = \sum_{x \in F_{p^m}} 2 \cdot \omega^{-\tau y^2(x_1^2 + z^2)}(p^m - 1) = 2(p^m - 1)^2
\]

(11)

Using \( p^m \equiv 1 \mod 4 \) and (8), we have

\[
X(x_1, y, z) = \sum_{z \in \text{QNR}} \omega^{-\tau y^2(x_1^2 + z^2)}(-p^m - 1) = \frac{p^m - 5}{2}(p^m + 1)^2
\]

(12)

Also, by separating \( 1 + z^d = 0 \) and \( 1 + z^d \neq 0 \) for \( 1 + z^2 \in \text{QNR} \), we have

\[
\sum_{x \in F_{p^m}} \sum_{x' \in F_{p^m}} \sum_{z \in \text{QNR}} X(x_1, y, z) = \sum_{z \in \text{QNR}} \sum_{x \in F_{p^m}} \omega^{-\tau y^2(x_1^2 + z^2)}(p^m - 1) = (p^m - 1)
\]

(13)

Combining (11), (12), and (13), \( \sum_{\tau=0}^{N-1} C^2(\tau) \) can be computed and the proof is completed. \( \square \)

Now, the cross-correlation distribution between \( s(2t + i) \) and \( s(d^t) \) can be derived as in the following theorem.

Theorem 7: Let \( n, m \) be the positive integers such that \( n = 2m \) with \( p^m \equiv 1 \mod 4 \). Let \( s(i) \) be a \( p \)-ary m-sequence of period \( p^n - 1 \) and \( d = \frac{(p^n-1)^2}{2} \). Then the distribution of the cross-correlation function between \( s(2t + i), \ i \in \{0, 1\} \) and \( s(i) \) is given as:

(i) For \( i = 0 \):

\[
C(a) = \begin{cases} \frac{-1}{p^n}, & \frac{1}{8}(3p^n - 4p^n - 7) \text{ times} \\ \frac{1}{2}p^n, & \frac{1}{2}(p^n - 1) \text{ times} \end{cases}
\]

(ii) For \( i = 1 \):

\[
C(a) = \begin{cases} \frac{-1}{p^n}, & \frac{1}{2}(p^n - 1) \text{ times} \\ \frac{1}{2}p^n, & \frac{1}{8}(p^n - 1) \text{ times} \end{cases}
\]

Proof: First, we prove the case of \( i = 0 \). Let

\[
C(a) = \begin{cases} \frac{-1}{p^n}, & N_1 \text{ times} \\ \frac{1}{2}p^n, & N_2 \text{ times} \\ \frac{-1}{2}p^n, & N_3 \text{ times} \end{cases}
\]

as \( \tau \) runs over \( 0 \leq \tau \leq \frac{p^n-1}{2} \) and \( a = \alpha^{2\tau} \). Then, we can derive the values \( N_1, N_2, \) and \( N_3 \) by solving the following system of equations obtained from Theorem 3, Lemma 4, and Lemma 6;
\[ N_1 + N_2 + N_3 = \frac{1}{2} (p^n - 1) \]
\[ -1 - p^n N_1 + \frac{1}{2} + p^n N_2 + \frac{1}{2} + 3p^n N_3 \]
\[ = \frac{1}{4} (p^n + 2p^n + 1) \]
\[ \left( \frac{1}{2} - p^n \right)^2 N_1 + \left( \frac{1}{2} + p^n \right)^2 N_2 + 3p^n N_3 \]
\[ = \frac{3}{8} p^n - 6p^n - 4p^n - 1. \]

For \( i = 1 \), the cross-correlation distribution can be similarly derived. \( \Box \)

4. Cross-Correlation for the Case of \( d = \frac{(p^n+1)^2}{p+1} \)

In this section, we assume that \( n = 2m, \ e|m \) with odd \( m/e \), and \( d = \frac{(p^n+1)^2}{p+1} \). We first consider the cross-correlation between \( s(t) \) and \( s(d't) \) for \( d' = d/2 \) as

\[ R_d(\gamma) = \sum_{t=0}^{p^n-2} \omega_{p^n}(\gamma \cdot t - \sigma^t) \]
\[ = \sum_{x \in F_{p^n}} \omega_{p^n}(y_1 - \sigma^t) \]
\[ = \frac{1}{2} E(-1, \gamma) + E(-\sigma^t, \sigma \gamma) - 1 \tag{14} \]

where \( x = \alpha^t \) and \( \gamma = \sigma^2 \). In [14], the distribution of \( R_d(\gamma) \) is studied by using the quadratic form \( Q_{a,b}(x) = \text{tr}_q(ax^{p^n+1} + bx^{3p^n+1}) \). Let \( \sigma \) be a fixed nonsquare in \( F_{p^n} \). Then (14) can be rewritten as

\[ R_d(\gamma) = \sum_{x \in F_{p^n}} \omega_{p^n}(y_1 - \sigma^t) \]
\[ = \frac{1}{2} [E(-1, \gamma) + E(-\sigma^t, \sigma \gamma)] - 1 \tag{15} \]

where \( E(a, b) = \sum_{x \in F_{p^n}} \omega_{p^n}(x^{p^n+1}) \).

Comparing the cross-correlation function between \( s(2t+i) \) and \( s(dt) \) to (15), we have

\[ C(a) = \frac{1}{2} \sum_{x \in F_{p^n}} \omega_{p^n}(ax^{i+1} - \sigma^t) \]
\[ = \frac{1}{2} E(-1, a) - 1 \]

where \( a = \alpha^{2i+1} \). Hence, the distribution of \( C(a) \) can be derived by determining the distribution of \( E(-1, a) \) for the cases of \( i = 0 \) and \( i = 1 \), respectively. For \( \gamma \in F_{p^n} \), the distribution of \( E(-1, \gamma) \) is given in [14] as follows.

**Lemma 8:** (14) Let \( Q_{a,b}(x) = \text{tr}_q(ax^{p^n+1} + bx^{3p^n+1}) \) and \( E(a, b) = \sum_{x \in F_{p^n}} \omega_{p^n}(ax^{p^n+1}) \). Then, the value distribution of \( E(-1, \gamma) \) for \( \gamma \in F_{p^n} \) is given as

\[
\begin{align*}
   p^n, & \quad \frac{(p^n+1)(p^n+2)}{2(p^n+1)} \text{ times} \\
   -p^n, & \quad \frac{1}{4} (p^n+1) \text{ times} \\
   \frac{1}{2} \mu(\gamma(-1)p^{n+1}), & \quad \frac{1}{2} \mu(\gamma(-1)p^{n+1}) \text{ times} \\
   \frac{1}{2} \mu(-\gamma(-1)p^{n+1}), & \quad \frac{1}{2} \mu(-\gamma(-1)p^{n+1}) \text{ times} \\
   -p^{n+1}, & \quad \frac{1}{4} (p^n+1) \text{ times} \\
   \sqrt{\eta_{1}(-1)p^{n+1}}, & \quad \frac{1}{2} \mu(-\gamma(-1)p^{n+1}) \text{ times} \\
   \sqrt{\eta_{1}(-1)p^{n+1}}, & \quad \frac{1}{2} \mu(p^{n+1}) \text{ times} \\
   -p^{n+1}, & \quad \frac{1}{4} (p^n+1) \text{ times}
\end{align*}
\]

where \( \eta_{1}(\cdot) \) is the quadratic character of \( F_{p^n} \).

Also, it can be shown by applying Lemma 8 in [14] that when \( \gamma \) is a nonsquare, \( E(-1, \gamma) \) can only have two values, \( \pm p^n \). When \( i = 1, a \) is a nonsquare and in that case, \( C(a) \) has two possible values \( -1/2p^n \) and \( -1/2p^n \). In order to find the value distribution of \( C(a) \) for \( i = 1 \), we need to calculate \( \sum_{\gamma} C(a) \) for \( i = 1 \). This can be obtained similarly to Lemma 4 and thus we omit its proof.

**Lemma 9:** For \( C(a) \) with \( i = 1 \), (mod 4), we have

\[
\begin{align*}
   \sum_{\gamma} C(a) & = \left\{ \begin{array}{ll}
   \frac{1}{4} (p^n+1), & \text{for } p^n \equiv 1 \pmod{4} \\
   \frac{1}{4} (p^n+2p^n+1), & \text{for } p^n \equiv 3 \pmod{4}.
   \end{array} \right. \tag{4}
\end{align*}
\]

Now we can derive the cross-correlation distribution as in the following theorem.

**Theorem 10:** Let \( n, m, e \) be the positive integers such that \( n = 2m, e|m \) with odd \( m/e \). Let \( s(t) \) be a \( p \)-ary m-sequence of period \( p^n-1 \) and \( d = \frac{(p^n+1)^2}{p+1} \). Then the cross-correlation distribution between \( s(2t+i), i \in \{0, 1\} \) and \( s(dt) \) is given as:

(i) For \( i = 0 \);

(ii) \( p^n \equiv 1 \pmod{4} 

\[
\begin{align*}
   C(a) & = \left\{ \begin{array}{ll}
   -p^n, & \quad \frac{1}{2} (p^n-1) \text{ times} \\
   \frac{1}{2} (p^n+1) \text{ times} \\
   -p^n, & \quad \frac{1}{2} (p^n+2p^n+1) \text{ times} \\
   \frac{1}{2} (p^n-2p^n-3) \text{ times} \\
   \frac{1}{2} (p^n-1) \text{ times} \\
   \frac{1}{2} (p^n+1) \text{ times} \\
   \frac{1}{2} (p^n+2p^n+1) \text{ times} \\
   \frac{1}{2} (p^n-2p^n-3) \text{ times} \\
   \frac{1}{2} (p^n-1) \text{ times} \\
   \frac{1}{2} (p^n+1) \text{ times} \\
   \frac{1}{2} (p^n+2p^n+1) \text{ times} \\
   \frac{1}{2} (p^n-2p^n-3) \text{ times} \\
   \frac{1}{2} (p^n-1) \text{ times} \\
   \frac{1}{2} (p^n+1) \text{ times} \\
   \frac{1}{2} (p^n+2p^n+1) \text{ times} \\
   \frac{1}{2} (p^n-2p^n-3) \text{ times} \\
   \frac{1}{2} (p^n-1) \text{ times} \\
   \frac{1}{2} (p^n+1) \text{ times} \\
   \frac{1}{2} (p^n+2p^n+1) \text{ times} \\
   \end{array} \right. \tag{4} \end{align*}
\]

(ii) \( p^n \equiv 1 \pmod{4} 

\[
\begin{align*}
   C(a) & = \left\{ \begin{array}{ll}
   -p^n, & \quad \frac{1}{2} (p^n-1) \text{ times} \\
   \frac{1}{2} (p^n+1) \text{ times} \\
   -p^n, & \quad \frac{1}{2} (p^n+2p^n+1) \text{ times} \\
   \frac{1}{2} (p^n-2p^n-3) \text{ times} \\
   \frac{1}{2} (p^n-1) \text{ times} \\
   \frac{1}{2} (p^n+1) \text{ times} \\
   \frac{1}{2} (p^n+2p^n+1) \text{ times} \\
   \frac{1}{2} (p^n-2p^n-3) \text{ times} \\
   \frac{1}{2} (p^n-1) \text{ times} \\
   \frac{1}{2} (p^n+1) \text{ times} \\
   \frac{1}{2} (p^n+2p^n+1) \text{ times} \\
   \frac{1}{2} (p^n-2p^n-3) \text{ times} \\
   \frac{1}{2} (p^n-1) \text{ times} \\
   \frac{1}{2} (p^n+1) \text{ times} \\
   \frac{1}{2} (p^n+2p^n+1) \text{ times} \\
   \end{array} \right. \tag{4} \end{align*}
\]
(ii)-2. \( p^n \equiv 3 \) (mod 4)

\[
C(a) = \begin{cases} 
\frac{-1+p^n}{2}, & \frac{1}{3}(p^n + 2p^n + 1) \text{ times} \\
\frac{-1+p^n}{2}, & \frac{1}{3}(p^n - 2p^n - 3) \text{ times}.
\end{cases}
\]

**Proof:** For \( i = 1 \), the value distribution can be derived by using Lemma 9 and the same method in Theorem 7. For \( i = 0 \), we can derive the value distribution by excluding the values of \( C(a) \) for \( i = 1 \) from the distribution of \( E(-1, \gamma) \) for \( \gamma \in F_{p^n} \), as in Lemma 8. \( \square \)

5. **Construction of New Sequence Families**

By using the decimated sequences studied in the previous sections, two new \( p \)-ary sequence families can be constructed.

**Definition 11:** Let \( n, m \) be positive integers such that \( n = 2m \). For two decimation factors \( d_1 = \frac{p^n+1}{2} \) with \( p^n \equiv 1 \) (mod 4) and \( d_2 = \frac{p^n+1}{2} \) with odd \( m/e \), new families of \( p \)-ary sequences of period \( N = \frac{p^n-1}{2} \) are defined as

\[
S_k = \{ s_{i,y,k}(t) | i \in [0,1], \gamma \in F_{p^n} \}, \quad k \in [0,1]
\]

where

\[
s_{i,y,k}(t) = \tau_1^i(\alpha^{2\gamma t}) + \tau_1^i(\gamma \alpha^{d_1 t}).
\]

The properties of the proposed sequence family \( S_k \) are given in the following theorem.

**Theorem 12:** Let \( S_k \) be the \( p \)-ary sequence family defined in Definition 11. Then the family size of \( S_k \) is \( 2p^n \) and the values of nontrivial correlation are the same as the values of the cross-correlation function between \( s(2t+i), i \in [0,1] \) and \( s_d(t) \) in Theorems 7 and 10.

**Proof:** We will prove the case of \( k = 1 \). Let \( s_1(t) = s_{i,y,1}(t) \in S_1 \) and \( s_2(t) = s_{j,y,1}(t) \in S_1 \). Then the cross-correlation function between \( s_1(t) \) and \( s_2(t) \) is given as

\[
C_{s_1,s_2}(\tau) = \sum_{t=0}^{N-1} \omega^{\tau t(ux^{2i+i})+\tau t(\gamma y x^{i+i})-\tau t(ux^{j+i})-\tau t(\gamma y x^{j+i})}
\]

\[
= \frac{1}{2} \sum_{x \in F_{p^n}} \omega^{\tau t(x^2(u^2+1)+\gamma y(u^{d_1}+1))}
\]

\[
= \frac{1}{2} \sum_{x \in F_{p^n}} \omega^{\tau t(px^2-\gamma x)}
\]

where \( x = \alpha^i, u = \alpha^{2x^{2i+i}} - \alpha^i, \) and \( v = \gamma y - \gamma y_1 \alpha^{d_1 t} \). It is clear that when \( i \neq j \), \( u \) cannot be zero and when \( i = j, \) \( u = 0 \) if and only if \( \tau \equiv 0 \) (mod \( N \)). And when \( \tau \equiv 0 \) (mod \( N \)), \( u = 0 \) if and only if \( \gamma y_1 = \gamma y_2 \). Thus the correlation function gives the in-phase autocorrelation only when \( \tau \equiv 0 \) (mod \( N \)), \( i = j, \) and \( \gamma y_1 = \gamma y_2 \). It means that \( s_1(t) \) and \( s_2(t) \) are cyclically distinct when \( (i, \gamma y_1) \neq (j, \gamma y_2) \) and therefore, the family size of \( S_1 \) can be obtained as \( 2 \times 2p^n \) from \( i \in [0,1] \) and \( \gamma \in F_{p^n} \).

Next, we show that the nontrivial values of \( C_{s_1,s_2}(\tau) \) are the same as the values of \( C(a) \), which are investigated in Theorem 7. Clearly, \( u \) can be 0, a square, or a nonsquare and since \( \gcd(p^n - 1, d_1) = p^n + 1, \alpha^{d_1 t} \in F_{p^n} \) and \( v \in F_{p^n} \). Also, \( x^2 \in F_{p^n} \) and thus when \( u \neq 0 \), two sequences \( \tau_1^i(x^d) \) and \( \tau_1^i(x^d) \) are cyclically equivalent. Therefore, when \( u \neq 0 \) and \( v \neq 0 \), the nontrivial correlation \( C_{s_1,s_2}(\tau) \) has the same values as \( C(a) \) in Theorem 7.

When \( u = 0 \) and \( v \neq 0 \), the correlation function becomes

\[
C_{s_1,s_2}(\tau) = \frac{1}{2} \sum_{x \in F_{p^n}} \omega^{\tau t(px^2-\gamma x^2)}
\]

This is obtained by the same way as in (8). And when \( v = 0 \) and \( u \neq 0 \), the correlation function can be rewritten as

\[
C_{s_1,s_2}(\tau) = \frac{1}{2} \sum_{x \in F_{p^n}} \omega^{\tau t(px^2-\gamma x)}
\]

This can be computed by using Lemma 2 and the possible values are \( \frac{-1+\gamma x^2}{2} \) and \( \frac{-1-x^2}{2} \), which are included in the values of \( C(a) \) in Theorem 7.

Therefore, it is shown that for every nontrivial correlation, the values of \( C_{s_1,s_2}(\tau) \) are the same as the values of \( C(a) \) in Theorem 7. The case \( k = 2 \) can be proved by the same method. Thus the proof is complete. \( \square \)

The parameters of some well known sequence families and the new sequence families \( S_1 \) and \( S_2 \) derived in this paper are listed in Table 1. Compared the proposed two \( p \)-ary sequence families with the \( p \)-ary Kasami sequence family in [24], the family size of the proposed sequence families is approximately \( 3 \sqrt{N} \) while that of the Kasami sequence family is approximately \( \sqrt{N} \), where the period of the proposed sequences is half of that of the Kasami sequences. The maximum magnitudes of correlation values of the proposed sequence families are approximately \( 2 \sqrt{N} \) and \( 0.7p^2 \sqrt{N} \) while that of the Kasami sequence family is approximately \( \sqrt{N} \).

6. **Conclusion**

In this paper, for an odd prime \( p \) and positive integers \( m \) and \( n = 2m \), the cross-correlation functions between two decimated sequences of a \( p \)-ary m-sequence of period \( p^n - 1 \) are investigated. Two decimation factors are 2 and \( d = 2d' \) where \( d' = \frac{p^n+1}{2} \) with \( p^n \equiv 1 \) (mod 4) [9], [10] and \( d' = \frac{p^n+1}{2} \) with odd \( m/e \) [11]–[14]. For both cases, the complete value distributions of the cross-correlation functions are derived.

We can construct new \( p \)-ary sequence families by using two decimated sequences. The period of the sequences is \( N = \frac{p^n-1}{2} \) and the size of the sequence families is \( 2p^n \approx 3 \sqrt{N} \). The values of nontrivial correlation of the proposed sequence families are the same as the values of
the cross-correlation between two decimated sequences with decimation factors 2 and \(d\). The maximum magnitudes of correlation values for two sequence families are given as

\[
-\frac{1+3p^k}{2} \approx 2\sqrt{N} \quad \text{and} \quad \frac{1-p^{3k}}{2} \approx 0.7p^e \sqrt{N}, \quad \text{respectively.}
\]

### References


Chang-Min Cho received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2010, where he is currently pursuing the Ph.D. degree in electrical engineering and computer science. His area of research interests includes pseudorandom sequences, cryptography, and error-correcting codes.

Ji-Youp Kim received the B.S. and M.S.EE 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.

Jong-Seon No received the B.S. and M.S.EE degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively and the Ph.D. degree in electrical engineering from Seoul National University, Seoul, Korea, in 1990. He served as a Senior MTS at Hughes Network Systems from February 1998 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.