Cross-Correlation Distribution Between Two Decimated Sequences by 2 and $\frac{(p^m+1)^2}{2}$

Chang-Min Cho, Ji-Youp Kim, and Jong-Seon No
Department of Electrical and Computer Engineering
Seoul National University
Seoul 151-742, Korea
{ccm8686, lakroforce}@ccl.snu.ac.kr, jsno@snu.ac.kr

***Abstract*—Let p be an odd prime and $n = 2m$ with $p^m \equiv 1$ (mod 4). In this paper, the cross-correlation distribution between two decimated sequences of a p-ary m-sequence, $s(2t+i)$ with $i \in \{0,1\}$ and $s(d't)$ with $d' = 2d$, $d = (\frac{p^m+1}{2})^2$ is determined.**

I. Introduction

Constructing sequences with good correlation property is important in pseudorandom sequence design. To achieve this, the cross-correlation between an m-sequence $s(t)$ and its decimated sequence $s(dt)$ has been studied for decades [1]-[10].

Recently, there have been researches on the construction of sequence families using two decimated sequences. For an odd prime p with $p \equiv 3$ (mod 4) and an odd integer n, Kim, Choi, No, and Chung [11] constructed a new p-ary sequence family by shifts and additions of two decimated sequences, where the decimation factors are 2 and $2(\frac{p^n-1}{2} - p^{n-1})$. Inspired by this result, Xia and Chen [12] constructed a new sequence family using two decimated sequences with the decimation factors 2 and $p^m + 1$.

In this paper, we show the cross-correlation results between two decimated sequences, $s(2t+i)$ and $s(d't)$, where $s(t)$ is a p-ary m-sequence with period $p^n - 1$, $i = 0, 1$ and $d' = 2d$. The 'original' decimation factor used in this paper is $d = (\frac{p^m+1}{2})^2$ with $n = 2m$ and $p^m \equiv 1$ (mod 4), which is studied by Seo, Kim, No, and Shin [8] and generalized by Luo [9]. For each case of $i = 0$ and $i = 1$, the cross-correlation distribution is derived.

II. Preliminaries

Let p be an odd prime, n, m be positive integers with $m|n$ and F_{p^n} be the finite field with p^n elements. The trace function $\mathrm{tr}_m^n(\cdot)$ from F_{p^n} to F_{p^m} is defined as

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$$

where $x \in F_{p^n}$. Let α be a primitive element of F_{p^n}. Then a p-ary m-sequence $s(t)$ of period $p^n - 1$ can be expressed in terms of the trace function as

$$s(t) = \mathrm{tr}_1^n(\alpha^t).$$

For a decimation factor d, the decimated sequence $s(dt)$ is defined as

$$s(dt) = \mathrm{tr}_1^n(\alpha^{dt})$$

with period $\frac{p^n-1}{c}$, where $c = \gcd(p^n - 1, d)$. The cross-correlation function between two p-ary sequences $a(t)$ and $b(t)$ of period L is defined as

$$C_{a,b}(\tau) = \sum_{t=0}^{L-1} \omega^{a(t+\tau)-b(t)}$$

where $\omega = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th root of unity. Let $a(t) = s(2t+i)$ and $b(t) = s(d't)$ with $i \in \{0,1\}$, $d' = 2d$ and $L = \frac{p^n-1}{2}$. The cross-correlation function between these two decimated sequences is given as

$$\begin{aligned} C_i(\tau) &= \sum_{t=0}^{L-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i})-\mathrm{tr}_1^n(\alpha^{d't})} \\ &= \frac{1}{2}\sum_{t=0}^{p^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i}-\alpha^{d't})} \\ &= \frac{1}{2}\sum_{x\in F_{p^n}} \omega^{\mathrm{tr}_1^n(ax^2-x^{d'})} - \frac{1}{2} \end{aligned} \quad (1)$$

where $x = \alpha^t$ and $a = \alpha^{2\tau+i}$. The second equality holds because $\gcd(p^n - 1, d')$ is a multiple of 2 and thus the equation

$$\sum_{t=0}^{L-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i}-\alpha^{d't})} = \sum_{t=L}^{p^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i}-\alpha^{d't})}$$

holds.

The following two lemmas are derived by Helleseth [2], which will be used in this paper.

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

$$\sum_{x\in F_{p^n}} \omega^{\mathrm{tr}_1^n(ax^{p^{n/2}+1})} = \begin{cases} p^n, & \text{if } a + a^{p^{n/2}} = 0 \\ -p^{n/2}, & \text{if } a + a^{p^{n/2}} \neq 0. \end{cases}$$

□

Lemma 2 [2]: For an odd prime p and an even integer n, we have

$$\sum_{x\in F_{p^n}} \omega^{\mathrm{tr}_1^n(ax^2)} = \begin{cases} p^n, & \text{if } a=0 \\ (-1)^{n+1}((-1)^{\frac{p-1}{2}}p)^{\frac{n}{2}}, & \text{if } a \text{ is a square in } a\in F_{p^n}^* \\ (-1)^n((-1)^{\frac{p-1}{2}}p)^{\frac{n}{2}}, & \text{if } a \text{ is a nonsquare in } a\in F_{p^n}^*. \end{cases}$$

□

III. Main Result

A. Possible Cross-Correlation Values

Throughout this section, the following notations will be used:

- p is an odd prime;
- $n=2m$, where m is a positive integer with $p^m \equiv 1 \pmod 4$;
- $L=\frac{p^n-1}{2}$;
- $d'=2d$ with $d=(\frac{p^m+1}{2})^2$;
- δ is a primitive element of F_{p^n};
- $\beta=\delta^{(p^m+1)/2}$;
- $\gamma=\delta^{2(p^m-1)}$;
- $\alpha=\beta\gamma$.

Then, the following properties hold:

- $\gcd(p^n-1,d')=p^m+1$;
- $\gcd((p^m+1)/2, 2(p^m-1))=1$;
- $\alpha=\beta\gamma$ is a primitive element of F_{p^n} because $\gcd((p^m+1)/2,2(p^m-1))=1$;
- $\beta^{p^m}=-\beta$;
- $\beta^d=\begin{cases}\beta, & \text{if } p=5 \mod 8 \text{ and } m \text{ odd} \\ -\beta, & \text{otherwise;}\end{cases}$
- $\gamma^{p^m}=\gamma^{-1}$ and $\gamma^d=1$;
- For any positive integer t, $\gamma^t\neq -1$.

These notations and properties are from [8], with some minor changes.

In this subsection, we determine the possible values of the cross-correlation function between $s(2t+i)$ and $s(d't)$, where $s(t)$ is a p-ary m-sequence with period p^n-1 and $i=0,1$. $s(2t+i)$ and $s(d't)$ have period of $L=\frac{p^n-1}{2}$ and p^m-1, respectively.

Theorem 3: The cross-correlation function between $s(2t+i)$, $i\in\{0,1\}$ and $s(d't)$ can take the following values:

$$\begin{cases}\{\frac{-1-p^m}{2}, \frac{-1+p^m}{2}, \frac{-1+3p^m}{2}\}, & \text{for } i=0 \\ \{\frac{-1-p^m}{2}, \frac{-1+p^m}{2}\}, & \text{for } i=1.\end{cases}$$

Proof: This theorem can be proved using the similar way as in the proof of Theorem 2 in [8]. Let $x=\alpha^j y^{\frac{p^m+1}{2}}$ with $y\in F_{p^n}$ and $0\le j<\frac{p^m+1}{2}$. Then, as y runs through F_{p^n} and j takes the values in $\{0,1,\ldots,\frac{p^m-1}{2}\}$, x runs through F_{p^n} $\frac{p^m+1}{2}$ times. Also, $y^{\frac{p^m+1}{2}d'}=y^{p^m+1}$ and (1) can be rewritten as

$$\begin{aligned} C_i(\tau)+\frac{1}{2} &= \frac{1}{2}\sum_{x\in F_{p^n}} \omega^{\mathrm{tr}_1^n(ax^2-x^{d'})} \\ &= \frac{1}{p^m+1}\sum_{j=0}^{\frac{p^m-1}{2}}\sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(a\alpha^{2j}y^{p^m+1}-\alpha^{d'j}y^{p^m+1})} \\ &= \frac{1}{p^m+1}\sum_{j=0}^{\frac{p^m-1}{2}}\sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(y^{p^m+1}(a\alpha^{2j}-\alpha^{d'j}))}. \end{aligned} \quad (2)$$

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

$$(a\alpha^{2j}-\alpha^{d'j})^{p^m}+a\alpha^{2j}-\alpha^{d'j}=0, \quad 0\le j<\frac{p^m+1}{2}. \quad (3)$$

Then, using Lemma 1, we have

$$\begin{aligned} C_i(\tau)+\frac{1}{2} &= \frac{1}{p^m+1}(p^{2m}K(a)+(-p^m)(\frac{p^m+1}{2}-K(a))) \\ &= p^m(K(a)-\frac{1}{2}). \end{aligned} \quad (4)$$

Therefore, the values of cross-correlation function are determined by the values of $K(a)$.

Let $2j=k$. Then $d'j=dk$ and using $\alpha=\beta\gamma$, (3) can be rewritten as

$$a^{p^m}(\beta\gamma)^{p^m k}-(\beta\gamma)^{dp^m k}+a(\beta\gamma)^k-(\beta\gamma)^{dk}=0, \quad 0\le k<p^m+1,\ k \text{ is even.} \quad (5)$$

Then, by using the properties of β and γ, (5) can be rewritten as

$$a^{p^m}\beta^k\gamma^{-k}-\beta^k+a\beta^k\gamma^k-\beta^k=0$$

and by multiplying $\beta^{-k}\gamma^k$, we have

$$a\gamma^{2k}-2\gamma^k+a^{p^m}=0, \quad 0\le k<p^m+1,\ k \text{ is even.} \quad (6)$$

Since (6) is a quadratic equation of γ^k, the possible number of solutions is 0, 1, or 2. Assume that (6) has two distinct solutions γ^{s_1} and γ^{s_2}, where s_1 and s_2 are both even. We can represent a as $a=\delta^{2\tau+i}$ and using the quadratic formula, we have

$$\gamma^{s_1+s_2}=\delta^{2(p^m-1)(s_1+s_2)}=a^{p^m-1}=\delta^{(2\tau+i)(p^m-1)}.$$

Therefore, we can derive

$$2(s_1+s_2)=2\tau+i \bmod p^m+1.$$

Since the left-hand side is always even, for $i=1$, there is no two distinct solutions for (6). Therefore, the possible values of $K(a)$ for the cases of $i=0$ and $i=1$ are determined as $\{0,1,2\}$ and $\{0,1\}$, respectively. □

B. Distribution of Cross-Correlation Values

Now, we derive the cross-correlation distribution. For the case of $i = 1$, by calculating $\sum_{\tau=0}^{L-1} C_i(\tau)$, the value distribution of $C_i(\tau)$ can be determined. When $i = 0$, by using $\sum_{\tau=0}^{L-1} C_i(\tau)$ and $\sum_{\tau=0}^{L-1} C_i^2(\tau)$, we can evaluate the cross-correlation distribution.

Lemma 4: Let $C_i(\tau)$ be defined in (1). Then,

$$\sum_{\tau=0}^{L-1} C_i(\tau) = \begin{cases} \frac{1}{4}(p^n + 2^m + 1), & \text{for } i = 0 \\ \frac{1}{4}(-p^n + 1), & \text{for } i = 1. \end{cases}$$

Proof:

$$\sum_{\tau=0}^{L-1} C_i(\tau) = \frac{1}{2} \sum_{\tau=0}^{L-1} \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax^2 - x^{d'})}$$
$$= \frac{1}{2} \sum_{x \in F_{p^n}^*} \omega^{-\mathrm{tr}_1^n(x^{d'})} \sum_{\tau=0}^{L-1} \omega^{\mathrm{tr}_1^n(ax^2)}.$$

Let $y = \alpha^\tau$ and $a = y^2\alpha^i$. By Lemma 2, we have

$$\sum_{\tau=0}^{L-1} \omega^{\mathrm{tr}_1^n(ax^2)} = \frac{1}{2} \sum_{y \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(x^2\alpha^i y^2)}$$
$$= \begin{cases} \frac{1}{2}(-p^m - 1), & \text{for } i = 0 \\ \frac{1}{2}(p^m - 1), & \text{for } i = 1. \end{cases} \quad (7)$$

Next, we calculate $\sum_{x \in F_{p^n}^*} \omega^{-\mathrm{tr}_1^n(x^{d'})}$. Since $\gcd(p^n - 1, d') = p^m + 1$, when x runs through $F_{p^n}^*$, $x^{d'}$ runs through $F_{p^m}^*$, $p^m + 1$ times. Then by Lemma 1,

$$\sum_{x \in F_{p^n}^*} \omega^{-\mathrm{tr}_1^n(x^{d'})} = \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(-x^{p^m+1})} = -p^m - 1. \quad (8)$$

Combining (7) and (8), $\sum_{\tau=0}^{L-1} C_i(\tau)$ can be obtained. □

The following lemma will be used to find $\sum_{\tau=0}^{L-1} C_i^2(\tau)$.

Lemma 5: (i) For $z \in F_{p^n}^*$, the number of solutions of $1 + z^{d'} = 0$ is $p^m + 1$.
(ii) For $z \in F_{p^n}^*$ satisfying $1 + z^{d'} = 0$, we have

$$1 + z^2 \in \begin{cases} \{0\}, & 2 \text{ times} \\ NQR, & p^m - 1 \text{ times} \end{cases}$$

where NQR is the set of nonsquares in $F_{p^n}^*$.
(iii) If $1 + z^{d'} \neq 0$, $1 + z^{d'} + (1 + z^{d'})^{p^m} \neq 0$.

Proof: (i) Since $\gcd(p^n - 1, d') = p^m + 1$, the mapping $z \to z^{d'}$ is a $p^m + 1$ to 1 mapping from $F_{p^n}^*$ onto $F_{p^m}^*$. Therefore, the number of z satisfying $1 + z^{d'} = 0$, i.e., $z^{d'} = -1$ is $p^m + 1$.
(ii) From (i), the number of z satisfying $1 + z^{d'} = 0$ is $p^m + 1$. Let α be a primitive element of F_{p^n}. Then, the values of z satisfying $1 + z^2$ can be written as $\alpha^{\frac{p^n-1}{4}}$ and $\alpha^{\frac{3}{4}(p^n-1)}$. In these two cases, $z^{d'} = z^{2d} = (-1)^d = -1$ holds since d is odd. Next, from Case 1-2 of Theorem 8 in [8], it was shown that for a square x satisfying $1 + x^d = 0$, $1 + x$ cannot be a square. Let $z^2 = x$. Then we have that for z satisfying $1 + z^{d'} = 0$, $1 + z^2$ can be either 0 or a nonsquare. Since there are 2 z's that satisfy $1 + z^2 = 0$, for other $p^m - 1$ values of z, $1 + z^2 \in NQR$.
(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 thus $(1 + z^{d'})^{p^m - 1} = 1$. Thus the proof is done. □

Lemma 6: For $C_i(\tau)$ with $i = 0$ in (1), we have

$$\sum_{\tau=0}^{L-1} C_i^2(\tau) = \frac{3p^{2n} - 6p^n - 4p^m - 1}{8}.$$

Proof:

$$\sum_{\tau=0}^{L-1} C_i^2(\tau) = \frac{1}{4} \sum_{\tau=0}^{L-1} \sum_{x_1 \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax_1^2 - x_1^{d'})} \sum_{x_2 \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax_2^2 - x_2^{d'})}$$
$$= \frac{1}{4} \sum_{x_1 \in F_{p^n}^*} \sum_{x_2 \in F_{p^n}^*} \omega^{-\mathrm{tr}_1^n(x_1^{d'} + x_2^{d'})} \sum_{y \in F_{p^n}^*} \frac{1}{2} \omega^{\mathrm{tr}_1^n(y^2(x_1^2 + x_2^2))} \quad (9)$$

where $y = \alpha^\tau$. Let $z = x_2/x_1$. Then (9) can be rewritten as

$$\sum_{\tau=0}^{L-1} C_i^2(\tau)$$
$$= \frac{1}{8} \sum_{x_1 \in F_{p^n}^*} \sum_{z \in F_{p^n}^*} \omega^{-\mathrm{tr}_1^n(x_1^{d'}(1 + z^{d'}))} \sum_{y \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(y^2 x_1^2(1 + z^2))}.$$

Define

$$X(x_1, y, z) = \omega^{-\mathrm{tr}_1^n(x_1^{d'}(1 + z^{d'}))} \sum_{y \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(y^2 x_1^2(1 + z^2))}$$

and let QR and NQR denote the set of squares and nonsquares in $F_{p^n}^*$, respectively. Then we have

$$\sum_{\tau=0}^{L-1} C_i^2(\tau) = \frac{1}{8} \sum_{x_1 \in F_{p^n}^*} \Big[\sum_{z \in F_{p^n}^*, 1 + z^2 = 0} X(x_1, y, z)$$
$$+ \sum_{z \in F_{p^n}^*, 1 + z^2 \in QR} X(x_1, y, z) + \sum_{z \in F_{p^n}^*, 1 + z^2 \in NQR} X(x_1, y, z) \Big].$$

For $z \in F_{p^n}^*$, from Theorem 67 of [14], we have

$$1 + z^2 \in \begin{cases} \{0\}, & 2 \text{ times} \\ QR, & \frac{p^n - 5}{2} \text{ times} \\ NQR, & \frac{p^n - 1}{2} \text{ times}. \end{cases}$$

Now, by Lemmas 1, 2, and 5, we have

$$\sum_{x_1 \in F_{p^n}^*} \sum_{z \in F_{p^n}^*, 1 + z^2 = 0} X(x_1, y, z)$$
$$= \sum_{x_1 \in F_{p^n}^*} 2 \cdot \omega^{-\mathrm{tr}_1^n(x_1^{d'} \cdot 0)}(p^n - 1) = 2(p^n - 1)^2 \quad (10)$$

$$\sum_{x_1\in F_{p^n}^*}\sum_{z\in F_{p^n}^*,1+z^2\in QR} X(x_1,y,z)$$
$$=\sum_{z\in F_{p^n}^*,1+z^2\in QR}\sum_{x_1\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n(x_1^{d'}(1+z^{d'}))}(-p^m-1)$$
$$=\frac{p^n-5}{2}(p^m+1)^2 \tag{11}$$

$$\sum_{x_1\in F_{p^n}^*}\sum_{z\in F_{p^n}^*,1+z^2\in NQR} X(x_1,y,z)$$
$$=\sum_{z\in F_{p^n}^*,1+z^2\in NQR}\sum_{x_1\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n(x_1^{d'}(1+z^{d'}))}(p^m-1)$$
$$=(p^m-1)[(p^m-1)(p^n-1)+(\frac{p^n-2p^m+1}{2})(-p^m-1)]. \tag{12}$$

Combining (11), (12), and (13), $\sum_{\tau=0}^{L-1}C_i^2(\tau)$ is derived. □

Using Lemmas 4 and 6, the cross-correlation distribution between $s(2t+i)$ and $s(d't)$ can be derived as in the following theorem.

Theorem 7: The cross-correlation distribution between $s(2t+i)$, $i\in\{0,1\}$ and $s(d't)$ is given as follows.
(i) For $i=0$

$$C_i(\tau)=\begin{cases}\frac{-1-p^m}{2}, & \frac{1}{8}(3p^n-4p^m-7) \text{ times}\\ \frac{-1+p^m}{2}, & \frac{p^m+1}{2} \text{ times}\\ \frac{-1+3p^m}{2}, & \frac{1}{8}(p^n-1) \text{ times.}\end{cases}$$

(ii) For $i=1$

$$C_i(\tau)=\begin{cases}\frac{-1-p^m}{2}, & \frac{1}{4}(p^n-1) \text{ times}\\ \frac{-1+p^m}{2}, & \frac{1}{4}(p^n-1) \text{ times.}\end{cases}$$

Proof: We prove for the case of $i=0$. Let

$$C_i(\tau)=\begin{cases}\frac{-1-p^m}{2}, & N_1 \text{ times}\\ \frac{-1+p^m}{2}, & N_2 \text{ times}\\ \frac{-1+3p^m}{2}, & N_3 \text{ times.}\end{cases}$$

Then, the value distribution of $C_i(\tau)$ can be obtained by solving the following system of equations

$$N_1+N_2+N_3=\frac{1}{2}(p^n-1)$$
$$\frac{-1-p^m}{2}N_1+\frac{-1+p^m}{2}N_2+\frac{-1+3p^m}{2}N_3$$
$$=\frac{1}{4}(p^n+2^m+1)$$
$$(\frac{-1-p^m}{2})^2N_1+(\frac{-1+p^m}{2})^2N_2+(\frac{-1+3p^m}{2})^2N_3$$
$$=\frac{3p^{2n}-6p^n-4p^m-1}{8}.$$

For $i=1$, the cross-correlation distribution can be derived by similar method. □

IV. Conclusion

In this paper, for an odd prime p and an even integer $n=2m$ with $p^m\equiv 1 \pmod 4$, we investigate the cross-correlation function between two decimated sequences of p-ary m-sequence, $s(2t+i)$ and $s(d't)$, where $d'=2d$ and $d=(\frac{p^m+1}{2})^2$ as in [8] [9]. The cross-correlation function takes three values when $i=0$ and takes two values when $i=1$. The complete cross-correlation distribution for each case is derived.

In the following, we give two examples to verify the main results in Theorem 7.

Example 8: Let $p=3$, $n=8$, and $m=4$. Then $L=3280$ and $d'=2d=3362$. By computer experiments, the cross-correlation distribution of $s(2t+i)$, $i=0,1$ and $s(d't)$ is given as
(i) $i=0$

$$\begin{cases}-41, & 2419 \text{ times}\\ 40, & 41 \text{ times}\\ 121, & 820 \text{ times.}\end{cases}$$

(ii) $i=1$

$$\begin{cases}-41, & 1640 \text{ times}\\ 40, & 1640 \text{ times.}\end{cases}$$

The numerical results coincide with the results presented in Theorem 7.

Example 9: Let $p=5$, $n=6$, and $m=3$. Then $L=7812$ and $d'=2d=7938$. By computer experiments, the cross-correlation distribution of $s(2t+i)$, $i=0,1$ and $s(d't)$ is given as
(i) $i=0$

$$\begin{cases}-63, & 5796 \text{ times}\\ 62, & 63 \text{ times}\\ 187, & 1953 \text{ times.}\end{cases}$$

(ii) $i=1$

$$\begin{cases}-63, & 3906 \text{ times}\\ 62, & 3906 \text{ times.}\end{cases}$$

The numerical results also coincide with the results presented in Theorem 7.

References

[1] H. M. Trachtenberg, "On the cross-correlation functions of maximal recurring sequences," Ph.D. dissertation, Univ. Southern California, Los Angeles, CA, 1970.

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

[3] E. N. Müller, "On the cross-correlation of sequences over $GF(p)$ with short periods," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 289-295, Jan. 1999.

[4] Z. Hu, X. Li, D. Mills, E. Müller, W. Sun, W. Williems, Y. Yang, and Z. Zhang, "On the cross-correlation of sequences with the decimation factor $d=\frac{p^n+1}{p+1}-\frac{p^n-1}{2}$," *Appl. Algebra Eng. Commun. Comput.*, vol. 12, pp. 255-263, 2001.

[5] Y. Xia, X. Zeng, and L. Hu, "Further crosscorrelation properties of sequences with the decimation factor $d=\frac{p^n+1}{p+1}-\frac{p^n-1}{2}$," *Appl. Algebra Eng. Commun. Comput.*, vol. 21, no. 5, pp. 329-342, 2010.

[6] G. J. Ness, T. Helleseth, and A. Kholosha, "On the correlation distribution of the Coulter-Matthews decimation," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2241-2247, May 2006.

[7] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter-Matthews function," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5345-5353, Dec. 2008.

[8] E. Y. Seo, Y. S. Kim, J. S. No, and D. J. Shin, "Cross-correlation distribution of p-ary m-sequence of period $p^{4k}-1$ and its decimated sequences by $(\frac{p^{2k}+1}{2})^2$," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3140-3149, Jul. 2008.

[9] J. Luo, "Cross correlation of nonbinary Niho-type sequences, *in Proc. IEEE Int. Symp. Information Theory*, Austin, Texas, Jun. 2010, pp. 1297-1299.

[10] S. T. Choi, T. Lim, J. S. No, and H. Chung, "On the cross-correlation of a p-ary m-sequences of period $p^{2m}-1$ and its decimated sequences by $\frac{(p^m+1)^2}{2(p+1)}$," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1873-1879, Mar. 2012.

[11] J. Y. Kim, S. T. Choi, J. S. No, and H. Chung, "A new family of p-ary sequences of period $\frac{p^n-1}{2}$ with low correlation," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3825-3830, Jun. 2011.

[12] Y. Xia and S. Chen, "A new family of p-ary sequences with low correlation constructed from decimated sequences," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 6037-6046, Sep. 2012.

[13] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*, Reading, MA: Addison-Wesley, 1983.

[14] L.E Dickson, *Linear Groups: with an Exposition of the Galois Field Theory*, New York, NY: Dover, 1958.