Cross-Correlation Distribution of p-ary m-Sequence of Period $p^{4k}-1$ and Its Decimated Sequences by $\left(\frac{p^{2k}+1}{2}\right)^2$

Eun-Young Seo
School of Electrical Engineering and Computer Science
Seoul National University
Seoul 151-742, Korea.
gourb@ccl.snu.ac.kr

Young-Sik Kim
Embedded Software Center
System LSI Division
Samsung Electronics Co.
Yongin 446-711, Korea
kingsi@ccl.snu.ac.kr

Jong-seon No
School of Electrical Engineering and Computer Science
Seoul National University
Seoul 151-742, Korea.
jsno@snu.ac.kr

Dong-Joon Shin
Division of Electronics and Computer Engineering
Hanyang University
Seoul 133-791, Korea.
djshin@hanyang.ac.kr

***Abstract*— For an odd prime p, $n=4k$, and $d=((p^{2k}+1)/2)^2$, there are $(p^{2k}+1)/2$ distinct decimated sequences $s(dt+l)$, $0\le l<(p^{2k}+1)/2$, of a p-ary m-sequence $s(t)$ of period p^n-1 because $\gcd(d,p^n-1)=(p^{2k}+1)/2$. In this paper, it is shown that the cross-correlation function between $s(t)$ and $s(dt+l)$, $0\le l<(p^{2k}+1)/2$, takes the values in $\{-1,-1-\sqrt{p^n},-1+\sqrt{p^n},-1+2\sqrt{p^n}\}$ and their cross-correlation distribution is also derived.**

I. Introduction

For the past decades, many families of sequences with good cross-correlation property have been found [1]–[4]. Especially, to construct a family of p-ary sequences of period p^n-1 with good correlation property, the cross-correlation distribution between a p-ary m-sequence $s(t)$ of period p^n-1 and its decimated sequence $s(dt)$ with $\gcd(d,p^n-1)=1$ has been studied for many years [5]–[8]. Also, there are some research results dealing with a decimation factor d which is not relatively prime to the period p^n-1 [9], [10].

For an odd prime p, $n=4k$, and $d=((p^{2k}+1)/2)^2$, there are $(p^{2k}+1)/2$ distinct decimated sequences $s(dt+l)$, $0\le l<(p^{2k}+1)/2$, of a p-ary m-sequence $s(t)$ of period p^n-1 because $\gcd(d,p^n-1)=(p^{2k}+1)/2$. In this paper, it is shown that the cross-correlation function between $s(t)$ and $s(dt+l)$, $0\le l<(p^{2k}+1)/2$, takes the values in $\{-1,-1-\sqrt{p^n},-1+\sqrt{p^n},-1+2\sqrt{p^n}\}$ and their cross-correlation distribution is also derived. Using $s(t)$ and $s(dt+l)$, a new family of p-ary sequences of period p^n-1 can be constructed, whose family size is p^n and the maximum magnitude of their cross-correlation values is $2\sqrt{p^n}-1$.

II. Preliminaries and Notations

Let p be an odd prime and F_{p^n} the finite field with p^n elements. Then the trace function $\mathrm{tr}_m^n(\cdot)$ from F_{p^n} to F_{p^m} is defined as $\mathrm{tr}_m^n(x)=\sum_{i=0}^{n/m-1}x^{p^{mi}}$, where $x\in F_{p^n}$ and $m|n$. 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 written in terms of the trace function as

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

In this paper, the following notations will be used:

- $n=4k$, where k is a positive integer;
- $d=((p^{2k}+1)/2)^2$;
- δ is a primitive element of F_{p^n};
- $\beta=\delta^{(p^{2k}+1)/2}$, $\gamma=\delta^{2(p^{2k}-1)}$, and $\alpha=\beta\gamma$.

The following properties will be frequently used in the subsequent sections:

- $\gcd((p^{2k}+1)/2,2(p^{2k}-1))=1$;
- $\gcd(p^n-1,((p^{2k}+1)/2)^2)=(p^{2k}+1)/2$;
- $d=(\frac{p^{2k}+1}{2})^2=\begin{cases}p^{2k} \pmod{2(p^{2k}-1)}\\ 0 \pmod{(p^{2k}+1)/2};\end{cases}$
- $\alpha=\beta\gamma$ is a primitive element of F_{p^n} because $\gcd((p^{2k}+1)/2,2(p^{2k}-1))=1$;
- $\beta^{p^{2k}}=-\beta$, $\beta^d=-\beta$, $\gamma^{p^{2k}}=\gamma^{-1}$, and $\gamma^d=1$;
- For any positive integer t, $\gamma^t\neq-1$.

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

$$s(dt+l)=\mathrm{tr}_1^n(\alpha^{dt+l}). \tag{1}$$

It is easy to check that all the decimated sequences $s(dt+l)$ are cyclically distinct. Then the cross-correlation function of $s(t)$ and its decimated sequence $s(dt+l)$ at shift τ is defined as

$$C_l(\tau)=\sum_{t=0}^{p^n-2}\omega^{\mathrm{tr}_1^n(\alpha^{t+\tau}-\alpha^{dt+l})}=\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(ax-bx^d)} \tag{2}$$

where ω is a primitive complex p-th root of unity, $a=\alpha^\tau$, and $b=\alpha^l$.

III. Evaluation of Cross-Correlation Values

In this section, the possible cross-correlation values in (2) of a p-ary m-sequence $s(t)$ and its decimated sequence $s(dt+l)$ in (1) will be derived. The following lemma was derived by

Helleseth [6], which will be used in the proof of the subsequent theorem.

Lemma 1: [6] Let p be an odd prime and n an even integer. Then

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

□

Theorem 2: The cross-correlation function between a p-ary m-sequence $s(t)$ and its decimated sequences $s(dt+l)$, $0 \le l < (p^{2k}+1)/2$, given in (1) takes the values in $\{-1,\ -1-\sqrt{p^n},\ -1+\sqrt{p^n},\ -1+2\sqrt{p^n}\}$.

Proof: Using the similar method in the proof of Theorem 3.8 in [6], this theorem can be proved. Let $x=\alpha^j y^{p^{2k}+1}$, where α is a primitive element of F_{p^n} and $0 \le j < p^{2k}+1$. Then, $y^{(p^{2k}+1)d} = y^{p^{2k}+1}$ for $y \in F_{p^n}$ and (2) can be rewritten as

$$C_l(\tau)+1 = \frac{1}{p^{2k}+1}\sum_{j=0}^{p^{2k}}\sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(y^{p^{2k}+1}(a\alpha^j - b\alpha^{dj}))}. \quad (3)$$

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

$$\mathrm{tr}_{2k}^n(a\alpha^j - b\alpha^{dj}) = (a\alpha^j - b\alpha^{dj})^{p^{2k}} + a\alpha^j - b\alpha^{dj} = 0, \quad 0 \le j < p^{2k}+1. \quad (4)$$

From Lemma 1, (3) can be given as

$$(p^{2k}+1)(C_l(\tau)+1) = -(p^{4k}+p^{2k}) + (p^{4k}+p^{2k})K(a,b)$$

and thus $C_l(\tau) = -1 + p^{2k}(K(a,b)-1)$. Using $\alpha=\beta\gamma$, (4) can be rewritten as

$$a^{p^{2k}}(\beta\gamma)^{p^{2k}j} - b^{p^{2k}}(\beta\gamma)^{dp^{2k}j} + a(\beta\gamma)^j - b(\beta\gamma)^{dj} = 0, \quad 0 \le j < p^{2k}+1. \quad (5)$$

Then, using $\beta^d=-\beta$, $\beta^{p^{2k}}=-\beta$, $\gamma^d=1$, and $\gamma^{p^{2k}}=\gamma^{-1}$, and multiplying $\beta^{-j}\gamma^j$, (5) can be written as

$$a\gamma^{2j} - b^{p^{2k}}\gamma^j - b(-1)^j\gamma^j + a^{p^{2k}}(-1)^j = 0. \quad (6)$$

The number of solutions $K(a,b)$ of (6) can be obtained by considering (6) separately as the following two quadratic equations of $(-1)^j\gamma^j$.

$$\text{even } j: a((-1)^j\gamma^j)^2 - (b+b^{p^{2k}})(-1)^j\gamma^j + a^{p^{2k}} = 0 \quad (7)$$

$$\text{odd } j: a((-1)^j\gamma^j)^2 + (b-b^{p^{2k}})(-1)^j\gamma^j - a^{p^{2k}} = 0. \quad (8)$$

Note that $(-1)^j\gamma^j$ covers all distinct elements as j takes the value in $\{0,1,\cdots,p^{2k}\}$ because the order $(p^{2k}+1)/2$ of γ is odd and the order of -1 is 2.

We will show that the total number of solutions for (7) and (8) is less than 4, which means that $K(a,b)$ should be $0,1,2$, or 3.

Clearly, a can be expressed as δ^τ. Suppose that (7) has two solutions, γ^{a_1} and γ^{a_2}. Then, it is clear that both a_1 and a_2 are even and by using these solutions, we obtain

$$2(a_1+a_2) = \tau \bmod (p^{2k}+1)$$

and τ must be even to have two solutions for (7). Also, suppose that (8) has two distinct solutions, $-\gamma^{b_1}$ and $-\gamma^{b_2}$. Then, it is clear that both b_1 and b_2 are odd. Similarly to the previous case, we can derive

$$2(b_1+b_2) = \tau + \frac{p^{2k}+1}{2} \bmod (p^{2k}+1).$$

Since τ should be even to have two solutions for (7) and $(p^{2k}+1)/2$ is odd, there are no b_1 and b_2 satisfying the above equation and there are no two distinct solutions for (8).

Conversely, if (8) has two distinct solutions, it can be similarly shown that (7) cannot have two distinct solutions. Therefore, $K(a,b)$ cannot be 4 and thus the possible values of $C_l(\tau)$ are -1, $-1-\sqrt{p^n}$, $-1+\sqrt{p^n}$, and $-1+2\sqrt{p^n}$. □

IV. Distribution of Cross-Correlation Values

In order to derive the cross-correlation distribution of a p-ary m-sequence $s(t)$ and its decimated sequences $s(dt+l)$, $0 \le l < (p^{2k}+1)/2$, $\sum C_l(\tau)$, $\sum C_l^2(\tau)$, and $\sum C_l^3(\tau)$ have to be calculated. Thus, we will evaluate those values in the following theorems and lemmas.

Theorem 3:

$$\sum_{\tau=0}^{p^n-2} C_l(\tau) = \begin{cases} \frac{-p^n+p^{\frac{n}{2}}}{2}+1, & \text{if } l=0 \\ p^{\frac{n}{2}}+1, & \text{otherwise.} \end{cases}$$

Proof: From (2), the summation of $C_l(\tau)$ can be represented as

$$\sum_{\tau=0}^{p^n-2} C_l(\tau) = \sum_{a\in F_{p^n}^*}\sum_{x\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax-bx^d)} = -\sum_{x\in F_{p^n}^*} \omega^{-\mathrm{tr}_1^n(bx^d)}.$$

Since d is odd and $\gcd((p^{2k}+1)/2, 2(p^{2k}-1)) = 1$, we have $\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(bx^d)} = \sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(bx^{(p^{2k}+1)/2})}$. Let $x=y^2$ for square x and otherwise, $x=zy^2$, where z is a nonsquare in F_{p^n}. Then we have

$$2(1-\sum_{\tau=0}^{p^n-2} C_l(\tau)) = \sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(by^{p^{2k}+1})} + \sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(bz^{\frac{p^{2k}+1}{2}}y^{p^{2k}+1})}. \quad (9)$$

From Lemma 1, the first summation is given as

$$\sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(by^{p^{2k}+1})} = -p^{\frac{n}{2}} \quad (10)$$

because $b+b^{p^{2k}}$ is not equal to 0 for all $b=\alpha^l$, $0 \le l < (p^{2k}+1)/2$.

In the second summation, let

$$bz^{\frac{p^{2k}+1}{2}} + (bz^{\frac{p^{2k}+1}{2}})^{p^{2k}} = 0. \quad (11)$$

Using $z^{p^{2k}(p^{2k}+1)/2} = -z^{(p^{2k}+1)/2}$, (11) reduces to $b^{p^{2k}-1} = 1$, which means that b has to be 1. Then the second summation is given as

$$\sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(bz^{\frac{p^{2k}+1}{2}} y^{p^{2k}+1})} = \begin{cases} p^n, & \text{if } b=1, \text{i.e., } l=0 \\ -p^{\frac{n}{2}}, & \text{otherwise.} \end{cases} \tag{12}$$

Plugging (10) and (12) into (9), $\sum_{\tau=0}^{p^n-2} C_l(\tau)$ can be obtained and thus the theorem is proved. □

Theorem 4:

$$\sum_{\tau=0}^{p^n-2} C_l^2(\tau) = \begin{cases} \frac{3p^{2n}+2p^{\frac{3n}{2}}-p^n-4p^{\frac{n}{2}}}{4} - 1, & \text{if } l=0 \\ p^{2n} - 2p^n - 2p^{\frac{n}{2}} - 1, & \text{otherwise.} \end{cases}$$

Proof: The summation of $C_l^2(\tau)$ can be written as

$$\sum_{\tau=0}^{p^n-2} C_l^2(\tau) = \sum_{x_1,x_2\in F_{p^n}^*} \omega^{-\mathrm{tr}_1^n(b(x_1^d+x_2^d))} \sum_{a\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(a(x_1+x_2))}.$$

The inner summation is -1 if $x_1 \neq -x_2$. Thus we have

$$\sum_{\tau=0}^{p^n-2} C_l^2(\tau) = (p^n-1)^2 - \sum_{x_1\in F_{p^n}^*} \sum_{\substack{x_2\in F_{p^n}^* \\ x_2\neq -x_1}} \omega^{-\mathrm{tr}_1^n(b(x_1^d+x_2^d))}.$$

Using Theorem 3, $\sum_{\tau=0}^{p^n-2} C_l^2(\tau)$ can be computed as

$$\sum_{\tau=0}^{p^n-2} C_l^2(\tau) = p^{2n} - p^n - \Big(\sum_{\tau=0}^{p^n-2} C_l(\tau)\Big)^2.$$

Thus, it is proved. □

Using the notations $\beta = \delta^{(p^{2k}+1)/2}$ and $\gamma = \delta^{2(p^{2k}-1)}$, where δ is a primitive element of F_{p^n}, the following lemmas and theorem can be derived, which will be used to find $\sum C_l^3(\tau)$ in Theorem 9.

Lemma 5: The $(p^{2k}+1)/2$ to 1 mapping $f\colon x \to x^d$ defined on $F_{p^n}^*$ has the following properties:

1) $f(\beta^{2u}\gamma^t) = \beta^{2u}$;

2) $f(\beta^{2u+1}\gamma^t) = -\beta^{2u+1}$

where $0 \le u < p^{2k}-1$ and $0 \le t < (p^{2k}+1)/2$.

Proof: Using $\beta^d = -\beta$ and $\gamma^d = 1$, the above relations can be obtained. □

Lemma 6: All the solutions of

$$1 + x^d - (1+x)^d = 0, \quad x \in F_{p^n} \tag{13}$$

are p^{2k} elements in $F_{p^{2k}}$.

Proof: It is clear that $x = -1$ is a solution of (13). Suppose that $x \neq -1$. Then (13) can be rewritten as $1+x^d = (1+x)^d = \beta^{2u}$. Therefore, from Lemma 5, for some integers t_1 and t_2, the solutions of (13) should be given as

$$x = (\beta^{2u}-1)\gamma^{t_1} = \beta^{2u}\gamma^{t_2} - 1. \tag{14}$$

If $t_1 \neq t_2$, it can be modified as

$$\beta^{2u} = \frac{1-\gamma^{t_1}}{\gamma^{t_2}-\gamma^{t_1}}. \tag{15}$$

Since β^{2u} is an element in $F_{p^{2k}}^*$ and $\gamma^{p^{2k}} = \gamma^{-1}$, raising the power $(p^{2k}-1)$ to both sides of (15) gives us $1 = \gamma^{t_2}$. From (14) and $t_2 = 0$, we have $t_1 = t_2 = 0$, which contradicts to $t_1 \neq t_2$. Therefore, we have $t_1 = t_2 = 0$ and $x = \beta^{2u} - 1$. Thus, including $x = -1$, all the solutions of (13) are p^{2k} elements in $F_{p^{2k}}$. □

Lemma 7: Let e vary over $0 \le e < p^{2k}-1$. For each i, $1 \le i < (p^{2k}+1)/2$, there exist a pair of solutions $e = e_1,\ p^{2k}-2-e_1$ satisfying $1+\beta^{2e+1} = \beta^u\alpha^i$, where α is a primitive element of F_{p^n} and u is some integer in $0 \le u < 2(p^{2k}-1)$.

Proof: It can be easily checked that $i \neq 0$ for all e. Suppose that for the same i, we have

$$1 + \beta^{2e_1+1} = \beta^{u_1}\alpha^i,\ 1 + \beta^{2e_2+1} = \beta^{u_2}\alpha^i$$

where $0 \le e_1 \neq e_2 < p^{2k}-1$. Then we can derive the relation of e_1 and e_2 by raising the power $2(p^{2k}-1)$ to the above equations and using $\beta^{p^{2k}-1} = -1$ as

$$\beta^{2e_2} - \beta^{2e_1} = \beta^{2(e_1+e_2+1)}(\beta^{2e_2} - \beta^{2e_1}).$$

Since $e_1 \neq e_2$, we have $e_1 + e_2 + 1 = 0 \bmod (p^{2k}-1)$. Therefore, for the same i, e_1 and $p^{2k}-2-e_1$ for e can satisfy $1+\beta^{2e+1} = \beta^u\alpha^i$. Since e can take $p^{2k}-1$ distinct values and i can take $(p^{2k}-1)/2$ distinct values, we can conclude that for each $i \neq 0$, there exist a pair of e_1 and $p^{2k}-2-e_1$ for e to satisfy $1+\beta^{2e+1} = \beta^u\alpha^i$. □

Next, we will consider the case of $1+x^d-(1+x)^d = \beta^u\alpha^i$ in the following theorem and count the number of solutions.

Theorem 8: Let

$$1 + x^d - (1+x)^d = \beta^u\alpha^i,\ x \in F_{p^n}^* \tag{16}$$

where $0 \le u < 2(p^{2k}-1)$ and $0 \le i < (p^{2k}+1)/2$. There are $(p^{2k}-1)(p^{2k}+3)/4$ solutions x for $i=0$ and $3(p^{2k}-1)/2$ solutions x for each $i \neq 0$, where u is some integer in $0 \le u < 2(p^{2k}-1)$.

Proof: We will prove this theorem by considering the following cases.

Case 1) $i = 0$:

We will show that there are $(p^{2k}-1)(p^{2k}+3)/4$ solutions x of (16) when $i=0$ by considering the following four cases.

Case 1-1) x is a square and $1+x$ is a square:

There are $(p^n-1)/4$ elements x such that both x and $1+x$ are squares by the result for cyclotomic number of order 2 in [13]. In this case, it is clear that both $1+x^d$ and $(1+x)^d$ are elements in $F_{p^{2k}}^*$ and the left-hand side of (16) is equal to β^u for some integer u in $0 \le u < 2(p^{2k}-1)$. Thus, by excluding the solutions of $1+x^d-(1+x)^d = 0$ using Lemma 6, the number of square solutions x of (16), in this case, is

$$\frac{p^{4k}-1}{4} - (p^{2k}-1) = \frac{(p^{2k}-1)(p^{2k}-3)}{4}.$$

Case 1-2) x is a square and $1+x$ is a nonsquare:

First, in this case, we will show that $1+x^d$ is equal to 0 if and only if i is equal to 0. If $1+x^d$ is equal to 0, i should be equal to 0 because $(1+x)^d$ is $-\beta^{2u_1+1}$ from Lemma 5. To prove the converse, we can show that if $1+x^d$ is not equal to zero, i is not equal to zero by inducing a contradiction.

Next, we will show that if x satisfies $1+x^d=0$, $1+x$ is a nonsquare. Note that x satisfying $1+x^d=0$ is a square. Since $x^d=-1$, x can be expressed as $-\gamma^{t_1}$ by Lemma 5. Suppose that $1+x$ is a square. Then, $1+x$ can be represented as $\beta^{2u}\gamma^{t_2}$ and we have $-\gamma^{t_1}=\beta^{2u}\gamma^{t_2}-1$, which can be rewritten as $\beta^{2u}=(1-\gamma^{t_1})\gamma^{-t_2}$. Raising the power $(p^{2k}-1)$ to both sides of the equation, we have $1=-\gamma^{2t_2-t_1}$. Since $\gamma^{2t_2-t_1}\neq -1$, $1+x$ should be a nonsquare.

It can be easily shown that there are $(p^{2k}-1)/2$ square solutions x in $F_{p^n}^*$ of $1+x^d=0$ because $x=-1$ should be excluded. Therefore, in this case, the number of square solutions x of (16) is $(p^{2k}-1)/2$.

Case 1-3) x is a nonsquare and $1+x$ is a square:

Using the similar method in Case 1-2) by replacing x by $1+x$ and $1+x$ by x in Case 1-2), respectively, in this case, the number of nonsquare solutions x of (16) is $(p^{2k}-1)/2$.

Case 1-4) x is a nonsquare and $1+x$ is a nonsquare:

First, we will show that when $x\in F_{p^n}^*$ is a nonsquare and $1+x$ a nonsquare, $x^d-(1+x)^d$ is equal to 0 if and only if i is equal to 0. It is clear that if $x^d-(1+x)^d$ is equal to 0, i is equal to 0 because $1=\beta^0$. To prove the converse, we can show that if $x^d-(1+x)^d$ is not equal to zero, i is not equal to zero by inducing a contradiction.

Next, we will count the number of x satisfying $x^d=(1+x)^d$, where both x and $1+x$ are nonsquares. Let $x^d=(1+x)^d=-\beta^{2u_1+1}$. Then, from Lemma 5, we have $\gamma^{t_1}\beta^{2u_1+1}=\gamma^{t_2}\beta^{2u_1+1}-1$, which can be rewritten as

$$\beta^{2u_1+1}=\frac{1}{\gamma^{t_2}-\gamma^{t_1}}. \tag{17}$$

Raising the power $(p^{2k}-1)$ to both sides of the above equation, we have $-1=-\gamma^{t_1+t_2}$, which implies $t_1=-t_2$. Also, we will show that u_1 satisfying (17) takes distinct value for each pair of distinct t_1 and $t_2=-t_1$. Suppose that for two distinct t_1 and t_1', (17) is satisfied with the same u_1. Then we have $\gamma^{-t_1}-\gamma^{t_1}=\gamma^{-t_1'}-\gamma^{t_1'}$, which can be rewritten as $\gamma^{-t_1-t_1'}(\gamma^{t_1'}-\gamma^{t_1})=\gamma^{t_1}-\gamma^{t_1'}$. However, that equation cannot be satisfied because $\gamma^{-(t_1+t_1')}\neq -1$. Since t_1 varies over $1\le t_1<(p^{2k}+1)/2$ in this case, the number of nonsquare solutions x of (16) is $(p^{2k}-1)/2$.

Case 2) $i\neq 0$:

For each $i\neq 0$, we will show that there are $3(p^{2k}-1)/2$ solutions x of (16) by considering the following four cases.

Case 2-1) x is a square and $1+x$ is a square:

As shown in Case 1-1), there is no solution of (16).

Case 2-2) x is a square and $1+x$ is a nonsquare:

From Lemma 5, for a square x making $1+x$ a nonsquare, there exist u_1 and u_2, $0\le u_1,u_2<p^{2k}-1$, satisfying

$$1+x^d=\beta^{2u_1},\ (1+x)^d=-\beta^{2u_2+1}. \tag{18}$$

Then, we have

$$\beta^{2u_1}+\beta^{2u_2+1}=\beta^u\alpha^i. \tag{19}$$

Now, we can show that there are $(p^{2k}-1)/2$ solutions x of (16) for each i, $1\le i<(p^{2k}+1)/2$, by proving the following three steps, but their proofs will be omitted.

- Step 1: The mapping from x to (u_1,u_2) given in (18) is one-to-one;
- Step 2: For each i, $1\le i<(p^{2k}+1)/2$, there are $(p^{2k}+1)/2$ possible solutions (u_1,u_2) satisfying (18) and (19);
- Step 3: For each i, $1\le i<(p^{2k}+1)/2$, exactly one possible solution in Step 2 cannot satisfy (18) and (19).

Case 2-3) x is a nonsquare and $1+x$ is a square:

Case 2-4) x is a nonsquare and $1+x$ is a nonsquare:

Similarly to the Case 2-2), we can show that the number of nonsquare solutions x of (16) is $(p^{2k}-1)/2$ for each i, $1\le i<(p^{2k}+1)/2$, in each of Case 2-3) and Case 2-4). □

Using Lemma 6 and Theorem 8, we can find $\sum C^3(\tau)$ as in the following theorem.

Theorem 9:

$$\sum_{\tau=0}^{p^n-2}C_l^3(\tau)=\begin{cases}\frac{3}{4}p^{2n+2k}-\frac{7}{4}p^{2n}-\frac{7}{4}p^{n+2k}\\ \qquad+\frac{5}{4}p^n+\frac{3}{2}p^{2k}+1, & \text{if } l=0\\ \frac{3}{4}p^{2n+2k}-2p^{2n}+\frac{1}{4}p^{n+2k}\\ \qquad+5p^n+3p^{2k}+1, & \text{otherwise.}\end{cases}$$

Proof: We can manipulate the summation of cubic power of the cross-correlation values as

$$\sum_{\tau=0}^{p^n-2}C_l^3(\tau)=(p^n-1)\sum_{\substack{x_1,x_2,x_3\in F_{p^n}^*\\ x_1+x_2+x_3=0}}\omega^{-\mathrm{tr}_1^n(b(x_1^d+x_2^d+x_3^d))}-\sum_{\substack{x_1,x_2,x_3\in F_{p^n}^*\\ x_1+x_2+x_3\neq 0}}\omega^{-\mathrm{tr}_1^n(b(x_1^d+x_2^d+x_3^d))}.$$

The first summation in the above equation becomes

$$(p^n-1)\sum_{\substack{x_1,x_2,x_3\in F_{p^n}^*\\ x_1+x_2+x_3=0}}\omega^{-\mathrm{tr}_1^n(b(x_1^d+x_2^d+x_3^d))}$$
$$=(p^n-1)\Big[\sum_{x_1,x_2\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n(b(x_1^d+x_2^d-(x_1+x_2)^d))}-(p^n-1)\Big].$$

The second summation can be represented as

$$-\sum_{x_1,x_2\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n(b(x_1^d+x_2^d)}\sum_{\substack{x_3\in F_{p^n}^*\\ x_3\neq -(x_1+x_2)}}\omega^{-\mathrm{tr}_1^n(bx_3^d)}$$
$$=-\sum_{x_1,x_2\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n(b(x_1^d+x_2^d))}\Big[\sum_{x_3\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n(bx_3^d)}-\omega^{\mathrm{tr}_1^n(b(x_1+x_2)^d)}\Big]-\sum_{x_1\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n(bx_1^d)}\omega^{\mathrm{tr}_1^n(bx_1^d)}.$$

Note that the last term is the compensation term for the case of $x_1 + x_2 = 0$. Thus we have

$$\sum_{\tau=0}^{p^n-2} C_l^3(\tau) = p^n \sum_{x_1, y \in F_{p^n}^*} \omega^{-\mathrm{tr}_1^n(bx_1^d(1+y^d-(1+y)^d))} + \Big(\sum_{\tau=0}^{p^n-2} C_l(\tau) \Big)^3 - (p^{2n} - p^n)$$

where $y = x_2/x_1$.
From Lemma 6 and Theorem 8, we know that

$$1 + x^d - (1+x)^d = \begin{cases} 0, & p^{2k}-1 \text{ times} \\ \beta^u, & \frac{(p^{2k}-1)(p^{2k}+3)}{4} \text{ times} \\ \beta^u \alpha^i, & \frac{3(p^{2k}-1)}{2} \text{ times for each nonzero } i \end{cases} \quad (20)$$

as x varies over $F_{p^n}^*$, where $1 \le i < (p^{2k}+1)/2$ and u is some integer in $0 \le u < 2(p^{2k}-1)$.
Thus, from (20), the summation of the cubic power of cross-correlation values can be derived as

$$\sum_{\tau=0}^{p^n-2} C_l^3(\tau) = \begin{cases} p^n\{(p^{2k}-1)(p^n-1) + \frac{(p^{2k}-1)(p^{2k}+3)}{4} A_0 + \\ \qquad \frac{3(p^{2k}-1)^2}{4} A_1\} - A_0^3 - (p^{2n} - p^n), & \text{if } l = 0 \\ p^n\{(p^{2k}-1)(p^n-1) + \frac{3(p^{2k}-1)}{2} A_0 + \\ \qquad \frac{(p^{2k}-1)(2p^{2k}-3)}{2} A_1\} - A_1^3 - (p^{2n} - p^n), & \text{otherwise} \end{cases}$$

where $A_0 = (p^n - p^{2k} - 2)/2$ and $A_1 = -p^{2k} - 1$. □

Using Theorems 2, 3, 4, and 9, the cross-correlation distribution of $s(t)$ and $s(dt+l)$ can be derived as in the following theorem.

Theorem 10: Let p be an odd prime, $n = 4k$, and $d = ((p^{2k}+1)/2)^2$. The cross-correlation distribution between a p-ary m-sequence $s(t)$ and its decimated sequences $s(dt+l)$, $0 \le l < (p^{2k}+1)/2$, is given as:

For $l = 0$,

$$C_l(\tau) = \begin{cases} -1, & \frac{(\sqrt{p^n}+1)(5\sqrt{p^n}-9)}{8} \text{ times} \\ -1-\sqrt{p^n}, & \frac{p^n-1}{4} \text{ times} \\ -1+\sqrt{p^n}, & \frac{\sqrt{p^n}+1}{2} \text{ times} \\ -1+2\sqrt{p^n}, & \frac{p^n-1}{8} \text{ times} \end{cases}$$

and otherwise,

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

as τ varies over $0 \le \tau < p^n - 1$. □

ACKNOWLEDGMENT

This research was supported by the MIC, Korea, under the ITRC support program and by the MOE, the MOCIE, and the MOLAB, Korea, through the fostering project of the Laboratory of Excellency.

REFERENCES

[1] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. 14, pp. 154–156, Jan. 1968.
[2] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Sci. Lab., Univ. Illinois, Urbana-Champaign, Tech. Rep. R-285 (AD 632574), 1996.
[3] J.-S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inf. Theory*, vol. 35, no. 2, pp. 371–379, Mar. 1989.
[4] J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth, "New family of p-ary sequences with optimal correlation property and large linear span," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1839–1844, Aug. 2004.
[5] H. M. Trachtenberg, "On the cross-correlation functions of maximal recurring sequences," *Ph.D. dissertation*, Univ. of Southern California, Los Angeles, CA, 1970.
[6] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, pp. 209–232, 1976.
[7] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 603–616, May 1991.
[8] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen, "Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1473–1481, May 2001.
[9] 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.
[10] 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.
[11] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397–399, May 1974.
[12] E.-Y. Seo, Y.-S. Kim, J.-S. No, and D.-J. Shin, "Cross-correlation distribution of p-ary m-sequence and its $p+1$ decimated sequences with shorter period," submitted to *IEEE Trans. Inf. Theory*, May 2006.
[13] T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics*. Chicago, IL: Markham, 1967.