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, Young-Sik Kim, Jong-Seon No, *Member, IEEE*, and Dong-Joon Shin, *Member, IEEE*

***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.**

***Index Terms*—p-ary m-sequences, cross-correlation, cross-correlation distribution, decimation, sequences.**

I. Introduction

FOR the past decades, many families of sequences with good cross-correlation property have been found by Gold [1], Kasami [2], No and Kumar [3], and Jang, Kim, No, and Helleseth [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]–[7].

However, the decimation factor d does not have to be relatively prime to the period of m-sequence to construct a family of p-ary sequences of period p^n-1 with family size p^n from $s(t)$ and $s(dt)$. There are some research results dealing with a decimation factor d which is not relatively prime to the period p^n-1 by Ness, Helleseth, and Kholosha [8], Kumar and Moreno [9], Müller [10], and Hu *et al.* [11]. In [8], the cross-correlation distribution between ternary m-sequence $s(t)$ and its decimated sequences $s(dt)$ and $s(dt+1)$ with $d=(3^k+1)/2$, where k is odd and $\gcd(n,k)=1$, has been found. Kumar and Moreno [9] derived the cross-correlation values between $s(t)$ and $s(dt)$ with $d=p^k+1$, where $n/\gcd(n,k)$ is odd. In this case, $\gcd(d,p^n-1)$ is 2 and the maximum magnitude of the cross-correlation values of these sequences is $\sqrt{p^n}+1$, which is optimal with respect to the Welch bound [12]. Furthermore, in Theorem 4 of [10], Müller found an upper bound on the cross-correlation values between the sequence $s(t)$ and only one decimated sequence $s(dt)$ when n is even, $n/\gcd(n,k)$ is not divisible by 4, and d is p^k+1. In [11], Hu *et al.* generalized the result in [10]. Seo, Kim, No, and Shin [13] extended the results by Müller [10] to derive the cross-correlation distribution of $s(t)$ and $s(dt+l)$, $0\le l<p+1$.

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, which extends the result in [14], 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.

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

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

where $x\in F_{p^n}$ and $m|n$. The trace function satisfies the following properties:

1) $\mathrm{tr}_m^n(ax+by)=a\mathrm{tr}_m^n(x)+b\mathrm{tr}_m^n(y)$, for all $a,b\in F_{p^m}$, $x,y\in F_{p^n}$;
2) $\mathrm{tr}_m^n(x^{p^m})=\mathrm{tr}_m^n(x)$, for all $x\in F_{p^n}$.

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 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:

- p is an odd prime;
- $n=4k$, where k is a positive integer;
- $d=((p^{2k}+1)/2)^2$;
- $F_{p^n}^*=F_{p^n}\backslash\{0\}$;

Manuscript received November 29, 2006; revised December 19, 2007. This work was supported by the MEST, the MKE, and the MOLAB, Korea, through the fostering project of the Laboratory of Excellency. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Nice, France, June 2007.

E.-Y. Seo is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: eunyoung00@gmail.com).

Y.-S. Kim is with Samsung Electronics, Co., Ltd., Yongin, Gyeonggi-do, 446-711, Korea (e-mail: mypurist@gmail.com).

J.-S. No is with the Department of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea (e-mail: jsno@snu.ac.kr).

D.-J. Shin is with the Department of Electronics and Computer Engineering, Hanyang University, Seoul 133-791, Korea (e-mail: djshin@hanyang.ac.kr).

Communicated by G. Gong, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2008.924694

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

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 $\gcd((p^{2k}+1)/2, 2(p^{2k}-1)) = 1$;
- $\beta^{p^{2k}} = -\beta$ and $\beta^d = -\beta$;
- $\gamma^{p^{2k}} = \gamma^{-1}$ 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 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

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

where ω is a primitive complex pth 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 subsequent theorem.

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

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

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 as 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

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

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

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

From Lemma 1, (3) can be given as

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

and thus

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

Using $\alpha = \beta\gamma$, (4) can be rewritten as

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

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

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

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

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

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

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

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

Note that $(-1)^j\gamma^j$ covers all distinct elements as j takes the value in $\{0, 1, \ldots, p^{2k}\}$ 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

$$2(p^{2k}-1)(a_1+a_2) = (p^{2k}-1)\tau \bmod (p^{4k}-1). \tag{9}$$

Therefore, we also have

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

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

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

Clearly, the inner summation is equal to -1. Thus, we have

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

Let

$$A(b)=\sum_{x\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n(bx^d)}.$$

Since d is odd and $\gcd((p^{2k}+1)/2, 2(p^{2k}-1))=1$, we have

$$A(b)=\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(bx^d)}=\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(bx^{\frac{p^{2k}+1}{2}})}.$$

Let $x=y^2$ for square x and otherwise, $x=zy^2$, where z is a nonsquare in F_{p^n}. Then we have

$$2(1+A(b))=\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(by^{p^{2k}+1})}+\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(bz^{\frac{p^{2k}+1}{2}}y^{p^{2k}+1})}. \tag{10}$$

From Lemma 1, the first summation is given as

$$\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(by^{p^{2k}+1})}=-p^{\frac{n}{2}} \tag{11}$$

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

$$bz^{\frac{p^{2k}+1}{2}}+(bz^{\frac{p^{2k}+1}{2}})^{p^{2k}}=0. \tag{12}$$

Using $z^{p^{2k}(p^{2k}+1)/2}=-z^{(p^{2k}+1)/2}$, (12) reduces to

$$b^{p^{2k}-1}=1$$

which means that b has to be 1. Then the second summation is given as

$$\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(bz^{\frac{p^{2k}+1}{2}}y^{p^{2k}+1})}=\begin{cases}p^n, & \text{if } b=1, \text{ i.e., } l=0\\ -p^{\frac{n}{2}}, & \text{otherwise.}\end{cases} \tag{13}$$

Plugging (11) and (13) into (10), $A(b)$ can be obtained as

$$A(b)=\begin{cases}\frac{p^n-p^{\frac{n}{2}}}{2}-1, & \text{if } b=1, \text{ i.e., } l=0\\ -p^{\frac{n}{2}}-1, & \text{otherwise}\end{cases} \tag{14}$$

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

$$\begin{aligned}&\sum_{\tau=0}^{p^n-2} C_l^2(\tau)\\&\quad=\sum_{a\in F_{p^n}^*}\sum_{x_1\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(ax_1-bx_1^d)}\sum_{x_2\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(ax_2-bx_2^d)}\\&\quad=\sum_{x_1\in F_{p^n}^*}\sum_{x_2\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(b\left(x_1^d+x_2^d\right)\right)}\sum_{a\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(a(x_1+x_2))}.\end{aligned}$$

The innermost summation is given as

$$\begin{cases}p^n-1, & \text{if } x_1=-x_2\\ -1, & \text{otherwise.}\end{cases}$$

Thus, we have

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

Let

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

Using $A(b)$ defined in the proof of Theorem 3, $B(b)$ can be computed as

$$\begin{aligned}B(b) &= \sum_{x_1 \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(bx_1^d)} \sum_{x_2 \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(bx_2^d)} - (p^n-1) \\ &= A^2(b) - p^n + 1\end{aligned}$$

and from (14), we have

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

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 $f: x \to x^d$ 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 following relations can be obtained:

$$f(\beta^{2u}\gamma^t) = \beta^{2ud}\gamma^{td} = \beta^{2u}$$

$$f(\beta^{2u+1}\gamma^t) = \beta^{2ud+d}\gamma^{td} = -\beta^{2u+1}.$$ □

Lemma 6: All the solutions of

$$1 + x^d - (1+x)^d = 0, \quad x \in F_{p^n} \tag{15}$$

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

Proof: Clearly, for an integer $u, 0 \le u < p^{2k}-1$, $\beta^{2u} \in F_{p^{2k}}^*$ and $\beta^{2u+1} \notin F_{p^{2k}}^*$. It can be easily shown that if one of x^d and $(1+x)^d$ is of the form β^{2u+1} and the other is of the form β^{2u}, (15) cannot be satisfied. Also, if they are β^{2u_1+1} and β^{2u_2+1}, (15) can be rewritten as $\beta(\beta^{2u_2} - \beta^{2u_1}) = 1$, which is impossible, because the left-hand side of it is not in $F_{p^{2k}}^*$. Thus, both x^d and $(1+x)^d$ should be the elements of $F_{p^{2k}}$ to satisfy (15). It is clear that $x = -1$ is a solution of (15). Suppose that $x \ne -1$. Then (15) 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 (15) should be given as

$$x = (\beta^{2u}-1)\gamma^{t_1} = \beta^{2u}\gamma^{t_2} - 1. \tag{16}$$

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

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

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 (17) gives us

$$1 = \left(\frac{1-\gamma^{t_1}}{\gamma^{t_2}-\gamma^{t_1}}\right)^{p^{2k}-1} = \frac{\gamma^{t_2}-\gamma^{t_1}}{1-\gamma^{t_1}} \cdot \frac{1-\gamma^{-t_1}}{\gamma^{-t_2}-\gamma^{-t_1}} = \gamma^{t_2}. \tag{18}$$

From (16) and (18), we have $t_1 = t_2 = 0$, which contradicts $t_1 \ne t_2$. Therefore, we have $t_1 = t_2 = 0$ and $x = \beta^{2u}-1$. Thus, including $x = -1$, all the solutions of (15) 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: If there exists a solution e for $i = 0$, we have $1 + \beta^{2e+1} = \beta^u$. However, if $u = 2u'$, $\beta^{2u'} - 1$ is an element in $F_{p^{2k}}$ and β^{2e+1} is not an element in $F_{p^{2k}}$, and if $u = 2u'+1$, $\beta(\beta^{2u'} - \beta^{2e})$ is not an element in $F_{p^{2k}}$. Therefore, we can assume that $i \ne 0$ for all e.

Next, suppose that for the same i, we have

$$\begin{aligned}1 + \beta^{2e_1+1} &= \beta^{u_1}\alpha^i \\ 1 + \beta^{2e_2+1} &= \beta^{u_2}\alpha^i\end{aligned}$$

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

$$\left(\frac{1+\beta^{2e_1+1}}{1+\beta^{2e_2+1}}\right)^{2(p^{2k}-1)} = \beta^{(u_1-u_2)2(p^{2k}-1)}$$

and by using $\beta^{p^{2k}-1} = -1$, it can be expressed as

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

This can be simplified as

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

Since $e_1 \ne e_2$, 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 $i \ne 0$, there exist a pair of e_1 and $p^{2k}-2-e_1$ for e to satisfy $1+\beta^{2e+1} = \beta^u\alpha^i$. □

Since the number of solutions for $1 + x^d - (1+x)^d = 0$ is already obtained in Lemma 6, 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

$$1 + x^d - (1+x)^d = \beta^u\alpha^i, \quad x \in F_{p^n}^* \tag{19}$$

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 $i \ne 0$, where u is some integer in $0 \le u < 2(p^{2k}-1)$.

Proof: The proof is given in Section V. □

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

Theorem 9: The statement of the theorem is given in the first expression at the bottom of the page.

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

$$\begin{aligned}\sum_{\tau=0}^{p^n-2} C_l^3(\tau) &= \sum_{a\in F_{p^n}^*}\Big(\sum_{x_1\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(ax_1-bx_1^d)}\\ &\quad\times\sum_{x_2\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n\left(ax_2-bx_2^d\right)}\sum_{x_3\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n\left(ax_3-bx_3^d\right)}\Big)\\ &= \sum_{x_1\in F_{p^n}^*}\sum_{x_2\in F_{p^n}^*}\sum_{x_3\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(b\left(x_1^d+x_2^d+x_3^d\right)\right)}\\ &\quad\times\sum_{a\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(a(x_1+x_2+x_3))}\\ &= (p^n-1)\sum_{\substack{x_1,x_2,x_3\in F_{p^n}^*\\ x_1+x_2+x_3=0}}\omega^{-\mathrm{tr}_1^n\left(b\left(x_1^d+x_2^d+x_3^d\right)\right)}\\ &\quad-\sum_{\substack{x_1,x_2,x_3\in F_{p^n}^*\\ x_1+x_2+x_3\neq 0}}\omega^{-\mathrm{tr}_1^n(b(x_1^d+x_2^d+x_3^d))}.\end{aligned}$$

The first summation in the above equation becomes

$$\begin{aligned}&(p^n-1)\sum_{\substack{x_1,x_2,x_3\in F_{p^n}^*\\ x_1+x_2+x_3=0}}\omega^{-\mathrm{tr}_1^n\left(b\left(x_1^d+x_2^d+x_3^d\right)\right)}\\ &\quad=(p^n-1)\sum_{\substack{x_1,x_2\in F_{p^n}^*\\ x_3=-(x_1+x_2)\neq 0}}\omega^{-\mathrm{tr}_1^n\left(b\left(x_1^d+x_2^d+x_3^d\right)\right)}\\ &\quad=(p^n-1)\Big[\sum_{x_1,x_2\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(b\left(x_1^d+x_2^d-(x_1+x_2)^d\right)\right)}\\ &\qquad-(p^n-1)\Big].\end{aligned}$$

Using (14), the second summation can be represented as the second expression at the bottom of the page. Note that the last term is the compensation term for the case of $x_1+x_2=0$. Then, the equation can be rewritten as

$$\sum_{x_1,x_2\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(b\left(x_1^d+x_2^d-(x_1+x_2)^d\right)\right)}-A^3(b)-(p^n-1).$$

Thus, we have

$$\begin{aligned}\sum_{\tau=0}^{p^n-2} C_l^3(\tau) &= p^n\sum_{x_1,x_2\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(b\left(x_1^d+x_2^d-(x_1+x_2)^d\right)\right)}-A^3(b)\\ &\quad-(p^n-1)^2-(p^n-1)\\ &= p^n\sum_{x_1,y\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(bx_1^d(1+y^d-(1+y)^d)\right)}-A^3(b)\\ &\quad-(p^{2n}-p^n)\end{aligned}$$

where $y=x_2/x_1$.

From Lemma 6 and Theorem 8, we know that

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

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 the third expression at the bottom of the page, 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 follows.

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

$$\begin{aligned}&-\sum_{x_1\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(bx_1^d\right)}\sum_{x_2\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(bx_2^d\right)}\sum_{\substack{x_3\in F_{p^n}^*\\ x_3\neq-(x_1+x_2)}}\omega^{-\mathrm{tr}_1^n\left(bx_3^d\right)}\\ &\quad=-\sum_{x_1\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(bx_1^d\right)}\sum_{x_2\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(bx_2^d\right)}\Big[\sum_{x_3\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(bx_3^d\right)}-\omega^{\mathrm{tr}_1^n\left(b(x_1+x_2)^d\right)}\Big]-\sum_{x_1\in F_{p^n}^*}\omega^{-\mathrm{tr}_1^n\left(bx_1^d\right)}\omega^{\mathrm{tr}_1^n\left(bx_1^d\right)}.\end{aligned}$$

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

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 $0\le\tau<p^n-1$.

Proof: For $l=0$, let

$$C_l(\tau)=\begin{cases}-1, & D_1 \text{ times}\\ -1-p^{2k}, & D_2 \text{ times}\\ -1+p^{2k}, & D_3 \text{ times}\\ -1+2p^{2k}, & D_4 \text{ times.}\end{cases}$$

Then, we can derive the values of D_1, D_2, D_3, and D_4 by solving the following linear equations obtained from Theorems 2, 3, 4, and 9:

$$\begin{aligned}&D_1+D_2+D_3+D_4=p^n-1\\&(-1)D_1-(p^{2k}+1)D_2+(p^{2k}-1)D_3+(2p^{2k}-1)D_4\\&=\frac{-p^n+p^{\frac{n}{2}}}{2}+1\\&(-1)^2D_1+(p^{2k}+1)^2D_2+(p^{2k}-1)^2D_3+(2p^{2k}-1)^2D_4\\&=\frac{3p^{2n}+2p^{\frac{3n}{2}}-p^n-4p^{\frac{n}{2}}}{4}-1\\&(-1)^3D_1-(p^{2k}+1)^3D_2+(p^{2k}-1)^3D_3+(2p^{2k}-1)^3D_4\\&=\frac{3}{4}p^{2n+2k}-\frac{7}{4}p^{2n}-\frac{7}{4}p^{n+2k}+\frac{5}{4}p^n+\frac{3}{2}p^{2k}+1.\end{aligned}$$

For $l\neq 0$, the cross-correlation distribution can be similarly derived. □

Remark: Using the result of Theorem 10, a new family of p-ary sequences of period p^n-1 and family size p^{2k} with good correlation property can be constructed.

V. Proof of Theorem 8

We will prove Theorem 8 by considering the following cases.

Case 1) $i=0$:
- **Case 1-1)** x is a square and $1+x$ is a square;
- **Case 1-2)** x is a square and $1+x$ is a nonsquare;
- **Case 1-3)** x is a nonsquare and $1+x$ is a square;
- **Case 1-4)** x is a nonsquare and $1+x$ is a nonsquare.

Case 2) $i\neq 0$:
- **Case 2-1)** x is a square and $1+x$ is a square;
- **Case 2-2)** x is a square and $1+x$ is a nonsquare;
- **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.

Case 1) $i=0$:

We will show that there are $(p^{2k}-1)(p^{2k}+3)/4$ solutions x of (19) when $i=0$ by considering the following four cases.

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

There are $(p^n-5)/4$ elements x such that both x and $1+x$ are squares by the result for cyclotomic number of order 2 in [20, p. 30, Lemma 6]. 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 (19) is equal to 0 or β^u for some integer u in $0\le u<2(p^{2k}-1)$. Since x and $x+1$ are squares in this case, we have to exclude $x=0,-1$. Thus, by excluding the solutions of $1+x^d-(1+x)^d=0$, which are not 0 and -1, using Lemma 6, the number of square solutions x of (19) in this case is

$$\frac{p^{4k}-5}{4}-(p^{2k}-2)=\frac{(p^{2k}-1)(p^{2k}-3)}{4}.$$

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

First, we will show that when $x\in F_{p^n}^*$ is a square and $1+x$ a nonsquare, $1+x^d$ 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 will show that if $1+x^d$ is not equal to zero, i is not equal to zero by inducing a contradiction as follows. Suppose that $(1+x)^d=-\beta^{2u_1+1}$, $1+x^d=\beta^{2u_2}$, and $i=0$. Then we have $\beta^{2u_1+1}+\beta^{2u_2}=\beta^u$, which is impossible and the converse is proved.

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 above equation, we have

$$1=\frac{1-\gamma^{-t_1}}{\gamma^{-t_2}}\cdot\frac{\gamma^{t_2}}{1-\gamma^{t_1}}=-\gamma^{2t_2-t_1}.$$

Since the above equation cannot be satisfied, $1+x$ 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 (19) is $(p^{2k}-1)/2$.

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

We can easily derive the following three results using a similar method to that used in Case 1-2) by replacing x by $1+x$ and $1+x$ by x in Case 1-2), respectively. Note that -1 is a square.

i) When $x\in F_{p^n}^*$ is a nonsquare and $1+x$ is a square, $1-(1+x)^d$ is equal to 0 if and only if i is equal to 0.
ii) If x satisfies $1-(1+x)^d=0$, x is a nonsquare.
iii) There are $(p^{2k}-1)/2$ nonsquare solutions x in $F_{p^n}^*$ of $(1+x)^d=1$ because $x=0$ should be excluded.

Therefore, in this case, the number of nonsquare solutions x of (19) 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 will show that if $x^d - (1+x)^d$ is not equal to zero, i is not equal to 0 by inducing a contradiction as follows. Suppose that $x^d = -\beta^{2u_1+1}$, $(1+x)^d = -\beta^{2u_2+1}$, and $i = 0$. Then we have $1 - \beta^{2u_1+1} + \beta^{2u_2+1} = \beta^u$, $u_1 \neq u_2$, which is impossible and the converse is proved.

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

$$\beta^{2u_1+1} = \frac{1}{\gamma^{t_2} - \gamma^{t_1}}. \tag{21}$$

Raising the power $p^{2k} - 1$ to both sides of the above equation, we have $-1 = (1/(\gamma^{t_2} - \gamma^{t_1}))^{p^{2k}-1} = -\gamma^{t_1+t_2}$, which implies $t_1 = -t_2$. Also, we will show that u_1 satisfying (21) 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', (21) 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, the above equation cannot be satisfied because $\gamma^{-(t_1+t_1')} \neq -1$. Since t_1 varies over $1 \leq t_1 < (p^{2k}+1)/2$, in this case, the number of nonsquare solutions x of (19) 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 (19) 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 (19).

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, $0 \leq u_1, u_2 < p^{2k} - 1$, satisfying

$$1 + x^d = \beta^{2u_1}, \quad (1+x)^d = -\beta^{2u_2+1}. \tag{22}$$

Then, we have

$$\beta^{2u_1} + \beta^{2u_2+1} = \beta^u \alpha^i. \tag{23}$$

Now, we will show that there are $(p^{2k}-1)/2$ solutions x of (19) for each i, $1 \leq i < (p^{2k}+1)/2$, by the following three steps.

- Step 1: It will be proved that the mapping from x to (u_1, u_2) given in (22) is one-to-one.
- Step 2: For each i, $1 \leq i < (p^{2k}+1)/2$, it will be proved that there are $(p^{2k}+1)/2$ possible solutions (u_1, u_2) satisfying (22) and (23).
- Step 3: For each i, $1 \leq i < (p^{2k}+1)/2$, it will be proved that exactly one possible solution in Step 2 cannot satisfy (22) and (23).

Step 1: By Lemma 5, for some t_1 and t_2, the solution x of (22) is obtained as

$$x = (\beta^{2u_1} - 1)\gamma^{t_1} = \beta^{2u_2+1}\gamma^{t_2} - 1. \tag{24}$$

In order to show that the mapping from x to (u_1, u_2) in (22) is one-to-one, it is enough to show that for the fixed (u_1, u_2) satisfying (22), there exists only one pair (t_1, t_2) satisfying (24). Suppose that there exists another (t_1', t_2') for the same (u_1, u_2) satisfying (24) such that

$$x = (\beta^{2u_1} - 1)\gamma^{t_1'} = \beta^{2u_2+1}\gamma^{t_2'} - 1. \tag{25}$$

By dividing (24) by (25) and raising the power $p^{2k}+1$ to both sides, we have

$$1 = \left(\frac{\beta^{2u_2+1}\gamma^{t_2} - 1}{\beta^{2u_2+1}\gamma^{t_2'} - 1}\right)^{p^{2k}+1} = \frac{-\beta^{2u_2+1}\gamma^{-t_2} - 1}{-\beta^{2u_2+1}\gamma^{-t_2'} - 1} \cdot \frac{\beta^{2u_2+1}\gamma^{t_2} - 1}{\beta^{2u_2+1}\gamma^{t_2'} - 1}.$$

It can be simplified to $\gamma^{-t_2-t_2'}(\gamma^{t_2'} - \gamma^{t_2}) = -(\gamma^{t_2'} - \gamma^{t_2})$. If $t_2 \neq t_2'$, $\gamma^{-t_2-t_2'} = -1$, which is impossible. Thus, there exists only one pair of (t_1, t_2) for a fixed (u_1, u_2) in (24) and (22) is a one-to-one mapping from x to (u_1, u_2).

Step 2: For each i, $1 \leq i < (p^{2k}+1)/2$, we will count the number of pairs (u_1, u_2) satisfying (22) (or (24)) and (23). Equation (23) can be rewritten as

$$\beta^{2u_1}(1 + \beta^{2(u_2-u_1)+1}) = \beta^u \alpha^i$$

and letting $e_1 = u_2 - u_1$, we have

$$1 + \beta^{2e_1+1} = \beta^{u-2u_1}\alpha^i. \tag{26}$$

Also, (24) can be rewritten as

$$(\beta^{2u_1} - 1)\gamma^{t_1} = \beta^{2(u_1+e_1)+1}\gamma^{t_2} - 1$$

which can be modified as

$$\beta^{2u_1} = \frac{1 - \gamma^{t_1}}{\beta^{2e_1+1}\gamma^{t_2} - \gamma^{t_1}}. \tag{27}$$

From Step 1, we know that u_1 takes different value for each possible pair (t_1, t_2) in (27). From Lemma 7, we already know that $1+\beta^{2e_1+1}$ and $1+\beta^{2(p^{2k}-2-e_1)+1}$ in (26) can be expressed using the same i. Thus, for the fixed e_1 and $p^{2k}-2-e_1$, we have to count the number of pairs (t_1, t_2) such that the right-hand side of (27) becomes the element of $F_{p^{2k}}^*$, which satisfies (27) for some u_1. Note that t_1 in (27) cannot be zero.

First, consider the case of fixed e_1. By raising the power $p^{2k}-1$ to both sides of (27), we need to find the number of solutions (t_1, t_2) for

$$1 = \left(\frac{1 - \gamma^{t_1}}{\beta^{2e_1+1}\gamma^{t_2} - \gamma^{t_1}}\right)^{p^{2k}-1} = \frac{1 - \gamma^{-t_1}}{-\beta^{2e_1+1}\gamma^{-t_2} - \gamma^{-t_1}} \cdot \frac{\beta^{2e_1+1}\gamma^{t_2} - \gamma^{t_1}}{1 - \gamma^{t_1}}$$

which can be modified as

$$\beta^{2e_1+1}\gamma^{t_2} - \gamma^{t_1} - \beta^{2e_1+1}\gamma^{t_2-t_1} = -\beta^{2e_1+1}\gamma^{-t_2} + \beta^{2e_1+1}\gamma^{t_1-t_2} - \gamma^{-t_1}.$$

By multiplying $\gamma^{t_1+t_2}$ to both sides, it can be rewritten as

$$\beta^{2e_1+1}(\gamma^{t_1} - \gamma^{2t_2})(\gamma^{t_1} - 1) = (\gamma^{t_1} - 1)(\gamma^{t_1} + 1)\gamma^{t_2}. \tag{28}$$

Since $t_1 \neq 0$, from (28), we can derive the following equation:

$$\begin{aligned}\gamma^{t_1} &= \frac{\beta^{2e_1+1}\gamma^{2t_2}+\gamma^{t_2}}{\beta^{2e_1+1}-\gamma^{t_2}} = \frac{\beta^{2e_1+1}\gamma^{t_2}+1}{\beta^{2e_1+1}\gamma^{-t_2}-1} \\ &= -(\beta^{2e_1+1}\gamma^{-t_2}-1)^{p^{2k}-1} \\ &= \{(\delta^{\frac{p^{2k}+1}{2}}(\beta^{2e_1+1}\gamma^{-t_2}-1)\}^{p^{2k}-1}. \end{aligned} \tag{29}$$

Note that γ^{t_1} is $(\delta^{2t_1})^{p^{2k}-1}$ and $\delta^{(p^{2k}+1)/2}$ is a nonsquare. Thus, we have to calculate the number of t_2, which makes $\beta^{2e_1+1}\gamma^{-t_2}-1$ a nonsquare. Since t_1 is not equal to 0, the power v in $\beta^{2e_1+1}\gamma^{-t_2}-1=\delta^v$ should not be an odd integer multiple of $(p^{2k}+1)/2$ to make the right-hand side of (29) not equal to 1, which will be considered in Step 3.

Second, we should also consider the case of the fixed $p^{2k}-2-e_1$ by replacing e_1 by $p^{2k}-2-e_1$ in (29). Therefore, we will consider the following two elements obtained for the fixed e_1 and $p^{2k}-2-e_1$:

$$\begin{cases} \beta^{2e_1+1}\gamma^{-t_2}-1, & \text{for } e_1 \\ \beta^{-2e_1-1}\gamma^{-t_2'}-1, & \text{for } p^{2k}-2-e_1. \end{cases} \tag{30}$$

From

$$\beta^{2e_1+1}\gamma^{-t_2}-1 = -\beta^{2e_1+1}\gamma^{-t_2}(\beta^{-2e_1-1}\gamma^{t_2}-1)$$

it is clear that if $\beta^{2e_1+1}\gamma^{-t_2}-1$ is a nonsquare (or square), $\beta^{-2e_1-1}\gamma^{t_2}-1$ is a square (or nonsquare) because $-\beta^{2e_1+1}\gamma^{-t_2}$ is a nonsquare. Therefore, in (30), if $\beta^{2e_1+1}\gamma^{-t_2}-1$ is a nonsquare for some t_2, $\beta^{-2e_1-1}\gamma^{-t_2'}-1$ is a square for $t_2'=-t_2$ and *vice versa*. Let

$$T = \left\{0,1,2,\ldots,\frac{p^{2k}-1}{2}\right\} \bmod \frac{p^{2k}+1}{2}.$$

For each e_1, let T_2 and $T_2' \subseteq T$ be the sets of t_2 and t_2' such that $\beta^{2e_1+1}\gamma^{-t_2}-1$ and $\beta^{-2e_1-1}\gamma^{-t_2'}-1$ are nonsquares, respectively. Then, it is clear that $T_2 \cup T_2' = T$ and $T_2 \cap T_2' = \phi$. Thus, the total number of t_2 and t_2', $0 \le t_2, t_2' < (p^{2k}+1)/2$, which make $\beta^{2e_1+1}\gamma^{-t_2}-1$ and $\beta^{-2e_1-1}\gamma^{-t_2'}-1$ nonsquares is $(p^{2k}+1)/2$. Therefore, it is proved that there are $(p^{2k}+1)/2$ possible solutions (u_1,u_2) satisfying (22) and (23) for each i.

Step 3: We will show that for each e_1 and $p^{2k}-2-e_1$, only one element among $(p^{2k}+1)/2$ possible solutions $T_2 \cup T_2'$ obtained in Step 2 should be excluded, which corresponds to a nonsquare $\beta^{2e_1+1}\gamma^{-t_2}-1 = \delta^{\frac{p^{2k}+1}{2}}w = \beta^w$ with odd integer w as mentioned in Step 2.

Suppose that the following is satisfied for some e_1, $0 \le e_1 < p^{2k}-1$, and t_2, $0 \le t_2 < (p^{2k}+1)/2$:

$$\beta^{2e_1+1}\gamma^{-t_2}-1 = \beta^{2s+1}. \tag{31}$$

Since it is clear that (31) cannot be satisfied for $t_2=0$, we do not consider $t_2=0$.

Claim 1: For each nonzero t_2, there exists distinct e_1 satisfying (31).

Proof: By raising the power $p^{2k}-1$ to both sides of (31) for $t_2 \neq 0$, we have

$$(\beta^{2e_1+1}\gamma^{-t_2}-1)^{p^{2k}-1} = \frac{-\beta^{2e_1+1}\gamma^{t_2}-1}{\beta^{2e_1+1}\gamma^{-t_2}-1} = -1$$

which can be simplified as

$$\beta^{2e_1+1} = \frac{2\gamma^{t_2}}{1-\gamma^{2t_2}}. \tag{32}$$

Since $(2\gamma^{t_2}/(1-\gamma^{2t_2}))^{p^{2k}-1} = -1$, there exists e_1 satisfying (32) for any t_2, $1 \le t_2 < (p^{2k}+1)/2$. Also, suppose that t_3, $t_3 \neq t_2$, also satisfies (32) for the same e_1. Then, we have $\gamma^{t_2+t_3} = -1$, which is impossible. Thus, we have distinct e_1, $0 \le e_1 < p^{2k}-1$, for each t_2, $1 \le t_2 < (p^{2k}+1)/2$. It is clear that for the half of e_1 in $0 \le e_1 < p^{2k}-1$, there is no t_2 satisfying (31). □

Claim 2: For each e_1, if there exists t_2 satisfying (31), there does not exist t_4 satisfying $\beta^{-2e_1-1}\gamma^{-t_4}-1 = \beta^{2s'+1}$ for some positive integer s' and *vice versa*.

Proof: Suppose that there exist t_2 and t_4 satisfying $\beta^{2e_1+1}\gamma^{-t_2}-1 = \beta^{2s+1}$ and $\beta^{-2e_1-1}\gamma^{-t_4}-1 = \beta^{2s'+1}$, respectively. Then, from (32), we can obtain

$$\frac{2\gamma^{t_2}}{1-\gamma^{2t_2}} = \frac{1-\gamma^{2t_4}}{2\gamma^{t_4}}.$$

By solving this equation, we have

$$\gamma^{t_2} = \frac{1-\gamma^{t_4}}{1+\gamma^{t_4}} \text{ or } \frac{\gamma^{t_4}+1}{\gamma^{t_4}-1}. \tag{33}$$

However, (33) is impossible because $(1-\gamma^{t_4})/(1+\gamma^{t_4})$ and $(\gamma^{t_4}+1)/(\gamma^{t_4}-1)$ are not elements of the form γ^{t_2}, which can be proved by raising the power $p^{2k}-1$ to both sides of (33). □

Because e_1 can take twice as many values as t_2, from *Claims 1* and *2*, for each pair of e_1 and $p^{2k}-2-e_1$, there exists only one element in $T_2 \cup T_2'$ satisfying (31), which should be excluded from the $(p^{2k}+1)/2$ possible solutions obtained in Step 2. Thus, the sum of the number of solutions t_2 of (29) for e_1 and the number of solutions t_2' of (29) for $p^{2k}-2-e_1$ is $(p^{2k}-1)/2$. Then, from Lemma 7 and the one-to-one mapping property between (u_1,u_2) and (t_1,t_2) by Step 1, there are $(p^{2k}-1)/2$ solutions (u_1,u_2) of (23) for each i. Thus, we can conclude that, in this case, the number of solutions x of (19) is $(p^{2k}-1)/2$ for each i, $1 \le i < (p^{2k}+1)/2$.

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

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

$$x^d = -\beta^{2u_1+1}, \quad 1-(1+x)^d = \beta^{2u_2}. \tag{34}$$

Then, we have

$$-\beta^{2u_1+1}+\beta^{2u_2} = \beta^u\alpha^i. \tag{35}$$

In this case, the number of solutions of (19) can be obtained similarly to the Case 2-2) as follows.

Step 1: The mapping from x to (u_1,u_2) given in (34) is one-to-one, which can be similarly proved as for Step 1 in Case2-2).

Step 2: (35) can be rewritten as

$$\beta^{2u_2}(1+\beta^{2(u_1-u_2+\frac{p^{2k}-1}{2})+1}) = \beta^u\alpha^i.$$

Let $e_1 = u_1 - u_2 + (p^{2k}-1)/2$. From (34) and Lemma 5, we have

$$\beta^{2(u_2+e_1-\frac{p^{2k}-1}{2})+1}\gamma^{t_1} = (1-\beta^{2u_2})\gamma^{t_2} - 1$$

which is modified as

$$\beta^{2u_2} = \frac{1-\gamma^{t_2}}{\beta^{2e_1+1}\gamma^{t_1} - \gamma^{t_2}}. \tag{36}$$

It is clear that $t_2 \neq 0$. Similarly to the Step 2 in Case 2-2), for the fixed e_1 and $p^{2k}-2-e_1$, we have to count the number of (t_1, t_2) such that the right-hand side of (36) becomes an element of $F^*_{p^{2k}}$. Note that t_2 cannot be zero for (36). Thus, we need to find the number of solutions (t_1, t_2) for

$$\begin{aligned} 1 &= \Big(\frac{1-\gamma^{t_2}}{\beta^{2e_1+1}\gamma^{t_1}-\gamma^{t_2}}\Big)^{p^{2k}-1} \\ &= \frac{1-\gamma^{-t_2}}{-\beta^{2e_1+1}\gamma^{-t_1}-\gamma^{-t_2}} \cdot \frac{\beta^{2e_1+1}\gamma^{t_1}-\gamma^{t_2}}{1-\gamma^{t_2}} \end{aligned}$$

which can be modified as

$$\begin{aligned} &\beta^{2e_1+1}\gamma^{t_1} - \gamma^{t_2} - \beta^{2e_1+1}\gamma^{t_1-t_2} \\ &\qquad = -\beta^{2e_1+1}\gamma^{-t_1} + \beta^{2e_1+1}\gamma^{t_2-t_1} - \gamma^{-t_2}. \end{aligned}$$

By multiplying $\gamma^{t_1+t_2}$ to both sides and combining terms, we have

$$\beta^{2e_1+1}(\gamma^{2t_1}-\gamma^{t_2})(\gamma^{t_2}-1) = \gamma^{t_1}(\gamma^{t_2}-1)(\gamma^{t_2}+1). \tag{37}$$

Since $t_2 \neq 0$, (37) can be represented as

$$\gamma^{t_2} = \frac{1-\beta^{2e_1+1}\gamma^{t_1}}{1+\beta^{2e_1+1}\gamma^{-t_1}} = (1+\beta^{2e_1+1}\gamma^{-t_1})^{p^{2k}-1}. \tag{38}$$

Then, we have to count the number of t_1 which makes $1+\beta^{2e_1+1}\gamma^{-t_1}$ a square. Similarly to the Step 2 in Case 2-2), it can be shown that the sum of the number of t_1's making $1+\beta^{2e_1+1}\gamma^{-t_1}$ a square for e_1 and the number of t_1''s making $1+\beta^{-2e_1-1}\gamma^{-t_1'}$ a square for $p^{2k}-2-e_1$ is $(p^{2k}+1)/2$.

Step 3: Among $(p^{2k}+1)/2$ solutions of (38), we will show that there is only one pair of (t_1, t_2) satisfying $\gamma^{2t_1} - \gamma^{t_2} = 0$, which does not satisfy (37). Assume that $\gamma^{2t_1} = \gamma^{t_2}$. Then, from (38), we have

$$\beta^{2e_1+1} = \frac{\gamma^{-t_1}-\gamma^{t_1}}{2}. \tag{39}$$

Similarly to *Claim 1* in Step 3 of Case 2-2), it can be easily checked that there exists distinct e_1 for each of $(p^{2k}-1)/2$ nonzero t_1's. Suppose that t_1 and e_1 satisfy (39) and also t_1', $t_1' \neq t_1$, and $p^{2k}-2-e_1$ satisfy (39). Then, we can obtain $(\gamma^{-t_1}-\gamma^{t_1})/2 = 2/(\gamma^{-t_1'}-\gamma^{t_1'})$. By solving this equation, we have

$$\gamma^{t_1'} = \frac{1-\gamma^{t_1}}{1+\gamma^{t_1}} \text{ or } \frac{\gamma^{t_1}+1}{\gamma^{t_1}-1}.$$

However, this is impossible and thus, in this case, the number of nonsquare solutions x of (19) is $(p^{2k}-1)/2$ for each i, $1 \leq i < (p^{2k}+1)/2$.

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

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

$$x^d = -\beta^{2u_1+1}, \quad (1+x)^d = -\beta^{2u_2+1}. \tag{40}$$

Then, we have

$$1 - \beta^{2u_1+1} + \beta^{2u_2+1} = \beta^u\alpha^i \tag{41}$$

where $u_1 \neq u_2$. In this case, the number of solutions of (19) can be obtained similarly to the Case 2-2) as follows.

Step 1: The mapping from x to (u_1, u_2) given in (40) is one-to-one, which can be similarly proved as for the Step 1 in Case 2-2).

Step 2: Let $\beta^{2u_2} - \beta^{2u_1} = \beta^{2e_1}$. From (40) and Lemma 5, we can derive

$$\beta^{2u_1+1} = \frac{\gamma^{t_2}\beta^{2e_1+1}-1}{\gamma^{t_1}-\gamma^{t_2}}$$

where $t_1 \neq t_2$. By raising the power $p^{2k}-1$ to both sides of this equation, we have

$$-1 = \frac{-\gamma^{-t_2}\beta^{2e_1+1}-1}{\gamma^{-t_1}-\gamma^{-t_2}} \cdot \frac{\gamma^{t_1}-\gamma^{t_2}}{\gamma^{t_2}\beta^{2e_1+1}-1}$$

which is modified as

$$\gamma^{t_1+t_2} = \frac{1+\gamma^{-t_2}\beta^{2e_1+1}}{1-\gamma^{t_2}\beta^{2e_1+1}} = (1-\gamma^{t_2}\beta^{2e_1+1})^{p^{2k}-1}. \tag{42}$$

Similarly to the Step 2 in Case 2-2), it can be shown that the sum of the number of t_2 making $1-\gamma^{t_2}\beta^{2e_1+1}$ a square for e_1 and the number of t_2' making $1-\gamma^{t_2'}\beta^{-2e_1-1}$ a square for $p^{2k}-2-e_1$ is $(p^{2k}+1)/2$.

Step 3: Similarly to the Step 3 in Case 2-3), we can show that among $(p^{2k}+1)/2$ solutions of (42), there exists only one t_2 such that $t_2 = t_1$, which cannot be a solution of (19) for each pair of e_1 and $p^{2k}-2-e_1$. Thus, in this case, the number of nonsquare solutions x of (19) is $(p^{2k}-1)/2$ for each i, $1 \leq i < (p^{2k}+1)/2$. □

REFERENCES

[1] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. IT-14, no. 1, pp. 154–156, Jan. 1968.

[2] T. Kasami, Weight Distribution Formula For Some Class of Cyclic Codes Coordinated Sci. Lab., Univ. Illinois at Urbana-Champaign, Urbana, IL, 1996, Tech. Rep. R-285 (AD 632574).

[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, 1970.

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

[7] 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.

[8] 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.

[9] 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.

[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] Z. Hu, Z. Li, D. Mills, E. N. Müller, W. Sun, W. Willems, Y. Yang, and Z. Zhang, "On the cross-correlation of sequences with the decimation factor $d=\frac{p^n+1}{p+1}-\frac{p^n-1}{2}$," *Applicable Algebra in Engineering, Communication and Computing*, vol. 12, pp. 255–263, 2001.

[12] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 3, pp. 397–399, May 1974.

[13] 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," *IEICE Trans. Fund. Electron., Commun. Comp. Sci.*, vol. E90-A, no. 11, pp. 2568–2574, Nov. 2007.

[14] 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 $((p^2k+1)/2)^2$," in *Proc. IEEE Int. Symp. Information Theory (ISIT2007)*, Nice, France, Jun. 2007, pp. 2516–2520.

[15] V. M. Sidel'nikov, "On mutual correlation of sequences," *Sovi. Math. –Dokl.*, vol. 12, no. 1, pp. 197–201, 1971.

[16] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inf. Theory*, vol. IT-28, no. 6, pp. 858–864, Nov. 1982.

[17] 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.

[18] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elservier, 1998.

[19] S. W. Golomb, *Shift Register Sequences*. San Francisco, Holden-Day: Aegean Park, 1967.

[20] T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics*. Chicago, IL: Markham, 1967.