Evaluation of Cross-Correlation Values of p-ary m-Sequence and its Decimated Sequence by $\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$

Sung-Tai Choi, Taehyung Lim, and Jong-Seon No
Department of Electrical Engineering and Computer Science, INMC
Seoul National University
Seoul 151-744, Korea
Email: stchoi@ccl.snu.ac.kr, jayelish@hotmail.com, and jsno@snu.ac.kr

Habong Chung
School of Electronics and Electrical Engineering
Hongik University
Seoul 121-791, Korea
Email: habchung@hongik.ac.kr

***Abstract*—For a prime $p \equiv 1 \bmod 4$, an odd integer n, and $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$, we investigate the cross-correlation values of p-ary m-sequence $m(t)$ of period $p^n - 1$ and its decimated m-sequence $m(dt)$. It is shown that the cross-correlation function between $m(t)$ and $m(dt)$ takes the values in $\left\{-1, -1 \pm p^{n/2}, -1 \pm \frac{1+\sqrt{p}}{2}p^{n/2}, -1 \pm \frac{1-\sqrt{p}}{2}p^{n/2}, -1 \pm \frac{p-1}{2}p^{n/2}\right\}$.**

***Index Terms*—Cross-correlation, m-sequence, decimated sequence, p-ary sequence.**

I. Introduction

Evaluation of the cross-correlation function between an m-sequence $m(t)$ and its decimated sequence $m(dt)$ has been studied by various researchers. Gold [1] evaluated the cross-correlation function for the case $d = 2^k + 1$ and $n/\gcd(n, k)$ odd. Welch [2] evaluated the cross-correlation function for the case $d = 2^{2k} - 2^k + 1$ and $n/\gcd(n, k)$ odd. Niho [3] found some decimation values for which the cross-correlation of two binary m-sequences has few correlation values and derived the distribution of the cross-correlation values. Trachtenberg [4] extended the results to nonbinary cases. For an odd prime p, he evaluated the cross-correlation function for the cases $d = (p^{2k} + 1)/2$ and $d = p^{2k} - p^k + 1$. For an odd prime p, Helleseth [5] found some decimation values for which the cross-correlation of two m-sequences has few correlation values and derived the distribution of the cross-correlation values. For the decimation value $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$, Muller [7] and Hu *et al.* [8] derived an upper bound on the magnitudes of the cross-correlations for $p = 3$ and an odd prime $p \equiv 3 \bmod 4$, respectively. In their studies, there are two distinct decimated sequences $m(dt)$ and $m(dt + 1)$ since $\gcd(d, p^n - 1) = 2$.

In this paper, for the same decimation d, but for a prime $p \equiv 1 \bmod 4$ and an odd integer n so that $\gcd(d, p^n - 1) = 1$, the possible values of the cross-correlation function between a p-ary m-sequence $m(t)$ and its decimated m-sequence $m(dt)$ are determined.

II. Preliminaries and Notations

A. Trace Functions and Cross-Correlation Function

Let p be a prime and F_{p^n} the finite field with p^n elements. Then the trace function $\mathrm{tr}_k^n(\cdot)$ from F_{p^n} to F_{p^k} is defined as

$$\mathrm{tr}_k^n(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{p^{ki}}$$

where $x \in F_{p^n}$ and $k|n$.

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

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

The periodic cross-correlation function between two p-ary sequences $s_1(t)$ and $s_2(t)$ of period N at shift τ is defined as

$$C(\tau) = \sum_{t=0}^{N-1} \omega^{s_1(t+\tau)-s_2(t)} \tag{1}$$

where ω is a p-th root of unity.

B. Quadratic Form

The quadratic character of F_{p^n} is defined as

$$\eta(x) = \begin{cases} 1, & \text{if } x \text{ is a square in } F_{p^n} \setminus \{0\} \\ -1, & \text{if } x \text{ is a nonsquare in } F_{p^n} \setminus \{0\} \\ 0, & \text{if } x = 0. \end{cases}$$

A quadratic form over F_p in n indeterminates is a homogeneous polynomial in $F_p[x_1, x_2, \cdots, x_n]$ of degree 2 and can be expressed as

$$f(x_1, x_2, \cdots, x_n) = \sum_{i,j \le n} a_{ij} x_i x_j$$

where $a_{ij} \in F_p$.

Let $(F_p)^n$ denote an n-dimensional vector space over F_p. The number of solutions $(x_1, x_2, \cdots, x_n) \in (F_p)^n$ satisfying the quadratic form $f(x_1, x_2, \cdots, x_n) = b$ for any $b \in F_p$ can be determined from the rank of the quadratic form $f(x_1, x_2, \cdots, x_n)$. The following lemma explains how to calculate the rank of a quadratic form.

978-1-4577-0594-6/11/$26.00 ©2011 IEEE

Lemma 1 ([7]): Let $f \in F_p[x_1, x_2, \cdots, x_n]$ be a quadratic form. Define

$$Z := \{\mathbf{z} \in (F_p)^n : f(\mathbf{x}+\mathbf{z}) - f(\mathbf{x}) = 0 \text{ for all } \mathbf{x} \in (F_p)^n\}. \tag{2}$$

Then Z is a subspace of $(F_p)^n$ and $\text{rank}(f) = n - \dim(Z)$.

A quadratic form $f(\mathbf{x})$ in n indeterminates over F_p can be regarded as a mapping $f(x)$ from F_{p^n} into F_p. Thus, we will also use the term 'quadratic form' for this mapping $f(x)$ in a finite extension field F_{p^n}. In this case, Lemma 1 in a finite field version can be restated as follows.

Corollary 2: The rank ρ of the quadratic form $f(x)$ from F_{p^n} to F_p can be determined by finding the number of elements that the form is independent of, i.e., $p^{n-\rho}$ is the number of $z \in F_{p^n}$ such that $f(x+z) = f(x)$ for all $x \in F_{p^n}$.

If a nonzero quadratic form $f \in F_p[x_1, x_2, \cdots, x_n]$ has a rank $k \leq n$, it can be rewritten as an equivalent canonical form $a_1x_1^2 + a_2x_2^2 + \cdots + a_kx_k^2$ with all nonzero a_i's. Hence for any $b \in F_p$, the number of solutions of $a_1x_1^2 + a_2x_2^2 + \cdots + a_kx_k^2 = b$ in $(F_p)^n$ is p^{n-k} times the number of solutions of the same equation in $(F_p)^k$. [9]

A quadratic form $f \in F_p[x_1, x_2, \cdots, x_k]$ in k indeterminates over F_p is said to be a nondegenerate quadratic form if f has a rank k, i.e., f can be expressed as the canonical form $a_1x_1^2 + a_2x_2^2 + \cdots + a_kx_k^2$ for $a_i \neq 0$. Let $\Delta = a_1a_2\cdots a_k$ denote the determinant of the quadratic form f. If f is a nondegenerate quadratic form of rank k, the number of solutions x in F_{p^k} satisfying $f(x) = b \in F_p$ is determined as the following lemma.

Lemma 3 (Theorem 6.26 and 6.27 [9]): Let η be the quadratic character of F_p. The number of solutions $N(b)$ of $f(\mathbf{x}) = b$ in $(F_p)^k$ when $f(\mathbf{x})$ is a nondegenerate quadratic form of rank k with determinant Δ and $b \in F_p$, is given as follows:

Case 1) k even;

$$N(b) = \begin{cases} p^{k-1} - \epsilon p^{\frac{k-2}{2}}, & \text{if } b \neq 0 \\ p^{k-1} + \epsilon(p-1)p^{\frac{k-2}{2}}, & \text{if } b = 0 \end{cases}$$

where $\epsilon = \eta((-1)^{k/2}\Delta)$.

Case 2) k odd;

$$N(b) = \begin{cases} p^{k-1} + \epsilon\eta(b)p^{\frac{k-1}{2}}, & \text{if } b \neq 0 \\ p^{k-1}, & \text{if } b = 0 \end{cases}$$

where $\epsilon = \eta((-1)^{(k-1)/2}\Delta)$.

C. Linearized Polynomial

Let p be a prime. A polynomial of the form

$$L(x) = \sum_i \alpha_i x^{p^i}$$

with coefficients in an extension field F_{p^n} of F_p is called a linearized polynomial over F_{p^n}. If F is an arbitrary extension field of F_p, then

$$L(\beta+\gamma) = L(\beta) + L(\gamma), \text{ for all } \beta, \gamma \in F$$
$$L(c\beta) = cL(\beta), \text{ for all } \beta \in F \text{ and } c \in F_p.$$

Hence the set of solutions of $L(x) = 0$ in F is considered as a vector subspace over F_p.

In the rest of the paper, the following notations are used:

- p is an odd prime such that $p \equiv 1 \bmod 4$;
- n is an odd positive integer;
- $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$;
- α is a primitive element of F_{p^n};
- ω is a primitive p-th root of unity;
- $F_{p^n}^*$ is a multiplicative group of F_{p^n}, i.e., $F_{p^n} \setminus \{0\}$.

III. Evaluation of Cross-Correlation Values

The periodic cross-correlation $C(\tau)$ between $m(t)$ and $m(dt)$ at shift τ is given as

$$\begin{aligned} C(\tau) &= \sum_{t=0}^{p^n-2} \omega^{m(t+\tau)-m(dt)} \\ &= \sum_{t=0}^{p^n-2} \omega^{\text{tr}_1^n(\alpha^{t+\tau}-\alpha^{dt})} \\ &= \sum_{x\in F_{p^n}^*} \omega^{\text{tr}_1^n(ax-x^d)} \end{aligned} \tag{3}$$

where $a = \alpha^\tau$.

Let $S(a)$ be the exponential sum defined by

$$S(a) = \sum_{x\in F_{p^n}} \omega^{\text{tr}_1^n(ax-x^d)}. \tag{4}$$

Then the cross-correlation $C(\tau)$ can be expressed as $C(\tau) = S(a) - 1$. Exactly the half of the elements in $F_{p^n}^*$ are squares and the other half are nonsquares. Using $\gcd(p+1, p^n-1) = 2$, we can represent each square in $F_{p^n}^*$ as $x = y^{p+1}$ for some $y \in F_{p^n}^*$. Since a nonsquare in F_p^* is also a nonsquare in $F_{p^n}^*$, we can represent nonsquares in $F_{p^n}^*$ as $x = ry^{p+1}$, where r is a nonsquare in F_p^*. Note that as y runs through $F_{p^n}^*$, y^{p+1} covers all the squares in $F_{p^n}^*$ exactly twice and so does ry^{p+1} for the nonsquares. Using $y^{d(p+1)} = y^2$ and $r^d = -r$, we can express $S(a)$ as

$$\begin{aligned} 2S(a) &= \sum_{y\in F_{p^n}} \omega^{\text{tr}_1^n(ay^{p+1}-y^2)} + \sum_{y\in F_{p^n}} \omega^{\text{tr}_1^n(ary^{p+1}-r^dy^2)} \\ &= \sum_{y\in F_{p^n}} \omega^{\text{tr}_1^n(ay^{p+1}-y^2)} + \sum_{y\in F_{p^n}} \omega^{r\text{tr}_1^n(ay^{p+1}+y^2)} \\ &= \sum_{y\in F_{p^n}} \omega^{g(y)} + \sum_{y\in F_{p^n}} \omega^{h(y)} \end{aligned} \tag{5}$$

where $g(y) = \text{tr}_1^n(ay^{p+1} - y^2)$ and $h(y) = r\text{tr}_1^n(ay^{p+1} + y^2)$.

If y is expressed in terms of a basis $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ of F_{p^n} over F_p as $y = \sum_{i=1}^n y_i\alpha_i$, where $y_i \in F_p$, then $g(y)$ can be represented as the quadratic form, that is,

$$\begin{aligned} g(y) &= \mathrm{tr}_1^n\Big(a(\sum_{i=1}^n y_i\alpha_i^p)(\sum_{i=1}^n y_i\alpha_i) - (\sum_{i=1}^n y_i\alpha_i)^2\Big) \\ &= \mathrm{tr}_1^n\Big(a\sum_{i=1}^n\sum_{j=1}^n (y_iy_j)(\alpha_i^p\alpha_j) - \sum_{i=1}^n\sum_{j=1}^n (y_iy_j)(\alpha_i\alpha_j)\Big) \\ &= \sum_{i=1}^n\sum_{j=1}^n y_iy_j\mathrm{tr}_1^n(a\alpha_i^p\alpha_j - \alpha_i\alpha_j) \\ &= \sum_{i=1}^n\sum_{j=1}^n y_iy_jg_{ij} \end{aligned}$$

where $g_{ij} = \mathrm{tr}_1^n(a\alpha_i^p\alpha_j - \alpha_i\alpha_j)$.

Similarly, we can show that $h(y)$ is also a quadratic form. From Lemma 1, Corollary 2, and Lemma 3, in order to evaluate the exponential sum $S(a)$, we need to know the ranks of the quadratic forms $g(y)$ and $h(y)$, i.e., the number of solutions $z \in F_{p^n}$ of the equations $g(y+z) = g(y)$ and $h(y+z) = h(y)$ satisfying for all $y \in F_{p^n}$.

Lemma 4: The number of solutions $z \in F_{p^n}$ satisfying $g(y+z) = g(y)$ for all $y \in F_{p^n}$ equals the number of solutions $z \in F_{p^n}$ satisfying

$$L_g(z) = a^pz^{p^2} - 2z^p + az = 0 \tag{6}$$

and the number of solutions $z \in F_{p^n}$ satisfying $h(y+z) = h(y)$ for all $y \in F_{p^n}$ equals the number of solutions $z \in F_{p^n}$ satisfying

$$L_h(z) = a^pz^{p^2} + 2z^p + az = 0. \tag{7}$$

Proof: The equation $g(y+z) = g(y)$ can be written as

$$\mathrm{tr}_1^n(a(y+z)^{p+1} - (y+z)^2) = \mathrm{tr}_1^n(ay^{p+1} - y^2). \tag{8}$$

Then (8) can be rewritten as

$$\mathrm{tr}_1^n(y^p(a^pz^{p^2} - 2z^p + az) + az^{p+1} - z^2) = 0. \tag{9}$$

Equation (9) holds for all $y \in F_{p^n}$ if and only if

$$\mathrm{tr}_1^n(az^{p+1} - z^2) = 0 \tag{10}$$

and (6) are satisfied simultaneously. Hence the number of solutions $z \in F_{p^n}$ satisfying (8) can be determined by finding the number of solutions $z \in F_{p^n}$ satisfying (6) and (10) simultaneously.

Now, we will show that all solutions $z \in F_{p^n}$ satisfying (6) also satisfy (10). From (6) we have

$$2z^p = a^pz^{p^2} + az.$$

Raising to the p^{i-1} power and multiplying by z^{p^i} gives

$$2z^{2p^i} = a^{p^i}z^{p^{i+1}+p^i} + a^{p^{i-1}}z^{p^i+p^{i-1}}. \tag{11}$$

Using (11), the left hand side of (10) can be rewritten as

$$\begin{aligned} &\mathrm{tr}_1^n(az^{p+1} - z^2) \\ &= \sum_{i=0}^{n-1}(a^{p^i}z^{p^{i+1}+p^i} - z^{2p^i}) \\ &= \sum_{i=0}^{n-1}\Big(a^{p^i}z^{p^{i+1}+p^i} - 2^{-1}(a^{p^i}z^{p^{i+1}+p^i} + a^{p^{i-1}}z^{p^i+p^{i-1}})\Big) \\ &= 0. \end{aligned}$$

Hence we only need to calculate the number of solutions for (6) to determine the number of solutions for $g(y+z) = g(y)$. The case of $h(y)$ can be proven similarly. ■

From Lemma 4, we have to find out the number of solutions $z \in F_{p^n}$ of (6) and (7) to find the rank of $g(y)$ and $h(y)$, respectively. Since the degree of $L_g(z)$ and $L_h(z)$ are both p^2 and they are both linearized forms, the possible numbers of solutions for both equations are $1, p$, or p^2. Moreover, the number of solutions for at least one of two equations $L_g(z)$ and $L_h(z)$ should be one, which is proved in the following lemma.

Lemma 5: Let n_g and n_h denote the number of solutions in F_{p^n} of $L_g(z) = 0$ and $L_h(z) = 0$, respectively. Then either n_g or n_h is one.

Proof: Assume that both equations $L_g(z) = 0$ and $L_h(z) = 0$ have nonzero solutions z_1 and z_2, respectively. $L_g(z_1) = 0$ and $L_h(z_2) = 0$ can be rewritten as

$$\begin{aligned} a^pz_1^{p^2-p} + az_1^{1-p} &= 2 \\ a^pz_2^{p^2-p} + az_2^{1-p} &= -2 \end{aligned}$$

and thus, we have

$$a^p(z_1^{p^2-p} + z_2^{p^2-p}) + a(z_1^{1-p} + z_2^{1-p}) = 0.$$

Since -1 cannot be represented as u^{p-1} for any $u \in F_{p^n}$, $z_1^{1-p} + z_2^{1-p} \neq 0$. Then we have

$$\begin{aligned} &a^{p-1}\frac{z_1^{p^2-p} + z_2^{p^2-p}}{z_1^{1-p} + z_2^{1-p}} \\ &= \left[az_1z_2(z_1^{p-1} + z_2^{p-1})\right]^{p-1} \\ &= -1 \end{aligned}$$

which is a contradiction since -1 cannot be represented as u^{p-1} for any $u \in F_{p^n}$. Hence at least one equation has no nonzero solutions, i.e., has only one solution $z = 0$. ■

From the above lemma, the possible (n_g, n_h) are $(1,1)$, $(1,p)$, $(1,p^2)$, $(p,1)$, and $(p^2,1)$. It is straightforward to derive the following corollary from the above lemma.

Corollary 6: Let r_g and r_h denote the ranks of the quadratic forms $g(y)$ and $h(y)$, respectively. The possible ranks of $g(y)$ and $h(y)$, (r_g, r_h), are (n,n), $(n,n-1)$, $(n,n-2)$, $(n-1,n)$, and $(n-2,n)$.

Next, we will present the upper bound of $|S(a)|$ given in (5) as Lemma 9. The following theorems are needed for the proof of Lemma 9.

Theorem 7 (Theorem 5.15 [9]): Let p be an odd prime and η the quadratic character of F_p. Then

$$\sum_{i=1}^{p-1}\eta(i)\omega^i = \begin{cases} p^{\frac{1}{2}}, & \text{if } p \equiv 1 \bmod 4 \\ ip^{\frac{1}{2}}, & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

where ω is a primitive p-th root of unity.

Theorem 8 (Theorem 5.38 [9]): Let $f \in F_{p^n}[x]$ be a polynomial of degree $s \geq 1$ with $\gcd(s, p^n) = 1$ and let χ be a nontrivial additive character of F_{p^n}. Then

$$|\sum_{c\in F_{p^n}} \chi(f(c))| \leq (s-1)p^{n/2}.$$

Lemma 9: The magnitude of the exponential sum $S(a)$ given in (5) is upper-bounded as

$$|S(a)| \leq \frac{p-1}{2}p^{\frac{n}{2}}.$$

Proof: We have to show that

$$\Big|\sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(ay^{p+1}-y^2)} + \sum_{y\in F_{p^n}} \omega^{r\mathrm{tr}_1^n(ay^{p+1}+y^2)}\Big| \leq (p-1)p^{\frac{n}{2}}. \tag{12}$$

Set $r = \alpha^{\frac{p^n-1}{p-1}}$, which is a nonsquare in F_{p^n} and genarator of F_p. Define $C_0 = \{x^2 | x \in F_{p^n}^*\}$ and $C_1 = F_{p^n}^* \setminus C_0$.

The first term in (12) can be written as

$$\sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(ay^{p+1}-y^2)} = 1 + 2\sum_{z\in C_0} \omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)}$$

where $z = y^2$.

Clearly, -1 is a square in F_{p^n} and $r^{\frac{p+1}{2}} = -r$. Then we have

$$\begin{aligned}\sum_{z\in C_0} \omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)} &= \sum_{u\in C_1} \omega^{\mathrm{tr}_1^n\left(a(ru)^{\frac{p+1}{2}}-ru\right)} \\ &= \sum_{u\in C_1} \omega^{r\mathrm{tr}_1^n(-au^{\frac{p+1}{2}}-u)} \\ &= \sum_{v\in C_1} \omega^{r\mathrm{tr}_1^n(av^{\frac{p+1}{2}}+v)}\end{aligned}$$

where $z = ru$ and $v = -u$. Hence the first term in (12) can be written as

$$\begin{aligned}\sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(ay^{p+1}-y^2)} =&1 + \sum_{z\in C_0} \omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)} \\ &+ \sum_{z\in C_1} \omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)}.\end{aligned} \tag{13}$$

Similarly, the second term in (12) can be written as

$$\sum_{y\in F_{p^n}} \omega^{r\cdot\mathrm{tr}_1^n(ay^{p+1}+y^2)} = 1 + 2\sum_{z\in C_0} \omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)}$$

where $z = y^2$.

Since

$$\begin{aligned}\sum_{z\in C_0} \omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)} &= \sum_{u\in C_1} \omega^{r\mathrm{tr}_1^n\left(a(ru)^{\frac{p+1}{2}}+ru\right)} \\ &= \sum_{u\in C_1} \omega^{\mathrm{tr}_1^n(-ar^2u^{\frac{p+1}{2}}+r^2u)} \\ &= \sum_{u\in C_1} \omega^{\mathrm{tr}_1^n(-ar^{p+1}u^{\frac{p+1}{2}}+r^2u)} \\ &= \sum_{v\in C_1} \omega^{\mathrm{tr}_1^n(av^{\frac{p+1}{2}}-v)}\end{aligned}$$

where $z = ru$ and $v = -r^2u$, the second term in (12) can be written as

$$\begin{aligned}\sum_{y\in F_{p^n}} \omega^{r\mathrm{tr}_1^n(ay^{p+1}+y^2)} =&1 + \sum_{z\in C_0} \omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)} \\ &+ \sum_{z\in C_1} \omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)}.\end{aligned} \tag{14}$$

From (13) and (14), $S(a)$ can be expressed as

$$\begin{aligned}2S(a) =& \sum_{y\in F_{p^n}} \omega^{\mathrm{tr}_1^n(ay^{p+1}-y^2)} + \sum_{y\in F_{p^n}} \omega^{r\mathrm{tr}_1^n(ay^{p+1}+y^2)} \\ =& 1 + \sum_{z\in C_0} \omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)} + \sum_{z\in C_1} \omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)} \\ &+ 1 + \sum_{z\in C_0} \omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)} + \sum_{z\in C_1} \omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)} \\ =& \sum_{z\in F_{p^n}} \omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)} + \sum_{z\in F_{p^n}} \omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)}.\end{aligned} \tag{15}$$

From Theorem 8, the magnitude of each term in (15) is upper-bounded as

$$\begin{aligned}&|\sum_{z\in F_{p^n}} \omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)}| \leq \frac{p-1}{2}p^{\frac{n}{2}} \\ &|\sum_{z\in F_{p^n}} \omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)}| \leq \frac{p-1}{2}p^{\frac{n}{2}}.\end{aligned}$$

Hence the proof is done. ■

Theorem 10: The cross-correlation function between a p-ary m-sequence $m(t)$ and its decimated sequence $m(dt)$ takes values in $\{-1, -1 \pm p^{n/2}, -1 \pm \frac{1+\sqrt{p}}{2}p^{n/2}, -1 \pm \frac{1-\sqrt{p}}{2}p^{n/2}, -1 \pm \frac{p-1}{2}p^{n/2}\}$.

Proof: From (5), the correlation function in (3) can be expressed using the function $S(a)$ as

$$C(\tau) = -1 + S(a) = -1 + \frac{1}{2}(\sum_{y\in F_{p^n}} \omega^{g(y)} + \sum_{y\in F_{p^n}} \omega^{h(y)})$$

where $g(y) = \mathrm{tr}_1^n(ay^{p+1} - y^2)$ and $h(y) = r\mathrm{tr}_1^n(ay^{p+1} + y^2)$.

Note that both $g(y)$ and $h(y)$ are quadratic forms. From Corollary 6, the possible ranks of $g(y)$ and $h(y)$ are (n, n),

$(n-1,n)$, $(n-2,n)$, $(n,n-1)$, and $(n,n-2)$. By using Lemma 3, we can derive the correlation values as follows:

Case 1) Rank of $g(y)=n-2$ and rank of $h(y)=n$ (or rank of $g(y)=n$ and rank of $h(y)=n-2$);

From Lemma 3 and Theorem 7, we have

$$\begin{aligned}2S(a) &= \sum_{y\in F_{p^n}} \omega^{g(y)} + \sum_{y\in F_{p^n}} \omega^{h(y)} \\ &= p^2\Big(p^{n-3} + \sum_{i=1}^{p-1}\left((p^{n-3}+\epsilon_g\eta(i)p^{\frac{n-3}{2}})\omega^i\right)\Big) \\ &+ \Big(p^{n-1} + \sum_{i=1}^{p-1}\left((p^{n-1}+\epsilon_h\eta(i)p^{\frac{n-1}{2}})\omega^i\right)\Big) \\ &= p^{\frac{n+1}{2}}\epsilon_g\sum_{i=1}^{p-1}\eta(i)\omega^i + p^{\frac{n-1}{2}}\epsilon_h\sum_{i=1}^{p-1}\eta(i)\omega^i \\ &= p^{\frac{n}{2}}(p\epsilon_g+\epsilon_h).\end{aligned}$$

Thus, we obtain

$$C(\tau) = -1 + \frac{p\epsilon_g+\epsilon_h}{2}p^{\frac{n}{2}}.$$

Both ϵ_g and ϵ_h should take values in $\{+1,-1\}$. However, when $\epsilon_g=\epsilon_h$, it contradicts to Lemma 9. Hence the possible case is $\epsilon_g=1$ and $\epsilon_h=-1$ or vice versa. Hence the possible values here are

$$\Big\{-1+\frac{p-1}{2}p^{n/2}, -1+\frac{-p+1}{2}p^{n/2}\Big\}.$$

Case 2) Rank of $g(y)=n-1$ and rank of $h(y)=n$ (or rank of $g(y)=n$ and rank of $h(y)=n-1$);

The case for rank n was dealt with in the previous case. Hence we only need to determine the exponential sum for rank $n-1$. From Lemma 3, we have

$$\begin{aligned}2S(a) &= \sum_{y\in F_{p^n}} \omega^{g(y)} + \sum_{y\in F_{p^n}} \omega^{h(y)} \\ &= p\Big(p^{n-2} + \epsilon_g(p-1)p^{\frac{n-3}{2}} \\ &\quad + \sum_{i=1}^{p-1}\left((p^{n-2}-\epsilon_g p^{\frac{n-3}{2}})\omega^i\right)\Big) + p^{\frac{n}{2}}\epsilon_h \\ &= p^{\frac{n}{2}}(\sqrt{p}\epsilon_g+\epsilon_h).\end{aligned}$$

Thus, we obtain

$$C(\tau) = -1 + \frac{\sqrt{p}\epsilon_g+\epsilon_h}{2}p^{\frac{n}{2}}.$$

Since ϵ_g and ϵ_h take values in $\{+1,-1\}$, the number of possible correlation values is 4 in this case. Hence the possible values here are

$$\Big\{-1+\frac{\sqrt{p}+1}{2}p^{n/2}, -1+\frac{\sqrt{p}-1}{2}p^{n/2}, \\ -1+\frac{-\sqrt{p}+1}{2}p^{n/2}, -1+\frac{-\sqrt{p}-1}{2}p^{n/2}\Big\}.$$

Case 3) Rank of $g(y)=n$ and rank of $h(y)=n$;

The case for rank n was dealt with in the previous cases. Hence we have

$$C(\tau) = -1 + \frac{\epsilon_g+\epsilon_h}{2}p^{\frac{n}{2}}.$$

Since ϵ_g and ϵ_h take values in $\{+1,-1\}$, the number of possible correlation values is 3 in this case. Hence the possible values here are

$$\big\{-1, -1+p^{n/2}, -1-p^{n/2}\big\}.$$

∎

IV. Concluding Remark

In this paper, we evaluate the values of cross-correlation function between a p-ary m-sequence $m(t)$ and its decimated sequence $m(dt)$, for $d=\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$, a prime $p\equiv 1 \bmod 4$, and n odd. In fact, we have derived the distribution of cross-correlation values. Due to the page limit, we did not include them, in this paper. The extended version [10], in which the derivation of the distribution of the cross-correlation values is included, will be soon submitted.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2011-0000328) and the KCC (Korea Communications Commission), Korea, under the R&D program supervised by the KCA (Korea Communications Agency) (KCA-2011-08913-04003).

References

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

[2] L. R. Welch, "Cross-correlation and quadratic forms," *Unpublished notes*, Univ. of Southern California, Los Angeles, CA.

[3] Y. Niho, "Multi-valued cross-correlation functions between two maximal reculsive sequences," *Ph.D. dissertation*, Univ. of Southern California, Los Angeles, CA, 1972.

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

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

[6] 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.

[7] 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.

[8] 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 $d=\frac{p^n+1}{p+1}-\frac{p^n-1}{2}$," *Applicable Algebra in Engineering, Communication and Computing*, vol. 12, pp. 255-263, 2001.

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

[10] S. T. Choi, T. Lim, J. S. No, and H. Chung, "Cross-Correlation Distribution of p-ary m-sequence and its Decimated sequence by $\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$," in preparation.