IEICE TRANS. FUNDAMENTALS, VOL.E90–A, NO.11 NOVEMBER 2007

PAPER

Cross-Correlation Distribution of p-Ary m-Sequence and Its $p + 1$ Decimated Sequences with Shorter Period*

Eun-Young SEO[†], **Young-Sik KIM**[†], ***Nonmembers***, **Jong-Seon NO**[†a)], ***and*** **Dong-Joon SHIN**[††], ***Members***

SUMMARY In this paper, the cross-correlation distribution between a p-ary m-sequence $s(t)$ and its $p + 1$ distinct decimated sequences $s(dt + l)$ is derived. For an odd prime p, an even integer n, and $d = p^k + 1$ with $\gcd(n, k) = 1$, there are $p + 1$ distinct decimated sequences $s(dt + l)$, $0 \le l < p + 1$, for a p-ary m-sequence $s(t)$ of period $p^n - 1$ because $\gcd(d, p^n - 1) = p + 1$. The maximum magnitude of their cross-correlation values is $1 + p\sqrt{p^n}$ if $l \equiv 0 \bmod p + 1$ for $n \equiv 0 \bmod 4$ or $l \equiv (p + 1)/2 \bmod p + 1$ for $n \equiv 2 \bmod 4$ and otherwise, $1 + \sqrt{p^n}$. Also by using $s(t)$ and $s(dt + l)$, a new family of p-ary sequences of period $p^n - 1$ is constructed, whose family size is p^n and $C_{\max}$ is $1 + p\sqrt{p^n}$.

key words: *cross-correlation, p-ary m-sequences, sequences*

1. Introduction

For over 40 years, m-sequences and their decimated sequences with good cross-correlation property have been found by Gold [1], Kasami [2], and No [3]. Also, 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 [4]–[6].

However, the decimation factor d is not necessarily 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 [7], Kumar and Moreno [8], and Müller [9]. In [7], the cross-correlation distribution of 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 $\gcd(n, k) = 1$, is found. Kumar and Moreno [8] derived the cross-correlation values of $s(t)$ and $s(dt)$ with $d = p^k + 1$, where $n/\gcd(n, k) = \text{odd}$. In this case, $\gcd(d, p^n - 1)$ is 2 and the maximum magnitude $C_{\max}$ of the cross-correlation values of the sequence family is $1 + \sqrt{p^n}$, which is optimal with respect to the Welch bound [10]. Furthermore, in Theorem 4 of [9], Müller found the upper bound on the cross-correlation values of the sequences $s(t)$ and only one decimated sequence $s(dt)$ when n is even, $n/\gcd(n, k)$ is not divisible by 4, and d is $p^k + 1$. Some sequence families with good correlation property are listed in Table 1.

Table 1 Parameters of some known sequence families.

Family	Alphabet	Period N	Family size	$C_{\max}$
Gold (n odd) [1]	2	$2^n - 1$	$N + 2$	$\sqrt{2(N + 1)} + 1$
Gold (n even) [1]	2	$2^n - 1$	$N + 2$	$2\sqrt{N + 1} + 1$
No [3]	2	$2^n - 1$	$\sqrt{N + 1}$	$\sqrt{N + 1} + 1$
Kumar et al. [8]	odd p	$p^n - 1$	$N + 1$	$\sqrt{N + 1} + 1$
Trachtenberg [4]	odd p	$p^n - 1$	$N + 1$	$\sqrt{p(N + 1)} + 1$
Sidel'nikov [13]	odd p	$p^n - 1$	$N + 1$	$\sqrt{N + 1} + 1$
Helleseth [5]	odd p	$p^n - 1$	$N + 1$	$2\sqrt{N + 1} + 1$
Bent [14]	p	$p^n - 1$	$\sqrt{N + 1}$	$\sqrt{N + 1} + 1$
Jang et al. [15]	odd p	$p^n - 1$	$N + 1$	$\sqrt{N + 1} + 1$
New Sequences	odd p	$p^n - 1$	$N + 1$	$p\sqrt{N + 1} + 1$

* p is a prime number.

In this paper, the cross-correlation distribution between a p-ary m-sequence $s(t)$ and its decimated sequences $s(dt + l)$, $0 \le l < p + 1$, is derived. For an odd prime p, an even integer n, and $d = p^k + 1$ with $\gcd(n, k) = 1$, there are $p + 1$ distinct decimated sequences $s(dt + l)$, $0 \le l < p + 1$, of a p-ary m-sequence $s(t)$ of period $p^n - 1$ since $\gcd(d, p^n - 1) = p + 1$. It is also shown that the maximum magnitude of their cross-correlation values is $1 + p\sqrt{p^n}$ if $l \equiv 0 \bmod p + 1$ for $n \equiv 0 \bmod 4$ or $l \equiv (p + 1)/2 \bmod p + 1$ for $n \equiv 2 \bmod 4$ and otherwise, $1 + \sqrt{p^n}$. By using $s(t)$ and $s(dt + l)$, a new family of p-ary sequences of period $p^n - 1$ is constructed, whose family size is p^n and $C_{\max}$ is $1 + p\sqrt{p^n}$.

2. Preliminaries

Let p be an odd prime, F_{p^n} the finite field with p^n elements, and $F_{p^n}^* = F_{p^n} \backslash \{0\}$. Then the trace function $\mathrm{tr}_m^n(\cdot)$ from F_{p^n} to F_{p^m} is defined as

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

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

Manuscript received February 28, 2007.
Manuscript revised May 30, 2007.
Final manuscript received August 2, 2007.

[†]The authors are with the Department of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea.
[††]The author is with the Division of Electronics and Computer Engineering, Hanyang University, Seoul 133-791, Korea.

*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.

a) E-mail: jsno@snu.ac.kr

DOI: 10.1093/ietfec/e90–a.11.2568

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 $x \in F_{p^n}$;
3) Let l be an integer such that $l|m|n$. Then $\mathrm{tr}_l^n(x) = \mathrm{tr}_l^m(\mathrm{tr}_m^n(x))$, for all $x \in F_{p^n}$;
4) For any $b \in F_{p^m}$, it holds that $|\{x \in F_{p^n} | \mathrm{tr}_m^n(x) = b\}| = p^{n-m}$;
5) Let $a \in F_{p^n}$. If $\mathrm{tr}_m^n(ax) = 0$ for all $x \in F_{p^n}$, then $a = 0$.

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

$$s(t) = \mathrm{tr}_1^n(\alpha^t). \tag{2}$$

Let n be an even integer and $d = p^k + 1$ with $\gcd(n, k) = 1$. Then, $\gcd(p^n - 1, d) = p + 1$ because $\gcd(p^n - 1, p^{2k} - 1) = p^2 - 1$ and $\gcd(p^n - 1, p^k - 1) = p - 1$. Therefore, we have $p+1$ distinct decimated sequences $s_l(dt)$ of period $(p^n - 1)/(p+1)$ using shift values l, $0 \le l < p + 1$, which are defined as

$$s_l(dt) = \mathrm{tr}_1^n(\alpha^{dt+l}). \tag{3}$$

Then the cross-correlation function of $s(t)$ and its decimated sequence $s_l(dt)$ at shift τ is defined as

$$\begin{aligned} C_l(\tau) &= \sum_{t=0}^{p^n-2} \omega^{s_l(dt)-s(t+\tau)} = \sum_{t=0}^{p^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{dt+l}-\alpha^{t+\tau})} \\ &= \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax^d - bx)} \end{aligned} \tag{4}$$

where ω is a primitive complex p-th root of unity, $a = \alpha^l$, and $b = \alpha^\tau$. From now on, we will use the notations $C_l(\tau)$ and $C_l(b)$, interchangeably.

Let ψ denote the canonical additive character of the additive group F_{p^n}, which is defined as

$$\psi(x) = e^{j2\pi \mathrm{tr}_1^n(x)/p}, \quad \text{for all } x \in F_{p^n}. \tag{5}$$

All additive characters of F_{p^n} can be expressed in terms of ψ.

A character χ of the multiplicative group $F_{p^n}^*$ is called a multiplicative character of F_{p^n}. Note that the quadratic character η of F_{p^n} is one of multiplicative characters defined by

$$\eta(x) = \begin{cases} 1, & \text{if } x \text{ is nonzero square in } F_{p^n} \\ -1, & \text{if } x \text{ is nonzero nonsquare in } F_{p^n} \\ 0, & \text{if } x = 0. \end{cases} \tag{6}$$

The Gauss sum $G(\chi, \psi)$ using additive and multiplicative characters becomes

$$G(\chi, \psi) = \sum_{x \in F_{p^n}^*} \chi(x)\psi(x). \tag{7}$$

Then for the quadratic character η, the associated Gauss sum can be explicitly evaluated as in the following theorem.

Theorem 1: [12, Theorem 5.15] Let p be an odd prime and η and ψ denote the quadratic character and canonical additive character of F_{p^n}, respectively. Then the Gauss sum is given by

$$G(\eta, \psi) = \begin{cases} (-1)^{n-1} p^{\frac{n}{2}}, & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{n-1} i^n p^{\frac{n}{2}}, & \text{if } p \equiv 3 \bmod 4 \end{cases} \tag{8}$$

where $i = \sqrt{-1}$. □

3. Upper Bound of Cross-Correlation Values

In this section, we will prove that the cross-correlation values $C_l(\tau)$ in (4) between a p-ary m-sequence $s(t)$ and its decimated sequence $s_l(dt)$ are upper bounded by $1 + \sqrt{p^n}$ or $1 + p\sqrt{p^n}$ according to the shift value l.

Let n be an even integer, α a primitive element of F_{p^n}, and $d = p^k + 1$ with $\gcd(n, k) = 1$. Define

$$Q_l(x) = \mathrm{tr}_1^n(\alpha^l x^d), \quad 0 \le l < p + 1. \tag{9}$$

If we represent x in terms of a basis $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ of F_{p^n} over F_p as $x = \sum_{i=1}^n x_i \alpha_i$, $x_i \in F_p$, then $Q_l(x)$ can be expressed as a quadratic form given as

$$\begin{aligned} Q_l(x) &= \sum_{i=1}^n \sum_{j=1}^n \mathrm{tr}_1^n(\alpha^l x_i x_j \alpha_i^{p^k} \alpha_j) \\ &= \sum_{i=1}^n \sum_{j=1}^n x_i x_j \mathrm{tr}_1^n(\alpha^l \alpha_i^{p^k} \alpha_j) = \sum_{i=1}^n \sum_{j=1}^n a_{ij} x_i x_j \end{aligned} \tag{10}$$

where $a_{ij} = \mathrm{tr}_1^n(\alpha^l \alpha_i^{p^k} \alpha_j) \in F_p$.

First, we determine the rank of the quadratic form $Q_l(x)$ defined in (10) in the following lemma.

Lemma 2: The rank of a quadratic form $Q_l(x)$ in (10) is given as

Rank of $Q_l(x)$

$$= \begin{cases} n-2, & \text{if } l \equiv 0 \bmod p+1 \text{ for } n \equiv 0 \bmod 4 \text{ or} \\ & \quad l \equiv \frac{p+1}{2} \bmod p+1 \text{ for } n \equiv 2 \bmod 4 \\ n, & \text{otherwise.} \end{cases} \tag{11}$$

Proof: The rank ρ of a quadratic form can be determined by finding the number of coordinates of which the quadratic form is independent, i.e., $p^{n-\rho}$ is the number of $z \in F_{p^n}$ such that $Q_l(x + z) = Q_l(x)$ for all $x \in F_{p^n}$. Then we have

$$\begin{aligned} &Q_l(x+z) - Q_l(x) \\ &\quad = \mathrm{tr}_1^n(\alpha^l (x+z)^{p^k+1} - \alpha^l x^{p^k+1}) \\ &\quad = \mathrm{tr}_1^n(\alpha^l x z^{p^k} + \alpha^l x^{p^k} z + \alpha^l z^{p^k+1}) \\ &\quad = \mathrm{tr}_1^n((\alpha^{lp^k} z^{p^{2k}} + \alpha^l z) x^{p^k}) + \mathrm{tr}_1^n(\alpha^l z^{p^k+1}). \end{aligned} \tag{12}$$

In order to satisfy $Q_l(x + z) - Q_l(x) = 0$ for all $x \in F_{p^n}$, we

must have

$$\alpha^{lp^k} z^{p^{2k}} + \alpha^l z = 0 \tag{13}$$

and

$$\mathrm{tr}_1^n(\alpha^l z^{p^k+1}) = 0. \tag{14}$$

If $\alpha^{lp^k} z^{p^{2k}} + \alpha^l z = 0$, then (14) is always satisfied because

$$\mathrm{tr}_1^n(\alpha^l z^{p^k+1}) = \mathrm{tr}_1^n(\alpha^{lp^k} z^{p^{2k}} z^{p^k}) = \mathrm{tr}_1^n(-\alpha^l z^{p^k+1}). \tag{15}$$

Thus, we only have to count the number of solutions z satisfying (13), which can be rewritten as

$$\alpha^{(p^k-1)l} z^{p^{2k}-1} = -1. \tag{16}$$

Let $z = \alpha^s$. Then, we have

$$\alpha^{(p^k-1)l} \alpha^{(p^{2k}-1)s} = -1 = \alpha^{\frac{p^n-1}{2}m} \tag{17}$$

where m is some odd integer. Then we have to count the number of integers s, $0 \le s < p^n-1$, satisfying the following congruence

$$(p^{2k}-1)s + (p^k-1)l \equiv \frac{p^n-1}{2}m \bmod p^n - 1. \tag{18}$$

We will use the well-known fact that $xs \equiv y \bmod r$ a solution s if and only if $\gcd(r, x)|y$ and in this case there are $\gcd(r, x)$ solutions. Also, we have $\gcd(p^n-1, p^{2k}-1) = p^{\gcd(n,2k)}-1 = p^2-1$. Now, we have to consider the following two cases.

Case 1) $n \equiv 0 \bmod 4$:

It is clear that p^2-1 divides $(p^n-1)m/2$ because $(p^n-1)/(p^2-1)$ is even. Therefore, in order to have solutions for (18), the following value

$$\frac{(p^k-1)l}{p^2-1} = \frac{(p^{k-1}+p^{k-2}+\cdots+p+1)l}{p+1} \tag{19}$$

should be an integer. From $\gcd(p^k-1, p^2-1) = p-1$, we have $\gcd(p^{k-1}+p^{k-2}+\cdots+p+1, p+1) = 1$ and the above value is an integer if and only if $l \equiv 0 \bmod p+1$. Therefore, when $l \equiv 0 \bmod p+1$, we have p^2-1 solutions s of (18) as

$$s = \frac{m(p^n-1)}{2(p^{2k}-1)} - \frac{l}{p^k+1} + \frac{p^n-1}{p^2-1}u \tag{20}$$

where $u = 0, 1, 2, \cdots, p^2-2$. This means that there are p^2-1 nonzero solutions $z = \alpha^s$ satisfying (13). Since $z = 0$ also satisfies (13), the rank of the quadratic form $Q_l(x)$ when $n \equiv 0 \bmod 4$ is given as

$$\begin{cases} n-2, & \text{for } l \equiv 0 \bmod p+1 \\ n, & \text{otherwise.} \end{cases} \tag{21}$$

Case 2) $n \equiv 2 \bmod 4$:

Similarly to Case 1, in order to have solutions for (18), p^2-1 should divide $(p^n-1)m/2 - (p^k-1)l$. Since $\gcd(p^2-1, p^k-1) = p-1$, the following value

$$\frac{m(1+p^2+\cdots+p^{n-2}) - \frac{2}{p+1}l(1+p+\cdots+p^{k-1})}{2} \tag{22}$$

should be an integer. Thus, there are p^2-1 solutions s of (18) given in (20) if and only if

$$l \equiv \frac{p+1}{2} \bmod p+1. \tag{23}$$

This also means that there are p^2-1 nonzero solutions $z = \alpha^s$ satisfying (13). Since $z = 0$ also satisfies (13), the rank of the quadratic form $Q_l(x)$ when $n \equiv 2 \bmod 4$ is given as

$$\begin{cases} n-2, & \text{for } l \equiv \frac{p+1}{2} \bmod p+1 \\ n, & \text{otherwise.} \end{cases} \tag{24}$$

□

Now, we can prove that the magnitude of the cross-correlation values is upper bounded by $1+\sqrt{p^n}$ or $1+p\sqrt{p^n}$ according to the shift value l as in the following theorem.

Theorem 3: Let n be an even integer, α a primitive element of F_{p^n}, and $d = p^k+1$ with $\gcd(n, k) = 1$. Then, we have the following relation for the cross-correlation values defined in (4).

$$|C_l(b)+1|^2 = \begin{cases} 0 \text{ or } p^{n+2}, & \text{if } l \equiv 0 \bmod p+1 \text{ for } n \equiv 0 \bmod 4 \text{ or} \\ & l \equiv \frac{p+1}{2} \bmod p+1 \text{ for } n \equiv 2 \bmod 4 \\ p^n, & \text{otherwise.} \end{cases} \tag{25}$$

Proof: From (4), we have

$$|C_l(\tau)+1|^2 = \sum_{x \in F_{p^n}} \sum_{y \in F_{p^n}} \omega^{\mathrm{tr}_1^n(\alpha^l(y^d-x^d)-\alpha^\tau(y-x))}. \tag{26}$$

Let $a = \alpha^l$, $b = \alpha^\tau$, and $z = y - x$. Then (26) becomes

$$\begin{aligned} |C_l(b)+1|^2 &= \sum_{z \in F_{p^n}} \omega^{\mathrm{tr}_1^n(-bz)} \sum_{x \in F_{p^n}} \omega^{\mathrm{tr}_1^n(a((x+z)^d-x^d))} \\ &= \sum_{z \in F_{p^n}} \omega^{\mathrm{tr}_1^n(-bz)} \sum_{x \in F_{p^n}} \omega^{Q_l(x+z)-Q_l(x)} \\ &= \sum_{z \in F_{p^n}} \omega^{\mathrm{tr}_1^n(az^{p^k+1}-bz)} \sum_{x \in F_{p^n}} \omega^{\mathrm{tr}_1^n((a^{p^k}z^{p^{2k}}+az)x^{p^k})}. \end{aligned} \tag{27}$$

Now, we will consider the following three cases.

Case 1) $l \equiv 0 \bmod p+1$ for $n \equiv 0 \bmod 4$:

By Lemma 2, the inner summation of (27) is equal to p^n when $z = 0$ or $z = \alpha^s$ for s given in (20) and in this case, we have $\mathrm{tr}_1^n(az^{p^k+1}) = 0$. Otherwise, the inner summation of (27) is equal to 0. Let $m' = m(p^2-1)/(p^{2k}-1)$ for s given in (20). Note that m' is an odd integer because k and m are odd integers. Then we have

$$|C_l(b)+1|^2 = p^n\left[1+\sum_{\substack{m'=1\\ m' \text{ is odd}}}^{2p^2-3}\omega^{\mathrm{tr}_1^n\left(b'\alpha^{\frac{m'(p^n-1)}{2(p^2-1)}}\right)}\right] \tag{28}$$

where $b' = -b\alpha^{-l/(p^k+1)+(p^n-1)u/(p^2-1)}$. Let $m' = 2m''+1$, where $0 \le m'' < p^2-1$. Then (28) can be rewritten as

$$|C_l(b)+1|^2 = p^n\left[1+\sum_{m''=0}^{p^2-2}\omega^{\mathrm{tr}_1^2\left(\alpha^{m''\frac{p^n-1}{p^2-1}}\mathrm{tr}_2^n\left(b'\alpha^{\frac{p^n-1}{2(p^2-1)}}\right)\right)}\right]. \tag{29}$$

Let $A = \mathrm{tr}_2^n(b'\alpha^{(p^n-1)/2(p^2-1)})$. If $A = 0$, $|C_l(b)+1|^2 = p^{n+2}$. Note that $A = 0$ occurs $p^{n-2}-1$ times as b' varies over $F_{p^n}^*$. Otherwise, by the balance property of the trace function, $|C_l(b)+1|^2 = 0$.

Case 2) $l \equiv (p+1)/2 \bmod p+1$ for $n \equiv 2 \bmod 4$:

Similarly to Case 1, we can also obtain that $|C_l(b)+1|^2$ is 0 or p^{n+2}.

Case 3) $l \not\equiv 0 \bmod p+1$ for $n \equiv 0 \bmod 4$ or $l \not\equiv (p+1)/2 \bmod p+1$ for $n \equiv 2 \bmod 4$:

The inner summation in (27) is p^n for $z = 0$ and 0, otherwise. Thus we have

$$|C_l(b)+1|^2 = p^n. \tag{30}$$

□

4. Distribution of Cross-Correlation Values

In this section, we derive the cross-correlation distribution of a p-ary m-sequence $s(t)$ and its $p+1$ distinct decimated sequences $s_l(dt)$ defined in (3). First, the number of solutions for the quadratic form is given as in the following theorem.

Theorem 4: [12, Theorem 6.26] Let f be a nondegenerate quadratic form over the finite field F_q, q odd, in n indeterminates, where n is even. Then for $b \in F_q$, the number of solutions of the equation $f(x_1,\cdots,x_n) = b$ in F_q^n is

$$q^{n-1} + v(b)q^{\frac{n}{2}-1}\eta((-1)^{\frac{n}{2}}\Delta) \tag{31}$$

where η is the quadratic character of F_q and $\Delta = \det(f)$ and $v(b) = -1$ if $b \neq 0$ and $v(b) = q-1$ if $b = 0$. □

By a nonsingular linear transformation in coordinates, the quadratic form $Q_l(x)$ with rank k in (10) can be transformed to [11]

$$Q_l(x) = \sum_{i=1}^{k} a_i x_i^2 \tag{32}$$

where $a_i \in F_p^*$ and $x_i \in F_p$. In this case, $\Delta = \det(Q_l) = a_1a_2\cdots a_k$.

By using Theorem 4, we can obtain the following cross-correlation distribution of $s(t)$ and $p+1$ distinct decimated sequences $s_l(dt)$, $0 \le l < p+1$.

Theorem 5: Let p be an odd prime, n an even integer, and $d = p^k+1$ with $\gcd(n,k) = 1$. Let $\Delta = a_1\cdots a_n$ and $\Delta' = a_1\cdots a_{n-2}$, where a_i's are defined in (32). Let η and ψ denote the quadratic character and canonical additive character of F_p, respectively. Then, the cross-correlation distribution of a p-ary m-sequence $s(t)$ and its decimated sequences $s_l(dt)$, $0 \le l < p+1$, becomes:

Case 1) $l \not\equiv 0 \bmod p+1$ for $n \equiv 0 \bmod 4$ or $l \not\equiv (p+1)/2 \bmod p+1$ for $n \equiv 2 \bmod 4$:

If $n \equiv 2 \bmod 4$ and $p \equiv 3 \bmod 4$, $0 \le \tau < p^n-1$, the distribution of cross-correlation values is given as

$$C_l(\tau) = \begin{cases} -1-p^{\frac{n}{2}}\eta(\Delta), \\ \quad p^{n-1}-(p-1)p^{\frac{n}{2}-1}\eta(\Delta)-1 \text{ times} \\ -1-p^{\frac{n}{2}}\eta(\Delta)\psi(u), \\ \quad p^{n-1}+p^{\frac{n}{2}-1}\eta(\Delta) \text{ times for each } u \in F_p^* \end{cases} \tag{33}$$

and otherwise,

$$C_l(\tau) = \begin{cases} -1+p^{\frac{n}{2}}\eta((-1)^{\frac{n}{2}}\Delta), \\ \quad p^{n-1}+(p-1)p^{\frac{n}{2}-1}\eta((-1)^{\frac{n}{2}}\Delta)-1 \text{ times} \\ -1+p^{\frac{n}{2}}\eta((-1)^{\frac{n}{2}}\Delta)\psi(u), \\ \quad p^{n-1}-p^{\frac{n}{2}-1}\eta((-1)^{\frac{n}{2}}\Delta) \text{ times for each } u \in F_p^*. \end{cases} \tag{34}$$

Case 2) $l \equiv 0 \bmod p+1$ for $n \equiv 0 \bmod 4$ or $l \equiv (p+1)/2 \bmod p+1$ for $n \equiv 2 \bmod 4$:

If $n \equiv 0 \bmod 4$ and $p \equiv 3 \bmod 4$, the distribution of cross-correlation values is given as

$$C_l(\tau) = \begin{cases} -1, \quad p^n-p^{n-2} \text{ times} \\ -1-p^{\frac{n}{2}+1}\eta(\Delta'), \\ \quad p^{n-3}+(p-1)p^{\frac{n}{2}-2}\eta(\Delta')-1 \text{ times} \\ -1-p^{\frac{n}{2}+1}\eta(\Delta')\psi(u), \\ \quad p^{n-3}-p^{\frac{n}{2}-2}\eta(\Delta') \text{ times for each } u \in F_p^* \end{cases} \tag{35}$$

and otherwise,

$$C_l(\tau) = \begin{cases} -1, \quad p^n-p^{n-2} \text{ times} \\ -1+p^{\frac{n}{2}+1}\eta((-1)^{\frac{n}{2}-1}\Delta'), \\ \quad p^{n-3}+(p-1)p^{\frac{n}{2}-2}\eta((-1)^{\frac{n}{2}-1}\Delta')-1 \text{ times} \\ -1+p^{\frac{n}{2}+1}\eta((-1)^{\frac{n}{2}-1}\Delta')\psi(u), \\ \quad p^{n-3}-p^{\frac{n}{2}-2}\eta((-1)^{\frac{n}{2}-1}\Delta') \text{ times for each } u \in F_p^*. \end{cases} \tag{36}$$

Proof: From (4), we have

$$C_l(b)+1 = \sum_{x\in F_{p^n}}\omega^{\mathrm{tr}_1^n(\alpha^l x^d-bx)} = \sum_{x\in F_{p^n}}\omega^{Q_l(x)-\mathrm{tr}_1^n(bx)} \tag{37}$$

where $b = \alpha^\tau$. It is easy to check that a nonsingular linear

transformation of variables as (32) can only permute the correlation values and therefore does not affect the distribution of correlation values.

From Lemma 2, the quadratic form $Q_l(x)$ has the rank n or $n-2$. Thus, we will consider the following two cases.

Case 1) $Q_l(x)$ has the full rank n:

Using (32) and $\mathrm{tr}_1^n(bx) = \sum_{i=1}^n b_i x_i$, where $b_i \in F_p$, the cross-correlation function can be rewritten as

$$\begin{aligned}
&C_l(b)+1\\
&=\sum_{(x_1,\cdots,x_n)\in F_p^n} \omega^{\sum_{i=1}^n a_i x_i^2-\sum_{i=1}^n b_i x_i}\\
&=\sum_{(x_1,\cdots,x_n)\in F_p^n} \psi\left(\sum_{i=1}^n a_i\left(x_i-\frac{b_i}{2a_i}\right)^2\right)\psi\left(-\sum_{i=1}^n\frac{b_i^2}{4a_i}\right)\\
&=\psi\left(-\sum_{i=1}^n\frac{b_i^2}{4a_i}\right)\sum_{x_1\in F_p}\psi\left(a_1\left(x_1-\frac{b_1}{2a_1}\right)^2\right)\\
&\quad\sum_{x_2\in F_p}\psi\left(a_2\left(x_2-\frac{b_2}{2a_2}\right)^2\right)\times\cdots\\
&\quad\times\sum_{x_n\in F_p}\psi\left(a_n\left(x_n-\frac{b_n}{2a_n}\right)^2\right) \qquad (38)
\end{aligned}$$

where a_i's are nonzero elements of F_p and $\psi(\cdot)$ is the canonical additive character of F_p, i.e., $\psi(u) = w^u$, $u \in F_p$.

Let $y_i = x_i - b_i/2a_i$ and $a_i y_i^2 = c_i$. If a_i is square (or nonsquare), then c_i will give each square(or nonsquare) of F_p twice when y_i runs through F_p. Using this fact, the value of $\sum_{y_i\in F_p}\psi(a_i y_i^2)$ can be represented as

$$\begin{aligned}
\sum_{y_i\in F_p}\psi(a_i y_i^2) &= \sum_{c_i\in F_p}\psi(c_i)(1+\eta(c_i a_i^{-1}))\\
&=\sum_{c_i\in F_p}\psi(c_i)+\sum_{c_i\in F_p}\psi(c_i)\eta(c_i a_i^{-1})\\
&=\eta(a_i^{-1})G(\eta,\psi) \qquad (39)
\end{aligned}$$

and thus

$$C_l(b)+1=\eta(a_1^{-1}\cdots a_n^{-1})G^n(\eta,\psi)\psi\left(-\sum_{i=1}^n\frac{b_i^2}{4a_i}\right). \qquad (40)$$

It is clear that $\eta(a_1^{-1}a_2^{-1}\cdots a_n^{-1}) = \eta(a_1 a_2\cdots a_n)$.

From Theorem 1, the Gauss sum is given as

$$G(\eta,\psi)=\begin{cases}\sqrt{p}, & \text{if } p\equiv 1 \bmod 4\\ i\sqrt{p}, & \text{if } p\equiv 3 \bmod 4.\end{cases} \qquad (41)$$

Since n is even, we have

$$G^n(\eta,\psi)=\begin{cases}-p^{\frac{n}{2}}, & \text{if } n\equiv 2 \bmod 4 \text{ and } p\equiv 3 \bmod 4\\ p^{\frac{n}{2}}, & \text{otherwise}\end{cases} \qquad (42)$$

and

$$C_l(b)+1=\begin{cases}-p^{\frac{n}{2}}\eta(\Delta)\psi\Big(-\sum_{i=1}^n\frac{b_i^2}{4a_i}\Big),\\ \quad\text{if } n\equiv 2 \bmod 4 \text{ and } p\equiv 3 \bmod 4\\ p^{\frac{n}{2}}\eta(\Delta)\psi\Big(-\sum_{i=1}^n\frac{b_i^2}{4a_i}\Big), \text{ otherwise}\end{cases} \qquad (43)$$

where $\Delta = a_1\cdots a_n$.

Note that $f(b_1, b_2, \cdots, b_n) = -\sum_{i=1}^n b_i^2/4a_i$ is another canonical quadratic form with coefficients $-1/4a_i$, $1 \le i \le n$. Using Theorem 4, we can count the number of solutions of $f(b_1, b_2, \cdots, b_n) = u$ where $u \in F_p$ and obtain the number of occurrences of $C_l(b)$ for $b \in F_{p^n}^*$ as follows.

If $n \equiv 2 \bmod 4$ and $p \equiv 3 \bmod 4$, -1 is a nonsquare and the cross-correlation distribution is derived as

$$C_l(b)+1=\begin{cases}-p^{\frac{n}{2}}\eta(\Delta),\\ \quad p^{n-1}-(p-1)p^{\frac{n}{2}-1}\eta(\Delta)-1 \text{ times}\\ -p^{\frac{n}{2}}\eta(\Delta)\psi(u),\\ \quad p^{n-1}+p^{\frac{n}{2}-1}\eta(\Delta) \text{ times for each } u\in F_p^*\end{cases} \qquad (44)$$

where $\Delta = a_1\cdots a_n$. Otherwise, we have

$$C_l(b)+1=\begin{cases}p^{\frac{n}{2}}\eta((-1)^{\frac{n}{2}}\Delta),\\ \quad p^{n-1}+(p-1)p^{\frac{n}{2}-1}\eta((-1)^{\frac{n}{2}}\Delta)-1 \text{ times}\\ p^{\frac{n}{2}}\eta((-1)^{\frac{n}{2}}\Delta)\psi(u),\\ \quad p^{n-1}-p^{\frac{n}{2}-1}\eta((-1)^{\frac{n}{2}}\Delta) \text{ times}\\ \quad \text{for each } u\in F_p^*.\end{cases} \qquad (45)$$

Case 2) $Q_l(x)$ has the rank $n-2$:

Using the fact that $a_{n-1} = a_n = 0$, the cross-correlation function can be rewritten as

$$\begin{aligned}
&C_l(b)+1\\
&=\sum_{(x_1,\cdots,x_n)\in F_p^n} w^{\sum_{i=1}^{n-2}a_i x_i^2-\sum_{i=1}^n b_i x_i}\\
&=\sum_{(x_1,\cdots,x_n)\in F_p^n}\psi\left(\sum_{i=1}^{n-2}a_i\left(x_i-\frac{b_i}{2a_i}\right)^2\right)\\
&\quad\psi\left(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\right)\psi(-b_{n-1}x_{n-1}-b_n x_n)\\
&=\sum_{(x_1,\cdots,x_{n-2})\in F_p^{n-2}}\psi\left(\sum_{i=1}^{n-2}a_i\left(x_i-\frac{b_i}{2a_i}\right)^2\right)\psi\left(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\right)\\
&\quad\times\sum_{(x_{n-1},x_n)\in F_p^2}\psi(-b_{n-1}x_{n-1}-b_n x_n). \qquad (46)
\end{aligned}$$

Note that the inner summation is p^2 if $b_{n-1} = b_n = 0$ or 0, otherwise. Since there are $p^n - p^{n-2}$ b's such that $b_{n-1} \neq 0$ or $b_n \neq 0$, $C_l(b)+1 = 0$ occurs $p^n - p^{n-2}$ times. If $b_{n-1} = b_n = 0$, we have

$$C_l(b)+1 = p^2\psi\left(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\right)\sum_{x_1\in F_p}\psi\left(a_1\left(x_1-\frac{b_1}{2a_1}\right)^2\right)\sum_{x_2\in F_p}\psi\left(a_2\left(x_2-\frac{b_2}{2a_2}\right)^2\right)\times\cdots\times\sum_{x_{n-2}\in F_p}\psi\left(a_{n-2}\left(x_{n-2}-\frac{b_{n-2}}{2a_{n-2}}\right)^2\right). \quad (47)$$

Let $y_i = x_i - b_i/2a_i$ and $a_i y_i^2 = c_i$. Then, similarly to Case 1, we have

$$\sum_{y_i\in F_p}\psi(a_i y_i^2) = \eta(a_i^{-1})G(\eta,\psi) \quad (48)$$

and then

$$C_l(b)+1 = p^2\eta(a_1^{-1}\cdots a_{n-2}^{-1})G^{n-2}(\eta,\psi)\psi\left(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\right). \quad (49)$$

From Theorem 1, we have

$$G^{n-2}(\eta,\psi) = \begin{cases} -p^{\frac{n}{2}-1}, \\ \quad \text{if } n\equiv 0 \bmod 4 \text{ and } p\equiv 3 \bmod 4 \\ p^{\frac{n}{2}-1}, \text{ otherwise} \end{cases} \quad (50)$$

and we have

$$C_l(b)+1 = \begin{cases} -p^{\frac{n}{2}+1}\eta(\Delta')\psi\left(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\right), \\ \quad \text{if } n\equiv 0 \bmod 4 \text{ and } p\equiv 3 \bmod 4 \\ p^{\frac{n}{2}+1}\eta(\Delta')\psi\left(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\right), \text{ otherwise} \end{cases} \quad (51)$$

where $\Delta' = a_1\cdots a_{n-2}$.

Using Theorem 4, we can obtain the number of occurrences of $C_l(b)$ for $b\in F_{p^n}^*$ as follows.
If $n\equiv 0 \bmod 4$ and $p\equiv 3 \bmod 4$, the cross-correlation distribution is derived as

$$C_l(b)+1 = \begin{cases} 0, \ p^n - p^{n-2} \text{ times} \\ -p^{\frac{n}{2}+1}\eta(\Delta'), \\ p^{n-3} + (p-1)p^{\frac{n}{2}-2}\eta(\Delta') - 1 \text{ times} \\ -p^{\frac{n}{2}+1}\eta(\Delta')\psi(u), \\ p^{n-3} - p^{\frac{n}{2}-2}\eta(\Delta') \text{ times for each } u\in F_p^* \end{cases} \quad (52)$$

and otherwise,

$$C_l(b)+1 = \begin{cases} 0, \ p^n - p^{n-2} \text{ times} \\ p^{\frac{n}{2}+1}\eta((-1)^{\frac{n}{2}-1}\Delta'), \\ p^{n-3} + (p-1)p^{\frac{n}{2}-2}\eta((-1)^{\frac{n}{2}-1}\Delta') - 1 \text{ times} \\ p^{\frac{n}{2}+1}\eta((-1)^{\frac{n}{2}-1}\Delta')\psi(u), \\ p^{n-3} - p^{\frac{n}{2}-2}\eta((-1)^{\frac{n}{2}-1}\Delta') \text{ times for each } u\in F_p^* \end{cases} \quad (53)$$

because if $n\equiv 0 \bmod 4$, -1 is a quadratic residue.

□

Thus, using a p-ary m-sequence $s(t)$ and its $p+1$ distinct decimated sequences $s_l(dt)$ in (3), we can construct the family $\mathcal{S}$ of p-ary sequences of period p^n-1 with family size p^n and $C_{\max} = p\sqrt{p^n}+1$ as

$$\mathcal{S} = \{s_\beta(t) = \mathrm{tr}_1^n(\alpha^t + \beta\alpha^{dt}) \mid \beta\in F_{p^n},\ 0\le t\le p^n-2\} \quad (54)$$

where p is an odd prime, n is an even integer, and $d = p^k+1$ with $\gcd(n,k)=1$. Note that when we calculate the cross-correlation values for p-ary sequences in $\mathcal{S}$, we may have the cross-correlation value $\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(ax^d)}$, which corresponds to $C_l(b)$ with $b=0$ in (4). From Theorem 5, we can obtain

$$\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(ax^d)} = \begin{cases} -1 - p^{\frac{n}{2}}\eta((-1)^{\frac{n}{2}}\Delta), \\ \quad \text{if } Q_l(x) \text{ has full rank} \\ -1 - p^{\frac{n}{2}+1}\eta((-1)^{\frac{n}{2}-1}\Delta'), \\ \quad \text{otherwise.} \end{cases} \quad (55)$$

Thus, $C_{\max}$ for $\mathcal{S}$ becomes

$$C_{\max} = p\sqrt{p^n}+1. \quad (56)$$

5. Conclusion

In this paper, the cross-correlation distribution between a p-ary m-sequence $s(t)$ and its decimated sequences $s(dt+l)$, $0\le l<p+1$, is derived. By using $s(t)$ and $s(dt+l)$, a new family of p-ary sequences of period p^n-1 is constructed, whose family size is p^n and $C_{\max}$ is $1+p\sqrt{p^n}$. It is interesting to find p-ary sequence families with good correlation property, which can be used for applications such as code-division multiple-access communication systems.

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, 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, March 1989.
[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, P. Felke, T. Helleseth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," IEEE Trans. Inf. Theory, vol.52, no.2, pp.613–627, Feb. 2006.
[7] 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.

[8] 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.
[9] 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.
[10] 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.
[11] L.E. Dickson, Linear Groups with an Exposition of the Galois Field Theory, Dover, New York, 1958.
[12] R. Lidl and H. Niederreiter, Finite Fields, vol.20 of Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.
[13] V.M. Sidel'nikov, "On mutual correlation of sequences," Soviet Math. Dokl., vol.12, no.1, pp.197–201, 1971.
[14] J.D. Olsen, R.A. Scholtz, and L.R. Welch, "Bent-function sequences," IEEE Trans. Inf. Theory, vol.28, no.6, pp.858–864, Nov. 1982.
[15] 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.

Eun-Young Seo received the B.S. and M.S. degrees in electrical engineering and computer science from Seoul National University, Seoul, Korea, in 2005 and 2007, respectively. Since March 2007, she is a researcher at Institute of New Media and Communication, Seoul National University, Seoul, Korea. Her research interests include pseudo-noise (PN) sequences and communication theory.

Young-Sik Kim received the B.S, M.S., and Ph.D. degrees in electrical engineering and computer science from Seoul National University, Seoul, Korea, in 2001, 2003, and 2007, respectively. Since March 2007, he is a senior engineer at Samsung Electronic, Co., Ltd., Korea. His research interests include pseudo-noise (PN) sequences, random number generation, cryptography, and error correcting codes.

Jong-Seon No received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988. He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, Korea, from September 1990 to July 1999. He joined the faculty of the School of Electrical Engineering and Computer Science, Seoul National University, in August 1999, where he is currently a Professor. His area of research interests includes error-correcting codes, sequences, cryptography, space-times codes, LDPC codes, and wireless communication systems.

Dong-Joon Shin received the B.S. degree in electronics engineering from Seoul National University, Seoul, Korea, the M.S. degree in electrical engineering from Northwestern University, Evanston, USA, and the Ph.D. degree in electrical engineering from University of Southern California, Los Angeles, USA. From 1999 to 2000, he was a member of technical staff in Wireless Network Division and Satellite Network Division, Hughes Network Systems, Maryland, USA. Since September 2000, he has been an Associate Professor in the Division of ECE at Hanyang University, Seoul, Korea. His current research interests include error-correcting codes, sequences, and discrete mathematics.