PAPER

Upper Bound on the Cross-Correlation between Two Decimated Sequences

Chang-Min CHO†a), Wijik LEE†b), *Nonmembers*, Jong-Seon NO†c), *and* Young-Sik KIM††d), *Members*

SUMMARY In this paper, for an odd prime p, two positive integers n, m with $n = 2m$, and $p^m \equiv 1 \pmod 4$, we derive an upper bound on the magnitude of the cross-correlation function between two decimated sequences of a p-ary m-sequence. The two decimation factors are 2 and $2(p^m + 1)$, and the upper bound is derived as $\frac{3}{2}p^m + \frac{1}{2}$. In fact, those two sequences correspond to the p-ary sequences used for the construction of Kasami sequences decimated by 2. This result is also used to obtain an upper bound on the cross-correlation magnitude between a p-ary m-sequence and its decimated sequence with the decimation factor $d = \frac{(p^m+1)^2}{2}$.

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

1. Introduction

In pseudorandom sequence design, finding sequences with low correlation property has been of great interest. Such sequences have various applications in code-division multiple-access (CDMA), radar, cryptography, and so on. To find sequence families with low correlation, lots of studies have attempted to find the cross-correlation between an m-sequence and its decimated sequences. The readers may refer to [1]–[12] for details on this topic.

Recently, the cross-correlation between two differently decimated sequences has been studied. Kim et al. [13] constructed a p-ary sequence family with low correlation by using two decimated sequences, where $p \equiv 3 \pmod 4$ is an odd prime, n is an odd integer, and the decimation factors are 2 and $2(\frac{p^n-1}{2} - p^{n-1})$. The results in [13] were generalized in [14], where the decimation factors are e and $e(\frac{p^n-1}{e} - p^{n-1})$ with $e|p^n - 1$ and $e < \frac{\sqrt{p^n}-1/\sqrt{p^n}}{2}$. Xia and Chen [15] constructed a p-ary sequence family by using sequences with decimation factors 2 and $p^m + 1$, and derived its correlation distribution. Lee et al. [16] obtained an upper bound on the cross-correlation magnitude of two decimated p-ary sequences and constructed new sequence families. The maximum correlation bound was derived by using Weil's bound [20] on exponential sums. In [17] and [18], the cross-correlation between p-ary sequences with decimation factors 2 and $d' = 2d$ was investigated, where the values d were studied in [1], [7], and [11]. Note that in most cases, one of the two decimation factors is 2 and then the sequence families constructed have period $\frac{p^n-1}{2}$, which is the half of that of an m-sequence.

In this paper, an upper bound on the magnitude of the cross-correlation between two decimated p-ary sequences is determined, where the decimation factors are 2 and $2(p^m+1)$ with $n = 2m$ and $p^m \equiv 1 \pmod 4$. In fact, those two sequences correspond to the p-ary sequences used for the construction of Kasami sequences decimated by 2. The upper bound is derived as $\frac{3}{2}p^m + \frac{1}{2}$, which is the same as that of [16]. It is obtained by showing equivalence to the exponential sum in [16] and applying Weil's bound.

Also, using the above result of the cross-correlation between two decimated sequences, an upper bound of cross-correlation magnitude between a p-ary m-sequence and its decimated sequence is derived. The decimation factor is $(p^m + 1)^2/2$, where $n = 2m$ and $p^m \equiv 1 \pmod 4$. Note that this decimation factor was investigated previously in [18] to construct a sequence family of half period.

The remainder of this paper is organized as follows. In Sect. 2, we give some notations and preliminaries for the trace function, sequences, and the character sums. In Sect. 3, we present upper bounds on the cross-correlation between two p-ary sequences. The concluding remarks are given in Sect. 4.

2. Preliminaries

Let p be an odd prime, m be a positive integer satisfying $p^m \equiv 1 \pmod 4$, and $n = 2m$. Let F_{p^n} denote the finite field with p^n elements and $F^*_{p^n} = F_{p^n}\backslash\{0\}$. The *trace function* $\mathrm{tr}^n_k(\cdot)$ from F_{p^n} to its subfield F_{p^k} is defined as

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

An element x in F_{p^n} can be expressed as

$$x = \sum_{i=1}^{\frac{n}{k}} c_i\alpha_i$$

where $c_i \in F_{p^k}$ and $\{\alpha_1, \ldots, \alpha_{n/k}\}$ is a basis of F_{p^n} over F_{p^k}.

Manuscript received May 3, 2016.
Manuscript revised October 13, 2016.
Manuscript publicized November 28, 2016.

†The authors are with the Department of ECE, INMC, Seoul National University, Seoul 151-744, Korea.
††The author is with the Department of Information and Communication Engineering, Chosun University, Gwangju 501-759, Korea.
a) E-mail: ccm8686@ccl.snu.ac.kr
b) E-mail: leewj422@ccl.snu.ac.kr
c) E-mail: jsno@snu.ac.kr
d) E-mail: iamyskim@chosun.ac.kr

DOI: 10.1587/transcom.2016EBP3182

The basis $\{\alpha_1, \ldots, \alpha_{n/k}\}$ is said to be *trace-orthogonal* if

$$\mathrm{tr}_k^n(\alpha_i\alpha_j) = \begin{cases} d_i, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases}$$

where $d_i \in F_{p^k}^*$. It is known that for any odd prime p, there exists a trace-orthogonal basis of F_{p^n} over F_{p^k} [19].

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 as

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

and its decimated sequences $s(dt + l)$ are given as

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

The cross-correlation function of two p-ary sequences $a(t)$ and $b(t)$ of period N is defined as

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

where $\omega = e^{2\pi\sqrt{-1}/p}$ is a primitive p-th root of unity.

For a finite abelian group G, a *character* of G is a homomorphism from G to the multiplicative group of complex numbers with absolute value 1. For a finite field, there are two kinds of characters, namely, an additive character and a multiplicative character.

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

$$\chi_1(x) = \omega^{tr_1^n(x)} \text{ for all } x \in F_{p^n}$$

and every additive character of F_{p^n} can be obtained as $\chi_b(x) = \chi_1(bx)$, for all $b, x \in F_{p^n}$.

A multiplicative character of F_{p^n} is defined as

$$\psi_j(\alpha^k) = e^{\frac{2\pi\sqrt{-1}jk}{p^n-1}} \text{ for } k = 0, 1, \ldots, p^n - 2.$$

If $j = (p^n - 1)/2$, then the character $\eta(x) = \psi_{(p^n-1)/2}(x)$ takes the value 1 if x is the square in $F_{p^n}^*$ and -1 if x is the nonsquare. This multiplicative character $\eta(x)$ is called the quadratic character of F_{p^n}.

The following lemma for the character sums, which is given by Weil [20], will be used in this paper.

Lemma 1: (Weil's bound [20]) Let $q = p^n$, χ be an additive character of the finite field F_q, and ψ a multiplicative character of F_q of order m. Let $f(x) \in F_q[x]$ be of degree $e \geq 1$ and $g(x) \in F_q[x]$ be with s distinct roots in $\bar{F}_q[x]$, where $g \neq c \cdot h^m$ for some $c \in F_q$, $f \neq h^p - h$ for $h \in \bar{F}_q[x]$, and $\bar{F}_q$ denotes the algebraic closure of F_q. Then we have

$$\left| \sum_{x \in F_q} \psi(g(x))\chi(f(x)) \right| \leq (e + s - 1)\sqrt{q}.$$

□

3. Main Results

3.1 The Cross-Correlation between $s(2t + i)$ and $s(2(p^m + 1)t + j)$

The cross-correlation function between $s(2t+i)$ and $s(2(p^m+1)t + j)$ of period $(p^n - 1)/2$ is given as

$$C_{i,j}(\tau) = \sum_{t=0}^{\frac{p^n-1}{2}-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i} - \alpha^{2(p^m+1)t+j})} \tag{1}$$

where $\gcd(p^n - 1, 2(p^m + 1)) = 2(p^m + 1)$, $i = 0, 1$, and $j = 0, p^m + 1$. In fact, those two sequences correspond to the p-ary sequences used for the construction of Kasami sequences decimated by 2. In this subsection, we derive the cross-correlation bound for the above two decimated sequences. It is easy to check that

$$\sum_{t=0}^{\frac{p^n-1}{2}-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i} - \alpha^{2(p^m+1)t+j})} = \sum_{t=\frac{p^n-1}{2}}^{p^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i} - \alpha^{2(p^m+1)t+j})}$$

and thus we can express the cross-correlation as

$$\begin{aligned} C_{i,j}(\tau) &= \frac{1}{2} \sum_{t=0}^{p^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)+i} - \alpha^{2(p^m+1)t+j})} \\ &= \frac{1}{2} \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax^2 - bx^{2(p^m+1)})} \end{aligned} \tag{2}$$

where $x = \alpha^t$, $a = \alpha^{2\tau+i}$, and $b = \alpha^j$. Let $y = x^2$ and QR denote the set of squares in $F_{p^n}^*$. Then as x runs through $F_{p^n}^*$, y runs through QR twice. Therefore, (2) can be rewritten as

$$\begin{aligned} C_b(a) &= \sum_{y \in QR} \omega^{\mathrm{tr}_1^n(ay - by^{p^m+1})} \\ &= \frac{1}{2}\left[\sum_{y \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ay - by^{p^m+1})} \right. \\ &\quad \left. + \sum_{y \in F_{p^n}^*} \eta(y)\omega^{\mathrm{tr}_1^n(ay - by^{p^m+1})} \right]. \end{aligned} \tag{3}$$

We want to find the upper bound of the cross-correlation magnitude $|C_b(a)|$. It is obvious from the correlation property of p-ary Kasami sequences that [21]

$$\left| \sum_{y \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ay - by^{p^m+1})} \right| \leq p^m + 1. \tag{4}$$

In order to prove our main theorem, the following results are needed.

Lemma 2: For an odd prime p, two integers n, m with $n = 2m$, and $p^m \equiv 1 \pmod 4$, there exist a', b', and $z \in F^*_{p^n}$ satisfying

$$\mathrm{tr}_1^n(ay - by^{p^m+1}) = \mathrm{tr}_1^n(a'z - b'z^2) \tag{5}$$

where as y runs through $F^*_{p^n}$, z also runs through all elements in $F^*_{p^n}$.

Proof: Using the property of the trace function, we have

$$\mathrm{tr}_1^n(by^{p^m+1}) = \mathrm{tr}_1^m(\mathrm{tr}_m^n(by^{p^m+1})) = \mathrm{tr}_1^m(2by^{p^m+1})$$

because $b = 1$ or $\alpha^{p^m+1} \in F_{p^m}$ and $y^{p^m+1} \in F_{p^m}$. Let $y = c_1\alpha_1 + c_2\alpha_2$, where $\{\alpha_1, \alpha_2\}$ is a trace-orthogonal basis of F_{p^n} over F_{p^m} and $c_1, c_2 \in F_{p^m}$. Then, we have

$$\begin{aligned}\mathrm{tr}_m^n(by^{p^m+1}) &= 2b(c_1\alpha_1 + c_2\alpha_2)^{p^m+1}\\ &= 2b(c_1^2\alpha_1^{p^m+1} + c_1c_2(\alpha_1^{p^m}\alpha_2 + \alpha_1\alpha_2^{p^m}) + c_2^2\alpha_2^{p^m+1})\\ &= 2b(c_1^2\alpha_1^{p^m+1} + c_1c_2(\mathrm{tr}_m^n(\alpha_1^{p^m}\alpha_2)) + c_2^2\alpha_2^{p^m+1}).\end{aligned} \tag{6}$$

It is easy to check that the sequence $\mathrm{tr}_1^m(2by^{p^m+1})$ is always the same sequence of period $p^m - 1$ with respect to cyclic shift. Therefore, we assume that $b = 1$ and then (6) becomes

$$\begin{aligned}&\mathrm{tr}_m^n(y^{p^m+1})\\ &= 2(c_1^2\alpha_1^{p^m+1} + c_1c_2(\mathrm{tr}_m^n(\alpha_1^{p^m}\alpha_2)) + c_2^2\alpha_2^{p^m+1}).\end{aligned} \tag{7}$$

For $\mathrm{tr}_1^n(b'z^2) = \mathrm{tr}_1^m(\mathrm{tr}_m^n(b'z^2))$ in (5), we can assume that $b' \in QR$. Then without loss of generality, we can let $b' = 1$ because we can choose another element $z' \in F_{p^n}$ such that $z'^2 = b'z^2$. Now let $z = e_1\alpha_1 + e_2\alpha_2$, $e_1, e_2 \in F_{p^m}$ and then $\mathrm{tr}_m^n(z^2)$ can be rewritten as

$$\begin{aligned}\mathrm{tr}_m^n(z^2) &= \mathrm{tr}_m^n((e_1\alpha_1 + e_2\alpha_2)^2)\\ &= e_1^2\mathrm{tr}_m^n(\alpha_1^2) + e_1e_2\mathrm{tr}_m^n(\alpha_1\alpha_2) + e_2^2\mathrm{tr}_m^n(\alpha_2^2)\\ &= e_1^2 d_1 + e_2^2 d_2\end{aligned} \tag{8}$$

where $d_1, d_2 \in F^*_{p^m}$ and the last equality holds from the property of trace-orthogonal basis.

From (7), we can choose the basis $\{\alpha_1, \alpha_2\}$ such that $\mathrm{tr}_m^n(\alpha_1^{p^m}\alpha_2) = 0$ as follows. From the property of trace-orthogonal basis, we have

$$\begin{aligned}\mathrm{tr}_m^n(\alpha_1\alpha_2) &= \alpha_1\alpha_2 + \alpha_1^{p^m}\alpha_2^{p^m}\\ &= \alpha_1\alpha_2(1 + \alpha_1^{p^m-1}\alpha_2^{p^m-1})\\ &= 0\end{aligned}$$

and thus we have

$$\alpha_1^{p^m-1} = -\alpha_2^{1-p^m}. \tag{9}$$

Suppose that

$$\begin{aligned}\mathrm{tr}_m^n(\alpha_1^{p^m}\alpha_2) &= \alpha_1^{p^m}\alpha_2 + \alpha_1\alpha_2^{p^m}\\ &= \alpha_1\alpha_2(\alpha_1^{p^m-1} + \alpha_2^{p^m-1})\\ &= 0.\end{aligned}$$

Then from (9), we have

$$(\alpha_1^{p^m-1})^2 = 1 \text{ and } (\alpha_2^{p^m-1})^2 = 1. \tag{10}$$

From (9) and (10), we have

$$\begin{aligned}&\alpha_1^{p^m-1} = 1 \text{ and } \alpha_2^{p^m-1} = -1\\ \text{or } &\alpha_1^{p^m-1} = -1 \text{ and } \alpha_2^{p^m-1} = 1.\end{aligned} \tag{11}$$

Any choice of (α_1, α_2) in (11) satisfies the trace-orthogonal property and the equation $\mathrm{tr}_m^n(\alpha_1^{p^m}\alpha_2) = 0$. Thus from now on, we simply let

$$\alpha_1 = 1 \text{ and } \alpha_2 = \alpha^{\frac{p^m+1}{2}}. \tag{12}$$

Then (7) becomes

$$\mathrm{tr}_m^n(y^{p^m+1}) = 2(c_1^2 + c_2^2\alpha^{\frac{(p^m+1)^2}{2}})$$

and (8) becomes

$$\mathrm{tr}_m^n(z^2) = 2(e_1^2 + e_2^2\alpha^{p^m+1}).$$

Then we can choose c_1, c_2, e_1, and e_2 such that $\mathrm{tr}_m^n(y^{p^m+1}) = \mathrm{tr}_m^n(z^2)$ holds. One simple choice of c_1, c_2, e_1, and e_2 is as follows:

$$c_1 = e_1 \text{ and } c_2 = \alpha^{\frac{p^n-1}{4}}e_2. \tag{13}$$

Next, we find the values a and a' such that the equation $\mathrm{tr}_m^n(ay) = \mathrm{tr}_m^n(a'z)$ holds, where the relationship between y and z is given in (13). Let $a = u_1\alpha_1 + u_2\alpha_2$ and $a' = v_1\alpha_1 + v_2\alpha_2$, where $u_1, u_2, v_1, v_2 \in F_{p^m}$. Then $\mathrm{tr}_m^n(ay)$ can be rewritten as

$$\begin{aligned}\mathrm{tr}_m^n(ay) &= \mathrm{tr}_m^n((u_1\alpha_1 + u_2\alpha_2)(c_1\alpha_1 + c_2\alpha_2))\\ &= \mathrm{tr}_m^n(c_1u_1\alpha_1^2 + (c_1u_2 + c_2u_1)\alpha_1\alpha_2 + c_2u_2\alpha_2^2).\end{aligned}$$

By choosing the trace-orthogonal basis as in (12), we have

$$\mathrm{tr}_m^n(ay) = 2(c_1u_1 + c_2u_2\alpha^{p^m+1})$$

and similarly,

$$\mathrm{tr}_m^n(a'z) = 2(e_1v_1 + e_2v_2\alpha^{p^m+1}).$$

Suppose that $\mathrm{tr}_m^n(ay) = \mathrm{tr}_m^n(a'z)$, where c_1, c_2, e_1, and e_2 are given in (13). Then we have

$$e_1u_1 + e_2u_2\alpha^{p^m+1+\frac{p^n-1}{4}} = e_1v_1 + e_2v_2\alpha^{p^m+1}. \tag{14}$$

There are many choices of u_1, u_2, v_1, and v_2 satisfying (14). A straightforward example is given as

$$u_1 = v_1 \text{ and } \alpha^{\frac{p^n-1}{4}}u_2 = v_2. \tag{15}$$

From the discussions above, we have found a condition for the functions $\mathrm{tr}_m^n(ay - y^{p^m+1})$ and $\mathrm{tr}_m^n(a'z - z^2)$ to be equivalent. Clearly, for fixed a and a' satisfying (15), as y runs through $F^*_{p^n}$, z satisfying (13) runs through $F^*_{p^n}$. Also note that for $b = \alpha^{p^m+1}$ and any square b', we can find the relationship between (a, y) and (a', z) such that (5) holds in the similar way. □

Theorem 3: For an odd prime p, two integers n, m with $n = 2m$, and $p^m \equiv 1 \pmod 4$, the magnitude of the following 'mixed' exponential sum is upper bounded as

$$\left|\sum_{y\in F_{p^n}^*} \eta(y)\omega^{\mathrm{tr}_1^n(ay-by^{p^m+1})}\right| \le 2p^m. \tag{16}$$

Proof: Let g be a function in $F_{p^n}[x]$ which maps z to y. It can be proved that such a function g exists and it has only one root 0 as follows. Consider the case $b = b' = 1$. The basis is given in (12) and the relationship between y and z is given in (13). Suppose that $g(z) = y$. From $z = e_1 + e_2\alpha^{(p^m+1)/2}$ and the property of the trace function, we have

$$2^{-1}\mathrm{tr}_m^n(z) = c_1$$

because $\mathrm{tr}_m^n(\alpha^{(p^m+1)/2}) = 0$ and $e_1, e_2 \in F_{p^m}$. And similarly, we have

$$2^{-1}\cdot\alpha^{\frac{p^n-1}{4}}\mathrm{tr}_m^n(z\cdot\alpha^{-\frac{p^m+1}{2}}) = c_2.$$

Therefore, the function g can be given as

$$g(z) = 2^{-1}(\mathrm{tr}_m^n(z) + \alpha^{\frac{(p^m+1)^2}{4}}\cdot\mathrm{tr}_m^n(z\cdot\alpha^{-\frac{p^m+1}{2}})).$$

It is obvious that $g(z)$ is a 1-to-1 function and has 0 as only one root. For $b = \alpha^{p^m+1}$ and any $b' \in QR$, the function $g: z \to y$ can also be obtained similarly.

Now from Lemma 1, we have

$$\left|\sum_{z\in F_{p^n}^*} \eta(g(z))\omega^{\mathrm{tr}_1^n(a'z-b'z^2)}\right| \le 2p^m.$$

Using Lemma 2 and $y = g(z)$, we have

$$\left|\sum_{y\in F_{p^n}^*} \eta(y)\omega^{\mathrm{tr}_1^n(ay-by^{p^m+1})}\right| \le 2p^m$$

and thus it is proved. □

Now we give our main theorem for the cross-correlation between two decimated sequences.

Theorem 4: Let p be an odd prime, n, m be the positive integers such that $n = 2m$ with $p^m \equiv 1 \pmod 4$, $i = 0, 1$, and $j = 0, p^m + 1$. Let $s(t)$ be a p-ary m-sequence of period $p^n - 1$. Then the magnitude of the cross-correlation function between its decimated sequences $s(2t + i)$ and $s(2(p^m + 1)t + j)$ is upper bounded as

$$|C_b(a)| \le \frac{3}{2}p^m + \frac{1}{2}.$$

Proof: Combining (4) and (16), the magnitude of the cross-correlation function in (3) can be given as

$$\begin{aligned}|C_b(a)| &\le \frac{1}{2}\left|\sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ay-by^{p^m+1})}\right| \\ &\quad + \frac{1}{2}\left|\sum_{y\in F_{p^n}^*} \eta(y)\omega^{\mathrm{tr}_1^n(ay-by^{p^m+1})}\right| \\ &\le \frac{3}{2}p^m + \frac{1}{2}.\end{aligned}$$

□

Here are two examples of the above theorem.

Example 5: Let $p = 5$, $n = 6$, and $m = 3$. Then $2(p^m + 1) = 252$ and by computer experiment, the maximum cross-correlation magnitude is given as 174.045, which is smaller than $\frac{3}{2}p^m + \frac{1}{2} = 188$. The number of distinct correlation values is given as 80.

Example 6: Let $p = 11$, $n = 4$, and $m = 2$. Then $2(p^m + 1) = 244$ and by numerical computations, the maximum cross-correlation magnitude is given as 181.83, which is smaller than $\frac{3}{2}p^m + \frac{1}{2} = 182$. The number of distinct correlation values is given as 130.

Note that for sequences with long period (i.e., large n or p), the maximum cross-correlation magnitude becomes close to the upper bound and the number of distinct correlation values increases as n or p increases.

From the numerical analysis, we believe that the result in Theorem 4 also holds when $p^m \equiv 3 \pmod 4$. But that is not easy to prove because it is difficult to find values a' and z satisfying (5).

Suppose that $\mathrm{tr}_m^n(y^{p^m+1}) = \mathrm{tr}_m^n(b'z^2)$ holds. For $p^m \equiv 3 \pmod 4$ case, it can be shown that no $b' \in QR$ can satisfy the equation above. Thus we assume that b' is a nonsquare and then without loss of generality, we can let $b' = \alpha$. Similar to (8), $\mathrm{tr}_m^n(\alpha z^2)$ can be rewritten as

$$\begin{aligned}\mathrm{tr}_m^n(\alpha z^2) &= \mathrm{tr}_m^n(\alpha(e_1\alpha_1 + e_2\alpha_2)^2) \\ &= e_1^2\mathrm{tr}_m^n(\alpha\alpha_1^2) + e_1e_2\mathrm{tr}_m^n(\alpha\alpha_1\alpha_2) + e_2^2\mathrm{tr}_m^n(\alpha\alpha_2^2).\end{aligned} \tag{17}$$

From (7) and (17), finding a condition for c_1, c_2, e_1, and e_2 to have $\mathrm{tr}_m^n(y^{p^m+1}) = \mathrm{tr}_m^n(\alpha z^2)$ does not seem to be an easy task. Thus we leave it as a future work and propose a following conjecture:

Conjecture 7: Let p be an odd prime, n, m be positive integers with $n = 2m$, $i = 0, 1$, and $j = 0, p^m + 1$. Let $s(t)$ be a p-ary m-sequence of period $p^n - 1$. Then the magnitude of the cross-correlation function between its decimated sequences $s(2t + i)$ and $s(2(p^m + 1)t + j)$ is upper bounded as

$$|C_b(a)| \le \frac{3}{2}p^m + \frac{1}{2}.$$

□

3.2 The Cross-Correlation between $s(t)$ and $s(\frac{(p^m+1)^2}{2}t)$

In [18], the cross-correlation between two decimated sequences $s(2t+i)$ and $s(\frac{(p^m+1)^2}{2}t)$ is investigated, where $s(t)$ is a p-ary m-sequence of period p^n-1, $n=2m$, and $p^m \equiv 1 \pmod 4$. In this subsection, we study the cross-correlation function between $s(t)$ and $s(\frac{(p^m+1)^2}{2}t)$, and derive the upper bound of the cross-correlation magnitude.

Theorem 8: Let p be an odd prime and n, m be the positive integers such that $n=2m$ with $p^m \equiv 1 \pmod 4$. Let $s(t)$ be a p-ary m-sequence of period p^n-1. Then the magnitude of the cross-correlation function between $s(t)$ and its decimated sequence $s(\frac{(p^m+1)^2}{2}t)$ is upper bounded as

$$|C(\tau)| \le 3p^m+1.$$

Proof: The cross-correlation function between $s(t)$ and $s(\frac{(p^m+1)^2}{2}t)$ is given as

$$\begin{aligned} C(\tau) &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{t+\tau}-\alpha^{\frac{(p^m+1)^2}{2}t})} \\ &= \sum_{x\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(\gamma x - x^{\frac{(p^m+1)^2}{2}})} \qquad (18) \end{aligned}$$

where $x=\alpha^t$ and $\gamma=x^\tau$. Let $x=y^2$ when x is a square and $x=\sigma y^2$ when x is a nonsquare, where σ is a fixed nonsquare in $F_{p^n}^*$. Then (18) can be rewritten as

$$\begin{aligned} C(\tau) = \frac{1}{2}\Bigg[&\sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(\gamma y^2 - y^{(p^m+1)^2})} \\ &+ \sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(\gamma\sigma y^2 - \sigma' y^{(p^m+1)^2})}\Bigg] \qquad (19) \end{aligned}$$

where $\sigma' = \sigma^{\frac{(p^m+1)^2}{2}}$. Since $(p^m+1)^2 = p^n+2p^m+1 \equiv 2(p^m+1) \pmod{p^n-1}$, we have

$$\begin{aligned} |C(\tau)| &= \frac{1}{2}\Bigg| \sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(\gamma y^2 - y^{2(p^m+1)})} + \sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(\gamma\sigma y^2 - \sigma' y^{2(p^m+1)})}\Bigg| \\ &\le \frac{1}{2}\Bigg[\Bigg| \sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(\gamma y^2 - y^{2(p^m+1)})}\Bigg| + \Bigg| \sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(\gamma\sigma y^2 - \sigma' y^{2(p^m+1)})}\Bigg|\Bigg] \\ &\le 3p^m+1. \qquad (20) \end{aligned}$$

The last inequality comes from (2) and Theorem 4, and the proof is complete. □

Some numerical analysis implies that the bound obtained in Theorem 8 may not be tight. For example, for $p=11$ and $n=4$, by computer experiment the maximum cross-correlation magnitude is given as 242.241, which is far smaller than the upper bound $3p^m+1=367$ from Theorem 8. Tighter upper bound may be found by more detailed investigation on the cross-correlation function. We remain this as a further work.

4. Conclusion

In this paper, some new results on the cross-correlation between two p-ary sequences are proposed. First, we derived an upper bound on the magnitude of the cross-correlation function between two decimated sequences of a p-ary m-sequence. Those sequences are given as $s(2t+i)$ and $s(2(p^m+1)+j)$, where p is an odd prime, n, m are positive integers with $n=2m$, $p^m \equiv 1 \pmod 4$, and $s(t)$ is a p-ary m-sequence of period p^n-1. The condition for two functions $\mathrm{tr}_1^n(ay-by^{p^m+1})$ and $\mathrm{tr}_1^n(a'z-b'z^2)$ to be equivalent is found and then using Weil's bound, the upper bound $\frac{3}{2}p^m+\frac{1}{2}$ is obtained.

Additionally, we give an upper bound on the magnitude of the cross-correlation between $s(t)$ and $s(\frac{(p^m+1)^2}{2}t)$. This upper bound is obtained by using the above result and is given as $3p^m+1$.

From the cross-correlation results given above, new sequence families with good correlation can be considered. Thus as a future work, we will research on the construction of sequence families using the sequences studied in this paper.

Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (B0717-16-0130, Research on Lightweight Post-Quantum Crypto-systems for IoT and Cloud Computing).

References

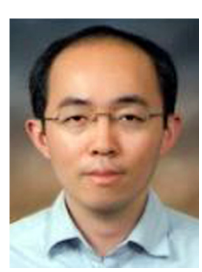
[1] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," Discrete Math., vol.16, no.3, pp.209–232, 1976.
[2] E.N. Müller, "On the cross-correlation of sequences over $GF(p)$ with short periods," IEEE Trans. Inf. Theory, vol.45, no.1, pp.289–295, Jan. 1999.
[3] G.J. Ness, T. Helesseth, and A. Kholosha, "On the correlation distribution of the Coulter-Mattews decimation," IEEE Trans. Inf. Theory, vol.52, no.5, pp.2241–2247, May 2006.
[4] 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. Fundamentals, vol.E90-A, no.11, pp.2568–2574, Nov. 2007.
[5] 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 $((p^{2k}+1)/2)^2$," IEEE Trans. Inf. Theory, vol.54, no.7, pp.3140–3149, July 2008.
[6] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter-Matthews function," IEEE Trans. Inf. Theory, vol.54, no.12, pp.5345–5353, Dec. 2008.

[7] J. Luo, "Cross correlation of nonbinary Niho-type sequences," Proc. IEEE Int. Symp. Information Theory, pp.1297–1299, Austin, USA, June 2010.
[8] S.T. Choi, J.Y. Kim, and J.S. No, "On the cross-correlation of a p-ary m-sequence and its decimated sequences by $d = \frac{p^n+1}{p^k+1} + \frac{p^n-1}{2}$," IEICE Trans. Commun., vol.E96-B, no.9, pp.2190–2197, Sept. 2013.
[9] Y. Xia, S. Chen, T. Helleseth, and C. Li, "Cross-correlation between a p-ary m-sequence and its all decimated sequences for $d = \frac{(p^m+1)(p^m+p-1)}{p+1}$," IEICE Trans. Fundamentals, vol.E97-A, no.4, pp.964–969, April 2014.
[10] T. Zhang, S. Li, T. Feng, and G. Ge, "Some new results on the cross correlation of m-sequences," IEEE Trans. Inf. Theory, vol.60, no.5, pp.3062–3068, May 2014.
[11] Y. Xia and S. Chen, "Cross-correlation distribution between a p-ary m-sequence and its decimated sequence with decimation factor $\frac{(p^m+1)^2}{2(p^e+1)}$," IEICE Trans. Fundamentals, vol.E97-A, no.5, pp.1103–1112, May 2014.
[12] Y. Xia, C. Li, X. Zeng, and T. Helleseth, "Some results on cross-correlation distribution between a p-ary m-sequence and its decimated sequences," IEEE Trans. Inf. Theory, vol.60, no.11, pp.7368–7381, Nov. 2014.
[13] J.Y. Kim, S.T. Choi, J.S. No, and H. Chung, "A new family of p-ary sequences of period $\frac{p^n-1}{2}$ with low correlation," IEEE Trans. Inf. Theory, vol.57, no.6, pp.3825–3830, June 2011.
[14] D.S. Kim, H.J. Chae, and H.Y. Song, "A generalization of the family of p-ary decimated sequences with low correlation," IEEE Trans. Inf. Theory, vol.57, no.11, pp.7614–7617, Nov. 2011.
[15] Y. Xia and S. Chen, "A new family of p-ary sequences with low correlation constructed from decimated sequences," IEEE Trans. Inf. Theory, vol.58, no.9, pp.6037–6046, Sept. 2012.
[16] W. Lee, J.Y. Kim, and J.S. No, "New families of p-ary sequences of period $\frac{p^n-1}{2}$ with low maximum correlation magnitude," IEICE Trans. Commun., vol.E97-B, no.11, pp.2311–2315, Nov. 2014.
[17] J.Y. Kim, C.M. Cho, W. Lee, and J.S. No, "On the cross-correlation between two decimated p-ary m-sequences by 2 and $4p^{n/2} - 2$," IEICE Trans. Commun., vol.E98-B, no.3, pp.415–421, March 2015.
[18] C.M. Cho, J.Y. Kim, and J.S. No, "New p-ary sequence families of period $\frac{p^n-1}{2}$ with good correlation property using two decimated m-sequences," IEICE Trans. Commun., vol.E98-B, no.7, pp.1268–1275, July 2015.
[19] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," SIAM J. Comput., vol.9, no.4, pp.758–767, Nov. 1980.
[20] A. Weil, "On some exponential sums," Proc. Natl. Acad. Sci. USA, vol.34, no.5, pp.204–207, 1948.
[21] S.C. Liu and J.F. Komo, "Nonbinary Kasami sequences over $GF(p)$," IEEE Trans. Inf. Theory, vol.38, no.4, pp.1409–1412, July 1992.
[22] R. Lidl and H. Niederreiter, Finite Fields, vol.20 of Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.

Chang-Min Cho received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2010, where he is currently pursuing the Ph.D. degree in electrical and computer engineering. His area of research interests includes pseudorandom sequences, cryptography, and error-correcting codes.

Wijik Lee received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2012, where he is currently pursuing the Ph.D. degree in electrical and computer engineering. His area of research interests includes pseudorandom sequences, 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 Department of Electrical and Computer Engineering, Seoul National University, in August 1999, where he is currently a Professor. From 1996 to 2008, he served as a Founding Chair of Seoul Chapter, IEEE Information Theory Society. He was a General Chair for Sequence and Their Applications 2004 (SETA2004) in Seoul, Korea. He also served as a General Co-Chair for International Symposium on Information Theory and Its Applications 2006 (ISITA 2006) and International Symposium on Information Theory 2009 (ISIT 2009) in Seoul, Korea. He was a recipient of IEEE Information Theory Society Chapter of the Year Award in 2007. He is elevated to IEEE Fellow in Research Engineer/Scientist through IEEE Information Theory Society, November, 2011. He has become Co-Editor-in-Chief of Journal of Communications and Networks, January, 2012. His area of research interests includes error-correcting codes, sequences, cryptography, LDPC codes, interference alignment and wireless communication systems.



Young-Sik Kim received B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from Seoul National University in 2001, 2003, and 2007, respectively. He joined Semiconductor Division, Samsung Electronics and carried out research and development of secure hardware IPs for various embedded systems, especially for smartcards until the end of August in 2010. He is now an associate professor at Chosun University, Gwangju, Korea. His research interests include post-quantum cryptography, IoT security, physical layer security, data hiding, channel coding, and signal design.