IEICE TRANS. FUNDAMENTALS, VOL.E95–A, NO.11 NOVEMBER 2012

INVITED PAPER *Special Section on Signal Design and Its Applications in Communications*

On the Cross-Correlation Distributions of *p*-Ary m-Sequences and Their Decimated Sequences*

Sung-Tai CHOI[†a)], ***Nonmember and*** **Jong-Seon NO**[†b)], ***Member***

SUMMARY In this paper, we analyze the existing results to derive the cross-correlation distributions of p-ary m-sequences and their decimated sequences for an odd prime p and various decimations d. Based on the previously known results, a methodology to obtain the distribution of their cross-correlation values is also formulated.

key words: *code division multiple access (CDMA), cross-correlation function, decimated sequence, p-ary m-sequence, sequence family*

1. Introduction

For the past decades, maximum length sequences (m-sequences) have been studied extensively. The m-sequences have the ideal autocorrelation property, i.e., out of phase autocorrelation values take -1, from which m-sequences are used in synchronization for various communication systems and in code division multiple access (CDMA) systems as user spreading codes.

Generally, picking every d-th element from a periodic sequence is called 'decimation'. For particular decimation values d, m-sequences have low cross-correlation values with their decimated sequences, which is the important property for construction of spreading codes in CDMA systems [1]–[3]. In [3], Kumar and Moreno constructed the sequence family whose alphabet size is an odd prime. The performance of their construction, in terms of family size and correlation magnitudes, outperforms those of the existing optimal sequence families with binary alphabet size. Hence, in the study of the cross-correlation between m-sequence and its decimated sequence, the case for an odd prime alphabet size has lots of interest.

For an odd prime p, many researchers have studied to evaluate the cross-correlation values of p-ary m-sequences and their decimated sequences [7]–[18]. In [7], Trachtenberg evaluated the cross-correlation values for $d = (p^{2k} + 1)/2$ and $d = p^{2k} - p^k + 1$. Helleseth [8] found more decimation values, for which the cross-correlation has a relatively small number of distinct values, and derived their distributions. Dobbertin, Helleseth, Kumar, and Martinsen [9] showed that the distribution of the cross-correlation has three values and derive their distribution when $d = 2 \cdot 3^m + 1$ and $n = 2m + 1$. Recently, Luo and Feng [15] determined the cross-correlation distribution for $d = (p^k + 1)/2$, which is a general case of the previous results in [7], [8], [12].

Many researchers also have studied the evaluation of cross-correlation values for the decimation values d such that $\gcd(d, p^n - 1) \neq 1$ [10]–[18]. For $d = (3^k + 1)/2$ and an odd integer k, which is the generalization of the Trachtenberg's case, Ness, Helleseth, and Kholosha [12] derived the distribution of the cross-correlation values. For an odd prime p, $n = 4k$, and $d = (p^{2k} + 1)^2/4$, Seo, Kim, No, and Shin [13] calculated the distribution of the cross-correlation values. Seo, Kim, No, and Shin [14] also obtained the distribution of the cross-correlation values for $d = p^k + 1$. For the decimation value $d = (p^n + 1)/(p + 1) + (p^n - 1)/2$, Muller [10] and Hu et al. [11] determined the upper bound on the magnitudes of the cross-correlation values for $p = 3$ and an odd prime, $p \equiv 3 \bmod 4$, respectively. For the same decimation value, Xia, Zeng, and Hu [16] calculated the distribution of the cross-correlation values. Choi, Lim, No, and Chung [17] obtained the upper bound on the magnitudes of the cross-correlation values for an odd prime, $p \equiv 3 \bmod 4$, $d = (p^m + 1)^2/(2(p + 1))$, $n = 2m$, and an odd integer m. For the generalized decimation of the previous case, $d = (p^m + 1)^2/(2(p^k + 1))$ with $k|m$, Luo, Helleseth, and Kholosha [18] derived the cross-correlation distribution partly. Table 1 lists the known results on the cross-correlation values of p-ary m-sequences and their decimated sequences for an odd prime p.

In this paper, we review and analyze the previously known results on the cross-correlation between p-ary m-sequences and their decimated sequences. A methodology to calculate the cross-correlation distribution or the upper bound on the magnitudes of cross-correlation values will be formulated systematically by using the following two steps:

1) Evaluation: Find possible candidate or actual values of the cross-correlation function by;
   1-1) Using a quadratic form technique.
   1-2) Transforming into known exponential sums.
   1-3) Calculating cross-correlation properties.
   1-4) Excluding redundant cross-correlation values.
2) Distribution: Determine the number of occurrences of

Manuscript received May 2, 2012.
Manuscript revised May 27, 2012.

[†]The authors are with the Department of Electrical Engineering and Computer Science, INMC, Seoul National University, Seoul 151-744, Korea.

*This material was presented in International Workshop on Signal Design and Its Applications in Communications, Guilin, China, October, 2011. This work was supported partly by the Chinese 111 project (No.111-2-14) and 973 Program (No.2012CB316100).

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

DOI: 10.1587/transfun.E95.A.1808

Table 1 Previously known results on the cross-correlation between p-ary m-sequences of period $N = p^n - 1$ and their decimated sequences.

Researcher	p	n	d	$\gcd(d, N)$	# corr.	$R_{\max}$
Helleseth [8]	odd prime	odd	$\frac{p^{2k}+1}{2}$ or $p^{2k} - p^k + 1$, odd $\frac{n}{e}$, $e = \gcd(n, k)$	1	3	$1 + p^{\frac{n+e}{2}}$
	$p^n \equiv 1 \bmod 4$		$\frac{p^n-1}{2} + p^i$, $0 \le i < n$	1	5	$-1 + \frac{1}{2}(p^n + p^{\frac{n}{2}})$
	2 mod 3	even	$\frac{p^n-1}{3} + p^i$, $0 \le i < n$	1	6	$-1 + \frac{1}{3}(p^n + 4p^{\frac{n}{2}})$
	$p^{\frac{n}{2}} \not\equiv 2 \bmod 3$	even	$2p^{n/2} - 1$	1	4	$-1 + 2p^{\frac{n}{2}}$
Dobbertin et al. [9]	3	odd	$2 \cdot 3^{(n-1)/2} + 1$	1	3	$1 + 3^{\frac{n+1}{2}}$
Luo and Feng [15]	odd prime	any	$\frac{p^k+1}{2}$, odd k/e, $e = \gcd(n, k)$	variable	variable	$1 + \frac{p^e-1}{2} p^{\frac{n}{2}}$
Xia et al. [16]	3 mod 4	odd	$\frac{p^n+1}{p+1} + \frac{p^n-1}{2}$	2	9	$1 + \frac{p+1}{2} p^{\frac{n}{2}}$
Seo et al. [13]	odd prime	0 mod 4	$\frac{(p^m+1)^2}{4}$, $n = 2m$	$\frac{p^m+1}{2}$	4	$-1 + 2p^{\frac{n}{2}}$
Choi et al. [17]	odd prime	2 mod 4	$\frac{(p^m+1)^2}{2(p+1)}$, $n = 2m$	$\frac{p^m+1}{2}$	$\star$	$1 + \frac{p+1}{2} p^{\frac{n}{2}}$

$\star$ denotes that the authors only derive the upper-bound on the magnitudes of the cross-correlation values.

each cross-correlation value by;

2-1) Calculating power sums of the cross-correlation function.

2-2) Finding a pair of the cross-correlation values with the same number of occurrences.

2-3) Determining the rank distribution of quadratic forms.

This paper is organized as follows. In Sect. 2, notations and preliminaries are given. In Sect. 3, we analyze the previously known results and formulate a methodology to obtain the cross-correlation distribution of p-ary m-sequences and their decimated sequences. In Sect. 4, existing results on the cross-correlation are explained in terms of the methodology suggested in Sect. 3. In Sect. 5, conclusion is given.

2. Notations and Preliminaries

2.1 Cross-Correlation Function

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

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

where $x \in \mathbb{F}_{p^n}$ and $k|n$. Let α be a primitive element of $\mathbb{F}_{p^n}$. Then a p-ary m-sequence $m(t)$ of period $p^n - 1$ can be expressed as

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

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

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

where $\omega = e^{j2\pi/p}$ is a primitive p-th root of unity and time index of the sequences should be calculated as integer modulus N.

From the above definitions, when $\gcd(d, p^n - 1) = 1$, the periodic cross-correlation function between p-ary m-sequence $m(t)$ and its decimated sequence by d, $m(dt)$, of period $p^n - 1$ at the shift τ is written as

$$\begin{aligned} C_d(\tau) &= \sum_{t=0}^{p^n-2} \omega^{m(t+\tau) - m(dt)} \\ &= \sum_{x \in \mathbb{F}_{p^n}} \chi(\delta x - x^d) - 1 \end{aligned} \tag{1}$$

where $\chi(\cdot) = \omega^{\mathrm{tr}_1^n(\cdot)}$ is a canonical additive character of $\mathbb{F}_{p^n}$ and $\delta = \alpha^\tau$. When $\gcd(d, p^n - 1) \neq 1$, there are $l = \gcd(d, p^n - 1)$ versions of decimated sequences and we denote the sequences by $m(dt + l)$, $0 \le l < \gcd(d, p^n - 1)$. Hence their cross-correlation functions are given as

$$\begin{aligned} C_d(l, \tau) &= \sum_{t=0}^{p^n-2} \omega^{m(t+\tau) - m(dt+l)} \\ &= \sum_{x \in \mathbb{F}_{p^n}} \chi(\delta x - \zeta x^d) - 1 \\ &= \sum_{x \in \mathbb{F}_{p^n}} \chi(x - \gamma x^d) - 1 \\ &= C_d(\gamma) \end{aligned} \tag{2}$$

where $\zeta = \alpha^l$ and $\gamma = \zeta/\delta^d$.

2.2 Quadratic Form

We define a quadratic form in e variables over $\mathbb{F}_{p^k}$ as a homogeneous polynomial in $\mathbb{F}_{p^k}[x_1, \ldots, x_e]$

$$f(\mathbf{x}) = f(x_1, \ldots, x_e) = \sum_{i,j=1}^{e} a_{ij} x_i x_j$$

where p is an odd prime and $a_{ij} = a_{ji} \in \mathbb{F}_{p^k}$. We then

associate f with the $e \times e$ symmetric matrix A whose (i, j) entry is a_{ij}. The matrix A is called the coefficient matrix of f and ρ denotes the rank of A. Then, there exists a nonsingular $e \times e$ matrix B over $\mathbb{F}_{p^k}$ such that $C = BAB^T$ is a diagonal matrix and $C = \mathrm{diag}(c_1, \ldots, c_\rho, 0, \cdots, 0)$, where $c_i \in \mathbb{F}_{p^k}^*$. Let $\Delta = c_1 \cdots c_\rho$.

A quadratic form $f(\mathbf{x})$ in e variables over $\mathbb{F}_{p^k}$ can be regarded as a mapping $f(x)$ from $\mathbb{F}_{p^{ek}}$ to $\mathbb{F}_{p^k}$ when $x_i \in \mathbb{F}_{p^k}$. Thus, we will also use the term 'quadratic form' for this mapping $f(x)$ in the finite extension field $\mathbb{F}_{p^{ek}}$.

If f is a quadratic form over $\mathbb{F}_{p^k}$ and $b \in \mathbb{F}_{p^k}$, then an explicit formula for the number of solutions of the equation $f(x_1, \ldots, x_e) = b$ in $(\mathbb{F}_{p^k})^e \approx \mathbb{F}_{p^{ek}}$ is given. Hence, the 'quadratic form' can be exploited to evaluate the cross-correlation function if the function is represented as a quadratic form. In the remainder of this section, some useful lemmas are listed without proof as follows.

Lemma 1: Consider the following function of $x \in \mathbb{F}_{p^n}$

$$\mathrm{tr}_1^n\left(\sum_i a_i x^{p^i+1}\right) = \mathrm{tr}_1^k(Q(x)),\ 0 \le i < n$$

where $a_i \in \mathbb{F}_{p^n}^*$ and k is the greatest common divisor of n and all nonzero i's. Then

$$Q(x) = \mathrm{tr}_k^n\left(\sum_i a_i x^{p^i+1}\right)$$

is a quadratic form in n/k variables over $\mathbb{F}_{p^k}$. □

Lemma 2 (Luo and Feng [15]): The rank ρ of the quadratic form $f(x)$ from $\mathbb{F}_{p^{ek}}$ to $\mathbb{F}_{p^k}$ is determined from the number of elements that the form is independent of, i.e., $(p^k)^{e-\rho}$ is the number of $z \in \mathbb{F}_{p^{ek}}$ such that $f(x+z) - f(x) - f(z) = 0$ for all $x \in \mathbb{F}_{p^{ek}}$. □

Lemma 3 (Luo and Feng [15]): Let $f(x)$ be a mapping from $\mathbb{F}_{p^{ek}}$ to $\mathbb{F}_{p^k}$ corresponding to a quadratic form $f(x) \in \mathbb{F}_{p^k}[x_1, x_2, \ldots, x_e]$ of rank ρ with Δ. Then we have

$$\sum_{x \in \mathbb{F}_{p^{ek}}} \omega^{\mathrm{tr}_1^k(f(x))} = \begin{cases} \eta(\Delta)(p^k)^{e-\frac{\rho}{2}}, & \text{if } p^k \equiv 1 \bmod 4 \\ j^\rho \eta(\Delta)(p^k)^{e-\frac{\rho}{2}}, & \text{if } p^k \equiv 3 \bmod 4 \end{cases} \tag{3}$$

where $j = \sqrt{-1}$ and $\eta(\cdot)$ is the quadratic character of $\mathbb{F}_{p^k}^*$ defined as

$$\eta(\Delta) = \begin{cases} 1, & \text{if } \Delta \text{ is a square in } \mathbb{F}_{p^k}^* \\ -1, & \text{if } \Delta \text{ is a nonsquare in } \mathbb{F}_{p^k}^*. \end{cases}$$

□

From the above lemmas, we calculate the exponential sum in (3) just by finding the rank of the corresponding quadratic form. This is the main reason why many researchers try to express the cross-correlation function as quadratic forms in their papers.

2.3 Known Exponential Sums

The following useful lemmas are introduced in [8], which are deployed to evaluate the cross-correlation values in [8] and [13].

Lemma 4 (Helleseth [8]): Let p be an odd prime and $d|p^n - 1$. Suppose that s is the least integer such that $d|p^s + 1$.

1) When d is an even integer, $(p^s+1)/d$ and $d/2s$ are odd integers;

$$\sum_{x \in \mathbb{F}_{p^n}} \chi(ax^d) = \begin{cases} p^n, & \text{for } a = 0 \\ (-1)^{\frac{n}{2s}+1}(d-1)p^{\frac{n}{2}}, & \text{for } a \in C_{\frac{d}{2}} \\ (-1)^{\frac{n}{2s}}p^{\frac{n}{2}}, & \text{for } a \notin C_{\frac{d}{2}}. \end{cases}$$

2) For all other cases;

$$\sum_{x \in \mathbb{F}_{p^n}} \chi(ax^d) = \begin{cases} p^n, & \text{for } a = 0 \\ (-1)^{\frac{n}{2s}+1}(d-1)p^{\frac{n}{2}}, & \text{for } a \in C_0 \\ (-1)^{\frac{n}{2s}}p^{\frac{n}{2}}, & \text{for } a \notin C_0 \end{cases}$$

where $C_j = \{\alpha^{di+j} \in \mathbb{F}_{p^n}^* | \ 0 \le i < \frac{p^n-1}{d},\ 0 \le j < d\}$. □

Lemma 5 (Helleseth [8]): Let p be an odd prime and n be an even integer. For $a \in \mathbb{F}_{p^n}$, we have

$$\sum_{x \in \mathbb{F}_{p^n}} \chi(ax^{p^{\frac{n}{2}}+1}) = \begin{cases} p^n, & \text{if } a + a^{p^{\frac{n}{2}}} = 0 \\ -p^{\frac{n}{2}}, & \text{if } a + a^{p^{\frac{n}{2}}} \neq 0. \end{cases}$$

□

Lemma 6 (Helleseth [8]): Let p be an odd prime. Then we have

$$\sum_{x \in \mathbb{F}_{p^n}} \chi(ax^2) = \begin{cases} p^n, & \text{if } a = 0 \\ (-1)^{n+1}((-1)^{\frac{p-1}{2}}p)^{\frac{n}{2}}, & \text{if } a \text{ is a square in } \mathbb{F}_{p^n}^* \\ (-1)^n((-1)^{\frac{p-1}{2}}p)^{\frac{n}{2}}, & \text{if } a \text{ is a nonsquare in } \mathbb{F}_{p^n}^*. \end{cases}$$

□

2.4 Special Functions

Let q be a power of prime. A polynomial of the form

$$L(x) = \sum_i a_i x^{q^i} \tag{4}$$

where $a_i \in \mathbb{F}_{q^m}$, is called a linearized polynomial over $\mathbb{F}_{q^m}$. If $\mathbb{F}$ is an arbitrary extension field of $\mathbb{F}_{q^m}$ which includes the roots of $L(x)$, then

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

Hence the set of solutions to $L(x) = 0$ in $\mathbb{F}$ forms a vector

subspace over $\mathbb{F}_q$, i.e., the number of solutions in $\mathbb{F}$ to $L(x) = 0$ is equal to a power of q.

A planar function $f(x)$ is a mapping $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ such that the function

$$f(x+a) - f(x)$$

is a permutation polynomial for any $a \in \mathbb{F}_{p^n}^*$.

3. Methodology for Cross-Correlation Distribution

For the distribution of the cross-correlation values of p-ary m-sequences and their decimated sequences, the next two steps are generally followed:

1) Evaluation: Find possible candidate or actual values of the cross-correlation function;
2) Distribution: Calculate the number of occurrences of each cross-correlation value.

In this section, we analyze the previously known results and formulate a methodology to evaluate the cross-correlation values and derive their distributions.

3.1 Evaluation of the Cross-Correlation Values

In the following subsections, we categorize the various evaluation methods of the cross-correlation values and give some examples of each method.

3.1.1 Quadratic Form Technique

The evaluation method using a quadratic form is the most popular way in many papers [7]–[17]. The method is performed as in the following three steps:

1) Transform the cross-correlation function into the exponential sums in (3);
2) Calculate the ranks of the corresponding quadratic forms;
3) Evaluate the exponential sum values from the ranks.

Here is an example for transforming the cross-correlation function into the exponential sum in terms of quadratic forms.

Example 1 (Trachtenberg [7]): For $d = (p^{2k}+1)/2$ and an odd integer n, the cross-correlation function in (1) is transformed into

$$\begin{aligned} C_d(\tau) &= -1 + \sum_{x \in F_{p^n}} \chi(\delta x - x^d) \\ &= -1 + \frac{1}{2}\left(\sum_{y \in F_{p^n}} \chi(\delta y^2 - y^{p^{2k}+1}) \right. \\ &\qquad \left. + \sum_{y \in F_{p^n}} \chi(\delta r y^2 - r^d y^{p^{2k}+1}) \right) \end{aligned} \tag{5}$$

where r is a nonsquare in F_{p^n} and $\delta = \alpha^\tau$. From Lemma 1, we know that the function is expressed as the two quadratic forms over F_p. □

Thereafter, we determine the rank of the quadratic forms in the cross-correlation function. They are calculated from Lemma 2 as in the following example.

Example 2 (Trachtenberg [7]): For the same case as Example 1, let $Q(y)$ denote one of the two quadratic forms in (5) given as

$$Q(y) = \mathrm{tr}_1^n(\delta y^2 - y^{p^{2k}+1}).$$

From Lemma 2, the rank of $Q(y)$ is determined by calculating the number of solutions $z \in \mathbb{F}_{p^n}$ satisfying $Q(y+z) = Q(y) + Q(z)$ for any $y \in \mathbb{F}_{p^n}$. Then we have

$$z^{p^{4k}} - (2\delta z)^{p^{2k}} + z = 0, \tag{6}$$

which is the linearized polynomial in (4). Let $e = \gcd(n,k)$. From Sect. 2.4 and Lemma 2, we derive that the number of solutions $z \in \mathbb{F}_{p^n}$ to (6) is 1, p^e, or p^{2e}, i.e., the possible ranks of $Q(y)$ are n, $n-e$, or $n-2e$. From Lemma 3, obtaining the rank of the quadratic form enables us to evaluate the exponential sum in (5), $\sum_{y \in \mathbb{F}_{p^n}} \chi(Q(y))$. We can calculate another exponential sum in (5), $\sum_{y \in F_{p^n}} \chi(\delta r y^2 - r^d y^{p^{2k}+1})$, similarly. □

3.1.2 Transforming into Known Exponential Sums

From Lemma 4, we can calculate the following exponential sum

$$\sum_{x \in \mathbb{F}_{p^n}} \chi(a x^d) \tag{7}$$

where d should divide both $p^n - 1$ and $p^s + 1$ for some integer s. If the cross-correlation function is represented as (7), we can use Lemma 4 for evaluation of the cross-correlation values. The following examples show how to express the cross-correlation function as the exponential sum in (7).

Example 3 (Helleseth [8]): For $d = (p^n-1)/3 + p^i$, $p \equiv 2 \bmod 3$, and an even integer n, the cross-correlation function in (1) can be rewritten as

$$\begin{aligned} C_d(\tau) = -1 + \frac{1}{3}\left(\sum_{x \in \mathbb{F}_{p^n}} \chi(x^3(\delta - 1)) \right. \\ \left. + \sum_{x \in \mathbb{F}_{p^n}} \chi(x^3(\delta - \beta)\alpha) + \sum_{x \in \mathbb{F}_{p^n}} \chi(x^3(\delta - \beta^2)\alpha^2) \right) \end{aligned} \tag{8}$$

where $\delta = \alpha^\tau$ and $\beta = \alpha^{p^{-i}(p^n-1)/3}$. We know that each exponential sum in (8) has the same form as (7). Hence, from Lemma 4, we can evaluate $C_d(\tau)$. □

In [13], the authors use Lemma 5 for the evaluation of cross-correlation values as in the following example.

Example 4 (Seo et al. [13]): For $d = ((p^m+1)/2)^2$ with $n = 2m$ and an even integer m, the cross-correlation function in (2) can be written in terms of the exponential sums in Lemma 5 as

$$C_d(l,\tau) = -1 + \frac{1}{p^m+1}\sum_{i=0}^{p^m}\sum_{x\in\mathbb{F}_{p^n}}\chi(x^{p^m+1}(\delta\alpha^i - \zeta\alpha^{di})) = \frac{(p^n+p^m)(K(\delta,\zeta)-1)}{p^m+1}$$

where $K(\delta,\zeta)$ is the number of $0 \le i < p^m+1$ satisfying

$$\mathrm{tr}_m^n(\delta\alpha^i - \zeta\alpha^{di}) = 0.$$

Then it is derived that $K(\delta,\zeta)$ should be 0,1,2, or 3. Hence, $C_d(l,\tau)$ has the values $-1, -1 \pm p^{\frac{n}{2}}$, and $-1+2p^{\frac{n}{2}}$. □

3.1.3 Calculating Cross-Correlation Function from Its Properties

In [9], some calculations of the cross-correlation function are used for the evaluation as in the following example.

Example 5 (Dobbertin et al. [9]): For $p=3$, $d = 2\cdot 3^m+1$, and $n = 2m+1$, the cross-correlation values are evaluated using the following steps:
1) $\sum_{\tau=0}^{3^n-2}(C_d(\tau)+1)^4 = 3^{3n+1}$;
2) 3^{m+1} divides $C_d(\tau)+1$ for all τ;
3) 1) and 2) imply $C_d(\tau) \in \{-1, -1\pm 3^{m+1}\}$ for all τ. □

3.1.4 Exclusion Techniques

The number of evaluated cross-correlation values sometimes exceeds the actual number of the values. Hence, the values which actually do not occur should be ruled out by certain techniques, which enable us to obtain explicit cross-correlation values. The techniques will be categorized as follows:

1) Using a planar function (perfect nonlinear) property;

If $f(x) = x^d$ is a planar function, then we have

$$\left|\sum_{x\in\mathbb{F}_{p^n}}\chi(af(x)+bx)\right|^2 = p^n \tag{9}$$

for any $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^n}$. From (9), some redundant cross-correlation values can be ruled out as in the following example.

Example 6 (Ness et al. [12]): For $p=3$, $d=(3^k+1)/2$ with an odd integer k, and $\gcd(k,n)=1$, the cross-correlation function in (2) can be written as

$$C_d(l,\tau) = -1 + \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{3^n}}\chi(\delta x^2 - \zeta x^{3^k+1}) + \sum_{x\in\mathbb{F}_{3^n}}\chi(\delta r x^2 - \zeta r^d x^{3^k+1})\right)$$

where r is a nonsquare in $\mathbb{F}_{3^n}$, $\delta = \alpha^\tau$, and $\zeta = \alpha^l$. Since $f(x) = x^d$ is shown to be a planar function over $\mathbb{F}_{3^n}$ in [20], we can apply (9) to $|1+C_d(l,\tau)|^2$. From the quadratic form technique, we can obtain the candidate values of $C_d(l,\tau)$. From (9), among the evaluated cross-correlation values, the following values

$$\left\{-1+\frac{1}{2}(\epsilon_1+\epsilon_2)j3^{\frac{n+1}{2}}, -1+\frac{1}{2}(\epsilon_1+\epsilon_2)3^{\frac{n+2}{2}}, -1+\frac{1}{2}(\epsilon_1 j+\sqrt{3}\epsilon_2)3^{\frac{n+1}{2}}\right\} \text{ with } \epsilon_1,\epsilon_2 = \pm 1$$

are excluded. □

2) Applying Weil bound;

The following lemma provides us the upper bound on the magnitudes of the exponential sum in terms of an additive character and some polynomial.

Lemma 7 (Weil's Theorem [19]): Let $f(x) \in \mathbb{F}_{p^n}[x]$ be a polynomial of degree $v \ge 1$ with $\gcd(v,p^n)=1$ and let χ be a nontrivial additive character of $\mathbb{F}_{p^n}$. Then we have

$$\left|\sum_{x\in\mathbb{F}_{p^n}}\chi(f(x))\right| \le (v-1)p^{\frac{n}{2}}.$$

□

In the following example, Lemma 7 is used for the exclusion of redundant cross-correlation values.

Example 7 (Xia et al. [16]): For an odd prime $p \equiv 3 \bmod 4$ and $d = (p^n+1)/(p+1) + (p^n-1)/2$ with an odd integer n, the cross-correlation function in (2) is written as

$$\begin{aligned} C_d(l,\tau) &= -1 + \sum_{x\in\mathbb{F}_{p^n}}\chi(x-\gamma x^d) \\ &= -1 + \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{p^n}}\chi(x^{p+1}-\gamma x^2) + \sum_{x\in\mathbb{F}_{p^n}}\chi(-x^{p+1}-\gamma x^2)\right) \\ &= -1 + \frac{1}{2}(S_1(\gamma)+S_2(\gamma)) \end{aligned}$$

where $\gamma = \zeta/\delta^d$, $S_1(\gamma) = \sum_{x\in\mathbb{F}_{p^n}}\chi(x^{p+1}-\gamma x^2)$, and $S_2(\gamma) = \sum_{x\in\mathbb{F}_{p^n}}\chi(-x^{p+1}-\gamma x^2)$. We can evaluate both $S_1(\gamma)$ and $S_2(\gamma)$ by the quadratic form technique. Among the derived values, for $C_d(l,\tau) = -1 \pm j(p-1)/2p^{n/2}$, we have

$$\begin{aligned} \sum_{x\in\mathbb{F}_{p^n}}\chi\left(x^{\frac{p+1}{2}}-\gamma x\right) &= \frac{1}{2}(S_1(\gamma)-S_2(\gamma)) \\ &= \pm\frac{(p+1)}{2}jp^{\frac{n}{2}}, \end{aligned}$$

which contradicts the Weil bound in Lemma 7. Hence, $C_d(l,\tau) = -1 \pm j(p-1)/2p^{n/2}$ are ruled out from the candidate cross-correlation values. □

3) Finding possible ranks of quadratic forms;

When the cross-correlation function is expressed in terms of quadratic forms, the number of possible ranks of the quadratic forms decides the number of candidate cross-correlation values. If the possible ranks of the quadratic forms are limited, we can reduce the number of the candidate cross-correlation values. We illustrate this idea in the following examples.

Example 8 (Luo and Feng [15]): For an odd prime p and $d = (p^k + 1)/2$ with an odd integer $k/\gcd(n, k)$, the cross-correlation function in (2) is expressed in terms of the two quadratic forms over $\mathbb{F}_{p^e}$ as

$$\begin{aligned} Q_1(x) &= \mathrm{tr}_e^n(\delta x^2 - \zeta x^{p^k+1}) \\ Q_2(x) &= \mathrm{tr}_e^n(\delta r x^2 - \zeta r^d x^{p^k+1}) \end{aligned}$$

where r is a nonsquare in $\mathbb{F}_{p^n}$, $e = \gcd(n, k)$, $\delta = \alpha^\tau$, and $\zeta = \alpha^l$. In [15], it is shown that at least one of the two quadratic forms has the rank $s = n/e$. Hence the cross-correlation values which correspond to the ranks $(\rho_1, \rho_2) = (s-1, s-1)$, $(s-1, s-2)$, $(s-2, s-1)$, and $(s-2, s-2)$ are ruled out, where ρ_1 and ρ_2 denote the ranks of the quadratic forms $Q_1(x)$ and $Q_2(x)$, respectively. □

Example 9 (Muller [10]): For $p = 3$ and $d = (p^n + 1)/4 + (p^n - 1)/2$ with an odd integer n, the cross-correlation function in (2) is expressed in terms of two quadratic forms. From Lemma 2, the corresponding linearized polynomials deciding the rank of the quadratic forms are given as

$$\begin{aligned} L_1(z) &= z^9 + \gamma^3 z^3 + z \\ L_2(z) &= z^9 - \gamma^3 z^3 + z \end{aligned}$$

where $\gamma = \zeta/\delta^d$ is defined in (2). Multiplying the two polynomials, we have

$$L_1(z)L_2(z) = z^2(z^{16} + 2z^8 - \gamma^6 z^4 + 1). \tag{10}$$

Then (10) has at most 10 solutions $z \in \mathbb{F}_{3^n}$. Hence the possible ranks (ρ_1, ρ_2) are limited to (n, n), $(n-1, n-1)$, $(n, n-1)$, and $(n, n-2)$ or vice versa, where ρ_1 and ρ_2 denote the ranks of the two quadratic forms, respectively. Note that there exists a better method, which is similar to the methods in [15] and [16], to exclude the rank $(n-1, n-1)$. □

3.2 Distribution of the Cross-Correlation Values

Let Ω_i denote the number of occurrences of the i-th cross-correlation value. Usually, in order to calculate Ω_i, sufficient independent equations in terms of Ω_i's should be obtained. In the following subsections, we categorize the existing methods to obtain the equations and give some examples of each method.

3.2.1 Power Sums of Cross-Correlation Function

In many papers [8], [9], [12], [13], [15], power sums of the cross-correlation function are calculated to obtain equations in terms of Ω_i's. The following lemma is needed to calculate the power sums.

Lemma 8 (Helleseth [8], Ness et al. [12]): When $\gcd(d, p^n - 1) = 1$, the first and second order power sums of the cross-correlation function are determined as

$$\begin{aligned} \sum_{\tau=0}^{p^n-2} C_d(\tau) &= 1 \\ \sum_{\tau=0}^{p^n-2} C_d^2(\tau) &= p^{2n} - p^n - 1. \end{aligned}$$

Generally, we have [8]

$$\sum_{\tau=0}^{p^n-2} C_d^v(\tau) = -(p^n - 1)^{v-1} + 2(-1)^{v-1} + \eta_v p^{2n}$$

where η_v is the number of solutions in $(\mathbb{F}_{p^n}^*)^v$ for

$$\begin{aligned} x_1 + x_2 + \cdots + x_{v-1} + 1 &= 0 \\ x_1^d + x_2^d + \cdots + x_{v-1}^d + 1 &= 0. \end{aligned} \tag{11}$$

Consider the case when $\gcd(d, p^n - 1) \neq 1$. Let $S(\delta, \zeta)$ denote the exponential sum in (2) given as

$$S(\delta, \zeta) = \sum_{x \in \mathbb{F}_{p^n}} \chi\left(\delta x - \zeta x^d\right) = C_d(l, \tau) + 1. \tag{12}$$

The first and second order power sums of the exponential sum are derived as

$$\begin{aligned} \sum_{\delta,\zeta \in \mathbb{F}_{p^n}} S(\delta, \zeta) &= p^{2n} \\ \sum_{\delta,\zeta \in \mathbb{F}_{p^n}} S^2(\delta, \zeta) &= p^{2n}. \end{aligned}$$

Generally, we have [12]

$$\sum_{\delta,\zeta \in \mathbb{F}_{p^n}} S^v(\delta, \zeta) = p^{2n}\eta_v$$

where η_v is the number of solutions in $(\mathbb{F}_{p^n})^v$ for

$$\begin{aligned} x_1 + x_2 + \cdots + x_v &= 0 \\ x_1^d + x_2^d + \cdots + x_v^d &= 0. \end{aligned} \tag{13}$$

□

Usually, it is not straightforward to compute (11) and (13) when v is larger than two. Here are some examples to illustrate the power sums in the determination of the distribution.

Example 10 (Ness et al. [12]): For $p = 3$, $d = (3^k + 1)/2$ with an odd integer k, and $\gcd(k, n) = 1$, the number of solutions $(x, y, z) \in \mathbb{F}_{3^n} \times \mathbb{F}_{3^n} \times \mathbb{F}_{3^n}$ of the equations

$$\begin{aligned} x + y + z &= 0 \\ x^d + y^d + z^d &= 0 \end{aligned}$$

is shown to be 3^n. Hence from Lemma 8, we have

$$\sum_{\delta,\zeta\in\mathbb{F}_{p^n}} S^3(\delta,\zeta) = 3^{3n}. \qquad \square$$

Example 11 (Luo and Feng [15]): For an odd prime p and $d = (p^k+1)/2$ with an odd integer $k/\gcd(n,k)$, the authors derive the following equations

$$(p^e-1)\sum_{(\delta,\zeta)\in N_1} S(\delta,\zeta) + (p^{2e}-1)\sum_{(\delta,\zeta)\in N_2} S(\delta,\zeta) = \frac{1}{2}p^n(p^e-1)(p^n-1)$$

and

$$(p^e-1)\sum_{(\delta,\zeta)\in N_1} S^2(\delta,\zeta)+(p^{2e}-1)\sum_{(\delta,\zeta)\in N_2} S^2(\delta,\zeta) = \begin{cases} \frac{1}{4}p^n(p^n-1)(2p^{n+e}-2p^n-p^{2e}+2p^e-1), \\ \qquad\qquad \text{if } p^e\equiv 1 \bmod 4 \\ \frac{1}{4}p^n(p^e-1)^2(p^n-1), \text{ if } p^e\equiv 3 \bmod 4, \text{ odd } \frac{n}{e} \\ -\frac{1}{4}p^n(p^e-1)^2(p^n-1), \text{ if } p^e\equiv 3 \bmod 4, \text{ even } \frac{n}{e} \end{cases}$$

where $e = \gcd(n,k)$, $N_i = \{(\delta,\zeta)\in(\mathbb{F}_{p^n})^2 |\ \rho_{\delta,\zeta} = s-i\}$, and $\rho_{\delta,\zeta}$ is the rank of the quadratic form $Q_1(x)$ defined in Example 8. This result is used to derive the distribution of the cross-correlation values. $\square$

3.2.2 Cross-Correlation Values with the Same Number of Occurrences

If there exist pairs of cross-correlation values with the same number of occurrences, we can reduce the number of unknown variables Ω_i's. In [12] and [16], this method is applied as in the following example.

Example 12 (Ness et al. [12]): For $p=3$, $d=(3^k+1)/2$ with an odd integer k, and $\gcd(k,n)=1$,

$$S(\delta,\zeta) = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(\delta x - \zeta x^d\right)$$

and

$$S(-\delta,-\zeta) = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-\delta x + \zeta x^d\right)$$

are a conjugate pair. Hence each conjugate pair has the same number of occurrences as δ and ζ run through $\mathbb{F}_{p^n}$. With this fact, the number of unknown variables can be reduced by half, i.e., only half of the equations in terms of Ω_i are needed to derive the distribution. $\square$

3.2.3 Rank Distribution of Quadratic Forms

Counting δ, ζ, and γ in (1) and (2), which correspond to specific ranks of quadratic forms, enables us to obtain equations of Ω_i as in the following example.

Example 13 (Xia et al. [16]): For $p\equiv 3 \bmod 4$ and $d=(p^n+1)/(p+1)+(p^n-1)/2$ with an odd integer n, $C_d(l,\tau)$ is represented in terms of the two quadratic forms over $\mathbb{F}_p$

$$Q_1(x) = \mathrm{tr}_1^n(x^{p+1}-\gamma x^2)$$
$$Q_2(x) = \mathrm{tr}_1^n(-x^{p+1}-\gamma x^2)$$

where γ is defined in (2). When γ runs through $\mathbb{F}_{p^n}^*$, the rank distribution is given as

$$(\rho_1,\rho_2) = \begin{cases} (n,n), & p^n-1-2p^{n-1}-\frac{2(p^{n-1}-1)}{p^2-1} \text{ times} \\ (n-1,n), & p^{n-1} \text{ times} \\ (n,n-1), & p^{n-1} \text{ times} \\ (n-2,n), & \frac{p^{n-1}-1}{p^2-1} \text{ times} \\ (n,n-2), & \frac{p^{n-1}-1}{p^2-1} \text{ times} \end{cases}$$

where ρ_1 and ρ_2 denote the ranks of the quadratic forms $Q_1(x)$ and $Q_2(x)$, respectively. This result gives us two independent equations in terms of Ω_i's, thus simplifying the computations. $\square$

4. Previously Known Results

In this section, we investigate how the formulated methodology in Sect. 3 is applied in the previously known results and introduce the main result of each paper. Before starting the section, let $\mathcal{N}$ denote the number of the distinct cross-correlation values and $R_{\max}$ the maximum magnitude of the cross-correlation values.

Theorem 1 (Helleseth [8]): For an odd prime p, $d=(p^{2k}+1)/2$ or $p^{2k}-p^k+1$ with $d\not\equiv p^i \bmod p^n-1$, an odd integer $n/\gcd(n,k)$, and $\gcd(d,p^n-1)=1$, we have $\mathcal{N}=3$ and $R_{\max}=1+p^{(n+e)/2}$, where $e=\gcd(n,k)$. The distribution of the cross-correlation values is given as

$$C_d(\tau) = \begin{cases} -1+p^{\frac{n+e}{2}} & \text{occurs } \frac{1}{2}(p^{n-e}+p^{\frac{n-e}{2}}) \text{ times} \\ -1 & \text{occurs } p^n-p^{n-e}-1 \text{ times} \\ -1-p^{\frac{n+e}{2}} & \text{occurs } \frac{1}{2}(p^{n-e}-p^{\frac{n-e}{2}}) \text{ times.} \end{cases}$$

Summary of the proof: $C_d(\tau)$ is transformed into the exponential sum of quadratic forms. Using the quadratic form technique, three cross-correlation values are evaluated. Since $\mathcal{N}=3$, i.e., there are three unknown values Ω_i, the three equations, $\sum_i \Omega_i$, $\sum_\tau C_d(\tau)$, and $\sum_\tau C_d^2(\tau)$, are obtained from Lemma 8 for their distribution. $\square$

Theorem 2 (Helleseth [8]): For an odd prime p such that $p^n\equiv 1 \bmod 4$, $d=(p^n-1)/2+p^i$, $0\le i<n$, and $\gcd(d,p^n-1)=1$, we have $\mathcal{N}=5$ and $R_{\max}=-1+(p^n+p^{n/2})/2$. The distribution of the cross-correlation values is given as

$$C_d(\tau) = \begin{cases} -1 & \text{occurs } \frac{1}{2}(p^n-5) \text{ times} \\ -1+(-1)^{n+1}((-1)^{\frac{p-1}{2}}p)^{\frac{n}{2}} & \\ & \text{occurs } \frac{1}{4}(p^n-1) \text{ times} \\ -1+(-1)^{n}((-1)^{\frac{p-1}{2}}p)^{\frac{n}{2}} & \\ & \text{occurs } \frac{1}{4}(p^n-1) \text{ times} \\ -1+\frac{1}{2}(p^n+(-1)^{n+1}((-1)^{\frac{p-1}{2}}p)^{\frac{n}{2}}) & \\ & \text{occurs once} \\ -1+\frac{1}{2}(p^n+(-1)^{n}((-1)^{\frac{p-1}{2}}p)^{\frac{n}{2}}) & \\ & \text{occurs once.} \end{cases}$$

Summary of the proof: For the evaluation of the cross-correlation values, $C_d(\tau)$ is transformed into the exponential sum in Lemma 6 and the five possible cross-correlation values are obtained. For their distribution, it is easily checked that the two cross-correlation values occur once when δ is equal to ± 1. Then, from

$$\sum_{i=1}^{\mathcal{N}} \Omega_i = p^n - 1$$
$$\sum_{\tau=0}^{p^n-2} (C_d(\tau)+1) = p^n$$
$$\sum_{\tau=0}^{p^n-2} (C_d(\tau)+1)^2 = p^{2n},$$

the remaining distribution is calculated. □

Theorem 3 (Helleseth [8]): For an odd prime p such that $p \equiv 2 \bmod 3$, an even integer n, $d = (p^n-1)/3 + p^i$, $0 \le i < n$, $f = p^{-i}(p^n-1)/3 \not\equiv 2 \bmod 3$, and $\gcd(d, p^n-1) = 1$, we have $\mathcal{N} = 6$ and $R_{\max} = -1 + (p^n + 2p^{n/2})/3$ or $-1 + (p^n + 4p^{n/2})/3$. The distribution of the cross-correlation values is given as:
i) When $f \equiv 0 \bmod 3$;

$$C_d(\tau) = \begin{cases} -1 & \\ \quad \text{occurs } \frac{1}{9}(4p^n + 2(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}} - 29) \text{ times} & \\ -1+(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}} & \\ \quad \text{occurs } \frac{1}{9}(2p^n + 2(-1)^{\frac{n}{2}}p^{\frac{n}{2}} - 4) \text{ times} & \\ -1+(-1)^{\frac{n}{2}}p^{\frac{n}{2}} & \\ \quad \text{occurs } \frac{1}{27}(8p^n + 2(-1)^{\frac{n}{2}}p^{\frac{n}{2}} - 10) \text{ times} & \\ -1+2(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}} & \\ \quad \text{occurs } \frac{1}{27}(p^n + 2(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}} + 1) \text{ times} & \\ -1+\frac{1}{3}(p^n + 2(-1)^{\frac{n}{2}}p^{\frac{n}{2}}) & \\ \quad \text{occurs once} & \\ -1+\frac{1}{3}(p^n + (-1)^{\frac{n}{2}+1}p^{\frac{n}{2}}) & \\ \quad \text{occurs twice.} \end{cases}$$

ii) When $f \equiv 1 \bmod 3$;

$$C_d(\tau) = \begin{cases} -1 & \\ \quad \text{occurs } \frac{1}{9}(4p^n + 2(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}} - 20) \text{ times} & \\ -1+(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}} & \\ \quad \text{occurs } \frac{1}{9}(2p^n + 2(-1)^{\frac{n}{2}}p^{\frac{n}{2}} - 4) \text{ times} & \\ -1+(-1)^{\frac{n}{2}}p^{\frac{n}{2}} & \\ \quad \text{occurs } \frac{1}{27}(8p^n + 2(-1)^{\frac{n}{2}}p^{\frac{n}{2}} - 28) \text{ times} & \\ -1+2(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}} & \\ \quad \text{occurs } \frac{1}{27}(p^n + 2(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}} - 8) \text{ times} & \\ -1+\frac{1}{3}(p^n + 2(-1)^{\frac{n}{2}}p^{\frac{n}{2}}) & \\ \quad \text{occurs twice} & \\ -1+\frac{1}{3}(p^n + 4(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}}) & \\ \quad \text{occurs once.} \end{cases}$$

Summary of the proof: For the evaluation of the cross-correlation values, $C_d(\tau)$ is transformed into the exponential sum in Lemma 4 and the six possible cross-correlation values are obtained. For their distribution, we need six equations.

The number of occurrences of two cross-correlation values is easy to derive. Remaining four equations are obtained from Lemma 8 as

$$\sum_{i=1}^{\mathcal{N}} \Omega_i = p^n - 1$$
$$\sum_{\tau=0}^{p^n-2} (C_d(\tau)+1) = p^n$$
$$\sum_{\tau=0}^{p^n-2} (C_d(\tau)+1)^2 = p^{2n}$$

and

$$\sum_{\tau=0}^{p^n-2} (C_d(\tau)+1)^3 = \eta_3 p^{2n}$$

where η_3 is the number of solutions $(x_1, x_2) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ to

$$x_1 + x_2 + 1 = 0$$
$$x_1^d + x_2^d + 1 = 0,$$

which is calculated as

$$\eta_3 = \begin{cases} \frac{1}{9}(p^n + 2(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}} + 10), & \text{for } f \equiv 0 \bmod 3 \\ \frac{1}{9}(p^n + 2(-1)^{\frac{n}{2}+1}p^{\frac{n}{2}} + 28), & \text{for } f \equiv 1 \bmod 3. \end{cases}$$

□

Theorem 4 (Helleseth [8]): For an odd prime p such that $p^{n/2} \not\equiv 2 \bmod 3$, an even integer n, $d = 2p^{n/2} - 1$, and $\gcd(d, p^n-1) = 1$, we have $\mathcal{N} = 4$ and $R_{\max} = -1 + 2p^{n/2}$. The distribution of the cross-correlation values is given as

$$C_d(\tau) = \begin{cases} -1 + p^{\frac{n}{2}} & \text{occurs } p^{\frac{n}{2}} \text{ times} \\ -1 & \text{occurs } \frac{1}{2}(p^n - p^{\frac{n}{2}} - 2) \text{ times} \\ -1 - p^{\frac{n}{2}} & \text{occurs } \frac{1}{3}(p^n - p^{\frac{n}{2}}) \text{ times} \\ -1 + 2p^{\frac{n}{2}} & \text{occurs } \frac{1}{6}(p^n - p^{\frac{n}{2}}) \text{ times.} \end{cases}$$

Summary of the proof: For the evaluation of the cross-correlation values, $C_d(\tau)$ is transformed into the exponential sum in Lemma 5 and the four possible cross-correlation values are obtained. For their distribution, the equations are obtained from Lemma 8 as

$$\sum_{i=1}^{\mathcal{N}} \Omega_i = p^n - 1$$
$$\sum_{\tau=0}^{p^n-2} (C_d(\tau)+1) = p^n$$
$$\sum_{\tau=0}^{p^n-2} (C_d(\tau)+1)^2 = p^{2n}$$

and

$$\sum_{\tau=0}^{p^n-2} (C_d(\tau)+1)^3 = \eta_3 p^{2n} = p^{\frac{5}{2}n}$$

where η_3 is the number of solutions $(x_1, x_2) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ to

$$x_1 + x_2 + 1 = 0$$
$$x_1^d + x_2^d + 1 = 0,$$

which is calculated as $\eta_3 = p^{n/2}$. □

Theorem 5 (Dobbertin et al. [9]): For $p = 3$, $d = 2 \cdot 3^m + 1$, $n = 2m + 1$, and $\gcd(d, p^n - 1) = 1$, we have $\mathcal{N} = 3$ and $R_{\max} = 1 + 3^{\frac{n+1}{2}}$. The distribution of the cross-correlation values is given as

$$C_d(\tau) = \begin{cases} -1 + 3^{\frac{n+1}{2}} & \text{occurs } \frac{1}{2}(3^{n-1} + 3^{\frac{n-1}{2}}) \text{ times} \\ -1 & \text{occurs } 3^n - 3^{n-1} - 1 \text{ times} \\ -1 - 3^{\frac{n+1}{2}} & \text{occurs } \frac{1}{2}(3^{n-1} - 3^{\frac{n-1}{2}}) \text{ times.} \end{cases}$$

Summary of the proof: Note that the cross-correlation function cannot be transformed into a quadratic form or the exponential sums in Sect. 2.3. Hence, the cross-correlation function properties are used to evaluate the cross-correlation values as in Example 5. For their distribution, since the number of cross-correlation values is three, the equations, $\sum_i \Omega_i$, $\sum_\tau C_d(\tau)$, and $\sum_\tau C_d^2(\tau)$, from Lemma 8 are needed. □

Theorem 6 (Luo and Feng [15]): For an odd prime p and $d = (p^k+1)/2$ with an odd integer $k/\gcd(n,k)$, $\mathcal{N}$ is variable and $R_{\max} = 1 + (p^e - 1)p^{n/2}/2$, where $e = \gcd(n,k)$. Let $s = n/e$, $q_0 = p^e$, and ${q_0}^* = (-1)^{(q_0-1)/2} q_0$. As δ and ζ run through $\mathbb{F}_{p^n}$, the distribution of the exponential sum in (12), $S(\delta,\zeta) = C_d(l,\tau) + 1$, is given as:

i) When s is an odd integer;

$$\begin{cases} \pm\sqrt{q_0^*}\, q_0^{\frac{s-1}{2}} & \text{occurs } \frac{(p^e-1)(p^n-1)(p^n+1)}{4(p^e+1)} \text{ times} \\ \frac{1}{2}(q_0 \pm \sqrt{q_0^*})\, q_0^{\frac{s-1}{2}} & \text{occurs } \frac{1}{2}p^{\frac{n-e}{2}}(p^{\frac{n-e}{2}}+1)(p^n-1) \text{ times} \\ \frac{1}{2}(-q_0 \pm \sqrt{q_0^*})\, q_0^{\frac{s-1}{2}} & \text{occurs } \frac{1}{2}p^{\frac{n-e}{2}}(p^{\frac{n-e}{2}}-1)(p^n-1) \text{ times} \\ \pm\frac{1}{2}(q_0-1)\sqrt{q_0^*}\, q_0^{\frac{s-1}{2}} & \text{occurs } \frac{(p^{n-e}-1)(p^n-1)}{p^{2e}-1} \text{ times} \\ 0 & \text{occurs } \frac{(p^{n+e}-3p^n+p^e+1)(p^n-1)}{2(p^e-1)} \text{ times} \\ p^n & \text{occurs once.} \end{cases}$$

ii) When s is an even integer;

$$\begin{cases} \epsilon q_0^{\frac{s}{2}} & \text{occurs } \frac{(p^{\frac{n}{2}}+\epsilon)^2(p^e-1)(p^n-1)}{4(p^e+1)} \text{ times} \\ \frac{1}{2}(\epsilon\sqrt{q_0^*}+1)q_0^{\frac{s}{2}} & \text{occurs } \frac{1}{2}p^{\frac{n}{2}-e}(p^{\frac{n}{2}}+1)(p^n-1) \text{ times} \\ \frac{1}{2}(\epsilon\sqrt{q_0^*}-1)q_0^{\frac{s}{2}} & \text{occurs } \frac{1}{2}p^{\frac{n}{2}-e}(p^{\frac{n}{2}}-1)(p^n-1) \text{ times} \\ \frac{1}{2}\epsilon(q_0-1)q_0^{\frac{s}{2}} & \text{occurs } \frac{(p^{\frac{n}{2}-e}+\epsilon)(p^{\frac{n}{2}}-\epsilon)(p^n-1)}{p^{2e}-1} \text{ times} \\ 0 & \text{occurs } \frac{(p^{n+e}-3p^n+p^e+1)(p^n-1)}{2(p^e-1)} \text{ times} \\ p^n & \text{occurs once} \end{cases}$$

where $\epsilon \in \{1, -1\}$.

Summary of the proof: Since the cross-correlation function is expressed in terms of two quadratic forms, their evaluation is performed by the quadratic form and exclusion techniques. Each of the two quadratic forms has the rank s, $s-1$, or $s-2$. Using the exclusion technique in Example 8, it is shown that at least one of the two quadratic forms has the rank s. Hence only the cross-correlation values corresponding to the ranks (s,s), $(s,s-1)$, and $(s,s-2)$ or vice versa actually occur. For their distribution, the authors obtain the rank distributions and the following equations

$$\sum_{\delta,\zeta\in\mathbb{F}_{p^n}} S(\delta,\zeta) = p^{2n}$$
$$\sum_{\delta,\zeta\in\mathbb{F}_{p^n}} S^2(\delta,\zeta) = \begin{cases} p^{3n}, & \text{if } p^e \equiv 1 \bmod 4 \\ p^{2n}, & \text{if } p^e \equiv 3 \bmod 4. \end{cases}$$

Also the equations in Example 11 are needed to compute their distribution. □

Theorem 7 (Xia et al. [16]): For an odd prime p such that $p \equiv 3 \bmod 4$, $d = (p^n+1)/(p+1) + (p^n-1)/2$ with an odd integer n, and $\gcd(d, p^n-1) = 2$, we have $\mathcal{N} = 9$ and $R_{\max} \approx 1 + (p+1)/2p^{n/2}$. As γ runs through $\mathbb{F}_{p^n}^*$, the distribution of $C_d(\gamma)$ in (2) is given as

$$C_d(\gamma) = \begin{cases} -1 & \text{occurs } \frac{(p-1)p^n-(p+3)}{2(p+1)} \text{ times} \\ -1 \pm jp^{\frac{n}{2}} & \text{occurs } \frac{(p-3)(p^n-1)}{4(p-1)} \text{ times} \\ -1 + \frac{\sqrt{p}\pm j}{2}p^{\frac{n}{2}} & \text{occurs } \frac{p^{n-1}+p^{\frac{n-1}{2}}}{2} \text{ times} \\ -1 + \frac{-\sqrt{p}\pm j}{2}p^{\frac{n}{2}} & \text{occurs } \frac{p^{n-1}-p^{\frac{n-1}{2}}}{2} \text{ times} \\ -1 \pm j\frac{p+1}{2}p^{\frac{n}{2}} & \text{occurs } \frac{p^{n-1}-1}{p^2-1} \text{ times.} \end{cases}$$

Summary of the proof: Since the cross-correlation function is expressed in terms of two quadratic forms, its evaluation is performed by the quadratic form and exclusion techniques. Each of the two quadratic forms has the rank n, $n-1$, or $n-2$. Then, it is shown that at least one of the two quadratic forms has the rank n. Using the Weil's bound as in Example 7, the two values $\{-1 + j(p-1)/2p^{n/2}, -1 + j(-p+1)/2p^{n/2}\}$ are ruled out. Note that each conjugate pair has the same number of occurrences as in Example 12. Finally, the two equations

$$\sum_{\gamma\in\mathbb{F}_{p^n}^*} S(\gamma) = 2p^n$$

$$\sum_{\gamma\in\mathbb{F}_{p^n}^*} S^2(\gamma) = 4p^n$$

where $S(\gamma) = 2C_d(\gamma) + 1$, are needed to compute the distribution. □

Theorem 8 (Seo et al. [13]): For an odd prime p, $d = (p^{n/2}+1)^2/4$ with $n \equiv 0 \bmod 4$, and $\gcd(d, p^n-1) = (p^{n/2}+1)/2$, we have $\mathcal{N} = 4$ and $R_{\max} = -1 + 2p^{n/2}$. As τ varies over $0 \le \tau < p^n - 1$, the distribution of $C_d(l,\tau)$ in (2) is given as:

1) When $l = 0$;

$$\begin{cases} -1 & \text{occurs } \frac{(p^{\frac{n}{2}}+1)(5p^{\frac{n}{2}}-9)}{8} \text{ times} \\ -1-p^{\frac{n}{2}} & \text{occurs } \frac{p^n-1}{4} \text{ times} \\ -1+p^{\frac{n}{2}} & \text{occurs } \frac{p^{\frac{n}{2}}+1}{2} \text{ times} \\ -1+2p^{\frac{n}{2}} & \text{occurs } \frac{p^n-1}{8} \text{ times.} \end{cases}$$

2) When $l \neq 0$;

$$\begin{cases} -1 & \text{occurs } \frac{3(p^n-1)}{8} \text{ times} \\ -1-p^{\frac{n}{2}} & \text{occurs } \frac{(p^{\frac{n}{2}}+1)(3p^{\frac{n}{2}}-7)}{8} \text{ times} \\ -1+p^{\frac{n}{2}} & \text{occurs } \frac{(p^{\frac{n}{2}}+1)(p^{\frac{n}{2}}+3)}{8} \text{ times} \\ -1+2p^{\frac{n}{2}} & \text{occurs } \frac{p^n-1}{8} \text{ times.} \end{cases}$$

Summary of the proof: The cross-correlation function is transformed into the exponential sum in Lemma 5. From Lemma 5, the cross-correlation function has the four cross-correlation values as in Example 4. For their distribution, the equations

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

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

and

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

where $m = n/2$, are computed. □

Theorem 9 (Choi et al. [17]): For an odd prime p, $d = (p^m+1)^2/(2(p+1))$ with $n \equiv 2 \bmod 4$, $n = 2m$, and $\gcd(d, p^n-1) = (p^m+1)/2$, we have $R_{\max} = 1+(p+1)p^{n/2}/2$.

Summary of the proof: The cross-correlation function is expressed as two quadratic forms. From the quadratic form technique, each quadratic form has the rank n, $n-1$, and $n-2$. Then, it is shown that at least one of the two quadratic forms has the rank n. Hence the evaluation of the cross-correlation values is done. □

Note that the authors remain the distribution of the cross-correlation values as an open problem in [17]. Recently, Luo and Helleseth [18] derived the distribution of the cross-correlation values for the case when $l = 0$.

5. Conclusion

In this paper, existing results for the cross-correlation distributions of p-ary m-sequences and their decimated sequences are reviewed for an odd prime p. Based on the previously known results, we formulate the methodology to evaluate the cross-correlation values and derive their distribution. Since some p-ary sequence families have better performance than optimal binary sequence families, it is worthwhile to consider the cross-correlation function for an odd prime alphabet size.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2012-0000186) and the KCC (Korea Communications Commission), Korea, under the R&D program supervised by the KCA (Korea Communications Agency) (KCA-2012-08-911-04-003).

References

[1] T. Kasami, "Weight distribution formula for some class of cyclic codes," Report of Coordinated Science Lab., Univ. Illinois, Urbana-Champaign, R-285 (AD 632574), 1966.
[2] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," IEEE Trans. Inf. Theory, vol.14, no.1, pp.154–156, Jan. 1968.
[3] 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.
[4] 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.
[5] 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.
[6] Y. Niho, Multi-valued cross-correlation functions between two maximal recursive sequences, Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, 1972.
[7] H.M. Trachtenberg, On the cross-correlation functions of maximal recurring sequences, Ph.D. Dissertation, Univ. of Southern California, Los Angeles, CA, 1970.
[8] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," Discrete Math., vol.16, pp.209–232, 1976.
[9] 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.
[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, 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.

[12] 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.

[13] 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 $(\frac{p^{2k}+1}{2})^2$," IEEE Trans. Inf. Theory, vol.54, no.7, pp.3140–3149, July 2008.

[14] 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.

[15] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter-Matthew function," IEEE Trans. Inf. Theory, vol.54, no.12, pp.5345–5353, Dec. 2008.

[16] Y. Xia, X. Zeng, and L. Hu, "Further crosscorrelation properties of sequences with the decimation factor $d = (p^n + 1)/(p + 1) - (p^n - 1)/2$," Appl. Algebra Eng. Commun. Comput., vol.21, no.5, pp.329–342, 2010.

[17] S.-T. Choi, T. Lim, J.-S. No, and H. Chung, "On the cross-correlation of a p-ary m-sequences of period $p^{2m} - 1$ and its decimated sequences by $(p^m + 1)^2/2(p + 1)$," IEEE Trans. Inf. Theory, vol.58, no.3, pp.1873–1879, March 2012.

[18] J. Luo, T. Helleseth, and A. Kholosha, "Two nonbinary sequences with six-valued cross correlation," Proc. Inter. Workshop on Signal Design and Its Application in Commun., pp.44–47, Guilin, China, Oct. 2011.

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

[20] R.S. Coulter and R.W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," Des. Codes Cryptogr., vol.10, no.2, pp.167–184, Feb. 1997.

[21] A.W. Bluher, "On $x^{q+1} + ax + b$," Finite Fields and Their Applications, vol.10, no.3, pp.285–305, July 2004.

Sung-Tai Choi received the B.S. degree in electrical engineering and computer science from Seoul National University, Seoul, Korea, in 2006, where he is currently working towards the Ph.D. degree in electrical engineering and computer science. His area of research interests includes pseudo random sequences, coding theory, cryptography, and communications theory.

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 with Hughes Network Systems, Germantown, MD, from February 1988 to July 1990. He was an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, from September 1990 to July 1999. He joined the faculty of the Department of Electrical Engineering and Computer Science, 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 research interests include error-correcting codes, sequences, cryptography, space-time codes, LDPC codes, and wireless communication systems.