On the Cross-Correlation of Ternary m-Sequences of Period $3^{4k+2}-1$ With Decimation $\frac{3^{4k+2}-3^{2k+1}+2}{4}+3^{2k+1}$

Ji-Youp Kim, Sung-Tai Choi, Taehyung Lim and Jong-Seon No
Department of Electrical Engineering and Computer Science
Seoul National University
Seoul 151-742, Korea
{lakroforce, stchoi}@ccl.snu.ac.kr, jsno@snu.ac.kr

Habong Chung
Department of Electronic and Electrical Engineering
Hongik University
Seoul 121-791, Korea
habchung@hongik.ac.kr

***Abstract*—In this paper, for an integer k, we evaluate an upper bound for the cross-correlation of a ternary m-sequence of period $N = 3^{4k+2}-1$ and its decimated sequence with decimation $d = \frac{3^{4k+2}-3^{2k+1}+2}{4}+3^{2k+1}$. It is found that the cross-correlation is upper bounded by $4.5 \cdot 3^{2k+1}+1$.**

***Index Terms*—cross-correlation, decimation, exponential sum, m-sequence, quadratic form**

I. Introduction

The cross-correlation between p-ary m-sequences and their decimated sequences by d has been extensively studied by many researchers. Trachtenberg [1] investigated the cross-correlation for the decimation $d = \frac{p^k+2}{2}$ and $d = p^{2k}-p^k+1$ when p is an odd prime. Helleseth [2] summarized many known results and evaluated cross-correlation distributions for various values of decimations. Muller [3] proved that for odd n, the cross-correlation between a teranry m-sequence and its decimation by $d = \frac{3^n+1}{3+1}+\frac{3^n-1}{2}$ is upper bounded by $2\sqrt{p^n}$. Hu *et al.* [4] generalized Muller's result to $p = 3 \bmod 4$, and Xia, Zeng, and Hu [5] have evaluated the correlation distribution. More recently, Ness and Helleseth, Kholosha [6] derived the distribution of the cross-correlation values for $p = 3$, $d = \frac{3^k+1}{2}$, where k is an odd integer with $\gcd(k,n) = 1$. For an odd prime p, even n, and $d = p^k+1$ with $\gcd(n,k) = 1$, Seo, Kim, No, and Shin [7] estimated the upper bound $1+p\sqrt{p^n}$. Choi, Lim, No, and Chung [8] investigated cross-correlation values for an odd prime p and decimation $d = \frac{(p^m+1)^2}{2(p+1)}$, where m is odd. For a more detailed overview on this subject, we refer the reader to [9].

In this paper, for an integer k, we derived an upper bound for the cross-correlation of a ternary m-sequence of period $3^{4k+2}-1$ and its decimation with $d = \frac{3^{4k+2}-3^{2k+1}+2}{4}+3^{2k+1}$. It is shown that the upper bound is given as $4.5 \cdot 3^{2k+1}+1$. For the derivation, we use the quadratic form theory as in [3]-[8], but in this case four quadratic forms are involved. To obtain possible rank combinations of quadratic forms, Bluher's result [10], [11] is employed. It is shown that quadratic forms have only even ranks and among four quadratic forms, at most one of them have the lowest rank.

The remainder of this paper is organized as follows. In Section II, we present preliminaries and notations. In Section III, we investigate the upper bound for the cross-correlation magnitude. Some discussion and a conjecture on the cross-correlation value is proposed in Section IV. Finally, concluding remarks are given in Section V.

II. Preliminaries

A. Trace Functions and Cross-Correlation Functions

Let p be a prime and n be an integer. Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements. The trace function $\mathrm{tr}_1^n : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is defined as

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

A p-ary m sequence $s(t)$ is defined to be

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

where α is a primitive element of $\mathbb{F}_{p^n}$. Let ω be a p-th root of unity in the complex field $\mathbb{C}$ and $a(t)$, $b(t)$ be sequences over $\mathbb{F}_p$ of period N. Then the cross-correlation function $C(\tau)$ between $a(t)$ and $b(t)$ at time shift τ is defined as

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

B. Quadratic Forms and Linearized Polynomials

A quadratic character $\eta(x)$ of $\mathbb{F}_{p^n}$ is defined as

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

A quadratic form over $\mathbb{F}_p$ with n indeterminates x_1, x_2, ... , x_n is a homogeneous polynomial of degree 2 in $\mathbb{F}_{p^n}[x_1, x_2, ..., x_n]$, which can be expressed as

$$f(x_1, x_2, ..., x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

978-1-4673-2579-0/12/$31.00 ©2012 IEEE

where $a_{ij} \in \mathbb{F}_p$. The matrix $A = (a_{ij})$ is called a coefficient matrix of f, and $\det(f) = \Delta$ is defined to be $\det(A)$. If the rank of A is k for some $0 \le k \le n$, then we say that the rank of f is also k. If $\text{rank}(f) = n$, f is said to be nondegenerate. For a nondegenerate quadratic form f over $\mathbb{F}_p$, one can calculate the number of solutions of $f(x_1, x_2, ..., x_n) = b$ for $b \in \mathbb{F}_p$ by the following lemma.

Lemma 1: [12] Let η be the quadratic character of $\mathbb{F}_p$. The number of solutions $N(b)$ of $f(x_1, x_2, ..., x_n) = b$ in $\mathbb{F}_p^n$, when f is a nondegenerate quadratic form in rank n with determinant Δ and $b \in \mathbb{F}_p$, is given as follows:
Case 1) n even;

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

where $\epsilon = \eta((-1)^{n/2}\Delta)$.
Case 2) n odd;

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

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

From Lemma 1, the following lemma is easily derived.

Lemma 2: [6] Let η be the quadratic character of $\mathbb{F}_3$. Let f be a nondegenerate quadratic form in n variables with determinant Δ and ω be the 3rd root of unity. Then

$$S = \sum_{x \in \mathbb{F}_{3^n}} \omega^{f(x)}$$

is given by

$$S = \begin{cases} \epsilon 3^{n/2}, & \text{if } n \text{ is even} \\ \epsilon i 3^{n/2}, & \text{if } n \text{ is odd} \end{cases}$$

where $\epsilon = \eta((-1)^{n/2}\Delta)$ for even n and $\epsilon = \eta((-1)^{(n-1)/2}\Delta)$ for odd n. □

For the case of $\text{rank}(f) = k < n$, we can obtain the number of solutions by multiplying the result of Lemma 1 or Lemma 2 by p^{n-k}. The rank of the quadratic form can be determined by the following lemma.

Lemma 3: [3] Let $f \in \mathbb{F}_p[x_1, x_2, ..., x_n]$ be a quadratic form. Define

$$Z = \{z \in \mathbb{F}_p^n : f(x+z) - f(x) = 0 \text{ for all } x \in \mathbb{F}_p^n\}.$$

Then Z is a subspace of $\mathbb{F}_p^n$ and $\text{rank}(r) = n - \dim(Z)$. □

Let q be a prime power and m be an integer. A polynomial of the form

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

with coefficients in $\mathbb{F}_{q^m}$ is called a linearized polynomial over $\mathbb{F}_{q^m}$. For an extension field F of $\mathbb{F}_{q^m}$, we have

$$L(x+y) = L(x) + L(y), \text{ for all } x, y \in F$$
$$L(cx) = cL(x), \text{ for all } x \in F \text{ and } c \in \mathbb{F}_q.$$

Thus the set of roots of a linearized polynomial is a vector space over $\mathbb{F}_q$ and the number of roots is a power of q.

C. Number of Solutions of $x^{p^s+1} - cx + c$

The following lemmas will be used to determine the number of solutions of some linearized polynomials.

Lemma 4: [10] [11] Let $h_c(x) = x^{p^s+1} - cx + c$, $c \in \mathbb{F}_{p^n}^*$. Then $h_c(x) = 0$ has either 0, 1, 2, or $p^{\gcd(s,n)} + 1$ roots in $\mathbb{F}_{p^n}^*$. □

Lemma 5: [10] Let F be a finite field of charateristic p and $c \in F^*$. Suppose q is a power of p and $F \cap \mathbb{F}_q = \mathbb{F}_Q$. Define $f(x) = x^{q+1} - cx + c$. Then the following are equivalent.

1) f has at least three roots in F;
2) f has exactly $Q+1$ roots in F;
3) f has at least two roots in F and $N_{F/\mathbb{F}_Q}(r-1) = 1$ for all root r in F.

□

By setting $F = \mathbb{F}_{p^{4k+2}}$, $q = p^{2k}$ in Lemma 5, we have the following result.

Corollary 6: Let k be an integer, $n = 4k+2$, and p be an odd prime. Then $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^{2k}} = \mathbb{F}_{p^2}$. Let $f(x) = x^{p^{2k}+1} - cx + c$, $c \in \mathbb{F}_{p^n}^*$. Then the following are equivalent.

1) f has exactly p^2+1 roots in $\mathbb{F}_{p^n}$;
2) f has at least two roots in $\mathbb{F}_{p^n}$ and

$$(r-1)^{\frac{p^n-1}{p^2-1}} = 1$$

for all root r in $\mathbb{F}_{p^n}$.

□

III. Upper Bound on the Cross-Correlation Function

Let k be an integer and $n = 2m = 2 + 4k$, $d = \frac{3^n - 3^m + 2}{4} + 3^m$. Suppose $\mathbb{F}_{3^n}$ is a finite field with 3^n elements. Set α be a primitive elements of $\mathbb{F}_{3^n}$. Let $N = 3^n - 1$ be the period of m-sequence in $\mathbb{F}_{3^n}$. Then $\gcd(N, d) = \frac{3^m+1}{4}$. Set $0 \le l < N/\gcd(N,d) = 4(3^m+1)$. We consider the cross-correlation function $C(\tau)$ between $\text{tr}_1^n(\alpha^t)$ and $\text{tr}_1^n(\alpha^{dt+l})$ with time shift τ. Then $C(\tau)$ is given as

$$\begin{aligned} C(\tau) &= \sum_{t=0}^{N-1} \omega^{\text{tr}_1^n(\alpha^t) - \text{tr}_1^n(\alpha^{d(t+\tau)+l})} \\ &= \sum_{t=0}^{N-1} \omega^{\text{tr}_1^n(\alpha^t - \gamma\alpha^{dt})} \\ &= \sum_{x \in \mathbb{F}_{3^n}^*} \omega^{\text{tr}_1^n(x - \gamma x^d)} \end{aligned}$$

where $\gamma = \alpha^{d\tau+l}$ and ω is a third primitive root of unity. Let $x = y^{3^{n-1}-1}$. Since $d(3^{n-1}-1) = 3^{n/2}+1 = 3^m+1 \bmod N$, we have

$$\mathrm{tr}_1^n(x - \gamma x^d) = \mathrm{tr}_1^n(y^{3^{n-1}-1} - \gamma y^{3^m+1}).$$

Thus we have quadratic forms in y. Since $(3^{n-1}-1, 3^n-1) = 4$, we must consider $a_i \in C_i$, $0 \le i \le 3$, so that

$$\begin{aligned} 4(1+C(\tau)) &= 4\left(\sum_{x\in\mathbb{F}_{3^n}} \omega^{\mathrm{tr}_1^n(x-\gamma x^d)}\right) \\ &= \sum_{i=0}^{3}\sum_{y\in\mathbb{F}_{3^n}} \omega^{\mathrm{tr}_1^n(a_i y^{3^{n-1}-1}-\gamma a_i^d y^{3^m+1})} \end{aligned}$$

where $C_i = \{\alpha^{4t+i} | 0 \le t < \frac{3^n-1}{4}\}$. Here $g_i(y) = \mathrm{tr}_1^n(a_i y^{3^{n-1}-1} - \gamma a_i^d y^{3^m+1})$, $0 \le i \le 3$, are quadratic forms. To derive the upper bound of the absolute values of the cross-correlation, it is standard to obtain the rank of the quadratic forms and apply Lemma 1. By Lemma 3, investigating the rank of $g_i(y)$ can be done by counting the number of z such that $g_i(y+z) - g_i(y) = 0$ for all $y \in \mathbb{F}_{3^n}$. Simplifying the equation $g_i(y+z) - g_i(y) = 0$ gives us

$$\begin{aligned} \mathrm{tr}_1^n(y({a_i}^3 z^3 + a_i z^{3^{n-1}} - (\gamma a_i^d)^{3^m} z^{3^m} - \gamma a_i^d z^{3^m}) \\ + a_i z^{3^{n-1}+1} - \gamma a_i^d z^{3^m+1}) = 0. \end{aligned}$$

To satisfy this equation for all y, we must have

$$\begin{aligned} {a_i}^3 z^3 + a_i z^{3^{n-1}} - (\gamma a_i^d)^{3^m} z^{3^m} - \gamma a_i z^{3^m} = 0 \\ \mathrm{tr}_1^n(a_i z^{3^{n-1}+1} - \gamma a_i^d z^{3^m+1}) = 0. \end{aligned}$$

Here we claim that the first equation is sufficient condition for the second. Indeed,

$$\begin{aligned} &{a_i}^3 z^3 + a_i z^{3^{n-1}} - (\gamma a_i^d)^{3^m} z^{3^m} - \gamma a_i^d z^{3^m} = 0 \\ &\Leftrightarrow {a_i}^3 z^{3+1} + a_i z^{3^{n-1}+1} - (\gamma a_i^d)^{3^m} z^{3^m+1} - \gamma a_i^d z^{3^m+1} = 0 \\ &\Leftrightarrow {a_i}^3 z^{3+1} - \gamma a_i^d z^{3^m+1} = -a_i z^{3^{n-1}+1} + (\gamma a_i^d)^{3^m} z^{3^m+1} \\ &\Rightarrow \mathrm{tr}_1^n({a_i}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}) \\ &\quad = -\mathrm{tr}_1^n(a_i z^{3^{n-1}+1} - (\gamma a_i^d)^{3^m} z^{3^m+1}) \\ &\Leftrightarrow \mathrm{tr}_1^n({a_i}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}) = -\mathrm{tr}_1^n({a_i}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}) \\ &\Leftrightarrow 2\mathrm{tr}_1^n({a_i}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}) = 0 \\ &\Leftrightarrow \mathrm{tr}_1^n({a_i}^3 z^{3+1} - \gamma a_i^d z^{3^m+1}) = 0. \end{aligned}$$

Let $f_i(z) = {a_i}^3 z^3 + a_i z^{3^{n-1}} - (\gamma a_i^d)^{3^m} z^{3^m} - \gamma a_i^d z^{3^m}$. By the discussion above, it is sufficient to count the number of roots of linearized polynomial $f_i(z)$. Now we prove that the number of roots of the linearized polynomial $f_i(z)$ is one of 1, 9, and 81. Note that the linearized polynomial $f_i(z)$ has the degree 3^{n-1}, which is not constant, but depends on n.

Lemma 7: The number of roots of the linearized polynomial $f_i(z)$, $i = 0, 1, 2$ or 3, is one of 1, 9, and 81.

Proof: We have the following equalities

$$\begin{aligned} &{a_i}^3 z^3 + a_i z^{3^{n-1}} - (\gamma a_i^d)^{3^m} z^{3^m} - \gamma a_i^d z^{3^m} = 0 \\ &\Leftrightarrow {a_i}^3 z^3 + a_i z^{3^{n-1}} = ((\gamma a_i^d)^{3^m} + \gamma a_i^d) z^{3^m}. \end{aligned}$$

Here we assume $z \neq 0$. By dividing the both sides by z^{3^m}, we obtain

$$\frac{{a_i}^3}{z^{3^m-3}} + a_i z^{3^{n-1}-3^m} = ((\gamma a_i^d)^{3^m} + \gamma a_i^d).$$

Let $X = z^{3^{m-1}-1}$. Since $(3^{m-1}-1, 3^n-1) = 3^2 - 1 = 8$, this transform is an 8-1 map. Define $B_i = (\gamma a_i^d)^{3^m} + \gamma a_i^d$ and $Y = a_i X$. Then the equality becomes

$$\begin{aligned} \frac{{a_i}^3}{X^3} + a_i X^{3^m} = B_i \\ \Leftrightarrow \frac{1}{Y^3} + {a_i}^{3^m+1} Y^{3^m} = B_i. \end{aligned}$$

Set $A_i = {a_i}^{3^m+1}$. Note $A \in \mathbb{F}_{3^m}$. Let $Y^3 = x$. It is a one-to-one mapping since $(3^n - 1, 3) = 1$. Thus,

$$\begin{aligned} \frac{1}{Y^3} + A_i Y^{3^m} = B_i \\ \Leftrightarrow \frac{1}{x} + A_i x^{3^{m-1}} = B_i \\ \Leftrightarrow 1 + A_i x^{3^{m-1}+1} = B_i x. \end{aligned}$$

Here we let $x = \frac{1}{B_i} y$. Then we have

$$\begin{aligned} 1 + A_i\left(\frac{1}{B_i} y\right)^{3^{m-1}+1} = B_i \frac{1}{B_i} y \\ \Leftrightarrow 1 + \frac{A_i}{B_i^{3^{m-1}+1}} y^{3^{m-1}+1} = y. \end{aligned} \quad (1)$$

Let $\frac{A_i}{B_i^{3^{m-1}+1}} = \frac{1}{c_i}$. Then (1) becomes

$$\begin{aligned} 1 + \frac{1}{c_i} y^{3^{m-1}+1} = y \\ \Leftrightarrow y^{3^{m-1}+1} - c_i y + c_i = 0. \end{aligned}$$

Then by Lemma 4, the number of solutions of $y^{3^{m-1}+1} - c_i y + c_i = 0$ is one of 0, 1, 2, and $3^{(m-1,n)} + 1 = 3^2 + 1 = 10$. Since the mapping is 8-1 map, the number of solutions is one among 0, 8, 16, and 80. Adding a zero root ($z = 0$), we have 1, 9, 17, and 81. Since the original equation is a linearized polynomial, 17 cannot be a number of root. Thus the linearized polynomial can have only 1, 9, and 81 roots. □

Next we show that among the four linearized polynomials $f_i(z)$, $0 \le i \le 3$, at most one polynomial can have 81 roots.

Lemma 8: Among the four linearized polynomials $f_i(z)$, $0 \le i \le 3$, at most one polynomial can have 81 solutions. Or equivalently, among four polynomials $h_i(y) = y^{3^{m-1}+1} - c_i y + c_i$, $0 \le i \le 3$, at most one polynomial can have 10 solutions.

Proof: Without loss of generality, we may assume that $a_i = \alpha^i$. By the previous lemma, we have the following relation

$$c_i = \frac{(\mathrm{tr}_m^n(\gamma a_i^d))^{3^{m-1}+1}}{a_i^{3^m+1}},\ y = \frac{\mathrm{tr}_m^n(\gamma a_i^d)}{a_i^3} z^{3^m-3}. \quad (2)$$

Suppose $\beta = \alpha^{\frac{3^n-1}{3^m-1}} = \alpha^{3^m+1}$ is a primitive element of the subfield $\mathbb{F}_{3^m}$. Since $a_i^{3^m+1} = (\alpha^i)^{3^m+1} = \beta^i$, for $i = 0, 2$, $a_i^{3^m+1}$ is a square in the subfield, and for $i = 1, 3$, $a_i^{3^m+1}$ is a nonsquare element of the subfield. The numerator $(\mathrm{tr}_m^n(\gamma a_i^d))^{3^{m-1}+1}$ is always a square in the subfield $\mathbb{F}_{3^m}$. Consequently, c_i is a square in the subfield if $i = 0, 2$, and a nonsquare if $i = 1, 3$. We claim that only $f_0(z)$ can have 81 roots. Suppose $f_i(z)$ has 81 roots. First assume that $i = 0$ or $i = 2$. By Corollary 6, we have

$$\left(\frac{y^{3^{m-1}+1}}{c_i}\right)^{\frac{3^n-1}{3^2-1}} = (y-1)^{\frac{3^n-1}{3^2-1}} = 1. \tag{3}$$

Since c_i is a square in $\mathbb{F}_{3^m}$, $c_i = \beta^{2k}$ for some k. Also note that $\beta = \alpha^{4l}$ for some l. Therefore we have

$$c_i^{\frac{3^n-1}{3^2-1}} = (\alpha^{8kl})^{\frac{3^n-1}{3^2-1}} = 1.$$

Thus $(y^{3^{m-1}+1})^{\frac{3^n-1}{3^2-1}} = 1$. Since $3^{m-1}+1 = 2 \bmod 4$, we can substitute as $y^{3^{m-1}+1} = x^{4k+2}$. Then we have

$$(x^{4k+2})^{\frac{3^n-1}{8}} = (x^{2k+1})^{\frac{3^n-1}{4}} = 1.$$

Therefore $y^{\frac{3^{m-1}+1}{2}} = x^{2k+1} = \alpha^{4l'}$ for some l'. But since $(\frac{3^{m-1}+1}{2}, 4) = 1$, we have $y = \alpha^{4l'}$. From (2), $ya_i^3 = \mathrm{tr}_m^n(\gamma a_i^d) z^{3^m-3}$. Here all terms in the right hand side are in C_0. We already observed that $y \in C_0$. Therefore we must have $a_i \in C_0$. This implies that $i = 0$. Now assume that $i = 1$ or $i = 3$. This means that c_i is a nonsquare in $\mathbb{F}_{3^n}$. Thus, we can write $c_i = \beta^{2k+1} = (\alpha^{4l})^{2k+1} = \alpha^{8lk+4l}$. Note that l is odd since m is odd. Applying Corollary 6 again, we have (3), but for this case, it follows that

$$c_i^{\frac{3^n-1}{3^2-1}} = (\alpha^{2lk+l})^{\frac{3^n-1}{2}} = (-1)^{(2k+1)l} = -1.$$

Therfore $(y^{3^{m-1}+1})^{\frac{3^n-1}{3^2-1}} = -1$. Since $3^{m-1}+1 = 2 \bmod 4$, we can substitute as $3^{m-1}+1 = 4k+2$ for some k. Then we have

$$(y^{2k+1})^{\frac{3^n-1}{4}} = -1 \Leftrightarrow \left(y^{\frac{3^n-1}{2}}\right)^k y^{\frac{3^n-1}{4}} = \alpha^{\frac{3^n-1}{2}k'} \tag{4}$$

where k' is some odd integer. Thus y must be a square in $\mathbb{F}_{3^n}$. Let $y = \alpha^{2l'}$ for some integer l'. From (4), it follows that

$$\alpha^{\frac{3^n-1}{2}l'} = \alpha^{\frac{3^n-1}{2}k'}.$$

Therefore, l' is odd. Thus $y \in C_2$. From (2), we have $a_i \in C_2$. This implies that c_i is in C_2, which contradicts $i = 1$ or $i = 3$. Therefore if $f_i(z)$ has 81 roots, then $i = 0$. □

It is well known that the number of roots of the linearized polynomial $f_i(z)$ is equal to $3^{n-rank(g_i(y))}$. Therefore by what we have dicussed so far, each $g_i(y)$ has a rank of n, $n-2$, or $n-4$, and only one of $g_i(y)$ can have the rank $n-4$ for $i = 0, 1, 2, 3$. Thus we can enumrate 9 possible rank combinations of $g_i(y)$, $i = 0, 1, 2, 3$, ignoring order as

$$\begin{aligned}&(n,n,n,n),\ (n,n,n,n-2),\ (n,n,n,n-4),\\ &(n,n,n-2,n-2),\ (n,n,n-2,n-4),\\ &(n,n-2,n-2,n-2),\ (n,n-2,n-2,n-4),\\ &(n-2,n-2,n-2,n-2),\ (n-2,n-2,n-2,n-4).\end{aligned} \tag{5}$$

For each of these rank combinations, we can derive the upper bound of the cross-correlation values using Lemma 2. We will check only for the last case, $(n-2, n-2, n-2, n-4)$. Using Lemma 2, it follows that

$$\begin{aligned}4(1+C(\tau)) &= \sum_{i=0}^{3}\sum_{y\in\mathbb{F}_{3^m}} \omega^{g_i(y)} \\ &= \epsilon_0 3^2 3^{\frac{n-2}{2}} + \epsilon_1 3^2 3^{\frac{n-2}{2}} + \epsilon_2 3^2 3^{\frac{n-2}{2}} \\ &\quad + \epsilon_3 3^4 3^{\frac{n-4}{2}} \\ &= 3(\epsilon_0+\epsilon_1+\epsilon_2)3^m + 3^2\epsilon_3 3^m \\ &\le 18 \cdot 3^m\end{aligned} \tag{6}$$

where ϵ_0, ϵ_1, ϵ_2, ϵ_3, are determined to be 1 or -1 according to the rank and determinant of the quadratic forms. Thus in this case, the magnitude of the cross-correlation function $C(\tau)$ is upper bounded by $4.5 \cdot 3^m + 1$. It is easily checked that among all the rank combinations above, $(n-2, n-2, n-2, n-4)$ yields the largest upper bound for $C(\tau)$. Therefore, we have the following theorem.

Theorem 9: For an integer $k \ge 0$, $n = 4k+2 = 2m$, $d = \frac{3^n-3^m+2}{4} + 3^m$, and $0 \le l < 4(3^m+1)$, the magnitude of the cross-correlation function $C(\tau)$ between $\mathrm{tr}_1^n(\alpha^t)$ and $\mathrm{tr}_1^n(\alpha^{dt+l})$ is upper bounded by

$$|C(\tau)| \le 4.5 \cdot 3^m + 1.$$

□

IV. Discussion

First we consider an example. Suppose $n = 4k+2 = 2m = 6$ and $d = 203$. For all l going through 0 to $4(3^m+1) - 1 = 103$, by computer search, the cross-correlation distribution between $\mathrm{tr}_1^n(\alpha^t)$ and $\mathrm{tr}_1^n(\alpha^{dt+l})$ is given as

$$C(\tau) = \begin{cases} -1, & 34328 \text{ times} \\ -28, & 18095 \text{ times} \\ 26, & 14973 \text{ times} \\ -82, & 833 \text{ times} \\ 80, & 938 \text{ times} \\ -55, & 4676 \text{ times} \\ 53 & 1869 \text{ times.} \end{cases}$$

Note that the cross-correlation is 7-valued. The similar result is obtained for $n = 10$. Based on these, we propose the following conjecture on the cross-correlation distribution.

Conjecture 10: For an integer $k \ge 0$, $n = 4k+2 = 2m$, $d = \frac{3^n-3^m+2}{4} + 3^m$, and $0 \le l < 4(3^m+1)$, the cross-correlation function $C(\tau)$ between $\mathrm{tr}_1^n(\alpha^t)$ and $\mathrm{tr}_1^n(\alpha^{dt+l})$ takes values in $\{-1, -1 \pm 3^m, -1 \pm 3^{m+1}, -1 \pm (3-1)3^m\}$.

Therefore the magnitude of $C(\tau)$ is upper bounded by $3 \cdot 3^m + 1$. □

The main difficulty of the problem originates from two factors. First, since there are more than two quadratic forms involved, we have to exclude more candidate values for the cross-correlation. In computer search, we found that every rank combination in (5) actually appear. Thus we have to rule out some combinations of ϵ_i values, so that some exponential sums in (6) cancel out each other. One typical technique to do this is to set $g_i(y) = rg_j(y)$ for some nonsquare r so that $\det(g_i) = r^k \det(g_j)$, where k is a rank of g_i and g_j. If k is odd, we can conclude that $\epsilon_i = -\epsilon_j$ as we wish to show. But in our case, all ranks of quadratic forms are even. This is the second factor which makes the problem difficult.

V. Conclusion

In this paper, we investigate the upper bound for the crosscorrelation function between a ternary m-sequence of period $n = 4k + 2$ and its decimated sequence with the decimation $d = \frac{3^{4k+2}-3^{2k+1}+2}{4} + 3^{2k+1}$. It is shown that the cross-correlation is upper bounded by $4.5 \cdot 3^{n/2} + 1$. For the derivation, it is proved that 1, 9, 81 are only possible number of solutions of linearized polynomials and only one among four linearized polynomials can have 81 roots. A conjecture on the exact cross-correlation value is proposed as an open problem.

Ackledgement

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

References

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

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

[3] E. N. Muller, "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.

[4] Z. Hu, X. Li, D. Mills, E. Mller, W. Sun, W. Willems, Y. Yang, and Z. Zhang, "On the crosscorrelation of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$," *Appl. Algebra Eng. Commun. Comput.*, vol. 12, no. 3, pp. 255263, 2001.

[5] Y. Xia, X. Zeng, and L. Hu, "Further crosscorrelation properties of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$," *Appl. Algebra Eng. Commun. Comput.*, vol. 21, no. 5, pp. 329342, 2010.

[6] 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.

[7] 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.

[8] S.-T. Choi, T. Lim, J.-S. No, and H. Chung, "On the crosscorrelation 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.

[9] S.-T. Choi and J.-S. No, "On the cross-correlation distributions of p-ary m-sequences and their decimated sequences," accepted for publication in *IEICE Trans. Fundamentals*.

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

[11] X. Zeng, N. Li and L. Hu, "A class of nonbinary codes and sequence families," *Sequences and Their Applications 2008*, Sep. 14-18, 2008.

[12] R.Lidl and H.Niederreliter, *Finite Fields*. Amsterdam, The Netherlands: Addison-Wesley, 1983, vol.20, Encyclopedia of Mathematics and its Applications.