On the Cross-Correlation of a Ternary m-sequence of Period $3^{4k+2}-1$ and Its Decimated Sequence by $\frac{(3^{2k+1}+1)^2}{8}$

Sung-Tai Choi and Jong-Seon No
Department of Electrical Engineering and Computer Science
Seoul National University
Seoul 151-742, Korea
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, we investigate into the cross-correlation of a ternary m-sequence $m(t)$ of period 3^n-1 and its decimated sequence $m(dt)$ by $d=\frac{(3^m+1)^2}{8}$, where $n=2m=4k+2$. It is shown that the magnitude of the cross-correlation values is upper bounded by $2\sqrt{3^n}+1$.**

I. Introduction

There have been lots of research to find a decimation value d such that the cross-correlation between a p-ary m-sequence $s(t)$ and its decimation $s(dt)$ is low. The values d with $\gcd(d,p^n-1)=1$ have been studied by Trachtenberg [1], Helleseth [2], and Dobbertin, Helleseth, Kumar, and Martinsen [3].

When the decimation value d is not relatively prime to the period p^n-1, the decimation $s(dt)$ has short period, $\frac{p^n-1}{\gcd(d,p^n-1)}$. For a ternary case, Ness, Helleseth, and Kholosha [4] derived the correlation distributions for $d=\frac{3^k+1}{2}$, $\gcd(k,n)=1$, and k an odd integer, which is Coulter-Matthews decimation. Muller [5] showed that the magnitude of correlation values is upper bounded by $2\sqrt{3^n}+1$ for $d=\frac{3^n+1}{4}+\frac{3^n-1}{2}$ and n an odd integer. Hu *et al.* [6] extended Muller's result to any odd prime case, i.e., for $d=\frac{p^n+1}{p+1}-\frac{p^n-1}{2}$ and derived the upper bound as $\frac{p+1}{2}\sqrt{p^n}$. Seo, Kim, No, and Shin [7] derived the correlation distributions for $d=\frac{(p^{2k}+1)^2}{4}$, when p is an odd prime and $n=4k$.

In this paper, an upper bound of the correlation values of a ternary m-sequence and its decimation sequence is derived for $d=\frac{(3^m+1)^2}{8}$, $n=2m$, and m an odd integer. Then $s(dt)$ has the period of $2(3^m-1)$ because $\gcd(d,3^n-1)=\frac{3^m+1}{2}$. It is shown that the magnitude of cross-correlation function $C_d(\tau)$ between $s(t)$ and $s(dt)$ is upper bounded by $2\sqrt{3^n}+1$.

II. Preliminaries

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

$$\mathrm{tr}_s^n(x)=\sum_{i=0}^{\frac{n}{s}-1}x^{p^{si}}$$

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

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

where ω_p is the p-th root of unity.

In the remaining part of this paper, the following notations will be used:

- $n=2m$, where m is an odd integer;
- $d=\frac{(3^m+1)^2}{8}$;
- α is a primitive element of F_{3^n};
- ω is a primitive third root of unity.

III. Quadratic Expression for Cross-Correlation Function

The cross-correlation between $s(t)$ and $s(dt)$ is given as

$$C_d(\tau)=\sum_{t=0}^{3^n-2}\omega^{\mathrm{tr}_1^n(\alpha^{t+\tau}-\alpha^{dt})}=\sum_{x\in F_{3^n}^*}\omega^{\mathrm{tr}_1^n(ax-x^d)} \quad (1)$$

where $x=\alpha^t$ and $a=\alpha^\tau$.

Let $C(a)$ be the function defined by

$$C(a)=\sum_{x\in F_{3^n}}\omega^{\mathrm{tr}_1^n(ax-x^d)}. \quad (2)$$

Then the cross-correlation function can be expressed as $C_d(\tau)=C(a)-1$.

Exactly the half of the elements in $F_{3^n}^*$ are squares and the other half are nonsquares. Since $\gcd(3^{m+1}+1,3^n-1)=2$, we can represent the squares as $x=y^{3^{m+1}+1}$ and nonsquares as $x=ry^{3^{m+1}+1}$, where $y\in F_{3^n}^*$ and r is a nonsquare in $F_{3^n}^*$. Also, note that as y runs through $F_{3^n}^*$, each $x\in F_{3^n}^*$ appears twice. Hence, we can express $C(a)$ as

$$2C(a)=\sum_{y\in F_{3^n}}\omega^{\mathrm{tr}_1^n(ay^{3^{m+1}+1}-y^{d(3^{m+1}+1)})}+\sum_{y\in F_{3^n}}\omega^{\mathrm{tr}_1^n(ary^{3^{m+1}+1}-r^dy^{d(3^{m+1}+1)})}.$$

Since $(3^{m+1}+1)d \equiv 3^m+1 \bmod 3^n-1$, we have

$$2C(a) = \sum_{y\in F_{3^n}} \omega^{\mathrm{tr}_1^n(ay^{3^{m+1}+1}-y^{3^m+1})} + \sum_{y\in F_{3^n}} \omega^{\mathrm{tr}_1^n(ary^{3^{m+1}+1}-r^d y^{3^m+1})}. \quad (3)$$

Let

$$\begin{aligned} g(y) &= \mathrm{tr}_1^n(ay^{3^{m+1}+1}-y^{3^m+1}) \\ h(y) &= \mathrm{tr}_1^n(ary^{3^{m+1}+1}-r^d y^{3^m+1}). \end{aligned}$$

If y is expressed in terms of a basis $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ of F_{3^n} over F_3 as $y=\sum_{i=1}^n y_i\alpha_i$, where $y_i\in F_3$, then the $g(y)$ and $h(y)$ are given as quadratic forms. It can be easily shown as

$$\begin{aligned} &g(y) \\ =&\mathrm{tr}_1^n\Big(a(\sum_{i=1}^n y_i\alpha_i^{3^{m+1}})(\sum_{i=1}^n y_i\alpha_i)-(\sum_{i=1}^n y_i\alpha_i^{3^m})(\sum_{i=1}^n y_i\alpha_i)\Big) \\ =&\mathrm{tr}_1^n\Big(a\sum_{i=1}^n\sum_{j=1}^n (y_iy_j)(\alpha_i^{3^{m+1}}\alpha_j)-\sum_{i=1}^n\sum_{j=1}^n (y_iy_j)(\alpha_i^{3^m}\alpha_j)\Big) \\ =&\sum_{i=1}^n\sum_{j=1}^n (y_iy_j)\mathrm{tr}_1^n\Big(a(\alpha_i^{3^{m+1}}\alpha_j)-(\alpha_i^{3^m}\alpha_j)\Big) \\ =&\sum_{i=1}^n\sum_{j=1}^n (y_iy_j)a_{ij} \end{aligned}$$

where $a_{ij}=\mathrm{tr}_1^n\Big(a(\alpha_i^{3^{m+1}}\alpha_j)-(\alpha_i^{3^m}\alpha_j)\Big)$. Similarly, we can show that $h(y)$ is also of a quadratic form because $h(y)$ is obtained from $g(y)$ by replacing a by ar.

Any quadratic form can be transformed to a canonical form with nonsingular transformation . The number of solutions $x\in F_{p^n}$ satisfying the quadratic form $f(x)=c$ for any $c\in F_p$ can be decided from the rank of the quadratic form $f(x)$. The rank ρ of the quadratic form $f(x)$ can be determined by finding the number of coordinates that the form is independent of, i.e., $p^{n-\rho}$ is the number of $z\in F_{p^n}$ such that $g(y+z)=g(y)$ for all $y\in F_{p^n}$, which is stated in the following lemma.

Lemma 1: [5] Let

$$f\in F_p[x_1,\cdots,x_n]$$

be a quadratic form. Furthermore, let

$$Y:=\{\mathbf{y}\in(F_p)^n : f(\mathbf{x}+\mathbf{y})-f(\mathbf{x})=0 \text{ for all } \mathbf{x}\in(F_p)^n\}.$$

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

In order to derive the values of the exponential sum $C(a)$, we have to find the rank of the quadratic forms $g(y)$ and $h(y)$, i.e., the number of solutions $z\in F_{3^n}$ of the equations $g(y+z)=g(y)$ and $h(y+z)=h(y)$ satisfying for all $y\in F_{3^n}$ as in the following lemma.

Lemma 2: The number of solutions $z\in F_{3^n}$ such that $g(y+z)=g(y)$ for all $y\in F_{3^n}$ equals the number of solutions $z\in F_{3^n}$ of

$$a^{3^{m+1}}z^{3^2}+z^3+az=0 \quad (4)$$

and the number of solutions $z\in F_{3^n}$ such that $h(y+z)=h(y)$ for all $y\in F_{3^n}$ equals the number of solutions $z\in F_{3^n}$ of

$$(ar)^{3^{m+1}}z^{3^2}-(r^{3d}+r^{d3^{m+1}})z^3+arz=0 \quad (5)$$

where r is a nonsquare in F_{3^n}.

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

$$\mathrm{tr}_1^n(a(y+z)^{3^{m+1}+1}-(y+z)^{3^m+1})=\mathrm{tr}_1^n(ay^{3^{m+1}+1}-y^{3^m+1}). \quad (6)$$

Then (6) can be rewritten as

$$\mathrm{tr}_1^n(y^{3^{m+1}}(a^{3^{m+1}}z^{3^2}+z^3+az)+az^{3^{m+1}+1}-z^{3^m+1})=0. \quad (7)$$

The equation (7) holds for all $y\in F_{3^n}$ if and only if

$$\begin{aligned} a^{3^{m+1}}z^{3^2}+z^3+az &= 0 \quad (8) \\ \mathrm{tr}_1^n(az^{3^{m+1}+1}-z^{3^m+1}) &= 0 \quad (9) \end{aligned}$$

are satisfied simultaneously. Hence the number of solutions $z\in F_{3^n}$ satisfying (6) can be determined by finding the number of solutions $z\in F_{3^n}$ satisfying (8) and (9).

Now, we will show that all solutions $z\in F_{p^n}$ satisfying (8) also satisfy (9). From (8) we have

$$-z^3=a^{3^{m+1}}z^{3^2}+az$$

and raising the 3^{i-1} power gives us

$$-z^{3^i}=a^{3^{m+i}}z^{3^{i+1}}+a^{3^{i-1}}z^{3^{i-1}}. \quad (10)$$

Using (10), (9) can be rewritten as

$$\begin{aligned} &\mathrm{tr}_1^n(az^{3^{m+1}+1}-z^{3^m+1}) \\ =&\sum_{i=1}^n a^{3^i}(z^{3^{m+1}+1})^{3^i}-\sum_{i=1}^n(z^{3^m+1})^{3^i} \\ =&\sum_{i=1}^n a^{3^i}(z^{3^{m+i+1}+3^i})-\sum_{i=1}^n(z^{3^{m+i}+3^i}) \\ =&\sum_{i=1}^n a^{3^i}(z^{3^{m+i+1}+3^i})+\sum_{i=1}^n(-z^{3^i}z^{3^{m+i}}) \\ =&\sum_{i=1}^n a^{3^i}(z^{3^{m+i+1}+3^i}) \\ &+\sum_{i=1}^n((a^{3^{m+i}}z^{3^{i+1}}+a^{3^{i-1}}z^{3^{i-1}})z^{3^{m+i}}) \\ =&\sum_{i=1}^n a^{3^i}(z^{3^{m+i+1}+3^i}) \\ &+\sum_{i=1}^n((a^{3^{m+i}}z^{3^{i+1}+3^{m+i}}+a^{3^{i-1}}z^{3^{i-1}+3^{m+i}})) \\ =&\,3\sum_{i=1}^n a^{3^i}(z^{3^{m+i+1}+3^i})=0. \end{aligned}$$

Hence we only need to calculate the number of solutions for (8) to determine the number of solutions for (7).

The other case $h(y)$ can be proved similarly. □

From Lemma 2, we have to find out the number of solutions $z \in F_{3^n}$ of (4) and (5) to find the rank of $g(y)$ and $h(y)$, respectively. Since the degree of equations are both 9 and the equations are both linearized forms, the possible number of solutions in F_{3^n} for both equations are $1, 3$, or 9.

Now, we will show that the number of solutions of (5) is always one in the following lemma.

Lemma 3: The equation (5)

$$(ar)^{3^{m+1}} z^9 - (r^{3d} + r^{d3^{m+1}}) z^3 + arz = 0$$

has $z = 0$ as its only solution in F_{3^n}, where r is a nonsquare in $F_{3^n}^*$.

Proof: First, we will show that

$$r^{3d} + r^{3^{m+1}d} = 0 \tag{11}$$

for any nonsquare r in F_{3^n}. Since we have

$$3d(3^m - 1) = \frac{(3^m+1)^2}{2(3+1)} 3(3^m - 1) = \frac{3^n - 1}{2} \frac{3^m + 1}{3+1} 3$$

and $\frac{3^m+1}{3+1} = 3^{m-1} - 3^{m-2} + 3^{m-3} - \cdots - 3 + 1$ is an odd integer, any nonsquare r satisfies

$$r^{3d} + r^{3^{m+1}d} = r^{3d}(1 + r^{3d(3^m-1)}) = 0.$$

From $r^{3d} + r^{3^{m+1}d} = 0$, (5) can be rewritten as

$$arz\Big((ar)^{3^{m+1}-1} z^{3^2-1} + 1\Big) = 0.$$

Since $3^2 - 1 | 3^{m+1} - 1$, $(ar)^{3^{m+1}-1} z^{3^2-1} = u^{3^2-1}$ for some $u \in F_{3^n}$. But there is no such u in F_{3^n} satisfying $u^{3^2-1} = -1$, since $3^2 - 1$ does not divide any odd multiples of $\frac{3^n-1}{2}$. □

From the above lemmas, we know that $g(y)$ has the rank of n, $n-1$, or $n-2$ and $h(y)$ has the rank of n.

IV. Upper Bound on Cross-Correlation Values

In this section, the upper bound on the magnitude of the cross-correlation function $C_d(\tau)$ of ternary m-sequence $m(t)$ and its decimated sequence $m(dt)$ in (1) will be derived.

First, we will define the quadratic character of F_{p^n} as

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

We will use the following lemmas for the proof of our main theorem of the upper bound on the cross-correlation values.

Lemma 4: [8] Let η be the quadratic character of F_p. The number of solutions $N(c)$ of $f(y) = c$ when $f(x)$ is a nondegenerate quadratic form in t variables with determinant Δ, is given as follows:

Case 1) t even;

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

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

Case 2) t odd;

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

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

□

Since $p = 3$ we can derive the following lemma from Lemma 4 easily. The result of the following lemma will be used to derive the correlation function.

Lemma 5: [4] Let η be the quadratic character of F_3 (i.e., $\eta(0) = 0$, $\eta(1) = 1$, and $\eta(2) = -1$). Let $f(x)$ be a nondegenerate quadratic form in t variables with determinant Δ. Then

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

is given by

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

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

□

Using Lemma 5, the upper bound on the magnitude of $C_d(\tau)$ in (1) is derived in the following theorem.

Theorem 6: Let $n = 2m$ and $d = \frac{(3^m+1)^2}{8}$, where m is an odd integer. Then the magnitude of $C_d(\tau)$ in (1) is upper bounded by

$$|C_d(\tau)| \leq 2 \cdot 3^{\frac{n}{2}} + 1.$$

Proof: First, we will derive the upper bound on the magnitude of $C(a)$. Using $g(y)$ and $h(y)$, (3) can be rewritten as

$$2C(a) = \sum_{y \in F_{3^n}} \omega^{g(y)} + \sum_{y \in F_{3^n}} \omega^{h(y)}$$

where $g(y) = \mathrm{tr}_1^n(ay^{3^{m+1}+1} - y^{3^m+1})$ and $h(y) = \mathrm{tr}_1^n(ary^{3^{m+1}+1} - r^d y^{3^m+1})$ are both quadratic forms and r is a nonsquare in $F_{3^n}^*$. Let ϵ_g and ϵ_h be the values defined in Lemma 5 corresponding to the quadratic forms of $g(y)$ and $h(y)$, respectively. Note that in the case when the rank ρ of a quadratic form is less than n, the corresponding exponential sum should be multiplied by $3^{n-\rho}$.

It follows from Lemma 2 that the possible rank combinations of the quadratic forms of $g(y)$ and $h(y)$ are (n, n), $(n-1, n)$, and $(n-2, n)$. Hence the following three cases should be considered to determine the value of $C(a)$.

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

From Lemma 5, we have

$$\begin{aligned} 2C(a) &= \textstyle\sum_{y \in F_{3^n}} \omega^{g(y)} + \sum_{y \in F_{3^n}} \omega^{h(y)} \\ &= (\epsilon_g + \epsilon_h) 3^{\frac{n}{2}}. \end{aligned}$$

Thus, we obtain $|C_d(\tau)| = |-1 + C(a)| \leq 3^{\frac{n}{2}} + 1$.

Case 2) Rank of $g(y) = n-1$ and rank of $h(y) = n$;
From Lemma 5, we have

$$\begin{aligned} 2C(a) &= \sum_{y \in F_{3^n}} \omega^{g(y)} + \sum_{y \in F_{3^n}} \omega^{h(y)} \\ &= (\sqrt{3}i\epsilon_g + \epsilon_h)3^{\frac{n}{2}}. \end{aligned}$$

In this case, we have $|C_d(\tau)| = |-1 + C(a)| \leq 3^{\frac{n}{2}} + 1$.

Case 3) Rank of $g(y) = n-2$ and rank of $h(y) = n$;
From Lemma 5, we have

$$\begin{aligned} 2C(a) &= \sum_{y \in F_{3^n}} \omega^{g(y)} + \sum_{y \in F_{3^n}} \omega^{h(y)} \\ &= (3\epsilon_g + \epsilon_h)3^{\frac{n}{2}}. \end{aligned}$$

We also have $|C_d(\tau)| = |-1 + C(a)| \leq 2 \cdot 3^{\frac{n}{2}} + 1$.

Hence the magnitude of $C_d(\tau)$ is upper bounded by $2 \cdot 3^{\frac{n}{2}} + 1$.

□

ACKNOWLEDGMENT

This work was supported by the IT R&D program of MKE/KEIT. [2008-F-007-02, Intelligent Wireless Communication Systems in 3 Dimensional Environment]

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,"*Discrete Math.*, vol. 16, pp. 209–232, 1976.

[3] 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.

[4] 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.

[5] 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.

[6] Z. Hu, X. Li, D. Mills, E. Muller, 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.

[7] Eun-Young Seo, Young-Sik Kim, Jong-Seon No, and Dong-Joon 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 Transactions on Information Theory*, vol. 54, no. 7, pp. 3140-3149, Jul. 2008.

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