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, Tae-Hyung Lim, Jong-Seon No,[1]
and Habong Chung[2]

[1]Department of EECS, INMC, Seoul National University, Seoul, Korea
[2]Department of EEE, Hongik University, Seoul, Korea

February 19, 2010

Outline

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 sequence $s(dt)$ is low.
- The values d with gcd$(d, p^n - 1) = 1$ have been studied by Trachtenberg, Helleseth, and etc..
- When the decimation value d is not relatively prime to the period $p^n - 1$, several research have been conducted.

$\Rightarrow$ For a ternary case, Ness, Helleseth, and Kholosha derived the correlation distributions for $d = \frac{3^k+1}{2}$ and $\gcd(k, n) = 1$, which is Coulter-Matthews decimation.

Introduction

⇒ For a tenary case, Muller showed that the magnitude of correlation values is upper bounded by $2\sqrt{3^n}+1$ for $d=\frac{3^n+1}{4}+\frac{3^n-1}{2}$. 0.2cm

⇒ Hu, et al. extended Muller's result to any odd prime case, i.e., for $d=(p^n+1)/(p+1)+(p^n-1)/2$ and derived the upper bound as $(p+1)/2\sqrt{p^n}$.

⇒ Seo, Kim, No, and Shin derived the correlation distributions for $d=\frac{(p^{2k}+1)^2}{4}$, when p is an odd prime and $n=4k$.

- We will show that the magnitude of cross-correlation function $C_l(\tau)$ between $s(t)$ and $s(dt+l)$ is upper bounded by $2\sqrt{3^n}+1$ for the new decimation value $d=(3^{n/2}+1)^2/8$.

Preliminaries

- **Trace functions**

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

$$\mathrm{tr}_k^n(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{p^{ki}} = x + x^{p^k} + x^{p^{2k}} + \cdots + x^{p^{(\frac{n}{k}-1)k}}$$

  where $x \in F_{p^n}$ and $k|n$.

- **m-sequence**

  Let α be a primitive element of F_{p^n}. Then a p-ary m-sequence $s(t)$ with the period of $p^n - 1$ can be expressed as

$$s(t) = \mathrm{tr}_1^n(\alpha^t) \ (0 \le t \le p^n - 2).$$

Preliminaries

- **Notations**
  - $n = 2m$, 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 third root of unity.

- **Cross-correlation**

  The cross-correlation function between two p-ary sequences $a(t)$ and $b(t)$ at shift τ is defined as

$$C(\tau) = \sum_{t=0}^{p^n-2} \omega_p^{a(t+\tau)-b(t)}$$

  where ω_p is the p-th root of unity.

Known Results on Quadratic Forms

- **Quadratic form**

  A quadratic form over $\mathbb{F}_q$ is a homogeneous polynomial in $\mathbb{F}_q[x_1, \cdots, x_n]$ of degree 2 and can be expressed as

$$f[x_1, x_2, \cdots, x_n] = \sum_{i,j \leq n} a_{ij} x_i x_j$$

  where $a_{ij} \in \mathbb{F}_q$.

$\Rightarrow$ The correlation properties of several well known sequence families are most easily extablished using the theory of quadratic forms.

- **How to decide the number of solutions**

  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 $f(x)$.

Known Results on Quadratic Forms

Lemma

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 rank$(f) = n -$ dim(Y).

Corollary

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 $f(y+z) = f(y)$ for all $y \in F_{p^n}$.

Known Results on Quadratic Forms

Lemma

(The number of solutions to a quadratic form)

Let f be a nondegenerate quadratic form over $\mathbb{F}_q$, q odd, in n of indeterminates. Then for $c \in \mathbb{F}_q$ the number of solutions $N(c)$ of the equation $f(x_1, \cdots, x_t) = c$ in $\mathbb{F}_q^t$ is

Case 1) n *even;*

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

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

Case 2) n *odd;*

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

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

Known Results on Quadratic Forms

- **Quadratic Character**

  Define the quadratic character of F_{p^n} as

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

- **Remark**

  For any $b \in \mathbb{F}_q$ the number of solutions of a quadratic form, $a_1 x_1^2 + \cdots + a_k x_k^2 = b$, in $\mathbb{F}_q^n$ is q^{n-k} times the number of solutions of the same equations in $\mathbb{F}_q^k$.

Quadratic Expression for Cross-Correlation Function

- The cross-correlation function of $s(t)$ and its decimated sequence $s(dt+l)$ at shift τ is expressed as

$$\begin{aligned} C_l(\tau) &= \sum_{t=0}^{3^n-2} \omega^{s(t+\tau)-s(dt+l)} \\ &= \sum_{t=0}^{3^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{t+\tau}-\alpha^{dt+l})} \\ &= \sum_{x\in F_{3^n}^*} \omega^{\mathrm{tr}_1^n(ax-bx^d)} \end{aligned}$$

where $a=\alpha^\tau$, and $b=\alpha^l$ with $0\leq l<\frac{p^m+1}{2}$.

$\Rightarrow$ How to express $\mathrm{tr}_1^n(ax-bx^d)$ into a quadratic form?

Quadratic Expression for Cross-Correlation Function

- The cross-correlation function of $s(t)$ and its decimated sequence $s(dt+l)$ at shift τ is expressed as

$$
\begin{aligned}
C_l(\tau) &= \sum_{t=0}^{3^n-2} \omega^{s(t+\tau)-s(dt+l)} \\
&= \sum_{t=0}^{3^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{t+\tau}-\alpha^{dt+l})} \\
&= \sum_{x\in F_{3^n}^*} \omega^{\mathrm{tr}_1^n(ax-bx^d)}
\end{aligned}
$$

where $a=\alpha^\tau$, and $b=\alpha^l$ with $0\le l<\frac{p^m+1}{2}$.

$\Rightarrow$ How to express $\mathrm{tr}_1^n(ax-bx^d)$ into a quadratic form?

Quadratic Expression for Cross-Correlation Function

- Let's focus on the function, $C(a,b)$, defined by

$$C(a,b) = \sum_{x \in F_{3^n}} \omega^{\mathrm{tr}_1^n(ax - bx^d)} = C_l(\tau) + 1. \quad (1)$$

- **Square and Nonsquare**
  - Square: α^{2i} in F_{p^n}
  - Nonsquare: α^{2i+1} in F_{p^n}

- 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 $F_{3^n}^*$. Hence (1) is expressed as

$$\begin{aligned} 2C(a,b) &= \sum_{y \in F_{3^n}} \omega^{\mathrm{tr}_1^n(ay^{3^{m+1}+1} - by^{d(3^{m+1}+1)})} \\ &+ \sum_{y \in F_{3^n}} \omega^{\mathrm{tr}_1^n(ary^{3^{m+1}+1} - br^d y^{d(3^{m+1}+1)})} \end{aligned} \quad (2)$$

Quadratic Expression for Cross-Correlation Function

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

$$
\begin{aligned}
2C(a,b) &= \sum_{y\in F_{3^n}} \omega^{\mathrm{tr}_1^n(ay^{3^{m+1}+1} - by^{3^m+1})} \\
&\quad + \sum_{y\in F_{3^n}} \omega^{\mathrm{tr}_1^n(ary^{3^{m+1}+1} - br^d y^{3^m+1})} \\
&= \sum_{y\in F_{3^n}} \omega^{g(y)} + \sum_{y\in F_{3^n}} \omega^{h(y)}
\end{aligned}
$$

where

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

Quadratic Expression for Cross-Correlation Function

- 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

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

where $a_{ij} = \mathrm{tr}_1^n \Big(a(\alpha_i^{3^{m+1}} \alpha_j) - b(\alpha_i^{3^m} \alpha_j) \Big)$.

Find the Rank of the Quadratic Forms

- In order to derive the values of the exponential sum $C(a,b)$, 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

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

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

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

$$(ar)^{3^{m+1}} z^{3^2} - ((br^d)^3 + (br^d)^{3^{m+1}}) z^3 + arz = 0 \quad (4)$$

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

Proof of the Lemma

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

$$\mathrm{tr}_1^n(a(y+z)^{3^{m+1}+1}-b(y+z)^{3^m+1})=\mathrm{tr}_1^n(ay^{3^{m+1}+1}-by^{3^m+1}). \quad (5)$$

Then (5) can be rewritten as

$$\mathrm{tr}_1^n(y^{3^{m+1}}(a^{3^{m+1}}z^{3^2}-(b^3+b^{3^{m+1}})z^3+az)+az^{3^{m+1}}-bz^{3^m+1})=0. \quad (6)$$

The equation (6) holds for all $y \in F_{3^n}$ if and only if

$$a^{3^{m+1}}z^{3^2}-(b^3+b^{3^{m+1}})z^3+az = 0 \quad (7)$$

$$\mathrm{tr}_1^n(az^{3^{m+1}}-bz^{3^m+1}) = 0 \quad (8)$$

are satisfied simultaneously. Hence the number of solutions $z \in F_{3^n}$ satisfying (5) can be determined by finding the number of solutions $z \in F_{3^n}$ satisfying (7) and (8).

Proof of the Lemma (Cont'd)

Now, we will show that all solutions $z \in F_{p^n}$ satisfying (7) also satisfy (8). From (7) we have

$$(b^3 + b^{3^{m+1}})z^3 = a^{3^{m+1}} z^{3^2} + az$$

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

$$(b^{3^i} + b^{3^{m+i}})z^{3^i} = a^{3^{m+i}} z^{3^{i+1}} + a^{3^{i-1}} z^{3^{i-1}}. \quad (9)$$

Using (9), (8) can be rewritten as

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

Proof of the Lemma (Cont'd)

$$
\begin{aligned}
&= \sum_{i=1}^{n} a^{3^i}(z^{3^{m+i+1}+3^i}) - \sum_{i=1}^{n} b^{3^i}(z^{3^{m+i}+3^i}) \\
&= \sum_{i=1}^{n} a^{3^i}(z^{3^{m+i+1}+3^i}) - \frac{1}{2}\sum_{i=1}^{n}(b^{3^i} + b^{3^{m+i}})(z^{3^{m+i}+3^i}) \\
&= \sum_{i=1}^{n} a^{3^i}(z^{3^{m+i+1}+3^i}) - \frac{1}{2}\Big(\sum_{j=1}^{n} a^{3^j}(z^{3^{m+j+1}+3^j}) + \sum_{k=1}^{n} a^{3^k}(z^{3^{m+k+1}+3^k})\Big) \\
&= 0
\end{aligned}
$$

where $j = m + i$, $k = i - 1$.
Hence we only need to calculate the number of solutions for (7) to determine the number of solutions for (6). □

Find the Rank of the Quadratic Forms

- From the Lemma, to find the rank of $g(y)$ and $h(y)$, we have to find out the number of solutions $z \in F_{3^n}$ of

$$\begin{cases} a^{3^{m+1}} z^{3^2} - (b^3 + b^{3^{m+1}}) z^3 + az = 0 \Rightarrow \text{Rank of } g(y) \\ (ar)^{3^{m+1}} z^{3^2} - ((br^d)^3 + (br^d)^{3^{m+1}}) z^3 + arz = 0 \Rightarrow \text{Rank of } h(y) \end{cases}$$

where $a = \alpha^\tau$, $b = \alpha^l$, and r is a nonsquare in $F^*_{3^n}$.

Lemma

The equation

$$(ar)^{3^{m+1}} z^9 - (r^{3d} + r^{d3^{m+1}}) z^3 + arz = 0 \qquad (10)$$

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

Proof of the Lemma

Proof:
First, we will show that

$$r^{3d} + r^{d3^{m+1}} = 0 \tag{11}$$

for any nonsquare r in F_{3^n}. The equation (11) can be rewritten as

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

Thus, we have

$$r^{3d(3^m-1)} = -1. \tag{12}$$

Since we have

$$3d(3^m - 1) = \frac{3(3^m + 1)(3^{2m} - 1)}{8},$$

and $3^m + 1 \equiv 4 \mod 8$, any nonsquare r satisfies (12).

Proof of the Lemma (Cont'd)

From $r^{3d} + r^{d3^{m+1}} = 0$, (10) can be rewritten as

$$a^{3^{m+1}-1} r^{3^{m+1}} z^8 = -1. \tag{13}$$

It is clear that the left hand side of (13) is a nonsquare while the right hand side of (13) is a square. Thus we have no nonzero solutions for (13). Therefore the only solution satisfying (10) is $z = 0$. □

Linearized Polynomials

- **Definition**

  A polynomial of the form

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

  with coefficients field in an extention field $\mathbb{F}_q^m$ of $\mathbb{F}_q$ is called a q-polymomial or linearized polynomial.

- If F is an arbitrary extension field of $\mathbb{F}_q^m$ and $L(x)$ is a linearized polynomial (i.e., a q-polynomial) over $\mathbb{F}_q^m$, then

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

  Hence the set of solutions in F is considered as a vector subspace over $\mathbb{F}_q$, i.e., the number of solution is the equation is a power of q.

The Rank of the Quadratic Form when $l = 0$

Corollary

When $l = 0$, i.e., the case that cross-correlation between $s(t)$ and $s(dt)$, the possible rank pairs of $g(y)$ and $h(y)$ are as the followings

$$\Psi(g(y), h(y)) = \begin{cases} (n, n), & \text{if } g(y+z) = g(y) \text{ has one solution} \\ (n-1, n), & \text{if } g(y+z) = g(y) \text{ has three solutions} \\ (n-2, n), & \text{if } g(y+z) = g(y) \text{ has nine solutions} \end{cases}$$

where $\Psi(f, g) = (r_f, r_f)$ and r_f, r_g denote the rank of f and g, respectively.

Find the Rank of the Quadratic Forms

Lemma

If $y^{3^m} - y$ is an element in F_{3^m} and $n = 2m$, where y is an element in F_{3^n}, then y should be an element in F_{3^m}.

Proof:
If

$$y^{3^m} - y \in F_{3^m}, y \in F_{3^n},$$

then we have

$$(y^{3^m} - y)^{3^m} = y^{3^m} - y.$$

Since $(y^{3^m} - y)^{3^m} = y^{3^{2m}} - y^{3^m} = y - y^{3^m}$, we have

$$y^{3^m} - y = 0,$$

which indicates y is an element of F_{3^m}. □

Find the Rank of the Quadratic Forms

Lemma

Suppose that $n = 2m = 4k + 2$, where k is an iteger. Let

$$f_A(y) = (Ay)^3 + \frac{1}{y}.$$

If A is a nonsquare in F_{3^m} and y is a nonsquare in F_{3^n} then $f_A(y)$ is not an element in F_{3^m}.

Proof:
Suppose that

$$f_A(y) \in F_{3^m},$$

then we have

$$\left(A^3y^3 + \frac{1}{y}\right)^{3^m} - \left(A^3y^3 + \frac{1}{y}\right) = 0. \quad (14)$$

Proof of the Lemma (Cont'd)

The lefthand side of (14) can be expressed as

$$(A^{3^m})^3(y^{3^m})^3 + \frac{1}{y^{3^m}} - A^3y^3 - \frac{1}{y}$$
$$= A^3(y^{3^m})^3 + \frac{1}{y^{3^m}} - A^3y^3 - \frac{1}{y}. \tag{15}$$

From (15), we can rewrite (14) as

$$A^3y^3\left(y^{3^m-1} - 1\right)^3 = \frac{y^{3^m-1} - 1}{y^{3^m}}. \tag{16}$$

Note that $y^{3^m-1} - 1 \neq 0$, i.e., y is not an element F_{3^m}, becuase y is a nonsquare in F_{3^n}. (If $y \in F_{3^m}$, then $y = \alpha^{(3^m+1)k}$ where α is a primitive element in F_{3^n}, $0 \leq k \leq 3^m - 2$. Thus, y must be a square in F_{3^n}. This is a contradiction.) Thus, (16) can be rewritten as

$$A^3y^3\left(y^{3^m-1} - 1\right)^2 = \frac{1}{y^{3^m}}. \tag{17}$$

Proof of the Lemma (Cont'd)

From (17), we have

$$\left(A^3 y^{3^m+1}\right)^{\frac{1}{2}} = \frac{1}{y^{3^m} - y}. \qquad (18)$$

Note that A^3 is expressed as $\alpha^{(3^m+1)k_1}$, where k_1 is an odd integer, becuase A is a nonsquare in F_{3^m} so is A^3. Similarly, y^{3^m+1} can be expressed as $\alpha^{(3^m+1)k_2}$, where k_2 is an odd integer, becuase y is a nonsquare in F_{3^n}. Hence, we have

$$A^3 y^{3^m+1} = \alpha^{(3^m+1)(k_1+k_2)} = \alpha^{(3^m+1)k'}$$

where k' is an even integer. Thus, the lefthand side of (18) can be rewritten as

$$\left(A^3 y^{3^m+1}\right)^{\frac{1}{2}} = \alpha^{(3^m+1)k} \qquad (19)$$

where $k = \frac{k'}{2}$. The equation (19) indicates that the lefthand side of (18) is an element in F_{3^m}

Proof of the Lemma (Cont'd)

From the equality of (18), we have

$$\frac{1}{y^{3^m} - y} \in F_{3^m}. \tag{20}$$

From (20), we have

$$y^{3^m} - y \in F_{3^m}. \tag{21}$$

From Lemma 7, (21) indicates

$$y \in F_{3^m}.$$

However, this is a contradiction to our assupmtion because y is a nonsqaure in F_{3^n}. Therfore, we can conclude that

$$f_A(y) \notin F_{3^m}.$$

□

Find the Rank of the Quadratic Forms

Theorem

The equation

$$a^{3^{m+1}}z^9-(b^3+b^{3^{m+1}})z^3+az=0$$

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

Proof: In order to prove the theorem, we have to show that

$$a^{3^{m+1}}z^8-(b^3+b^{3^{m+1}})z^2+a=0 \tag{22}$$

has no solution in $F_{3^n}^*$ when a is a nonsquare in $F_{3^n}^*$.
We can rewrite (22) as

$$a^{3^{m+1}}z^6+az^{-2}=b^3+b^{3^{m+1}}. \tag{23}$$

Proof of the Theorem (cont'd)

The right hand side of (23) is expressed as $tr_m^n(b^3)$, which is an element in F_{3^m}. Thus, if we can show that

$$\left\{z|a^{3^{m+1}}z^6 + az^{-2} \in F_{3^m}, z \in F_{3^n}^*, a \text{ is a nonsquare in } F_{3^n}\right\} = \phi, \tag{24}$$

then the proof of the theorem will be completed.
To prove the above statement, we suppose that there is z such that

$$a^{3^{m+1}}z^6 + az^{-2} \in F_{3^m}$$

where $z \in F_{3^n}^*$ and a is a nonsquare in F_{3^n}. Then we have

$$\left(a^{3^m+1}\right)^3 \left(\frac{z^2}{a}\right)^3 + \left(\frac{a}{z^2}\right) \in F_{3^m}. \tag{25}$$

Proof of the Theorem (cont'd)

If we set a^{3^m+1} as A and $\frac{z^2}{a}$ as y, then (25) can be rewritten as

$$A^3y^3 + \frac{1}{y} \in F_{3^m}$$

where A is a nonsquare in F_{3^m} and y is a nonsquare in F_{3^n}. However, this is a contradiction to Lemma 8. Therefore, we have completed the proof. □

- **Remark**

  When $l \neq 0$, the equations to decide the rank of $g(y)$ and $h(y)$ has the form of the above theorem by turns. Therefore we know that at least one of the equations has one solution according to the theorem.

The Rank of the Quadratic Form when $l \neq 0$

Corollary

The possible rank combination of $g(y)$ and $h(y)$ are as follows:
Case 1) $a = \alpha^\tau$ *is a square in* $F_{3^n}^*$

$$\Psi(g(y), h(y)) = \begin{cases} (n, n), & \text{if } g(y+z) = g(y) \text{ has one solution} \\ (n-1, n), & \text{if } g(y+z) = g(y) \text{ has three solutions} \\ (n-2, n), & \text{if } g(y+z) = g(y) \text{ has nine solutions.} \end{cases}$$

Case 2) $a = \alpha^\tau$ *is a nonsquare in* $F_{3^n}^*$

$$\Psi(g(y), h(y)) = \begin{cases} (n, n), & \text{if } h(y+z) = h(y) \text{ has one solution} \\ (n, n-1), & \text{if } h(y+z) = h(y) \text{ has three solutions} \\ (n, n-2), & \text{if } h(y+z) = h(y) \text{ has nine solutions.} \end{cases}$$

where $\Psi(f, g) = (r_f, r_f)$ *and* r_f, r_g *denote the rank of* f *and* g, *respectively.*

Upper Bound on Cross-Correlation Values

- Define the quadratic character of F_{p^n} as

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

Lemma

Let η be the quadratic residue 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.

Upper Bound on Cross-Correlation Values

Theorem

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

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

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

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

where
$g(y) = \mathrm{tr}_1^n(ay^{3^{m+1}+1} - by^{3^m+1})$ and $h(y) = \mathrm{tr}_1^n(ary^{3^{m+1}+1} - br^d y^{3^m+1})$ have both quadratic forms and r is a nonsquare in F_{3^n}.

Proof of the Theorem (cont'd)

Let ϵ_g and ϵ_h be the values defined in Lemma 11 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 4 that the possible rank combinations of the quadratic forms of $g(y)$ and $h(y)$ are (n, n), $(n-1, n)$, and $(n-2, n)$ or vice versa. Hence the following three cases should be considered to determine the value of $C(a, b)$.

Case 1) The rank pair of $g(y)$ and $h(y)$ is (n, n);
From Lemma 11, we have

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

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

Proof of the Theorem (cont'd)

Case 2) The rank pair of $g(y)$ and $h(y)$ is $(n, n-1)$, or vice versa;
From Lemma 11, we have

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

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

Case 3) The rank pair of $g(y)$ and $h(y)$ is $(n, n-2)$, or vice versa.;
From Lemma 11, we have

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

We also have $|C_l(\tau)| = |-1 + C(a,b)| \leq 2 \cdot 3^{\frac{n}{2}} + 1$.
Hence the magnitude of $C_l(\tau)$ is upper bounded by $2 \cdot 3^{\frac{n}{2}} + 1$.

□

Conclusion

- We investigate into the cross-correlation of a ternary m-sequence $m(t)$ of period $3^n - 1$ and its decimated sequence $m(dt + l)$, $0 \leq l \leq \frac{(p^m+1)}{2}$, 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 $2\sqrt{3^n} + 1$.
- Furtherwork: Construct new sequence family from the sequences.