On the Cross-Correlation of a $p$-Ary $m$-Sequence and Its Decimated Sequences by $d = \frac{p^n+1}{p^k+1} + \frac{p^n-1}{2}$

Sung-Tai CHOI(a), Ji-Youp KIM(b), Nonmembers, and Jong-Seon NO(c), Member

SUMMARY In this paper, for an odd prime $p$ such that $p = 3 \mod 4$, odd $n$, and $d = (p^n + 1)/(p^k + 1) + (p^n - 1)/2$ with $k\eta$, the value distribution of the exponential sum $S(a, b)$ is calculated as $a$ and $b$ run through $\mathbb{F}_{p^\eta}$. The sequence family $G$ in which each sequence has the period of $N = p^n - 1$ is also constructed. The family size of $G$ is $p^\eta$ and the correlation magnitude is roughly upper bounded by $(p^k + 1)\sqrt{N}/2$. The weight distribution of the relevant cyclic code $C$ over $\mathbb{F}_p$ with the length $N$ and the dimension $\dim_{\mathbb{F}_p}C = 2n$ is also derived.

key words: cross-correlation, cyclic code, decimated sequence, exponential sum, $m$-sequence, sequence family, quadratic form, weight distribution

1. Introduction

Maximal length sequences ($m$-sequences) are used in synchronization for various communication systems and in code division multiple access (CDMA) systems as user spreading codes since they have ideal autocorrelation properties. First, when the magnitude of $S(a, b)$ for $a$ and $b$ run through $\mathbb{F}_{p^\eta}$ is small enough, then the value distribution of $S(a, b)$ is likely to be derived. However, its value distribution is hard to derive due to some technical problems, the upper bound on the magnitudes of $S(a, b)$ is still meaningful for the construction of sequence families with low correlation property. The general methodology to drive the value distribution of $S(a, b)$ is formulated in [19].

Not much is known about the weight distributions of cyclic codes except for very specific cases. Of particular interest, for the alphabet size of an odd prime $p$, the value distribution of $S(a, b)$ and the weight distribution of the corresponding cyclic code were derived for $d_1 = 1$ and $d_2 = (p^k + 1)/2$ in [14]. In [15], the same work is done for $d_1 = 2$ and $d_2 = p^k + 1$. Recently, the value distribution of $S(a, b)$ for $d_1 = 1$, $d_2 = (p^k + 1)/(p^k + 1) + (p^k - 1)/2$, odd prime $p$ such that $p \equiv 3 \mod 4$, and odd $n$ is derived in [3].

In this paper, the value distribution of $S(a, b)$ is calculated for $d_1 = 1$ and $d_2 = (p^k + 1)/(p^k + 1) + (p^k - 1)/2$ with $k\eta$, an odd prime $p$ such that $p \equiv 3 \mod 4$, and odd $n$. Using the result, the maximum magnitude of cross-correlation values of the sequence family $G$ and the weight distribution of the cyclic code $C$ are derived, respectively. Our result includes the result in [3] as a special case.

This paper is organized as follows. In Sect. 2, preliminaries are stated. In Sect. 3, the value distribution of $S(a, b)$ is derived. In Sect. 4, the upper bound of cross-correlation magnitude of the sequence family $G$ is calculated. In Sect. 5, the weight distribution of the cyclic code $C$ is obtained. The conclusion is given in Sect. 6.

2. Preliminaries

2.1 Exponential Sum $S(a, b)$ and the Hamming Weight of the Code $C$

Let $p$ be a prime and $\mathbb{F}_{p^\eta}$ the finite field with $p^n$ elements. Then the trace function $tr_p^\eta()$ from $\mathbb{F}_{p^\eta}$ to $\mathbb{F}_p$ is defined as

$$tr_p^\eta(x) = \sum_{i=0}^{\frac{\eta-1}{\gcd(\eta, n)}} x^{p^i}$$

where $x \in \mathbb{F}_{p^\eta}$ and $k\eta$. Let $a$ be a primitive element of $\mathbb{F}_{p^\eta}$ and $\mathbb{F}_{p^\eta}^\times = \mathbb{F}_{p^\eta} \setminus \{0\}$. 

Copyright © 2013 The Institute of Electronics, Information and Communication Engineers
We will consider
\[ S(a, b) = \sum_{x \in \mathbb{F}_{p^r}} \chi(ax + bx^d), \]  
which is the case when \( d_1 = 1 \) and \( d_2 = d \) in (1).

Let \( C \) be the cyclic code over \( \mathbb{F}_p \) with the length \( N = p^n - 1 \) consisting of the codewords of the form
\[ c(a, b) = (c_0, c_1, \ldots, c_{N-1}), \quad a, b \in \mathbb{F}_p, \]
where \( c_i = \text{tr}^n_i(aa^i + ba^{di}), 0 \leq i \leq N - 1 \). The Hamming weight of the codeword \( c(a, b) \) is defined as
\[ H_w(c(a, b)) = |\{i|0 \leq i \leq N - 1, c_i \neq 0\}|. \]

2.2 Quadratic Form

We define a quadratic form in \( e \) variables over \( \mathbb{F}_{p^r} \) as a homogeneous polynomial in \( \mathbb{F}_{p^r}[x_1, \ldots, x_e] \)
\[ f(x) = f(x_1, \ldots, x_e) = \sum_{i=1}^e a_{ij} x_i x_j \]
where \( p \) is an odd prime and \( a_{ij} = a_{ji} \in \mathbb{F}_{p^r} \). We then associate \( f \) with an \( e \times e \) symmetric matrix \( A \) whose \((i, j)\) entry is \( a_{ij} \). The matrix \( A \) is called the coefficient matrix of \( f \) and \( r \) denotes the rank of \( A \). Then there exists a nonsingular \( e \times e \) matrix \( B \) over \( \mathbb{F}_{p^r} \) such that \( H = BAB^{-T} \) is a diagonal matrix, that is, \( H = \text{diag}(h_1, \ldots, h_r, 0, \ldots, 0) \), where \( h_i \in \mathbb{F}_{p^r} \). Let \( \Delta = h_1 \cdots h_r \), which will be used in Lemma 3.

A quadratic form \( f(x) \) in \( e \) variables over \( \mathbb{F}_{p^r} \) can be regarded as a mapping \( f(x) \) from \( \mathbb{F}_{p^r}^e \) to \( \mathbb{F}_{p^s} \), when \( x_i \in \mathbb{F}_{p^r} \). Thus, we will also use the term ‘quadratic form’ for this mapping \( f(x) \) in \( \mathbb{F}_{p^r}^e \).

If \( f \) is a quadratic form over \( \mathbb{F}_{p^r} \) and \( b \in \mathbb{F}_{p^r} \), then an explicit formula for the number of solutions of the equation \( f(x_1, \ldots, x_e) = b \) in \( (\mathbb{F}_{p^r})^e \approx \mathbb{F}_{p^{re}} \) can be given. Hence the ‘quadratic form’ can be exploited to evaluate \( S(a, b) \) if the \( S(a, b) \) is represented as a quadratic form. In the remainder of this section, some useful lemmas on a quadratic form are listed as follows.

**Lemma 1:** Consider the function given by
\[ \text{tr}_l^n \left( \sum_j a_j x^{p^r j + 1} \right) = \text{tr}_l^n(f(x)) \]
where \( i \geq 0 \) are integers, \( a_i \in \mathbb{F}_{p^r} \), and \( k|n \). Then
\[ f(x) = tr_l^n \left( \sum_j a_j x^{p^r j + 1} \right) \]
is a quadratic form in \( n/k \) variables over \( \mathbb{F}_{p^k} \).

**Proof:** Any \( x \in \mathbb{F}_{p^r} \) is represented as
\[ x = x_1 a_1 + x_2 a_2 + \cdots x_e a_e, \quad x_i \in \mathbb{F}_{p^r} \]
where \( e = n/k \) and \((a_1, a_2, \ldots, a_e) \) is a basis of \( \mathbb{F}_{p^r} \) over \( \mathbb{F}_{p^l} \).

Substituting (4) into (3), we have
\[ f(x) = \text{tr}_l^n \left( \sum_j a_j \left( \sum_{i=1}^e x_i a_j^{p^r i} \right) \right) = \sum_{j=1}^e \sum_{i=1}^e x_i a_j^{p^r i} a_j^{p^r i}, \]
which is a quadratic form with \( e \) variables over \( \mathbb{F}_{p^k} \).

**Lemma 2** (Luo and Feng [14]): The rank \( r \) of the quadratic form \( f(x) \) from \( \mathbb{F}_{p^r} \) to \( \mathbb{F}_{p^s} \) determined from the number of elements that the form \( f(x) \) is independent of, i.e., \((p^r)^{r-}\) is the number of \( x \in \mathbb{F}_{p^r} \) such that \( f(x + y) - f(x) - f(y) = 0 \) for all \( y \in \mathbb{F}_{p^s} \).

**Lemma 3** (Luo and Feng [14]): Let \( f(x) \) be a mapping from \( \mathbb{F}_{p^r} \) to \( \mathbb{F}_{p^s} \) corresponding to the quadratic form \( f(x) \in \mathbb{F}_{p^r}[x_1, x_2, \ldots, x_e] \) with rank \( r \). Assume that the quadratic form has the diagonal matrix \( H = \text{diag}(h_1, \ldots, h_r, 0, \ldots, 0) \) where \( h_i \in \mathbb{F}_{p^r} \). Then we have
\[ \sum_{x \in \mathbb{F}_{p^r}} \omega^{p^r \text{tr}_l^n(f(x))} = \begin{cases} p^s \text{tr}_l^n(H), & \text{if } p^s \equiv 1 \mod 4 \\ \text{tr}_l^n(H)^{p^s - 2}, & \text{if } p^s \equiv 3 \mod 4 \end{cases} \]
where \( j = \sqrt{-1}, \Delta = h_1 h_2 \cdots h_r \), and \( \eta(A) \) is the quadratic character of \( \mathbb{F}_{p^r}^* \) defined as
\[ \eta(x) = \begin{cases} 1, & \text{if } x \text{ is a square in } \mathbb{F}_{p^r}^* \\ -1, & \text{if } x \text{ is a nonsquare in } \mathbb{F}_{p^r}^* \end{cases} \]
and \( \psi \) and \( \xi \) are defined as
\[ \psi = \begin{cases} (-1)^{k-1} \tau, & \text{if } p \equiv 1 \mod 4 \\ (-1)^{k+1} \tau, & \text{if } p \equiv 3 \mod 4 \text{ and } k \text{ is even} \end{cases} \]
and \( \xi = (-1)^{\frac{k-1}{2}} \).

2.3 Linearized Polynomial

Let \( q \) be a power of prime. A polynomial of the form
\[ \phi(x) = \sum_j a_j x^j \]
where \( a_j \in \mathbb{F}_{p^r} \), is called a linearized polynomial over \( \mathbb{F}_{p^r} \).

If \( F \) is an arbitrary extension field of \( \mathbb{F}_{p^r} \) which includes the roots of \( \phi(x) \), then
\[ \phi(\beta + \gamma) = \phi(\beta) + \phi(\gamma), \quad \text{for all } \beta, \gamma \in F \]
\[ \phi(c \beta) = c \phi(\beta), \quad \text{for all } \beta \in F \text{ and } c \in \mathbb{F}_q. \]

Hence the set of solutions of \( \phi(x) = 0 \) in \( F \) forms a vector subspace over \( \mathbb{F}_q \), i.e., the number of solutions in \( F \) of \( \phi(x) = 0 \) is equal to a power of \( q \).
2.4 Weil’s Bound

The following lemma provides the upper bound on the magnitudes of the exponential sums, which is known as Weil’s bound.

Lemma 4 (Theorem 5.38 [17]): Let \( f(x) \in \mathbb{F}_p[x] \) be a polynomial of degree \( l \geq 1 \) with \( \gcd(l, p^g) = 1 \) and let \( \chi \) be a nontrivial additive character of \( \mathbb{F}_{p^g} \). Then, we have

\[
\left| \sum_{x \in \mathbb{F}_{p^g}} \chi(f(x)) \right| \leq (l - 1)p^{\frac{g}{2}}.
\]

\( \square \)

3. Value Distribution of \( S(a, b) \)

3.1 Evaluation of \( S(a, b) \)

In this paper, the value distribution of \( S(a, b) \) in (2) will be calculated as \( a \) and \( b \) run through \( \mathbb{F}_{p^g} \) for the following parameters:

- \( p \) is an odd prime such that \( p \equiv 3 \mod 4 \);
- \( n \) is an odd integer;
- \( d = (p^n + 1)/(p^k + 1) + (p^n - 1)/2 \) with \( kn \).

When either \( a \) or \( b \) is equal to zero, \( S(a, b) \) is determined as in the following lemma.

Lemma 5: When either \( a \) or \( b \) is equal to zero, \( S(a, b) \) is determined as

\[
S(a, b) = \begin{cases} 
  p^g, & \text{when } a = b = 0 \\
  0, & \text{when } a \neq 0 \text{ and } b = 0 \\
  \pm j p^{\frac{g}{2}}, & \text{when } a = 0 \text{ and } b \neq 0.
\end{cases}
\]

Proof: The case of \( b = 0 \) is easily proved. We need to prove the case when \( a = 0 \) and \( b \neq 0 \). Since \( \gcd(d, p^n - 1) = 2 \), we have

\[
S(0, b) = \sum_{x \in \mathbb{F}_{p^n}} \chi(bx^d) = \sum_{x \in \mathbb{F}_{p^n}} \chi(bx^2), \quad b \in \mathbb{F}_{p^n}.
\]

Note that \( \text{tr}_n^1(bx^2) \) is a quadratic form in \( n \) variables over \( \mathbb{F}_p \). From Lemma 2, it is straightforward that the quadratic form \( \text{tr}_n^1(bx^2) \) always has rank \( n \). Hence, from Lemma 3, we have \( S(0, b) = \pm j p^{\frac{g}{2}} \).

Next, we will calculate \( S(a, b) \) for \( a, b \in \mathbb{F}_{p^n} \). Note that \( \gcd(p^k + 1, p^n - 1) = 2, d(p^k + 1) \equiv 2 \mod (p^n - 1) \), and \( -1 \) is a nonsquare in \( \mathbb{F}_{p^g} \). Replacing \( x \) by \( x^{p^g + 1} \) for squares in \( \mathbb{F}_{p^g} \) and \( -x^{p^g + 1} \) for nonsquares in \( \mathbb{F}_{p^g} \), \( S(a, b) \) is expressed in terms of quadratic forms as

\[
S(a, b) = \sum_{x \in \mathbb{F}_{p^n}} \chi(ax + bx^d)
\]

\[
= \frac{1}{2} \left( \sum_{x \in \mathbb{F}_{p^n}} \chi(ax^{p^g + 1} + bx^2) + \sum_{x \in \mathbb{F}_{p^n}} \chi(-ax^{p^g + 1} + bx^2) \right)
\]

where

\[
S_1(a, b) = \sum_{x \in \mathbb{F}_{p^n}} \chi(ax^{p^g + 1} + bx^2)
\]

and

\[
S_2(a, b) = \sum_{x \in \mathbb{F}_{p^n}} \chi(-ax^{p^g + 1} + bx^2).
\]

From Lemma 1, both

\[
Q_1(x) = \text{tr}_n^1(ax^{p^g + 1} + bx^2)
\]

and

\[
Q_2(x) = \text{tr}_n^1(-ax^{p^g + 1} + bx^2)
\]

are quadratic forms in \( e \) variables over \( \mathbb{F}_{p^n} \), where \( e = n/k \). Thus, from Lemma 3, \( S_1(a, b) \) and \( S_2(a, b) \) can be computed if their ranks are obtained. From Lemma 2, in order to derive the rank of the quadratic form \( Q_1(x) \), we need to count the number of solutions \( x \in \mathbb{F}_{p^n} \) satisfying

\[
Q_1(x + y) - Q_1(x) - Q_1(y) = 0, \quad \text{for all } y \in \mathbb{F}_{p^n},
\]

which can be rewritten as

\[
\phi_{a,b}(x) = a x^{p^g} + b x^{p^g} + ax = 0.
\]

Since the polynomial \( \phi_{a,b}(x) \) is a linearized polynomial over \( \mathbb{F}_{p^n} \) and its degree is \( p^{2g} \), the number of roots \( x \in \mathbb{F}_{p^n} \) of \( \phi_{a,b}(x) \) can be \( 1, p^k, \) or \( p^{2k} \). Thus, from Lemma 2, \( Q_1(x) \) can have the rank \( e, e - 1, \) or \( e - 2 \), where \( e = n/k \). Similarly, the corresponding linearized polynomial of \( Q_2(x) \) is given as \( \phi_{-a,b}(x) \) and the possible rank of \( Q_2(x) \) is also \( e, e - 1, \) or \( e - 2 \).

Therefore, from Lemma 3, each of \( S_1(a, b) \) and \( S_2(a, b) \) has the values

\[
\begin{aligned}
  &\pm j p^{\frac{g}{2}}, & \text{for } r = e \\
  &\pm \sqrt{p} p^{\frac{g}{2}}, & \text{for } r = e - 1 \\
  &\pm j p^{\frac{g}{2}}, & \text{for } r = e - 2
\end{aligned}
\]

where \( r \) denotes the rank of the corresponding quadratic form and \( e = n/k \).

However, there exist the values of \( S(a, b) \) which actually do not occur when \( a \) and \( b \) run through \( \mathbb{F}_{p^g} \) and they will be ruled out as in the following lemmas.

Lemma 6: At least one of \( \phi_{a,b}(x) \) and \( \phi_{-a,b}(x) \) has a single root \( x = 0 \in \mathbb{F}_{p^n} \), i.e., at least one of \( Q_1(x) \) and \( Q_2(x) \) always has the rank \( e \).

Proof: Assume that both \( \phi_{a,b}(x) \) and \( \phi_{-a,b}(x) \) have nonzero roots \( x_1 \in \mathbb{F}_{p^n} \) and \( x_2 \in \mathbb{F}_{p^n} \), respectively. Then, we have

\[
\phi_{a,b}(x_1) = 0 \Leftrightarrow a x_1^{p^g} + 2 b x_1^{p^g - 1} + a = 0
\]

\]}
\[ \phi_{-a,b}(x_2) = 0 \Leftrightarrow a^p x_2^{p-1} - 2b^p x_2^{p-1} + a = 0. \] (7)

Using (7), we can remove \(2b^p\) as
\[ a^p(x_1^{p-2} - x_2^{p-2}) + a(x_1^{p-2} + x_2^{p-2}) = 0. \] (8)

Since \(x_1^{p-2} + x_2^{p-2} \neq 0\), (8) is rewritten as
\[ \frac{a^p - 1}{x_1^{p-2} + x_2^{p-2}} = \frac{a^p - 1}{x_1^{p-2} + x_2^{p-2}} = -1. \] (9)

The left-hand side of (9) is the \((p^k-1)\)-th power in \(\mathbb{F}_{p^r}\), while \(-1\) is a nonsquare in \(\mathbb{F}_{p^r}\), which is a contradiction. Hence the proof is done. \(\Box\)

In [3], they excluded some redundant values of \(S(a, b)\) by using the Weil’s bound in Lemma 4. Similarly, the following lemma is stated.

**Lemma 7:** Two candidate values of \(S(a, b)\), \(\pm j p^{n/2} (p^k - 1)/2\), do not actually occur when \(a\) and \(b\) run through \(\mathbb{F}_{p^r}\).

**Proof:** If the rank of \(Q_2(x)\) is odd, \(S_2(a, b)\) has a pure imaginary value in (10). Then we have
\[
S_1(a, b) = 2 \sum_{x \in \mathbb{F}_{p^r}} \chi(ax^{p^{n/2}+1} + bx) + 1
\]
\[
- S_2(a, b) = \sum_{x \in \mathbb{F}_{p^r}} \chi(ax^{p^{n/2}+1} - bx) = 2 \sum_{x \in \mathbb{F}_{p^r}} \chi(ax^{p^{n/2}+1} + bx) + 1
\]
where \(C_0\) and \(C_i\) are sets of squares and nonsquares in \(\mathbb{F}_{p^r}\), respectively. Hence we have
\[
\sum_{x \in \mathbb{F}_{p^r}} \chi(ax^{p^{n/2}+1} + bx) = \frac{1}{2}(S_1(a, b) - S_2(a, b)).
\]
Assume that \(S_1(a, b) = \pm j p^{n/2}\) and \(S_2(a, b) = \mp j p^{n/2}\) or vice versa. Then we have
\[
\left| \sum_{x \in \mathbb{F}_{p^r}} \chi(ax^{p^{n/2}+1} + bx) \right| = \frac{p^{k+1}}{2} p^{\frac{3}{2}} p^{rac{3}{2}},
\]
which contradicts the Weil bound in Lemma 4. Thus the values \(S(a, b) = (S_1(a, b) + S_2(a, b))/2 = \pm j (p^k - 1)p^{n/2}/2\) are excluded.

Using the above lemmas, the possible candidate values of \(S(a, b)\) can be derived as in the following theorem.

**Theorem 1:** \(S(a, b)\) for \(a, b \in \mathbb{F}_{p^r}\) has the following candidate values
\[
\left\{ p^n, 0, \pm j p^{\frac{3}{2}}, \frac{\sqrt{p}}{2} j p^{\frac{3}{2}}, -\frac{\sqrt{p}}{2} j p^{\frac{3}{2}}, \pm j p^{k+1}/2 \right\}. \quad (10)
\]

**Proof:** From Lemmas 5–7 and (6), the proof is easily done. \(\Box\)

The above theorem also indicates that the magnitudes of the cross-correlation values of a \(p\)-ary m-sequence and its decimated sequences by \(d\) are upper bounded by
\[
\sqrt{1 + ((p^k + 1)/2)^2 p^n} \approx (p^k + 1)^{\sqrt{N}/2}.
\]

### 3.2 Value Distribution of \(S(a, b)\)

Using the result in Theorem 1, we will derive the value distribution of \(S(a, b)\). Let \(v_i, 0 \leq i \leq 9\), be the \(i\)-th value in (10), that is, \(v_0 = p^n, v_1 = 0, v_2 = j p^{\frac{3}{2}}, v_3 = -v_2, v_4 = j p^{k+1}, v_5 = v_2, v_6 = -\frac{\sqrt{p}}{2} j p^{\frac{3}{2}}, v_7 = v_6, v_8 = j p^{k+1}, v_9, v_9 = v_2\), and \(v_9 = v_5\). Let \(\Omega_i, 0 \leq i \leq 9\), be the number of occurrences of \(v_i\) when \(a\) and \(b\) run through \(\mathbb{F}_{p^r}\). If \(\Omega_0 = 1\). Since \(S(-a, -b) = S^*(a, b)\), each conjugate pair in (10) has the same number of occurrences, that is, \(\Omega_0 = \Omega_3, \Omega_4 = \Omega_5, \Omega_6 = \Omega_7, \) and \(\Omega_0 = \Omega_9\). Hence we need five independent equations in terms of \(\Omega_i\)’s to determine the entire value distribution. Since \(\sum_{x \in \mathbb{F}_{p^r}} \chi(ax) = 0\) for any \(a \in \mathbb{F}_{p^r}\), it is straightforward to obtain the following three equations
\[
\sum_{i=0}^{9} \Omega_i = p^{2n} \quad (11)
\]
\[
\sum_{i=0}^{9} v_i \Omega_i = \sum_{a,b \in \mathbb{F}_{p^r}} S(a, b) = \sum_{b, x, y \in \mathbb{F}_{p^r}} \chi(b(x^d + y^d)) \sum_{a \in \mathbb{F}_{p^r}} \chi(a(x + y)) = p^n \sum_{b, x, y \in \mathbb{F}_{p^r}} \chi(2by^d) = p^{2n} \quad (12)
\]
and
\[
\sum_{i=0}^{9} v_i^2 \Omega_i = \sum_{a,b \in \mathbb{F}_{p^r}} S^2(a, b) = \sum_{b, x, y \in \mathbb{F}_{p^r}} \chi(b(x^d + y^d)) \sum_{a \in \mathbb{F}_{p^r}} \chi(a(x + y)) = p^n \sum_{b, x, y \in \mathbb{F}_{p^r}} \chi(2by^d) = p^{2n}. \quad (13)
\]

**Lemma 8** (Theorems 4.6, 5.4, and 5.6 [18]): Let \(f(z) = z^{p^n+1} - \psi z + \psi, \psi \in \mathbb{F}_{p^r}\). Then \(f(z)\) has either 0, 1, 2, or \(p^{gcd(k,n)} + 1\) roots in \(\mathbb{F}_{p^r}\). The number of \(\psi \in \mathbb{F}_{p^r}\), such that \(f(z)\) has exactly one root in \(\mathbb{F}_{p^r}\), is equal to \(p^{gcd(k,n)}\). If \(z_0 \in \mathbb{F}_{p^r}\) is the unique root of the equation, then \(z_0\) should satisfy
\[
(z_0 - 1)^{\frac{p^{gcd(k,n)}}{p^{gcd(k,n)} - 1}} = 1. \quad (14)
\]

The number of \(\psi \in \mathbb{F}_{p^r}\), such that \(f(z)\) has exactly \(p^{gcd(k,n)} + 1\) roots in \(\mathbb{F}_{p^r}\), is equal to \(\frac{p^{gcd(k,n)} - 1}{p^{gcd(k,n)} - 1}\). Any root \(z_0 \in \mathbb{F}_{p^r}\) from the \(p^{gcd(k,n)} + 1\) roots should satisfy (14). \(\Box\)

From the above lemma, the remaining two equations in terms of \(\Omega_i\)’s are obtained as in the following lemma.
Lemma 9: We have

\[
N_1 = \Omega_4 + \Omega_5 + \Omega_6 + \Omega_7 = 2p^{n-k}(p^n - 1) \tag{15}
\]
\[
N_2 = \Omega_8 + \Omega_9 = \frac{2(p^{n-k} - 1)(p^n - 1)}{p^{2k} - 1}. \tag{16}
\]

Proof: From (6), Lemmas 2 and 6, \(N_1\) is equal to the number of \((a, b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n\) such that either \(\phi_{a,b}(x)\) or \(\phi_{-a,b}(x)\) in (7) has \(p^k\) roots in \(\mathbb{F}_p^n\). Similarly, \(N_2\) is equal to the number of \((a, b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n\) such that either \(\phi_{a,b}(x)\) or \(\phi_{-a,b}(x)\) has \(p^{2k}\) roots in \(\mathbb{F}_p^n\).

Consider \(\phi_{a,b}(x)\) and let \(x^{p^k-1} = y\). Then \(\phi_{a,b}(x)/x\) in (7) is written as

\[
a^{p^k}y^{p^k+1} = 2y^{p^k}y + a = 0. \tag{17}
\]

Let \(y_1\) and \(y_2\) be the distinct solutions to (17). Then we have

\[
y_1y_2(y_1 - y_2)^{p^k} = y_1^{p^k+1} - y_2^{p^k+1} = -y_2\left(\frac{2y^{p^k}y + a}{a^{p^k}}\right) + y_1\left(\frac{2y^{p^k}y + a}{a^{p^k}}\right) = y_1 - y_2 = y_2 - a^{p^k-1}.
\]

Thus we have

\[
y_1y_2 = (y_1 - y_2)^{p^k-1}a^{1-p^k},
\]

which means that neither \(y_1\) nor \(y_2\) is \((p^k-1)\)-th power in \(\mathbb{F}_p^n\), or both \(y_1\) and \(y_2\) are not \((p^k-1)\)-th power in \(\mathbb{F}_p^n\). Therefore, letting \(z = (-2b^{p^k}/a)y = -(2b^{p^k}/a)x^{p^k-1},\) we have;

\[
\phi_{a,b}(x) \text{ has } p^k - 1 \text{ nonzero roots in } \mathbb{F}_p^n,
\]

\[
\Leftrightarrow \text{ (17) has a single solution } y_0 \in \mathbb{F}_p^n,
\]

\[
\text{and } \frac{a^{p^k}z_0}{2b^{p^k}} = -\zeta^{p^k-1} \text{ for some } \zeta \in \mathbb{F}_p^n, \tag{18}
\]

and

\[
\phi_{a,b}(x) \text{ has } p^{2k} - 1 \text{ nonzero roots in } \mathbb{F}_p^n,
\]

\[
\Leftrightarrow \text{ (17) has } p^{k+1} \text{ nonzero solutions } y_0 \in \mathbb{F}_p^n \text{ and any nonzero solution from the } p^k + 1 \text{ solutions satisfies that } \frac{a^{p^k}z_0}{2b^{p^k}} = -\zeta^{p^k-1} \text{ for some } \zeta \in \mathbb{F}_p^n, \tag{19}
\]

where \(y_0 = (-a/(2b^{p^k}))z_0\).

Let \(\gamma = 4b^{p^k}a/p^{2k}\). Then \(\phi_{a,b}(x)\) in (7) is rewritten as

\[
z^{p^k+1} - \gamma z + \gamma = 0, \tag{20}
\]

which has the same form as the polynomial in Lemma 8. From Lemma 8, when the number of roots \(z \in \mathbb{F}_p^n\) of (20) is 1 or \(p^k + 1, \psi\ is always a square in \(\mathbb{F}_p^n\) because

\[
(z_0 - 1)^{p^k-1} = \left(\frac{z_0^{p^k+1}}{\psi}\right)^{p^k-1} = 1 \tag{21}
\]

where \(z_0\) is a root of \(f(z)\) and \((p^n - 1)/(p^k - 1)\) is odd. Fortunately, \(\gamma = 4b^{p^k}a/p^{2k}\) is a square in \(\mathbb{F}_p^n\) in this case. Thus, Lemma 8 can be used for the proof of this theorem.

Now, we will calculate the number of \((a, b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n\) satisfying (18) and (19), respectively. Lemma 8 tells us that the number of \(\gamma \in \mathbb{F}_p^n\) such that (20) has a single solution in \(\mathbb{F}_p^n\) is \(p^{2k-1}\) and the number of \(\gamma \in \mathbb{F}_p^n\) such that (20) has \(p^k + 1\) solutions in \(\mathbb{F}_p^n\) is \((p^{k+1} - 1)/(p^k - 1)\). Since for any \(b \in \mathbb{F}_p^n, \gamma\ runs through all the squares in \(\mathbb{F}_p^n\) twice as \(a\ runs through \mathbb{F}_p^n, \) the number of \((a, b)\) such that (20) has a single solution is \(2p^{n-k}(p^n - 1)\) and the number of \((a, b)\) such that (20) has \(p^k + 1\ solutions is \(2(p^{n-k} - 1)(p^n - 1)/(p^k - 1)\).

Now, from (18) and (19), we have to check that each solution \(z_0\) of (20) satisfies \(\frac{a^{p^k}z_0}{2b^{p^k}} = -\zeta^{p^k-1}\) for some \(\zeta \in \mathbb{F}_p^n\). Substituting \(\gamma = 4b^{p^k}a/p^{2k}\), (21) is rewritten as

\[
(z_0 - 1)^{p^k-1} = \left(\frac{a^{p^k}z_0}{2b^{p^k}}\right)^{p^k-1} = \left(\frac{a\gamma}{2\psi}\right)^{2p^k-1} = 1. \tag{22}
\]

Note that \(a = \pm \mu \in \mathbb{F}_p^n\) maps to the same value of \(\gamma\). From (22), we have

\[
\frac{a^{p^k}z_0}{2b^{p^k}} = \rho^{\frac{p^k-1}{2}},
\]

for some \(\rho \in \mathbb{F}_p^n\). Then, in order to satisfy (18) and (19), we have

\[
-\rho^{\frac{p^k-1}{2}} = \alpha^{\frac{p^k}{2}} - p^{k-1} \rho^{\frac{p^k}{2}} = \zeta^{p^k-1}. \tag{24}
\]

From (24), \(\rho\) must be a nonsquare in \(\mathbb{F}_p^n\). However, in (23), one of \(a = \pm \mu \in \mathbb{F}_p^n\) gives a square \(\rho\) and the other gives a nonsquare \(\rho\). Thus, one of \(a = \pm \mu \in \mathbb{F}_p^n\) should be excluded from the counting of \((a, b)\). Hence, the number of \((a, b)\) satisfying (18) and (19) is \(p^{n-k}(p^n - 1)\) and \((p^{n-k} - 1)(p^n - 1)/(p^k - 1),\) respectively.

For the case of \(\phi_{a,b}(x)\), we just consider \(-a\) instead of \(a\). Similar to the previous case, the number of \((a, b)\) such that \(\phi_{-a,b}(x)\) has \(p^k\) roots is \(p^{n-k}(p^n - 1)\) and the number of \((a, b)\) such that \(\phi_{-a,b}(x)\) has \(p^{2k}\) roots is \((p^{n-k} - 1)(p^n - 1)/(p^k - 1),\) respectively.

From Lemma 6, one of \(\phi_{a,b}(x)\) and \(\phi_{-a,b}(x)\) always has a single root in \(\mathbb{F}_p^n\). Therefore, there exists no intersection of \((a, b)\) between the previous two cases, that is,

\[
N_1 = 2p^{n-k}(p^n - 1)
\]
\[
N_2 = 2(p^{n-k} - 1)(p^n - 1)/p^{2k} - 1.
\]

Thus, the value distribution of \(S(a, b)\) can be derived as follows.

**Theorem 2:** As \(a\) and \(b\) run through \(\mathbb{F}_p^n\), the value distribution of \(S(a, b)\) is determined as
5. Weight Distribution of Cyclic Code $C$

Let $C$ be the cyclic code over $\mathbb{F}_p$, with length $N = p^n - 1$, in which each codeword is defined as

$$c(a, b) = (c_0, c_1, \ldots, c_{N-1}), \ a, b \in \mathbb{F}_p$$

where $c_i = \text{tr}_{p}(aa^i + ba^{di}), \ 0 \leq i \leq N - 1$. The Hamming weight of the codeword $c(a, b)$ is expressed as

$$H_w(c(a, b)) = |\{i|0 \leq i \leq N - 1, c_i = 0\}|$$

Thus, the correlation function $\rho_{c(a, b)}$ is given by

$$\rho_{c(a, b)}(\tau) = |\{i|0 \leq i \leq N - 1, \sigma_i c_i = 0\}|$$

Using (25) and Lemma 10, the weight distribution of the cyclic code is given as follows.

**Theorem 4:** The weight distribution $\{w_0, w_1, \ldots, w_{N\tau}\}$ of the cyclic code $C$ over $\mathbb{F}_p$, with the length $N$ and the dimension $\dim_{\mathbb{F}_p} C = 2n$ is given as

$$w_i = \begin{cases} 
1, & \text{when } i = 0 \\
(p^n - 1)(p^{n-1}p^{-k+1}), & \text{when } i = (p-1)(p^{n-1}) \\
(p^n - 1)(p^{n-1}p^{-k+\frac{d}{2}}), & \text{when } i = (p-1)(p^{n-1} + \frac{1}{2}) \\
(p^n - 1)(p^{n-1}p^{-k+\frac{d}{2}+1}), & \text{when } i = (p-1)(p^{n-1} + \frac{1}{2}) \\
(p^n - 1)(p^{n-1}p^{-k+1}), & \text{when } i = (p-1)(p^{n-1} - 1) \\
\end{cases}$$

**Proof:** From (25), we have to calculate
to determine $H_\nu(c(a,b))$. Since $p \equiv 3 \mod 4$ and $n$ is odd, $\pm j p^\nu$ is equal to $\pm (\sqrt{p^\nu})^\nu$. Hence, from Lemma 10, we can determine the image of $\mu$ map of each value of $S(a,b)$ as

$$
\mu(S(a,b)) = \sum_{l=1}^{p-1} S(la, lb) = \sum_{l=1}^{p-1} \sigma(S(a,b))
$$

to determine $H_\nu(c(a,b))$.

Thus, from (25), the proof is done. \hfill \square

6. Conclusion

In this paper, the value distribution of the exponential sum $S(a,b)$ as $a$ and $b$ run through $\mathbb{F}_p$ is derived. Using the result, we construct the sequence family $G$ in which each sequence has the period of $N = p^n - 1$. The family size is $p^n$ and the correlation magnitude is roughly upper bounded by $(p^k + 1) \sqrt{N}/2$. The weight distribution of the cyclic code $C$ over $\mathbb{F}_p$ with the length $N$ and the dimension $\dim_{\mathbb{F}_p} C = 2n$ is also determined. Our result includes the result in [3] as a special case.

References

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.