Weight Distribution of Some Cyclic Codes

Sung-Tai Choi, Ji-Youp Kim, and Jong-Seon No
Department of Electrical Engineering and Computer Science, INMC
Seoul National University
Seoul 151-744, Korea
Email: {stchoi,lakroforce}@ccl.snu.ac.kr and jsno@snu.ac.kr

Habong Chung
School of Electronics and Electrical Engineering
Hongik University
Seoul 121-791, Korea
Email: habchung@hongik.ac.kr

***Abstract*—In this paper, for an odd prime p such that $p \equiv 3 \bmod 4$, odd n, and $d = (p^n+1)/(p^k+1) + (p^n-1)/2$ with $k|n$, the value distribution of the exponential sum $S(a,b)$ when a and b run through F_{p^n} is calculated. The weight distribution of the relevant cyclic code $\mathcal{C}$ over F_p with the length $L = p^n - 1$ and the dimension $\dim_{F_p}\mathcal{C} = 2n$ is also derived. Our result generalizes the case in [5].**

***Index Terms*—Cross-correlation, cyclic code, exponential sum, weight distribution**

I. Introduction

Cyclic codes are the most important class of linear block codes for a wide variety of applications. However, not much is known about the weight distributions of these codes except in very specific cases. Especially, for an odd prime p, the value distribution of the exponential sum and the weight distribution of the relevant cyclic code are derived [3],[4]. Recently, the value distribution of the exponential sum for $d = (p^n+1)/(p+1) + (p^n-1)/2$, odd prime p such that $p \equiv 3 \bmod 4$, and odd n is derived in [5].

In this paper, the value distribution of the exponential sum is calculated for $d = (p^n+1)/(p^k+1) + (p^n-1)/2$ with $k|n$, an odd prime p such that $p \equiv 3 \bmod 4$, and odd n, which contains the result of [5] as a special case. Deploying the result, the weight distribution of the relevant cyclic code $\mathcal{C}$ is also derived.

This paper is organized as follows. In Section II, some preliminaries and notations are stated. In Section III, the value distribution of the exponential sum is derived. In Section IV, the weight distribution of the relevant cyclic code $\mathcal{C}$ is calculated. In Section V, we conclude the paper.

II. Notations and Preliminaries

A. Exponential Sum and the Hamming Weight of the Code $\mathcal{C}$

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

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$$

where $x \in F_{p^n}$ and $m|n$. Let α be a primitive element of F_{p^n} and $F_{p^n}^* = F_{p^n} \setminus \{0\}$.

In this paper, the value distribution of the exponential sum

$$S(a,b) = \sum_{x \in F_{p^n}} \chi(ax + bx^d)$$

when a and b run through F_{p^n} is considered, where ω is a primitive p-th root of unity and $\chi(\cdot) = \omega^{\mathrm{tr}_1^n(\cdot)}$ is a canonical multiplicative character of F_{p^n}.

Let $\mathcal{C}$ be the cyclic code over F_p with the length $L = p^n - 1$ in which each codeword is defined as

$$c(a,b) = (c_0, c_1, \ldots, c_{L-1}),\ a, b \in F_{p^n}$$

where $c_i = \mathrm{tr}_1^n(a\alpha^i + b\alpha^{di})$, $0 \le i \le L-1$. The Hamming weight of the codeword $c(a,b)$ is given as

$$H_w(c(a,b)) = \big|\{i | 0 \le i \le L-1, c_i \neq 0\}\big|.$$

B. Quadratic Form

We define a quadratic form in k variables over F_{p^s} as a homogeneous polynomial in $F_{p^s}[x_1, \ldots, x_k]$

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

where p is an odd prime and $a_{ij} = a_{ji} \in F_{p^s}$. We then associate f with the $k \times k$ 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 $k \times k$ matrix B over F_{p^s} such that $C = BAB^T$ is a diagonal matrix and $C = \mathrm{diag}(c_1, \ldots, c_r, 0, \cdots, 0)$, where $c_i \in F_{p^s}^*$. Let $\Delta = c_1 \cdots c_r$ and η be the quadratic character of F_{p^s}, which will be used in the following lemmas. A quadratic form $f(\mathbf{x})$ in k variables over F_{p^s} can be regarded as a mapping $f(x)$ from $F_{p^{sk}}$ to F_{p^s} when $x_i \in F_{p^s}$. Thus, we will also use the term 'quadratic form' for this mapping $f(x)$ in $F_{p^{sk}}$.

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

$$\mathrm{tr}_1^n\Big(\sum_i a_i x^{p^i+1}\Big) = \mathrm{tr}_1^s\big(f(x)\big),\ 0 \le i < n$$

where $a_i \in F_{p^n}^*$ and s is a great common divisor of n and all nonzero i's. Then

$$f(x) = \mathrm{tr}_s^n\Big(\sum_i a_i x^{p^i+1}\Big)$$

is a quadratic form over F_{p^s}. ■

Lemma 2 (Luo and Feng [3]): The rank r of the quadratic form $f(x)$ from $F_{p^{sk}}$ to F_{p^s} can be determined from the number of elements that the form is independent of, i.e., $(p^s)^{k-r}$ is the number of $y \in F_{p^{sk}}$ such that $f(x+y) - f(x) - f(y) = 0$ for all $x \in F_{p^{sk}}$. ■

Lemma 3 (Luo and Feng [3]): Let $f(x)$ be a mapping from $F_{p^{sk}}$ to F_{p^s} corresponding to a quadratic form $f(\mathbf{x}) \in F_{p^s}[x_1, x_2, \ldots, x_k]$ of rank r with Δ. Then we have

$$\sum_{x \in F_{p^{sk}}} \omega^{\mathrm{tr}_1^s(f(x))} = \begin{cases} \eta(\Delta)(p^s)^{k-\frac{r}{2}}, & \text{if } p^s \equiv 1 \bmod 4 \\ j^r \eta(\Delta)(p^s)^{k-\frac{r}{2}}, & \text{if } p^s \equiv 3 \bmod 4 \end{cases} \quad (1)$$

where $j = \sqrt{-1}$. ∎

III. Value Distribution of $S(a, b)$

A. Parameters

In this paper, the value distribution of the exponential sum $S(a, b)$ when a and b run through F_{p^n} is considered. Here are some parameters used in the remainder of this paper:

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

B. Evaluation of $S(a, b)$

When either a or b is equal to zero, $S(a, b)$ is given as the following lemma.

Lemma 4: When either a or b is equal to zero, $S(a, b)$ is determined as

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

∎

Note that $\gcd(p^k + 1, p^n - 1) = 2$ and -1 is a nonsquare in F_{p^n}. Then, for $a, b \in F_{p^n}^*$, $S(a, b)$ can be transformed into the exponential sums of the quadratic forms as

$$\begin{aligned} S(a,b) &= \sum_{x \in F_{p^n}} \chi(ax + bx^d) \\ &= \frac{1}{2}\big(S_1(a,b) + S_2(a,b)\big) \end{aligned} \quad (2)$$

where $S_1(a, b) = \sum_{x \in F_{p^n}} \chi(ax^{p^k+1} + bx^2)$ and $S_2(a, b) = \sum_{x \in F_{p^n}} \chi(-ax^{p^k+1} + bx^2)$. From Lemma 1, it is easily verified that both

$$Q_1(x) = \mathrm{tr}_k^n(ax^{p^k+1} + bx^2)$$

and

$$Q_2(x) = \mathrm{tr}_k^n(-ax^{p^k+1} + bx^2)$$

are quadratic forms over F_{p^k}. Thus, from Lemma 3, we are able to calculate the exponential sums $S_1(a, b)$ and $S_2(a, b)$. From Lemma 2, in order to derive the rank of the quadratic form $Q_1(x)$, we need to calculate the number of solutions $x \in F_{p^n}$ satisfying

$$\begin{aligned} &Q_1(x + y) - Q_1(x) - Q_1(y) = 0, \text{ for all } y \in F_{p^n} \\ \Leftrightarrow\ &\phi_{a,b}(x) = a^{p^k} x^{p^{2k}} + 2b^{p^k} x^{p^k} + ax = 0. \end{aligned}$$

Since the polynomial $\phi_{a,b}(x)$ is a linearized polynomial over F_{p^n}, it is easily checked that the number of roots $x \in F_{p^n}$ is 1, p^k, or p^{2k}. 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 $e - 2$.

From Lemma 3, it is easily checked that each exponential sum of $S_1(a, b)$ and $S_2(a, b)$ has the values

$$\begin{cases} \pm j p^{\frac{n}{2}}, & \text{for } r = e \\ \pm\sqrt{p^k} p^{\frac{n}{2}}, & \text{for } r = e - 1 \\ \pm j p^k p^{\frac{n}{2}}, & \text{for } r = e - 2 \end{cases} \quad (3)$$

where r denotes the rank of the corresponding quadratic form.

From the two techniques in [5], some exponential sum values which actually do not occur can be ruled out for explicit evaluation as the following lemmas.

Lemma 5: At least one of $\phi_{a,b}(x)$ and $\phi_{-a,b}(x)$ has a single root in F_{p^n}, i.e., one of the two quadratic forms $Q_1(x)$ and $Q_2(x)$ must have the rank e. ∎

Lemma 6 (Theorem 5.38 [6]): Let $f(x) \in F_{p^n}[x]$ be a polynomial of degree $l \geq 1$ with $\gcd(l, p^n) = 1$ and let χ be a nontrivial additive character of F_{p^n}. Then

$$\Big| \sum_{x \in F_{p^n}} \chi(f(x)) \Big| \leq (l - 1) p^{\frac{n}{2}}.$$

∎

In [5], they used the wise method to exclude some exponential sum values which do not occur by using Weil's bound in Lemma 6. Similarly, the following lemma can be derived.

Lemma 7: The two candidate values of $S(a, b)$, $\pm j(p^k - 1)/2p^{n/2}$, do not actually occur when a and b run through $F_{p^n}^*$. ∎

Theorem 8: The exponential sum $S(a, b)$ for $a, b \in F_{p^n}$ has the following candidate values

$$\{p^n, 0, \pm j p^{\frac{n}{2}}, \frac{\sqrt{p^k} \pm j}{2} p^{\frac{n}{2}}, \frac{-\sqrt{p^k} \pm j}{2} p^{\frac{n}{2}}, \pm j \frac{p^k + 1}{2} p^{\frac{n}{2}}\}. \quad (4)$$

∎

C. Value Distribution of $S(a, b)$

So far, it is derived that the exponential sum $S(a, b)$ can have the ten candidate values as in Theorem 8. Let v_i, $0 \leq i \leq 9$, be the i-th value in (4) through the given order. Let Ω_i, $0 \leq i \leq 9$, be the number of occurrences of v_i when a and b run through F_{p^n}. Note that each conjugate pair has the same number of occurrences. Hence we need five independent equations in terms of Ω_i to determine the distribution. It is easy to derive the following three equations

$$\sum_{i=0}^{9} \Omega_i = p^{2n} \quad (5)$$

$$\sum_{i=0}^{9} v_i \Omega_i = \sum_{a,b \in F_{p^n}} S(a,b) = p^{2n} \quad (6)$$

and

$$\sum_{i=0}^{9} v_i^2 \Omega_i = \sum_{a,b \in F_{p^n}} S^2(a,b) = p^{2n}. \quad (7)$$

From the results in [7], the distribution of the ranks of the quadratic forms $Q_1(x)$ and $Q_2(x)$ when a and b run through $F_{p^n}^*$ can be derived. Hence the remaining two equations in terms of Ω_i's can be obtained from the rank distribution.

From the above lemma, the following lemma is derived.

Lemma 9: We have

$$N_1 = \Omega_4 + \Omega_5 + \Omega_6 + \Omega_7 = 2p^{n-k}(p^n - 1) \quad (8)$$

$$N_2 = \Omega_8 + \Omega_9 = \frac{2(p^{n-k}-1)(p^n-1)}{p^{2k}-1}. \quad (9)$$

■

From the derived five equations (5)–(9), each value of Ω_i is determined as in the following theorem.

Theorem 10: The value distribution of the exponential sum $S(a,b)$ when a and b run through F_{p^n} is given as

$$S(a,b) = \begin{cases} p^n, & \text{once} \\ 0, & \frac{(p^k-1)(p^{2n}-1)}{2(p^k+1)} \text{ times} \\ \pm j p^{n/2}, & \frac{p^{2n}-1}{4} - \frac{(p^n-1)^2}{2(p^k-1)} \text{ times} \\ \frac{\sqrt{p^k}\pm j}{2} p^{\frac{n}{2}}, & \frac{(p^n-1)(p^{n-k}+p^{\frac{n-k}{2}})}{2} \text{ times} \\ \frac{-\sqrt{p^k}\pm j}{2}, & \frac{(p^n-1)(p^{n-k}-p^{\frac{n-k}{2}})}{2} \text{ times} \\ \pm j \frac{p^k+1}{2} p^{\frac{n}{2}}, & \frac{(p^{n-k}-1)(p^n-1)}{p^{2k}-1} \text{ times.} \end{cases}$$

■

IV. The Weight Distribution of $\mathcal{C}$

Let $\mathcal{C}$ is the cyclic code over F_p with length $L = p^n - 1$ in which each codeword is defined as

$$c(a,b) = (c_0, c_1, \ldots, c_{L-1}), \ a, b \in F_{p^n}$$

where $c_i = \mathrm{tr}_1^n(a\alpha^i + b\alpha^{di})$, $0 \le i \le L-1$. The Hamming weight of the codeword $c(a,b)$ is given as

$$\begin{aligned} H_w(c(a,b)) &= L - \frac{1}{p} \sum_{i=0}^{L-1} \sum_{j=0}^{p-1} (\chi(a\alpha^i + b\alpha^{di}))^j \\ &= p^{n-1}(p-1) - \frac{1}{p}\mu(S(a,b)) \end{aligned} \quad (10)$$

where $\mu(S(a,b)) = \sum_{j=1}^{p-1} S(ja, jb)$. Hence the Hamming weight of the codeword $c(a,b)$ is determined by calculating $\mu(S(a,b))$. Let $\{w_0, w_1, \ldots, w_L\}$ be the weight distribution of $\mathcal{C}$, where w_i is the number of occurrences of the codewords $c(a,b)$ of Hamming weight i, $0 \le i \le L$, when a and b run through F_{p^n}. The following lemma is used for the calculation of $\mu(S(a,b))$.

Lemma 11 (Lemma 4 in [2]): Let ω be a primitive p-th root of unity and $(\frac{\cdot}{p})$ the Legendre symbol. The Galois group of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ is $\{\sigma_i | 1 \le i \le p-1\}$ where the automorphism σ_i of $\mathbb{Q}(\omega)$ is determined by $\sigma_i(\omega) = \omega^i$. The unique quadratic subfield of $\mathbb{Q}(\omega)$ is $\mathbb{Q}(\sqrt{p^*})$, where $p^* = (\frac{-1}{p})p$ and $\sigma_i(\sqrt{p^*}) = (\frac{i}{p})\sqrt{p^*}$, $1 \le i \le p-1$.

Theorem 12: The weight distribution $\{w_0, w_1, \ldots, w_L\}$ of the cyclic code $\mathcal{C}$ over F_p with the length $L = p^n - 1$ and the dimension $\dim_{F_p}\mathcal{C} = 2n$ is given as

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

■

V. Conclusion

In this paper, the value distribution of the exponential sum $S(a,b)$ when a and b run through F_{p^n} and the weight distribution of the relevant cyclic code $\mathcal{C}$ over F_p with the length $L = p^n - 1$ and the dimension $\dim_{F_p}\mathcal{C} = 2n$ are derived for an odd prime p such that $p \equiv 3 \bmod 4$, $d = (p^n+1)/(p^k+1) + (p^n-1)/2$ with $k|n$, and odd n. Our result includes the result in [5] as a special case.

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

[2] K. Feng and J. Luo, "Weight distribution of some reducible cyclic codes," *Finite Fields Appl.*, vol. 14, no. 2, pp. 390–409, Apr. 2008.

[3] 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.

[4] J. Luo and K. Feng, "On the weight distributions of two classes of cyclic codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5332–5344, Dec. 2008.

[5] 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.

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

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