Several Classes of Codes and Sequences Derived From a $\mathbb{Z}_4$-Valued Quadratic Form

Nian Li, Xiaohu Tang, *Member, IEEE*, and Tor Helleseth, *Fellow, IEEE*

***Abstract*—Let m and k be positive integers with $m/\gcd(m,k)$ being odd, for $a \in \mathbb{R}$ and $b \in \mathbb{L}$, the exponential sum $\sum_{x\in\mathbb{L}} i^{Tr(ax+2bx^{2^k+1})}$ is studied systematically in this paper, where $i=\sqrt{-1}$, $\mathbb{R}=\mathbb{GR}(4,m)$ is a Galois ring, $\mathbb{L}$ is the Teichmüller set of $\mathbb{R}$ and $Tr(\cdot)$ is the trace function from the Galois ring $\mathbb{R}$ to $\mathbb{Z}_4$. Through the discussions on the solutions of certain equations and the newly developed theory of $\mathbb{Z}_4$-valued quadratic forms, the distribution of the exponential sum is completely determined. As its applications, we can determine the Lee weight and Hamming weight distributions of a class of codes $\mathcal{C}^k$ over $\mathbb{Z}_4$ and the correlation distribution of a quaternary sequence family $\mathcal{U}^k$, respectively. Furthermore, the Hamming weight distributions of the binary codes obtained from $\mathcal{C}^k$ under the most significant bit (MSB) and Gray maps are also determined. For the MSB map sequences of $\mathcal{U}^k$, the nontrivial maximal correlation value is given and the correlation distribution is determined for the Gray map sequences of $\mathcal{U}^k$. It should be noted that the distribution of the exponential sum for the case $\gcd(m,k)\neq 1$ is obtained for the first time, and then the corresponding codes and sequences are novel.**

***Index Terms*—Correlation distribution, Galois ring, Gray map, Hamming weight, Lee weight, most significant bit (MSB) map, quadratic form.**

I. Introduction

Let $\mathbb{Z}_l=\{0,1,\ldots,l-1\}$ be the ring of integers modulo l. The Galois ring $\mathbb{R}=\mathbb{GR}(4,m)$ with 4^m elements is the Galois extension of degree m over $\mathbb{Z}_4$. Due to the easy implementation in modulators and the better correlation properties than binary sequences according to the Welch and Sidelnikov bounds [13], [22], many researchers have studied codes and sequences over Galois rings in the last decade [3], [5], [8], [9], [14], [17]–[19], [21].

Throughout this paper, let m and k be positive integers with $\gcd(m,k)=d$ and m/d being odd. A class of exponential sum over a Galois ring is denoted by

$$\rho(a,b)=\sum_{x\in\mathbb{L}} i^{Tr(ax+2bx^{2^k+1})}, a\in\mathbb{R}, b\in\mathbb{L} \qquad (1)$$

where $i=\sqrt{-1}$, $\mathbb{L}$ is the Teichmüller set of $\mathbb{R}$ and $Tr(\cdot)$ is the trace function from the Galois ring $\mathbb{R}$ to $\mathbb{Z}_4$ (see Section II-B). Several classes of codes and sequence families have been obtained from the distribution of $\rho(a,b)$ for some specific values of the parameters m and k. The distribution of $\rho(a,b)$ for $k=1$ had been studied in [8] to determine the correlation distribution of the quaternary sequence family $\mathcal{S}(1)$. Codes with the same weight distribution as the Goethals codes and the Delsarte-Goethals codes were obtained based on the distribution of $\rho(a,b)$ for odd m and $\gcd(m,k)=1$ [5]. Most recently, the theory of $\mathbb{Z}_4$-valued quadratic forms [11] was used to analyze the exponential sum $\rho(a,b)$ and new sequence families were obtained in [11] and [12], in which the distribution of $\rho(a,b)$ for odd m and $k=1$ was also determined.

In this paper, based on the discussions of the properties of certain equations over a finite field and the newly developed theory of $\mathbb{Z}_4$-valued quadratic forms, the distribution of the exponential sum $\rho(a,b)$ is uniformly determined, which generalizes the results in [5] and [8] and will play an important role in determining the weight distributions and correlation distributions of several classes of codes and sequences, respectively. Concretely, as applications of the exponential sum $\rho(a,b)$, we can determine both the Lee weight and Hamming weight distributions of a class of codes $\mathcal{C}^k$ over $\mathbb{Z}_4$. By choosing cyclicly inequivalent codewords from $\mathcal{C}^k$, a quaternary sequence family $\mathcal{U}^k$ is obtained and the correlation distribution is also determined. The quaternary codes $\mathcal{C}^k$ extend the results in [5], and the family $\mathcal{U}^k$ is a generalization of family $\mathcal{S}(1)$ in [8]. In addition, two classes of binary codes and sequence families are obtained by performing the MSB and Gray maps on $\mathcal{C}^k$ and $\mathcal{U}^k$, respectively. The Hamming weight distributions of both the binary MSB map code $\pi(\mathcal{C}^k)$ and Gray map code $\phi(\mathcal{C}^k)$ are determined. The binary sequence family $\pi(\mathcal{U}^k)$ is the MSB map sequences of $\mathcal{U}^k$, and we only can give a bound on the nontrivial maximal correlation value. The correlation distribution of this family was determined only for odd m and any k with $\gcd(m,k)=1$ [25]. For the general case, it is still unknown. The other binary sequence family $\varphi(\mathcal{U}^k)$ is obtained from $\mathcal{U}^k$ under the modified Gray map and its correlation distribution is completely determined, which generalizes the family $\mathcal{V}(1)$ in [12]. We check all the above distributions by computer experiments.

The remainder of this paper is organized as follows. Section II gives some preliminaries. In Section III, we determine the rank distribution of a class of quadratic forms over a Galois ring, and the distribution of the exponential sum $\rho(a,b)$ is determined in Section IV. As applications of the distribution of $\rho(a,b)$, several classes of codes and sequence families are discussed in Sections V and VI, respectively, and the concluding remarks are given in Section VII.

Manuscript received September 27, 2010; revised November 04, 2010; accepted April 26, 2011. Date of current version November 11, 2011. N. Li and X. Tang were supported in part by the National Science Foundation of China (NSFC) under Grant 60772086 and in part by the Australia-China Special Fund under Grant 61011120055. T. Helleseth was supported by the Norwegian Research Council.

N. Li and X. Tang are with the Provincial Key Lab of Information Coding and Transmission, Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, 610031, China (e-mail: xhutang@ieee.org; nianli.2010@gmail.com).

T. Helleseth is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: tor.helleseth@ii.uib.no).

Communicated by M. G. Parker, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2011.2156382

0018-9448/$26.00 © 2011 IEEE

II. Preliminaries

A. Correlation Function

For any two sequences $\mathbf{a}=\{\mathbf{a}(t)\}_{t=0}^{N-1}$ and $\mathbf{b}=\{\mathbf{b}(t)\}_{t=0}^{N-1}$ of period N over $\mathbb{Z}_l$, the cross correlation function $R_{\mathbf{a},\mathbf{b}}(\tau)$ is defined as

$$R_{\mathbf{a},\mathbf{b}}(\tau)=\sum_{t=0}^{N-1} w^{\mathbf{a}(t+\tau)-\mathbf{b}(t)}$$

where w is a primitive complex lth root of unity and $0\le\tau\le N-1$.

B. Galois Rings

The Galois ring $\mathbb{R}=\mathbb{GR}(4,m)$ is the Galois extension of degree m over $\mathbb{Z}_4$. Let $\mu:\mathbb{Z}_4\longrightarrow\mathbb{Z}_2$ be the modulus 2 reduction. Naturally, the mapping μ induces a homomorphism from the Galois ring $\mathbb{R}$ to the finite field $\mathbb{F}_{2^m}$ with 2^m elements. For every element $z\in\mathbb{R}$, it can be uniquely expressed in the form

$$z=x+2y,\ x,y\in\mathbb{L}$$

where $\mathbb{L}$ is the Teichmüller set of $\mathbb{R}$ defined by $\mathbb{L}=\{z\in\mathbb{R}:z^{2^m}=z\}$. For more details, the reader is referred to [3], [8]–[10] and [14].

Unlike in the finite field $\mathbb{F}_{2^m}$ of size 2^m, the addition operation in the Teichmüller set $\mathbb{L}$ is not closed. Specially, for any $x,y\in\mathbb{L}$, there exists a unique $z\in\mathbb{L}$ such that $z=x+y+2\sqrt{xy}$. For convenience in this paper we define a new operation $\oplus$ on $\mathbb{L}$ by

$$x\oplus y=x+y+2\sqrt{xy}.$$

Essentially, $(\mathbb{L},\oplus,\cdot)$ is isomorphic to the finite field $\mathbb{F}_{2^m}$.

The trace functions $tr:\mathbb{L}\longrightarrow\mathbb{Z}_2$ and $Tr:\mathbb{R}\longrightarrow\mathbb{Z}_4$ are respectively defined as

$$tr(x)=\oplus_{j=0}^{m-1}x^{2^j},\ x\in\mathbb{L}$$
$$Tr(x+2y)=\sum_{j=0}^{m-1}(x^{2^j}+2y^{2^j}),\ x,y\in\mathbb{L}.$$

One can easily check that the trace functions $tr(\cdot)$ and $Tr(\cdot)$ are linear functions over $\mathbb{Z}_2$ and $\mathbb{Z}_4$, respectively. Moreover, the identity $2Tr(x)=2tr(x)$ holds for all $x\in\mathbb{L}$.

C. MSB and Gray Maps

In this paper, two maps are involved. The first one is the MSB map from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ defined by

$$\pi(0)=0,\pi(1)=0,\pi(2)=1,\pi(3)=1$$

and another one is the Gray map from $\mathbb{Z}_4$ to $\mathbb{Z}_2\times\mathbb{Z}_2$ defined by $\phi(x)=(\pi(x),\pi(3x))$ for $x\in\mathbb{Z}_4$, i.e.,

$$\phi(0)=(0,0),\phi(1)=(0,1)$$
$$\phi(2)=(1,1),\phi(3)=(1,0).$$

When performing the MSB map π and Gray map ϕ on the quaternary sequence $\{\mathbf{a}(t)\}_{t=0}^{N-1}$, we naturally obtain the MSB map sequence $\pi_{\mathbf{a}}=\{\pi(\mathbf{a}(t))\}_{t=0}^{N-1}$ and the Gray map sequence $\phi_{\mathbf{a}}=\{\phi_{\mathbf{a}}(t)\}_{t=0}^{2N-1}$, where

$$\phi_{\mathbf{a}}(t)=\begin{cases}\pi(\mathbf{a}(t_0)), & t=2t_0,\\ \pi(3\mathbf{a}(t_0)), & t=2t_0+1.\end{cases}$$

If N is odd, it is more convenient to use the modified Gray map sequence $\varphi_{\mathbf{a}}=\{\varphi_{\mathbf{a}}(t)\}_{t=0}^{2N-1}$ proposed by Nechaev [10], which is defined as

$$\varphi_{\mathbf{a}}(t)=\begin{cases}\pi(\mathbf{a}(t_0)), & t=2t_0,\\ \pi(3\mathbf{a}(t_0+\frac{N+1}{2})), & t=2t_0+1.\end{cases}$$

The correlation functions of the quaternary sequences and those of their MSB map and modified Gray map sequences have the following relations.

Lemma 1 ([20]): Let $\{\mathbf{a}(t)\}_{t=0}^{N-1}$ and $\{\mathbf{b}(t)\}_{t=0}^{N-1}$ be two quaternary sequences of odd length N. Then

$$R_{\pi_{\mathbf{a}},\pi_{\mathbf{b}}}(\tau)=\mathfrak{Re}(R_{\mathbf{a},\mathbf{b}}(\tau))-\mathfrak{Im}(R_{3\mathbf{a},\mathbf{b}}(\tau))$$

where $\mathfrak{Re}(x)$ and $\mathfrak{Im}(x)$ represent the real and imaginary parts of x, respectively.

Lemma 2 ([6]): Let $\{\mathbf{a}(t)\}_{t=0}^{N-1}$ and $\{\mathbf{b}(t)\}_{t=0}^{N-1}$ be two quaternary sequences of odd length N. Then

$$R_{\varphi_{\mathbf{a}},\varphi_{\mathbf{b}}}(\tau)=\begin{cases}2\cdot\mathfrak{Re}(R_{\mathbf{a},\mathbf{b}}(\tau_0)), & \text{if } \tau=2\tau_0,\\ 2\cdot\mathfrak{Re}(R_{3\mathbf{a},\mathbf{b}}(\tau_0+\frac{N+1}{2})), & \text{if } \tau=2\tau_0+1.\end{cases}$$

D. $\mathbb{Z}_4$-Valued Quadratic Forms

Definition 1: A symmetric bilinear form on $\mathbb{L}$ is a mapping $B:\mathbb{L}\times\mathbb{L}\longrightarrow\mathbb{Z}_2$ with two properties

1) symmetry: $B(x,y)=B(y,x)$;
2) bilinearity: for any $\alpha,\beta\in\mathbb{Z}_2$, $B(\alpha x\oplus\beta y,z)=\alpha B(x,z)\oplus\beta B(y,z)$.

Specifically, B is called alternating if $B(x,x)=0$ for all $x\in\mathbb{L}$.

The rank of B is defined as $\mathrm{rank}(B)=m-\dim_{\mathbb{Z}_2}(\mathrm{rad}(B))$, where

$$\mathrm{rad}(B)=\{x\in\mathbb{L}:B(x,y)=0,\ \forall y\in\mathbb{L}\}. \tag{2}$$

Definition 2 ([2]): A $\mathbb{Z}_4$-valued quadratic form is a mapping $Q:\mathbb{L}\longrightarrow\mathbb{Z}_4$ that satisfies

1) $Q(0)=0$, and
2) $Q(x\oplus y)=Q(x)+Q(y)+2B(x,y)$,

where $B:\mathbb{L}\times\mathbb{L}\longrightarrow\mathbb{Z}_2$ is a symmetric bilinear form. In addition, Q is called alternating if its associated bilinear form B is alternating.

Similarly, the rank of the $\mathbb{Z}_4$-valued quadratic form Q is defined as $\mathrm{rank}(Q)=\mathrm{rank}(B)$.

Given a $\mathbb{Z}_4$-valued quadratic form $Q:\mathbb{L}\longrightarrow\mathbb{Z}_4$, we are particularly interested in the distribution of the values of the exponential sum

$$\chi_Q(u)=\sum_{x\in\mathbb{L}}i^{Q(x)}(-1)^{tr(ux)}$$

when u ranges over $\mathbb{L}$.

If Q is alternating, it is well-known that the distribution completely depends on its rank r.

Lemma 3 ([6]): Let Q be an alternating $\mathbb{Z}_4$-valued quadratic form of rank r, then the distribution of $\{\chi_Q(u), u \in \mathbb{L}\}$ is given by

$$\begin{cases} \pm 2^{m-\frac{r}{2}}, & 2^{r-1} \pm 2^{\frac{r}{2}-1} \text{times} \\ 0, & 2^m - 2^r \text{ times}. \end{cases}$$

Recently, Schmidt developed the theory of $\mathbb{Z}_4$-valued quadratic form and established the similar result.

Lemma 4 ([11]): Let Q be a nonalternating $\mathbb{Z}_4$-valued quadratic form of rank r. Then the distribution of the values in the multiset $\{\chi_Q(u) : u \in \mathbb{L}\}$ is as follows. If r is odd, we have

$$\begin{cases} 0, & 2^m - 2^r \text{ times} \\ \pm(1+i)2^{m-\frac{r+1}{2}}, & 2^{r-2} \pm 2^{\frac{r-3}{2}} \text{ times} \\ \pm(1-i)2^{m-\frac{r+1}{2}}, & 2^{r-2} \pm 2^{\frac{r-3}{2}} \text{times}. \end{cases}$$

If r is even, we have

$$\begin{cases} 0, & 2^m - 2^r \text{times} \\ \pm 2^{m-\frac{r}{2}}, & 2^{r-2} \pm 2^{\frac{r}{2}-1} \text{ times} \\ \pm 2^{m-\frac{r}{2}} i, & 2^{r-2} \text{ times (each)}. \end{cases}$$

The following lemma about the greatest common division will be used in the proofs of our results.

Lemma 5: For positive integers u and v, we have $\gcd(2^u - 1, 2^v - 1) = 2^{\gcd(u,v)} - 1$ and

$$\gcd(2^u - 1, 2^v + 1) = \begin{cases} 1, & \text{if } \frac{u}{\gcd(u,v)} \text{ is odd} \\ 1 + 2^{\gcd(u,v)}, & \text{otherwise.} \end{cases}$$

III. Rank Distribution of $\mathbb{Z}_4$-Valued Quadratic Form $Q_{b,c}(x)$

In this section, we mainly discuss the rank distribution of the quadratic form

$$Q_{b,c}(x) = Tr(2bx^{1+2^k} + cx), x \in \mathbb{L}$$

where $b, c \in \mathbb{L}$.

Notice that $Q_{b,c}(x)$ is a $\mathbb{Z}_4$-valued quadratic form and its associated bilinear form is

$$B_{b,c}(x, y) = tr(bx^{2^k} y \oplus bxy^{2^k} \oplus c^2 xy).$$

By (2), to determine the rank of $Q_{b,c}(x)$, it is sufficient to consider the roots of

$$bx^{2^k} \oplus b^{2^{m-k}} x^{2^{m-k}} \oplus c^2 x = 0. \tag{3}$$

Taking 2^kth power on both sides of (3), then it equivalently becomes $xg(y) = 0$, where

$$g(y) = b^{2^k} y^{1+2^k} \oplus c^{2^{k+1}} y \oplus b \tag{4}$$

and $y = x^{2^k - 1}$.

Similar to the discussion in [4], [7], and [24], some properties of the roots of $g(y) = 0$ can be obtained. First, we need the following lemma.

Lemma 6 ([11]): Let $h(x) = x^{2^s+1} \oplus \varepsilon x \oplus \varepsilon$ with $\varepsilon \in \mathbb{L}^* = \mathbb{L} \backslash \{0\}$ and $D = 2^{\gcd(s,m)}$. Then $h(x) = 0$ has 0, 1, 2 or $D + 1$ solutions in $\mathbb{L}$. Assume that N_j denote the number of $\varepsilon \in \mathbb{L}^*$ such that $h(x)$ has exactly j roots in $\mathbb{L}$, where $j = 0, 1, 2, D+1$. If $\nu = \frac{m}{\gcd(s,m)}$ is odd, then

$$N_0 = \tfrac{D^{\nu+1}+D}{2(D+1)}, \qquad N_1 = D^{\nu-1} - 1$$
$$N_2 = \tfrac{(D-2)(D^{\nu}-1)}{2(D-1)}, \qquad N_{D+1} = \tfrac{D^{\nu-1}-1}{D^2-1}.$$

Furthermore, if $h(x) = 0$ has exactly one solution $x_0 \in \mathbb{L}$, then $(x_0 \oplus 1)^{\frac{2^m-1}{D-1}} = 1$.

Lemma 7: For $bc \neq 0$, let $g(y)$ be defined by (4). Then:

1) The equation $g(y) = 0$ has either 0, 1, 2 or $1+2^d$ solutions in $\mathbb{L}$.
2) If y_1 and y_2 are two different solutions of $g(y) = 0$, then $(y_1 y_2)^{\frac{2^m-1}{2^d-1}} = 1$.
3) If $g(y) = 0$ has at least three solutions $y_1, y_2, y_3 \in \mathbb{L}$, then $y_i^{\frac{2^m-1}{2^d-1}} = 1$ for $i = 1, 2, 3$.
4) If $g(y) = 0$ has exactly one solution $y_0 \in \mathbb{L}$, then $y_0^{\frac{2^m-1}{2^d-1}} = 1$.

Remark 1: The analogy of properties 2) and 3) over a finite field with characteristic 2 was obtained in [4] and [7], and the analogy of properties 1), 3), and 4) over a finite field with odd characteristic was discussed in [24].

Based on Lemma 7 and $\gcd(2^k - 1, 2^m - 1) = 2^d - 1$, one can deduce that the possible ranks of $B_{b,c}(x, y)$ are m, $m - d$ or $m - 2d$. Moreover, the rank distribution of $B_{b,c}(x, y)$ can be determined. To achieve this goal, for $j = 0, d, 2d$, define

$$\mathcal{R}_j = \{(b, c) \in \mathbb{L} \times \mathbb{L} \setminus \{(0, 0)\} : \text{rank}(B_{b,c}(x, y)) = m - j\}.$$

Proposition 1: When $(b, c) \in \mathbb{L} \times \mathbb{L} \setminus \{(0, 0)\}$, the distribution of $\text{rank}(B_{b,c}(x, y))$ is given by

$$\begin{cases} |\mathcal{R}_0| = \frac{(2^m-1)(2^{m+2d}-2^{m+d}-2^m+2^{2d})}{2^{2d}-1} \\ |\mathcal{R}_d| = (2^m - 1)2^{m-d} \\ |\mathcal{R}_{2d}| = \frac{(2^m-1)(2^{m-d}-1)}{2^{2d}-1}. \end{cases}$$

Proof: It is easy to see that the rank of $B_{b,c}(x, y)$ is m if $b = 0$ and $c \neq 0$ and the rank of $B_{b,c}(x, y)$ is $m - d$ if $b \neq 0$ and $c = 0$. Hereafter, we focus on the case of $b \neq 0$ and $c \neq 0$. Rewrite (4) as

$$g(y) = b\zeta^{-1} \left(z^{2^k+1} \oplus \zeta z \oplus \zeta \right) \tag{5}$$

if $bc \neq 0$ and let $y = \frac{b}{c^{2^k+1}} z$ and $\zeta = \frac{c^{2^{k+1}(2^k+1)}}{b^{2^k+1}}$. Applying Lemma 7, we know that $g(y) = 0$ has 0, 1, 2, or $2^d + 1$ solutions, which is discussed case by case as follows.

Case 1 When $g(y) = 0$ has no solutions, then (3) has only zero solution; thus, in this case, the rank of $B_{b,c}(x, y)$ is m.

Case 2 If $g(y) = 0$ has exactly one solution, then by Lemma 7–4), the solution is a $(2^d - 1)$th power in $\mathbb{L}$. Thus, (3) has $(2^d - 1) + 1 = 2^d$ solutions, i.e., the rank of $B_{b,c}(x, y)$ is $m - d$.

Case 3 If $g(y) = 0$ has two solutions $y_1, y_2 \in \mathbb{L}$, then by Lemma 7–2), y_1, y_2 are either both $(2^d - 1)$th powers

or both not (2^d-1)th powers in $\mathbb{L}$. The former cannot be true since in that case (3) would have exactly $2^{d+1}-1$ roots in $\mathbb{L}$, which contradicts the fact that the number of roots of (3) is a power of 2. Therefore, both roots are not (2^d-1)th powers in $\mathbb{L}$ and (3) has no nonzero root in $\mathbb{L}$, i.e., $\mathrm{rank}(B_{b,c}(x,y))$ is m.

Case 4 If $g(y)=0$ has 2^d+1 solutions, by Lemma 7–3), all of them are (2^d-1)th powers in $\mathbb{L}$. Hence, (3) has 2^{2d} solutions, i.e., the rank of $B_{b,c}(x,y)$ is $m-2d$ for this case.

According to (5), the number of solutions of $g(y)=0$ is equal to that of $z^{2^k+1}\oplus\zeta z\oplus\zeta=0$. Suppose that N_j denote the number of $\zeta\in\mathbb{L}^*$ such that $z^{2^k+1}\oplus\zeta z\oplus\zeta=0$ has exactly j roots in $\mathbb{L}$, where $j=0,1,2,2^d+1$. Then by Lemma 6, one has

$$N_0=\frac{2^{d-1}(2^m+1)}{2^d+1},\qquad N_1=2^{m-d}-1$$
$$N_2=\frac{(2^{d-1}-1)(2^m-1)}{2^d-1},\qquad N_{2^d+1}=\frac{2^{m-d}-1}{2^{2d}-1}.$$

Note that $\zeta=\frac{c^{2^{k+1}(2^k+1)}}{b^{2^{k+1}}}$. By Lemma 5, $\gcd(2^m-1,2^k+1)=1$ since m/d is odd. Thus, for any fixed $b\in\mathbb{L}^*$, ζ runs through $\mathbb{L}^*$ when c runs through $\mathbb{L}^*$. Therefore, ζ runs through $\mathbb{L}^*$ 2^m-1 times when (b,c) ranges over $\mathbb{L}^*\times\mathbb{L}^*$. This together with the cases for $b=0$ or $c=0$, result in

$$\begin{aligned}|\mathcal{R}_0|&=(2^m-1)+(2^m-1)(N_0+N_2)\\&=\frac{(2^m-1)\left(2^{m+2d}-2^{m+d}-2^m+2^{2d}\right)}{2^{2d}-1}.\end{aligned}$$

Similarly, we have

$$|\mathcal{R}_d|=(2^m-1)2^{m-d}$$
$$|\mathcal{R}_{2d}|=\frac{(2^m-1)(2^{m-d}-1)}{2^{2d}-1}$$

respectively. This finishes the proof. □

IV. Distribution of the Exponential Sum $\rho(a,b)$

In this section, the distribution of the exponential sum $\rho(a,b)$ defined by (1) is completely determined by the rank distribution of $Q_{b,c}(x)$ and the theory of $\mathbb{Z}_4$-valued quadratic forms.

Let $a=c+2c'$, $c,c'\in\mathbb{L}$. Then by (1), the exponential sum $\rho(a,b)$ can be rewritten as

$$\begin{aligned}\rho(a,b)&=\xi(b,c,c')\\&=\sum_{x\in\mathbb{L}} i^{Tr\left(cx+2bx^{1+2^k}\right)}(-1)^{tr(c'x)}\\&=\sum_{x\in\mathbb{L}} i^{Q_{b,c}(x)}(-1)^{tr\left(c'x\right)},\end{aligned}$$

where $Q_{b,c}(x)=Tr(2bx^{1+2^k}+cx)$. Note that $Q_{b,c}(x)$ is alternating if and only if $c=0$.

Theorem 1: When (a,b) runs through $\mathbb{R}\times\mathbb{L}$, the distribution of the exponential sum $\rho(a,b)$ is given in Tables I and II for odd m and even m respectively.

Proof: Herein we only give the proof for odd m since the case for even m can be similarly proven. The values of the exponential sum $\rho(a,b)=\xi(b,c,c')$ can be calculated as follows.

Case 1 $b=0$ and $c=0$.

TABLE I
VALUE DISTRIBUTION OF $\rho(a,b)$ FOR ODD m

Value	Frequency
2^m	1
0	$(2^m-1)(\frac{2^{2m}+2^{2m-3d}}{2^d+1}-2^{m-2d}+1)$
$\pm(1+i)2^{\frac{m-1}{2}}$	$(2^m-1)(2^{m-2}\pm 2^{\frac{m-3}{2}})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$\pm(1-i)2^{\frac{m-1}{2}}$	$(2^m-1)(2^{m-2}\pm 2^{\frac{m-3}{2}})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$\pm 2^{\frac{m+d}{2}}$	$(2^m-1)((2^{m-d-2}\pm 2^{\frac{m-d}{2}-1})2^{m-d}+2^{m-d-2})$
$\pm 2^{\frac{m+d}{2}}i$	$(2^m-1)(2^{m-d}-1)2^{m-d-2}$(each)
$\pm(1+i)2^{\frac{m+2d-1}{2}}$	$(2^m-1)(2^{m-2d-2}\pm 2^{\frac{m-2d-3}{2}})\frac{2^{m-d}-1}{2^{2d}-1}$
$\pm(1-i)2^{\frac{m+2d-1}{2}}$	$(2^m-1)(2^{m-2d-2}\pm 2^{\frac{m-2d-3}{2}})\frac{2^{m-d}-1}{2^{2d}-1}$

TABLE II
VALUE DISTRIBUTION OF $\rho(a,b)$ FOR EVEN m

Value	Frequency
2^m	1
0	$(2^m-1)(\frac{2^{2m}+2^{2m-3d}}{2^d+1}-2^{m-2d}+1)$
$\pm 2^{\frac{m}{2}}$	$(2^m-1)(2^{m-2}\pm 2^{\frac{m}{2}-1})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$\pm 2^{\frac{m}{2}}i$	$(2^m-1)\frac{2^{m-2}(2^{m+2d}-2^{m+d}-2^m+2^{2d})}{2^{2d}-1}$(each)
$\pm 2^{\frac{m+d}{2}}$	$(2^m-1)((2^{m-d-2}\pm 2^{\frac{m-d}{2}-1})2^{m-d}+2^{m-d-2})$
$\pm 2^{\frac{m+d}{2}}i$	$(2^m-1)(2^{m-d}-1)2^{m-d-2}$(each)
$\pm 2^{\frac{m+2d}{2}}$	$(2^m-1)(2^{m-2d-2}\pm 2^{\frac{m-2d}{2}-1})\frac{2^{m-d}-1}{2^{2d}-1}$
$\pm 2^{\frac{m+2d}{2}}i$	$(2^m-1)\frac{2^{m-2d-2}(2^{m-d}-1)}{2^{2d}-1}$(each)

TABLE III
LEE WEIGHT DISTRIBUTION OF $\mathcal{C}^k$ FOR ODD m

Lee Weight	Frequency
0	1
2^m	$(2^m-1)(\frac{2^{2m}+2^{2m-3d}}{2^d+1}-2^{m-2d}+(2^{m-d}-1)2^{m-d-1}+1)$
$2^m\pm 2^{\frac{m-1}{2}}$	$(2^m-1)(2^{m-1}\mp 2^{\frac{m-1}{2}})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$2^m\pm 2^{\frac{m+d}{2}}$	$(2^m-1)((2^{m-d-2}\mp 2^{\frac{m-d}{2}-1})2^{m-d}+2^{m-d-2})$
$2^m\pm 2^{\frac{m+2d-1}{2}}$	$(2^m-1)(2^{m-2d-1}\mp 2^{\frac{m-2d-1}{2}})\frac{2^{m-d}-1}{2^{2d}-1}$

This is a trivial case, one can easily obtain

$$\xi(0,0,c')=\sum_{x\in\mathbb{L}}(-1)^{tr(c'x)}=\begin{cases}0, & if\ c'\neq 0\\ 2^m, & if\ c'=0.\end{cases}\tag{6}$$

Case 2 $b\neq 0$ and $c=0$.

For $c=0$, $Q_{b,0}(x)$ is alternating and the rank of $Q_{b,0}(x)$ is $m-d$ for any $b\in\mathbb{L}^*$. Then by the fact $m-d=d(\frac{m}{d}-1)$ is even and Lemma 3, one can deduce that the exponential sum $\xi(b,0,c')$ has the following distribution

$$\begin{cases}\pm 2^{\frac{m+d}{2}}, & (2^m-1)\left(2^{m-d-1}\pm 2^{\frac{m-d}{2}-1}\right)\ \text{times}\\ 0, & (2^m-1)\left(2^m-2^{m-d}\right)\ \text{times.}\end{cases}\tag{7}$$

when (b,c') runs through $\mathbb{L}^*\times\mathbb{L}$.

Case 3 $b=0$ and $c\neq 0$.

If $b=0$, the rank of $Q_{0,c}(x)$ is m for any $c\in\mathbb{L}^*$. In this case, $Q_{0,c}(x)$ is nonalternating, then by Lemma 4, when (c,c') runs through $\mathbb{L}^*\times\mathbb{L}$, $\xi(0,c,c')$ has the following distribution

$$\begin{cases}\pm(1+i)2^{\frac{m-1}{2}}, & (2^m-1)(2^{m-2}\pm 2^{\frac{m-3}{2}})\,\text{times}\\ \pm(1-i)2^{\frac{m-1}{2}}, & (2^m-1)(2^{m-2}\pm 2^{\frac{m-3}{2}})\,\text{times.}\end{cases}\tag{8}$$

Case 4 $b\neq 0$ and $c\neq 0$.

For $bc\neq 0$, the rank of $Q_{b,c}(x)$ is m, $m-d$ or $m-2d$. Note that $m-d$ is even and $m-2d$ is odd if m is odd.

TABLE IV
LEE WEIGHT DISTRIBUTION OF $\mathcal{C}^k$ FOR EVEN m

Lee Weight	Frequency
0	1
2^m	$(2^m-1)(2^{2m-1}+2^{m-1}+2^{m-3d-1}(\frac{2^{m+3d}+2^m}{2^d+1}-2^{2d}-2^d)+1)$
$2^m \pm 2^{\frac{m}{2}}$	$(2^m-1)(2^{m-2} \mp 2^{\frac{m}{2}-1})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$2^m \pm 2^{\frac{m+d}{2}}$	$(2^m-1)((2^{m-d-2} \mp 2^{\frac{m-d}{2}-1})2^{m-d}+2^{m-d-2})$
$2^m \pm 2^{\frac{m+2d}{2}}$	$(2^m-1)(2^{m-2d-2} \mp 2^{\frac{m-2d}{2}-1})\frac{2^{m-d}-1}{2^{2d}-1}$

This fact together with Lemma 4 and Proposition 1 imply that when (b,c) runs through $\mathcal{R}_0\backslash\{(0,c): c\in\mathbb{L}^*\}$ and c' runs through $\mathbb{L}$, $\xi(b,c,c')$ has the distribution

$$\begin{cases} \pm(1+i)2^{\frac{m-1}{2}}, & (|\mathcal{R}_0|-2^m+1)\left(2^{m-2}\pm 2^{\frac{m-3}{2}}\right) \text{ times} \\ \pm(1-i)2^{\frac{m-1}{2}}, & (|\mathcal{R}_0|-2^m+1)\left(2^{m-2}\pm 2^{\frac{m-3}{2}}\right) \text{ times}. \end{cases}$$

Similarly, when (b,c) runs through $\mathcal{R}_d\backslash\{(b,0): b\in\mathbb{L}^*\}$ and c' runs through $\mathbb{L}$, one can deduce that $\xi(b,c,c')$ has the distribution

$$\begin{cases} 0, & (|\mathcal{R}_d|-2^m+1)\left(2^m-2^{m-d}\right) \text{ times} \\ \pm 2^{\frac{m+d}{2}}, & (|\mathcal{R}_d|-2^m+1)\left(2^{m-d-2}\pm 2^{\frac{m-d}{2}-1}\right) \text{ times} \\ \pm 2^{\frac{=m+d}{2}}i, & (|\mathcal{R}_d|-2^m+1)\,2^{m-d-2} \text{ times (each)}. \end{cases}$$

and when (b,c) runs through $\mathcal{R}_{2d}$ and c' runs through $\mathbb{L}$, $\xi(b,c,c')$ has the distribution

$$\begin{cases} 0, & (2^m-2^{m-2d})|\mathcal{R}_{2d}| \text{ times} \\ \pm(1+i)2^{\frac{m+2d-1}{2}}, & (2^{m-2d-2}\pm 2^{\frac{m-2d-3}{2}})|\mathcal{R}_{2d}| \text{ times} \\ \pm(1-i)2^{\frac{m+2d-1}{2}}, & (2^{m-2d-2}\pm 2^{\frac{m-2d-3}{2}})|\mathcal{R}_{2d}| \text{ times}. \end{cases}$$

respectively.

Hence, combining Cases 1–4 and Proposition 1, the theorem follows. This finishes the proof. □

We have determined the distribution of the exponential sum $\rho(a,b)$ in a uniform way, which generalizes the cases discussed in [5] and [8].

V. SEVERAL CLASSES OF CODES AND THEIR WEIGHT DISTRIBUTIONS

As an application of the exponential sum $\rho(a,b)$, firstly we are able to determine the Lee and Hamming weight distributions of a class of quaternary codes and the Hamming weight distributions of the corresponding binary codes obtained by the MSB and Gray maps.

A. Quaternary Code $\mathcal{C}^k$ and its Lee Weight Distribution

The Lee weight of an element $a \in \mathbb{Z}_4$ is defined as $w_L(a) = 1-\mathfrak{Re}(i^a)$. Then, the Lee weight of a codeword $\mathbf{c}=(\mathbf{c}_1,\mathbf{c}_2,\ldots,\mathbf{c}_n)$ is

$$w_L(\mathbf{c}) = n-\mathfrak{Re}\left(\sum_{j=1}^{n} i^{\mathbf{c}_j}\right).$$

Define a quaternary code as

$$\mathcal{C}^k = \{\mathbf{c}(a,b): a\in\mathbb{R}, b\in\mathbb{L}\} \tag{9}$$

TABLE V
HAMMING WEIGHT DISTRIBUTION OF $\mathcal{C}^k$ FOR ODD m

Hamming Weight	Frequency
0	1
2^{m-1}	$(2^m-1)(2^m-2^{m-d}+1)$
$2^{m-1}\pm 2^{\frac{m+d}{2}-1}$	$(2^m-1)(2^{m-d-1}\mp 2^{\frac{m-d}{2}-1})$
$3\cdot 2^{m-2}$	$(2^m-1)(2^{m-d}-1)(2^m-2^{m-d-1}+2^{m-2d})$
$3\cdot 2^{m-2}\pm 2^{\frac{m-3}{2}}$	$(2^m-1)(2^{m-1}\mp 2^{\frac{m-1}{2}})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$3\cdot 2^{m-2}\pm 2^{\frac{m+d}{2}-1}$	$(2^m-1)(2^{m-d}-1)(2^{m-d-2}\mp 2^{\frac{m-d}{2}-1})$
$3\cdot 2^{m-2}\pm 2^{\frac{m+2d-3}{2}}$	$(2^m-1)(2^{m-2d-1}\mp 2^{\frac{m-2d-1}{2}})\frac{2^{m-d}-1}{2^{2d}-1}$

where $\mathbf{c}(a,b)=(Tr(ax+2bx^{2^k+1}))_{x\in\mathbb{L}}$. By the definition of Lee weight, one has

$$w_L(\mathbf{c}(a,b)) = 2^m-\mathfrak{Re}\left(\sum_{x\in\mathbb{L}} i^{Tr\left(ax+2bx^{2^k+1}\right)}\right). \tag{10}$$

Then the Lee weight distribution of $\mathcal{C}^k$ follows from Theorem 1 and (10).

Theorem 2: When (a,b) runs through $\mathbb{R}\times\mathbb{L}$, the Lee weight distribution of $\mathcal{C}^k$ is given as in Tables III and IV for odd m and even m, respectively.

Remark 2: The Lee weight distribution of $\{\mathbf{c}(u,a,b) = (u+Tr(ax+2bx^{2^k+1}))_{x\in\mathbb{L}} : u\in\mathbb{Z}_4, a\in\mathbb{R}, b\in\mathbb{L}\}$ for odd m and $\gcd(m,k)=1$ was determined in [5]. Note that $w_L(\mathbf{c}(u,a,b)) = 2^m-\mathfrak{Re}(i^u\rho(a,b))$. Thus, based on the distribution of $\rho(a,b)$, we can easily extend the results in [5] by a different approach.

B. Quaternary Code $\mathcal{C}^k$ and its Hamming Weight Distribution

The Hamming weight of a codeword $\mathbf{c}=(\mathbf{c}_1,\mathbf{c}_2,\ldots,\mathbf{c}_n)$ is defined as the number of nonzero $\mathbf{c}_j$ for $1\le j\le n$, and is denoted by $w_H(\mathbf{c})$. In this subsection, we determine the Hamming weight distribution of the quaternary code $\mathcal{C}^k$ defined by (9).

The Hamming weight of the codeword $\mathbf{c}(a,b)\in\mathcal{C}^k$ can be expressed as

$$\begin{aligned} w_H(\mathbf{c}(a,b)) &= 2^m-|\{x\in\mathbb{L}:\mathbf{c}(a,b)=0\}| \\ &= 2^m-\frac{1}{4}\sum_{x\in\mathbb{L}}\sum_{\lambda\in\mathbb{Z}_4} i^{\lambda\mathbf{c}(a,b)} \\ &= 2^m-\frac{1}{4}\sum_{\lambda\in\mathbb{Z}_4}\sum_{x\in\mathbb{L}} i^{Tr\left(\lambda ax+2\lambda bx^{1+2^k}\right)} \\ &= 2^m-\frac{1}{4}\sum_{\lambda\in\mathbb{Z}_4}\rho(\lambda a,\lambda b). \end{aligned}$$

TABLE VI
HAMMING WEIGHT DISTRIBUTION OF $\mathcal{C}^k$ FOR EVEN m

Hamming Weight	Frequency
0	1
2^{m-1}	$(2^m-1)(2^m-2^{m-d}+1)$
$2^{m-1}\pm 2^{\frac{m+d}{2}-1}$	$(2^m-1)(2^{m-d-1}\mp 2^{\frac{m-d}{2}-1})$
$3\cdot 2^{m-2}$	$(2^m-1)2^{m-3d-1}\Big((2^m-1)2^{3d}+(2^m+1)(2^{2d}-2^d)+2^m\Big)$
$3\cdot 2^{m-2}\pm 2^{\frac{m}{2}-1}$	$(2^m-1)(2^{m-2}\mp 2^{\frac{m}{2}-1})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$3\cdot 2^{m-2}\pm 2^{\frac{m+d}{2}-1}$	$(2^m-1)(2^{m-d}-1)(2^{m-d-2}\mp 2^{\frac{m-d}{2}-1})$
$3\cdot 2^{m-2}\pm 2^{\frac{m+2d}{2}-1}$	$(2^m-1)(2^{m-2d-2}\mp 2^{\frac{m-2d}{2}-1})\frac{2^{m-d}-1}{2^{2d}-1}$

Note that $\rho(3a,3b)=\overline{\rho(a,b)}$, where $\bar{\cdot}$ denotes the complex conjugate. Then we have

$$w_H(\mathbf{c}(a,b))=3\cdot 2^{m-2}-\frac{1}{2}\mathfrak{Re}(\rho(a,b))-\frac{1}{4}\rho(2a,2b).$$

In what follows, we only consider the weight distribution of $\mathcal{C}^k$ for odd m because the case for even m can be obtained in the same manner.

Suppose that $a=c+2c'$, $c,c'\in\mathbb{L}$, then $\rho(2a,2b)=2^m$ if $c=0$ and $\rho(2a,2b)=0$ otherwise. Thus, one has

$$w_H(\mathbf{c}(a,b))=2^{m-1}-\frac{1}{2}\mathfrak{Re}(\rho(a,b)) \tag{11}$$

if $c=0$, and for $c\neq 0$, one can get

$$w_H(\mathbf{c}(a,b))=3\cdot 2^{m-2}-\frac{1}{2}\mathfrak{Re}(\rho(a,b)). \tag{12}$$

Applying (11) to (6) and (7), when $c=0$ the weight distribution of $\mathcal{C}^k$ is

$$\begin{cases} 0, & 1 \text{ time} \\ 2^{m-1}, & (2^m-1)(2^m-2^{m-d}+1) \text{ times} \\ 2^{m-1}\mp 2^{\frac{m+d-2}{2}}, & (2^m-1)\frac{(2^{m-d}\pm 2^{\frac{m-d}{2}})}{2} \text{ times}. \end{cases} \tag{13}$$

Subsequently applying (12) to the distribution of $\rho(a,b)$ for $c\neq 0$, the weight distribution of $\mathcal{C}^k$ when $c\neq 0$ is

$$\begin{cases} 3\cdot 2^{m-2}, & \left(2^m-2^{m-d-1}+2^{m-2d}\right) \\ & (2^m-1)\left(2^{m-d}-1\right) \text{ times} \\ 3\cdot 2^{m-2}\mp 2^{\frac{m-3}{2}}, & (2^m-1)\left(2^{m-1}\pm 2^{\frac{m-1}{2}}\right) \\ & \frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1} \text{ times} \\ 3\cdot 2^{m-2}\mp 2^{\frac{m+d}{2}-1}, & (2^m-1)\left(2^{m-d}-1\right) \\ & \left(2^{m-d-2}\pm 2^{\frac{m-d}{2}-1}\right) \text{ times} \\ 3\cdot 2^{m-2}\mp 2^{\frac{m+2d-3}{2}}, & \left(2^{m-2d-1}\pm 2^{\frac{m-2d-1}{2}}\right) \\ & (2^m-1)\frac{2^{m-d}-1}{2^{2d}-1} \text{ times}. \end{cases} \tag{14}$$

Therefore, combining (13) and (14), the Hamming weight distribution of the quaternary code $\mathcal{C}^k$ is obtained.

Theorem 3: When (a,b) runs through $\mathbb{R}\times\mathbb{L}$, the Hamming weight distribution of $\mathcal{C}^k$ is given in Tables V and VI for odd m and even m, respectively.

C. Binary Code $\pi(\mathcal{C}^k)$ and its Hamming Weight Distribution

In this subsection, assume that $m>3$ and we consider the binary code obtained from $\mathcal{C}^k$ under the MSB map.

Let $\pi(\mathbf{c})=(\pi(\mathbf{c}_1),\pi(\mathbf{c}_2),\ldots,\pi(\mathbf{c}_n))$ for $\mathbf{c}=(\mathbf{c}_1,\mathbf{c}_2,\ldots,\mathbf{c}_n)\in\mathcal{C}^k$, and define

$$\pi(\mathcal{C}^k)=\{\pi(\mathbf{c}(a,b)):a\in\mathbb{R},b\in\mathbb{L}\}$$

where $\mathbf{c}(a,b)=(Tr(ax+2bx^{1+2^k}))_{x\in\mathbb{L}}$.

To determine the Hamming weight distribution of $\pi(\mathcal{C}^k)$, define

$$N_{a,b}(t)=\left|\{x\in\mathbb{L}:\ Tr(ax+2bx^{1+2^k})=t\}\right|$$

for $a\in\mathbb{R}$, $b\in\mathbb{L}$ and $t\in\mathbb{Z}_4$. Then the Hamming weight of $\pi(\mathbf{c}(a,b))\in\pi(\mathcal{C}^k)$ is

$$w_H\left(\pi(\mathbf{c}(a,b))\right)=N_{a,b}(2)+N_{a,b}(3). \tag{15}$$

In addition, the exponential sum can be rewritten as

$$\rho(a,b)=\sum_{x\in\mathbb{L}} i^{Tr\left(ax+2bx^{1+2^k}\right)}=\sum_{t\in\mathbb{Z}_4}N_{a,b}(t)i^t.$$

Then one gets

$$\begin{cases} N_{a,b}(0)-N_{a,b}(2)=\mathfrak{Re}(\rho(a,b)) \\ N_{a,b}(1)-N_{a,b}(3)=\mathfrak{Im}(\rho(a,b)) \\ N_{a,b}(0)+N_{a,b}(1)+N_{a,b}(2)+N_{a,b}(3)=2^m \end{cases}$$

associated with (15) which gives

$$w_H\left(\pi(\mathbf{c}(a,b))\right)=2^{m-1}-\frac{\mathfrak{Re}\left(\rho(a,b)\right)+\mathfrak{Im}\left(\rho(a,b)\right)}{2}.$$

Thus, the Hamming weight distribution of $\pi(\mathcal{C}^k)$ follows from Theorem 1.

Theorem 4: When (a,b) runs through $\mathbb{R}\times\mathbb{L}$, the Hamming weight distribution of the binary code $\pi(\mathcal{C}^k)$ is given in Tables VII and VIII for odd m and even m respectively.

D. Binary Code $\phi(\mathcal{C}^k)$ and Its Hamming Weight Distribution

For the Gray map, let $\phi(\mathbf{c})=(\phi(\mathbf{c}_1),\phi(\mathbf{c}_2),\ldots,\phi(\mathbf{c}_n))$ for $\mathbf{c}=(\mathbf{c}_1,\mathbf{c}_2,\ldots,\mathbf{c}_n)\in\mathcal{C}^k$, and define

$$\phi(\mathcal{C}^k)=\{\phi(\mathbf{c}(a,b)):a\in\mathbb{R},b\in\mathbb{L}\}$$

where $\mathbf{c}(a,b)=(Tr(ax+2bx^{1+2^k}))_{x\in\mathbb{L}}$.

TABLE VII
HAMMING WEIGHT DISTRIBUTION OF $\pi(\mathcal{C}^k)$ FOR ODD m

Hamming Weight	Frequency
0	1
2^{m-1}	$(2^m-1)\Big((2^m+1)(2^{m-1}-2^{m-2d-1})+\frac{2^{2m-1}+2^{2m-3d-1}}{2^d+1}+1\Big)$
$2^{m-1}\pm 2^{\frac{m-1}{2}}$	$(2^m-1)(2^{m-2}\mp 2^{\frac{m-3}{2}})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$2^{m-1}\pm 2^{\frac{m+d}{2}-1}$	$(2^m-1)2^{m-d}(2^{m-d-1}\mp 2^{\frac{m-d}{2}-1})$
$2^{m-1}\pm 2^{\frac{m+2d-1}{2}}$	$(2^m-1)(2^{m-2d-2}\mp 2^{\frac{m-2d-3}{2}})\frac{2^{m-d}-1}{2^{2d}-1}$

TABLE VIII
HAMMING WEIGHT DISTRIBUTION OF $\pi(\mathcal{C}^k)$ FOR EVEN m

Hamming Weight	Frequency
0	1
2^{m-1}	$(2^m-1)(\frac{2^{2m}+2^{2m-3d}}{2^d+1}-2^{m-2d}+1)$
$2^{m-1}\pm 2^{\frac{m}{2}-1}$	$(2^m-1)(2^{m-1}\mp 2^{\frac{m}{2}-1})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$2^{m-1}\pm 2^{\frac{m+d}{2}-1}$	$(2^m-1)2^{m-d}(2^{m-d-1}\mp 2^{\frac{m-d}{2}-1})$
$2^{m-1}\pm 2^{\frac{m+2d}{2}-1}$	$(2^m-1)(2^{m-2d-1}\mp 2^{\frac{m-2d}{2}-1})\frac{2^{m-d}-1}{2^{2d}-1}$

It is well-known that [6]

$$w_H\left(\phi(\mathbf{c}(a,b))\right)=w_L\left(\mathbf{c}(a,b)\right)=2^m-\mathfrak{Re}\left(\rho(a,b)\right).$$

Therefore, the Hamming weight distribution of $\phi(\mathcal{C}^k)$ is the same as the Lee weight distribution of $\mathcal{C}^k$, so we omit the Hamming weight distribution of $\phi(\mathcal{C}^k)$ here.

VI. SEVERAL SEQUENCE FAMILIES AND THEIR CORRELATION DISTRIBUTIONS

In this section, by choosing cyclicly inequivalent codewords from the codes obtained above, we are also able to obtain some sequence families and completely determine the correlation distributions based on the distribution of the exponential sum $\rho(a,b)$.

A. Quaternary Sequence Family $\mathcal{U}^k$ and its Correlation Distribution

For $\gamma=(\gamma_0,\gamma_1)\in\mathbb{R}\times\mathbb{L}$, define the quaternary sequence $\{\mathbf{s}_\gamma(t)\}_{t=0}^{\infty}$ by

$$\mathbf{s}_\gamma(t)=Tr\left(\gamma_0\beta^t\right)+2Tr\left(\gamma_1\beta^{(2^k+1)t}\right) \tag{16}$$

where β is a primitive element in $\mathbb{L}$. Note that $\gcd(2^m-1,2^k+1)=1$ by Lemma 5. Thus, the least positive period of $\{\mathbf{s}_\gamma(t)\}$ is 2^m-1 for any $\gamma=(\gamma_0,\gamma_1)\neq(0,0)\in\mathbb{R}\times\mathbb{L}$.

Two sequences $\{\mathbf{s}_\gamma(t)\}$ and $\{\mathbf{s}_{\gamma'}(t)\}$ are cyclically equivalent if there exists an integer τ such that $\{\mathbf{s}_\gamma(t+\tau)\}=\{\mathbf{s}_{\gamma'}(t)\}$. This equivalence relation partitions $\{\mathbb{R}\times\mathbb{L}\}\setminus\{(0,0)\}$ into $(2^{3m}-1)/(2^m-1)=2^{2m}+2^m+1$ equivalent classes. Define $P(m)$ to be the set formed by choosing one element from each equivalent class. Clearly

$$|P(m)|=2^{2m}+2^m+1 \tag{17}$$

and such that any two sequences $\{\mathbf{s}_\gamma(t)\}$ and $\{\mathbf{s}_{\gamma'}(t)\}$ are not cyclically equivalent if $\gamma,\gamma'\in P(m)$.

A family $\mathcal{U}^k$ of the quaternary sequences is defined by

$$\mathcal{U}^k=\{\{\mathbf{s}_\gamma(t)\}:\gamma\in P(m)\}.$$

For two quaternary sequences $\{\mathbf{s}_\gamma(t)\},\{\mathbf{s}_{\gamma'}(t)\}\in\mathcal{U}^k$, their correlation at shift τ is

$$\begin{aligned}R_{\mathbf{s}_\gamma,\mathbf{s}_{\gamma'}}(\tau)&=\sum_{t=0}^{2^m-2}i^{Tr\left(z_0\beta^t\right)+2Tr\left(z_1\beta^{(2^k+1)t}\right)}\\&=\rho\left(z_0,z_1\right)-1\end{aligned}$$

where $z_0=\gamma_0\beta^\tau-\gamma_0'$ and $z_1=\gamma_1\beta^{(2^k+1)\tau}\oplus\gamma_1'$.

Given $z=(z_0,z_1)\in\mathbb{R}\times\mathbb{L}$, consider the number of solutions $(\gamma,\gamma')\in P(m)\times P(m)$ and $0\le\tau<2^m-1$ to

$$\begin{cases}z_0=&\gamma_0\beta^\tau-\gamma_0',\\z_1=&\gamma_1\beta^{(2^k+1)\tau}\oplus\gamma_1'.\end{cases}$$

Clearly, for arbitrary fixed $\gamma_0'\neq-z_0$ (resp. $\gamma_1'\neq z_1$) and fixed $0\le\tau<2^m-1$, there exists exactly one $\gamma_0\in\mathbb{R}$ (resp. $\gamma_1\in\mathbb{L}$) satisfying the above equations system. That is, when (γ,γ') runs through $P(m)\times P(m)$ and τ varies from 0 to 2^m-2, $-z=\gamma'-\gamma$ ranges over $P(m)$ $2^{2m}+2^m$ times, and $(\mathbb{R}\times\mathbb{L})\backslash P(m)$ $2^{2m}+2^m+1$ times.

Next, assume that κ is a complex value and N_κ is the number of the occurrence of $\rho(a,b)=\kappa$ when (a,b) ranges over $(\mathbb{R}\times\mathbb{L})\backslash\{(0,0)\}$. Since $\rho(a\beta^\tau,b\beta^{(2^k+1)\tau})=\rho(a,b)$ for all $0\le\tau<2^m-1$, it follows from the definition of $P(m)$ that $\rho(z_0,z_1)=\kappa$ occurs $N_\kappa/(2^m-1)$ times when (z_0,z_1) runs through $P(m)$, and $(2^m-2)N_\kappa/(2^m-1)$ times when (z_0,z_1) runs through $(\mathbb{R}\times\mathbb{L}\setminus\{(0,0)\})\backslash P(m)$. Therefore, when (γ,γ') runs through $P(m)\times P(m)$ and τ varies from 0 to 2^m-2, $\rho(z_0,z_1)=\kappa$ occurs

$$\frac{\left(2^{2m}+2^m\right)\times N_\kappa+\left(2^{2m}+2^m+1\right)\times(2^m-2)N_\kappa}{2^m-1}=\frac{2^{3m}-2}{2^m-1}N_\kappa$$

times for any $(z_0,z_1)\in\mathbb{R}\times\mathbb{L}\setminus\{(0,0)\}$. Specially, $\rho(z_0,z_1)=\rho(0,0)$ occurs $2^{2m}+2^m+1$ times since $(0,0)\notin P(m)$.

Then by Theorem 1, the correlation distribution of the quaternary sequence family $\mathcal{U}^k$ is as follows.

Theorem 5: The correlation distribution of family $\mathcal{U}^k$ is given in Tables IX and X for odd m and even m respectively.

Remark 3: The correlation distribution of family $\mathcal{U}^k$ for odd m and $k=1$ had been determined in [8] and [11] by different methods. In this paper, based on the techniques developed in [1] and [11], we can generalize the family to $\mathcal{U}^k$ for positive integers m and k with $m/\gcd(m,k)$ being odd.

TABLE IX
CORRELATION DISTRIBUTION OF FAMILY $\mathcal{U}^k$ FOR ODD m

Value	Frequency
$-1+2^m$	$2^{2m}+2^m+1$
-1	$(2^{3m}-2)(\frac{2^{2m}+2^{2m-3d}}{2^d+1}-2^{m-2d}+1)$
$-1\pm(1+i)2^{\frac{m-1}{2}}$	$(2^{3m}-2)(2^{m-2}\pm 2^{\frac{m-3}{2}})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$-1\pm(1-i)2^{\frac{m-1}{2}}$	$(2^{3m}-2)(2^{m-2}\pm 2^{\frac{m-3}{2}})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$-1\pm 2^{\frac{m+d}{2}}$	$(2^{3m}-2)[(2^{m-d-2}\pm 2^{\frac{m-d}{2}-1})2^{m-d}+2^{m-d-2}]$
$-1\pm 2^{\frac{m+d}{2}}i$	$(2^{3m}-2)(2^{m-d}-1)2^{m-d-2}$(each)
$-1\pm(1+i)2^{\frac{m+2d-1}{2}}$	$(2^{3m}-2)(2^{m-2d-2}\pm 2^{\frac{m-2d-3}{2}})\frac{2^{m-d}-1}{2^{2d}-1}$
$-1\pm(1-i)2^{\frac{m+2d-1}{2}}$	$(2^{3m}-2)(2^{m-2d-2}\pm 2^{\frac{m-2d-3}{2}})\frac{2^{m-d}-1}{2^{2d}-1}$

TABLE X
CORRELATION DISTRIBUTION OF FAMILY $\mathcal{U}^k$ FOR EVEN m

Value	Frequency
$-1+2^m$	$2^{2m}+2^m+1$
-1	$(2^{3m}-2)(\frac{2^{2m}+2^{2m-3d}}{2^d+1}-2^{m-2d}+1)$
$-1\pm 2^{\frac{m}{2}}$	$(2^{3m}-2)(2^{m-2}\pm 2^{\frac{m}{2}-1})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$-1\pm 2^{\frac{m}{2}}i$	$(2^{3m}-2)\frac{2^{m-2}(2^{m+2d}-2^{m+d}-2^m+2^{2d})}{2^{2d}-1}$(each)
$-1\pm 2^{\frac{m+d}{2}}$	$(2^{3m}-2)[(2^{m-d-2}\pm 2^{\frac{m-d}{2}-1})2^{m-d}+2^{m-d-2}]$
$-1\pm 2^{\frac{m+d}{2}}i$	$(2^{3m}-2)(2^{m-d}-1)2^{m-d-2}$(each)
$-1\pm 2^{\frac{m+2d}{2}}$	$(2^{3m}-2)(2^{m-2d-2}\pm 2^{\frac{m-2d}{2}-1})\frac{2^{m-d}-1}{2^{2d}-1}$
$-1\pm 2^{\frac{m+2d}{2}}i$	$(2^{3m}-2)\frac{2^{m-2d-2}(2^{m-d}-1)}{2^{2d}-1}$(each)

B. Binary Sequence Family Obtained From the MSB Map

Let $\pi(\mathbf{s}) = (\pi(\mathbf{s}_1), \pi(\mathbf{s}_2), \ldots, \pi(\mathbf{s}_n))$ for $\mathbf{s} = (\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_n) \in \mathbb{Z}_4^n$. Clearly, for two sequences $\mathbf{s}_\gamma(t)$ and $\mathbf{s}_{\gamma'}(t)$ defined by (16), we have $\pi(\mathbf{s}_\gamma(t)) = \pi(\mathbf{s}_{\gamma'}(t+\tau))$ if there exists an integer τ such that $\mathbf{s}_\gamma(t) = \mathbf{s}_{\gamma'}(t+\tau)$. Thus, define a binary sequence family as

$$\pi\left(\mathcal{U}^k\right) = \{\pi\left(\mathbf{s}_\gamma(t)\right) : \gamma \in P(m)\}$$

where $\mathbf{s}_\gamma(t)$ and $P(m)$ are defined by (16) and (17), respectively.

In order to investigate the properties of the family $\pi(\mathcal{U}^k)$, we need the representation of the set $P(m)$. Definitely, one can verify that $P(m)$ can be expressed as

$$P(m) = P_1(m) \cup P_2(m) \cup P_3(m)$$

where $P_1(m) = \{\gamma = (1+2v, b) : b, v \in \mathbb{L}\}$, $P_2(m) = \{\gamma = (2v, 1) : v \in \mathbb{L}\}$ and $P_3(m) = \{\gamma = (2, 0)\}$.

For two sequences $\pi(\mathbf{s}_\gamma(t)), \pi(\mathbf{s}_{\gamma'}(t)) \in \pi(\mathcal{U}^k)$, by Lemma 1 their correlation is determined by $R_{\mathbf{s}_\gamma, \mathbf{s}_{\gamma'}}(\tau)$ and $R_{3\mathbf{s}_\gamma, \mathbf{s}_{\gamma'}}(\tau)$, where $\gamma, \gamma' \in P(m)$. Note that $3\mathbf{s}_\gamma(t) \in \mathcal{U}^k$ if $\mathbf{s}_\gamma(t) \in \mathcal{U}^k$. Since the relations between $R_{\mathbf{s}_\gamma, \mathbf{s}_{\gamma'}}(\tau)$ and $R_{3\mathbf{s}_\gamma, \mathbf{s}_{\gamma'}}(\tau)$ are unknown, we can not obtain the correlation distribution from Lemma 1 and the correlation distribution of $\mathcal{U}^k$. However, we can give a bound on the nontrivial maximal correlation value of $\pi(\mathcal{U}^k)$.

Theorem 6: The nontrivial maximal correlation value of family $\pi(\mathcal{U}^k)$ is bounded by $2^{\frac{m+2d+1}{2}} + 1$ if m is odd and $2^{\frac{m+2d}{2}+1} + 1$ if m is even.

Remark 4: For odd m and $k = 1$, the correlation distribution of $\{\pi(\mathbf{s}_\gamma(t)) : \gamma \in P_1(m)\}$ is determined by Yu and Gong [23], and it was generalized to the family $\pi(\mathcal{U}^k)$ for odd m and any k with $\gcd(m, k) = 1$ by Zhou and Tang [25]. For the general case, it is still unknown.

C. Binary Sequence Family Obtained From the Modified Gray Map

In this subsection, a family of binary sequences with period $2(2^m - 1)$ is obtained under the modified Gray map, and the correlation distribution is determined by making use of the exponential sum.

Let β be a primitive element in $\mathbb{L}$ and $\eta \in \mathbb{L}$ with $tr(\eta) = 1$, define the quaternary sequence $\{\mathbf{s}_{\gamma,u}(t)\}_{t=0}^{\infty}$ as

$$\mathbf{s}_{\gamma,u}(t) = Tr((\eta + 2v)\beta^t) + 2Tr(b\beta^{(1+2^k)t}) + u$$

where $\gamma = (\eta + 2v, b) \in \mathbb{R} \times \mathbb{L}$, $u \in \mathbb{Z}_4$, $v \in \mathbb{H}$, and $\mathbb{H} = \{v \in \mathbb{L} : tr(v) = 0\}$.

By performing the modified Gray map on sequences $\mathbf{s}_{\gamma,u}(t)$, a family of binary sequences with period $2(2^m - 1)$ is obtained as follows:

$$\varphi(\mathcal{U}^k) = \left\{\varphi_{\mathbf{s}_{\gamma,u}}(t) : \gamma = (\eta + 2v, b), b \in \mathbb{L}, v \in \mathbb{H}, u \in \mathbb{Z}_2\right\}.$$

For odd m and $k = 1$, if one takes $\eta = 1$, then family $\varphi(\mathcal{U}^1) = \mathscr{V}(1)$, and its correlation distribution has been determined in [12]. In this paper, the correlation distribution of family $\varphi(\mathcal{U}^k)$ is completely determined for all positive integers m and k satisfying $m/\gcd(m, k)$ is odd. The key technique is to use distribution of $\rho(a, b)$, from which the correlation distribution can be similarly determined as in [12], [15], [16]. Hence, we just describe a sketch of the proof here, see [12], [15], [16] for more details.

For $j = 1, 2$, let $\gamma_j = (\eta + 2v_j, b_j), b_j \in \mathbb{L}, v_j \in \mathbb{H}, u_j \in \mathbb{Z}_2$, according to Lemma 2, the correlation function of the sequences $\varphi_{\mathbf{s}_{\gamma_1,u_1}}(t)$ and $\varphi_{\mathbf{s}_{\gamma_2,u_2}}(t)$ at shift τ, $0 \le \tau \le 2^{m+1} - 3$, is discussed as follows. For simplicity, define

$$\varsigma(\gamma, u) = 2 \cdot \mathfrak{Re}\left(\sum_{t=0}^{2^m-2} i^{\mathbf{s}_{\gamma,u}(t)}\right)$$

and let $\Delta_1 = \{(\eta + 2v, b) : v \in \mathbb{H}, b \in \mathbb{L}\}$ and $\Delta_2 = \{((\eta + 2v)\delta, b) : v \in \mathbb{H}, b \in \mathbb{L}, \delta \in \mathbb{L}\backslash\mathbb{Z}_2\}$.

For fixed $\gamma_2 \in \Delta_1$ and $u_1, u_2 \in \mathbb{Z}_2$, one gets

$$\begin{aligned}&\{\{\mathbf{s}_{\gamma_1,u_1}(t+\tau_0)\} - \{\mathbf{s}_{\gamma_2,u_2}(t)\} : \gamma_1 \in \Delta_1, 0 < \tau_0 \le 2^m - 2\}\\ &= \{\{\mathbf{s}_{\gamma_1,u_1}(t)\} - \{\mathbf{s}_{\gamma_2,u_2}(t)\} : \gamma_1 \in \Delta_2\}\\ &= \{\{\mathbf{s}_{\gamma_1-\gamma_2,u_1-u_2}(t)\} : \gamma_1 \in \Delta_2\}\end{aligned}$$

and

$$\begin{aligned}&\{\{3\mathbf{s}_{\gamma_1,u_1}(t+\tau_0+2^{m-1})\} - \{\mathbf{s}_{\gamma_2,u_2}(t)\} : \gamma_1 \in \Delta_1\\ &\qquad 0 \le \tau_0 \le 2^m - 2, \tau_0 \ne 2^{m-1} - 1\}\\ &= \{\{\mathbf{s}_{3\gamma_1-\gamma_2,3u_1-u_2}(t)\} : \gamma_1 \in \Delta_2\}\end{aligned}$$

Thus, it follows from Lemma 2 that the correlation distribution of $\varphi(\mathcal{U}^k)$ for $\tau \ne 0$ and $\tau \ne 2^m - 1$ is the distribution of the multiset

$$\begin{aligned}\{\varsigma\left(3^j\gamma_1 - \gamma_2, 3^j u_1 - u_2\right) : \gamma_1 \in \Delta_2, \gamma_2 \in \Delta_1,\\ u_1, u_2 \in \mathbb{Z}_2, j = 0, 1\}\end{aligned} \quad (18)$$

TABLE XI
CORRELATION DISTRIBUTION OF FAMILY $\varphi(\mathcal{U}^k)$ FOR ODD m.

Value	Frequency
$2(2^m-1)$	2^{2m}
0	$2^{2m}(2^m-2)(2^{m-d}-1)[\frac{2^{m+d}+2^{m-2d}}{2^d+1}+2^{m-d-1}]+2^{4m}$
-2	$3\cdot 2^{2m-2}(2^m-2)(2^{m-d}-1)(\frac{2^{m+d}+2^{m-2d}}{2^d+1}+2^{m-d-1})+2^{2m}[3\cdot 2^{m-2}(2^m-2^{m-d})+2^{m-d}-1]$
2	$2^{2m-2}(2^m-2)(2^{m-d}-1)(\frac{2^{m+d}+2^{m-2d}}{2^d+1}+2^{m-d-1})+2^{3m-2}(2^m-2^{m-d})$
$\pm 2^{\frac{m+1}{2}}$	$2^{3m-1}(2^m-2)\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$(each)
$\pm 2^{\frac{m+d}{2}+1}$	$2^{2m}(2^m-2)(2^{m-d}-1)2^{m-d-2}$(each)
$\pm 2^{\frac{m+2d+1}{2}}$	$2^{3m-2d-1}\frac{(2^m-2)(2^{m-d}-1)}{2^{2d}-1}$(each)
$\pm 2^{\frac{m+1}{2}}-2$	$3\cdot 2^{2m-2}(2^m-2)(2^{m-1}\pm 2^{\frac{m-1}{2}})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$\pm 2^{\frac{m+1}{2}}+2$	$2^{2m-2}(2^m-2)(2^{m-1}\mp 2^{\frac{m-1}{2}})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$\pm 2^{\frac{m+d}{2}+1}-2$	$2^{2m-2}(2^{m-d-2}\pm 2^{\frac{m-d}{2}-1})[3\cdot(2^m-2)(2^{m-d}-1)+3\cdot 2^m-4]+2^{3m-d-2}(3\cdot 2^{m-2}-1)$
$\pm 2^{\frac{m+d}{2}+1}+2$	$2^{2m-2}(2^{m-d-2}\mp 2^{\frac{m-d}{2}-1})[(2^m-2)(2^{m-d}-1)+2^m]+2^{4m-d-4}$
$\pm 2^{\frac{m+2d+1}{2}}-2$	$(2^m-2)(2^{m-2d-1}\pm 2^{\frac{m-2d-1}{2}})\frac{3\cdot 2^{2m-2}(2^{m-d}-1)}{2^{2d}-1}$
$\pm 2^{\frac{m+2d+1}{2}}+2$	$(2^m-2)(2^{m-2d-1}\mp 2^{\frac{m-2d-1}{2}})\frac{2^{2m-2}(2^{m-d}-1)}{2^{2d}-1}$

TABLE XII
CORRELATION DISTRIBUTION OF FAMILY $\varphi(\mathcal{U}^k)$ FOR EVEN m

Value	Frequency
$2(2^m-1)$	2^{2m}
0	$[2^{m+2d}(2^d+2)+2^{m-d}-2^{3d}-1]\frac{2^{3m-2d-1}(2^m-2)}{2^d+1}+2^{4m}$
-2	$[2^{m+2d}(2^d+2)+2^{m-d}-2^{3d}-1]\frac{3\cdot 2^{3m-2d-3}(2^m-2)}{2^d+1}+2^{2m}[3\cdot 2^{m-2}(2^m-2^{m-d})+2^{m-d}-1]$
2	$[2^{m+2d}(2^d+2)+2^{m-d}-2^{3d}-1]\frac{2^{3m-2d-3}(2^m-2)}{2^d+1}+2^{3m-2}(2^m-2^{m-d})$
$\pm 2^{\frac{m}{2}+1}$	$(2^m-2)2^{3m-2}\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$(each)
$\pm 2^{\frac{m+d}{2}+1}$	$2^{2m}(2^m-2)(2^{m-d}-1)2^{m-d-2}$(each)
$\pm 2^{\frac{m+2d}{2}+1}$	$2^{3m-2d-2}\frac{(2^{m-d}-1)(2^m-2)}{2^{2d}-1}$(each)
$\pm 2^{\frac{m}{2}+1}-2$	$3\cdot 2^{2m-2}(2^m-2)(2^{m-2}\pm 2^{\frac{m}{2}-1})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$\pm 2^{\frac{m}{2}+1}+2$	$2^{2m-2}(2^m-2)(2^{m-2}\mp 2^{\frac{m}{2}-1})\frac{2^{m+2d}-2^{m+d}-2^m+2^{2d}}{2^{2d}-1}$
$\pm 2^{\frac{m+d}{2}+1}-2$	$2^{2m-2}(2^{m-d-2}\pm 2^{\frac{m-d}{2}-1})[3\cdot(2^m-2)(2^{m-d}-1)+3\cdot 2^m-4]+2^{3m-d-2}(3\cdot 2^{m-2}-1)$
$\pm 2^{\frac{m+d}{2}+1}+2$	$2^{2m-2}(2^{m-d-2}\mp 2^{\frac{m-d}{2}-1})[(2^m-2)(2^{m-d}-1)+2^m]+2^{4m-d-4}$
$\pm 2^{\frac{m+2d}{2}+1}-2$	$(2^m-2)(2^{m-2d-2}\pm 2^{\frac{m-2d}{2}-1})\frac{3\cdot 2^{2m-2}(2^{m-d}-1)}{2^{2d}-1}$
$\pm 2^{\frac{m+2d}{2}+1}+2$	$(2^m-2)(2^{m-2d-2}\mp 2^{\frac{m-2d}{2}-1})\frac{2^{2m-2}(2^{m-d}-1)}{2^{2d}-1}$

Similar to the proof of Theorem 7 in [12], one can conclude that $3^j\gamma_1-\gamma_2$ runs through $\mathbb{R}_1\times\mathbb{L}$ 2^{2m-2} times for given $j\in\{0,1\}$ when (γ_1,γ_2) ranges over $\Delta_2\times\Delta_1$, where $\mathbb{R}_1=\{x+2y: x\in\mathbb{L}\backslash\{0,\eta\}, y\in\mathbb{L}\}$. Furthermore, when j ranges over $\{0,1\}$ and (u_1,u_2) runs through $\mathbb{Z}_2\times\mathbb{Z}_2$, the numbers $3^ju_1-u_2$ take the values 0, 1, 2, and 3 that occur 3, 1, 1, and 3 times respectively. This implies the multiset (18) has the following distribution: $\varsigma(\epsilon,0)$ occurs $3\cdot 2^{2m-2}$ times, $\varsigma(\epsilon,1)$ occurs 2^{2m-2} times, $\varsigma(\epsilon,2)$ occurs 2^{2m-2} times, and $\varsigma(\epsilon,3)$ occurs $3\cdot 2^{2m-2}$ times, respectively, where ϵ ranges over $\mathbb{R}_1\times\mathbb{L}$. Thus, we can calculate the values of $\varsigma(\epsilon,u)$ for $\epsilon\in\mathbb{R}_1\times\mathbb{L}$ and $u\in\mathbb{Z}_4$ as below.

Suppose that $\epsilon=(\epsilon_0+2\epsilon_1,\epsilon_2)$, where $\epsilon_0+2\epsilon_1\in\mathbb{R}_1$ and $\epsilon_2\in\mathbb{L}$, then we have

$$\varsigma(\epsilon,u)=2\cdot\mathfrak{Re}\Big(i^u\Big(-1+\xi(\epsilon_2,\epsilon_0,\epsilon_1)\Big)\Big). \tag{19}$$

Firstly, by (6) and (7) and Theorem 1, one can derive the distribution of $\xi(\epsilon_2,\epsilon_0,\epsilon_1)$ when $(\epsilon_2,\epsilon_0,\epsilon_1)$ runs through $\mathbb{L}\times\mathbb{L}^*\times\mathbb{L}$. Next, based on the fact that $\xi(\epsilon_2,\epsilon_0,\epsilon_1)$ has the same distribution as $\xi(\epsilon_2,1,\epsilon_1)$ for any fixed $\epsilon_0\neq 0$ one can determine the distribution of $\xi(\epsilon_2,1,\epsilon_1)$ when (ϵ_2,ϵ_1) runs through $\mathbb{L}\times\mathbb{L}$ and derive that the distribution of $\{-1+\xi(\epsilon_2,\epsilon_0,\epsilon_1):(\epsilon_2,\epsilon_0,\epsilon_1)\in\mathbb{L}\times\mathbb{L}\backslash\{0,\eta\}\times\mathbb{L}\}$ is (2^m-2) times of that of $\{-1+\xi(\epsilon_2,1,\epsilon_1):(\epsilon_2,\epsilon_1)\in\mathbb{L}\times\mathbb{L}\}$. Then, the correlation distribution of the family $\varphi(\mathcal{U}^k)$ for $\tau\neq 0$ and $\tau\neq 2^m-1$ is determined.

Similarly, from the proof of Theorem 7 in [12], we can obtain that the correlation distribution of $\varphi(\mathcal{U}^k)$ for $\tau=0$ is as follows: $\varsigma(\epsilon,0)$ occurs 2^{2m} times, $\varsigma(\epsilon,1)$ occurs 2^{2m-1} times, and $\varsigma(\epsilon,3)$ occurs 2^{2m-1} times respectively, where ϵ ranges over $2\mathbb{H}\times\mathbb{L}$, and the correlation distribution of $\varphi(\mathcal{U}^k)$ for $\tau=2^m-1$ is as follows: $\varsigma(\epsilon,0)$ occurs 2^{2m-1} times, $\varsigma(\epsilon,2)$ occurs 2^{2m-1} times, and $\varsigma(\epsilon,3)$ occurs 2^{2m} times respectively, where ϵ ranges over $2(\mathbb{L}\backslash\mathbb{H})\times\mathbb{L}$. Thus, for the cases $\tau=0$ and $\tau=2^m-1$, we need to discuss $\varsigma(\epsilon,u)$ for $\epsilon\in 2\mathbb{L}\times\mathbb{L}$.

If $\epsilon\in 2\mathbb{L}\times\mathbb{L}$, then $\epsilon_0=0$. From (19), we have

$$\varsigma(\epsilon,u)=2\cdot\mathfrak{Re}\Big(i^u\Big(-1+\xi(\epsilon_2,0,\epsilon_1)\Big)\Big).$$

For $\epsilon_2 = 0$, one gets $\xi(0,0,\epsilon_1) = 2^m$ if $\epsilon_1 = 0$, and $\xi(0,0,\epsilon_1) = 0$ otherwise. Then by (7), when (ϵ_2,ϵ_1) runs through $\mathbb{L}\times\mathbb{L}$, the distribution of $\xi(\epsilon_2,0,\epsilon_1)$ is

$$\begin{cases} 2^m, & 1 \text{ time} \\ 0, & (2^m-1)\left(2^m-2^{m-d}+1\right) \text{ times} \\ \pm 2^{\frac{m+d}{2}}, & (2^m-1)\left(2^{m-d-1}\pm 2^{\frac{m-d}{2}-1}\right) \text{ times.} \end{cases}$$

Moreover, if $\epsilon_1 \neq 0$, we have $\xi(\epsilon_2,0,\epsilon_1) = \xi(\epsilon_2\epsilon_1^{-(2^k+1)},0,1)$ for each $\epsilon_2 \in \mathbb{L}$. Therefore, the distribution of $\{\xi(\epsilon_2,0,\epsilon_1) : \epsilon_2 \in \mathbb{L}\}$ is the same for any fixed $\epsilon_1 \neq 0$. On the other hand, for $\epsilon_1 = 0$, we have $\xi(\epsilon_2,0,0) = 2^m$ if $\epsilon_2 = 0$ and $\xi(\epsilon_2,0,0) = 0$ otherwise, since the mapping $x \mapsto \epsilon_2 x^{2^k+1}$ is a permutation on $\mathbb{L}$ due to $\gcd(2^m-1, 2^k+1) = 1$. Hence, one can derive that the distribution of $\xi(\epsilon_2,0,\epsilon_1)$ is

$$\begin{cases} 2^m, & 1 \text{ time} \\ 0, & (2^m-1)+\left(2^m-2^{m-d}\right)\left(2^{m-1}-1\right) \text{ times} \\ \pm 2^{\frac{m+d}{2}}, & \left(2^{m-1}-1\right)\left(2^{m-d-1}\pm 2^{\frac{m-d}{2}-1}\right) \text{ times.} \end{cases}$$

when (ϵ_1,ϵ_2) runs through $\mathbb{H}\times\mathbb{L}$, and when (ϵ_1,ϵ_2) runs through $(\mathbb{L}\backslash\mathbb{H})\times\mathbb{L}$, the distribution is given by

$$\begin{cases} 0, & 2^{m-1}\left(2^m-2^{m-d}\right) \text{ times} \\ \pm 2^{\frac{m+d}{2}}, & 2^{m-1}\left(2^{m-d-1}\pm 2^{\frac{m-d}{2}-1}\right) \text{ times.} \end{cases}$$

Thus, the correlation distribution of $\varphi(\mathcal{U}^k)$ for $\tau = 0$ and $\tau = 2^m-1$ can also be obtained from the above analysis. Then the correlation distribution of $\varphi(\mathcal{U}^k)$ can be completely determined as follows.

Theorem 7: The correlation distribution of family $\varphi(\mathcal{U}^k)$ is given in Tables XI and XII for odd m and even m, respectively.

Remark 5: Note that a different form of $\mathbb{Z}_4$-valued quadratic forms were considered to construct large family of sequences in [11] and [12]. However, comparing with the $\mathbb{Z}_4$-valued quadratic form they used, our parameters are more flexible.

VII. Conclusion

In this paper, based on the properties of the roots of certain equations over a finite field and the newly developed theory of $\mathbb{Z}_4$-valued quadratic forms [11], the distribution of a class of exponential sums over a Galois ring is completely determined. As its applications, both the Lee weight and Hamming weight distributions of a class of codes $\mathcal{C}^k$ over $\mathbb{Z}_4$ are determined. By choosing cyclicly inequivalent codewords from $\mathcal{C}^k$, a family $\mathcal{U}^k$ of quaternary sequences is obtained and its correlation distribution is also determined. The quaternary codes $\mathcal{C}^k$ extend the results in [5], and the family $\mathcal{U}^k$ is a generalization of family $\mathcal{S}(1)$ in [8].

Furthermore, by performing the MSB and Gray maps to $\mathcal{C}^k$ and $\mathcal{U}^k$, two classes of binary codes and sequence families are obtained, respectively. The Hamming weight distributions of the binary codes are determined. For the binary sequence families, the correlation distribution of the sequence family obtained from $\mathcal{U}^k$ under the modified Gary map is completely determined, which generalizes the family $\mathcal{V}(1)$ in [12]. While the nontrivial maximal correlation value of the sequence family obtained from $\mathcal{U}^k$ under the MSB map is given, the correlation distribution remains open except for odd m and any k with $\gcd(m,k) = 1$[25].

All the distributions in this paper have been verified by computer experiments. While for $m/(m,k)$ even case, it is more complicated and is a good topic for further research.

References

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

[2] E. Brown, Jr., "Generalizations of the Kervaire invariant," *Ann. Math*, vol. 95, no. 2, pp. 368–383, Mar. 1972.

[3] S. Boztas, R. Hammons, and P. V. Kumar, "4-phase sequences with near-optimum correlation properties," *IEEE Trans. Inf. Theory*, vol. 14, no. 3, pp. 1101–1113, May 1992.

[4] T. Helleseth, L. Hu, A. Kholosha, X. Zeng, N. Li, and W. Jiang, "Period-different m -sequences with at most four-valued cross correlation," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3305–3311, Jul. 2009.

[5] T. Helleseth and P. V. Kumar, "Codes with the same weight distribution as the Goethals codes and the Delsarte-Goethals codes," *Des. Codes Crypt.*, vol. 9, no. 3, pp. 257–266, Nov. 1996.

[6] T. Helleseth and P. V. Kumar, "Sequences With Low Correlation," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlandds: Elsevier, 1998.

[7] L. Hu, X. Zeng, N. Li, and W. Jiang, "Period-different m-sequences with at most four-valued cross correlation," in *Proc. 11th IEEE Singapore Int. Conf. Communication System (ICCS 2008)*, pp. 446–450.

[8] P. V. Kumar, T. Helleseth, A. Calderbank, and A. Hammons, Jr, "Large families of quaternary sequences with low correlation," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 579–592, Mar. 1996.

[9] R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.

[10] A. A. Nechaev, "Kerdock code in a cyclic form," *Discr. Math. Appl.*, no. 2, pp. 365–384, 1991.

[11] K.-U. Schmidt, "$\mathbb{Z}_4$ -valued quadratic forms and quaternary sequence families," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5803–5810, Dec. 2009.

[12] K.-U. Schmidt, "On the correlation distrbution of Delsarte-Goethals sequences," *Des. Codes Crypt.*, vol. 59, no. 1-3, pp. 333–347, Apr. 2011.

[13] V. Sidelnikov, "On mutual correlation of sequences," *Soviet Math. Dokl.*, vol. 12, pp. 197–201, 1971.

[14] P. Solé, "A quaternary cyclic code, and a familly of quadriphase sequences with low correlation properties," *Lecture Notes Comput. Sci.*, vol. 388, pp. 193–201, 1989.

[15] X. H. Tang, T. Helleseth, L. Hu, and W. Jiang, "Two new families of optimal binary sequences obtained from quaternary sequences," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 433–436, Apr. 2009.

[16] X. H. Tang, T. Helleseth, and A. Johansen, "On the correlation distribution of Kerdock sequences," *Lecture Notes Comput. Sci.*, vol. 5203, pp. 121–129, 2008.

[17] X. H. Tang and P. Udaya, "A note on the optimal quadriphase sequences families," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 433–436, Jan. 2007.

[18] X. H. Tang, P. Udaya, and P. Z. Fan, "Quadriphase sequences obtained from binary quadratic form sequences," *Lecture Notes Comput. Sci.*, vol. 3486, pp. 243–254, 2005.

[19] X. H. Tang, T. Helleseth, and P. Z. Fan, "A new optimal quaternary sequence family of length $2(2^n-1)$ obtained from the orthogonal transformation of families $\mathcal{B}$ and $\mathcal{C}$," *Des. Codes Crypt.* , vol. 53, no. 3, pp. 137–148, Dec. 2009.

[20] P. Udaya and M. U. Siddiqi, "Optimal biphase sequences with large linear complexity derived from sequences over $\mathbb{Z}_4$," *IEEE Trans. Inf. Theory*, vol. 42, no. 1, pp. 206–216, Jan. 1996.

[21] P. Udaya and M. U. Siddiqi, "Optimal and suboptimal quadriphase sequences derived from maximal length sequences over $\mathbb{Z}_4$," *Appl. Alg. Eng. Commun. Comput.*, vol. 9, no. 2, pp. 161–191, 1998.

[22] L. Welch, "Lower bounds on the maximum crosscorrelation on the signals," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 3, pp. 397–399, May 1974.

[23] N. Y. Yu and G. Gong, "A new binary sequence family with low correlation and large size," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1624–1636, Apr. 2006.

[24] X. Zeng, N. Li, and L. Hu, "A class of nonbinary codes and sequence families," *Lecture Notes Comput. Sci.*, vol. 5203, pp. 81–94, 2008.
[25] Z. C. Zhou and X. H. Tang, "New families of binary sequences with low correlation and lagre size," *IEICE Trans. Fundam.*, vol. E92-A, no. 1, pp. 291–297, Jan. 2009.

Nian Li received the B.S. and M.S. degrees in mathematics from Hubei University, Wuhan, China, in 2006 and 2009, respectively. He is currently pursuing the Ph.D. degree at the Southwest Jiaotong University, Chengdu, China. His research interests include sequence design and coding theory.

Xiaohu Tang (M'04) received the B.S. degree in applied mathematics from the Northwest Polytechnic University, Xi'an, China, the M.S. degree in applied mathematics from the Sichuan University, Chengdu, China, and the Ph.D. degree in electronic engineering from the Southwest Jiaotong University, Chengdu, China, in 1992, 1995, and 2001 respectively.

From 2003 to 2004, he was a postdoctoral member in the Department of Electrical and Electronic Engineering, Hong Kong University of Science and Technology. From 2007 to 2008, he was a visiting professor at University of Ulm, Germany. Since 2001, he has been in the Institute of Mobile Communications, Southwest Jiaotong University, where he is currently a professor. His research interests include sequence design, coding theory and cryptography.

Dr. Tang was the recipient of the National excellent Doctoral Dissertation award in 2003 (China), the Humboldt Research Fellowship in 2007 (Germany).

Tor Helleseth (M'89–SM'96–F'97) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively.

From 1973 to 1980, he was a Research Assistant at the Department of Mathematics, University of Bergen. From 1981 to 1984, he was at the Chief Headquarters of Defense in Norway. Since 1984, he has been a Professor in the Department of Informatics at the University of Bergen. During the academic years 1977–1978 and 1992–1993, he was on sabbatical leave at the University of Southern California, Los Angeles, and during 1979–1980, he was a Research Fellow at the Eindhoven University of Technology, Eindhoven, The Netherlands. His research interests include coding theory and cryptology.

From 1991 to 1993, Prof. Helleseth served as an Associate Editor for Coding Theory for IEEE TRANSACTIONS ON INFORMATION THEORY. He was Program Chairman for Eurocrypt'93 and for the Information Theory Workshop in 1997 in Longyearbyen, Norway. He was a Program Co-Chairman for SETA04 in Seoul, Korea, and SETA06 in Beijing, China. He was also a Program Co-Chairman for the IEEE Information Theory Workshop in Solstrand in 2007. During 2007–2009, he served on the Board of Governors for the IEEE Information Theory Society. In 1997, he was elected an IEEE Fellow for his contributions to coding theory and cryptography.