# Seven Classes of Three-Weight Cyclic Codes

Zhengchun Zhou and Cunsheng Ding, *Senior Member, IEEE*

***Abstract*—Cyclic codes are a subclass of linear codes and have applications in consumer electronics, data storage systems, and communication systems as they have efficient encoding and decoding algorithms, compared with linear block codes. In this paper, seven classes of three-weight cyclic codes over GF($p$) whose duals have two zeros are presented, where $p$ is an odd prime. The weight distributions of the seven classes of cyclic codes are settled. Some of the cyclic codes are optimal in the sense that they meet certain bounds on linear codes. The application of these cyclic codes in secret sharing is also considered.**

***Index Terms*—Cyclic codes, linear codes, weight distribution, weight enumerator, secret sharing.**

## I. Introduction

Let $p$ be a prime. An $[n,\kappa,d]$ linear code over GF($p$) is a $\kappa$-dimensional subspace of GF$(p)^n$ with minimum nonzero (Hamming) weight $d$. A linear $[n,\kappa]$ code $\mathcal{C}$ over GF($p$) is called *cyclic* if $(c_0,c_1,\cdots,c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1},c_0,c_1,\cdots,c_{n-2}) \in \mathcal{C}$. By identifying any vector $(c_0,c_1,\cdots,c_{n-1}) \in \mathrm{GF}(p)^n$ with a polynomial $\sum_{i=0}^{n-1} c_i x^i \in \mathrm{GF}(p)[x]/(x^n-1)$, any linear code $\mathcal{C}$ of length $n$ over GF($p$) corresponds to a subset of the quotient ring $\mathrm{GF}(p)[x]/(x^n-1)$. A linear code $\mathcal{C}$ is cyclic if and only if the corresponding subset in $\mathrm{GF}(p)[x]/(x^n-1)$ is an ideal of the ring $\mathrm{GF}(p)[x]/(x^n-1)$.

It is well known that every ideal of $\mathrm{GF}(p)[x]/(x^n-1)$ is principal. Let $\mathcal{C} = \langle g(x) \rangle$ be a cyclic code, where $g(x)$ is monic and has the smallest degree among all the generators of $\mathcal{C}$. Then $g(x)$ is unique and called the *generator polynomial,* and $h(x) = (x^n-1)/g(x)$ is referred to as the *parity-check* polynomial of $\mathcal{C}$. If the parity-check polynomial $h(x)$ of a code $\mathcal{C}$ of length $n$ over GF($p$) is the product of $\ell$ distinct irreducible polynomials over GF($p$), we say that the dual code $\mathcal{C}^{\perp}$ has $\ell$ zeros.

Let $A_i$ denote the number of codewords with Hamming weight $i$ in a code $\mathcal{C}$ of length $n$. The *weight enumerator* of $\mathcal{C}$ is defined by $1+A_1y+A_2y^2+\cdots+A_ny^n$. The *weight distribution* $\{A_0,A_1,\ldots,A_n\}$ is an important research topic in coding theory. First, it contains crucial information as to estimate the error correcting capability and the probability of error detection and correction with respect to some algorithms [13]. Second, due to rich algebraic structures of cyclic codes, the weight distribution is often related to interesting and challenging problems in number theory [11]. A code $\mathcal{C}$ is said to be a $t$-weight code if the number of nonzero $A_i$ in the sequence $(A_1,A_2,\cdots,A_n)$ is equal to $t$ [17].

Cyclic codes have been widely used in consumer electronics, data transmission technologies, broadcast systems, and computer applications for error detection and correction as they have efficient encoding and decoding algorithms compared with linear block codes. Cyclic codes with a few weights are of special interest in secret sharing schemes as the access structures of the secret sharing schemes derived from such cyclic code can be easily determined and are interesting [4], [8], [25].

In this paper, seven classes of three-weight cyclic codes over GF($p$) whose duals have two zeros are presented, where $p$ is an odd prime. The weight distributions of the seven classes of cyclic codes are settled. Some of the cyclic codes are optimal in the sense that they meet certain bounds on linear codes. As a demonstration of applications of these cyclic codes, the access structures of the secret sharing schemes derived from these codes are analyzed.

This paper is organized as follows. Section II fixes some notations for this paper. Section III defines cyclic codes over GF($p$) whose duals have two zeros. Section IV introduces a few known classes of three-weight cyclic codes and their weight distributions. Section V presents two lemmas that will be needed in the sequel. Section VI defines seven classes of cyclic codes and determines their weight distributions. Section VII studies the access structures of the secret sharing schemes derived from these cyclic codes. Section VIII summarizes and concludes this paper.

## II. Some Notations Fixed Throughout this Paper

Throughout this paper, we adopt the following notations unless otherwise stated:

- $p$ is a prime and $q = p^m$, where $m$ is a positive integer.
- $n = q-1$, which is the length of a cyclic code over GF($p$).
- $\mathrm{Tr}_1^j(x)$ is the trace function from GF($p^j$) to GF($p$) for any positive integer $j$.
- $\chi$ is the canonical additive character on GF($q$), i.e., $\chi(x) = e^{2\pi\sqrt{-1}\mathrm{Tr}_1^m(x)/p}$ for any $x \in \mathrm{GF}(q)$.
- $\chi_1$ is the canonical additive character on GF($p$), i.e., $\chi_1(x) = e^{2\pi\sqrt{-1}x/p}$ for any $x \in \mathrm{GF}(p)$.
- $\mathsf{C}_a$ denotes the $p$-cyclotomic coset modulo $n$ containing $a$, where $a$ is any integer with $0 \le a \le q-2$, and $\ell_a := |\mathsf{C}_a|$

Manuscript received February 5, 2013; revised May 14 and June 27, 2013. The editor coordinating the review of this paper and approving it for publication was L. Dolecek.

Z. Zhou is with the School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China (e-mail: zzc@home.swjtu.edu.cn). He is also with the State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093).

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (e-mail: cding@ust.hk).

Z. Zhou's research was supported by the Natural Science Foundation of China, Proj. No. 61201243 and Proj. No. 61373009, The Hong Kong Research Grants Council, Proj. No. 600812, the application fundamental research plan project of Sichuan Province under Grant 2013JY0167, and the Fundamental Research Funds for the Central Universities under Grants SWJTU12CX053, SWJTU12ZT15 and SWJTU12ZT14. C. Ding's research was supported by The Hong Kong Research Grants Council, Proj. No. 600812.

Digital Object Identifier 10.1109/TCOMM.2013.072213.130107

TABLE I
WEIGHT DISTRIBUTION I

| Weight $w$ | No. of codewords $A_w$ |
|---|---|
| $0$ | $1$ |
| $(p-1)p^{m-1}-p^{(m-1)/2}$ | $\frac{1}{2}(p-1)(p^m-1)(p^{m-1}+p^{(m-1)/2})$ |
| $(p-1)p^{m-1}$ | $(p^m-1)(p^{m-1}+1)$ |
| $(p-1)p^{m-1}+p^{(m-1)/2}$ | $\frac{1}{2}(p-1)(p^m-1)(p^{m-1}-p^{(m-1)/2})$ |

denotes the size of the cyclotomic coset $\mathtt{C}_a$.

- By the Database we mean the collection of the tables of best linear codes known maintained by Markus Grassl at http://www.codetables.de/.

## III. Cyclic Codes Whose Duals Have Two Zeros

Given a positive integer $m$, recall that $q = p^m$ and $n = q-1$ throughout this paper. Let $\alpha$ be a generator of the multiplicative group $\mathrm{GF}(q)^*$. For any $0 \le a \le q-2$, denote by $m_a(x)$ the minimal polynomial of $\alpha^{-a}$ over $\mathrm{GF}(p)$.

Let $0 \le u \le q-2$ and $0 \le v \le q-2$ be any two integers such that $\mathtt{C}_u \cap \mathtt{C}_v = \emptyset$. Let $\mathcal{C}_{(u,v,q,m)}$ be the cyclic code over $\mathrm{GF}(p)$ with length $n$ whose codewords are given by

$$\mathbf{c}(a,b) = (c_0, c_1, \ldots, c_{n-1}), \quad \forall\, (a,b) \in \mathrm{GF}(p^{\ell_u}) \times \mathrm{GF}(p^{\ell_v}) \quad (1)$$

where

$$c_i = \mathrm{Tr}_1^{\ell_u}\left(a\alpha^{iu}\right) + \mathrm{Tr}_1^{\ell_v}\left(b\alpha^{iv}\right), \quad 0 \le i \le n-1.$$

By Delsarte's Theorem, the code $\mathcal{C}_{(u,v,q,m)}$ has parity-check polynomial $m_u(x)m_v(x)$ and dimension $\ell_u + \ell_v$. There are a lot of references on the code $\mathcal{C}_{(u,v,q,m)}$ (see for example [2], [7], [9], [10], [15], [16], [18], [19], [20], [22], [23], [26]).

This class of cyclic codes $\mathcal{C}_{(u,v,q,m)}$ may have many nonzero weights. Note that $\mathcal{C}_{(u,v,q,m)}$ cannot be a constant-weight code as its parity-check polynomial has two zeros and the minimal polynomials of the two zeros are distinct. In most cases $\mathcal{C}_{(u,v,q,m)}$ has at least three nonzero weights, provided that $\mathtt{C}_u \cap \mathtt{C}_v = \emptyset$, $\ell_u > 1$ and $\ell_v > 1$ (see [12]). Hence it is very interesting to study three-weight cyclic codes $\mathcal{C}_{(u,v,q,m)}$.

## IV. Some Known Nonbinary Three-Weight Cyclic Codes

Carlet, Ding and Yuan employed some special monomials to construct three-weight cyclic codes and proved the following theorem [4], [24].

*Theorem 4.1:* ([24], [9]) Let $m \ge 3$ be odd and let $p$ be an odd prime. Then $\mathcal{C}_{(1,v,p,m)}$ is a three-weight $[p^m-1, 2m]$ cyclic code with the weight distribution in Table I if

- $v = p^h + 1$ or
- $v = (p^h+1)/2$, where $p = 3$, $\gcd(m,h) = 1$ and $h$ is odd.

When $m$ is even, the codes $\mathcal{C}_{(1,v,p,m)}$ defined by the monomials $x^v$ in Theorem 4.1 have five nonzero weights. For information on the duals of the three-weight cyclic codes described in Theorem 4.1, the reader is referred to [4].

Luo and Feng [14] extended the second construction in Theorem 4.1 and proved the following theorem.

*Theorem 4.2:* ([14]) Let $m \ge 3$ be odd and let $p$ be an odd prime. Then $\mathcal{C}_{(1,v,p,m)}$ is a three-weight $[p^m-1, 2m]$ cyclic code with the weight distribution in Table II if $v = (p^h+1)/2$, where $h$ is a positive integer satisfying $\gcd(2m,h) = 1$.

TABLE II
WEIGHT DISTRIBUTION II

| Weight $w$ | No. of codewords $A_w$ |
|---|---|
| $0$ | $1$ |
| $(p-1)p^{m-1}-\frac{p-1}{2}p^{(m-1)/2}$ | $(p^m-1)(p^{m-1}+p^{(m-1)/2})$ |
| $(p-1)p^{m-1}$ | $(p^m-1)(p^m-2p^{m-1}+1)$ |
| $(p-1)p^{m-1}+\frac{p-1}{2}p^{(m-1)/2}$ | $(p^m-1)(p^{m-1}-p^{(m-1)/2})$ |

When $p = 3$, the weight distribution depicted in Table I is the same as that in Table II .

A few more classes of three-weight nonbinary cyclic codes are available in the literature (see for example [5], [21]). We will not introduce them here as we do not need the weight distribution formulas of these codes in this paper. Similarly, we will not touch on references on binary three-weight codes as this paper deals with nonbinary three-weight codes.

## V. Two Auxiliary Results About Exponential Sums

In this section, we introduce two lemmas on exponential sums over finite fields. Recall that $\chi$ and $\chi_1$ are respectively the canonical additive characters of $\mathrm{GF}(q)$ and $\mathrm{GF}(p)$.

The following lemmas will be needed in the sequel.

*Lemma 5.1:* Let $m$ be odd and $h \ge 0$ be any integer. Define

$$S(a,b) = \sum_{x \in \mathrm{GF}(q)} \chi\left(ax^{p^h+1} + bx\right).$$

Then, as $(a,b)$ runs through $\mathrm{GF}(q)^2$, the values of the sum $\sum_{y \in \mathrm{GF}(p)^*} S(ya, yb)$ have the following distribution

| Value | Frequency |
|---|---|
| $(p-1)p^m$ | $1$ |
| $p^{(m+1)/2}$ | $\frac{p-1}{2}(p^m-1)(p^{m-1}+p^{(m-1)/2})$ |
| $0$ | $(p^m-1)(p^{m-1}+1)$ |
| $-p^{(m+1)/2}$ | $\frac{p-1}{2}(p^m-1)(p^{m-1}-p^{(m-1)/2})$. |

*Proof:* According to the definition of $S(a,b)$, we have

$$\begin{aligned} &\sum_{y \in \mathrm{GF}(p)^*} S(ya, yb) \\ &= -q + \sum_{x \in \mathrm{GF}(q)} \sum_{y \in \mathrm{GF}(p)} \chi_1\left(y\mathrm{Tr}_1^m(ax^{p^h+1} + bx)\right) \\ &= -q + p + \sum_{x \in \mathrm{GF}(q)^*} \sum_{y \in \mathrm{GF}(p)} \chi_1\left(y\mathrm{Tr}_1^m(ax^{p^h+1} + bx)\right) \\ &= (p-1)q - pW_{a,b} \qquad (2) \end{aligned}$$

where $W_{a,b} = \#\{x \in \mathrm{GF}(q)^* : \mathrm{Tr}_1^m(ax^{p^h+1} + bx) \ne 0\}$. Note that $W_{a,b}$ is exactly the Hamming weight of the codeword

$$\left(\mathrm{Tr}_1^m(ax^{p^h+1} + bx)\right)_{x \in \mathrm{GF}(q)^*}$$

in the code $\mathcal{C}_{(1,p^h+1,p,m)}$. By Theorem 4.1, the weight distribution of $\mathcal{C}_{(1,p^h+1,p,m)}$ is listed in Table I. The value distribution of $\sum_{y \in \mathrm{GF}(p)^*} S(ya, yb)$ then follows from (2) and the weight distribution in Table I. ■

*Lemma 5.2:* Let $m$ be odd and $h$ be an integer with $\gcd(m,h) = 1$. Define

$$R(a,b) = \sum_{x \in \mathrm{GF}(q)} \chi\left(ax^{p^h+1} + bx^2\right).$$

Then, as $(a,b)$ runs through $\mathrm{GF}(q)^2$, the values of the sum

$$\sum_{y\in \mathrm{GF}(p)^*} (R(ya,yb)+R(-ya,yb))$$

have the following distribution

| Value | Frequency |
|---|---|
| $2(p-1)p^m$ | $1$ |
| $(p-1)p^{(m+1)/2}$ | $(p^{m-1}+p^{(m-1)/2})(p^m-1)$ |
| $0$ | $(p^m-2p^{m-1}+1)(p^m-1)$ |
| $-(p-1)p^{(m+1)/2}$ | $(p^{m-1}-p^{(m-1)/2})(p^m-1)$. |

*Proof:* When $h$ is even, the conclusion has been proved in Theorem 3.4 of [26] (see also [14]). We now assume that $h$ is odd. Let $\lambda=\alpha^{(p^m-1)/(p-1)}$, where $\alpha$ is a generator of $\mathrm{GF}(q)^*$. Then $\lambda$ is a generator of $\mathrm{GF}(p)^*$, a nonsquare in $\mathrm{GF}(q)$ and satisfies $\lambda^{(p^h-1)/2}=-1$ as $h$ is odd. By the definition of $R(a,b)$, we have

$$\begin{aligned}
&\sum_{y\in \mathrm{GF}(p)^*} R(ya,yb)\\
&= \sum_{x\in \mathrm{GF}(q)}\sum_{y\in \mathrm{GF}(p)^*} \chi\left(y(ax^{p^h+1}+bx^2)\right)\\
&= -q+p+\sum_{x\in \mathrm{GF}(q)^*}\sum_{y\in \mathrm{GF}(p)} \chi_1\left(y\mathrm{Tr}_1^m(ax^{p^h+1}+bx^2)\right)\\
&= p-q+2\sum_{x\in C_0^{(2,q)}}\sum_{y\in \mathrm{GF}(p)} \chi_1\left(y\mathrm{Tr}_1^m(ax^{(p^h+1)/2}+bx)\right) \quad (3)
\end{aligned}$$

where $C_0^{(2,q)}$ denotes the set of all nonzero squares in $\mathrm{GF}(q)$. Similarly, we have

$$\begin{aligned}
&\sum_{y\in \mathrm{GF}(p)^*} R(-ya,yb)\\
&= p-q+2\sum_{x\in C_0^{(2,q)}}\sum_{y\in \mathrm{GF}(p)} \chi_1\left(y\mathrm{Tr}_1^m(-ax^{(p^h+1)/2}+bx)\right)\\
&= p-q+2\sum_{x\in C_0^{(2,q)}}\sum_{y\in \mathrm{GF}(p)} \chi_1\left(y\mathrm{Tr}_1^m(a(\lambda x)^{(p^h+1)/2}+b\lambda x)\right)\\
&= p-q+2\sum_{x\in C_1^{(2,q)}}\sum_{y\in \mathrm{GF}(p)} \chi_1\left(y\mathrm{Tr}_1^m(ax^{(p^h+1)/2}+bx)\right) \quad (4)
\end{aligned}$$

where $C_1^{(2,q)}$ denotes the set of all nonsquares in $\mathrm{GF}(q)$, and in the second and third identities we respectively used the fact that $\lambda$ is an element in $\mathrm{GF}(p)$ with $\lambda^{(p^h-1)/2}=-1$ and the fact that $\lambda x$ runs through $C_1^{(2,q)}$ as $x$ runs through $C_0^{(2,q)}$.

Combining (3) and (4), we arrive at

$$\begin{aligned}
&\sum_{y\in \mathrm{GF}(p)^*} (R(ya,yb)+R(-ya,yb))\\
&= -2q+2p+2\sum_{x\in \mathrm{GF}(q)^*}\sum_{y\in \mathrm{GF}(p)} \chi_1\left(y\mathrm{Tr}_1^m(ax^{(p^h+1)/2}+bx)\right)\\
&= 2(p-1)q-2pW_{a,b} \quad (5)
\end{aligned}$$

where $W_{a,b}=\#\{x\in \mathrm{GF}(q)^*:\mathrm{Tr}_1^m(ax^{(p^h+1)/2}+bx)\neq 0\}$, which is exactly the Hamming weight of the codeword

$$\left(\mathrm{Tr}_1^m(ax^{(p^h+1)/2}+bx)\right)_{x\in \mathrm{GF}(q)^*}$$

in the code $\mathcal{C}_{(1,(p^h+1)/2,p,m)}$. By Theorem 4.2, the weight distribution of this code is given by Table II. The conclusion then follows from (5) and the weight distribution listed in Table II. ■

## VI. Seven Classes of Three-Weight Cyclic Codes and Their Weight Enumerators

In this section, we propose seven classes of three-weight cyclic codes $\mathcal{C}_{(u,v,p,m)}$ over $\mathrm{GF}(p)$ where $u=1$ and $v$ is some integer with $\mathsf{C}_v\cap\mathsf{C}_1=\emptyset$ and $\ell_v=m$. It is obvious that the code $\mathcal{C}_{(1,v,p,m)}$ has length $q-1$ and dimension $2m$.

In terms of exponential sums, the Hamming weight $\mathrm{wt}(\mathbf{c}(a,b))$ of the codeword $\mathbf{c}(a,b)$ of (1) in $\mathcal{C}_{(1,v,p,m)}$ is given by

$$\mathrm{wt}(\mathbf{c}(a,b))=(p-1)p^{m-1}-\frac{1}{p}\sum_{y\in \mathrm{GF}(p)^*} T_v(ya,yb) \quad (6)$$

where

$$T_v(a,b)=\sum_{x\in \mathrm{GF}(q)} \chi(ax+bx^v) \quad (7)$$

for each $(a,b)\in \mathrm{GF}(q)^2$. Throughout this section, the function $T_v(a,b)$ is always defined as in (7) for any given $v$.

The following lemma will be frequently used in the sequel when we determine the weight distributions of the seven classes of cyclic codes.

*Lemma 6.1:* Let $s$ be any integer with $\gcd(s,q-1)=2$. Then

$$T_v(a,b)=\frac{1}{2}\left(\sum_{x\in \mathrm{GF}(q)} \chi(ax^s+bx^{sv})+\sum_{x\in \mathrm{GF}(q)} \chi(a\lambda x^s+b\lambda^v x^{sv})\right)$$

where $\lambda$ is any fixed nonsquare in $\mathrm{GF}(q)^*$.

*Proof:* Let $C_0^{(2,q)}$ denote the set of all nonzero squares in $\mathrm{GF}(q)$. Then

$$T_v(a,b)=1+\sum_{x\in C_0^{(2,q)}} \chi(ax+bx^v)+\sum_{x\in C_0^{(2,q)}} \chi(a\lambda x+b\lambda^v x^v). \quad (8)$$

Note that $\gcd(q-1,s)=2$. When $x$ runs through $\mathrm{GF}(q)$, $x^s$ runs twice through the nonzero squares in $\mathrm{GF}(q)$ and takes on the value 0 once. Similarly, $\lambda x^s$ runs twice through all the nonsquares in $\mathrm{GF}(q)$ and takes on the value 0 once. The conclusion then follows directly from (8) and the discussions above. ■

### A. The First Class of Three-Weight Cyclic Codes

In this subsection, we study the cyclic codes $\mathcal{C}_{(1,v,p,m)}$, where $m$ is odd, $p=3$, and $v=3^{(m+1)/2}-1$. The parameters of the codes are described in the following theorem.

*Theorem 6.2:* Let $m$ be odd, $p=3$, and $v=3^{(m+1)/2}-1$. Then $\mathcal{C}_{(1,v,p,m)}$ is a $[p^m-1,2m]$ cyclic code over $\mathrm{GF}(p)$ with the weight distribution in Table II.

*Proof:* Let $h=(m+1)/2$ and $s=3^h+1$. Then $\gcd(s,3^m-1)=2$ since $m$ is odd. It is easy to check that $sv\equiv 2 \pmod{3^m-1}$. Noticing that $v$ is even and $-1$ is a nonsquare in $\mathrm{GF}(q)$. By Lemma 6.1, we have

$$T_v(a,b) \;=\; \frac{1}{2}\left(R_v(a,b)+R_v(-a,b)\right)$$

where

$$R_v(a,b)=\sum_{x\in \mathrm{GF}(q)} \chi\left(ax^{3^h+1}+bx^2\right).$$

It then follows from (6) that

$$\begin{aligned}&\mathrm{wt}(\mathbf{c}(a,b))\\ &\quad = 2\times 3^{m-1} - \tfrac{1}{6}\textstyle\sum_{y\in \mathrm{GF}(3)^*}\left(R_v(ya,yb)+R_v(-ya,yb)\right). \quad (9)\end{aligned}$$

Note that $\gcd(m,h)=\gcd(m,(m+1)/2)=1$, the weight distribution of the code $\mathcal{C}_{(1,v,3,m)}$ then follows from Equation (9) and Lemma 5.2. ■

*Example 6.3:* Let $p=3$ and $m=5$. Then $v=26$ and $\mathcal{C}_{(1,v,p,m)}$ is a $[242,6,153]$ code over GF(3) with weight enumerator $1+21780y^{153}+19844y^{162}+17424y^{171}$. It has the same parameters as the best known cyclic codes in the Database. It is optimal or almost optimal since the upper bound on the minimal distance of any ternary linear code with length 242 and dimension 6 is 154.

### B. The Second Class of Three-Weight Cyclic Codes

In this subsection, we investigate the cyclic codes $\mathcal{C}_{(1,v,p,m)}$, where $m\equiv 3 \pmod 4$, $p=3$, and $v=(3^{(m+1)/2}-1)/2$. The parameters of the codes are described in the following theorem.

*Theorem 6.4:* Let $m\equiv 3 \pmod 4$, $p=3$ and $v=(3^{(m+1)/2}-1)/2$. Then $\mathcal{C}_{(1,v,p,m)}$ is a $[p^m-1,2m]$ cyclic code over GF$(p)$ with the weight distribution in Table I.

*Proof:* Let $h=(m+1)/2$ and $s=3^h+1$. Since $m\equiv 3 \pmod 4$, $\gcd(s,3^m-1)=2$ and $v$ is even. Note that $sv=(3^{m+1}-1)/2$. Thus $sv\equiv(3^m+1)/2 \ (\bmod\ 3^m-1)$. Select $\lambda=-1$ as a nonsquare in GF$(q)$. Applying Lemma 6.1, we have

$$T_v(a,b) \;=\; \frac{1}{2}\left(Q_v(a,b)+Q_v(-a,b)\right). \qquad (10)$$

Herein

$$\begin{aligned} Q_v(a,b) &= \sum_{x\in \mathrm{GF}(q)} \chi\left(ax^{3^h+1}+bx^{(3^m+1)/2}\right)\\ &= 1+\sum_{x\in C_0^{(2,q)}} \chi\left(ax^{3^h+1}+bx^{(3^m+1)/2}\right)+\\ &\qquad \sum_{x\in C_0^{(2,q)}} \chi\left(a(\lambda x)^{3^h+1}+b(\lambda x)^{(3^m+1)/2}\right)\\ &= 1+2\sum_{x\in C_0^{(2,q)}} \chi\left(ax^{3^h+1}+bx\right)\end{aligned}$$

where $C_0^{(2,q)}$ denotes the set of all nonzero squares in GF$(q)$, and the last identity followed from the observation that $x^{(3^m+1)/2}=x$ for any $x\in C_0^{(2,q)}$. It is easily seen that

$$Q_v(a,b)+Q_v(a,-b) \;=\; 2S_v(a,b) \qquad (11)$$

and

$$Q_v(-a,b)+Q_v(-a,-b) \;=\; 2S_v(-a,b) \qquad (12)$$

where

$$S_v(a,b) \;=\; \sum_{x\in \mathrm{GF}(q)} \chi\left(ax^{3^h+1}+bx\right). \qquad (13)$$

Note that

$$\begin{aligned} S_v(-a,b) &= \sum_{x\in \mathrm{GF}(q)} \chi\left(-a(-x)^{3^h+1}-b(-x)\right)\\ &= \sum_{x\in \mathrm{GF}(q)} \chi\left(-ax^{3^h+1}-bx\right)\\ &= S_v(-a,-b). \qquad (14)\end{aligned}$$

Combining Equations (10)–(14), we then have

$$\sum_{y\in \mathrm{GF}(3)^*} T_v(ya,yb) \;=\; \sum_{y\in \mathrm{GF}(3)^*} S_v(ya,yb). \qquad (15)$$

It then follows from (6) and (10) that

$$\mathrm{wt}(\mathbf{c}(a,b)) \;=\; 2\times 3^{m-1}-\frac{1}{3}\sum_{y\in \mathrm{GF}(3)^*} S_v(ya,yb). \qquad (16)$$

The weight distribution of the code $\mathcal{C}_{(1,v,3,m)}$ then follows from Equation (16) and Lemma 5.1. ■

*Example 6.5:* Let $p=3$ and $m=3$. Then $v=8$ and $\mathcal{C}_{(1,v,p,m)}$ is a $[26,6,15]$ code over GF(3) with weight enumerator $1+312y^{15}+260y^{18}+156y^{21}$. It has the same parameters as the optimal cyclic code in the Database.

### C. The Third Class of Three-Weight Cyclic Codes

In this subsection, we deal with the cyclic codes $\mathcal{C}_{(1,v,p,m)}$, where $m\equiv 1 \pmod 4$, $p=3$, and $v=(3^{(m+1)/2}-1)/2+(3^m-1)/2$. The parameters of the codes are described in the following theorem.

*Theorem 6.6:* Let $m\equiv 1 \pmod 4$, $p=3$ and $v=(3^{(m+1)/2}-1)/2+(3^m-1)/2$. Then $\mathcal{C}_{(1,v,q,m)}$ is a $[p^m-1,2m]$ cyclic code over GF$(p)$ with the weight distribution in Table I.

*Proof:* Let $h=(m+1)/2$ and $s=3^h+1$. Then $\gcd(s,3^m-1)=2$ since $m$ is odd. It is easy to verify that $v$ is even and $sv\equiv(3^m+1)/2 \ (\bmod\ 3^m-1)$. The proof of this theorem is then similar to that of Theorem 6.4 and is omitted here. ■

### D. The Fourth Class of Three-Weight Cyclic Codes

In this subsection, we treat the cyclic codes $\mathcal{C}_{(1,v,p,m)}$, where $m\equiv 3 \pmod 4$, $p=3$, and $v=(3^{m+1}-1)/8$. The parameters of the codes are described in the following theorem.

*Theorem 6.7:* Let $m\equiv 3 \pmod 4$, $p=3$ and $v=(3^{m+1}-1)/8$. Then $\mathcal{C}_{(1,v,p,m)}$ is a $[p^m-1,2m]$ cyclic code over GF$(p)$ with the weight distribution in Table I.

*Proof:* Let $h=1$ and $s=3^h+1$. Since $m\equiv 3 \pmod 4$, $\gcd(s,3^m-1)=2$ and $v$ is even. It is straightforward to verify that $sv\equiv(3^m+1)/2 \ (\bmod\ 3^m-1)$. The proof of this theorem is then similar to that of Theorem 6.4 and is omitted here. ■

*Example 6.8:* Let $p=3$ and $m=7$. Then $v=820$ and $\mathcal{C}_{(1,v,p,m)}$ is a $[2186,14,1431]$ code over GF(3) with weight enumerator $1+1652616y^{1431}+1595780y^{1458}+1534572y^{1485}$.

### E. The Fifth Class of Three-Weight Cyclic Codes

In this subsection, we consider the cyclic codes $\mathcal{C}_{(1,v,p,m)}$, where $p=3$ and $v=(3^{m+1}-1)/8+(3^m-1)/2$ for $m\equiv 1 \pmod 4$. The parameters of the codes are described in the following theorem.

*Theorem 6.9:* Let $m\equiv 1 \pmod 4$, $p=3$ and $v=(3^{m+1}-1)/8+(3^m-1)/2$. Then $\mathcal{C}_{(1,v,p,m)}$ is a $[p^m-1,2m]$ cyclic code over GF$(p)$ with the weight distribution in Table I.

*Proof:* Let $h=1$ and $s=3^h+1$. Then $\gcd(s,3^m-1)=2$. It is not hard to verify that $v$ is even and $sv\equiv(3^m+1)/2 \ (\bmod\ 3^m-1)$. The proof of this theorem is then similar to that of Theorem 6.4 and omitted here. ■

*Example 6.10:* Let $p = 3$, $m = 9$. Then $v = 17222$ and $\mathcal{C}_{(1,v,p,m)}$ is a $[19682, 18, 13041]$ code over GF(3) with weight enumerator $1+130727844y^{13041}+129153284y^{13122}+127539360y^{13203}$.

### *F. The Sixth Class of Three-Weight Cyclic Codes*

In this subsection, we analyze the cyclic codes $\mathcal{C}_{(1,v,p,m)}$, where $m \equiv 3 \pmod 4$, $p = 3$, and $v = \left(3^{(m+1)/4}-1\right)\left(3^{(m+1)/2}+1\right)$. The parameters of the codes are described in the following theorem.

*Theorem 6.11:* Let $m \equiv 3 \pmod 4$, $p = 3$ and $v = \left(3^{(m+1)/4}-1\right)\left(3^{(m+1)/2}+1\right)$. Then $\mathcal{C}_{(1,v,3,m)}$ is a $[3^m-1, 2m]$ cyclic code over GF(3) with the weight distribution in Table II.

*Proof:* Let $h = (m+1)/4$ and $s = 3^h+1$. Since $m \equiv 3 \pmod 4$, $\gcd(s, 3^m-1) = 2$ and $v$ is even. It is easy to check that $sv \equiv 2 \pmod{3^m-1}$. Select $\lambda = -1$ as a nonsquare in GF$(p^m)$. Applying Lemma 6.1, we have

$$T_v(a,b) \quad = \quad \frac{1}{2}\left(R_v(a,b)+R_v(-a,b)\right) \tag{17}$$

where

$$R_v(a,b) = \sum_{x\in \mathrm{GF}(q)} \chi\left(ax^{3^h+1}+bx^2\right).$$

It then follows from (6) and (17) that

$$\begin{aligned} &\mathrm{wt}(\mathbf{c}(a,b)) \\ &\quad = \quad 2\times 3^{m-1} - \frac{1}{6}\sum_{y\in \mathrm{GF}(3)^*}\left(R_v(ya,yb)+R_v(-ya,yb)\right) \end{aligned} \tag{18}$$

The weight distribution of the code $\mathcal{C}_{(1,v,3,m)}$ then follows from (18) and Lemma 5.2. ■

## VII. Application of the Three-Weight Cyclic Codes in Secret Sharing

Secret sharing is an interesting topic of cryptography and has been studied for over thirty years. In a secret sharing scheme, a dealer will create a secret to be shared among a group of participants. The dealer will compute a share of the secret for each participant, and will distribute them to all participants. Some of the subgroups of the participants will be able to recover the secret after combining their shares together, while other subgroups will not be able to do so. In this section, we will study the secret sharing schemes based on all the three-weight codes presented in this paper, as a demonstration of applications of these codes.

### *A. A Construction of Secret Sharing Schemes Based on Linear Codes*

Let $G = (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1})$ be a generator matrix of an $[n,k,d]$ linear code $\mathcal{C}$ over GF$(p)$. For all the linear codes mentioned in this section we assume that no column vector of any generator matrix is the zero vector. One way of using linear codes to construct secret sharing schemes is the following.

*The secrets and parties involved:* In the secret sharing scheme constructed from $\mathcal{C}$, the secret is an element of GF$(p)$, and $n-1$ parties $P_1, P_2, \cdots, P_{n-1}$ and a dealer are involved.

*The computation and distribution of shares:* To compute the shares with respect to a secret $s$, the dealer chooses randomly a vector $\mathbf{u} = (u_0, \ldots, u_{k-1}) \in \mathrm{GF}(p)^k$ such that $s = \mathbf{u}\mathbf{g}_0$. There are altogether $p^{k-1}$ such vectors $\mathbf{u} \in \mathrm{GF}(p)^k$. The dealer then treats $\mathbf{u}$ as an information vector and computes the corresponding codeword

$$\mathbf{t} = (t_0, t_1, \ldots, t_{n-1}) = \mathbf{u}G.$$

He then gives $t_i$ to party $P_i$ as share for each $i \geq 1$.

*Recovering the secret:* Note that $t_0 = \mathbf{u}\mathbf{g}_0 = s$. A set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ determines the secret if and only if $\mathbf{g}_0$ is a linear combination of $\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_m}$.

The following lemma tells which subgroups of participants can recover the secret [25].

*Lemma 7.1:* Let $G$ be a generator matrix of an $[n,k]$ code $\mathcal{C}$ over GF$(p)$. In the secret sharing scheme based on $\mathcal{C}$, a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ determine the secret if and only if there is a codeword

$$(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0) \tag{19}$$

in the dual code $\mathcal{C}^{\perp}$, where $c_{i_j} \neq 0$ for at least one $j$, $1 \leq i_2 < \ldots < i_m \leq n-1$ and $1 \leq m \leq n-1$.

If there is a codeword of (19) in $\mathcal{C}^{\perp}$, then the vector $\mathbf{g}_0$ is a linear combination of $\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_m}$, say, $\mathbf{g}_0 = \sum_{j=1}^{m} x_j \mathbf{g}_{i_j}$. Then the secret $s$ is recovered by computing $s = \sum_{j=1}^{m} x_j t_{i_j}$.

If a group of participants can recover the secret by combining their shares, then any group of participants containing this group can also recover the secret. A group of participants is called a *minimal access set* if they can recover the secret with their shares, but any of its proper subgroups cannot do so. Here a proper subgroup has fewer members than this group. Due to these facts, we are only interested in the set of all minimal access sets. To determine this set, we need the notion of minimal codewords.

The *support* of a vector $\mathbf{c} \in \mathrm{GF}(p)^n$ is defined to be

$$\{0 \leq i \leq n-1 : c_i \neq 0\}.$$

A codeword $\mathbf{c}_2$ *covers* a codeword $\mathbf{c}_1$ if the support of $\mathbf{c}_2$ contains that of $\mathbf{c}_1$.

If a nonzero codeword $\mathbf{c}$ covers only its multiples, but no other nonzero codewords, then it is called a *minimal codeword.* If the first coordinate of a minimal codeword is 1, it is called a *minimal AS-codeword.*

It follows from Lemma 7.1 and the discussions above that there is a one-to-one correspondence between the set of minimal access sets and the set of minimal AS-codewords of the dual code $\mathcal{C}^{\perp}$. To determine the access structure of a secret sharing scheme, we need to determine only the set of minimal AS-codewords, i.e., a subset of the set of all minimal codewords. However, in almost every case we should be able to determine the set of all minimal codewords as long as we can determine the set of minimal AS-codewords.

The shares for the participants depend on the selection of the generator matrix $G$ of the code $\mathcal{C}$. However, by Lemma 7.1 the selection of $G$ does not affect the access structure of the secret sharing scheme. Hence in the sequel we will call it the secret sharing scheme based on $\mathcal{C}$, without mentioning the generator matrix used to computer the shares.

### B. The Access Structure of The Secret Sharing Schemes Based on Special Linear Codes

*Theorem 7.2:* [25] Let $\mathcal{C}$ be an $[n,k]$ code over GF$(p)$, and let $G=[\mathbf{g}_0,\mathbf{g}_1,\cdots,\mathbf{g}_{n-1}]$ be its generator matrix. If each nonzero codeword of $\mathcal{C}$ is a minimal vector, then in the secret sharing scheme based on $\mathcal{C}^{\perp}$, there are altogether $p^{k-1}$ minimal access sets. In addition, we have the following:

1) If $\mathbf{g}_i$ is a multiple of $\mathbf{g}_0$, $1\leq i\leq n-1$, then participant $P_i$ must be in every minimal access set. Such a participant is called a *dictatorial participant*.
2) If $\mathbf{g}_i$ is not a multiple of $\mathbf{g}_0$, $1\leq i\leq n-1$, then participant $P_i$ must be in $(p-1)p^{k-2}$ out of $p^{k-1}$ minimal access sets.

In view of Theorem 7.2, it is an interesting problem to construct codes where each nonzero codeword is a minimal vector. Such a linear code gives a secret sharing scheme with the interesting access structure described in Theorem 7.2.

If the weights of a linear code are close enough to each other, then each nonzero codeword of the code is minmal, as described by the following proposition [1].

*Lemma 7.3:* In an $[n,k]$ linear code $\mathcal{C}$ over GF$(p)$, let $w_{min}$ and $w_{max}$ be the minimum and maximum nonzero weights respectively. If

$$\frac{w_{min}}{w_{max}}>\frac{p-1}{p},$$

then each nonzero codeword of $\mathcal{C}$ is minimal.

### C. The Access Structure of The Secret Sharing Schemes Derived From the Codes of This Paper

The cyclic codes of this paper are very interesting for secret sharing due to the following lemma.

*Lemma 7.4:* In every cyclic code $\mathcal{C}_{(1,v,p,m)}$ in the seven classes presented in this paper, every nonzero codeword is minimal.

*Proof:* Every cyclic code $\mathcal{C}_{(1,v,p,m)}$ in the seven classes presented in this paper has parameters $[p^m-1,2m]$ and the weight distribution of either Table I or Table II. Note that $p\geq 3$.

If the code has the weight distribution of Table I, then it is easily verified that

$$\frac{w_{min}}{w_{max}}=\frac{(p-1)p^{(m-1)/2}-1}{(p-1)p^{(m-1)/2}+1}>\frac{p-1}{p},$$

provided that $m\geq 3$.

If the code has the weight distribution of Table II, then it is similarly verified that

$$\frac{w_{min}}{w_{max}}=\frac{(p-1)p^{(m-1)/2}-(p-1)/2}{(p-1)p^{(m-1)/2}+(p-1)/2}>\frac{p-1}{p},$$

provide that $m\geq 3$.

The desired conclusion then follows from Lemma 7.3. This completes the proof of this lemma. ■

The main result of this section is the following.

*Theorem 7.5:* Let $\mathcal{C}_{(1,v,p,m)}$ be any code in the seven classes of this paper, and let $G=[\mathbf{g}_0,\mathbf{g}_1,\cdots,\mathbf{g}_{n-1}]$ be its generator matrix. In the secret sharing scheme based on $\mathcal{C}^{\perp}_{(1,v,p,m)}$, the total number of participants is equal to $p^m-2$ and there are altogether $p^{2m-1}$ minimal access sets. In addition, we have the following:

Ca If $\mathbf{g}_i$ is a multiple of $\mathbf{g}_0$, $1\leq i\leq p^m-2$, then participant $P_i$ must be in every minimal access set. Such a participant is called a *dictatorial participant*.

Cb If $\mathbf{g}_i$ is not a multiple of $\mathbf{g}_0$, $1\leq i\leq p^m-2$, then participant $P_i$ must be in $(p-1)p^{2m-2}$ out of $p^{2m-1}$ minimal access sets.

*Proof:* The desired conclusions follow from Theorem 7.2 and Lemma 7.4. ■

The access structure of the secret sharing scheme based on $\mathcal{C}^{\perp}_{(1,v,p,m)}$ has only two possible cases described in Theorem 7.5. In Case Ca, there is a dictator in the scheme who must be in every minimal access set, while the other participants have equal importance in the scheme. In Case Cb, every participant has equal importance in the scheme. Both access structures are interesting as they may be required in different scenarios.

For many of the cyclic codes presented in this paper, the prime $p$ is either 3 or 5. So the space $\mathbb{Z}_p$ is too small. For real-world applications, a secret space should be of huge size. To employ the secret sharing schemes derived from the codes of this paper, each element of the secret space can be encoded into a sequence of elements from GF$(p)$ using an encoding rule, the elements of the sequence are then shared in order one by one by the participants.

## VIII. Summary and Concluding Remarks

The contributions of this paper include the construction of the seven classes of three-weight cyclic codes and the determination of their weight distributions. These cyclic codes are interesting and important due to the following:

1) They have only three nonzero weights and are interesting in certain applications such as the one in [3]. If a linear code over GF$(q)$ has a few weights, it is more likely that $w_{min}/w_{max}>(q-1)/q$. Such a code is interesting for the application in secret sharing as demonstrated in Section VII.
2) Some of the specific codes in the seven classes are optimal in the sense that their error-correcting capability is the best possible when the length and the dimension are fixed (see the codes in some of the examples in this paper).
3) When the codes presented in this paper are employed for error detection, the probability of an undetected error with respect to a communication channel could be computed. We elaborate on this statement a little below. When a codeword $\mathbf{c}$ in a linear code $\mathcal{C}$ is transmitted over a binary symmetric channel (BSC) with probability $\varepsilon$, errors may occur during transmission. If the received message is not a codeword in $\mathcal{C}$, we will be able to detect the error. However, if the received message is another codeword $\mathbf{c}'\neq\mathbf{c}$, we have no way to detect the error. Thus, we have a undetected error. Let $P_{ue}(\mathcal{C},BSC)$ denote the probability that this happens. It is known that [13, p. 38]

$$P_{ue}(\mathcal{C},BSC)=\sum_{i=1}^{n}A_i\varepsilon^i(1-\varepsilon)^{n-i},$$

where $(A_0, A_1, \cdots, A_n)$ denotes the weight distribution of the code $\mathcal{C}$.

Since the weight distributions of all the codes presented in this paper are known, we are able to compute this probability $P_{ue}(\mathcal{C}, BSC)$ exactly. In addition, since the codes have only three nonzero weights, the probability $P_{ue}(\mathcal{C}, BSC)$ may be smaller compared with many other codes. This is another advantage of the three-weight codes over other codes when they are used for error detection.

4) When the specific codes of this paper are employed for secret sharing, the access structure of the secret sharing schemes can be determined and is in fact very nice, as shown in Section VII. Note that every linear code gives a secret sharing scheme. It is believed that determining the access structure of the secret sharing scheme is very hard for linear codes in general.

The major mathematical difficulty overcome in this paper is the determination of the values of the exponential sums that are required in calculating the weight distributions of these cyclic codes. The technical breakthrough for computing the values of the exponential sums is the discovery of the noninvertible transformations described in Sections V and VI. It is well known that the weight distribution problem for cyclic codes is in general very hard and it is settled for only a very small number of classes of codes.

## Acknowledgments

The authors are very grateful to the reviewers and the Associate Editor, Dr. Lara Dolecek, for their comments and suggestions that improved the presentation and quality of this paper.

## References

[1] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 2010–2017, 1998.

[2] N. Boston and G. McGuire, "The weight distributions of cyclic codes with two zeros and zeta functions," *J. Symbolic Comput.,* vol. 45, no. 7, pp. 723–733, July 2010.

[3] A. R. Calderbank and J. M. Goethals, "Three-weight codes and association schemes," *Philips J. Res.,* vol. 39, pp. 143–152, 1984.

[4] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Trans. Inf. Theory,* vol. 51, no. 6, pp. 2089–2102, June 2005.

[5] S.-T. Choi, J.-Y. Kim, J.-S. No, and H. Chung, "Weight distribution of some cyclic codes," in *Proc. 2012 International Symposium on Information Theory,* pp. 2911–2913.

[6] C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo, and M.Mishima, "Sets of frequency hopping sequences: bounds and optimal constructions," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3297–3304, July 2009.

[7] C. Ding, Y. Liu, C. Ma, and L. Zeng, "The weight distributions of the duals of cyclic codes with two zeros," *IEEE Trans. Inf. Theory,* vol. 57, no. 12, pp. 8000–8006, Dec. 2011.

[8] C. Ding and A. Salomaa, "Secret sharing schemes with nice access structures," *Fundamenta Informaticae,* vol. 71, nos. 1–2, pp. 65–79, 2006.

[9] K. Feng and J. Luo, "Value distribution of exponential sums from perfect nonlinear functions and their applications," *IEEE Trans. Inf. Theory,* vol. 53, no. 9, pp. 3035–3041, Sept. 2007.

[10] T. Feng, "On cyclic codes of length $2^{2^r}-1$ with two zeros whose dual codes have three weights," *Des. Codes Cryptogr.,* vol. 62, no. 3, pp. 253–258, Mar. 2012.

[11] I. Honkala and A. Tietäväinen, "Codes and number theory," in *Handbook of Coding Theory,* Vol. II, V. S. Pless and W. C. Huffman (Eds.), pp. 1143–1194. Elsevier, 1998.

[12] D. J. Katz, "Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth," *J. Comb. Theory Ser. A*, vol. 119, pp. 1644–1659, 2012.

[13] T. Kløve, *Codes for Error Detection.* World Scientific, 2007.

[14] 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.

[15] C. Ma, L. Zeng, Y. Liu, D. Feng, and C. Ding, "The weight enumerator of a class of cyclic codes," *IEEE Trans. Inf. Theory*, vol. 57, no.1, pp. 397–402, Jan. 2011.

[16] G. McGuire, "On three weights in cyclic codes with two zeros," *Finite Fields Appl.,* vol. 10, no. 1, pp. 97–104, Jan. 2004.

[17] J. H. van Lint, *Introduction to Coding Theory,* 3rd ed. Springer-Verlag, 1999.

[18] G. Vega, "The weight distribution of an extended class of reducible cyclic codes," *IEEE Trans. Inf. Theory,* vol. 58, no. 7, pp. 4862–4869, July 2012.

[19] G. Vega and C. A. Vázquez, "The weight distribution of a family of reducible cyclic codes," in *Arithmetic of Finite Fields,* Lecture Notes in Computer Science 7369, Springer-Verlag, 2012, pp. 16–28.

[20] B. Wang, C. Tang, Y. Qi, Y. Yang, and M. Xu, "The weight distributions of cyclic codes and elliptic curves," *IEEE Trans. Inf. Theory,* vol. 58, no. 12, pp. 7253–7259, Dec. 2012.

[21] 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, Nov. 2010.

[22] M. Xiong, "The weight distributions of a class of cyclic codes," *Finite Fields Appl.,* vol. 18, no. 5, pp. 933–945, Sept. 2012.

[23] M. Xiong, "The weight distributions of a class of cyclic codes II," *Des. Codes Cryptogr.,* to appear.

[24] J. Yuan, C. Carlet, and C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," *IEEE Trans. Inf. Theory,* vol. 52, no. 2, pp. 712–717, Feb. 2006.

[25] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Trans. Inf. Theory,* vol. 52, no.1, pp. 206–212, Jan. 2006.

[26] Z. Zhou and C. Ding, "A class of three-weight cyclic codes," arXiv:1302.0569, 2013.

**Zhengchun Zhou** received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in information security from Southwest Jiaotong University, Chengdu, China, in 2001, 2004, and 2010, respectively. From 2012 to 2013, he was a postdoctoral member in the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology. He is currently an associate professor with the School of Mathematics, Southwest Jiaotong University. His research interests include sequence design and coding theory.

**Cunsheng Ding** (M'98–SM'05) was born in 1962 in Shaanxi, China. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992 he was a Lecturer of Mathematics at Xidian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently Professor of Computer Science and Engineering, he was Assistant Professor of Computer Science at the National University of Singapore.

His research fields are cryptography and coding theory. He has coauthored four research monographs, and served as a guest editor or editor for ten journals. Dr. Ding co-received the State Natural Science Award of China in 1989.