Three-weight cyclic codes and their weight distributions

Cunsheng Ding a, Chunlei Li b, Nian Li c, Zhengchun Zhou d,∗

a Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong
b Department of Electrical Engineering and Computer Science, University of Stavanger, 4036, Stavanger, Norway
c Department of Informatics, University of Bergen, N-5020 Bergen, Norway
d School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China

Abstract

Cyclic codes have been an important topic of both mathematics and engineering for decades. They have been widely used in consumer electronics, data transmission technologies, broadcasting systems, and computer applications as they have efficient encoding and decoding algorithms. The objective of this paper is to provide a survey of three-weight cyclic codes and their weight distributions. Information about the duals of these codes is also given when it is available.

1. Introduction

Let q be a prime power. A linear [n, k, d; q] code over GF(q) is a k-dimensional subspace of GF(q)n with minimum nonzero (Hamming) weight d. An [n, k] linear code C over GF(q) is called cyclic if (c0, c1, . . . , cn−1) ∈ C implies (cn−1, c0, c1, . . . , cn−2) ∈ C. By identifying any vector (c0, c1, . . . , cn−1) ∈ GF(q)n with

\[ c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in GF(q)[x]/(x^n - 1), \]

any linear code C of length n over GF(q) corresponds to a subset of the ring GF(q)[x]/(x^n - 1). A linear code C is cyclic if and only if the corresponding subset in GF(q)[x]/(x^n - 1) is an ideal of the ring GF(q)[x]/(x^n - 1).

It is well known that every ideal of GF(q)[x]/(x^n - 1) is principal. Let \( C = (g(x)) \) be a cyclic code, where g(x) is monic and has the smallest degree among all the generators of 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 C. If the parity check polynomial h(x) of a code C of length n over GF(q) is the product of s distinct irreducible polynomials over GF(q), we say that the dual code \( C^\perp \) has s zeros.

Let \( A_i \) denote the number of codewords with Hamming weight i in a linear code C of length n. The weight enumerator of C is defined by

\[ 1 + A_1z + A_2z^2 + \cdots + A_nz^n. \]
The weight distribution \((1, A_1, \ldots, A_n)\) 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 \[39\]. Second, due to rich algebraic structures of cyclic codes, the weight distribution is often related to interesting and challenging problems in number theory. A code \(C\) is said to be a \(t\)-weight code if the number of nonzero \(A_i\) in the sequence \((A_1, A_2, \ldots, A_n)\) is equal to \(t\).

Cyclic codes have been widely used in consumer electronics, data transmission technologies, broadcast systems, and computer applications as they have efficient encoding and decoding algorithms. Cyclic codes with a few weights are of special interest in authentication codes as certain parameters of the authentication codes constructed from these cyclic codes are easy to compute \[22\], and in secret sharing schemes as the access structures of such secret sharing schemes derived from such cyclic codes are easy to determine \[8, 21, 62\]. Cyclic codes with a few weights are also of special interest in designing frequency hopping sequences \[17\]. Three-weight cyclic codes have also applications in association schemes \[3\]. These are some of the motivations for studying cyclic codes with a few weights.

There is a nice survey of two-weight linear codes by Calderbank and Kantor \[4\]. To the best of our knowledge, there is no such reference on two-weight cyclic codes in literature. The reader is referred to \[27\] and the references therein for recent progress in two-weight cyclic codes. The objective of this paper is to provide a survey on three-weight cyclic codes and their weight distributions. Information on the duals of these three-weight codes is also given when it is available.

The remainder of this paper is organized as follows. Section 2 fixes some notations for this paper. Section 3 surveys three-weight cyclic codes whose duals have only one zero. Section 4 gives a well-rounded treatment of three-weight cyclic codes. Section 5 presents a generic construction of three-weight cyclic codes. Section 6 introduces a method of shortening some three-weight cyclic codes. Section 7 makes some concluding remarks.

2. Some notations fixed throughout this paper

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

(a) \(p\) is a prime, and \(q\) is a positive power of \(p\).
(b) \(r = q^m\), where \(m\) is a positive integer.
(c) \(n\) denotes the length of a cyclic code over \(GF(q)\) and is either \(r - 1\) or a divisor of \(r - 1\).
(d) \(\mathbb{Z}_M = \{0, 1, \ldots, M - 1\}\) denotes the ring of integers modulo \(M\).
(e) \(\text{Tr}_{q^m/q}(\alpha)\) is the trace function from \(GF(q^m)\) to \(GF(q)\).
(f) \(C_2\) denotes the \(q\)-cyclotomic coset modulo \(n\) containing \(a\), where \(a\) is any integer with \(0 \leq a \leq n - 1\), and \(\ell_a := |C_a|\), which is the size of the \(q\)-cyclotomic coset \(C_a\).

3. Three-weight cyclic codes whose duals have one zero

Let \(N > 1\) be an integer dividing \(r - 1\), and put \(n = (r - 1)/N\). Let \(\gamma\) be a generator of \(GF(r)^*\) and let \(\theta = \gamma^N\). The set

\[
E(r, N) = \{(\text{Tr}_{r/q}(\beta), \text{Tr}_{r/q}(\beta\theta), \ldots, \text{Tr}_{r/q}(\beta\theta^{r-1})) : \beta \in GF(r)\}
\]

is called an \([n, m_0]\) irreducible cyclic code over \(GF(q)\), where \(\text{Tr}_{r/q}\) is the trace function from \(GF(r)\) onto \(GF(q)\), \(m_0\) is the multiplicative order of \(q\) modulo \(n\) and \(m_0\) divides \(m\). The parity-check polynomial of \(E(r, N)\) is the minimal polynomial over \(GF(q)\) of \(\theta - 1\) and is irreducible.

Irreducible cyclic codes are an interesting topic of study for decades. The celebrated Golay code is an irreducible cyclic code and was used on the Mariner Jupiter–Saturn Mission. Irreducible cyclic codes form a special class of cyclic codes and are interesting in theory as they are minimal cyclic codes. The total number of nonzero Hamming weights in an irreducible cyclic code could be any positive integer. Their weight distributions are extremely complicated. The reader is referred to \[23\] for information on the weight distribution of irreducible codes.

The following theorem documents a class of three-weight irreducible cyclic codes \[13,23\].

**Theorem 3.1.** Let \(N\) be a divisor of \(r - 1\). When \(\gcd((r - 1)/(q - 1), N) = 3\) and \(p \equiv 1 \pmod{3}\), the set \(E(r, N)\) in (1) is a \([(q^m - 1)/N, m]\) code with the following weight enumerator:

\[
1 + \frac{r - 1}{3} z^\frac{(q-1)(r-c_1d_1^2)}{N} + \frac{r - 1}{3} z^\frac{(q-1)(r+c_1\sqrt{d_1})}{N} + \frac{r - 1}{3} z^\frac{(q-1)(r+c_1\sqrt{-d_1})}{N},
\]

where \(c_1\) and \(d_1\) are uniquely given by \(4q^{m/3} = c_1^2 + 27d_1^2, c_1 \equiv 1 \pmod{3}\) and \(\gcd(c_1, p) = 1\).

4. Three-weight cyclic codes whose duals have two zeros

In this section, we deal with three-weight cyclic codes whose duals have two zeros, and distinguish between the binary and nonbinary cases. We will also discuss relations between the weight distribution of a cyclic code whose dual has two zeros and the correlation value distribution of two related maximum-length sequences.
4.1. Perfect and almost perfect nonlinear functions on GF(r)

A function $f : GF(r) \rightarrow GF(r)$ is called almost perfect nonlinear (APN) if

$$\max_{a \in GF(r)^*} \max_{b \in GF(r)} |\{x \in GF(r) : f(x + a) - f(x) = b\}| = 2,$$

and is referred to as perfect nonlinear or planar if

$$\max_{a \in GF(r)^*} \max_{b \in GF(r)} |\{x \in GF(r) : f(x + a) - f(x) = b\}| = 1.$$

There is no perfect nonlinear (planar) function on $GF(q^m)$ for even $q$. However, there are APN functions on $GF(2^m)$. Both planar and APN functions over $GF(q^m)$ for odd $q$ exist [7]. Some planar and APN monomials will be employed to construct three-weight cyclic codes in subsequent sections.

4.2. Three-weight cyclic codes whose duals have two zeros

Throughout this section let $n = r - 1 = q^m - 1$. Let $\gamma$ be a generator of the multiplicative group $GF(r)^*$. For any $0 \leq a \leq r - 2$, denote by $m_a(x)$ the minimal polynomial of $\gamma^{-a}$ over $GF(q)$.

Let $1 \leq u \leq r - 2$ and $1 \leq v \leq r - 2$ be any two integers such that $C_u \cap C_v = \emptyset$. Let $C_{(u,v,q,m)}$ be the cyclic code over $GF(q)$ with length $n$ whose codewords are given by

$$c(a, b) = (c_0, c_1, \ldots, c_{m-1}), \quad \forall (a, b) \in GF(qu) \times GF(qv),$$

where $\ell_u$ is the size of the $q$-cyclovlatic coset $C_u$ and
denotes $\ell_u \gamma^\ell_p \gamma^{\ell_q}$, $0 \leq i \leq n - 1$.

By Delsarte’s Theorem, the code $C_{(u,v,q,m)}$ has parity-check polynomial $m_u(x)m_v(x)$ and dimension $\ell_u + \ell_v$. The code $C_{(u,v,q,m)}$ may have many nonzero weights. In the sequel we will focus on those codes $C_{(u,v,q,m)}$ with exactly three nonzero weights, and always assume that $C_u \cap C_v = \emptyset$. Hence $m_u(x)$ and $m_v(x)$ are always distinct.

The Hamming weight $WT(c(a, b))$ of the codeword $c(a, b)$ of (2) in $C_{(u,v,q,m)}$ is given by

$$WT(c(a, b)) = \frac{(q - 1)r}{q} - \frac{1}{q} \sum_{\gamma \in GF(q)^*} \sum_{x \in GF(r)} \chi(axy^u + bxy^v),$$

where $\chi$ is the canonical additive character of $GF(r)$.

There are a lot of references on the codes $C_{(u,v,q,m)}$ (see for example [2,20,28,29,47–49,54–56,59,60]). It is obvious that $C_{(u,v,q,m)}$ cannot be a constant-weight code as its parity-check polynomial has two zeros. It was shown in [57] that $C_{(u,v,q,m)}$ could be a two-weight code for $q > 2$ and some special $u$ and $v$. However, the code $C_{(u,v,q,m)}$ has at least three nonzero weights in general. Hence it is very interesting to study three-weight cyclic codes $C_{(u,v,q,m)}$.

4.3. Weights in $C_{(1,v,q,m)}$ and the crosscorrelation values of two periodic sequences

As before, let $\gamma$ be a generator of $GF(r)^*$. Define a sequence $s^\infty = (s_i)_{i=0}^\infty$ where

$$s_i = Tr_{1/q}(\gamma^i), \quad i \geq 0.$$

The sequence $s^\infty$ has least period $r - 1$ and is called a maximum-length sequence over $GF(q)$. Let $v$ be any integer with $1 \leq v \leq r - 2$. The $v$-decimated version of the sequence $s^\infty$ is denoted by $s(v)^\infty$ and defined by

$$s(v)_i = Tr_{1/q}(\gamma^{iv}), \quad i \geq 0.$$

The sequence $s(v)^\infty$ has least period $(r - 1)/\text{gcd}(r - 1, v)$. When and only when $\text{gcd}(r - 1, v) = 1$, the sequence $s(v)^\infty$ is a maximum-length sequence.

Let $\chi_q$ and $\chi$ be the canonical additive characters of $GF(q)$ and $GF(r)$ respectively. The crosscorrelation value at $0 \leq \tau \leq r - 2$ of the two sequences $s(v)^\infty$ and $s^\infty$ is defined by

$$C_v(\tau) = \sum_{i=0}^{r-2} \chi_q(s(v)_{i+\tau} - s_i)
= \sum_{i=0}^{r-2} \chi_q(\text{Tr}_{1/q}(\gamma^{i\tau} \gamma^v - \gamma^i))
= -1 + \sum_{x \in GF(r)} \chi(\gamma^{i\tau} x^v - x).$$

\[\text{(4)}\]
We now consider the Hamming weights in the code $C_{(1,v,q,m)}$ under the condition that $\gcd(v, r - 1) = 1$. It follows from (3) that

$$\WT(c(0, b)) = \frac{(q - 1)r}{q} - \frac{1}{q} \sum_{y \in GF(q)} \sum_{x \in GF(r)} \chi(byx^r) = \frac{(q - 1)r}{q}$$

for all $b \in GF(r)^*$. Similarly, we have

$$\WT(c(a, 0)) = \frac{(q - 1)r}{q} - \frac{1}{q} \sum_{y \in GF(q)} \sum_{x \in GF(r)} \chi(axy) = \frac{(q - 1)r}{q}$$

for all $a \in GF(r)^*$.

Now we assume that $ab \neq 0$. In this case we have

$$\sum_{x \in GF(r)} \chi(axy + byx^r) = \sum_{x \in GF(r)} \chi((y^{\tau(a,b,y)}y^m - z)$$

where $0 \leq \tau(a, b, y) \leq r - 2$ is the unique integer such that

$$(y^r)^{\tau(a,b,y)} = \frac{b}{(-a)^v}y^{1-v}.$$  

(5)

Note that such $\tau(a, b, y)$ must exist as $y^v$ is also a generator of $GF(r)^*$. It then follows from (3) that

$$\WT(c(a, b)) = \frac{(q - 1)r}{q} - \frac{1}{q} \sum_{y \in GF(q)} \sum_{x \in GF(r)} \chi(axy^r + byx^r)$$

$$= \frac{(q - 1)r}{q} - \frac{1}{q} \sum_{y \in GF(q)^*} (1 + C_v(\tau(a, b, y))).$$  

(6)

Hence, we have the following remarks about the correlation value distribution of the two sequences $s^\infty$ and $s(v)^\infty$ and the weight distribution of the code $C_{(1,v,q,m)}$.

(a) It should be noted that the code $C_{(1,v,q,m)}$ may have more or less than $\ell$ weights even if the correlation function of the two sequences $s^\infty$ and $s(v)^\infty$ takes on $\ell$ different values.

(b) When $\gcd(v, r - 1) \neq 1$, one may not be derived from the other.

(c) When $\gcd(v, r - 1) = 1$ and $v - 1 \equiv 0 \pmod{q - 1}$, it follows from (5) that

$$\frac{b}{(-a)^v}y^{1-v} = \frac{b}{(-a)^v}$$

which is independent of $y \in GF(q)^*$. In this special case, (6) becomes

$$\WT(c(a, b)) = \frac{(q - 1)r}{q} \left[r - 1 - C_v(\tau(a, b, y))\right].$$  

(7)

where $ab \neq 0$. Thus in this case the determination of the weight distribution of the code $C_{(1,v,q,m)}$ is equivalent to that of the correlation value distribution of the two sequences $s^\infty$ and $s(v)^\infty$.

The formula in (7) was already observed by Katz [38]. However, our discussion in this section may give more information on the coding theory problem and the sequence problem, as the formula of (6) is new.

4.4. Binary cyclic codes $C_{(u,v,2,m)}$ with three weights

In this subsection, we consider the codes $C_{(u,v,q,m)}$ for the case that $q = 2$. McGuire tried to give a classification of the codes $C_{(v,v,2,m)}$ with three-weights, and proved some nonexistence results [48]. The objective of this section is to introduce known three-weight codes $C_{(v,v,2,m)}$ together with their weight distributions.

4.4.1. Binary three-weight cyclic codes $C_{(1,v,2,m)}$ from some monomials

In this subsection, we will describe three-weight binary cyclic codes $C_{(1,v,2,m)}$, where the integer $v$ is selected in such a way that $x^v$ is highly nonlinear over $GF(2^m)$. The following is a list of known APN monomials $x^v$ over $GF(2^m)$.

1. $v = 2^m - 2$, where $m$ is odd [150].
2. $v = 2^h + 1$ with $\gcd(h, m) = 1$, where $1 \leq h \leq (m - 1)/2$ if $m$ is odd and $1 \leq h \leq (m - 2)/2$ if $m$ is even [31].
3. $v = 2^{2h} - 2^h + 1$ with $\gcd(h, m) = 1$, where $1 \leq h \leq (m - 1)/2$ if $m$ is odd and $1 \leq h \leq (m - 2)/2$ if $m$ is even [36].
4. $v = 2^{(m-1)/2} + 3$, where $m$ is odd [24,35].
5. $v = 2^{(m-1)/2} + 2^{(m-1)/4} - 1$, where $m \equiv 1 \pmod{4}$ [25,35].
6. $v = 2^{(m-1)/2} + 2^{(3m-1)/4} - 1$, where $m \equiv 3 \pmod{4}$ [25,35].
7. $v = 2^i + 2^{2i} + 2^{3i} + 2^i - 1$, where $m = 5i$ [25].
Some of these APN monomials yield three-weight codes, while others do not. Hence, the APN property of the monomial \( x^v \) does not guarantee that the code \( C_{(1,v,2,m)} \) has three weights. Conversely, the APN property is not necessary for the code \( C_{(1,v,2,m)} \) to be a three-weight code.

The following theorem describes all three-weight cyclic subcodes of the shortened second-order Reed–Muller codes. Kasami first obtained the weight distributions of these codes [37]. Goethals described a method for analyzing these codes [30]. Calderbank and Goethals investigated the relations between these three-weight codes and association schemes [3]. Further information about these codes may be found in MacWilliams and Sloane [46, Chapter 15] and Schoof [52].

**Theorem 4.1** ([37,30,31]). Let \( m \geq 4 \) and \((u, v) = (1, 2^e + 1)\) for some integer \( e \leq m/2 \). Then \( C_{(1,v,2,m)} \) is a three-weight code if and only if either \( m \) is odd and \( \gcd(n, v) = 1 \) or \( m \) is even and \( v = 2^{m/2} + 1 \), where \( n = 2^m - 1 \).

The weight distribution of these codes can be described as follows.

When \( \gcd(n, v) = 1 \), we have \( \gcd(m, 2e) = \gcd(m, e) \). Define \( l = (m - \gcd(m, e)) / 2 \). Then the dimension of \( C_{(1,v,2,m)} \) is \( 2m \), and the weight distribution of \( C_{(1,v,2,m)} \) is given in Table 1. The dual code of \( C_{(1,v,2,m)} \) has parameters \([n, n - 2m, d^\perp] \), where

\[
d^\perp = \begin{cases} 
3 & \text{if } \gcd(e, m) > 1; \\
5 & \text{if } \gcd(e, m) = 1. 
\end{cases}
\]

When \( m \) is even and \((u, v) = (1, 2^{m/2} + 1)\), the dimension of \( C_{(1,v,2,m)} \) is \( 3m/2 \) and the weight distribution of \( C_{(1,v,2,m)} \) is given in Table 2. The dual code of \( C_{(1,v,2,m)} \) has parameters \([n, n - 3m/2, 3] \).

The following theorem describes a few classes of the codes \( C_{(1,v,2,m)} \) with three weights. The proof of the following theorem follows directly from (7) and the correlation value distribution of the two sequences \( s^\infty \) and \( s^v \) in the corresponding references on sequences. Note that the determination of the weight distribution of the code \( C_{(1,v,2,m)} \) is equivalent to that of the crosscorrelation of \( s^\infty \) and \( s^v \) because \( q = 2 \) and \( \gcd(v, 2^m - 1) = 1 \) for all the \( v \)'s in Theorem 4.2.

**Theorem 4.2.** The binary cyclic code \( C_{(1,v,2,m)} \) has dimension \( 2m \) and the weight distribution of Table 1, where \( l = (m - 1)/2 \) for odd \( m \) and \( l = (m - 2)/2 \) for even \( m \), for the following \( v \):

- (a) \( v = 2^{2h} - 2^h + 1 \), where \( m/\gcd(h, m) \) is odd [36].
- (b) \( v = 2^{(m-1)/2} + 3 \), where \( m \) is odd [35].
- (c) \( v = 2^{(m-1)/2} + 2^{(m-1)/4} - 1 \), where \( m \equiv 1 \pmod{4} [25,35] \).
- (d) \( v = 2^{(m-1)/2} + 2^{(m-3)/4} - 1 \), where \( m \equiv 3 \pmod{4} [25,35] \).
- (e) \( v = 2^{(m+2)/2} + 3 \), where \( m \equiv 2 \pmod{4} [11] \).
- (f) \( v = 2^{m/2} + 2^{(m+2)/4} + 1 \), where \( m \equiv 2 \pmod{4} [11] \).

It is known that the duals of the codes in Theorem 4.2 have parameters \([2^m - 1, 2^m - 1 - 2m, 5] \) and are optimal [6]. Theorem 4.1 has the same conclusion for the exponent \( v = 2^e + 1 \) with \( \gcd(e, m) = 1 \).

4.4.2. Binary three-weight cyclic codes \( C_{(u,v,2,m)} \) with dimension \( 3m/2 \)

**Theorem 4.3.** Let \( m \) be even and let \( h \) be an integer such that \( 1 \leq h \leq m - 1 \) and \( h \neq m/2 \). Define

\[
\hat{h} = \gcd(m/2, h), \quad \tilde{h} = \gcd(h + m/2, 2h), \quad u = 2^{m/2} + 1, \quad v = 2^h + 1.
\]

Then \( C_{(u,v,2,m)} \) is an \([n, 3m/2] \) binary cyclic code with the weight distribution given in Table 3 if \( \tilde{h} = 2\hat{h} \).
The codes of Theorem 4.3 and their weight distributions were described in [45], where the authors also proved that \( C_{(u,v,2,m)} \) is a four-weight binary cyclic code in the case of \( h = \hat{h} \).

The following theorem gives another family of cyclic codes \( C_{(u,v,2,m)} \) with dimension \( 3m/2 \) [40].

**Theorem 4.4.** Let \( m \geq 2 \) be even. Let \( u = 2^{m/2} + 1 \), and let \( v = v_1(2^{m/2} - 1) + 1 \) with \( v_1 \equiv \frac{1}{2} \pmod{2^{m/2} + 1} \), where \( \frac{1}{2} \) represents the inverse of 2 modulo \( 2^\frac{m}{2} + 1 \). Define \( \ell = \gcd(2v_1 - 1, 2^{m/2} + 1) \). Then \( C_{(u,v,2,m)} \) is an \([n, 3m/2]\) binary cyclic code with the weight distribution given in Table 4.

### 4.5. Nonbinary cyclic codes \( C_{(u,v,q,m)} \) with three weights

We consider the codes \( C_{(u,v,q,m)} \) for the case \( q > 2 \) in this subsection. Note that in this case, the determination of the crosscorrelation value distribution of two maximum-length sequences may not be equivalent to that of the weight distribution of the corresponding cyclic code. However, as made clear in Section 4.3, the two problems are equivalent in the special case that \( \gcd(v, q^m - 1) = 1 \) and \( v - 1 \equiv 0 \pmod{q - 1} \). If this happens in some case in this section, we will point it out.

#### 4.5.1. Three-weight cyclic codes from the pair \((u,v) = (q - 1, q + 1)\)

The following is a class of three-weight cyclic codes documented in [42].

**Theorem 4.5.** Let \( q \) be even and \( m = 2 \). Define \( u = q - 1 \) and \( v = q + 1 \). Then \( C_{(u,v,q,m)} \) is a \([q^2 - 1, 3]\) three-weight cyclic code over GF\((q)\) with the weight distribution in Table 5.

### 4.5.2. Three-weight cyclic codes from planar functions

In this subsection, we introduce three-weight cyclic codes \( C_{(1,v,q,m)} \) over GF\((q)\) defined by planar monomials \( x^v \) over GF\((q)\). The following is a list of known planar monomials \( x^v \) over GF\((q)\), where \( q \) is an odd prime:

- (a) \( v = q^6 + 1 \), where \( m \slash \gcd(m, h) \) is odd [12].
- (b) \( v = (3^h + 1)/2 \), where \( q = 3, h \) is odd, and \( \gcd(m, h) = 1 \) [10].

Planar functions were employed to construct nonbinary cyclic codes in [8,61]. Some of them are three-weight codes and are described in the following theorem. Note that any planar monomial \( x^v \) over GF\((q)\) gives automatically a cyclic code \( C_{(1,v,q,m)} \) over GF\((q)\). However, the converse is not true.

<table>
<thead>
<tr>
<th>Weight ( w )</th>
<th>No. of codewords ( A_w )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( 2^{m-1} - (2\ell - 1)2^{(m-2)/2} )</td>
<td>( \frac{(2^{m-1}2^{m/2} - (\ell + 1))}{2^\ell} )</td>
</tr>
<tr>
<td>( 2^{m-1} - (\ell - 1)2^{(m-2)/2} )</td>
<td>( \frac{(2^{m-1}2^{m/2} - 2^{(m/2 - 1)})}{2^\ell} )</td>
</tr>
<tr>
<td>( 2^{m-1} + 2^{(m-2)/2} )</td>
<td>( 2^{m/2} - 1 + \frac{(2^{m-1}2^{m/2} - 1)(2^{m/2} + 1)}{2^\ell} )</td>
</tr>
</tbody>
</table>

### Table 3
Weight distribution of the codes of Theorem 4.3.

<table>
<thead>
<tr>
<th>Weight ( w )</th>
<th>No. of codewords ( A_w )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( 2^{n/2} - 2^{n/2-1} )</td>
<td>( \frac{2^n(q-1)(q^2-1)}{2^{n/2}} )</td>
</tr>
<tr>
<td>( 2^n - 2^{n/2} )</td>
<td>( q^2 - 1 )</td>
</tr>
<tr>
<td>( 2^n - 1 )</td>
<td>( q - 1 )</td>
</tr>
</tbody>
</table>

### Table 4
Weight distribution of the codes of Theorem 4.4.

<table>
<thead>
<tr>
<th>Weight ( w )</th>
<th>No. of codewords ( A_w )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( q^2 - q - 1 )</td>
<td>( (q - 1)(q^2 - 1) )</td>
</tr>
<tr>
<td>( q^2 - q )</td>
<td>( q^2 - 1 )</td>
</tr>
<tr>
<td>( q^2 - 1 )</td>
<td>( q - 1 )</td>
</tr>
</tbody>
</table>

### Table 5
Weight distribution of the codes of Theorem 4.5.

<table>
<thead>
<tr>
<th>Weight ( w )</th>
<th>No. of codewords ( A_w )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( q^2 - q - 1 )</td>
<td>( (q - 1)(q^2 - 1) )</td>
</tr>
<tr>
<td>( q^2 - q )</td>
<td>( q^2 - 1 )</td>
</tr>
<tr>
<td>( q^2 - 1 )</td>
<td>( q - 1 )</td>
</tr>
</tbody>
</table>
Corollary 4.8

Theorem 4.6

Theorem 4.9.

In this subsection, we introduce three-weight cyclic codes \( C_{(1,v,q,m)} \) over \( \text{GF}(q) \) defined by highly nonlinear monomials \( x^v \) over \( \text{GF}(q) \). We first introduce a general construction of three-weight cyclic codes as follows [41].

Theorem 4.10

Let \( m \geq 3 \) be odd, and let \( q \) be any odd prime. If \( v \) is an integer satisfying \( (q^h + 1) \equiv 2 \pmod{q^m - 1} \) for some positive integer \( h \), then \( C_{(1,v,q,m)} \) is a \([q^m - 1, 2m] \) cyclic code with the weight distribution of

(a) Table 7 when \( v \equiv 1 + (q - 1)/2 \pmod{q - 1} \); and
(b) Table 8 when \( v \equiv 1 \pmod{q - 1} \),

where \( e = \gcd(m, h) \).
Corollary 4.11. Let $q = 3$. Then $C_{(1,v,q,m)}$ is a $[q^m - 1, 2m]$ cyclic code over $GF(q)$ with the weight distribution in Table 7 for the following $m$ and $v$:

(a) $m$ is odd and $v = (3^{m+1} - 1)/4$ [18].
(b) $m$ is odd and $v = 3^{(m+1)/2} - 1$ [65].
(c) $m \equiv 3 \pmod{4}$ and $v = (3^{(m+1)/2} - 1)/2$ [65].
(d) $m \equiv 1 \pmod{4}$ and $v = (3^{(m+1)/2} - 1)/2 + (3^m - 1)/2$ [65].
(e) $m \equiv 3 \pmod{4}$ and $v = 3^{m+1}/8$ [65].
(f) $m \equiv 1 \pmod{4}$ and $v = \frac{3^{m+1}-1}{8} + \frac{3^m-1}{2}$ [65].
(g) $m \equiv 3 \pmod{4}$ and $v = \left(3^{(m+1)/4} - 1\right) \left(3^{(m+1)/2} + 1\right)$ [65].
(h) $m \equiv 2^t - 1 \pmod{2^t}$ for any integer $t \geq 2$ and

$$v = \left(3^{(m+1)/2^h} - 1\right) \prod_{l=1}^{h-1} 3^{(m+1)/2^l} + 1$$

for any $h$ with $2 \leq h \leq t$ [18, 41].

It was proved in [19] that the duals of the codes of Corollary 4.11 have parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ and are optimal.

The following corollary describes two classes of three-weight cyclic codes, which were proved in [65], and are special cases of Theorem 4.10.

Corollary 4.12 ([65]). Let $q = 5$. Then $C_{(1,v,q,m)}$ is a $[q^m - 1, 2m]$ cyclic code over $GF(q)$ with the weight distribution in Table 7, where $e = 1$, for the following $m$ and $v$:

(a) $m$ is odd and $v = \frac{5^{m-1}}{4} + \frac{5^{(m+1)/2} - 1}{2}$.
(b) $m$ is odd, $v = \frac{5^{h+1}}{2}$ and $\gcd(2m, h) = 1$. 

Theorem 4.10 is a unification and also a generalization of many classes of three-weight codes documented in [9, 18, 65], where most of the constructions are based on APN monomials. The following is a summary of known APN monomials $x^e$ over $GF(q^m)$ where $q$ is an odd prime:

1. $v = 3$, where $q > 3$ [34].
2. $v = 3^{(m+1)/2} - 1$ [34].
3. $v = q^m - 2$, where $q > 2$ and $q \equiv 2 \pmod{3}$ [34].
4. $v = \frac{q^m - 1}{q - 2}$, where $q^m = 3, 7 \pmod{20}, q^m = 7, q^m \neq 27$ and $m$ is odd [34].
5. $v = \frac{q^m + 1}{2} + \frac{q^m - 1}{2}$, where $q^m = 3 \pmod{8}$ [34].
6. $v = \frac{q^m + 1}{4}$, where $q^m = 7 \pmod{8}$ [34].
7. $v = \frac{2q^m - 1}{q - 2}$, where $q^m = 2 \pmod{3}$ [34].
8. $v = q^m - 3$, where $q = 3$ and $m$ is odd [34].
9. $v = q^m + 2$, where $q^m \equiv 1 \pmod{3}$ and $m = 2l$ [34].
10. $v = \frac{q^m + 1}{2}$, where $q = 5$ and $\gcd(2m, h) = 1$ [34].
11. $v = (3^{(m+1)/4} - 1) (3^{(m+1)/2} + 1)$, where $m \equiv 3 \pmod{4}$ and $q = 3$ [63].

12. Let $q = 3$, and

$$v = \begin{cases} \frac{3^{(m+1)/2} - 1}{2} & \text{if } m \equiv 3 \pmod{4} \\ \frac{3^{(m+1)/2} - 1}{2} + \frac{3^m - 1}{2} & \text{if } m \equiv 1 \pmod{4} \end{cases}$$

[63]

13. Let $q = 3$, and

$$v = \begin{cases} \frac{3^{m+1} - 1}{8} & \text{if } m \equiv 3 \pmod{4} \\ \frac{3^{m+1} - 1}{8} + \frac{3^m - 1}{2} & \text{if } m \equiv 1 \pmod{4} \end{cases}$$

[63]

14. $v = \frac{5^{m-1}}{4} + \frac{5^{(m+1)/2} - 1}{2}$, where $q = 5$ and $m$ is odd [63].

It is noted that some of the APN monomials above do not yield a three-weight cyclic code over $GF(q)$, while others do. The following corollary describes eight classes of three-weight cyclic codes, which were proved in [65, 18, 41], and are special cases of Theorem 4.10.
The following corollary documents three classes of three-weight cyclic codes, which are special cases of Theorem 4.10.

**Corollary 4.13** ([18]). Let \( m \geq 3 \) be odd and let \( q = 3 \). Then \( C_{1,v,q,m} \) is a \( [q^m - 1, 2m] \) cyclic code over \( GF(q) \) with the weight distribution in Table 8, where \( e = 1 \), if \( v \) takes on one of the following:

(a) \( v = (3^{m+1} - 1) / 4 + (3^m - 1) / 2 \).
(b) \( v = (3^{(m+1)/8} - 1)(3^{(m+1)/4} + 1)(2^{(m+1)/2} + 1) + \frac{3^m - 1}{2} \), where \( m \equiv 7 \mod 8 \).
(c) \( v = (3^{(m+1)/4} - 1)(3^{(m+1)/2} + 1) + \frac{3^m - 1}{2} \), where \( m \equiv 3 \mod 4 \).

Note that \( \gcd(v, r - 1) = 1 \) and \( v - 1 \equiv 0 \mod (q - 1) \) for all the \( v \)'s listed in Corollary 4.13. It follows from the discussions in Section 4.3 and the weight distribution of the code \( C_{1,v,q,m} \) of Corollary 4.13 that the crosscorrelation function of any maximum-length sequence of period \( r - 1 \) over \( GF(q) \) and its \( v \)-decimated version takes on only the following three out-of-phase correlation values:

\[-1 + q^{(m+1)/2}, \quad -1, \quad -1 - q^{(m+1)/2}.\]

The following corollary follows from Theorem 4.10.

**Corollary 4.14** ([41]). Let \( m \geq 3 \) be odd and \( q \) be any odd prime. Let the sets \( S_t, t = 0, 1, \) be defined by

\[ S_t = \left\{ \frac{(q + 1)(q^m - 1) - 4q(q^{m+1} - 1)}{2(q - 1)} + \frac{i(q^m - 1)}{2}, \quad \frac{(q - 3)(q^m - 1) + 4(q^{m+1} - 1)}{2(q - 1)} + \frac{i(q^m - 1)}{2} \right\}.

(i) If \( v \in S_0 \), then \( C_{1,v,q,m} \) is a \( [q^m - 1, 2m] \) cyclic code with the weight distribution in Table 7, where \( e = 1 \).

(ii) If \( v \in S_1 \), then \( C_{1,v,q,m} \) is a \( [q^m - 1, 2m] \) cyclic code with the weight distribution in Table 8, where \( e = 1 \).

Note that \( \gcd(v, r - 1) = 1 \) and \( v - 1 \equiv 0 \mod (q - 1) \) for all the \( v \)'s listed in Corollary 4.14 (ii). It follows from the discussions in Section 4.3 and the weight distribution of the code \( C_{1,v,q,m} \) of Corollary 4.14 (ii) that the crosscorrelation function of any maximum-length sequence of period \( r - 1 \) over \( GF(q) \) and its \( v \)-decimated version takes on only three out-of-phase correlation values.

The three-weight codes of the following theorem are documented in [58,9] which are also special cases of Theorem 4.10.

**Theorem 4.15.** Let \( q \equiv 3 \mod 4 \) be an odd prime. Let \( m \) be an odd integer. Define \( v = (q^m + 1) / (q^2 + 1) + (q^m - 1) / 2 \), where \( e \) divides \( m \). Then \( C_{1,v,q,m} \) is a \( [q^m - 1, 2m] \) cyclic code over \( GF(q) \) with the weight distribution in Table 7.

Note that \( x^{(q^m+1)/(q^2+1)}(x^{q^m-1})/2 \) is APN when \( q = 3 \). This code of Theorem 4.15 is defined by APN monomials when \( q = 3 \).

**4.5.4. Three-weight cyclic codes from the Kasami–Welch–Trachtenberg functions**

The monomial \( x^v \) over a prime field \( GF(q) \) is called Kasami–Welch–Trachtenberg function if \( v = q^{2h} - q^h + 1 \) and \( m/\gcd(h, m) \) is odd [26]. For such a \( v \), we have the following.

**Theorem 4.16.** The code \( C_{1,v,q,m} \) has length \( q^m - 1 \), dimension \( 2m \) and the weight distribution of Table 8, where \( e = \gcd(h, m) \), if \( v = q^{2h} - q^h + 1 \) (or equivalently \( v = q^{m-h} + q^h - 1 \)), where \( m/e \) is odd and \( q \) is an odd prime.

**Proof.** For the two sequences \( s^\infty \) and \( s(v)^\infty \) defined in Section 4.3, it was proved in [53,33] that the crosscorrelation function takes on only the following three values

\[-1, \quad -1 \pm q^{(m+e)/2}.\]

where \( e = \gcd(h, m) \). Note that \( m/\gcd(h, m) \) is odd and \( q \) is an odd prime. It can be easily proved that \( \gcd(v, q^m - 1) = 1 \) and \( v - 1 \equiv 0 \mod (q - 1) \). It then follows from (7) that the code \( C_{1,v,q,m} \) has the following three weights

\[(q - 1)q^{m-1}, \quad (q - 1)(q^{m-1} \pm q^{(m+e)/2}).\]

The frequencies of the weights can be derived from the results in [53,33].

Note that \( q^{m-h} + q^h - 1 \) and \( q^{2h} - q^h + 1 \) are in the same \( q \)-cyclotomic coset modulo \( r - 1 \). Theorem 4.16 also holds for \( v = q^{m-h} + q^h - 1 \).

**4.5.5. Three-weight cyclic codes from the Trachtenberg–Helleseth functions**

**Theorem 4.17.** The code \( C_{1,v,q,m} \) has length \( q^m - 1 \), dimension \( 2m \) and the weight distribution of Table 8, where \( e = \gcd(h, m) \), if \( v = (q^{2h} + 1)/2, m/e \) is odd and \( q \) is an odd prime.
Theorem 4.20. Let $q$ be an odd prime and let $h$ be a positive integer such that $m / \text{gcd}(m, h)$ is odd. Define \[ u = \frac{q^m + 1}{2}, \quad v = \frac{q^h + 1}{2} \] and let $e = \text{gcd}(m, h)$. Then the cyclic code $C_{(u, v, q, m)}$ has only three weights under certain conditions. The following two theorems describe these three-weight cyclic codes.

Theorem 4.18. Let $q = 3$ and let $m$ be odd. If $\nu = 2 \times 3^{(m-1)/2} + 1$, then $C_{(1, v, q, m)}$ has dimension $2m$ and the weight distribution of Table 8, where $e = 1$.

Proof. For the two sequences $s^{\infty}$ and $s(\nu)^{\infty}$ defined in Section 4.3, it was proved in [26] that the correlation value distribution is

- $-1 + 3^{(m+1)/2}$ frequency $1/2 (3^{m-1} + 3^{(m+1)/2})$
- $-1/2 (3^m - 3^{m-1} - 1)$
- $-1 - 3^{(m+1)/2}$ frequency $1/2 (3^{m-1} - 3^{(m+1)/2})$.

Note that $m$ is odd and $q = 3$. It can be easily proved that $\gcd(v, q^m - 1) = 1$ and $v - 1 \equiv 0 \pmod{q - 1}$. The desired weight distribution of the code $C_{(1, v, q, m)}$ then follows from (7) and the correlation value distribution above.

4.5.6. Three-weight cyclic codes from the generalized Welch functions

Theorem 4.19. Let $h$ be even and $e$ be odd. Then $C_{(u, v, q, m)}$ is a three-weight cyclic code with parameters $[q^m - 1, 2m, q^m - q^{m-1} - q^{-1}(q^{(m+e-2)/2})]$. Moreover the weight distribution of $C_{(u, v, q, m)}$ is given in Table 7.

Theorem 4.20. Let $h/e$ be odd. Then $C_{(u, v, q, m)}$ is a three-weight cyclic code with parameters $[q^m - 1, 2m, q^m - q^{m-1} - (q - 1)q^{(m+e-2)/2}]$. Moreover the weight distribution of $C_{(u, v, q, m)}$ is given in Table 8.

4.5.7. Three-weight cyclic codes from the pair $(u, v) = ((q^m + 1)/2, (q^h + 1)/2)$

In this subsection, let $q$ be an odd prime and let $h$ be a positive integer such that $m / \text{gcd}(m, h)$ is odd. Define

\[ u = \frac{q^m + 1}{2}, \quad v = \frac{q^h + 1}{2} \]

and let $e = \text{gcd}(m, h)$. Then the cyclic code $C_{(u, v, q, m)}$ has only three weights under certain conditions. The following two theorems describe these three-weight cyclic codes.

4.5.8. Other three-weight cyclic codes $C_{(u, v, q, m)}$

Two classes of nonbinary three-weight cyclic codes $C_{(u, v, q, m)}$ are described in [44]. We omitted these codes here as it is not easy to describe these codes.

5. A generic construction of three-weight cyclic codes $C_{(u, v, q, m)}$

In this section, we present a generic construction of three-weight cyclic codes $C_{(u, v, q, m)}$, which is described in the following theorem.

Theorem 5.1. Let $C_{(1, v, q, m)}$ be a three-weight code with length $r - 1$. Then for any positive integer $u$ with $\gcd(u, r - 1) = 1$, $C_{(u, v, q, m)}$ is a two-weight code and $C_{(u, v, q, m)}$ has the same weight distribution as $C_{(1, v, q, m)}$.

Proof. Let $z = x^u$. Since $\gcd(u, r - 1) = 1$, $x^u$ is a permutation of $\text{GF}(r)$. Hence

\[ \sum_{x \in \text{GF}(r)} \chi(ax^u + bx^v) = \sum_{z \in \text{GF}(r)} \chi(az + bz^v) \]

for any $(a, b) \in \text{GF}(r)^2$. The desired conclusion then follows from [3] and the assumptions of this theorem.
6. Three-weight cyclic codes shortened from the codes $C_{(u,v,q,m)}$

Let $1 \leq u \leq r - 2$ and $1 \leq v \leq r - 2$ be any two integers such that $C_u \cap C_v = \emptyset$. Define

$$\bar{n} = \frac{r - 1}{\gcd(r - 1, u, v)}.$$  \hfill (8)

Let $\tilde{C}_{(u,v,q,m)}$ denote the cyclic code over GF$(q)$ with length $\bar{n}$ and parity-check polynomial $m_u(x)m_v(x)$. Then the dimension of $\tilde{C}_{(u,v,q,m)}$ is also $\ell_u + \ell_v$. Clearly, the code $\tilde{C}_{(u,v,q,m)}$ is a replication of $\tilde{C}_{(u,v,q,m)}$ altogether $\gcd(r - 1, u, v)$ times. By dividing all the nonzero weights in $C_{(u,v,q,m)}$ with $\gcd(r - 1, u, v)$, we obtain all the nonzero weights in $\tilde{C}_{(u,v,q,m)}$. The frequency of any weight $w_1$ in $C_{(u,v,q,m)}$ is the same as that of the corresponding weight $w_1/\gcd(r - 1, u, v)$ in $\tilde{C}_{(u,v,q,m)}$. Hence the weight distribution of the codes $\tilde{C}_{(u,v,q,m)}$ is settled also for all the codes discussed in this paper. Clearly, $\tilde{C}_{(u,v,q,m)}$ is a three-weight cyclic code if and only if $C_{(u,v,q,m)}$ is so. For example, the codes of Theorem 4.3 can be shortened in this way.

As an example, we demonstrate this shortening technique. Let $m_1$ and $m_2$ be two divisors of $m$ such that $\gcd(m_1, m_2) = 1$ and $\gcd(m_1 - m_2, q - 1) = 1$. Put

$$u = \frac{q^m - 1}{q^{m_1} - 1}, \quad v = \frac{q^m - 1}{q^{m_2} - 1}. $$

The code $C_{(u,v,q,m)}$ has length $n = q^m - 1$. We would now find out the dimension and weight distribution of the code $C_{(u,v,q,m)}$.

It is easy to check that

$$\gcd(r - 1, u, v) = \frac{(q - 1)(q^m - 1)}{(q^{m_1} - 1)(q^{m_2} - 1)}.$$  \hfill (9)

By definition,

$$\bar{n} = \frac{(q^{m_1} - 1)(q^{m_2} - 1)}{q - 1}. $$

The code $\tilde{C}_{(u,v,q,m)}$ has length $\bar{n}$ and its parameters are given in the following theorem [43].

**Theorem 6.1.** Let $m_1$ and $m_2$ be divisors of $m$ with $\gcd(m_1, m_2) = 1$ and $\gcd(m_1 - m_2, q - 1) = 1$. Define $u = (q^m - 1)/\left(q^{m_1} - 1\right)$ and $v = (q^m - 1)/\left(q^{m_2} - 1\right)$. Then $\tilde{C}_{(u,v,q,m)}$ is a $[\frac{(q^{m_1} - 1)(q^{m_2} - 1)}{q - 1}, m_1 + m_2]$ three-weight cyclic code over GF$(q)$ with the weight distribution in Table 9.

The following then follows from Theorem 6.1 and the discussions above.

**Theorem 6.2.** Let $m_1$ and $m_2$ be divisors of $m$ with $\gcd(m_1, m_2) = 1$ and $\gcd(m_1 - m_2, q - 1) = 1$. Define $u = (q^m - 1)/\left(q^{m_1} - 1\right)$ and $v = (q^m - 1)/\left(q^{m_2} - 1\right)$. Then $C_{(u,v,q,m)}$ is a $[q^m - 1, m_1 + m_2]$ three-weight cyclic code over GF$(q)$ with the weight distribution in Table 10, where $\gcd(r - 1, u, v)$ is given in (9).

The foregoing example shows that the weight distribution of any three-weight cyclic code over GF$(q)$ of length $q^m - 1$ can be employed to give the weight distribution of a three-weight cyclic code over GF$(q)$ of length $q^m - 1$. 

---

**Table 9**

<table>
<thead>
<tr>
<th>Weight $w$</th>
<th>No. of codewords $A_w$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0$</td>
<td>$1$</td>
</tr>
<tr>
<td>$q^{m_1} - (q^{m_2} - 1)$</td>
<td>$q^{m_1} - 1$</td>
</tr>
<tr>
<td>$q^{m_1} - (q^{m_2 - 1})$</td>
<td>$q^{m_2} - 1$</td>
</tr>
<tr>
<td>$q^{m_1} + m_2 - 1$ $- q^{m_1} - (q^{m_2 - 1})$</td>
<td>$(q^m - 1)(q^{m_2} - 1)$</td>
</tr>
</tbody>
</table>

**Table 10**

<table>
<thead>
<tr>
<th>Weight $w$</th>
<th>No. of codewords $A_w$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0$</td>
<td>$1$</td>
</tr>
<tr>
<td>$q^{m_1} - (q^{m_2} - 1) \gcd(r - 1, u, v)$</td>
<td>$q^{m_1} - 1$</td>
</tr>
<tr>
<td>$q^{m_2} - (q^{m_1} - 1) \gcd(r - 1, u, v)$</td>
<td>$q^{m_2} - 1$</td>
</tr>
<tr>
<td>$(q^{m_1} + m_2 - 1) - q^{m_1} - (q^{m_2 - 1}) \gcd(r - 1, u, v)$</td>
<td>$(q^m - 1)(q^{m_2} - 1)$</td>
</tr>
</tbody>
</table>
7. Concluding remarks

In this paper we surveyed only three-weight cyclic codes over finite fields. A number of constructions of three-weight linear codes are available in the literature, see, for example, [5,14–16,35,61,62]. The three-weight cyclic codes or their duals may give association schemes [3], authentication codes [22], secret sharing schemes [8,62], and frequency hopping sequences [17].

Acknowledgments

The authors are very grateful to the reviewers and the Associate Editor, Prof. Steven Thomas Dougherty, for their comments and suggestions that improved the presentation and quality of this paper.

References


