Discrete Mathematics 313 (2013) 434–446

Contents lists available at SciVerse ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Perspective

Hamming weights in irreducible cyclic codes[☆]

Cunsheng Ding[a], Jing Yang[b,*]

[a] Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

[b] Department of Mathematical Sciences, Tsinghua University, Beijing, 100084, China

ARTICLE INFO

Article history:
Received 23 February 2012
Received in revised form 5 November 2012
Accepted 7 November 2012
Available online 4 December 2012

Keywords:
Cyclic codes
Cyclotomy
Difference sets
Gaussian periods
Irreducible cyclic codes
Weight distribution

ABSTRACT

The objectives of this paper are to survey and extend earlier results on the weight distributions of irreducible cyclic codes, present a divisibility theorem and develop bounds on the weights in irreducible cyclic codes.

1. Introduction

Irreducible cyclic codes are an interesting type of codes and have applications in space communications. They have been studied for decades and a lot of progress has been made.

Throughout this paper, let p be a prime, $q = p^s$ for a positive integer s, and $r = q^m$ for a positive integer m. A linear $[n, k, d]$ code over $\mathrm{GF}(q)$ is a k-dimensional subspace of $\mathrm{GF}(q)^n$ with minimum (Hamming) distance d. 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

$$1 + A_1x + A_2x^2 + \cdots + A_nx^n.$$

A linear $[n, k]$ code $\mathcal{C}$ over the finite field $\mathrm{GF}(q)$ is called *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. Let $\gcd(n, q) = 1$. By identifying any vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathrm{GF}(q)^n$ with

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

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

Note that every ideal of $\mathrm{GF}(q)[x]/(x^n - 1)$ is principal. Let $\mathcal{C} = (g(x))$ be a cyclic code, where $g(x)$ is monic and $\deg(f)$ is minimal. Then $g(x)$ is called the *generator polynomial* and $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check* polynomial of $\mathcal{C}$.

☆ C. Ding's research is supported by the Hong Kong Research Grants Council, Project No. 600812. J. Yang's research is supported in part by the National Natural Science Foundation of China (No. 10990011, 11001145, 11101233), the Ph.D. Programs Foundation of Ministry of Education of China (No. 20090002120013), and the Science and Technology on Information Assurance Laboratory Foundation (No. KJ-12-01).

* Corresponding author.
E-mail addresses: cding@ust.hk (C. Ding), jingyang@math.tsinghua.edu.cn (J. Yang).

0012-365X/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2012.11.009

Let $N > 1$ be an integer dividing $r-1$, and put $n = (r-1)/N$. Let α be a primitive element of GF(r) and let $\theta = \alpha^N$. The set

$$\mathcal{C}(r, N) = \{(\mathrm{Tr}_{r/q}(\beta), \mathrm{Tr}_{r/q}(\beta\theta), \ldots, \mathrm{Tr}_{r/q}(\beta\theta^{n-1})) : \beta \in \mathrm{GF}(r)\} \tag{1}$$

is called an *irreducible cyclic* $[n, m_0]$ *code* over GF(q), where $\mathrm{Tr}_{r/q}$ 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.

Irreducible cyclic codes have been an interesting subject of study for many years. The celebrated Golay code is an irreducible cyclic code and was used on the Mariner Jupiter–Saturn Mission. They form a special class of codes and are interesting in theory as they are minimal cyclic codes. The weight distribution, i.e., the vector $(1, A_1, A_2, \ldots, A_{n-1})$, of the irreducible cyclic codes has been determined for a small number of special cases.

The objectives of this paper are to survey and extend earlier results on the weight distributions of irreducible cyclic codes (see Theorems 23, 21, 15, 17, 18, 19 and 20 as extensions and generalizations of earlier results), to completely characterize one-weight irreducible cyclic codes (Theorem 16), which is an extension of the result in [28], and to present a divisibility theorem and develop bounds on the weights in irreducible cyclic codes (see Theorems 24 and 13).

2. Group characters, cyclotomy, and Gaussian periods

In this section, we present results on group characters, cyclotomy and Gaussian sums which will be needed in the sequel.

2.1. Group characters and Gaussian sums

Let $\mathrm{Tr}_{q/p}$ denote the trace function from GF(q) to GF(p). An *additive character* of GF(q) is a nonzero function χ from GF(q) to the set of complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any pair $(x, y) \in \mathrm{GF}(q)^2$. For each $b \in \mathrm{GF}(q)$, the function

$$\chi_b(c) = e^{2\pi\sqrt{-1}\mathrm{Tr}_{q/p}(bc)/p} \quad \text{for all } c \in \mathrm{GF}(q) \tag{2}$$

defines an additive character of GF(q). When $b = 0$, $\chi_0(c) = 1$ for all $c \in \mathrm{GF}(q)$, and is called the *trivial additive character* of GF(q). The character χ_1 in (2) is called the *canonical additive character* of GF(q).

A *multiplicative character* of GF(q) is a nonzero function ψ from $\mathrm{GF}(q)^*$ to the set of complex numbers such that $\psi(xy) = \psi(x)\psi(y)$ for all pairs $(x, y) \in \mathrm{GF}(q)^* \times \mathrm{GF}(q)^*$. Let g be a fixed primitive element of GF(q). For each $j = 1, 2, \ldots, q-1$, the function ψ_j with

$$\psi_j(g^k) = e^{2\pi\sqrt{-1}jk/(q-1)} \quad \text{for } k = 0, 1, \ldots, q-2 \tag{3}$$

defines a multiplicative character with order $(q-1)/\gcd(q-1, j)$ of GF(q). When $j = q-1$, $\psi_0(c) = 1$ for all $c \in \mathrm{GF}(q)^*$, and is called the *trivial multiplicative character* of GF(q).

Let q be odd and $j = (q-1)/2$ in (3), we then get a multiplicative character η such that $\eta(c) = 1$ if c is the square of an element and $\eta(c) = -1$ otherwise. This η is called the *quadratic character* of GF(q).

Let ψ be a multiplicative character with order k where $k|(q-1)$ and χ an additive character of GF(q). Then the *Gaussian sum* $G(\psi, \chi)$ of order k is defined by

$$G(\psi, \chi) = \sum_{c \in \mathrm{GF}(q)^*} \psi(c)\chi(c).$$

Since $G(\psi, \chi_b) = \bar{\psi}(b)G(\psi, \chi_1)$, we just consider $G(\psi, \chi_1)$, briefly denoted as $G(\psi)$, in the sequel. If $\psi \neq \psi_0$, then

$$|G(\psi)| = q^{1/2}. \tag{4}$$

Generally, to explicitly determine the value of Gaussian sums is a challenging task. At present, they can be determined in a few cases. Among them is the following case of $k = 2$.

If $q = p^s$, where p is an odd prime and s is a positive integer, then

$$G(\eta) = \begin{cases} (-1)^{s-1}q^{1/2} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{s-1}(\sqrt{-1})^s q^{1/2} & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{5}$$

The following result [15] is useful in the sequel.

Lemma 1. *Let χ be a nontrivial additive character of* GF(q) *with q odd, and let $f(x) = a_2x^2 + a_1x + a_0 \in \mathrm{GF}(q)[x]$ with $a_2 \neq 0$. Then*

$$\sum_{c \in \mathrm{GF}(q)} \chi(f(c)) = \chi(a_0 - a_1^2(4a_2)^{-1})\eta(a_2)G(\eta). \tag{6}$$

The Gaussian sums of small order, such as $k = 3, 4, 5, 6$, and 12, can be also determined; see [5]. In another special case, called "semi-primitive" case, the Gaussian sums are known and given in the following lemma [5].

Lemma 2. *Assume that $N \neq 2$ and there exists a positive integer j such that $p^j \equiv -1 \pmod N$, and the j is the least such. Let $q = p^{2j\gamma}$ for some integer γ. Then the Gaussian sums of order N over $\mathrm{GF}(q)$ are given by*

$$G(\psi) = \begin{cases} (-1)^{\gamma-1}\sqrt{q}, & \text{if } p = 2, \\ (-1)^{\gamma-1+\frac{\gamma(p^j+1)}{N}}\sqrt{q}, & \text{if } p \geqslant 3. \end{cases}$$

Furthermore, for $1 \leqslant i \leqslant N-1$, the Gaussian sums $G(\psi^i)$ are given by

$$G(\psi^i) = \begin{cases} (-1)^i\sqrt{q}, & \text{if } N \text{ is even, } p, \gamma \text{ and } \dfrac{p^j+1}{N} \text{ are odd;} \\ (-1)^{\gamma-1}\sqrt{q}, & \text{otherwise.} \end{cases}$$

If p generates a subgroup of the group $(\mathbb{Z}/N\mathbb{Z})^*$ with index $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p\rangle] = 2$ and $-1 \notin \langle p\rangle \subset (\mathbb{Z}/N\mathbb{Z})^*$, which is the so-called "*quadratic residues*" or "*index* 2" case, Gaussian sums are also explicitly determined. See [31] and its references for details. We list one of the results [31] in the index 2 case below, which is useful in the sequel.

Lemma 3. *Let $N_1 = l^\lambda$ where $3 \neq l \equiv 3 \pmod 4$ is a prime and λ is a positive integer. Let $f = \mathrm{ord}_{N_1}(p)$, $r = p^{fs}$ for some positive integer s, and ψ be a primitive multiplicative character of order N_1 over $\mathrm{GF}(r)^*$. Assume that $f = \frac{\varphi(N_1)}{2}$, which means that p generates the quadratic residues modulo N_1, then, for $1 \leqslant t \leqslant \lambda$, we have that*

$$\begin{aligned} G(\psi^{l^{\lambda-t}}) &= (-1)^{s-1} \cdot p^{\frac{s(f-hl^{\lambda-t})}{2}} \cdot \left(\frac{a+b\sqrt{-l}}{2}\right)^{sl^{\lambda-t}} \\ &:= P_t^{(s,\lambda)}\left(A_t^{(s,\lambda)} + B_t^{(s,\lambda)}\sqrt{-l}\right), \end{aligned}$$

where h is the ideal class number of $\mathbb{Q}(\sqrt{-l})$, a, b are integers given by

$$\begin{cases} a^2 + lb^2 = 4p^h \\ a \equiv -2p^{\frac{l-1+2h}{4}} \pmod l, \end{cases}$$

and $P_t^{(s,\lambda)}$, $A_t^{(s,\lambda)}$, $B_t^{(s,\lambda)} \in \mathbb{Z}$ are defined as

$$\begin{aligned} &P_t^{(s,\lambda)} = (-1)^{s-1} \cdot p^{\frac{s(f-hl^{\lambda-t})}{2}}; \\ &A_t^{(s,\lambda)} = \mathrm{Re}\left(\frac{a+b\sqrt{-l}}{2}\right)^{sl^{\lambda-t}}; \qquad B_t^{(s,\lambda)} = \mathrm{Im}\left(\frac{a+b\sqrt{-l}}{2}\right)^{sl^{\lambda-t}} \Big/ \sqrt{l}. \end{aligned} \tag{7}$$

2.2. Cyclotomy

Let $r - 1 = nN$ for two positive integers $n > 1$ and $N > 1$, and let α be a fixed primitive element of $\mathrm{GF}(r)$. Define $C_i^{(N,r)} = \alpha^i\langle\alpha^N\rangle$ for $i = 0, 1, \ldots, N-1$, where $\langle\alpha^N\rangle$ denotes the subgroup of $\mathrm{GF}(r)^*$ generated by α^N. The cosets $C_i^{(N,r)}$ are called the *cyclotomic classes* of order N in $\mathrm{GF}(r)$. The *cyclotomic numbers* of order N are defined by

$$(i, j)^{(N,r)} = \left|(C_i^{(N,r)} + 1) \cap C_j^{(N,r)}\right|$$

for all $0 \leq i \leq N-1$ and $0 \leq j \leq N-1$.

We will need the following lemma [10] in the sequel.

Lemma 4. *Let $r - 1 = nN$ and let q be a prime power. Then*

$$\sum_{u=0}^{N-1}(u, u+k)^{(N,r)} = \begin{cases} n-1, & \text{if } k = 0, \\ n, & \text{if } k \neq 0. \end{cases}$$

To determine the weight distribution of some classes of linear codes in the sequel, we need the following lemma.

Lemma 5. *Let e_1 be a positive divisor of $r-1$ and let i be any integer with $0 \le i < e_1$. We have the following multiset equality:*

$$\left\{xy : y \in \mathrm{GF}(q)^*,\ x \in C_i^{(e_1,r)}\right\} = \frac{(q-1)\gcd((r-1)/(q-1), e_1)}{e_1} * C_i^{(\gcd((r-1)/(q-1),e_1),r)}, \tag{8}$$

where $\frac{(q-1)\gcd((r-1)/(q-1),e_1)}{e_1} * C_i^{(\gcd((r-1)/(q-1),e_1),r)}$ denotes the multiset in which each element in the set $C_i^{(\gcd((r-1)/(q-1),e_1),r)}$ appears in the multiset with multiplicity $\frac{(q-1)\gcd((r-1)/(q-1),e_1)}{e_1}$.

Proof. We just prove the conclusion for $i = 0$. The proof is similar for $i \neq 0$ since

$$C_i^{(\gcd((r-1)/(q-1),e_1),r)} = \alpha^i C_0^{(\gcd((r-1)/(q-1),e_1),r)}.$$

Note that every $y \in \mathrm{GF}(q)^*$ can be expressed as $y = \alpha^{\frac{r-1}{q-1}\ell}$ for an unique ℓ with $0 \le \ell < q-1$ and every $x \in C_0^{(e_1,r)}$ can be expressed as $x = \alpha^{e_1 j}$ for an unique j with $0 \le j < (r-1)/e_1$. Then we have

$$xy = \alpha^{\frac{r-1}{q-1}\ell + e_1 j}.$$

It follows that

$$xy = \alpha^{\frac{r-1}{q-1}\ell + e_1 j} = (\alpha^{\gcd((r-1)/(q-1),e_1)})^{\frac{r-1}{(q-1)\gcd((r-1)/(q-1),e_1)}\ell + \frac{e_1}{\gcd((r-1)/(q-1),e_1)}j}.$$

Note that

$$\gcd\left(\frac{r-1}{(q-1)\gcd((r-1)/(q-1), e_1)}, \frac{e_1}{\gcd((r-1)/(q-1), e_1)}\right) = 1.$$

When ℓ ranges over $0 \le \ell < q-1$ and j ranges over $0 \le j < (r-1)/e_1$, xy takes on the value 1 exactly $\frac{q-1}{e_1}\gcd((r-1)/(q-1), e_1)$ times.

Let $x_{i_1} \in C_0^{(e_1,r)}$ for $i_1 = 1$ and $i_1 = 2$, and let $y_{i_2} \in \mathrm{GF}(q)^*$ for $i_2 = 1$ and $i_2 = 2$. Then $\frac{x_1}{x_2} \in C_0^{(e_1,r)}$ and $\frac{y_1}{y_2} \in \mathrm{GF}(q)^*$. Note that $x_1y_1 = x_2y_2$ if and only if $\frac{x_1}{x_2}\frac{y_1}{y_2} = 1$. Then the conclusion of the lemma for the case $i = 0$ follows from the discussions above. □

2.3. Gaussian periods

The *Gaussian periods* are defined by

$$\eta_i^{(N,r)} = \sum_{x \in C_i^{(N,r)}} \chi(x), \quad i = 0, 1, \ldots, N-1,$$

where χ is the canonical additive character of $\mathrm{GF}(r)$.

The following lemma presents some basic properties of Gaussian periods, and will be useful later.

Lemma 6 ([26]). *Let symbols be the same as before. Then we have*

1. $\sum_{i=0}^{N-1} \eta_i = -1$.
2. $\sum_{i=0}^{N-1} \eta_i\eta_{i+k} = r\theta_k - n$ *for all* $k \in \{0, 1, \ldots, N-1\}$, *where*

$$\theta_k = \begin{cases} 1 & \text{if } n \text{ is even and } k = 0 \\ 1 & \text{if } n \text{ is odd and } k = N/2 \\ 0 & \text{otherwise}, \end{cases}$$

and equivalently $\theta_k = 1$ if and only if $-1 \in C_k^{(N,r)}$.

Gaussian periods are closely related to Gaussian sums. By the discrete Fourier transform, it is known that

$$\eta_i^{(N,r)} = \frac{1}{N}\sum_{j=0}^{N-1} \zeta_N^{-ij} G(\psi^j) = \frac{1}{N}\left[-1 + \sum_{j=1}^{N-1} \zeta_N^{-ij} G(\psi^j)\right], \tag{9}$$

where $\zeta_N = e^{2\pi\sqrt{-1}/N}$ and ψ is a primitive multiplicative character of order N over $\mathrm{GF}(r)^*$.

The values of the Gaussian periods in general are also very hard to compute. However, they can be computed in a few cases. To present some known results on Gaussian periods, we need to introduce period polynomials.

The *period polynomials* $\psi_{(N,r)}(X)$ are defined by

$$\psi_{(N,r)}(X) = \prod_{i=0}^{N-1} \left(X - \eta_i^{(N,r)}\right).$$

It is known that $\psi_{(N,r)}(X)$ is a polynomial with integer coefficients [21]. We will need the following four lemmas whose proofs can be found in [21].

Lemma 7. *Let $N = 3$. Let c and d be defined by $4r = c^2 + 27d^2$, $c \equiv 1 \pmod 3$, and, if $p \equiv 1 \pmod 3$, then $\gcd(c, p) = 1$. These restrictions determine c uniquely, and d up to sign. Then we have*

$$\psi_{(3,r)}(X) = X^3 + X^2 - \frac{r-1}{3}X - \frac{(c+3)r-1}{27}.$$

Lemma 8. *Let $N = 3$. We have the following results on the factorization of $\psi_{(3,r)}(X)$.*
(a) *If $p \equiv 2 \pmod 3$, then $s \cdot m$ is even, and*

$$\psi_{(3,r)}(X) = \begin{cases} 3^{-3}(3X+1+2\sqrt{r})(3X+1-\sqrt{r})^2 & \text{if } s \cdot m/2 \text{ even}, \\ 3^{-3}(3X+1-2\sqrt{r})(3X+1+\sqrt{r})^2 & \text{if } s \cdot m/2 \text{ odd}. \end{cases}$$

(b) *If $p \equiv 1 \pmod 3$, and $s \cdot m \not\equiv 0 \pmod 3$, then $\psi_{(3,r)}(X)$ is irreducible over the rationals.*
(c) *If $p \equiv 1 \pmod 3$, and $s \cdot m \equiv 0 \pmod 3$, then*

$$\psi_{(3,r)}(X) = \frac{1}{27}\left(3X+1-c_1 r^{\frac{1}{3}}\right)\left(3X+1+\frac{1}{2}(c_1+9d_1)r^{\frac{1}{3}}\right)\cdot\left(3X+1+\frac{1}{2}(c_1-9d_1)r^{\frac{1}{3}}\right),$$

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

Lemma 9. *Let $N = 4$. Let u and v be defined by $r = u^2 + 4v^2$, $u \equiv 1 \pmod 4$, and, if $p \equiv 1 \pmod 4$, then $\gcd(u, p) = 1$. These restrictions determine u uniquely, and v up to sign.*

If n is even, then

$$\psi_{(4,r)}(X) = X^4 + X^3 - \frac{3r-3}{8}X^2 + \frac{(2u-3)r+1}{16}X + \frac{r^2-(4u^2-8u+6)r+1}{256}.$$

If n is odd, then

$$\psi_{(4,r)}(X) = X^4 + X^3 + \frac{r+3}{8}X^2 + \frac{(2u+1)r+1}{16}X + \frac{9r^2-(4u^2-8u-2)r+1}{256}.$$

Lemma 10. *Let $N = 4$. We have the following results on the factorization of $\psi_{(4,r)}(X)$.*
(a) *If $p \equiv 3 \pmod 4$, then $s \cdot m$ is even, and*

$$\psi_{(4,r)}(X) = \begin{cases} 4^{-4}(4X+1+3\sqrt{r})(4X+1-\sqrt{r})^3 & \text{if } s \cdot m/2 \text{ even}, \\ 4^{-4}(4X+1-3\sqrt{r})(4X+1+\sqrt{r})^3 & \text{if } s \cdot m/2 \text{ odd}. \end{cases}$$

(b) *If $p \equiv 1 \pmod 4$, and $s \cdot m$ is odd, then $\psi_{(4,r)}(X)$ is irreducible over the rationals.*
(c) *If $p \equiv 1 \pmod 4$, and $s \cdot m \equiv 2 \pmod 4$, then*

$$\psi_{(4,r)}(X) = 4^{-4}\left((4X+1)^2 + 2\sqrt{r}(4X+1) - r - 2\sqrt{r}u\right)\left((4X+1)^2 - 2\sqrt{r}(4X+1) - r + 2\sqrt{r}u\right),$$

the quadratics being irreducible, the u is defined in Lemma 9.
(d) *If $p \equiv 1 \pmod 4$, and $s \cdot m \equiv 0 \pmod 4$, then*

$$\begin{aligned}\psi_{(4,r)}(X) = {} & 4^{-4}\left((4X+1)+\sqrt{r}+2r^{1/4}u_1\right)\left((4X+1)+\sqrt{r}-2r^{1/4}u_1\right) \\ & \times \left((4X+1)-\sqrt{r}+4r^{1/4}v_1\right)\left((4X+1)-\sqrt{r}-4r^{1/4}v_1\right)\end{aligned}$$

where u_1 and v_1 are given by $p^{s\cdot m/2} = u_1^2 + 4v_1^2$, $u_1 \equiv 1 \pmod 4$ and $\gcd(u_1, p) = 1$.

The following lemma follows from Lemma 1 and (5).

Lemma 11. *When $N = 2$, the Gaussian periods are given by the following:*

$$\eta_0^{(2,r)} = \begin{cases} \dfrac{-1+(-1)^{s\cdot m-1}r^{1/2}}{2} & \text{if } p \equiv 1 \pmod 4 \\ \dfrac{-1+(-1)^{s\cdot m-1}(\sqrt{-1})^{s\cdot m}r^{1/2}}{2} & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

and $\eta_1^{(2,r)} = -1 - \eta_0^{(2,r)}$.

By Lemma 2 and (9), the Gaussian periods in the semi-primitive case are known and are described in the following lemma [2,21].

Lemma 12. *Assume that $N > 2$ and there exists a positive integer j such that $p^j \equiv -1 \pmod N$, and the j is the least such. Let $r = p^{2j\gamma}$ for some integer γ.*

(a) *If γ, p and $(p^j+1)/N$ are all odd, then*

$$\eta_{N/2}^{(N,r)} = \frac{(N-1)\sqrt{r}-1}{N}, \qquad \eta_k^{(N,r)} = -\frac{\sqrt{r}+1}{N} \quad \text{for } k \neq N/2.$$

(b) *In all other cases,*

$$\eta_0^{(N,r)} = \frac{(-1)^{\gamma+1}(N-1)\sqrt{r}-1}{N}, \qquad \eta_k^{(N,r)} = \frac{(-1)^{\gamma}\sqrt{r}-1}{N} \quad \text{for } k \neq 0.$$

From Lemma 3 and (9), the Gaussian periods in the so-called quadratic residues (or index 2) case can be also computed. The results with $3 \neq N \equiv 3 \pmod 4$ being odd prime are given in [4,21].

3. The weights in irreducible cyclic codes

Let $N > 1$ be an integer dividing $r-1$, and put $n = (r-1)/N$. Let α be a primitive element of $\mathrm{GF}(r)$ and let $\theta = \alpha^N$. Let $Z(r,a)$ denote the number of solutions $x \in \mathrm{GF}(r)$ of the equation $\mathrm{Tr}_{r/q}(ax^N) = 0$. Let $\zeta_p = e^{2\pi\sqrt{-1}/p}$, and $\chi(x) = \zeta_p^{\mathrm{Tr}_{r/p}(x)}$, where $\mathrm{Tr}_{r/p}$ is the trace function from $\mathrm{GF}(r)$ to $\mathrm{GF}(p)$. Then χ is an additive character of $\mathrm{GF}(r)$. We have then by Lemma 5

$$\begin{aligned} Z(r,a) &= \frac{1}{q}\sum_{y\in\mathrm{GF}(q)}\sum_{x\in\mathrm{GF}(r)} \zeta_p^{\mathrm{Tr}_{q/p}(y\mathrm{Tr}_{r/q}(ax^N))} \qquad (10)\\ &= \frac{1}{q}\sum_{y\in\mathrm{GF}(q)}\sum_{x\in\mathrm{GF}(r)} \chi(yax^N)\\ &= \frac{1}{q}\left[q+r-1+N\sum_{y\in\mathrm{GF}(q)^*}\sum_{x\in C_0^{(N,r)}}\chi(yax)\right]\\ &= \frac{1}{q}\left[q+r-1+(q-1)\gcd\left(\frac{r-1}{q-1},N\right)\cdot\sum_{z\in C_0^{\left(\gcd\left(\frac{r-1}{q-1},N\right),r\right)}}\chi(az)\right]. \qquad (11)\end{aligned}$$

Then the Hamming weight of the codeword

$$(\mathrm{Tr}_{r/q}(\beta), \mathrm{Tr}_{r/q}(\beta\theta), \ldots, \mathrm{Tr}_{r/q}(\beta\theta^{n-1}))$$

in the irreducible cyclic code of (1), for $0 \neq \beta \in C_i^{\gcd(\frac{r-1}{q-1},N),r}$, is equal to

$$n - \frac{Z(r,\beta)-1}{N} = \frac{(q-1)\left(r-1-\gcd\left(\frac{r-1}{q-1},N\right)\eta_i^{\left(\gcd\left(\frac{r-1}{q-1},N\right),r\right)}\right)}{qN}. \qquad (12)$$

The weight expression of (12) is the key observation of this paper and proves that the determination of the weight distribution of an irreducible cyclic code is equivalent to that of the Gaussian periods of order $N_1 = \gcd((r-1)/(q-1), N)$. McEliece [17] gave a different proof of (12) by Gaussian sums. From (9) we know that the weights of an irreducible cyclic code can be expressed as a linear combination of Gaussian sums.

Theorem 13. *Let $N_1 = \gcd((r-1)/(q-1), N)$. Then for all i with $0 \le i \le N_1 - 1$, we have*

(i) $\eta_i^{(N_1,r)} \in \mathbb{Z}$;
(ii) $N_1\eta_i^{(N_1,r)} + 1 \equiv 0 \pmod q$; *and*
(iii) $\left|\eta_i^{(N_1,r)} + \frac{1}{N_1}\right| \leqslant \left\lfloor \frac{(N_1-1)\sqrt{r}}{N_1}\right\rfloor$.

Proof. The conclusions of Parts (i) and (ii) follow from (12) directly, and that of Part (iii) follows from (4) and (9). □

Theorem 13 is an interesting result in the theory of cyclotomy.

Theorem 14. *Let $N_1 = \gcd((r-1)/(q-1), N)$. Then the Hamming weight of every codeword in the irreducible cyclic code of (1) is divisible by*

$$\frac{(q-1)}{\gcd(q-1, N/N_1)}.$$

Proof. By (12), the Hamming weight of every nonzero codeword is equal to

$$\frac{q-1}{\gcd(q-1, N/N_1)} \frac{r-(1+N_1\eta_i)}{q\frac{N}{\gcd(q-1,N/N_1)}}.$$

The desired conclusion then follows from the fact that

$$\gcd\left(q-1, q\frac{N}{\gcd(q-1, N/N_1)}\right) = 1. \quad \square$$

Particularly, when N divides $(r-1)/(q-1)$, the Hamming weight of every codeword in the irreducible cyclic code of (1) is divisible by $q-1$.

Example 1. Let $q = 5, m = 4, N = 4$. Then the irreducible cyclic code of (1) over GF(q) has length 156, dimension 4, and the following weight distribution:

$$1 + 156x^{112} + 156x^{124} + 156x^{128} + 156x^{136}.$$

So by Theorem 14, 4 is a common divisor of all nonzero weights. Note that

$$\gcd(112, 124, 128, 136) = 4.$$

Example 2. Let $q = 3. m = 4, N = 2$. Then the irreducible cyclic code of (1) over GF(q) has length 40, dimension 4, and the following weight distribution:

$$1 + 40x^{24} + 40x^{30}.$$

So by Theorem 14, 2 is a common divisor of all nonzero weights. Note that $\gcd(24, 30) = 6$.

4. The weight distribution when $N_1 = \gcd((r-1)/(q-1), N) = 1$

Theorem 15. *Let N be a positive divisor of $r-1$ such that $N_1 = \gcd((r-1)/(q-1), N) = 1$. Then the set $\mathcal{C}(r, N)$ in (1) is a $[(q^m-1)/N, m, (q-1)q^{m-1}/N]$ constant-weight code with the weight enumerator*

$$1 + (r-1)x^{\frac{(q-1)q^{m-1}}{N}}.$$

Proof. Since N divides $r-1$ and $\gcd((r-1)/(q-1), N) = 1$, N must divide $q-1$. It follows that

$$\gcd((r-1)/(q-1), N) = \gcd(m, N) = 1.$$

Let α be the generator of GF$(r)^*$. For any $a \neq 0$, it follows from (12) and Lemma 11 that for any $\beta \in$ GF$(r)^*$ the Hamming weight of any codeword

$$\mathbf{c}(\beta) = (\mathrm{Tr}_{r/q}(\beta), \mathrm{Tr}_{r/q}(\beta\theta), \ldots, \mathrm{Tr}_{r/q}(\beta\theta^{n-1}))$$

of the code $\mathcal{C}(r, N)$ is equal to

$$n - \frac{Z(r, \beta) - 1}{N} = \frac{(q-1)q^{m-1}}{N}.$$

The weight distribution and dimension of the code follow. This completes the proof. □

Theorem 16. *Let N be a positive divisor of $r-1$. Then the set $\mathcal{C}(r, N)$ in (1) is a $[(q^m-1)/N, m]$ constant-weight code if and only if $N_1 = \gcd((r-1)/(q-1), N) = 1$.*

Table 1
Numeral examples of Theorem 17.

q	m	N	$\gcd\left(\frac{r-1}{q-1}, N\right)$	$[n, k, d]$	Weight distribution
9	2	8	2	[10, 2, 8]	$1 + 40x^8 + 40x^{10}$
9	2	16	2	[5, 2, 4]	$1 + 40x^4 + 40x^5$
3	4	2	2	[40, 4, 24]	$1 + 40x^{24} + 40x^{30}$
3	4	4	4	[20, 4, 12]	$1 + 60x^{12} + 20x^{18}$

Proof. Theorem 15 shows that the condition is sufficient. We now prove the necessity of the condition. Let $N_1 = \gcd((r-1)/(q-1), N)$ and $n_1 = (r-1)/N_1$. Assume that $\mathcal{C}(r, N)$ is a constant weight code. It then follows from (12) that $1 + N_1\eta_i$ is a constant λ for all i. Define $\zeta_i = 1 + N_1\eta_i$. Then the formulas in Lemma 6 becomes

1. $\sum_{i=0}^{N_1-1} \zeta_i = 0$.
2. $\sum_{i=0}^{N_1-1} \zeta_i\zeta_{i+k} = N_1(N_1\theta_k - 1)r$ for all $k \in \{0, 1, \ldots, N_1 - 1\}$, where

$$\theta_k = \begin{cases} 1 & \text{if } n_1 \text{ is even and } k = 0 \\ 1 & \text{if } n_1 \text{ is odd and } k = N_1/2 \\ 0 & \text{otherwise,} \end{cases}$$

and equivalently $\theta_k = 1$ if and only if $-1 \in C_k^{(N_1,r)}$.

Since N_1 is a divisor of $(r-1)/(q-1)$, $\mathrm{GF}(q)^* \subset C_0^{(N_1,r)}$. It follows that $\theta_0 = 1$. Hence, we have

$$N_1\lambda = 0, \qquad N_1\lambda^2 = N_1(N_1 - 1)r.$$

Whence, $N_1 = 1$. This completes the proof. □

Theorem 16 above is a complete characterization of one-weight irreducible cyclic codes in the general case that N is any divisor of $r - 1$, which is different from Theorem 1 in [28], where Vega and Wolfmann considered only the case that N is a divisor of $q - 1$ and use the period of the parity-check polynomial of the code for the characterization. Theorem 15 is extension of Theorem 6 in [8].

5. The weight distribution when $N_1 = \gcd((r-1)/(q-1), N) = 2$

Theorem 17. *Let N be a positive divisor of $r - 1$. If $N_1 = \gcd((r-1)/(q-1), N) = 2$, then the set $\mathcal{C}(r, N)$ in (1) is a $[(q^m - 1)/N, m, (q-1)(r - \sqrt{r})/Nq]$ two-weight code with the weight enumerator*

$$1 + \frac{r-1}{2}x^{\frac{(q-1)(r-\sqrt{r})}{qN}} + \frac{r-1}{2}x^{\frac{(q-1)(r+\sqrt{r})}{qN}}.$$

Proof. Since $N_1 = \gcd((r-1)/(q-1), N) = 2$, m is even and q is odd. Let α be the generator of $\mathrm{GF}(r)^*$. Let $a \in C_h^{(2,r)}$. It then follows from (12) and Lemma 11 that for any $\beta \in \mathrm{GF}(r)^*$ the Hamming weight of any codeword

$$\mathbf{c}(\beta) = (\mathrm{Tr}_{r/q}(\beta), \mathrm{Tr}_{r/q}(\beta\theta), \ldots, \mathrm{Tr}_{r/q}(\beta\theta^{n-1}))$$

of the code $\mathcal{C}(r, N)$ is equal to

$$n - \frac{Z(r, \beta) - 1}{N} = \frac{(q-1)(r \mp \sqrt{r})}{qN} > 0.$$

Note that $|C_0^{(2,r)}| = |C_1^{(2,r)}| = (r-1)/2$. The weight distribution and dimension of the code follow. This completes the proof. □

Theorem 17 is an extension of Theorem 7 in Baumert and McEliece [2]. We list some numeral examples in Table 1.

6. The weight distribution when $N_1 = \gcd((r-1)/(q-1), N) = 3$

Theorem 18. *Let N be a divisor of $r - 1$. When $N_1 = \gcd((r-1)/(q-1), N) = 3$ and $p \equiv 1 \pmod 3$, the set $\mathcal{C}(r, N)$ in (1) is a $[((q^m - 1)/N), m]$ code with the following weight distribution:*

$$1 + \frac{r-1}{3}x^{\frac{(q-1)\left(r - c_1 r^{\frac{1}{3}}\right)}{Nq}} + \frac{r-1}{3}x^{\frac{(q-1)\left[r + \frac{1}{2}(c_1 + 9d_1)r^{\frac{1}{3}}\right]}{Nq}} + \frac{r-1}{3}x^{\frac{(q-1)\left[r + \frac{1}{2}(c_1 - 9d_1)r^{\frac{1}{3}}\right]}{Nq}},$$

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 $\gcd(c_1, p) = 1$.

Table 2
Numeral examples of Theorem 18.

q	m	N	$\gcd\left(\frac{r-1}{q-1}, N\right)$	$[n, k, d]$	Weight distribution
7	3	6	3	[57, 3, 45]	$1+114x^{45}+114x^{48}+114x^{54}$
7	3	18	3	[19, 3, 15]	$1+114x^{15}+114x^{16}+114x^{27}$

Table 3
Numeral examples of Theorem 19.

q	m	N	$\gcd\left(\frac{r-1}{q-1}, N\right)$	$[n, k, d]$	Weight distribution
4	6	3	3	[1365, 6, 1008]	$1+2730x^{1008}+1365x^{1056}$
4	6	9	3	[455, 6, 336]	$1+2730x^{336}+1365x^{352}$
4	3	3	3	[21, 3, 12]	$1+21x^{12}+42x^{18}$
4	3	9	3	[7, 3, 4]	$1+21x^{4}+42x^{6}$

Proof. By assumption $\gcd(m, q-1) = 3$. It then follows from (8) that

$$\left\{xy : y \in \mathrm{GF}(q)^*,\ x \in C_i^{(N,r)}\right\} = \frac{3(q-1)}{N} * C_i^{(3,r)}.$$

Since $N_1 = \gcd((r-1)/(q-1), N) = 3$, $(r-1)/(q-1) \mod 3 = m \mod 3 = 0$. Note that every element of $\mathrm{GF}(q)^*$ is of the form $\alpha^{i(r-1)/(q-1)}$ for some integer i. Hence, $\mathrm{GF}(q)^* \subset C_0^{(3,r)}$. It then follows from Lemma 8 that the Gaussian periods $\eta_i^{(3,r)}$ take only the following three distinct values:

$$\frac{-1+c_1r^{1/3}}{3}, \qquad \frac{-1-\frac{1}{2}(c_1+9d_1)r^{1/3}}{3}, \qquad \frac{-1-\frac{1}{2}(c_1-9d_1)r^{1/3}}{3}.$$

It then follows from (12) that for any $\beta \in \mathrm{GF}(r)^*$ the Hamming weight of any codeword

$$\mathbf{c}(\beta) = (\mathrm{Tr}_{r/q}(\beta), \mathrm{Tr}_{r/q}(\beta\theta), \ldots, \mathrm{Tr}_{r/q}(\beta\theta^{n-1}))$$

of the code $\mathcal{C}(r, q-1)$ is equal to

$$n - \frac{Z(r,\beta)-1}{N} = \frac{1}{q}\left[q+r-1+3(q-1)\eta_i^{(3,r)}\right] > 0.$$

Note that $|C_i^{(3,r)}| = (r-1)/3$. The weight distribution and dimension of the code then follow. This completes the proof. □

Theorem 18 of this section is an extension of Theorem 14 in [8] and Theorem 6 in [7]. We list some numeral examples in Table 2.

Theorem 19. *Let N be a divisor of $r-1$. Suppose that $\gcd((r-1)/(q-1), N) = 3$ and $p \equiv 2 \pmod 3$. If $s \cdot m \equiv 0 \pmod 4$, then $\mathcal{C}(r, N)$ is a $[(r-1)/N, m, (q-1)(r-\sqrt{r})/Nq]$ code over $\mathrm{GF}(q)$ with the weight distribution*

$$1 + \frac{2(r-1)}{3}x^{\frac{(q-1)(r-\sqrt{r})}{Nq}} + \frac{r-1}{3}x^{\frac{(q-1)(r+2\sqrt{r})}{Nq}}.$$

If $s \cdot m \equiv 2 \pmod 4$, then $\mathcal{C}(r, N)$ is a $[(r-1)/N, m, (q-1)(r-2\sqrt{r})/Nq]$ code over $\mathrm{GF}(q)$ with the weight distribution

$$1 + \frac{r-1}{3}x^{\frac{(q-1)(r-2\sqrt{r})}{Nq}} + \frac{2(r-1)}{3}x^{\frac{(q-1)(r+\sqrt{r})}{Nq}}.$$

Proof. Note that $\gcd((r-1)/(q-1), N) = 3$ and $p \equiv 2 \pmod 3$. This theorem becomes a special case of Theorem 23. □

We list some numeral examples of Theorem 19 in Table 3.

7. The weight distribution when $N_1 = \gcd((r-1)/(q-1), N) = 4$

Theorem 20. *Let N be a divisor of $r-1$. If $N_1 = \gcd((r-1)/(q-1), N) = 4$ and $p \equiv 1 \pmod 4$, $\mathcal{C}(r, N)$ is a $[(r-1)/N, m]$ code over $\mathrm{GF}(q)$ with the weight distribution*

$$1 + \frac{r-1}{4}x^{\frac{(q-1)(r+\sqrt{r}+2u_1r^{1/4})}{Nq}} + \frac{r-1}{4}x^{\frac{(q-1)(r+\sqrt{r}-2u_1r^{1/4})}{Nq}} + \frac{r-1}{4}x^{\frac{(q-1)(r-\sqrt{r}+4v_1r^{1/4})}{Nq}} + \frac{r-1}{4}x^{\frac{(q-1)(r-\sqrt{r}-4v_1r^{1/4})}{Nq}}$$

where u_1 and v_1 are given by $q^{m/2} = u_1^2 + 4v_1^2$, $u_1 \equiv 1 \pmod 4$, and $\gcd(u_1, p) = 1$.

Table 4
Numeral examples of Theorem 20.

q	m	N	N_1	$[n, k, d]$	Weight distribution
5	4	4	4	[156, 4, 112]	$1+156x^{112}+156x^{124}+156x^{128}+156x^{136}$
5	4	16	4	[39, 4, 28]	$1+156x^{28}+156x^{31}+156x^{32}+156x^{34}$

If $\gcd((r-1)/(q-1), N) = 4$ *and* $p \equiv 3 \pmod 4$, $\mathcal{C}(r, N)$ *is a* $[(r-1)/N, m]$ *code over* GF(q) *with the weight distribution*

$$1+\frac{3(r-1)}{4}x^{\frac{(q-1)(r-\sqrt{r})}{Nq}}+\frac{r-1}{4}x^{\frac{(q-1)(r+3\sqrt{r})}{Nq}}.$$

Proof. Note that $\gcd((r-1)/(q-1), N) = 4$. Then similar to the proof of Theorem 18, we can prove the weight distribution formula with the help of Lemma 10 and (12). □

Theorem 20 of this section is an extension of Theorem 21 in [8] and Theorem 7 in [7]. We list some numeral examples in Tables 3 and 4, where $N_1 = \gcd(\frac{r-1}{q-1}, N)$.

8. The weight distribution in the quadratic residue case

In another special case, called the "quadratic residue" or "index 2" case, for the weight distribution of the irreducible cyclic code, we conclude the following theorem.

Theorem 21. *Let notations be defined as in Lemma 3. For* $1 \leqslant i \leqslant N_1 = l^{\lambda}$, *define*

$$\begin{cases} i_2 := v_l(i), \quad \text{i.e., } l^{i_2} \parallel i; \\ i_1 := i/l^{i_2} \in (\mathbb{Z}/l^{\lambda-i_2}\mathbb{Z})^*, \end{cases}$$

where $l^{i_2} \parallel i$ *means that* l^{i_2} *divides* i *but* l^{i_2+1} *does not divide* i. *Then the Hamming weight of the codeword* $c(\beta)$ *with* $\beta \in C_i^{(N_1,r)}$ *is given by*

$$\begin{aligned} w_H(c(\beta)) &= \frac{q-1}{Nq}\left[r-\sum_{u=1}^{l^{\lambda}-1} G(\psi^u, \chi_1)\psi^{-u}(g^i)\right] \\ &= \frac{q-1}{Nq}\left[r-\sum_{t=0}^{i_2} l^t\left(A_t^{(s,\lambda)}P_t^{(s,\lambda)}-A_{t+1}^{(s,\lambda)}P_{t+1}^{(s,\lambda)}\right)-\left(\frac{i_1}{l}\right)l^{i_2+1}P_{i_2+1}^{(s,\lambda)}B_{i_2+1}^{(s,\lambda)}\right], \end{aligned}$$

where we take $A_0 = A_{\lambda+1} = B_{\lambda+1} = 0$ *and* $\left(\frac{i_1}{l}\right)$ *denotes the Legendre symbol.*

Proof. The conclusions of this theorem follow from (12), Lemma 3 and the conditions stated in this theorem. □

Regarding Theorem 21, we have the following remarks.

(a) Theorem 21 is an extension of the main results obtained by Baumert and Mykkeltveit [4] and the main results of [5, Section 11.7].
(b) With the explicit formulas of Theorem 21 and the recursive relation of $A_t^{(s,\lambda)}$, $B_t^{(s,\lambda)}$, $P_t^{(s,\lambda)}$ with respect to λ, one can derive the recursive algorithms presented in [20].
(c) According to the conclusions of [31], there are six subcases for Gauss sums in the index 2 case. Theorem 21 is the corresponding result for one of the six subcases.

Example 3. Let $q = 2, m = 42$ and $N = 7^2 = 49$. Then the set $\mathcal{C}(r, N)$ in (1) is an $[n = 89756051247, k = 42, d = 44877307904]$ code over GF(2) with the weight distribution

$$1+nx^{44877307904}+3nx^{44877832192}+21nx^{44877979648}+21nx^{44878086144}+3nx^{44878356480}.$$

Example 4. Let $q = 3, m = 55$ and $N = 11^2 = 121$. Then the set $\mathcal{C}(r, N)$ in (1) is an

$$[n = 1441729016604299000588186, k = 55, d = 96115267773383062564477 8]$$

code over GF(3) with the weight distribution

$$1+6nx^{961152677733830625644778}+55nx^{961152677735964537698190}+55nx^{961152677736445713945528}+5nx^{961152677738914357301436}.$$

9. The weight distribution in the case that n is a prime power

The following result is presented in [25].

Theorem 22. *Let $q = p^s$. Let t be an odd prime and ℓ be a positive integer. Assume that the multiplicative order of q modulo t^ℓ is t^d, where $0 \le d < \ell$. Define $m = t^d$ and $N = (q^m - 1)/t^j$ for any j with $1 \le j \le \ell$.*

If $j \le \ell - d$, then the set $\mathcal{C}(r, N)$ in (1) is a $[t^j, 1, t^j]$ constant-weight code over $\mathrm{GF}(q)$ with the weight enumerator

$$1 + (q-1)x^{t^j}.$$

If $j > \ell - d$, then the set $\mathcal{C}(r, N)$ in (1) is a $[t^j, t^{j-(\ell-d)}]$ cyclic code over $\mathrm{GF}(q)$ with the weight enumerator

$$\sum_{w=0}^{t^{r-\ell+d}} \binom{t^{j-\ell+d}}{w} x^{t^{(\ell-d)}w}.$$

Example 5. Let $q = 2^2$ and $t^\ell = 3^3$. Then the order of q modulo t^ℓ is 3^2. Define $m = 3^2 = 9$ and $N = (q^m - 1)/t^2$. Then $n = t^2 = 9$, and the set $\mathcal{C}(r, N)$ in (1) is a $[9, 3, 3]$ cyclic code over $\mathrm{GF}(4)$ with the weight enumerator

$$1 + 9x^3 + 27x^6 + 27x^9.$$

10. The weight distribution in the semi-primitive and related cases

Theorem 23. *Let p be a prime and $s \cdot m$ be even. Let N be a positive divisor of $r - 1$ and $N_1 = \gcd((r-1)/(q-1), N) > 2$. Assume there exists a positive integer j such that $p^j \equiv -1 \pmod{N_1}$, and the j is the least such. Define $\gamma = s \cdot m/2j$.*

(a) *If γ, p and $(p^j+1)/N_1$ are all odd, then the set $\mathcal{C}(r, N)$ in (1) is a $[(q^m-1)/N, m]$ code over $\mathrm{GF}(q)$ with the weight enumerator*

$$1 + \frac{r-1}{N_1} x^{\frac{(q-1)(r-(N_1-1)\sqrt{r})}{qN}} + \frac{(r-1)(N_1-1)}{N_1} x^{\frac{(q-1)(r+\sqrt{r})}{qN}},$$

provided that $N_1 < \sqrt{r} + 1$.

(b) *In all other cases, the set $\mathcal{C}(r, N)$ in (1) is a $[(q^m - 1)/N, m]$ code with the weight enumerator*

$$1 + \frac{r-1}{N_1} x^{\frac{(q-1)(r+(-1)^\gamma(N_1-1)\sqrt{r})}{qN}} + \frac{(r-1)(N_1-1)}{N_1} x^{\frac{(q-1)(r-(-1)^\gamma\sqrt{r})}{qN}},$$

provided that $\sqrt{r} + (-1)^\gamma(N_1 - 1) > 0$.

Proof. The conclusions of this theorem follow from (12), Lemma 12 and the conditions stated in this theorem. □

Regarding Theorem 23, we have the following remarks.

(a) When $N_1 = N$, this is the classical semi-primitive case, and the weight distribution of the code was studied by Delsarte and Goethals [6], McEliece [18], and Baumert and McEliece [2].

(b) When $N_1 < N$, this may not be the semiprimitive case for N. For example, let $q = 7$, $m = 2$ and $N = 12$. We now prove that this is not the semi-primitive case for $N = 12$. To this end, we prove that there is no positive integer j such that $7^j \equiv -1 \pmod{12}$, which is equivalent to the following system of congruences:

$$7^j \equiv -1 \pmod 4 \quad \text{and} \quad 7^j \equiv -1 \pmod 3$$

by the Chinese Remainder Theorem. The second congruence does not have a solution. In this case $N_1 = 4$ and N_1 divides $7^1 + 1$. By Theorem 23 the code over $\mathrm{GF}(7)$ has length 4, dimension 2 and weight enumerator

$$1 + 12x^2 + 36x^4.$$

This shows that some non-semiprimitive cases can be settled using the results of the semiprimitive cases.

(c) The condition that $N_1 < \sqrt{r} + 1$ or $\sqrt{r} + (-1)^\gamma(N_1 - 1) > 0$ is to ensure that the dimension of the code is m.

(d) Theorem 2.1 in [9] is a special case of Theorem 23 above.

Theorem 23 describes a class of two-weight irreducible cyclic codes over $\mathrm{GF}(q)$, and is an extension of Theorem 6 in Baumert and McEliece [2]. It is an interesting problem to find out all two-weight irreducible cyclic codes over $\mathrm{GF}(q)$. Schmidt and White have given a characterization of all two-weight irreducible cyclic codes over $\mathrm{GF}(q)$ when q is prime [23], and Rao and Pinnawala [22] have constructed another type of two-weight codes. However, the conditions for the characterization given in [23] may not be easily used for finding out all two-weight irreducible cyclic codes over $\mathrm{GF}(p)$. It follows from (10) that the code $\mathcal{C}(r, N)$ in (1) has at most two nonzero weights if and only if the Gaussian periods $\eta_i^{(\gcd((r-1)/(q-1),N),r)}$ take on at most two distinct values. A special case of this is the case of uniform cyclotomy [3]. It might be possible to give another characterization in this direction.

Table 5
The lower bound of Theorem 24.

n	k	d	q	Lower bound of Theorem 24	$\frac{r-1}{q-1} \bmod N$
5	4	2	2	2	0
21	6	8	2	8	0
21	3	12	2^2	12	0
85	4	64	2^2	64	1
13	3	9	3	9	1
40	4	24	3	24	0
121	5	81	3	81	1
312	4	240	5	236	0

11. The weight distribution in a few other cases and other results

Gaussian periods of order 5, 6, 8 and 12 are computed in [13] and [11] respectively. So the weight distribution of the code $\mathcal{C}(r, N)$ in (1) can be computed by these Gaussian periods and (12). However, the weight formulas will be complicated due to the messy expression of these Gaussian periods. Two-weight projective irreducible cyclic codes are characterized by Wolfmann [30].

Two recursive algorithms were developed for computing the weight distribution of certain irreducible cyclic codes [20]. The weight enumerators of all nondegenerate irreducible cyclic binary $[n, m]$-codes have been computed for which $N = (2^m - 1)/n < 500$, $k \le 27$ by MacWilliams and Seery [16], and $k > 27$ by Ward [29]. The weights of irreducible cyclic codes are discussed by Aubry and Langevin [1], Moisio [19] and by Segal and Ward [24]. The relations between the weight distributions of irreducible cyclic codes and the Hasse–Davenport curves are dealt with by van der Vlugt [27]. Chains of irreducible cyclic codes and relations among their weight distributions are presented in [14,12].

12. Bounds on weights in irreducible cyclic codes

Since it is notoriously hard to determine the weight distributions of the irreducible cyclic codes, it would be interesting to develop tight bounds on the weights in irreducible cyclic codes. Such tight bounds can give information on the error-correcting capability of this class of cyclic codes. The objective of this section is to develop such tight bounds.

Theorem 24. *Let N be a positive divisor of $r - 1$ and define $N_1 = \gcd((r-1)/(q-1), N)$. Let m_0 be the multiplicative order of q modulo n. Then the set $\mathcal{C}(r, N)$ in (1) is a $[(q^m - 1)/N, m_0]$ cyclic code over $\mathrm{GF}(q)$ in which the weight w of every nonzero codeword satisfies that*

$$w_H(c(\beta)) \ge (q-1)\left\lceil \frac{r - \lfloor (N_1 - 1)\sqrt{r} \rfloor}{qN} \right\rceil,$$

$$w_H(c(\beta)) \le (q-1)\left\lfloor \frac{r + \lfloor (N_1 - 1)\sqrt{r} \rfloor}{qN} \right\rfloor.$$

In particular, if $N_1(N_1 - 1) < r$, then $m_0 = m$.

Proof. The results of this theorem follow from Theorem 13 and (12). □

The lower bound of Theorem 24 is tight when $\gcd((r-1)/(q-1), N)$ is small, but it may be not in some other cases. In fact, when $\gcd((r-1)/(q-1), N) = 1$, the lower and upper bounds of Theorem 24 are the same, and they are indeed achieved as the code in this case is a constant-weight code. Table 5 lists some experimental data, where n, k, d are the length, dimension and minimum nonzero weight of the code.

13. Summary and open problems

The contributions of this paper include the following:

- A survey of earlier results on the weight distributions of irreducible cyclic codes.
- Extensions and generalizations of earlier results on the weight distributions of irreducible cyclic codes (Theorems 23, 21, 15, 17, 18, 19 and 20).
- A complete characterization of one-weight irreducible cyclic codes (Theorem 16), which is an extension of the result in [28].
- The weight divisibility of irreducible cyclic codes (Theorem 14).
- A lower and upper bound on the weights in irreducible cyclic codes (Theorem 24).
- A property on Gaussian periods (Theorem 13).

While it is hard to determine the weight distributions of the irreducible cyclic codes in general, it is possible to solve this problem for other special cases. One open problem would be a simpler characterization of two-weight irreducible cyclic codes than the one presented in [23] by Schmidt and White.

Acknowledgments

The authors are grateful to the reviewers for their comments that improved the presentation and quality of this paper.

References

[1] Y. Aubry, P. Langevin, On the weights of binary irreducible cyclic codes, in: O. Ytrehus (Ed.), Coding and Cryptography, in: Lecture Notes in Computer Science, vol. 3969, Springer Verlag, 2006, pp. 46–54.
[2] L.D. Baumert, R.J. McEliece, Weights of irreducible cyclic codes, Inf. Control 20 (2) (1972) 158–175.
[3] L.D. Baumert, W.H. Mills, R.L. Ward, Uniform cyclotomy, J. Number Theory 14 (1982) 67–82.
[4] L.D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, DSN Progr. Rep. 16 (1973) 128–131.
[5] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, J. Wiley and Sons Company, New York, 1997.
[6] P. Delsarte, J.M. Goethals, Irreducible binary cyclic codes of even dimension, in: Proc. Second Chapel Hill Conf. on Combinatorial Mathematics and its Applications, Univ. North Carolina, Chapel Hill, NC, 1970, pp. 100–113.
[7] C. Ding, A class of three-weight and four-weight codes, in: C. Xing, et al. (Eds.), Proc. of the Second International Workshop on Coding Theory and Cryptography, in: Lecture Notes in Computer Science, vol. 5557, Springer Verlag, 2009, pp. 34–42.
[8] C. Ding, The weight distribution of some irreducible cyclic codes, IEEE Trans. Inform. Theory 55 (3) (2009) 955–960.
[9] C. Ding, J. Luo, H. Niederreiter, Two-weight codes punctured from irreducible cyclic codes, in: Y. Li, S. Lin, H. Niederreiter, H. Wang, C. Xing, S. Zhang (Eds.), Proceedings of the First Worshop on Coding and Cryptography, World Scientific, Singapore, 2008, pp. 119–124.
[10] C. Ding, J. Yin, Sets of optimal frequency hopping sequences, IEEE Trans. Inform. Theory 54 (8) (2008) 3741–3745.
[11] S.J. Gurak, Periodic polynomials for F_q of fixed small degree, CRM Proc. Lecture Notes 36 (2004) 127–145.
[12] T. Helleseth, T. Kløve, J. Mykkeltveit, The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$, Discrete Math. 18 (2) (1977) 179–211.
[13] A. Hoshi, Explicit lifts of quintic Jacobi sums and periodic polynomials for F_q, Proc. Japan Acad. Ser. A 82 (2006) 87–92.
[14] T. Kløve, The weight distribution for a class of irreducible cyclic codes, Discrete Math. 20 (1977) 87–90.
[15] L. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[16] F. MacWilliams, J. Seery, The weight distributions of some minimal cyclic codes, IEEE Trans. Inform. Theory 27 (6) (1981) 796–806.
[17] R.J. McEliece, Irreducible cyclic codes and Gauss sums, combinatorics, in: Proc. NATO Advanced Study Inst., Breukelen, 1974, Part 1: Theory of Designs, Finite Geometry and Coding Theory, in: Math. Centre Tracts, vol. 55, Math. Centrum, Amsterdam, 1974, pp. 179–196.
[18] R.J. McEliece, A class of two-weight codes, Jet Propulsion Laboratory Space Program Summary 37–41, vol. IV, 264–266.
[19] M.J. Moisio, Exponential sums, Gauss sums and cyclic codes, Ph.D. Thesis, Acta Univ. Oul. A, 306, 1998.
[20] M.J. Moisio, K.O. Väänänen, Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes, IEEE Trans. Inform. Theory 45 (4) (1999) 1244–1249.
[21] G. Myerson, Period polynomials and Gauss sums for finite fields, Acta Arith. 39 (1981) 251–264.
[22] A. Rao, N. Pinnawala, A family of two-weight irreducible cyclic codes, IEEE Trans. Inform. Theory 56 (6) (2010) 2568–2570.
[23] B. Schmidt, C. White, All two-weight irreducible cyclic codes, Finite Fields Appl. 8 (2002) 1–17.
[24] R. Segal, R.L. Ward, Weight distributions of some irreducible cyclic codes, Math. Comp. 46 (173) (1986) 341–354.
[25] A. Sharma, G.K. Bakshi, The weight distribution of some irreducible cyclic codes, Finite Fields Appl. 18 (1) (2012) 144–159.
[26] T. Storer, Cyclotomy and Difference Sets, Markham, Chicago, 1967.
[27] M. van der Vlugt, Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes, J. Number Theory 55 (1995) 145–159.
[28] G. Vega, J. Wolfmann, New classes of 2-weight cyclic codes, Des. Codes Cryptogr. 42 (2007) 327–334.
[29] R.L. Ward, Weight enumerators of more irreducible cyclic binary codes, IEEE Trans. Inform. Theory 39 (5) (1993) 1701–1709.
[30] J. Wolfmann, Are 2-weight projective cyclic codes irreducible? IEEE Trans. Inform. Theory 51 (2) (2005) 733–737.
[31] J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, Sci. China Math. 53 (9) (2010) 2525–2542.