Designs, Codes and Cryptography (2023) 91:2213–2221
https://doi.org/10.1007/s10623-023-01193-w

The b-symbol weight distributions of all semiprimitive irreducible cyclic codes

Gerardo Vega[1]

Received: 11 June 2022 / Revised: 14 December 2022 / Accepted: 27 January 2023 /
Published online: 1 March 2023

Abstract
Up to a new invariant $\mu(b)$, the complete b-symbol weight distribution of a particular kind of two-weight irreducible cyclic codes, was recently obtained by Zhu et al. (Des Codes Cryptogr 90(5):1113–1125, 2022). The purpose of this paper is to simplify and generalize the results of Zhu et al., and obtain the b-symbol weight distributions of all one-weight and two-weight semiprimitive irreducible cyclic codes.

Keywords b-Symbol error · b-Symbol Hamming weight distribution · Semiprimitive irreducible cyclic code

Mathematics Subject Classification 94B14 · 11T71 · 94B27

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements. An $[n, l]$ linear code, $\mathscr{C}$, over $\mathbb{F}_q$ is an l-dimensional subspace of $\mathbb{F}_q^n$ (see for example [4, Section 1.4]). In this context, the vectors of $\mathscr{C}$ are called *codewords*. Let A_i be the number of codewords with Hamming weight i in $\mathscr{C}$ (recall that the *Hamming weight* of a codeword c is the number of nonzero coordinates in c). Then, the sequence $A_0, A_1, \ldots, A_n$ is called the *Hamming weight distribution* of $\mathscr{C}$, and the polynomial $A_0 + A_1T + \ldots + A_nT^n$ is called the *Hamming weight enumerator* of $\mathscr{C}$. An N-*weight* code is a code such that the cardinality of the set of nonzero weights is N. That is, $N = |\{i : A_i \neq 0, i = 1, 2, 3, \ldots, n\}|$.

A linear code $\mathscr{C}$ of length n is *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathscr{C}$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathscr{C}$. Cyclic codes have wide applications in storage and communication systems because, unlike encoding and decoding algorithms for linear codes, encoding/decoding algorithms for cyclic codes can be implemented easily and efficiently by employing shift

Communicated by L. Mérai.

✉ Gerardo Vega
gerardov@unam.mx

[1] Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, e 04510 Ciudad de México, Mexico

registers with feedback connections (see for example [6, p. 209]). As usual in cyclic codes, we always assume that the length n of any cyclic code is relatively prime to q.

By identifying any vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ with the polynomial $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]$, it follows that any linear code $\mathscr{C}$ of length n over $\mathbb{F}_q$ corresponds to a subset of the residue class ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Moreover, it is well known that the linear code $\mathscr{C}$ is cyclic if and only if the corresponding subset is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ (see for example [5, Theorem 9.36]).

Note that every ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is principal. Thus, if $\mathscr{C}$ is a cyclic code of length n over $\mathbb{F}_q$, then $\mathscr{C} = \langle g(x)\rangle$, where $g(x)$ is a monic polynomial, such that $g(x) \mid (x^n - 1)$. This polynomial is unique, and it is called the *generator polynomial* of $\mathscr{C}$ ([6, Theorem 1, p. 190]). On the other hand, the polynomial $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity check polynomial* of $\mathscr{C}$. A cyclic code over $\mathbb{F}_q$ is called *irreducible* (*reducible*) if its parity check polynomial is irreducible (reducible) over $\mathbb{F}_q$.

Denote by $w_H(\cdot)$ the usual Hamming weight function. For $1 \le b < n$, let the Boolean function $\bar{\mathcal{Z}} : \mathbb{F}_q^b \to \{0, 1\}$ be defined by $\bar{\mathcal{Z}}(v) = 0$ iff v is the zero vector in $\mathbb{F}_q^b$. The *b-symbol Hamming weight*, $w_b(\mathbf{x})$, of $\mathbf{x} = (x_0, \cdots, x_{n-1}) \in \mathbb{F}_q^n$ is defined as

$$w_b(\mathbf{x}) := w_H(\bar{\mathcal{Z}}(x_0, \ldots, x_{b-1}), \bar{\mathcal{Z}}(x_1, \ldots, x_b), \cdots, \bar{\mathcal{Z}}(x_{n-1}, \ldots, x_{b+n-2 \pmod n}))\,.$$

When $b = 1$, $w_1(\mathbf{x})$ is exactly the Hamming weight of $\mathbf{x}$, that is $w_1(\mathbf{x}) = w_H(\mathbf{x})$. For any $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, we define the *b-symbol distance* (b-distance for short) between $\mathbf{x}$ and $\mathbf{y}$, $d_b(\mathbf{x}, \mathbf{y})$, as $d_b(\mathbf{x}, \mathbf{y}) := w_b(\mathbf{x} - \mathbf{y})$, and for a code $\mathscr{C}$ (linear or not) over $\mathbb{F}_q$ of length n, the *b-symbol minimum Hamming distance*, $d_b(\mathscr{C})$, of $\mathscr{C}$ is defined as $d_b(\mathscr{C}) := \min d_b(\mathbf{x}, \mathbf{y})$, with $\mathbf{x}, \mathbf{y} \in \mathscr{C}$ and $\mathbf{x} \neq \mathbf{y}$. In this context we will say that $\mathscr{C}$ is a *b-symbol code* with parameters $(n, M, d_b(\mathscr{C}))_q$, where $M = |\mathscr{C}|$. Let $A_i^{(b)}$ denote the number of codewords with b-symbol Hamming weight i in $\mathscr{C}$. The *b-symbol Hamming weight enumerator* of $\mathscr{C}$ is defined by

$$1 + A_1^{(b)}T + A_2^{(b)}T^2 + \cdots + A_n^{(b)}T^n.$$

Note that if $b = 1$, then the b-symbol Hamming weight enumerator of $\mathscr{C}$ is the ordinary Hamming weight enumerator of $\mathscr{C}$. Some contributions to the b-symbol Hamming weight enumerator of a code can be found in [3, 9, 11, 12] and the references therein.

Up to a new invariant $\mu(b)$, the complete b-symbol weight distribution of some irreducible cyclic codes was recently obtained in [12]. The irreducible cyclic codes considered therein, belong to a particular kind of one-weight and two-weight irreducible cyclic codes that were recently characterized in terms of their lengths ([10]). Thus, the purpose of this paper is to present a generalization for the invariant $\mu(b)$, which will allow us to obtain the b-symbol Hamming weight distributions of all one-weight and two-weight irreducible cyclic codes, excluding only the exceptional two-weight irreducible cyclic codes studied in [8].

This work is organized as follows: In Sect. 2, we fix some notation and recall some definitions and some known results to be used in subsequent sections. Section 3 is devoted to presenting preliminary results. Particularly, in this section, we give an alternative proof of an already known result which determines the weight distributions of all one-weight and two-weight semiprimitive irreducible cyclic codes. In Sect. 4, we use such alternative proof, in order to determine the b-symbol weight distributions of all one-weight and two-weight semiprimitive irreducible cyclic codes.

2 Notation, definitions and known results

Unless otherwise specified, throughout this work we will use the following:
Notation. For integers v and w, with $\gcd(v, w) = 1$, $\mathrm{Ord}_v(w)$ will denote the *multiplicative order* of w modulo v. By using p, t, q, r, and Δ, we will denote positive integers such that p is a prime number, $q = p^t$ and $\Delta = \frac{q^r-1}{q-1}$. From now on, γ will denote a fixed primitive element of $\mathbb{F}_{q^r}$. Let u be an integer such that $u|(q^r - 1)$. For $i = 0, 1, \ldots, u-1$, we define $\mathcal{C}_i^{(u,q^r)} := \gamma^i \langle \gamma^u \rangle$, where $\langle \gamma^u \rangle$ denotes the subgroup of $\mathbb{F}_{q^r}^*$ generated by γ^u. The cosets $\mathcal{C}_i^{(u,q^r)}$ are called the *cyclotomic classes* of order u in $\mathbb{F}_{q^r}$. For an integer u, such that $\gcd(p, u) = 1$, p is said to be *semiprimitive modulo* u if there exists a positive integer d such that $u|(p^d + 1)$. Additionally, we will denote by "$\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}$" the *trace mapping* from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$.
Main assumption. From now on, we are going to use n and N as integers in such a way that $nN = q^r - 1$, with the important assumption that $r = \mathrm{Ord}_n(q)$. Under these circumstances, observe that if $h_N(x) \in \mathbb{F}_q[x]$ is the *minimal polynomial* of γ^{-N} (see for example [6, p. 99]), then, due to Delsarte's Theorem [1], $h_N(x)$ is parity-check polynomial of an irreducible cyclic code of length n and dimension r over $\mathbb{F}_q$.

The following gives an explicit description of an irreducible cyclic code of length n and dimension r over $\mathbb{F}_q$.

Definition 1 Let q, r, n, and N be as before. Then the set

$$\mathscr{C} := \{(\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a\gamma^{Ni}))_{i=0}^{n-1} \mid a \in \mathbb{F}_{q^r}\},$$

is called an *irreducible cyclic code* of length n and dimension r over $\mathbb{F}_q$.

An important kind of irreducible cyclic codes are the so-called *semiprimitive irreducible cyclic codes*:

Definition 2 [10, Definition 4] With our current notation and main assumption, fix $u = \gcd(\Delta, N)$. Then, any $[n, r]$ irreducible cyclic code over $\mathbb{F}_q$ is *semiprimitive* if $u \geq 2$ and the prime p is semiprimitive modulo u.

Apart from a few exceptional codes, it is well known that all two-weight irreducible cyclic codes are semiprimitive. In fact, it is conjectured in [8] that the number of these exceptional codes is eleven.

The *canonical additive character* of $\mathbb{F}_q$ is defined as follows:

$$\chi(x) := e^{2\pi\sqrt{-1}\mathrm{Tr}(x)/p} \qquad \text{for all } x \in \mathbb{F}_q$$

where "Tr" denotes the trace mapping from $\mathbb{F}_q$ to the prime field $\mathbb{F}_p$. Let $a \in \mathbb{F}_q$. The orthogonality relation for the canonical additive character χ of $\mathbb{F}_q$ is given by (see for example [5, Chapter 5]):

$$\sum_{x\in\mathbb{F}_q} \chi(ax) = \begin{cases} q & \text{if } a = 0, \\ 0 & \text{otherwise.} \end{cases}$$

This property plays an important role in numerous applications of finite fields. Among them, this property is useful for determining the Hamming weight of a given vector over a finite field; for example if $V = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, then

$$w_H(V) = n - \frac{1}{q}\sum_{i=0}^{n-1}\sum_{y\in\mathbb{F}_q}\chi(ya_i). \tag{1}$$

Let χ' be the canonical additive character of $\mathbb{F}_{q^r}$ and let $u \geq 1$ be an integer such that $u|(q^r-1)$. For $i = 0, 1, \ldots, u-1$, the i-th *Gaussian period*, $\eta_i^{(u,q^r)}$, of order u for $\mathbb{F}_{q^r}$ is defined to be

$$\eta_i^{(u,q^r)} := \sum_{x\in\mathcal{C}_i^{(u,q^r)}} \chi'(x).$$

Suppose that $a \in \mathcal{C}_i^{(u,q^r)}$. Since $\sum_{x\in\mathbb{F}_{q^r}} \chi'(ax^u) = u\eta_i^{(u,q^r)} + 1$ and $\eta_0^{(1,q^r)} + 1 = 0$, the following result is a direct consequence of Theorem 1 in [7]:

Theorem 1 *With our notation suppose that $rt = 2sd$ and $u|(p^d+1)$, for positive integers s, d and u. Then*

$$\frac{u\eta_i^{(u,q^r)}+1}{q^{r/2}} = \begin{cases} (-1)^{s-1}(u-1) & \text{if } i \equiv \delta \pmod{u}, \\ (-1)^s & \text{if } i \not\equiv \delta \pmod{u}, \end{cases}$$

where the integer δ is defined in terms of the following two cases:

$$\delta := \begin{cases} 0 & \text{if } u = 1;\ \text{or } p = 2;\ \text{or } p > 2 \text{ and } 2|s;\ \text{or } p > 2, 2 \nmid s,\ \text{and } 2|\frac{p^d+1}{u}, \\ \frac{u}{2} & \text{if } p > 2, 2\nmid s \text{ and } 2 \nmid \frac{p^d+1}{u}. \end{cases}$$

Remark 1 As shown below, by means of the previous theorem, it is possible to determine, in a single result, the Hamming weight enumerator of all one-weight and semiprimitive two-weight irreducible cyclic codes.

Under certain circumstances, and for a fixed coset $\mathcal{C}_i^{(N,q^r)}$, it is necessary to consider the set of products of the form xy, where $x \in \mathcal{C}_i^{(N,q^r)}$ and $y \in \mathbb{F}_q^*$. The following result goes in this direction:

Lemma 1 *[2, Lemma 5] Let N be a positive divisor of q^r-1 and let i be any integer with $0 \leq i < N$. Fix $u = \gcd(\Delta, N)$. We have the following multiset equality:*

$$\left\{xy : x \in \mathcal{C}_i^{(N,q^r)},\ y \in \mathbb{F}_q^*\right\} = \frac{(q-1)u}{N} * \mathcal{C}_i^{(u,q^r)},$$

where $\frac{(q-1)u}{N} * \mathcal{C}_i^{(u,q^r)}$ denotes the multiset in which each element in the set $\mathcal{C}_i^{(u,q^r)}$ appears in the multiset with multiplicity $\frac{(q-1)u}{N}$.

The following definitions are inspired by and similar to those of [12].

Definition 3 Let b be an integer, with $1 \leq b \leq r$. Let $\mathcal{P}(b)$ be the subset of cardinality $(q^b-1)/(q-1)$ in $\mathbb{F}_{q^r}^*$ defined as

$$\mathcal{P}(b) := \bigcup_{j=1}^{b-1}\{\gamma^{(j-1)N} + x_1\gamma^{jN} + \cdots + x_{b-j}\gamma^{(b-1)N} : x_1, \ldots, x_j \in \mathbb{F}_q\} \cup \{\gamma^{(b-1)N}\}.$$

Remark 2 Note that $\mathcal{P}(1)=\{1\}$.

Definition 4 Let b be as in Definition 3 and fix $u=\gcd(\Delta, N)$. For $0 \leq i < u$, we define $\mu_{(i)}(b)$ as

$$\mu_{(i)}(b) := |\{x \in \mathcal{P}(b) : x \in \mathcal{C}_i^{(u,q^r)}\}|.$$

Remark 3 Since $\mathcal{C}_0^{(2,q^r)} = \{x \in \mathbb{F}_{q^r}^* : x \text{ is a square in } \mathbb{F}_{q^r}^*\}$, note that $\mu_{(i)}(b)$ is indeed a generalization of the invariant $\mu(b)$ in [12]. Furthermore, note that $\mu_{(0)}(1)=1$ and $\mu_{(i)}(1)=0$, for $1 \leq i < u$.

The following important result from [12], is key in order to achieve our goals.

Lemma 2 *[12, Lemma 4.3] Let $\mathscr{C}$ be as in Definition 1 and let $c(a) \in \mathscr{C}$ be a codeword. Then, for any integer $1 \leq b \leq r$,*

$$w_b(c(a)) = \frac{1}{q^{b-1}} \sum_{\theta \in \mathcal{P}(b)} w_H(c(\theta a)).$$

Remark 4 The previous lemma is key for us because, although the condition $\gcd(\frac{q^r-1}{q-1}, N) = 2$ is one of the main assumptions in [12], Lemma 4.3 is beyond such condition. However it is important to observe that there is a small misprint in the proof of Lemma 4.3; more specifically the equality

$$n - w_1(c(a)) = \sum_{x \in I} \frac{1}{q} \sum_{y \in \mathbb{F}_q} \chi(yax),$$

should be

$$n - w_1(c(a)) = \sum_{x \in I} \frac{1}{q} \sum_{y \in \mathbb{F}_q} \chi(yax^N).$$

3 Preliminary results

In the light of Remark 3, the following is a generalization of [12, Lemma 2.1].

Lemma 3 *Let b and $\mu_{(i)}(b)$ be as in Definition 4. If $b=r$ then, for any $0 \leq i < u$, we have*

$$\mu_{(i)}(r) = \frac{1}{u}|\mathcal{P}(b)| = \frac{\Delta}{u}.$$

Proof Clearly

$$\mathbb{F}_{q^r}^* = \bigsqcup_{x \in \mathcal{P}(b)} x\mathbb{F}_q^*,$$

where $\sqcup$ is a disjoint union. Now, since $u|\Delta$ and $\langle \gamma^{\Delta} \rangle = \mathbb{F}_q^*$, $x \in \mathcal{C}_i^{(u,q^r)}$ if and only if each element of $x\mathbb{F}_q^*$ is also in $\mathcal{C}_i^{(u,q^r)}$. This implies that

$$\mu_{(i)}(r)(q-1) = \frac{q^r-1}{u},$$

which is the number of elements in $\mathcal{C}_i^{(u,q^r)}$. This completes the proof. □

It is already known the Hamming weight enumerator of all one-weight and semiprimitive two-weight irreducible cyclic codes over any finite field (see for example [8, 10]). By means of the following theorem we recall such a result and give an alternative proof of it. As will be clear later, this alternative proof will be important for fulfilling our goals.

Theorem 2 *Let $\mathscr{C}$ be as in Definition 1. Fix $u = \gcd(\Delta, N)$. Assume that $u = 1$ or p is semiprimitive modulo u. Let d be the smallest positive integer such that $u|(p^d + 1)$ and let $s = 1$ if $u = 1$ and $s = (rt)/(2d)$ if $u > 1$. Fix*

$$W_A = \frac{nq^{r/2-1}}{\Delta}(q^{r/2} - (-1)^{s-1}(u-1)) \quad \textit{and} \quad W_B = \frac{nq^{r/2-1}}{\Delta}(q^{r/2} - (-1)^{s}).$$

Then, $\mathscr{C}$ is an $[n, r]$ irreducible cyclic code whose Hamming weight enumerator is

$$1 + \frac{q^r - 1}{u} T^{W_A} + \frac{(q^r - 1)(u - 1)}{u} T^{W_B}. \tag{2}$$

Remark 5 Note that Theorem 2 gives, in a single result, an explicit description of the Hamming weight enumerators of all one-weight ($u = 1$) and two-weight ($2 \le u < \Delta$) irreducible cyclic codes, excluding only the exceptional two-weight irreducible cyclic codes studied in [8]. Therefore observe that the two-weight irreducible cyclic codes considered in [12] ($u = \gcd(\Delta, N) = 2$) belong also to Theorem 2.

Proof First note that if $u > 1$, then there must exist an integer s such that $rt = 2sd$.

For $a \in \mathbb{F}_{q^r}^*$, let $c(a) = (\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a\gamma^{Ni}))_{i=0}^{n-1} \in \mathscr{C}$. Let χ and χ' be the canonical additive characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^r}$, respectively. Thus, by the orthogonality relation for the character χ (see (1)) the Hamming weight of the codeword $c(a)$, $w_H(c(a))$, is

$$\begin{aligned} w_H(c(a)) &= n - \frac{1}{q}\sum_{i=0}^{n-1}\sum_{y\in\mathbb{F}_q} \chi(y\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a\gamma^{Ni})) \\ &= n - \frac{n}{q} - \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{x\in C_0^{(N,q^r)}} \chi'(yax) \\ &= n - \frac{n}{q} - \frac{(q-1)u}{qN}\sum_{z\in C_0^{(u,q^r)}} \chi'(az) \end{aligned}$$

where the last equality holds by Lemma 1. Now, suppose that $a \in C_i^{(u,q^r)}$ for some $0 \le i < u$. Thus

$$\begin{aligned} w_H(c(a)) &= n - \frac{n}{q} - \frac{(q-1)}{qN}u\eta_i^{(u,q^r)} \\ &= \frac{n}{\Delta q}(q^r - 1) - \frac{n}{\Delta q}u\eta_i^{(u,q^r)} \\ &= \frac{nq^{r-1}}{\Delta} - \frac{n}{\Delta q}(u\eta_i^{(u,q^r)} + 1) \\ &= \frac{nq^{r-1}}{\Delta} - \frac{nq^{r/2-1}}{\Delta}\frac{(u\eta_i^{(u,q^r)} + 1)}{q^{r/2}} \\ &= \frac{nq^{r/2-1}}{\Delta}(q^{r/2} - \frac{u\eta_i^{(u,q^r)} + 1}{q^{r/2}}). \end{aligned}$$

Let δ be as in Theorem 1 and observe that $i \equiv \delta \pmod{u}$ iff $a \in \mathcal{C}_{\delta}^{(u,q^r)}$. Therefore, owing to Theorem 1, we have

$$w_H(c(a)) = \begin{cases} W_A \text{ if } a \in \mathcal{C}_{\delta}^{(u,q^r)}, \\ \\ W_B \text{ if } a \in \mathbb{F}_{q^r}^* \setminus \mathcal{C}_{\delta}^{(u,q^r)}. \end{cases} \tag{3}$$

The result now follows from the fact that $|\mathcal{C}_{\delta}^{(u,q^r)}| = \frac{q^r-1}{u}$ and $|\mathbb{F}_{q^r}^* \setminus \mathcal{C}_{\delta}^{(u,q^r)}| = \frac{(q^r-1)(u-1)}{u}$. □

4 The *b*-symbol weight distribution of all one-weight and two-weight semiprimitive irreducible cyclic codes

We are now in conditions to present our main results.

Theorem 3 *Assume the same notation and assumptions as in Theorem 2. Let $\mathcal{P}(b)$, $\mu_{(i)}(b)$, and δ be as before. For $0 \le i < u$ and $1 \le b \le r$, let*

$$W_i^{(b)} = \frac{(q-1)q^{r/2-b}}{N} \left[|\mathcal{P}(b)| \left(q^{r/2} - (-1)^s \right) + (-1)^s u \mu_{((\delta - i) \pmod{u})}(b) \right] \tag{4}$$

Then, the b-symbol Hamming weight enumerator of $\mathscr{C}$ is

$$A(T) = 1 + \frac{q^r - 1}{u} \sum_{i=0}^{u-1} T^{W_i^{(b)}}. \tag{5}$$

Proof Let $a \in \mathbb{F}_{q^r}^*$ and let $c(a) \in \mathscr{C}$. Let W_A and W_B be as in Theorem 2 and suppose that $a \in \mathcal{C}_i^{(u,q^r)}$, for some $0 \le i < u$. Thus, from (3), $w_H(c(\theta a)) = W_A$ iff $\theta a \in \mathcal{C}_{\delta}^{(u,q^r)}$ iff $\theta \in \mathcal{C}_{(\delta - i) \pmod{u}}^{(u,q^r)}$. But there are exactly $\mu_{((\delta - i) \pmod{u})}(b)$ elements θ in $\mathcal{P}(b)$ that satisfy the condition $\theta \in \mathcal{C}_{(\delta - i) \pmod{u}}^{(u,q^r)}$. Therefore, owing to Lemma 2, $w_b(c(a)) = W_i^{(b)}$ where

$$W_i^{(b)} = \frac{1}{q^{b-1}} \left[\mu_{((\delta - i) \pmod{u})}(b) W_A + \left(|\mathcal{P}(b)| - \mu_{((\delta - i) \pmod{u})}(b) \right) W_B \right].$$

Hence, (4) follows by considering the explicit values of W_A and W_B in Theorem 2. Finally, the b-symbol Hamming weight enumerator of $\mathscr{C}$ follows from (3) and from the fact that $|\mathcal{C}_i^{(u,q^r)}| = \frac{q^r-1}{u}$, for any $0 \le i < u$. □

Note that the previous theorem is also valid for $b = 1$. In fact, in this case, the ordinary Hamming weight enumerator in (2) is exactly the same as the 1-symbol Hamming weight enumerator of (5) (take into consideration Remarks 2 and 3). Therefore we see that Theorem 3 not only simplifies and generalizes [12, Corollary 3.1] but also generalizes Theorem 2.

Example 1 The following are some examples of Theorem 3.

(a) Let $(q, r, N, b) = (3, 4, 2, 3)$. Thus $u = \gcd(\Delta, N) = 2$, $s = 2$, $\delta = 0$, and $|\mathcal{P}(b)| = q^2 + q + 1 = 13$. Since $\mu_{(0)}(b) = 8$ (see [12, Example 2.3]), $\mu_{(1)}(b) = |\mathcal{P}(b)| - \mu_{(0)}(b) =$

5. Therefore, owing to Theorems 2 and 3, $W_A = 30$, $W_B = 24$, $W_0^{(3)} = 40$, $W_1^{(3)} = 38$, and $\mathscr{C}$ is a $[40, 4]_3$ irreducible cyclic code whose ordinary and 3-symbol Hamming weight enumerators are $1 + 40T^{24} + 40T^{30}$ and $1 + 40T^{38} + 40T^{40}$, respectively.

(b) Let $(q, r, N, b) = (2, 4, 3, 2)$. Thus $u = \gcd(\Delta, N) = 3$, $s = 2$, $\delta = 0$, and $|\mathcal{P}(b)| = q + 1 = 3$. We take $\mathbb{F}_{16} = \mathbb{F}_2(\gamma)$ with $\gamma^4 + \gamma + 1 = 0$. Hence $\mathcal{P}(b) = \{1 = \gamma^0, \gamma^3, 1 + \gamma^3 = \gamma^{14}\}$. This means that $\mu_{(0)}(b) = 2$, $\mu_{(1)}(b) = 0$, and $\mu_{(2)}(b) = 1$. Therefore, owing to Theorems 2 and 3, $W_A = 4$, $W_B = 2$, $W_0^{(2)} = 5$, $W_1^{(2)} = 4$, $W_2^{(2)} = 3$, and $\mathscr{C}$ is a $[5, 4]_2$ irreducible cyclic code whose ordinary and 2-symbol Hamming weight enumerators are $1+10T^2+5T^4$ and $1+5(T^3+T^4+T^5)$, respectively.

(c) Let $(q, r, N, b) = (4, 3, 9, 2)$. Thus $u = \gcd(\Delta, N) = 3$, $s = 3$, $\delta = 0$, and $|\mathcal{P}(b)| = q + 1 = 5$. Let $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ with $\alpha^2 + \alpha + 1 = 0$. We take $\mathbb{F}_{64} = \mathbb{F}_4(\gamma)$ with $\gamma^3 + \gamma^2 + \gamma + \alpha = 0$. Hence $\mathcal{P}(b) = \{1 = \gamma^0, \gamma^9, 1 + \gamma^9 = \gamma^{27}, 1 + \alpha\gamma^9 = \gamma^5, 1 + \alpha^2\gamma^9 = \gamma^{40}\}$. This means that $\mu_{(0)}(b) = 3$, $\mu_{(1)}(b) = 1$, and $\mu_{(2)}(b) = 1$. Therefore, owing to Theorems 2 and 3, $W_A = 4$, $W_B = 6$, $W_0^{(2)} = 6$, $W_1^{(2)} = W_2^{(2)} = 7$, and $\mathscr{C}$ is a $[7, 3]_4$ irreducible cyclic code whose ordinary and 2-symbol Hamming weight enumerators are $1 + 21T^4 + 42T^6$ and $1 + 21T^6 + 42T^7$, respectively.

(d) Let $(q, r, N, b) = (5, 5, 4, 3)$. Thus $u = \gcd(\Delta, N) = 1$ and $|\mathcal{P}(b)| = \mu_{(0)}(b) = q^2 + q + 1 = 31$. Therefore, owing to Theorems 2 and 3, $W_A = 625$, $W_0^{(3)} = 775$, and $\mathscr{C}$ is a $[781, 5]_5$ one-weight irreducible cyclic code whose ordinary and 3-symbol Hamming weight enumerators are $1 + 3124T^{625}$ and $1 + 3124T^{775}$, respectively.

Remark 6 With the help of a C program, the previous numerical examples were corroborated. Such C program is available via email upon request.

As Example 1-(d) has shown, it is quite easy to obtain the b-symbol Hamming weight enumerator of a one-weight irreducible cyclic code (that is, when $u = 1$). The following result shows it in the general case.

Theorem 4 *Assume the same notation as in Theorem 3. If $u = \gcd(\Delta, N) = 1$, then, for any $1 \le b \le r$, the b-symbol Hamming weight enumerator of $\mathscr{C}$ is*

$$A(T) = 1 + (q^r - 1)T^{\frac{q^r - q^{r-b}}{N}}.$$

Proof If $u = 1$, then $\mu_{(0)}(b) = |\mathcal{P}(b)| = \frac{q^b-1}{q-1}$. Thus the result now follows from (4). □

Remark 7 If $\mathscr{C}$ is an $(n, M, d_b(\mathscr{C}))_q$ b-symbol code, with $b \le d_b(\mathscr{C}) \le n$, then Ding et al. [3] established the Singleton-type bound $M \le q^{n-d_b(\mathscr{C})+b}$. Therefore, an $(n, M, d_b(\mathscr{C}))_q$ b-symbol code $\mathscr{C}$ with $M = q^{n-d_b(\mathscr{C})+b}$ is called a *maximum distance separable* (MDS for short) b-symbol code.

Similar to Theorem 3.3 in [12] we also have:

Theorem 5 *Let $\mathscr{C}$ be as in Definition 1. Let $a \in \mathbb{F}_{q^r}^*$ and consider the codeword $c(a) = (Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a\gamma^{Ni}))_{i=0}^{n-1}$ in $\mathscr{C}$. Then*

$$w_r(c(a)) = n, \tag{6}$$

and $\mathscr{C}$ is an MDS b-symbol code.

Proof Suppose that $a \in \mathcal{C}_i^{(u,q^r)}$ for some $0 \leq i < u$. Thus, by the proof of Theorem 3, $w_r(c(a)) = W_i^{(r)}$ where

$$W_i^{(r)} = \frac{(q-1)q^{r/2-r}}{N}\left[|\mathcal{P}(r)|\left(q^{r/2} - (-1)^s\right) + (-1)^s u \mu_{((\delta - i) \pmod{u})}(r)\right]$$

But, owing to Lemma 3, $\mu_{((\delta-i) \pmod{u})}(r) = \frac{\Delta}{u}$. On the other hand, $|\mathcal{P}(r)| = \Delta = \frac{q^r-1}{q-1}$ and $n = \frac{q^r-1}{N}$. Thus, (6) now follows. Finally, since $d_b(\mathscr{C}) = n$ and $|\mathscr{C}| = q^r$, $\mathscr{C}$ is an MDS b-symbol code by Remark 7. □

Acknowledgements The author would like to thank the anonymous reviewers for their valuable comments and suggestions.

Data Availability All data generated or analyzed during this study are included in this published article. Any supporting data is available from the corresponding author on reasonable request.

Declarations

Conflict of interest The author has no conflicts of interest and no financial disclosures to report.

References

1. Delsarte P.: On subfield subcodes of Reed–Solomon codes. IEEE Trans. Inf. Theory **21**(5), 575–576 (1975).
2. Ding C., Yang J.: Hamming weights in irreducible cyclic codes. Discret. Math. **313**(4), 434–446 (2013).
3. Ding B., Zhang T., Ge G.: Maximum distance separable codes for b-symbol read channels. Finite Fields Appl. **49**, 180–197 (2018).
4. Huffman C.W., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
5. Lidl R., Niederreiter H.: Finite Fields. Cambridge University Press, Cambridge (1983).
6. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, North-Holland (1978).
7. Moisio M.: A note on evaluations of some exponential sums. Acta Arith. **93**, 117–119 (2000).
8. Schmidt B., White C.: All two-weight irreducible cyclic codes? Finite Fields Appl. **8**(1), 1–17 (2002).
9. Shi M., Özbudak F., Solé P.: Geometric approach to b-symbol Hamming weights of cyclic codes. IEEE Trans. Inf. Theory **67**(6), 3735–3751 (2021).
10. Vega G.: A characterization of all semiprimitive irreducible cyclic codes in terms of their lengths. Appl. Algebra Eng. Commun. Comput. **30**(5), 441–452 (2019).
11. Yaakobi E., Bruck J., Siegel P.H.: Constructions and decoding of cyclic codes over b-symbol read channels. IEEE Trans. Inf. Theory **62**(4), 1541–1551 (2016).
12. Zhu H., Shi M., Özbudak F.: Complete b-symbol weight distribution of some irreducible cyclic codes. Des. Codes Cryptogr. **90**(5), 1113–1125 (2022).