Available online at www.sciencedirect.com
ScienceDirect
Finite Fields and Their Applications 14 (2008) 22–40
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions

Hai Q. Dinh

Department of Mathematical Sciences, Kent State University, 4314 Mahoning Avenue, Warren, OH 44483, USA

Received 15 February 2006; revised 11 March 2007

Communicated by Gary L. Mullen

Abstract

We investigate negacyclic and cyclic codes of length p^s over the finite field $\mathbb{F}_{p^a}$. Negacyclic codes of length p^s are precisely the ideals of the chain ring $\frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}+1\rangle}$. This structure is then used to obtain the Hamming distance distribution of the class of such negacyclic codes, which also provides Hamming weight distributions and enumerations of several codes. An one-to-one correspondence between negacyclic and cyclic codes is established to carry accordingly those results of negacyclic codes to cyclic codes.

Keywords: Cyclic codes; Negacyclic codes; Finite fields; Hamming distance; Hamming weight; MacWilliams identity; Repeated-root codes

1. Introduction

Negacyclic and cyclic codes over finite fields have been well studied since the late 1950s. However, most of the research is concentrated on the situation when the code length n is relatively prime to the characteristic of the field F. In such case, cyclic codes of length n are classified as ideals $\langle f(x)\rangle$ of $\frac{F[x]}{\langle x^n-1\rangle}$, where $f(x)$ is a divisor of x^n-1. The case when the code length n is divisible by the characteristics p of the field yields the so-called repeated-root codes, which were first studied in the 1990s by Castagnoli et al. [3], and van Lint [25], where they showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad.

E-mail address: hdinh@kent.edu.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2007.07.001

However, such codes are optimal in a few cases, that motivates researchers to further investigate this class of codes (see, for example, [17,24]).

We have been studied repeated-root negacyclic codes over several classes of finite chain rings. In 2004, the structure of negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$ was obtained [9]. In 2005 [7], we provided the structure of such codes over Galois rings $\mathrm{GR}(2^a, m)$, a more general class of rings, and also gave the Hamming distances of most of those codes over $\mathbb{Z}_{2^a}$. Recently in 2007, we computed the Hamming distances of all those codes [8], and furthermore provided the Lee, homogeneous, and Euclidean distances of all such codes. Our computation in [7–9] were based on the fact that the characteristic of the residue fields of the rings is 2, which makes it possible to obtain the structure of the codes under consideration, they are linearly ordered as ideals of a chain rings. In cases that the characteristic of the residue fields of the chain rings are odd primes, those codes are no longer linearly ordered.

For example, negacyclic codes of length p^s over $\mathbb{Z}_{p^a}$, where p is odd, are ideals of the residue ring $\frac{\mathbb{Z}_{p^a}[x]}{\langle x^{p^s}+1\rangle}$. This residue ring is a local ring, but not a chain ring. However, if we replace the Galois ring $\mathbb{Z}_{p^a}$ by the Galois field $\mathbb{F}_{p^a}$, where we do not have to deal with abundant zero-divisors, it can be showed that the residue ring $\frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}+1\rangle}$ is a chain ring (cf. Proposition 3.2), so the computation techniques we have used in [7,8] can be extended to study the Hamming distances of the codes.

The purpose of this paper is to investigate (repeated-root) negacyclic and cyclic codes of length p^s over $\mathbb{F}_{p^a}$, concentrating on the Hamming distance distributions of those classes of codes, and the Hamming weight distributions and enumerator of each code. The Hamming distance distribution of a class of codes plays a very important role, for instance, in estimating decoding error probabilities. This distance distribution is very difficult to compute in general, however, for the class of negacyclic codes of length p^s over $\mathbb{F}_{p^a}$, their chain structure will help to determine the exact values of their Hamming distances, and furthermore provide Hamming weight distributions and enumerators of numerous codes.

The rest of this paper is arranged as follows. In Section 2, we give some preliminaries about codes over finite fields $\mathbb{F}_{p^a}$, i.e., p^a-ary codes, including a version for p^a-ary codes of the MacWilliams identities, which will be used in Section 4 to determine the Hamming weight distributions and enumerations of several negacyclic codes. Section 3 gives a chain structure of all p^a-ary negacyclic codes of length p^s, those codes are precisely the ideals $\langle (x+1)^i\rangle$, $i = 0, 1, \ldots, p^s$, of the chain ring $\frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}+1\rangle}$. Using this structure, we are able to compute the Hamming distances of all such negacyclic codes in Section 4. This computation also helps us, in Section 5, to determine completely the Hamming weight distributions and enumerations of numerous negacyclic codes. Finally, Section 6 provides a one-to-one correspondence between negacyclic codes and cyclic codes of length p^s over $\mathbb{F}_{p^a}$, which carries all results we have obtained for negacyclic codes to cyclic codes accordingly.

2. Background and notations

A ring R is called a local ring if it has a unique maximal right (left) ideal. R is called a chain ring if the set of all right (left) ideals of R is linearly ordered under set-theoretic inclusion.

For a finite field F, consider the set F^n of n-tuples of elements from F as a vector space over F. Any nonempty subset $C \subseteq F^n$ is called a code of length n over F, the code C is linear

if in addition, C is a subspace of F^n. Given an n-tuple $(x_0, x_1, \ldots, x_{n-1}) \in F^n$, the cyclic shift τ and negashift ν on F^n are defined as usual, i.e.,

$$\tau(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_0, x_1, \ldots, x_{n-2}),$$

and

$$\nu(x_0, x_1, \ldots, x_{n-1}) = (-x_{n-1}, x_0, x_1, \ldots, x_{n-2}).$$

A code C is called cyclic if $\tau(C) = C$, and C is called negacyclic if $\nu(C) = C$. Cyclic codes over finite fields were first studied in the late 1950s by Prange [19–22], while negacyclic codes over finite fields were introduced by Berlekamp in the late 1960s [1,2].

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\frac{F[x]}{\langle x^n+1\rangle}$ ($\frac{F[x]}{\langle x^n-1\rangle}$), $xc(x)$ corresponds to a nega shift (cyclic shift) of $c(x)$. From that, the following fact is well-known and straightforward:

2.1. Proposition. *A linear code C of length n is negacyclic (cyclic) over F if and only if C is an ideal of $\frac{F[x]}{\langle x^n+1\rangle}$ ($\frac{F[x]}{\langle x^n-1\rangle}$).*

For n-tuples $x = (x_0, x_1, \ldots, x_{n-1})$, $y = (y_0, y_1, \ldots, y_{n-1}) \in F^n$, their inner product is defined as usual $x \cdot y = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1}$. Two n-tuples x, y are called orthogonal if $x \cdot y = 0$. For a linear code C over F, its *dual code* $C^\perp$ is the set of n-tuples over F that are orthogonal to all codewords of C, i.e.,

$$C^\perp = \{x \mid x \cdot y = 0,\ \forall y \in C\}.$$

A code C is called self-orthogonal if $C \subseteq C^\perp$, and it is called self-dual if $C = C^\perp$.

Let $a = (a_1, a_2, \ldots, a_n) \in F^n$, the *Hamming weight* of a, denoted by $\mathrm{wt}(a)$, is the number of nonzero components of a. The Hamming distance $d(a, b)$ of two codewords a, b is the number of components in which they differ, which is the Hamming weight $\mathrm{wt}(a - b)$ of $a - b$. For a linear code C, the Hamming weight and the Hamming distance $d(C)$ are the same, and defined as the smallest Hamming weight of nonzero codewords of C:

$$d(C) = \min\{\mathrm{wt}(a) \mid a \neq \mathbf{0},\ a \in C\}.$$

Furthermore, the Hamming weight enumerator of C is defined by

$$W_C(x, y) = \sum_{v \in C} x^{n-\mathrm{wt}(v)} y^{\mathrm{wt}(v)} = \sum_{j=0}^{n} A_j x^{n-j} y^j,$$

where the Hamming weight distributions A_j's are the number of codewords of Hamming weight j in C. Although the Hamming weight distributions and Hamming weight enumerators do not completely specify a code, they give important information on both theoretical and practical aspects (see for example [10,15,18]). MacWilliams [13–15] provided a relation of the Hamming weight enumerators of a code C over a finite field and that of its dual $C^\perp$, we include here the version for p^a-ary linear codes.

2.2. Theorem *(MacWilliams identity for p^a-ary linear codes). Let C be a p^a-ary linear codes with dual code $C^\perp$, then*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C\big(x + \big(p^a - 1\big)y, x - y\big).$$

From Theorem 2.2, we get a connection between the Hamming weight distributions of linear p^a-ary codes C and $C^\perp$ (cf. [15]).

2.3. Proposition. *Let A_i and A'_i be the number of codewords of Hamming weight i in C and $C^\perp$, where the code length is n, then*

$$A'_k = \frac{1}{|C|} \sum_{i=0}^{n} A_i P_k(i; n),$$

where $P_k(x; n)$ is the Krawtchouk polynomial in x of degree k, defined by

$$P_k(x; n) = \sum_{i=0}^{k} (-1)^i \big(p^a - 1\big)^{k-i} \binom{x}{i} \binom{n-x}{k-i}.$$

The Krawtchouk polynomials $P_k(x; n)$ were named after their originator Krawtchouk (cf. [11, 12,23]). They were first used in coding theory by Delsarte (cf. [4–6]). The binomial coefficients $\binom{x}{m}$ in the Krawtchouk polynomials are defined for any real number x as follows:

$$\binom{x}{m} = \begin{cases} \frac{x(x-1)\cdots(x-m+1)}{m!} & \text{if } m \text{ is a positive integer,} \\ 1 & \text{if } m = 0, \\ 0 & \text{otherwise.} \end{cases}$$

In this paper, we study the structure of negacyclic codes of length p^s over the finite field $\mathbb{F}_{p^a}$, and establish the Hamming distance of all such negacyclic codes, and Hamming weight distributions and enumerators of several codes. We then build a one-to-one correspondence between negacyclic and cyclic codes to carry those properties to cyclic codes of length p^s over $\mathbb{F}_{p^a}$. Hereafter, in order to simplify notation, we denote

$$\mathcal{F}(a, s) = \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s} + 1\rangle}.$$

3. Structure of negacyclic codes

3.1. Proposition. *The followings hold true in $\mathcal{F}(a, s)$:*

(a) *For any nonnegative integer t, $(x + 1)^{p^t} = x^{p^t} + 1$.*
(b) *$x + 1$ is nilpotent with the nilpotency index p^s.*

Proof. We have

$$(x+1)^{p^t} = x^{p^t} + 1 + \sum_{i=1}^{p^t-1} \binom{p^t}{i} x^i.$$

Since, p divides $\binom{p^t}{i}$ for $1 \leqslant i \leqslant p^t - 1$, $\sum_{i=1}^{p^t-1} \binom{p^t}{i} x^i = 0$ in $\mathbb{F}_{p^a}[x]$. Thus, $(x+1)^{p^t} = x^{p^t} + 1$ in $\mathcal{F}(a,s)$, proving (a). (b) is just a direct consequence of (a). □

3.2. Proposition. *$\mathcal{F}(a,s)$ is a chain ring, with exactly the following ideals*:

$$\mathcal{F}(a,s) = \langle (x+1)^0 \rangle \supsetneq \langle (x+1)^1 \rangle \supsetneq \cdots \supsetneq \langle (x+1)^{p^s-1} \rangle \supsetneq \langle (x+1)^{p^s} \rangle = \langle 0 \rangle.$$

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_{p^s-1} x^{p^s-1} \in \mathcal{F}(a,s)$, where $a_0, a_1, \ldots, a_{p^s-1} \in \mathbb{F}_{p^a}$. Then there are $b_0, b_1, \ldots, b_{p^s-1} \in \mathbb{F}_{p^a}$, such that $f(x)$ can be represented as

$$f(x) = b_0 + b_1(x+1) + \cdots + b_{p^s-1}(x+1)^{p^s-1}.$$

If $b_0 = 0$, then $f(x) = (x+1)g(x)$, whence, $f(x) \in \langle x+1 \rangle$. If $b_0 \neq 0$, then $f(x) = b_0 + (x+1)g(x)$, as $x+1$ is nilpotent in $\mathcal{F}(a,s)$, $f(x)$ is invertible. We have shown that for any element $f(x)$ in $\mathcal{F}(a,s)$, either $f(x)$ is a unit, or $f(x) \in \langle x+1 \rangle$. That means, $\mathcal{F}(a,s)$ is a local ring with the maximum ideal $\langle x+1 \rangle$, hence, $\mathcal{F}(a,s)$ is a chain ring (cf. [16]). Since the nilpotency index of $x+1$ is p^s, the ideals of $\mathcal{F}(a,s)$ form the desired strictly inclusive chain. □

Since p^a-ary negacyclic codes of length p^s are the ideals of $\mathcal{F}(a,s)$, we now have a list of all of them.

3.3. Theorem. *p^a-ary negacyclic codes of length p^s are precisely the ideals $\langle (x+1)^i \rangle$, $i = 0, 1, \ldots, p^s$, of the ring $\mathcal{F}(a,s)$.*

Clearly, for $i = 0, 1, \ldots, p^s$, the cardinality of each code $\langle (x+1)^i \rangle \subseteq \mathcal{F}(a,s)$ is $p^{a(p^s-i)}$, hence, the cardinality of its dual is p^{ai} (cf. [16]). Because the dual of a negacyclic code is also a negacyclic code, it implies that the dual code of $\langle (x+1)^i \rangle$ is $\langle (x+1)^{p^s-i} \rangle$. We summarize that in the following theorem.

3.4. Theorem. *Let C be a p^a-ary negacyclic codes of length p^s, then $C = \langle (x+1)^i \rangle \subseteq \mathcal{F}(a,s)$, for some $i \in \{0, 1, \ldots, p^s\}$, and C has $p^{a(p^s-i)}$ codewords. The dual of C is $C^\perp = \langle (x+1)^{p^s-i} \rangle$, which contains p^{ai} codewords.*

As a direct consequence of Theorem 3.4, we get a result about self-orthogonal p^a-ary negacyclic code of length p^s, and the existence of self-dual p^a-ary negacyclic code of length p^s.

3.5. Corollary. *A p^a-ary negacyclic code of length p^s, $\langle (x+1)^i \rangle \subseteq \mathcal{F}(a,s)$, is self-orthogonal if and only if $\frac{p^s}{2} \leqslant i \leqslant p^s$. Self-dual p^a-ary negacyclic code of length p^s exists if and only if $p = 2$. When $p = 2$, there is only one self-dual 2^a-ary negacyclic code of length 2^s, namely, $\langle (x+1)^{2^{s-1}} \rangle \subset \frac{\mathbb{F}_{2^a}[x]}{\langle x^{2^s}+1 \rangle}$.*

4. Hamming distances of negacyclic codes

In this section, in order to simplify notation, for $i = 0, 1, \ldots, p^s$, we denote each code $\langle (x+1)^i \rangle$ by $\mathbf{C}[i]$, and its Hamming distance by d_i. Recall that

$$\mathcal{F}(a,s) = \mathbf{C}[0] \supsetneq \mathbf{C}[1] \supsetneq \cdots \supsetneq \mathbf{C}\big[p^s - 1\big] \supsetneq \mathbf{C}\big[p^s\big] = \langle 0 \rangle.$$

Hence, $d_{p^s} = 0$, and $1 = d_0 \leqslant d_1 \leqslant d_2 \leqslant \cdots \leqslant d_{p^s-1}$.

4.1. Proposition. *For $1 \leqslant i \leqslant p^{s-1}$, $\mathbf{C}[i]$ has Hamming distance $d_i = 2$.*

Proof. Any codeword of Hamming weight 1 is of the form ux^j, which is invertible in $\mathcal{F}(a,s)$, hence $\mathbf{C}[i]$ cannot contain any codeword of Hamming weight 1. That means $d_i \geqslant 2$. Obviously, $x+1 \in \mathbf{C}[1]$, and by Proposition 3.1, $x^{p^{s-1}} + 1 = (x+1)^{p^{s-1}} \in \mathbf{C}[p^{s-1}]$. Thus,

$$2 \leqslant d_1 \leqslant d_2 \leqslant \cdots \leqslant d_{p^s-1} \leqslant 2.$$

Therefore, $d_i = 2$, for $1 \leqslant i \leqslant p^{s-1}$. □

4.2. Proposition. *Let α be an integer such that $1 \leqslant \alpha \leqslant p-1$, then $\mathbf{C}[\alpha p^{s-1}]$ has Hamming distance $2 \leqslant d_{\alpha p^{s-1}} \leqslant \alpha + 1$.*

Proof. As argued in the proof of Proposition 4.1, $d_{\alpha p^{s-1}} \geqslant 2$. Computing in $\mathcal{F}(a,s)$, we get

$$(x+1)^{\alpha p^{s-1}} = \big(x^{p^{s-1}} + 1\big)^{\alpha} = \sum_{j=0}^{\alpha} \binom{\alpha}{j} x^{p^{s-1} j}.$$

Thus, $(x+1)^{\alpha p^{s-1}}$ has Hamming weight $\alpha + 1$, implying $2 \leqslant d_{\alpha p^{s-1}} \leqslant \alpha + 1$. □

In order to compute Hamming distances, we need the concept of *coefficient weight* of polynomials, which we initiated in [8, Definition 3.5]:

4.3. Definition. Given a polynomial of degree n, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, we define the coefficient weight of f, denoted by $\mathrm{cw}(f)$, to be the integer given by

$$\mathrm{cw}(f) = \begin{cases} 0, & \text{if } f \text{ is a monomial,} \\ \min\{|i-j| \colon a_i \neq 0,\ a_j \neq 0,\ i \neq j\}, & \text{otherwise.} \end{cases}$$

Note that $\mathrm{cw}(f)$ is the smallest distance among nonzero terms of $f(x)$. Therefore, if $g(x)$ is a polynomial whose degree is less than $\mathrm{cw}(f)$, then $\mathrm{wt}(f(x)\, g(x)) = \mathrm{wt}(f(x)) \cdot \mathrm{wt}(g(x))$.

4.4. Proposition. *$\mathbf{C}[(p-1)p^{s-1}]$ has Hamming distance $d_{(p-1)p^{s-1}} = p$.*

Proof. By Proposition 4.2, $d_{(p-1)p^{s-1}} \leqslant p$. Let $c(x)$ be a nonzero codeword of $\mathbf{C}[(p-1)p^{s-1}]$, that means there is a nonzero element $f(x) \in \mathcal{F}(a,s)$ such that $c(x) = f(x)\,(x+1)^{(p-1)p^{s-1}} = f(x) \sum_{j=0}^{p-1} \binom{p-1}{j} x^{p^{s-1} j}$. In light of the Division Algorithm, we can assume without loss of

generality that $\deg(f) < p^{s-1}$. Now, since $\mathrm{cw}(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-1}j}) = p^{s-1}$, it follows that $\mathrm{wt}(c(x)) = \mathrm{wt}(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-1}j}) \cdot \mathrm{wt}(f(x)) \geqslant p$. Therefore $d_{(p-1)p^{s-1}} \geqslant p$, which forces $d_{(p-1)p^{s-1}} = p$. □

4.5. Proposition. *Let $m_k = p^s - p^{s-k} = (p-1)\sum_{i=1}^{k} p^{s-i}$, for $1 \leqslant k \leqslant s$, then $\mathbf{C}[m_k]$ has Hamming distance $d_{m_k} = p^k$.*

Proof. First of all,

$$(x+1)^{m_k} = (x+1)^{(p-1)\sum_{i=1}^{k} p^{s-i}} = \prod_{i=1}^{k}\left(x^{p^{s-i}}+1\right)^{p-1} = \prod_{i=1}^{k}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}.$$

If $k = 1$, we get the desired result from Proposition 4.4. For $2 \leqslant k \leqslant s$, we divide our computation into $k-1$ steps as follows.

Step 1.

$$\begin{cases} \mathrm{cw}(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-1}j}) = p^{s-1}, \\ \deg(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-2}j}) = p^{s-1} - p^{s-2}, \\ \mathrm{wt}(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-1}j}) = p \end{cases}$$

$$\Longrightarrow \quad \begin{cases} \mathrm{wt}(\prod_{i=1}^{2}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}) = \mathrm{wt}(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-1}j}) \cdot \mathrm{wt}(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-2}j}) \\ \quad = p^2, \\ \mathrm{cw}(\prod_{i=1}^{2}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}) = p^{s-2}, \\ \deg(\prod_{i=1}^{2}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}) = (p-1)(p^{s-1}+p^{s-2}) = p^s - p^{s-2}. \end{cases}$$

Let $c_2(x)$ be any nonzero codeword of $\mathbf{C}[m_2]$, then there is a nonzero element $f_2(x) \in \mathcal{F}(a,s)$ such that $c_2(x) = f_2(x)\prod_{i=1}^{2}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}$. Since

$$\deg\left(\prod_{i=1}^{2}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) = p^s - p^{s-2},$$

by the Division Algorithm, we can assume without loss of generality that $\deg(f_2) < p^{s-2}$. Because $\mathrm{cw}(\prod_{i=1}^{2}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}) = p^{s-2}$, we get $\mathrm{wt}(c(x)) = \mathrm{wt}(\prod_{i=1}^{2}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}) \cdot \mathrm{wt}(f_2(x)) \geqslant p^2$. Therefore, $d_{m_2} \geqslant p^2$, implying $d_{m_2} = p^2$.

Step 2. From Step 1, we get

$$\begin{cases} \mathrm{cw}(\prod_{i=1}^{2}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}) = p^{s-2}, \\ \deg(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-3}j}) = p^{s-2} - p^{s-3}, \\ \mathrm{wt}(\prod_{i=1}^{2}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}) = p^2 \end{cases}$$

$$\Longrightarrow \quad \begin{cases} \mathrm{wt}\left(\prod_{i=1}^{3}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) \\ \quad = \mathrm{wt}\left(\prod_{i=1}^{2}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right)\cdot \mathrm{wt}\left(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-3}j}\right) = p^3, \\ \mathrm{cw}\left(\prod_{i=1}^{3}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) = p^{s-3}, \\ \deg\left(\prod_{i=1}^{3}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) = (p-1)(p^{s-1}+p^{s-2}+p^{s-3}) = p^s - p^{s-3}. \end{cases}$$

Let $c_3(x)$ be any nonzero codeword of $\mathbf{C}[m_3]$, then there is a nonzero element $f_3(x) \in \mathcal{F}(a,s)$ such that $c_3(x) = f_3(x)\prod_{i=1}^{3}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}$. Since

$$\deg\left(\prod_{i=1}^{3}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) = p^s - p^{s-3},$$

by the Division Algorithm, we can assume without loss of generality that $\deg(f_3) < p^{s-3}$. Because $\mathrm{cw}(\prod_{i=1}^{3}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}) = p^{s-3}$, we get $\mathrm{wt}(c(x)) = \mathrm{wt}(\prod_{i=1}^{3}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j})\cdot \mathrm{wt}(f_3(x)) \geqslant p^3$. Therefore, $d_{m_3} \geqslant p^3$, implying $d_{m_3} = p^3$.

Step $k-1$. From Step $k-2$, we get

$$\begin{cases} \mathrm{cw}\left(\prod_{i=1}^{k-1}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) = p^{s-k+1}, \\ \deg\left(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-k}j}\right) = p^{s-k+1} - p^{s-k}, \\ \mathrm{wt}\left(\prod_{i=1}^{k-1}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) = p^{k-1} \end{cases}$$

$$\Longrightarrow \quad \begin{cases} \mathrm{wt}\left(\prod_{i=1}^{k}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) \\ \quad = \mathrm{wt}\left(\prod_{i=1}^{k-1}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right)\cdot \mathrm{wt}\left(\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-k}j}\right) = p^k, \\ \mathrm{cw}\left(\prod_{i=1}^{k}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) = p^{s-k}, \\ \deg\left(\prod_{i=1}^{k}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) = (p-1)\sum_{i=1}^{k}p^{s-i} = p^s - p^{s-k}. \end{cases}$$

Let $c_k(x)$ be any nonzero codeword of $\mathbf{C}[m_k]$, then there is a nonzero element $f_k(x) \in \mathcal{F}(a,s)$ such that $c_k(x) = f_k(x)\prod_{i=1}^{k}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}$. Since

$$\deg\left(\prod_{i=1}^{k}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}\right) = p^s - p^{s-k},$$

by the Division Algorithm, we can assume without loss of generality that $\deg(f_k) < p^{s-k}$. Because $\mathrm{cw}(\prod_{i=1}^{k}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j}) = p^{s-k}$, we get $\mathrm{wt}(c(x)) = \mathrm{wt}(\prod_{i=1}^{k}\sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-i}j})\cdot \mathrm{wt}(f_k(x)) \geqslant p^k$. Therefore, $d_{m_k} \geqslant p^k$, implying $d_{m_k} = p^k$. □

4.6. Proposition. *Let $1 \leqslant t \leqslant p-1$, and $(p-1)p^{s-1} + (t-1)p^{s-2} + 1 \leqslant i \leqslant (p-1)p^{s-1} + tp^{s-2}$. Then $\mathbf{C}[i]$ has Hamming distance $d_i = (t+1)p$.*

Proof. Let $i = (p-1)p^{s-1} + (t-1)p^{s-2} + l$, $1 \leqslant l \leqslant p^{s-2}$. Then

$$(x+1)^i = (x+1)^{(p-1)p^{s-1}}(x+1)^{(t-1)p^{s-2}+l}.$$

Let $c(x)$ be a nonzero codeword of $\mathbf{C}[i]$, then there is a nonzero element $f(x) \in \mathcal{F}(a,s)$ such that $c(x) = (x+1)^i f(x)$. By the Division Algorithm, we can assume without loss of generality that $\deg(f) < p^s - i = p^{s-1} - (t-1)p^{s-2} - l$. Now

$$c(x) = (x+1)^i f(x) = (x+1)^{(p-1)p^{s-1}}\big[(x+1)^{(t-1)p^{s-2}+l} f(x)\big].$$

As in Proposition 4.4, $\mathrm{cw}((x+1)^{(p-1)p^{s-1}}) = p^{s-1}$, and $\mathrm{wt}((x+1)^{(p-1)p^{s-1}}) = p$. Clearly,

$$\deg\big((x+1)^{(t-1)p^{s-2}+l} f(x)\big) = (t-1)p^{s-2} + l + \deg(f) < p^{s-1},$$

therefore

$$\begin{aligned}\mathrm{wt}\big(c(x)\big) &= \mathrm{wt}\big((x+1)^{(p-1)p^{s-1}}\big) \cdot \mathrm{wt}\big((x+1)^{(t-1)p^{s-2}+l} f(x)\big) \\ &= p \cdot \mathrm{wt}\big((x+1)^{(t-1)p^{s-2}+l} f(x)\big).\end{aligned}$$

Now the codeword $(x+1)^{(t-1)p^{s-2}+l} f(x)$, with $\deg(f) < p^{s-1} - (t-1)p^{s-2} - l$, can be viewed as an element of the code $\langle (x+1)^{(t-1)p^{s-2}} \rangle \subset \mathcal{F}(a, s-1)$, which has Hamming distance $t+1$ as we will show in Proposition 4.10. Hence, $\mathrm{wt}((x+1)^{(t-1)p^{s-2}+l} f(x)) \geqslant t+1$, implying $\mathrm{wt}(c(x)) \geqslant (t+1)p$. Consequently, $d_i = (t+1)p$. □

Using arguements similar to Propositions 4.5 and 4.6, we get the Hamming distances of all negacyclic codes $\mathbf{C}[i]$ when $(p-1)p^{s-1} \leqslant i \leqslant p^s - 1$.

4.7. Proposition. *Let t, k be integers such that $1 \leqslant t \leqslant p-1$, and $1 \leqslant k \leqslant s-1$. For integer i with*

$$(p-1)\sum_{i=1}^{k} p^{s-i} + (t-1)p^{s-k-1} + 1 \leqslant i \leqslant (p-1)\sum_{i=1}^{k} p^{s-i} + tp^{s-k-1},$$

i.e.,

$$p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \leqslant i \leqslant p^s - p^{s-k} + tp^{s-k-1},$$

the code $\mathbf{C}[i]$ has Hamming distance $d_i = (t+1)p^k$.

4.8. Lemma. *For any prime p, and integer j with $1 \leqslant j \leqslant p-1$, the following hold*:

(a) $\binom{p-2}{j} \equiv (j+1)(-1)^j \pmod{p}$,
(b) $\binom{p-1}{j} \equiv (-1)^j \pmod{p}$,
(c) $k\binom{p-2}{j} + \binom{p-2}{j-1} \equiv (kj + k - j)(-1)^j \pmod{p}$.

Proof. (a) follows from

$$\binom{p-2}{j} = \frac{(p-2)\cdots(p-1-j)}{j!} \equiv \frac{(-1)^j(j+1)!}{j!} \pmod p \equiv (j+1)(-1)^j \pmod p.$$

Now using (a), we get

$$\binom{p-1}{j} = \binom{p-2}{j} + \binom{p-2}{j-1} \equiv (j+1)(-1)^j + j(-1)^{j-1} \pmod p \equiv (-1)^j \pmod p,$$

proving (b). Finally, (c) follows from (a) and (b) as

$$\begin{aligned} k\binom{p-2}{j} + \binom{p-2}{j-1} &= (k-1)\binom{p-2}{j} + \binom{p-1}{j} \\ &\equiv (k-1)(j+1)(-1)^j + (-1)^j \pmod p \\ &\equiv (kj+k-j)(-1)^j \pmod p. \qquad \square \end{aligned}$$

4.9. Proposition. *Let β be an integer such that $1 \leqslant \beta \leqslant p-2$, then the code $\mathbf{C}[\beta p^{s-1}+1]$ has Hamming distance $d_{\beta p^{s-1}+1} \geqslant \beta+2$.*

Proof. We first show that the assertion holds for $\beta = p-2$. Let $c(x)$ be any nonzero element of $\mathbf{C}[(p-2)p^{s-1}+1]$, then there is a nonzero element $f(x) \in \mathcal{F}(a,s)$ such that $c(x) = (x+1)^{(p-2)p^{s-1}}(x+1)f(x)$. By the Division Algorithm, we can assume that $\deg(f) < p^s - (p-2)p^{s-1} - 1 = 2p^{s-1} - 1$. Denote $g(x) = (x+1)f(x)$, then $\mathrm{wt}(g(x)) \geqslant 2$, and

$$c(x) = (x+1)^{(p-2)p^{s-1}} g(x) = \sum_{j=0}^{p-2} \binom{p-2}{j} x^{p^{s-1}j}\, g(x).$$

Note that $\mathrm{cw}(\sum_{j=0}^{p-2}\binom{p-2}{j}x^{p^{s-1}j}) = p^{s-1}$, and $\mathrm{wt}(\sum_{j=0}^{p-2}\binom{p-2}{j}x^{p^{s-1}j}) = p-1$. We consider five cases.

Case 1. $\mathrm{wt}(g(x)) = 2$, and $\mathrm{cw}(g(x)) \neq p^{s-1}$. Then

$$\mathrm{wt}\big(c(x)\big) = \mathrm{wt}\left(\sum_{j=0}^{p-2}\binom{p-2}{j}x^{p^{s-1}j}\right)\cdot \mathrm{wt}\big(g(x)\big) = 2(p-1) \geqslant p.$$

Case 2. $\mathrm{wt}(g(x)) = 2$, and $\mathrm{cw}(g(x)) = p^{s-1}$. As $g(x) = (x+1)f(x)$, $g(x)$ must be of the form $g(x) = rx^i(x^{p^{s-1}}+1) = rx^i(x+1)^{p^{s-1}}$, where $0 \leqslant i \leqslant p^{s-1}-1$, and $r \in \mathbb{F}_{p^a} - \{0\}$. Thus,

$$c(x) = rx^i(x+1)^{p^{s-1}}(x+1)^{(p-2)p^{s-1}} = rx^i\,(x+1)^{(p-1)p^{s-1}} = rx^i \sum_{j=0}^{p-1}\binom{p-1}{j}x^{p^{s-1}j}.$$

Hence, $\mathrm{wt}(c(x)) = p$.

Case 3. $\mathrm{wt}(g(x)) \geqslant 3$, and there is no pair of (nonzero) terms $r_1x^{i_1}$, $r_2x^{i_2}$ of $g(x)$ such that $|i_1 - i_2| = p^{s-1}$. Then

$$\mathrm{wt}\big(c(x)\big) = \mathrm{wt}\left(\sum_{j=0}^{p-2}\binom{p-2}{j}x^{p^{s-1}j}\right)\cdot \mathrm{wt}\big(g(x)\big) \geqslant 3(p-1) > p.$$

Case 4. $\mathrm{wt}(g(x)) \geqslant 3$, and there is exactly one pair of (nonzero) terms $r_1x^{i_1}$, $r_2x^{i_2}$ of $g(x)$ such that $|i_1 - i_2| = p^{s-1}$. Let $g_1(x) = r_1x^{i_1} + r_2x^{i_2}$, and $g_2(x) = g(x) - g_1(x)$. Without loss of generality, $g_1(x)$ can be represented as $g_1(x) = rx^i(kx^{p^{s-1}} + 1)$, where $0 \leqslant i \leqslant p^{s-1} - 1$, and $r, k \in \mathbb{F}_{p^a} - \{0\}$. Therefore,

$$\begin{aligned}(x+1)^{(p-2)p^{s-1}}g_1(x) &= rx^i\big(kx^{p^{s-1}} + 1\big)\sum_{j=0}^{p-2}\binom{p-2}{j}x^{p^{s-1}j}\\ &= rx^i\left[kx^{(p-1)p^{s-1}} + \left(\sum_{j=1}^{p-2}\alpha_j x^{p^{s-1}j}\right) + 1\right],\end{aligned}$$

where, for $1 \leqslant j \leqslant p-2$,

$$\alpha_j = k\binom{p-2}{j} + \binom{p-2}{j-1}.$$

By Lemma 4.8(c), in $\mathbb{F}_{p^a}$, $\alpha_j = (kj + k - j)(-1)^j$. Thus, $\alpha_j = 0$ if and only if $kj + k - j = 0 \pmod p$, i.e., $j(k-1) = -k \pmod p$. Hence, $\alpha_j = 0$ if and only if $k \neq 1$, and $j = -k(k-1)^{-1}$. That means, for $1 \leqslant j \leqslant p-2$, there is at most one value of j which makes $a_j = 0$. Therefore, $\mathrm{wt}((x+1)^{(p-2)p^{s-1}}g_1(x)) \geqslant p-1$. On the other hand,

$$\mathrm{wt}\big((x+1)^{(p-2)p^{s-1}}g_2(x)\big) = \mathrm{wt}\left(\sum_{j=0}^{p-2}\binom{p-2}{j}x^{p^{s-1}j}\right)\cdot \mathrm{wt}\big(g_2(x)\big) \geqslant p-1.$$

Hence,

$$\mathrm{wt}\big(c(x)\big) = \mathrm{wt}\big((x+1)^{(p-2)p^{s-1}}g_1(x)\big) + \mathrm{wt}\big((x+1)^{(p-2)p^{s-1}}g_2(x)\big) \geqslant 2(p-1) \geqslant p.$$

Case 5. $\mathrm{wt}(g(x)) \geqslant 3$, and there are more than one pairs of (nonzero) terms $r_1x^{i_1}$, $r_2x^{i_2}$ of $g(x)$ such that $|i_1 - i_2| = p^{s-1}$. It is sufficient to assume that there are two such pairs, i.e., there are terms $r_1x^{i_1}$, $r_2x^{i_2}$, $r_3x^{i_3}$, $r_4x^{i_4}$ of $g(x)$ such that $|i_1 - i_2| = |i_3 - i_4| = p^{s-1}$. Since, $\deg(g(x)) < 2p^{s-1}$, all terms $r_1x^{i_1}$, $r_2x^{i_2}$, $r_3x^{i_3}$, $r_4x^{i_4}$ are distinct. Let $g_1(x) = r_1x^{i_1} + r_2x^{i_2}$, $g_3(x) = r_3x^{i_3} + r_4x^{i_4}$, and $g_2(x) = g(x) - g_1(x) - g_3(x)$. As obtained in Case 4, $\mathrm{wt}((x+1)^{(p-2)p^{s-1}}g_1(x)) \geqslant p-1$, and $\mathrm{wt}((x+1)^{(p-2)p^{s-1}}g_3(x)) \geqslant p-1$. Whence,

$$\begin{aligned}\mathrm{wt}\big(c(x)\big) &= \mathrm{wt}\big((x+1)^{(p-2)p^{s-1}}g_1(x)\big) + \mathrm{wt}\big((x+1)^{(p-2)p^{s-1}}g_3(x)\big)\\ &\quad + \mathrm{wt}\big((x+1)^{(p-2)p^{s-1}}g_2(x)\big) \geqslant 2(p-1) \geqslant p.\end{aligned}$$

Therefore, we have shown that the Hamming weight of any nonzero element $c(x)$ in $\mathbf{C}[(p-2)p^{s-1}+1]$ is at least p, implying $\mathbf{C}[(p-2)p^{s-1}+1]$ has Hamming distance $d_{(p-2)p^{s-1}+1} \geqslant p$, i.e., the statement is true for $\beta = p-2$. Repeating this process for $\beta = p-3, p-4, \ldots, 2, 1$, we get that the statement holds for all β with $1 \leqslant \beta \leqslant p-2$. □

4.10. Proposition. *Let β, γ be integers such that $0 \leqslant \beta \leqslant p-2$, and $\beta p^{s-1}+1 \leqslant \gamma \leqslant (\beta+1)p^{s-1}$, then $\mathbf{C}[\gamma]$ has Hamming distance $d_\gamma = \beta+2$.*

Proof. If $\beta = 0$, the statement is true by Proposition 4.1. Consider $1 \leqslant \beta \leqslant p-2$, as $\beta p^{s-1}+1 \leqslant \gamma \leqslant (\beta+1)p^{s-1}$, we get $\mathbf{C}[\beta p^{s-1}+1] \supsetneq \mathbf{C}[\gamma] \supsetneq \mathbf{C}[(\beta+1)p^{s-1}]$, and hence, $d_{\beta p^{s-1}+1} \leqslant d_\gamma \leqslant d_{(\beta+1)p^{s-1}}$. On the other hand, in light of Propositions 4.9 and 4.2, $d_{\beta p^{s-1}+1} \geqslant \beta+2$, and $d_{(\beta+1)p^{s-1}} \leqslant \beta+2$. Hence, the conclusion follows. □

Thus, we have obtained the Hamming distances of all p^a-ary negacyclic codes of length p^s. We summarize that in the following theorem.

4.11. Theorem. *Let C be a p^a-ary negacyclic codes of length p^s, then $C = \langle (x+1)^i \rangle \subseteq \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}+1 \rangle}$, for $i \in \{0, 1, \ldots, p^s\}$. The Hamming distance d_i of C is determined by*

$$d_i = \begin{cases} 1, & \text{if } i = 0, \\ \beta+2, & \text{if } \beta p^{s-1}+1 \leqslant i \leqslant (\beta+1)p^{s-1} \text{ where } 0 \leqslant \beta \leqslant p-2, \\ (t+1)p^k, & \text{if } p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \leqslant i \leqslant p^s - p^{s-k} + tp^{s-k-1} \\ & \text{where } 1 \leqslant t \leqslant p-1, \text{ and } 1 \leqslant k \leqslant s-1, \\ 0, & \text{if } i = p^s. \end{cases}$$

4.12. Corollary. *Let C be a 2^a-ary cyclic codes of length 2^s, then $C = \langle (x+1)^i \rangle \subseteq \frac{\mathbb{F}_{2^a}[x]}{\langle x^{2^s}+1 \rangle}$, for $i \in \{0, 1, \ldots, 2^s\}$. The Hamming distance d_i of C is determined by*

$$d_i = \begin{cases} 1, & \text{if } i = 0, \\ 2, & \text{if } 1 \leqslant i \leqslant 2^{s-1}, \\ 2^{k+1}, & \text{if } 2^s - 2^{s-k} + 1 \leqslant i \leqslant 2^s - 2^{s-k} + 2^{s-k-1} \text{ where } 1 \leqslant k \leqslant s-1, \\ 0, & \text{if } i = 2^s. \end{cases}$$

5. Hamming weight enumerators and distributions of negacyclic codes

5.1. Proposition. *Codewords of the code $C = \langle (x+1)^{p^s-1} \rangle \subset \mathcal{F}(a, s)$ are*

$$\left\{ \eta \left[1 + \binom{p^s-1}{1} x + \cdots + \binom{p^s-1}{p^s-2} x^{p^s-2} + x^{p^s-1} \right] \,\middle|\, \eta \in \mathbb{F}_{p^a} \right\}.$$

In particular, its Hamming weight distributions and enumerator are

$$A_j = \begin{cases} 1, & \text{if } j = 0, \\ p^a - 1, & \text{if } j = p^s, \\ 0, & \text{if } 1 \leqslant j \leqslant p^s - 1, \end{cases}$$

$$W_C(x, y) = x^{p^s} + \left(p^a - 1\right) y^{p^s}.$$

Proof. In $\mathcal{F}(a,s)$, $(x+1)^{p^s-1} = 1 + \binom{p^s-1}{1}x + \cdots + \binom{p^s-1}{p^s-2}x^{p^s-2} + x^{p^s-1}$, the result follows since, by Theorem 3.4, $|C| = p^a$. □

5.2. Proposition. *The code $C = \langle x+1\rangle \subset \mathcal{F}(a,s)$ has Hamming weight distributions and enumerator as*

$$A_j = \frac{p^a-1}{p^a}\binom{p^s}{j}\left[\left(p^a-1\right)^{j-1} + (-1)^j\right],$$

$$W_C(x,y) = \frac{p^a-1}{p^a}\sum_{j=0}^{p^s}\binom{p^s}{j}\left[\left(p^a-1\right)^{j-1} + (-1)^j\right]x^{p^s-j}y^j.$$

Proof. In light of Theorem 3.4, the dual code of C is $C^\perp = \langle (x+1)^{p^s-1}\rangle$. Hence, applying MacWilliams identities give

$$\begin{aligned} W_C(x,y) &= \frac{1}{|C^\perp|}W_{C^\perp}\left(x+\left(p^a-1\right)y, x-y\right) = \frac{1}{p^a}\left[x+\left(p^a-1\right)y\right]^{p^s} + \frac{p^a-1}{p^a}(x-y)^{p^s} \\ &= \frac{1}{p^a}\sum_{j=0}^{p^s}\binom{p^s}{j}x^{p^s-j}\left(p^a-1\right)^j y^j + \frac{p^a-1}{p^a}\sum_{j=0}^{p^s}\binom{p^s}{j}x^{p^s-j}(-1)^j y^j \\ &= \frac{p^a-1}{p^a}\sum_{j=0}^{p^s}\binom{p^s}{j}\left[\left(p^a-1\right)^{j-1} + (-1)^j\right]x^{p^s-j}y^j. \qquad \square \end{aligned}$$

5.3. Proposition. *The code $C = \langle (x+1)^{(p-1)p^{s-1}}\rangle \subset \mathcal{F}(a,s)$ has Hamming weight distributions and enumerator as*

$$A_j = \begin{cases} \binom{p^{s-1}}{t}(p^a-1)^t, & \text{if } j = pt, \text{for } 0 \leqslant t \leqslant p^{s-1}, \\ 0, & \text{otherwise,} \end{cases}$$

$$W_C(x,y) = \sum_{t=0}^{p^{s-1}}\binom{p^{s-1}}{t}\left(p^a-1\right)^t x^{p^s-pt}y^{pt}.$$

Proof. Each codeword $c(x)$ in C has the form $c(x) = (x+1)^{(p-1)p^{s-1}}f(x)$. By the Division Algorithm, we can assume without loss of generality that $\deg(f) < p^s - (p-1)p^{s-1} = p^{s-1}$. As in Proposition 4.4, $\mathrm{wt}((x+1)^{(p-1)p^{s-1}}) = p$, and $\mathrm{cw}((x+1)^{(p-1)p^{s-1}}) = p^{s-1} > \deg(f)$. It means $\mathrm{wt}(c(x)) = \mathrm{wt}((x+1)^{(p-1)p^{s-1}}) \cdot \mathrm{wt}(f(x)) = p \cdot \mathrm{wt}(f(x))$. Therefore, the Hamming weight distributions of C are

$$A_j = \begin{cases} \binom{p^{s-1}}{t}(p^a-1)^t, & \text{if } j = pt, \text{for } 0 \leqslant t \leqslant p^{s-1}, \\ 0, & \text{otherwise,} \end{cases}$$

and hence the Hamming weight enumerator of C is

$$W_C(x,y) = \sum_{t=0}^{p^{s-1}} \binom{p^{s-1}}{t} \big(p^a - 1\big)^t x^{p^s - pt} y^{pt}. \qquad \square$$

More generally, our computation in Proposition 4.5 can be used to give a connection between the Hamming weight distributions of the code $\langle x^{\gamma+(p-1)\sum_{i=1}^{k} p^{s-i}} \rangle \subset \mathcal{F}(a,s)$ and that of the code $\langle (x+1)^{\gamma} \rangle \subset \mathcal{F}(a,s-k)$, for $1 \leqslant k \leqslant s$ and $0 \leqslant \gamma \leqslant p^{s-k} - 1$, as follows.

5.4. Theorem. *Let k, γ be integers such that $1 \leqslant k \leqslant s$, and $0 \leqslant \gamma \leqslant p^{s-k} - 1$. Then the code $C = \langle (x+1)^{\gamma + p^s - p^{s-k}} \rangle \subset \mathcal{F}(a,s)$ has Hamming weight distributions $A_j^{\gamma+p^s-p^{s-k}}(a,s)$, $0 \leqslant j \leqslant p^s$, and Hamming weight enumerator $W_C(x,y)$ as*

$$A_j^{\gamma+p^s-p^{s-k}}(a,s) = \begin{cases} A_t^{\gamma}(a,s-k), & \text{if } j = p^k t, \text{ for } 0 \leqslant t \leqslant p^{s-k}, \\ 0, & \text{otherwise,} \end{cases}$$

$$W_C(x,y) = \sum_{t=0}^{p^{s-k}} A_t^{\gamma}(a,s-k) x^{p^s - p^k t} y^{p^k t},$$

where $A_t^{\gamma}(a,s-k)$ is the number of codewords of length t of the code $\langle (x+1)^{\gamma} \rangle \subset \mathcal{F}(a,s-k)$.

Proof. Note that $p^s - p^{s-k} = (p-1)\sum_{i=1}^{k} p^{s-i}$. Hence, computing in $\mathcal{F}(a,s)$,

$$(x+1)^{p^s - p^{s-k}} = (x+1)^{(p-1)\sum_{i=1}^{k} p^{s-i}} = \prod_{i=1}^{k} \big(x^{p^{s-i}} + 1\big)^{p-1} = \prod_{i=1}^{k} \sum_{j=0}^{p-1} \binom{p-1}{j} x^{p^{s-i} j}.$$

Also, as computed in Proposition 4.5, we get

$$\begin{cases} \operatorname{wt}\big((x+1)^{p^s-p^{s-k}}\big) = \operatorname{wt}\big((x+1)^{(p-1)\sum_{i=1}^{k} p^{s-i}}\big) = \operatorname{wt}\left(\prod_{i=1}^{k} \sum_{j=0}^{p-1} \binom{p-1}{j} x^{p^{s-i} j}\right) = p^k, \\ \operatorname{cw}\big((x+1)^{p^s-p^{s-k}}\big) = \operatorname{cw}\big((x+1)^{(p-1)\sum_{i=1}^{k} p^{s-i}}\big) = \operatorname{cw}\left(\prod_{i=1}^{k} \sum_{j=0}^{p-1} \binom{p-1}{j} x^{p^{s-i} j}\right) = p^{s-k}, \\ \deg\big((x+1)^{p^s-p^{s-k}}\big) = p^s - p^{s-k}. \end{cases}$$

Consider an arbitrary nonzero codeword $c(x)$ of C, then there is a nonzero element $f(x) \in \mathcal{F}(a,s)$ such that $c(x) = (x+1)^{\gamma+p^s-p^{s-k}} f(x) = (x+1)^{p^s-p^{s-k}} (x+1)^{\gamma} f(x)$. As $\deg((x+1)^{p^s-p^{s-k}}) = p^s - p^{s-k}$, by the Division Algorithm, it can be assumed without loss of generality that $\deg((x+1)^{\gamma} f(x)) < p^{s-k}$. Because $\operatorname{cw}((x+1)^{p^s-p^{s-k}}) = p^{s-k}$, it follows that

$$\operatorname{wt}\big(c(x)\big) = \operatorname{wt}\big((x+1)^{p^s-p^{s-k}}\big) \cdot \operatorname{wt}\big((x+1)^{\gamma} f(x)\big) = p^k \cdot \operatorname{wt}\big((x+1)^{\gamma} f(x)\big).$$

As $f(x) \in \mathcal{F}(a,s)$ with $\deg((x+1)^\gamma f(x)) < p^{s-k}$, $(x+1)^\gamma f(x)$ can be viewed as an element of the code $C_\gamma = \langle (x+1)^\gamma \rangle \subset \mathcal{F}(a, s-k)$, whose Hamming weight distributions are $A_t^\gamma(a, s-k)$, $0 \leqslant t \leqslant p^{s-k}$.

Thus, the Hamming weight distributions of C are

$$A_j^{\gamma+p^s-p^{s-k}}(a,s) = \begin{cases} A_t^\gamma(a, s-k), & \text{if } j = p^k t, \text{ for } 0 \leqslant t \leqslant p^{s-k}, \\ 0, & \text{otherwise,} \end{cases}$$

and the Hamming weight enumerator of C is

$$W_C(x,y) = \sum_{t=0}^{p^{s-k}} A_t^\gamma(a, s-k) x^{p^s - p^k t} y^{p^k t}. \qquad \square$$

5.5. Corollary. *For each code C, let A_j be the number of codewords of Hamming weight j in C, $0 \leqslant j \leqslant p^s$, and $W_C(x,y)$ be the Hamming weight enumerator of C. Let $1 \leqslant k \leqslant s$, and $P_m(x;n)$ be the Krawtchouk polynomials in x of degree m, as defined in Proposition* 2.3:

$$P_m(x;n) = \sum_{i=0}^{m} (-1)^i \left(p^a - 1\right)^{m-i} \binom{x}{i} \binom{n-x}{m-i}.$$

Then

(i) *The code $C = \langle (x+1)^{p^s - p^{s-k}} \rangle \subset \mathcal{F}(a,s)$:*

$$A_j = \begin{cases} \binom{p^{s-k}}{t} (p^a - 1)^t, & \text{if } j = p^k t, \text{for } 0 \leqslant t \leqslant p^{s-k}, \\ 0, & \text{otherwise,} \end{cases}$$

$$W_C(x,y) = \sum_{t=0}^{p^{s-k}} \binom{p^{s-k}}{t} \left(p^a - 1\right)^t x^{p^s - p^k t} y^{p^k t}.$$

(ii) *The code $C = \langle (x+1)^{1+p^s - p^{s-k}} \rangle \subset \mathcal{F}(a,s)$:*

$$A_j = \begin{cases} \frac{p^a - 1}{p^a} \binom{p^{s-k}}{t} [(p^a - 1)^{t-1} + (-1)^t], & \text{if } j = p^k t, \text{for } 0 \leqslant t \leqslant p^{s-k}, \\ 0, & \text{otherwise,} \end{cases}$$

$$W_C(x,y) = \frac{p^a - 1}{p^a} \sum_{t=0}^{p^{s-k}} \binom{p^{s-k}}{t} \left[\left(p^a - 1\right)^{t-1} + (-1)^t\right] x^{p^s - p^k t} y^{p^k t}.$$

(iii) *The code $C = \langle (x+1)^{p^{s-k}} \rangle \subset \mathcal{F}(a,s)$:*

$$A_j = \frac{1}{p^{a p^{s-k}}} \sum_{t=0}^{p^{s-k}} \binom{p^{s-k}}{t} \left(p^a - 1\right)^t P_j\left(p^k t; p^s\right),$$

$$W_C(x,y)=\frac{1}{p^{ap^{s-k}}}\sum_{t=0}^{p^{s-k}}\binom{p^{s-k}}{t}\big(p^a-1\big)^t\big[x+\big(p^a-1\big)y\big]^{p^s-p^kt}(x-y)^{p^kt}.$$

(iv) *The code* $C=\langle(x+1)^{p^{s-k}-1}\rangle\subset\mathcal{F}(a,s)$:

$$A_j=\frac{p^a-1}{p^{ap^{s-k}}}\sum_{t=0}^{p^{s-k}}\binom{p^{s-k}}{t}\big[\big(p^a-1\big)^{t-1}+(-1)^t\big]P_j\big(p^kt;p^s\big),$$

$$W_C(x,y)=\frac{p^a-1}{p^{ap^{s-k}}}\sum_{t=0}^{p^{s-k}}\binom{p^{s-k}}{t}\big[\big(p^a-1\big)^{t-1}+(-1)^t\big]\big[x+\big(p^a-1\big)y\big]^{p^s-p^kt}(x-y)^{p^kt}.$$

Proof. Using Theorem 5.4 for $\gamma=0$ and $\gamma=1$, we get (i) and (ii). Clearly, $\langle(x+1)^{p^s-p^{s-k}}\rangle$ is the dual of $\langle(x+1)^{p^{s-k}}\rangle$, and $\langle(x+1)^{1+p^s-p^{s-k}}\rangle$ is the dual $\langle(x+1)^{p^{s-k}-1}\rangle$, hence, applying Theorem 2.2 and Proposition 2.3 to (i) and (ii) gives (iii) and (iv). □

6. Cyclic codes

If $p=2$, then the classes of negacyclic and cyclic codes over $\mathbb{F}_{2^a}$ coincide. When p is odd, let n be an odd integer, and consider the map

$$\xi:\frac{\mathbb{F}_{p^a}[x]}{\langle x^n+1\rangle}\to\frac{\mathbb{F}_{p^a}[x]}{\langle x^n-1\rangle}$$

given by $\xi(f(x))=f(-x)$. For polynomial $f(x),g(x)\in\mathbb{F}_{p^a}[x]$, $f(x)\equiv g(x)\pmod{x^n+1}$ if and only if there exists a polynomial $h(x)\in\mathbb{F}_{p^a}[x]$ such that $f(x)-g(x)=h(x)(x^n+1)$, if and only if

$$f(-x)-g(-x)=h(-x)\big[(-x)^n+1\big]=-h(-x)\big(x^n-1\big)$$

if and only if $f(-x)\equiv g(-x)\pmod{x^n-1}$. That means, for $f,g\in\frac{\mathbb{F}_{p^a}[x]}{\langle x^n+1\rangle}$, $\xi(f(x))=\xi(g(x))$ if and only if $f(x)=g(x)$, whence, ξ is well defined and one-to-one. Clearly, ξ is onto and it is easy to verify that ξ is a ring homomorphism. Hence, ξ is a ring isomorphism. Thus, we get the following result.

6.1. Proposition. *Let p be an odd prime, then the map $\xi:\frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}+1\rangle}\to\frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1\rangle}$, given by $f(x)\mapsto f(-x)$, is a ring isomorphism. In particular, for $A\subseteq\frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}+1\rangle}$, $B\subseteq\frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1\rangle}$ such that $\xi(A)=B$, then A is an ideal of $\frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}+1\rangle}$ if and only if B is an ideal of $\frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1\rangle}$. Equivalently, A is a negacyclic code of length p^s over $\mathbb{F}_{p^a}$ if and only if B is a cyclic code of length p^s over $\mathbb{F}_{p^a}$.*

Therefore, our results about negacyclic codes of length p^s over $\mathbb{F}_{p^a}$ in Sections 3–5 can be carried correspondingly to cyclic codes of length p^s over $\mathbb{F}_{p^a}$.

6.2. Theorem. *(Cf. Theorems 3.3, 3.4.) p^a-ary cyclic codes of length p^s are precisely the ideals $\langle (x-1)^i \rangle$, $i = 0, 1, \ldots, p^s$, of the ring $\frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1\rangle}$. A cyclic code $C = \langle (x-1)^i \rangle$ has $p^{a(p^s-i)}$ codewords. The dual of C is $C^\perp = \langle (x-1)^{p^s-i} \rangle$, which contains p^{ai} codewords.*

6.3. Corollary. *(Cf. Corollary 3.5.) A p^a-ary cyclic code of length p^s, $\langle (x-1)^i \rangle \subseteq \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1\rangle}$, is self-orthogonal if and only if $\frac{p^s}{2} \leqslant i \leqslant p^s$. Self-dual p^a-ary cyclic code of length p^s exists if and only if $p = 2$. When $p = 2$, there is only one self-dual 2^a-ary cyclic code of length 2^s, namely, $\langle (x-1)^{2^{s-1}} \rangle \subset \frac{\mathbb{F}_{2^a}[x]}{\langle x^{2^s}-1\rangle}$.*

6.4. Theorem. *(Cf. Theorem 4.11.) Let C be a p^a-ary cyclic codes of length p^s, then $C = \langle (x-1)^i \rangle \subseteq \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1\rangle}$, for $i \in \{0, 1, \ldots, p^s\}$. The Hamming distance d_i of C is determined by*

$$d_i = \begin{cases} 1, & \text{if } i = 0, \\ \beta + 2, & \text{if } \beta p^{s-1} + 1 \leqslant i \leqslant (\beta+1)p^{s-1} \text{ where } 0 \leqslant \beta \leqslant p-2, \\ (t+1)p^k, & \text{if } p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \leqslant i \leqslant p^s - p^{s-k} + tp^{s-k-1} \\ & \text{where } 1 \leqslant t \leqslant p-1, \text{ and } 1 \leqslant k \leqslant s-1, \\ 0, & \text{if } i = p^s. \end{cases}$$

6.5. Proposition. *For each code C, let A_j be the number of codewords of Hamming weight j in C, and $W_C(x, y)$ be the Hamming weight enumerator of C. Let $1 \leqslant k \leqslant s$, and $P_m(x; n)$ be the Krawtchouk polynomials in x of degree m, as defined in Proposition* 2.3:

$$P_m(x; n) = \sum_{i=0}^{m} (-1)^i \left(p^a - 1\right)^{m-i} \binom{x}{i} \binom{n-x}{m-i}.$$

Then

(i) *The cyclic code $C = \langle (x-1)^{p^s-1} \rangle \subset \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1\rangle}$ (cf. Proposition* 5.1):

$$A_j = \begin{cases} 1, & \text{if } j = 0, \\ p^a - 1, & \text{if } j = p^s, \\ 0, & \text{if } 1 \leqslant j \leqslant p^s - 1. \end{cases}$$

$$W_C(x, y) = x^{p^s} + \left(p^a - 1\right) y^{p^s}.$$

(ii) *The cyclic code $C = \langle x - 1 \rangle \subset \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1\rangle}$ (cf. Proposition* 5.2):

$$A_j = \frac{p^a - 1}{p^a} \binom{p^s}{i} \left[\left(p^a - 1\right)^{i-1} + (-1)^i \right],$$

$$W_C(x, y) = \frac{p^a - 1}{p^a} \sum_{j=0}^{p^s} \binom{p^s}{i} \left[\left(p^a - 1\right)^{i-1} + (-1)^i \right] x^{p^s - i} y^i.$$

(iii) *The code* $C = \langle (x-1)^{p^s - p^{s-k}} \rangle \subset \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1 \rangle}$ (*cf. Corollary* 5.5(i)):

$$A_j = \begin{cases} \binom{p^{s-k}}{t}(p^a-1)^t, & \text{if } j = p^k t, \text{ for } 0 \leqslant t \leqslant p^{s-k}, \\ 0, & \text{otherwise,} \end{cases}$$

$$W_C(x,y) = \sum_{t=0}^{p^{s-k}} \binom{p^{s-k}}{t} \big(p^a-1\big)^t x^{p^s - p^k t} y^{p^k t}.$$

(iv) *The cyclic code* $C = \langle (x-1)^{1+p^s - p^{s-k}} \rangle \subset \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1 \rangle}$ (*cf. Corollary* 5.5(ii)):

$$A_j = \begin{cases} \frac{p^a-1}{p^a}\binom{p^{s-k}}{t}[(p^a-1)^{t-1} + (-1)^t], & \text{if } j = p^k t, \text{ for } 0 \leqslant t \leqslant p^{s-k}, \\ 0, & \text{otherwise,} \end{cases}$$

$$W_C(x,y) = \frac{p^a-1}{p^a} \sum_{t=0}^{p^{s-k}} \binom{p^{s-k}}{t} \big[\big(p^a-1\big)^{t-1} + (-1)^t\big] x^{p^s - p^k t} y^{p^k t}.$$

(v) *The cyclic code* $C = \langle (x-1)^{p^{s-k}} \rangle \subset \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1 \rangle}$ (*cf. Corollary* 5.5(iii)):

$$A_j = \frac{1}{p^{ap^{s-k}}} \sum_{t=0}^{p^{s-k}} \binom{p^{s-k}}{t} \big(p^a-1\big)^t P_j\big(p^k t; p^s\big),$$

$$W_C(x,y) = \frac{1}{p^{ap^{s-k}}} \sum_{t=0}^{p^{s-k}} \binom{p^{s-k}}{t} \big(p^a-1\big)^t \big[x + \big(p^a-1\big)y\big]^{p^s - p^k t} (x-y)^{p^k t}.$$

(vi) *The cyclic code* $C = \langle (x-1)^{p^{s-k}-1} \rangle \subset \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1 \rangle}$ (*cf. Corollary* 5.5(iv)):

$$A_j = \frac{p^a-1}{p^{ap^{s-k}}} \sum_{t=0}^{p^{s-k}} \binom{p^{s-k}}{t} \big[\big(p^a-1\big)^{t-1} + (-1)^t\big] P_j\big(p^k t; p^s\big),$$

$$W_C(x,y) = \frac{p^a-1}{p^{ap^{s-k}}} \sum_{t=0}^{p^{s-k}} \binom{p^{s-k}}{t} \big[\big(p^a-1\big)^{t-1} + (-1)^t\big] \big[x + \big(p^a-1\big)y\big]^{p^s - p^k t} (x-y)^{p^k t}.$$

6.6. Theorem *(cf. Theorem 5.4). Let* k, γ *be integers such that* $1 \leqslant k \leqslant s$, *and* $0 \leqslant \gamma \leqslant p^{s-k} - 1$. *Then the cyclic code* $C = \langle (x-1)^{\gamma + p^s - p^{s-k}} \rangle \subset \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^s}-1 \rangle}$ *has Hamming weight distributions* $A_j^{\gamma + p^s - p^{s-k}}(a,s)$, $0 \leqslant j \leqslant p^s$, *and Hamming weight enumerator* $W_C(x,y)$ *as*

$$A_j^{\gamma + p^s - p^{s-k}}(a,s) = \begin{cases} A_t^{\gamma}(a, s-k), & \text{if } j = p^k t, \text{ for } 0 \leqslant t \leqslant p^{s-k}, \\ 0, & \text{otherwise,} \end{cases}$$

$$W_C(x, y) = \sum_{t=0}^{p^{s-k}} A_t^{\gamma}(a, s-k) x^{p^s - p^k t} y^{p^k t},$$

where $A_t^{\gamma}(a, s-k)$ *is the number of codewords of length* t *of the cyclic code* $\langle (x-1)^{\gamma} \rangle \subset \frac{\mathbb{F}_{p^a}[x]}{\langle x^{p^{s-k}} - 1 \rangle}$.

Acknowledgments

The author is grateful to the referees for a very meticulous reading of this manuscript. Their suggestions were valuable to create an improved final version.

References

[1] E.R. Berlekamp, Negacyclic Codes for the Lee Metric, in: Proceedings of the Conference on Combinatorial Mathematics and Its Applications, Univ. North Carolina Press, Chapel Hill, NC, 1968, pp. 298–316.
[2] E.R. Berlekamp, Algebraic Coding Theory, revised ed., Aegean Park, 1984.
[3] G. Castagnoli, J.L. Massey, P.A. Schoeller, N. von Seemann, On repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (1991) 337–342.
[4] P. Delsarte, Bounds for unrestricted codes, by linear programing, Philips Res. Rep. 27 (1972) 272–289.
[5] P. Delsarte, Four fundamental characters of a code and their combinatorial significance, Inform. Control 23 (1973) 407–438.
[6] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. 10 (1973).
[7] H.Q. Dinh, Negacyclic codes of length 2^s over Galois rings, IEEE Trans. Inform. Theory 51 (2005) 4252–4262.
[8] H.Q. Dinh, Complete distances of all negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$, IEEE Trans. Inform. Theory 53 (2007) 147–161.
[9] H.Q. Dinh, S.R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50 (2004) 1728–1744.
[10] W.C. Huffman, V. Pless, Fundamentals of Error-correcting Codes, Cambridge Univ. Press, Cambridge, 2003.
[11] M. Krawtchouk, Sur une généralisation des polynomes d'Hermite, C. R. Acad. Sci. Paris 189 (1929) 620–622.
[12] M. Krawtchouk, Sur la distribution des racines des polynomes orthogonaux, C. R. Acad. Sci. Paris 196 (1933) 739–741.
[13] F.J. MacWilliams, Error-correcting codes for multiple-level transmissions, Bell System Tech. J. 40 (1961) 281–308.
[14] F.J. MacWilliams, Combinatorial problems of elementary abelian groups, PhD Diss., Harvard University, Cambridge, MA, 1962.
[15] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, 10th ed., North-Holland, Amsterdam, 1998.
[16] B.R. McDonald, Finite Rings with Identity, Pure and Appl. Math., vol. 28, Dekker, New York, 1974.
[17] C.-S. Nedeloaia, Weight distributions of cyclic self-dual codes, IEEE Trans. Inform. Theory 49 (2003) 1582–1591.
[18] V. Pless, W.C. Huffman, Handbook of Coding Theory, Elsevier, Amsterdam, 1998.
[19] E. Prange, Cyclic error-correcting codes in two symbols, technical notes, TN-57-103, Air Force Cambridge Research Labs, Bedford, MA, September 1957.
[20] E. Prange, Some cyclic error-correcting codes with simple decoding algorithms, TN-58-156, Air Force Cambridge Research Labs, Bedford, MA, April 1958.
[21] E. Prange, The use of coset equivalence in the analysis and decoding of group codes, TN-59-16, Air Force Cambridge Research Labs, Bedford, MA, 1959.
[22] E. Prange, An algorithm for factoring $x^n - 1$ over a finite field, TN-59-175, Air Force Cambridge Research Labs, Bedford, MA, October 1959.
[23] G. Szegő, Orthogonal Polynomials, revised ed, Colloq. Publ., vol. 23, Amer. Math. Soc., New York, 1959, pp. 35–37.
[24] L.-Z. Tang, C.B. Soh, E. Gunawan, A note on the q-ary image of a q^m-ary repeated-root cyclic code, IEEE Trans. Inform. Theory 43 (1997) 732–737.
[25] J.H. van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (1991) 343–345.