REVISTA DE LA UNIÓN MATEMÁTICA ARGENTINA
Vol. 62, No. 1, 2021, Pages 219–242
Published online: June 24, 2021
https://doi.org/10.33044/revuma.1840

WEIGHT DISTRIBUTION OF CYCLIC CODES DEFINED BY QUADRATIC FORMS AND RELATED CURVES

RICARDO A. PODESTÁ AND DENIS E. VIDELA

Abstract. We consider cyclic codes $\mathcal{C}_{\mathcal{L}}$ associated to quadratic trace forms in m variables $Q_R(x) = \mathrm{Tr}_{q^m/q}(xR(x))$ determined by a family $\mathcal{L}$ of q-linearized polynomials R over $\mathbb{F}_{q^m}$, and three related codes $\mathcal{C}_{\mathcal{L},0}$, $\mathcal{C}_{\mathcal{L},1}$, and $\mathcal{C}_{\mathcal{L},2}$. We describe the spectra for all these codes when $\mathcal{L}$ is an even rank family, in terms of the distribution of ranks of the forms Q_R in the family $\mathcal{L}$, and we also compute the complete weight enumerator for $\mathcal{C}_{\mathcal{L}}$. In particular, considering the family $\mathcal{L} = \langle x^{q^\ell} \rangle$, with ℓ fixed in $\mathbb{N}$, we give the weight distribution of four parametrized families of cyclic codes $\mathcal{C}_\ell$, $\mathcal{C}_{\ell,0}$, $\mathcal{C}_{\ell,1}$, and $\mathcal{C}_{\ell,2}$ over $\mathbb{F}_q$ with zeros $\{\alpha^{-(q^\ell+1)}\}$, $\{1, \alpha^{-(q^\ell+1)}\}$, $\{\alpha^{-1}, \alpha^{-(q^\ell+1)}\}$, and $\{1, \alpha^{-1}, \alpha^{-(q^\ell+1)}\}$ respectively, where $q = p^s$ with p prime, α is a generator of $\mathbb{F}_{q^m}^*$, and $m/(m,\ell)$ is even. Finally, we give simple necessary and sufficient conditions for Artin–Schreier curves $y^p - y = xR(x) + \beta x$, p prime, associated to polynomials $R \in \mathcal{L}$ to be optimal. We then obtain several maximal and minimal such curves in the case $\mathcal{L} = \langle x^{p^\ell} \rangle$ and $\mathcal{L} = \langle x^{p^\ell}, x^{p^{3\ell}} \rangle$.

1. Introduction

Let $q = p^s$, with p prime. A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$ of dimension k. If $\mathcal{C}$ has minimal distance $d = \min\{d(c,c') : c, c' \in \mathcal{C},\ c \neq c'\}$, where $d(\cdot,\cdot)$ is the Hamming distance in $\mathbb{F}_q^n$, then $\mathcal{C}$ is called an $[n,k,d]$-code. One of the most important families of codes are the cyclic ones. A code is *cyclic* if given a codeword $c = (c_1, \ldots, c_n) \in \mathcal{C}$ the cyclic shift $s(c) = (c_n, c_1, \ldots, c_{n-1})$ is also in $\mathcal{C}$. The weight of $c \in \mathcal{C}$ is $w(c) = \#\{0 \leq i \leq n : c_i \neq 0\}$; that is, the number of non-zero coordinates of c. For $0 \leq i \leq n$ the numbers $A_i = \#\{c \in \mathcal{C} : w(c) = i\}$ are called the frequencies and the sequence $\mathrm{Spec}(\mathcal{C}) = (A_0, A_1, \ldots, A_n)$ is called *the weight distribution* or *the spectrum* of $\mathcal{C}$. A very good reference for general coding theory is the book [7].

Fix α a generator of $\mathbb{F}_{q^m}^*$. Consider $h(x) = h_1(x) \cdots h_t(x) \in \mathbb{F}_q[x]$, where the $h_j(x)$'s are different irreducible polynomials over $\mathbb{F}_q$. For each $j = 1, \ldots, t$, let $g_j = \alpha^{-s_j}$ be a root of $h_j(x)$, n_j be the order of g_j, and m_j be the minimum positive integer such that $q^{m_j} \equiv 1 \pmod{n_j}$. Then, $\deg(h_j(x)) = m_j$ for all j.

2020 *Mathematics Subject Classification.* Primary 94B15; Secondary 11T24, 11E04, 11G20.
Key words and phrases. Cyclic codes, quadratic forms, weight distribution, optimal curves.
Partially supported by CONICET, FONCYT, and SECyT-UNC.

Put $n = \frac{q^m-1}{\delta}$, where $\delta = \gcd(q^m - 1, s_1, \dots, s_t)$. Then, by Delsarte's theorem of trace and duals ([2]), the q-ary code $\mathcal{C} = \{c(a_1, \dots, a_t) : a_j \in \mathbb{F}_{q^{m_j}}\}$ with

$$c(a_1, \dots, a_t) = \Big(\sum_{j=1}^{t} \mathrm{Tr}_{q^{m_j}/q}(a_j), \sum_{j=1}^{t} \mathrm{Tr}_{q^{m_j}/q}(a_j g_j), \dots, \sum_{j=1}^{t} \mathrm{Tr}_{q^{m_j}/q}(a_j g_j^{n-1}) \Big), \quad (1.1)$$

where $\mathrm{Tr}_{q^{m_j}/q}$ is the trace function from $\mathbb{F}_{q^{m_j}}$ to $\mathbb{F}_q$, is an $[n, k]$-cyclic code with check polynomial $h(x)$ and dimension $k = m_1 + \cdots + m_t$.

The computation of the spectra of cyclic codes is in general a difficult task. The recent survey [3] by Dinh, Li, and Yue shows the progress made on this problem in the last 20 years using different techniques: exponential sums, special nonlinear functions over finite fields, quadratic forms, Hermitian forms graphs, Cayley graphs, Gauss and Kloosterman sums. In [5], Feng and Luo computed the weight distribution of the cyclic code of length $n = p^m - 1$ with zeros $\{\alpha^{-1}, \alpha^{-(p^\ell+1)}\}$, where α is a generator of $\mathbb{F}_{p^m}^*$, $\ell \geq 0$ and $m/(m, \ell)$ odd, by using a perfect nonlinear function. In another work ([4]), they used quadratic forms to calculate the weight distribution of the cyclic codes with zeros $\{\alpha^{-2}, \alpha^{-(p^\ell+1)}\}$ and $\{\alpha^{-1}, \alpha^{-2}, \alpha^{-(p^\ell+1)}\}$, respectively, when p is an odd prime and $(m, \ell) = 1$. These methods were used by other authors to calculate the spectra of other cyclic codes over $\mathbb{F}_p$ when p is an odd prime. All these results are summarized in Theorem 2.4 in [3].

In this paper, we will explicitly compute the weight distributions of some general families of cyclic codes over $\mathbb{F}_q$. In particular, we will compute the spectra of cyclic codes with zeros $\{\alpha^{-(q^\ell+1)}\}$, $\{1, \alpha^{-(q^\ell+1)}\}$, $\{\alpha^{-1}, \alpha^{-(q^\ell+1)}\}$, and $\{1, \alpha^{-1}, \alpha^{-(q^\ell+1)}\}$ in all characteristics, where α is a generator of $\mathbb{F}_{q^m}^*$ and $m/(m, \ell)$ is even (i.e. new cases not covered in [5] and more general ones), by using quadratic forms and related exponential sums.

We now give a brief summary of the results in the paper. In Section 2 we recall quadratic forms Q in m variables over finite fields and their absolute invariants: the rank and the type. We define certain exponential sums $S_{Q,b}(\beta)$ and compute their values and distributions (Lemma 2.2). We then consider the particular quadratic form $Q_{\gamma,\ell}(x) = \mathrm{Tr}_{q^m/q}(\gamma x^{q^\ell+1})$, with $\gamma \in \mathbb{F}_q$, $\ell \in \mathbb{N}$. We recall the distribution of ranks and types given by Klapper in [8] and [9]. These facts will be later used (Sections 3–5) to compute the spectra of some families of cyclic codes.

In the next section, we consider cyclic codes defined by general quadratic forms determined by q-linearized polynomials and compute their spectra in some cases. More precisely, we consider $\mathcal{L} = \langle x^{q^{\ell_1}}, x^{q^{\ell_2}}, \dots, x^{q^{\ell_s}} \rangle \subset \mathbb{F}_{q^m}[x]$, the associated code

$$\mathcal{C}_{\mathcal{L}} = \{(\mathrm{Tr}_{q^m/q}(xR(x)))_{x \in \mathbb{F}_{q^m}^*} : R \in \mathcal{L}\}$$

and three related codes $\mathcal{C}_{\mathcal{L},0}$, $\mathcal{C}_{\mathcal{L},1}$, and $\mathcal{C}_{\mathcal{L},2}$ (see (3.2)). If $\mathcal{L}$ is an even rank family (see Definition 3.1) we give the weight distributions of $\mathcal{C}_{\mathcal{L}}$, $\mathcal{C}_{\mathcal{L},0}$, $\mathcal{C}_{\mathcal{L},1}$, and $\mathcal{C}_{\mathcal{L},2}$ (see Theorems 3.3 and 3.4 and Tables 1–4). In Proposition 3.7 we also give the complete weight enumerator of $\mathcal{C}_{\mathcal{L}}$.

In the next sections we consider two particular even rank families: $\mathcal{L} = \langle x^{q^\ell} \rangle$ and $\mathcal{L} = \langle x^{q^\ell}, x^{q^{3\ell}} \rangle$, with $\ell \in \mathbb{N}$. In Section 4, we compute the spectrum of the

code $\mathcal{C}_\ell$ defined by the family of quadratic forms $Q_{\gamma,\ell} = \mathrm{Tr}_{q^m/q}(\gamma x^{q^\ell+1})$, $\gamma \in \mathbb{F}_{q^m}$, and the spectra of the related codes $\mathcal{C}_{\ell,0}$, $\mathcal{C}_{\ell,1}$, and $\mathcal{C}_{\ell,2}$ (see Theorems 4.1 and 4.4 and Tables 5–8). As a consequence, $\mathcal{C}_\ell$ turns out to be a 2-weight code. The complete weight enumerator of $\mathcal{C}_\ell$ is given in Corollary 4.2. In Section 5 we obtain similar results for the codes $\mathcal{C}_{\ell,3\ell}$, $\mathcal{C}_{\ell,3\ell,0}$, $\mathcal{C}_{\ell,3\ell,1}$, and $\mathcal{C}_{\ell,3\ell,2}$ (see Theorem 5.2 and Tables 9–10).

In the last section, we consider Artin–Schreier curves of the form

$$C_{R,\beta} : y^p - y = xR(x) + \beta x$$

where p is prime, $\beta \in \mathbb{F}_{p^m}$, and R is a p-linearized polynomial over $\mathbb{F}_{p^m}$. In Proposition 6.1 we give simple necessary and sufficient conditions for these curves to be optimal, that is, curves attaining the equality in the Hasse–Weil bound, in terms of the degree of R and the rank r of the associated quadratic form $Q_R(x) = \mathrm{Tr}_{p^m/p}(xR(x))$. We then show in Theorem 6.3 that there are several maximal and minimal curves in the family

$$y^p - y = \gamma x^{p^\ell+1} + \beta x, \qquad \gamma \in \mathbb{F}_{p^m}^*,\ \beta \in \mathbb{F}_{p^m}.$$

In the binary case $p = 2$, Van der Geer and Van der Vlugt have found the same curves for $\ell = 1$ and $\beta = 0$ (see [12]). Thus, we extend their result for any p, ℓ, and β. We also show the existence of optimal curves of the form

$$x^p - y = \gamma_1 x^{p^\ell+1} + \gamma_3 x^{p^{3\ell}+1} + \beta x$$

with $\gamma_1, \gamma_3 \in \mathbb{F}_{p^m}^*$, $\beta \in \mathbb{F}_{p^m}$.

2. Quadratic forms over finite fields and exponential sums

A quadratic form in $\mathbb{F}_{q^m}$ is an homogeneous polynomial $q(x)$ in $\mathbb{F}_{q^m}[x]$ of degree 2. We want to consider more general functions. Any function

$$Q : \mathbb{F}_{q^m} \to \mathbb{F}_q$$

can be identified with a polynomial of m variables over $\mathbb{F}_q$ via an isomorphism $\mathbb{F}_{q^m} \simeq \mathbb{F}_q^m$ of $\mathbb{F}_q$-vector spaces. Such Q is said to be a *quadratic form* if the corresponding polynomial is homogeneous of degree 2. The *rank* of Q is the minimum number r of variables needed to represent Q as a polynomial in several variables. Alternatively, the rank of Q can be computed as the codimension of the $\mathbb{F}_q$-vector space $V = \{y \in \mathbb{F}_{q^m} : Q(y) = 0,\ Q(x+y) = Q(x),\ \forall x \in \mathbb{F}_{q^m}\}$. That is, $|V| = q^{m-r}$. Two quadratic forms Q_1, Q_2 are *equivalent* if there is an invertible $\mathbb{F}_q$-linear function $S : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ such that $Q_1(x) = Q_2(S(x))$.

Fix Q a quadratic form from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. It will be convenient to consider, for each $\beta \in \mathbb{F}_{q^m}$ and $\xi \in \mathbb{F}_q$, the number

$$N_{Q,\beta}(\xi) = \#\{x \in \mathbb{F}_{q^m} : Q(x) + \mathrm{Tr}_{q^m/q}(\beta x) = \xi\}.$$

We will abbreviate $N_Q(\xi) = N_{Q,0}(\xi)$, $N_{Q,\beta} = N_{Q,\beta}(0)$, and $N_Q = N_Q(0) = \#\ker Q$. It is a classic result that quadratic forms over finite fields are classified in three different equivalent classes. This classification depends on the parity of the characteristic (see for instance [10]). But in both characteristics (even or odd), there

are 2 classes with even rank (usually called type 1 and 3) and one of odd rank. For even rank, we will use the notation

$$\varepsilon_Q = \begin{cases} +1 & \text{if } Q \text{ is of type 1,} \\ -1 & \text{if } Q \text{ is of type 3,} \end{cases}$$

and call this sign the *type* of Q. The number $N_Q(\xi)$ does not depend on the characteristic and it is given by

$$N_Q(\xi) = q^{m-1} + \varepsilon_Q\, \nu(\xi)\, q^{m-\frac{r}{2}-1},$$

where $\nu(0) = q-1$ and $\nu(z) = 1$ if $z \in \mathbb{F}_q^*$ (see [10]). From the works [8, 9] of Klapper we also know the distribution of these numbers $N_{Q,\beta}(\xi)$, which are given as follows.

Lemma 2.1. *Let Q be a quadratic form of m variables over $\mathbb{F}_q$ of even rank r. Then, for all $\xi \in \mathbb{F}_q$, there are $q^m - q^r$ elements $\beta \in \mathbb{F}_{q^m}$ such that $N_{Q,\beta}(\xi) = q^{m-1}$ and $q^{r-1} + \varepsilon_Q\, \nu(c)\, q^{\frac{r}{2}-1}$ elements $\beta \in \mathbb{F}_{q^m}$ such that $N_{Q,\beta}(\xi) = q^{m-1} + \varepsilon_Q\, \nu(\xi + c)\, q^{m-\frac{r}{2}-1}$, where c runs on $\mathbb{F}_q$.*

Given a quadratic form Q, we can consider the exponential sums

$$S_{Q,b}(\beta) = \sum_{a\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}\left(a(Q(x)+\mathrm{Tr}_{q^m/q}(\beta x)+b)\right)}, \tag{2.1}$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$, and put $S_Q(\beta) = S_{Q,0}(\beta)$. We now give the values of $S_{Q,b}(\beta)$ as well as their distributions.

Lemma 2.2. *Let $Q(x)$ be a quadratic form over $\mathbb{F}_q$ of even rank r. Then,*

$$S_Q(\beta) = \begin{cases} 0 & q^m - q^r \ \textit{times}, \\ \varepsilon(q-1)q^{m-\frac{r}{2}} & q^{r-1} + \varepsilon(q-1)q^{\frac{r}{2}-1} \ \textit{times}, \\ -\varepsilon q^{m-\frac{r}{2}} & (q^{r-1} - \varepsilon q^{\frac{r}{2}-1})(q-1) \ \textit{times}; \end{cases}$$

$$S_{Q,b}(\beta) = \begin{cases} 0 & q^m - q^r \ \textit{times}, \\ \varepsilon(q-1)q^{m-\frac{r}{2}} & q^{r-1} - \varepsilon q^{\frac{r}{2}-1} \ \textit{times}, \\ -\varepsilon q^{m-\frac{r}{2}} & q^r - q^{r-1} + \varepsilon q^{\frac{r}{2}-1} \ \textit{times}. \end{cases}$$

Proof. Notice that

$$\begin{aligned} S_Q(\beta) &= \sum_{a\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(a(Q(x)+\mathrm{Tr}_{q^m/q}(\beta x)))} \\ &= \sum_{x\in\mathbb{F}_{q^m}} \sum_{a\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{q/p}(a(Q(x)+\mathrm{Tr}_{q^m/q}(\beta x)))} - q^m. \end{aligned}$$

Hence, $S_Q(\beta) = qN_{Q,\beta}(0) - q^m$. Similarly, we get $S_{Q,b}(\beta) = qN_{Q,\beta}(-b) - q^m$. The result now follows from Lemma 2.1. □

The quadratic form $\mathrm{Tr}_{q^m/q}(\gamma x^{q^\ell+1})$. A whole family of quadratic forms over $\mathbb{F}_q$ in m variables are given by

$$Q_R(x) = \mathrm{Tr}_{q^m/q}(xR(x)),$$

where $R(x)$ is a q-linearized polynomial over $\mathbb{F}_q$. We are interested in the simplest case, when $R(x)$ is the monomial $R_{\gamma,\ell}(x) = \gamma x^{q^\ell}$ with $\ell \in \mathbb{N}$, $\gamma \in \mathbb{F}_{q^m}^*$, i.e.

$$Q_{\gamma,\ell}(x) = \mathrm{Tr}_{q^m/q}(\gamma x^{q^\ell+1}).$$

The next theorems, due to Klapper, give the distribution of ranks and types of the family of quadratic forms $\{Q_{\gamma,\ell}(x) = \mathrm{Tr}_{q^m/q}(\gamma x^{q^\ell+1}) : \gamma \in \mathbb{F}_{q^m},\ \ell \in \mathbb{N}\}$.

For integers m, ℓ we will use the notations

$$m_\ell = \tfrac{m}{(m,\ell)} \qquad \text{and} \qquad \varepsilon_\ell = (-1)^{\frac{1}{2}m_\ell}$$

and denote the set of $(q^\ell+1)$-th powers in $\mathbb{F}_{q^m}$ by

$$S_{q,m}(\ell) = \{x^{q^\ell+1} : x \in \mathbb{F}_{q^m}^*\}. \tag{2.2}$$

Theorem 2.3 (Even characteristic, [8])**.** *Let q be a power of 2 and $m, \ell \in \mathbb{N}$ such that m_ℓ is even. Then $Q_{\gamma,\ell}$ is of even rank and we have:*

(a) *If $\varepsilon_\ell = \pm 1$ and $\gamma \in S_{q,m}(\ell)$ then $Q_{\gamma,\ell}$ is of type ∓ 1 and has rank $m - 2(m,\ell)$.*
(b) *If $\varepsilon_\ell = \pm 1$ and $\gamma \notin S_{q,m}(\ell)$ then $Q_{\gamma,\ell}$ is of type ± 1 and has rank m.*

For q odd, consider the sets of integers

$$\begin{aligned} X_{q,m}(\ell) &= \{0 \le t \le N : t \equiv 0\,(L)\} \quad \text{and} \\ Y_{q,m}(\ell) &= \{0 \le t \le N : t \equiv \tfrac{L}{2}\,(L)\}, \end{aligned} \tag{2.3}$$

where $N = q^m - 1$ and $L = q^{(m,\ell)} + 1$.

Theorem 2.4 (Odd characteristic, [9])**.** *Let q be a power of an odd prime p and let m, ℓ be non-negative integers. Put $\gamma = \alpha^t$ with α a primitive element in $\mathbb{F}_{q^m}$. Then, we have:*

(a) *If $\varepsilon_\ell = 1$ and $t \in X_{q,m}(\ell)$ then $Q_{\gamma,\ell}$ is of type -1 and has rank $m - 2(m,\ell)$.*
(b) *If $\varepsilon_\ell = 1$ and $t \notin X_{q,m}(\ell)$ then $Q_{\gamma,\ell}$ is of type 1 and has rank m.*
(c) *If m_ℓ is even, $\varepsilon_\ell = -1$, and $t \in Y_{q,m}(\ell)$ then $Q_{\gamma,\ell}$ is of type 1 and has rank $m - 2(m,\ell)$.*
(d) *If m_ℓ is even, $\varepsilon_\ell = -1$, and $t \notin Y_{q,m}(\ell)$ then $Q_{\gamma,\ell}$ is of type -1 and has rank m.*

We will need the following result whose proof is elementary.

Lemma 2.5. *Let q be a prime power and m, ℓ integers. If m_ℓ is even then we have $(q^m - 1, q^\ell + 1) = q^{(m,\ell)} + 1$.*

Lemma 2.6. *Let $M = \#S_{q,m}(\ell)$, $M_1 = \#X_{q,m}(\ell)$, and $M_2 = \#Y_{q,m}(\ell)$; put $M' = q^m - 1 - M$, $M_1' = q^m - 1 - M_1$, and $M_2' = q^m - 1 - M_2$. If m_ℓ is even then*

$$M = M_1 = M_2 = \frac{q^m - 1}{q^{(m,\ell)} + 1} \quad \text{and} \quad M' = M_1' = M_2' = q^{(m,\ell)}\frac{q^m - 1}{q^{(m,\ell)} + 1}.$$

Proof. Let α be a primitive element of $\mathbb{F}_{q^m}$; then $S_{q,m}(\ell) = \langle \alpha^{q^\ell+1} \rangle$, and this implies that $M = \frac{q^m-1}{(q^m-1,q^\ell+1)} = \frac{q^m-1}{q^{(m,\ell)}+1}$, by Lemma 2.5. On the other hand, if k, N, s_1, and s_2 are non-negative integers with $k \mid N$ and $0 \leq s_1, s_2 \leq k-1$, then

$$\#\{i \in \{1,\dots,N\} : i \equiv s_1 \bmod k\} = \#\{i \in \{1,\dots,N\} : i \equiv s_2 \bmod k\} = \tfrac{N}{k}.$$

Therefore, if $q^{(m,\ell)}+1 \mid q^m-1$, we have that $M_1 = M_2 = \frac{q^m-1}{q^{(m,\ell)}+1}$. Clearly, we obtain $M' = M_1' = M_2' = q^{(m,\ell)}M$ as was to be shown. □

3. Weight distribution of cyclic codes defined by trace forms

Let $\mathcal{L} \subset \mathbb{F}_{q^m}[x]$ be a finite dimensional $\mathbb{F}_{q^m}$-subspace containing q-linearized polynomials only, i.e.

$$\mathcal{L} = \langle x^{q^{\ell_1}}, x^{q^{\ell_2}}, \dots, x^{q^{\ell_s}} \rangle \subset \mathbb{F}_{q^m}[x]$$

for some non-negative integers $\ell_1, \dots, \ell_s$ with $\ell_i \neq \ell_j$ for $i \neq j$. Define the q-ary code

$$\mathcal{C}_{\mathcal{L}} = \Big\{ c_R = \big(\operatorname{Tr}_{q^m/q}(xR(x)) \big)_{x \in \mathbb{F}_{q^m}^*} : R \in \mathcal{L} \Big\} \subset \mathbb{F}_q^n \tag{3.1}$$

with length $n = q^m - 1$ and the related codes

$$\begin{aligned}
\mathcal{C}_{\mathcal{L},0} &= \Big\{ c_{R,b} = \big(\operatorname{Tr}_{q^m/q}\big(xR(x)\big) + b \big)_{x \in \mathbb{F}_{q^m}^*} : R \in \mathcal{L},\ b \in \mathbb{F}_q \Big\}, \\
\mathcal{C}_{\mathcal{L},1} &= \Big\{ c_R(\beta) = \big(\operatorname{Tr}_{q^m/q}(xR(x) + \beta x) \big)_{x \in \mathbb{F}_{q^m}^*} : R \in \mathcal{L},\ \beta \in \mathbb{F}_{q^m} \Big\}, \\
\mathcal{C}_{\mathcal{L},2} &= \Big\{ c_{R,b}(\beta) = \big(\operatorname{Tr}_{q^m/q}(xR(x) + \beta x) + b \big)_{x \in \mathbb{F}_{q^m}^*} : R \in \mathcal{L},\ \beta \in \mathbb{F}_{q^m},\ b \in \mathbb{F}_q \Big\}.
\end{aligned} \tag{3.2}$$

Notice that $c_{R,b} = c_R + b$ and $c_{R,b}(\beta) = c_R(\beta) + b$; moreover, we have that $c_{R,0} = c_R(0) = c_R$, $c_{R,b}(0) = c_{R,b}$, and $c_{R,0}(\beta) = c_R(\beta)$. Then, we have

$$\mathcal{C}_{\mathcal{L}} \subset \mathcal{C}_{\mathcal{L},0}, \quad \mathcal{C}_{\mathcal{L},1} \subset \mathcal{C}_{\mathcal{L},2}.$$

All of these codes are cyclic since one can check that their codewords have the form (1.1). In our case, this can be seen directly. If α is a primitive element of $\mathbb{F}_{q^m}$ then

$$c_R = (\operatorname{Tr}_{q^m/q}(xR(x)))_{x \in \mathbb{F}_{q^m}^*} = (\operatorname{Tr}_{q^m/q}(\alpha^i R(\alpha^i)))_{i=0}^{q^m-2}.$$

The cyclic shift of c_R is

$$s(c_R) = (\operatorname{Tr}_{q^m/q}(\alpha^i R(\alpha^i)))_{i=0}^{q^m-2} = c_S$$

with $S(x) = \alpha^{-1}R(\alpha^{-1}x) \in \mathcal{L}$, hence $s(c_R)$ is in $\mathcal{C}_{\mathcal{L}}$ and the code is cyclic. Similarly for the other codes.

Definition 3.1. A family $\mathcal{L} \subset \mathbb{F}_{q^m}[x]$ of q-linearized polynomials has the *even rank property* or is an *even rank family* if the quadratic form $Q_R(x) = \operatorname{Tr}_{q^m/q}(xR(x))$ has even rank for any $R \in \mathcal{L}$.

Let $\mathcal{L}$ be an even rank family of q-linearized polynomials. Then, the quadratic form $Q_R(x) = \mathrm{Tr}_{q/p}(xR(x))$ has constant type in the family; that is, $Q_R(x)$ is either of type 1 or of type -1 for every $R \in \mathcal{L}$. Therefore, given r a non-negative integer, we can define

$$\begin{aligned} K_r &= \{R \in \mathcal{L} : Q_R \text{ has rank } r\}, \\ K_{r,1} &= \{R \in \mathcal{L} \setminus \{0\} : Q_R \text{ has rank } r \text{ of type } 1\}, \\ K_{r,2} &= \{R \in \mathcal{L} \setminus \{0\} : Q_R \text{ has rank } r \text{ of type } 3\}. \end{aligned} \tag{3.3}$$

We have $K_0 = \{0\}$ and $K_r = K_{r,1} \sqcup K_{r,2}$ for $r > 0$, and we denote their cardinalities by

$$M_{r,1} = \#K_{r,1}, \qquad M_{r,2} = \#K_{r,2}, \qquad M_r = \#K_r. \tag{3.4}$$

Note that $M_0 = 1$ and $M_r = M_{r,1} + M_{r,2}$ for $r > 0$. Finally, we denote the set of ranks in $\mathcal{L}$ by

$$R_{\mathcal{L}} = \{r \in \mathbb{Z}_{\geq 0} : \text{there exists } R \in \mathcal{L} \text{ with } Q_R \text{ of rank } r\}. \tag{3.5}$$

For any positive integer r, we define the set

$$[r]_q := \{q^\ell + 1 : 0 < \ell < r\} = \{q+1, q^2+1, \ldots, q^{r-1}+1\}.$$

We now restate Lemma 2.1 in [14] in more generality and give a proof for completeness. We will need the lemma to calculate the dimensions of the four families of codes considered in this section.

Lemma 3.2. *Let m be a positive even integer and let $M = \{1\} \cup [\frac{m}{2}]_q$. If α is a primitive element of $\mathbb{F}_{q^m}$ then we have:*

(a) *α^{-u} and α^{-v} are not conjugated for all distinct elements $u, v \in M$.*
(b) *The minimum $m_u \in \{1, \ldots, m\}$ such that $q^{m_u} u \equiv u \pmod{q^m - 1}$ is m, for all $u \in M$.*

Proof. For (a) it is enough to show that $q^s(q^{\ell_1} + 1) \not\equiv q^{\ell_2} + 1 \pmod{q^m - 1}$ and that $q^s \not\equiv q^\ell + 1 \pmod{q^m - 1}$ for $1 \leq s \leq m-1$ and $\ell, \ell_1, \ell_2 < \frac{m}{2}$ with $\ell_1 \neq \ell_2$. We will show the first statement. Suppose that there is some $s \in \{1, \ldots, m\}$ such that $q^s(q^{\ell_1} + 1) \equiv q^{\ell_2} + 1 \pmod{q^m - 1}$. Then,

$$q^{s+\ell_1} + q^s \equiv q^{\ell_2} + 1 \pmod{q^m - 1}.$$

If $s + \ell_1 < m$ then $q^{s+\ell_1} + q^s = q^{\ell_2} + 1$ as integers. The uniqueness of the q-ary expansion of integers implies that $s + \ell_1 = \ell_2$ and $s = 0$, which cannot happen. Now, if $s + \ell_1 > m$ then $s > \frac{m}{2}$ since by hypothesis $\ell_1 < \frac{m}{2}$, and hence there exists a positive integer $t < \frac{m}{2}$ such that $s = m - t$. Notice that $\ell_1 > t$ and $0 < \ell_1 - t < \frac{m}{2}$, thus $q^{s+\ell_1} + q^s \equiv q^{\ell_1 - t} + q^s \pmod{q^m - 1}$ and hence

$$q^{\ell_1 - t} + q^s \equiv q^{\ell_2} + 1 \pmod{q^m - 1}.$$

Since all the powers are less than m, we obtain $q^{\ell_1 - t} + q^s = q^{\ell_2} + 1$. By the uniqueness of the q-ary expansion of integers, and since $s > 0$, we obtain $s = \ell_2$ and $\ell_1 - t = 0$, which cannot occur. Therefore, α^{-u} and α^{-v} are not conjugated

for all $u \neq v$ in $[\frac{m}{2}]_q$. In a similar way, it can be shown that α^{-1} and α^{-u} are not conjugated for all $u \in [\frac{m}{2}]_q$.

Item (b) can be proved by an argument similar to that given in (a). □

We are now in a position to give the weight distribution of the four codes considered. We will do this in two different theorems.

Theorem 3.3. *Let q be a prime power, m a non-negative integer, and consider an ideal $\mathcal{L} = \langle x^{q^{\ell_1}}, x^{q^{\ell_2}}, \ldots, x^{q^{\ell_s}} \rangle$ in $\mathbb{F}_{q^m}[x]$ such that $1 \leq \ell_1 < \ell_2 < \cdots < \ell_s < \frac{m}{2}$. If $\mathcal{L}$ is an even rank family then the dimensions of the cyclic codes $\mathcal{C}_{\mathcal{L}}$ and $\mathcal{C}_{\mathcal{L},0}$ are ms and $ms+1$, respectively, and their spectra are given by Tables 1 and 2 below.*

weight	frequency
$w_0 = 0$	1
$w_{1,i} = q^m - q^{m-1} + (-1)^i (q-1) q^{m-\frac{r}{2}-1}$	$M_{r,i}$

TABLE 1. Weight distribution of $\mathcal{C}_{\mathcal{L}}$ ($r \in R_{\mathcal{L}}$, $i = 1, 2$).

weight	frequency
$w_0 = 0$	1
$w_1 = q^m - 1$	$q - 1$
$w_{2,i} = q^m - q^{m-1} + (-1)^i (q-1) q^{m-\frac{r}{2}-1}$	$M_{r,i}$
$w_{3,i} = q^m - q^{m-1} + (-1)^{i+1} q^{m-\frac{r}{2}-1} - 1$	$M_{r,i}(q-1)$

TABLE 2. Weight distribution of $\mathcal{C}_{\mathcal{L},0}$ ($r \in R_{\mathcal{L}}$, $i = 1, 2$).

Proof. By definition, $w(c_R) = \#\{x \in \mathbb{F}_{q^m}^* : Q_R(x) \neq 0\}$; then

$$w(c_R) = q^m - 1 - \#\{x \in \mathbb{F}_{q^m}^* : Q_R(x) = 0\}.$$

Analogously, $w(c_{R,b}) = q^m - 1 - \#\{x \in \mathbb{F}_{q^m}^* : Q_R(x) = -b\}$. Then we have that

$$w(c_{R,b}) = \begin{cases} q^m - N_{Q_R}(0) & \text{if } b = 0, \\ q^m - N_{Q_R}(-b) - 1 & \text{if } b \neq 0. \end{cases}$$

If Q_R has rank r and type ε_R then

$$w(c_{R,b}) = \begin{cases} q^m - q^{m-1} - \varepsilon_R \, (q-1) \, q^{m-\frac{r}{2}-1} & \text{if } b = 0, \\ q^m - q^{m-1} + \varepsilon_R \, q^{m-\frac{r}{2}-1} - 1 & \text{if } b \neq 0. \end{cases}$$

From these facts, using the numbers M_r, M_{r_i} and the set $R_{\mathcal{L}}$, we obtain the weights and frequencies given in Tables 1 and 2, and the result thus follows.

Let us consider the polynomial

$$h(x) = h_{\ell_1}(x) \cdots h_{\ell_s}(x),$$

where $h_{\ell_j}(x)$ is the minimal polynomial of $\alpha^{-(q^{\ell_j}+1)}$ over $\mathbb{F}_q$ with α a primitive element of $\mathbb{F}_{q^m}$ for each $j = 1, \dots, s$. By Delsarte's theorem, if $n = \frac{q^m-1}{\delta}$ with $\delta = \gcd(q^m - 1, q^{\ell_1} + 1, \dots, q^{\ell_s} + 1)$, then $h(x)$ is the check polynomial of the cyclic code

$$\mathcal{C}^*_{\mathcal{L}} = \left\{ c(a_1, \dots, a_s) = \left(\sum_{j=1}^{s} \mathrm{Tr}_{q^m/q}(a_j g_j^i) \right)_{i=1}^{n} : a_j \in \mathbb{F}_{q^m} \right\} \subset \mathbb{F}_q^n,$$

where $g_j = \alpha^{q^{\ell_j}+1}$ for $j = 1, \dots, s$. Since the dimension of a cyclic code is given by the degree of its check polynomial, we have

$$\dim \mathcal{C}^*_{\mathcal{L}} = \deg h(x).$$

By the general theory of finite fields, the degree of the minimal polynomial over $\mathbb{F}_q$ of an element $u \in \mathbb{F}_q$ is given by the size of its cyclotomic coset, and this size coincides with the minimum $1 \leq m_u \leq m$ such that

$$q^{m_u} u \equiv u \pmod{q^m - 1}.$$

By Lemma 3.2, all of the elements in $\mathcal{L}$ are not conjugated to each other and $\deg h_{\ell_j}(x) = m$ for $j = 1, \dots, s$. Hence $\deg h(x) = sm$ and thus $\dim \mathcal{C}^*_{\mathcal{L}} = sm$.

On the other hand, if $R(x) = a_1 x^{q^{\ell_1}} + \cdots + a_s x^{q^{\ell_s}} \in \mathcal{L}$, by linearity of the trace function we have that

$$\begin{aligned} c_R &= \left(\mathrm{Tr}_{q^m/q}(xR(x)) \right)_{x \in \mathbb{F}^*_{q^m}} \\ &= \left(\sum_{j=1}^{s} \mathrm{Tr}_{q^m/q}(a_j \alpha^{i(q^{\ell_j}+1)}) \right)_{i=1}^{q^m-1} = \left(\sum_{j=1}^{s} \mathrm{Tr}_{q^m/q}(a_j g_j^i) \right)_{i=1}^{q^m-1}. \end{aligned}$$

Notice that if $n = \frac{q^m-1}{\delta}$ as before, by modularity we get

$$\left(\sum_{j=1}^{s} \mathrm{Tr}_{q^m/q}(a_j g_j^i) \right)_{i=1}^{n} = \left(\sum_{j=1}^{s} \mathrm{Tr}_{q^m/q}(a_j g_j^i) \right)_{i=(t-1)n+1}^{tn} \tag{3.6}$$

for every $1 \leq t \leq \delta$. Thus, denoting $\mathbf{c} = c(a_1, \dots, a_s) \in \mathcal{C}_{\mathcal{L}}$, by (3.6) we have that

$$c_R = \big(\underbrace{\mathbf{c} \,|\, \cdots \,|\, \mathbf{c}}_{\delta\text{-times}} \big).$$

Hence, all the words in $\mathcal{C}_{\mathcal{L}}$ are obtained by δ-concatenation of the words of the cyclic code $\mathcal{C}^*_{\mathcal{L}}$, and hence the dimensions of these codes are the same. Therefore $\dim \mathcal{C}_{\mathcal{L}} = \dim \mathcal{C}^*_{\mathcal{L}} = sm$. The same argument shows that $\dim \mathcal{C}_{\mathcal{L},0} = sm + 1$. □

Theorem 3.4. *Let q be a prime power, m a non-negative integer, and consider an ideal $\mathcal{L} = \langle x^{q^{\ell_1}}, x^{q^{\ell_2}}, \dots, x^{q^{\ell_s}} \rangle$ in $\mathbb{F}_{q^m}[x]$ such that $1 \leq \ell_1 < \ell_2 < \cdots < \ell_s < \frac{m}{2}$. If $\mathcal{L}$ is an even rank family, then the dimensions of the cyclic codes $\mathcal{C}_{\mathcal{L},1}$ and $\mathcal{C}_{\mathcal{L},2}$ are $m(s+1)$ and $m(s+1)+1$, respectively, and their spectra are given by Tables 3 and 4 below.*

weight	frequency
$w_0 = 0$	1
$w_{1,i} = q^m - q^{m-1}$	$\sum_{r\in R_{\mathcal{L}}} M_r(q^m - q^r)$
$w_{2,i} = q^m - q^{m-1} + (-1)^i(q-1)q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^{r-1} + (-1)^{i+1}(q-1)q^{\frac{r}{2}-1})$
$w_{3,i} = q^m - q^{m-1} + (-1)^{i+1}q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^{r-1} + (-1)^i q^{\frac{r}{2}-1})(q-1)$

TABLE 3. Weight distribution of $\mathcal{C}_{\mathcal{L},1}$ ($r \in R_{\mathcal{L}}$, $i = 1, 2$).

weight	frequency
$w_0 = 0$	1
$w_1 = q^m - q^{m-1}$	$\sum_{r\in R_{\mathcal{L}}} M_r(q^m - q^r)$
$w_{2,i} = q^m - q^{m-1} + (-1)^i(q-1)q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^{r-1} + (-1)^{i+1}(q-1)q^{\frac{r}{2}-1})$
$w_{3,i} = q^m - q^{m-1} + (-1)^{i+1}q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^{r-1} + (-1)^i q^{\frac{r}{2}-1})(q-1)$
$w_4 = q^m - 1$	$q-1$
$w_5 = q^m - q^{m-1} - 1$	$(q-1)\sum_{r\in R_{\mathcal{L}}} M_r(q^m - q^r)$
$w_{6,i} = q^m - q^{m-1} - 1 + (-1)^i(q-1)q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^{r-1} + (-1)^i q^{\frac{r}{2}-1})(q-1)$
$w_{7,i} = q^m - q^{m-1} - 1 + (-1)^{i+1}q^{m-\frac{r}{2}-1}$	$M_{r,i}(q^r - q^{r-1} + (-1)^{i+1}q^{\frac{r}{2}-1})(q-1)$

TABLE 4. Weight distribution of $\mathcal{C}_{\mathcal{L},2}$ ($r \in R_{\mathcal{L}}$, $i = 1, 2$).

Proof. The dimensions of $\mathcal{C}_{\mathcal{L},1}$ and $\mathcal{C}_{\mathcal{L},2}$ can be obtained in the same way as in Theorem 3.3 using Lemma 3.2.

Now, let $R \in \mathcal{L}$ and suppose that the quadratic form Q_R has rank r and type ε_R. Let us compute the weights of the codewords of $\mathcal{C}_{\mathcal{L},1}$:

$$w(c_R(\beta)) = q^m - 1 - \#\{x \in \mathbb{F}_{q^m}^* : Q_R(x) + \mathrm{Tr}_{q^m/q}(\beta x) = 0\}.$$

By the orthogonality property of the characters of $\mathbb{F}_q$, we have that

$$\begin{aligned} w(c_R(\beta)) &= q^m - 1 - \tfrac{1}{q}\sum_{a\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^m}^*} \zeta_p^{\mathrm{Tr}_{q/p}(a(Q_R(x)+\mathrm{Tr}_{q^m/q}(\beta x)))} \\ &= q^m - 1 - \tfrac{1}{q}\Big\{\sum_{a\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(a(Q_R(x)+\mathrm{Tr}_{q^m/q}(\beta x)))} - q\Big\} \\ &= q^m - 1 - \tfrac{1}{q}\Big\{\sum_{a\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(a(Q_R(x)+\mathrm{Tr}_{q^m/q}(\beta x)))} + q^m - q\Big\}. \end{aligned}$$

Therefore

$$w(c_R(\beta)) = q^m - q^{m-1} - \tfrac{1}{q}S_{Q_R}(\beta),$$

where S_{Q_R} is the exponential sum (2.1), with $b = 0$. In the same way, when $b \neq 0$, we get

$$w(c_{R,b}(\beta)) = q^m - q^{m-1} - 1 - \tfrac{1}{q} S_{Q_R,b}(\beta).$$

Notice that if $R = 0$, then $Q_R = 0$ and, for all $\beta \neq 0$, we have $w(c_0(\beta)) = q^m - q^{m-1}$. If R and β are zeros, then $w(c_{0,b}(0)) = q^m - 1$ if $b \neq 0$. When $b = 0$ we will denote $c_R(\beta) = c_{R,0}(\beta)$.

Now, let $K_{r,1}$ and $K_{r,2}$ be as in (3.3). Then, $\varepsilon_R = (-1)^{i+1}$ if $R \in K_{r,i}$, $i = 1, 2$. By Lemma 2.2, we have that

$$w(c_{R,b}(\beta)) = \begin{cases} 0 & \text{if } b = 0,\ R = 0, \\ q^m - q^{m-1} & \text{if } b = 0,\ R \in K_{r,i}, \\ & \text{for } q^m - q^r\ \beta' s, \\ q^m - q^{m-1} + (-1)^i (q-1) q^{m-\frac{r}{2}-1} & \text{if } b = 0,\ R \in K_{r,i}, \\ & \text{for } q^{r-1} + (-1)^{i+1}(q-1) q^{\frac{r}{2}-1}\ \beta' s, \\ q^m - q^{m-1} + (-1)^{i+1} q^{m-\frac{r}{2}-1} & \text{if } b = 0,\ R \in K_{r,i}, \\ & \text{for } (q^{r-1} + (-1)^i q^{\frac{r}{2}-1})(q-1)\ \beta' s, \\ q^m - 1 & \text{if } b \neq 0,\ R = 0,\ \beta = 0, \\ q^m - q^{m-1} - 1 & \text{if } b \neq 0,\ R \in K_{r,i}, \\ & \text{for } q^m - q^r\ \beta' s, \\ q^m - q^{m-1} + (-1)^i (q-1) q^{m-\frac{r}{2}-1} - 1 & \text{if } b \neq 0,\ R \in K_{r,i}, \\ & \text{for } q^{r-1} + (-1)^i q^{\frac{r}{2}-1}\ \beta' s, \\ q^m - q^{m-1} + (-1)^{i+1} q^{m-\frac{r}{2}-1} - 1 & \text{if } b \neq 0,\ R \in K_{r,i}, \\ & \text{for } q^r - q^{r-1} + (-1)^{i+1} q^{\frac{r}{2}-1}\ \beta' s, \end{cases}$$

with $i = 1, 2$. From this, the result readily follows. □

Remark 3.5. (i) A code is *t-divisible* if the weight of every codeword is divisible by t. Note that from Tables 1–4, the code $\mathcal{C}_{\mathcal{L}}$ is $q^{m-\frac{r}{2}-1}(q-1)$-divisible, the code $\mathcal{C}_{\mathcal{L},0}$ is $(q-1)$-divisible if and only if $M_{r,2} = 0$, and $\mathcal{C}_{\mathcal{L},1}$ is $q^{m-\frac{r}{2}-1}$-divisible.

(ii) If one performs the sum of the frequencies in each of the Tables 1–4 one checks that the dimensions of the codes are the ones given in Theorems 3.3–3.4.

Complete weight enumerator. Suppose that the elements of $\mathbb{F}_q$ are ordered, say $\omega_0 = 0, \omega_1, \ldots, \omega_{q-1}$. The composition of the vector $v = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_q^n$ is defined by

$$\operatorname{comp}(v) = (t_0, t_1, \ldots, t_{q-1}),$$

where each $t_i = t_i(v) = \#\{0 \leq j \leq n-1 : v_j = \omega_i\}$. Clearly, we have that $\sum_{i=0}^{q-1} t_i = n$. Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_q$ and let

$$A(t_0, t_1, \ldots, t_{q-1}) = \#\{c \in \mathcal{C} : \operatorname{comp}(c) = (t_0, t_1, \ldots, t_{q-1})\}.$$

The *complete weight enumerator* of $\mathcal{C}$ is the polynomial

$$W_{\mathcal{C}}(z_0, z_1, \ldots, z_{q-1}) = \sum_{(t_0,\ldots,t_{q-1}) \in B_n} A(t_0, t_1, \ldots, t_{q-1})\ z_0^{t_0} z_1^{t_1} \cdots z_{q-1}^{t_{q-1}},$$

where $B_n = \{(t_0, \dots, t_{q-1}) : t_i \geq 0,\ t_0 + \cdots + t_{q-1} = n\}$.

Lemma 3.6. *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_q$ such that $t_i(c) = t_j(c)$ for all $i, j > 0$ and $c \in \mathcal{C}$. Then, if $A_\ell = \#\{c \in \mathcal{C} : w(c) = \ell\}$, we have that*

$$W_{\mathcal{C}}(z_0, z_1, \dots, z_{q-1}) = \sum_{\ell=0}^{n} A_\ell\ z_0^{n-\ell} z_1^{\frac{\ell}{q-1}} \cdots z_{q-1}^{\frac{\ell}{q-1}}.$$

Proof. Let $c = (c_0, \dots, c_{n-1}) \in \mathcal{C}$. Since $t_i(c) = t_j(c)$ for $i, j > 0$ and $\sum_{i=0}^{q-1} t_i = n$, we have that $t_i = \frac{n-t_0}{q-1}$. On the other hand, since

$$w(c) = n - \#\{0 \leq j \leq n-1 : c_j = 0\} = n - t_0,$$

we have that $t_0 = n - w(c)$, and thus $t_1 = \frac{w(c)}{q-1}$ (note that $\mathcal{C}$ has to be necessarily $(q-1)$-divisible). Therefore, we have that $A(t_0, \dots, t_{q-1}) = A_{w(c)}$ if $t_0 = n - w(c)$ for some $c \in \mathcal{C}$ and $t_i = t_j$ for all $i, j > 0$, and $A(t_0, \dots, t_{q-1}) = 0$ otherwise. □

As a direct consequence of the previous lemma, we obtain the complete weight enumerator of $\mathcal{C}_{\mathcal{L}}$.

Proposition 3.7. *Let q be a prime power, m a non-negative integer, and consider an ideal $\mathcal{L} = \langle x^{q^{\ell_1}}, x^{q^{\ell_2}}, \dots, x^{q^{\ell_s}} \rangle$ in $\mathbb{F}_{q^m}[x]$ such that $1 \leq \ell_1 < \ell_2 < \cdots < \ell_s < \frac{m}{2}$. If $\mathcal{L}$ is an even rank family then the complete weight enumerator of $\mathcal{C}_{\mathcal{L}}$ is given by*

$$W_{\mathcal{C}_{\mathcal{L}}}(z_0, \dots, z_{q-1}) = z_0^n + \sum_{i=1}^{2} \sum_{r \in R_{\mathcal{L}}} M_{r,i}\ z_0^{a(r,i)} z_1^{b(r,i)} \cdots z_{q-1}^{b(r,i)},$$

where $M_{r,i}$ and $R_{\mathcal{L}}$ are as in (3.4) *and* (3.5) *and also*

$$a(r,i) = q^{m-1} + (-1)^{i+1}(q-1)q^{m-\frac{r}{2}-1} - 1,$$
$$b(r,i) = q^{m-1} + (-1)^i q^{m-\frac{r}{2}-1}.$$

4. The codes associated to $x^{q^\ell+1}$

Here, we consider the codes $\mathcal{C}_{\mathcal{L}}$, $\mathcal{C}_{\mathcal{L},0}$, $\mathcal{C}_{\mathcal{L},1}$, and $\mathcal{C}_{\mathcal{L},2}$ from the previous section but in the particular case of $\mathcal{L} = \langle x^{q\ell} \rangle$, that we denote by $\mathcal{C}_\ell$, $\mathcal{C}_{\ell,0}$, $\mathcal{C}_{\ell,1}$, and $\mathcal{C}_{\ell,2}$. We will compute the spectra of these codes using Theorems 3.3 and 3.4 and Tables 1–4, by explicitly computing the rank distribution in $\mathcal{L}$ and their associated numbers $M_{r,i}$.

The codes $\mathcal{C}_\ell$ and $\mathcal{C}_{\ell,0}$. Consider the irreducible cyclic code $\mathcal{C}_\ell$ and the code $\mathcal{C}_{\ell,0}$ over $\mathbb{F}_q$, with check polynomial $h_\ell(x)$ and $h_\ell(x)(x-1)$, respectively, where h_ℓ is the minimal polynomial of $\alpha^{-(q^\ell+1)}$, with α a primitive element. By Delsarte's theorem these codes can be described by

$$\begin{aligned} \mathcal{C}_\ell &= \Big\{ c(\gamma) = \big(\mathrm{Tr}_{q^m/q}(\gamma \alpha^{(q^\ell+1)i}) \big)_{i=0}^{n-1} : \gamma \in \mathbb{F}_{q^m} \Big\}, \\ \mathcal{C}_{\ell,0} &= \Big\{ c_b(\gamma) = \big(\mathrm{Tr}_{q^m/q}(\gamma \alpha^{(q^\ell+1)i}) + b \big)_{i=0}^{n-1} : \gamma \in \mathbb{F}_{q^m}, b \in \mathbb{F}_q \Big\}. \end{aligned} \tag{4.1}$$

Now we give the parameters and the spectra of these codes.

Theorem 4.1. *Let q be a prime power and m, ℓ positive integers such that $\ell < \frac{m}{2}$ and $m_\ell = \frac{m}{(m,\ell)}$ is even. Then, $\mathcal{C}_\ell$ is a $[n, m, d]_q$-code with $n = \frac{q^m-1}{D}$ and $d = \frac{1}{D}q^{\frac{m}{2}-1}(q-1)d'$, where $D = q^{(m,\ell)} + 1$ and*

$$d' = \begin{cases} q^{\frac{m}{2}} - 1 & \text{if } \frac{1}{2}m_\ell \text{ is even,} \\ q^{\frac{m}{2}} - q^{(m,\ell)} & \text{if } \frac{1}{2}m_\ell \text{ is odd.} \end{cases}$$

On the other hand, $\mathcal{C}_{\ell,0}$ is a $[n, m+1, \hat{d}]_q$-code with $\hat{d} = \frac{1}{D}(q^{m-1}(q-1) - \bar{d})$ and

$$\bar{d} = \begin{cases} q^{\frac{m}{2}+(m,\ell)-1} + 1 & \text{if } \frac{1}{2}m_\ell \text{ is even,} \\ q^{\frac{m}{2}+(m,\ell)-1}(q-1) & \text{if } \frac{1}{2}m_\ell \text{ is odd.} \end{cases}$$

The weight distributions of $\mathcal{C}_\ell$ and $\mathcal{C}_{\ell,0}$ are given by Tables 5 and 6 below.

weight	frequency
0	1
$\frac{1}{D}\left\{q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}+(m,\ell)-1}\right\}$	n
$\frac{1}{D}\left\{q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-1}\right\}$	$nq^{(m,\ell)}$

TABLE 5. Weight distribution of $\mathcal{C}_\ell$.

weight	frequency
0	1
$\frac{1}{D}(q^m - 1)$	$q-1$
$\frac{1}{D}\left\{q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}+(m,\ell)-1}\right\}$	n
$\frac{1}{D}\left\{q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-1}\right\}$	$nq^{(m,\ell)}$
$\frac{1}{D}\left\{q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}+(m,\ell)-1} - 1\right\}$	$n(q-1)$
$\frac{1}{D}\left\{q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-1} - 1\right\}$	$nq^{(m,\ell)}(q-1)$

TABLE 6. Weight distribution of $\mathcal{C}_{\ell,0}$.

Proof. Let us begin by computing the length n of these codes. Since m_ℓ is even, by Lemma 2.5 we have that $n = \frac{q^m-1}{q^{(m,\ell)}+1}$. Thus $q^{(m,\ell)} + 1 \mid q^m - 1$ and by Lemma 2.6 we have $n = M$ or $n = M_1 = M_2$ in even or odd characteristic respectively, where M, M_1, and M_2 are the cardinalities of the sets $S_{q,m}(\ell)$, $X_{q,m}(\ell)$, and $Y_{q,m}(\ell)$ defined in (2.2) and (2.3). Notice that in this case $q^m - 1 - M = nq^{(m,\ell)}$ in even characteristic and $q^m - 1 - M_1 = q^m - 1 - M_2 = nq^{(m,\ell)}$ in odd characteristic.

Let $\mathcal{L}_\ell = \langle x^{q^\ell} \rangle$; then

$$R \in \mathcal{L}_\ell \quad \Leftrightarrow \quad R(x) = \gamma x^{q^\ell} = R_\gamma(x) \text{ for some } \gamma \in \mathbb{F}_{q^m}.$$

Thus $Q_R(x) = \mathrm{Tr}_{q^m/q}(\gamma x^{q^\ell+1}) = Q_{\gamma,\ell}(x)$.

Notice that the codes $\mathcal{C}_{\mathcal{L}_\ell}$ and $\mathcal{C}_{\mathcal{L}_\ell,0}$ as in (3.1) are obtained from $(q^m-1, q^\ell+1)$-copies of the codes $\mathcal{C}_\ell$ and $\mathcal{C}_{\ell,0}$ in (4.1), respectively. In terms of weights, this means that

$$w(c_b(\gamma)) = \frac{w(c_{R_\gamma,b})}{(q^m-1, q^\ell+1)}.$$

By Theorems 2.3 and 2.4, $\mathcal{L}_\ell$ is an even rank family. Furthermore, $R_{\mathcal{L}_\ell} = \{0, m, m-2(m,\ell)\}$. If q is even, by Theorem 2.3 we have that

$$\begin{aligned} &M_{m,2} = M_{m-2(m,\ell),1} = 0, \quad M_{m,1} = nq^{(m,\ell)}, \quad M_{m-2(m,\ell),2} = n, \quad \text{if } \tfrac{1}{2}m_\ell \text{ is even;} \\ &M_{m,1} = M_{m-2(m,\ell),2} = 0, \quad M_{m-2(m,\ell),1} = n, \quad M_{m,2} = nq^{(m,\ell)}, \quad \text{if } \tfrac{1}{2}m_\ell \text{ is odd.} \end{aligned}$$

Similarly, if q is odd, Theorem 2.4 implies that

$$\begin{aligned} &M_{m,2} = M_{m-2(m,\ell),1} = 0, \quad M_{m,1} = nq^{(m,\ell)}, \quad M_{m-2(m,\ell),2} = n, \quad \text{if } \tfrac{1}{2}m_\ell \text{ is even;} \\ &M_{m,1} = M_{m-2(m,\ell),2} = 0, \quad M_{m-2(m,\ell),1} = n, \quad M_{m,2} = nq^{(m,\ell)}, \quad \text{if } \tfrac{1}{2}m_\ell \text{ is odd.} \end{aligned}$$

Now, by Theorem 3.3, we obtain the weights and frequencies given in Tables 5 and 6. Finally, by studying the values in the tables, we get the minimal distances for both codes. □

Under the hypothesis of Theorem 4.1 we have the following result.

Corollary 4.2. *The complete weight enumerator of $\mathcal{C}_\ell$ is given by*

$$W_{\mathcal{C}_\ell}(z_0, \dots, z_{q-1}) = z_0^n + n z_0^{a_0} z_1^{a_1} \cdots z_{q-1}^{a_1} + n q^{(m,\ell)} z_0^{a_0'} z_1^{a_1'} \cdots z_{q-1}^{a_1'},$$

where

$$\begin{aligned} &a_0 = n - \tfrac{(q-1)q^{m-1}}{D}\big(1 + (-1)^{\frac{1}{2}m_\ell} q^{(m,\ell)-\frac{m}{2}}\big), \quad a_1 = \tfrac{q^{m-1}}{D}\big(1 + (-1)^{\frac{1}{2}m_\ell} q^{(m,\ell)-\frac{m}{2}}\big), \\ &a_0' = n - \tfrac{(q-1)q^{m-1}}{D}\big(1 + (-1)^{\frac{1}{2}m_\ell+1} q^{-\frac{m}{2}}\big), \qquad a_1' = \tfrac{q^{m-1}}{D}\big(1 + (-1)^{\frac{1}{2}m_\ell+1} q^{-\frac{m}{2}}\big), \end{aligned}$$

with $D = q^{(m,\ell)} + 1$.

Example 4.3. Let $q = 2$, $m = 8$, and $\ell = 1$. By Theorems 3.3 and 3.4 the codes $\mathcal{C}_\ell$ and $\mathcal{C}_{\ell,0}$ have parameters $[85, 8, 40]$ and $[85, 9, 37]$ respectively, with weight enumerators given by

$$\begin{aligned} W_{\mathcal{C}_\ell}(x) &= 1 + 170x^{120} + 85x^{144}, \\ W_{\mathcal{C}_{\ell,0}}(x) &= 1 + 85x^{37} + 170x^{40} + 170x^{45} + 85x^{48} + x^{85}. \end{aligned}$$

The codes $\mathcal{C}_{\ell,1}$ and $\mathcal{C}_{\ell,2}$. Consider now the codes $\mathcal{C}_{\ell,1}$ and $\mathcal{C}_{\ell,2}$ over $\mathbb{F}_q$, with check polynomials $h_\ell(x)h_1(x)$ and $h_\ell(x)h_1(x)(x-1)$, respectively. Here, h_ℓ and $h_1(x)$ are the minimal polynomials of $\alpha^{-(q^\ell+1)}$ and α^{-1} respectively, where α is a primitive element of $\mathbb{F}_{q^m}$. By Delsarte's theorem, these codes are given by

$$\mathcal{C}_{\ell,1} = \Big\{ c(\gamma,\beta) = \big(\operatorname{Tr}_{q^m/q}(\gamma x^{q^\ell+1} + \beta x)\big)_{x\in\mathbb{F}_{q^m}^*} : \gamma,\beta \in \mathbb{F}_{q^m} \Big\},$$

$$\mathcal{C}_{\ell,2} = \Big\{ c_b(\gamma,\beta) = \big(\operatorname{Tr}_{q^m/q}(\gamma x^{q^\ell+1}\beta x) + b\big)_{x\in\mathbb{F}_{q^m}^*} : \gamma,\beta \in \mathbb{F}_{q^m}, b \in \mathbb{F}_q \Big\}.$$

As before, for positive integers m,ℓ such that $m/(m,\ell)$ is even we put $n = \frac{q^m-1}{q^{(m,\ell)}+1}$. We now give the parameters and the spectra of these codes.

Theorem 4.4. *Let q be a prime power and m,ℓ positive integers such that m_ℓ is even. Then, $\mathcal{C}_{\ell,1}$ is a $[N,2m,d]_q$-code with $N = q^m-1$ and $d = q^{m-1}(q-1) - d'$, with*

$$d' = \begin{cases} q^{\frac{m}{2}+(m,\ell)-1} & \text{if } \frac{1}{2}m_\ell \text{ is even,} \\ (q-1)q^{\frac{m}{2}+(m,\ell)-1} & \text{if } \frac{1}{2}m_\ell \text{ is odd,} \end{cases}$$

and $\mathcal{C}_{\ell,2}$ is a $[N,2m+1,d-1]_q$-code. The weight distributions of the codes $\mathcal{C}_{\ell,1}$ and $\mathcal{C}_{\ell,2}$ are given by Tables 7 and 8 below.

weight	frequency
0	1
$q^m - q^{m-1}$	$n(q^m - q^{m-2(m,\ell)}) + q^m - 1$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-1}$	$nq^{(m,\ell)}(q^{m-1} + (-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}-1})$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}+(m,\ell)-1}$	$n(q^{m-1-2(m,\ell)} + (-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-(m,\ell)-1})$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-1}$	$nq^{(m,\ell)}(q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}-1})(q-1)$
$q^m - q^{m-1} + (-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}+(m,\ell)-1}$	$n(q^{m-1-2(m,\ell)} + (-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-(m,\ell)-1})(q-1)$

TABLE 7. Weight distribution of $\mathcal{C}_{\ell,1}$.

Proof. Note that $\mathcal{C}_{\ell,1} = \mathcal{C}_{\mathcal{L}_\ell,1}$ and $\mathcal{C}_{\ell,2} = \mathcal{C}_{\mathcal{L}_\ell,2}$ with $\mathcal{L}_\ell = \langle x^{q^\ell}\rangle$, where $\mathcal{C}_{\mathcal{L}_\ell,1}, \mathcal{C}_{\mathcal{L}_\ell,2}$ are the codes defined in (3.2). Then, by Theorem 3.4, it is enough to compute the numbers $M_{r,1}$, $M_{r,2}$ and the set $R_{\mathcal{L}_\ell}$. They were calculated in the proof of Theorem 4.1. Therefore, Tables 7 and 8 give the spectra of the codes $\mathcal{C}_{\ell,1}$ and $\mathcal{C}_{\ell,2}$ as was to be shown. □

Example 4.5. Let $q=2$, $m=8$, and $\ell=1$ as in Example 4.3. By Theorem 4.4, the codes $\mathcal{C}_{\ell,1}$ and $\mathcal{C}_{\ell,2}$ have parameters $[255,16,112]$ and $[255,17,111]$, respectively. Also, we have

$$W_{\mathcal{C}_{\ell,1}}(x) = 1 + 3060\,x^{112} + 23120\,x^{120} + 16575\,x^{128} + 20400\,x^{136} + 2380\,x^{144},$$

$$W_{\mathcal{C}_{\ell,2}}(x) = 1 + 2380\,x^{111} + 3060\,x^{112} + 20400\,x^{119} + 23120\,x^{120} + 16575\,x^{127} + 16575\,x^{128} + 23120\,x^{135} + 20400\,x^{136} + 3060\,x^{143} + 2380\,x^{144} + x^{255}.$$

weight	frequency
0	1
$q^m-q^{m-1}-1$	$n(q^m-q^{m-2(m,\ell)})(q-1)+(q^m-1)(q-1)$
$q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-1}-1$	$nq^{(m,\ell)}(q^{m-1}+(-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}-1})(q-1)$
$q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}+(m,\ell)-1}-1$	$n(q^{m-1-2(m,\ell)}+(-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-(m,\ell)-1})(q-1)$
$q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-1}-1$	$nq^{(m,\ell)}(q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-1})(q-1)$
$q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}+(m,\ell)-1}-1$	$n(q^{m-2(m,\ell)}-q^{m-1-2(m,\ell)}+(-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}-(m,\ell)-1})(q-1)$
q^m-1	$q-1$
q^m-q^{m-1}	$n(q^m-q^{m-2(m,\ell)})+q^m-1$
$q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-1}$	$nq^{(m,\ell)}(q^{m-1}+(-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}-1})$
$q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell}(q-1)q^{\frac{m}{2}+(m,\ell)-1}$	$n(q^{m-1-2(m,\ell)}+(-1)^{\frac{1}{2}m_\ell+1}(q-1)q^{\frac{m}{2}-(m,\ell)-1})$
$q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-1}$	$nq^{(m,\ell)}(q^{m-1}+(-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}-1})(q-1)$
$q^m-q^{m-1}+(-1)^{\frac{1}{2}m_\ell+1}q^{\frac{m}{2}+(m,\ell)-1}$	$n(q^{m-1-2(m,\ell)}+(-1)^{\frac{1}{2}m_\ell}q^{\frac{m}{2}-(m,\ell)-1})(q-1)$

TABLE 8. Weight distribution of $\mathcal{C}_{\ell,2}$.

Remark 4.6. (i) From Tables 5–8 we see that $\mathcal{C}_\ell$ is a 2-weight code, $\mathcal{C}_{\ell,0}$ and $\mathcal{C}_{\ell,1}$ are 5-weight codes, and $\mathcal{C}_{\ell,2}$ is an 11-weight code. Also, one checks that $\mathcal{C}_\ell$ is $q^{\frac{m}{2}-1}(q-1)$-divisible and $\mathcal{C}_{\ell,1}$ is $q^{\frac{m}{2}-1}$-divisible. These facts are in accordance with Klapper's Theorems 2.3 and 2.4 and Remark 3.5.

(ii) In the binary case ($q=2$), the codes $\mathcal{C}_{\mathcal{L},0}$ and $\mathcal{C}_{\mathcal{L},2}$ have symmetric spectrum, that is, $A_i=A_{n-i}$ for every i, since the codeword $(1,1,\dots,1,1)$ belongs to these codes.

Remark 4.7. It can be shown, via Pless power moments, that if $q=2$ and $(m,\ell)=1$ the dual code of $\mathcal{C}_{\ell,1}$ is optimal in the sense that its minimal distance is maximum in the class of cyclic codes with generator polynomial $m_\alpha(x)m_{\alpha^t}(x)$ over $\mathbb{F}_2$. This condition of optimality is equivalent to the function $f(x)=x^t$ defined over $\mathbb{F}_{2^m}$ being an APN function (see [1]). In our case, $f_\ell(x)=x^{2^\ell+1}$, with $(m,\ell)=1$, is a well-known APN function, namely the Kasami–Gold function.

5. Codes associated to $\mathcal{L}_{\ell,3\ell}$

In this section we consider the codes $\mathcal{C}_{\mathcal{L}}$, $\mathcal{C}_{\mathcal{L},0}$, $\mathcal{C}_{\mathcal{L},1}$, and $\mathcal{C}_{\mathcal{L},2}$ associated to the family of p-linearized polynomials

$$\mathcal{L}=\mathcal{L}_{\ell,3\ell}=\langle x^{p^\ell},x^{p^{3\ell}}\rangle\subset\mathbb{F}_{p^m}[x],$$

where p is an odd prime and $m_\ell=m/(m,\ell)$ is even. The next theorem summarizes, in our notation, the results proved in [13].

Theorem 5.1 ([13])**.** *Let p be an odd prime and let m,ℓ be non-negative integers such that $m_\ell=m/(m,\ell)$ is even with $m>6\ell$ and denote $\delta=(m,\ell)$. Then, $\mathcal{L}_{\ell,3\ell}$ is an even rank family with $R_{\mathcal{L}_{\ell,3\ell}}=\{m,m-2\delta,m-4\delta,m-6\delta\}$ (see* (3.5)*). Moreover, the numbers $M_{r,i}$, as defined in* (3.4)*, have the following expressions:*

(a) *If* $\frac{1}{2}m_\ell$ *is odd, then* $M_{m,1} = M_{m-2\delta,2} = M_{m-4\delta,1} = M_{m-6\delta,2} = 0$ *and*

$$M_{m,2} = \frac{p^{2m+6\delta}-p^{2m+4\delta}-p^{2m+\delta}+p^{m+4\delta}+p^{m+\delta}-p^{6\delta}-p^{\frac{3m}{2}+5\delta}+p^{\frac{3m}{2}+4\delta}+p^{\frac{m}{2}+5\delta}-p^{\frac{m}{2}+4\delta}}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1},$$

$$M_{m-2\delta,1} = \frac{p^{2m-2\delta}(p^{7\delta}-p^{2\delta}-1)+p^{m-2\delta}(p^{5\delta}-p^{6\delta}+p^{2\delta}+1)-p^{3\delta}(p^{2\delta}-p^{\delta}+1)+(p^{\frac{3m}{2}}-p^{\frac{m}{2}})S_p(\delta)}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1},$$

$$M_{m-4\delta,2} = \frac{p^{2m-3\delta}(p^{5\delta}+p^{\delta}-1)-p^{m-3\delta}(p^{6\delta}+p^{4\delta}+p^{\delta}-1)+p^{\delta}(p^{2\delta}-p^{\delta}+1)-(p^{\frac{3m}{2}-2\delta}-p^{\frac{m}{2}-2\delta})S_p(\delta)}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1},$$

$$M_{m-6\delta,1} = \frac{p^{2m-3\delta}-p^{m}-p^{m-3\delta}+1+p^{\frac{3m}{2}-\delta}-p^{\frac{3m}{2}-2\delta}-p^{\frac{m}{2}-\delta}+p^{\frac{m}{2}-2\delta}}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1},$$

where $S_p(\delta) = \sum_{i=0}^{5}(-1)^{i+1}p^{i\delta}$.

(b) *If* $\frac{1}{2}m_\ell$ *is even, then* $M_{m,2} = M_{m-2\delta,1} = M_{m-4\delta,2} = M_{m-6\delta,1} = 0$ *and*

$$M_{m,2} = \frac{p^{2m+6\delta}-p^{2m+4\delta}-p^{2m+\delta}+p^{m+4\delta}+p^{m+\delta}-p^{6\delta}+p^{\frac{3m}{2}+5\delta}-p^{\frac{3m}{2}+4\delta}-p^{\frac{m}{2}+5\delta}+p^{\frac{m}{2}+4\delta}}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1},$$

$$M_{m-2\delta,2} = \frac{p^{2m-2\delta}(p^{7\delta}-p^{2\delta}-1)+p^{m-2\delta}(p^{5\delta}-p^{6\delta}+p^{2\delta}+1)-p^{3\delta}(p^{2\delta}-p^{\delta}+1)-(p^{\frac{3m}{2}}-p^{\frac{m}{2}})S_p(\delta)}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1},$$

$$M_{m-4\delta,1} = \frac{p^{2m-3\delta}(p^{5\delta}+p^{\delta}-1)-p^{m-3\delta}(p^{6\delta}+p^{4\delta}+p^{\delta}-1)+p^{\delta}(p^{2\delta}-p^{\delta}+1)+(p^{\frac{3m}{2}-2\delta}-p^{\frac{m}{2}-2\delta})S_p(\delta)}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1},$$

$$M_{m-6d,2} = \frac{p^{2m-3\delta}-p^{m}-p^{m-3\delta}+1-p^{\frac{3m}{2}-\delta}+p^{\frac{3m}{2}-2\delta}+p^{\frac{m}{2}-\delta}-p^{\frac{m}{2}-2\delta}}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}.$$

In [13], the distribution of ranks and types given in the previous theorem was used to calculate the spectra of the codes $\mathcal{C}_{\mathcal{L}}$ and $\mathcal{C}_{\mathcal{L},1}$ with $\mathcal{L} = \mathcal{L}_{\ell,3\ell}$. Fortunately, this information is also enough to calculate the spectra of $\mathcal{C}_{\mathcal{L},0}$ and $\mathcal{C}_{\mathcal{L},2}$, which follows directly from Theorems 3.3, 3.4, and 5.1.

Theorem 5.2. *Let* p *be an odd prime and let* m, ℓ *be positive integers such that* $m_\ell = m/(m,\ell)$ *is even with* $m > 6\ell$. *Then* $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},0}$ *is a* $[n, 2m+1, d]_p$*-code with* $n = p^m - 1$ *and* $d = p^{m-1}(p-1) - d'$, *where*

$$d' = \begin{cases} p^{\frac{m}{2}+3(m,\ell)-1}+1 & \text{if } \frac{1}{2}m_\ell \text{ is even,} \\ (p-1)p^{\frac{m}{2}+3(m,\ell)-1} & \text{if } \frac{1}{2}m_\ell \text{ is odd,} \end{cases}$$

and $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},2}$ *is a* $[n, 3m+1, \hat{d}]_p$*-code with* $\hat{d} = d$ *if* $\frac{1}{2}m_\ell$ *is even and* $\hat{d} = d-1$ *if* $\frac{1}{2}m_\ell$ *is odd. The weight distributions of the codes* $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},0}$ *and* $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},2}$ *are given by Tables 9 and 10 below.*

We set these notations for the next two tables:

$$\begin{aligned} F_0 &= \frac{p^{2m+6\delta}-p^{2m+4\delta}-p^{2m+\delta}+p^{m+4\delta}+p^{m+\delta}-p^{6\delta}+\varepsilon_\ell(p^{\frac{3m}{2}+5\delta}-p^{\frac{3m}{2}+4\delta}-p^{\frac{m}{2}+5\delta}+p^{\frac{m}{2}+4\delta})}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}, \\ F_1 &= \frac{p^{2m-2\delta}(p^{7\delta}-p^{2\delta}-1)+p^{m-2\delta}(p^{5\delta}-p^{6\delta}+p^{2\delta}+1)-p^{3\delta}(p^{2\delta}-p^{\delta}+1)-\varepsilon_\ell(p^{\frac{3m}{2}}-p^{\frac{m}{2}})S_p(\delta)}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}, \\ F_2 &= \frac{p^{2m-3\delta}(p^{5\delta}+p^{\delta}-1)-p^{m-3\delta}(p^{6\delta}+p^{4\delta}+p^{\delta}-1)+p^{\delta}(p^{2\delta}-p^{\delta}+1)+\varepsilon_\ell(p^{\frac{3m}{2}-2\delta}-p^{\frac{m}{2}-2\delta})S_p(\delta)}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}, \\ F_3 &= \frac{p^{2m-3\delta}-p^{m}-p^{m-3\delta}+1-\varepsilon_\ell(p^{\frac{3m}{2}-\delta}-p^{\frac{3m}{2}-2\delta}-p^{\frac{m}{2}-\delta}+p^{\frac{m}{2}-2\delta})}{p^{6\delta}+p^{5\delta}-p^{4\delta}+p^{2\delta}-p^{\delta}-1}, \end{aligned} \tag{5.1}$$

with $S_p(\delta) = \sum_{i=0}^{5}(-1)^{i+1}p^{i\delta}$.

weight	frequency
0	1
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}(p-1)p^{\frac{m}{2}-1}$	F_0
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}(p-1)p^{\frac{m}{2}+(m,\ell)-1}$	F_1
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}(p-1)p^{\frac{m}{2}+2(m,\ell)-1}$	F_2
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}(p-1)p^{\frac{m}{2}+3(m,\ell)-1}$	F_3
$p^m - 1$	$p-1$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}-1} - 1$	$(p-1)F_0$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}+(m,\ell)-1} - 1$	$(p-1)F_1$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}}p^{\frac{m}{2}+2(m,\ell)-1} - 1$	$(p-1)F_2$
$p^m - p^{m-1} + (-1)^{\frac{m_\ell}{2}+1}p^{\frac{m}{2}+3(m,\ell)-1} - 1$	$(p-1)F_3$

TABLE 9. Weight distribution of $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},0}$.

Remark 5.3. The weight distributions of $\mathcal{C}_{\mathcal{L}_{\ell,3\ell}}$ and $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},1}$ are determined by those of $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},0}$ and $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},2}$, respectively. More precisely, the weight distribution of $\mathcal{C}_{\mathcal{L}_{\ell,3\ell}}$ is given by the first 5 rows of Table 9, and the spectrum of $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},1}$ is given by the first 10 rows of Table 10. Therefore, $\mathcal{C}_{\mathcal{L}_{\ell,3\ell}}$ is a 4-weight code, $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},0}$ and $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},1}$ are 9-weight codes, and $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},2}$ is a 19-weight code.

As a direct consequence of Proposition 3.7 we obtain the following result.

Corollary 5.4. *Under the same hypothesis of Theorem 5.2, the complete weight enumerator of $\mathcal{C}_{\mathcal{L}_{\ell,3\ell}}$ is given by*

$$W_{\mathcal{C}_{\mathcal{L}_{\ell,3\ell}}}(z_0,\dots,z_{p-1}) = z_0^{p^m-1} + \sum_{i=0}^{3} F_i\, z_0^{a_i} z_1^{b_i}\cdots z_{p-1}^{b_i}, \tag{5.2}$$

where, for each $i = 0,\dots,3$, the numbers F_i are given in (5.1) *and*

$$a_i = p^{m-1} + (-1)^i \varepsilon_\ell (p-1) p^{\frac{m}{2}+i(m,\ell)-1} - 1,$$
$$b_i = p^{m-1} + (-1)^{i+1} \varepsilon_\ell\, p^{\frac{m}{2}+i(m,\ell)-1}.$$

Proof. By Remark 5.3, the weight enumerator of $\mathcal{C}$ is $W_{\mathcal{C}}(x) = 1 + \sum_{i=0}^{3} R_i\, x^{c_i}$, where

$$c_i = (p-1)\big(p^{m-1} + (-1)^{i+1}\varepsilon_\ell\, p^{\frac{m}{2}+i(m,\ell)+1}\big). \tag{5.3}$$

Thus, by Proposition 3.7, we obtain (5.2), where $a_i = p^m - 1 - c_i$ and $b_i = \frac{c_i}{p-1}$. From these identities and (5.3) we get the desired expressions for a_i and b_i, and thus the result follows. □

weight	frequency
0	1
$p^m - p^{m-1}$	$p^m - 1 + \sum_{i=0}^{3} R_i(p^m - p^{m-i(m,\ell)})$
$p^m - p^{m-1} + (-1)^{\frac{m}{2}+1}(p-1)p^{\frac{m}{2}-1}$	$(p^{m-1} + (-1)^{\frac{m}{2}}(p-1)p^{\frac{m}{2}-1})F_0$
$p^m - p^{m-1} + (-1)^{\frac{m}{2}}(p-1)p^{\frac{m}{2}+(m,\ell)-1}$	$(p^{m-2(m,\ell)-1} + (-1)^{\frac{m}{2}+1}(p-1)p^{\frac{m}{2}-(m,\ell)-1})F_1$
$p^m - p^{m-1} + (-1)^{\frac{m}{2}+1}(p-1)p^{\frac{m}{2}+2(m,\ell)-1}$	$(p^{m-4(m,\ell)-1} + (-1)^{\frac{m}{2}}(p-1)p^{\frac{m}{2}-2(m,\ell)-1})F_2$
$p^m - p^{m-1} + (-1)^{\frac{m}{2}}(p-1)p^{\frac{m}{2}+3(m,\ell)-1}$	$(p^{m-6(m,\ell)-1} + (-1)^{\frac{m}{2}+1}(p-1)p^{\frac{m}{2}-3(m,\ell)-1})F_3$
$p^m - p^{m-1} + (-1)^{\frac{m}{2}}p^{\frac{m}{2}-1}$	$(p^{m-1} + (-1)^{\frac{m}{2}+1}p^{\frac{m}{2}-1})(p-1)F_0$
$p^m - p^{m-1} + (-1)^{\frac{m}{2}+1}p^{\frac{m}{2}+(m,\ell)-1}$	$(p^{m-2(m,\ell)-1} + (-1)^{\frac{m}{2}}p^{\frac{m}{2}-(m,\ell)-1})(p-1)F_1$
$p^m - p^{m-1} + (-1)^{\frac{m}{2}}p^{\frac{m}{2}+2(m,\ell)-1}$	$(p^{m-4(m,\ell)-1} + (-1)^{\frac{m}{2}+1}p^{\frac{m}{2}-2(m,\ell)-1})(p-1)F_2$
$p^m - p^{m-1} + (-1)^{\frac{m}{2}+1}p^{\frac{m}{2}+3(m,\ell)-1}$	$(p^{m-6(m,\ell)-1} + (-1)^{\frac{m}{2}}p^{\frac{m}{2}-3(m,\ell)-1})(p-1)F_3$
$p^m - 1$	$p-1$
$p^m - p^{m-1} - 1$	$(p-1)(p^m - 1 + \sum_{i=0}^{3} R_i(p^m - p^{m-i(m,\ell)}))$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m}{2}+1}(p-1)p^{\frac{m}{2}-1}$	$(p^{m-1} + (-1)^{\frac{m}{2}+1}p^{\frac{m}{2}-1})(p-1)F_0$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m}{2}}(p-1)p^{\frac{m}{2}+(m,\ell)-1}$	$(p^{m-2(m,\ell)-1} + (-1)^{\frac{m}{2}}p^{\frac{m}{2}-(m,\ell)-1})(p-1)F_1$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m}{2}+1}(p-1)p^{\frac{m}{2}+2(m,\ell)-1}$	$(p^{m-4(m,\ell)-1} + (-1)^{\frac{m}{2}+1}p^{\frac{m}{2}-2(m,\ell)-1})(p-1)F_2$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m}{2}}(p-1)p^{\frac{m}{2}+3(m,\ell)-1}$	$(p^{m-6(m,\ell)-1} + (-1)^{\frac{m}{2}}p^{\frac{m}{2}-3(m,\ell)-1})(p-1)F_3$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m}{2}}p^{\frac{m}{2}-1}$	$(p^m - p^{m-1} + (-1)^{\frac{m}{2}}p^{\frac{m}{2}-1})(p-1)F_0$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m}{2}+1}p^{\frac{m}{2}+(m,\ell)-1}$	$(p^{m-2(m,\ell)} - p^{m-2(m,\ell)-1} + (-1)^{\frac{m}{2}+1}p^{\frac{m}{2}-(m,\ell)-1})(p-1)F_1$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m}{2}}p^{\frac{m}{2}+2(m,\ell)-1}$	$(p^{m-4(m,\ell)} - p^{m-4(m,\ell)-1} + (-1)^{\frac{m}{2}}p^{\frac{m}{2}-2(m,\ell)-1})(p-1)F_2$
$p^m - p^{m-1} - 1 + (-1)^{\frac{m}{2}+1}p^{\frac{m}{2}+3(m,\ell)-1}$	$(p^{m-6(m,\ell)} - p^{m-6(m,\ell)-1} + (-1)^{\frac{m}{2}+1}p^{\frac{m}{2}-3(m,\ell)-1})(p-1)F_3$

TABLE 10. Weight distribution of $\mathcal{C}_{\mathcal{L}_{\ell,3\ell},2}$.

6. Optimal curves

Fix $q = p^m$ with p prime. In this section we will consider Artin–Schreier curves of the form

$$C_{R,\beta} : \quad y^p - y = xR(x) + \beta x, \tag{6.1}$$

where $R(x)$ is any p-linearized polynomial over $\mathbb{F}_q$ and $\beta \in \mathbb{F}_q$. A good treatment of Artin–Schreier curves is given by Güneri and Özbudak in [6]. They are associated to the codes $\mathcal{C}_{\mathcal{L},*}$ studied in Sections 3–5, which are defined by quadratic forms $Q_R(x) = \mathrm{Tr}_{p^m/p}(xR(x))$, or similar ones, of Section 2. Given a family $\mathcal{L}$ of p-linearized polynomials, we define the family

$$\Gamma_{\mathcal{L}} = \{C_{R,\beta} : R \in \mathcal{L}, \beta \in \mathbb{F}_q\} \tag{6.2}$$

of curves $C_{R,\beta}$ as in (6.1).

We begin by showing necessary and sufficient conditions for the family $\mathcal{L}$ to contain optimal curves (maximal or minimal); that is, curves attaining equality in the Hasse–Weil bound (see [11, Theorem 5.2.3])

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

Proposition 6.1. *Assume $\mathcal{L}$ is an even rank family of p-linearized polynomials over $\mathbb{F}_{p^m}$. Let $R \in \mathcal{L}$, r be the rank of the quadratic form $Q_R(x) = \mathrm{Tr}_{p^m/p}(xR(x))$,*

and $v = v_p(\deg R)$ *be the* p*-adic value of* $\deg R$*. Then, the family* $\Gamma_{\mathcal{L}}$ *in* (6.2) *contains optimal curves, both maximal and minimal, if and only if there is some* $R \in \mathcal{L}$ *with*

$$v = \frac{m-r}{2}.$$

In this case we have:

(i) *If* p *is odd, the curve* $C_{R,\beta} \in \Gamma_{\mathcal{L}}$ *is maximal (resp. minimal) if and only if the codeword* $c_R(\beta) = (\mathrm{Tr}_{p^m/p}(xR(x)+\beta x))_{x\in\mathbb{F}_{p^m}^*}$ *in* $\mathcal{C}_{\mathcal{L},1}$ *has weight* $w(c_R(\beta)) = w_{2,1}$ *(resp.* $w_{2,2}$*) as in Table 3.*

(ii) *If* $p = 2$*, the curve* $C_{R,\beta} \in \Gamma_{\mathcal{L}}$ *is maximal (resp. minimal) if and only if either* $w(c_R(\beta)) = w_{2,1}$ *(resp.* $w_{2,2}$*) or else* $w(c_R(\beta)) = w_{3,2}$ *(resp.* $w_{3,1}$*) as in Table 3.*

Proof. Consider the cyclic code $\mathcal{C}_{\mathcal{L},1} = \{c_R(\beta) : R \in \mathcal{L},\ \beta \in \mathbb{F}_{p^m}\}$ as in (3.2), where $c_R(\beta) = (\mathrm{Tr}_{p^m/p}(xR(x)+\beta x))_{x\in\mathbb{F}_{p^m}^*}$. The weight of the codeword $c_R(\beta)$ is related to the number of $\mathbb{F}_{p^m}$-rational points of the curve $C_{R,\beta}$ given in (6.1). In fact, by Hilbert's Theorem 90 we have

$$\mathrm{Tr}_{p^m/p}(xR(x)+\beta x) = 0 \quad \Leftrightarrow \quad y^p - y = xR(x) + \beta x \ \text{ for some } y \in \mathbb{F}_{p^m}.$$

Since $C_{R,\beta}$ is a p-covering of $\mathbb{P}^1$, considering the point at infinity, we get

$$\begin{aligned} \#C_{R,\beta}(\mathbb{F}_{p^m}) &= 1 + p\,\#\{x \in \mathbb{F}_{p^m} : \mathrm{Tr}_{p^m/p}(xR(x)+\beta x) = 0\} \\ &= p^{m+1} + 1 - p\,w(c_R(\beta)), \end{aligned} \tag{6.3}$$

where the values of $w(c_R(\beta))$ are given in Table 3 with $q = p$.

On the other hand, as an application of the Riemann–Hurwitz formula, the curve $y^p - y = f(x)$ with $f(x) \in \mathbb{F}_q[x]$ has genus $g = \frac{1}{2}(p-1)(\deg f)$, since the degree of f is coprime with p (see [6, Example 2.4]). Hence, $C_{R,\beta}$ has genus

$$g(C_{R,\beta}) = \tfrac{1}{2}(p-1)(\deg R) = \tfrac{1}{2}(p-1)p^v,$$

since for $R \neq 0$ we have

$$(\deg xR(x) + \beta x, p) = (p^v + 1, p) = 1.$$

By the Hasse–Weil bound for curves we have that

$$p^m + 1 - (p-1)p^{v+\frac{m}{2}} \leq \#C_R(\mathbb{F}_{p^m}) \leq p^m + 1 + (p-1)p^{v+\frac{m}{2}}. \tag{6.4}$$

To find maximal or minimal curves we need to ensure equality in the above inequalities; that is, by (6.3) and (6.4) we want that

$$p^{m+1} - p\,w(c_R(\beta)) = p^m \pm (p-1)p^{v+\frac{m}{2}},$$

where the sign + (resp. −) corresponds to a maximal (resp. minimal) curve. By looking at Table 3 with $q = p$, we check that this could only happen if and only if $v = \frac{m-r}{2}$ and the weight $w(c_R(\beta))$ is $w_{2,1}$ (resp. $w_{2,2}$) for a maximal (resp. minimal) curve. Because of the presence of the factors $p-1$ in the weights, additional curves appear in the case $p = 2$. They correspond to $w(c_R(\beta)) = w_{3,2}$ (resp. $w_{3,1}$) for a maximal (resp. minimal) curve. Since the type of the quadratic form is fixed, only one of the two kinds of maximal (or minimal) curves can appear if $p = 2$. □

Next, as an application of the spectrum of cyclic codes, for a fixed number ℓ we consider the Artin–Schreier curves

$$\begin{aligned} C_{\gamma,\beta} &: y^p - y = \gamma x^{p^\ell+1} + \beta x, && \gamma \in \mathbb{F}_{p^m}^*,\ \beta \in \mathbb{F}_{p^m}, \\ C_{\gamma_1,\gamma_2,\beta} &: y^p - y = \gamma_1 x^{p^{3\ell}+1} + \gamma_2 x^{p^\ell+1} + \beta x, && \gamma_1,\gamma_2 \in \mathbb{F}_{p^m}^*,\ \beta \in \mathbb{F}_{p^m}, \end{aligned} \tag{6.5}$$

related to the codes $\mathcal{C}_{\ell,1}$ and $\mathcal{C}_{\{\ell,3\ell\},1}$ of Sections 4 and 5, respectively, and we will show that the families $\{C_{\gamma,\beta}\}$ and $\{C_{\gamma_1,\gamma_2,\beta}\}$ contain several maximal and minimal curves.

We begin by computing the $\mathbb{F}_{p^m}$-rational points of the curves in the first family $\{C_{\gamma,\beta}\}$.

Proposition 6.2. *Let m and ℓ be positive integers such that m_ℓ is even and let p be a prime number. Consider the curve $C_{\gamma,\beta}$ as in* (6.5) *with $\gamma \in \mathbb{F}_{p^m}^*$ and $\beta \in \mathbb{F}_{p^m}$. Fix $\gamma = \alpha^t$ and put $\varepsilon_\ell = (-1)^{\frac{1}{2}m_\ell}$. Then we have:*

(a) *If $p > 2$, with $\frac{1}{2}m_\ell$ even and $t \equiv 0 \pmod{p^{(m,\ell)}+1}$, then*

$$\#C_{\gamma,\beta}(\mathbb{F}_{p^m}) = \begin{cases} p^m + 1 & \text{for } p^m - p^{m-2(m,\ell)}\ \beta\text{'s}, \\ p^m + 1 - p^{(m,\ell)}(p-1)p^{\frac{m}{2}} & \text{for } p^{m-2(m,\ell)-1} - (p-1)p^{\frac{m}{2}-(m,\ell)-1}\ \beta\text{'s}, \\ p^m + 1 + p^{(m,\ell)}p^{\frac{m}{2}} & \text{for } (p^{m-2(m,\ell)-1} + p^{\frac{m}{2}-(m,\ell)-1})(p-1)\ \beta\text{'s}. \end{cases}$$

(b) *If $p > 2$, with $\frac{1}{2}m_\ell$ even and $t \not\equiv 0 \pmod{p^{(m,\ell)}+1}$, then*

$$\#C_{\gamma,\beta}(\mathbb{F}_{p^m}) = \begin{cases} p^m + 1 + (p-1)p^{\frac{m}{2}} & \text{for } p^{m-1} + (p-1)p^{\frac{m}{2}}\ \beta\text{'s}, \\ p^m + 1 - p^{\frac{m}{2}} & \text{for } (p-1)(p^{m-1} - p^{\frac{m}{2}-1})\ \beta\text{'s}. \end{cases}$$

(c) *If $p > 2$, with $\frac{1}{2}m_\ell$ odd and $t \equiv \frac{p^{(m,\ell)}+1}{2} \pmod{p^{(m,\ell)}+1}$, then*

$$\#C_{\gamma,\beta}(\mathbb{F}_{p^m}) = \begin{cases} p^m + 1 & \text{for } p^m - p^{m-2(m,\ell)}\ \beta\text{'s}, \\ p^m + 1 + p^{(m,\ell)}(p-1)p^{\frac{m}{2}} & \text{for } p^{m-2(m,\ell)-1} + (p-1)p^{\frac{m}{2}-(m,\ell)-1}\ \beta\text{'s}, \\ p^m + 1 - p^{(m,\ell)}p^{\frac{m}{2}} & \text{for } (p^{m-2(m,\ell)-1} - p^{\frac{m}{2}-(m,\ell)-1})(p-1)\ \beta\text{'s}. \end{cases}$$

(d) *If $p > 2$, with $\frac{1}{2}m_\ell$ odd and $t \not\equiv \frac{p^{(m,\ell)}+1}{2} \pmod{p^{(m,\ell)}+1}$, then*

$$\#C_{\gamma,\beta}(\mathbb{F}_{p^m}) = \begin{cases} p^m + 1 - (p-1)p^{\frac{m}{2}} & \text{for } p^{m-1} - (p-1)p^{\frac{m}{2}-1}\ \beta\text{'s}, \\ p^m + 1 + p^{\frac{m}{2}} & \text{for } (p^{m-1} + p^{\frac{m}{2}-1})(p-1)\ \beta\text{'s}. \end{cases}$$

(e) *If $p = 2$ and $\gamma \in S_{2,m}(\ell) = \{x^{2^\ell+1} : x \in \mathbb{F}_{2^m}^*\}$ then*

$$\#C_{\gamma,\beta}(\mathbb{F}_{2^m}) = \begin{cases} 2^m + 1 & \text{for } 2^m - 2^{m-2(m,\ell)}\ \beta\text{'s}, \\ 2^m + 1 - \varepsilon_\ell\, 2^{\frac{m}{2}+(m,\ell)} & \text{for } 2^{m-2(m,\ell)-1} - \varepsilon_\ell\, 2^{\frac{m}{2}-(m,\ell)-1}\ \beta\text{'s}, \\ 2^m + 1 + \varepsilon_\ell\, 2^{\frac{m}{2}+(m,\ell)} & \text{for } 2^{m-2(m,\ell)-1} + \varepsilon_\ell\, 2^{\frac{m}{2}-(m,\ell)-1}\ \beta\text{'s}. \end{cases}$$

(f) *If $p = 2$ and $\gamma \notin S_{2,m}(\ell)$ then*

$$\#C_{\gamma,\beta}(\mathbb{F}_{2^m}) = \begin{cases} 2^m + 1 + \varepsilon_\ell\, 2^{\frac{m}{2}} & \text{for } 2^{m-1} + \varepsilon_\ell\, 2^{\frac{m}{2}-1}\ \beta\text{'s}, \\ 2^m + 1 - \varepsilon_\ell\, 2^{\frac{m}{2}} & \text{for } 2^{m-1} - \varepsilon_\ell\, 2^{\frac{m}{2}-1}\ \beta\text{'s}. \end{cases}$$

Proof. Consider the code $\mathcal{C}_{\ell,1} = \{c_{\gamma,\beta} = (\mathrm{Tr}_{p^m/p}(\gamma x^{p^\ell+1}+\beta x))_{x\in\mathbb{F}_{p^m}^*} : \gamma,\beta \in \mathbb{F}_{p^m}\}$. By the same argument as in the previous proof, we have that

$$\#C_{\gamma,\beta}(\mathbb{F}_{p^m}) = p^{m+1} + 1 - p\, w(c_{\gamma,\beta}).$$

Thus, the number of rational points of $C_{\gamma,\beta}$ is obtained from Tables 5–8, using Theorems 2.3 and 2.4, by straightforward calculations. □

We now show the existence of optimal curves in the family $\{C_{\gamma,\beta}\}$. We will use Proposition 6.1 to prove the existence of optimal curves and Proposition 6.2 to count them.

Theorem 6.3. *Let p be a prime number. Let m and ℓ be non-negative integers with $\ell \,|\, m$ such that $m_\ell = \frac{m}{\ell}$ is even and $\gamma = \alpha^t \in \mathbb{F}_{p^m}$. Then we have:*

(a) *Let p be odd. Then the curve $C_{\gamma,\beta}$ as in* (6.5) *is*
  (i) *minimal if $\frac{1}{2}m_\ell$ is even and $t \equiv 0 \pmod{p^\ell+1}$, for $p^{m-2\ell-1} - (p-1)p^{\frac{m}{2}-\ell-1}$ elements β;*
  (ii) *maximal if $\frac{1}{2}m_\ell$ is odd and $t \equiv \frac{p^\ell+1}{2} \pmod{p^\ell+1}$, for $p^{m-2\ell-1} + (p-1)p^{\frac{m}{2}-\ell-1}$ elements β.*

(b) *Let $p = 2$ and $\gamma \in S_{2,m}(\ell) = \{x^{2^\ell+1} : x \in \mathbb{F}_{2^m}^*\}$. Then,*
  (i) *there are $2^{m-2\ell-1} - 2^{\frac{m}{2}-\ell-1}$ elements β such that $C_{\gamma,\beta}$ is minimal;*
  (ii) *there are $2^{m-2\ell-1} + 2^{\frac{m}{2}-\ell-1}$ elements β such that $C_{\gamma,\beta}$ is maximal.*

Proof. Consider the family $\mathcal{L} = \langle x^{p^\ell}\rangle$ of p-linearized polynomials over $\mathbb{F}_{p^m}$, with p prime. By Klapper's Theorems 2.3 and 2.4, $\mathcal{L}$ is an even rank family. Thus, the family of curves $\Gamma_{\mathcal{L}}$ in (6.1) is in fact the family $\{C_{\gamma,\beta}\}$ in (6.5). Now, applying Proposition 6.1, by using Tables 3 and 7 and Theorems 2.3 and 2.4, we get the existence part of the statement. Finally, invoking Proposition 6.2 we get the number of such optimal curves. □

Example 6.4. Suppose that $p = 2$, $m = 4$, and $\ell = 1$. Consider the curve

$$C_{\gamma,\beta} : y^2 + y = \gamma x^3 + \beta x, \quad \gamma \in \mathbb{F}_{16}^*,\ \beta \in \mathbb{F}_{16},$$

which is in particular an elliptic curve. Suppose that $\gamma \in S_{2,4}(1) = \{x^3 : x \in \mathbb{F}_{16}^*\}$. Then, by Theorem 6.3, $C_{\gamma,\beta}$ is minimal for only one element β and it is maximal for 3 elements β.

If $\gamma = z^3$ for some $z \in \mathbb{F}_{16}^*$ then, by the affine change of variable $u = zx$, the curve $C_{\gamma,\beta}$ turns out to be isomorphic to the curve

$$C_{1,\lambda} : y^2 + y = u^3 + \lambda u,$$

where $\lambda = \beta z^{-1}$. This curve is minimal (9 rational points) only for $\lambda = 0$ and it is maximal (25 rational points) for $\lambda = 1$, α^5, and α^{10}. That is,

$$y^2 + y = u^3$$

is a minimal elliptic curve and

$$y^2 + y = u^3 + u, \qquad y^2 + y = u^3 + \alpha^5 u, \qquad y^2 + y = u^3 + \alpha^{10} u$$

are maximal elliptic curves over $\mathbb{F}_{16}$.

We now show that the family $\{C_{\gamma_1,\gamma_2,\beta}\}$ contains optimal curves.

Proposition 6.5. *Let p be an odd prime and let m, ℓ be non-negative integers such that $\ell \,|\, m$, $m_\ell = \frac{m}{\ell}$ is even, and $m > 6\ell$. If $\frac{1}{2}m_\ell$ is odd (resp. even), the Artin–Schreier curve $C_{\gamma_1,\gamma_2,\beta}$ as in* (6.5) *is maximal (resp. minimal) for some $\gamma_1, \gamma_2 \in \mathbb{F}_{p^m}^*$ and $\beta \in \mathbb{F}_{p^m}$.*

Proof. The family $\mathcal{L} = \langle x^{p^\ell}, x^{3\ell}\rangle$ of p-linearized polynomials over $\mathbb{F}_{p^m}$ has the even rank property, by Theorem 5.1. By Table 10 and Theorem 5.2, we have that if $\frac{1}{2}m_\ell$ is odd (resp. even) then there exists $R \in \mathcal{L}$ with $\deg R = p^{3\ell}$ and Q_R of rank $r = m - 6\ell$ and type 1 (resp. 3). Thus, we have that

$$v = \tfrac{m-r}{2} = 3\ell,$$

where $v = v_p(\deg R)$, and the result follows directly from Proposition 6.1. □

Example 6.6. Take p an odd prime, $\ell = 1$, and $m > 6$ even. Then, the Artin–Schreier curve

$$y^p - y = \gamma_1 x^{p^3+1} + \gamma_2 x^{p+1} + \beta x$$

is maximal in $\mathbb{F}_{p^{4k}}$ and minimal in $\mathbb{F}_{p^{4k+2}}$ for any $k \geq 2$, for at least one $\gamma_1, \gamma_2 \in \mathbb{F}_{p^m}^*$ and $\beta \in \mathbb{F}_{p^m}$, where $\mathbb{F}_{p^m}$ stands for $\mathbb{F}_{p^{4k}}$ or $\mathbb{F}_{p^{4k+2}}$ depending on the case.

For instance,

$$y^3 - y = \gamma_1 x^{28} + \gamma_2 x^4 + \beta x$$

is maximal in $\mathbb{F}_{3^8} = \mathbb{F}_{6561}$ and minimal in $\mathbb{F}_{3^{10}} = \mathbb{F}_{59049}$ for at least one $\gamma_1, \gamma_2, \beta$ in the corresponding field. Similarly,

$$y^5 - y = \gamma_1 x^{125} + \gamma_2 x^6 + \beta x$$

is maximal in $\mathbb{F}_{5^8} = \mathbb{F}_{390625}$ and minimal in $\mathbb{F}_{5^{10}} = \mathbb{F}_{9765625}$ for some elements $\gamma_1, \gamma_2, \beta$ in the ground field.

References

[1] P. Charpin, Open problems on cyclic codes, in *Handbook of coding theory, Vol. I, II*, 963–1063, North-Holland, Amsterdam, 1998. MR 1667947.

[2] P. Delsarte, On subfield subcodes of modified Reed-Solomon codes, *IEEE Trans. Inform. Theory* **21** (1975), no. 5, 575–576. MR 0411819.

[3] H. Q. Dinh, C. Li and Q. Yue, Recent progress on weight distributions of cyclic codes over finite fields, *J. Algebra Comb. Discrete Struct. Appl.* **2** (2015), no. 1, 39–63. MR 3319695.

[4] K. Feng and J. Luo, Weight distribution of some reducible cyclic codes, *Finite Fields Appl.* **14** (2008), no. 2, 390–409. MR 2401983.

[5] K. Feng and J. Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, *IEEE Trans. Inform. Theory* **53** (2007), no. 9, 3035–3041. MR 2417669.

[6] C. Güneri and F. Özbudak, Artin-Schreier extensions and their applications, in *Topics in geometry, coding theory and cryptography*, 105–133, Algebr. Appl., 6, Springer, Dordrecht, 2007. MR 2278036.

[7] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003. MR 1996953.

[8] A. Klapper, Cross-correlations of geometric sequences in characteristic two, *Des. Codes Cryptogr.* **3** (1993), no. 4, 347–377. MR 1232065.

[9] A. Klapper, Cross-correlations of quadratic form sequences in odd characteristic, *Des. Codes Cryptogr.* **11** (1997), no. 3, 289–305. MR 1451733.

[10] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, 20, Addison-Wesley, Advanced Book Program, Reading, MA, 1983. MR 0746963.

[11] H. Stichtenoth, *Algebraic function fields and codes*, second edition, Graduate Texts in Mathematics, 254, Springer-Verlag, Berlin, 2009. MR 2464941.

[12] G. van der Geer and M. van der Vlugt, Reed-Muller codes and supersingular curves. I, *Compositio Math.* **84** (1992), no. 3, 333–367. MR 1189892.

[13] D. Zheng et al., The weight distributions of two classes of p-ary cyclic codes, *Finite Fields Appl.* **29** (2014), 202–224. MR 3225389.

[14] Z. Zhou et al., The weight enumerator of three families of cyclic codes, *IEEE Trans. Inform. Theory* **59** (2013), no. 9, 6002–6009. MR 3096974.

Ricardo A. Podestá✉
CIEM, Universidad Nacional de Córdoba, CONICET, FAMAF, Av. Medina Allende 2144, Ciudad Universitaria, 5000 Córdoba, República Argentina
`podesta@famaf.unc.edu.ar`

Denis E. Videla
CIEM, Universidad Nacional de Córdoba, CONICET, FAMAF, Av. Medina Allende 2144, Ciudad Universitaria, 5000 Córdoba, República Argentina
`devidela@famaf.unc.edu.ar`

Received: November 28, 2019
Accepted: April 9, 2020