Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Finite Fields and Their Applications 14 (2008) 44–58

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Multidimensional cyclic codes and Artin–Schreier type hypersurfaces over finite fields

Cem Güneri [a], Ferruh Özbudak [b,*]

[a] *Faculty of Engineering and Natural Sciences, Sabancı University, Tuzla, 34956 İstanbul, Turkey*
[b] *Department of Mathematics, Middle East Technical University, İnönü Bulvarı, 06531 Ankara, Turkey*

Received 3 March 2006; revised 27 October 2006

Available online 17 December 2006

Communicated by H. Stichtenoth

Abstract

We obtain a trace representation for multidimensional cyclic codes via Delsarte's theorem. This relates the weights of the codewords to the number of affine rational points of Artin–Schreier type hypersurfaces over finite fields. Using Deligne's and Hasse–Weil–Serre inequalities we get bounds on the minimum distance. Comparison of the bounds is made and illustrated by examples. Some applications of our results are given. We obtain a bound on certain character sums over $\mathbb{F}_2$ which gives better estimates than Deligne's inequality in some cases. We also improve the minimum distance bounds of Moreno–Kumar on p-ary subfield subcodes of generalized Reed–Muller codes for some parameters.

Keywords: Multidimensional cyclic code; Artin–Schreier type hypersurface; Deligne's inequality; Hasse–Weil–Serre inequality

1. Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^e$. Multidimensional cyclic codes are natural generalizations of usual cyclic codes to many variables. Namely, a q-ary ℓ-D cyclic code of volume (length) $n_1 \times \cdots \times n_\ell$ is an ideal of the quotient ring $\mathbb{F}_q[x_1, \ldots, x_\ell]/(x_1^{n_1} - 1, \ldots, x_\ell^{n_\ell} - 1)$, where $n_1, \ldots, n_\ell$ are positive integers which are usually assumed to be relatively prime

[*] Corresponding author.
E-mail addresses: guneri@sabanciuniv.edu (C. Güneri), ozbudak@metu.edu.tr (F. Özbudak).

1071-5797/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2006.12.003

to q. Structure and minimum distance bounds for these codes are studied, for example, in [1, 7–10,13–17].

We fix integers $\ell \geqslant 1$, $m \geqslant 2$ and $n_1, n_2, \ldots, n_\ell \geqslant 1$ such that $n_t \mid (q^m - 1)$ for each $1 \leqslant t \leqslant \ell$. In this paper we obtain a natural trace representation for q-ary ℓ-D cyclic codes of volume $n_1 \times \cdots \times n_\ell$ using a corresponding finite set of multivariate polynomials over $\mathbb{F}_{q^m}$. This representation leads to consideration of Artin–Schreier type hypersurfaces of the form $y^q - y = f(x_1, \ldots, x_\ell)$, where $f(x_1, \ldots, x_\ell) \in \mathbb{F}_{q^m}[x_1, \ldots, x_\ell]$. We obtain a minimum distance bound using Deligne's inequality [2, Proposition 3.8]. Under restrictive conditions, we obtain another bound on the minimum distance using Hasse–Weil–Serre inequality [19, Theorem V.3.1]. We compare these bounds and we observe that when both of these apply, the bound from Hasse–Weil–Serre inequality gives better results. In this way, for $q = 2$ we also obtain an improvement of Deligne's character sum inequality [2, Proposition 3.8] in some cases. Some applications of our results are also provided. We improve the minimum distance bounds of Moreno–Kumar on p-ary subfield subcodes of generalized Reed–Muller codes in Example 4.1. We obtain bounds on the minimum distance of a class of 2-D cyclic codes in Example 4.2, to which the results of [7] cannot be applied. Using the methods here, an extension of [7, Theorem 6.1] is obtained in Example 4.3.

The paper is organized as follows. In Section 2 we give the trace representation. Minimum distance bounds from Deligne's and Hasse–Weil–Serre inequalities are given in Section 3. The applications are presented in Section 4.

The following notation will be fixed throughout the paper. Let Ω be the set $\{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_\ell - 1\}$. An element $(i_1, \ldots, i_\ell)$ of Ω is denoted as $\boldsymbol{i}$. We denote the monomial $x_1 \cdots x_\ell$ as $\boldsymbol{x}$. Moreover for each $\boldsymbol{i} = (i_1, \ldots, i_\ell) \in \Omega$, the monomial $x_1^{i_1} \cdots x_\ell^{i_\ell}$ is denoted as $\boldsymbol{x}^{\boldsymbol{i}}$ in short. For $1 \leqslant t \leqslant \ell$, we fix a primitive n_tth root of unity $\zeta_t \in \mathbb{F}_{q^m}$ and denote $(\zeta_1, \ldots, \zeta_\ell)$ by $\boldsymbol{\zeta}$. Similarly, $(\zeta_1^{i_1}, \ldots, \zeta_\ell^{i_\ell})$ is denoted by $\boldsymbol{\zeta}^{\boldsymbol{i}}$. The ideal $\langle x_1^{n_1} - 1, \ldots, x_\ell^{n_\ell} - 1\rangle$ of $\mathbb{F}_q[x_1, \ldots, x_\ell]$ is denoted by $\mathfrak{a}$. We let $R = \mathbb{F}_q[x_1, \ldots, x_\ell]/\mathfrak{a}$ and represent its elements as $f(\boldsymbol{x}) + \mathfrak{a}$, where

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{j} \in \Omega} a_{\boldsymbol{j}} \boldsymbol{x}^{\boldsymbol{j}} \in \mathbb{F}_q[x_1, \ldots, x_\ell].$$

Evaluation of $f(\boldsymbol{x})$ at $\boldsymbol{\zeta}^{\boldsymbol{i}}$ is denoted by $f(\boldsymbol{\zeta}^{\boldsymbol{i}})$. Note that R can be identified with the space $\mathbb{F}_q^{n_1 \times \cdots \times n_\ell}$ of q-ary $n_1 \times \cdots \times n_\ell$ arrays (or vectors of length $n_1 \cdots n_\ell$) via the map

$$\sum_{\boldsymbol{j} \in \Omega} a_{\boldsymbol{j}} \boldsymbol{x}^{\boldsymbol{j}} + \mathfrak{a} \mapsto (a_{\boldsymbol{j}})_{\boldsymbol{j} \in \Omega}. \tag{1.1}$$

Using this identification, we will represent the codewords of ℓ-D cyclic codes as cosets of polynomials or arrays ((2.4) and Remark 3.2, respectively). For a nonempty subset S of Ω, we set

$$\mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in S\} = \left\{\sum_{\boldsymbol{i} \in S} \lambda_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}}\colon \lambda_{\boldsymbol{i}} \in \mathbb{F}_q\right\}.$$

The space $\mathrm{Span}_{\mathbb{F}_{q^m}}\{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in S\}$ is defined similarly. Finally, we use the symbols tr_m and Tr_m to denote the trace maps from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$ and $\mathbb{F}_p$, respectively.

2. Trace representation

In this section we give some basic results on q-ary ℓ-D cyclic codes of volume $n_1 \times \cdots \times n_\ell$ and we obtain a trace representation using Delsarte's theorem [3]. First we define an action of the cyclic group of order m on Ω. For $\boldsymbol{i} \in \Omega$, let $q\boldsymbol{i} = (j_1, \ldots, j_\ell)$ be the element of Ω given by

$$j_t \equiv q i_t \mod n_t \quad \text{for } 1 \leqslant t \leqslant \ell. \tag{2.1}$$

A subset of Ω is called closed if it is a union of some orbits of this action. The empty set is also considered as a closed set. Let $\mathcal{U}$ be the collection of all such closed subsets of Ω throughout. Note that for $U \in \mathcal{U}$, the complement $U^c = \Omega \setminus U$ and $-U = \{-\boldsymbol{i}\colon -\boldsymbol{i} \in U\}$ are also closed sets, where $-\boldsymbol{i} = (j_1, \ldots, j_\ell)$ such that $j_t \equiv -i_t \bmod n_t$ for $1 \leqslant t \leqslant \ell$.

Proposition 2.1. *There is a one-to-one correspondence between the q-ary ℓ-D cyclic codes of volume $n_1 \times \cdots \times n_\ell$ and the elements of $\mathcal{U}$. For an element $U \in \mathcal{U}$, the corresponding q-ary ℓ-D cyclic code C_U is*

$$C_U = \{f(\boldsymbol{x}) + \mathfrak{a} \in R\colon\ f(\boldsymbol{\zeta}^{\boldsymbol{i}}) = 0 \textit{ for each } \boldsymbol{i} \in U\}. \tag{2.2}$$

Conversely for a q-ary ℓ-D cyclic code C of volume $n_1 \times \cdots \times n_\ell$, the corresponding closed set $Z(C) \in \mathcal{U}$ is

$$Z(C) = \{\boldsymbol{i} \in \Omega\colon\ f(\boldsymbol{\zeta}^{\boldsymbol{i}}) = 0 \textit{ for each } f(\boldsymbol{x}) + \mathfrak{a} \in C\}. \tag{2.3}$$

Proof. See [6, Proposition 2.12]. □

For an ℓ-D cyclic code C, the closed set $Z(C)$ given in (2.3) is called the zero set of C. For $Z(C) \neq \emptyset$, a subset of $Z(C)$ consisting of exactly one representative from each orbit of the action (2.1) in $Z(C)$ is called a basic zero set (of C or $Z(C)$) in Ω.

For a q-ary ℓ-D cyclic code C of volume $n_1 \times \cdots \times n_\ell$, the dual

$$C^\perp = \left\{\sum_{\boldsymbol{i} \in \Omega} b_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} + \mathfrak{a} \in R\colon\ \sum_{\boldsymbol{i} \in \Omega} a_{\boldsymbol{i}} b_{\boldsymbol{i}} = 0 \text{ for each } \sum_{\boldsymbol{i} \in \Omega} a_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} + \mathfrak{a} \in C\right\}$$

is also a q-ary ℓ-D cyclic code of the same volume.

Proposition 2.2. *Let U be the zero set of an ℓ-D cyclic code C and $C^\perp$ be the dual code. We have that* $\dim_{\mathbb{F}_q}(C) = |U^c|$ *and* $Z(C^\perp) = -(U^c)$.

Proof. The proof follows from [6, Theorem 2.17] and [6, Proposition 2.20]. □

Remark 2.3. The results above also hold when $m = 1$. Note that the action (2.1) is trivial and any subset of Ω is closed in this case. Hence for any $m \geqslant 1$, there is a one-to-one correspondence between q^m-ary ℓ-D cyclic codes of volume $n_1 \times \cdots \times n_\ell$ and all subsets of Ω.

Note that if $U = \Omega$, then the corresponding ℓ-D cyclic code is the trivial code $\{0 + \mathfrak{a}\} \subseteq R$. The next theorem gives a natural representation for nontrivial ℓ-D cyclic codes using polynomials from $\mathbb{F}_{q^m}[\boldsymbol{x}]$.

Theorem 2.4. *For $U \in \mathcal{U} \setminus \{\Omega\}$, let C_U be the corresponding ℓ-D cyclic code over $\mathbb{F}_q$ of volume $n_1 \times \cdots \times n_\ell$. If I is a basic zero set of $-(U^c)$ (or $C^\perp$), then we have*

$$C_U = \left\{ \sum_{\boldsymbol{j} \in \Omega} \operatorname{tr}_m\bigl(f\bigl(\boldsymbol{\zeta}^{\boldsymbol{j}}\bigr)\bigr)\boldsymbol{x}^{\boldsymbol{j}} + \mathfrak{a} \in R\colon\ f(\boldsymbol{x}) \in \operatorname{Span}_{\mathbb{F}_{q^m}}\bigl\{\boldsymbol{x}^{\boldsymbol{i}}\colon\ \boldsymbol{i} \in I\bigr\} \right\}. \tag{2.4}$$

This representation of C_U is called its trace representation.

Proof. Let $\mathfrak{a}_m$ be the ideal $\langle x_1^{n_1} - 1, \ldots, x_\ell^{n_\ell} - 1\rangle$ of $\mathbb{F}_{q^m}[x_1, \ldots, x_\ell]$. Let $R_m = \mathbb{F}_{q^m}[x_1, \ldots, x_\ell]/\mathfrak{a}_m$ and $\overline{D}$ be the q^m-ary ℓ-D cyclic code of volume $n_1 \times \cdots \times n_\ell$ corresponding to $-(U^c)$. For $\boldsymbol{i}, \boldsymbol{i}' \in \Omega$, let $\boldsymbol{i} \cdot \boldsymbol{i}'$ be the element $(j_1, \ldots, j_\ell)$ of Ω such that $j_t \equiv i_t i'_t \bmod n_t$ for $1 \leqslant t \leqslant \ell$. Using Remark 2.3 and (2.2) we obtain that

$$\overline{D} = \left\{ \sum_{\boldsymbol{j} \in \Omega} a_{\boldsymbol{j}} \boldsymbol{x}^{\boldsymbol{j}} + \mathfrak{a}_m \in R_m\colon\ \sum_{\boldsymbol{j} \in \Omega} a_{\boldsymbol{j}} \boldsymbol{\zeta}^{\boldsymbol{i} \cdot \boldsymbol{j}} = 0 \text{ for each } \boldsymbol{i} \in -\bigl(U^c\bigr) \right\}.$$

Let $\overline{C}$ be the $\mathbb{F}_{q^m}$-linear code in R_m defined as

$$\overline{C} = \left\{ \sum_{\boldsymbol{j} \in \Omega} f\bigl(\boldsymbol{\zeta}^{\boldsymbol{j}}\bigr)\boldsymbol{x}^{\boldsymbol{j}} + \mathfrak{a}_m \in R_m\colon\ f(\boldsymbol{x}) \in \operatorname{Span}_{\mathbb{F}_{q^m}}\bigl\{\boldsymbol{x}^{\boldsymbol{i}}\colon\ \boldsymbol{i} \in -\bigl(U^c\bigr)\bigr\} \right\}.$$

It follows from the definitions that $\overline{D} \subseteq \overline{C}^\perp$. Moreover the $\mathbb{F}_{q^m}$-linear evaluation map from $\operatorname{Span}_{\mathbb{F}_{q^m}}\{\boldsymbol{x}^{\boldsymbol{i}}\colon\ \boldsymbol{i} \in -(U^c)\}$ onto $\overline{C}$ sending $f(\boldsymbol{x})$ to $\sum_{\boldsymbol{j} \in \Omega} f(\boldsymbol{\zeta}^{\boldsymbol{j}})\boldsymbol{x}^{\boldsymbol{j}} + \mathfrak{a}_m \in R_m$ is one-to-one. Therefore $\dim_{\mathbb{F}_{q^m}} \overline{C} = |-(U^c)|$. Since $\overline{D}$ is the q^m-ary ℓ-D cyclic code corresponding to $-(U^c)$, we have $\dim_{\mathbb{F}_{q^m}} \overline{D} = |U|$ (cf. Proposition 2.2) and hence $\overline{D} = \overline{C}^\perp$.

Note that the restriction $\overline{D}|_{\mathbb{F}_q} = \overline{D} \cap R$ is equal to $C_U^\perp$. Hence by Delsarte's theorem ([3] or [19, VIII.1.2]), we have

$$C_U = \operatorname{tr}_m\bigl(\overline{D}^\perp\bigr) = \operatorname{tr}_m(\overline{C}),$$

where tr_m is defined on the codewords of $\overline{C}$ by

$$\operatorname{tr}_m\left(\sum_{\boldsymbol{j} \in \Omega} f\bigl(\boldsymbol{\zeta}^{\boldsymbol{j}}\bigr)\boldsymbol{x}^{\boldsymbol{j}} + \mathfrak{a}_m \right) = \sum_{\boldsymbol{j} \in \Omega} \operatorname{tr}_m\bigl(f\bigl(\boldsymbol{\zeta}^{\boldsymbol{j}}\bigr)\bigr) + \mathfrak{a}.$$

Noting that it is enough to use I rather than $-(U^c)$ in the trace representation (2.4) we complete the proof. □

3. Minimum distance bounds and applications

In this section we obtain minimum distance bounds for ℓ-D cyclic codes.

For $f(\boldsymbol{x}) \in \mathbb{F}_{q^m}[\boldsymbol{x}]$, let $N(f)$ denote the number of affine rational points of the Artin–Schreier type hypersurface

$$y^q - y = f(x_1, \dots, x_\ell)$$

in $\mathbb{A}^{\ell+1}(\mathbb{F}_{q^m})$. We have

$$N(f) = q^{m\ell} + \sum_{c \in \mathbb{F}_q \setminus \{0\}} \sum_{(x_1,\dots,x_\ell) \in \mathbb{F}_{q^m}^\ell} e^{2\pi i \frac{\mathrm{Tr}_m(cf(x_1,\dots,x_\ell))}{p}} \tag{3.1}$$

(see [18, Lemma 2, p. 52]).

Let $Ev : \mathbb{F}_{q^m}[\boldsymbol{x}] \to \mathbb{F}_q^{(q^m-1)^\ell}$ be the evaluation map sending $f(\boldsymbol{x})$ to $(\mathrm{tr}_m(f(\boldsymbol{\alpha})))$, where $\boldsymbol{\alpha}$ runs through $(\mathbb{F}_{q^m} \setminus \{0\})^\ell$. Using Hilbert's Theorem 90 (cf. [11, Theorem 2.25]) we obtain:

Lemma 3.1. *Let $f(\boldsymbol{x}) = \sum_{\boldsymbol{i} \in I} \lambda_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} \in \mathbb{F}_{q^m}[\boldsymbol{x}]$, where I is a finite set of ℓ-tuples of nonnegative integers. Assume that $i_1, \dots, i_\ell \geqslant 1$ for each $\boldsymbol{i} \in I$. For the Hamming weight $\|Ev(f)\|$ of the vector $Ev(f) \in \mathbb{F}_q^{(q^m-1)^\ell}$, we have*

$$\|Ev(f)\| = q^{m\ell} - \frac{N(f)}{q}.$$

Except for Example 4.3 we will let $n_1 = \dots = n_\ell = q^m - 1$. Moreover we assume that $i_1, \dots, i_\ell \geqslant 1$ for each $\boldsymbol{i} \in I$ (cf. Lemma 3.1). Hence, for $U \in \mathcal{U} \setminus \{\Omega\}$, C_U will be the q-ary ℓ-D cyclic code of volume $(q^m - 1) \times \dots \times (q^m - 1)$ corresponding to U. If I is a basic zero set of $-(U^c)$, then the weights of codewords in C_U are related to $\|Ev(f)\|$ for $f \in \mathrm{Span}_{\mathbb{F}_{q^m}}\{\boldsymbol{x}^{\boldsymbol{i}} : \boldsymbol{i} \in I\}$ by (2.4).

Remark 3.2. Assume that $n_t \neq q^m - 1$ for some $1 \leqslant t \leqslant \ell$. Let $f(x_1, \dots, x_\ell) \in \mathbb{F}_{q^m}[x_1, \dots, x_\ell] \setminus \{0\}$ be a polynomial with the corresponding codeword

$$\boldsymbol{a} = \left(\mathrm{tr}_m\left(f(1, \dots, 1)\right), \dots\dots, \mathrm{tr}_m\left(f\left(\zeta_1^{n_1-1}, \dots, \zeta_\ell^{n_\ell-1}\right)\right)\right) \in \mathbb{F}_q^{n_1 \times \dots \times n_\ell}$$

in some ℓ-D cyclic code of volume $n_1 \times \dots \times n_\ell$ (cf. (1.1) and (2.4)). Let $\bar{n} = q^m - 1$, $\bar{\zeta}_1 = \dots = \bar{\zeta}_\ell$ all be a primitive $\bar{n}$th root of unity and $\bar{f}(x_1, \dots, x_\ell) \in \mathbb{F}_{q^m}[x_1, \dots, x_\ell]$ be the polynomial

$$\bar{f}(x_1, \dots, x_\ell) = f\left(x_1^{\bar{n}/n_1}, \dots, x_\ell^{\bar{n}/n_\ell}\right).$$

Then the codeword

$$\bar{\boldsymbol{a}} = \left(\mathrm{tr}_m\left(\bar{f}(1, \dots, 1)\right), \dots\dots, \mathrm{tr}_m\left(\bar{f}\left(\bar{\zeta}_1^{\bar{n}-1}, \dots, \bar{\zeta}_\ell^{\bar{n}-1}\right)\right)\right) \in \mathbb{F}_q^{\bar{n}^\ell}$$

is the corresponding codeword of $\bar{f}(x_1, \dots, x_\ell)$ in an ℓ-D cyclic code $\overline{C}$ of volume $\bar{n} \times \cdots \times \bar{n}$. We have the following relation between the Hamming weights of $\boldsymbol{a}$ and $\bar{\boldsymbol{a}}$:

$$\left\| Ev(\bar{f}) \right\| = \|\bar{\boldsymbol{a}}\| = \|\boldsymbol{a}\| \left(\frac{\bar{n}}{n_1} \right) \dots \left(\frac{\bar{n}}{n_\ell} \right).$$

For $\boldsymbol{i} \in \Omega$, the sum $i_1 + \cdots + i_\ell$ is denoted as $|\boldsymbol{i}|$. For $\boldsymbol{i} \neq \boldsymbol{0}$, let t be the largest integer such that $\frac{i_1}{p^t}, \dots, \frac{i_\ell}{p^t}$ are all integers. We denote t by $j_p(\boldsymbol{i})$ and the ℓ-tuple $(\frac{i_1}{p^t}, \dots, \frac{i_\ell}{p^t})$ by $h_p(\boldsymbol{i})$. We take $j_p(\boldsymbol{0}) = 0$ and $h_p(\boldsymbol{0}) = \boldsymbol{0}$ by convention. For a polynomial $f(\boldsymbol{x}) = \sum_{\boldsymbol{i} \in I} \lambda_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} \in \mathrm{Span}_{\mathbb{F}_{q^m}} \{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in I\}$ and $c \in \mathbb{F}_q \setminus \{0\}$, let $P_{f,c}(\boldsymbol{x})$ be the multivariate polynomial

$$P_{f,c}(\boldsymbol{x}) := \sum_{\boldsymbol{i} \in I} (c\lambda_{\boldsymbol{i}})^{p^{-j_p(\boldsymbol{i})}} \boldsymbol{x}^{h_p(\boldsymbol{i})} \in \mathbb{F}_{q^m}[\boldsymbol{x}]. \tag{3.2}$$

Our first bound is an application of Theorem 2.4 and Deligne's inequality [2, Proposition 3.8].

Theorem 3.3. *Assume that for each $f(\boldsymbol{x}) \in \mathrm{Span}_{\mathbb{F}_{q^m}} \{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in I\}$ and $c \in \mathbb{F}_q \setminus \{0\}$ the condition*

$$P_{f,c}(\boldsymbol{x}) = 0 \quad \Longrightarrow \quad f(\boldsymbol{x}) = 0 \tag{3.3}$$

holds. Let $d = \max\{|h_p(\boldsymbol{i})|\colon \boldsymbol{i} \in I\}$. Then the minimum distance of C_U satisfies

$$d(C_U) \geqslant q^{m\ell} - q^{m\ell-1} - \left\lfloor \frac{(q-1)(d-1)(q^m)^{\ell-\frac{1}{2}}}{q} \right\rfloor.$$

Proof. For $f(\boldsymbol{x}) \in \mathrm{Span}_{\mathbb{F}_{q^m}} \{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in I\}$, using (3.1) and (3.2) we have

$$N(f) = q^{m\ell} + \sum_{c \in \mathbb{F}_q \setminus \{0\}} \sum_{\boldsymbol{x} \in \mathbb{F}_{q^m}^\ell} e^{2\pi i \frac{\mathrm{Tr}_m(cf(\boldsymbol{x}))}{p}} = q^{m\ell} + \sum_{c \in \mathbb{F}_q \setminus \{0\}} \sum_{\boldsymbol{x} \in \mathbb{F}_{q^m}^\ell} e^{2\pi i \frac{\mathrm{Tr}_m(P_{f,c}(\boldsymbol{x}))}{p}}.$$

For each $c \in \mathbb{F}_q \setminus \{0\}$, using (3.3) and Deligne's inequality we obtain

$$\left| \sum_{\boldsymbol{x} \in \mathbb{F}_{q^m}^\ell} e^{2\pi i \frac{\mathrm{Tr}_m(P_{f,c}(\boldsymbol{x}))}{p}} \right| \leqslant (d-1)\bigl(q^m\bigr)^{\ell-\frac{1}{2}}.$$

As $N(f)$ is an integer divisible by q, we further have

$$N(f) \leqslant q^{m\ell} + q \left\lfloor \frac{(q-1)(d-1)(q^m)^{\ell-\frac{1}{2}}}{q} \right\rfloor. \tag{3.4}$$

The proof follows from Theorem 2.4, Lemma 3.1 and (3.4). □

Remark 3.4. Note that for $q = p$, the condition (3.3) holds.

Theorem 3.3 gives a very neat result in a general case. Next, we obtain a minimum distance bound from Hasse–Weil–Serre inequality. To simplify the statement of the next theorem, we introduce some further notation. For $f(\boldsymbol{x}) \in \mathrm{Span}_{\mathbb{F}_{q^m}}\{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in I\}$, $c \in \mathbb{F}_q \setminus \{0\}$, $a \in \{1, \dots, \ell\}$, and $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_{a-1}, \alpha_{a+1}, \dots, \alpha_\ell) \in \mathbb{F}_{q^m}^{\ell-1}$, let $\hat{f}_{a,\boldsymbol{\alpha}}(x) = f(\alpha_1, \dots, \alpha_{a-1}, x, \alpha_{a+1}, \dots, \alpha_\ell) \in \mathbb{F}_{q^m}[x]$ and $\hat{P}_{f,c,a,\boldsymbol{\alpha}}(x) \in \mathbb{F}_{q^m}[x]$ be the univariate polynomial defined by

$$\hat{P}_{f,c,a,\boldsymbol{\alpha}}(x) = P_{\hat{f}_{a,\boldsymbol{\alpha}},c}(x). \tag{3.5}$$

Moreover let $d_{f,c,a,\boldsymbol{\alpha}}$ be the degree of the polynomial $\hat{P}_{f,c,a,\boldsymbol{\alpha}}(x)$. We will denote the subset consisting of $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^{\ell-1}$ such that $\hat{P}_{f,c,a,\boldsymbol{\alpha}}(x)$ is the zero polynomial for some $c \in \mathbb{F}_q \setminus \{0\}$ by $M_{f,a}$. Finally, for $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^{\ell-1} \setminus M_{f,a}$ we let

$$\bar{d}_{f,a,\boldsymbol{\alpha}} = \sum_{c \in \mathbb{F}_q \setminus \{0\}} (d_{f,c,a,\boldsymbol{\alpha}} - 1).$$

Theorem 3.5. *Assume that there exists a nonempty subset A of $\{1, \dots, \ell\}$ such that for each $f(\boldsymbol{x}) \in \mathrm{Span}_{\mathbb{F}_{q^m}}\{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in I\}$, $a \in A$, and $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^{\ell-1}$, the univariate polynomial*

$$\hat{P}_{f,c,a,\boldsymbol{\alpha}}(x) \quad \textit{is either always the zero polynomial or never the zero polynomial} \tag{3.6}$$

as c runs through $\mathbb{F}_q \setminus \{0\}$. Then we have

$$d(C_U) \geqslant q^{m\ell} - q^{m\ell-1} - \min_{a \in A} \max_{f} \left\{ |M_{f,a}|(q-1)q^{m-1} + \sum_{\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^{\ell-1} \setminus M_{f,a}} \left\lfloor \frac{\bar{d}_{f,a,\boldsymbol{\alpha}} \lfloor 2q^{m/2} \rfloor}{2q} \right\rfloor \right\},$$

where the maximum is over $f(\boldsymbol{x}) \in \mathrm{Span}_{\mathbb{F}_{q^m}}\{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in I\} \setminus \{0\}$.

Proof. For $f(\boldsymbol{x}) \in \mathrm{Span}_{\mathbb{F}_{q^m}}\{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in I\} \setminus \{0\}$ and $a \in A$, using (3.1) and (3.5) we get

$$N(f) = q^{m\ell} + \sum_{\boldsymbol{\alpha} \in M_{f,a}} \sum_{c \in \mathbb{F}_q \setminus \{0\}} \sum_{x \in \mathbb{F}_{q^m}} e^{2\pi i \frac{\mathrm{Tr}_m(\hat{P}_{f,c,a,\boldsymbol{\alpha}}(x))}{p}} + \sum_{\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^{\ell-1} \setminus M_{f,a}} \sum_{c \in \mathbb{F}_q \setminus \{0\}} \sum_{x \in \mathbb{F}_{q^m}} e^{2\pi i \frac{\mathrm{Tr}_m(\hat{P}_{f,c,a,\boldsymbol{\alpha}}(x))}{p}}.$$

Note that

$$\sum_{\boldsymbol{\alpha} \in M_{f,a}} \sum_{c \in \mathbb{F}_q \setminus \{0\}} \sum_{x \in \mathbb{F}_{q^m}} e^{2\pi i \frac{\mathrm{Tr}_m(\hat{P}_{f,c,a,\boldsymbol{\alpha}}(x))}{p}} = |M_{f,a}|(q-1)q^m.$$

For $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^{\ell-1} \setminus M_{f,a}$, using [5, Theorem 2.1 and Proposition 1.2], [19, Proposition 3.7.8] and Hasse–Weil–Serre inequality we obtain

$$\left| \sum_{c\in\mathbb{F}_q\setminus\{0\}} \sum_{x\in\mathbb{F}_{q^m}} e^{2\pi i \frac{\mathrm{Tr}_m(cg_{\boldsymbol{\alpha}}(x))}{p}} \right| \leqslant q \left\lfloor \frac{\bar{d}_{f,a,\boldsymbol{\alpha}} \lfloor 2q^{m/2} \rfloor}{2q} \right\rfloor.$$

Now the proof follows from Theorem 2.4 and Lemma 3.1. □

We note that for $q = p$, the condition (3.6) holds for any nonempty subset A of $\{1,\ldots,\ell\}$. Using Theorem 3.5 and simple bounds on $|M_{f,a}|$ and $\bar{d}_{f,a,\boldsymbol{\alpha}}$, we improve the bound of Theorem 3.3 in general.

Example 3.6. Let $\ell = 2$, $q = p$, m be an even integer, $1 \leqslant r \leqslant m-1$ and $s = r+1$. We use the notation of Theorem 3.5. Let $\boldsymbol{i}_1 = (p^r, 1), \boldsymbol{i}_2 = (p^{r-1}, p), \ldots, \boldsymbol{i}_s = (1, p^r)$. It is clear that $I = \{\boldsymbol{i}_1, \ldots, \boldsymbol{i}_s\}$ is a basic zero set in $\Omega = \{0, 1, \ldots, p^m - 2\} \times \{0, 1, \ldots, p^m - 2\}$. For $f(\boldsymbol{x}) = \lambda_1 \boldsymbol{x}^{\boldsymbol{i}_1} + \cdots + \lambda_s \boldsymbol{x}^{\boldsymbol{i}_s} \in \mathrm{Span}_{\mathbb{F}_{p^m}}\{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in I\} \setminus \{0\}$, $c \in \mathbb{F}_p \setminus \{0\}$, $a = 1$ and $\alpha \in \mathbb{F}_{p^m}$ we have

$$\hat{P}_{f,c,a,\alpha}(x) = \big((\lambda_1\alpha)^{\frac{1}{p^r}} + \big(\lambda_2\alpha^p\big)^{\frac{1}{p^{r-1}}} + \cdots + \big(\lambda_s\alpha^{p^r}\big)\big)cx.$$

Hence $M_{f,1}$ is the subset of $\mathbb{F}_{p^m}$ consisting of α such that

$$\lambda_1\alpha + \lambda_2^p\alpha^{p^2} + \cdots + \lambda_s^{p^r}\alpha^{p^{2r}} = 0.$$

Hence $|M_{f,1}| \leqslant p^{2r}$ and if $\alpha \notin M_{f,1}$, then $\bar{d}_{f,1,\alpha} = 0$. Therefore using Theorem 3.5 we obtain

$$d(C_U) \geqslant p^{2m} - p^{2m-1} - p^{2r}(p-1)p^{m-1}. \tag{3.7}$$

Using Theorem 3.3 we would only get

$$d(C_U) \geqslant p^{2m} - p^{2m-1} - (p-1)p^{r-1}p^{\frac{3m}{2}}. \tag{3.8}$$

Note that (3.8) is nontrivial only if $r < \frac{m}{2}$. Moreover if $r < \frac{m}{2}$, then

$$p^{2r}(p-1)p^{m-1} < (p-1)p^{r-1}p^{\frac{3m}{2}}$$

and hence (3.7) is better than (3.8). Next we show that the bound of Theorem 3.5 is tight for $r < \frac{m}{2}$. As $\mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^m}$, there exist r elements $v_1, \ldots, v_r$ of $\mathbb{F}_{p^m}$, which are linearly independent over $\mathbb{F}_{p^2}$. Let V be their $\mathbb{F}_{p^2}$-linear span and $h(x) \in \mathbb{F}_{p^m}[x]$ be the additive polynomial $h(x) = \prod_{v\in V}(x - v)$. Since the set V of the zeroes of $h(x)$ is an $\mathbb{F}_{p^2}$-linear subspace of $\mathbb{F}_{p^m}$, the polynomial $h(x)$ is of the form $h(x) = h_1x + h_2x^{p^2} + \cdots + h_rx^{p^{2r}}$. Hence $|M_{f,1}| = p^{2r}$ for some $f(\boldsymbol{x}) \in \mathrm{Span}_{\mathbb{F}_{p^m}}\{\boldsymbol{x}^{\boldsymbol{i}}\colon \boldsymbol{i} \in I\} \setminus \{0\}$ and the bound of Theorem 3.5 is tight in this case.

For $q = p = 2$, using the methods in the proof of Theorem 3.5, we obtain the following corollary. It gives better upper bounds than [2, Proposition 3.8] in some cases. We keep the notation and the assumptions of this section.

Corollary 3.7. *For $m \geqslant 2$ and $q = p = 2$, we have that*

$$\left|\sum_{x \in \mathbb{F}_{2^m}^{\ell}} (-1)^{\mathrm{tr}_m(f(x))}\right| \leqslant \min_{a \in \{1,\dots,\ell\}} \max_{f} \left\{ |M_{f,a}| 2^m + 2 \sum_{\alpha \in \mathbb{F}_{2^m}^{\ell-1} \setminus M_{f,a}} \left\lfloor \frac{\bar{d}_{f,a,\alpha} \lfloor 2^{m/2+1} \rfloor}{4} \right\rfloor \right\},$$

where the maximum is over $f(x) \in \mathrm{Span}_{\mathbb{F}_{2^m}}\{x^i \colon i \in I\} \setminus \{0\}$.

4. Applications

As a first application we improve the minimum distance bound given in [12, Theorem 8 and Section 5, Note 1] for p-ary subfield subcodes of generalized Reed–Muller codes for some parameters.

Example 4.1. For $q = p$, $\ell \geqslant 2$, $m \geqslant 2$ and $0 \leqslant d \leqslant \ell(p^m - 1)$, let $R_d(\ell, p^m)$ be the generalized Reed–Muller code of order d and length $p^{\ell m}$ over $\mathbb{F}_{p^m}$. It is well known that for $d < \ell(p^m - 1)$, the dual $R_d(\ell, p^m)^{\perp}$ of $R_d(\ell, p^m)$ is $R_{\ell(p^m-1)-d-1}(\ell, p^m)$. Let $B_d(\ell, p^m)$ be the p-ary subfield subcode of $R_d(\ell, p^m)$. Using Delsarte's Theorem [3] and Deligne's inequality [2, Proposition 3.8], Moreno and Kumar obtained lower bounds for the minimum distance $d(B_{\ell(p^m-1)-d-1}(\ell, p^m)^{\perp})$ of the dual p-ary code $B_{\ell(p^m-1)-d-1}(\ell, p^m)^{\perp}$. Moreover they showed that for fixed d and large p^m, the bound of [12] is considerably better than the bound of [4], which is obtained by applying the BCH bound. In this example we apply the methods of Theorem 3.5 in order to find even better bounds. For simplicity we consider only the case $\ell = 2$ and we assume $d \geqslant 2$. Let $\bar{d}$ be the largest integer coprime to p and less than or equal to d. We further assume that

$$p^m + p \left\lfloor \frac{(p-1)(\bar{d}-1)\lfloor 2p^{m/2} \rfloor}{2p} \right\rfloor \leqslant p^{m+1}, \tag{4.1}$$

which is equivalent to $\lfloor \frac{(p-1)(\bar{d}-1)\lfloor 2p^{m/2} \rfloor}{2p} \rfloor \leqslant p^m - p^{m-1}$. Let D_d be the maximum of the integers

$$p^m \left(p^m + p \left\lfloor \frac{(p-1)(\bar{d}-1)\lfloor 2p^{m/2} \rfloor}{2p} \right\rfloor \right), \tag{4.2}$$

and

$$\begin{aligned} &\left(p^m - (d-t) p^{\lfloor \log_p(\frac{d-1}{t}) \rfloor}\right) \left(p^m + p \left\lfloor \frac{(p-1)(t-1)\lfloor 2p^{m/2} \rfloor}{2p} \right\rfloor \right) \\ &\quad + p^{m+1}(d-t) p^{\lfloor \log_p(\frac{d-1}{t}) \rfloor} \end{aligned} \tag{4.3}$$

as t runs through the integers coprime to p from 1 to d. We prove that if (4.1) holds, then

$$d\left(B_{2(p^m-1)-d-1}\left(2, p^m\right)^{\perp}\right) \geqslant p^{2m} - \frac{D_d}{p}. \tag{4.4}$$

The bound in (4.4) is a considerable improvement of [12, Theorem 8 and Section 5, Note 1] for some parameters. For example when $p = 2$, $m = 5$ and $d = 2, 3, 4, 5, 6$, the assumption (4.1) holds and by (4.4) we obtain

$$d\big(B_{59}(2,32)^{\perp}\big) \geqslant 496, \qquad d\big(B_{58}(2,32)^{\perp}\big) \geqslant 352, \qquad d\big(B_{57}(2,32)^{\perp}\big) \geqslant 341,$$
$$d\big(B_{56}(2,32)^{\perp}\big) \geqslant 160, \qquad d\big(B_{55}(2,32)^{\perp}\big) \geqslant 155,$$

while [12, Theorem 8] would only give

$$d\big(B_{59}(2,32)^{\perp}\big) \geqslant 422, \qquad d\big(B_{58}(2,32)^{\perp}\big) \geqslant 331, \qquad d\big(B_{57}(2,32)^{\perp}\big) \geqslant 241,$$
$$d\big(B_{56}(2,32)^{\perp}\big) \geqslant 150, \qquad d\big(B_{55}(2,32)^{\perp}\big) \geqslant 60.$$

Now we prove (4.4). We are interested in the number of affine rational points of Artin–Schreier hypersurfaces

$$z^p - z = h(x, y)$$

where $h(x, y)$ is a polynomial in $\mathbb{F}_{p^m}[x, y]$ of degree at most d. Using the method of Theorem 3.5, we consider the univariate polynomials $f(x) = h(x, \alpha) \in \mathbb{F}_{p^m}[x]$ as α runs through $\mathbb{F}_{p^m}$. These are polynomials of the form

$$f(x) = \sum_{i=0}^{d} f_i(\alpha)x^i,$$

where $f_i(\alpha) = \sum_{j=0}^{d-i} f_{i,j}\alpha^j$ with $f_{i,j} \in \mathbb{F}_{p^m}$. Moreover if $f_{i,j} = 0$ for each $1 \leqslant i \leqslant d$ and $0 \leqslant j \leqslant d - i$, then we assume that $(f_{0,1}, \ldots, f_{0,d}) \neq \mathbf{0}$, since otherwise the corresponding codeword of $B_{2(p^m-1)-d-1}(2, p^m)^{\perp}$ is either the zero codeword or a codeword of Hamming weight p^{2m}. Using the operator $ax^{rp} \mapsto a^{1/p}x^r$, it is enough to consider the class of polynomials of the form

$$g(x) = g_0(\alpha) + \sum_{\substack{1 \leqslant t \leqslant d \\ \gcd(t,p)=1}} g_t(\alpha)x^t,$$

where $g_0(\alpha) = \sum_{j=0}^{d} f_{0,j}\alpha^j$, and for $1 \leqslant t \leqslant d$ with $\gcd(t, p) = 1$,

$$g_t(\alpha) = \sum_{u=0}^{\lfloor \log_p(\frac{d}{t}) \rfloor} \big(f_{tp^u,0} + f_{tp^u,1}\alpha + \cdots + f_{tp^u,d-tp^u}\alpha^{d-tp^u}\big)^{1/p^u}.$$

For $1 \leqslant t \leqslant d$ with $\gcd(t, p) = 1$ we have

$$\left\lfloor \log_p\left(\frac{d}{t}\right) \right\rfloor = \begin{cases} \lfloor \log_p(\frac{d-1}{t}) \rfloor + 1 & \text{if } \log_p(\frac{d}{t}) \text{ is an integer,} \\ \lfloor \log_p(\frac{d-1}{t}) \rfloor & \text{if } \log_p(\frac{d}{t}) \text{ is not an integer,} \end{cases}$$

and we define $\delta_t \in \mathbb{F}_{p^m}$ as

$$\delta_t = \begin{cases} (f_{tp^v,0})^{1/p} & \text{if } v = \log_p(\frac{d}{t}) \text{ is an integer,} \\ 0 & \text{if } \log_p(\frac{d}{t}) \text{ is not an integer.} \end{cases}$$

For $1 \leqslant t \leqslant d$ with $\gcd(t, p) = 1$, we obtain

$$g_t(\alpha) = \delta_t + \sum_{u=0}^{\lfloor \log_p(\frac{d-1}{t}) \rfloor} \left(f_{tp^u,0} + f_{tp^u,1}\alpha + \cdots + f_{tp^u,d-tp^u}\alpha^{d-tp^u}\right)^{1/p^u}.$$

Note that

$$\left(g_t(\alpha)\right)^{(p^{\lfloor \log_p(\frac{d-1}{t}) \rfloor})}$$

is a polynomial in $\mathbb{F}_{p^m}[\alpha]$ of degree at most $(d-t)p^{\lfloor \log_p(\frac{d-1}{t}) \rfloor}$. Hence for $1 \leqslant t \leqslant d$ with $\gcd(t, p) = 1$, either $g_t(\alpha) = 0$ for each $\alpha \in \mathbb{F}_{p^m}$ or otherwise if there exists $\alpha \in \mathbb{F}_{p^m}$ such that $g_t(\alpha) \neq 0$, then the element $g_t(\alpha) \in \mathbb{F}_{p^m}$ is zero for at most $(d-t)p^{\lfloor \log_p(\frac{d-1}{t}) \rfloor}$ distinct $\alpha \in \mathbb{F}_{p^m}$.

Consider first the case that for each $1 \leqslant t \leqslant d$ with $\gcd(t, p) = 1$, the element $g_t(\alpha) = 0$ for each $\alpha \in \mathbb{F}_{p^m}$. In this case the number of affine rational points of the Artin–Schreier hypersurface $z^p - z = h(x, y)$ is equal to p^m times the number of affine rational points of the Artin–Schreier curve

$$z^p - z = f_0(y) \tag{4.5}$$

in $\mathbb{A}^2(\mathbb{F}_{p^m})$. Then the number of affine rational points of the hypersurface (4.5) is bounded from above by the integer in (4.2).

Next we consider the remaining case and let t be the largest integer with $1 \leqslant t \leqslant d$ and $\gcd(t, p) = 1$ such that there exists $\alpha \in \mathbb{F}_{p^m}$ with $g_t(\alpha) \neq 0$. In this case the number of affine rational points of the Artin–Schreier hypersurface $z^p - z = h(x, y)$ is the same as the number of affine rational points of the hypersurface

$$z^p - z = g_0(y) + \sum_{\substack{1 \leqslant i \leqslant t \\ \gcd(i,p)=1}} g_i(y)x^i. \tag{4.6}$$

As the element $g_t(y) \in \mathbb{F}_{p^m}$ is zero for at most $(d-t)p^{\lfloor \log_p(\frac{d-1}{t}) \rfloor}$ distinct values of $y \in \mathbb{F}_{p^m}$, the number of affine rational points of the hypersurface (4.6) is bounded from above by the integer in (4.3). Therefore using (4.1), Lemma 3.1 and Theorem 3.5, we complete the proof of (4.4).

In the following application we consider the minimum distance of 2-D cyclic codes whose dual has 3 basic zeroes for which [7, Proposition 6.5] does not apply.

Example 4.2. For $\ell = 2$, $m \geqslant 2$, positive integers $i, j \leqslant q^m - 2$ coprime to p, and integers $1 \leqslant u < v$ with $ip^v \leqslant q^m - 2$, let $\boldsymbol{i}_1 = (i, j)$, $\boldsymbol{i}_2 = (ip^u, j)$ and $\boldsymbol{i}_3 = (ip^v, j)$. Assume that the integers $j, jq, \ldots, jq^{m-1}$ are all distinct modulo $q^m - 1$. Then $\{\boldsymbol{i}_1, \boldsymbol{i}_2, \boldsymbol{i}_3\}$ is a basic zero set in $\Omega = \{0, 1, \ldots, q^m - 2\} \times \{0, 1, \ldots, q^m - 2\}$. Let U be the element of $\mathcal{U}$ such that $\{\boldsymbol{i}_1, \boldsymbol{i}_2, \boldsymbol{i}_3\}$ is a basic zero set of $-(U^c)$. By Theorem 3.3 we have

$$d(C_U) \geqslant q^{2m} - q^{2m-1} - \left\lfloor \frac{(q-1)(ip^v + j - 1)q^{3m/2}}{q} \right\rfloor. \tag{4.7}$$

Now we want to apply Theorem 3.5. We assume that

$$\left\lfloor \frac{(q-1)(\max\{i,j\}-1)\lfloor 2q^{m/2}\rfloor}{2q} \right\rfloor \leqslant q^m - q^{m-1}. \tag{4.8}$$

Under the notation of Theorem 3.5, we first consider the case $a=2$. Let $(\lambda_1,\lambda_2,\lambda_3)\in\mathbb{F}_{q^m}^3\setminus\{\mathbf{0}\}$, $\alpha\in\mathbb{F}_{q^m}$, $f(x,y)=\lambda_1x^iy^j+\lambda_2x^{ip^u}y^j+\lambda_3x^{ip^v}y^j$ and $\hat{f}_{2,\alpha}(y)=f(\alpha,y)=(\lambda_1\alpha^i+\lambda_2\alpha^{ip^u}+\lambda_3\alpha^{ip^v})y^j\in\mathbb{F}_{q^m}[y]$. Note that $\hat{f}_{2,\alpha}(y)$ is identically zero if and only if $\alpha\in\mathbb{F}_{q^m}$ is a solution of

$$\lambda_1x^i+\lambda_2x^{ip^u}+\lambda_3x^{ip^v}=0. \tag{4.9}$$

Let $S_q(i;u,v)$ be the maximum of the cardinalities of the solution sets in $\mathbb{F}_{q^m}$ of Eq. (4.9) as $(\lambda_1,\lambda_2,\lambda_3)$ runs through $\mathbb{F}_{q^m}^3\setminus\{\mathbf{0}\}$. Let

$$D_1=\bigl(q^m-S_q(i;u,v)\bigr)\left(q^m+q\left\lfloor\frac{(q-1)(j-1)\lfloor 2q^{m/2}\rfloor}{2q}\right\rfloor\right)+S_q(i;u,v)q^{m+1}.$$

Using Theorem 3.5, when (4.8) holds, we obtain

$$d(C_U)\geqslant q^{2m}-\frac{D_1}{q}. \tag{4.10}$$

Next we consider the case $a=1$. Let $(\lambda_1,\lambda_2,\lambda_3)\in\mathbb{F}_{q^m}^3\setminus\{\mathbf{0}\}$, $\alpha\in\mathbb{F}_{q^m}$ and $f(x,y)=\lambda_1x^iy^j+\lambda_2x^{ip^u}y^j+\lambda_3x^{ip^v}y^j$. For $c\in\mathbb{F}_q\setminus\{0\}$, let

$$\hat{P}_{f,c,1,\alpha}(x)=\bigl(\bigl(\lambda_1c\alpha^j\bigr)+\bigl(\lambda_2c\alpha^j\bigr)^{p^{-u}}+\bigl(\lambda_3c\alpha^j\bigr)^{p^{-v}}\bigr)x^i. \tag{4.11}$$

If $q\neq p$, in some cases there exist $c_1,c_2\in\mathbb{F}_q\setminus\{0\}$ with $\hat{P}_{f,c_1,1,\alpha}(x)$ is identically zero while $\hat{P}_{f,c_2,1,\alpha}(x)$ is not identically zero. Assume that $q=p$ and let $S_p(j;v-u,v)$ be the maximum of the cardinalities of the solution sets in $\mathbb{F}_{p^m}$ of

$$\lambda_1x^{jp^v}+\lambda_2x^{jp^{v-u}}+\lambda_3x^j=0$$

as $(\lambda_1,\lambda_2,\lambda_3)$ runs through $\mathbb{F}_{p^m}^3\setminus\{\mathbf{0}\}$. Let

$$D_2=\bigl(p^m-S_p(j;v-u,v)\bigr)\left(p^m+p\left\lfloor\frac{(p-1)(i-1)\lfloor 2p^{m/2}\rfloor}{2p}\right\rfloor\right)+S_p(j;v-u,v)p^{m+1}.$$

If $q=p$ and (4.8) holds, then using Theorem 3.5 we obtain

$$d(C_U)\geqslant p^{2m}-\frac{D}{p}, \tag{4.12}$$

where $D=\min\{D_1,D_2\}$.

It is clear that

$$S_q(i;u,v) \leqslant ip^v - i + 1 \quad \text{and} \quad S_p(j;v-u,v) \leqslant jp^v - j + 1. \tag{4.13}$$

Let

$$D_1^* = \bigl(q^m - (ip^v - i + 1)\bigr)\left(q^m + q\left\lfloor \frac{(q-1)(j-1)\lfloor 2q^{m/2}\rfloor}{2q}\right\rfloor\right) + \bigl(ip^v - i + 1\bigr)q^{m+1},$$
$$D_2^* = \bigl(p^m - (jp^v - j + 1)\bigr)\left(p^m + p\left\lfloor \frac{(p-1)(i-1)\lfloor 2p^{m/2}\rfloor}{2p}\right\rfloor\right) + \bigl(jp^v - j + 1\bigr)p^{m+1}.$$

Using (4.10) and (4.13), when (4.8) holds, we also obtain

$$d(C_U) \geqslant q^{2m} - \frac{D_1^*}{q}. \tag{4.14}$$

If $q = p$ and (4.8) holds, by (4.12) and (4.13) we further have

$$d(C_U) \geqslant p^{2m} - \frac{D^*}{p}, \tag{4.15}$$

where $D^* = \min\{D_1^*, D_2^*\}$. For fixed i, j, p, u and v, if q^m is sufficiently large and (4.8) holds, then the bound (4.14) is better than the bound (4.7). For $q = p$ and fixed i, j, p, u, v, if m is sufficiently large and (4.8) holds, then

$$D^* = \begin{cases} D_2^* & \text{if } i \leqslant j, \\ D_1^* & \text{if } j \leqslant i \end{cases}$$

and the bound (4.15) is better than the bound (4.7). Note that it follows, as explained in Example 3.6, that $S_q(1;1,2) = S_p(1;1,2) = p^2$. Therefore the bounds in (4.13) are tight for some special cases.

The next application generalizes [7, Theorem 6.1]. It also gives an illustration of Remark 3.2.

Example 4.3. For $\ell \geqslant 2$ and $m \geqslant 2$, let $n_1, \ldots, n_{\ell-1}$ be divisors of $q^m - 1$, $n_1 \geqslant 3$ and $n_\ell = q^m - 1$. Let $1 \leqslant i_1 < i_2 \leqslant n_1 - 1$, $\boldsymbol{i}_1 = (i_1, 1, \ldots, 1)$ and $\boldsymbol{i}_2 = (i_2, 1, \ldots, 1)$. It is clear that $\{\boldsymbol{i}_1, \boldsymbol{i}_2\}$ is a basic zero set in $\Omega = \{0, 1, \ldots, n_1 - 1\} \times \cdots \times \{0, 1, \ldots, n_{\ell-1} - 1\} \times \{0, 1, \ldots, q^m - 2\}$. Let U be the closed subset of Ω such that $\{\boldsymbol{i}_1, \boldsymbol{i}_2\}$ is a basic zero set of $-(U^c)$. Let C_U be the q-ary ℓ-D cyclic code of volume $n_1 \cdots n_{\ell-1}(q^m - 1)$ corresponding to U. Let $u_1 = \frac{q^m-1}{n_1}, \ldots, u_{\ell-1} = \frac{q^m-1}{n_{\ell-1}}$ and

$$\theta = \frac{q^m - 1}{\gcd(u_1(i_2 - i_1), q^m - 1)} = \frac{n_1}{\gcd(i_2 - i_1, n_1)}.$$

In this example we will show that C_U is a 2-weight code consisting of $q^{2m} - (q^m - 1)\theta - 1$ codewords of weight

$$n_1 n_2 \cdots n_{\ell-1}\bigl(q^m - q^{m-1}\bigr) \tag{4.16}$$

and $(q^m-1)\theta$ codewords of weight

$$\left(n_1 - \frac{n_1}{\theta}\right) n_2 \cdots n_{\ell-1}\bigl(q^m - q^{m-1}\bigr). \tag{4.17}$$

Using Remark 3.2, we consider Artin–Schreier type hypersurfaces of the form

$$y^q - y = f(\boldsymbol{x}) = \lambda_1 x_1^{u_1 i_1} x_2^{u_2} \cdots x_{\ell-1}^{u_{\ell-1}} x_\ell + \lambda_2 x_1^{u_1 i_2} x_2^{u_2} \cdots x_{\ell-1}^{u_{\ell-1}} x_\ell, \tag{4.18}$$

where $\lambda_1, \lambda_2 \in \mathbb{F}_{q^m}$. Let $\alpha_1, \ldots, \alpha_{\ell-1} \in \mathbb{F}_{q^m} \setminus \{0\}$ and consider the univariate polynomial

$$\bigl(\lambda_1 \alpha_1^{u_1 i_1} + \lambda_2 \alpha_1^{u_1 i_2}\bigr)\beta x \in \mathbb{F}_{q^m}[x], \tag{4.19}$$

where $\beta = \alpha_2^{u_2} \cdots \alpha_{\ell-1}^{u_{\ell-1}}$ if $\ell \geqslant 3$, and $\beta = 1$ if $\ell = 2$. For $\alpha_1, \beta \in \mathbb{F}_{q^m} \setminus \{0\}$, the polynomial in (4.19) is identically zero if and only if

$$\lambda_1 + \alpha_1^{u_1(i_2 - i_1)}\lambda_2 = 0. \tag{4.20}$$

Let S be the subset of $(\mathbb{F}_{q^m} \setminus \{0\})^2$ consisting of (λ_1, λ_2) such that there exists $\alpha_1 \in \mathbb{F}_{q^m} \setminus \{0\}$ satisfying (4.20). Then $|S| = \theta(q^m - 1)$. Moreover for $(\lambda_1, \lambda_2) \in S$, the number of $\alpha_1 \in \mathbb{F}_{q^m} \setminus \{0\}$ satisfying (4.20) is $\frac{q^m-1}{\theta}$. Therefore if $(\lambda_1, \lambda_2) \in S$, then for the number $N(f)$ of affine rational points of the hypersurface (4.18) we have

$$\begin{aligned} N(f) = {} & \left(q^m - 1 - \frac{q^m-1}{\theta}\right)\bigl(q^m-1\bigr)^{\ell-2} q^m \\ & + \left(\bigl(q^m-1\bigr)^{\ell-1} - \left(q^m - 1 - \frac{q^m-1}{\theta}\right)\bigl(q^m-1\bigr)^{\ell-2}\right) q^{m+1} \\ & + \bigl(q^{m(\ell-1)} - \bigl(q^m-1\bigr)^{\ell-1}\bigr) q^{m+1}. \end{aligned}$$

If $(\lambda_1, \lambda_2) \notin S \cup \{(0,0)\}$, then it is not difficult to observe that

$$N(f) = \bigl(q^m-1\bigr)^{\ell-1} q^m + \bigl(q^{m(\ell-1)} - \bigl(q^m-1\bigr)^{\ell-1}\bigr) q^{m+1}.$$

Hence for the Hamming weight of $Ev(f) \in \mathbb{F}_q^{(q^m-1)^\ell}$, we have that if $(\lambda_1, \lambda_2) \in S$, then

$$\bigl\|Ev(f)\bigr\| = q^{m\ell} - \frac{N(f)}{q} = \left(q^m - 1 - \frac{q^m-1}{\theta}\right)\bigl(q^m-1\bigr)^{\ell-2}\bigl(q^m - q^{m-1}\bigr)$$

and if $(\lambda_1, \lambda_2) \notin S \cup \{(0,0)\}$, then

$$\bigl\|Ev(f)\bigr\| = \bigl(q^m-1\bigr)^{\ell-1}\bigl(q^m - q^{m-1}\bigr).$$

We obtain (4.16) and (4.17) using Remark 3.2.

Acknowledgments

The authors thank the editor and the anonymous referees for very useful suggestions. The second author is partially supported by the Turkish Academy of Sciences in the framework of Young Scientists Award Programme (F.Ö./TÜBA-GEBIP/2003-13).

References

[1] H. Chabanne, G.H. Norton, The n-dimensional key equation and a decoding application, IEEE Trans. Inform. Theory 40 (1) (1994) 200–203.

[2] P. Deligne, Applications de la formule des traces aux sommes trigonométriques, in: SGA $4\frac{1}{2}$ Cohomologie Etale, in: Lecture Notes in Math., vol. 569, 1978, pp. 168–232.

[3] P. Delsarte, On subfield subcodes of Reed–Solomon codes, IEEE Trans. Inform. Theory 21 (5) (1975) 575–576.

[4] P. Delsarte, J.M. Goethals, F.J. MacWilliams, On generalized Reed–Muller codes and their relatives, Inform. Control 16 (1970) 403–442.

[5] A. Garcia, H. Stichtenoth, Elementary abelian p-extensions of algebraic function fields, Manuscripta Math. 72 (1991) 67–79.

[6] C. Güneri, Artin–Schreier families and 2-D cyclic codes, PhD thesis, Louisiana State University, 2001, http://etd02.lnx390.lsu.edu/docs/available/etd-0713101-132954/unrestricted/guneridissert.pdf.

[7] C. Güneri, Artin–Schreier curves and weights of two-dimensional cyclic codes, Finite Fields Appl. 10 (4) (2004) 481–505.

[8] T. Ikai, H. Kosako, Y. Kojima, Two-dimensional cyclic codes, Electron. Commun. Japan 57-A (1975) 27–35.

[9] H. Imai, A theory of two-dimensional cyclic codes, Inform. Control 34 (1977) 1–21.

[10] J.M. Jensen, The concatenated structure of cyclic and abelian codes, IEEE Trans. Inform. Theory 31 (1985) 788–793.

[11] R. Lidl, H. Niederreieter, Finite Fields, Cambridge Univ. Press, Cambridge, 1997.

[12] O. Moreno, P.V. Kumar, Minimum distance bounds for cyclic codes and Deligne's theorem, IEEE Trans. Inform. Theory 39 (5) (1993) 1524–1534.

[13] O. Pretzel, Finding recursions for multidimensional arrays, Inform. and Comput. 173 (1) (2002) 1–14.

[14] R.E. Sabin, On minimum distance bounds for abelian codes, Appl. Algebra Engrg. Comput. 3 (1992) 183–197.

[15] K. Saints, Algebraic methods for the encoding and decoding problems for multidimensional cyclic codes and algebraic–geometric codes, PhD thesis, Cornell University, 1995.

[16] S. Sakata, Decoding binary 2-D cyclic codes by the 2-D Berlekamp–Massey algorithm, IEEE Trans. Inform. Theory 37 (4) (1991) 1200–1203.

[17] K. Saints, C. Heegard, Algebraic–geometric codes and multidimensional cyclic codes: A unified theory and algorithms for decoding using Gröbner bases, IEEE Trans. Inform. Theory 41 (6) (1993) 1733–1751.

[18] S.A. Stepanov, Arithmetic of Algebraic Curves, Plenum, New York, 1994.

[19] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993.