Finite Fields and Their Applications 18 (2012) 396–433

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Quadratic forms of codimension 2 over finite fields containing $\mathbb{F}_4$ and Artin–Schreier type curves

Ferruh Özbudak[a,*], Elif Saygı[b], Zülfükar Saygı[c]

[a] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, İnönü Bulvarı, 06531 Ankara, Turkey
[b] Primary Mathematics Education Division, Department of Primary Education, Faculty of Education, Hacettepe University, 06550 Ankara, Turkey
[c] Department of Mathematics, TOBB University of Economics and Technology, Söğütözü, 06530 Ankara, Turkey

ARTICLE INFO

Article history:
Received 26 April 2010
Revised 17 September 2011
Accepted 28 September 2011
Available online 7 October 2011
Communicated by James W.P. Hirschfeld

MSC:
11G20
11E08
94B27

Keywords:
Artin–Schreier type curve
Quadratic form
Maximal curve

ABSTRACT

Let $\mathbb{F}_q$ be a finite field containing $\mathbb{F}_4$. Let $k \geqslant 2$ be an integer. We give a full classification of quadratic forms over $\mathbb{F}_{q^k}$ of codimension 2 provided that certain three coefficients are from $\mathbb{F}_4$. As an application of this we obtain new results on the classification of maximal and minimal curves over $\mathbb{F}_{q^k}$. We also give some nonexistence results on certain systems of equations over $\mathbb{F}_{q^k}$.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

Let q be an integer which is a power of a prime. Let $k \geqslant 2$ be an integer and $m = \lfloor \frac{k}{2} \rfloor$, the integer part of $k/2$. Let $\epsilon_0, \epsilon_1, \ldots, \epsilon_m \in \mathbb{F}_{q^k}$. The map

$$\begin{aligned} Q : \mathbb{F}_{q^k} &\to \mathbb{F}_q, \\ x &\mapsto \operatorname{Tr}\bigl(x\bigl(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m}\bigr)\bigr) \end{aligned}$$

[*] Corresponding author. Fax: +90 312 2102985.
E-mail addresses: ozbudak@metu.edu.tr (F. Özbudak), esaygi@hacettepe.edu.tr (E. Saygı), zsaygi@etu.edu.tr (Z. Saygı).

1071-5797/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2011.09.008

is a quadratic form over $\mathbb{F}_{q^k}$. It is well known (cf. [19, Proposition 6.4.1]) that the quadratic form Q is related to an Artin–Schreier type curve given by the affine equation

$$\chi: \quad y^q - y = x\big(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m}\big). \tag{1.1}$$

We assume that at least one of $\epsilon_0, \epsilon_1, \ldots, \epsilon_m$ is nonzero if q is odd and at least one of $\epsilon_1, \ldots, \epsilon_m$ is nonzero if q is even. Then the genus of χ is positive. The radical of Q is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^k}$. There is another invariant $\Lambda(Q)$ of Q, which is an integer in the set $\{-1, 0, 1\}$. The dimension of the radical and the value of $\Lambda(Q)$ determine the number of $\mathbb{F}_{q^k}$-rational points of χ.

If the codimension of the radical is 0, then it is not difficult to determine the invariant $\Lambda(Q)$ of Q and the number of $\mathbb{F}_{q^k}$-rational points of χ (see Proposition 7.1 below). We consider the problem of determining Q explicitly when the radical is of codimension 2 and $\mathbb{F}_q$ is an extension field of $\mathbb{F}_4$. It is well known that when q is even, the codimension is an even integer and hence it natural to consider this problem after codimension 0 case. Our result is an extension of [4].

We put an extra condition. We assume that $\epsilon_0, \epsilon_1 \in \mathbb{F}_4$ and $\epsilon_2 \in \mathbb{F}_4$ for $k \geqslant 4$; that is, the first three coefficients are in $\mathbb{F}_4$ instead of $\mathbb{F}_{q^k}$ for $k \geqslant 4$. Then we explicitly determine all of the coefficients of Q when the codimension is 2, depending on ϵ_0, ϵ_1 and ϵ_2. We obtain that there are very strict restrictions on k, q and the coefficients when the codimension is 2. We give a full classification of such quadratic forms in our main result (see Theorem 3.1). Note that in [4] the coefficients are only in $\mathbb{F}_2$.

Maximal curves (see Section 7.1 for definition) of the form (1.1) were studied and certain classification results were obtained in the literature (see, for example, the references given in Section 7.1). In particular it is shown that (cf. [2]) χ is a Galois subcover of the Hermitian curve

$$H: \quad y^{q^{k/2}} + y = x^{q^{k/2}+1}$$

over $\mathbb{F}_{q^k}$, when k is even. However as far as we know, there is no general result in the literature giving the coefficients of χ explicitly when χ is maximal. It seems a difficult problem when Q is not trivial and the codimension of Q is not small. Moreover such results are also not known when χ is minimal.

As an application of our main result we determine the coefficients of Q explicitly when χ is maximal or minimal, under the conditions that $\mathbb{F}_q$ is an extension of $\mathbb{F}_4$, $\epsilon_0, \epsilon_1, \epsilon_2 \in \mathbb{F}_4$ and the codimension of Q is 2 (see also Remark 7.3). In particular we note that there are rather complicated conditions on the coefficients of Q, the extension degree k and q (see Proposition 7.2).

As we obtain a full classification of such quadratic forms, in the course of our proof we obtained existence results of certain systems of equations over $\mathbb{F}_{q^k}$. This full classification also implies certain nonexistence results of the corresponding systems of equations over $\mathbb{F}_{q^k}$. We report them in Section 7.2, which would be useful in some applications.

We note that our results and methods are more complicated than [4]. Nevertheless our main motivation and approaches stem from [4]. In particular we would like to indicate that the technical lemmas [4, Lemma 2.3] and Lemma 5.4 below seem very interesting.

This paper is organized as follows. In Section 2 we give some preliminaries. We state our main result in Section 3. We consider the proof of necessary conditions in Section 4 and the proof of sufficient conditions in Section 5. The proofs of the main and related results are completed in Section 6. In Section 7 we give applications to curves over finite fields (see Section 7.1) and systems of equations over finite fields (see Section 7.2). We also give a motivation for our application and an exposition on related results for curves over finite fields in Section 7.1.

2. Preliminaries

In this section we recall some basic facts that we use. Let $q \geqslant 2$ be an integer which is a power of 2. We recall some basic facts from quadratic forms (see, for example, [14, Chapter 6]). For an integer $k \geqslant 2$, a map $Q : \mathbb{F}_{q^k} \to \mathbb{F}_q$ is called a quadratic form if

i. $Q(ax) = a^2 Q(x)$ for all $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^k}$, and
ii. $B(x, y) = Q(x + y) + Q(x) + Q(y)$ is a bilinear map from $\mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$ to $\mathbb{F}_q$.

The radical of Q is defined as

$$W = \{x \in \mathbb{F}_{q^k}\colon\ B(x, y) = 0 \text{ for all } y \in \mathbb{F}_{q^k}\}.$$

It is easy to observe that W is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^k}$. It is well known that k- $\dim_{\mathbb{F}_q} W$ is even. Let w denote the dimension of W over $\mathbb{F}_q$. Let $N(Q)$ denote the number

$$N(Q) = \left|\{x \in \mathbb{F}_{q^k}\colon\ Q(x) = 0\}\right|.$$

It is also well known (cf. [14, Theorem 6.32]) that there exists an invariant $\Lambda(Q)$ in the set $\{-1, 0, 1\}$ such that

$$N(Q) = q^{k-1} + \Lambda(Q)(q - 1)q^{\frac{k+w}{2}-1}.$$

Next we recall two important results from [4].

Theorem 2.1. *(See [4, Theorem 1.2].) Let $q = 2^h$, $Q : \mathbb{F}_{q^k} \to \mathbb{F}_q$ be a quadratic form and let $m = \lfloor k/2 \rfloor$. Then there exist $\epsilon_0, \epsilon_1, \ldots, \epsilon_m \in \mathbb{F}_{q^k}$ such that*

$$Q(x) = \operatorname{Tr}\bigl(x\bigl(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m}\bigr)\bigr). \tag{2.1}$$

Moreover $\epsilon_0, \epsilon_1, \ldots, \epsilon_m$ are uniquely determined, except when k is even in which case ϵ_m is only unique modulo $\mathbb{F}_{q^m}$.

If the codimension of the radical is 2, then we have further information on Q.

Theorem 2.2. *(See [4, Corollary 1.3].) Let $q = 2^h$ and $\epsilon_0, \epsilon_1, \ldots, \epsilon_m$ be the coefficients corresponding to Q as in* (2.1)*. Then we have $w = k - 2$ if and only if there exist $a, b \in \mathbb{F}_{q^k}$ such that the set $\{a, b\}$ is linearly independent over $\mathbb{F}_q$ and for $1 \leqslant i \leqslant \lfloor (k - 1)/2 \rfloor$ we have*

$$\epsilon_i = a^{q^i} b + ab^{q^i}, \tag{2.2}$$

and if k is even, then furthermore

$$\epsilon_m - ab^{q^m} \in \mathbb{F}_{q^m}.$$

Moreover we have the following:

- *if $\Lambda(Q) = 1$, then*

$$\epsilon_0 = ab;$$

- *if $\Lambda(Q) = -1$, then there exists $s \in \mathbb{F}_q$ such that $\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ and*

$$\epsilon_0 = a^2 + ab + sb^2,$$

where $\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_2}$ is the trace from $\mathbb{F}_q$ to $\mathbb{F}_2$;

- *if $\Lambda(Q) = 0$, then there exists $c \in \mathbb{F}_{q^k}$ such that $\{a, b, c\}$ is linearly independent over $\mathbb{F}_q$ and*

$$\epsilon_0 = c^2 + ab.$$

3. Main result

In this section we state our main result and some related results. First we introduce some notation. For certain integers $k \geqslant 4$, first we define three types of polynomials $A_1(\epsilon_0, \epsilon_1)$, $A_2(\epsilon_0, \epsilon_1)$ and $A_3(\epsilon_0, \epsilon_1, \epsilon_2)$ in $\mathbb{F}_4[x]$. For simplicity of notation we indicate neither the variable x nor their dependence on k in denoting these polynomials. Let $m = \lfloor \frac{k}{2} \rfloor$.

- If $4 \mid k$, then for $\epsilon_0, \epsilon_1 \in \mathbb{F}_4$ let

$$A_1(\epsilon_0, \epsilon_1) = \epsilon_0 x + \epsilon_1 \left(x^q + x^{q^3} + \cdots + x^{q^{m-1}}\right) \in \mathbb{F}_4[x].$$

- If $3 \mid k$, then for $\epsilon_0, \epsilon_1 \in \mathbb{F}_4$ let

$$A_2(\epsilon_0, \epsilon_1) = \epsilon_0 x + \epsilon_1 \left(x^q + x^{q^2} + x^{q^4} + x^{q^5} + \cdots\right) \in \mathbb{F}_4[x],$$

  where the last term of $A_2(\epsilon_0, \epsilon_1)$ is $\epsilon_1 x^{q^m}$ if $k \equiv 3 \bmod 6$ and $\epsilon_1 x^{q^{m-1}}$ if $k \equiv 0 \bmod 6$.
- If $5 \mid k$, then for $\epsilon_0, \epsilon_1, \epsilon_2 \in \mathbb{F}_4$ let

$$\begin{aligned} A_3(\epsilon_0, \epsilon_1, \epsilon_2) = \epsilon_0 x &+ \epsilon_1 \left(x^q + x^{q^4} + x^{q^6} + x^{q^9} + \cdots\right) \\ &+ \epsilon_2 \left(x^{q^2} + x^{q^3} + x^{q^7} + x^{q^8} + \cdots\right), \end{aligned}$$

  where last terms of $A_3(\epsilon_0, \epsilon_1, \epsilon_2)$ are $\epsilon_1(x^{q^{m-4}} + x^{q^{m-1}})$ and $\epsilon_2(x^{q^{m-3}} + x^{q^{m-2}})$ if $k \equiv 0 \bmod 10$, and $\epsilon_1(x^{q^{m-3}} + x^{q^{m-1}})$ and $\epsilon_2(x^{q^{m-4}} + x^{q^m})$ if $k \equiv 5 \bmod 10$.

Now we state our main result.

Theorem 3.1. *Let $q = 4^r$, $k \geqslant 4$ be an integer and set $m = \lfloor \frac{k}{2} \rfloor$. Let $\epsilon_0, \epsilon_1, \epsilon_2 \in \mathbb{F}_4$, and for $k \geqslant 8$ let $\epsilon_3, \ldots, \epsilon_{m-1} \in \mathbb{F}_{q^k}$ and*

$$\epsilon_m \in \begin{cases} \mathbb{F}_{q^m} & \text{if } k \text{ is even,} \\ \mathbb{F}_{q^k} & \text{if } k \text{ is odd.} \end{cases}$$

For $k = 6$ we let $\epsilon_3 \in \mathbb{F}_{q^3}$ and for $k = 7$ we let $\epsilon_3 \in \mathbb{F}_{q^7}$. Let Q be the quadratic form from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$ defined as

$$Q(x) = \mathrm{Tr}\left(x \sum_{i=0}^{m} \epsilon_i x^{q^i}\right), \tag{3.1}$$

where Tr is the trace map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. If the $\mathbb{F}_q$-dimension of the radical of Q is $k - 2$, then exactly one of the following holds:

(1) *$4 \mid k$, $q = 4^r$ where $r \geqslant 1$ is an odd integer, $\epsilon_1 \neq 0$, $\epsilon_0 \neq 0$, $\epsilon_0 \neq \epsilon_1$ and for $1 \leqslant i \leqslant \lfloor \frac{k-1}{2} \rfloor$ we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \bmod 2, \\ 0 & \text{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m} \epsilon_i x^{q^i}$ *is equal to*

$$R(x) = A_1(\epsilon_0, \epsilon_1) + \gamma x^{q^m},$$

where γ *is an arbitrary element of* $\mathbb{F}_{q^m}$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to* 1 *in this case.*

(2) $4 \mid k$, $q = 4^r$ *where* $r \geqslant 1$ *is an odd integer,* $\epsilon_1 \neq 0$, $\epsilon_0 = 0$ *or* $\epsilon_0 = \epsilon_1$, *and for* $1 \leqslant i \leqslant \lfloor \frac{k-1}{2} \rfloor$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \textit{if } i \equiv 1 \bmod 2, \\ 0 & \textit{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m} \epsilon_i x^{q^i}$ *is equal to*

$$R(x) = A_1(\epsilon_0, \epsilon_1) + \gamma x^{q^m},$$

where γ *is an arbitrary element of* $\mathbb{F}_{q^m}$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to* -1 *in this case.*

(3) $4 \mid k$, $q = 4^r$ *where* $r \geqslant 2$ *is an even integer,* $\epsilon_1 \neq 0$ *and for* $1 \leqslant i \leqslant \lfloor \frac{k-1}{2} \rfloor$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \textit{if } i \equiv 1 \bmod 2, \\ 0 & \textit{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m} \epsilon_i x^{q^i}$ *is equal to*

$$R(x) = A_1(\epsilon_0, \epsilon_1) + \gamma x^{q^m},$$

where γ *is an arbitrary element of* $\mathbb{F}_{q^m}$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to* -1 *in this case.*

(4) $3 \mid k$, $q = 4^r$ *where* $r \geqslant 1$ *is an integer,* $\epsilon_1 \neq 0$, $\epsilon_0 = \epsilon_1$ *and for* $1 \leqslant i \leqslant \lfloor \frac{k-1}{2} \rfloor$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \textit{if } i \equiv 1 \textit{ or } 2 \bmod 3, \\ 0 & \textit{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m} \epsilon_i x^{q^i}$ *is equal to*

$$R(x) = A_2(\epsilon_0, \epsilon_1) + \gamma x^{q^m},$$

where $\gamma = 0$ *if* k *is odd and* γ *is an arbitrary element of* $\mathbb{F}_{q^m}$ *if* k *is even. Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to* 1 *in this case.*

(5) $3 \mid k$, $q = 4^r$ *where* $r \geqslant 1$ *is an integer,* $\epsilon_1 \neq 0$, $\epsilon_0 \neq \epsilon_1$ *and for* $1 \leqslant i \leqslant \lfloor \frac{k-1}{2} \rfloor$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \textit{if } i \equiv 1 \textit{ or } 2 \bmod 3, \\ 0 & \textit{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m} \epsilon_i x^{q^i}$ *is equal to*

$$R(x) = A_2(\epsilon_0, \epsilon_1) + \gamma x^{q^m},$$

where $\gamma = 0$ *if* k *is odd and* γ *is an arbitrary element of* $\mathbb{F}_{q^m}$ *if* k *is even. Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to* 0 *in this case.*

(6) *$5 \mid k$, $q = 4^r$ where $r \geqslant 2$ is an even integer, $\epsilon_1 \neq 0$, $\epsilon_2 \neq 0$, $\epsilon_2 \neq \epsilon_1$, $\epsilon_0 \notin \{0, \epsilon_1, \epsilon_2\}$ and for $1 \leqslant i \leqslant \lfloor \frac{k-1}{2} \rfloor$ we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \textit{if } i \equiv 1 \textit{ or } 4 \bmod 5, \\ \epsilon_2 & \textit{if } i \equiv 2 \textit{ or } 3 \bmod 5, \\ 0 & \textit{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m} \epsilon_i x^{q^i}$ is equal to

$$R(x) = A_3(\epsilon_0, \epsilon_1, \epsilon_2) + \gamma x^{q^m},$$

where $\gamma = 0$ if k is odd and γ is an arbitrary element of $\mathbb{F}_{q^m}$ if k is even. Moreover the invariant $\Lambda(Q)$ of Q is equal to 1 in this case.

(7) *$5 \mid k$, $q = 4^r$ where $r \geqslant 1$ is an odd integer, $\epsilon_1 \neq 0$, $\epsilon_2 \neq 0$, $\epsilon_2 \neq \epsilon_1$, $\epsilon_0 \notin \{0, \epsilon_1, \epsilon_2\}$ and for $1 \leqslant i \leqslant \lfloor \frac{k-1}{2} \rfloor$ we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \textit{if } i \equiv 1 \textit{ or } 4 \bmod 5, \\ \epsilon_2 & \textit{if } i \equiv 2 \textit{ or } 3 \bmod 5, \\ 0 & \textit{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m} \epsilon_i x^{q^i}$ is equal to

$$R(x) = A_3(\epsilon_0, \epsilon_1, \epsilon_2) + \gamma x^{q^m},$$

where $\gamma = 0$ if k is odd and γ is an arbitrary element of $\mathbb{F}_{q^m}$ if k is even. Moreover the invariant $\Lambda(Q)$ of Q is equal to -1 in this case.

(8) *$5 \mid k$, $q = 4^r$ where $r \geqslant 1$ is an integer, $\epsilon_1 \neq 0$, $\epsilon_2 \neq 0$, $\epsilon_2 \neq \epsilon_1$, $\epsilon_0 \in \{0, \epsilon_1, \epsilon_2\}$ and for $1 \leqslant i \leqslant \lfloor \frac{k-1}{2} \rfloor$ we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \textit{if } i \equiv 1 \textit{ or } 4 \bmod 5, \\ \epsilon_2 & \textit{if } i \equiv 2 \textit{ or } 3 \bmod 5, \\ 0 & \textit{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m} \epsilon_i x^{q^i}$ is equal to

$$R(x) = A_3(\epsilon_0, \epsilon_1, \epsilon_2) + \gamma x^{q^m},$$

where $\gamma = 0$ if k is odd and γ is an arbitrary element of $\mathbb{F}_{q^m}$ if k is even. Moreover the invariant $\Lambda(Q)$ of Q is equal to 0 in this case.

Conversely, for each of the eight cases above, there exist $\epsilon_0, \epsilon_1, \epsilon_2, \ldots, \epsilon_{m-1}, \epsilon_m \in \mathbb{F}_4 \subseteq \mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ satisfying the corresponding conditions. Hence we have quadratic forms as in (3.1) *from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$, even with coefficients from $\mathbb{F}_4$, such that their radicals are of codimension 2 and their invariants $\Lambda(Q)$ are given as in the eight cases above.*

There are 8 cases in Theorem 3.1. For clarity we state Theorem 3.1 in detail above. It would be useful to express the results of Theorem 3.1 in short together. We summarize the results of Theorem 3.1 in Table 1. We recall that the polynomials $A_1(\epsilon_0, \epsilon_1)$, $A_2(\epsilon_0, \epsilon_1)$ and $A_3(\epsilon_0, \epsilon_1, \epsilon_2)$ in $\mathbb{F}_4[x]$ are defined in the beginning of this section.

Table 1
Summary of Theorem 3.1. Here $k \geqslant 4$, $\epsilon_1 \in \mathbb{F}_4 \setminus \{0\}$ in all cases and $R(x) = A(x) + \gamma x^{q^m}$, where $A(x)$ is given in the table and $\gamma = 0$ if k is odd and γ is an arbitrary element of $\mathbb{F}_{q^m}$ if k is even.

k	q	$A(x)$	$\Lambda(Q_R)$
$4 \mid k$	4^r, r odd	$A_1(\epsilon_0, \epsilon_1)$, $\epsilon_0 \notin \{0, \epsilon_1\}$	1
$4 \mid k$	4^r, r odd	$A_1(\epsilon_0, \epsilon_1)$, $\epsilon_0 \in \{0, \epsilon_1\}$	−1
$4 \mid k$	4^r, r even	$A_1(\epsilon_0, \epsilon_1)$	−1
$3 \mid k$	4^r	$A_2(\epsilon_0, \epsilon_1)$, $\epsilon_0 = \epsilon_1$	1
$3 \mid k$	4^r	$A_2(\epsilon_0, \epsilon_1)$, $\epsilon_0 \neq \epsilon_1$	0
$5 \mid k$	4^r, r even	$A_3(\epsilon_0, \epsilon_1, \epsilon_2)$, $\epsilon_2 \notin \{0, \epsilon_1\}$, $\epsilon_0 \notin \{0, \epsilon_1, \epsilon_2\}$	1
$5 \mid k$	4^r, r odd	$A_3(\epsilon_0, \epsilon_1, \epsilon_2)$, $\epsilon_2 \notin \{0, \epsilon_1\}$, $\epsilon_0 \notin \{0, \epsilon_1, \epsilon_2\}$	−1
$5 \mid k$	4^r	$A_3(\epsilon_0, \epsilon_1, \epsilon_2)$, $\epsilon_2 \notin \{0, \epsilon_1\}$, $\epsilon_0 \in \{0, \epsilon_1, \epsilon_2\}$	0

Remark 3.2. Recall that in Theorem 3.1, if k is even, then we only consider the case that $\epsilon_m \in \mathbb{F}_{q^m} \subsetneq \mathbb{F}_{q^k}$. The remaining case that $\epsilon_m \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^m}$ holds with only the following small change in the statement: We use the expression as in Table 1. If $\epsilon_m \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^m}$, then the statements are exactly the same; only the condition that $\gamma \in \mathbb{F}_{q^m}$ is changed to the condition that $\gamma - \epsilon_m \in \mathbb{F}_{q^m}$.

In order to complete the study of quadratic forms of codimension 2, we give the results for the remaining cases $k \in \{2, 3\}$ in the following proposition.

Proposition 3.3. *Let $q = 4^r$, $k \in \{2, 3\}$ be an integer and $m = 1$. Let $\epsilon_0, \epsilon_1 \in \mathbb{F}_4$. Let Q be the quadratic form from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. If the $\mathbb{F}_q$-dimension of the radical is $k - 2$, then exactly one of the following holds:*

(1) *$k = 3$, $q = 4^r$ where $r \geqslant 1$ is an integer, $\epsilon_1 \neq 0$ and $\epsilon_0 = \epsilon_1$. The invariant $\Lambda(Q)$ is equal to 1 in this case.*
(2) *$k = 3$, $q = 4^r$ where $r \geqslant 1$ is an integer, $\epsilon_1 \neq 0$ and $\epsilon_0 \neq \epsilon_1$. The invariant $\Lambda(Q)$ is equal to 0 in this case.*

In particular $k \neq 2$ and $\Lambda(Q) \neq -1$. Conversely, for each of the two cases above, there exist $\epsilon_0, \epsilon_1 \in \mathbb{F}_4 \subseteq \mathbb{F}_q \subseteq \mathbb{F}_{q^3}$, satisfying the corresponding conditions.

4. Necessary conditions

In this section we prove the necessary conditions of Theorem 3.1. First we prove two general lemmas that we will use in our proofs.

The following is a restatement of [4, Lemma 2.2]. For completeness we include a proof here.

Lemma 4.1. *Let $\mathbb{F}$ be a finite field of characteristic 2. Let $x, y \in \mathbb{F}$ and t be a positive integer. We put*

$$u = x + y \quad \text{and} \quad v = xy.$$

Then the following holds:

$$x^{2^t+1} + y^{2^t+1} = u^{2^t+1} + \left[v u^{2^t+1-2} + v^2 u^{2^t+1-2^2} + v^{2^2} u^{2^t+1-2^3} + \cdots + v^{2^{t-1}} u^{2^t+1-2^t}\right].$$

Proof. We proceed by induction on t. First we assume that $t = 1$. Note that

$$\begin{aligned} u^{2+1} &= (x+y)^{2+1} \\ &= \left(x^2 + y^2\right)(x+y) \\ &= x^3 + y^3 + x^2 y + x y^2 \\ &= x^3 + y^3 + xy(x+y). \end{aligned}$$

As the characteristic is 2, this is equivalent to

$$x^3+y^3=u^{2+1}+xy(x+y)=u^{2+1}+vu,$$

which completes the proof for $t=1$.

Let $t\geqslant 2$ and assume that the lemma holds for $t-1$, which is the induction hypothesis. We have that $2^t=2^{t-1}+2^{t-1}$ and hence

$$(x+y)^{2^t+1}=(x+y)^{2^{t-1}+1}(x+y)^{2^{t-1}}. \tag{4.1}$$

By the induction hypothesis we obtain that

$$\begin{aligned}(x+y)^{2^{t-1}+1}={}&x^{2^{t-1}+1}+y^{2^{t-1}+1}\\&+\big(vu^{2^{t-1}+1-2}+v^2u^{2^{t-1}+1-2^2}+\cdots+v^{2^{t-2}}u^{2^{t-1}+1-2^{t-1}}\big).\end{aligned} \tag{4.2}$$

Note that

$$\begin{aligned}\big(x^{2^{t-1}+1}+y^{2^{t-1}+1}\big)(x+y)^{2^{t-1}}&=\big(x^{2^{t-1}+1}+y^{2^{t-1}+1}\big)\big(x^{2^{t-1}}+y^{2^{t-1}}\big)\\&=x^{2^t+1}+y^{2^t+1}+(xy)^{2^t-1}(x+y)\\&=x^{2^t+1}+y^{2^t+1}+v^{2^t-1}u.\end{aligned} \tag{4.3}$$

Moreover

$$\begin{aligned}&\big(vu^{2^{t-1}+1-2}+v^2u^{2^{t-1}+1-2^2}+\cdots+v^{2^{t-2}}u^{2^{t-1}+1-2^{t-1}}\big)(x+y)^{2^{t-1}}\\&\quad=\big(vu^{2^{t-1}+1-2}+v^2u^{2^{t-1}+1-2^2}+\cdots+v^{2^{t-2}}u^{2^{t-1}+1-2^{t-1}}\big)u^{2^{t-1}}\\&\quad=vu^{2^t+1-2}+v^2u^{2^t+1-2^2}+\cdots+v^{2^{t-2}}u^{2^t+1-2^{t-1}}.\end{aligned} \tag{4.4}$$

Combining (4.1), (4.2), (4.3) and (4.4) we get that

$$\begin{aligned}u^{2^t+1}&=(x+y)^{2^t+1}\\&=x^{2^t+1}+y^{2^t+1}+vu^{2^t+1-2}+v^2u^{2^t+1-2^2}+\cdots+v^{2^{t-1}}u^{2^t+1-2^t},\end{aligned}$$

which completes the proof. □

The following lemma gives an important tool that we will use. Its analog over $\mathbb{F}_2$ is given in the proof of [4, Theorem 2.4]. By using almost the same arguments we obtain the following lemma.

Lemma 4.2. *Let $\mathbb{F}_4\subseteq\mathbb{F}_q\subseteq\mathbb{F}$ with $\mathbb{F}$ finite and let $\epsilon_1,\epsilon_2\in\mathbb{F}_4$. Assume that there exist $a,b\in\mathbb{F}$ such that*

$$\begin{aligned}\epsilon_1&=ab^q+a^qb,\quad\textit{and}\\\epsilon_2&=ab^{q^2}+a^{q^2}b.\end{aligned}$$

We put

$$u=a^{q-1}+b^{q-1}\quad\textit{and}\quad v=ab.$$

Let $q = 2^t$. Then we have that

$$v^q \epsilon_2 = \epsilon_1^2 + \epsilon_1^2 \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}.$$

Proof. Let $A = a^{q-1}$, $B = b^{q-1}$, $X = A + B$, and $Y = AB$. Note that

$$X = a^{q-1} + b^{q-1} = u, \quad \text{and} \quad Y = (ab)^{q-1} = v^{q-1}. \tag{4.5}$$

Using Lemma 4.1 we have that

$$\begin{aligned} A^{q+1} + B^{q+1} &= A^{2^t+1} + B^{2^t+1} \\ &= (A+B)^{q+1} + \left(YX^{q+1-2} + Y^2 X^{q+1-2^2} + \cdots + Y^{q/2} X^{q+1-q}\right). \end{aligned} \tag{4.6}$$

We observe that

$$\frac{\epsilon_2}{v} = a^{q^2-1} + b^{q^2-1} = A^{q+1} + B^{q+1}. \tag{4.7}$$

Hence using (4.5), (4.6) and (4.7) we obtain that

$$\frac{\epsilon_2}{v} = u^{q+1} + \left(v^{q-1} u^{q+1-2} + v^{2(q-1)} u^{q+1-2^2} + \cdots + v^{q/2(q-1)} u^{q+1-q}\right). \tag{4.8}$$

Multiplying (4.8) by v^{q+1} and noting that $\epsilon_1 = uv$ we get that

$$v^q \epsilon_2 = \epsilon_1^{q+1} + \left(v^{q+1} \epsilon_1^{q+1-2} + v^{2(q+1)} \epsilon_1^{(q+1)-4} + \cdots + v^{q/2(q+1)} \epsilon_1^{(q+1)-q}\right). \tag{4.9}$$

As $\epsilon_1 \in \mathbb{F}_4 \subseteq \mathbb{F}_q$, we have that $\epsilon_1^q = \epsilon_1$. Therefore using (4.9) we obtain that

$$\begin{aligned} v^q \epsilon_2 &= \epsilon_1^2 + \epsilon_1^2 \left(v^{q+1} \epsilon_1 + v^{2(q+1)} \epsilon_1^2 + \cdots + v^{q/2(q+1)} \epsilon_1^{q/2}\right) \\ &= \epsilon_1^2 + \epsilon_1^2 \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}, \end{aligned}$$

which completes the proof. □

For the rest of this section we fix the following notation and assumptions. Let $q \geqslant 4$ be an integer which is a power of 4. Let $k \geqslant 4$ be an integer and put $m = \lfloor \frac{k}{2} \rfloor$. Let $\epsilon_0, \epsilon_1, \epsilon_2 \in \mathbb{F}_4$. For $k \geqslant 8$ let $\epsilon_3, \ldots, \epsilon_{m-1} \in \mathbb{F}_{q^k}$ and let $\epsilon_m \in \mathbb{F}_{q^k}$ if k is odd and $\epsilon_m \in \mathbb{F}_{q^m}$ if k is even. Let $Q : \mathbb{F}_{q^k} \to \mathbb{F}_q$ be the quadratic form given by

$$Q(x) = \operatorname{Tr}\left(x \sum_{i=0}^{m} \epsilon_i x^{q^i}\right),$$

where Tr is the trace map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. We assume that the $\mathbb{F}_q$-dimension of the radical of Q is $k-2$. Using Theorem 2.2 we obtain $a, b \in \mathbb{F}_{q^k}$ such that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$ and

$$\begin{aligned}\epsilon_1 &= ab^q + a^q b,\\ \epsilon_2 &= ab^{q^2} + a^{q^2} b,\\ &\vdots\\ \epsilon_{m-1} &= ab^{q^{m-1}} + a^{q^{m-1}} b.\end{aligned} \tag{4.10}$$

Moreover if k is odd, then

$$\epsilon_m = ab^{q^m} + a^{q^m} b, \tag{4.11}$$

and if k is even, then

$$a^{q^m} b \in \mathbb{F}_{q^m}. \tag{4.12}$$

We also have the following:

1. If $\Lambda(Q) = 1$, then

$$\epsilon_0 = ab.$$

2. If $\Lambda(Q) = -1$, then we obtain $s \in \mathbb{F}_q$ such that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ and

$$\epsilon_0 = a^2 + ab + sb^2.$$

3. If $\Lambda(Q) = 0$, then we obtain $c \in \mathbb{F}_{q^k}$ such that $\{a, b, c\}$ is linearly independent over $\mathbb{F}_q$ and

$$\epsilon_0 = c^2 + ab.$$

Now we are ready to start to prove the necessary conditions of Theorem 3.1. First we show that $\epsilon_1 \neq 0$. Indeed, otherwise using (4.10) we have $\epsilon_1 = ab^q + a^q b$, and hence

$$ab\left(a^{q-1} + b^{q-1}\right) = 0.$$

As $\{a, b\}$ is linearly independent over $\mathbb{F}_q$, $ab \neq 0$ and then

$$a^{q-1} + b^{q-1} = 0.$$

This implies that $(a/b)^{q-1} = 1$, or equivalently,

$$\frac{a}{b} = \alpha \in \mathbb{F}_q \setminus \{0\},$$

which is a contradiction to the fact that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$.

In the rest of this section we prove the necessary conditions corresponding to the cases $\epsilon_2 = 0$, $\epsilon_2 = \epsilon_1$ and $\epsilon_2 \neq \epsilon_1$ in three subsections.

4.1. Case $\epsilon_2 = 0$

In this subsection we consider the case that $\epsilon_2 = 0$.

Proposition 4.3. *We keep the notation and assumptions as above. If $\epsilon_2 = 0$, then we have that*

(1) $4 \mid k$,
(2) $a, b \in \mathbb{F}_{q^2}$,
(3) $\epsilon_1 = \epsilon_3 = \epsilon_5 = \cdots = \epsilon_{m-1}$, *and* $\epsilon_2 = \epsilon_4 = \epsilon_6 = \cdots = \epsilon_{m-2} = 0$.

Proof. Using (4.10), Lemma 4.2 and the fact that $\epsilon_2 = 0$ we obtain that

$$0 = \epsilon_1^2 + \epsilon_1^2 \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}, \tag{4.13}$$

where $v = ab$. As $\epsilon_1 \neq 0$, dividing (4.13) by ϵ_1^2 we get that

$$1 = \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i} = \epsilon_1 v^{q+1} + \sum_{i=1}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}. \tag{4.14}$$

Taking the square of (4.14) we have that

$$1 = \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^{i+1}} = \sum_{i=1}^{t} \left(\epsilon_1 v^{q+1}\right)^{2^i} = \left(\epsilon_1 v^{q+1}\right)^{2^t} + \sum_{i=1}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}. \tag{4.15}$$

Adding (4.14) and (4.15) we obtain that

$$\epsilon_1 v^{q+1} = \left(\epsilon_1 v^{q+1}\right)^{2^t} = \left(\epsilon_1 v^{q+1}\right)^{q} = \epsilon_1 v^{(q+1)q}, \tag{4.16}$$

where we use the fact that $\mathbb{F}_4 \subseteq \mathbb{F}_q$ and hence $\epsilon_1^q = \epsilon_1$. Note that (4.16) implies that

$$v^{q+1} \in \mathbb{F}_q.$$

As $v = ab \neq 0$ (otherwise the set $\{a, b\}$ is linearly dependent over $\mathbb{F}_q$), then we have that

$$v^{(q+1)(q-1)} = v^{q^2-1} = 1,$$

in particular $v \in \mathbb{F}_{q^2}$.

Recall that $\epsilon_2 = 0$ and

$$\epsilon_2 = v\left(a^{q^2-1} + b^{q^2-1}\right).$$

As $v \neq 0$, therefore $a^{q^2-1} + b^{q^2-1} = 0$ and $a/b \in \mathbb{F}_{q^2}$. Hence

$$v\frac{a}{b} = ab\frac{a}{b} = a^2 \in \mathbb{F}_{q^2},$$

which implies that $a \in \mathbb{F}_{q^2}$ as the characteristic is 2. Then using the fact that $v = ab \in \mathbb{F}_{q^2}$ we obtain that $b \in \mathbb{F}_{q^2}$.

Next we use (4.10) in order to prove (3) of the proposition. Using (4.10) and the fact that $a, b \in \mathbb{F}_{q^2}$ we obtain that

$$\epsilon_2 = ab^{q^2} + a^{q^2}b = ab + ab = 0,$$
$$\epsilon_3 = ab^{q^3} + a^{q^3}b = ab^q + a^q b = \epsilon_1,$$
$$\epsilon_4 = ab^{q^4} + a^{q^4}b = ab + ab = 0.$$

Continuing in this way we complete the proof of (3) of the proposition.

Finally we prove (1) of the proposition. First we show that k is even. Indeed, otherwise k is odd and $a, b \in \mathbb{F}_{q^k}$ and $a, b \in \mathbb{F}_{q^2}$ by (2), we have $a, b \in \mathbb{F}_{q^2} \cap \mathbb{F}_{q^k} = \mathbb{F}_q$. This contradicts to the assumption that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$. Hence k is even. Then by (4.12) we have

$$ab^{q^m} \in \mathbb{F}_{q^m}. \tag{4.17}$$

As k is even and $m = k/2$, we have that

$$m = \begin{cases} \text{even} & \text{if } k \equiv 0 \bmod 4, \\ \text{odd} & \text{if } k \equiv 2 \bmod 4. \end{cases} \tag{4.18}$$

If $k \equiv 2$ mod 4, then by (4.17) and (4.18) we have that

$$ab^{q^m} = ab^q \in \mathbb{F}_{q^2} \cap \mathbb{F}_{q^m} = \mathbb{F}_q. \tag{4.19}$$

Then

$$\left(ab^q\right)^q = a^q b^{q^2} = a^q b \in \mathbb{F}_q. \tag{4.20}$$

Using (4.19) and (4.20) we get that

$$\epsilon_1 = ab^q + a^q b = 0,$$

which is a contradiction. Therefore using (4.18) we complete the proof of the proposition. □

4.2. Case $\epsilon_2 = \epsilon_1$

In this subsection we consider the case that $\epsilon_2 = \epsilon_1$.

Proposition 4.4. *We keep the notation and assumptions as above. If $\epsilon_2 = \epsilon_1$, then we have that*

(1) $3 \mid k$,
(2) $a, b \in \mathbb{F}_{q^3}$,
(3) $\epsilon_1 = \epsilon_4 = \epsilon_7 = \cdots = \epsilon_{m-2}$, $\epsilon_2 = \epsilon_5 = \epsilon_8 = \cdots = \epsilon_{m-1} = \epsilon_1$, *and* $\epsilon_3 = \epsilon_6 = \epsilon_9 = \cdots = \epsilon_{m-3} = 0$. *Moreover $\epsilon_m = \epsilon_1$ if k is odd.*

Proof. Using (4.10), Lemma 4.2 and the fact that $\epsilon_2 = \epsilon_1$, we obtain that

$$v^q \epsilon_1 = \epsilon_1^2 + \epsilon_1^2 \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}, \tag{4.21}$$

where $v = ab$. Dividing (4.21) by ϵ_1 we get that

$$v^q = \epsilon_1 + \epsilon_1 \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}. \tag{4.22}$$

Taking the square of (4.22) we have that

$$\begin{aligned} v^{2q} &= \epsilon_1^2 + \epsilon_1^2 \sum_{i=1}^{t} \left(\epsilon_1 v^{q+1}\right)^{2^i} \\ &= \epsilon_1^2 + \epsilon_1^2 \epsilon_1^q v^{q(q+1)} + \epsilon_1^2 \sum_{i=1}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i} \\ &= \epsilon_1^2 + v^{q(q+1)} + \epsilon_1^2 \sum_{i=1}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}, \end{aligned} \tag{4.23}$$

where we use the facts that $\mathbb{F}_4 \subseteq \mathbb{F}_q$, $\epsilon_1^q = \epsilon_1$ and $\epsilon_1^3 = 1$.

Note that (4.21) is equivalent to

$$\epsilon_1 v^q = \epsilon_1^2 + v^{q+1} + \sum_{i=1}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}. \tag{4.24}$$

Adding (4.23) and (4.24) we get that

$$v^{2q} + \epsilon_1 v^q = v^{q+1} + v^{q(q+1)}. \tag{4.25}$$

Dividing (4.25) by v^q and rearranging the terms we conclude that

$$v + v^q + v^{q^2} = \epsilon_1. \tag{4.26}$$

We consider the equation

$$Z^2 + Z + \epsilon_1 v^{q+1} = 0. \tag{4.27}$$

We will show that the set of solutions of the equation in (4.27) is $\{va^{q-1}/\epsilon_1, vb^{q-1}/\epsilon_1\}$. First note that $va^{q-1}/\epsilon_1 \neq vb^{q-1}/\epsilon_1$. Indeed, otherwise $a^{q-1} = b^{q-1}$ and hence $a/b \in \mathbb{F}_q$, which implies a contradiction to the fact that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$. Using (4.10) we have

$$\frac{va^{q-1}}{\epsilon_1} + \frac{vb^{q-1}}{\epsilon_1} = \frac{a^q b + ab^q}{\epsilon_1} = 1.$$

Moreover we also have

$$\left(\frac{va^{q-1}}{\epsilon_1}\right)\left(\frac{vb^{q-1}}{\epsilon_1}\right)=\frac{a^2b^2a^{q-1}b^{q-1}}{\epsilon_1^2}=\epsilon_1(ab)^{q+1}=\epsilon_1 v^{q+1}.$$

These imply that $\{va^{q-1}/\epsilon_1, vb^{q-1}/\epsilon_1\}$ is the set of solutions of the equation in (4.27).

Let z be an arbitrary element of $\{va^{q-1}/\epsilon_1, vb^{q-1}/\epsilon_1\}$. Using (4.27), its square, its 4-th power, ..., and its $q/2$-th power we obtain that

$$\begin{aligned} z^2+z&=\epsilon_1 v^{q+1},\\ z^4+z^2&=\left(\epsilon_1 v^{q+1}\right)^2,\\ &\vdots\\ z^q+z^{q/2}&=\left(\epsilon_1 v^{q+1}\right)^{q/2}. \end{aligned} \tag{4.28}$$

Summing the equations in (4.28) we get that

$$z^q+z=\sum_{i=0}^{t-1}\left(\epsilon_1 v^{q+1}\right)^{2^i}. \tag{4.29}$$

Multiplying (4.21) by ϵ_1 we have

$$\epsilon_1^2 v^q=1+\sum_{i=0}^{t-1}\left(\epsilon_1 v^{q+1}\right)^{2^i}. \tag{4.30}$$

Combining (4.29) and (4.30) we obtain

$$z^q=z+1+\epsilon_1^2 v^q. \tag{4.31}$$

Taking the q-th power of (4.31) we get that

$$\begin{aligned} z^{q^2}&=z^q+1+\epsilon_1^2 v^{q^2}\\ &=\left(z+1+\epsilon_1^2 v^q\right)+1+\epsilon_1^2 v^{q^2}\\ &=z+\epsilon_1^2 v^q+\epsilon_1^2 v^{q^2}. \end{aligned} \tag{4.32}$$

Using (4.31) and (4.32) we have

$$\begin{aligned} z^{q^2+q}&=z^2+z\left(1+\epsilon_1^2 v^q+\epsilon_1^2 v^q+\epsilon_1^2 v^{q^2}\right)+\epsilon_1^2 v^q+\epsilon_1^2 v^{q^2}+\epsilon_1 v^{2q}+\epsilon_1 v^{q^2+q}\\ &=\left(z+\epsilon_1 v^{q+1}\right)+z\left(1+\epsilon_1^2 v^{q^2}\right)+\epsilon_1^2 v^q+\epsilon_1^2 v^{q^2}+\epsilon_1 v^{2q}+\epsilon_1 v^{q^2+q}\\ &=z\left(\epsilon_1^2 v^{q^2}\right)+\left(\epsilon_1^2 v^q+\epsilon_1^2 v^{q^2}+\epsilon_1 v^{q+1}+\epsilon_1 v^{2q}+\epsilon_1 v^{q^2+q}\right). \end{aligned} \tag{4.33}$$

From (4.26) we obtain that

$$\epsilon_1 v^{q+1}+\epsilon_1 v^{2q}+\epsilon_1 v^{q^2+q}=\epsilon_1 v^q\left(v+v^q+v^{q^2}\right)=\epsilon_1^2 v^q. \tag{4.34}$$

Combining (4.33) and (4.34) we conclude that

$$z^{q^2+q} = z\big(\epsilon_1^2 v^{q^2}\big) + \epsilon_1^2 v^{q^2}. \tag{4.35}$$

Then using (4.35) we get that

$$\begin{aligned} z^{q^2+q+1} &= z^2\big(\epsilon_1^2 v^{q^2}\big) + z\epsilon_1^2 v^{q^2} \\ &= \big(z + \epsilon_1 v^{q+1}\big)\epsilon_1^2 v^{q^2} + z\epsilon_1^2 v^{q^2} \\ &= v^{q^2+q+1}. \end{aligned} \tag{4.36}$$

For $z = va^{q-1}/\epsilon_1$, from (4.36) we obtain that

$$v^{q^2+q+1}\frac{a^{q^3-1}}{\epsilon_1^{q^2+q+1}} = v^{q^2+q+1} \quad \text{and hence} \quad a^{q^3-1} = 1, \tag{4.37}$$

where we use that $\epsilon_1^{q^2+q+1} = \epsilon_1^3 = 1$. Therefore $a \in \mathbb{F}_{q^3}$. Similarly putting $z = vb^{q-1}/\epsilon_1$ in (4.36) we obtain that $b \in \mathbb{F}_{q^3}$.

Next we prove (3) of the proposition. This part of the proof is similar to the proof of (3) of Proposition 4.3. As $a, b \in \mathbb{F}_{q^3}$, using (4.10) and (4.11) we obtain that

$$\begin{aligned} \epsilon_3 &= ab^{q^3} + a^{q^3}b = ab + ab = 0, \\ \epsilon_4 &= ab^{q^4} + a^{q^4}b = ab^q + a^qb = \epsilon_1, \\ \epsilon_5 &= ab^{q^5} + a^{q^5}b = ab^{q^2} + a^{q^2}b = \epsilon_2 = \epsilon_1, \\ \epsilon_6 &= ab^{q^6} + a^{q^6}b = ab + ab = 0. \end{aligned}$$

Continuing in this way we complete the proof of (3) of the proposition.

Finally we prove (1) of the proposition. As $a, b \in \mathbb{F}_{q^3}$ and $\{a, b\}$ is linearly independent over $\mathbb{F}_q$, at least one of a, b is in $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$. Recall that $a, b \in \mathbb{F}_{q^k}$. Then we obtain that $3 \mid k$. Indeed, otherwise if $a \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ (or $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$), then $a \in \mathbb{F}_{q^3} \cap \mathbb{F}_{q^k} = \mathbb{F}_q$ (or $b \in \mathbb{F}_q$), which is a contradiction. This completes the proof. □

4.3. Case $\epsilon_2 \neq \epsilon_1$

In this subsection we consider the case that $\epsilon_2 \notin \{0, \epsilon_1\}$.

Proposition 4.5. *We keep the notation and assumptions as above. If $\epsilon_2 \notin \{0, \epsilon_1\}$, then we have that*

(1) $5 \mid k$,
(2) $a, b \in \mathbb{F}_{q^5}$,
(3) $\epsilon_1 = \epsilon_6 = \epsilon_{11} = \cdots = \epsilon_{m-4}$, $\epsilon_2 = \epsilon_7 = \epsilon_{12} = \cdots = \epsilon_{m-3}$, $\epsilon_3 = \epsilon_8 = \epsilon_{13} = \cdots = \epsilon_{m-2} = \epsilon_2$, $\epsilon_4 = \epsilon_9 = \epsilon_{14} = \cdots = \epsilon_{m-1} = \epsilon_1$, *and* $\epsilon_5 = \epsilon_{10} = \epsilon_{15} = \cdots = \epsilon_{m-5} = 0$.
Moreover $\epsilon_m = \epsilon_2$ if k is odd.

Proof. Using (4.10) and Lemma 4.2 we obtain that

$$v^q\epsilon_2 = \epsilon_1^2 + \epsilon_1^2 \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i} = \epsilon_1^2 + \epsilon_1^2\epsilon_1 v^{q+1} + \epsilon_1^2 \sum_{i=1}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}. \tag{4.38}$$

Taking the square of (4.38) we get that

$$v^{2q}\epsilon_2^2 = \epsilon_1 + \epsilon_1 \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^{i+1}} = \epsilon_1 + \epsilon_1\epsilon_1^q v^{q(q+1)} + \epsilon_1 \sum_{i=1}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}. \tag{4.39}$$

Multiplying (4.39) by ϵ_1 and then adding the result to (4.38) we obtain that

$$v^{2q}\epsilon_1\epsilon_2^2 + v^q\epsilon_2 = \left(\epsilon_1^2 + \epsilon_1^2\epsilon_1^q v^{q(q+1)}\right) + \left(\epsilon_1^2 + \epsilon_1^2\epsilon_1 v^{q+1}\right) = v^{q^2+q} + v^{q+1}. \tag{4.40}$$

Dividing (4.40) by v^q we get that

$$v^q\epsilon_1\epsilon_2^2 + \epsilon_2 = v^{q^2} + v. \tag{4.41}$$

Taking the q-th power of (4.41) and then multiplying the result with $\epsilon_1^2\epsilon_2$ we obtain that

$$v^{q^2} + \epsilon_1^2\epsilon_2^2 = \epsilon_1^2\epsilon_2 v^{q^3} + \epsilon_1^2\epsilon_2 v^q. \tag{4.42}$$

Taking the q^2-th power of (4.41) we have that

$$v^{q^3}\epsilon_1\epsilon_2^2 + \epsilon_2 = v^{q^4} + v^{q^2}. \tag{4.43}$$

Adding (4.41), (4.42) and (4.43) we get that

$$v^{q^4} + \left(\epsilon_1^2\epsilon_2 + \epsilon_1\epsilon_2^2\right)v^{q^3} + \left(\epsilon_1^2\epsilon_2 + \epsilon_1\epsilon_2^2\right)v^q + v = \epsilon_1^2\epsilon_2^2. \tag{4.44}$$

Note that $\epsilon_1 + \epsilon_2 \neq 0$ as $\epsilon_2 \neq \epsilon_1$. Moreover, as $\epsilon_1\epsilon_2 \neq 0$, we have

$$\epsilon_1 + \epsilon_2 \neq \epsilon_1 \quad \text{and} \quad \epsilon_1 + \epsilon_2 \neq \epsilon_2.$$

Therefore the set $\{\epsilon_1, \epsilon_2, \epsilon_1 + \epsilon_2\}$ consists of the three distinct nonzero elements of $\mathbb{F}_4$ and hence

$$\epsilon_1\epsilon_2(\epsilon_1 + \epsilon_2) = \epsilon_1^2\epsilon_2 + \epsilon_1\epsilon_2^2 = 1. \tag{4.45}$$

Using (4.44) and (4.45) we get that

$$v^{q^4} + v^{q^3} + v^{q^2} + v^q + v = \epsilon_1^2\epsilon_2^2. \tag{4.46}$$

Recall from the proof of Proposition 4.4 that the set $\{va^{q-1}/\epsilon_1, vb^{q-1}/\epsilon_1\}$ is the set of the solutions of the equation

$$Z^2 + Z = \epsilon_1 v^{q+1}. \tag{4.47}$$

In the rest of this proof, we follow a similar but more involved method than the one in the proof of Proposition 4.4. Let z be an arbitrary element of $\{va^{q-1}/\epsilon_1, vb^{q-1}/\epsilon_1\}$. As in (4.29) using (4.47) we obtain that

$$z^q + z = \sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i}. \tag{4.48}$$

Multiplying (4.38) with ϵ_1 we get that

$$\sum_{i=0}^{t-1} \left(\epsilon_1 v^{q+1}\right)^{2^i} = 1 + \epsilon_1\epsilon_2 v^q. \tag{4.49}$$

Combining (4.48) and (4.49) we have

$$z^q = z + 1 + \epsilon_1\epsilon_2 v^q. \tag{4.50}$$

Using (4.50) and (4.47) we obtain that

$$\begin{aligned} z^{q+1} &= z^2 + z\left(1 + \epsilon_1\epsilon_2 v^q\right) \\ &= \left(z + \epsilon_1 v^{q+1}\right) + z\left(1 + \epsilon_1\epsilon_2 v^q\right) \\ &= z\left(\epsilon_1\epsilon_2 v^q\right) + \epsilon_1 v^{q+1}. \end{aligned} \tag{4.51}$$

Taking the q-th power of (4.51) and then using (4.50) we have

$$\begin{aligned} z^{q^2+q} &= z^q\left(\epsilon_1\epsilon_2 v^{q^2}\right) + \epsilon_1 v^{q^2+q} \\ &= \left(z + 1 + \epsilon_1\epsilon_2 v^q\right)\left(\epsilon_1\epsilon_2 v^{q^2}\right) + \epsilon_1 v^{q^2+q} \\ &= z\left(\epsilon_1\epsilon_2 v^{q^2}\right) + \epsilon_1\epsilon_2 v^{q^2} + \epsilon_1^2\epsilon_2^2 v^{q^2+q} + \epsilon_1 v^{q^2+q}. \end{aligned}$$

Then multiplying by z and using (4.47) we get that

$$\begin{aligned} z^{q^2+q+1} &= z^2\left(\epsilon_1\epsilon_2 v^{q^2}\right) + z\left(\epsilon_1\epsilon_2 v^{q^2} + \epsilon_1^2\epsilon_2^2 v^{q^2+q} + \epsilon_1 v^{q^2+q}\right) \\ &= \left(z + \epsilon_1 v^{q+1}\right)\left(\epsilon_1\epsilon_2 v^{q^2}\right) + z\left(\epsilon_1\epsilon_2 v^{q^2} + \epsilon_1^2\epsilon_2^2 v^{q^2+q} + \epsilon_1 v^{q^2+q}\right) \\ &= z\left(\epsilon_1^2\epsilon_2^2 v^{q^2+q} + \epsilon_1 v^{q^2+q}\right) + \epsilon_1^2\epsilon_2 v^{q^2+q+1}. \end{aligned} \tag{4.52}$$

Taking the q-th power of (4.52) and then using (4.50) we have

$$\begin{aligned} z^{q^3+q^2+q} &= z^q\left(\epsilon_1^2\epsilon_2^2 v^{q^3+q^2} + \epsilon_1 v^{q^3+q^2}\right) + \epsilon_1^2\epsilon_2 v^{q^3+q^2+q} \\ &= \left(z + 1 + \epsilon_1\epsilon_2 v^q\right)\left(\epsilon_1^2\epsilon_2^2 v^{q^3+q^2} + \epsilon_1 v^{q^3+q^2}\right) + \epsilon_1^2\epsilon_2 v^{q^3+q^2+q} \\ &= z\left(\epsilon_1^2\epsilon_2^2 v^{q^3+q^2} + \epsilon_1 v^{q^3+q^2}\right) + \epsilon_1^2\epsilon_2^2 v^{q^3+q^2} + \epsilon_1 v^{q^3+q^2} + v^{q^3+q^2+q}. \end{aligned}$$

Then multiplying by z and then using (4.47) we get that

$$\begin{aligned} z^{q^3+q^2+q+1} &= \big(z+\epsilon_1 v^{q+1}\big)\big(\epsilon_1^2\epsilon_2^2 v^{q^3+q^2}+\epsilon_1 v^{q^3+q^2}\big)+z\big(\epsilon_1^2\epsilon_2^2 v^{q^3+q^2}+\epsilon_1 v^{q^3+q^2}+v^{q^3+q^2+q}\big) \\ &= z\big(v^{q^3+q^2+q}\big)+\big(\epsilon_1^2+\epsilon_2^2\big)v^{q^3+q^2+q+1}. \end{aligned} \tag{4.53}$$

Taking the q-th power of (4.53) and then using (4.50) we obtain that

$$\begin{aligned} z^{q^4+q^3+q^2+q} &= \big(z+1+\epsilon_1\epsilon_2 v^q\big)\big(v^{q^4+q^3+q^2}\big)+\big(\epsilon_1^2+\epsilon_2^2\big)v^{q^4+q^3+q^2+q} \\ &= z\big(v^{q^4+q^3+q^2}\big)+\big(\epsilon_1^2+\epsilon_2^2+\epsilon_1\epsilon_2\big)v^{q^4+q^3+q^2+q}+v^{q^4+q^3+q^2}. \end{aligned} \tag{4.54}$$

As $\epsilon_1 \neq \epsilon_2$ we have that $\epsilon_1\epsilon_2 \neq \epsilon_1^2$, $\epsilon_1\epsilon_2 \neq \epsilon_2^2$ and $\epsilon_1^2 \neq \epsilon_2^2$. Therefore the set $\{\epsilon_1^2, \epsilon_2^2, \epsilon_1\epsilon_2\}$ consists of the three distinct nonzero elements of $\mathbb{F}_4$ and hence

$$\epsilon_1^2+\epsilon_2^2+\epsilon_1\epsilon_2 = 0. \tag{4.55}$$

Combining (4.54) and (4.55) we get that

$$z^{q^4+q^3+q^2+q} = z\big(v^{q^4+q^3+q^2}\big)+v^{q^4+q^3+q^2}.$$

Then multiplying by z and using (4.47) we obtain that

$$z^{q^4+q^3+q^2+q+1} = \big(z+\epsilon_1 v^{q+1}\big)\big(v^{q^4+q^3+q^2}\big)+zv^{q^4+q^3+q^2} = \epsilon_1 v^{q^4+q^3+q^2+q+1}. \tag{4.56}$$

For $z = va^{q-1}/\epsilon_1$ in (4.56) we obtain that

$$v^{q^4+q^3+q^2+q+1}\frac{a^{q^5-1}}{\epsilon_1^{q^4+q^3+q^2+q+1}} = \epsilon_1 v^{q^4+q^3+q^2+q+1} \tag{4.57}$$

and hence

$$a^{q^5-1} = \epsilon_1^5\epsilon_1 = \epsilon_1^6 = 1. \tag{4.58}$$

Therefore $a \in \mathbb{F}_{q^5}$. Similarly putting $z = vb^{q-1}/\epsilon_1$ in (4.56) we conclude that $b \in \mathbb{F}_{q^5}$.

Next we prove (3) of the proposition, whose proof is slightly different from the ones in Propositions 4.3 and 4.4. As $a, b \in \mathbb{F}_{q^5}$, using (4.10) and (4.11) we obtain that

$$\begin{aligned} \epsilon_5 &= ab^{q^5}+a^{q^5}b = ab+ab = 0, \\ \epsilon_6 &= ab^{q^6}+a^{q^6}b = ab^q+a^qb = \epsilon_1, \\ \epsilon_7 &= ab^{q^7}+a^{q^7}b = ab^{q^2}+a^{q^2}b = \epsilon_2, \\ \epsilon_8 &= ab^{q^8}+a^{q^8}b = ab^{q^3}+a^{q^3}b = \epsilon_3, \\ \epsilon_9 &= ab^{q^9}+a^{q^9}b = ab^{q^4}+a^{q^4}b = \epsilon_4. \end{aligned} \tag{4.59}$$

Here we also use the fact that $\epsilon_3 \in \mathbb{F}_q \subseteq \mathbb{F}_{q^2}$ and $\epsilon_4 \in \mathbb{F}_q$. We have

$$\begin{aligned} \epsilon_3 &= \epsilon_3^{q^2} = \big(ab^{q^3}+a^{q^3}b\big)^{q^2} = a^{q^2}b+ab^{q^2} = \epsilon_2, \\ \epsilon_4 &= \epsilon_4^q = (ab^{q^4}+a^{q^4}b)^q = a^qb+ab^q = \epsilon_1. \end{aligned} \tag{4.60}$$

Combining (4.59) and (4.60) we obtain that

$$\epsilon_3 = \epsilon_2, \qquad \epsilon_4 = \epsilon_1, \qquad \epsilon_5 = 0, \qquad \epsilon_6 = \epsilon_1, \qquad \epsilon_7 = \epsilon_2.$$

Continuing in this way we complete the proof of (3) of the proposition.

Finally we prove (1) of the proposition. As $a, b \in \mathbb{F}_{q^k}$ and $\{a, b\}$ is linearly independent over $\mathbb{F}_q$, either a or b is in $\mathbb{F}_{q^5} \setminus \mathbb{F}_q$. Then there exists an element in $\mathbb{F}_{q^k}$ which is also in $\mathbb{F}_{q^5} \setminus \mathbb{F}_q$. This implies that $\mathbb{F}_{q^5} \subseteq \mathbb{F}_{q^k}$ and hence $5 \mid k$, which completes the proof. □

5. Sufficient conditions

In this section we prove the sufficient conditions of Theorem 3.1. We present our results in three subsections, which correspond to the subsections of Section 4. We note that combining the necessary and sufficient conditions in Theorem 3.1, we obtain various nonexistence results that we present in Section 7 below. We find it interesting to note that the result in this section are quite rigid. Namely small changes to the statements in Sections 5.1, 5.2 and 5.3 below transform these existence results to the corresponding nonexistence results of Section 7.2.

5.1. Case $\epsilon_2 = 0$

In this subsection we obtain the sufficiency conditions corresponding to Section 4.1. Namely we prove the following proposition.

Proposition 5.1. *Let $q = 4^r$, $\epsilon_0 \in \mathbb{F}_4$ and $\epsilon_1 \in \mathbb{F}_4 \setminus \{0\}$. We have the following:*

(1) *If $\epsilon_0 \neq 0$, $\epsilon_0 \neq \epsilon_1$ and r is odd, then there exist $a, b \in \mathbb{F}_{q^2}$ such that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$ and*

$$\begin{aligned} \epsilon_0 &= ab, \\ \epsilon_1 &= ab^q + a^q b. \end{aligned}$$

(2) *Assume that one of the following holds:*
  i. *$\epsilon_0 \neq 0$, $\epsilon_0 \neq \epsilon_1$ and r is even,*
  ii. *$\epsilon_0 = 0$ or $\epsilon_0 = \epsilon_1$ (and r is an arbitrary positive integer).*

  Then there exist $a, b \in \mathbb{F}_{q^2}$ and $s \in \mathbb{F}_q$ such that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$, $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$, and

$$\begin{aligned} \epsilon_0 &= a^2 + ab + sb^2, \\ \epsilon_1 &= ab^q + a^q b. \end{aligned}$$

Proof. First we prove (1) and we assume that $\epsilon_0 \neq 0$, $\epsilon_0 \neq \epsilon_1$ and r is odd. As r is odd, it is easy to observe that $q = 4^r \equiv -1 \bmod 5$ and hence $5 \mid (q+1)$. Let ω be a primitive element in $\mathbb{F}_{q^2}$ and for $i \in \{1, 2\}$ we set that

$$\alpha_i = \omega^{i\frac{q+1}{5}}, \qquad a_i = \alpha_i \quad \text{and} \quad b_i = \frac{\epsilon_0}{\alpha_i}.$$

Note that it is enough to prove that

$$\left\{a_i^{q-1} + b_i^{q-1} \colon i \in \{1, 2\}\right\} = \mathbb{F}_4 \setminus \mathbb{F}_2. \tag{5.1}$$

Indeed, for $\epsilon_0 \in \mathbb{F}_4 \setminus \{0\}$, we have that

$$\{\epsilon_1/\epsilon_0\colon\ \epsilon_1 \in \mathbb{F}_4,\ \epsilon_1 \neq 0 \text{ and } \epsilon_1 \neq \epsilon_0\} = \mathbb{F}_4 \setminus \mathbb{F}_2.$$

Let $A = \omega^{\frac{q^2-1}{5}}$. Note that $\alpha_1^{q-1} = A$ and $\alpha_2^{q-1} = A^2$. Hence (5.1) is equivalent to

$$\left\{A + \frac{1}{A}, A^2 + \frac{1}{A^2}\right\} = \left\{A + A^4, A^2 + A^3\right\} = \mathbb{F}_4 \setminus \mathbb{F}_2. \tag{5.2}$$

As $A^5 = 1$ and ω is primitive we have $A \neq 1$,

$$\min\left\{i \geqslant 1\colon\ A^i = 1\right\} = 5 \quad \text{and} \quad A^4 + A^3 + A^2 + A + 1 = 0. \tag{5.3}$$

Hence using (5.3) we obtain that

$$A + A^4 \neq A^2 + A^3, \qquad A + A^4 \notin \{0, 1\} \quad \text{and} \quad A^2 + A^3 \notin \{0, 1\}. \tag{5.4}$$

Combining (5.2) and (5.4) we note that it is enough to prove that

$$\left(A + A^4\right)^3 = \left(A^2 + A^3\right)^3 = 1. \tag{5.5}$$

We have

$$\begin{aligned} \left(A + A^4\right)^3 &= A^3 + A^2A^4 + AA^8 + A^{12} = A^3 + A + A^4 + A^2, \quad \text{and} \\ \left(A^2 + A^3\right)^3 &= A^6 + A^4A^3 + A^2A^6 + A^9 = A + A^2 + A^3 + A^4. \end{aligned} \tag{5.6}$$

Combining (5.3) and (5.6) we obtain (5.5), which completes the proof of (1).

Next we prove (2) and assume that one of the conditions in (2) holds. Let $s \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ and let γ be an arbitrary element of $\mathbb{F}_4 \setminus \mathbb{F}_2$. We put

$$\theta = \begin{cases} 0 & \text{if } \epsilon_0 = 0, \\ 1 & \text{if } \epsilon_0 = \epsilon_1, \\ \gamma & \text{if } \epsilon_0 \neq 0,\ \epsilon_0 \neq \epsilon_1 \text{ and } r \text{ is even.} \end{cases}$$

Note that

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(1) = 2r = 0,$$

and if r is even

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\gamma) = \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2} \circ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_4}(\gamma) = \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(r\gamma) = 0.$$

Therefore $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s + \theta) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\theta) = 1 + 0 = 1$.

We consider the polynomial

$$x^2 + x + s + \theta \in \mathbb{F}_q[x]. \tag{5.7}$$

As $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s+\theta)=1$, using Hilbert's Theorem 90 (cf. [14, Theorem 2.25]) we obtain that the polynomial in (5.7) is irreducible. Therefore there exists $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that

$$\alpha^2+\alpha+s+\theta=0. \tag{5.8}$$

Using (5.8), its square, its 4-th power, ..., and its $q/2$-th power we obtain that

$$\begin{aligned} \alpha^2+\alpha &= s+\theta, \\ \alpha^4+\alpha^2 &= (s+\theta)^2, \\ \alpha^8+\alpha^4 &= (s+\theta)^4, \\ &\vdots \\ \alpha^q+\alpha^{q/2} &= (s+\theta)^{q/2}. \end{aligned} \tag{5.9}$$

Summing the equations in (5.9) we get that

$$\alpha^q+\alpha=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s+\theta)=1. \tag{5.10}$$

We put

$$a=\epsilon_1^2\alpha \quad \text{and} \quad b=\epsilon_1^2.$$

As $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, the set $\{a,b\}$ is linearly independent over $\mathbb{F}_q$. Moreover we have

$$\begin{aligned} a^2+ab+sb^2 &= \left(\alpha^2+\alpha+s\right)b^2 \\ &= \theta\epsilon_1 \\ &= \begin{cases} 0 & \text{if } \epsilon_0=0, \\ \epsilon_1 & \text{if } \epsilon_0=\epsilon_1, \\ \gamma\epsilon_1 & \text{if } \epsilon_0\neq 0,\ \epsilon_0\neq\epsilon_1 \text{ and } r \text{ is even.} \end{cases} \end{aligned}$$

Using (5.10) we also have

$$ab^q+a^qb=\left(\alpha+\alpha^q\right)b^{q+1}=b^{q+1}=\left(\epsilon_1^2\right)^q\epsilon_1^2=\epsilon_1^2\epsilon_1^2=\epsilon_1.$$

This completes the proof of (1). □

5.2. Case $\epsilon_2=\epsilon_1$

In this subsection we obtain the sufficiency conditions corresponding to Section 4.2. It is given in the following proposition.

Proposition 5.2. *Let q be a power of 4. Let $\epsilon_0 \in \mathbb{F}_4$ and $\epsilon_1 \in \mathbb{F}_4 \setminus \{0\}$. We have the following*:

(1) *If $\epsilon_0 = \epsilon_1$ (in particular $\epsilon_0 \neq 0$), then there exist $a, b \in \mathbb{F}_{q^3}$ such that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$ and*

$$\begin{aligned} \epsilon_0 &= ab, \\ \epsilon_1 &= ab^q + a^q b, \quad \textit{and} \\ ab^{q^2} + a^{q^2} b &= ab^q + a^q b. \end{aligned}$$

(2) *If $\epsilon_0 \neq \epsilon_1$ (for example if $\epsilon_0 = 0$), then there exists $\{a, b, c\} \subseteq \mathbb{F}_{q^3}$ such that $\{a, b, c\}$ is linearly independent over $\mathbb{F}_q$ and*

$$\begin{aligned} \epsilon_0 &= c^2 + ab, \\ \epsilon_1 &= ab^q + a^q b, \quad \textit{and} \\ ab^{q^2} + a^{q^2} b &= ab^q + a^q b. \end{aligned}$$

Proof. We first prove (1). Assume that $\epsilon_0 = \epsilon_1$. Let ω be a primitive element in $\mathbb{F}_{q^3}$. As $q \equiv 1 \bmod 3$, we have $3 \mid q^2 + q + 1$. We set $\alpha = \omega^{(q^2+q+1)/3}$. Then the order of α is $3(q-1)$, $\alpha^{3(q-1)} - 1 = (\alpha^{q-1} - 1)(\alpha^{2(q-1)} + \alpha^{q-1} + 1)$ and hence

$$\alpha^{2(q-1)} + \alpha^{q-1} + 1 = 0. \tag{5.11}$$

We put $a = \epsilon_1^2 \alpha^{-2}$ and $b = \epsilon_1^2 \alpha^2$. Then $\frac{b}{a} = \alpha^4$ and $\alpha^{4(q-1)} \neq 1$, that is, $\frac{b}{a} \notin \mathbb{F}_q$, which implies that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$. Note that $2(q+1) \equiv 2 \cdot 2 \equiv 1 \bmod 3$ and hence $2(q^2-1) = 2(q-1)(q+1) \equiv q-1 \bmod 3(q-1)$. Hence we have that

$$\alpha^{2(q^2-1)} = \alpha^{q-1}, \qquad \alpha^{-2(q^2-1)} = \alpha^{2(q-1)}, \qquad \alpha^{-(q-1)} = \alpha^{2(q-1)}. \tag{5.12}$$

Using (5.11) and (5.12) we obtain that

$$\begin{aligned} ab &= \epsilon_1, \\ ab^q + a^q b &= \epsilon_1^{2(q+1)} \alpha^{2(q-1)} + \epsilon_1^{2(q+1)} \alpha^{-2(q-1)} = \epsilon_1, \\ ab^{q^2} + a^{q^2} b &= \epsilon_1^{2(q^2+1)} \alpha^{2(q^2-1)} + \epsilon_1^{2(q^2+1)} \alpha^{-2(q^2-1)} = \epsilon_1. \end{aligned}$$

This completes the proof of (1).

Next we prove (2). Assume that $\epsilon_0 \neq \epsilon_1$. We keep ω and α as in the proof of (1) and let $\beta = \alpha^2$. Note that $\gcd(2, 3(q-1)) = 1$ and hence the order of β is the same as the order of α, which is $3(q-1)$. We still have $a = \epsilon_1^2 \beta^{-1}$ and $b = \epsilon_1^2 \beta$. Then by the proof of (1) we have $ab = \epsilon_1$, $ab^q + a^q b = \epsilon_1$ and $ab^{q^2} + a^{q^2} b = \epsilon_1$.

Let $\eta \in \mathbb{F}_4 \setminus \{0\}$, $c = \eta^2$ and $\epsilon_0 = \eta + \epsilon_1$. It is enough to prove that the set $\{\eta^2, \epsilon_1^2 \beta^{-1}, \epsilon_1^2 \beta\}$ is linearly independent over $\mathbb{F}_q$. As $\eta^2, \epsilon_1^2 \in \mathbb{F}_4$, it is equivalent to show that the set $\{1, \beta^{-1}, \beta\}$ is linearly independent over $\mathbb{F}_q$. First we note that $\beta \notin \mathbb{F}_{q^2}$. Indeed, otherwise the order of β should divide $q^2 - 1 = (q+1)(q-1)$, and hence

$$3(q-1) \mid (q+1)(q-1) \quad \Rightarrow \quad 3 \mid (q+1),$$

which is a contradiction as $q \equiv 1 \bmod 3$. Now we show that $\{1, \beta^{-1}, \beta\}$ is linearly independent over $\mathbb{F}_q$. Otherwise there exist $c_1, c_2, c_3 \in \mathbb{F}_q$ such that $c_1 + c_2\beta^{-1} + c_3\beta = 0$, or equivalently $c_2 + c_1\beta + c_3\beta^2 = 0$. We consider the polynomial

$$c_2 + c_1 x + c_3 x^2 \in \mathbb{F}_q[x]. \tag{5.13}$$

If $c_3 = 0$, then any root of the polynomial in (5.13) is in $\mathbb{F}_q$. If $c_3 \neq 0$, then the polynomial in (5.13) is reducible or irreducible over $\mathbb{F}_q$. If it is reducible, then its roots are only in $\mathbb{F}_q \subseteq \mathbb{F}_{q^2}$. If it is irreducible, then its roots are in $\mathbb{F}_{q^2}$. As β is a root of the polynomial in (5.13), these imply that $\beta \in \mathbb{F}_{q^2}$, which is a contradiction. This completes the proof of (2). □

5.3. Case $\epsilon_2 \neq \epsilon_1$

In this subsection we obtain the sufficiency conditions corresponding to Section 4.3. This is the most difficult part. Nevertheless there is a special subcase, which is much easier. We start with this subcase in the following lemma.

Lemma 5.3. *Let $q = 4^r$, $\epsilon_0 \in \mathbb{F}_4$, $\epsilon_1, \epsilon_2 \in \mathbb{F}_4 \setminus \{0\}$ and $\epsilon_2 \neq \epsilon_1$. If $\epsilon_0 \notin \{0, \epsilon_1, \epsilon_2\}$ and r is even, then there exist $a, b \in \mathbb{F}_{q^5}$ such that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$ and*

$$\begin{aligned} \epsilon_0 &= ab, \\ \epsilon_1 &= ab^q + a^q b, \quad \textit{and} \\ \epsilon_2 &= ab^{q^2} + a^{q^2} b. \end{aligned}$$

Proof. As $q = 4^r$ and r is even, we have $q \equiv 1 \bmod 5$ and hence $5 \mid q^4 + q^3 + q^2 + q + 1$. Let ω be a primitive element in $\mathbb{F}_{q^5}$ and define $\beta = \omega^{\frac{q^4+q^3+q^2+q+1}{5}}$. Then the order of β is $5(q-1)$. Let

$$A = \beta^{(q-1)}, \qquad u_1 = A^3 + A^2 \quad \text{and} \quad u_2 = A + A^4. \tag{5.14}$$

As $A^5 = 1$ and ω is primitive, we have $A \neq 1$,

$$\min\{i \geqslant 1\colon\ A^i = 1\} = 5 \quad \text{and} \quad A^4 + A^3 + A^2 + A + 1 = 0. \tag{5.15}$$

Moreover $u_1^2 = (A^3 + A^2)^2 = A^6 + A^4 = A + A^4 = u_2$, $u_2^2 = (A + A^4)^2 = A^2 + A^8 = A^2 + A^3 = u_1$ and hence u_1 and u_2 are the roots of the polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$. In particular $u_1, u_2 \in \mathbb{F}_4$. Using also (5.14) and (5.15) we obtain that

$$u_1 \neq u_2, \qquad \{u_1, u_2\} = \mathbb{F}_4 \setminus \mathbb{F}_2.$$

We first set $a = \epsilon_0^2\beta$ and $b = \epsilon_0^2\beta^{-1}$. They are independent over $\mathbb{F}_q$ as $(a/b)^{q-1} = \beta^{2(q-1)} \neq 1$. Now, we compute

$$\begin{aligned} ab &= \epsilon_0, \\ ab^q + a^q b &= \epsilon_0^{2(1+q)}\left(\beta^{1-q} + \beta^{q-1}\right) = \epsilon_0\left(A^{-1} + A\right) = \epsilon_0 u_2, \\ ab^{q^2} + a^{q^2} b &= \epsilon_0^{2(1+q^2)}\left(\beta^{1-q^2} + \beta^{q^2-1}\right) = \epsilon_0\left(A^{-(1+q)} + A^{q+1}\right) = \epsilon_0 u_1, \end{aligned}$$

where we use that $q \equiv 1 \bmod 5$ and hence $A^{q+1} = A^2$, $A^{-(1+q)} = A^3$.

Similarly if we set $a = \epsilon_0^2 \beta^2$ and $b = \epsilon_0^2 \beta^{-2}$, then we obtain that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$ and

$$\begin{aligned} ab &= \epsilon_0, \\ ab^q + a^q b &= \epsilon_0^{2(1+q)} \big(\beta^{2(1-q)} + \beta^{2(q-1)}\big) = \epsilon_0 \big(A^2 + A^3\big) = \epsilon_0 u_1, \\ ab^{q^2} + a^{q^2} b &= \epsilon_0^{2(1+q^2)} \big(\beta^{2(1-q^2)} + \beta^{2(q^2-1)}\big) = \epsilon_0 \big(A + A^4\big) = \epsilon_0 u_2. \end{aligned}$$

This completes the proof. □

Next we give a very technical lemma. It is related to [4, Lemma 2.3]. We find both [4, Lemma 2.3] and the following lemma very interesting. Using the following lemma we complete the sufficiency conditions in the most difficult case in Proposition 5.5 below. We have obtained the statement of the following lemma using various ad hoc techniques. Its statement complies exactly with the tools we need in order to complete the sufficiency conditions of the remaining cases of Theorem 3.1 in Proposition 5.5 below.

Lemma 5.4. *Let n be a non-negative integer and $q_0 = 4^{(5^n)}$. Let $e, d \in \mathbb{F}_4 \setminus \{0\}$ with $e \neq d$. Let $f(x) \in \mathbb{F}_4[x]$ be the polynomial depending on q_0, e and d defined as*

$$f(x) = x^{q_0+1}\big(1 + ex^{-2} + e^2x^{-4} + ex^{-8} + e^2x^{-16} + \cdots + e^2x^{-q_0}\big) + d. \tag{5.16}$$

Let y be a root of $f(x)$ in an extension field of $\mathbb{F}_{q_0}$. Then the following hold:

(1) $y \in \mathbb{F}_{q_0^5} \setminus \mathbb{F}_{q_0}$.
(2) $y^{2q_0} + de^2 y^{q_0+1} + y^2 = d^2e^2$.
(3) $y^{q_0^2+1} + y^{2q_0} = d^2e^2$.
(4) $y^{q_0^3+1} + y^{q_0^2+q_0} = e$.

Proof. As y is a root of $f(x)$ we have

$$1 + ey^{-2} + e^2y^{-4} + ey^{-8} + \cdots + e^2y^{-q_0} = dy^{-(q_0+1)}. \tag{5.17}$$

Taking the square of (5.17) we get

$$1 + e^2y^{-4} + ey^{-8} + e^2y^{-16} + \cdots + ey^{-2q_0} = d^2y^{-2(q_0+1)}. \tag{5.18}$$

Adding (5.17) and (5.18), we obtain

$$ey^{-2} + ey^{-2q_0} = dy^{-(q_0+1)} + d^2y^{-2(q_0+1)}. \tag{5.19}$$

Multiplying (5.19) by $e^2y^{2q_0+2}$ we get the identity in (2) of the lemma.

Next we prove the identity in (3) of the lemma. Multiplying (2) by de^2y^{-2} we have

$$de^2y^{2q_0-2} + d^2ey^{q_0-1} = de^2 + ey^{-2}. \tag{5.20}$$

Using (5.20), its square, its 4-th power, …, and its $q_0/2$-th power we obtain that

$$\begin{aligned} de^2y^{2(q_0-1)} + d^2ey^{q_0-1} &= de^2 + ey^{-2}, \\ d^2ey^{4(q_0-1)} + de^2y^{2(q_0-1)} &= d^2e + e^2y^{-4}, \\ de^2y^{8(q_0-1)} + d^2ey^{4(q_0-1)} &= de^2 + ey^{-8}, \\ &\vdots \\ d^2ey^{q_0(q_0-1)} + de^2y^{\frac{q_0}{2}(q_0-1)} &= d^2e + e^2y^{-q_0}. \end{aligned} \tag{5.21}$$

As $e, d \in \mathbb{F}_4 \backslash \{0\}$ with $e \neq d$ we have that $de^2 \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Then $de^2 + (de^2)^2 = de^2 + d^2e = 1$. Moreover $q_0 = 4^{(5^n)} = 2^{(2 \cdot 5^n)}$ and hence the number of equations in (5.21) is $2 \cdot 5^n$. Therefore summing the equations in (5.21), for the right-hand side we get

$$\begin{aligned} &5^n\big(de^2 + d^2e\big) + \big(ey^{-2} + e^2y^{-4} + ey^{-8} + \cdots + e^2y^{-q_0}\big) \\ &\quad = 1 + \big(ey^{-2} + e^2y^{-4} + ey^{-8} + \cdots + e^2y^{-q_0}\big) \\ &\quad = dy^{-(q_0+1)}, \end{aligned} \tag{5.22}$$

where we use (5.17) in the third equation in (5.22). Summing the equations in (5.21), for the left-hand side we have

$$d^2ey^{q_0(q_0-1)} + d^2ey^{q_0-1}. \tag{5.23}$$

Combining (5.22) and (5.23) we obtain that

$$d^2e\big(y^{q_0(q_0-1)} + y^{q_0-1}\big) = dy^{-(q_0+1)}. \tag{5.24}$$

Multiplying (5.24) by $de^2y^{q_0+1}$ we prove the identity in (3) of the lemma.

Now we prove the identity in (4) of the lemma. Multiplying (5.24) by de^2 we obtain

$$y^{q_0^2-q_0} + y^{q_0-1} = d^2e^2y^{-(q_0+1)}. \tag{5.25}$$

Taking the q_0-th power of (5.25) we get

$$y^{q_0^3-q_0^2} + y^{q_0^2-q_0} = d^2e^2y^{-(q_0^2+q_0)}. \tag{5.26}$$

Adding (5.25) and (5.26) we have

$$y^{q_0^3-q_0^2} + y^{q_0-1} = d^2e^2y^{-(q_0+1)} + d^2e^2y^{-(q_0^2+q_0)}. \tag{5.27}$$

Multiplying (5.27) by $y^{q_0^2+1}$ we arrive

$$y^{q_0^3+1} + y^{q_0^2+q_0} = d^2e^2y^{q_0^2-q_0} + d^2e^2y^{-q_0+1}. \tag{5.28}$$

Note that adding identities in (2) and (3) of the lemma we have

$$y^{q_0^2+1} = de^2y^{q_0+1} + y^2. \tag{5.29}$$

Multiplying (5.29) by $d^2e^2y^{-q_0-1}$ we get

$$d^2e^2y^{q_0^2-q_0}+d^2e^2y^{-q_0+1}=e. \tag{5.30}$$

Combining (5.28) and (5.30) we prove the identity in (4) of the lemma.

It remains to prove the identity in (1) of the lemma. Taking the q_0-th power of (5.29) we have

$$y^{q_0^3+q_0}=de^2y^{q_0^2+q_0}+y^{2q_0}. \tag{5.31}$$

Multiplying (5.31) by y^{-q_0+1} we get

$$y^{q_0^3+1}=de^2y^{q_0^2+1}+y^{q_0+1}. \tag{5.32}$$

Taking the q_0-th power of (5.32) we obtain

$$y^{q_0^4+q_0}=de^2y^{q_0^3+q_0}+y^{q_0^2+q_0}. \tag{5.33}$$

Multiplying (5.31) by de^2 and adding to (5.33) we have

$$y^{q_0^4+q_0}=\left(d^2e+1\right)y^{q_0^2+q_0}+de^2y^{2q_0}. \tag{5.34}$$

Multiplying (5.34) by y^{-q_0+1} we get

$$y^{q_0^4+1}=\left(d^2e+1\right)y^{q_0^2+1}+de^2y^{q_0+1}. \tag{5.35}$$

Taking the q_0-th power of (5.35) we obtain

$$y^{q_0^5+q_0}=\left(d^2e+1\right)y^{q_0^3+q_0}+de^2y^{q_0^2+q_0}. \tag{5.36}$$

Multiplying (5.36) by y^{-q_0} we get

$$y^{q_0^5}=\left(d^2e+1\right)y^{q_0^3}+de^2y^{q_0^2}. \tag{5.37}$$

Dividing (5.29) by y and then taking the q_0-th power of the result we obtain the identities

$$\begin{aligned} y^{q_0^2}&=de^2y^{q_0}+y,\\ y^{q_0^3}&=de^2y^{q_0^2}+y^{q_0}. \end{aligned} \tag{5.38}$$

Using (5.37) and the identities in (5.38) we obtain

$$\begin{aligned} y^{q_0^5}={}&\left(d^2e+1\right)\left(de^2y^{q_0^2}+y^{q_0}\right)+de^2y^{q_0^2}\left(1+de^2+de^2\right)y^{q_0^2}+\left(d^2e+1\right)y^{q_0}de^2y^{q_0}+y\\ &+\left(d^2e+1\right)y^{q_0}\left(de^2+d^2e+1\right)y^{q_0}+y. \end{aligned} \tag{5.39}$$

Note that $de^2\in\mathbb{F}_4\setminus\mathbb{F}_2$ as $d\neq e$ and $e,d\in\mathbb{F}_4\setminus\{0\}$. Hence $de^2+d^2e+1=\alpha^2+\alpha+1=0$, where α is a primitive element in $\mathbb{F}_4$. Hence using (5.39) we get

$$y^{q_0^5}=y,$$

which proves that $y \in \mathbb{F}_{q_0^5}$. Assume that $y \in \mathbb{F}_{q_0}$. Then using say (5.38), we obtain

$$y = \left(de^2 + 1\right)y,$$

which implies that $de^2 = 0$ as $y \neq 0$. This completes the proof. □

The following proposition gives the sufficiency conditions corresponding to Section 4.3.

Proposition 5.5. *Let $q = 4^r$, $\epsilon_0 \in \mathbb{F}_4$, $\epsilon_1, \epsilon_2 \in \mathbb{F}_4 \setminus \{0\}$ and $\epsilon_2 \neq \epsilon_1$. We have the following*:

(1) *If $\epsilon_0 \notin \{0, \epsilon_1, \epsilon_2\}$ and r is even, then there exist $a, b \in \mathbb{F}_{q^5}$ such that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$ and*

$$\begin{aligned} \epsilon_0 &= ab, \\ \epsilon_1 &= ab^q + a^q b, \quad \textit{and} \\ \epsilon_2 &= ab^{q^2} + a^{q^2} b. \end{aligned}$$

(2) *If $\epsilon_0 \notin \{0, \epsilon_1, \epsilon_2\}$ and r is odd, then there exist $a, b \in \mathbb{F}_{q^5}$ and $s \in \mathbb{F}_q$ such that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$, $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$, and*

$$\begin{aligned} \epsilon_0 &= a^2 + ab + sb^2, \\ \epsilon_1 &= ab^q + a^q b, \quad \textit{and} \\ \epsilon_2 &= ab^{q^2} + a^{q^2} b. \end{aligned}$$

(3) *If $\epsilon_0 \in \{0, \epsilon_1, \epsilon_2\}$, then there exist $a, b, c \in \mathbb{F}_{q^5}$ such that $\{a, b, c\}$ is linearly independent over $\mathbb{F}_q$, and*

$$\begin{aligned} \epsilon_0 &= c^2 + ab, \\ \epsilon_1 &= ab^q + a^q b, \quad \textit{and} \\ \epsilon_2 &= ab^{q^2} + a^{q^2} b. \end{aligned}$$

Proof. Let n be the non-negative integer and t_0 be the positive integer such that $r = 5^n t_0$ and $\gcd(5, t_0) = 1$. We set the positive integer q_0, as $q_0 = 4^{5^n}$ and hence we have $q = q_0^{t_0}$. Note that $\mathbb{F}_{q_0} \subseteq \mathbb{F}_q$ and $\mathbb{F}_{q_0^5} \subseteq \mathbb{F}_{q^5}$.

Let $e, d \in \mathbb{F}_4 \setminus \{0\}$ be arbitrary elements with $e \neq d$, which will be determined later. Let $f(x)$ be the polynomial given in (5.16) depending on q_0, e and d. Let y be a root of $f(x)$ in some extension field of $\mathbb{F}_{q_0}$. By (1) of Lemma 5.4, we have $y \in \mathbb{F}_{q_0^5} \subseteq \mathbb{F}_{q^5}$ and $y \notin \mathbb{F}_{q_0}$. As $\gcd(5, t_0) = 1$ we have $\mathbb{F}_{q_0^5} \cap \mathbb{F}_q = \mathbb{F}_{q_0^5} \cap \mathbb{F}_{q_0^{t_0}} = \mathbb{F}_{q_0}$. Therefore we have even $y \notin \mathbb{F}_q$. Indeed, otherwise $y \in \mathbb{F}_{q_0^5} \cap \mathbb{F}_q = \mathbb{F}_{q_0}$, which is a contradiction to (1) of Lemma 5.4.

First we prove (3) of the proposition. Let $c_1 \in \mathbb{F}_4 \backslash \{0\}$ and $c_2 \in \mathbb{F}_4 \backslash \{0, 1\}$ be arbitrary elements to be determined later. We put

$$a = y^{q_0}, \qquad b = y, \quad \text{and} \quad c = c_1 + c_2(a + b).$$

We first prove that $\{a, b, c\}$ is linearly independent over $\mathbb{F}_q$. Indeed, otherwise there exist $v_1, v_2, v_3 \in \mathbb{F}_q$, not all zero, such that

$$v_1 y^{q_0} + v_2 y + v_3 c_1 + v_3 y^{q_0} + v_3 y = 0. \tag{5.40}$$

If $v_1 + v_3 = 0$, then from (5.40) we have

$$(v_2 + v_3)y + v_3 c_1 = 0. \tag{5.41}$$

If also $v_2 + v_3 = 0$, then $v_3 = 0$ by (5.41). This implies that $v_1 = v_2 = v_3 = 0$, which is a contradiction. If instead $v_2 + v_3 \neq 0$, then by (5.41) we get $y \in \mathbb{F}_q$, which is a contradiction as well (see (1) of Lemma 5.4). Hence we have $v_1 + v_3 \neq 0$. Then dividing (5.40) by $v_1 + v_3$ we obtain that there exist $u_0, u_1 \in \mathbb{F}_q$ such that

$$y^{q_0} = u_1 y + u_0. \tag{5.42}$$

By (2) of Lemma 5.4, we have

$$y^{2q_0} + de^2 y^{q_0+1} + y^2 + d^2e^2 = 0. \tag{5.43}$$

Combining (5.42) and (5.43) we conclude that

$$\begin{aligned} 0 &= (u_1 y + u_0)^2 + de^2\bigl(u_1 y^2 + u_0 y\bigr) + y^2 + d^2e^2 \\ &= y^2\bigl(1 + u_1^2 + u_1 de^2\bigr) + y\bigl(u_0 de^2\bigr) + \bigl(u_0^2 + d^2e^2\bigr). \end{aligned} \tag{5.44}$$

If $1 + u_1^2 + u_1 de^2 \neq 0$ or $u_0 de^2 \neq 0$, then by (5.44) y is a root of a polynomial of degree 2 or degree 1 in $\mathbb{F}_q[x]$. This implies that $y \in \mathbb{F}_{q^2}$ and hence $y \in \mathbb{F}_{q^2} \cap \mathbb{F}_{q^5} = \mathbb{F}_q$, which is a contradiction. Hence for the coefficients in (5.44) we have

$$1 + u_1^2 + u_1 de^2 = u_0 de^2 = u_0^2 + d^2e^2 = 0. \tag{5.45}$$

As $d, e \in \mathbb{F}_4 \setminus \{0\}$, using (5.45) we obtain that $u_0 = 0$, which also leads the contradiction $d^2e^2 = 0$. This proves that $\{a, b, c\}$ is linearly independent over $\mathbb{F}_q$.

Next we compute the values $c^2 + ab$, $ab^q + a^q b$ and $ab^{q^2} + a^{q^2} b$. Throughout these computations we use the properties of the arithmetic of $\mathbb{F}_4$ given in Table 2. We have

$$\begin{aligned} c^2 + ab &= \bigl(c_1 + c_2\bigl(y^{q_0} + y\bigr)\bigr)^2 + y^{q_0+1} \\ &= c_1^2 + c_2^2 y^{2q_0} + c_2^2 y^2 + y^{q_0+1} \\ &= c_1^2 + c_2^2\bigl(de^2 y^{q_0+1} + y^2 + d^2e^2\bigr) + c_2^2 y_2 + y^{q_0+1} \\ &= \bigl(c_2^2 de^2 + 1\bigr) y^{q_0+1} + \bigl(c_1^2 + c_2^2 d^2e^2\bigr) \\ &= c_1^2 + c_2^2 d^2e^2, \end{aligned} \tag{5.46}$$

where we use (2) of Lemma 5.4 and Table 2 (see the column corresponding to $de^2c_2^2 + 1$) for the third and fifth equations in (5.46), respectively.

Recall that t_0 is a positive integer with $\gcd(5, t_0) = 1$ and $q = q_0^{t_0}$. If $t_0 \equiv 1 \bmod 5$, then as $y \in F_{q_0^5}$ we have $y^q = y^{q_0}$ and

$$ab^q + a^q b = y^{q_0} y^q + y^{q_0 q} y = y^{2q_0} + y^{q_0^2+1} = d^2e^2, \tag{5.47}$$

where we use (3) of Lemma 5.4. Moreover we have

Table 2
Some equalities in $\mathbb{F}_4=\{0,1,\alpha,\alpha^2\}$ where α is a root of the primitive polynomial $x^2+x+1\in\mathbb{F}_2[x]$.

d	e	c_2	c_1	$c_1^2+c_2^2d^2e^2$	d^2e^2	$de^2c_2^2+1$	Line number
1	α	α^2	1	0	α^2	0	line 1
			α	α	α^2	0	line 2
			α^2	α^2	α^2	0	line 3
	α^2	α	1	0	α	0	line 4
			α	α	α	0	line 5
			α^2	α^2	α	0	line 6
α	1	α	1	α^2	α^2	0	line 7
			α	1	α^2	0	line 8
			α^2	0	α^2	0	line 9
	α^2	α^2	1	α^2	1	0	line 10
			α	1	1	0	line 11
			α^2	0	1	0	line 12
α^2	1	α^2	1	α	α	0	line 13
			α	1	α	0	line 14
			α^2	0	α	0	line 15
	α	α	1	α	1	0	line 16
			α	1	1	0	line 17
			α^2	0	1	0	line 18

$$ab^{q^2}+a^{q^2}b=y^{q_0}y^{q^2}+y^{q_0q^2}y=y^{q_0^2+q_0}+y^{q_0^3+1}=e, \tag{5.48}$$

where we use (4) of Lemma 5.4.

Similarly using Lemma 5.4 we obtain the following results:
If $t_0\equiv 2 \bmod 5$, then we have $y^q=y^{q_0^2}$ and

$$\begin{aligned} ab^q+a^qb&=e,\\ ab^{q^2}+a^{q^2}b&=d^2e^2. \end{aligned} \tag{5.49}$$

If $t_0\equiv 3 \bmod 5$, then we have $y^q=y^{q_0^3}$ and

$$\begin{aligned} ab^q+a^qb&=e,\\ ab^{q^2}+a^{q^2}b&=d^2e^2. \end{aligned} \tag{5.50}$$

If $t_0\equiv 4 \bmod 5$, then we have $y^q=y^{q_0^4}$ and

$$\begin{aligned} ab^q+a^qb&=d^2e^2,\\ ab^{q^2}+a^{q^2}b&=e. \end{aligned} \tag{5.51}$$

If $t_0\equiv 1 \bmod 5$, then combining (5.46), (5.47), (5.48) and Table 2 we complete the proof of (3) of the proposition. If $t_0\equiv 2,3$ or 4 mod 5, similarly using (5.49), (5.50) or (5.51), respectively, instead of (5.47) and (5.48), we complete the proof of (3) of the proposition. For example, if $\epsilon_1=1$, then $\epsilon_2\in\mathbb{F}_4\setminus\{0,\epsilon_1\}=\{\alpha,\alpha^2\}$ and $\epsilon_0\in\{0,\epsilon_1,\epsilon_2\}$. Hence there are 6 values that we need to prove that all of these values are assumed, which are

$$(\epsilon_0,\epsilon_1,\epsilon_2)=\bigl\{(0,1,\alpha),\bigl(0,1,\alpha^2\bigr),(1,1,\alpha),\bigl(1,1,\alpha^2\bigr),(\alpha,1,\alpha),\bigl(\alpha^2,1,\alpha^2\bigr)\bigr\}.$$

If $t_0\equiv 1 \bmod 5$, then we show that all of these values are assumed using lines 18, 12, 17, 11, 16 and 10 of Table 2.

Note that for $\epsilon_1 = \alpha$ there are 6 such values and for $\epsilon_1 = \alpha^2$ there are 6 such values. Totally there are 18 distinct values which correspond one-to-one to 18 lines of Table 2. This completes the proof of (3) of the proposition.

Next we prove (2) of the proposition. Assume that r is odd. We put

$$a = de^2 y^{q_0}, \qquad b = d^2 ey \quad \text{and} \quad s = de^2 \in \mathbb{F}_4 \subseteq \mathbb{F}_q.$$

As $d, e \in \mathbb{F}_4 \setminus \{0\}$ with $d \neq e$, $de^2 \in \mathbb{F}_4 \setminus \{0, 1\}$. Then $\operatorname{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(de^2) = \alpha + \alpha^2 = 1$, where α is a primitive element in $\mathbb{F}_4$. As r is odd we conclude that

$$\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = \operatorname{Tr}_{\mathbb{F}_4/\mathbb{F}_2} \circ \operatorname{Tr}_{\mathbb{F}_{4^r}/\mathbb{F}_4}(s) = \operatorname{Tr}_{\mathbb{F}_4/\mathbb{F}_2}\bigl(rde^2\bigr) = \operatorname{Tr}_{\mathbb{F}_4/\mathbb{F}_2}\bigl(de^2\bigr) = 1. \tag{5.52}$$

First we show that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$. Note that in the beginning of the proof of (3) above we have proved that the set $\{y^{q_0}, y, c\}$, where c is a certain element of $\mathbb{F}_{q^5}$, is linearly independent over $\mathbb{F}_q$. This implies in particular that $\{y^{q_0}, y\}$ is linearly independent over $\mathbb{F}_q$. Hence as $de^2, d^2e \in \mathbb{F}_4 \subseteq \mathbb{F}_q$, the set $\{a, b\} = \{de^2 y^{q_0}, d^2 ey\}$ is also linearly independent over $\mathbb{F}_q$.

It remains to compute the values of $a^2 + ab + sb^2$, $ab^q + a^q b$ and $ab^{q^2} + a^{q^2} b$. Using similar methods as in the proof of (3) of the proposition above we obtain that

$$\begin{aligned} a^2 + ab + sb^2 &= d, \\ ab^q + a^q b &= \begin{cases} d^2e^2, & \text{if } t_0 \equiv 1 \text{ or } 4 \bmod 5, \\ e, & \text{if } t_0 \equiv 2 \text{ or } 3 \bmod 5, \end{cases} \\ ab^{q^2} + a^{q^2} b &= \begin{cases} e, & \text{if } t_0 \equiv 1 \text{ or } 4 \bmod 5, \\ d^2e^2, & \text{if } t_0 \equiv 2 \text{ or } 3 \bmod 5. \end{cases} \end{aligned} \tag{5.53}$$

For example we have

$$\begin{aligned} a^2 + ab + sb^2 &= d^2 ey^{2q_0} + y^{q_0+1} + de^2\bigl(de^2 y^2\bigr) \\ &= d^2 ey^{2q_0} + y^{q_0+1} + d^2 ey^2 \\ &= d^2 e\bigl(y^{2q_0} + de^2 y^{q_0+1} + y^2\bigr) \\ &= d^2 e\bigl(d^2 e^2\bigr) = d \end{aligned}$$

where we use (2) of Lemma 5.4 in the third equation above.

Combining (5.52), (5.53) and Table 2 we complete the proof of (2) of the proposition. For example, let $t_0 \equiv 2 \bmod 5$ and $\epsilon_1 = \alpha$ under the notation of Table 2. Then $\epsilon_2 \in \mathbb{F}_4 \setminus \{0, \epsilon_1\} = \{\alpha^2, 1\}$ and $\epsilon_0 \notin \{0, \epsilon_1, \epsilon_2\}$. Hence there are 2 values that we need to consider, which are

$$(\epsilon_0, \epsilon_1, \epsilon_2) = \bigl\{\bigl(\alpha^2, \alpha, 1\bigr), \bigl(1, \alpha, \alpha^2\bigr)\bigr\}.$$

These values are attained in lines $\{16, 17, 18\}$ and $\{1, 2, 3\}$ of Table 2, respectively. In particular for each value of $(\epsilon_0, \epsilon_1, \epsilon_2)$, there are 3 distinct possible lines. There are altogether $3 \cdot 2 = 6$ distinct values of $(\epsilon_0, \epsilon_1, \epsilon_2)$, which correspond to the 18 lines of Table 2. This is a 1 to 3 correspondence. In this correspondence, the different 3 lines corresponding to a given value of $(\epsilon_0, \epsilon_1, \epsilon_2)$ have the same values of d and e. Finally we note that the proof of (1) of the proposition follows from Lemma 5.3. This completes the proof. □

6. Proofs of Theorem 3.1 and Proposition 3.3

In this section we complete the proofs of Theorem 3.1 and Proposition 3.3.

Proof of Theorem 3.1. It follows using the results of Section 4 and Section 5. For the necessary conditions we have the results in Section 4. For the sufficiency conditions we have various restrictions on $\epsilon_0, \epsilon_1, \epsilon_2$. Note that there are certain cases that we do not consider. In fact using the well-known facts from quadratic forms, we immediately get that such cases are not needed to consider. For example in Proposition 5.2 we observe that under the assumption of $\epsilon_2 = \epsilon_1$, the case $\epsilon_0 = \epsilon_1$ holds in (1) of Proposition 5.2, which implies that the invariant $\Lambda(Q)$ is 1 (see also Table 1). The remaining case $\epsilon_0 \neq \epsilon_1$ holds in (2) of Proposition 5.2, which implies that the invariant $\Lambda(Q)$ is 0. Clearly a quadratic form cannot have two different $\Lambda(Q)$ values simultaneously. Hence there is no situation giving $\Lambda(Q) = -1$ in Proposition 5.2, or equivalently under the assumption that $\epsilon_2 = \epsilon_1$. We note that we have presented such nonexistence results in Section 7.2 below. □

Proof of Proposition 3.3. First we assume that $k = 2$ and consider the necessity part. Then using Theorem 2.2 there exist $a, b \in \mathbb{F}_{q^2}$ such that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$ and the invariant $\Lambda(Q)$ is 1 or -1. Moreover $ab^{q^2} + a^{q^2}b = 0$. Then the arguments in the proof of Proposition 4.3 hold. These imply in particular that $4 \mid k$, which is a contradiction. This proves that the case $k = 2$ is void.

Next we assume that $k = 3$ and consider the necessity part. Here again by Theorem 2.2 we get that there exist $a, b \in \mathbb{F}_{q^3}$ such that $\{a, b\}$ is linearly independent over $\mathbb{F}_q$. Moreover $\epsilon_1 = ab^q + a^q b$ and $\epsilon_1 \neq 0$. Then $ab^{q^2} + a^{q^2}b = (ab^q + a^q b)^{q^2} = \epsilon_1^{q^2} = \epsilon_1$, where we use the fact that $\epsilon_1 \in \mathbb{F}_4 \subseteq \mathbb{F}_q$. It remains to show the sufficiency of the cases (1) and (2) of the proposition. This part follows immediately from Proposition 5.2. □

7. Applications to curves and system of equations

In this section we give some applications of our results in Section 3 to algebraic curves over finite fields and to certain systems of equations over finite fields. We present them in two subsections.

7.1. Algebraic curves over finite fields

In this subsection we give some classification results for certain curves over finite fields.

Throughout this subsection by a curve we mean a smooth, geometrically irreducible projective curve defined over a finite field. Curves over finite fields have interesting applications in coding theory, cryptography, finite geometry and related areas (see, for example, [11,19,16,20,12,15,17]). It is an important problem to classify curves over finite fields depending on their number of rational points. These kind of results are important for certain applications cited in the references above.

Let $\mathbb{F}_q$ be a finite field with q elements. For an integer $k \geqslant 1$, let χ be a curve defined over $\mathbb{F}_{q^k}$. Let $N(\chi)$ and $g(\chi)$ denote the number of $\mathbb{F}_{q^k}$-rational points and the genus of χ, respectively. The Hasse–Weil inequality states that

$$1 + q^k - 2g(\chi)q^{\frac{k}{2}} \leqslant N(\chi) \leqslant 1 + q^k + 2g(\chi)q^{\frac{k}{2}}. \tag{7.1}$$

For certain families of curves, it is difficult to determine the distribution of $N(\chi)$ in the interval given by the lower and upper bounds in (7.1). Moreover not all the values in this interval are attained in general. A curve is called maximal if the upper bound in (7.1) is attained and minimal if the lower bound is attained. There are interesting results on existence and classification of maximal and minimal curves using various approaches (see, for example, [18,5,1,3,13,21,6,2,7–9]).

Let q be an integer which is a power of a prime, in particular q may be odd or even. Let $k \geqslant 2$ be an integer and $m = \lfloor \frac{k}{2} \rfloor$. In this subsection we consider the curve χ over $\mathbb{F}_{q^k}$ given by the affine equation

$$\chi: \quad y^q - y = x\big(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m}\big). \tag{7.2}$$

Here $\epsilon_0, \epsilon_1, \dots, \epsilon_m \in \mathbb{F}_{q^k}$ and at least one of them is nonzero. If q is even we further assume that at least one of $\epsilon_1, \dots, \epsilon_m$ is nonzero. Let $l = \max\{i\colon\ 0 \leqslant i \leqslant m,\ \epsilon_i \neq 0\}$, that is the largest index i such that $\epsilon_i \neq 0$. Using [19, Proposition III.7.10] we determine the genus $g(\chi)$ of χ as

$$g(\chi) = \frac{(q-1)q^l}{2}. \tag{7.3}$$

The curve χ is directly related to the quadratic form $Q : \mathbb{F}_{q^k} \to \mathbb{F}_q$ (see also Section 2) given by

$$Q(x) = \mathrm{Tr}\left(x \sum_{i=0}^{m} \epsilon_i x^{q^i}\right),$$

where Tr is the trace map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. Recall that the corresponding bilinear form on $\mathbb{F}_{q^k}$ is defined as $B(x, y) = Q(x + y) - Q(x) - Q(y)$, which holds in both cases that q is odd or q is even. Let w be the $\mathbb{F}_q$-dimension of the radical

$$W = \left\{x \in \mathbb{F}_{q^k}\colon\ B(x, y) = 0 \text{ for all } y \in \mathbb{F}_{q^k}\right\}.$$

Another invariant of Q is $\Lambda(Q)$, which is an integer in the set $\{-1, 0, 1\}$. Recall that $N(Q)$ denotes the number

$$N(Q) = \left|\left\{x \in \mathbb{F}_{q^k}\colon\ Q(x) = 0\right\}\right|,$$

and $\Lambda(Q)$ can be defined as the integer such that

$$N(Q) = q^{k-1} + \Lambda(Q)(q-1)q^{\frac{k+w}{2}-1}. \tag{7.4}$$

Using Hilbert's Theorem 90 and (7.4), for the number $N(\chi)$ of $\mathbb{F}_{q^k}$-rational points of χ we obtain that

$$N(\chi) = 1 + q^k + \Lambda(Q)(q-1)q^{\frac{k+w}{2}}. \tag{7.5}$$

Therefore we get information for the curve χ using the quadratic form Q. In particular when $w = k$, i.e., the codimension of Q is 0, we completely classify such curves depending their $\mathbb{F}_{q^k}$-rational points in the next proposition. Note that the following proposition holds both in even and odd characteristics.

Proposition 7.1. *Let q be an integer which is a power of a prime. Let $k \geqslant 2$ be an integer. Let $m = \lfloor \frac{k}{2} \rfloor$. Let $\epsilon_0, \epsilon_1, \dots, \epsilon_m \in \mathbb{F}_{q^k}$. If q is even, then we assume that at least one of $\epsilon_1, \epsilon_2, \dots, \epsilon_m$ is nonzero. If q is odd, then we assume that at least one of $\epsilon_0, \epsilon_1, \dots, \epsilon_m$ is nonzero. Let $Q : \mathbb{F}_{q^k} \to \mathbb{F}_q$ be the quadratic form given by*

$$Q(x) = \mathrm{Tr}\left(x \sum_{i=0}^{m} \epsilon_i x^{q^i}\right),$$

where Tr *is the trace map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. Let χ be the curve over $\mathbb{F}_{q^k}$ given by the affine equation*

$$\chi\colon\quad y^q - y = x\left(\epsilon_0 x + \epsilon_1 x^q + \dots + \epsilon_m x^{q^m}\right).$$

Assume also that the codimension of the radical of Q is 0. Then the following hold:

(1) *If k is even, $\epsilon_0 = \epsilon_1 = \cdots = \epsilon_{m-1} = 0$ and $\epsilon_m \in \mathbb{F}_{q^k} \setminus \{0\}$ with $\epsilon_m + \epsilon_m^{q^m} = 0$, then for the invariant $\Lambda(Q)$ of Q and the number $N(\chi)$ of $\mathbb{F}_{q^k}$-rational points of χ we have*

$$\Lambda(Q) = 1 \quad \textit{and} \quad N(\chi) = q^{k+1} + 1.$$

In particular χ is a maximal curve.

(2) *Otherwise, that is, if k is odd, or if k is even and $((\epsilon_0, \epsilon_1, \ldots, \epsilon_{m-1}) \neq (0, 0, \ldots, 0)$ or $\epsilon_m \in \mathbb{F}_{q^k} \setminus \{0\}$ with $\epsilon_m + \epsilon_m^{q^m} \neq 0)$, then for the invariant $\Lambda(Q)$ of Q and the number $N(\chi)$ of $\mathbb{F}_{q^k}$-rational points of χ we have*

$$\Lambda(Q) = 0 \quad \textit{and} \quad N(\chi) = q^k + 1.$$

In particular (when q^k is a square), χ is neither maximal nor minimal.

Proof. We first show that $\Lambda(Q) \neq -1$. Indeed, otherwise using (7.4) for the cardinality $N(Q)$ we obtain that $N(Q) = q^{k-1} - (q-1)q^{k-1}$. It is clear that the cardinality is non-negative and

$$N(Q) = q^{k-1} - (q-1)q^{k-1} \geqslant 0,$$

which gives a contradiction if $q \neq 2$. Next assume that $\Lambda(Q) = -1$ and $q = 2$. Then $N(Q) = 0$. However if $x = 0$, then

$$Q(x) = \mathrm{Tr}\left(x \sum_{i=0}^{m} \epsilon_i x^{q^i}\right) = 0,$$

and hence $N(Q) \geqslant 1$, which implies a contradiction. This proves that $\Lambda(Q) \neq -1$.

Next we assume that $\Lambda(Q) = 1$. First we show that this assumption implies that k is even. Indeed, otherwise for the integer $l = \max\{i\colon\ 0 \leqslant i \leqslant m,\ \epsilon_i \neq 0\}$, we have

$$l \leqslant m = \frac{k-1}{2} < \frac{k}{2}. \tag{7.6}$$

By the Hasse–Weil inequality we have

$$N(\chi) \leqslant 1 + q^k + \frac{2(q-1)q^l}{2} q^{\frac{k}{2}} = 1 + q^k + (q-1)q^{l+\frac{k}{2}}. \tag{7.7}$$

As $\Lambda(Q) = 1$ and the codimension is 0, using (7.5) we have

$$N(\chi) = 1 + q^k + (q-1)q^k. \tag{7.8}$$

Comparing (7.7) and (7.8) we obtain that $q^k \leqslant q^{l+\frac{k}{2}}$, and hence

$$\frac{k}{2} \leqslant l,$$

which is a contradiction to (7.6).

Next we show that $\epsilon_m \neq 0$. Indeed, otherwise $l < m = \frac{k}{2}$ and by the same reasoning above we get a contradiction.

Under the assumption that $\Lambda(Q) = 1$, it remains to show that $\epsilon_0 = \epsilon_1 = \cdots = \epsilon_{m-1} = 0$ and $\epsilon_m + \epsilon_m^{q^m} = 0$. First note that as $\epsilon_m \neq 0$ and $\Lambda(Q) = 1$, we have

$$N(\chi) = 1 + q^k + (q-1)q^k = 1 + q^{k+1} = 1 + q^k + 2g(\chi)q^{\frac{k}{2}},$$

where $g(\chi) = \frac{(q-1)q^m}{2}$ is the genus of χ. Hence χ is maximal. Next we recall the notion of q-cyclotomic coset modulo $q^k - 1$. For $1 \leqslant i \leqslant q^k - 2$, let $t(i)$ be the smallest non-negative integer such that $q^{t(i)+1}i \equiv i \bmod (q^k - 1)$. The q-cyclotomic coset containing i modulo $q^k - 1$ is the set $\{i, qi, q^2 i, \ldots, q^{t(i)}i\}$. If $1 \leqslant i_1 < i_2 \leqslant q^{k/2} + 1$, then the q-cyclotomic coset containing i_1 modulo $q^k - 1$ is distinct from the q-cyclotomic coset containing i_2 modulo $q^k - 1$. Therefore using [10, Corollary 2.6] we conclude that $\epsilon_0 = \epsilon_1 = \cdots = \epsilon_{m-1} = 0$ and $\epsilon_m + \epsilon_m^{q^m} = 0$.

Hence in the other cases $\Lambda(Q) = 0$. That implies that if k is odd, then $\Lambda(Q) = 0$. Moreover if k is even and $(\epsilon_0, \epsilon_1, \ldots, \epsilon_{m-1}) \neq (0, 0, \ldots, 0)$, then $\Lambda(Q) = 0$. Also if k is even, $(\epsilon_0, \epsilon_1, \ldots, \epsilon_{m-1}) = (0, 0, \ldots, 0)$ and $\epsilon_m \in \mathbb{F}_{q^k}$ with $\epsilon_m + \epsilon_m^{q^m} \neq 0$, then $\Lambda(Q) = 0$. It is easy to observe these do not give maximal or minimal curves. This completes the proof. □

In the rest of this subsection we assume that $q \geqslant 4$ is an integer, which is a power of 4. It is well known that the codimension of the radical of a quadratic form is even when the characteristic of the finite field is 2. Hence after Proposition 7.1 it is natural to consider the case that the codimension is 2. Using Hilbert's Theorem 90, Theorem 3.1 and Proposition 3.3, we immediately obtain a classification of curves of the form

$$\chi: \quad y^q + y = x\big(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m}\big).$$

Here the main assumptions are that q is a power of 4, the codimension of the corresponding quadratic form is 2 and $\epsilon_0, \epsilon_1, \epsilon_2 \in \mathbb{F}_4$. We prefer not to state this result explicitly, which can be derived easily from Theorem 3.1, Remark 3.2 and Proposition 3.3. Instead we give its consequences on maximal and minimal curves in the next proposition.

Proposition 7.2. *Let $q = 4^r$, $k \geqslant 2$ be an integer and $m = \lfloor \frac{k}{2} \rfloor$. Let $\epsilon_0, \epsilon_1 \in \mathbb{F}_4$. For $k \geqslant 4$ let $\epsilon_2 \in \mathbb{F}_4$. For $k \geqslant 6$ let $\epsilon_3, \ldots, \epsilon_m \in \mathbb{F}_{q^k}$. Let Q be the quadratic form from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$ defined as*

$$Q(x) = \operatorname{Tr}\left(x \sum_{i=0}^{m} \epsilon_i x^{q^i}\right),$$

where Tr *is the trace map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. Assume that at least one of $\epsilon_1, \ldots, \epsilon_m$ is nonzero. Let χ be the curve over $\mathbb{F}_{q^k}$ given by the affine equation*

$$\chi: \quad y^q + y = x\big(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m}\big).$$

Assume also that the codimension of the radical of Q is 2. Then we have the following:

(1) *If χ is maximal, then one of the following holds:*
   (a) *$4 \mid k$, $q = 4^r$ where $r \geqslant 1$ is an odd integer, $\epsilon_1 \neq 0$, $\epsilon_0 \notin \{0, \epsilon_1\}$, $\epsilon_m = 0$ and for $1 \leqslant i \leqslant m - 1$ we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \bmod 2, \\ 0 & \text{otherwise.} \end{cases}$$

(b) $6 \mid k$, $q = 4^r$ *where* $r \geqslant 1$ *is an integer,* $\epsilon_1 \neq 0$, $\epsilon_0 = \epsilon_1$ *and for* $1 \leqslant i \leqslant m-1$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \text{ or } 2 \bmod 3, \\ 0 & \text{otherwise.} \end{cases}$$

(c) $10 \mid k$, $q = 4^r$ *where* $r \geqslant 2$ *is an even integer,* $\epsilon_1 \neq 0$, $\epsilon_2 \notin \{0, \epsilon_1\}$, $\epsilon_0 \notin \{0, \epsilon_1, \epsilon_2\}$ *and for* $1 \leqslant i \leqslant m-1$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \text{ or } 4 \bmod 5, \\ \epsilon_2 & \text{if } i \equiv 2 \text{ or } 3 \bmod 5, \\ 0 & \text{otherwise.} \end{cases}$$

(2) *If* χ *is minimal, then one of the following holds*:

(a) $4 \mid k$, $q = 4^r$ *where* $r \geqslant 1$ *is an odd integer,* $\epsilon_1 \neq 0$, $\epsilon_0 = 0$ *or* $\epsilon_0 = \epsilon_1$, *and for* $1 \leqslant i \leqslant m-1$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \bmod 2, \\ 0 & \text{otherwise.} \end{cases}$$

(b) $4 \mid k$, $q = 4^r$ *where* $r \geqslant 2$ *is an even integer,* $\epsilon_1 \neq 0$ *and for* $1 \leqslant i \leqslant m-1$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \bmod 2, \\ 0 & \text{otherwise.} \end{cases}$$

(c) $10 \mid k$, $q = 4^r$ *where* $r \geqslant 1$ *is an odd integer,* $\epsilon_1 \neq 0$, $\epsilon_2 \notin \{0, \epsilon_1\}$, $\epsilon_0 \notin \{0, \epsilon_1, \epsilon_2\}$ *and for* $1 \leqslant i \leqslant m-1$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \text{ or } 4 \bmod 5, \\ \epsilon_2 & \text{if } i \equiv 2 \text{ or } 3 \bmod 5, \\ 0 & \text{otherwise.} \end{cases}$$

Conversely if either of the conditions in (1a), (1b) *or* (1c) *hold, then* χ *is a maximal curve with the number* $N(\chi)$ *of* $\mathbb{F}_q$*-rational points and genus* $g(\chi)$ *of* χ *as*

$$N(\chi) = 1 + q^k + (q-1)q^{k-1} = 1 + 2q^k - q^{k-1},$$
$$g(\chi) = \frac{(q-1)q^{\frac{k}{2}-1}}{2}.$$

Also if either of the conditions in (2a), (2b) *or* (2c) *hold, then* χ *is a minimal curve with the number* $N(\chi)$ *of* $\mathbb{F}_q$*-rational points and genus* $g(\chi)$ *of* χ *as*

$$N(\chi) = 1 + q^k - (q-1)q^{k-1} = 1 + q^{k-1},$$
$$g(\chi) = \frac{(q-1)q^{\frac{k}{2}-1}}{2}.$$

Proof. Assume that χ is maximal. We first show that $\epsilon_m = 0$. Indeed, otherwise the genus of χ is $g(\chi) = \frac{(q-1)q^m}{2}$ and hence by the maximality of χ

$$N(\chi) = 1 + q^k + (q-1)q^{m+\frac{k}{2}}. \tag{7.9}$$

As the dimension w of the radical is $k-2$, using (7.5) we obtain

$$N(\chi) \leqslant 1 + q^k + (q-1)q^{k-1}, \tag{7.10}$$

and the equality holds only if $\Lambda(Q) = 1$. Comparing (7.9) and (7.10) we obtain that $m + \frac{k}{2} \leqslant k-1$. Then

$$m = \left\lfloor \frac{k}{2} \right\rfloor \leqslant \frac{k}{2} - 1,$$

a contradiction. As at least one of $\epsilon_1, \ldots, \epsilon_m$ is nonzero by the assumption, this shows in particular that there is no maximal curve under assumption of the proposition when $m = 1$, or equivalently $k \in \{2, 3\}$. Hence we assume that $m \geqslant 2$, or equivalently $k \geqslant 4$.

Next we show that $\epsilon_{m-1} \neq 0$ and k is even. Indeed note that for the integer $l = \max\{i\colon\ 0 \leqslant i \leqslant m,\ \epsilon_i \neq 0\}$ we have

$$1 \leqslant l \leqslant m-1 \tag{7.11}$$

and the genus of χ is $g(\chi) = \frac{(q-1)q^l}{2}$. Then by the maximality of χ we get

$$N(\chi) = 1 + q^k + (q-1)q^{l+\frac{k}{2}}. \tag{7.12}$$

As the dimension w of the radical is $k-2$, using (7.5) we have

$$N(\chi) = 1 + q^k + \Lambda(Q)q^{k-1}, \tag{7.13}$$

where $\Lambda(Q) \in \{-1, 0, 1\}$. If $\Lambda(Q) \in \{-1, 0\}$, then $(q-1)q^{l+\frac{k}{2}} > 0 \geqslant \Lambda(Q)q^{k-1}$ and hence the right-hand sides of (7.12) and (7.13) are distinct, which gives a contradiction. Therefore $\Lambda(Q) = 1$ and comparing (7.12) and (7.13) we obtain that

$$l + \frac{k}{2} = k - 1,$$

which implies that $l = \frac{k}{2} - 1$, $\epsilon_{m-1} \neq 0$ and k is even. Moreover it is easy to observe that under the conditions of the proposition, χ is a maximal curve if and only if $k \geqslant 4$, k is even and $\Lambda(Q) = 1$. Using Theorem 3.1 we obtain the cases for such quadratic forms Q. For example among the cases (1), (2) and (3) of Theorem 3.1, only the case (1) of Theorem 3.1 gives maximal curves. This is case (1a) of the current proposition. Secondly among the cases (4) and (5) of Theorem 3.1, under the extra condition that k is even (and hence $6 \mid k$), only the case (4) of Theorem 3.1 gives maximal curves. This is the case (1b) of the current proposition. Similarly using the cases (6), (7) and (8) of Theorem 3.1, we obtain the case (1c) of the current proposition.

Next we assume that χ is minimal. The proof is very similar the case χ is maximal above. We again obtain that $k \geqslant 4$, $\epsilon_m = 0$, $\epsilon_{m-1} \neq 0$ and k is even. But now it is necessary that $\Lambda(Q) = -1$. Then using Theorem 3.1 similarly we obtain the cases (2a), (2b) and (2c) of the current proposition.

The converse statement implying explicit construction of maximal and minimal curves with the stated genera is clear from arguments above. This completes the proof. □

Remark 7.3. Note that a main assumption in Proposition 7.2 is that the codimension of Q is 2. It is easy to observe from the proof of Proposition 7.2 that this assumption would be replaced with the following assumption, which may be useful in some applications. We keep the notation and assumptions of Proposition 7.2 except the condition that the codimension of Q is 2. Instead of this condition we assume that $\epsilon_m = 0$ and $\epsilon_{m-1} \neq 0$. Then the same conditions of Proposition 7.2 hold. In its proof it is important to note that the new condition implies that the genus of χ is $\frac{(q-1)q^{m-1}}{2}$. Then by definition and (7.5) we obtain that the codimension is 2 if χ is maximal or minimal.

7.2. Some nonexistence results on systems of equations over finite fields containing $\mathbb{F}_4$

In this subsection we give certain nonexistence results in Proposition 7.4 below. It is a consequence of Theorem 3.1 and the simple but useful observation that the invariant $\Lambda(Q)$ of a quadratic form Q can only attain a unique value in the set $\{-1, 0, 1\}$. Let $q \geqslant 4$ be a power of 4, $k \geqslant 4$ be an integer. Under certain conditions on $\epsilon_0, \epsilon_1, \epsilon_2$, we obtain a full classification of quadratic forms of the form (3.1) in Theorem 3.1. We refer to Table 1 for the summary of the results of Theorem 3.1. For example when $\epsilon_2 = 0$, the invariant $\Lambda(Q)$ cannot be 0 (see the first three lines of Table 1). By Theorem 2.2, the case $\Lambda(Q) = 0$ implies an existence result for a system of equations over $\mathbb{F}_q$. Hence we obtain a nonexistence result for that system in case (1) of the next proposition. We note here that this existence and nonexistence depends on the parity of r. If r is even as in case (2) of Proposition 7.4 below, then we have a nonexistence result. However if r is odd, then the same system gives the corresponding existence result, which is proved in (1) of Proposition 5.1 in Section 5 above.

The other nonexistence results of the following proposition are obtained similarly.

Proposition 7.4. *Let $q = 4^r$, $k \geqslant 4$ be an integer, $\epsilon_0, \epsilon_2 \in \mathbb{F}_4$ and $\epsilon_1 \in \mathbb{F}_4 \setminus \{0\}$. We have the following*:

(1) *There is no $\mathbb{F}_q$-linearly independent set $\{a, b, c\} \subseteq \mathbb{F}_{q^k}$ such that*

$$\begin{aligned} \epsilon_0 &= c^2 + ab, \\ \epsilon_1 &= ab^q + a^q b, \quad \textit{and} \\ \epsilon_2 &= ab^{q^2} + a^{q^2} b = 0. \end{aligned}$$

(2) *If r is an even integer then there is no $\mathbb{F}_q$-linearly independent set $\{a, b\} \subseteq \mathbb{F}_{q^k}$ such that*

$$\begin{aligned} \epsilon_0 &= ab, \\ \epsilon_1 &= ab^q + a^q b, \quad \textit{and} \\ \epsilon_2 &= ab^{q^2} + a^{q^2} b = 0. \end{aligned}$$

(3) *There is no $\mathbb{F}_q$-linearly independent set $\{a, b\} \subseteq \mathbb{F}_{q^k}$ such that there exists $s \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$,*

$$\begin{aligned} \epsilon_0 &= a^2 + ab + sb^2, \\ \epsilon_1 &= ab^q + a^q b, \quad \textit{and} \\ \epsilon_2 &= ab^{q^2} + a^{q^2} b = \epsilon_1. \end{aligned}$$

(4) *If r is an even integer then there is no $\mathbb{F}_q$-linearly independent set $\{a, b\} \subseteq \mathbb{F}_{q^k}$ such that there exists $s \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$,*

$$\begin{aligned} \epsilon_0 &= a^2 + ab + sb^2, \\ \epsilon_1 &= ab^q + a^q b, \\ \epsilon_2 &= ab^{q^2} + a^{q^2} b \neq 0 \quad \textit{and} \\ \epsilon_2 &\neq \epsilon_1. \end{aligned}$$

(5) *If r is an odd integer then there is no $\mathbb{F}_q$-linearly independent set $\{a, b\} \subseteq \mathbb{F}_{q^k}$ such that*

$$\begin{aligned} \epsilon_0 &= ab, \\ \epsilon_1 &= ab^q + a^q b, \\ \epsilon_2 &= ab^{q^2} + a^{q^2} b \neq 0 \quad \textit{and} \\ \epsilon_2 &\neq \epsilon_1. \end{aligned}$$

Acknowledgments

We would like to thank the anonymous reviewer for his/her detailed and useful comments. The first and the third authors were partially supported by TÜBİTAK under Grant No. TBAG-109T672.

References

[1] M. Abdón, F. Torres, On maximal curves in characteristic two, Manuscripta Math. 99 (1) (1999) 39–53.
[2] E. Çakçak, F. Özbudak, Some Artin–Schreier type function fields over finite fields with prescribed genus and number of rational places, J. Pure Appl. Algebra 210 (1) (2007) 113–135.
[3] A. Cossidente, G. Korchmáros, F. Torres, On curves covered by the Hermitian curve, J. Algebra 216 (1) (1999) 56–76.
[4] R.W. Fitzgerald, Highly degenerate quadratic forms over finite fields of characteristic 2, Finite Fields Appl. 11 (2) (2005) 165–181.
[5] R. Fuhrmann, A. Garcia, F. Torres, On maximal curves, J. Number Theory 67 (1) (1997) 29–51.
[6] A. Garcia, M.Q. Kawakita, S. Miura, On certain subcovers of the Hermitian curve, Comm. Algebra 34 (3) (2006) 973–982.
[7] A. Garcia, F. Özbudak, Some maximal function fields and additive polynomials, Comm. Algebra 35 (5) (2007) 1553–1566.
[8] A. Garcia, S. Tafazolian, Certain maximal curves and Cartier operators, Acta Arith. 135 (3) (2008) 199–218.
[9] A. Garcia, S. Tafazolian, On additive polynomials and certain maximal curves, J. Pure Appl. Algebra 212 (11) (2008) 2513–2521.
[10] C. Güneri, Artin–Schreier curves and weights of two dimensional cyclic codes, Finite Fields Appl. 10 (4) (2004) 481–505.
[11] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, second ed., Oxford Math. Monogr., The Clarendon Press, Oxford Univ. Press, New York, 1998.
[12] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Ser. Appl. Math., Princeton Univ. Press, Princeton, NJ, 2008.
[13] G. Korchmáros, F. Torres, On the genus of a maximal curve, Math. Ann. 323 (3) (2002) 589–608.
[14] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
[15] E. Martínez-Moro, C. Munuera, D. Ruano (Eds.), Advances in Algebraic Geometry Codes, Ser. Coding Theory Cryptol., vol. 5, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2008.
[16] H. Niederreiter, C. Xing, Rational Points on Curves over Finite Fields: Theory and Applications, Cambridge Univ. Press, Cambridge, 2001.
[17] H. Niederreiter, C. Xing, Algebraic Geometry in Coding Theory and Cryptography, Princeton Univ. Press, Princeton, NJ, 2009.
[18] H.G. Rück, H. Stichtenoth, A characterization of Hermitian function fields over finite fields, J. Reine Angew. Math. 457 (1994) 185–188.
[19] H. Stichtenoth, Algebraic Function Fields and Codes, second ed., Grad. Texts in Math., vol. 254, Springer-Verlag, Berlin, 2009.
[20] M.A. Tsfasman, S.G. Vlăduţ, D. Nogin, Algebraic Geometric Codes: Basic Notions, Math. Surveys Monogr., vol. 139, American Mathematical Society, Providence, RI, 2007.
[21] P.H. Viana, J.E.A. Rodriguez, Eventually minimal curves, Bull. Braz. Math. Soc. (N.S.) 36 (1) (2005) 39–58.