QUADRATIC FORMS OF CODIMENSION 2 OVER CERTAIN FINITE FIELDS OF EVEN CHARACTERISTIC

FERRUH ÖZBUDAK, ELİF SAYGI, ZÜLFÜKAR SAYGI

ABSTRACT. Let $\mathbb{F}_q$ be a finite field of characteristic 2, not containing $\mathbb{F}_4$. Let $k \geq 2$ be an even integer. We give a full classification of quadratic forms over $\mathbb{F}_{q^k}$ of codimension 2 provided that certain three coefficients are from $\mathbb{F}_4$.

Key words and phrases: Quadratic form, Artin-Schreier type curve, maximal curve, minimal curve

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

$$\begin{array}{rccl} Q : \mathbb{F}_{q^k} & \to & \mathbb{F}_q \\ x & \mapsto & \mathrm{Tr}\left(x\left(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m}\right)\right) \end{array} \tag{0.1}$$

is a quadratic form over $\mathbb{F}_{q^k}$. It is well known that the quadratic form Q is related to Artin-Schreier type curve

$$\chi : \quad y^q + y = x\left(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m}\right). \tag{0.2}$$

Here we assume that at least one of $\epsilon_1, \ldots, \epsilon_m$ is nonzero and hence 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 $\{-1, 0, 1\}$. By Hilbert's Theorem 90 (cf. [4, Theorem 2.25]) and the basic theory of quadratic forms, it is well known that 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 the invariant $\Lambda(Q)$ of Q can be determined, actually also when the characteristic of $\mathbb{F}_q$ is odd (cf. [6]). The next case in characteristic 2 is the case of codimension 2 as the codimension must be an even integer. Recently we have considered this problem when $\mathbb{F}_q$ is an extension of $\mathbb{F}_4$ under the extra condition that certain coefficients are in $\mathbb{F}_4$ (see [6]).

We still keep such a condition. However we note that the quadratic form is considered in $\mathbb{F}_{q^k}$. Hence if q is an odd power of 2 and k is even, then the map (0.1) is still a quadratic form and this problem is not considered in [6]. In this study we consider this problem and obtain again a full classification of such quadratic forms of codimension 2 when q is an odd power of 2 and k is even. Our result is an extension of [1]. We use some methods from [1], which become more complicated in our study.

We note that combining this result with the ones of [6] we complete the problem of classification of quadratic forms of codimension 2 over arbitrary finite fields provided that the first three coefficients are from $\mathbb{F}_4$ for $k \geq 4$. As these coefficients are from $\mathbb{F}_4$, we have $\mathbb{F}_4 \subseteq \mathbb{F}_{q^k}$. The case $\mathbb{F}_4 \subseteq \mathbb{F}_q$ is studied in [6] and here we study the remaining case that q is an odd power of 2 and k is even.

Ferruh Özbudak is with Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey; e-mail: ozbudak@metu.edu.tr,

Elif Saygı is with Department of Math. Education, Hacettepe University, Beytepe, 06532, Ankara, Turkey; e-mail: esaygi@hacettepe.edu.tr.

Zülfükar Saygı is with Department of Mathematics, TOBB University of Economics and Technology, Söğütözü 06530, Ankara, Turkey; e-mail: zsaygi@etu.edu.tr.

In the rest of this paper we state our main result in this study. Here we also note that as in [6] using our main result below we obtain new results on the classification of maximal and minimal curves of the form (0.2) (cf., for example, [2, 7, 5, 8, 3], and also the references in [6]), when q is an odd power of 2 and k is even. We will explain them in the full version of this paper.

First we introduce some notation. For certain even integers $k \geq 4$, we define six types of polynomials $A_1(\epsilon_0, \epsilon_1)$, $A_2(\epsilon_0, \epsilon_1)$, $A_3(\epsilon_0, \epsilon_1, \epsilon_2)$, $A_4(\epsilon_0, \epsilon_1)$, $A_5(\epsilon_0, \epsilon_1)$ and $A_6(\epsilon_0, \epsilon_1, \epsilon_2)$ 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 $m = \frac{k}{2}$.

- If $4|k$, then for $\epsilon_0, \epsilon_1 \in \mathbb{F}_4$ let
$$A_1(\epsilon_0, \epsilon_1) = \epsilon_0 x + \epsilon_1 \left(x^q + x^{q^3} + \cdots + x^{q^{m-1}} \right).$$
- If $3|k$, then for $\epsilon_0, \epsilon_1 \in \mathbb{F}_4$ let
$$A_2(\epsilon_0, \epsilon_1) = \epsilon_0 x + \epsilon_1 \left(x^q + x^{q^2} + x^{q^4} + x^{q^5} + \cdots + x^{q^{m-2}} + x^{q^{m-1}} \right).$$
- If $6|k$, then for $\epsilon_0, \epsilon_1, \epsilon_2 \in \mathbb{F}_4$ let
$$\begin{aligned} A_3(\epsilon_0, \epsilon_1, \epsilon_2) = \epsilon_0 x &+ \epsilon_1 \left(x^q + x^{q^5} + x^{q^7} + x^{q^{11}} + \cdots \right) \\ &+ \epsilon_2 \left(x^{q^2} + x^{q^4} + x^{q^8} + x^{q^{10}} + \cdots \right). \end{aligned}$$
where last terms in $A_3(\epsilon_0, \epsilon_1, \epsilon_2)$ are $\epsilon_1 \left(x^{q^{m-5}} + x^{q^{m-1}} \right)$ and $\epsilon_2 \left(x^{q^{m-4}} + x^{q^{m-2}} \right)$ if $k \equiv 0 \mod 12$, and $\epsilon_1 \left(x^{q^{m-4}} + x^{q^{m-2}} \right)$ and $\epsilon_2 \left(x^{q^{m-5}} + x^{q^{m-1}} \right)$ if $k \equiv 6 \mod 12$.
- If $12|k$, then for $\epsilon_0, \epsilon_1 \in \mathbb{F}_4$ let
$$A_4(\epsilon_0, \epsilon_1) = \epsilon_0 x + \left(\epsilon_1 x^q + x^{q^3} + \epsilon_1^2 x^{q^5} + \epsilon_1 x^{q^7} + x^{q^9} + \epsilon_1^2 x^{q^{11}} + \cdots + \epsilon_1^2 x^{q^{m-1}} \right).$$
- If $8|k$, then for $\epsilon_0, \epsilon_1 \in \mathbb{F}_4$ let
$$A_5(\epsilon_0, \epsilon_1) = \epsilon_0 x + \epsilon_1 \left(x^q + x^{q^2} + \epsilon_1 x^{q^3} + x^{q^5} + x^{q^6} + \epsilon_1 x^{q^7} + \cdots + \epsilon_1 x^{q^{m-1}} \right).$$
- If $8|k$, then for $\epsilon_0, \epsilon_1, \epsilon_2 \in \mathbb{F}_4$ let
$$\begin{aligned} A_6(\epsilon_0, \epsilon_1, \epsilon_2) = \epsilon_0 x &+ \epsilon_1 \left(x^q + \epsilon_1 x^{q^3} + x^{q^5} + \epsilon_1 x^{q^7} + \cdots + x^{q^{m-3}} + \epsilon_1 x^{q^{m-1}} \right) \\ &+ \epsilon_2 \left(x^{q^2} + x^{q^6} + x^{q^{10}} + \cdots + x^{q^{m-2}} \right). \end{aligned}$$

Now we state our main result.

Theorem 1. *Let $q \geq 2$ be an integer which is an odd power of 2. Let $k \geq 4$ be an even integer and set $m = \frac{k}{2}$. Let $\epsilon_0, \epsilon_1, \epsilon_2 \in \mathbb{F}_4$, and for $k \geq 8$ let $\epsilon_3, \ldots, \epsilon_{m-1}, \epsilon_m \in \mathbb{F}_{q^k}$. Let Q be the quadratic form from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$ defined as*

$$Q(x) = \mathrm{Tr}\left(x \sum_{i=0}^{m} \epsilon_i x^{q^i} \right), \tag{0.3}$$

where Tr *is the trace map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. Moreover let r be the positive odd integer with $q = 2^r$. If the $\mathbb{F}_q$-dimension of the radical of Q is $k-2$, then exactly one of the followings holds:*

a) *If $\epsilon_1 = 1$, then*
   a.1) *$4|k$, $\epsilon_0 = 0$, and for $1 \leq i \leq m-1$ we have*
$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \mod 2, \\ 0 & \text{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_1(\epsilon_0, \epsilon_1)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to 1 in this case.*

a.2) $4|k$, $\epsilon_0 \neq 0$, *and for* $1 \leq i \leq m-1$ *we have*

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

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_1(\epsilon_0, \epsilon_1)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to -1 in this case.*

a.3) $3|k$, $\epsilon_0 = \epsilon_1$, *and for* $1 \leq i \leq m-1$ *we have*

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

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_2(\epsilon_0, \epsilon_1)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to -1 in this case.*

a.4) $3|k$, $\epsilon_0 \neq \epsilon_1$, *and for* $1 \leq i \leq m-1$ *we have*

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

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_2(\epsilon_0, \epsilon_1)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to 0 in this case.*

a.5) $6|k$, $\epsilon_2 \notin \{0, \epsilon_1\}$, $\epsilon_0 = \epsilon_2$, *and for* $1 \leq i \leq m-1$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \text{ or } 5 \mod 6, \\ \epsilon_2 & \text{if } i \equiv 2 \text{ or } 4 \mod 6, \\ 0 & \text{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_3(\epsilon_0, \epsilon_1, \epsilon_2)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to -1 in this case.*

a.6) $6|k$, $\epsilon_2 \notin \{0, \epsilon_1\}$, $\epsilon_0 \neq \epsilon_2$, *and for* $1 \leq i \leq m-1$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \text{ or } 5 \mod 6, \\ \epsilon_2 & \text{if } i \equiv 2 \text{ or } 4 \mod 6, \\ 0 & \text{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_3(\epsilon_0, \epsilon_1, \epsilon_2)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to 0 in this case.*

b) *If* $\epsilon_1 \in \mathbb{F}_4 \setminus \mathbb{F}_2$, *then*

b.1) $12|k$, $\epsilon_0 = 0$, *and for* $1 \leq i \leq m-1$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \mod 6, \\ 1 & \text{if } i \equiv 3 \mod 6, \\ \epsilon_1^2 & \text{if } i \equiv 5 \mod 6, \\ 0 & \text{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_4(\epsilon_0, \epsilon_1)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to -1 in this case.*

b.2) $12|k$, $\epsilon_0 \neq 0$, *and for* $1 \leq i \leq m-1$ *we have*

$$\epsilon_i = \begin{cases} \epsilon_1 & \text{if } i \equiv 1 \mod 6, \\ 1 & \text{if } i \equiv 3 \mod 6, \\ \epsilon_1^2 & \text{if } i \equiv 5 \mod 6, \\ 0 & \text{otherwise.} \end{cases}$$

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_4(\epsilon_0, \epsilon_1)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to 0 in this case.*

b.3) $8|k$, $\epsilon_0 = \epsilon_1^{r+1}$, *and for* $1 \leq i \leq m-1$ *we have*

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

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_5(\epsilon_0, \epsilon_1)$ *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to 1 in this case.*

b.4) $8|k$, $\epsilon_0 = \epsilon_1^{r-1}$, *and for* $1 \leq i \leq m-1$ *we have*

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

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_5(\epsilon_0, \epsilon_1)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to -1 in this case.*

b.5) $8|k$, $\epsilon_0 \in \{0, \epsilon_1\}$, *and for* $1 \leq i \leq m-1$ *we have*

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

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_5(\epsilon_0, \epsilon_1)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to 0 in this case.*

b.6) $8|k$, $\big(r \equiv 1 \mod 4$ *and* $(\epsilon_0, \epsilon_2) \in \{(\epsilon_1, 1), (1, \epsilon_1^2)\}\big)$ *or* $\big(r \equiv 3 \mod 4$ *and* $(\epsilon_0, \epsilon_2) \in \{(\epsilon_1, \epsilon_1^2), (\epsilon_1^2, 1)\}\big)$ *and for* $1 \leq i \leq m-1$ *we have*

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

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_6(\epsilon_0, \epsilon_1, \epsilon_2)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to 1 in this case.*

b.7) $8|k$, $\big(r \equiv 1 \mod 4$ *and* $(\epsilon_0, \epsilon_2) \in \{(\epsilon_1, \epsilon_1^2), (\epsilon_1^2, 1)\}\big)$ *or*
$\big(r \equiv 3 \mod 4$ *and* $(\epsilon_0, \epsilon_2) \in \{(\epsilon_1, 1), (1, \epsilon_1^2)\}\big)$ *and for* $1 \leq i \leq m-1$ *we have*

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

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_6(\epsilon_0, \epsilon_1, \epsilon_2)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to -1 in this case.*

b.8) $8|k$, $\epsilon_2 \notin \{0, \epsilon_1\}$, $\epsilon_0 \in \{0, \epsilon_2\}$ *and for* $1 \leq i \leq m-1$ *we have*

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

In particular the polynomial $\sum_{i=0}^{m-1} \epsilon_i x^{q^i}$ *is equal to* $R(x) = A_6(\epsilon_0, \epsilon_1, \epsilon_2)$. *Moreover the invariant* $\Lambda(Q)$ *of* Q *is equal to 0 in this case.*

For each of these 14 cases above, the coefficient ϵ_m *is determined uniquely in* $\mathbb{F}_{q^k}$ *modulo* $\mathbb{F}_{q^m}$ *and hence map defined by* $\mathrm{Tr}\left(xR(x) + \gamma x^{q^m+1}\right)$, *where* γ *is an arbitrary element of* $\mathbb{F}_{q^k}$ *with* $(\gamma - \epsilon_m) \in \mathbb{F}_{q^m}$, *gives the same quadratic form as in (0.3).*

Conversely, for each of the 14 cases above, there exist $\epsilon_0, \epsilon_1, \epsilon_2, \cdots, \epsilon_{m-1}, \epsilon_m \in \mathbb{F}_4 \subseteq \mathbb{F}_{q^k}$ *satisfying the corresponding conditions. Therefore we have quadratic forms as in (0.3) 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 14 cases above.*

From the proof of Theorem 1 we easily obtain that if $k = 2$ and $\epsilon_0, \epsilon_1 \in \mathbb{F}_{q^k}$, then there is no quadratic form over $\mathbb{F}_{q^k}$ of codimension 2 in the form (0.1), when q is an odd power of 2.

Finally we note that the conditions on the main results in Theorem 1 above and [6, Theorem 3.1] are very different.

References

[1] R. W. Fitzgerald, Highly Degenerate Quadratic Forms over finite fields of characteristic 2, *Finite Fields Appl.*, vol. 11, pp. 165-181, (2005).

[2] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Univ. Press, New York, (1998).

[3] J. W. P. Hirschfeld, G. Korchmáros, F. Torres, *Algebraic Curves over a Finite Field*, Princeton Univ. Press, Princeton, (2008).

[4] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, (1997).

[5] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge Univ. Press, Cambridge, (2001).

[6] F. Özbudak, E. Saygı and Z. Saygı, Quadratic Forms of Codimension 2 over Finite Fields Containing $\mathbb{F}_4$ and Artin-Schreier Type Curves, submitted.

[7] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, (2008).

[8] M. A. Tsfasman, S. G. Vladut, D. Nogin *Algebraic Geometric Codes: Basic Notations*, Mathematical Surveys and monographs vol. 139, American Mathematical Society, Providence, RI, (2007).