Counting quadratic forms of codimension 2 in characteristic 2 and relations to maximal curves

Ferruh Ozbudak, Zülfükar Saygy

Counting quadratic forms of codimension 2 in characteristic 2 and relations to maximal curves

Ferruh Özbudak[1] and Zülfükar Saygı[2]

[1] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey
ozbudak@metu.edu.tr

[2] Department of Mathematics, TOBB University of Economics and Technology, Söğütözü 06530, Ankara, Turkey
zsaygi@etu.edu.tr

Abstract. Let $\mathbb{F}_q$ be an arbitrary finite field of characteristic 2 and $k \geq 2$ be an arbitrary integer. We count the number of quadratic forms of codimension 2 on $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ and we give some related results, including some relations to certain maximal curves over finite fields.

Keywords: quadratic forms over finite fields of characteristic 2, maximal curves over finite fields

1 Introduction

Let $q = 2^t$ with $t \geq 1$ (a power of 2), $k \geq 2$ be an integer and $m = \lfloor k/2 \rfloor$, the integer part of $m/2$. For a positive integer ℓ, let $\mathbb{F}_{2^\ell}$ denote a finite field with 2^ℓ elements (of characteristic 2). Let $Q : \mathbb{F}_{q^k} \to \mathbb{F}_q$ be an arbitrary quadratic form. We assume without loss of generality (see Section 2 below) that there exist uniquely determined $\epsilon_0, \epsilon_1, \ldots, \epsilon_{m-1} \in \mathbb{F}_{q^k}$ and some $\epsilon_m \in \mathbb{F}_{q^k}$ such that for $x \in \mathbb{F}_{q^k}$ we have

$$Q(x) = \mathrm{Tr}\left(x\left(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m}\right)\right). \tag{1}$$

Here ϵ_m is uniquely determined if k is odd and ϵ_m is determined uniquely only modulo $\mathbb{F}_{q^m}$ if k is even. Throughout the paper Tr denotes the trace map from $\mathbb{F}_{q^k}$ onto $\mathbb{F}_q$, while $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}$ denotes the trace map from $\mathbb{F}_q$ onto $\mathbb{F}_2$.

In this paper we count the number of quadratic forms on $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ of codimension 2. We also count the subset of them with the invariant $\Lambda(Q) = 1$. Our results depend on the function $S(\epsilon)$ we introduce in Definition 1 below. We also give some related results on the maximal curves of the form

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

Our results generalize some of the results of Fitzgerald in [3].

2 Background

In this section we recall basic definitions and some facts that we use in this paper. A *quadratic form on* $\mathbb{F}_{q^k}$ *over* $\mathbb{F}_q$ is a map such that

- $Q(\alpha x) = \alpha^2 Q(x)$ for all $\alpha \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^k}$, and
- The related map $B(x, y)$ on $\mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$ defined by

$$B(x, y) = Q(x + y) + Q(x) + Q(y)$$

  is a bilinear map over $\mathbb{F}_q$.

The *radical* W of Q is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^k}$ given by

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

Let w be the $\mathbb{F}_q$-dimension of W. Its codimension $k - w$ is always even. By codimension of Q we mean the difference $k - w$.

There is another invariant $\Lambda(Q)$ of Q, which is an integer in the set $\{-1, 0, 1\}$. In fact if $w = 0$, then Q is called *non-degenerate* and $\Lambda(Q)$ is the *Arf invariant* of Q [1], which is in the subset $\{-1, 1\}$. Let $N(Q)$ denote the cardinality

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

The invariant $\Lambda(Q)$ maybe defined as the integer satisfying

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

(see, for example, [5, Section 6.2]).

The following is a useful characterization of quadratic forms, which allows us to make the assumption on Q in the beginning of Section 1.

Theorem 1 (see [2]). *Let $Q : \mathbb{F}_{q^k} \to \mathbb{F}_q$ be a quadratic form and $m = \lfloor k/2 \rfloor$. There exist $\epsilon_0, \epsilon_1, \ldots, \epsilon_m \in \mathbb{F}_{q^k}$ such that*

$$Q(x) = \mathrm{Tr}\left(x \left(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m} \right) \right). \tag{3}$$

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 (see [2]). *Let $\epsilon_0, \epsilon_1, \ldots, \epsilon_m$ be the coefficients corresponding to Q as in (3). 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 $0 \le i \le \lfloor (k-1)/2 \rfloor$ we have*

$$\epsilon_i = a^{q^i} b + a b^{q^i}, \tag{4}$$

and if k is even, then furthermore

$$\epsilon_m - a b^{q^m} \in \mathbb{F}_{q^m}. \tag{5}$$

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* $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(s) = 1$ *and*

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

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

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

The following result will be used in a proof below.

Lemma 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*

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

Then the following holds:

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

3 Main Results

In this section we present our main results. First we give an "if and only if" characterization of quadratic forms of codimension 2. The following theorem will be useful in our counting results.

Theorem 3. *Q has a codimension 2 radical if and only if there exists a nonzero* $v \in \mathbb{F}_{q^k}^*$ *such that each of the following holds:*

i) $\epsilon_1 \neq 0$, *and we have*

$$v = ab \textit{ and } \frac{\epsilon_1}{v} = a^{q-1} + b^{q-1},$$

for some $a, b \in \mathbb{F}_{q^k}$.

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

iii) For all $3 \leq i \leq \left\lfloor \frac{k-1}{2} \right\rfloor$, *we have*

$$\epsilon_i = \left(\epsilon_1^{q-1}\right)^{q^{i-2}}\epsilon_{i-2} + \left(\epsilon_2\epsilon_1^{-1}\right)^{q^{i-2}}\epsilon_{i-1}.$$

iv) If $k = 2m$ *then* $\left(\epsilon_m - ab^{q^m}\right) \in \mathbb{F}_{q^m}$, *where* a, b *are the elements in* $\mathbb{F}_{q^k}$ *satisfying i).*

Proof. ($\Rightarrow$) Assume that Q has a codimension 2 radical, then using Theorem 2 we know that there exist $a, b \in \mathbb{F}_{q^k}$ such that the set $\{a, b\}$ is linearly independent over $\mathbb{F}_q$ and (4) holds. Set $u = a^{q-1} + b^{q-1}$ and $v = ab$. As a, b are linearly independent over $\mathbb{F}_q$, we have $u \neq 0$. Then we obtain that $\epsilon_1 = a^q b + ab^q = uv \neq 0$, and hence item i) holds.

We know that

$$\begin{aligned} \epsilon_2 &= a^{q^2} b + ab^{q^2} \\ &= ab\left(\left(a^{q-1}\right)^{q+1} + \left(b^{q-1}\right)^{q+1}\right). \end{aligned} \tag{6}$$

Then using Lemma 1 and (6) we get that

$$v^q \epsilon_2 = \epsilon_1^{q+1}\left(1 + \sum_{i=0}^{t-1}\left(v^{q+1}\epsilon_1^{-2}\right)^{2^i}\right), \tag{7}$$

which shows item ii).

Now consider the equation

$$0 = \left(y + \frac{a^q b}{\epsilon_1}\right)\left(y + \frac{ab^q}{\epsilon_1}\right) = y^2 + y + \frac{v^{q+1}}{\epsilon_1^2}. \tag{8}$$

Using (8), its square, its 4-th power, ..., and its $q/2$-th power we obtain that

$$\begin{aligned} y^2 + y &= \frac{v^{q+1}}{\epsilon_1^2}, \\ y^4 + y^2 &= \left(\frac{v^{q+1}}{\epsilon_1^2}\right)^2, \\ &\vdots \\ y^q + y^{q/2} &= \left(\frac{v^{q+1}}{\epsilon_1^2}\right)^{q/2}. \end{aligned} \tag{9}$$

Summing the equations in (9) we get that

$$y^q + y = \sum_{i=0}^{t-1}\left(\frac{v^{q+1}}{\epsilon_1^2}\right)^{2^i}. \tag{10}$$

Combining (7) and (10), we get that

$$y^q + y = 1 + \frac{v^q \epsilon_2}{\epsilon_1^{q+1}}. \tag{11}$$

We know that the set of solutions of (8) is $\left\{\frac{a^q b}{\epsilon_1}, \frac{ab^q}{\epsilon_1}\right\}$. Now we first put $\frac{a^q b}{\epsilon_1}$ in (11). Then we have

$$\frac{a^{q^2} b^q}{\epsilon_1^q} + \frac{a^q b}{\epsilon_1} = 1 + \frac{v^q \epsilon_2}{\epsilon_1^{q+1}}, \tag{12}$$

which implies that

$$a^{q^2} = \epsilon_1^{q-1} a + a^q \epsilon_2 \epsilon_1^{-1}. \tag{13}$$

Similarly putting $\frac{ab^q}{\epsilon_1}$ in (11) we obtain that

$$b^{q^2} = \epsilon_1^{q-1} b + b^q \epsilon_2 \epsilon_1^{-1}. \tag{14}$$

Now using (13) and (14) together with (4) we see that item iii) holds. Finally item iv) follows from (5).

($\Leftarrow$) Now suppose that items i),ii),iii) and iv) hold. Let $a, b \in \mathbb{F}_{q^k}$ satisfying

$$v = ab \text{ and } \frac{\epsilon_1}{v} = a^{q-1} + b^{q-1}. \tag{15}$$

Then we see that a and b are linearly independent over $\mathbb{F}_q$ as $v \in \mathbb{F}_{q^k}^*$ shows $a \neq 0$ and $b \neq 0$, while $\epsilon_1 \neq 0$ shows $a^{q-1} \neq b^{q-1}$, that is, $a/b \notin \mathbb{F}_q^*$.

Using (15) we obtain that

$$\epsilon_1 = ab\left(a^{q-1} + b^{q-1}\right) = a^q b + ab^q. \tag{16}$$

Now putting $v = ab$ in item iii) and using (16), we obtain that

$$\epsilon_2 = a^{q^2} b + ab^{q^2}. \tag{17}$$

Using (16) and (17) together with item iii), for $3 \leq i \leq \left\lfloor \frac{k-1}{2} \right\rfloor$ we get that

$$\epsilon_i = a^{q^i} b + ab^{q^i}. \tag{18}$$

Finally using Theorem 2, the linear independence of a and b, (18) and item iv) we get that Q has a codimension 2 radical.

The following definition is crucial.

Definition 1. *For $\epsilon \in \mathbb{F}_{q^k}^*$, let $S(\epsilon)$ be the number of $v \in \mathbb{F}_{q^k}^*$ such that there exist $a, b \in \mathbb{F}_{q^k}$ satisfying*

$$v = ab \text{ and } \frac{\epsilon}{v} = a^{q-1} + b^{q-1}.$$

If $q = 2$, then $S(\epsilon)$ reduces to the number of $v \in \mathbb{F}_{2^k}$ such that there exist $a, b \in \mathbb{F}_{2^k}$ satisfying

$$v = ab \text{ and } \frac{\epsilon}{v} = a + b.$$

This condition is equivalent to the condition that a and b are the roots of the equation

$$y^2 + \frac{\epsilon}{v} y + v = 0.$$

Using Hilbert's Theorem 90 and a result of Klapper [4], Fitzgerald computed $S(\epsilon)$ exactly in [3, Lemma 2.2].

For general $\mathbb{F}_q$ of characteristic 2, it seems more difficult to compute $S(\epsilon)$ exactly. Using some computer experiments we currently can only conjecture that for $\epsilon \in \mathbb{F}_{q^k}^*$ it holds that

$$S(\epsilon) = \begin{cases} \dfrac{q^k - q}{2(q-1)}, & \text{if } k \text{ is odd,} \\ \dfrac{q^k - (-1)^m(q-1)q^{m+1} - q}{2(q-1)}, & \text{if } k = 2m \text{ and } \epsilon \in \mathbb{F}_{q^k}^{*(q+1)}, \\ \dfrac{q^k + (-1)^m(q-1)q^m - q}{2(q-1)}, & \text{if } k = 2m \text{ and } \epsilon \notin \mathbb{F}_{q^k}^{*(q+1)}. \end{cases}$$

This conjecture is true when $q = 2$ (see [3]) and, for example,

$$(q,k) \in \{(4,5)(4,6)(4,7),(8,5)(8,6)\},$$

that we verified by a computer.

Now we determine the number of quadratic forms of codimension 2.

Theorem 4. *The number of quadratic forms of codimension* 2 *on* $\mathbb{F}_{q^k}$ *over* $\mathbb{F}_q$ *is*

$$q^k \sum_{\epsilon \in \mathbb{F}_{q^k}^*} \frac{S(\epsilon)}{q(q+1)/2}.$$

Proof. We know that $\epsilon_0 \in \mathbb{F}_{q^k}$. So there are q^k choices for ϵ_0. Now for any fixed $\epsilon = \epsilon_1 \in \mathbb{F}_{q^k}^*$, we will show that there are $\dfrac{S(\epsilon_1)}{q(q+1)/2}$ choices for ϵ_2. For each $v \in \mathbb{F}_{q^k}^*$ satisfying $v = ab$ and $\dfrac{\epsilon_1}{v} = a^{q-1} + b^{q-1}$ for some $a, b \in \mathbb{F}_{q^k}$, we get an $\epsilon_2(v) = a^{q^2}b + ab^{q^2}$.

Let v, a, b and $\epsilon_2(v)$ be one choice. Now for any $\alpha, \beta \in \mathbb{F}_q$ we set

$$a' = a + \beta(\alpha a + b) \quad b' = \alpha a + b \quad \text{and} \quad v' = a'b'. \tag{19}$$

Using (19) we obtain that

$$\begin{aligned} v'\left((a')^{q-1} + (b')^{q-1}\right) &= a'b'\left((a')^{q-1} + (b')^{q-1}\right) \\ &= (a + \beta(\alpha a + b))^q (\alpha a + b) + (a + \beta(\alpha a + b))(\alpha a + b)^q \\ &= a^q b + ab^q = \epsilon_1, \end{aligned}$$

which gives

$$\frac{\epsilon_1}{v'} = (a')^{q-1} + (b')^{q-1}.$$

Furthermore using (19) we have

$$(a')^{q^2}b' + a'(b')^{q^2} = a^{q^2}b + ab^{q^2} = \epsilon_2(v),$$

which shows that all the choices in (19) give the same ϵ_2.

Here we note that using item ii) of Theorem 3 there are at most $q(q+1)/2$ v's giving the same ϵ_2. Now we will show that there are exactly $q(q+1)/2$ different v's giving the same ϵ_2 in (19). Let $\alpha_1, \beta_1, \alpha_2, \beta_2 \in \mathbb{F}_q$ and for $i \in \{1, 2\}$

$$a_i = a + \beta_i(\alpha_i a + b) \quad b_i = \alpha_i a + b. \tag{20}$$

Then if $a_1 b_1 = a_2 b_2$ we have

$$(a + \beta_1(\alpha_1 a + b))\,(\alpha_1 a + b) = (a + \beta_2(\alpha_2 a + b))\,(\alpha_2 a + b)$$

which implies that

$$\beta_1 = \beta_2 \quad \text{and} \quad \left(\alpha_1 = \alpha_2 \text{ or } \alpha_1 = \alpha_2 + \beta_1^{-1}\right). \tag{21}$$

Therefore using (21) we see that there are $q + (q-1)q/2 = (q+1)q/2$ different v's giving the same ϵ_2.

We count also the number of quadratic forms Q of codimension 2 having invariant $\Lambda(Q) = 1$.

Corollary 1. *The number of quadratic forms Q of codimension 2 on $\mathbb{F}_{q^k}$ with $\Lambda(Q) = 1$ is*

$$\sum_{\epsilon \in \mathbb{F}^*_{q^k}} S(\epsilon).$$

Proof. We fix $\epsilon = \epsilon_1 \in \mathbb{F}^*_{q^k}$. By the proof of Theorem 4, the number of possible choices for ϵ_2 is $\dfrac{S(\epsilon_1)}{q(q+1)/2}$. Moreover there is a $q(q+1)/2$-to-1 map between the set of possible values of v (whose cardinality is $S(\epsilon_1)$) and the set of possible choices of ϵ_2. Also $\Lambda(Q) = 1$ if and only if $\epsilon_0 = v$ by Theorem 2. Therefore the number we are counting is

$$\frac{q(q+1)}{2} \sum_{\epsilon_1 \in \mathbb{F}^*_{q^k}} \frac{S(\epsilon_1)}{q(q+1)/2}.$$

4 Relations to Certain Maximal Curves

In this section we give some related results to maximal curves of the form

$$\chi: \quad y^q + y = x\left(\epsilon_0 x + \epsilon_1 x^q + \cdots + \epsilon_m x^{q^m}\right). \tag{22}$$

Assume that Q is of codimension 2 and $k \geq 6$. Let ℓ be the integer

$$\ell = \max\{0 \leq i \leq m : \epsilon_i \neq 0\}.$$

By Theorem 3 we have that $\epsilon_1 \neq 0$ and hence $\ell \geq 1$, χ is algebraically closed over $\mathbb{F}_{q^k}$ and its genus is

$$g = \frac{(q-1)q^\ell}{2}.$$

Next we show that $\ell \in \{m-1, m\}$ using Hasse-Weil bound [6, Theorem 5.2.3].

Proposition 1. *Assume that Q is a quadratic form on $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ of codimension 2 and $k \geq 6$. Let Q be as in (1) without loss of generality. Then $\epsilon_{m-1} \neq 0$ or $\epsilon_m \neq 0$.*

Proof. Assume the contrary and hence for the genus g of the curve χ in (22) we have

$$g \leq \frac{(q-1)q^{m-2}}{2}.$$

By choosing ϵ_0 appropriately we can assume that $\Lambda(Q) = 1$ without loss of generality. Using Hilbert Theorem 90 and (2), for the number $\#\chi$ of $\mathbb{F}_{q^k}$ rational points of χ we obtain that

$$\#\chi = 1 + qN(Q) = 1 + q^k + (q-1)q^{k-1}. \tag{23}$$

Moreover by Hasse-Weil inequality we have

$$\#\chi \leq 1 + q^k + 2gq^{k/2} = 1 + q^k + (q-1)q^{m+k/2-2}. \tag{24}$$

Comparing (23) and (24) we get that

$$k - 1 \leq m + k/2 - 2.$$

which is a contradiction.

Assume further that $k \geq 6$ and Q is a quadratic form of codimension 2 on $\mathbb{F}q^k$ over $\mathbb{F}_q$. Using Theorem 3 we choose and fix $\epsilon_1, a, b \in \mathbb{F}^*_{q^k}$. Furthermore we determine the other coefficients $\epsilon_2, \ldots, \epsilon_{m-1} \in \mathbb{F}_{q^k}$ uniquely and $\epsilon_m \in \mathbb{F}_{q^k}$ uniquely if k is odd and uniquely modulo $\mathbb{F}_{q^m}$ if k is even following Theorem 3. If k is even and $ab^{q^m} \in \mathbb{F}_{q^m}$ we put $\epsilon_m = 0$ without loss of generality. Let χ be the curve in (22) with these coefficients.

Proposition 2. *Under the notation and assumptions as above, χ is maximal if and only if each of the following items hold:*

i) k is even,

ii) $\Lambda(Q) = 1$,
iii) $ab^{q^m} \in \mathbb{F}_{q^m}$.

Note that Corollary 1 is useful for counting such quadratic forms satisfying items i) and ii) of Proposition 2. However to determine how many of them also satisfy item iii) of Proposition 2 seems to be difficult (see also [3, Section 3]).

Acknowledgments. The authors would like to thank the anonymous reviewers for their valuable comments. The authors were partially supported by TÜBİTAK under Grant No. TBAG–109T672. The work of Z. Saygı was also supported by TÜBİTAK under Grant No. TBAG–109T344.

References

1. C. Arf, Untersuchungen über quadratische Formen in Körpern der Charakteristik 2, I, *J. Reine Angew. Math*, vol. 183, pp. 148–167, (1941).
2. R. W. Fitzgerald, Highly Degenerate Quadratic Forms over finite fields of characteristic 2, *Finite Fields Appl.*, vol. 11, pp. 165-181, (2005).
3. R. W. Fitzgerald, Highly Degenerate Quadratic Forms over $\mathbb{F}_2$, *Finite Fields Appl.*, vol. 13, pp. 778-792, (2007).
4. A. Klapper, Cross-correlations of geometric sequences in characteristic 2, *Des. Codes Cryptogr.*, vol. 3, pp. 347-377, (1993).
5. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, (1997).
6. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, (2008).