11-2007

Highly Degenerate Quadratic Forms over F_2

Robert W. Fitzgerald
Southern Illinois University Carbondale, rfitzg@math.siu.edu

Published in *Finite Fields and Their Applications*, *13, 778-792. doi: 10.1016/j.ffa.2005.11.005*

Highly degenerate quadratic forms over F_2

Robert W. Fitzgerald

Abstract

Let K be a finite extension of F_2. We consider quadratic forms written as the trace of $xR(x)$, where $R(x)$ is a linearized polynomial. We determine the K and $R(x)$ where the form has a radical of codimension 2. This is applied to constructing maximal Artin-Schreier curves.

Set $F = F_2$ and let $K = F_{2^k}$ be an extension of degree k. Let

$$R_{\bar{\varepsilon}}(x) = \sum_{i=0}^{m} \epsilon_i x^{2^i},$$

with each $\epsilon_i \in K$ and either $k = 2m$ or $k = 2m+1$. We consider the quadratic forms $Q_{\bar{\varepsilon}}^K : K \to F$ given by $Q_{\bar{\varepsilon}}^K(x) = tr_{K/F}(xR_{\bar{\varepsilon}}(x))$.

These trace forms have appeared in a variety of contexts. They have been used to compute weight enumerators of certain binary codes [1], [2] , to construct curves with many rational points and the associated trace codes [9], as part of an authentication scheme [3], and to construct certain binary sequences in [6] and [5].

In each of these applications one wants the number of solutions (in K) to $Q_{\bar{\varepsilon}}^K(x) = 0$, denoted by $N(Q_{\bar{\varepsilon}}^K)$. This is easily worked out (see [8], 6.26,6.32) in terms of the standard classification of quadratic forms:

$$N(Q_{\bar{\varepsilon}}^K) = \tfrac{1}{2}(2^k + \Lambda(Q_{\bar{\varepsilon}}^K)\sqrt{2^{k+w}}). \tag{1}$$

where w is the dimension of the radical, $v = (k-w)/2$ and

$$\Lambda(Q_{\bar{\varepsilon}}^K) = \begin{cases} 0, & \text{if } Q_{\bar{\varepsilon}}^K \simeq z^2 + \sum_{i=1}^{v} x_i y_i \\ 1, & \text{if } Q_{\bar{\varepsilon}}^K \simeq \sum_{i=1}^{v} x_i y_i \\ -1, & \text{if } Q_{\bar{\varepsilon}}^K \simeq x_1^2 + y_1^2 + \sum_{i=1}^{v} x_i y_i. \end{cases}$$

However, there is no simple way to determine the dimension of the radical or the invariant Λ. The one general result is due to Klapper [7] which only covers the case when R consists of a single term. In roughly half the applications ([1], [2], [9]) one wants highly degenerate forms, which give large $N(Q_{\bar{\varepsilon}}^K)$ when $\Lambda = 1$. In a previous paper [4] we considered only those R with all coefficients $\epsilon_i \in F_2$ but allowed F to be any finite field of characteristic 2. Here we restrict to $F = F_2$, the case of most applications, and allow arbitrary coefficients ε_i. Our main result is to determine all such $R_{\bar{\varepsilon}}$, and all extensions K, such that the radical of $Q_{\bar{\varepsilon}}^K$ has codimension at most 2. We compute the invariant Λ in each case. We apply the result to a classification of maximal Artin-Schreier curves $y^2 = xR_{\bar{\varepsilon}}(x)$.

The two situations, $\varepsilon_i \in F_2$ (treated in [4]) and $F = F_2$ (treated here), look similar but are in fact quite different. For instance, when $K = F_{2^9}$, there are exactly two quadratic forms of codimension 2 radical with $\varepsilon_i \in F_2$ but over 22 million with arbitrary ε_i. The classification here is then not a list of possible $R_{\bar{\varepsilon}}$ but formulas showing how an arbitrary $\varepsilon_0, \varepsilon_1$ determine the other ε_i. We also give formulas for the number of forms of codimension 2 radical of each invariant Λ.

1 Determining the coefficients

We recall the basic result from [4].

Lemma 1.1. *(1) The radical of $Q_{\bar{\varepsilon}}^K$ does not depend on ε_0, that is, if $\varepsilon_i = \varepsilon_i'$ for $i \geq 1$ then*

$$rad(Q_{\bar{\varepsilon}}^K) = rad(Q_{\bar{\varepsilon}'}^K).$$

(2) We have $\dim rad(Q_{\bar{\varepsilon}}^K) = k - 2$ iff there exist independent (over F) $a, b \in K$ such that

$$\varepsilon_i = a^{2^i} b + a b^{2^i}, \tag{2}$$

for $1 \leq i \leq m$, except when $k = 2m$ in which case $\varepsilon_m \equiv a^{2^m} b \pmod{F_{2^m}}$. Moreover, $\Lambda(Q_{\bar{\varepsilon}}^K) = +1$ if $\varepsilon_0 = ab$, $\Lambda(Q_{\bar{\varepsilon}}^K) = -1$ if $\varepsilon_0 = a^2 + ab + b^2$ and $\Lambda(Q_{\bar{\varepsilon}}^K) = 0$ in all other cases.

If Equation 2 holds then $\varepsilon_1 = ab(a+b)$ so that $\varepsilon_1 = 0$ implies $a = 0$, $b = 0$ or $a = b$. This contradicts the independence of a, b. Hence if $Q_{\bar{\varepsilon}}^K$ has a codimension 2 radical then $\varepsilon_1 \neq 0$. We will use this fact constantly, and without further mention, throughout.

Set $h = \lfloor (k-1)/2 \rfloor$. Then Equation 2 holds for $1 \leq i \leq h$ (that is, we have excluded the exceptional case $i = m$ when $k = 2m$).

Lemma 1.2. *$Q_{\bar{\varepsilon}}^K$ has a codimension 2 radical iff there exists a $v \in K^*$ such that each of the following holds:*

1. *$\varepsilon_1 \neq 0$ and $y^2 + (\varepsilon_1/v)y + v$ splits in K.*

2. *For all $2 \leq i \leq h$,*

$$v^{2^{i-1}}\varepsilon_i = \varepsilon_1^{2^{i-1}}\varepsilon_{i-1} + \varepsilon_1 v^{2^i-1}.$$

3. *If $k = 2m$ then $\varepsilon_m \equiv a^{2^m} b \pmod{F_{2^m}}$, where a, b are the roots of (1).*

Proof: First suppose $Q_{\bar{\varepsilon}}^K$ has a codimension 2 radical. Let $a, b \in K$ be the elements giving Lemma 1.1 (2). Set $u = a + b$ and $v = ab$. Then $\varepsilon_1 = a^b + ab^2 = uv$. Hence

$$y^2 + \frac{\varepsilon_1}{v}y + v = (y+a)(y+b)$$

splits in K.

From [4] p. 173,

$$v\sum_{j=0}^{i-1} u^{2^i-2^{j+1}+1}v^{2^j-1} = \varepsilon_i.$$

Replacing u by ε_1/v, and multiplying by v^{2^i-2} gives

$$\sum_{j=0}^{i-1} \varepsilon_1^{2^i-2^{j+1}+1}v^{3(2^j-1)} = \varepsilon_i v^{2^i-2}.$$

Hence

$$\begin{aligned}
\varepsilon_1^{2^{i-1}}\sum_{j=0}^{i-2}\varepsilon_1^{2^{i-1}-2^{j+1}+1}v^{3(2^j-1)} + \varepsilon_1 v^{3(2^{i-1}-1)} &= \varepsilon_i v^{2^i-2} \\
\varepsilon_1^{2^{i-1}}\varepsilon_{i-1}v^{2^{i-1}-2} + \varepsilon_1 v^{3(2^{i-1}-1)} &= \varepsilon_i v^{2^i-2} \\
\varepsilon_1^{2^{i-1}}\varepsilon_{i-1} + \varepsilon_1 v^{2^i-1} &= \varepsilon_i v^{2^{i-1}},
\end{aligned}$$

which gives (2). And (3) follows Lemma 1.1.

Now suppose (1), (2) and (3) hold. Let $a, b \in K$ be the roots of (1). Note that a and b are independent over F as $v \neq 0$ shows $a \neq 0$ and $b \neq 0$, while $\varepsilon_1 \neq 0$ shows $a \neq b$. Note that $v = ab$ and $\varepsilon_1/v = a + b$. So $\varepsilon_1 = a^2b + ab^2$. We show by induction that Lemma 1.1 (2) holds for all $2 \leq i \leq h$. We have by (2) and induction that

$$\begin{aligned} (ab)^{2^i}\varepsilon_{i+1} &= [ab(a+b)]^{2^i}(a^{2^i}b + ab^{2^i}) + ab(a+b)(ab)^{2^{i+1}-1} \\ \varepsilon_{i+1} &= (a^{2^i} + b^{2^i})(a^{2^i}b + ab^{2^i}) + (ab)^{2^i}(a+b) \\ &= a^{2^{i+1}}b + ab^{2^{i+1}}. \end{aligned}$$

This, with (3), shows $Q_{\bar{\varepsilon}}^K$ has a codimension 2 radical. $\square$

We want a formula for ε_i that does not depend on v, only on the initial coefficients ε_1 and ε_2. Now

$$\begin{aligned} v^3 &= \frac{\varepsilon_2}{\varepsilon_1}v^2 + \varepsilon_1^2 \\ v^4 &= \frac{\varepsilon_2}{\varepsilon_1}\varepsilon v^3 + \varepsilon_1^2 v = \frac{\varepsilon_2^2}{\varepsilon_1^2}v^2 + \varepsilon_1^2 v + \varepsilon_1\varepsilon_2. \end{aligned}$$

Hence for each $i \geq 0$ we can write

$$v^{2^i} = A_i v^2 + B_i v + C_i,$$

where $A_i, B_i, C_i \in F(\varepsilon_1, \varepsilon_2)$.

Lemma 1.3. *Suppose $v^2\varepsilon_2 = \varepsilon_1^3 + v^3\varepsilon_1$.*

1. *We have $A_1 = 1, B_1 = 0, C_1 = 0$ and for each $i \geq 1$*

$$A_{i+1} = \frac{\varepsilon_2^2}{\varepsilon_1^2}A_i^2 + B_i^2 \qquad B_{i+1} = \varepsilon_1^2 A_i^2 \qquad C_{i+1} = \varepsilon_1\varepsilon_2 A_i^2 + C_i^2.$$

2. *$C_i^2 = \varepsilon_1^2 A_i B_i$ for $i \geq 1$.*
3. *$\varepsilon_2^2 A_i^2 B_i + \varepsilon_1^4 A_i^3 + \varepsilon_1^2 B_i^3 = \varepsilon_1^{2^{i+1}}$ for $i \geq 1$.*
4. *$(\varepsilon_2 A_i + \varepsilon_1 B_i)C_i + \varepsilon_1^3 A_i^2 = \varepsilon_1^{2^i}(\varepsilon_2 A_{i-1}\varepsilon + \varepsilon_1 B_{i-1})$ for all $i \geq 1$.*

Proof: (1) We have

$$\begin{aligned} v^{2^{i+1}} &= A_i^2 v^4 + B_i^2 v^2 + C_i^2 \\ &= (\frac{\varepsilon_2^2}{\varepsilon_1^2} A_i^2 + B_i^2) v^2 + \varepsilon_1^2 A_i^2 v + (\varepsilon_1 \varepsilon_2 A_i^2 + C_i^2). \end{aligned}$$

(2) This is true for $i = 1$. And

$$\begin{aligned} \varepsilon_1^2 A_{i+1} B_{i+1} &= (\varepsilon_2^2 A_i^2 + \varepsilon_1^2 B_i^2) \varepsilon_1^2 A_i^2 \\ &= \varepsilon_1^2 \varepsilon_2^2 A_i^4 + \varepsilon_1^4 A_i^2 B_i^2 \\ &= \varepsilon_1^2 \varepsilon_2^2 A_i^4 + C_i^4 \quad \text{(by induction)} \\ &= C_{i+1}^2, \end{aligned}$$

by (1).

(3) This is true for $i = 1$. And

$$\begin{aligned} \varepsilon_2^2 A_{i+1}^2 B_{i+1} \quad + \quad & \varepsilon_1^4 A_{i+1}^3 + \varepsilon_1^2 B_{i+1}^3 \\ &= (\frac{\varepsilon_2^2}{\varepsilon_1^2} A_i^2 + B_i^2)^2 \varepsilon_1^2 \varepsilon_2^2 A_i^2 + \varepsilon_1^4 (\frac{\varepsilon_2^2}{\varepsilon_1^2} A_i^2 \varepsilon^2 + B_i^2)^3 + \varepsilon_1^2 (\varepsilon_1^2 A_i^2)^3 \\ &= \varepsilon_2^4 A_i^4 B_i^2 + \varepsilon_1^4 B_i^6 + \varepsilon_1^8 A_i^6 \\ &= (\varepsilon_2^2 A_i^2 B_i + \varepsilon_1^4 A_i^3 + \varepsilon_1^2 B_i^3)^2 = (\varepsilon_1^{2^{i+1}})^2 = \varepsilon_1^{2^{i+2}}, \end{aligned}$$

using induction.

(4) This is true for $i = 1$. And

$$\begin{aligned} (\varepsilon_2 A_{i+1} \quad + \quad & \varepsilon_1 B_{i+1}) C_{i+1} + \varepsilon_1^3 A_{i+1}^2 \\ &= (\varepsilon_2 [\frac{\varepsilon_2^2}{\varepsilon_1^2} A_i^2 + B_i^2] + \varepsilon_1^3 A_i^2)(\varepsilon_1 \varepsilon_2 A_i^2 + C_i^2) + \varepsilon_1^3 (\frac{\varepsilon_2^2}{\varepsilon_1^2} A_i^2 + B_i^2)^2 \\ &= (\frac{\varepsilon_2^3}{\varepsilon_1^2} A_i^2 C_i^2 + \varepsilon_2 B_i^2 C_i^2) + \varepsilon_1^4 \varepsilon_2 A_i^4 + (\varepsilon_1 \varepsilon_2^2 A_i^2 B_i^2 + \varepsilon_1^2 A_i^2 C_i^2 + \varepsilon_1^3 B_i^4) \\ &= \frac{\varepsilon_2}{\varepsilon_1^2} C_i^2 (\varepsilon_2^2 A_i^2 + \varepsilon_1^2 B_i^2) + \varepsilon_1^4 \varepsilon_2 A_i^4 + \varepsilon_1 B_i (\varepsilon_2^2 A_i^2 B_i + \varepsilon_1^4 A_i^3 + \varepsilon_1^2 B_i^3) \\ &= \frac{\varepsilon_2}{\varepsilon_1^2} (\varepsilon_1^3 A_i^2 + \varepsilon_1^{2^i} (\varepsilon_2 A_{i-1} + \varepsilon_1 B_{i-1}))^2 + \varepsilon_1^4 \varepsilon_2 A_i^4 + \varepsilon_1 B_i \varepsilon_1^{2^{i+1}} \\ &= \frac{\varepsilon_2}{\varepsilon_1^2} \varepsilon_1^{2^{i+1}} (\varepsilon_2^2 A_{i-1}^2 + \varepsilon_1^2 B_{i-1}^2) + \varepsilon_1 B_i \varepsilon_1^{2^{i+1}} \\ &= \varepsilon_1^{2^{i+1}} (\varepsilon_2 A_i + \varepsilon_1 B_i). \end{aligned}$$

Here the third line uses (2) while the fourth line uses induction and (3). $\square$

Proposition 1.4. *Suppose $v^2\varepsilon_2 = \varepsilon_1 v^3 + \varepsilon_1^3$. Then Lemma 1.2 (2) holds iff $\varepsilon_{i+1} = \varepsilon_2 A_i + \varepsilon_1 B_i = \varepsilon_1\sqrt{A_{i+1}}$ for all $i \geq 1$.*

Proof: Suppose Lemma 1.2 (2) holds. The second equation is true for $i = 1$. For $i > 1$, Lemma 1.3 (1) gives :

$$\begin{aligned}
\varepsilon_{i+1} &= \frac{\varepsilon_1 v^{2^{i+1}-1} + \varepsilon_1^{2^i}\varepsilon_i}{v^{2^i}} \\
&= \frac{\frac{\varepsilon_1}{v}(A_{i+1}v^2 + B_{i+1}v + C_{i+1}) + \varepsilon_1^{2^i}\varepsilon_i}{A_i v^2 + B_i v + C_i}.
\end{aligned}$$

Now

$$\frac{1}{v} = \frac{1}{\varepsilon_1^2}v^2 + \frac{\varepsilon_2}{\varepsilon_1^3}v.$$

Then

$$\begin{aligned}
\varepsilon_{i+1} &= \frac{\frac{1}{\varepsilon_1}C_{i+1}v^2 + (\frac{\varepsilon_2}{\varepsilon_1^2}C_{i+1} + \varepsilon_1 A_{i+1})v + \varepsilon_1 B_{i+1} + \varepsilon_1^{2^i}\varepsilon_i}{A_i v^2 + B_i v + C_i} \\
&= \frac{(\varepsilon_2 A_i^2 + \frac{1}{\varepsilon_1}C_i^2)v^2 + (\frac{\varepsilon_2}{\varepsilon_1^2}C_i^2 + \varepsilon_1 B_i^2)v + \varepsilon_1^3 A_i^2 + \varepsilon_1^{2^i}\varepsilon_i}{A_i v^2 + B_i v + C_i}.
\end{aligned}$$

By Lemma 1.3 (2)

$$\begin{aligned}
(\varepsilon_2 A_i + \varepsilon_1 B_i)A_i &= \varepsilon_2 A_i^2 + \varepsilon_1 A_i B_i = \varepsilon_2 A_i^2 + \frac{1}{\varepsilon_1}C_i^2 \\
(\varepsilon_2 A_i + \varepsilon_1 B_i)B_i &= \varepsilon_2 A_i B_i + \varepsilon_1 B_i^2 = \frac{\varepsilon_2}{\varepsilon_1^2}C_i^2 + \varepsilon_1 B_i^2.
\end{aligned}$$

Lastly, from Lemma 1.3 (4)

$$\begin{aligned}
(\varepsilon_2 A_i + \varepsilon_1 B_i)C_i &= \varepsilon_1^3 A_i^2 + \varepsilon_1^{2^i}(\varepsilon_2 A_{i-1} + \varepsilon_1 B_{i-1}) \\
&= \varepsilon_1^3 A_i^2 + \varepsilon_1^{2^i}\varepsilon_i,
\end{aligned}$$

using induction. Hence $\varepsilon_{i+1} = \varepsilon_2 A_i + \varepsilon_1 B_i$.

For the converse, the steps may be reversed. □

Theorem 1.5. *$Q_{\bar{\varepsilon}}^K$ has codimension 2 radical iff there exists $v \in K^*$ such that each of the following holds*

1. *$\varepsilon_1 \neq 0$ and $y^2 + (\varepsilon_1/v)y + v$ splits in K,*

2. $v^2\varepsilon_2 = \varepsilon_1^3 + \varepsilon_1 v^3$*,*

3. for $i \geq 2$ *we have*

$$\varepsilon_{i+1} = \frac{\varepsilon_2}{\varepsilon_1^2}\varepsilon_i^2 + \frac{1}{\varepsilon_1}\varepsilon_{i-1}^4,$$

4. if $k = 2m$ *then* $\varepsilon_m \equiv a^{2^m} b \pmod{F_{2^m}}$*, where* a, b *are the roots of (1).*

Moreover, in this case,

$$\Lambda(Q_{\bar{\varepsilon}}^K) = \begin{cases} 1, & \text{if } \epsilon_0 = v \\ -1, & \text{if } \epsilon_0 = v + (\varepsilon_1/v)^2 \\ 0, & \text{otherwise.} \end{cases}$$

Proof: We need to show that Lemma 1.1 (2) is equivalent to the statement (3) here, given (1) and (2). We first check that Lemma 1.1 implies (3).

$$\begin{aligned} \varepsilon_{i+1} &= \varepsilon_2 A_i + \varepsilon_1 B_i \qquad \text{by Proposition 1.4} \\ &= \varepsilon_2(\sqrt{A_i})^2 + \varepsilon_1^3(\sqrt{A_{i-1}})^4 \qquad \text{by Lemma 1.3 (1)} \\ &= \frac{\varepsilon_2}{\varepsilon_1^2}\varepsilon_i^2 + \frac{1}{\varepsilon_1}\varepsilon_{i-1}^4 \qquad \text{by Proposition 1.4.} \end{aligned}$$

Next we check that (3) implies Lemma 1.1 (2). It is enough to show $\varepsilon_{i+1} = \varepsilon_2 A_i + \varepsilon_1 B_i$, by Proposition 1.4. We use induction. The case $i = 1$ is clear.

$$\begin{aligned} \varepsilon_{i+1} &= \frac{\varepsilon_2}{\varepsilon_1^2}\varepsilon_i^2 + \frac{1}{\varepsilon_1}\varepsilon_{i-1}^4 \qquad \text{by (3)} \\ &= \frac{\varepsilon_2}{\varepsilon_1^2}(\varepsilon_2 A_{i-1} + \varepsilon_1 B_{i-1})^2 + \frac{1}{\varepsilon_1}\varepsilon_{i-1}^4 \qquad \text{by induction} \\ &= \frac{\varepsilon_2^3}{\varepsilon_1^2}A_{i-1}^2 + \varepsilon_2 B_{i-1}^2 + \frac{1}{\varepsilon_1}\varepsilon_{i-1}^4 \\ &= \varepsilon_2\left(\frac{\varepsilon_2^2}{\varepsilon_1^2}A_{i-1}^2 + B_{i-1}^2\right) + \frac{1}{\varepsilon_1}\varepsilon_{i-1}^4 \\ &= \varepsilon_2 A_i + \frac{1}{\varepsilon_1}(\varepsilon_1\sqrt{A_{i-1}})^4 \qquad \text{by Lemma 1.3 (1) and induction} \\ &= \varepsilon_2 A_i + \varepsilon_1 B_i, \end{aligned}$$

using Lemma 1.3 (1) again.

Lastly, we check the invariants. As a, b are roots of $y^2 + (\varepsilon_1/v)y + v$, we have $v = ab$ and $\varepsilon_1/v = a + b$. Now, by Lemma 1.1, $\Lambda(Q_{\bar{\varepsilon}}^K) = +1$ iff $\varepsilon_0 = ab$, which is v. And $\Lambda(Q_{\bar{\varepsilon}}^K) = -1$ iff $\varepsilon_0 = a^2 + ab + b^2 = v + (\varepsilon_1/v)^2$. $\square$

Proposition 1.6. *Equation (3) of Theorem 1.5 is equivalent to:*

$$\varepsilon_i = \frac{\varepsilon_2^{s_i}}{\varepsilon_1^{\ell_i}} \sum_{j \in \Delta_i} \varepsilon_1^{5(t_i - j)} \varepsilon_2^{3j},$$

where $\ell_i = 2^{i-1} - 2$,

$$s_i = \begin{cases} 0, & \text{if } i \text{ is odd} \\ 1, & \text{if } i \text{ is even,} \end{cases} \qquad t_i = \begin{cases} (2^{i-1} - 1)/3, & \text{if } i \text{ is odd} \\ (2^{i-1} - 2)/3, & \text{if } i \text{ is even,} \end{cases}$$

$\Delta_3 = \{0, 1\}$, $\Delta_4 = \{0, 1, 2\}$ *and for* $i \geq 5$

$$\Delta_i = (A_i + \{0, 1, 2\}) \cup (2A_{i-1} + \{4, 5\})$$

where

$$A_i = \{0\} \cup \{2^{n_1} + 2^{n_2} + \cdots + 2^{n_r} : n_j - n_{j-1} \geq 2, n_1 \leq i - 3, n_r \geq 3\}.$$

Proof: Assume first that Theorem 1.5 (3) holds. The formulas for ε_3 and ε_4 can be checked directly. We use induction. Suppose i is odd (the case of i even is similar). Then

$$\begin{aligned} s_{i-1} &= 0 \qquad s_i = 1 \qquad s_{i+1} = 0 \\ 2\ell_{i-1} &= \ell_i - 2 \qquad 2\ell_i = \ell_{i+1} - 2 \\ 2t_{i-1} &= t_i + 1 \qquad 2t_i = t_{i+1}. \end{aligned}$$

We have

$$\begin{aligned} \varepsilon_{i+1} &= \frac{\varepsilon_2}{\varepsilon_1^2} \varepsilon_i^2 + \frac{1}{\varepsilon_1} \varepsilon_{i-1}^4 \\ &= \frac{\varepsilon_2}{\varepsilon_1^2} \left[\frac{1}{\varepsilon_1^{\ell_i}} \sum_{j \in \Delta_i} \varepsilon_i^{5(t_i - j)} \varepsilon_2^{3j} \right]^2 + \frac{1}{\varepsilon_1} \left[\frac{\varepsilon_2}{\varepsilon_1^{\ell_{i-1}}} \sum_{j \in \Delta_{i-1}} \varepsilon_1^{5(t_{i-1} - j)} \varepsilon_2^{3j} \right]^4 \\ &= \frac{\varepsilon_2}{\varepsilon_1^{2\ell_i + 2}} \sum_{j \in \Delta_i} \varepsilon_1^{5(2t_i - 2j)} \varepsilon_2^{3(2j)} + \frac{\varepsilon_2^4}{\varepsilon_1^{2\ell_i - 3}} \sum_{j \in \Delta_{i-1}} \varepsilon_1^{5(2t_i - 4j - 2)} \varepsilon_2^{3(4j)} \\ &= \frac{\varepsilon_2}{\varepsilon_1^{\ell_{i+1}}} \left[\sum_{j \in \Delta_i} \varepsilon_1^{5(t_{i+1} - 2j)} \varepsilon_2^{3(2j)} + \sum_{j \in \Delta_{i-1}} \varepsilon_1^{5(t_{i+1} - 4j - 1)} \varepsilon_2^{3(4j+1)} \right]. \end{aligned}$$

Note that there are no terms in common to the two sums. Set

$$\Delta_{i+1} = 2\Delta_i \cup (4\Delta_{i-1} + 1).$$

Then we have

$$\varepsilon_{i+1} = \frac{\varepsilon_2^{s_{i+1}}}{\varepsilon_1^{\ell_{i+1}}} \sum_{j \in \Delta_{i+1}} \varepsilon_1^{5(t_{i+1}-j)} \varepsilon_2^{3j}.$$

Hence we need only check that $\Delta_{i+1} = (A_{i+1} + \{0,1,2\}) \cup (2A_{i-1} + \{4,5\})$. We do this by induction on i.

Claim $A_{i+1} = 2A_i \cup (4A_{i-1} + 8)$. The inclusion $\supset$ is easy to check. Suppose $\alpha = 2^{n_1} + \cdots 2^{n_r} \in A_{i+1}$. If $n_r \geq 4$ then

$$\alpha = 2(2^{n_1 - 1} + \cdots + 2^{n_r - 1}) \in 2A_i.$$

If $n_r = 3$ then $n_{r-1} \geq 5$ and

$$\alpha = 4(2^{n_1-2} + \cdots 2^{n_{r-1}-2}) + 8 \in 4A_{i-1} + 8,$$

proving the **Claim**.

We have $\Delta_{i+1} = 2\Delta_i \cup (4\Delta_{i-1} + 1)$ so by induction

$$\begin{aligned} \Delta_{i+1} = (2A_i + \{0,2,4\}) &\cup (4A_{i-1} + \{8,10\}) \\ \cup(4A_{i-1} + \{1,5,9\}) &\cup (8A_{i-2} + \{17,21\}). \end{aligned}$$

Now by the **Claim**

$$\begin{aligned} A_{i+1} &= 2A_i \cup (4A_{i-1} + 8) \\ A_{i+1} + 2 &= (2A_i + 2) \cup (4A_{i-1} + 10) \\ A_{i+1} + 1 &= (2A_i + 1) \cup (4A_{i-1} + 9) \\ &= 2[2A_{i-1} \cup (4A_{i-2} + 8)] + 1 \cup (4A_{i-1} + 9) \\ &= (4A_{i-1} + 1) \cup (8A_{i-2} + 17) \cup (4A_{i-1} + 9) \\ 2A_i + 5 &= 2[2A_{i-1} \cup (4A_{i-2} + 8)] + 5 \\ &= (4A_{i-1} + 5) \cup (8A_{i-2} + 21). \end{aligned}$$

Thus $\Delta_{i+1} = (A_{i+1} + \{0,1,2\}) \cup (2A_i + \{4,5\})$.

The converse follows from a simple, but tedious, substitution. $\square$

Here are the first few ε_i:

$$\begin{aligned}
\varepsilon_3 &= \frac{1}{\varepsilon_1^2}(\varepsilon_2^3 + \varepsilon_1^5) \\
\varepsilon_4 &= \frac{\varepsilon_2}{\varepsilon_1^6}(\varepsilon_2^6 + \varepsilon_1^5\varepsilon_2^3 + \varepsilon_1^{10}) \\
\varepsilon_5 &= \frac{1}{\varepsilon_1^{14}}(\varepsilon_2^{15} + \varepsilon_1^5\varepsilon_2^{12} + \varepsilon_1^{10}\varepsilon_2^9 + \varepsilon_1^{20}\varepsilon_2^3 + \varepsilon_1^{25}) \\
\varepsilon_6 &= \frac{\varepsilon_2}{\varepsilon_1^{30}}(\varepsilon_2^{30} + \varepsilon_1^5\varepsilon_2^{27} + \varepsilon_1^{10}\varepsilon_2^{24} + \varepsilon_1^{20}\varepsilon_2^{18} + \varepsilon_1^{25}\varepsilon_2^{15} + \varepsilon_1^{40}\varepsilon_2^6 + \varepsilon_1^{45}\varepsilon_2^3 + \varepsilon_1^{50}).
\end{aligned}$$

The next two Δ_i are:

$$\begin{aligned}
\Delta_7 &= \{0, 1, 3, 4, 5, 11, 12, 13, 16, 17, 19, 20, 21\} \\
\Delta_8 &= \{0, 1, 2, 5, 6, 8, 9, 10, 21, 22, 24, 25, 26, 32, 33, 34, 37, 38, 40, 41, 42\}.
\end{aligned}$$

2 Construction and Examples

Construction: Choose any $\varepsilon_0 \in K$ and $\varepsilon_1 \in K^*$. Find all $v \in K^*$ such that $y^2 + (\varepsilon_1/v)y + v$ splits in K. Set $\varepsilon_2 = (\varepsilon_1 v^3 + \varepsilon_1^3)/v^2$. Let ε_i, for $3 \le i \le \lfloor (k-1)/2 \rfloor$, be given by Corollary 1.6. If $k = 2m$ then set $\varepsilon_m = a^{2^m} b$, where a, b are the roots of $y^2 + (\varepsilon_1/v)y + v$. Take

$$R_{\bar{\varepsilon}} = \sum_{j=0}^{m} \varepsilon_j x^{2^j}.$$

Corollary 2.1. *The construction gives all $R_{\bar{\varepsilon}}$ such that $Q_{\bar{\varepsilon}}^K$ has a codimension 2 radical.*

Proof: This is a re-statement of Theorem 1.5. □

We wish to count the number of such $R_{\bar{\varepsilon}}$.

Lemma 2.2. *The number S of $v \in K^*$ such that $y^2 + (\epsilon_1/v)y + v$ splits in K is*

$$S = \begin{cases} \frac{1}{2}(2^k - 2), & \text{if } k \text{ is odd} \\ \frac{1}{2}(2^k - (-1)^m 2^{m+1} - 2), & \text{if } k = 2m \text{ and } \epsilon_1 \in K^{*3} \\ \frac{1}{2}(2^k + (-1)^m 2^m - 2), & \text{if } k = 2m \text{ and } \epsilon_1 \notin K^{*3}. \end{cases}$$

Proof: Let $q : K \to F$ be $q(x) = \mathrm{tr}_{K/F}(\epsilon_1^{-2}x^3)$. We first check that $S = N(q) - 1$, where $N(q)$ denotes the number of zeros of q in K. Now

$$\frac{v^2}{\epsilon_1^2}(y^2 + \frac{\epsilon_1}{v}y + v) = \left(\frac{vy}{\epsilon_1}\right)^2 + \left(\frac{vy}{\epsilon_1}\right) + \frac{v^3}{\epsilon_1^2}.$$

Hence $y^2 + (\epsilon_1/v)y + v$ splits in K iff $s^2 + s + (v^3/\epsilon_1^2)$ splits in K iff we have $\mathrm{tr}_{K/F}(v^3/\epsilon_1^2) = 0$ iff $q(v) = 0$.

Now we use Equation 1 and Klapper's classification [7] which says, for this case,

1. $\mathrm{rad}\, q \neq 0$ iff $\epsilon_1^{-2} \in K^{*3}$ iff $\epsilon_1 \in K^{*3}$, in which case $\dim \mathrm{rad}\, q = 2$.

2. $q(\mathrm{rad}\, q) \neq 0$ iff k is odd.

3. If $\epsilon_1 \in K^{*3}$ and $k = 2m$ then

$$\Lambda(q) = \begin{cases} 1, & \text{if } m \text{ is odd} \\ -1, & \text{if } m \text{ is even.} \end{cases}$$

   If $\epsilon_1 \notin K^{*3}$ and $k = 2m$ then

$$\Lambda(q) = \begin{cases} 1, & \text{if } m \text{ is even} \\ -1, & \text{if } m \text{ is odd.} \end{cases}$$

The result now follows. □

Theorem 2.3. *The number of $R_{\bar{\varepsilon}}$ over K with $Q^K_{R_{\bar{\varepsilon}}}$ having a codimension 2 radical is*

$$\tfrac{1}{6}q(q-1)(q-2) = \binom{q}{3}.$$

For a fixed ϵ_1, ϵ_2, three have invariant $+1$, one has invariant -1 and the rest have invariant 0.

Proof: First note that there are q choices for ϵ_0, $q-1$ choices for the non-zero ϵ_1. We **Claim** that there are $S/3$ choices for ε_2. Fix $\varepsilon_1 \in K^*$. For each $v \in K^*$ such that $y^2 + (\varepsilon_1/v)y + v$ has roots in K, say $a(v)$ and $b(v)$, we get an $\varepsilon_2(v)$ via $\varepsilon_2(v) = a(v)^4 b(v) + a(v)b(v)^4$.

Let v_1, $a(v_1)$, $b(v_1)$ and $\varepsilon_2(v_1)$ be one choice. Note $a(v_1)b(v_1) = v_1$ and $a(v_1) + b(v_1) = \varepsilon_1/v$. Set $v_2 = a(v_1)(a(v_1) + b(v_1))$. Then

$$\frac{\varepsilon_1}{v_2} = \frac{1}{a(v_1)} \frac{\varepsilon_1}{a(v_1) + b(v_1)} = \frac{v_1}{a(v_1)} = b(v_1).$$

Hence $y^2 + (\varepsilon_1/v_2)y + v_2$ has roots $a(v_2) = a(v_1)$ and $b(v_2) = a(v_1) + b(v_1)$. So

$$\begin{aligned} \varepsilon_2(v_2) = a(v_1)^4(a(v_1) + b(v_1)) \quad &+ \quad a(v_1)(a(v_1) + b(v_1))^4 \\ &= \quad a(v_1)^4 b(v_1) + a(v_1)b(v_1)^4 = \varepsilon_2(v_1). \end{aligned}$$

Similarly, if $v_3 = (a(v_1) + b(v_1))b(v_1)$ then $\varepsilon_2(v_3) = \varepsilon_2(v_1)$ also. Hence there are at least three v's giving the same ε_2. And we have $\varepsilon_1 v^3 + \varepsilon_1^3 = \varepsilon_2 v^2$, by Lemma 1.2 (2), so there are exactly three v's giving the same ε_2. Thus the number of ε_2 is $S/3$, proving the **Claim**. The other ε_i are determined by Theorem 1.5.

This shows the number of $R_{\bar{\varepsilon}}$ is $q(q-1)S/3$. When k is odd, this is the desired formula, by Lemma 2.2. Now say $k = 2m$ is even. Then $|K^{*3}| = (q-1)/3$. So, again using Lemma 2.2, the number of $R_{\bar{\varepsilon}}$ is

$$\begin{aligned} q\frac{q-1}{3} \cdot \frac{1}{3}(2^{k-1} - (-1)^m 2^m - 1) \quad &+ \quad q\frac{2(q-1)}{3} \cdot \frac{1}{3}(2^{k-1} + (-1)^m 2^{m-1} - 1) \\ &= \quad \frac{q}{9}(2^k - 1)(2^k + 2^{k-1} - 3) \\ &= \quad \frac{q}{3}(2^k - 1)(2^{k-1} - 1) \\ &= \quad \frac{1}{6}q(q-1)(q-2). \end{aligned}$$

Lastly, fix ε_1 and ε_2. The invariant Λ is $+1$ iff $\varepsilon_0 = v$, by Theorem 1.5. We have previously shown there are three v's giving the same ε_2, so there are three ε_0's with $\Lambda(Q^K_{\bar{\varepsilon}}) = +1$. Again by Theorem 1.5, $\Lambda(Q^K_{\bar{\varepsilon}}) = -1$ iff $\varepsilon_0 = v + (\varepsilon_1/v)^2 = a(v)^2 + a(v)b(v) + b(v)^2$. The three choices for $(a(v), b(v))$ are $(a, b), (a, a+b), (a+b, b)$. In each case, $a(v)^2 + a(v)b(v) + b(v)^2$ is $a^2 + ab + b^2$. Thus there is only one ε_0 giving an invariant of -1. □

Example 2.4. Let $K = F_{2^6}$ with primitive element α, a root of $x^6 + x + 1$. Suppose $\varepsilon_1 = \alpha$, a non-cube. A simple computer search will show there are 9 possible ε_2's, in agreement with by Theorem 2.3. Then ε_3 can be computed, from the exceptional case of the Construction and

$$R_{\bar{\varepsilon}} = \varepsilon_0 x + \varepsilon_1 x^2 + \varepsilon_2 x^4 + \varepsilon_3 x^8.$$

The values are (recall that ε_3 is only defined modulo F_8):

ε_2	ε_3
$\alpha + \alpha^2$	$\alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$
$1 + \alpha^3 + \alpha^5$	$1 + \alpha + \alpha^4 + \alpha^5$
$\alpha^2 + \alpha^3 + \alpha^4$	$1 + \alpha^4 + \alpha^5$
$1 + \alpha^4$	$1 + \alpha$
$1 + \alpha^3 + \alpha^4$	$\alpha + \alpha^3 + \alpha^4$
$1 + \alpha^2 + \alpha^3 + \alpha^5$	$\alpha + \alpha^3 + \alpha^5$
$\alpha + \alpha^3 + \alpha^4$	$1 + \alpha^4 + \alpha^5$
α^3	$\alpha^2 + \alpha^4$
α^2	$\alpha + \alpha^4 + \alpha^5$.

We consider the fourth line, $\varepsilon_1 = \alpha$, $\varepsilon_2 = 1 + \alpha^4$ and $\varepsilon_3 = 1 + \alpha$, in more detail. There are three v's giving ε_2, namely,

$$1 + \alpha \quad \alpha^4 + \alpha^5 \quad \alpha + \alpha^3 + \alpha^4.$$

Then $\Lambda(Q^K_{\bar{\varepsilon}}) = +1$ iff ε_0 is any one of these v's. And $\Lambda(Q^K_{\bar{\varepsilon}}) = -1$ iff $\varepsilon_0 = v + (\alpha/v)^2 = 1 + \alpha^3 + \alpha^5$.

In total, there are $41,664$ quadratic forms on K with a codimension 2 radical. Of these, 651 have invariant -1, while 1953 have invariant $+1$ and the rest have invariant 0.

Example 2.5. Let $K = F_{2^7}$ with primitive element β, a root of $x^7 + x + 1$. Suppose $\varepsilon_1 = 1$. Again a simple computer search will show there are 21 possible ε_2's, in agreement with by Theorem 2.3. Then ε_3 can be computed from Theorem 1.5. We list the results, writing (i, j) for $\varepsilon_2 = \beta^i$ and $\varepsilon_3 = \beta^j$.

(21,3)	(37,96)	(41,24)	(42,6)	(47,2)	(55,58)	(59,83)
(61,8)	(74,65)	(82,48)	(84,12)	(87,1)	(91,29)	(93,105)
(94,4)	(107,64)	(109,78)	(110,116)	(117,32)	(118,39)	(122,16).

Example 2.6. Here we start with an ε_1 and ε_2 and then find fields K that allow this choice. Let $\varepsilon_1 = 1$ and $\varepsilon_2 = \gamma$ where $\gamma^3 = \gamma + 1$, so that $\varepsilon_2 \in F_{2^3}$. Then, as $x^3 + \gamma x^2 + 1$ is irreducible over F_{2^3} we have that $v \in F_{2^9}$. In fact, $v = \delta^7$ where δ is a root of $x^9 + x^4 + 1$. Now $x^2 + (1/v)x + v$ is irreducible

over F_{2^9}. Hence $a, b \in K = F_{2^{18}}$. The sequence of ε_i's is periodic with period 9:

$$1, \gamma, \gamma, \gamma^2 + 1, \gamma + 1, \gamma, \gamma^2, 1, 0.$$

Hence, if $\varepsilon_1 = 1$ and $\varepsilon_2 = \gamma$, $Q_{\bar{\varepsilon}}^K$ has codimension 2 radical iff $18|k$ and

$$R = \sum_{i=1}^{m} \varepsilon_i x^{2^i}.$$

Here $k = 2m$. Note that the top term ε_m is always 0 (recall that ε_m is taken modulo $GF(2^m)$).

3 Maximal Artin-Schreier curves

The Artin-Schreier curve we consider is:

$$C_{\bar{\varepsilon}} : y^2 + y = xR_{\bar{\varepsilon}}(x).$$

The number of points in K-projective space on $C_{\bar{\varepsilon}}$ is:

$$\#C_{\bar{\varepsilon}}(K) = 2^k + \Lambda(Q_{\bar{\varepsilon}}^K)\sqrt{2^{k+w}} + 1,$$

where $w = \dim \operatorname{rad}(Q_{\bar{\varepsilon}}^K)$. The Hasse-Weil bound is:

$$\#C_{\bar{\varepsilon}}(K) \leq 2^k + 2^\ell\sqrt{2^k} + 1,$$

where $2^\ell = \deg R_{\bar{\varepsilon}}$. Clearly equality will hold in the Hasse-Weil bound only if k is even.

Corollary 3.1. *Suppose $k = 2m$ and $\varepsilon_m \in F_{2^m}$, $\varepsilon_{m-1} \neq 0$. Then the number of points on $C_{\bar{\varepsilon}}$ equals the Hasse-Weil bound iff $Q_{\bar{\varepsilon}}^K$ has a radical of codimension 2 and $\Lambda(Q_{\bar{\varepsilon}}^K) = +1$.*

Proof: The conditions on ε_m and ε_{m-1} yield $\deg R_{\bar{\varepsilon}} = 2^{m-1}$, as ε_m is taken modulo F_{2^m}. Now match the two formulas above. $\square$

If $\varepsilon_m \notin F_{2^m}$ then $\deg R_{\bar{\varepsilon}} = 2^m$and the number of points on $C_{\bar{\varepsilon}}$ equals the Hasse-Weil bound only if $\dim \operatorname{rad}(Q_{\bar{\varepsilon}}^K) = k$, a vacuous case. There are examples of Artin-Schreier curves meeting the Hasse-Weil bound with $\varepsilon_m \in F_{2^m}$ and $\varepsilon_{m-1} = 0$, see [4].

The simplest way to find $R_{\bar{\varepsilon}}$ satisfying the conditions of Corollary 3.1 is to apply the Construction of Section 2 to $L := F_{2^m}$. Namely, choose $\varepsilon_1 \in L$ and find $v \in L$ such that $y^2 + (\varepsilon_1/v)y + v$ splits in L. Then compute ε_i as usual.

Corollary 3.2. *The Construction of Section 2 applied to L yields $R_{\bar{\varepsilon}}$ with $\varepsilon_m \in F_{2^m}$, $\varepsilon_{m-1} \neq 0$ and the radical of $Q_{\bar{\varepsilon}}^K$ having codimension 2. Taking $\varepsilon_0 = v$ gives $\Lambda(Q_{\bar{\varepsilon}}^K) = +1$ and so the number of points on $C_{\bar{\varepsilon}}$ equals the Hasse-Weil bound.*

Proof: Let $a, b \in L = F_{2^m}$ be the roots of $y^2 + (\varepsilon_1/v)y + v$. Ten $\varepsilon_m = A^{2^m} b \in L$. If $\varepsilon_{m-1} = 0$ then $a^{2^{m-1}} b = ab^{2^{m-1}}$. Squaring gives $a^{2^m} b^2 = a^2 b^{2^m}$. As $a, b \in L$, we get $ab^2 = a^2 b$ and $\varepsilon_1 = 0$, a contradiction. So $\varepsilon_{m-1} \neq 0$. The rest follows from Theorem 1.5 and Corollary 3.1. $\square$

There are other examples of $R_{\bar{\varepsilon}}$ that satisfy the conditions of Corollary 3.1.

Example 3.3. Suppose $k = 6$. If $\varepsilon_3 = a^8 b$ is in $L = F_8$ then $\varepsilon_3 = \varepsilon_3^8 = ab^8$. So $a^8 b + ab^8 = 0$. Now $a^8 b + ab^8$ is the usual formula for ε_3 (that is, in all cases except $k = 6$) so the formulas of Proposition 1.6 hold. We get $\varepsilon_2^3 + \varepsilon_1^5 = 0$. Hence ε_1 must be a cube.

Conversely, suppose $\varepsilon_1 = \eta^3$ for some $\eta \in K$. Note that if ω is a primitive cube root of unity in K then $\varepsilon_1 = (\eta\omega)^3$ also. Now let β be a root of $x^3 + x^2 + 1$; note $\beta \in L$. Set $v = \beta\eta^2$. Then $\mathrm{tr}_{K/F}(v^3/\varepsilon_1^2) = \mathrm{tr}_{K/F}(\beta^3) = 0$ as $\beta \in L$. So $y^2 + (\varepsilon_1/v)y + v$ splits in K. Following the construction of Section 2, set

$$\varepsilon_2 = \varepsilon_1(v + (\varepsilon_1/v)^2) = \varepsilon_1(\beta\eta^2 + (\eta/\beta)^2) = \eta^5(\beta + 1/\beta^2) = \eta^5.$$

So $\varepsilon_2^3 + \varepsilon_1^5 = 0$, $a^8 b = ab^8$ and $\varepsilon_3 = a^8 b \in L$.

There are three choices for η and so three choices for ε_2. Given ε_1 and ε_2, there are three choices for ε_0 yielding $\Lambda(Q_{\bar{\varepsilon}}^K) = +1$, by Theorem 2.3. Hence when ε_1 is a cube there are exactly nine $R_{\bar{\varepsilon}}$ satisfying the conditions of Corollary 3.1. When ε_1 is not a cube there are none. So the number of $R_{\bar{\varepsilon}}$ with $\varepsilon_3 \in L$, $\varepsilon_2 \neq 0$, $Q_{\bar{\varepsilon}}^K$ having a codimension 2 radical and $\Lambda(Q_{\bar{\varepsilon}}^K) = +1$ is

$$9 \cdot \frac{2^6 - 1}{3} = 3(2^6 - 1) = 189.$$

Example 3.4. Let $k = 8$. Suppose $\varepsilon_4 = a^{16} b \in L = F_{16}$. As in the previous example, the usual formula for ε_4:

$$\varepsilon_4 = \frac{\varepsilon_2}{\varepsilon_1^6}(\varepsilon_2^6 + \varepsilon_1^5\varepsilon_2^3 + \varepsilon_1^{10})$$

must be 0. So either $\varepsilon_2 = 0$ or $\varepsilon_2^3 = \varepsilon_1^5\omega$, where ω is a root of $x^2 + x + 1$. Note that $\omega \in K$ but $\omega \notin K^{*3}$ as 9 does not divide $2^8 - 1 = 255$. Now if

$\varepsilon_2 = 0$ then $\varepsilon_1 v^3 + \varepsilon_1^3 = 0$ and ε_1^3 is a cube (equivalently, ε_1 is a cube, as the order of ε_1 is odd). If $\varepsilon_2^3 = \varepsilon_1^5\omega$ then ε_1^2 is not a cube, as ω is not. We check the converse.

First say $\varepsilon_1 = \eta^3$ for some $\eta \in K$. We follow the Construction of Section 2. Set $v = \eta^2$. Then $y^2 + (\varepsilon_1/v)y + v$ has roots $\eta\omega, \eta\omega^2$ and so splits in K. Then $\varepsilon_2 = \varepsilon_1(v + (\varepsilon_1/v)^2) = 0$. By Proposition 1.6 $\varepsilon_3 = \varepsilon_1^{11} \neq 0$ and $\varepsilon_4 = (\eta\omega)^{16}(\eta\omega^2) = \eta^{17} \in F_{16}$ as $(\eta^{17})^{15} = 1$.

Next say ε_1^2 is not a cube. Then ε_1^2 is in the same coset of K^{*3} as either ω or ω^2. We may assume $\varepsilon_1^2\omega = \mu^3$, for some $\mu \in K$. Now set $v = \mu\omega^2$. Then $\mathrm{tr}_{K/F}(v^3/\varepsilon_1^2) = \mathrm{tr}_{K/F}(\omega) = 0$ as $\omega \in F_4$. So $y^2 + (\varepsilon_1/v)y + v$ splits in K. Following the Construction, set $\varepsilon_2 = \varepsilon_1(v + (\varepsilon_1/v)^2) = \varepsilon_1\mu$. So $\varepsilon_2^3 = \varepsilon_1^3\mu^3 = \varepsilon_1^5\omega$. Hence $\varepsilon_4 \in F_{16}$. Lastly,

$$\varepsilon_3 = \frac{1}{\varepsilon_1^2}(\varepsilon_2^3 + \varepsilon_1^5) = \frac{1}{\varepsilon_1^2}(\varepsilon_1^5\omega + \varepsilon_1^5) = \varepsilon_1^2(\omega + 1) = \varepsilon_1^2\omega^2 \neq 0,$$

as desired.

Thus for each cube ε_1 there is exactly one choice for ε_2, namely $\varepsilon_2 = 0$. For each non-cube ε_1 there are three choices for ε_2, since there are three choices for μ. And, as before, given $\varepsilon_1, \varepsilon_2$ there are three choices for ε_0 to get $\Lambda(Q_{\bar{\varepsilon}}^K) = +1$. Hence the number of $R_{\bar{\varepsilon}}$ with $\varepsilon_4 \in F_{16}, \varepsilon_3 \neq 0$, $Q_{\bar{\varepsilon}}^K$ having a radical of codimension 2 and $\Lambda(Q_{\bar{\varepsilon}}^K) = +1$ is:

$$3 \cdot \frac{2^8 - 1}{3} + 9 \cdot \frac{2(2^8 - 1)}{3} = 7(2^8 - 1) = 1785.$$

These then are the maximal Artin-Schreier curves over $K = F_{2^8}$.

Additional computations suggest that each case behaves like one of the two examples above and that the number of $R_{\bar{\varepsilon}}$ that satisfy the conditions of Corollary 3.1 is:

$$\begin{cases} 3(q-1), & \text{if } m \text{ is odd} \\ 7(q-1), & \text{if } m \text{ is even.} \end{cases}$$

But we are unable to show this.

Lastly, [9] deserves a comment since it has results that appear similar to ours. There is, in fact, little overlap. Equation (2) here is a special case ($w = m-2$) of Equation (7) in [9]. But the concerns are different. In [9] they seek only to determine the degree of $R(x)$ while we seek to determine the coefficients. When the codimension 2 radical case is considered in [9], they obtain either no information on the coefficients (Section 4, I) or information only on the top coefficient (Section 5, I).

[9] also constructs curves that attain the Hasse-Weil bound but they are fibre products of Artin-Schreier curves, rather than the single curves considered here. Taking $r = 1$ in [9] Proposition 5.2 (ii) does prove the existence of one Artin-Schreier curve attaining the Hasse-Weil bound. In this section, we found many maximal Artin-Schreier curves (Corollary 3.2) and have suggested a method to find all of them.

References

[1] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

[2] P. Delsarte and J.-M. Goethals, Irreducible binary codes of even dimension, in: 1970 Proc. Second Chapel Hill Conference on Combinatorial Mathematics and Its Applications, Univ. North Carolina, Chapel Hill, NC, 1970, pp. 100–113.

[3] C. Ding, A. Salomaa, P. Solé and X. Tian, Three constructions of authentication/secrecy codes, in: M. Fossorier, T. Høholdt, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Toulouse, 2003), Lecture Notes in Computer Science, vol. 2643, Springer-Verlag, Berlin, 2003, pp. 24–33.

[4] R. Fitzgerald, Highly degenerate quadratic forms over finite fields of characteristic 2, Finite Fields and Their Applications 11 (2005) 165–181.

[5] R. Fitzgerald and J. Yucas, Pencils of quadratic forms over GF(2) Discrete Math. 283 (2004) 71–79.

[6] K. Khoo, G. Gong and D. R. Stinson, New family of Gold-like sequences, in: IEEE International Symposium on Information Theory 02, 2002, p. 181.

[7] A. Klapper, Cross-correlation of geometric series in characteristic two, Des., Codes, and Cryptogr. 3 (1993) 347–377.

[8] R. Lidl and H. Niederreiter, Finite Fields (second edition), Encyclopedia of Mathematics and Its Applications, vol 20, Cambridge University Press, Cambridge, 1997.

[9] G. van der Geer and M. van der Vlugt, Quadratic forms, generalized Hamming weights of codes and curves with many points, J. Number Theory 59 (1996) 20–36.

Department of Mathematics, Southern Illinois University, Carbondale, IL 62901, Email: rfitzg@math.siu.edu