2005

Highly Degenerate Quadratic Forms over Finite Fields of Characteristic 2

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

Published in *Finite Fields and Their Applications*, 11, 165-181.

HIGHLY DEGENERATE QUADRATIC FORMS OVER FINITE FIELDS OF CHARACTERISTIC 2

Robert W. Fitzgerald

Southern Illinois University

Abstract. Let K/F be an extension of finite fields of characteristic two. We consider quadratic forms written as the trace of $xR(x)$, where $R(x)$ is a linearized polynomial. We show all quadratic forms can be so written, in an essentially unique way. We classify those R, with coefficients 0 or 1, where the form has a codimension 2 radical. This is applied to maximal Artin-Schreier curves and factorizations of linearized polynomials.

Let q be a 2-power, $q = 2^t$. Set $F = GF(q)$ and let $K = GF(q^k)$ be an extension. Let

$$R(x) = \sum_{j=0}^{h} \epsilon_j x^{q^j},$$

with each $\epsilon_j \in K$. We consider the quadratic forms $Q_R^K : K \to F$ given by $Q_R^K(x) = tr_{K/F}(xR(x))$.

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 [8], as part of an authentication scheme [3], and to construct certain binary sequences in [5] and [4].

In each of these applications one wants the number of solutions (in K) to $Q_R^K(x) = 0$, denoted by $N(Q_R^K)$. This is easily worked out (see [7, 6.26,6.32]) in terms of the standard classification of quadratic forms:

$$N(Q_R^K) = \tfrac{1}{q}(q^k + \Lambda(Q_R^K)(q-1)\sqrt{q^{k+w}}).$$

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

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

Here s is any element of F with $\mathrm{tr}_{F/GF(2)}(s) = 1$.

Key words and phrases. quadratic form, trace, linearized polynomial.

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 [6] which only covers the case when R consists of a single term. In roughly half the applications ([1,2,8]) one wants highly degenerate forms, which give large $N(Q_R^K)$ when $\Lambda = 1$. We restrict to those R with all coefficients $\epsilon_i \in GF(2)$ as is the case in each of the cited papers except [8]. Our main result is to determine all such R, and all extensions K, such that the radical of Q_R^K has codimension (namely $2v$) at most 2. We compute the invariant Λ in each case.

We first show that every quadratic form $Q : K \to F$ can be written as Q_R^K in an essentially unique way. Thus our result is more general than it appears. We apply our main result to obtain a classification of those R such that the number of points on the Artin-Schreier curve $y^q + y = xR(x)$ equals the Hasse-Weil bound. We also obtain results on the factors of self-reciprocal linearized polynomials.

1. Quadratic forms.

A *quadratic form* $Q : K \to F$ is a map such that

(1) $Q(ax) = a^2Q(x)$ for all $a \in F$ and $x \in K$, and
(2) $B(x, y) :\equiv Q(x + y) + Q(x) + Q(y)$ is a bilinear map $K \times K \to F$.

The radical of Q is

$$\operatorname{rad} Q = \{x \in K : B(x, y) = 0 \quad \text{for all } y \in K\}.$$

The codimension of the radical, $k - \dim \operatorname{rad} Q$ is always even.

To simplify notation, we write simply tr for $\mathrm{tr}_{K/F}$. We will write Tr_K for the absolute trace $\mathrm{tr}_{K/GF(2)}$.

Proposition 1.1. *Let $Q : K \to F$ be a quadratic form. Let $m = \lfloor k/2 \rfloor$. Let $h = \frac{1}{2}$codim rad$Q$.*

(1) *There exist $c, a_1, b_1, \dots, a_h, b_h \in K$, independent over F, such that*

$$Q(x) = \begin{cases} tr(cx)^2 + \sum_{i=1}^h tr(a_ix)tr(b_ix), & \text{if } \Lambda(Q) = 0 \\ \sum_{i=1}^h tr(a_ix)tr(b_ix), & \text{if } \Lambda(Q) = 1 \\ tr(a_1x)^2 + tr(b_1x)^2 + \sum_{i=1}^h tr(a_ix)tr(b_ix), & \text{if } \Lambda(Q) = -1. \end{cases}$$

(2) *There exist $\epsilon_0, \epsilon_1, \dots, \epsilon_m \in K$ such that*

$$Q(x) = tr\left(x \cdot \sum_{i=0}^m \epsilon_i x^{q^i}\right).$$

Proof. (1) Suppose $\Lambda(Q) = 1$. Pick a basis of K over F and let M be the matrix of Q with respect to this basis. We apply the classification of quadratic forms. Let $H = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and let N be the $k \times k$ matrix with h copies of H on the diagonal and the rest zero. Then there exists an invertible $k \times k$ matrix P over F such that

$$\begin{aligned} M &= P^t N P \\ Q(X) &= X^t P^t N P X \\ Q(X) &= \sum_{i=1}^{h} (r_{2i-1}X)(r_{2i}X), \end{aligned}$$

where r_j is the jth row of P. As map from $K \to F$, rather than from $F^k \to F$, each r_jX is linear and so equal to $\mathrm{tr}(d_jx)$ for some $d_j \in K$. The rows of P are independent over F so the d_j are also. This gives the desired representation of Q.

The cases when $\Lambda(Q) = 0$ or -1 are similar except the first copy of H in N is replaced by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

respectively.

(2)This proof is taken from [9,3.2, 5.1]. Our only change is to correct a slight error in the $i = 1$ term and to include the cases of $\Lambda(Q) = 0, -1$.

$$\begin{aligned} \mathrm{tr}(ax)\mathrm{tr}(bx) &= \mathrm{tr}(\mathrm{tr}(ax)bx) \\ &= \mathrm{tr}\left(\sum_{i=0}^{k-1} (ax)^{q^i} (bx) \right). \end{aligned}$$

Now

$$\mathrm{tr}(a^{q^i} b) = \mathrm{tr}(a b^{q^{k-i}})$$

so that

$$\mathrm{tr}(ax)\mathrm{tr}(bx) = \begin{cases} \mathrm{tr}(abx^2 + \sum_{i=1}^{m} (a^{q^i} b + a b^{q^i}) x^{q^i}), & \text{if } k = 2m+1 \text{ is odd} \\ \mathrm{tr}(abx^2 + \sum_{i=1}^{m} (a^{q^i} b + a b^{q^i}) x^{q^i} + a^{q^m} b x^{q^m}), & \text{if } k = 2m \text{ is even.} \end{cases}$$

In either case,

$$\mathrm{tr}(ax)\mathrm{tr}(bx) = \mathrm{tr}\left(x \cdot \sum_{j=0}^{m} \epsilon'_j x^{q^i+1} \right),$$

for some $\epsilon'_j \in K$. Lastly,

$$\mathrm{tr}(cx)^2 = \mathrm{tr}((cx)^2) = \mathrm{tr}(x \cdot c^2 x).$$

Thus (1) implies (2). $\square$

The first representation of (1.1) is not unique. For instance,

$$\mathrm{tr}(ax)^2 + \mathrm{tr}(ax)\mathrm{tr}(bx) + \mathrm{tr}(bx)^2 = \mathrm{tr}(ax)^2 + \mathrm{tr}(ax)\mathrm{tr}((a+b)x) + \mathrm{tr}((a+b)x)^2.$$

However, for the second representation we have:

Theorem 1.2. *Let $Q : K \to F$ be a quadratic form and let $m = \lfloor k/2 \rfloor$. Then there exist unique $\epsilon_i \in K$, $0 \le i \le m$, such that*

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

except when k is even in which case ϵ_m is only unique modulo $GF(q^m)$.

Proof. We count. If we fix a basis of K over F then each quadratic form is represented uniquely by an upper triangular matrix. Hence there are $q^{k(k+1)/2}$ many quadratic forms.

Suppose $k = 2m+1$. The number of $R(x) = \sum_{i=0}^{m} \epsilon_m x^{q^i}$ is $(q^k)^{m+1} = q^{k(k+1)/2}$. Since this is the number of quadratic forms, (1.1) implies the representation $Q(x) = \mathrm{tr}(xR(x))$ is unique.

Suppose $k = 2m$. Note that

$$(x^{q^m+1})^{q^m-1} = x^{q^k-1} \in GF(2^m)$$

for all $x \in K$. Thus if $\epsilon \in GF(q^m)$ then $\mathrm{tr}(x \cdot \epsilon x^{q^m}) = 0$ for all $x \in K$. The number of $R(x) = \sum_{i=0}^{m} \epsilon_i x^{q^i}$, with $\epsilon_0, \ldots, \epsilon_{m-1} \in K$ and $\epsilon_m \in K/GF(q^m)$ is

$$(q^k)^m \cdot (q^m) = q^{2m^2+m} = q^{k(k+1)/2}.$$

As before, this shows the representation of $Q(x)$ as $\mathrm{tr}(xR(x))$ is unique (taking ϵ_m modulo $GF(q^m)$). □

Throughout the remainder of the paper we assume

$$R(x) = \sum_{j=0}^{h} \epsilon_j x^{q^j} \qquad \text{with } \epsilon_j \in GF(2),$$

where $h = \lfloor (k-1)/2 \rfloor$. Here we have dropped the ϵ_m term when $k = 2m$ as $\epsilon_m = 0$ or 1, both of which are in $GF(2^m)$.

Corollary 1.3. *Let $R = \sum_{i=0}^{h} \epsilon_i x^{q^i}$, where each $\epsilon_i \in GF(2)$ and $h = \lfloor (k-1)/2 \rfloor$. Then Q_R^K has radical of codimension 2 iff there exist independent $a, b, c \in K$ such that*

$$\text{(Ei)} \qquad a^{q^i} b + a b^{q^i} = \epsilon_i \quad \textit{for } 1 \le i \le h$$

and

$$\text{(E0)} \qquad \epsilon_0 = \begin{cases} c^2 + ab, & \textit{if } \Lambda(Q_R^K) = 0 \\ ab, & \textit{if } \Lambda(Q_R^K) = 1 \\ a^2 + ab + sb^2, & \textit{if } \Lambda(Q_R^K) = -1, \end{cases}$$

plus, if $k = 2m$,

$$\text{(Em)} \qquad a^{q^m} b \in GF(q^m).$$

Again here $s \in F$ is an element with $Tr_F(s) = 1$.

Proof. We have by (1.1)(1) that the quadratic forms with radical of codimension 2 are

$$\mathrm{tr}(cx)^2 + \mathrm{tr}(ax)\mathrm{tr}(bx) \quad \mathrm{tr}(ax)\mathrm{tr}(bx) \quad \mathrm{tr}(ax)^2 + \mathrm{tr}(ax)\mathrm{tr}(bx) + s\mathrm{tr}(bx)^2,$$

where the invariants are $0, 1, -1$ respectively (see [9, 3.1]). The computation of $\mathrm{tr}(ax)\mathrm{tr}(bx)$ in (1.1)(2) gives the equations (Ei) for $1 \le i \le h$. (Em) follows as

$$\mathrm{tr}(a^{q^m} b x^{q^m+1}) = 0 \quad \text{iff} \quad a^{q^m} b \in GF(q^m),$$

by (1.2). And $\mathrm{tr}(cx)^2 = \mathrm{tr}((cx)^2) = \mathrm{tr}(c^2 x \cdot x)$ yields the three forms of (E0). $\square$

2. The Main Theorem.

We begin with three lemmas needed to solve the equations (Ei).

Lemma 2.1. *Suppose $y^2 = y + z$. Then*

$$y^{2^i} = y + z + z^2 + z^4 + \cdots + z^{2^{i-1}}.$$

Proof. Induction. $\square$

The following identity is well-known and may be derived in many ways. For instance, one may take Waring's identity, expressing the sum of two nth powers in terms of a Dickson polynomial, modulo 2. We use instead a simple induction argument.

Lemma 2.2. *Let $u = x + y$ and $v = xy$. Then*

$$x^{2^n+1} + y^{2^n+1} = u^{2^n+1} + \sum_{i=0}^{n-1} u^{2^n+1-2^{i-1}} v^{2^i}.$$

Proof. By induction,

$$\begin{aligned} x^{2^{n+1}+1} + y^{2^{n+1}+1} &= (x^{2^n} + y^{2^n})(x^{2^n+1} + y^{2^n+1}) + x^{2^n} y^{2^n+1} + x^{2^n+1} y^{2^n} \\ &= u^{2^n}(u^{2^n+1} + \sum_{i=0}^{n-1} u^{2^n+1-2^{i-1}} v^{2^i}) + uv^{2^n} \\ &= u^{2^{n+1}+1} + \sum_{i=0}^{n} u^{2^{n+1}+1-2^{i-1}} v^{2^i}, \end{aligned}$$

as desired. $\square$

The following highly technical lemma is need to compute the invariant Λ in one case.

Lemma 2.3. *Let $v = 2^{3^r}$ and let*

$$g_v(x) = x^{v+1}(1 + x^{-2} + x^{-4} + \cdots + x^{-v}) + 1.$$

Let δ be a root of $g_v(x)$ in some extension of F. Then

(1) $\delta \in GF(v^3) \setminus GF(v)$
(2) $\delta^{2v} + \delta^{v+1} + \delta^2 = 1$
(3) $\delta^{v^2+1} + \delta^{2v} = 1$
(4) $\delta^2 + \delta^{v^2+v} = 1$.

Proof. We have

$$1 + \delta^{-2} + \delta^{-4} + \cdots + \delta^{-v} = \delta^{-(v+1)}.$$

Add this to its square to get

$$\delta^{-2} + \delta^{-2v} = \delta^{-(v+1)} + \delta^{-2(v+1)}.$$

Multiply by $\delta^{2(v+1)}$ to get (2).

Re-write (2) by dividing by δ^2

$$\delta^{2(v-1)} + \delta^{v-1} + (1 + \delta^{-2}) = 0. \tag{5}$$

This has the form $y^2 + y + z = 0$ with $y = \delta^{v-1}$ and $z = 1 + \delta^{-2}$. By (1.4)

$$\delta^{(v-1)v} = \delta^{v-1} + z + z^2 + \cdots + z^{v/2}.$$

As v is an odd power of 2 there are an odd number of z^i terms. So

$$\begin{aligned}\delta^{(v-1)v} &= \delta^{v-1} + 1 + \delta^{-2} + \delta^{-4} + \cdots + \delta^{-v} \\ &= \delta^{v-1} + \delta^{-(v+1)},\end{aligned}$$

by the original equation. Then

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

giving (3).

Now multiply (5) by δ^{v-1} to get

$$\begin{aligned}\delta^{3(v-1)} &= \delta^{2(v-1)} + \delta^{v-1} + \delta^{v-3} \\ &= 1 + \delta^{-2} + \delta^{v-3},\end{aligned}$$

using (5). Multiply by δ^{v+3} to get $\delta^{4v} = \delta^{v+3} + \delta^{v+1} + \delta^{2v}$. Apply (2), divide by δ^2 and apply (2) again:

$$\delta^{4v} + \delta^{v+3} = \delta^2 + 1$$
$$\delta^{4v-2} + \delta^{v+1} = 1 + \delta^{-2}$$
$$\delta^{4v-2} + \delta^{-2} = \delta^{2v} + \delta^2. \tag{6}$$

Next divide (3) by δ

$$\delta^{v^2} + \delta^{2v-1} = \delta^{-1}. \tag{7}$$

Square (7) and apply (6)

$$\begin{aligned} \delta^{2v^2} + \delta^{4v-2} &= \delta^{-2} \\ \delta^{2v^2} &= \delta^{2v} + \delta^2. \end{aligned} \tag{8}$$

Now raise (7) to the vth power

$$\begin{aligned} \delta^{v^3} &= \delta^{2v^2-v} + \delta^{-v} \\ &= \delta^{-v}(\delta^{2v^2} + 1) \\ &= \delta^{-v}(\delta^{2v} + \delta^2 + 1) \quad \text{by (8)} \\ &= \delta^{-v}\delta^{v+1} = \delta, \end{aligned}$$

using (2). Hence $\delta \in GF(v^3)$, giving (1). If $\delta \in GF(v)$ then $\delta^{v^2+1} = \delta^2$ and $\delta^{2v} = \delta^2$ also which contradicts (3). Thus $\delta \notin GF(v)$.

Lastly, re-write (3)

$$1 = \delta^{v^2+1} + \delta^{2v} = \delta^{v^3+v^2} + \delta^{2v} = (\delta^{v^2+v} + \delta^2)^v.$$

Hence $\delta^{v^2+v} + \delta^2 = 1$, giving (4). $\square$

Set

$$Ad(x) = \sum_{\substack{j=1 \\ d\nmid j}}^{h} x^{q^j}$$

Theorem 2.4. *Let $R = \sum_{i=0}^{h} \epsilon_i x^{q^i}$, where each $\epsilon_i \in GF(2)$ and $h = \lfloor (k-1)/2 \rfloor$. Then Q_R^K has radical of codimension 2 iff*

(1) *$3|k$ and $R = A3$ or $x + A3$, or*
(2) *$4|k$ and $R = A2$ or $x + A2$.*

The classification in these cases (assuming the restriction on k) is

$$\begin{aligned} \Lambda(Q_{A2}^K) &= -1 \\ \Lambda(Q_{x+A2}^K) &= \begin{cases} 1, & \text{if } t \text{ is odd} \\ -1, & \text{if } t \text{ is even} \end{cases} \\ \Lambda(Q_{A3}^K) &= 0 \\ \lambda(Q_{x+A3}^K) &= \begin{cases} 1, & \text{if } t \text{ is even} \\ -1, & \text{if } t \text{ is odd.} \end{cases} \end{aligned}$$

Recall that $q = 2^t$.

Proof. In the first half of the proof we find all extensions K, all independent $a, b, c \in K$, and all ϵ_i, $i \geq 1$, that satisfy the equations (Ei), for $i \geq 1$, and (Em). We will see that R must be $A2, x + A2, A3$ or $x + A3$ with the desired restrictions on k.

Set $u = a^{q-1} + b^{q-1}$ and $v = ab$. Then (E1) is $uv = \epsilon_1$. If $\epsilon_1 = 0$ then either $a = 0$, $b = 0$ or $a^{q-1} = b^{q-1}$ (and so $a = \lambda b$ for some $\lambda \in F$), contradicting the independence of a, b over F. Thus $\epsilon_1 = 1$ and $u = 1/v$.

Now (E2) is

$$ab((a^{q-1})^{q+1} + (b^{q-1})^{q+1}) = \epsilon_2$$
$$v\left[u^{q+1} + \sum_{i=0}^{t-1} u^{q+1-2^{i+1}}(v^{q-1})^{2^i}\right] = \epsilon_2,$$

using (2.2). Replacing u by $1/v$ and multiplying by v^q yields

$$\sum_{i=0}^{t-1} v^{2^i(q+1)} = \epsilon_2 v^q. \tag{2.5}$$

We first treat the case of $\epsilon_2 = 0$. Set $w = v^{q+1}$. Then, by (2.5), $w^{q/2} + \cdots + w + 1 = 0$. Hence $w^q = w, w \in F$ and $Tr_F(w) = 1$.

Now the $(q+1)$st roots of $w \in F$ lie in $L = GF(q^2)$ since if z generates $GF(q^2)^*$ then z^{q+1} generates $GF(q)^*$. Thus $v = ab \in L$. As $\epsilon_2 = 0$ we have $(a/b)^{q^2-1} = 1$ and so $a/b \in L$ also. Thus $a, b \in L$. Now if $a, b \in F$ then they are dependent over F. Hence at least one of a, b is in $L \setminus F$. Say $a \in L \setminus F$. So if $a \in K$ then $2|k$.

By construction, $\epsilon_1 = 1$ and $\epsilon_2 = 0$. As $a \in L$ we have

$$a^{q^i} = \begin{cases} a, & \text{if } i \text{ is even} \\ a^q, & \text{if } i \text{ is odd,} \end{cases}$$

and similarly for b. Hence for $i \geq 3$

$$\epsilon_i = a^{q^i}b + ab^{q^i} = \begin{cases} \epsilon_1, & \text{if } i \text{ is odd} \\ \epsilon_2, & \text{if } i \text{ is even.} \end{cases}$$

Thus $R = A2$ or $x + A2$.

Lastly, we know $k = 2m$ is even so we check (Em). If m is odd then

$$a^{q^m}b = a^q b = a^{q-1}v = a^{q-1}/u \in L \setminus F,$$

so that $a^{q^m}b \notin GF(q^m)$. And if m is even then $a^{q^m}b = ab \in GF(q^2) \subset GF(q^m)$. Thus to have a solution in K we require that m be even, that is, that $4|k$.

We now treat the case of $\epsilon_2 = 1$. From (2.5) we have:

$$v^{(q+1)q/2} + v^{(q+1)q/4} + \cdots v^{q+1} + 1 = v^q.$$

Squaring this gives

$$\begin{aligned} v^{(q+1)q} &= v^{(q+1)q/2} + \cdots + v^{(q+1)2} + 1 + v^{2q} \\ &= v^{q+1} + v^q + v^{2q}, \end{aligned} \tag{2.6}$$

by (2.5). Divide this by v^q and then raise to the qth power:

$$\begin{aligned} v^{q^2} &= 1 + v + v^q \\ v^{q^3} &= 1 + v^q + v^{q^2} = v. \end{aligned} \tag{2.7}$$

Thus $v \in E \equiv GF(q^3)$ and $\mathrm{tr}_{E/F}(v) = 1$.

Now $va^{q-1} = a^q b$ and $vb^{q-1} = ab^q$ sum to 1 and their product is $a^{q+1}b^{q+1} = v^{q+1}$. Thus va^{q-1} and vb^{q-1} are roots of $y^2 + y + v^{q+1} \in E[y]$. Now

$$\begin{aligned} \mathrm{Tr}_E(v^{q+1}) &= \sum_{i=0}^{t-1} v^{2^i(q+1)} + \sum_{i=0}^{t-1} v^{2^i(q+1)q} + \sum_{i=0}^{t-1} v^{2^i(q+1)q^2} \\ &= (1+v^q) + (1+v^q)^q + (1+v^q)^{q^2} \quad \text{by (2.5)} \\ &= 1 + v^q + v^{q^2} + v^{q^3} = 0, \end{aligned}$$

by (2.7). Thus $y^2 + y + v^{q+1}$ has its roots in E, by [7, 3.79]. So a^{q-1} and b^{q-1} are in E.

Next, by (2.1)

$$\begin{aligned} y^q &= y + v^{q+1} + v^{2(q+1)} + \cdots + v^{(q+1)q/2} \\ y^q &= y + 1 + v^q \qquad \text{by (2.5)} \\ y^{q^2} &= y + v^q + v^{q^2} \\ y^{q^2+q} &= y^2 + +y(1+v^{q^2}) + v^q + v^{q^2} + v^{2q} + v^{q^2+q} \\ &= yv^{q^2} + v^{q^2} \qquad \text{by (2.7)} \\ y^{q^2+q+1} &= yv^{q^2} + v^{q^2+q+1} + yv^{q^2} = v^{q^2+q+1}. \end{aligned}$$

Hence, dividing by v^{q^2+q+1} yields $a^{q^3-1} = 1 = b^{q^3-1}$. Thus $a, b \in E$. In particular,

$$\epsilon_3 = a^{q^3}b + ab^{q^3} = ab + ab = 0.$$

By construction $\epsilon_1 = 1 = \epsilon_2$. And

$$a^{q^i} = \begin{cases} a, & \text{if } i \equiv 0 \pmod 3 \\ a^q, & \text{if } i \equiv 1 \pmod 3 \\ a^{q^2}, & \text{if } i \equiv 2 \pmod 3). \end{cases}$$

Thus for $i \geq 3$, $\epsilon_i = \epsilon_j$ where $j \in \{1, 2, 3\}$ and $i \equiv j \pmod 3$. Hence $R = A3$ or $x + A3$.

Again, if $a,b\in F$ then they are dependent over F. Hence at least one of a,b is in $E\setminus F$. Say $a\in E\setminus F$. So if $a\in K$ then $3|k$. Finally, if $k=2m$ is even we must check (Em). But $a^{q^m}b\in E=GF(q^3)\subset GF(q^m)$, as $3|k$, so (Em) is satisfied. This completes the first half of the proof.

In the second half of the proof we show that each of $R=A2, x+A2, A3$ and $x+A3$ does give a quadratic form with radical of codimension 2 (assuming the restrictions on k) and compute their invariants. We do this by finding explicit solutions to the equations (Ei). There are six cases.

First consider Q^K_{A2} when $4|k$. Fix an $s\in F$ with $\mathrm{Tr}_F(s)=1$. Then $y^2+y+s\in F[y]$ is irreducible. Let $\alpha\in GF(q^2)\subset K$ be a root. Let β be a primitive element of $GF(q^2)$. Set $b=\beta^{q-1}$ and $a=\alpha b$. These are independent over F as $\alpha\notin F$. We compute

$$\text{(E0)}\qquad a^2+ab+sb^2=b^2((a/b)^2+(a/b)+s)=0$$

$$\text{(E1)}\qquad a^qb+ab^q=(\alpha^q+\alpha)b^{q+1}=\mathrm{Tr}_F(s)\delta^{q^2-1}=1$$

$$\text{(E2)}\qquad a^{q^2}b+ab^{q^2}=ab+ab=0.$$

Also $ab\in GF(q^2)$ implies $\epsilon_{i+2}=\epsilon_i$ for $i\geq 1$. If $k=2m$ then $a^{q^m}b\in GF(q^2)\subset GF(q^m)$ as m is even, so that (Em) is satisfied. Hence

$$\mathrm{tr}(ax)^2+\mathrm{tr}(ax)\mathrm{tr}(bx)+s\mathrm{tr}(bx)^2=Q^K_{A2}(x).$$

By (1.3) Q^K_{A2} has radical with codimension 2 and invariant -1.

Next consider Q^K_{x+A2} when $4|k$ and $q=2^t$ with t odd. Let $\beta\in GF(q^2)\subset K$ be primitive. As t is odd, $3|(q+1)$. Set

$$a=\beta^{(q-2)(q+1)}\beta^{(q+1)/3}\qquad b=\beta^{2(q+1)/3}.$$

Note that a and b are independent over F as $(b/a)^{q-1}=\beta^{(q^2-1)/3}\neq 1$ so that $b/a\notin F$. We compute

$$\text{(E0)}\qquad ab=\beta^{(q-2)(q+1)}\beta^{q+1}=\beta^{q^2-1}=1$$

$$\text{(E1)}\qquad a^qb+ab^q=a^{q-1}+b^{q-1}=\beta^{(q^2-1)/3}+\beta^{2(q^2-1)/3}=1$$

$$\text{(E2)}\qquad a^{q^2}b+ab^{q^2}=ab+ab=0.$$

As in the previous case $\epsilon_{i+2}=\epsilon_i$ for $i\geq 1$ and (Em) is satisfied. Hence $\mathrm{tr}(ax)\mathrm{tr}(bx)=Q^K_{x+A2}(x)$ is, by (1.3), a form of codimension 2 radical and invariant 1.

Next consider Q^K_{x+A2} when $4|k$ and t even. Fix $s\in F$ with $\mathrm{Tr}_F(s)=1$. Then $\mathrm{Tr}_F(s+1)=\mathrm{Tr}_F(s)=1$ as t is even. Thus $x^2+x+s+1$ is irreducible over F. Let $\alpha\in GF(q^2)\subset K$ be a root. Set $a=\alpha$ and $b=1$; they are independent over F as $\alpha\notin F$. Then

$$\text{(E0)}\qquad a^2+ab+sb^2=\alpha^2+\alpha+s=1$$

$$\text{(E1)}\qquad a^qb+ab^q=\alpha^q+\alpha=\mathrm{Tr}_F(s+1)=1$$

$$\text{(E2)}\qquad a^{q^2}b+ab^{q^2}=ab+ab=0.$$

Again $\epsilon_{i+2} = \epsilon_i$ for $i \geq 1$ and (Em) is satisfied. Hence $\mathrm{tr}(ax)^2 + \mathrm{tr}(ax)\mathrm{tr}(bx) + s\mathrm{tr}(bx)^2 = Q^K_{x+A2}(x)$ is, by (1.3), a form of codimension 2 radical and invariant -1.

We now consider Q^K_{A3} when $3|k$. Let 3^r be the highest power of 3 dividing t so that $t = 3^r t_0$ with $(3, t_0) = 1$. Set $v = 2^{3^r}$ so that $q = v^{t_0}$. Let δ be a root of the polynomial g_v of (2.3). Then $\delta \in GF(v^3) \subset GF(q^3) \subset K$ by (2.3)(1). Set $a = \delta^v$, $b = \delta$ and $c = \delta^v + \delta + 1$. We first check that a, b, c are independent over $F = GF(q)$. If not then 1 is in the F-span of a and b. Hence $a = gb + h$ for some $g, h \in F$ and so $\delta^v = g\delta + h$. We plug into (2.3)(2):

$$\delta^{2v} + \delta^{v+1} + \delta^2 = 1$$
$$h^2 + h\delta + (1 + g + g^2)\delta^2 = 1. \tag{2.8}$$

Now $\delta \notin GF(v)$, by (2.3)(1), and so has degree 3 over $GF(v)$. As $(3, t_0) = 1$, δ has degree 3 over $F = GF(v^{t_0})$ as well. Thus $1, \delta, \delta^2$ are independent over F. Then (2.8) gives $h^2 = 1$ and $h = 0$, a contradiction. Thus a, b, c are independent over F.

We compute (E0)

$$c^2 + ab = 1 + \delta^2 + \delta^{2v} + \delta^{v+1} = 0 \quad \text{by (2.3)(2)}.$$

For the other equations, first suppose $t_0 \equiv 1 \pmod 3$. Then $\delta^q = \delta^{v^{t_0}} = \delta^v$ as $\delta^{v^3} = \delta$. Similarly, $\delta^{q^2} = \delta^{v^{2t_0}} = \delta^{v^2}$. Then

$$a^q b + ab^q = \delta^{v^2+1} + \delta^{2v} = 1 \quad \text{by (2.3)(3)} \tag{E1}$$
$$a^{q^2} b + ab^{q^2} = \delta^{v^3+1} + \delta^{v^2+v} = \delta^2 + \delta^{v^2+v} = 1 \quad \text{by (2.3)(4)} \tag{E2}$$
$$a^{q^3} b + ab^{q^3} = ab + ab = 0. \tag{E3}$$

When $t_0 = 2 \pmod 3$ then $\delta^q = \delta^{v^2}$ and $\delta^{q^2} = \delta^v$. Then

$$a^q b + ab^q = \delta^{v^3+1} + \delta^{v^2+v} = 1 \tag{E1}$$
$$a^{q^2} b + ab^{q^2} = \delta^{v^2+1} + \delta^{2v} = 1 \tag{E2}$$
$$a^{q^3} b + ab^{q^3} = ab + ab = 0. \tag{E3}$$

Also $\epsilon_{i+3} = \epsilon_i$ for $i \geq 1$ and if $k = 2m$ then $a^{q^m} b \in GF(q^3) \subset GF(q^m)$ so that (Em) holds. Hence Q^K_{A3} has radical of codimension 2 and invariant 0.

Next consider Q^K_{x+A3} when $3|k$ and t is odd. Since t is odd we can pick $s = 1$ as our element of F with absolute trace 1. Let v, δ, a and b be as in the previous case. We know a, b are independent over F and $\epsilon_1 = 1 = \epsilon_2$, $\epsilon_3 = 0$, $\epsilon_{i+3} = \epsilon_i$ for $i \geq 1$ and that (Em) holds.We need only check (E0):

$$a^2 + ab + b^2 = \delta^{2v} + \delta^{v+1} + \delta^2 = 1$$

by (2.3)(2). Hence Q^K_{x+A3} has radical of codimension 2 and invariant -1.

Lastly, we consider Q_{x+A3} when $3|k$ and t is even. Then $GF(q^3) \subset K$; let γ be a primitive element of $GF(q^3)$. As t is even, 3 divides q^2+q+1. Set $\varphi = \gamma^{(q^2+q+1)/3}$. Then φ has order $3(q-1)$ so that $\varphi^{2(q-1)} + \varphi^{q-1} + 1 = 0$. Set $a = \varphi^{-2}$ and $b = \varphi^2$. They are independent over F as $(b/a)^{q-1} = \varphi^{4(q-1)} = \varphi^{q-1} \neq 1$ so that $b/a \notin F$. We compute

$$ab = 1 \tag{E0}$$

$$a^q b + ab^q = a^{q-1} + b^{q-1} = \varphi^{q-1} + \varphi^{2(q-1)} = 1 \tag{E1}$$

$$a^{q^2} b + ab^{q^2} = (\varphi^{q-1})^{q+1} + (\varphi^{q-1})^{q+1} = \varphi^{q-1} + \varphi^{2(q-1)} = 1 \tag{E2}$$

$$a^{q^3} b + ab^{q^3} = ab + ab = 0. \tag{E3}$$

Also $\epsilon_{i+3} = \epsilon_i$ for $i \geq 1$ and if $k = 2m$ then $a^{q^m} b \in GF(q^3) \subset GF(q^m)$ so that (Em) holds. Hence Q^K_{x+A3} has radical of codimension 2 and invariant 1. $\square$

3. Artin-Schreier curves with many rational points.

We again consider polynomials

$$R(x) = \sum_{i=0}^{h} \epsilon_i x^{q^i},$$

with each $\epsilon_i \in GF(2) = F$ and $h = \lfloor k - 1/2 \rfloor$. The Artin-Schreier curve is

$$C_R : y^q + y = xR(x).$$

This has genus $g = \frac{1}{2}(q-1)\deg R(x)$ by [8, VI.4.1]. We consider both the curve and the quadratic form over K. The number of points in K-projective space on C_R is

$$\#C_R(K) = qN(Q^K_R) + 1 = q^k + \Lambda(Q^K_R)(q-1)\sqrt{q^{k+w}} + 1,$$

where $w = \dim \operatorname{rad}(Q^K_R)$. We will compare this to the Hasse-Weil bound

$$\#C_R(K) \leq q^k + 1 + 2g\sqrt{q^k} = q^k + 1 + (q-1)q^\ell\sqrt{q^k},$$

where $\ell = \deg R(x)$. Clearly equality will hold in the Hasse-Weil bound only if k is even.

Theorem 3.1. *Suppose $k = 2m$ and the top coefficient $\epsilon_{m-1} = 1$. Then the number of points on C_R equals the Hasse-Weil bound iff one of the following holds*

1. *t is odd, $R = x + A2$ and $4|k$,*
2. *t is even, $R = x + A3$ and $6|k$.*

Proof. Note that $\deg R(x) = \ell = m-1$. The number of points on C_R equals the Hasse-Weil bound iff

$$\begin{aligned} \Lambda(Q_R^K)(q-1)\sqrt{q^{k+w}} &= (q-1)q^{m-1}\sqrt{q^k} \\ \Lambda(Q_R^K)\sqrt{q^w} &= q^{m-1} \\ w = 2(m-1) = k-2 \quad &\text{and} \quad \Lambda(Q_R^K) = 1. \end{aligned}$$

This holds, by (1.7), iff either (1) or (2) hold. □

The restriction that $\epsilon_{m-1} = 1$ is necessary.

Example. Let $k = 12$ so that $\ell = 5$. Set $R = x + x^4 + x^{16}$. Then $\epsilon_4 = 1$ and $\epsilon_5 = 0$. In particular, the genus of C_R is $g = 2^{4-1} = 8$. Also $\dim \mathrm{rad}(Q_R^K) = 8$ and $\Lambda(Q_R^K) = 1$. This may be checked as follows:

Let δ satisfy $\delta^6 = \delta + 1$. Set

$$a_1 = \delta^{28} \quad b_1 = \delta^{56} \quad a_2 = \delta^7 \quad b_2 = \delta^{35}.$$

Then $a_1b_1 + a_2b_2 = 1$. Set

$$\epsilon_i = a_1^{2^i} b_1 + a_1 b_1^{2^i} + a_2^{2^i} b_2 + a_2 b_2^{2^i}.$$

Then we may compute that $\epsilon_1 = 0$, $\epsilon_2 = 1$, $\epsilon_3 = 0$, $\epsilon_4 = 1$, $\epsilon_5 = 0$, $\epsilon_6 = 0$ and $\epsilon_{i+6} = \epsilon_i$ for $i \geq 1$. Thus

$$\begin{aligned} R &= \mathrm{tr}(a_1x)\mathrm{tr}(b_1x) + \mathrm{tr}(a_2x)\mathrm{tr}(b_2x) \\ Q_R^K &\simeq x_1x_2 + x_3x_4, \end{aligned}$$

giving the stated dimension of the radical and the invariant Λ.

Now

$$\begin{aligned} N(Q_R^K) &= \tfrac{1}{2}(2^{12} + \sqrt{2^{12+8}}) = \tfrac{1}{2}(2^{12} + 2^{10}) \\ \#C_R(K) &= 1 + 2^{12} + 2^{10}. \end{aligned}$$

The Hasse-Weil bound is $1 + 2^{12} + 2 \cdot 8\sqrt{2^{12}} = 1 + 2^{12} + 2^{10}$. Hence there are other Artin-Schreier curves meeting the Hasse-Weil bound besides those of (3.1).

4. Factoring linearized polynomials.

Here we will restrict to the case $q = 2$. For $R = \sum_{j=0}^{h} \epsilon_j x^{2^j}$ define

$$R^*(x) = \sum_{j=1}^{h} \epsilon_j (x^{2^{h+j}} + x^{2^{h-j}}).$$

Then by [4,Lemma 8]

$$\mathrm{rad} Q_R^K = \{a \in K : R^*(a) = 0\}.$$

Notice that R^* is a self-reciprocal, linearized polynomial and that any self-reciprocal, linearized polynomial of degree 2^{2h} arises in this way. If S is a self-reciprocal, linearized polynomial we will say T is the associated form if T is linearized and $T^* = S$.

Proposition 4.1. *Suppose k is even and $2h = k-2$. Let S be a self-reciprocal, linearized polynomial of degree $2h$ with associated form T. The following are equivalent:*

(1) *S divides $x^{2^k} + x$.*
(2) *All irreducible factors of S have degree d, where d divides k.*
(3) *Either $6|k$ and $T = A3$; or $4|k$ and $T = A2$.*

Proof. (1) $\leftrightarrow$ (2) is clear. (1) implies every root of S lies in $K = GF(2^k)$. Since Q_T^K has a radical consisting of the roots of S in K, we have $\dim \mathrm{rad} Q_T^K = k-2$ and so of codimension 2. This gives (3). Conversely, (3) gives Q_T^K has codimension 2 radical and so every root of S lies in K. $\square$

Proposition 4.2. *Let k be odd and $2h = k-1$. Let S be a self-reciprocal, linearized polynomial of degree $2h$ with associated form T. The following are equivalent:*

(1) *S divides $(x^{2^k} + x)(x^{2^k} + x + 1)$.*
(2) *Every irreducible factor of S either has degree d (where $d|k$), or has the form $p(x^2 + x + 1)$, where p is irreducible of degree d (where again $d|k$).*
(3) *$3|k$ and $T = A3$.*

Proof. (1) $\rightarrow$ (2). Let $q(x)$ be an irreducible factor of S. Then q divides q_k or $q_k + 1$, where $q_k = x^{2^k} + x$. In the first case, we have $\deg q = d$, where $d|k$. So suppose we are in the second case.

Now the roots of S not in K look like $a + \beta$, where $a \in K$ is a root and $\beta^2 = \beta + 1$. Namely, say $S(\alpha) = 0$ and $\alpha \notin K$. Then $q_k(\alpha) = 1$. Now

$$\beta^{2^j} = \begin{cases} \beta, & \text{if } j \text{ is even} \\ \beta^2, & \text{if } j \text{ is odd.} \end{cases}$$

In particular, $q_k(\beta) = 1$. Since either both $h \pm i$ are even or both are odd, we have $\beta^{h+i} + \beta^{h-i} = 0$ and so $S(\beta) = 0$. S and q_k are linearized so that their roots are additive. Hence $S(\alpha + \beta) = 0$ and $q_k(\alpha + \beta) = 0$. Thus $a = \alpha + \beta$ is a root of S in K.

Pick a root of $q(x)$, say $a+\beta$, where $a \in K$ is also a root of S. Now a^2+a is also a root of S. Let $p(x)$ be the irreducible polynomial of a^2+a. Set $d = \deg p$; note that $d|k$. Set $q_0(x) = p(x^2+x+1)$. Now

$$q_0(a+\beta) = p(a^2+a+\beta^2+\beta+1) = p(a^2+a) = 0.$$

Thus $q(x)$ divides $q_0(x)$. We will be done if we show $\deg q = 2d$, the same as $\deg q_0$.

Now $\deg q = [F(a+\beta) : F]$. We have

$$(a+\beta)^2 + (a+\beta) + 1 = a^2 + a.$$

Hence

$$F \subset F(a^2+a) \subset F(a+\beta).$$

Moreover, if $a+\beta \in F(a^2+a)$ then $\beta \in F(a)$. But $a \in K$ and $[K : F]$ is odd, so this is impossible. Hence

$$[F(a+\beta) : F] \geq 2[F(a^2+a) : F] = 2 \deg p = 2d.$$

Thus $q(x) = q_0(x) = p(x^2+x+1)$.

(2) $\to$ (1). Let π_1 be the product of irreducible factors of S that are of degree d, with $d|k$. Then $\pi_1 | q_k$. Let π_2 be the product of the irreducible factors of S of type $p(x^2+x+1)$, with p irreducible of degree d, $d|k$. Let π_3 be the product of the p's. Then $\pi_2(x) = \pi_3(x^2+x+1)$ and $\pi_3 | q_k$. Hence π_2 divides

$$q_k(x^2+x+1) = x^{2^{k+1}} + x^{2^k} + x^2 + x = q_k^2 + q_k = q_k(q_k+1).$$

Moreover, no root of π_2 is in K (as each irreducible factor has even degree). Thus π_2 divides q_k+1. And so $S = \pi_1\pi_2$ divides $q_k(q_k+1)$.

(1) $\to$ (3). Let A denote the roots of S that are also roots of q_k and let B be the roots of S that are also roots of q_k+1. As before, $S(\beta) = 0$ and $\beta \notin K$. The map $A \to B$ by $a \mapsto a+\beta$ is bijective. Hence $|A| = 2^{k-2}$. Now $\mathrm{rad} Q_T^K = A$ and so has codimension 2. Apply the main theorem (2.4) to get (3).

(3) $\to$ (1). We have that the codimension of $\mathrm{rad} Q_T^K$ is 2 so that 2^{k-2} roots of S lie in K. The other roots of S are $a+\beta$, for $a \in K$ a root of S. Now each root $a \in K$ is a root of q_k. And for each $a+\beta$ we have

$$(a+\beta)^{2^k} + (a+\beta) + 1 = (a^{2^k} + a) + (\beta^{2^k} + \beta + 1) = 0,$$

as k is odd. So S divides $q_k(q_k+1)$. $\square$

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*, 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*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Toulouse, 2003) (M. Fossorier, T. Høholdt and A. Poli, eds.), Lecture Notes in Computer Science, vol. 2643, Springer-Verlag, Berlin, 2003, pp. 24–33.
4. R. Fitzgerald and J. Yucas, *Pencils of quadratic forms over GF(2)*, preprint.
5. K. Khoo, G. Gong and D. R. Stinson, *New family of Gold-like sequences*, IEEE International Symposium on Information Theory 02, 2002, p. 181.
6. A. Klapper, *Cross-correlation of geometric series in characteristic two*, Des., Codes, and Cryptogr. **3** (1993), 347–377.
7. R. Lidl and H. Niederreiter, *Finite Fields (second edition)*, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.
8. H. Stichtenoth, *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, Berlin, 1993.
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.

Carbondale, IL 62901
E-mail address: rfitzg@ math.siu.edu