Trace Forms over Finite Fields of Characteristic 2 with Prescribed Invariants

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

Follow this and additional works at: http://opensiuc.lib.siu.edu/math_articles
Part of the Mathematics Commons
Published in Finite Fields and Their Applications, 15(1), 69-81.

Recommended Citation
Fitzgerald, Robert W. "Trace Forms over Finite Fields of Characteristic 2 with Prescribed Invariants." (Feb 2009).
Trace forms over finite fields of characteristic 2 with prescribed invariants

Robert W. Fitzgerald

Abstract

Set $F = F_2$ and $K = F_{2^k}$. Let

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

with each $\epsilon_i \in \{0, 1\}$. Our trace forms are the quadratic forms $Q^K_K : K \to F$ given by $Q^K_K(x) = \text{tr}_{K/F}(xR(x))$. 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 [5], as part of an authentication scheme [3], and to construct certain binary sequences in [7, 8, 6].

In each of these applications one wants the number of solutions (in $K$) to $Q^K_K(x) = 0$, denoted by $N(Q^K_K)$. This is easily worked out (see [10], 6.26, 6.32) in terms of the standard classification of quadratic forms:

$$N(Q^K_K) = \frac{1}{2}(2^k + \Lambda(Q^K_K) \sqrt{2^{k+r(Q^K_K)}}),$$

where $r(Q^K_K) = \text{dim rad}(Q^K_K)$ and

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

However, given $R$ and $K$, there is no simple way to determine the invariants $r(Q^K_K)$ and $\Lambda(Q^K_K)$. The only known results cover the case of one-term
and two-term $R$ [4]. Here we solve the inverse problem: Given $K$, determine all possible pairs of invariants $(r, \Lambda)$ and construct the $R$ with these invariants. We use this to construct new maximal Artin-Schreier curves.

1 General Results

We fix the notation. When $R$ is fixed, we write $r(k)$ for $\dim \text{rad}(Q^k_R)$ and $\Lambda(k)$ for $\Lambda(Q^k_R)$. For a linearized polynomial $L(x) = \sum a_i x^{2i}$ over $K$, we set $L_{dn}(x) = \sum a_i x^{2i}$. And for a polynomial $\ell(x) = \sum a_i x^i$ over $K$, we set $\ell_{up}(x) = \sum a_i x^{2i}$.

Given $R(x) = \sum_{i=0}^{h} a_i x^{2i}$, we set

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

Note that $(R^*)_{dn}(1) = 0$. Set $f^{(r)}(x) = x^d f(1/x)$, where $d = \deg f$. Then $f$ is self-reciprocal iff $f(x) = f^{(r)}(x)$.

Let $d$ be odd. We need to distinguish two cases. We say $d$ is in Case 1 when $-1$ is a power of 2 modulo $d$. We write $\eta(d) = 1$ to indicate Case 1 and let $w(d)$ be the least positive integer with $2^w \equiv -1 \pmod{d}$. We say $d$ is in Case 2 when $-1$ is not a power of 2 modulo $d$. We write $\eta(d) = 0$ to indicate Case 2 and let $w(d)$ be the least positive integer with $2^w \equiv 1 \pmod{d}$. Note that

$$2^{w(d)} \equiv (-1)^{\eta(d)} \pmod{d}$$

in either case.

We summarize the known results on factors of $x^k + 1$.

**Lemma 1.1.**

1. If $k = tn$ where $t$ is a 2-power and $n$ is odd then $x^k + 1 = \prod_{d|n} Q_\phi(x)^{\nu(d)}$, where $Q_\phi$ is the cyclotomic polynomial of order $d$.

2. Let $d$ be odd. Set $\nu(d) = \varphi(d)/(2w(d))$.

   (a) In Case 1, $Q_\phi(x)$ factors as a product of $\nu(d)$ many (distinct) irreducible, self-reciprocal polynomials of degree $2w(d)$. 

2
(b) In Case 2, $Q_d(x)$ factors as a product of $\nu(d)$ many (distinct) pairs $f(x)f^{(r)}(x)$, where $f(x)$ is irreducible, degree $w(d)$, and not self-reciprocal.

Proof: (1) follows from $x^k + 1 = (x^n + 1)^t$ and (2) follows from [13].

We will use the term self-reciprocal factor of $Q_d(x)$, $d$ odd, to mean irreducible, self-reciprocal factors in Case 1 and pairs $f(x)f^{(r)}(x)$ with $f(x)$ irreducible in Case 2. Thus, in either case, $Q_d(x)$ is a product of $\nu(d)$ many (distinct) self-reciprocal factors of degree $2w(d)$.

The key result is:

Proposition 1.2. $\dim \text{rad}(Q^K_R) = \deg(x^k + 1, (R^*)_{dn}(x))$.

Proof: Now $\alpha \in \text{rad}(Q^K_R)$ iff $\alpha \in K$ and $R^*(\alpha) = 0$ by [6] Lemma 8. Since the roots of $x^{2k} + x$ are distinct, we have

$$|\text{rad}(Q^K_R)| = \deg(x^{2k} + x, R^*(x))$$
$$= \deg(x^k + 1, (R^*)_{dn}(x))_{up}$$
$$= 2^{\deg(x^k + 1, (R^*)_{dn}(x))}.$$  

We have used that for linearized $L_1$ and $L_2$ that $(L_1, L_2) = ((L_1)_{dn}, (L_2)_{dn})_{up}$, by [10], p. 111. Hence the result follows.

The following is a substantial improvement over [4] Theorem 3.3.

Theorem 1.3. Write $k = tn$ with $t$ a 2-power and $n$ odd. Set $T = F_{2^t}$ and $D = \{d : d|n, d > 1\}$. Then:

1. $r(Q^K_R) = s_1 + \sum_{d \in D} 2s_dw(d)$ for some $s_d$ such that
   
   (a) if $t = 1$ then $s_1 = 1$;
   
   (b) if $t > 1$ then $s_1$ is even and $0 < s_1 \leq t$;
   
   (c) for $d \in D$, $0 \leq s_d \leq t\nu(d)$.

2. $\Lambda(Q^K_R) = (-1)^{\sum_{d \in D} s_d\eta(d)} \left(\frac{2}{n}\right)^t \Lambda(Q^T_R)$. Here $\left(\frac{2}{n}\right)$ is the Jacobi symbol, detecting whether or not 2 is a square modulo $n$.

Proof: (1) If irreducible $f$ divides $(R^*)_{dn}$ then so does $f^{(r)}$ since $(R^*)_{dn}$ is self-reciprocal. Hence Lemma 1.1 yields:

$$(x^k + 1, (R^*)_{dn}) = (x + 1)^{s_1} \prod_{d \in D} \prod_{i=1}^{\nu(d)} g^d_i(x)^{u_i(d)},$$

3
where the \(g^d_i\) are the self-reciprocal factors of \(Q_d\) and \(0 \leq u_i(d) \leq t\). Set 
\[s_d = \sum_{i=1}^{\nu(d)} u_i(d)\]. Note that \(0 \leq s_d \leq t\nu(d)\). Then 1.2 gives 
\[r(Q^K_R) = s_1 + \sum_{d \in D} s_d \cdot 2w(d)\].

We check the bounds on \(s_1\). First, \((R^*)_{dn}\) and \(x^k + 1\) are both divisible by \(x + 1\) so that \(s_1 \geq 1\). And \(s_1 \leq t\) as \(t\) is the highest power of \(x + 1\) dividing \(x^k + 1\). If \(t = 1\) then \(s_1 = 1\). Suppose \(t > 1\). Suppose, by way of contradiction, that \(s_1\) is odd. In particular, \(s_1 < t\) so that \((x + 1)^{s_1 + 1}\) divides \(x^k + 1 = (x^n + 1)^t\). Write \((R^*)_{dn} = h(x) \cdot (x^k + 1, (R^*)_{dn})\) for some \(h(x)\). Then \(h(x)\) is self-reciprocal and \(\deg h(x)\) is odd. Then \(h(1) = 0\) and so \((x + 1)^{s_1 + 1}\) also divides \((R^*)_{dn}\), contrary to the assumption that \(s_1\) is the highest power of \(x + 1\) dividing both \(x^k + 1\) and \((R^*)_{dn}\). Hence \(s_1\) is even.

(2) Let \(p\) be an odd prime dividing \(n\). Write \(n = p^\ell m\) where \((p, m) = 1\). Note that \(k = p^\ell tm\). Set 
\[D_0 = \{d \in D : p|d\}\] \[D_1 = \{d \in D : p \nmid d\} = \{\text{divisors } d > 1 \text{ of } m\}\].

For \(E = \mathbb{F}_{2^e}\) recall that we write \(r(e)\) for \(r(Q^E_R)\) and \(\Lambda(e)\) for \(\Lambda(Q^E_R)\). By [4] Theorem 3.1, 
\[\Lambda(k)2^{\frac{1}{2}(r(k) - r(tm))} = \left(\frac{2}{p^e}\right)^t \Lambda(tm) \pmod{p}\].

As \(x^m + 1\) divides \(x^k + 1\), we have 
\[(x^m + 1, (R^*)_{dn}) = (x + 1)^{s_1} \prod_{d \in D_1} \prod_{i=1}^{\nu(d)} g^d_i(x)^{u_i(x)},\]

for the same \(s_1\) and \(u_i(d)\) as before. So 
\[r(m) = s_1 + \sum_{d \in D_1} s_d \cdot 2w(d)\] 
\[r(k) - r(m) = \sum_{d \in D_0} s_d \cdot 2w(d)\] 
\[2^{\frac{1}{2}(r(k) - r(m))} = 2^{\sum_{D_0} s_d w(d)} \equiv (-1)^{\sum_{D_0} s_d \eta(d)} \pmod{p},\]
as \( p \) divides each \( d \in D_0 \). Then

\[
\Lambda(k) = \left( \frac{2}{p^t} \right) (-1) \sum_{d \in D_0} s_d \eta(d) \Lambda(t m).
\]

A simple induction argument completes the proof. \( \square \)

The proof of 1.3 shows that every possible pair of invariants \((r, \Lambda)\) does in fact arise. We record this as:

**Corollary 1.4.** Write \( d = t n \) as before. Suppose \( s_1 \) and \( s_d, d \in D \) satisfy the conditions of Theorem 1.3. Then \( r(Q^K_R) = s_1 + \sum_D 2 s_d w(d) \) iff

\[
(R^s)_{dn} = h(x)(x+1)^{s_1} \prod_{d \in D}^{\nu(d)} \prod_{i=1} g_i^d(x)^{u_i(d)},
\]

where the \( g_i^d \) are self-reciprocal factors of \( Q_d(x) \), \( s_d = \sum_{i=1}^{\nu(d)} u_i(d) \) and \( h(x) \) is self-reciprocal and prime to \((x^k+1)/(\prod_D \prod g_i^d(x)^{u_i(d)})\).

We note that if the coefficients, \( a_i \), of \( R \) are allowed to take on any value in \( K \) then every quadratic form over \( K \) arises as a \( Q^K_R \) (for some \( R \)) [5] Proposition 1.1, and so all invariant pairs are possible. Thus 1.3 gives the restrictions on the quadratic forms \( Q^K_R \) that follow from restricting the coefficients to 0, 1.

### 2 When \( k \) is prime

**Example 2.1.** Suppose \( k = 43 \). Here we are in Case 1, \( w(k) = 7 \) and 2 is not a square modulo \( k \). Say \( R(1) = 0 \) so that \( \Lambda(1) = 1 \) (see [4] Corollary 3.4). The possible values of \((r(Q^K_R), \Lambda(Q^K_R))\) are:

\[
(1, -1) \quad (15, +1) \quad (29, -1) \quad (43, +1).
\]

We construct all \( R(x) \) of degree \( 2^9 \) with \( r(Q^K_R) = 15 \) and \( \Lambda(Q^K_R) = +1 \). First, \( x^{43} + 1 = (x + 1)f_1f_2f_3 \) where

\[
\begin{align*}
    f_1 &= x^{14} + x^{13} + x^{11} + x^7 + x^3 + x + 1 \\
    f_2 &= x^{14} + x^{12} + x^{10} + x^7 + x^4 + x^2 + 1 \\
    f_3 &= x^{14} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1.
\end{align*}
\]

5
Then \((R^*)_{dn} = h(x)f_i\) for some \(i\) and some self-reciprocal \(h\) of degree 4 with \(h(1) = 0\). There are only two choices for \(h\), namely, \(h_1 = x^4 + 1\) and \(h_2 = x^4 + x^3 + x^2 + x + 1\). So there are six choices for \((R^*)_{dn}\). Note that \(R\) and \(R + x\) yield the same \(R^*\), so we take whichever of \(R\), \(R + x\) satisfies \(R(1) = 0\). We obtain:

<table>
<thead>
<tr>
<th>((R^*)_{dn})</th>
<th>(R)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(h_1 f_1)</td>
<td>(x^{2^9} + x^{2^9} + x^{2^1} + x^{2^7})</td>
</tr>
<tr>
<td>(h_2 f_1)</td>
<td>(x^{2^9} + x^{2^8} + x^{2^2} + x^{2^3})</td>
</tr>
<tr>
<td>(h_1 f_2)</td>
<td>(x^{2^9} + x^{2^8} + x^{2^6} + x^{2^2} + x^{2^4} + x)</td>
</tr>
<tr>
<td>(h_2 f_2)</td>
<td>(x^{2^9} + x^{2^7} + x^{2^5} + x^{2^4} + x^{2^3} + x^2)</td>
</tr>
<tr>
<td>(h_1 f_3)</td>
<td>(x^{2^9} + x^{2^7} + x^{2^3} + x^{2^2} + x^2 + x)</td>
</tr>
<tr>
<td>(h_2 f_3)</td>
<td>(x^{2^9} + x^{2^8} + x^{2^7} + x^{2^3})</td>
</tr>
</tbody>
</table>

The goal of this section is to imitate the example and count the number of \(R\) with a given pair of invariants \((r, \Lambda)\).

**Lemma 2.2.** Let \(d\) be even. Let \(f(x) \in F[x]\) be self-reciprocal of degree \(d\) and satisfy \(f(1) = 1\). Let \(N > d\) be even. The number of self-reciprocal \(g(x) \in F[x]\) which are multiples of \(f\), degree \(N\) and satisfy \(g(1) = 0\) is \(2^{\frac{1}{2}(N-d)-1}\).

**Proof:** Write \(g(x) = h(x)f(x)\). We require that \(h(x)\) be self-reciprocal, degree \(N - d\) and have \(h(1) = 0\). The last condition implies that \(h(x)\) has no middle term (that is, \(x^{(N-d)/2}\)). Thus \(h(x)\) is determined by the coefficients of \(x^i, 1 \leq i < \frac{1}{2}(N - d)\), giving the result. \(\square\)

**Lemma 2.3.** Let \(f_1, f_2, \ldots, f_t\) be pairwise prime, self-reciprocal polynomials in \(F[x]\) of even degree \(d\) that satisfy \(f_i(1) = 1\). Let \(N\) be even and set

\[
\ell = \min \left\{ \left[ \frac{N}{d} \right] - 1, t \right\}.
\]

The number of self-reciprocal \(h(x) \in F[x]\) of degree \(N\), prime to \(f_1 \cdot f_2 \cdots f_t\) and satisfying \(h(1) = 0\) is:

\[
\sum_{m=0}^{\ell} (-1)^m \binom{t}{m} 2^{\frac{1}{2}(N-dm)-1}.
\]
Proof: Let $M(f)$ denote the set of self-reciprocal polynomials $h(x) \in F[x]$ of degree $N$ with $h(1) = 0$ and $f | h$. Let
\[
M(f_{i_1}, f_{i_2}, \ldots, f_{i_m}) = \bigcap_{j=1}^{m} M(f_{i_j}),
\]
where $m \leq t$. If $N \leq dm$ then $M(f_{i_1}, \ldots, f_{i_m}) = \emptyset$ (if $N = dm$ then we must have $h(1) = 1$), Otherwise, $dm < N$ so that $m \leq \ell$. Apply 2.2 to $f = f_{i_1} \cdot f_{i_2} \cdots f_{i_m}$ to get
\[
|M(f_{i_1}, f_{i_2}, \ldots, f_{i_m})| = \begin{cases} 2^\frac{1}{2}(N-dm) - 1, & \text{if } m \leq \ell \\ 0, & \text{if } m > \ell. \end{cases}
\]
The total number of self-reciprocal $h(x)$ of degree $N$ with $h(1) = 0$ is $2^\frac{1}{2}N - 1$. So the number of $h(x)$ of the statement is:
\[
2^\frac{1}{2}N - 1 - \sum_{i=1}^{t} |M(f_{i})| = 2^\frac{1}{2}N - 1 - \sum_{m=1}^{t} \sum_{i_1 < \cdots < i_m} |M(f_{i_1}, \ldots, f_{i_m})|
\]
\[
= 2^\frac{1}{2}N - 1 - \sum_{m=1}^{t} (-1)^{m+1} \binom{t}{m} 2^\frac{1}{2}(N-dm) - 1
\]
\[
= \sum_{m=0}^{\ell} (-1)^m \binom{t}{m} 2^\frac{1}{2}(N-dm) - 1.
\]

We continue to write $\nu(k)$ for $\varphi(k)/(2w(k))$.

Theorem 2.4. Let $k$ be a prime. For any $R$:
1. $\dim \text{rad}(Q^K_R) = 1 + 2sw(k)$ for some $0 \leq s \leq v(k)$.
2. If $R(1) = 1$ then $\Lambda(Q^K_R) = 0$.
3. If $R(1) = 0$ then $\Lambda(Q^K_R) = (-1)^{s_0(k)}(\frac{2}{k})$.
4. The number of $R$ of degree $2^N$ with $R(1) = 0$ and $\dim \text{rad}(Q^K_R) = 1 + 2sw(k)$ is:
\[
\binom{\nu(k)}{s} \sum_{m=0}^{\ell} (-1)^m \binom{\nu(k) - s}{m} 2^{N-w(k)(s+m)-1},
\]
where
\[ \ell = \min \left\{ \left\lceil \frac{N}{w(k)} \right\rceil - s - 1, \nu(k) - s \right\} . \]

Proof: (1), (2) and (3) follow from Theorem 1.3. To prove (4), fix \( s \). By Corollary 1.4, \( (x^k + 1, (R^*)_{dn}) \) is \( x + 1 \) times a product of \( s \) self-reciprocal factors of \( Q_k(x) \), each of degree \( 2w(k) \). \( Q_k(x) \) has \( \nu(k) \) many self-reciprocal factors. Choose \( s \) of them, call their product \( g \) and let \( f_1, f_2, \ldots, f_t \), \( t = \nu(k) - s \), be the other self-reciprocal factors. Then
\[ R^* = h(x)g(x) \]
where \( h(x) \) is self-reciprocal, \( h(1) = 0 \) (so that \( x + 1 \) is a factor of \( R^* \)), of degree \( 2N - 2sw(k) \) (as deg \( R = 2^N \) iff deg \( R^* = 2N \) and \( h(x) \) is prime to \( g \). Given this choice of the \( s \) factors then Lemma 2.3 gives the number of such \( h \)'s as:
\[ \sum_{m=0}^{\ell} (-1)^m \binom{\nu(k) - s}{m} 2^{\frac{1}{2}(2N-2sw(k)-m-2w(k))} - 1, \]
where
\[ \ell = \min \left\{ \left\lceil \frac{2N - 2sw(k)}{2w(k)} \right\rceil - 1, \nu(k) - s \right\} \]
\[ = \min \left\{ \left\lceil \frac{N}{w(k)} \right\rceil - s - 1, \nu(k) - s \right\} . \]

Hence the number of \( R^* \) of degree \( 2^{2N} \) with \( (x^k + 1, (R^*)_{dn}) = (x + 1)g(x) \) is:
\[ \binom{\nu(k)}{s} \sum_{m=0}^{\ell} (-1)^m \binom{\nu(k) - s}{m} 2^{N-w(k)(s+m)} - 1. \]

Both \( R \) and \( R + x \) yield the same \( R^* \) and exactly one of \( R, R + x \) maps \( 1 \) to \( 1 \). So the number of \( R \) with \( R(1) = 1 \) and \( \dim \text{rad}(Q_R^K) = 1 + 2sw(k) \) is given by the same formula. \( \square \)

One may easily check the formula on Example 2.1. There \( k = 43, w(k) = 7 \) and so \( \nu(k) = 3 \). The example considered \( R \) of degree \( 2^9 \) and \( r = 15 \) (which is \( s = 1 \)). Then \( \ell = \min \{ \left\lceil \frac{9}{7} - 1 - 1, 6 - 1 \right\} \} = 0 \) and the number of such \( R \) is:
\[ \binom{3}{1} (-1)^0 \binom{6-1}{0} 2^{9-7-1} = 6, \]
which agrees with the example.
3 When $k$ is a product of two primes

The values of $w(d)$, over divisors of $k$, are not independent. Thus the formulas for $\dim \text{rad}(Q_K^R)$ and $\Lambda(Q_K^R)$ of Theorem 1.3 simplify. But the underlying number theory is complicated. We illustrate these points by considering the easy case of $k$ being a product of two primes.

Lemma 3.1. Let $p$ be an odd prime and let $\epsilon = \pm 1$.

1. If $2^w \equiv \epsilon \pmod{p}$ then $2^{wp} \equiv \epsilon \pmod{p^2}$.

2. $p^2$ is in Case 1 iff $p$ is.

3. $w(p^2) = w(p)$ or $pw(p)$.

Proof: (1) We have:

$$2^{wp} - \epsilon = (2^w - \epsilon)(2^{wp-1} + \epsilon 2^{wp-2} + \cdots + \epsilon^{p-2} 2^w + \epsilon^{p-1}).$$

Modulo $p$, the second factor is $p\epsilon p^{p-1}$. Thus $p^2$ divides $2^{wp} - \epsilon$.

(2) If $p$ is in Case 1 then $2^v \equiv -1 \pmod{p}$ for some $w$. Then (1) shows $p^2$ is also in Case 1. And if $p^2$ is in Case 1 then $2^v \equiv -1 \pmod{p^2}$ for some $v$. So $2^v \equiv -1 \pmod{p}$ and $p$ is in Case 1.

(3) We have $w(p)|w(p^2)$ and by (1), $w(p^2)|pw(p)$.

Remark 3.2. It is possible for $w(p^2)$ to equal $w(p)$, but exceedingly rare. If $w(p^2) = w(p)$ then $p$ is a Wieferich prime, meaning that $2^{p-1} \equiv 1 \pmod{p^2}$ (see [11]). A computer search [9] has shown that the only Wieferich primes less than $1.25 \times 10^{15}$ are 1093 and 3511. Both 1093 and 3511 satisfy $w(p) = w(p^2)$ (this can easily be checked with a computer). Further, 1093 is in Case 1 (with $w(1093) = 182$) and 3511 is in Case 2 (with $w(3511) = 1755$).

A typical simplification of Theorem 1.3 is:

Corollary 3.3. Let $k = p^2$, with $p$ and odd prime that is not a Wieferich prime. Then

$$\dim \text{rad}(Q_K^R) = 1 + (2s_1 + 2ps_2)w(p)$$

$$\Lambda(Q_K^R) = (-1)^{(s_1 + s_2)\eta(p)}\Lambda(1).$$

The simplification for Wieferich primes can also be easily worked out. In the next result, $v_2(n)$ denotes the highest power of 2 dividing $n$.
Proposition 3.4. Let $p$ and $q$ be distinct odd primes.

1. $pq$ is in Case 1 iff $p$ and $q$ are in Case 1 and also $v_2(w(p)) = v_2(w(q))$. In this case, $w(pq) = \text{lcm}(w(p), w(q))$.

2. If $p$ and $q$ are in Case 1 and $v_2(w(p)) \neq v_2(w(q))$ then $w(pq) = \text{2lcm}(w(p), w(q))$.

3. If $p$ is in Case 1 and $q$ is in Case 2 then $w(pq) = \text{lcm}(2w(p), w(q))$.

4. If $p$ and $q$ are in Case 2 then $w(pq) = \text{lcm}(w(p), w(q))$.

Proof: (1) Suppose $pq$ is in Case 1. Then $2^{w(pq)}$ is -1 modulo $pq$, hence modulo $p$ and $q$. So both $p$ and $q$ are in Case 1. We want to show that $v_2(w(p)) = v_2(w(q))$. Suppose instead that $v_2(w(p)) < v_2(w(q))$. Let $L = \text{lcm}(w(p), w(q))$; note that $L/w(p)$ is even. Now $w(p)$ and $w(q)$ divide $w(pq)$ so $L$ divides $w(pq)$. Hence $w(pq)/w(p)$ is even. But $2^{w(pq)/(w(pq)/w(p))} \equiv 1 \pmod{p}$ and $2^{w(pq)/w(p)} \equiv -1 \pmod{pq}$, a contradiction. So $v_2(w(p)) = v_2(w(q))$.

Conversely, suppose $p$ and $q$ are in Case 1 and $v_2(w(p)) = v_2(w(q))$. Then $L/w(p)$ and $L/w(q)$ are odd. So $2^L$ is -1 modulo $p$ and $q$, hence modulo $pq$. Thus $pq$ is in Case 1. Note that $w(pq)/L$ and clearly $L/w(pq)$. So $w(pq) = \text{lcm}(w(p), w(q))$.

(2) Here $pq$ is in Case 2 so that $w(pq)$ is the order of 2 modulo $pq$. As $p$ and $q$ are in Case 1, the order of 2 modulo $p$ is $2w(p)$ and modulo $q$ it is $2w(q)$. Hence $w(pq) = \text{2lcm}(w(p), w(q))$. Parts (3) and (4) are similar. □

Examples (1) We consider $k = 11 \cdot 43$. We have $p = 11$ is in Case 1 (with $w(p) = 5$) and $q = 43$ is also in Case 1 (with $w(q) = 7$). Thus by (1) of Proposition 3.4 we have that $k$ is in Case 1 and $w(k) = 35$. Theorem 1.3 becomes:

$$\dim \text{rad}(Q_K^R) = 1 + 10s_1 + 14s_2 + 70s_3$$

$$\Lambda(Q_K^R) = (-1)^{(s_1+s_2+s_3)}\Lambda(1),$$

where $0 \leq s_1 \leq 1$, $0 \leq s_2 \leq 3$ and $0 \leq s_3 \leq 6$. Each choice of $s_i$ occurs for some $R$.

(2) The case $k = 21$ was considered in [4] where a computer search showed that $\dim \text{rad}(Q_K^R) = 5$ was not possible. We may now easily check this. Here $w(3) = 1$, $w(7) = 3$ and $w(21) = 6$. Hence $\dim \text{rad}(Q_K^R) = 1 + 2s_1 + 6s_2 + 12s_3$
with each $s_i \in \{0, 1\}$. Thus 5, 11 and 17 are precisely the odd values missed by $\dim \text{rad}(Q^K_K)$.

(3) The value of $\dim \text{rad}(Q^K_K)$ does not always determine $\Lambda(Q^K_K)$, even when $R(1) = 0$ (so that $\Lambda(1) = 1$). Consider $k = 19 \cdot 73$. Here $p = 19$ is in Case 1 with $w(p) = 9$ and 2 not a square modulo $p$. And $q = 73$ is in Case 2 with $w(q) = 9$ and 2 a square modulo $q$. So

$$\dim \text{rad}(Q^K_K) = 1 + 18s_1 + 18s_2 + 36s_3$$

$$\Lambda(Q^K_K) = (-1)^{s_1 + 1}\Lambda(1),$$

where $0 \leq s_1 \leq 1$, $0 \leq s_2 \leq 4$ and $0 \leq s_3 \leq 36$. Then $\dim \text{rad}(Q^K_K) = 19$ has two solutions, namely $(s_1, s_2, s_3) = (1, 0, 0)$ and $(0, 1, 0)$, that yield different values of $\Lambda(Q^K_K)$. We can construct specific examples using Corollary 1.4. We can take $Q_{19}$ or $(x^9 + x + 1)(x^9 + x^8 + 1)$ (a self-reciprocal factor of $Q_{73}$) for $(x^k + 1, (R^*)_{\text{dn}})$. Assuming $R(1) = 0$ so that $\Lambda(1) = 1$, these yield

$$R_1 = x^{2^{10}} + x^{2^9}$$
$$R_2 = x^{2^{10}} + x^{2^9} + x^{2^8} + x^{2^7} + x^{2^2} + x^2.$$

Both give radicals of dimension 19 but $\Lambda(Q^K_K_{R_1}) = +1$ while $\Lambda(Q^K_K_{R_2}) = -1$.

### 4 Maximal Artin-Schreier Curves

The Artin-Schreier curves considered here are:

$$C_R(K) : y^2 + y = xR(x),$$

where $x, y \in K$. This has genus $g = \frac{1}{2} \deg R(x)$ by [12] VI.4.1. The number of points in $K$-projective space on $C_R$ is:

$$\#C_R(K) = 2N(Q^K_K) + 1 = 2^k + 1 + \Lambda(Q^K_K)\sqrt{2^k + r},$$

where $r = \dim \text{rad}(Q^K_K)$ and we have used Equation 1. The curve is maximal if equality holds in the Hasse-Weil bound

$$\#C_R(K) \leq 2^k + 1 + 2\sqrt{2^k} = 2^k + 1 + \deg R(x)\sqrt{2^k}.$$

Clearly equality holds only if $k$ is even. Maximal curves yield the best algebraic geometry codes.
Lemma 4.1. Let $k$ be even and $r = \dim \text{rad}(Q^K_R)$. Then $C_R(K)$ is maximal iff

1. $\deg R(x) = 2^{r/2}$ and
2. $\Lambda(Q^K_R) = +1$.

Proof: We require $\Lambda(Q^K_R)\sqrt{2^{k+r}} = \deg R(x)\sqrt{k}$, which yields the result. $\Box$

In [5] we found all $R$ and $K$ with $C_R(K)$ maximal and $k - r = 2$ (note: the codimension $k - r$ is necessarily even). We also gave one example, found by computer search, of a maximal $C_R(K)$ with $k - r = 4$. As Lemma 4.1 prescribes the invariants of $Q^K_R$, we may now find all codimension 4 maximal curves, at least for a wide range of $k$.

As $k$ must be even, Theorem 1.3 reduces the computation of $\Lambda(Q^K_R)$ to that of $\Lambda(Q^T_R)$ where $T = F_{2^t}$ for $t$, the highest 2-power dividing $k$. We have been unable to do this in general, hence our restrictions on $k$.

Define

for $0 \leq i \leq 1$ \quad $S_i = \text{number of } \epsilon_j = 1 \text{ with } j \equiv i \pmod{2}$
for $0 \leq i \leq 3$ \quad $T_i = \text{number of } \epsilon_j = 1 \text{ with } j \equiv i \pmod{4}$.

Lemma 4.2. 1. Suppose $K = F_4$. Then:

$$\Lambda(Q^K_R) = \begin{cases} 
0, & \text{if } S_0 \text{ is odd} \\
+1, & \text{if } S_0 \text{ is even.}
\end{cases}$$

2. Suppose $K = F_{16}$. Then:

$$\Lambda(Q^K_R) = \begin{cases} 
0, & \text{if } T_0 \text{ is odd and } T_1 + T_3 \text{ is even} \\
+1, & \text{if } T_0 \equiv T_1 + T_3 \pmod{2} \\
-1, & \text{if } T_0 \text{ is even and } T_1 + T_3 \text{ is odd.}
\end{cases}$$

Proof: We check (2). If $x \in K$ then $x^{2^i} = x^{2^j}$ when $i \equiv j \pmod{4}$. Hence, as a function on $K$, $R = T_0x + T_1x^2 + T_2x^4 + T_3x^8$. Further, $x^3 \in F_4$ so that $\text{tr}(x^3) = 0$ and

$$\text{tr}(x^9) = \text{tr}(x^{18}) = \text{tr}(x^3).$$
Thus $Q_R(x) = \text{tr}(T_0x^2 + (T_1 + T_3)x^3)$ for all $x \in K$. A simple computation shows that

$$N(Q_R^K) = \begin{cases} 
4, & \text{if } T_0 \text{ even, } T_1 + T_3 \text{ odd} \\
8, & \text{if } T_0 \text{ odd, } T_1 + T_3 \text{ even} \\
12, & \text{if } T_0 \text{ odd, } T_1 + T_3 \text{ odd} \\
16, & \text{if } T_0 \text{ even, } T_1 + T_3 \text{ even}.
\end{cases}$$

Comparing with Equation 1 gives the result. The proof of (1) is similar and easier.

Lemma 4.3. Let $r = \dim \text{rad}(Q_R^K)$. If $C_R(K)$ is maximal with $k - r = 4$ then $k$ is divisible by 3 or 8. Further, if $k$ is divisible by 5 but not 8 then $s_5$ is its maximal value.

Proof: Assume $k$ is not divisible by 8. Write $k = tn$ with $n$ odd and $t = 2$ or 4. By 1.3

$$k - 4 = s_1 + \sum_{d|n} 2s_dw(d),$$

with $s_1 \in \{2, t\}$ and $0 \leq s_d \leq t\nu(d)$. Note that the maximum values, $s_1 = t$ and $s_d = t\nu(d)$, make the right side of Equation 2 equal to $k$. We are looking for a solution just below the maximum.

If $w(d) \leq 2$ then $d$ divides $2^2 \pm 1, 2 \pm 1$ and so $d = 3$ or 5. Thus if no $d$ is 3 or 5 then every $w(d) > 2$ and there is no solution to Equation 2.

Suppose, if possible, that 3 does not divide $k$. Then $k = 5m$ for some even $m$. Write $m = 2m_0$. The only solution to Equation 2 is:

$$s_1 = t \quad s_5 = t - 1 \quad s_d = t\nu(d) \quad \text{for } d \neq 5.$$

This is also the only solution if $s_5$ is not maximal (whether or not 3 divides $k$). Our construction, Corollary 1.4, shows that

$$(x^k + 1, (R^*)_{dn}) = (x + 1)^tQ_5^{-1}\prod_{d \neq 5} Q_d^t = (x^k + 1)/Q_5.$$

By Lemma 4.1, $\deg R = 2^{(k - 4)/2}$ and so $\deg(R^*)_{dn} = k - 4$. Hence

$$R^* = \frac{x^k + 1}{Q_5} = \frac{(x + 1)(x^k + 1)}{x^5 + 1} = (x + 1)\sum_{i=0}^{m-1} x^{5i}.$$
And so
\[ R = \epsilon x + \sum_{i=0}^{m_0-1} \left( x^{2^5(m_0-i)-2} + x^{2^5(m_0-i)-3} \right), \]
for \( \epsilon \in \{0, 1\} \).

Lemma 4.1 gives \( \Lambda(Q^K_R) = +1 \) while Theorem 1.3 gives \( \Lambda(Q^K_R) = -\Lambda(t) \). Hence \( t = 4 \) since, by Lemma 4.2, \( \Lambda(2) \neq -1 \). So Lemma 4.2 gives \( T_0 \) is even and \( T_1 + T_3 \) is odd. We have \( R \) explicitly so we compute the \( T_i \), writing \( m_0 = 4 \ell + u \):

<table>
<thead>
<tr>
<th>( u )</th>
<th>( T_0 )</th>
<th>( T_1 )</th>
<th>( T_2 )</th>
<th>( T_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( 2\ell + \epsilon )</td>
<td>( 2\ell )</td>
<td>( 2\ell )</td>
<td>( 2\ell )</td>
</tr>
<tr>
<td>1</td>
<td>( 2\ell + \epsilon )</td>
<td>( 2\ell )</td>
<td>( 2\ell + 1 )</td>
<td>( 2\ell + 1 )</td>
</tr>
<tr>
<td>2</td>
<td>( 2\ell + 1 + \epsilon )</td>
<td>( 2\ell )</td>
<td>( 2\ell + 1 )</td>
<td>( 2\ell + 2 )</td>
</tr>
<tr>
<td>3</td>
<td>( 2\ell + 2 + \epsilon )</td>
<td>( 2\ell + 1 )</td>
<td>( 2\ell + 1 )</td>
<td>( 2\ell + 2 )</td>
</tr>
</tbody>
</table>

If \( \epsilon = 1 \) then only \( u = 2 \) gives \( T_0 \) even, but the \( T_1 + T_3 \) is even. Hence \( \epsilon = 0 \) and we must have \( u \) odd. But then \( k = 5 \cdot 2m_0 = 5 \cdot 2(4\ell + u) \) is not divisible by \( t = 4 \), a contradiction. Hence \( k \) is divisible by 3.

**Example 4.4.** Lemma 4.3 can fail when \( k - r = 6 \). We use Corollary 1.4 to construct an example with \( k = 20 \). We need \( r = 14 = s_1 + 4s_5 \) so we take \( s_1 = 2 \) and \( s_5 = 3 \). Then

\[
(x^k + 1, (R^*)_{dn}) = (x + 1)^2Q_5^3 = (x^{10} + 1)(x^4 + x^3 + x^2 + x + 1)
\]

\[
R = x^{2^7} + x^{2^6} + x^{2^5} + x^{2^4} + x^{2^3} + \epsilon x.
\]

As before, \( \Lambda(Q^K_R) = -\Lambda(4) \) so that we require \( T_0 \) to be even and \( T_1 + T_3 \) to be odd. Thus taking \( \epsilon = 1 \) gives an example of a maximal curve with \( k - r = 6 \) and \( k \) not divisible by either 3 or 8.

**Theorem 4.5.** Suppose \( k \) is even but not a multiple of 8. Let \( r = \dim \text{rad}(Q^K_R) \). Then the maximal curves \( C_R(K) \) with \( k - r = 4 \) are precisely:

1. \( k = 6m \) with \( m \) odd and
   \[
   R = x^2 + \sum_{i=1}^{3(m-1)/2} \left( x^{2^6i+1} + x^{2^6i-1} \right).
   \]

2. \( k = 12m \) with \( m \) odd and
   \[
   R = x + \sum_{i=0}^{m-1} \left( x^{2^{6i+4}} + x^{2^{6i+2}} \right).
   \]
3. $k = 12m$ with $m$ odd and

$$R = x + \sum_{i=0}^{m-1} \left( x^{6i+4} + x^{6i+3} + x^{6i+2} \right).$$

**Proof:** From Lemma 4.3 we have $k = 6m$ or $12m$ with $m$ odd. We first do the case $k = 6m$. Equation 2 becomes:

$$k - 4 = 2 + 2s_3 + \sum_{d|3m, d \neq 3} 2s_dw(d),$$

for $0 \leq s_3 \leq 2$ and $0 \leq s_d \leq 2\nu(d)$. The only solution is $s_3 = 0$ and $s_d = 2\nu(d)$ for $d \neq 3$, since all $w(d) > 2$ except for $d = 5$ when $s_5$ is its maximal value 2 by Lemma 4.3. Thus

$$(x^k + 1, (R^*)_{dn}) = \frac{x^k + 1}{Q_3^2} = (x^2 + 1) \sum_{i=0}^{m-1} x^{6i}.$$

Lemma 4.1 gives $\deg R = 2^{(k-4)/2}$ and $\deg (R^*)_{dn} = k - 4$. Hence $R^*$ is this gcd and

$$R = \epsilon x + \sum_{i=1}^{3(m-1)/2} \left( x^{26i+1} - x^{26i-1} \right).$$

Lastly, $\Lambda(Q_R^k) = +1$ by Lemma 4.1 while $\Lambda(Q_R^k) = \Lambda(2)$ by Theorem 1.3. Hence $\epsilon = 0$ by Lemma 4.2.

Now suppose $k = 12m$ with $m$ odd. Equation 1 becomes:

$$k - 4 = s_1 + 2s_3 + \sum_{d|3m, d \neq 3} 2s_dw(d),$$

where $s_1 \in \{2, 4\}$, $0 \leq s_3 \leq 4$ and $0 \leq s_d \leq 4\nu(d)$. As before, each $s_d$, $d \neq 1, 3$, is its maximal value. So there are two solutions, $(s_1, s_3) = (4, 2)$ and $(2, 3)$. In the first case, $(R^*)_{dn} = (x^k + 1)/Q_3^2$ and $R$ has the form (2). Here Lemma 4.2 is used to determine the coefficient of $x$. In the second case, $(R^*)_{dn} = (x^k + 1)/(x^6 + 1)$ and $R$ has the form (3).

We note that the example of [5] is statement (2) of Theorem 4.5 with $m = 1$. 

15
References


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