Explicit maximal and minimal curves of Artin–Schreier type from quadratic forms

Daniele Bartoli¹ · Luciane Quoos² · Zülfükar Saygı³ · Emrah Sercan Yılmaz⁴

Received: 1 February 2019 / Revised: 12 December 2019 / Accepted: 16 December 2019 / Published online: 2 January 2020
© Springer-Verlag GmbH Germany, part of Springer Nature 2020

Abstract
In this note we present explicit examples of maximal and minimal curves over finite fields in odd characteristic. The curves are of Artin–Schreier type and the construction is closely related to quadratic forms from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.

Keywords Algebraic curves · Rational points · Maximal curves · Minimal curves

Mathematics Subject Classification 11G20 · 11E08

1 Introduction

In the interaction between algebraic curves over finite fields and applications in coding theory, cryptography, quasi-random numbers, and related areas it is important to know the exact number of rational points that a curve can have; see for example [7,10,11,16,17]. In particular, curves of Artin–Schreier type have been widely investigated. Also,
many of the known constructions of maximal or minimal curves are closely related to quadratic forms and the link between curves of the type \( y^2 + y = xS(x) \), where \( S(x) \) is a linearized polynomial, with quadratic forms was explicitly studied in 1992; see [18].

Recently, some characterizations and classification results were obtained in the literature. Let \( \mathbb{F}_q \) denote the finite field with \( q \) elements and \( n \) be a positive integer. For finite fields of characteristic 2, a full classification of quadratic forms from \( \mathbb{F}_{q^n} \) to \( \mathbb{F}_q \) whose radicals have codimension 2 is provided in the following cases: all the coefficients are from \( \mathbb{F}_2 \) or at least three are in \( \mathbb{F}_4 \). As an application, maximal and minimal curves are obtained, see [4,5,12–14]. Later on, some results on quadratic functions and maximal Artin–Schreier curves over finite fields having odd characteristic have been presented in [1,2]. In [15], by using some techniques developed in [3], a conjecture presented in [2] is proved and explicit classes of maximal and minimal Artin–Schreier type curves in odd characteristic are presented. In this work we determine examples of minimal and maximal curves over \( \mathbb{F}_q \) of the following type

\[
X_S : \quad y^q - y = xS(x) = \sum_{i=0}^{m} s_i x^{q^i+1}. \tag{1}
\]

Our investigation is based on the type of the quadratic form associated with this curve. In Proposition 2 we characterize the polynomials \( S(x) \) of degree \( q^m-1 \) over \( \mathbb{F}_{q^{2m}} \) providing maximal curves, for the case \( S(x) \in \mathbb{F}_{q^m}[x] \) we explicitly compute the coefficients of \( S(x) \) in Theorem 2 generalizing results in [2]. In Sect. 4 we work with symmetric polynomials \( S(x) \) and generalize results in [15, Theorems 3.4, 3.5, 3.7 and 3.8]; see Remarks 3 and 4.

## 2 Preliminaries

Throughout this paper by a curve we mean a geometrically irreducible and projective curve over a finite field of odd characteristic. For a positive integer \( m \) consider the \( \mathbb{F}_q \)-linearized polynomial of degree \( q^m \)

\[ S(x) = s_0 x + s_1 x^{q} + \cdots + s_m x^{q^m} \in \mathbb{F}_{q^n}[x]. \]

As already mentioned, we investigate curves \( X_S \) as in (1). Such curves have a unique singular point at infinity (which is \( \mathbb{F}_{q^n} \)-rational). Also, there is a unique place centered on it; see for instance [16, Proposition 3.7.10]. This means that the number of \( \mathbb{F}_{q^n} \)-rational points of \( X \) equals the number of degree one places in the corresponding function field. These curves are related with quadratic forms. As a definition, a quadratic form \( Q : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q \) is a map such that

(i) \( Q(ax) = a^2 Q(x) \) for all \( a \in \mathbb{F}_q \) and \( x \in \mathbb{F}_{q^n} \).
(ii) \( B(x, y) = Q(x + y) - Q(x) - Q(y) \) is a bilinear map over \( \mathbb{F}_{q^n} \).

The radical \( W \) associated with the quadratic form \( Q \) is defined as

\[ W = \{ x \in \mathbb{F}_{q^n} : B(x, y) = 0 \text{ for all } y \in \mathbb{F}_{q^n} \}. \]
Note that $W$ is an $\mathbb{F}_{q^n}$-linear subspace of $\mathbb{F}_{q^n}$. Let $w$ be its $\mathbb{F}_{q^n}$-dimension; the integer $n - w$ is called the codimension of the radical.

The quadratic form associated with curves $\mathcal{X}_S$ in (1) is

$$Q_S(x) = \text{Tr}(x S(x)),$$

where $\text{Tr}(\cdot)$ denotes the trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q}$, that is, $\text{Tr}(x) = x + x^q + \cdots + x^{q^{n-1}}$.

Let $N(\mathcal{X}_S)$ be the number of $\mathbb{F}_{q^n}$-rational points of the curve $\mathcal{X}_S$ and $N(Q_S)$ denote the following cardinality

$$N(Q_S) = \left| \left\{ x \in \mathbb{F}_{q^n} \mid Q_S(x) = 0 \right\} \right|.$$

From Hilbert’s Theorem 90 we obtain

$$N(\mathcal{X}_S) = 1 + q N(Q_S),$$

and furthermore by the Hasse-Weil inequality we know that

$$q^n + 1 - 2g(\mathcal{X}_S)\sqrt{q^n} \leq N(\mathcal{X}_S) \leq q^n + 1 + 2g(\mathcal{X}_S)\sqrt{q^n},$$

where $g(\mathcal{X}_S)$ is the genus of $\mathcal{X}_S$.

Recall that a curve is said to be maximal or minimal if the number of its $\mathbb{F}_{q^n}$-rational points attains the upper or the lower bound in Hasse-Weil inequality respectively. In this note we provide examples of linearized polynomials $S(x)$ for which the corresponding curve $\mathcal{X}_S$ is maximal or minimal. Since by [18, Proposition 13.4]

$$N(\mathcal{X}_S) = \begin{cases} 1 + q^n - (q - 1)q^{n-w} & \text{if } n - w \text{ is even}, \\ 1 + q^n & \text{if } n - w \text{ is odd}, \end{cases}$$

and by [16, Proposition 3.7.10] $\mathcal{X}_S$ has genus $g(\mathcal{X}_S) = \frac{q - 1}{2} q^m$ (assuming $s_m \neq 0$), for even $n - w$ the curve $\mathcal{X}_S$ is maximal or minimal over $\mathbb{F}_{q^n}$ if and only if the dimension of the $\mathbb{F}_q$-vector space $W$ is $w = 2m$. In this direction, a useful description of the vector space $W$ is the following.

**Lemma 1** [3, Lemma 2.1] Let $S(x) = s_0 + s_1 x^q + \cdots + s_m x^{q^n} \in \mathbb{F}_{q^n}[x]$ and $Q(x) = \text{Tr}(x S(x))$ be the quadratic form associated to $S(x)$. The elements in the radical $W = \{ x \in \mathbb{F}_{q^n} : B(x, y) = 0 \text{ for all } y \in \mathbb{F}_{q^n} \}$ are the roots in $\mathbb{F}_{q^n}$ of the polynomial

$$\sum_{i=0}^{m-1} s_{m-i} x^{q^i} + 2s_0 x^{q^m} + \sum_{i=1}^{m} s_i x^{q^{m+i}} \in \mathbb{F}_{q^n}[x],$$

and $W$ has dimension at most $2m$.

We conclude this preliminary section with two known results about minimal or maximal curves of type $\mathcal{X}_S$. Although in general it is not easy to establish if $\mathcal{X}_S$ is minimal or maximal, the following results provide some conditions for it.
Proposition 1 [7,15] Let $q$ be a prime power and let $m \geq 1$ be an integer. Consider the curve $\mathcal{X}_S$ over $\mathbb{F}_{q^{2m}}$ defined by
\[
\mathcal{X}_S : \quad y^q - y = x \left( s_0 x + s_1 x^q + \cdots + s_m x^{q^m} \right).
\]
Assume that $s_m \neq 0$ and $\mathcal{X}_S$ is maximal over $\mathbb{F}_{q^{2m}}$. Then $s_0 = s_1 = \cdots = s_{m-1} = 0$ and $s_m + s_m q^m = 0$. The converse holds as well.

Theorem 1 [15] Let $q$ be a power of an odd prime and $k, m$ be positive integers with $m \geq 2k$. Let
\[
S(x) = s_k x^q + s_{k+1} x^{q+k+1} + \cdots + s_{m-k} x^{q^{m-k}} \in \mathbb{F}_{q^{2m}}[x] \quad \text{with} \quad s_k s_{m-k} \neq 0.
\]
Assume that the radical of the quadratic form $\text{Tr}(x S(x))$ has dimension $2m - 2k$ over $\mathbb{F}_q$. Then the curve
\[
\mathcal{X}_S : \quad y^q - y = x S(x)
\]
is a minimal curve over $\mathbb{F}_{q^{2m}}$.

3 Explicit curves from quadratic forms whose radicals have codimension two

We start this section providing a characterization of maximal curves from quadratic forms whose radicals have codimension two over $\mathbb{F}_{q^{2m}}$.

Proposition 2 Let $q$ be a power of an odd prime, $m \geq 2$ be a positive integer and
\[
S(x) = s_0 x + s_1 x^q + \cdots + s_{m-1} x^{q^{m-1}} \in \mathbb{F}_{q^{2m}}[x] \quad \text{with} \quad s_0 s_{m-1} \neq 0.
\]
Assume that the radical of the quadratic form $\text{Tr}(x S(x))$ has dimension $2m - 2$ over $\mathbb{F}_q$. Then the curve
\[
\mathcal{X}_S : \quad y^q - y = x S(x)
\]
is a maximal curve over $\mathbb{F}_{q^{2m}}$ if and only if the following equations are satisfied
\[
\begin{align*}
c^q s_1 &= - \left( c^2 q s_0^q + s_0 \right) \\
c^q s_2 &= - \left( 2 c^q s_0^q + c^{q^2+q} s_1^q + s_1 \right) \\
c^q s_3 &= - \left( c^q s_1^q + c^{q^3+q^2} s_2^q + s_2 \right) \\
& \vdots \\
c^q s_i &= - \left( c^q s_{i-2}^q + c^{q^2+q} s_{i-1}^q + s_{i-1} \right) \\
& \vdots \\
c^q s_{m-1} &= - \left( c^q s_{m-3}^q + c^{q^m-1+q} s_{m-2}^q + s_{m-2} \right)
\end{align*}
\]
and
\[ c^q s^q_{m-2} + c^{q^m + q} s^q_{m-1} + s_{m-1} = 0 \]
\[ c s_{m-1} + (c s_{m-1})^{q^e} = 0 \] (3)
for some \( c \in \mathbb{F}_{q^{2m}} \setminus \{0\} \).

**Proof** Let \( E_1 = \mathbb{F}_{q^{2m}}(x, y) \) with \( y^q - y = x S(x) \) be the function field of \( \mathcal{X}_S \). As the dimension of the radical is \( 2m - 2 \), \( \deg(S(x)) = q^{m-1} \) and \( s_{m-1} \neq 0 \), \( E_1 \) (or equivalently \( \mathcal{X}_S \)) is either maximal or minimal over \( \mathbb{F}_{q^{2m}} \). Using [3, Proposition 5.1] we can construct an extension field \( E_2 \) of \( E_1 \) such that

\[ E_2 \text{ is maximal (minimal)} \iff E_1 \text{ is maximal (minimal)} \]

Moreover an affine equation for \( E_2 \) is also given: \( E_2 = \mathbb{F}_{q^{2m}}(z, t) \) with
\[ t^q - t = z R(z) \]

Here [3, Proposition 5.1] proves the existence of an element \( c \in \mathbb{F}_{q^{2m}} \setminus \{0\} \) such that
\begin{align*}
D(x)^q &= S(x^q + cx) - cs_0 x \\
R(x) &= c S(x^q + cx) + D(x) + cs_0 x^q
\end{align*}

in the polynomial ring \( \mathbb{F}_{q^{2m}}[x] \). Then using (4) we obtain that
\begin{align*}
D(x)^q &= \sum_{i=0}^{m-1} s_i x^{q^{i+1}} + \sum_{i=0}^{m-1} s_i (cx)^{q^i} - cs_0 x \\
R(x) &= c \left( \sum_{i=0}^{m-1} s_i x^{q^{i+1}} + \sum_{i=0}^{m-1} s_i (cx)^{q^i} \right) \\
&\quad + \left( \sum_{i=0}^{m-1} s_i^{(1/q)} x^{q^i} + \sum_{i=1}^{m-1} s_i^{(1/q)} (cx)^{q^{i-1}} \right) + cs_0 x^q.
\end{align*}

Using Proposition 1, \( E_2 \) is maximal if and only if the coefficients of \( R(x) \) satisfies the equations in (2) and (3), which completes the proof. \( \square \)

If we suppose that all the coefficients \( s_i \) of \( S(x) \) are in \( \mathbb{F}_{q^{m}} \) we obtain the explicit classifications in Theorems 2, 3 and 4. These results include the maximal curves obtained in [2] as a special subcase. Also, note that in [2] only the case \( q = p \) (prime case) is considered under the condition that \( \gcd(p, n) = \gcd(p, 2m) = 1 \). Here we have no such condition.

**Theorem 2** Let \( q \) be a power of an odd prime, \( m \geq 2 \) be a positive integer and
\[ S(x) = s_0 x + s_1 x^q + \cdots + s_{m-1} x^{q^{m-1}} \in \mathbb{F}_{q^m}[x] \quad \text{with} \quad s_0 s_{m-1} \neq 0. \]
Then the radical of the quadratic form $\text{Tr}(xS(x))$ has dimension $2m - 2$ over $\mathbb{F}_q$ and the curve

$$\mathcal{X}_S : \quad y^q - y = xS(x)$$

is a maximal curve over $\mathbb{F}_{q^{2m}}$ if and only if $q \equiv 3 \mod 4$, $m$ is odd, $s_0 \in \mathbb{F}_{q^m} \setminus \{0\}$ and for $1 \leq i \leq m - 1$ we have

$$s_i = \begin{cases} 
0 & \text{if } i \text{ is odd}, \\
2s_0^{(q^{i+1})/2} & \text{if } i \text{ is even}.
\end{cases}$$

**Proof** Let $m \geq 2$ and assume the curve $\mathcal{X}_S$ is maximal over $\mathbb{F}_{q^{2m}}$. By (3) in Proposition 2 we know that there exists $c \in F_{q^m} \setminus \{0\}$ satisfying

$$cs_{m-1} + (cs_{m-1})q^{m} = 0.$$ 

Since $s_{m-1} \in F_{q^m} \setminus \{0\}$ we conclude $c + c^{q^m} = 0$. Moreover, using the first equation in (2) we get

$$c^q s_1 + c^{2q} s_0^q + s_0 = 0.$$ 

Taking the powers $q^{m-1}$ and $q^{2m-1}$ respectively and using $s_0, s_1 \in \mathbb{F}_{q^m}$ we obtain that

$$-cs_1^{q^{m-1}} + c^2 s_0 + s_0^{q^{m-1}} = 0,$$

$$cs_1^{q^{m-1}} + c^2 s_0 + s_0^{q^{m-1}} = 0.$$ 

Combining these two equations gives $s_1 = 0$ and $c^2 = -s_0^{q^{m-1}-1}$.

This shows that the case $m = 2$ cannot happen since $s_0 s_{m-1} = s_0 s_1 = 0$. Let us assume $m \geq 3$. For $i = 2$, we have $c^{q^2} s_2 + 2c^q s_0^q + c^{q^2 + q} s_1^q + s_1 = 0$ and for $i = 3, \ldots, m - 1$ we have the equations

$$c^{q^i} s_i + c^{q^{i-2}} s_{i-2}^q + c^{q^{i+1} + q} s_{i-1}^q + s_{i-1} = 0.$$ 

When $q \equiv 3 \mod 4$ we obtain

$$s_i = \begin{cases} 
0 & \text{if } i \text{ is odd}, \\
2s_0^{(q^{i+1})/2} & \text{if } i \text{ is even},
\end{cases}$$

and when $q \equiv 1 \mod 4$

$$s_i = \begin{cases} 
0 & \text{if } i \text{ is odd}, \\
(-1)^i/2 \cdot 2s_0^{(q^{i+1})/2} & \text{if } i \text{ is even}.
\end{cases}$$
where \( i \in \{1, \ldots, m - 1\} \).

Since \( s_{m-1} \neq 0 \), we have \( m - 1 \) is even, so \( m \) must be odd. Moreover, since \( s_{m-2} = 0 \) and \( c^q s_m^2 = -c \), the first equation in (3)

\[
c^q s_{m-2} + c^q s_{m-1}^2 + s_{m-1} = 0
\]
gives us

\[
c^{q+1} = s_{m-1} \Rightarrow (-s_0^{q-1})(q+1) = 2s_0^{(q-1)/2} \Rightarrow (q+1) = 1.
\]

This can happen only when \( q \equiv 3 \pmod{4} \).

Suppose now that \( q \equiv 3 \pmod{4} \), \( m \) is odd and

\[
s_i = \begin{cases} 
0 & \text{if } i \text{ is odd}, \\
2s_0^{(q+1)/2} & \text{if } i \text{ is even}.
\end{cases}
\]

Let

\[
Q(x) = \text{Tr}\left( x \sum_{i=0}^{m-1} s_i x^{q^i} \right).
\]

Then

\[
\text{Tr} (Q(x + y) - Q(x) - Q(y)) = \text{Tr}\left( 2s_0 xy + \sum_{i=1}^{(m-1)/2} s_0^{(q^{2i}+1)/2} (x^{q^{2i}y} + y^{q^{2i}x}) \right)
\]

\[
= \text{Tr}\left( s_0^{(q^{m-1})/2} y^m \sum_{i=0}^{m-1} s_0^{(q^{2i+1})/2} x^{q^{2i+1}} \right)
\]

\[
= \text{Tr}\left( s_0^{(q^{m-1})/2} y^m \sum_{i=0}^{m-1} (sx)^{q^{2i+1}} \right)
\]

where \( s \) is a square root of \( s_0 \) in \( \mathbb{F}_{q^{2m}} \). Using \( (sx)^{q^{2m}} - (sx) = s(x^{q^{2m}} - x) \),

\[
\deg \left( x + x^3 + \cdots + x^{2m-1}, x^{2m-1} \right) = 2m - 2, \text{ and the coefficients } s_i \text{'s come from the Eqs. (2) and (3) of Proposition 2 we get the result.}
\]

\( \square \)

**Remark 1** The maximal curves in Theorem 2 have genus \( q^{m-1}(q - 1)/2 \). By [3, Theorem 6.12] such curves are covered by the corresponding Hermitian curve. Note that subcovers of the Hermitian curves with the same genus could be also obtained using [6, Proposition 3.1].

**Theorem 3** Let \( q \equiv 1 \pmod{4} \) be a power of an odd prime and \( m \geq 2 \) be a positive odd integer. Consider
\[ S(x) = s_0x + s_1x^q + \cdots + s_{m-1}x^{q^{m-1}} \in \mathbb{F}_{q^m}[x] \quad \text{with} \quad s_0s_{m-1} \neq 0 \]

where

\[ s_i = \begin{cases} 0 & \text{if } i \text{ is odd,} \\ 2s_0^{(q^i+1)/2} & \text{if } i \text{ is even} \end{cases} \]

for \( i = 1, \ldots, m-1 \). Then the radical of the quadratic form \( \text{Tr}(xS(x)) \) has dimension \( 2m-2 \) over \( \mathbb{F}_q \) and the curve is a minimal curve over \( \mathbb{F}_{q^{2m}} \).

**Proof** The calculation of the dimension of \( \text{Tr}(xS(x)) \) in Theorem 2 works here too. Since its dimension is \( 2m-2 \) and the curve \( X_S \) is not maximal by Theorem 2, we obtain that \( X_S \) is minimal. \[ \square \]

**Theorem 4** Let \( q \equiv 1 \pmod{4} \) be a power of an odd prime, \( m \geq 2 \) be a positive even integer and

\[ S(x) = s_0x + s_1x^q + \cdots + s_{m-1}x^{q^{m-1}} \in \mathbb{F}_{q^m}[x] \quad \text{with} \quad s_0s_{m-1} \neq 0, \]

where

\[ s_i = \begin{cases} 0 & \text{if } i \text{ is odd,} \\ s_1^{(q^i+1)/(q+1)} & \text{if } i \text{ is even} \end{cases} \]

for \( i = 0, \ldots, m-1 \). Then the radical of the quadratic form \( \text{Tr}(xS(x)) \) has dimension \( 2m-2 \) over \( \mathbb{F}_q \) and the curve is a minimal curve over \( \mathbb{F}_{q^{2m}} \).

**Proof** Let

\[ Q(x) = \text{Tr}\left( x \sum_{i=0}^{m-1} s_i x^{q^i} \right). \]

Then

\[
\text{Tr}\left( Q(x + y) - Q(x) - Q(y) \right) = \text{Tr}\left( \sum_{i=1}^{m/2} s_1^{(q^{2i-1}+1)/(q+1)} (x^{q^{2i-1}} y + x y^{q^{2i-1}}) \right)
\]

\[
= \text{Tr}\left( s_1^{(q^m-1)/(q+1)} y q^{m} \sum_{i=0}^{m-1} s_1^{(q^{2i+1}+1)/(q+1)} x^{q^{2i+1}} \right)
\]

\[
= \text{Tr}\left( s_1^{(q^m-1)/(q+1)} x y q^{m} \sum_{i=0}^{m-1} (s x)^{q^{2i+1}} \right)
\]

with fixing \( s \) a \((q + 1)\)-th root of \( s_1 \) in \( \mathbb{F}_{q^{2m}} \). Since \((s x)^{q^{2m}} - (s x) = s (x^{q^{2m}} - x)\) and \( \deg \left( x + x^3 + \cdots + x^{2m-1}, x^{2m} - 1 \right) = 2m - 2 \), we have the result. \[ \square \]
4 Maximal or minimal curves from symmetric polynomials

In this section we provide some constructions of maximal or minimal curves using certain symmetric polynomials. We consider an integer \( r \geq 1 \), a divisor \( k \) of \( n \), and a polynomial \( f(x) \) such that

\[
f(x) = \sum_{i=0}^{2r} a_i x^i \in \mathbb{F}_q[x], \quad f(x) \mid x^k - 1, \quad \text{and } a_{r-i} = a_{r+i} \forall i = 1, \ldots, r. \tag{5}
\]

**Theorem 5** Let \( n \geq 2 \) be even and \( k \equiv 2 \pmod{4} \) a divisor of \( n/2 \). Let

\[
G(x) = \sum_{i=1}^{r} a_{r+i} x^{q^{k/2-i}} + a_r x^{q^{k/2}} + \sum_{i=1}^{r} a_{r+i} x^{q^{k/2+i}}.
\]

Then the curve \( X_{f,k} \) defined by the affine equation

\[
y^q - y = xS(x) = x \sum_{j=0}^{\frac{n}{2}-1} G(x)^q \]

is minimal over \( \mathbb{F}_{q^n} \).

**Proof** The genus of the curve \( \mathcal{X}_{f,k} \) is \( g = \frac{n-1}{2} q^{\frac{n-k}{2}+r} \). For \( w \) the \( \mathbb{F}_q \)-dimension of the radical \( W \) associated to the quadratic form \( Q(x) = \text{Tr}(xS(x)) \) we have: \( \mathcal{X}_S \) is minimal or maximal over \( \mathbb{F}_{q^n} \) if and only if \( w = n - k + 2r \). We have

\[
W = \left\{ x \in \mathbb{F}_{q^n} : \sum_{j=0}^{\frac{n}{2}-1} G(x)^q \right\} = \left\{ x \in \mathbb{F}_{q^n} : \sum_{j=0}^{\frac{n}{2}-1} \left( a_r x^{q^r} + \sum_{i=1}^{r} \left( a_{r-i} x^{q^{r-i}} + a_{r+i} x^{q^{r+i}} \right) \right)^q = 0 \right\}.
\]

Therefore the corresponding associated polynomial to

\[
\sum_{j=0}^{\frac{n}{2}-1} \left( a_r x^{q^r} + \sum_{i=1}^{r} \left( x^{q^{r-i}} + x^{q^{r+i}} \right) \right)^q
\]
is
\[ f(x)(1 + x^k + x^{2k} + \cdots + x^{n-k}) \]
and \(\deg \left( (\gcd \left( f(x)(1 + x^k + x^{2k} + \cdots + x^{n-k}), x^n - 1 \right) \right) = n - k + 2r = w. This shows that the curve \(X_{f,k}\) is either maximal or minimal over \(\mathbb{F}_{q^n}\). Since the highest and the lowest powers in \(S(x)\) are \(q^{n-k}x^r\) and \(q^{k-r}\), by Theorem 1 we conclude that \(X_{f,k}\) is minimal. \(\square\)

Now we construct a family of curves over \(\mathbb{F}_{q^n}\) that are either maximal or minimal over \(\mathbb{F}_{q^n}\). We omit the proof since it is very similar to the proof of Theorem 5.

**Theorem 6** Let \(4 \leq n = (2s + 1)k\) be even. Let
\[
G(x) = \frac{a_r}{2} x + \sum_{i=1}^{r} a_{r+i} x^{q^i},
\]
\[
\tilde{G}(x) = \sum_{i=1}^{r} a_{r-i} x^{q^{k-i}} + a_r x^{q^k} + \sum_{i=1}^{r} a_{r+i} x^{q^{k+i}}.
\]
Then the curve \(X_{f,k}\) of affine equation \(y^q - y = x \left( \sum_{j=0}^{n-k-1} \left( \tilde{G}(x) \right)^{q^j} \right) + xG(x)\) is either maximal or minimal.

The next proposition provides some simple examples of polynomials \(f(x)\) satisfying conditions in (5).

**Proposition 3** Let \(r, s, k \geq 1\) be integers. The following polynomials \(f(x)\) satisfy conditions in (5).

(i) \(f(x) = \sum_{i=0}^{2r} x^i\), where \(2r + 1 \mid k\).
(ii) \(f(x) = \sum_{i=0}^{2r} (-1)^i x^i\), where \(2(2r + 1) \mid k\).
(iii) \(f(x) = \sum_{i=0}^{2r/s} x^{is}\), where \(s \mid r\) and \(s(2r + 1) \mid k\).
(iv) \(f(x) = \sum_{i=0}^{2r/s} (-1)^i x^{is}\), where \(s \mid r\) and \(2s(2r + 1) \mid k\).
(v) \(f(x) = x^{2r} + \left( \sum_{i=2}^{2r-2} x^i \right) + 1\), where \(s = \begin{cases} 6, & r \equiv 0, 1 \pmod{3} \\ 2, & r \equiv 2 \pmod{3} \end{cases}\) and \(s(2r - 1) \mid k\).
(vi) \(f(x) = x^{2r} + \left( \sum_{i=2}^{2r-2} (-1)^i x^i \right) + 1\), where \(s = \begin{cases} 6, & r \equiv 0, 1 \pmod{3} \\ 2, & r \equiv 2 \pmod{3} \end{cases}\) and \(s(2r - 1) \mid k\).

**Proof** The first four statements follow immediately from the factorization of \(x^k - 1\). The last two items are proved as follows.

(v) We have that \(f(x) = x^{2r} + \left( \sum_{i=2}^{2r-2} x^i \right) + 1 = (1 + x + x^2 + \cdots + x^{2r-2}) (x^2 - x + 1). Suppose r \equiv 0, 1 \pmod{3}, then 6(2r - 1) \mid k. Since x^{6(2r-1)} - 1 divides x^k - 1 it is enough to show that \(f(x) \mid x^{6(2r-1)} - 1. We have that
\[ x^{6(2r-1)} - 1 = (x^{2r-1} - 1) \left( 1 + x^{2r-1} + x^{2(2r-1)} + x^{3(2r-1)} + x^{4(2r-1)} + x^{5(2r-1)} \right) \]
\[ = (x - 1) (1 + x + x^2 + \cdots + x^{2r-2}) \left( 1 + x^{2r-1} + x^{2(2r-1)} \right) \left( 1 + x^3 \right) \]
\[ \cdot \left( 1 - x^3 + x^6 - \cdots + x^{3(2r-1)-3} \right) \]
and \( f(x) \mid x^{6(2r-1)} - 1 \). Suppose now \( r \equiv 2 \pmod{3} \) then \( 3 \mid 2r - 1, 2(2r - 1) \mid k \). Since \( x^{2(2r-1)} - 1 \) divides \( x^k - 1 \) it is enough to show that \( f(x) \mid x^{2(2r-1)} - 1 \).

We have that
\[ x^{2(2r-1)} - 1 = (x^{2r-1} - 1)(x^{2r-1} + 1) = (x - 1)(1 + x + \cdots + x^{2r-2})(1 + x^3)(1 - x^3 + \cdots + x^{2r-1-3}) \]
and \( f(x) \mid x^{2(2r-1)} - 1 \).

(vi) We have that
\[ f(x) = x^{2r} + \left( \sum_{i=2}^{2r-2} (-1)^i x^i \right) + 1 = (1 - x + x^2 - \cdots + x^{2r-2})(x^2 + x + 1). \]

Suppose \( r \equiv 0, 1 \pmod{3} \) and therefore \( 6(2r-1) \mid k \). Since \( x^{6(2r-1)} - 1 \) divides \( x^k - 1 \) it is enough to show that \( f(x) \mid x^{6(2r-1)} - 1 \). We can write
\[ x^{6(2r-1)} - 1 = (x^{3(2r-1)} - 1)(x^{3(2r-1)} + 1) = (x^3 - 1)(1 + x^3 + \cdots + x^{3(2r-1)-3})(x + 1) \]
\[ \cdot (1 - x + x^2 - \cdots + x^{2r-2})(x^{2(2r-1)} - x^{2r-1} + 1) \]
and \( f(x) \mid x^{6(2r-1)} - 1 \). Suppose now \( r \equiv 2 \pmod{3} \) then \( 3 \mid 2r - 1, 2(2r - 1) \mid k \). Since \( x^{2(2r-1)} - 1 \) divides \( x^k - 1 \) it is enough to show that \( f(x) \mid x^{2(2r-1)} - 1 \).

We have that
\[ x^{2(2r-1)} - 1 = (x^{2r-1} - 1)(x^{2r-1} + 1) = (x^3 - 1)(1 + x^3 + \cdots + x^{2r-1-3})(x + 1)(1 - x + \cdots + x^{2r-2}) \]
and \( f(x) \mid x^{2(2r-1)} - 1 \).

□

Another interesting family of symmetric polynomials over \( \mathbb{F}_p \) satisfying Condition (5) is provided by the cyclotomic polynomials. Assume that \( d \) is not divisible by the characteristic \( p \) of \( \mathbb{F}_q \). The \( d \)-th cyclotomic polynomial \( \Phi_d(x) \) over \( \mathbb{F}_q \) is defined as
\[ \Phi_d(x) = \prod_{\gcd(s,d) = 1}^d (x - \xi^s), \]

where \( \xi \) is a primitive \( d \)th root of unity over \( \mathbb{F}_q \). In particular \( \Phi_d(x) \) is always a divisor of \( x^d - 1 \), but not necessarily irreducible over \( \mathbb{F}_q \). The following are well-known results about cyclotomic polynomials (see for example [8]).

(i) The cyclotomic polynomial \( \Phi_d(x) \in \mathbb{F}_p [x], \) where \( \gcd(d, p) = 1 \).

(ii) Let \( d > 1 \) coprime to \( p \) and \( \Phi_d(x) = \sum_{k=0}^{\phi(d)} a_k x^k \). Then \( a_{\phi(d) - i} = a_i \) for all \( 0 \leq i \leq \phi(d) \).

For \( \Phi_d(x) = \sum_{k=0}^{\phi(d)} a_k x^k \) we define \( \varphi_d(x) = \sum_{k=0}^{\phi(d)} a_k x^{q^k} \).

**Theorem 7** Let \( k \) be a positive even integer and \( d \) be a positive divisor of \( k \) which is bigger than 2. Then the curve

\[ \mathcal{X} : y^q - y = x \sum_{j=0}^{n-1} \varphi_d(x)^{a + kj} \]

is minimal over \( \mathbb{F}_{q^n} \) where \( n \) divisible by \( 2k \) and \( \phi(d) + 2a = k \).

**Proof** By Lemma 1 we have

\[ W = \left\{ x \in \mathbb{F}_{q^n} \mid \sum_{j=0}^{n-1} (\varphi(x))^{q^k} = 0 \right\}. \]

Therefore the corresponding associated polynomial to \( \sum_{j=0}^{n-1} (\varphi(x))^{q^j} \) is

\[ \Phi_d(x)(1 + x^k + \cdots + x^{n-k}) \]

and \( \deg \gcd(\Phi_d(x)(1 + x^k + \cdots + x^{n-k}), x^n - 1) = n - k + \phi(d) = n - 2a \). Now the result follows from Theorem 1. \( \Box \)

**Remark 3** Theorem 7 includes the explicit classes of minimal curves given in [15, Theorem 3.4 and Theorem 3.5]. If we use \( \phi_2(x) = x^2 - x + 1 \), that is, \( \varphi_2(x) = x^{-2} - x + x \), then Theorem 7 reduces to [15, Theorem 3.4]. Furthermore, if we use \( \phi_4(x) = x^2 + x + 1 \), that is, \( \varphi_4(x) = x^{q^2} + x^q + x \), then Theorem 7 reduces to [15, Theorem 3.5].

**Theorem 8** Let \( k \) be a positive even integer and \( d \geq 2 \) a divisor of \( k \). Then the curve

\[ \mathcal{X} : y^q - y = x \sum_{j=0}^{n-k-1} \varphi_d(x)^{q^{a+kj}} + x \sum_{i=0}^{\phi(d)-1} c_i x^{q^{\phi(d)-i}} + \frac{c_\phi(d)/2}{x^2} \]

is minimal over \( \mathbb{F}_{q^{2n}} \) where \( n \equiv k \mod 2k, n > k \) and \( \phi(d) + 2a = 2k \).
Proof} By Lemma 1 we have

\[ W = \left\{ x \in \mathbb{F}_{q^n} \mid \sum_{j=0}^{n-1} (\varphi(x))^{q^kj} = 0 \right\}. \]

Therefore the corresponding associated polynomial to \( \sum_{j=0}^{n-1} (\varphi(x))^{q^kj} \) is

\[ \Phi_d(x)(1 + x^k + \cdots + x^{n-k}) \]

and \( \deg \gcd (\Phi_d(x)(1 + x^k + \cdots + x^{n-k}), x^n - 1) = n - k + \phi(d) = n - k + \phi(d) \). Since \( W \subset \mathbb{F}_{q^n} \) and the dimension of \( W \) over \( \mathbb{F}_q \) is even, \( \mathcal{X} \) is maximal or minimal over \( \mathbb{F}_{q^n} \) and hence it is minimal over \( \mathbb{F}_{q^{2n}} \). \( \square \)

Remark 4 Theorem 8 includes the explicit classes of minimal curves given in [15, Theorem 3.7 and Theorem 3.8]. Similar to Remark 3 if we use \( \phi_2(x) = x^2 - x + 1 \) and \( \phi_4(x) = x^2 + x + 1 \), then Theorem 8 reduces to the minimal curves given in [15, Theorem 3.7] and [15, Theorem 3.8] respectively.

Acknowledgements Research of the first author partially supported by Ministry for Education, University and Research of Italy (MIUR) (Project PRIN 2012 Geometrie di Galois e strutture di incidenza-Prot. N.2012XZE22K_005) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA-INdAM). Research of the fourth author supported by Science Foundation Ireland Grant 13/IA/1914. The authors would like to thank the anonymous reviewer for his/her useful comments.

References

1. Anbar, N., Meidl, W.: More on quadratic functions and maximal Artin–Schreier curves. Appl. Algebra Eng. Commun. Comput. 26(5), 409–426 (2015)
2. Anbar, N., Meidl, W.: Quadratic functions and maximal Artin–Schreier curves. Finite Fields Appl. 30, 49–71 (2014)
3. Çakçak, E., Özbudak, F.: Some Artin–Schreier type function fields over finite fields with prescribed genus and number of rational places. J. Pure Appl. Algebra 210(1), 113–135 (2007)
4. Fitzgerald, R.W.: Highly degenerate quadratic forms over finite fields of characteristic 2. Finite Fields Appl. 11, 165–181 (2005)
5. Fitzgerald, R.W.: Highly degenerate quadratic forms over over \( \mathbb{F}_2 \). Finite Fields Appl. 13, 778–792 (2007)
6. Garcia, A., Stichtenoth, H., Xing, C.: On subfields of the Hermitian function field. Compos. Math. 120, 137–170 (2000)
7. Güneri, C.: Artin-Schreier curves and weights of two-dimensional cyclic codes. Finite Fields Appl. 10(4), 481–505 (2004)
8. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1997)
9. McGuire, G., Yılmaz, E.S.: Divisibility of L-polynomials for a family of Artin–Schreier curves. J. Pure Appl. Algebra 223(8), 3341–3358 (2019)
10. Niederreiter, H., Xing, C.: Rational Points on Curves over Finite Fields: Theory and Applications. Cambridge University Press, Cambridge (2001)
11. Niederreiter, H., Xing, C.: Algebraic Geometry in Coding Theory and Cryptography. Princeton University Press, Princeton (2009)
12. Özbudak, F., Saygı, E., Saygı, Z.: Quadratic forms of codimension 2 over certain finite fields of even characteristic. Cryptogr. Commun. 3, 241–257 (2011)
13. Özbudak, F., Saygı, E., Saygı, Z.: Quadratic forms of codimension 2 over finite fields containing $\mathbb{F}_4$ and Artin–Schreier type curves. Finite Fields Appl. 18, 396–433 (2012)

14. Özbudak, F., Saygı, Z.: On the number of quadratic forms having codimension 2 radicals in characteristic 2 giving maximal/minimal curves. Commun. Algebra 42(9), 3795–3810 (2014)

15. Özbudak, F., Saygı, Z.: Explicit maximal and minimal curves over finite fields of odd characteristics. Finite Fields Appl. 42, 81–92 (2016)

16. Stichtenoth, H.: Algebraic Function Fields and Codes. Springer, Berlin (2009)

17. Tsfasman, M.A., Vladut, S.G., Nogin, D.: Algebraic Geometric Codes: Basic Notions. American Mathematical Society, Providence (2007)

18. Van Der Geer, G., Van Der Vlugt, M.: Reed–Muller codes and supersingular curves. I. Compos. Math. 84(3), 333–367 (1992)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.