Explicit Maximal and Minimal Curves over Finite Fields of Odd Characteristics

Ferruh Ozbudak, Zülfükar Saygı

Explicit Maximal and Minimal Curves over Finite Fields of Odd Characteristics

Ferruh Özbudak[1,2] and Zülfükar Saygı[3]

[1] Department of Mathematics, Middle East Technical University,
Dumlupınar Bul., No:1, 06800, Ankara, Turkey
[2] Institute of Applied Mathematics, Middle East Technical University,
Dumlupınar Bul., No:1, 06800, Ankara, Turkey
[3] Department of Mathematics, TOBB University of Economics and Technology,
Söğütözü 06530, Ankara, Turkey
ozbudak@metu.edu.tr,zsaygi@etu.edu.tr

Abstract. In this work we present explicit classes of maximal and minimal Artin–Schreier type curves over finite fields having odd characteristics. Our results include the proof of Conjecture 5.9 given in [1] as a very special subcase. We use some techniques developed in [2], which were not used in [1] at all.

Keywords: Algebraic curves, Rational points, Maximal curves, Minimal curves.

1 Introduction

Algebraic curves over finite fields have various applications in coding theory, cryptography, quasi-random numbers and related areas (see, for example, [6, 7, 11, 12]). For these applications it is important to know the number of rational points of the curve. Throughout this paper by a curve we mean a smooth, geometrically irreducible and projective curve over a finite field of odd characteristic.

Let p be an odd prime, e be a positive integer, $q = p^e$ and n be a positive integer. Let $\mathbb{F}_{q^n}$ denote the finite field with q^n elements. Let $h \geq 0$ and

$$S(x) = s_0 x + s_1 x^q + \cdots + s_h x^{q^h} \in \mathbb{F}_{q^n}[x]$$

be an $\mathbb{F}_q$-linearized polynomial of degree q^h in $\mathbb{F}_{q^n}[x]$. We consider the Artin-Schreier type curves χ given by

$$\chi : \quad y^q - y = xS(x) = \sum_{i=0}^{h} s_i x^{q^i+1}. \tag{1}$$

These curves are related with the quadratic forms

$$Q(x) = \mathrm{Tr}(xS(x)) \tag{2}$$

where Tr denote the trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. Let $N(Q)$ denote the cardinality

$$N(Q) = |\{x \in \mathbb{F}_{q^n} \mid \mathrm{Tr}\,(xS(x)) = 0\}|$$

and let $N(\chi)$ be the number of $\mathbb{F}_{q^n}$ rational points of the curve χ. Then using Hilbert's Theorem 90 we have

$$N(\chi) = 1 + qN(Q),$$

and hence determining $N(\chi)$ is the same as determining $N(Q)$. Note that in general, it is difficult to determine $N(\chi)$. For the number $N(\chi)$, the Hasse-Weil inequality states that

$$q^n + 1 - 2g(\chi)\sqrt{q^n} \leq N(\chi) \leq q^n + 1 + 2g(\chi)\sqrt{q^n}$$

where $g(\chi)$ is the genus of χ. We know that there exist curves attaining the Hasse-Weil bounds. If the upper bound is attained then the curve is called a maximal curve and if the lower bound is attained then the curve is called a minimal curve. Here we note that using [11, Proposition 3.7.10] the genus of the curve χ in (1) is $g(\chi) = \dfrac{(q-1)q^h}{2}$.

Using the relations between the curve χ in (1) and the quadratic form Q in (2) some characterizations and classification results on maximal and minimal curves are obtained in [3, 4, 8–10] for the curves over finite fields with even characteristics. Also using similar relations some results are obtained for the curves over finite fields with odd characteristics in [1]. Furthermore for all integers $n \equiv 0 \mod 12$ and for all primes p, $5 \leq p \leq 29$ with $\gcd(p, n) = 1$ the following conjecture is given in [1, Conjecture 5.9].

Conjecture 1. [1] Let $p > 3$ be an odd prime and let n be an integer relatively prime to p and divisible by 12. Then the curve χ over $\mathbb{F}_{p^n}$ defined by

$$\chi: \quad y^p - y = x \sum_{j=0}^{\frac{n}{12}-1} \left(x^{p^4} - x^{p^3} + x^{p^2} \right)^{p^{6j}}$$

is a minimal curve.

Similar observations and discussions are also given in the last section of [1]. In this paper we prove a much more stronger version of the conjecture above. We also give explicit classes of many other maximal and minimal curves. We use some techniques developed in [2], which were not used in [1] at all.

2 Preliminaries

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

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

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

is a bilinear map over $\mathbb{F}_{q^n}$.

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

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

Let w be the $\mathbb{F}_q$-dimension of W. By codimension of the radical we mean the difference $n - w$.

The following result was proven in [5] using some tools from algebraic geometry. Here we give a different proof using only elementary tools. We will use the following proposition later.

Proposition 1. *Let q be a prime power and $m \geq 1$ be an integer. Consider the curve χ over $\mathbb{F}_{q^{2m}}$ defined by*

$$\chi: \quad y^q - y = x \left(a_0 x + a_1 x^q + \cdots + a_m x^{q^m} \right).$$

Assume that $a_m \neq 0$ and χ is maximal over $\mathbb{F}_{q^{2m}}$. Then $a_0 = a_1 = \cdots = a_{m-1} = 0$ and $a_m + a_m{}^{q^m} = 0$. The converse holds as well.

Proof. As $a_m \neq 0$, the genus of χ is $\frac{(q-1)q^m}{2}$ and hence it has $1 + q^{2m+1}$ many rational points in $\mathbb{F}_{q^{2m}}$. By Hilbert's Theorem 90 this means that

$$\mathrm{Tr}\left(x \left(a_0 x + a_1 x^q + \cdots + a_m x^{q^m} \right) \right) = 0 \quad \text{for all } x \in \mathbb{F}_{q^{2m}},$$

where Tr is the trace from $\mathbb{F}_{q^{2m}}$ to $\mathbb{F}_q$.

Let $I \subseteq \{0, 1, \ldots, m-1\}$ be the subset consisting of $0 \leq i \leq m-1$ with $a_i \neq 0$. Assume that $I \neq \emptyset$. For each $i \in I$ and $0 \leq \ell \leq 2m-1$ let $n_{i,\ell}$ be the integer

$$0 \leq n_{i,\ell} \leq q^{2m} - 1 \quad \text{with} \quad n_{i,\ell} \equiv q^{(i+1)\ell} \mod (q^{2m} - 1).$$

Note that $1, q+1, \ldots, q^{m-1}+1, q^m+1$ are in distinct q-cyclotomic cosets modulo $(q^{2m}-1)$. Hence there exists a polynomial $H(T) \in \mathbb{F}_{q^{2m}}[T]$ defined as

$$H(T) = \left(a_m + a_m{}^{q^m}\right) T^{q^m+1} + \sum_{i \in I} \sum_{\ell=0}^{2m-1} a_i^{q^\ell} T^{n_{i,\ell}},$$

such that $H(x) = 0$ for all $x \in \mathbb{F}_{q^{2m}}$. If $H(T)$ is not the zero polynomial we get a contradiction as $H(T)$ has degree strictly less that $q^{2m}-1$ and has q^{2m} distinct zeroes. This implies that $I = \emptyset$ and $a_m + a_m{}^{q^m} = 0$. The converse holds trivially. □

3 Main results

In this section we state and prove our results. Note that in the proof of the following theorem we use the notion of function fields. The theory of algebraic curves is essentially equivalent to the theory of function fields. For a brief survey of the relations between algebraic curves and function fields we refer to [11, Appendix B].

Theorem 1. *Let q be a power of an odd prime and $m \geq 2$ be an integer. Let*

$$S(x) = a_1 x^q + \cdots + a_{m-1} x^{q^{m-1}} \in \mathbb{F}_{q^{2m}}[x] \quad \textit{with} \quad a_1 a_{m-1} \neq 0.$$

Assume that the radical of the quadratic form $\mathrm{Tr}(xS(x))$ has dimension $2m-2$ over $\mathbb{F}_q$. Then the curve

$$\chi : \quad y^q - y = xS(x)$$

is a minimal curve over $\mathbb{F}_{q^{2m}}$.

Proof. Let $\mathbb{E}_1 = \mathbb{F}_{q^{2m}}(x, y)$ with $y^q - y = xS(x)$ be the function field of χ. As the dimension of the radical is $2m-2$ and $a_{m-1} \neq 0$, it is rather well known that $\mathbb{E}_1$ (or equivalently χ) is either maximal or minimal over $\mathbb{F}_{q^{2m}}$ (see, for example, [2]). Using [2, Proposition 5.1] we obtain that an extension field $\mathbb{E}_2$ of $\mathbb{E}_1$ such that

$$\mathbb{E}_2 \text{ is maximal (minimal)} \Leftrightarrow \mathbb{E}_1 \text{ is maximal (minimal)}.$$

Moreover an affine equation for $\mathbb{E}_2$ is also given: $\mathbb{E}_2 = \mathbb{F}_{q^{2m}}(z, t)$ with

$$t^q - t = zR(z).$$

Here [2, Proposition 5.1] proves existence of $c \in \mathbb{F}_{q^{2m}}^*$ such that

$$\begin{aligned} D(x)^q &= S(x^q + cx) \quad \text{and} \\ R(x) &= cD(x)^q + D(x) \end{aligned} \tag{3}$$

in the polynomial ring $\mathbb{F}_{q^{2m}}[x]$. Put

$$R(x) = b_0 x + b_1 x^q + \cdots + b_m x^{q^m}.$$

Using (3) we obtain that

$$b_0 = (c^q a_1)^{1/q} \neq 0.$$

If $\mathbb{E}_2$ is maximal, then $b_0 = 0$ by Proposition 1. Hence $\mathbb{E}_2$ and $\mathbb{E}_1$ are minimal, which completes the proof. □

Using a similar idea we prove the following

Theorem 2. *Let q be a power of an odd prime and $m \geq 4$ be an integer. Let*

$$S(x) = a_2 x^{q^2} + \cdots + a_{m-2} x^{q^{m-2}} \in \mathbb{F}_{q^{2m}}[x] \quad \textit{with} \quad a_2 a_{m-2} \neq 0.$$

Assume that the radical of the quadratic form $\mathrm{Tr}(xS(x))$ has dimension $2m-4$ over $\mathbb{F}_q$. Then the curve

$$\chi : \quad y^q - y = xS(x)$$

is a minimal curve over $\mathbb{F}_{q^{2m}}$.

Generalizing the technique in the above theorems we have the following result.

Theorem 3. *Let q be a power of an odd prime and k, m be positive integers with $m \geq 2k$. Let*

$$S(x) = a_k x^{q^k} + a_{k+1} x^{q^{k+1}} + \cdots + a_{m-k} x^{q^{m-k}} \in \mathbb{F}_{q^{2m}}[x] \quad \textit{with} \quad a_k a_{m-k} \neq 0.$$

Assume that the radical of the quadratic form $\mathrm{Tr}(xS(x))$ has dimension $2m-2k$ over $\mathbb{F}_q$. Then the curve

$$\chi : \quad y^q - y = xS(x)$$

is a minimal curve over $\mathbb{F}_{q^{2m}}$.

Using the above theorems we obtain the following explicit class of minimal curves. Note that this result includes [1, Conjecture 5.9].

Theorem 4. *Let q be a power of an odd prime and let n be an integer divisible by 12. Then the curve χ over $\mathbb{F}_{q^n}$ defined by*

$$\chi : \quad y^q - y = x \sum_{j=0}^{\frac{n}{12}-1} \left(x^{q^4} - x^{q^3} + x^{q^2} \right)^{q^{6j}}$$

is a minimal curve.

Proof. We have

$$S(x) = \sum_{j=0}^{\frac{n}{12}-1} \left(x^{q^4} - x^{q^3} + x^{q^2} \right)^{q^{6j}}.$$

Then the radical W of the quadratic form $\mathrm{Tr}(xS(x))$ becomes

$$\begin{aligned} W &= \left\{ x \in \mathbb{F}_{q^n} \mid \sum_{j=0}^{\frac{n}{12}-1} \left(\left(x^{q^4} - x^{q^3} + x^{q^2} \right)^{q^{6j}} + \left(x^{q^{-4}} - x^{q^{-3}} + x^{q^{-2}} \right)^{q^{-6j}} \right) = 0 \right\} \\ &= \left\{ x \in \mathbb{F}_{q^n} \mid \sum_{j=0}^{\frac{n}{6}-1} \left(x^{q^2} - x^q + x \right)^{q^{6j}} = 0 \right\}. \end{aligned}$$

Then the corresponding q-associate of $\sum_{j=0}^{\frac{n}{6}-1} \left(x^{q^2} - x^q + x \right)^{q^{6j}}$ becomes

$$\left(x^2 - x + 1 \right) \left(1 + x^6 + x^{12} + \cdots + x^{n-6} \right).$$

As $12|n$ and $x^n - 1 = (x^6 - 1)\left(1 + x^6 + x^{12} + \cdots + x^{n-6}\right)$ we have

$$\deg\left(\gcd\left(x^n - 1, \left(x^2 - x + 1\right)\left(1 + x^6 + x^{12} + \cdots + x^{n-6}\right)\right)\right) = n - 4,$$

which means that $\dim_{\mathbb{F}_q} W = n - 4$. Then we complete the proof using Theorem 2. □

Using Theorem 2 and similar observation as in the proof of Theorem 4 we obtain the following result.

Theorem 5. *Let q be a power of an odd prime and let n be an integer divisible by 12. Then the curve χ over $\mathbb{F}_{q^n}$ defined by*

$$\chi: \quad y^q - y = x \sum_{j=0}^{\frac{n}{12}-1} \left(x^{q^4} + x^{q^3} + x^{q^2}\right)^{q^{6j}}$$

is a minimal curve.

In the following theorems we obtain maximal and minimal curves depending on the characteristic of the finite fields. We observe that the results are true for all odd primes of the form $p \equiv 1 \mod 6$ and $p = 3$.

Theorem 6. *Let $n = 6$ and $p = 3$ or p is a prime satisfying $p \equiv 1 \mod 6$. Then the curve χ over $\mathbb{F}_{p^n}$ defined by*

$$\chi: \quad y^p - y = x\left(-2x^p + x\right)$$

is a minimal curve if $p \equiv 1 \mod 4$ and a maximal curve if $p \equiv 3 \mod 4$.

Proof. Let $S(x) = -2x^p + x$ and $c \in \mathbb{F}_p$ is a root of $c^2 - c + 1 = 0$. Note that $c^2 - c + 1 = 0$ has roots $c_1 = \frac{1+\sqrt{-3}}{2}$ and $c_2 = \frac{1-\sqrt{-3}}{2}$ in $\mathbb{F}_p$, since -3 is a quadratic residue as $p \equiv 1 \mod 6$. Then define

$$\begin{aligned} D(x)^p &= S(x^p + cx) - cx \\ &= -2x^{p^2} + (1-2c)x^p. \end{aligned}$$

Then we have $D(x) = -2x^p + (1-2c)x$. Now define

$$\begin{aligned} R(x) &= cS(x^p + cx) + D(x) + cx^p \\ &= -2cx^{p^2} - cx. \end{aligned}$$

Then the radical of $\mathrm{Tr}(xR(x))$ becomes

$$\begin{aligned} W_R &= \left\{x \in \mathbb{F}_{p^6} \mid (-2c)^{p^2} x^{p^4} - 2cx^{p^2} - 2cx = 0\right\} \\ &= \left\{x \in \mathbb{F}_{p^6} \mid x^{p^4} + x^{p^2} + x = 0\right\}. \end{aligned}$$

Corresponding p-associate becomes $t^4 + t^2 + 1$ and as $\deg\left(\gcd\left(t^6 - 1, t^4 + t^2 + 1\right)\right) = 4$ we obtain that $\dim W_R = 4$.

Now we will use the same scenario. Assume that $S_1(x) = 2x^{p^2} + x$. Then define

$$\begin{aligned} D_1(x)^p &= S_1(x^p + c_1 x) - c_1 x \\ &= 2x^{p^3} + 2c_1^{p^2} x^{p^2} + x^p. \end{aligned}$$

Then we have $D_1(x) = 2x^{p^2} + 2c_1^p x^p + x$. Now define

$$\begin{aligned} R_1(x) &= c_1 S_1(x^p + c_1 x) + D_1(x) + c_1 x^p \\ &= 2c_1 x^{p^3} + 2\left(c_1^{p^2+1} + 1\right)x^{p^2} + 2\left(c_1^p + c_1\right)x^p + (c_1^2 + 1)x. \end{aligned}$$

Then we know that the curve $y^p - y = xR_1(x)$ is maximal if and only if the following system has a solution in $\mathbb{F}_{p^6}$ (see Proposition 1):

$$\begin{aligned} (2c_1) + (2c_1)^{p^3} &= 0 \\ c_1^{p^2+1} + 1 &= 0 \\ c_1^p + c_1 &= 0 \\ c_1^2 + 1 &= 0. \end{aligned}$$

Note that this system has a solution in $\mathbb{F}_{p^6}$ if and only if -1 is a quadratic nonresidue modulo p, that is, $p \equiv 3 \mod 4$. □

Similarly we obtain the following result.

Theorem 7. *Let $n = 6$ and $p = 3$ or p is a prime satisfying $p \equiv 1 \mod 6$. Then the curve χ over $\mathbb{F}_{p^n}$ defined by*

$$\chi : \quad y^p - y = x\left(2x^p + x\right)$$

is a minimal curve if $p \equiv 1 \mod 4$ and a maximal curve if $p \equiv 3 \mod 4$.

Remark 1. In the proof of Theorem 1 we have used [2, Proposition 5.1], which guarantees the existence of $c \in \mathbb{F}_{q^{2m}}^*$ such that

$$\begin{aligned} D(x)^q &= S(x^q + cx) \quad \text{and} \\ R(x) &= cD(x)^q + D(x). \end{aligned}$$

Now we want to give explicit c's for our Theorem 4. Assume that $q = p \equiv 1 \mod 6$ and $n = 12$. Let

$$S(x) = x^{p^4} - x^{p^3} + x^{p^2}.$$

Then let us define

$$D(x)^p = S(x^p + cx) = x^{p^5} - x^{p^4} + x^{p^3} + (cx)^{p^4} - (cx)^{p^3} + (cx)^{p^2}$$

which gives

$$D(x) = x^{p^4} - x^{p^3} + x^{p^2} + (cx)^{p^3} - (cx)^{p^2} + (cx)^p.$$

Also define

$$\begin{aligned} R(x) &= cD(x)^p + D(x) \\ &= c\left(x^{p^5} - x^{p^4} + x^{p^3} + (cx)^{p^4} - (cx)^{p^3} + (cx)^{p^2}\right) + x^{p^4} - x^{p^3} + x^{p^2} + (cx)^{p^3} - (cx)^{p^2} + (cx)^p \\ &= cx^{p^5} + \left(c^{p^4+1} - c + 1\right)x^{p^4} + \left(2c - c^{p^3+1} - 1\right)x^{p^3} + \left(c^{p^2+1} - c + 1\right)x^{p^2} + c^p x^p. \end{aligned}$$

We know that $x^2 - x + 1 = 0$ has roots in $\mathbb{F}_p$, since -3 is a quadratic residue as $p \equiv 1 \mod 6$. If we take $c \in \mathbb{F}_p$ as a root of $x^2 - x + 1 = 0$ then $c^{p^4+1} - c + 1 = c^{p^2+1} - c + 1 = 0$. Therefore we have

$$\begin{aligned} R(x) &= cx^{p^5} + \left(2c - c^{p^3+1} - 1\right)x^{p^3} + c^p x^p \\ &= c\left(x^{p^5} + x^{p^3} + x^p\right) \end{aligned}$$

since $c^p = c$ and $c^{p^3+1} = c^2$. Then the radical of $\mathrm{Tr}(xR(x))$ becomes

$$\begin{aligned} W &= \left\{x \in \mathbb{F}_{q^{12}} \mid x^{p^5} + x^{p^3} + x^p + x^{p^{-5}} + x^{p^{-3}} + x^{p^{-1}} = 0\right\} \\ &= \left\{x \in \mathbb{F}_{q^{12}} \mid x^{p^{10}} + x^{p^8} + x^{p^6} + x + x^{p^2} + x^{p^4} = 0\right\}. \end{aligned}$$

Corresponding p-associate becomes

$$t^{10} + t^8 + t^6 + t^4 + t^2 + 1 = \left(t^4 + t^2 + 1\right)\left(t^6 + 1\right),$$

which means that $\dim W = 10$.

Note that the same technique is also works for $n > 12$ for the case $q = p \equiv 1 \mod 6$.

References

1. N. Anbar, W. Meidl, *Quadratic functions and maximal Artin-Schreier curves*, Finite Fields Appl. 30 (2014) 49–71.
2. E. Çakçak, F. Özbudak, *Some Artin-Schreier type function fields over finite fields with prescribed genus and number of rational places*, J. Pure Appl. Algebra 210 (2007) 113–135.
3. R. W. Fitzgerald, *Highly degenerate quadratic forms over finite fields of characteristic 2*, Finite Fields Appl. 11 (2005) 165–181.
4. R. W. Fitzgerald, *Highly degenerate quadratic forms over over* $\mathbb{F}_2$, Finite Fields Appl. 13 (2007) 778–792.
5. C. Güneri, Artin-Schreier curves and weights of two-dimensional cyclic codes. Finite Fields Appl. 10(4) (2004) 481–505.
6. H. Niederreiter, C. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge Univ. Press, Cambridge, 2001.
7. H. Niederreiter, C. Xing, *Algebraic Geometry in Coding Theory and Cryptography*, Princeton Univ. Press, Princeton, 2009.
8. F. Özbudak, E. Saygı, Z. Saygı, *Quadratic forms of codimension 2 over certain finite fields of even characteristic*, Cryptogr. Commun. 3 (2011) 241–257.
9. F. Özbudak, E. Saygı, Z. Saygı, *Quadratic forms of codimension 2 over finite fields containing* $\mathbb{F}_4$ *and ArtinSchreier type curves*, Finite Fields Appl. 18 (2012) 396–433.
10. F. Özbudak, Z. Saygı, *On the Number of Quadratic Forms Having Codimension 2 Radicals in Characteristic 2 Giving Maximal/Minimal Curves*, Communications in Algebra 42(9) (2014) 3795–3810.
11. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 2009.
12. M.A. Tsfasman, S.G. Vladut, D. Nogin, *Algebraic Geometric Codes: Basic Notions* American Mathematical Society, Providence, 2007.