Max-Planck-Institut für Mathematik
Bonn

Quadratic functions and Artin-Schreier curves in odd characteristic

by

Nurdagül Anbar

Max-Planck-Institut für Mathematik
Preprint Series 2014 (36)

Quadratic functions and Artin-Schreier curves in odd characteristic

Nurdagül Anbar

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

MPIM 14-36

QUADRATIC FUNCTIONS AND ARTIN-SCHREIER CURVES IN ODD CHARACTERISTIC

MPIM Preprint by Nurdagül Anbar
nurdagulanbar2@gmail.com

1. Abstract

For an odd prime p and an even integer n with $\gcd(n,p) > 1$, we consider quadratic functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ of codimension k. For various values of k, we obtain classes of quadratic functions giving rise to maximal and minimal Artin-Schreier curves over $\mathbb{F}_{p^n}$. We completely classify all maximal and minimal curves obtained from quadratic functions of codimension 2 and coefficients in the prime field $\mathbb{F}_p$. These results complement earlier results in [1] for the case that $\gcd(n,p) = 1$. This is a joint work with Wilfried Meidl.

2. Introduction

In this article we consider the Artin-Schreier cover of the $\mathbb{F}_{p^n}$-projective line given by

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1} \quad \text{with} \quad a_i \in \mathbb{F}_{p^n} \ , \tag{2.1}$$

where $\lfloor m \rfloor$ denotes the integer part of the real number m. The genus $g(\mathcal{X})$ of $\mathcal{X}$ is $\frac{(p-1)p^l}{2}$, where l is the largest integer with $a_l \neq 0$, see (see Proposition 3.7.8 in [20]). By the Hasse-Weil bound, the number of rational points $N(\mathcal{X})$ of $\mathcal{X}$ satisfies

$$1 + p^n - 2g(\mathcal{X})p^{\frac{n}{2}} \leq N(\mathcal{X}) \leq 1 + p^n + 2g(\mathcal{X})p^{\frac{n}{2}} \ ,$$

i.e.

$$1 + p^n - (p-1)p^{\frac{n+2l}{2}} \leq N(\mathcal{X}) \leq 1 + p^n + (p-1)p^{\frac{n+2l}{2}} \ . \tag{2.2}$$

The curve is called maximal (respectively minimal) if it attains the upper (respectively lower) bound in (2.2).

By Hilbert's Theorem 90, the number of rational points $N(\mathcal{X})$ of $\mathcal{X}$ is given by

$$N(\mathcal{X}) = 1 + pN_0(Q) \ ,$$

where $N_0(Q)$ is the number of solutions of $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}) = 0$ and $\mathrm{Tr_n}(z)$ is the absolute trace of $z \in \mathbb{F}_{p^n}$.

As we will see, the determination of $N_0(Q)$ requires the exact evaluation of the character sum

$$\sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{\mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})} \ , \tag{2.3}$$

called the Walsh coefficient of $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$ at 0. Only a few character sums of the form (2.3) have been determined explicitly. In [12, 5] the character sum (2.3) is determined for monomials $Q(x) = \mathrm{Tr_n}(ax^{p^i+1})$ for an odd prime p. Using these results, all maximal and minimal curves of the form $y^p - y = ax^{p^i+1}$ are classified. Some more results are known for $p = 2$, see [6, 10, 11, 14, 18, 19]. Moreover, results on the distribution of character sum can be found in [2, 8, 9].

In the recent paper [1], some more classes of character sums of the form (2.3) for odd primes p with $\gcd(n, p) = 1$ and coefficients a_i in the prime field have been evaluated, which induce some more classes of minimal and maximal curves. We summarize the main results of [1] in the following two propositions. By $v(m)$ we denote the 2-adic valuation of an integer m.

Proposition 2.1. *Let n be an even integer with $\gcd(n, p) = 1$, and let k be an even divisor of n. The curve $\mathcal{X}$ over $\mathbb{F}_{p^n}$ given by*

$$\mathcal{X} : y^p - y = c(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1}), \quad c \in \mathbb{F}_p^*$$

is maximal if and only if $p \equiv 3 \mod 4$ and $n \equiv 2 \mod 4$, and minimal if and only if $v(k) = v(n)$ and $p \equiv 1 \mod 4$, or $v(k) = v(n)$, $p \equiv 3 \mod 4$ and $n \equiv 0 \mod 4$.
The curve $\mathcal{X}$ over $\mathbb{F}_{p^n}$ given by

$$\mathcal{X} : y^p - y = c(x^{p^{\frac{k}{2}}+1} + x^{p^{\frac{3k}{2}}+1} + \cdots + x^{p^{\frac{n-k}{2}}+1}), \quad c \in \mathbb{F}_p^*$$

is minimal if and only if $v(k) < v(n)$ (and never maximal).

Using the results of Proposition 2.1, in [1] all maximal and minimal curves over $\mathbb{F}_{p^n}$ of the form (2.1) with coefficients in the prime field $\mathbb{F}_p$, p odd, and genus $\frac{p-1}{2}p^{(n-2)/2}$ have been classified under the assumption that $\gcd(p, n) = 1$. We can state the result as follows.

Proposition 2.2. *Let n be an even integer with $\gcd(n, p) = 1$, and let $\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1} =: \mathcal{Q}(x)$ be a curve of genus $g(\mathcal{X}) = \frac{p-1}{2}p^{(n-2)/2}$, where coefficients a_i lie in the prime field $\mathbb{F}_p$. Then $\mathcal{X}$ is maximal over $\mathbb{F}_{p^n}$ if and only if*

- *$n \equiv 2 \bmod 4$, $p \equiv 3 \bmod 4$, and $\mathcal{Q}(x) = c(x^2 + 2x^{p^2+1} + \cdots + 2x^{p^{\frac{n}{2}-1}+1})$, $c \in \mathbb{F}_p^*$,*

and $\mathcal{X}$ is minimal over $\mathbb{F}_{p^n}$ if and only if

- *$n \equiv 2 \mod 4$, $p \equiv 1 \bmod 4$, and $\mathcal{Q}(x) = c(x^2 + 2x^{p^2+1} + \cdots + 2x^{p^{\frac{n}{2}-1}+1})$, $c \in \mathbb{F}_p^*$, or*
- *$n \equiv 0 \mod 4$, and $\mathcal{Q}(x) = c(x^{p+1} + x^{p^3+1} + \cdots + x^{p^{\frac{n}{2}-1}+1})$, $c \in \mathbb{F}_p^*$.*

In all proofs in [1] the condition $\gcd(n, p) = 1$ plays a central role. The objective of this article is to analyze the analog curves for the more complicated case that $\gcd(n, p) > 1$.

In Section 3 we present some results on the *Walsh transform* of quadratic functions, which will be needed in the sequel. In Section 4 we relate the number of points of a curve of the form (2.1) to the Walsh coefficient at zero of the corresponding quadratic function. In Section 5 we present some new classes of maximal and minimal curves of the form (2.1) for the case that

$\gcd(n,p) > 1$. In particular, combining with the results in [1] on the case $\gcd(n,p) = 1$, we classify all maximal and minimal curves of the form (2.1) obtained from quadratic functions of codimension 2 whose coefficients lie in the prime field $\mathbb{F}_p$.

3. Quadratic functions and Walsh transform

Let n be an integer and let p be an odd prime. Omitting linear and constant terms, a quadratic function Q, i.e. a function of algebraic degree 2, from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ can be represented in trace form as

$$Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}) \tag{3.1}$$

with $a_0, \dots, a_{\lfloor n/2 \rfloor} \in \mathbb{F}_{p^n}$. If n is odd, this representation is unique. Observing that $x^{p^{n/2}+1} \in \mathbb{F}_{p^{n/2}}$, we obtain that $\mathrm{Tr}_n(a_{n/2} x^{p^{n/2}+1}) = \mathrm{Tr}_{n/2}(x^{p^{n/2}+1} \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^{n/2}}}(a_{n/2}))$. Consequently, if n is even, then the coefficient $a_{n/2}$ is only unique modulo the group $G = \{a \in \mathbb{F}_{p^n} \mid \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^{n/2}}}(a) = 0\}$. In this article we are interested in curves of the form (2.1) obtained from quadratic functions Q, which attain the Hasse-Weil bound (2.2). In particular, we are only interested in the case that n is even.

For a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, an element $a \in \mathbb{F}_{p^n}$ for which the derivative $D_a f(x) = f(x + a) - f(x)$ is constant is called a *linear structure* of f. The set Ω of the linear structures of f is a subspace of $\mathbb{F}_{p^n}$ called the *linear space* of f, see [15, 21]. As easily seen, for all $a \in \Omega$ and $x \in \mathbb{F}_{p^n}$, we have $f(x + a) = f(x) + f(a) - f(0)$. In particular, f is linear on Ω if $f(0) = 0$.

The Walsh coefficient $\widehat{Q}(b)$ of Q at the value $b \in \mathbb{F}_{p^n}$ is the character sum

$$\widehat{Q}(b) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(x) - \mathrm{Tr_n}(bx)} \ , \quad \epsilon_p = e^{2\pi i/p} \ .$$

As well known, every quadratic function Q from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is s-plateaued, i.e. for all $b \in \mathbb{F}_{p^n}$ we have $\widehat{Q}(b) = 0$ or $|\widehat{Q}(b)| = p^{\frac{n+s}{2}}$ for a fixed integer $0 \le s < n$, depending on Q. This integer s is exactly is the dimension (over $\mathbb{F}_p$) of the *linear space* Ω of Q, see [3].

The linear space of a quadratic function (3.1) is the kernel (in $\mathbb{F}_{p^n}$) of the linearized polynomial (cf. [12, 13])

$$L(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i} + a_i^{p^{n-i}} x^{p^{n-i}} \ .$$

Consequently $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is s-plateaued if and only if

$$\deg(\gcd(L(x), x^{p^n} - x)) = p^s \ . \tag{3.2}$$

If all coefficients a_i of $Q(x)$ are in the prime field $\mathbb{F}_p$, then then the linearized polynomial corresponding to Q is

$$L(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i} + a_i x^{p^{n-i}} \tag{3.3}$$

with the *p-associate*

$$A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^i + a_i x^{n-i} \ . \tag{3.4}$$

Using the concept of the p-associate we can then facilitate the determination of s in Equation 3.2 as

$$s = \deg(\gcd(A(x), x^n - 1)) \ ,$$

see also [1, 13, 17]. We observe that $A(x) = x^d h(x)$ for a non-negative integer d and a self-reciprocal polynomial h of degree $n-2d$. Consequently, if $A(x)$ is the associate of a linearized polynomial corresponding to an s-plateaued function Q with coefficients in $\mathbb{F}_p$, then

$$\begin{aligned} \gcd(A(x), x^n - 1) \quad &= \quad \frac{x^n - 1}{f(x)} \ , \\ \text{with} \qquad & f(x) = (x-1)^{\delta}(1 + b_1 x + \cdots + b_1 x^{n-s-1-\delta} + x^{n-s-\delta}) \ , \ \delta \in \{0,1\} \ . \end{aligned}$$

The polynomial $A(x)$ can then be written as

$$\begin{aligned} A(x) \quad &= \quad (x-1)^{(1-\delta)} \frac{x^n - 1}{f(x)} g(x) \ , \\ \text{where} \qquad & g(x) = c_0 + c_1 x + \cdots + c_1 x^{n-s-2+\delta} + c_0 x^{n-s-1+\delta} \text{ with } \gcd(f(x), g(x)) = 1 \ . \end{aligned} \tag{3.5}$$

An important notion for functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is *extended affine equivalence (EA-equivalence)*. Two functions f, g from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ are called EA-equivalent if there exist a linearized permutation polynomial $\mathcal{P}(x)$, a linearized polynomial $\mathcal{L}(x)$ and constants $a, e \in \mathbb{F}_p$, $d \in \mathbb{F}_{p^n}$ such that $g(x) = af(\mathcal{P}(x) + d) + \mathcal{L}(x) + e$.

In the framework of the isomorphic vector space $\mathbb{F}_p^n$, the Walsh transform of a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is given by

$$\widehat{f}(b) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f(x) - b \cdot x} \ , \quad b \in \mathbb{F}_p^n \ ,$$

where $b \cdot x$ denotes the dot product in $\mathbb{F}_p^n$. In this framework two functions f, g from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ are EA-equivalent if there exist an invertible $n \times n$-matrix P over $\mathbb{F}_p$, elements $\mathbf{u}, \mathbf{v} \in \mathbb{F}_p^n$ and constants $a, e \in \mathbb{F}_p$ such that $g(\mathbf{x}) = af(P\mathbf{x} + \mathbf{u}) + \mathbf{v} \cdot \mathbf{x} + e$ for all $\mathbf{x} \in \mathbb{F}_p^n$.

It is well known that Walsh spectrum (value set of the Walsh transform) and algebraic degree are invariant under EA-equivalence. In particular affine coordinate transformations do not change the Walsh spectrum. More precisely, the effect of coordinate transformations is given as follows.

T1: $f(\widehat{\mathbf{x} + \mathbf{u}})(\mathbf{b}) = \epsilon_p^{\mathbf{b} \cdot \mathbf{u}} \widehat{f}(\mathbf{b})$, T2: if $P \in \mathrm{GL}_n(\mathbb{F}_p)$ then $\widehat{f(P\mathbf{x})}(\mathbf{b}) = \widehat{f}((P^{-1})^T\mathbf{b})$, where P^T denotes the transpose of the matrix P.

4. Walsh transform and the number of points

Objective in this section is to relate the number of rational points $N(\mathcal{X})$ of $\mathcal{X}$ given as in (2.1) to the Walsh coefficient $\widehat{Q}(0)$ of $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$ at 0. This will be used in Section 5 to obtain some classes of maximal and minimal curves. We choose here a different approach than in [1] based on character sums. We first show that for odd p a quadratic function Q without an affine term satisfies $\widehat{Q}(0) = \zeta p^{(n+s)/2}$ for some $\zeta \in \{1, -1, i, -i\}$. In particular this shows $\widehat{Q}(0) \neq 0$.

Lemma 4.1. *For an integer n and an odd prime p, let $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$, $a_i \in \mathbb{F}_{p^n}$. Then*

$$\widehat{Q}(0) = \begin{cases} \pm p^{\frac{n+s}{2}} & \text{if } n-s \text{ even, or } n-s \text{ odd and } p \equiv 1 \bmod 4, \\ \pm i p^{\frac{n+s}{2}} & \text{if } n-s \text{ odd and } p \equiv 3 \bmod 4 \end{cases}$$

for some integer $0 \le s \le n-1$.

Proof. We may consider the isomorphic vector space $\mathbb{F}_p^n$. Any quadratic function (without a linear or constant term) from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ can be transformed by an affine coordinate transformation to a diagonal form

$$Q(x) = d_1 x_1^2 + \cdots + d_{n-s} x_{n-s}^2$$

for some integer $0 \le s \le n-1$, and $d_i \neq 0$ for $i = 1, \ldots, n-s$, see [16, Section 6.2]. By Properties T1 and T2, an affine coordinate transformation does not change the Walsh coefficient at 0. For the function $q(x) = dx^2$ on $\mathbb{F}_p$, by [16, Theorem 5.33] and [16, Theorem 5.15] we have

$$\widehat{Q}(0) = \sum_{x \in \mathbb{F}_p} \epsilon_p^{dx^2} = \eta(d) G(\eta, \chi_1) = \begin{cases} \eta(d) p^{\frac{1}{2}} & \text{if } p \equiv 1 \bmod 4, \\ \eta(d) i p^{\frac{1}{2}} & \text{if } p \equiv 3 \bmod 4, \end{cases} \tag{4.1}$$

where χ_1 is the canonical additive character of $\mathbb{F}_p$, η denotes the quadratic character of $\mathbb{F}_p$, and $G(\eta, \chi_1)$ is the associated Gaussian sum. This shows the correctness for $n = 1$.
For two functions $g_1 : \mathbb{F}_p^m \to \mathbb{F}_p$ and $g_2 : \mathbb{F}_p^n \to \mathbb{F}_p$, the direct sum $g_1 \oplus g_2$ from $\mathbb{F}_p^n \times \mathbb{F}_p^m = \mathbb{F}_p^{m+n}$ to $\mathbb{F}_p$ is defined by $(g_1 \oplus g_2)(x, y) = g_1(x) + g_2(y)$. As easily seen,

$$\widehat{(g_1 \oplus g_2)}(u, v) = \widehat{g_1}(u) \widehat{g_2}(v) \ . \tag{4.2}$$

The assertion for arbitrary n follows then from (4.1), applying (4.2) recursively to $q_i(x_i) = d_i x_i^2$, $1 \le i \le n$, together with the simple observation that for $n-s+1 \le i \le n$, where $d_i = 0$, we have $\widehat{q_i}(0) = p$. $\square$

Let $f \in \mathbb{F}_{p^n}[x]$, and let m be an integer with $\gcd(m,n)=t$. Then, following the arguments in [7], for the number $N(f)$ of solutions $(x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ of $y^{p^m} - y = f(x)$ we have

$$\begin{aligned} p^n N(f) &= \sum_{a,x,y\in\mathbb{F}_{p^n}} \epsilon_p^{\mathrm{Tr_n}(a(f(x)-(y^{p^m}-y)))} = \sum_{a,x\in\mathbb{F}_{p^n}} \epsilon_p^{\mathrm{Tr_n}(af(x))} \sum_{y\in\mathbb{F}_{p^n}} \epsilon_p^{\mathrm{Tr_n}(ay-ay^{p^m})} \\ &= \sum_{a,x\in\mathbb{F}_{p^n}} \epsilon_p^{\mathrm{Tr_n}(af(x))} \sum_{y\in\mathbb{F}_{p^n}} \epsilon_p^{\mathrm{Tr_n}(y^{p^m}(a^{p^m}-a))} = p^n \sum_{a\in\mathbb{F}_{p^t}} \sum_{x\in\mathbb{F}_{p^n}} \epsilon_p^{\mathrm{Tr_n}(af(x))} , \end{aligned} \tag{4.3}$$

where in the last step we used that $a^{p^m} - a$ vanishes if and only if $a \in \mathbb{F}_{p^t} = \mathbb{F}_{p^m} \cap \mathbb{F}_{p^n}$. We use Equation 4.3 to express the number of rational points over $\mathbb{F}_{p^n}$ of a curve

$$\mathcal{X} : y^q - y = \sum_{i=0}^{l} a_i x^{q^i+1} , \quad a_i \in \mathbb{F}_{p^n} , 0 \le i \le l ,$$

with $q = p^m$ for any divisor m of n. In the proof of the subsequent Theorem we will use the following Lemma, see [4, Theorem 1].

Lemma 4.2. *For a divisor m of n and $q = p^m$, a quadratic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ of the form $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/(2m)\rfloor} b_i x^{q^i+1})$, $b_i \in \mathbb{F}_q$, is s-plateaued for an integer $0 \le s < n$ which is divisible by m. For a nonzero element $a \in \mathbb{F}_q$, the function $Q_a(x)$ given by $Q_a(x) = \mathrm{Tr}_n(a\sum_{i=0}^{\lfloor n/(2m)\rfloor} b_i x^{q^i+1})$ is also s-plateaued with the same integer s, and*

$$\widehat{Q_a}(b) = \mu(a)^{\frac{n-s}{m}} \widehat{Q}(b) , \quad b \in \mathbb{F}_{p^n} ,$$

where μ denotes the quadratic character in $\mathbb{F}_q$.

Theorem 4.3. *For an odd prime p and a divisor m of n let $q = p^m$, and let $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{l} a_i x^{q^i+1})$, $lm \le n/2$, be an s-plateaued quadratic function from $\mathbb{F}_{p^n} \to \mathbb{F}_p$. Set $k := \frac{n-s}{m}$. Then the number of rational points of*

$$\mathcal{X} : y^q - y = \sum_{i=0}^{l} a_i x^{q^i+1}$$

over $\mathbb{F}_{p^n}$ is given by

$$N(\mathcal{X}) = 1 + pN_0(Q) = \begin{cases} 1 + p^n + (q-1)\widehat{Q}(0) & \textit{if } k \textit{ is even,} \\ 1 + p^n & \textit{if } k \textit{ is odd.} \end{cases}$$

Proof. Let $N(Q)$ be the number of solutions in $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ of $y^q - y = \sum_{i=0}^{l} a_i x^{q^i+1}$, and hence $N(\mathcal{X}) = 1 + N(Q)$. Denoting the set of nonzero squares in $\mathbb{F}_q$ by Sq and the set of non-squares in $\mathbb{F}_q$ by NSq, by Equation 4.3 we have

$$N(Q) = \sum_{a\in\mathbb{F}_{p^m}} \sum_{x\in\mathbb{F}_{p^n}} \epsilon_p^{Q_a(x)} = p^n + \sum_{a\in Sq} \widehat{Q_a}(0) + \sum_{a\in NSq} \widehat{Q_a}(0).$$

First suppose that $k = \frac{n-s}{m}$ is even. Then by Lemma 4.2 we have $\widehat{Q_a}(0) = \widehat{Q}(0)$ for all $a \ne 0$. Consequently, $N(Q) = p^n + (q-1)\widehat{Q}(0)$ and the statement for k even follows.

If $k = \frac{n-s}{m}$ is odd, then again by Lemma 4.2, $\widehat{Q_a}(0) = \widehat{Q}(0)$ if a is a nonzero square in $\mathbb{F}_p$, and $\widehat{Q_a}(0) = -\widehat{Q}(0)$ if a is a non-square in $\mathbb{F}_p$. Hence $N(Q) = p^n$. □

Combining Lemma 4.1 and Theorem 4.3 we get the next corollary.

Corollary 4.4. *For an odd prime p and a divisor m of n, let $q = p^m$, and let $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{l} a_i x^{q^i+1})$, $lm \le n/2$, be an s-plateaued quadratic function from $\mathbb{F}_{p^n} \to \mathbb{F}_p$. The number of $\mathbb{F}_{p^n}$-rational points of the curve*

$$\mathcal{X} : y^q - y = \sum_{i=0}^{l} a_i x^{q^i+1}$$

is given by

$$N(\mathcal{X}) = \begin{cases} 1 + p^n + \Lambda(p^m - 1)p^{\frac{n+s}{2}} & \text{if } (n-s)/m \text{ is even,} \\ 1 + p^n & \text{if } (n-s)/m \text{ is odd,} \end{cases}$$

where

$$\Lambda = \begin{cases} 1 & \text{if } \widehat{Q}(0) = p^{\frac{n+s}{2}}, \\ -1 & \text{if } \widehat{Q}(0) = -p^{\frac{n+s}{2}}. \end{cases}$$

Remark 4.5. Lemma 4.1 implies that $\widehat{Q}(0) \neq 0$ if p is odd and Q does not contain a linear term. However, if the quadratic function contains a linear term, then we may have $\widehat{Q}(0) = 0$, i.e. the function Q is balanced. In this case $N(\mathcal{X}) = 1 + p^n$.

Since we are particularly interested in maximal (respectively minimal) curves $\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}$ of the form (2.1), we consider quadratic functions $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ with even n. The subsequent corollary describes the conditions on Q required to obtain maximal (respectively minimal) curves.

Corollary 4.6. *Let $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$ be an s-plateaued quadratic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, and suppose that $l \le n/2$ is the largest integer for which a_l is non-zero. Then*

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}$$

is a maximal (respectively minimal) curve over $\mathbb{F}_{p^n}$ if and only if n is even, $s = 2l$ and $\Lambda = 1$ (respectively $\Lambda = -1$).

Proof. The statement follows from Corollary 4.4 and Inequality 2.2 with $g(\mathcal{X}) = \frac{p-1}{2} p^l$. □

Remark 4.7. If $\mathcal{X}$ is maximal or minimal, then the dimension s of the linear space of Q must be even.

Corollary 4.8. *Let $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{n/2} a_i x^{p^i+1})$ be an s-plateaued function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, and set $k := n - s$. The curve $\mathcal{X} : y^p - y = \sum_{i=0}^{n/2} a_i x^{p^i+1}$ over $\mathbb{F}_{p^n}$ is maximal or minimal if and only if*

$$a_{\frac{n}{2}} = a_{\frac{n}{2}-1} = \cdots = a_{\frac{n-k}{2}+1} = 0 \;\; \text{and} \;\; a_{\frac{n-k}{2}} \neq 0 \; .$$

Proof. The statement follows from Corollary 4.6 with $l = \frac{n-k}{2}$. $\square$

We remark that $a_{\frac{n}{2}} = a_{\frac{n}{2}-1} = \cdots = a_{\frac{n-k}{2}+1} = 0$ together with the Hasse-Weil bound already implies $a_{\frac{n-k}{2}} \neq 0$.

5. Maximal and minimal curves

In this section we consider curves over $\mathbb{F}_{p^n}$ of the form $\mathcal{X} : y^p - y = \sum a_i x^{p^i+1}$ with coefficients a_i in the prime field $\mathbb{F}_p$ and $\gcd(n,p) > 1$. Our results complement the results of [1], where similar curves for the easier case that $\gcd(n,p) = 1$ have been considered. We first completely characterize all maximal and minimal curves obtained from quadratic functions $Q(x) = \mathrm{Tr_n}(\sum a_i x^{p^i+1})$ of codimension 2, i.e. quadratic functions with linear space of dimension $s = n-2$. Then we presents some more infinite classes of maximal and minimal curves of various genus, i.e. curves obtained from quadratic functions of various codimension.

We start with a lemma which excludes many curves from being maximal or minimal. The proof of the lemma is also given implicitly in the proof of Theorem 5.5 in [1] on curves obtained from quadratic functions of codimension 2.

Lemma 5.1. *Let $\mathcal{X} : y^p - y = \sum_{i=0}^{l} a_i x^{p^i+1}$ with coefficients in the prime field $\mathbb{F}_p$ and $l \leq n/2$. Let $A(x)$ be the p-associate* (3.4) *of the linearized polynomial* (3.3) *of $Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{l} a_i x^{p^i+1})$. If the curve $\mathcal{X}$ over $\mathbb{F}_{p^n}$ is maximal or minimal, then*

$$\gcd(A(x), x^n - 1) = \frac{x^n - 1}{f(x)}$$

for a polynomial $f(x)$ with $f(1) = 0$.

Proof. Let $\gcd(x^n - 1, A(x)) = (x^n - 1)/f(x)$ for a polynomial $f(x)$ of (even) degree k, which is not divisible by $x - 1$. Then

$$A(x) = (x-1)\frac{x^n - 1}{f(x)} g(x)$$

with

$$f(x) = b_0 + b_1 x + \cdots + b_1 x^{k-1} + b_0 x^k, \quad g(x) = c_0 + c_1 x + \cdots + c_1 x^{k-2} + c_0 x^{k-1} \in \mathbb{F}_p[x]$$

and $\gcd(f(x), g(x)) = 1$. Consequently, we have the following equality.

$$A(x)(b_0 + b_1 x + \cdots + b_1 x^{k-1} + b_0 x^k) = (x^{n+1} - x^n - x + 1)(c_0 + c_1 x + \cdots + c_1 x^{k-2} + c_0 x^{k-1}) \tag{5.1}$$

By Corollary 4.8, the corresponding curve is maximal or minimal if and only if

$$A(x) = a_0 + a_1 x + \cdots + a_{\frac{n-k}{2}} x^{\frac{n-k}{2}} + a_{\frac{n-k}{2}} x^{\frac{n+k}{2}} + \cdots + a_1 x^{n-1} + a_0 x^n \ \text{ with } \ a_{\frac{n-k}{2}} \neq 0 \ .$$

Comparing the coefficients of $x^{\frac{n+k}{2}}$ in Equality 5.1, we then obtain that

$$2a_{\frac{n-k}{2}} b_0 = 0 \ .$$

Since $f(x)$ has degree k and $a_{\frac{n-k}{2}} \neq 0$, we get a contradiction. □

We consider now quadratic functions $Q(x)$ (with coefficients in the prime field $\mathbb{F}_p$) of codimension 2, i.e. the associate $A(x)$ of the corresponding linearized polynomial satisfies $\gcd(A(x), x^n-1) = (x^n-1)/f(x)$ for a polynomial $f(x)$ of degree 2.

Theorem 5.2. *Let p be an odd prime with $\gcd(n,p) > 1$, and let $Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{l} a_i x^{p^i+1})$ be a quadratic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ with coefficients in $\mathbb{F}_p$, for which the linear space has dimension $n-2$. The curve $\mathcal{X} : y^p - y = \sum_{i=0}^{l} a_i x^{p^i+1}$ over $\mathbb{F}_{p^n}$ is maximal if and only if*

- $\mathcal{X} : y^p - y = c(x^2 + 2x^{p^2+1} + \cdots + 2x^{p^{\frac{n}{2}-1}+1})$, $c \in \mathbb{F}_p^*$, $n \equiv 2 \bmod 4$ *and* $p \equiv 3 \bmod 4$.

The curve $\mathcal{X} : y^p - y = \sum_{i=0}^{l} a_i x^{p^i+1}$ over $\mathbb{F}_{p^n}$ is minimal if and only if

- $\mathcal{X} : y^p - y = c(x^2 + 2x^{p^2+1} + \cdots + 2x^{p^{\frac{n}{2}-1}+1})$, $c \in \mathbb{F}_p^*$, $n \equiv 2 \mod 4$ *and* $p \equiv 1 \bmod 4$, *or*
- $\mathcal{X} : y^p - y = c(x^{p+1} + x^{p^3+1} + \cdots + x^{p^{\frac{n}{2}-1}+1})$, $c \in \mathbb{F}_p^*$ *and* $n \equiv 0 \mod 4$.

Proof. By Lemma 5.1, $\gcd(A(x), x^n-1) = (x^n-1)/f(x)$ for a quadratic polynomial $f(x)$ which is divisible by $x-1$. Hence we must have $f(x) = x^2-1$. By (3.5), the polynomial $A(x)$ is then of the form

(a) $A(x) = cx\frac{x^n-1}{x^2-1}$ for some $c \in \mathbb{F}_p^*$, or
(b) $A(x) = c\frac{x^n-1}{x^2-1}(x^2+ax+1)$ for some $a \neq \pm 2$ and $c \in \mathbb{F}_p^*$.

First we consider the case (a). In this case

$$A(x) = \begin{cases} c(x^{n-1} + x^{n-3} + \cdots + x^{n/2+2} + x^{n/2} + x^{n/2-2} + \cdots + x^3 + x) & \text{if } n \equiv 2 \mod 4 \\ c(x^{n-1} + x^{n-3} + \cdots + x^{n/2+1} + x^{n/2-1} + \cdots + x^3 + x) & \text{if } n \equiv 0 \mod 4, \end{cases}$$

and hence the corresponding quadratic function is given by

$$Q(x) = \begin{cases} \mathrm{Tr}_n\left(c(x^{p+1} + x^{p^3+1} + \cdots + x^{p^{n/2-2}+1} + (1/2)x^{p^{n/2}+1})\right) & \text{if } n \equiv 2 \mod 4 \\ \mathrm{Tr}_n\left(c(x^{p+1} + x^{p^3+1} + \cdots + x^{p^{n/2-1}+1})\right) & \text{if } n \equiv 0 \mod 4. \end{cases}$$

By Corollary 4.8, we obtain a maximal or minimal curve from $Q(x)$ only for $n \equiv 0 \bmod 4$. To determine whether the resulting curve is maximal or minimal, we have to calculate $\widehat{Q}(0)$ explicitly, for $Q(x) = \mathrm{Tr}_n(c(x^{p+1} + x^{p^3+1} + \cdots + x^{p^{n/2-1}+1}))$. We note by Lemma 4.2 the sign in $\widehat{Q}(0)$ is independent from the constant $c \in \mathbb{F}_p^*$ since $n-2$ is even. We therefore may without loss of generality choose $c = 1$. Then the linearized polynomial corresponding to Q is given by

$$L(x) = x^{p^{n-1}} + x^{p^{n-3}} + \cdots + x^{p^{n/2+1}} + x^{p^{n/2-1}} + \cdots + x^{p^3} + x^p .$$

Since we suppose that $\gcd(n,p) > 1$, we put $n = mp^e$, $e \geq 1$, and $\gcd(p,m) = 1$. Then we can write $L(x)$ as

$$\begin{aligned} L(x) &= \sum_{k=0}^{(m-2)/2} x^{p^{1+2kp^e}} + x^{p^{3+2kp^e}} + \cdots + x^{p^{2p^e-1+2kp^e}} \\ &= \sum_{k=0}^{(m-2)/2} \left(x^p + x^{p^3} + \cdots + x^{p^{2p^e-1}}\right)^{p^{2kp^e}}. \end{aligned}$$

For an element $x \in \mathbb{F}_{p^{2p^e}}$ we have

$$L(x) = (m/2)\left(x + x^{p^2} + \cdots + x^{p^{2p^e-2}}\right)^p.$$

Set $\tilde{L}(x) = x + x^{p^2} + \cdots + x^{p^{2p^e-2}}$ so that $L(x) = (m/2)\tilde{L}(x)^p$ for $x \in \mathbb{F}_{p^{2p^e}}$. Clearly, $|\mathrm{Ker}(\tilde{L})| \leq \deg\tilde{L} = p^{2p^e-2}$. (In fact, $x^{p^{2p^e}} - x = (x^{p^2} - x) \circ \tilde{L}(x)$, and hence the zeros of $\tilde{L}$ lie in $\mathbb{F}_{p^{2p^e}}$, which implies that $|\mathrm{Ker}(\tilde{L})| = \deg\tilde{L} = p^{2p^e-2}$.) We can pick $\alpha \in \mathbb{F}_{p^{2p^e}}$ such that $\tilde{L}(\alpha) \neq 0$, and hence $L(\alpha) \neq 0$. Then, since $L(tx) = (m/2)t^p\tilde{L}(x)^p$ for all $t \in \mathbb{F}_{p^2}$ and $x \in \mathbb{F}_{p^{2p^e}}$, the 2-dimensional vector space $\Omega^c := \alpha\mathbb{F}_{p^2}$ satisfies $\Omega \cap \Omega^c = \{0\}$, where $\Omega := \mathrm{Ker}(L)$ is the linear space of Q. Consequently, Ω^c is a complement of Ω in $\mathbb{F}_{p^n}$.

To determine the Walsh coefficient of Q at 0, we write $x \in \mathbb{F}_{p^n}$ as $x = y + z$ with $y \in \Omega$ and $z \in \Omega^c$, and take an advantage of the fact that Q is linear on Ω. We have

$$\widehat{Q}(0) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{Q(x)} = (\sum_{y \in \Omega} \epsilon_p^{Q(y)})(\sum_{z \in \Omega^c} \epsilon_p^{Q(z)}) = \begin{cases} p^{n-2}\sum_{z \in \Omega^c} \epsilon_p^{Q(z)} & \text{if } Q(y) = 0 \text{ for all } y \in \Omega, \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 4.1 $\widehat{Q}(0) \neq 0$, so we conclude that $\widehat{Q}(0) = p^{n-2}\sum_{z \in \Omega^c} \epsilon_p^{Q(z)}$.

For $z \in \Omega^c$ with $z = \alpha t$, $t \in \mathbb{F}_{p^2}$, we get

$$\begin{aligned} Q(z) &= \mathrm{Tr}_n\left(\alpha t\left((\alpha t)^p + (\alpha t)^{p^3} + \cdots + (\alpha t)^{p^{n/2-1}}\right)\right) \\ &= \mathrm{Tr}_n\left(t^{p+1}\left(\alpha^{p+1} + \alpha^{p^3+1} + \cdots + \alpha^{p^{n/2-1}+1}\right)\right) \\ &= t^{p+1}\mathrm{Tr}_n\left(\alpha^{p+1} + \alpha^{p^3+1} + \cdots + \alpha^{p^{n/2-1}+1}\right) \\ &= t^{p+1}Q(\alpha). \end{aligned}$$

In the last equality we used that $t^{p+1} \in \mathbb{F}_p$ if $t \in \mathbb{F}_{p^2}$. For the Walsh coefficient of Q at 0 we then obtain

$$\begin{aligned} \widehat{Q}(0) &= p^{n-2}\sum_{t \in \mathbb{F}_{p^2}} \epsilon_p^{Q(\alpha)t^{p+1}} = p^{n-2}\left(1 + (p+1)\sum_{y \in \mathbb{F}_p \setminus \{0\}} (\epsilon_p^{Q(\alpha)})^y\right) \\ &= p^{n-2}(1 + (p+1)(-1)) = -p^{n-1}. \end{aligned}$$

Note that in the last step we can exclude that $Q(\alpha) = 0$, otherwise we get $\widehat{Q}(0) = p^n$, a contradiction. This finishes the proof for the case (a).

Now we consider the case (b), where $A(x) = c(x^{n-2} + x^{n-4} + \cdots + x^2 + 1)(x^2 + ax + 1)$ for some $a \neq \pm 2$ and $c \in \mathbb{F}_p^*$. Again we can without loss of generality choose $c = 1$. In order to get a maximal or minimal curve, the coefficient $a_{n/2}$ of $x^{n/2}$ must be zero by Corollary 4.8. This holds if and only if $n \equiv 2 \mod 4$ and

$$A(x) = (x^{n-2} + x^{n-4} + \cdots + x^{n/2+1} + x^{n/2-1} + \cdots + x^2 + 1)(x^2 + 1) \ .$$

The corresponding linearized polynomial is then given by

$$L(x) = x^{p^n} + 2x^{p^{n-2}} + \cdots + 2x^{p^{n/2+3}} + 2x^{p^{n/2+1}} + \cdots + 2x^{p^4} + 2x^{p^2} + x \ .$$

Since $x^{p^n} = x$ for an element $x \in \mathbb{F}_{p^n}$, we can evaluate $L(x)$ as

$$\begin{aligned} L(x) &= 2\left(x + x^{p^2} + \cdots + x^{p^{2p^e-2}}\right) + 2\left(x^{p^{2p^e}} + x^{p^{2p^e+2}} + \cdots + x^{p^{4p^e-2}}\right) \\ &\quad + \cdots + 2\left(x^{p^{(m-2)p^e}} + x^{p^{(m-2)p^e+2}} + \cdots + x^{p^{n-2}}\right) \ . \end{aligned}$$

In this representation each parenthesis contains exactly p^e summands. We observe that for an element x in $\mathbb{F}_{p^{2p^e}}$, we have $L(x) = m(x + x^{p^2} + \cdots + x^{p^{2p^e-2}}) = m\tilde{L}(x)$. As observed above, the kernel $\mathrm{Ker}(\tilde{L})$ in $\mathbb{F}_{p^n}$ of $\tilde{L}$ lies in $\mathbb{F}_{p^{2p^e}}$ and has cardinality p^{2p^e-2}, and there exists an element $\alpha \in \mathbb{F}_{p^{2p^e}}$ such that $\tilde{L}(\alpha) \neq 0$, hence $L(\alpha) \neq 0$. Since $L(t\alpha) = m\tilde{L}(t\alpha) = mt\tilde{L}(\alpha)$ for all $t \in \mathbb{F}_{p^2}$, the 2-dimensional vector space $\Omega^c = \alpha\mathbb{F}_{p^2}$ over $\mathbb{F}_p$ is again a complement in $\mathbb{F}_{p^n}$ of Ω, the linear space of Q. As in the case (a),

$$\widehat{Q}(0) = p^{n-2} \sum_{z \in \Omega^c} \epsilon_p^{Q(z)} = p^{n-2} \sum_{t \in \mathbb{F}_{p^2}} \epsilon_p^{Q(t\alpha)}.$$

We have

$$\begin{aligned} Q(t\alpha) &= (m/2)\mathrm{Tr}_{2p^e}\left((t\alpha)^2 + 2(t\alpha)^{p^2+1} + 2(t\alpha)^{p^4+1} + \cdots + 2(t\alpha)^{p^{n/2-1}+1}\right) \\ &= (m/2)\mathrm{Tr}_{2p^e}\left(t^2(\alpha^2 + 2\alpha^{p^2+1} + 2\alpha^{p^4+1} + \cdots + 2\alpha^{p^{n/2-1}+1})\right) \\ &= (m/2)\mathrm{Tr}_2\left(\beta t^2\right) \ , \end{aligned}$$

where $\beta = \mathrm{Tr}_{\mathbb{F}_{p^{2p^e}}/\mathbb{F}_{p^2}}(\alpha^2 + 2\alpha^{p^2+1} + 2\alpha^{p^4+1} + \cdots + 2\alpha^{p^{n/2-1}+1})$. If $\beta = 0$ then

$$\widehat{Q}(0) = p^{n-2} \sum_{t \in \mathbb{F}_{p^2}} \epsilon_p^{Q(t\alpha)} = p^{n-2} \sum_{t \in \mathbb{F}_{p^2}} (\epsilon_p^{(m/2)})^{\mathrm{Tr}_2\left(\beta t^2\right)} = p^n,$$

which is a contradiction. Hence $\beta \neq 0$, and

$$\widehat{Q}(0) = p^{n-2} \sum_{t \in \mathbb{F}_{p^2}} \epsilon_p^{Q(t\alpha)} = p^{n-2} \sum_{t \in \mathbb{F}_{p^2}} (\epsilon_p^{(m/2)})^{\mathrm{Tr}_2\left(\beta t^2\right)} = (-1)^{\frac{p+1}{2}} \eta(\beta) p^{n-1},$$

where last equality follows from Corollary 3 in [12].

As a final step we determine the quadratic character $\eta(\beta)$ of $\beta \in \mathbb{F}_{p^2}$. Since $\mathbb{F}_{p^{2p^e}}$ is the compositum of $\mathbb{F}_{p^{p^e}}$ and $\mathbb{F}_{p^2}$, and $\tilde{L}(t\gamma) = t\tilde{L}(\gamma)$ for all $t \in \mathbb{F}_{p^2}$ and $\gamma \in \mathbb{F}_{p^{p^e}}$, we cannot have

$\tilde{L}(\gamma) = 0$ for all $\gamma \in \mathbb{F}_{p^{p^e}}$. Hence without loss of generality we can choose $\alpha \in \mathbb{F}_{p^{p^e}}$. Using the fact that $\alpha^{p^{p^e}} = \alpha$, for any non-negative integer j we get

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_{p^{2p^e}}/\mathbb{F}_{p^2}}(\alpha^j) &= \alpha^j + \alpha^{jp^2} + \alpha^{jp^4} + \cdots + \alpha^{jp^{p^e-1}} + \alpha^{jp^{p^e+1}} + \cdots + \alpha^{jp^{2p^e-2}} \\
&= \alpha^j + \alpha^{jp^2} + \alpha^{jp^4} + \cdots + \alpha^{jp^{p^e-1}} + \alpha^{jp} + \cdots + \alpha^{jp^{p^e-2}} \\
&= \alpha^j + \alpha^{jp} + \alpha^{jp^2} + \cdots + \alpha^{jp^{p^e-2}} + \alpha^{jp^{p^e-1}} \\
&= \mathrm{Tr}_{p^e}(\alpha^j).
\end{aligned}$$

In particular this shows that $\beta \in \mathbb{F}_p^*$, and therefore β is a square in $\mathbb{F}_{p^2}$. As a consequence, $\widehat{Q}(0) = (-1)^{\frac{p+1}{2}} p^{n-1}$. □

Remark 5.3. Theorem 5.2 is considerably harder to obtain than the analog theorem in [1] for the case that $\gcd(n,p) = 1$. Together with the result on the case $\gcd(n,p) = 1$, Theorem 5.2 completely classifies all maximal and minimal curves obtained from quadratic functions in odd characteristic p of codimension 2 and coefficients in the prime field $\mathbb{F}_p$. Maximal and minimal curves obtained from quadratic functions in characteristic 2 of codimension 2 and coefficients in $\mathbb{F}_2$ are characterized in [10].

We finish this section with a generalization of Theorem 5.2 to quadratic fucnctions for which the p-associate $A(x)$ satisfies $\gcd(A(x), x^n - 1) = (x^n - 1)/(x^k - 1)$ for an (even) divisor k of n. As a result we obtain infinite classes of maximal and minimal curves obtained from quadratic function with various codimenson k, respectively curves of various genus. The easier case that $\gcd(n,p) = 1$ has been dealt with in [1, Theorem 5.3]. In fact, the proof of Theorem 5.3 in [1] holds more generally for the case that $\gcd(n/k,p) = 1$. Hence we here suppose that $\gcd(n/k,p) > 1$.

Theorem 5.4. *Let n be an even integer divisible by p and let k be an even divisor of n with $\gcd(n/k,p) > 1$. Let $Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{l} a_i x^{p^i+1})$ be a quadratic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ with coefficients in $\mathbb{F}_p$ for which the associate $A(x) \in \mathbb{F}_p[x]$ of the corresponding linearized polynomial $L(x)$ satisfies*

$$\gcd(A(x), x^n - 1) = \frac{x^n - 1}{x^k - 1} .$$

Then the curve $\mathcal{X} : y^p - y = \sum_{i=0}^{l} a_i x^{p^i+1}$ over $\mathbb{F}_{p^n}$ is maximal if and only if

- *$\mathcal{X} : y^p - y = c(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1})$, $c \in \mathbb{F}_p^*$, $p \equiv 3 \mod 4$ and $v(k) = v(n)$, where $v(m)$ denote the 2-adic valuation of an integer m.*

The curve $\mathcal{X} : y^p - y = \sum_{i=0}^{l} a_i x^{p^i+1}$ over $\mathbb{F}_{p^n}$ is minimal if and only if

- *$\mathcal{X} : y^p - y = c(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1})$, $c \in \mathbb{F}_p^*$, $p \equiv 1 \mod 4$ and $v(k) = v(n)$, or*
- *$\mathcal{X} : y^p - y = c(x^{p^{\frac{k}{2}}+1} + x^{p^{\frac{3k}{2}}+1} + \cdots + x^{p^{\frac{n-k}{2}}+1})$, $c \in \mathbb{F}_p^*$, $v(k) < v(n)$.*

Proof. We distinguish two cases, the case that $v(n) > v(k)$ and the case that $v(n) = v(k)$.

Case(i): $v(n) > v(k)$

In this case $(x^n-1)/(x^k-1) = 1+x^k+\cdots+x^{n/2-k}+x^{n/2}+x^{n/2+k}+\cdots+x^{n-2k}+x^{n-k}$. Recall that $A(x) = (x^n-1)/(x^k-1)g(x)$, where $g(x) = c_0+c_1x+\cdots+c_1x^{k-1}+c_0x^k$ and $\gcd(x^k-1, g(x)) = 1$. Then with coefficient comparison we observe that the condition in Corollary 4.8 is satisfied, i.e. we obtain a maximal or minimal curve, if and only if

$$A(x) = cx^{k/2}\left(1 + x^k + \cdots + x^{n/2-k} + x^{n/2} + x^{n/2+k} + \cdots + x^{n-2k} + x^{n-k}\right) .$$

Again, without loss of generality we consider the case $c = 1$ by Lemma 4.2. The corresponding linearized polynomial $L(x)$ and the quadratic function $Q(x)$ are then given as follows.

$$\begin{aligned}
L(x) &= \left(x + x^{p^k} + \cdots + x^{p^{n/2-k}} + x^{p^{n/2}} + x^{p^{n/2+k}} + \cdots + x^{p^{n-2k}} + x^{p^{n-k}}\right)^{p^{k/2}} \\
Q(x) &= \mathrm{Tr}_n\left(x^{p^{k/2}+1} + x^{p^{3k/2}+1} + \cdots + x^{p^{(n-k)/2}+1}\right)
\end{aligned}$$

We put $n/k = p^e m$, $\gcd(m,p) = 1$, and write $L(x)^{p^{-k/2}}$ as

$$\begin{aligned}
L(x)^{p^{-k/2}} &= \left(x + x^{p^k} + \cdots + x^{p^{(p^e-1)k}}\right) + \left(x^{p^{p^e k}} + x^{p^{(p^e+1)k}} + \cdots + x^{p^{(2p^e-1)k}}\right) \\
&\quad + \cdots + \left(x^{p^{(m-1)p^e k}} + x^{p^{((m-1)p^e+1)k}} + \cdots + x^{p^{(mp^e-1)k}}\right) \\
&= \left(x + x^{p^k} + \cdots + x^{p^{(p^e-1)k}}\right) + \left(x + x^{p^k} + \cdots + x^{p^{(p^e-1)k}}\right)^{p^{p^e k}} \\
&\quad + \cdots + \left(x + x^{p^k} + \cdots + x^{p^{(p^e-1)k}}\right)^{p^{(m-1)p^e k}} \\
&= \sum_{i=0}^{m-1}\left(x + x^{p^k} + \cdots + x^{p^{(p^e-1)k}}\right)^{p^{ip^e k}} .
\end{aligned}$$

We note that, in this representation, each parenthesis contains exactly p^e elements. Set $\tilde{L}(x) = x + x^{p^k} + \cdots + x^{p^{(p^e-1)k}}$. Then for all $x \in \mathbb{F}_{p^{p^e k}}$ we have $L(x) = m\tilde{L}(x)^{p^{k/2}}$, and hence we can pick an element $\alpha \in \mathbb{F}_{p^{p^e k}}$ with $\tilde{L}(\alpha) \neq 0$ and consequently $L(\alpha) \neq 0$. Again observing that $\tilde{L}(t\alpha) = t\tilde{L}(\alpha)$ for all $t \in \mathbb{F}_{p^k}$, we see that $\Omega^c := \alpha\mathbb{F}_{p^k}$ is a complement of Ω in $\mathbb{F}_{p^n}$. We evaluate Q on Ω^c as

$$\begin{aligned}
Q(t\alpha) &= \mathrm{Tr}_n\left((t\alpha)^{p^{k/2}+1} + (t\alpha)^{p^{3k/2}+1} + \cdots + (t\alpha)^{p^{(n-k)/2}+1}\right) \\
&= m\mathrm{Tr}_{p^e k}\left(t^{p^{k/2}+1}(\alpha^{p^{k/2}+1} + \alpha^{p^{3k/2}+1} + \cdots + \alpha^{p^{(n-k)/2}+1})\right) \\
&= m\mathrm{Tr}_k(t^{p^{k/2}+1}\beta) ,
\end{aligned}$$

where $\beta = \mathrm{Tr}_{\mathbb{F}_{p^{p^e k}}/\mathbb{F}_{p^k}}(\alpha^{p^{k/2}+1} + \alpha^{p^{3k/2}+1} + \cdots + \alpha^{p^{(n-k)/2}+1})$. Consequently

$$\widehat{Q}(0) = p^{n-k}\sum_{t\in\mathbb{F}_{p^k}}\epsilon_p^{Q(\alpha t)} = p^{n-k}\sum_{t\in\mathbb{F}_{p^k}}\epsilon_p^{m\mathrm{Tr}_k(\beta t^{p^{k/2}+1})} = p^{n-k}(-p^{k/2}) = -p^{n-k/2} ,$$

where the last equality follows from Lemma 2 (iii) in [12]. Note that we again can exclude that $\beta = 0$, otherwise $\widehat{Q}(0) = p^n$, which is a contradiction.

Case(ii): $v(n) = v(k)$

In this case $A(x) = (x^n - 1)/(x^k - 1)g(x)$, where $g(x) = c_0 + c_1 x + \cdots + c_1 x^{k-1} + c_0 x^k$ and $\gcd(x^k - 1, g(x)) = 1$. By Corollary 4.8, with coefficient comparison we see that we obtain a maximal or minimal curve if and only if

$$A(x) = c(1 + x^k)\left(1 + \cdots + x^{\frac{n-k}{2}} + x^{\frac{n+k}{2}} + \cdots + x^{n-k}\right) = 1 + 2x^k + \cdots + 2x^{n-k} + x^n, c \in \mathbb{F}_p^* .$$

Choosing $c = 1$, the corresponding linearized polynomial $L(x)$ and quadratic function $Q(x)$ are given as follows.

$$\begin{aligned} L(x) &= x + 2x^{p^k} + \cdots + 2x^{p^{(n-k)/2}} + 2x^{p^{(n+k)/2}} + \cdots + 2x^{p^{n-k}} + x^{p^n} \\ Q(x) &= \mathrm{Tr}_n\left(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1}\right) \end{aligned}$$

Since $x^{p^n} = x$ for an element $x \in \mathbb{F}_{p^n}$, we can evaluate $L(x)$ as

$$\begin{aligned} L(x) &= 2(x + x^{p^k} + \cdots + x^{p^{(p^e-1)k}}) + 2(x^{p^{p^e k}} + x^{p^{(p^e+1)k}} + \cdots + x^{p^{(2p^e-1)k}}) \\ &\quad + \cdots + 2(x^{p^{(m-1)p^e k}} + x^{p^{((m-1)p^e+1)k}} + \cdots + x^{p^{(m-1)p^e k + (p^e-1)k}}) \\ &= 2\sum_{i=0}^{m-1} (x + x^{p^k} + \cdots + x^{p^{(p^e-1)k}})^{p^{ip^e k}} . \end{aligned}$$

Hence for an element $x \in \mathbb{F}_{p^{p^e k}}$, we have $L(x) = 2m(x + x^{p^k} + \cdots + x^{p^{(p^e-1)k}}) = 2m\tilde{L}(x)$. Again we can pick an element $\alpha \in \mathbb{F}_{p^{p^e k}}$ with $\tilde{L}(\alpha) \neq 0$ and equivalently, $L(\alpha) \neq 0$. Using that $\tilde{L}$ is an $\mathbb{F}_{p^k}$-linear map, we again observe that $\Omega^c := \alpha\mathbb{F}_{p^k}$ is a complement of Ω. Again we evaluate Q at $t\alpha$ for $t \in \mathbb{F}_{p^k}$.

$$\begin{aligned} Q(t\alpha) &= \mathrm{Tr}_n\left((t\alpha)^2 + 2(t\alpha)^{p^k+1} + \cdots + 2(t\alpha)^{p^{\frac{n-k}{2}}+1}\right) \\ &= m\mathrm{Tr}_{p^e k}\left(t^2(\alpha^2 + 2\alpha^{p^k+1} + \cdots + 2\alpha^{p^{\frac{n-k}{2}}+1})\right) \\ &= m\mathrm{Tr}_k\left(\beta t^2\right) , \end{aligned}$$

where $\beta = \mathrm{Tr}_{\mathbb{F}_{p^{p^e k}}/\mathbb{F}_{p^k}}(\alpha^2 + 2\alpha^{p^k+1} + \cdots + 2\alpha^{p^{\frac{n-k}{2}}+1})$. Note that β can not be zero since $\widehat{Q}(0) \neq p^n$. Then by Corollary 3 in [12] we have

$$\widehat{Q}(0) = p^{n-k}\sum_{t \in \mathbb{F}_{p^k}} \epsilon_p^{Q(t\alpha)} = p^{n-k}\sum_{t \in \mathbb{F}_{p^k}} (\epsilon_p^m)^{\mathrm{Tr}_k(\beta t^2)} = (-1)^{\frac{p+1}{2}}\eta(\beta)p^{n-k/2} ,$$

where η is the quadratic character in $\mathbb{F}_{p^k}$.

Now we show that β is a square in $\mathbb{F}_{p^k}$. Write $k = p^\ell r$ with $\gcd(p, r) = 1$ for some non-negative integer ℓ. Firstly note that as $\mathbb{F}_{p^{p^e k}}$ is compositum of $\mathbb{F}_{p^k}$ and $\mathbb{F}_{p^{p^{e+\ell}}}$ without loss of generality we can chose $\alpha \in \mathbb{F}_{p^{p^{e+\ell}}}$. Then for any non-negative integer j we consider

$$\mathrm{Tr}_{\mathbb{F}_{p^{p^e k}}/\mathbb{F}_{p^k}}(\alpha^j) = \alpha^j + (\alpha^j)^{p^k} + (\alpha^j)^{p^{2k}} + \cdots + (\alpha^j)^{p^{(p^e-1)k}} .$$

Since $\{0, k, 2k, \cdots, (p^e-1)k\} \equiv \{0, p^\ell, 2p^\ell, \cdots, (p^e-1)p^\ell\} \mod p^{e+\ell}$, by using the fact that $\alpha^{p^{p^{e+\ell}}} = \alpha$ we obtain the following equalities.

$$\alpha^j + (\alpha^j)^{p^k} + (\alpha^j)^{p^{2k}} + \cdots + (\alpha^j)^{p^{(p^e-1)k}} = \alpha^j + (\alpha^j)^{p^{p^\ell}} + (\alpha^j)^{p^{2p^\ell}} + \cdots + (\alpha^j)^{p^{(p^e-1)p^\ell}} = \mathrm{Tr}_{\mathbb{F}_{p^{p^{e+\ell}}}/\mathbb{F}_{p^{p^\ell}}}(\alpha^j)$$

This shows that $\beta \in \mathbb{F}_{p^{p^\ell}}$. On the other hand the extension degree of $\mathbb{F}_{p^k} : \mathbb{F}_{p^{p^\ell}}$ is an even integer as k is an even integer. This implies that β is a square in $\mathbb{F}_{p^k}$. As a consequence, we have $\widehat{Q}(0) = (-1)^{\frac{p+1}{2}} p^{n-k/2}$.

$\square$

References

[1] N. Anbar, W. Meidl, Quadratic Functions and Maximal Artin-Schreier Curves, Finite Fields and Their Applications, to appear.

[2] E. Çakçak, F. Özbudak, Some Artin-Schreier type function fields over finite fields with prescribed genus and number of rational places. J. of Pure and Appl. Algebra 210 (1) (2007) 113–135.

[3] A. Çeşmelioğlu, G. McGuire, W. Meidl, A construction of weakly and non-weakly regular bent functions. J. Comb. Theory, Series A 119 (2012), 420–429.

[4] A. Çeşmelioğlu, W. Meidl, Not weakly regular bent polynomials from vectorial quadratic functions. Preprint 2013.

[5] R. Coulter, Explicit evaluations of some Weil sums. Acta Arith. 83 (1998), 241–251.

[6] R. Coulter, On the evaluation of a class of Weil sums in characteristic 2. New Zealand J. Math. 28 (1999), 171–184.

[7] R. Coulter, The number of rational points of a class of Artin-Schreier curves. Finite Fields Appl. 8 (2002), 397–413.

[8] K. Feng, J. Luo, Weight distribution of some reducible cyclic codes. Finite Fields Appl. 14 (2008), 390–409.

[9] K. Feng, J. Luo, On the weight distributions of two classes of cyclic codes. IEEE Trans. Inform. Theory 54 (2008), 5332–5344.

[10] R.W. Fitzgerald, Highly degenerate quadratic forms over finite fields of characteristic 2. Finite Fields Appl. 11 (2005), 165–181.

[11] R.W. Fitzgerald, Trace forms over finite fields of characteristic 2 with prescribed invariants. Finite Fields Appl. 15 (2009), 69–81.

[12] T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inform. Theory 52 (2006), 2018–2032.

[13] K. Khoo, G. Gong, D. Stinson, A new characterization of semi-bent and bent functions on finite fields, Designs, Codes, Cryptogr. 38 (2006), 279–295.

[14] J. Lahtonen, G. McGuire, H. N. Ward, Gold and Kasami-Welch functions, quadratic forms, and bent functions, Adv. Math. Commun. vol. 1, no. 2 (2007), 243–250.

[15] X. Lai, Additive and linear structures of cryptographic functions, Fast Software Encryption, Lecture Notes in Comput. Sci. 1008 (1995), 75–85.

[16] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.

[17] W. Meidl, S. Roy, A. Topuzoğlu, Enumeration of quadratic functions with prescribed Walsh spectrum. Preprint 2013.

[18] F. Özbudak, E. Saygı, Z. Saygı, Quadratic forms of codimension 2 over certain finite fields of even characteristic, Cryptogr. Commun. 3 (2011), 241–257.

[19] F. Özbudak, E. Saygı, Z. Saygı, Quadratic forms of codimension 2 over finite fields containing $\mathbb{F}_4$ and Artin-Schreier type curves, Finite Fields Appl. 8 (2012), 396–433.

[20] H. Stichtenoth, Algebraic function fields and codes, 2nd Edition, Graduate Texts in Mathematics 254, Springer Verlag, 2009.

[21] Y. Zheng, X.M. Zhang, On plateaued functions. IEEE Trans. Inform. Theory 47 (2001), 1215–1223.