Finite Fields Appl. 8 (2002), 397-413

The number of rational points of a class of Artin-Schreier curves*

Robert S. Coulter

Information Security Research Centre
Queensland University of Technology
GPO Box 2434, Brisbane, Queensland 4001
Australia.
E-mail: shrub@isrc.qut.edu.au

We determine the number of $\mathbb{F}_q$-rational points of a class of Artin-Schreier curves by using recent results concerning evaluations of some exponential sums. In particular, we determine infinitely many new examples of maximal and minimal plane curves in the context of the Hasse-Weil bound.

1. INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field with $q = p^e$ elements and $\mathcal{P}^n(\mathbb{F}_q)$ be the n-dimensional projective space over $\mathbb{F}_q$. For any $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree d, define the homogenous polynomial $f^* \in \mathbb{F}_q[X_0, \ldots, X_n]$ by $f^*(X_0, \ldots, X_n) = X_0^d f(X_1/X_0, \ldots, X_n/X_0)$. The set of $\mathbb{F}_q$-rational points of an algebraic hypersurface X_f is the set of all points $P \in \mathcal{P}^n(\mathbb{F}_q)$ satisfying $f^*(P) = 0$. The hypersurface X_f is called a plane curve if $n = 2$. If g denotes the genus of the curve and N denotes the number of $\mathbb{F}_q$-rational points on the curve, then we have the classical Hasse-Weil bound

$$|N - (q+1)| \leq 2g\sqrt{q},$$

provided the polynomial $f(X_1, X_2)$ is absolutely irreducible. In the two extremes, where $|N-(q+1)| = 2g\sqrt{q}$, a curve is called *maximal* or *minimal* in the obvious way.

An Artin-Schreier curve is a plane curve with equation of the form

$$y^q + \delta y = f(x)$$

with δ in some finite extension field $\mathbb{K}$ of $\mathbb{F}_q$ and $f \in \mathbb{K}[X]$. Artin-Schreier curves have been studied extensively in several contexts, see for example the articles [5, 6, 7, 8, 10, 14]. Note also that the Hermitian curve, $y^q+y = x^{q+1}$ over $\mathbb{F}_{q^2}$, is an Artin-Schreier curve. This curve has genus $q(q-1)/2$.

Stichtenoth, see [13, Chapter V.3], showed that curves over $\mathbb{F}_{q^2}$ of genus $> q(q-1)/2$ could not be maximal. Rück and Stichtenoth [12] have since shown that the Hermitian curve is the only maximal curve over $\mathbb{F}_{q^2}$ of genus $q(q-1)/2$, see also [4].

The solution to the problem of determining the number of points on a plane curve often relies on the explicit evaluation of an exponential sum (or vice versa). For $a, b \in \mathbb{F}_q$ and any integer α, we define $S_\alpha(a,b)$ by

$$S_\alpha(a,b) = \sum_{x \in \mathbb{F}_q} \chi_1(ax^{p^\alpha+1} + bx).$$

The explicit evaluation of $S_\alpha(a,b)$ was carried out in the articles [1, 2, 3]. It is the purpose of this article to use these evaluations to determine the number of $\mathbb{F}_q$-rational points on the Artin-Schreier curve

$$y^{p^n} - y = ax^{p^\alpha+1} + L(x)$$

where $a \in \mathbb{F}_q^*$, $t = gcd(n,e) = (n,e)$ divides $d = (\alpha, e)$, and $L \in \mathbb{F}_q[X]$ is a p^t-polynomial. This is accomplished by reducing the problem to a formula involving $S_\alpha(a,b)$ and then determining the value of this formula under the various conditions which arise. In so doing, we determine infinitely many new examples of both maximal and minimal curves, for any choice of t.

2. DEFINITIONS AND PRELIMINARIES

Throughout this article $\mathbb{F}_q$ denotes the finite field of $q = p^e$ elements where p is a prime, α is a natural number, $d = (\alpha, e)$ and n is any natural number such that $t = (n,e)$ divides d. We denote by $\mathbb{F}_q^*$ the non-zero elements of $\mathbb{F}_q$ and identify a generator of $\mathbb{F}_q^*$ by ζ. For any k dividing e we can define the *trace function* $\mathrm{Tr}_k : \mathbb{F}_q \to \mathbb{F}_{p^k}$ by

$$\mathrm{Tr}_k(x) = x + x^{p^k} + x^{p^{2k}} + \ldots + x^{p^{k(e/k-1)}}$$

for all $x \in \mathbb{F}_q$. The trace function satisfies $\mathrm{Tr}_k(x+y) = \mathrm{Tr}_k(x) + \mathrm{Tr}_k(y)$, $\mathrm{Tr}_k(x^{p^k}) = \mathrm{Tr}_k(x)$ and $\mathrm{Tr}_k(\beta x) = \beta \mathrm{Tr}_k(x)$ for all $x, y \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_{p^k}$. We shall denote the *absolute trace*, Tr_1, simply by Tr.

A p^s*-polynomial* is any polynomial $L \in \mathbb{F}_q[X]$ of the shape

$$L(X) = \sum_i a_i X^{p^{si}}.$$

Every p^s-polynomial is a p-polynomial. Also known as linearised or additive polynomials, p-polynomials satisfy $L(x+y) = L(x) + L(y)$ for all $x, y \in \mathbb{F}_q$.

We recall that a polynomial is called a *permutation polynomial* over $\mathbb{F}_q$ if it induces a permutation of $\mathbb{F}_q$ under evaluation. It is easy to establish that a linearised polynomial L is a permutation polynomial over $\mathbb{F}_q$ if and only if $L(x) = 0$ implies $x = 0$.

There are two classes of characters associated with a finite field: the additive characters defined on $\mathbb{F}_q$ and the multiplicative characters defined on $\mathbb{F}_q^*$. The *canonical additive character* of $\mathbb{F}_q$, denoted χ_1, is defined by

$$\chi_1(x) = \exp\left(2\pi i \mathrm{Tr}(x)/p\right)$$

for all $x \in \mathbb{F}_q$. Every additive character, χ_c with $c \in \mathbb{F}_q$, can be obtained from the canonical character by $\chi_c(x) = \chi_1(cx)$ for all $x \in \mathbb{F}_q$. The properties of the trace function imply $\chi_1(x+y) = \chi_1(x)\chi_1(y)$ and $\chi_1(x^p) = \chi_1(x)$ for all $x, y \in \mathbb{F}_q$. A proof of the following lemma is provided in [9, Lemma 7.1.3].

Lemma 2.1. *Denote by χ_1 the canonical additive character of $\mathbb{F}_q$ with $q = p^e$. Let $a \in \mathbb{F}_q$ be arbitrary and let k be some integer dividing e. Then*

$$\sum_{\beta \in \mathbb{F}_{p^k}} \chi_1(c\beta) = \begin{cases} p^k & \text{if } Tr_k(c) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

For $0 \le j \le q-2$, we define a multiplicative character λ_j of $\mathbb{F}_q$ by

$$\lambda_j(\zeta^k) = \exp\left(2\pi i jk/(q-1)\right)$$

for $k = 0, \ldots, q-2$. When p is odd we shall use η to denote the *quadratic character* of $\mathbb{F}_q$. That is $\eta = \lambda_{(q-1)/2}$.

For any additive character χ and any multiplicative character λ of $\mathbb{F}_q$ we can define the classical Gaussian sum $G(\lambda, \chi)$ by

$$G(\lambda, \chi) = \sum_{x \in \mathbb{F}_q^*} \lambda(x)\chi(x).$$

Introduced by Gauss, these sums are used to consider the interaction between the additive and multiplicative groups of a finite field. They have been studied extensively, see [11, Chapter 5] for further information. We shall require the following result on Gaussian sums.

Lemma 2.2 ([11, Theorem 5.15]). *For $\mathbb{F}_q$ a finite field of odd characteristic we have*

$$G(\eta, \chi_1) = \begin{cases} (-1)^{e-1}\sqrt{q} & \text{if } p \equiv 1 \bmod 4, \\ (-1)^{e-1} i^e \sqrt{q} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

The following lemma on greatest common divisors will prove useful. A proof is given in [1, 3].

Lemma 2.3. *Let $d = (\alpha, e)$ and p be a prime. If e/d is odd then*

$$(p^\alpha + 1, p^e - 1) = \begin{cases} 1 & \textit{if } p = 2, \\ 2 & \textit{otherwise.} \end{cases}$$

If e/d is even then $(p^\alpha + 1, p^e - 1) = p^d + 1$.

Finally, we will need several results concerning the question of when two related equations are solvable.

Theorem 2.1 ([1, Theorem 4.1]). *Let p be odd. For any $a \in \mathbb{F}_q^*$, the equation $a^{p^\alpha} x^{p^{2\alpha}} + ax = 0$ is solvable for $x \in \mathbb{F}_q^*$ if and only if e/d is even with $e = 2m$ and*

$$a^{(q-1)/(p^d+1)} = (-1)^{m/d}.$$

In such cases there are $p^{2d} - 1$ non-zero solutions.

Theorem 2.2 ([3, Theorem 3.1]). *Let $q = 2^e$. For any $a \in \mathbb{F}_q^*$ consider the equation $a^{2^\alpha} x^{2^{2\alpha}} + ax = 0$ over $\mathbb{F}_q$.*

(i)If e/d is odd then there are 2^d solutions to this equation for any choice of $a \in \mathbb{F}_q^*$.

(ii)If e/d is even then there are two possible cases. If $a = \zeta^{k(2^d+1)}$ for some k then there are 2^{2d} solutions to the equation. If $a \neq \zeta^{k(2^d+1)}$ for any k then there exists one solution only, $x = 0$.

The polynomial $a^{p^\alpha} X^{p^{2\alpha}} + aX$ is a linearised polynomial. Thanks to the simple statement for when a linearised polynomial is a permutation polynomial, it can be seen that Theorems 2.1 and 2.2 provide explicit descriptions for when this polynomial is a permutation polynomial over $\mathbb{F}_q$.

3. WHEN IS $A^{P^\alpha} X^{P^{2\alpha}} + AX + B^{P^\alpha} = 0$ SOLVABLE?

As mentioned earlier, the value of $S_\alpha(a, b)$ was explicitly determined in the articles [1, 2, 3]. Unfortunately, in some cases the results rely on knowing when the equation

$$a^{p^\alpha} x^{p^{2\alpha}} + ax + b^{p^\alpha} = 0$$

with $a, b \in \mathbb{F}_q$ and $\alpha \in \mathbb{N}$, can be solved for $x \in \mathbb{F}_q$, in particular when e/d is even. In this section we determine necessary and sufficient conditions for solving this equation when e/d is even.

Let $f_a(X) = a^{p^\alpha} X^{p^{2\alpha}} + aX$ with $a \in \mathbb{F}_q^*$ and suppose e/d is even with $e = 2m$. We wish to consider when the equation $f_a(x) = -b^{p^\alpha}$ has solutions $x \in \mathbb{F}_q$. Clearly it has a unique solution when f_a is a permutation polynomial. In the remaining cases we now derive conditions on a and b for when the equation is solvable. The following proposition follows from Theorems 2.1 and 2.2.

Proposition 3.1. *Let e/d be even with $e = 2m$. The polynomial f_a is not a permutation polynomial over $\mathbb{F}_q$ if and only if $a = \zeta^{k+i(p^d+1)}$ for some integer i and fixed k given by*

$$k = \begin{cases} 0 & \text{if } p = 2 \text{ or } p \text{ odd and } m/d \text{ even} \\ (p^d+1)/2 & \text{if } p \text{ odd and } m/d \text{ odd.} \end{cases}$$

Proposition 3.2. *Let e/d be even with $e = 2m$. Set*

$$a_0 = \begin{cases} 1 & \text{if } p = 2 \\ \zeta^{(q-1)/2(p^d-1)} & \text{if } p \text{ odd.} \end{cases}$$

Then $a_0 \in \mathbb{F}_{p^{2d}}^*$ and f_{a_0} is not a permutation polynomial.

Proof. It is a simple matter to confirm $a_0 \in \mathbb{F}_{p^{2d}}^*$. If $p = 2$, then f_{a_0} is not a permutation polynomial by the previous proposition. If p is odd, then

$$\begin{aligned} a_0^{(q-1)/(p^d+1)} &= (\zeta^{(q-1)/2(p^d-1)})^{(q-1)/(p^d+1)} \\ &= (\zeta^{(q-1)/2})^{(q-1)/(p^{2d}-1)} \\ &= (-1)^{1+p^{2d}+\ldots+p^{2d((m/d)-1)}} \\ &= (-1)^{m/d}. \end{aligned}$$

By Theorem 2.1, f_{a_0} is not a permutation polynomial. ▮

Note that if f_a is not a permutation polynomial, we can always write a as $a = a_0\zeta^{i(p^d+1)}$ for some integer i. We define $a_j = a_0\zeta^{j(p^d+1)}$ for all integers j.

Proposition 3.3. *Let e/d be even. Set $t = (p^\alpha + 1)/(p^d + 1)$. There exists a unique element $\gamma \in \mathbb{F}_q^*$ such that $\gamma^t = \zeta$ and $\zeta^{i(p^d+1)} = \gamma^{i(p^\alpha+1)}$ for all integers i. Thus $a_j = a_0\gamma^{j(p^\alpha+1)}$ for all integers j.*

Proof. As $(p^\alpha+1, q-1) = p^d+1$, the monomial X^t is a permutation polynomial. So we can solve uniquely for $\gamma^t = g$. The remainder of the proposition follows immediately. ▮

Theorem 3.3. *Let e/d be even so that $e = 2m$ for some integer m. Define*

$$a_0 = \begin{cases} 1 & \text{if } p = 2 \\ \zeta^{(q-1)/2(p^d-1)} & \text{if } p \text{ odd.} \end{cases}$$

For $a \in \mathbb{F}_q^*$, set $f_a(X) = a^{p^\alpha} X^{p^{2\alpha}} + aX$ and consider the equation

$$f_a(x) + b^{p^\alpha} = 0.$$

(i)If $a \neq a_0\zeta^{s(p^d+1)}$ for any integer s, then the equation can be solved uniquely in x for any choice of $b \in \mathbb{F}_q$.

(ii)If $a = a_0\zeta^{s(p^d+1)}$ for some integer s, then the equation is solvable if and only if $Tr_{2d}(b\gamma^{-s}) = 0$ where $\gamma \in \mathbb{F}_q^*$ is the unique element satisfying $\gamma^{(p^\alpha+1)/(p^d+1)} = \zeta$.

The proof will require the following lemma.

Lemma 3.4. *Let $\mathbb{K}$ be a finite extension of $\mathbb{F}_q$, $q = p^e$, with $[\mathbb{K} : \mathbb{F}_q] = k$. Then for $v \in \mathbb{K}$ we have $Tr_{\mathbb{K}/\mathbb{F}_q}(v) = 0$ if and only if $v = w^{q^t} - w$, with t any integer satisfying $(t, k) = 1$, for some $w \in \mathbb{K}$ dependent on t.*

Proof. There are q^{k-1} distinct elements $v \in \mathbb{K}$ satisfying $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}_q}(v) = 0$. Fix an integer t satisfying $(t, k) = 1$. For any element $w \in \mathbb{K}$ it is clear from the properties of the trace function that $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}_q}(w^{q^t} - w) = 0$. Furthermore, the polynomial $X^{q^t} - X$ has q^{k-1} distinct images over $\mathbb{K}$ as $x^{q^t} - x = y^{q^t} - y$ if and only if $x - y \in \mathbb{F}_q$. Hence every $v \in \mathbb{K}$ which satisfies $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}_q}(v) = 0$ can be written in the form $v = w^{q^t} - w$. ▮

This lemma is an extension of [11, Theorem 2.25].

Proof (Proof of Theorem 3.3). Part (i) follows trivially from Theorems 2.1 and 2.2. We need to establish (ii). Note first that $a_0^{p^\alpha-1} = -1$ in any characteristic, as $a_0 = 1$ in characteristic 2 while odd characteristic follows from α/d being odd. Fix $a_j = a_0\zeta^{j(p^d+1)} = a_0\gamma^{j(p^\alpha+1)}$. Then the equation $f_{a_j}(x) + b^{p^\alpha} = 0$ can be simplified to

$$-b^{p^\alpha} = -a_0\gamma^{jp^\alpha}(\gamma^j x)^{p^{2\alpha}} + a_0\gamma^{jp^\alpha}\gamma^j x.$$

Dividing through by $-a_0\gamma^{jp^\alpha}$ and making a change of variable by setting $y = \gamma^j x$ we obtain the equation

$$y^{p^{2\alpha}} - y = a_0^{-1}(b\gamma^{-j})^{p^\alpha}.$$

By Lemma 3.4, this equation is solvable in y if and only if

$$\mathrm{Tr}_{2d}(a_0^{-1}(b\gamma^{-j})^{p^\alpha}) = 0.$$

Since $a_0 \in \mathbb{F}_{p^{2d}}^*$, this trace mapping is zero if and only if $\mathrm{Tr}_{2d}(b\gamma^{-j}) = 0$. Thus the equation $f_{a_j}(x) + b^{p^\alpha} = 0$ is solvable in $x \in \mathbb{F}_q^*$ if and only if $\mathrm{Tr}_{2d}(b\gamma^{-j}) = 0$. ▮

4. PREVIOUS RESULTS

We shall now review the previous results on the evaluation of $S_\alpha(a,b)$. This recall, along with the previous section, will allow us to provide a more unified treatment of the evaluation of $S_\alpha(a,b)$, especially when e/d is even. Throughout $a \neq 0$. The following results come from the articles [1, 2, 3].

4.1. When e/d is odd

Theorem 4.4. *Let e/d be odd. Then*

$$S_\alpha(a,0) = \begin{cases} 0 & \text{if } p = 2, \\ (-1)^{e-1}\sqrt{q}\ \eta(a) & \text{if } p \equiv 1 \bmod 4, \\ (-1)^{e-1}i^e\sqrt{q}\ \eta(a) & \text{if } p \equiv 3 \bmod 4, \end{cases}$$

where η denotes the multiplicative quadratic character.

Theorem 4.5. *Let $p = 2$, $b \in \mathbb{F}_q^*$ and suppose e/d is odd. Then*

$$S_\alpha(a,b) = S_\alpha(1, bc^{-1})$$

where $c \in \mathbb{F}_q^*$ is the unique element satisfying $c^{2^\alpha+1} = a$. If $Tr_d(b) \neq 1$ then $S_\alpha(1,b) = 0$. If $Tr_d(b) = 1$ then there exists some element $w \in \mathbb{F}_q$

such that $b = w^{2^{2\alpha}} + w + 1$ *and*

$$S_\alpha(1,b) = \chi_1(w^{2^\alpha+1} + w)\left(\frac{2}{e/d}\right)^d 2^{(e+d)/2}$$

where $\left(\frac{2}{s}\right)$ *is the Jacobi symbol.*

Theorem 4.6. *Let* q *and* e/d *be odd, and set* $f(X) = a^{p^\alpha}X^{p^{2\alpha}} + aX$. *Let* x_0 *be the unique solution of the equation* $f(x) = -b^{p^\alpha}$, $b \neq 0$. *Then*

$$S_\alpha(a,b) = \begin{cases} (-1)^{e-1}\sqrt{q}\ \eta(-a)\ \overline{\chi_1(ax_0^{p^\alpha+1})} & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{e-1}i^{3e}\sqrt{q}\ \eta(-a)\ \overline{\chi_1(ax_0^{p^\alpha+1})} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

4.2. When e/d is even

Theorem 4.7. *Let* e/d *be even with* $e = 2m$. *Set* $f(X) = a^{p^\alpha}X^{p^{2\alpha}} + aX$. *Define*

$$a_0 = \begin{cases} 1 & \text{if } p = 2 \\ \zeta^{(q-1)/2(p^d-1)} & \text{if } p \text{ odd.} \end{cases}$$

Then $S_\alpha(a,b) = 0$ *unless the equation* $f(x) = -b^{p^\alpha}$ *is solvable. There are two possibilities.*

(i)If $a \neq a_0\zeta^{s(p^d+1)}$ *for any integer* s*, then, for any choice of* $b \in \mathbb{F}_q$*, the equation has a unique solution* x_0 *and*

$$S_\alpha(a,b) = (-1)^{m/d}p^m\overline{\chi_1(ax_0^{p^\alpha+1})}.$$

(ii)If $a = a_0\zeta^{s(p^d+1)}$ *for some integer* s*, then the equation is solvable if and only if* $Tr_{2d}(b\gamma^{-s}) = 0$ *where* $\gamma \in \mathbb{F}_q^*$ *is the unique element satisfying* $\gamma^{(p^\alpha+1)/(p^d+1)} = \zeta$*. In such cases*

$$S_\alpha(a,b) = -(-1)^{m/d}p^{m+d}\overline{\chi_1(ax_0^{p^\alpha+1})},$$

where x_0 *is any solution to* $f(x) = -b^{p^\alpha}$.

While the statements of those results concerning e/d odd do not warrant further discussion (than that given in the previous articles), the same cannot be said for this single statement for e/d even. Firstly, the cases

$b = 0$ and $b \neq 0$ have previously been dealt with separately. Secondly, it will be seen from a comparison of [2, Theorem 2] and [3, Theorem 5.3(ii)] that, for $b \neq 0$, there appears to be a second possibility in characteristic 2. In fact, this second possibility can be removed. For this reason, we give an abridged proof of this theorem.

Proof (Abridged proof of Theorem 4.7). If $a \neq \zeta^{k+s(p^d+1)}$, then [3, Theorem 5.3(i)] and [2, Theorem 1(ii)] coincide for $b \neq 0$. If $b = 0$ then $x_0 = 0$, and $\chi_1(ax_0^{p^\alpha+1}) = 1$. The results [1, Theorem 2] and [3, Theorem 5.2] for $S_\alpha(a, 0)$ can be seen to match the statement given above.

Let $a = \zeta^{k+s(p^d+1)}$ for a set integer i. For $S_\alpha(a, 0)$, it is easily seen that [1, Theorem 2] and [3, Theorem 5.2] coincide. For $b \neq 0$, [2, Theorem 1(ii)] shows that our result holds for odd characteristic. Although it is assumed throughout [2] that p is odd, only a single part of the entire proof of [2, Theorem 1(ii)] does not hold in characteristic 2. To complete the proof for characteristic 2, we need to show $\mathrm{Tr}_d(ac^{2^\alpha+1}) = 0$ where c is any root of f. Any such $c \neq 0$ satisfies $c^{2^{2\alpha}-1} = a^{1-2^\alpha}$ from which we can see that any root of f satisfies $c^{2^\alpha+1} = \beta a^{-1}$ where $\beta \in \mathbb{F}_{2^d}$. Hence $\mathrm{Tr}_d(ac^{2^\alpha+1}) = \mathrm{Tr}_d(\beta) = 0$ as e/d is even. It remains to show that the case $b = 0$ can be absorbed by the more general statement. So, suppose $b = 0$ and $a = a_0\zeta^{s(p^d+1)} = a_0\gamma^{s(p^\alpha+1)}$. We need to show that $\chi_1(ax_0^{p^\alpha+1}) = 1$ (or, equivalently, $\mathrm{Tr}(ax_0^{p^\alpha+1}) = 0$) for any root x_0 of f (as $f(0) = 0$ and $\chi_1(0) = 1$). Characteristic 2 follows from the preceding argument as $\mathrm{Tr}(ax_0^{p^\alpha+1}) = \mathrm{Tr}_{\mathbb{F}_{p^d}/\mathbb{F}_p}(\mathrm{Tr}_d(ax_0^{p^\alpha+1})) = \mathrm{Tr}_{\mathbb{F}_{p^d}/\mathbb{F}_p}(0) = 0$. In odd characteristic, as $a_0^{p^\alpha} = -a_0$, any root x_0 of f satisfies $(\gamma^j x_0)^{p^{2\alpha}} = \gamma^j x_0$. So $\mathrm{Tr}(ax_0^{p^\alpha+1}) = \mathrm{Tr}_(ax_0^{p^\alpha+1})^{p^\alpha} = -\mathrm{Tr}(ax_0^{p^\alpha+1}) = 0$. ▮

5. FIRST EXAMINATION

Set n to be any positive integer and $t = (n, e)$. Let $f \in \mathbb{F}_q[X]$ and define $N_n(f)$ to be the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of the equation

$$f(x) = y^{p^n} - y.$$

By the orthogonality relations of characters we have

$$\begin{aligned} qN_n(f) &= \sum_{h,x,y\in\mathbb{F}_q} \chi_1\big(hf(x) - h(y^{p^n} - y)\big) \\ &= \sum_{h,x\in\mathbb{F}_q} \left(\chi_1\big(hf(x)\big) \sum_{y\in\mathbb{F}_q} \chi_1(-hy^{p^n} + hy)\right) \\ &= \sum_{h,x\in\mathbb{F}_q} \left(\chi_1\big(hf(x)\big) \sum_{y\in\mathbb{F}_q} \chi_1\big(y^{p^n}(h^{p^n} - h)\big)\right). \end{aligned}$$

The inner sum is q if $h^{p^n} - h = 0$ (so that $h \in \mathbb{F}_{p^t}$), otherwise the inner sum is zero.

Lemma 5.5. *With notation as above,*

$$N_n(f) = \sum_{h\in\mathbb{F}_{p^t}} \sum_{x\in\mathbb{F}_q} \chi_1\left(hf(x)\right).$$

In this article, we wish to determine $N_n(f)$ where $f(X) = aX^{p^\alpha+1} + L(X)$ and $t = (n, e)$ divides (α, e).

For any integer t dividing $d = (\alpha, e)$, define $N_{\alpha,t}(a, b) = N_t(aX^{p^\alpha+1}+bX)$ to be the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of the equation

$$ax^{p^\alpha+1} + bx = y^{p^t} - y,$$

where $a, b \in \mathbb{F}_q$ with $a \neq 0$. We now show that our general problem is equivalent to determining $N_{\alpha,t}(a, b)$ for a particular b which is dependent on the p^t-polynomial L.

Theorem 5.8. *Let n be any integer such that $t = (n, e)$ divides $d = (\alpha, e)$ and $L \in \mathbb{F}_q[X]$ be a p^t-polynomial given by*

$$L(X) = \sum_{i=0}^{e/t-1} b_i X^{p^{ti}}.$$

Set $b = \sum_{i=0}^{e/t-1} b_i^{p^{e-ti}}$ and $f_\alpha(X) = aX^{p^\alpha+1} + L(X)$. Then $N_n(f_\alpha) = N_{\alpha,t}(a, b)$.

Proof. From Lemma 5.5 we have

$$\begin{aligned}
N_n(f_\alpha) &= \sum_{h\in\mathbb{F}_{p^t}} \sum_{x\in\mathbb{F}_q} \chi_1\left(hf_\alpha(x)\right) \\
&= \sum_{h\in\mathbb{F}_{p^t}} \sum_{x\in\mathbb{F}_q} \left(\chi_1(hax^{p^\alpha+1}) \prod_{i=0}^{e/t-1} \chi_1(hb_i x^{p^{ti}}) \right) \\
&= \sum_{h\in\mathbb{F}_{p^t}} \sum_{x\in\mathbb{F}_q} \left(\chi_1(hax^{p^\alpha+1}) \prod_{i=0}^{e/t-1} \chi_1\left(x(hb_i)^{p^{e-ti}}\right) \right) \\
&= \sum_{h\in\mathbb{F}_{p^t}} \sum_{x\in\mathbb{F}_q} \left(\chi_1(hax^{p^\alpha+1}) \prod_{i=0}^{e/t-1} \chi_1(hxb_i^{p^{e-ti}}) \right) \\
&= \sum_{h\in\mathbb{F}_{p^t}} \sum_{x\in\mathbb{F}_q} \chi_1(hax^{p^\alpha+1} + hbx) \\
&= N_{\alpha,t}(a,b).
\end{aligned}$$

∎

Sections 6 and 7 will be concerned with determining $N_{\alpha,t}(a,b)$. Section 8 identifies some curves which meet the Hasse-Weil bound.

6. THE NUMBER OF SOLUTIONS WHEN E/D IS ODD

Throughout this section we assume e/d is odd. We deal with characteristic 2 first.

THEOREM 6.9. *Set $p = 2$. Let e/d be odd and let $c \in \mathbb{F}_q^*$ be the unique element satisfying $c^{2^\alpha+1} = a$. Then $N_{\alpha,t}(a,b) = N_{\alpha,t}(1, bc^{-1})$. If $Tr_d(b) \notin \mathbb{F}_{2^t}^*$ then $N_{\alpha,t}(1,b) = q$. If $Tr_d(b) \in \mathbb{F}_{2^t}^*$ then $N_{\alpha,t}(1,b) = q + S_\alpha(1, b\beta)$ where $\beta \in \mathbb{F}_{2^t}^*$ satisfies $\beta = Tr_d(b)^{-1}$.*

Proof. By Lemma 5.5, we have

$$\begin{aligned}
N_{\alpha,t}(a,b) &= q + \sum_{h\in\mathbb{F}_{2^t}^*}\sum_{x\in\mathbb{F}_q}\chi_1(hax^{2^\alpha+1}+hbx)\\
&= q + \sum_{h\in\mathbb{F}_{2^t}^*}\sum_{x\in\mathbb{F}_q}\chi_1\left(h(cx)^{2^\alpha+1}+hbc^{-1}(cx)\right)\\
&= q + \sum_{h\in\mathbb{F}_{2^t}^*}\sum_{y\in\mathbb{F}_q}\chi_1(hy^{2^\alpha+1}+hbc^{-1}y)\\
&= N_{\alpha,t}(1,bc^{-1}).
\end{aligned}$$

For each $h\in\mathbb{F}_{2^t}^*$ there exists a unique element $\gamma\in\mathbb{F}_{2^t}^*$ satisfying $\gamma^{2^\alpha+1}=h$. Hence, by Lemma 5.5,

$$\begin{aligned}
N_{\alpha,t}(1,b) &= q + \sum_{h\in\mathbb{F}_{2^t}^*}\sum_{x\in\mathbb{F}_q}\chi_1(hx^{2^\alpha+1}+hbx)\\
&= q + \sum_{\gamma\in\mathbb{F}_{2^t}^*}\sum_{x\in\mathbb{F}_q}\chi_1\left((\gamma x)^{2^\alpha+1}+b\gamma^{2^\alpha}(\gamma x)\right)\\
&= q + \sum_{\gamma\in\mathbb{F}_{2^t}^*} S_\alpha(1,b\gamma).
\end{aligned}$$

By Theorems 4.4 and 4.5, $S_\alpha(1,b\gamma)=0$ unless $\mathrm{Tr}_d(b\gamma)=\gamma\mathrm{Tr}_d(b)=1$. If $\mathrm{Tr}_d(b)\notin\mathbb{F}_{2^t}^*$ then $\gamma\mathrm{Tr}_d(b)\neq 1$ for all $\gamma\in\mathbb{F}_{2^t}^*$ and so $N_{\alpha,t}(1,b)=q$. If $\mathrm{Tr}_d(b)\in\mathbb{F}_{2^t}^*$ then there exists a unique element $\beta\in\mathbb{F}_{2^t}^*$ satisfying $\beta=\mathrm{Tr}_d(b)^{-1}$. For all $\gamma\in\mathbb{F}_{2^t}^*\setminus\{\beta\}$ we still have $S_\alpha(1,b\gamma)=0$. The result follows. ▮

Before continuing to odd characteristic, we make the following observations. Firstly, let η denote the quadratic character of $\mathbb{F}_q$ and η' denote the quadratic character of $\mathbb{F}_{p^t}$. Then for any $h\in\mathbb{F}_{p^t}^*$ we have

$$\eta(h)=\begin{cases}1 & \text{if } e/t \text{ is even,}\\ \eta'(h) & \text{if } e/t \text{ is odd.}\end{cases}$$

Secondly, denote by μ_1 the canonical additive character of $\mathbb{F}_{p^t}$. Then we have

$$\chi_1(x)=\mu_1\left(\mathrm{Tr}_t(x)\right)$$

for all $x\in\mathbb{F}_q$.

THEOREM 6.10. *Let $q=p^e$ be odd and $f(X)=a^{p^\alpha}X^{p^{2\alpha}}+aX$. Let e/d be odd and define x_0 to be the unique solution of the equation $f(x)=-b^{p^\alpha}$. There are two possibilities.*

(i)If e/t is odd then $N_{\alpha,t}(a,b) = q$ provided $Tr_t(ax_0^{p^\alpha+1}) = 0$. If $Tr_t(ax_0^{p^\alpha+1}) \neq 0$ then

$$N_{\alpha,t}(a,b) = q + \begin{cases} \eta\big(a\,Tr_t(ax_0^{p^\alpha+1})\big)p^{(e+t)/2} & \textit{if } p \equiv 1 \bmod 4, \\ \eta\big(a\,Tr_t(ax_0^{p^\alpha+1})\big)(-1)^{(3e+t)/2}p^{(e+t)/2} & \textit{if } p \equiv 3 \bmod 4. \end{cases}$$

(ii)If e/t is even then $e = 2m$. If $Tr_t(ax_0^{p^\alpha+1}) = 0$, then

$$N_{\alpha,t}(a,0) = q - \begin{cases} p^m(p^t-1)\ \eta(a) & \textit{if } p \equiv 1 \bmod 4, \\ (-1)^m p^m(p^t-1)\ \eta(a) & \textit{if } p \equiv 3 \bmod 4. \end{cases}$$

If $Tr_t(ax_0^{p^\alpha+1}) \neq 0$, then

$$N_{\alpha,t}(a,b) = q + \begin{cases} p^m\ \eta(a) & \textit{if } p \equiv 1 \bmod 4, \\ (-1)^m p^m\ \eta(a) & \textit{if } p \equiv 3 \bmod 4. \end{cases}$$

Proof. Set $S = \sum_{h\in\mathbb{F}^*_{p^t}} \eta(h)$. Combining Lemma 5.5 and Theorem 4.4 we have

$$N_{\alpha,t}(a,0) = q + \begin{cases} S\eta(a)(-1)^{e-1}p^{e/2} & \text{if } p \equiv 1 \bmod 4, \\ S\eta(a)(-1)^{e-1}i^e p^{e/2} & \text{if } p \equiv 3 \bmod 4, \end{cases}$$

while combining Lemma 5.5 and Theorem 4.6 yields

$$N_{\alpha,t}(a,b) = q + \Bigg(\sum_{h\in\mathbb{F}^*_{p^t}} \eta(-ha)\overline{\chi_1(hax_0^{p^\alpha+1})}\Bigg)(-1)^{e-1}p^{e/2} \qquad (1)$$

if $p \equiv 1 \bmod 4$, and

$$N_{\alpha,t}(a,b) = q + \Bigg(\sum_{h\in\mathbb{F}^*_{p^t}} \eta(-ha)\overline{\chi_1(hax_0^{p^\alpha+1})}\Bigg)(-1)^{e-1}i^{3e}p^{e/2} \qquad (2)$$

if $p \equiv 3 \bmod 4$.

Suppose e/t is odd. As $\eta(h) = \eta'(h)$ for all $h \in \mathbb{F}^*_{p^t}$, then $S = 0$ and we obtain the claimed result ($b = 0$ implies $x_0 = 0$). Let μ_1 be the canonical additive character of $\mathbb{F}_{p^t}$ and $\mu = \mu_{\mathrm{Tr}_t(ax_0^{p^\alpha+1})}$. Recall also $\eta(xy) = \eta(x)\eta(y)$ for all $x, y \in \mathbb{F}^*_q$. We can identify the sum in (1) and (2) as

$$\sum_{h\in\mathbb{F}^*_{p^t}} \eta(-ha)\chi_1(-hax_0^{p^\alpha+1}) = \eta(a)G(\eta',\mu),$$

where $G(\eta', \mu)$ is the Gaussian sum on $\mathbb{F}_{p^t}^*$. If $\mathrm{Tr}_t(ax_0^{p^\alpha+1}) = 0$ then $G(\eta', \mu) = 0$ as μ is the trivial additive character. If $\mathrm{Tr}_t(ax_0^{p^\alpha+1}) \neq 0$ then

$$G(\eta', \mu) = \eta' \left(\mathrm{Tr}_t(ax_0^{p^\alpha+1}) \right) G(\eta', \mu_1),$$

see [11, Theorem 5.12(i)]. Lemma 2.2 can now be used to determine the value of $G(\eta', \mu_1)$. Also, as e/t is odd and $\mathrm{Tr}_t(x) \in \mathbb{F}_{p^t}$ for all $x \in \mathbb{F}_q$, we have $\eta' \left(\mathrm{Tr}_t(ax_0^{p^\alpha+1}) \right) = \eta \left(\mathrm{Tr}_t(ax_0^{p^\alpha+1}) \right)$. Combining these comments with (1) and (2) completes the proof for e/t odd.

Now suppose e/t is even. Then $e = 2m$ and $\eta(h) = 1$ for all $h \in \mathbb{F}_{p^t}^*$. In this case $S = p^t - 1$, giving the result. For $b \neq 0$, the sum in Equations 1 and 2 can be simplified to

$$\eta(a) \sum_{h \in \mathbb{F}_{p^t}^*} \overline{\chi_1(hax_0^{p^\alpha+1})}.$$

Lemma 2.1 can be used to obtain the explicit value of this sum:

$$\sum_{h \in \mathbb{F}_{p^t}^*} \overline{\chi_1(hax_0^{p^\alpha+1})} = \begin{cases} p^t - 1 & \text{if } \mathrm{Tr}_t(ax_0^{p^\alpha+1}) = 0, \\ -1 & \text{otherwise.} \end{cases}$$

The result follows. ▮

7. THE NUMBER OF SOLUTIONS WHEN *E/D* IS EVEN

It remains to deal with the case e/d even. Unlike the case e/d odd, here we are able to give a single treatment for all characteristics.

THEOREM 7.11. *Let e/d be even so that $e = 2m$ for some integer m. Define*

$$a_0 = \begin{cases} 1 & \textit{if } p = 2 \\ \zeta^{(q-1)/2(p^d-1)} & \textit{if } p \textit{ odd.} \end{cases}$$

Then $N_{\alpha,t}(a, b) = q$ unless the equation

$$a^{p^\alpha} x^{p^{2\alpha}} + ax + b^{p^\alpha} = 0 \tag{3}$$

is solvable. There are two possibilities.

(i)If $a \neq a_0\zeta^{s(p^d+1)}$ for any integer s then Equation 3 is always solvable with unique solution x_0. Under this scenario we have

$$N_{\alpha,t}(a,b) = q + \begin{cases} (-1)^{m/d}p^m(p^t-1) & \text{if } Tr_t(ax_0^{p^\alpha+1}) = 0, \\ -(-1)^{m/d}p^m & \text{if } Tr_t(ax_0^{p^\alpha+1}) \neq 0. \end{cases}$$

(ii)If $a = a_0\zeta^{s(p^d+1)}$ for some integer s, then Equation 3 is solvable if and only if $Tr_{2d}(b\gamma^{-s}) = 0$ where $\gamma \in \mathbb{F}_q^*$ is the unique element satisfying $\gamma^{(p^\alpha+1)/(p^d+1)} = \zeta$. In such cases we have

$$N_{\alpha,t}(a,b) = q + \begin{cases} -(-1)^{m/d}p^{m+d}(p^t-1) & \text{if } Tr_t(ax_0^{p^\alpha+1}) = 0, \\ (-1)^{m/d}p^{m+d} & \text{if } Tr_t(ax_0^{p^\alpha+1}) \neq 0, \end{cases}$$

where x_0 is any solution to Equation 3.

Proof. To apply Theorem 4.7 we need to consider the equation

$$(ha)^{p^\alpha}x^{p^{2\alpha}} + hax + (hb)^{p^\alpha} = 0.$$

However, as $h \in \mathbb{F}_{p^t}^*$, this equation is equivalent to

$$a^{p^\alpha}x^{p^{2\alpha}} + ax + b^{p^\alpha} = 0.$$

(Note that this does not imply that $S_\alpha(ha,hb) = S_\alpha(a,b)$.) By Theorem 4.7 we have $S_\alpha(ha,hb) = 0$ if (3) is not solvable, in which case $N_{\alpha,t}(a,b) = q$. For the rest of the proof we assume that (3) is solvable. There are two cases.

If $a \neq a_0\zeta^{s(p^d+1)}$ for any integer s, then Equation 3 is always solvable with unique solution x_0. Combining Theorem 4.7 with Lemma 5.5 gives

$$\begin{aligned} N_{\alpha,t}(a,b) &= q + (-1)^{m/d}p^m \sum_{h\in\mathbb{F}_{p^t}^*} \overline{\chi_1(hax_0^{p^\alpha+1})} \\ &= q + (-1)^{m/d}p^m \sum_{h\in\mathbb{F}_{p^t}^*} \chi_1(-hax_0^{p^\alpha+1}) \\ &= q + (-1)^{m/d}p^m \sum_{h\in\mathbb{F}_{p^t}^*} \chi_1(hax_0^{p^\alpha+1}). \qquad (4) \end{aligned}$$

Applying Lemma 2.1 yields the result.

If $a = a_0\zeta^{s(p^d+1)}$ for some integer s, then Theorem 3.3 states that Equation 3 is solvable if and only if $\mathrm{Tr}_{2d}(b\gamma^{-s}) = 0$. When this holds, Theorem 4.7 tells us that

$$S_\alpha(ha, hb) = -(-1)^{m/d} p^{m+d}\, \overline{\chi_1(hax_0^{p^\alpha+1})}.$$

Following a similar method to our first case we can derive the result. ∎

8. EXAMPLES OF CURVES WHICH MEET THE HASSE-WEIL BOUND

Let us define the curve

$$C(X, Y) = aX^{p^\alpha+1} + L(X) + Y - Y^{p^n}$$

over $\mathbb{F}_q$, $q = p^e$, $t = (n, e)$ dividing (α, e), and L a p^t-polynomial. If degree$(L) \leq p^\alpha$ then [13, Proposition VI.4.1] provides us with the following important facts:

- the curve is absolutely irreducible,
- the genus of the curve is $g = p^\alpha(p^n - 1)/2$.

It is a simple matter to show there is only one point at infinity for this curve and that all points of the curve are non-singular. Thus the number of $\mathbb{F}_q$-rational points defined by the curve C is $1 + N_{\alpha,t}(a, b)$ for a suitable choice of $b \in \mathbb{F}_q$. Our results allow us to determine those curves within the class of Artin-Schreier curves considered in this paper which attain the Hasse-Weil bound and so are either maximal or minimal curves.

Theorem 8.12. *Let $q = p^e$ and select integers n and α such that $t = (n, e)$ divides (α, e). Let $L \in \mathbb{F}_q[X]$ be a p^t-polynomial given by*

$$L(X) = \sum_{i=0}^{e/t-1} b_i X^{p^{ti}}$$

with $b_i = 0$ for all $i > \alpha/t$. Set $b = \sum_{i=0}^{e/t-1} b_i^{p^{e-ti}}$. The number of $\mathbb{F}_q$-rational points on the Artin-Schreier curve described by the equation

$$y^{p^n} - y = ax^{p^\alpha+1} + L(x)$$

attains the Hasse-Weil bound if and only if all of the following conditions are met.

(i)$e = 2m$.

(ii)n *divides* α *and* α *divides* m.

(iii)$a = a_0\zeta^{s(p^\alpha+1)}$ *for some integer* s *where* a_0 *is given by*

$$a_0 = \begin{cases} 1 & \text{if } p = 2 \\ \zeta^{(q-1)/2(p^\alpha-1)} & \text{if } p \text{ odd.} \end{cases}$$

(iv) $Tr_{2\alpha}(b\zeta^{-s}) = 0$ *(so that the equation* $a^{p^\alpha}x^{p^{2\alpha}} + ax + b^{p^\alpha} = 0$ *is solvable with solution* x_0 *say).*

(v) $Tr_t(ax_0^{p^\alpha+1}) = 0$.

In all cases, the curve is maximal if m/α *is odd and minimal if* m/α *is even.*

Suppose $b = 0$ and let x_0 be any solution of the equation $a^{p^\alpha}x^{p^{2\alpha}} + ax = 0$. Then $(ax_0^{p^\alpha+1})^{p^\alpha} = -ax_0^{p^\alpha+1}$. If p is odd, then

$$\begin{aligned} \mathrm{Tr}_t(ax_0^{p^\alpha+1}) &= \mathrm{Tr}_t\left((ax_0^{p^\alpha+1})^{p^\alpha}\right) \\ &= \mathrm{Tr}_t(-ax_0^{p^\alpha+1}) \end{aligned}$$

and so $\mathrm{Tr}_t(ax_0^{p^\alpha+1}) = 0$. If $p = 2$, then $ax_0^{p^\alpha+1} \in \mathbb{F}_{2^\alpha}$. As e/α is even, $\mathrm{Tr}_\alpha(ax_0^{p^\alpha+1}) = 0$ and

$$\begin{aligned} \mathrm{Tr}_t(ax_0^{2^\alpha+1}) &= \mathrm{Tr}_{\mathbb{F}_{2^\alpha}/\mathbb{F}_{2^t}}\left(\mathrm{Tr}_\alpha(ax_0^{2^\alpha+1})\right) \\ &= 0. \end{aligned}$$

So, if $b = 0$, then (iv) and (v) hold trivially.

We end with some comments on the results of Wolfmann in [14]. Let $q = p^t$ and k a positive integer. Wolfmann considered the number of rational points on the Artin-Schreier curve defined over $\mathbb{F}_{q^k}$ by the equation

$$y^q - y = ax^s + b$$

where $a, b \in \mathbb{F}_{q^k}$, $a \neq 0$ and s is any positive integer relatively prime to p. One need only consider the case s dividing $q^k - 1$. Wolfmann succeeded in calculating the number of rational points on these curves in the following scenario:

(i) $k = 2t$.

(ii) there exists a divisor r of t such that $q^r \equiv -1 \bmod s$.

A careful check of the two sets of conditions reveals that, when $L(X) = 0$, the conditions described by Theorem 8.12 satisfy the conditions considered by Wolfmann. There is therefore some overlap between Theorem 8.12 and Corollaries 1,2 and 3 of [14]. The two results are, however, not equivalent.

REFERENCES

1. R.S. Coulter, *Explicit evaluations of some Weil sums*, Acta Arith. **83** (1998), 241–251.
2. ———, *Further evaluations of Weil sums*, Acta Arith. **86** (1998), 217–226.
3. ———, *On the evaluation of a class of Weil sums in characteristic 2*, New Zealand J. Math. **28** (1999), 171–184.
4. R. Fuhrmann and F. Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Math. **89** (1996), 103–106.
5. G. van der Geer and M. van der Vlugt, *Reed-Muller codes and supersingular curves, I*, Compositio Math. **84** (1992), 333–367.
6. ———, *Fibre products of Artin-Schreier curves and generalized Hamming weights of codes*, J. Combin. Theory Ser. A **70** (1995), 337–348.
7. ———, *On the existence of supersingular curves of given genus*, J. reine angew. Math. **458** (1995), 53–61.
8. A. Hefez and N. Kakuta, *Polars of Artin-Schreier curves*, Acta Arith. **77** (1996), 57–70.
9. D. Jungnickel, *Finite Fields: Structure and Arithmetics*, Bibliographisches Institut, Mannheim, Leipzig, Vienna, 1993.
10. G. Lachaud, *Artin-Schreier curves, exponential sums, and the Carlitz-Uchiyama bound for geometric codes*, J. Number Theory **39** (1991), 18–40.
11. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).
12. H-G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. reine angew. Math. **457** (1994), 185–188.
13. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.
14. J. Wolfmann, *The number of points on certain algebraic curves over finite fields*, Comm. Algebra **17** (1989), 2055–2060.