ACTA ARITHMETICA
164.2 (2014)

Complete arcs arising from a generalization of the Hermitian curve

by

Herivelto Borges (São Carlos), Beatriz Motta (Juiz de Fora)
and Fernando Torres (Campinas)

1. Introduction. Let $\mathbb{F}_q$ and $\mathrm{PG}(2,q)$ denote the finite field of order q and the projective plane over $\mathbb{F}_q$, respectively. A pointset $\mathcal{K} \subseteq \mathrm{PG}(2,q)$ of size N is called an *arc* of *degree* d, or simply an (N,d)-*arc*, if no line of $\mathrm{PG}(2,q)$ meets $\mathcal{K}$ in more than d points. An (N,d)-arc $\mathcal{K}$ is called *complete* if it is not contained in an $(N+1,d)$-arc, that is, if for every $P \in \mathrm{PG}(2,q) \setminus \mathcal{K}$ there is a line through P meeting $\mathcal{K}$ in exactly d points. A basic problem in finite geometry is the existence and uniqueness of complete arcs. For basic facts on these objects, the reader is referred to the book [14] by Hirschfeld.

Throughout this paper by a *plane curve* we shall mean a projective, geometrically irreducible plane curve. Let $\mathcal{X}$ be a plane curve of degree d defined over $\mathbb{F}_q$. The set of the $\mathbb{F}_q$-rational points of $\mathcal{X}$ in $\mathrm{PG}(2,q)$, denoted by $\mathcal{X}(\mathbb{F}_q)$, is a natural example of an (N,d)-arc with $N = \#\mathcal{X}(\mathbb{F}_q)$ (Bézout's Theorem). The problem of the completeness of $\mathcal{X}(\mathbb{F}_q)$ as an (N,d)-arc was raised by Hirschfeld and Voloch in 1988 [16]. For instance, if $\mathcal{X}$ is a conic in odd characteristic or the *Hermitian curve*, the plane curve defined by the affine equation $y^{q+1} = x^q + x$ over $\mathbb{F}_{q^2}$, then the set of rational points is a complete arc (see for example [14, Ch. 8, Lemma 7.20]). A generalization of the Hermitian curve is given by an $\mathbb{F}_q$-*Frobenius nonclassical* plane curve, that is, a plane curve over $\mathbb{F}_q$ such that the $\mathbb{F}_q$-Frobenius map takes each nonsingular point of the curve to the tangent line at that point (cf. [13]). Such curves are usually equipped with a large number of rational points (loc. cit.) so that one can expect to handle examples of complete arcs of large size compared with their degrees. Recently Giulietti et al. [12] and Borges [1] studied the set of $\mathbb{F}_q$-rational points of further examples of

2010 *Mathematics Subject Classification*: Primary 05B25, 11T23, 11T24; Secondary 14H25.
Key words and phrases: finite field, plane arc, Hermitian curve, Artin–Schreier curve.

DOI: 10.4064/aa164-2-1

$\mathbb{F}_q$-Frobenius nonclassical plane curves that also give rise to complete arcs. For background on curves over finite fields we refer to the book [15].

Any (N, d)-arc arising from a plane curve gives rise to an algebraic geometry (AG) code with parameters $[N, 3, N - d']$, $d' \le d$ (see, for example, [22, Sect. 3.1.1]). Here, if the arc is complete, the corresponding code has minimum distance equal to $N - d$ and it cannot be extended to a code with larger minimum distance. This is analogous to the well known relation between complete $(N, 2)$-arcs and nonextendable MDS codes (loc. cit.).

In this article we investigate (N, d)-arcs derived from the set of rational points of a Frobenius nonclassical curve introduced by Borges and Conceição in [2] (see Section 2 here) and which is a natural generalization of the Hermitian curve. Our main result is Theorem 5.4. The computation of the degree of the corresponding arcs is closely related to the study of rational points of a class of Artin–Schreier curves (see (2.2)); here Coulter's approach [5–8] is used. By taking advantage of the aforementioned computation regarding rational points, we slightly extend some results of Wolfmann [23] and Coulter [8] by pointing out some examples of maximal curves of Artin–Schreier type (see Theorem 4.1).

2. The curve $\mathcal{H}$. Let q be a power of a prime p. Let ℓ be an integer with $\ell \ge 2$ and define $r = r(\ell)$ as the smallest integer $r \ge \ell/2$ such that $\gcd(\ell, r) = 1$; that is,

$$r = \begin{cases} 1 & \text{if } \ell = 2, \\ \ell/2 + 1 & \text{if } \ell \equiv 0 \pmod 4, \\ \ell/2 + 2 & \text{if } \ell \ge 6,\ \ell \equiv 2 \pmod 4, \\ (\ell + 1)/2 & \text{if } \ell \text{ is odd.} \end{cases} \tag{2.1}$$

For a symbol z, set

$$\mathbf{T}(z) := z^{q^{\ell-1}} + z^{q^{\ell-2}} + \cdots + z.$$

In particular, $\mathbf{T} : \mathbb{F}_{q^\ell} \to \mathbb{F}_q$ denotes the trace map from $\mathbb{F}_{q^\ell}$ to $\mathbb{F}_q$. In [2] the plane curve $\mathcal{H}$ defined by the affine equation

$$\mathbf{T}(y) = \mathbf{T}(x^{q^r+1}) \pmod{x^{q^\ell} - x}$$

over $\mathbb{F}_{q^\ell}$ was considered. The main properties of this curve are listed below.

THEOREM 2.1 ([2]). *Let ℓ and r be as above. Suppose $p > 2$ if $\ell = 2$. The curve $\mathcal{H}$ has degree $q^{\ell-1} + q^{r-1}$, genus $q^r(q^{\ell-1} - 1)/2$, and its number of $\mathbb{F}_{q^\ell}$-rational points in $\mathrm{PG}(2, q^\ell)$ is $q^{2\ell-1} + 1$. It has just one point at infinity of projective coordinates $(X : Y : Z) = (0 : 1 : 0)$, which is also its only singular point whenever $\ell \ge 3$. Furthermore, the curve is $\mathbb{F}_{q^\ell}$-Frobenius nonclassical.*

Notice that the number of $\mathbb{F}_{q^\ell}$-rational points of the nonsingular model of $\mathcal{H}$ is also $q^{2\ell-1}+1$ (loc. cit.). If $p>2$ and $\ell=2$, then it is clear that $\mathcal{H}$ is the Hermitian curve and thus $\mathcal{H}(\mathbb{F}_{q^2})$ is a well known complete $(q^3+1, q+1)$-arc. Here we focus on the more complicated case $\ell \geq 3$.

REMARK 2.2. In [10], Garcia and Stichtenoth considered the plane curve $\mathcal{C}$ defined by the affine equation

$$y^{q^{\ell-1}} + \cdots + y^q + y = x^{q^{\ell-1}+q^{\ell-2}} + \cdots + x^{q+1}$$

over $\mathbb{F}_{q^\ell}$ with $\ell \geq 2$; see also [3, 18, 19]. This curve has degree $q^{\ell-1}+q^{\ell-2}$, genus $q^{\ell-1}(q^{\ell-1}-1)/2$ and $q^{2\ell-1}+1$ $\mathbb{F}_{q^\ell}$-rational points in $\mathrm{PG}(2,\mathbb{F}_{q^\ell})$. The nonsingular model of $\mathcal{C}$ also has $q^{2\ell-1}+1$ rational points over $\mathbb{F}_{q^\ell}$ (loc. cit.).

For $\ell=2$ and $p>2$ both plane curves $\mathcal{C}$ and $\mathcal{H}$ are the Hermitian curve. For $\ell=3$, they define the same curve. For $\ell=4$ and $\ell=6$, their degrees, genus and numbers of rational points are the same. In general, the numbers of their rational points coincide; however, the degree and genus of $\mathcal{H}$ are smaller than those of $\mathcal{C}$. In particular, the ratios (number of rational points)/degree and (number of rational points)/genus are better on the curve $\mathcal{H}$. Such rates are particularly important, for example in the context of finite geometry or coding theory via AG codes (see, for example, [15]).

As mentioned in the Introduction, the main goal of this paper is the study of the arc $\mathcal{K} := \mathcal{H}(\mathbb{F}_{q^\ell})$ in $\mathrm{PG}(2,q^\ell)$ arising from the set of $\mathbb{F}_{q^\ell}$-rational points of the plane curve $\mathcal{H}$ (see Section 5). To deal with the parameters of $\mathcal{K}$, the Frobenius nonclassicality property of $\mathcal{H}$ is not needed. In fact, only the degree and the number of $\mathbb{F}_{q^\ell}$-rational points of $\mathcal{H}$ stated in Theorem 2.1 are used. The approach is the natural one: consider $\mathbb{F}_{q^\ell}$-lines $\mathcal{L}: y+bx+c=0$ and count the number $M_\ell(b,c)$ of $\mathbb{F}_{q^\ell}$-rational points of $\mathcal{H}$ lying on $\mathcal{L}$. This number is related to the degree d of $\mathcal{H}$ so that $M_\ell(b,c) \leq d$. Then $M_\ell(b,c)$ is equal to the number of $\mathbb{F}_{q^\ell}$-solutions of the one-variable equation

$$\mathbf{T}(x^{q^r+1} + bx + c) = 0$$

and thus it can be computed by means of the relation

$$N_\ell(b,c) = qM_\ell(b,c), \tag{2.2}$$

where $N_\ell(b,c)$ is the number of $\mathbb{F}_{q^\ell}$-affine points of the Artin–Schreier curve of the type

$$y^q - y = x^{q^r+1} + bx + c, \tag{2.3}$$

with r defined as in (2.1).

Thus we are led to the problem of the computation of rational points on curves over finite fields of Artin–Schreier type. Such computations were already performed by several authors. For example, in 1989 Wolfmann [23]

used quadratic forms to calculate the number of $\mathbb{F}_{q^\ell}$-affine points of Artin–Schreier curves of the type

$$y^q - y = ax^s + c,$$

where $a \in \mathbb{F}_{q^\ell}^*$, $c \in \mathbb{F}_{q^\ell}$, ℓ is even and s is a certain divisor of $q^\ell - 1$. Later on, in 2002, Coulter [8] used facts on exponential sums [5–7] to compute the number of $\mathbb{F}_q$-rational points on Artin–Schreier curves of the type

$$y^{p^n} - y = ax^{p^\alpha+1} + L(x), \tag{2.4}$$

where $a \in \mathbb{F}_q^*$, $t := \gcd(n, e)$ divides $u := \gcd(\alpha, e)$, with $q = p^e$, and $L(x) \in \mathbb{F}_q[x]$ is a p^t-linearized polynomial. We recall that Wolfmann's and Coulter's results have some overlap but they are not equivalent.

3. The number of rational affine points of a class of Artin–Schreier curves. Throughout this section let $q = p^n$ be a power of a prime p, and let ℓ and r be integers with $\ell \geq 2$ and $r \geq 0$. By considering the curve (2.3) and by taking into account the type of the curve (2.4) studied by Coulter, we are led to compute the number of $\mathbb{F}_{q^\ell}$-affine points of Artin–Schreier curves of the type

$$y^q - y = ax^{q^r+1} + L(x) + c,$$

where $a \in \mathbb{F}_{q^\ell}^*$, $c \in \mathbb{F}_{q^\ell}$ and $L(x) = \sum_{i=0}^{\ell-1} b_i x^{q^i} \in \mathbb{F}_{q^\ell}[x]$ is a q-linearized polynomial. If we set $b := \sum_{i=0}^{\ell-1} b_i^{q^{\ell-i}}$, arguing as in [8, Thm. 5.8], then computing $\mathbb{F}_{q^\ell}$-rational affine points of curves as above is in fact equivalent to computing $\mathbb{F}_{q^\ell}$-affine points of Artin–Schreier curves of the type

$$y^q - y = ax^{q^r+1} + bx + c, \tag{3.1}$$

where $a \in \mathbb{F}_{q^\ell}^*$, $b, c \in \mathbb{F}_{q^\ell}$. This observation is useful in computing the degree of the arcs in Section 5.

Let $N_{\ell,r}(a, b, c)$ denote the number of $\mathbb{F}_{q^\ell}$-affine points of the curve (3.1). By [8, Lemma 5.5] we have an exponential sum of the type

$$N_{\ell,r}(a, b, c) = \sum_{h \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_{q^\ell}} \chi_1(hax^{q^r+1} + hbx + hc),$$

where $\chi_1(x) = \exp(2\pi\sqrt{-1}\,\mathbf{t}(x)/p)$ is the canonical additive character of $\mathbb{F}_{q^\ell}$ with $\mathbf{t} : \mathbb{F}_{q^\ell} \to \mathbb{F}_p$ being the absolute trace map. For $A, B, C \in \mathbb{F}_{q^\ell}$ we consider the following Weil sum on $\mathbb{F}_{q^\ell}$:

$$R_{\ell,r}(A, B, C) := \sum_{x \in \mathbb{F}_{q^\ell}} \chi_1(Ax^{q^r+1} + Bx + C).$$

Thus

$$N_{\ell,r}(a, b, c) = \sum_{h \in \mathbb{F}_q} R_{\ell,r}(ha, hb, hc). \tag{3.2}$$

It turns out that $R_{\ell,r}(A,B,C) = R_{\ell,r}(A,B,0)\chi_1(C)$, where $R_{\ell,r}(A,B,0)$ was obtained by Coulter [5–7]. Its computation depends on properties of certain polynomials over $\mathbb{F}_{q^\ell}$ such as those in Remark 3.1 below (see also Remark 5.2).

REMARK 3.1. Let ℓ and r be integers with $\ell \geq 2$ and $r \geq 0$. Suppose that ℓ/u is odd, where $u = \gcd(\ell, r)$. Let p be the characteristic of $\mathbb{F}_{q^\ell}$. Let $\mathbf{T}_u : \mathbb{F}_{q^\ell} \to \mathbb{F}_{q^u}$ be the trace map.

(1) If $p = 2$, then $\gcd(q^r+1, q^\ell-1) = 1$ [7, Lemma 2.1] and thus x^{q^r+1} is a permutation polynomial over $\mathbb{F}_{q^\ell}$ and hence over $\mathbb{F}_q$. Moreover, for $b \in \mathbb{F}_{q^\ell}$ with $\mathbf{T}_u(b) = 1$, the equation $x^{q^{2r}} + x + 1 = b$ has a solution in $\mathbb{F}_{q^\ell}$ (see [7, remark after the proof of Theorem 4.2]).

(2) If $p > 2$, then $f(x) = a^{q^r} x^{q^{2r}} + ax$ with $a \in \mathbb{F}_{q^\ell}^*$ is also a permutation polynomial over $\mathbb{F}_{q^\ell}$ (see [6, remark after Lemma 2.2]).

From Theorems 4.4–4.7 in [8] we can now compute the sum $R_{\ell,r}(a,b,c)$ as follows.

LEMMA 3.2. *Let $q = p^n$ be a power of a prime p. Let ℓ and r be integers with $\ell \geq 2$ and $r \geq 0$. Set $u = \gcd(\ell, r)$. Let $a, b, c \in \mathbb{F}_{q^\ell}$, $a \neq 0$. Let η_1 be the quadratic character of $\mathbb{F}_{q^\ell}$ and χ_1 be the canonical additive character of $\mathbb{F}_{q^\ell}$. Let $f(x) = a^{q^r} x^{q^{2r}} + ax$ (cf. Remark* 3.1(2) *above).*

(1) *Let ℓ/u be odd. Then*

$$R_{\ell,r}(a,0,c) = \begin{cases} 0 & \text{if } p = 2, \\ (-1)^{n\ell-1} q^{\ell/2} \eta_1(a)\chi_1(c) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{n\ell-1}(-1)^{n\ell/2} q^{\ell/2} \eta_1(a)\chi_1(c) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

For $b \neq 0$, the following cases arise:

(i) *If $p = 2$ and $h \in \mathbb{F}_{q^\ell}$, then*

$$R_{\ell,r}(ah, bh, ch) = R_{\ell,r}(h, ba_1{}^{-1}h, ch),$$

where $a_1 \in \mathbb{F}_{q^\ell}^*$ is the solution of $x^{q^r+1} = a$. Moreover, let $\mathbf{T}_u : \mathbb{F}_{q^\ell} \to \mathbb{F}_{q^u}$ be the trace map. Then $R_{\ell,r}(1,b,c) = 0$ provided that $\mathbf{T}_u(b) \neq 1$; otherwise, there is $w \in \mathbb{F}_{q^\ell}$ such that $b = w^{q^{2r}} + w + 1$ and

$$R_{\ell,r}(1,b,c) = \chi_1(w^{q^r+1} + w) \left(\frac{2}{\ell/u}\right)^{nu} q^{(\ell+u)/2} \chi_1(c),$$

where the Jacobi symbol $\left(\frac{2}{v}\right)$ is defined by the formula

$$\left(\frac{2}{v}\right) = \begin{cases} 1 & \text{if } v \equiv \pm 1 \pmod 8, \\ -1 & \text{if } v \equiv \pm 3 \pmod 8. \end{cases}$$

(ii) *If $p > 2$, then $R_{\ell,r}(a,b,c)$ is given by*

$$\begin{cases} (-1)^{n\ell-1} q^{\ell/2} \eta_1(-a) \overline{\chi_1(a x_0^{q^r+1})} \chi_1(c) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{n\ell-1} i^{3n\ell} q^{\ell/2} \eta_1(-a) \overline{\chi_1(a x_0^{q^r+1})} \chi_1(c) & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where $x_0 \in \mathbb{F}_{q^\ell}$ is the solution of $f(x) = -b^{q^r}$ and $i = \sqrt{-1}$.

(2) *Let ℓ/u be even.*

(i) *If $f(x) = -b^{q^r}$ has no solution in $\mathbb{F}_{q^\ell}$, then $R_{\ell,r}(a,b,c) = 0$.*

(ii) *If $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^\ell}$ and $x_0 \in \mathbb{F}_{q^\ell}$ is the solution of $f(x) = -b^{q^r}$, then*

$$R_{\ell,r}(a,b,c) = (-1)^{\ell/2u} q^{\ell/2} \overline{\chi_1(a x_0^{q^r+1})}\, \chi_1(c).$$

(iii) *If $f(x)$ is not a permutation polynomial but $f(x) = -b^{q^r}$ has a solution x_0 in $\mathbb{F}_{q^\ell}$, then*

$$R_{\ell,r}(a,b,c) = (-1)^{\ell/2u+1} q^{\ell/2+u} \overline{\chi_1(a x_0^{q^r+1})}\, \chi_1(c).$$

Theorems 3.3, 3.5 and 3.6 compute $N_{\ell,r}(a,b,c)$. We begin with the case $p = 2$ and ℓ/u odd; the final result is closely related to [8, Thm. 6.9].

THEOREM 3.3. *Let*

(a) $q = 2^n$;
(b) ℓ *and* r *be integers with* $\ell \geq 2$ *and* $r \geq 0$ *such that* ℓ/u *is odd, where* $u = \gcd(\ell, r)$;
(c) $\mathbf{T}_u : \mathbb{F}_{q^\ell} \to \mathbb{F}_{q^u}$ *be the trace map;*
(d) $a, b, c \in \mathbb{F}_{q^\ell}$, $a \neq 0$;
(e) $a_1 \in \mathbb{F}_{q^\ell}^*$ *be the solution of* $x^{q^r+1} = a$.

Then $N_{\ell,r}(a,b,c) = N_{\ell,r}(1, b a_1^{-1}, c)$. If $\mathbf{T}_u(b) \notin \mathbb{F}_q^*$, then $N_{\ell,r}(1,b,c) = q^\ell$; otherwise,

$$N_{\ell,r}(1,b,c) = q^\ell + \chi_1(\omega^{q^r+1} + \omega) \left(\frac{2}{\ell/u}\right)^{nu} q^{(\ell+u)/2} \chi_1(\mathbf{T}_u(b)^{-2} c),$$

where $\omega \in \mathbb{F}_{q^\ell}$ is such that $b \mathbf{T}_u(b)^{-1} = \omega^{q^{2r}} + \omega + 1$, and $\left(\frac{2}{v}\right)$ is the Jacobi symbol defined above.

Proof. We use Lemma 3.2(1)(i). The first part is clear from (3.2). Write

$$N_{\ell,r}(1,b,c) = q^\ell + \sum_{h \in \mathbb{F}_q^*} R_{\ell,r}(h, hb, hc).$$

For each $h \in \mathbb{F}_q^*$, $R_{\ell,r}(h,hb,hc) = R_{\ell,r}(1, h_1 b, h_1^2 c)$ with $h_1 \in \mathbb{F}_q^*$ such that ${h_1}^{q^r+1} = h$. If $\mathbf{T}_u(b) \notin \mathbb{F}_q^*$, then $\mathbf{T}_u(h_1 b) \neq 1$ and hence $R(h,hb,h,c) = 0$ so that $N_{\ell,r}(1,b,c) = q^\ell$. Let $\mathbf{T}_u(b) \in \mathbb{F}_q^*$; then $\mathbf{T}_u(h_1 b) = 1$ if and only if

$h_1 = \mathbf{T}_u(b)^{-1}$, so that

$$N_{\ell,r}(1,b,c) = q^\ell + R_{\ell,r}(1, h_1 b, h_1^2 c),$$

and the result follows. ∎

We recall next some results regarding Gaussian sums over finite fields.

LEMMA 3.4. *Let $\mathbb{F}_q$ be the finite field of order $q = p^n$ with p a prime. Let η be the quadratic character of $\mathbb{F}_q$ and let χ be the canonical additive character of $\mathbb{F}_q$. For $F \in \mathbb{F}_q$, let $\chi^F(h) := \chi(Fh)$ for $h \in \mathbb{F}_q$.*

(i) *Set $G(\eta, \chi^F) := \sum_{h \in \mathbb{F}_q^*} \eta(h)\chi^F(h)$. Then*

$$G(\eta, \chi^F) = \begin{cases} 0 & \text{if } F = 0, \\ (-1)^{n-1} q^{1/2}\, \eta(F) & \text{if } F \neq 0,\ p \equiv 1 \pmod 4, \\ (-1)^{n-1}(-1)^{n/2} q^{1/2} \eta(F) & \text{if } F \neq 0,\ p \equiv 3 \pmod 4. \end{cases}$$

(ii) *We have*

$$G(1, \chi^F) := \sum_{h \in \mathbb{F}_q^*} \chi^F(h) = \begin{cases} q-1 & \text{if } F = 0, \\ -1 & \text{if } F \neq 0. \end{cases}$$

Proof. (i) For $F = 0$, see [17, Thm. 5.4]. If $F \neq 0$, the result follows from Theorems 5.12(i) and 5.15 in [17].

(ii) This follows from relation (5.8) in [17, p. 192]. ∎

The following result is closely related to [8, Thm. 6.10].

THEOREM 3.5. *Let*

(a) $q = p^n$ *be a power of a prime* $p > 2$;
(b) ℓ *and* r *be integers with* $\ell \geq 2$ *and* $r \geq 0$ *such that* ℓ/u *is odd, where* $u = \gcd(\ell, r)$;
(c) $a, b, c \in \mathbb{F}_{q^\ell}$, $a \neq 0$;
(d) $\mathbf{T} : \mathbb{F}_{q^\ell} \to \mathbb{F}_q$ *be the trace map*;
(e) η_1 *be the quadratic character of* $\mathbb{F}_{q^\ell}$;
(f) $f(x) = a^{q^r} x^{q^{2r}} + ax$ *and* $x_0 \in \mathbb{F}_{q^\ell}$ *be the solution of* $f(x) = -b^{q^r}$;
(g) $c_1 = a x_0^{q^r+1} - c$.

Then there are two cases:

(1) *Let ℓ be odd. If $\mathbf{T}(c_1) = 0$, then $N_{\ell,r}(a,b,c) = q^\ell$; otherwise, $N_{\ell,r}(a,b,c)$ is given by*

$$q^\ell + \begin{cases} q^{(\ell+1)/2} \eta_1(a\mathbf{T}(c_1)) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{n(\ell+1)/2} q^{(\ell+1)/2} \eta_1(a\mathbf{T}(c_1)) & \text{if } p \equiv 3 \pmod 4,\ b = 0, \\ (-1)^{n(3\ell+1)/2} q^{(\ell+1)/2} \eta_1(a\mathbf{T}(c_1)) & \text{if } p \equiv 3 \pmod 4,\ b \neq 0. \end{cases}$$

(2) *Let ℓ be even. Then $N_{\ell,r}(a,b,c)$ is given by*

$$q^\ell + \begin{cases} (-1)q^{\ell/2}(q-1)\eta_1(a) & \text{if } p \equiv 1 \pmod 4,\ \mathbf{T}(c_1)=0,\\ q^{\ell/2}\eta_1(a) & \text{if } p \equiv 1 \pmod 4,\ \mathbf{T}(c_1)\neq 0,\\ (-1)^{1+n\ell/2}q^{\ell/2}(q-1)\eta_1(a) & \text{if } p \equiv 3 \pmod 4,\ \mathbf{T}(c_1)=0,\\ (-1)^{n\ell/2}q^{\ell/2}\eta_1(a) & \text{if } p \equiv 3 \pmod 4,\ \mathbf{T}(c_1)\neq 0. \end{cases}$$

Proof. Let η be the quadratic character of $\mathbb{F}_q$ and χ be the canonical additive character of $\mathbb{F}_q$. By the transitivity of trace maps, $\chi_1 = \chi \circ \mathbf{T}$. Concerning the quadratic characters of $\mathbb{F}_{q^\ell}$ and $\mathbb{F}_q$, for $h \in \mathbb{F}_q^*$ we have $\eta_1(h) = \eta(h)$ if ℓ is odd; otherwise $\eta_1(h) = 1$.

Let ℓ be odd. Let $p \equiv 1 \pmod 4$. Then, from (3.2) and Lemma 3.2(1),

$$N_{\ell,r}(a,0,c) = q^\ell + (-1)^{n\ell-1}q^{\ell/2}\eta_1(a)G(\eta,\chi^F),$$

where $G(\eta,\chi^F)$ is the Gaussian sum in Lemma 3.4 with $F = \mathbf{T}(c_1)$, and the result follows. The case $p \equiv 3 \pmod 4$ is similar.

For ℓ even, we use the Gaussian sum $G(1,\chi^F)$ of Lemma 3.4. ∎

The next result is close to [8, Thm. 7.11].

THEOREM 3.6. *Let*

(a) $q = p^n$ *be the power of a prime* p;
(b) ℓ *and* r *be integers with* $\ell \geq 2$ *and* $r \geq 0$ *such that* ℓ/u *is even with* $u = \gcd(\ell, r)$;
(c) $\mathbf{T} : \mathbb{F}_{q^\ell} \to \mathbb{F}_q$ *be the trace map*;
(d) $a, b, c \in \mathbb{F}_{q^\ell}$, $a \neq 0$;
(e) $f(x) = a^{q^r}x^{q^{2r}} + ax$.

Suppose that $f(x) = -b^{q^r}$ has no roots in $\mathbb{F}_{q^\ell}$. Then $N_{\ell,r}(a,b,c) = q^\ell$; otherwise, let $x_0 \in \mathbb{F}_{q^\ell}$ be a root of $f(x) = -b^{q^r}$. Set $c_1 = ax_0^{q^r+1} - c$.

(1) *If $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^\ell}$, then*

$$N_{\ell,r}(a,b,c) = q^\ell + \begin{cases} (-1)^{\ell/2u}q^{\ell/2}(q-1) & \text{if } \mathbf{T}(c_1)=0,\\ (-1)^{\ell/2u+1}q^{\ell/2} & \text{if } \mathbf{T}(c_1)\neq 0. \end{cases}$$

(2) *If $f(x)$ is not a permutation polynomial, then*

$$N_{\ell,r}(a,b,c) = q^\ell + \begin{cases} (-1)^{\ell/2u+1}q^{\ell/2+u}(q-1) & \text{if } \mathbf{T}(c_1)=0,\\ (-1)^{\ell/2u}q^{\ell/2+u} & \text{if } \mathbf{T}(c_1)\neq 0. \end{cases}$$

Proof. The first part follows from (3.2) and Lemma 3.2(2)(i). If $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^\ell}$ with x_0 as above, by (3.2) and Lemma 3.2(2)(ii) we have

$$N_{\ell,r}(a,b,c) = q^\ell + (-1)^{\ell/2u}q^{\ell/2}G(1,\chi^F)$$

with $F = \mathbf{T}(c_1)$, and the result follows from Lemma 3.4. If $f(x)$ is not a permutation polynomial, the proof is similar. ∎

4. On maximal Artin–Schreier curves. Let $q = p^n$ be a power of a prime p and let ℓ and r be integers with $\ell \geq 2$ and $r \geq 0$. Let $a, b, c \in \mathbb{F}_{q^\ell}$, $a \neq 0$. In Section 3 we computed the number $N_{\ell,r}(a,b,c)$ of $\mathbb{F}_{q^\ell}$-rational affine points of the Artin–Schreier curve of the type (3.1), namely

$$y^q - y = ax^{q^r+1} + bx + c.$$

This curve has exactly one singular point which is unibranched; thus the number of $\mathbb{F}_{q^\ell}$-rational points of its nonsingular model over $\mathbb{F}_{q^\ell}$, denoted by $\mathcal{X} = \mathcal{X}_{\ell,r}(a,b,c)$, is exactly

$$N_{\ell,r}(a,b,c) + 1.$$

The Hasse–Weil bound (see [20, Thm. V.2.3], [15, Thm. 9.18]) asserts that

$$|\#\,\mathcal{X}(\mathbb{F}_{q^\ell}) - (q^\ell + 1)| \leq 2gq^{\ell/2},$$

where g is the genus of the curve. Here we have $g = q^r(q-1)/2$ (see, for example, [20, Prop. VI.4.1]). We are looking for examples of $\mathbb{F}_{q^\ell}$-*maximal curves* of the type $\mathcal{X}_{\ell,r}(a,b,c)$, that is, those whose number of $\mathbb{F}_{q^\ell}$-rational points attains the Hasse–Weil upper bound; equivalently, those curves such that

$$N_{\ell,r}(a,b,c) = q^\ell + q^{\ell/2+r}(q-1). \tag{4.1}$$

It then follows that $q^{\ell/2}$ must be an integer, that is, $n\ell$ must be an even integer. See [15, Ch. 10] for general results on maximal curves.

We consider two cases according to the parity of ℓ/u with $u := \gcd(\ell, r)$.

Case A: ℓ/u is odd. If $p = 2$, Theorem 3.3 does not provide an example where (4.1) holds true. Let $p > 2$. Let $f(x)$ and c_1 be as in Theorem 3.5 (cf. Remark 3.1). If $\mathcal{X}_{\ell,r}(a,b,c)$ is $\mathbb{F}_{q^\ell}$-maximal, Theorem 3.5 implies that ℓ must be even, $r = 0$ and $\mathbf{T}(c_1) = 0$. Under these conditions, the curve $\mathcal{X}_{\ell,0}(a,b,c)$ is $\mathbb{F}_{q^\ell}$-maximal if and only if either $p \equiv 1 \pmod 4$ and a is not a square in $\mathbb{F}^*_{q^\ell}$, or $p \equiv 3 \pmod 4$, $a \in \mathbb{F}^*_{q^\ell}$ is a square and $n\ell/2$ is odd, or $p \equiv 3 \pmod 4$, $a \in \mathbb{F}^*_{q^\ell}$ is not a square and $n\ell/2$ is even.

Case B: ℓ/u is even. Thus $r \geq 1$. By Theorem 3.6, a necessary condition to have (4.1) is that $f(x) = -b^{q^r}$ has a root in $\mathbb{F}_{q^\ell}$ and $\mathbf{T}(c_1) = 0$, where $f(x)$ and c_1 are as in Case A above. Under these conditions, $\mathcal{X}_{\ell,r}(a,b,c)$ is $\mathbb{F}_{q^\ell}$-maximal if and only if $u = \gcd(\ell, r) = r$ and $\ell/(2u)$ is odd.

We summarize the above computations in the following.

Theorem 4.1. *Let*

(a) $q = p^n$ *be a power of a prime* p;
(b) ℓ *and* r *be integers with* $\ell \geq 2$ *and* $r \geq 0$;

(c) $\mathbf{T} : \mathbb{F}_{q^\ell} \to \mathbb{F}_q$ *be the trace map*;
(d) $a, b, c \in \mathbb{F}_{q^\ell}$, $a \neq 0$;
(e) $f(x) = a^{q^r} x^{q^{2r}} + ax$.

Let $\mathcal{X} = \mathcal{X}_{\ell,r}(a,b,c)$ *be the nonsingular model of the Artin–Schreier curve of the type* (3.1) *over* $\mathbb{F}_{q^\ell}$. *If* $\mathcal{X}$ *is an* $\mathbb{F}_{q^\ell}$*-maximal curve, then the following conditions must be satisfied*:

(i) $n\ell$ *is even*;
(ii) *the equation* $f(x) = -b^{q^r}$ *has a solution* $x_0 \in \mathbb{F}_{q^\ell}$ *such that* $\mathbf{T}(c_1) = 0$, *where* $c_1 = ax_0^{q^r+1} - c$.

Conversely, if these conditions are satisfied then $\mathcal{X}$ *is* $\mathbb{F}_{q^\ell}$*-maximal if and only if one of the following conditions holds true*:

(1) $r = 0$, ℓ *is even*, $p \equiv 1 \pmod 4$, *and* a *is not a square in* $\mathbb{F}_{q^\ell}$;
(2) $r = 0$, ℓ *is even*, $p \equiv 3 \pmod 4$, *and either* $n\ell/2$ *odd and* a *is a square in* $\mathbb{F}_{q^\ell}$, *or* $n\ell/2$ *is even and* a *is not a square in* $\mathbb{F}_{q^\ell}$;
(3) $r \geq 1$, $2r$ *divides* ℓ *and* $\ell/2r$ *is odd, and* $f(x)$ *is not a permutation polynomial over* $\mathbb{F}_{q^\ell}$.

Remark 4.2. Under conditions (i), (ii) of Theorem 4.1, the curve $\mathcal{X}_{\ell,r}(a,b,c)$ is $\mathbb{F}_{q^\ell}$-minimal (in the sense that the lower Hasse–Weil bound above is attained) if and only if one of the following conditions holds true:

(1′) $r = 0$, ℓ is even, $p \equiv 1 \pmod 4$, and a is a square in $\mathbb{F}_{q^\ell}$;
(2′) $r = 0$, ℓ is even, $p \equiv 3 \pmod 4$, and either $n\ell/2$ is odd and a is not a square in $\mathbb{F}_{q^\ell}$, or $n\ell/2$ is even and a is a square in $\mathbb{F}_{q^\ell}$;
(3′) $r \geq 1$, $2r$ divides ℓ and $\ell/2r$ is even, and $f(x)$ is not a permutation polynomial over $\mathbb{F}_{q^\ell}$.

Remark 4.3. There are examples of maximal curves for each case in Theorem 4.1 (cf. [8, Thm. 3.3], [21, Thm. 1]).

Remark 4.4. The notation is as in Theorem 4.1. Let $p \equiv 3 \pmod 4$ and $n\ell/2$ be odd. If a is a nonzero square, then $\mathcal{X} = \mathcal{X}_{\ell,0}(a,b,c)$ can be defined by an equation of the type

$$y^q - y = x^2 + c',$$

where $c' \in \mathbb{F}_{q^\ell}$. Since the solution in $\mathbb{F}_{q^\ell}$ of $f(x) = 2x = 0$ is $x_0 = 0$, by Theorem 4.1, $\mathbf{T}(c') = 0$ and thus $\mathcal{X}$ is uniquely defined by

$$y^q - y = x^2.$$

This example is missing in [8, Thm. 8.12] and it is a particular case of [21, Thm. 1].

Remark 4.5. Let $\mathcal{X} = \mathcal{X}_{\ell,r}(a,b,c)$ be an $\mathbb{F}_{q^\ell}$-maximal curve satisfying Theorem 4.1(3) with $\ell = 2r$. Then by [9, Thm. 2.3], $\mathcal{X}$ is $\mathbb{F}_{q^\ell}$-isomorphic to

a curve of type $\mathcal{X}_{\ell,r}(\alpha,0,0)$, where $f(x)=\alpha^{q^r}x^{q^{2r}}+\alpha x$ is not a permutation polynomial. We may choose $\alpha=1$ if $p=2$; otherwise $\alpha=\varsigma^{(q^r+1)/2}$, with ς a generator of $\mathbb{F}_{q^\ell}^*$ [8, Prop. 3.2].

REMARK 4.6. Çakçak and Özbudak [4] considered maximal curves that include those studied by Coulter [8]; in particular, they showed that these examples are covered by Hermitian curves. As a matter of fact, there are maximal curves which are not covered by Hermitian curves; cf. [11]. Are maximal curves in (3.1) with $\mathbf{T}(c)=0$ isomorphic to Coulter's curves? Is a maximal curve in (3.1) with $\mathbf{T}(c)\neq 0$ isomorphic to a curve in [4]? Must such a curve be covered by the Hermitian curve?

5. The arc arising from $\mathcal{H}$. Throughout this section we let $q=p^n$ be a power of a prime p, ℓ an integer with $\ell\geq 3$, and $r=r(\ell)$ be the integer defined in (2.1); in particular, $u=\gcd(\ell,r)=1$. We are interested in the arc property derived from the pointset

$$\mathcal{K}=\mathcal{H}(\mathbb{F}_{q^\ell})\subseteq \mathrm{PG}(2,q^\ell)$$

defined from the set of $\mathbb{F}_{q^\ell}$-rational points of the curve $\mathcal{H}$ introduced in Section 2. By Theorem 2.1, $\mathcal{K}$ is an (N,d)-arc with parameters

$$N=q^{2\ell-1}+1 \quad\text{and}\quad d=q^{\ell-1}+q^{r-1}. \tag{5.1}$$

By (2.2), the degree d of the arc is also closely related to the number $N_\ell(b,c):=N_{\ell,r}(1,b,c)$ of $\mathbb{F}_{q^\ell}$-affine points of Artin–Schreier curves of the type (2.3), namely

$$y^q-y=x^{q^r+1}+bx+c,$$

where $b,c\in\mathbb{F}_{q^\ell}$. We have $N_\ell(b,c)\leq qd$. The numbers $N_\ell(b,c)$ can be deduced directly from Theorems 3.3, 3.5, 3.6 above. For the sake of convenience we explicitly state such results below.

LEMMA 5.1. *Consider the same notation as above; in particular, $q=p^n$ with p a prime and ℓ is an integer with $\ell\geq 3$, $b,c\in\mathbb{F}_{q^\ell}$. In addition, let $\mathbf{T}:\mathbb{F}_{q^\ell}\to\mathbb{F}_q$ be the trace map and let χ_1 be the canonical additive character of $\mathbb{F}_{q^\ell}$. Let $f(x)=x^{q^{2r}}+x$ with r as in (2.1).*

(1) *Suppose that ℓ is odd.*

(i) *Let $p=2$. If $\mathbf{T}(b)=0$, then $N_\ell(b,c)=q^\ell$; otherwise,*

$$N_\ell(b,c)=q^\ell+\chi_1(\omega^{q^r+1}+\omega)\left(\frac{2}{\ell}\right)^n q^{(\ell+1)/2}\chi_1(\mathbf{T}(b)^{-2}c),$$

where $\omega\in\mathbb{F}_{q^\ell}$ is such that $b\mathbf{T}(b)^{-1}=\omega^{q^{2r}}+\omega+1$, and $\left(\frac{2}{v}\right)$ is the Jacobi symbol.

(ii) *Let $p > 2$. Let x_0 be the solution of $f(x) = -b^{q^r}$ (cf. Remark 3.1). Let η be the quadratic character of $\mathbb{F}_q$. Define $c_1 = ax_0^{q^r+1} - c$. If $\mathbf{T}(c_1) = 0$, then $N_\ell(b,c) = q^\ell$; otherwise,*

$$N_\ell(b,c) = q^\ell + \begin{cases} q^{(\ell+1)/2}\eta(\mathbf{T}(c_1)) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{n(\ell+1)/2}q^{(\ell+1)/2}\eta(\mathbf{T}(c_1)) & \text{if } p \equiv 3 \pmod 4,\ b = 0, \\ (-1)^{n(3\ell+1)/2}q^{(\ell+1)/2}\eta(\mathbf{T}(c_1)) & \text{if } p \equiv 3 \pmod 4,\ b \neq 0. \end{cases}$$

(2) *Suppose that ℓ is even. If $f(x) = -b^{q^r}$ has no roots in $\mathbb{F}_{q^\ell}$, then $N_\ell(b,c) = q^\ell$; otherwise, let $x_0 \in \mathbb{F}_{q^\ell}$ be a root of $f(x) = -b^{q^r}$. Set $c_1 = ax_0^{q^r+1} - c$.*

(i) *If $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^\ell}$, then*

$$N_\ell(b,c) = q^\ell + \begin{cases} (-1)^{\ell/2}q^{\ell/2}(q-1) & \text{if } \mathbf{T}(c_1) = 0, \\ (-1)^{\ell/2+1}q^{\ell/2} & \text{if } \mathbf{T}(c_1) \neq 0. \end{cases}$$

(ii) *If $f(x)$ is not a permutation polynomial, then*

$$N_\ell(b,c) = q^\ell + \begin{cases} (-1)^{\ell/2+1}q^{\ell/2+1}(q-1) & \text{if } \mathbf{T}(c_1) = 0, \\ (-1)^{\ell/2}q^{\ell/2+1} & \text{if } \mathbf{T}(c_1) \neq 0. \end{cases}$$

Next we are concerned with the permutation property of the polynomial $f(x)$ which arises in the lemma above.

REMARK 5.2. Let $f(x) = x^{q^{2r}} + x \in \mathbb{F}_{q^\ell}[x]$ with q a power of a prime p, ℓ an integer with $\ell \geq 3$, and r as in (2.1). If $p = 2$, it is clear that $f(x)$ is not a permutation polynomial. If $p > 2$, then Remark 3.1 can be improved so that $f(x)$ is a permutation polynomial if and only if either ℓ is odd, or $\ell \equiv 2 \pmod 4$ (see [5, remark after the proof of Theorem 4.1]).

Recall that N, d and r stand for the integers defined in (5.1) and (2.1).

QUESTION 5.3. Is the pointset $\mathcal{K} = \mathcal{H}(\mathbb{F}_{q^\ell})$ defined above a complete (N,d)-arc in $\mathrm{PG}(2,q^\ell)$?

CASE A. The answer to Question 5.3 is affirmative provided that $p \equiv 1 \pmod 4$ and ℓ is odd with $\ell \geq 3$.

In fact, let $P \in \mathrm{PG}(2,q^\ell) \setminus \mathcal{K}$. We shall show that there is a line $\mathcal{L} : y + bx + c = 0$ in $\mathrm{PG}(2,q^\ell)$ such that $P \in \mathcal{L}$ and $\#\,\mathcal{K} \cap \mathcal{L} = d$.

If $P = (A : B : 1)$, we look for $\mathcal{L}$ with $c = -bA - B$ (so that $P \in \mathcal{L}$). Let us consider the Artin–Schreier curve of the type

$$y^q - y = x^{q^r+1} - Ax^{q^r} - Ax^{q^{r-1}} + B - \lambda,$$

where $\lambda \in \mathbb{F}_{q^\ell}$ is such that $\mathbf{T}(\lambda)$ is a nonzero square in $\mathbb{F}_q$. As already mentioned in Section 3 (cf. [8, Thm. 5.8]), this curve has the same number of $\mathbb{F}_{q^\ell}$-affine points as a certain curve of the type (3.1). Thus, by Lemma

5.1(1)(ii), the curve above has at least $q^\ell - q^r$ $\mathbb{F}_{q^\ell}$-affine points; let (x_0, y_0) be one of such points and set $b := -x_0^{q^r} - x_0^{q^{r-1}}$. Then

$$-b^{q^r} = x_0^{q^{2r}} + x_0^{q^{2r-1}},$$

and thus x_0 is also the solution of the equation $f(x) = -b^{q^r}$, with $f(x) = x^{q^{2r}} + x$, as $2r - 1 = \ell$. Moreover, by construction,

$$c_1 = x_0^{q^r+1} - c = x_0^{q^r+1} + bA + B = x_0^{q^r+1} - Ax_0^{q^r} - Ax_0^{q^{r-1}} + B;$$

so $\mathbf{T}(c_1) = \mathbf{T}(\lambda)$ is a nonzero square in $\mathbb{F}_q$. The result now follows from Lemma 5.1(1)(ii) and (2.2).

Now let $P = (1 : B : 0)$. Here we look for a line of the type $\mathcal{L} : y - Bx + c = 0$ with some $c \in \mathbb{F}_{q^\ell}$. Let $x_0 \in \mathbb{F}_{q^\ell}$ be a solution of $f(x) = B^{q^r}$ (cf. Remark 5.2) and let c be such that $\mathbf{T}(x_0^{q^r+1} - c)$ is a nonzero square in $\mathbb{F}_q$; the result follows.

Case B. The answer to Question 5.3 is also affirmative if $p \equiv 3 \pmod 4$ and ℓ is odd with $\ell \geq 3$.

The proof is similar to Case A; here we choose $\lambda \in \mathbb{F}_{q^\ell}$ according to the parity of either $n(\ell + 1)/2$ or $n(3\ell + 1)/2$.

Case C. Let $p > 2$ and ℓ be even with $\ell \geq 6$ and $\ell \equiv 2 \pmod 4$. Then the answer to Question 5.3 is negative.

In fact, here $\mathcal{K}$ is a complete (N, d_1)-arc with $d_1 = q^{\ell-1} + q^{r-3}$ (which is clearly less than the degree d of $\mathcal{H}$). To see this, let $\mathcal{L}$ be a line in $\mathrm{PG}(2, q^\ell)$ defined by the equation $\alpha X + \beta Y + \gamma Z = 0$. We claim that $\#\,\mathcal{K} \cap \mathcal{L} \leq d_1$. If $\beta = 0$, then it is easy to see that $\#\,\mathcal{K} \cap \mathcal{L} \leq q^{\ell-1}$. For $\beta \neq 0$, the claim follows from Lemma 5.1(2)(i), as $\ell/2 = r - 2$ and $f(x)$ is a permutation polynomial (see Remark 5.2).

Now we prove the completeness of the (N, d_1)-arc $\mathcal{K}$. The proof is similar to Case A. Let $P \in \mathrm{PG}(2, q^\ell) \setminus \mathcal{K}$. If $P = (A : B : 1)$, we look for a line $\mathcal{L} : y + bx + c = 0$ such that $c = -bA - B$ and $\#\,\mathcal{K} \cap \mathcal{L} = d_1$. Let us consider the Artin–Schreier curve of the type

$$y^q - y = x^{q^r+1} - Ax^{q^r} - Ax^{q^{r-4}} + B - \lambda,$$

where $\lambda \in \mathbb{F}_{q^\ell}$ is such that $\mathbf{T}(\lambda) \neq 0$. We see that this curve has at least $q^\ell - q^{r-2}(q - 1)$ $\mathbb{F}_{q^\ell}$-affine points. Let (x_0, y_0) be one of these points, and let $b := -x_0^{q^r} - x_0^{q^{r-4}}$. Therefore $f(x_0) = -b^{q^r}$ since $2r - 4 = \ell$. Also, by construction, $\mathbf{T}(x_0^{q^r+1} - c) = \mathbf{T}(\lambda) \neq 0$. Now the result follows from Lemma 5.1(2)(i) and (2.2).

Finally, let $P = (1 : B : 0)$ and $x_0 \in \mathbb{F}_{q^\ell}$ be a solution of $f(x) = B^{q^r}$ (cf. Remark 5.2); choose $c \in \mathbb{F}_{q^\ell}$ such that $\mathbf{T}(x_0^{q^r+1} - c) \neq 0$. Then the line $\mathcal{L} : y - Bx + c = 0$ is such that $P \in \mathcal{L}$ and $\#\,\mathcal{K} \cap \mathcal{L} = d_1$ by Lemma 5.1(2)(i).

Case D_1. Let $p = 2$ and ℓ be odd with $\ell \geq 3$. We assume $q = 2^n$ with n even; otherwise, we assume n odd and $\ell \equiv \pm 1 \pmod 8$. Here the answer to Question 5.3 is also negative.

In fact, let us consider the following set:

$$\bar{\mathcal{K}} := \{(1 : B : 0) \in \mathrm{PG}(2, q^\ell) : \mathbf{T}(B) = 0\}.$$

We claim that the pointset

$$\mathcal{K}_1 := \mathcal{K} \cup \bar{\mathcal{K}}$$

is a complete (N_1, d)-arc in $\mathrm{PG}(2, q^\ell)$ with $N_1 = N + q^{\ell-1}$. That $\mathcal{K}_1$ is an (N_1, d)-arc is clear by Lemma 5.1(1)(i); next we prove its completeness. Let $P \in \mathrm{PG}(2, \mathbb{F}_{q^\ell}) \setminus \mathcal{K}_1$.

If $P = (A : B : 1)$, we look for a line $\mathcal{L} : y + bx + c = 0$ with $c = -bA - B$ such that $\#\,\mathcal{K}_1 \cap \mathcal{L} = d$. Let $\gamma \in \mathbb{F}_q^*$ and consider the Artin–Schreier curve of the type

$$y^q - y = x^{q^r+1} + x - (x^q + x + 1)A\gamma^{-1} - B\gamma^{-2}.$$

Arguing as in Case A, we can see that this curve has at least one affine $\mathbb{F}_{q^\ell}$-point, say (x_0, y_0). We let $b := (x_0^{q^{2r}} + x_0 + 1)\gamma$. Then, as $2r = \ell + 1$ and $p = 2$, we have $\mathbf{T}(b) = \gamma$ so that $b\mathbf{T}(b)^{-1} = x_0^{q^{2r}} + x_0 + 1$. After some computation,

$$x_0^{q^r+1} + x_0 + \mathbf{T}(b)^{-2}c = y_0^q - y_0$$

and, by the transitivity of the trace map,

$$N_\ell(b, c) = q^\ell + \left(\frac{2}{\ell}\right)^n q^r$$

by Lemma 5.1(1)(i); the result follows.

Now let $P = (1 : B : 0)$ with $\mathbf{T}(B) \neq 0$. We look for a line $\mathcal{L} : y - Bx + c = 0$ with $\#\,\mathcal{K}_1 \cap \mathcal{L} = d$. Let $\omega \in \mathbb{F}_{q^\ell}$ be such that $B\,\mathbf{T}(B)^{-1} = \omega^{q^{2r}} + \omega + 1$ (see Remark 3.1). Define $c = (\omega^{q^r+1} + \omega)\mathbf{T}(B)^2$. Then

$$\omega^{q^r+1} + \omega + c\mathbf{T}(B)^{-2} = 0,$$

and the result follows again from Lemma 5.1(1)(i).

Case D_2. Let $p = 2$ and ℓ be odd with $\ell \geq 3$. We assume $q = 2^n$ with n odd and $\ell \equiv \pm 3 \pmod 8$. Here the answer to Question 5.3 is also negative.

In fact, let us consider the set

$$\bar{\mathcal{K}} := \{(1 : B : 0) \in \mathrm{PG}(2, q^\ell) : \mathbf{T}(B) \neq 0\}.$$

We claim that the pointset

$$\mathcal{K}_1 := \mathcal{K} \cup \bar{\mathcal{K}}$$

is in fact a complete $(N_1, q^{\ell-1})$-arc in $\mathrm{PG}(2, q^\ell)$ with $N_1 = N + q^\ell - q^{\ell-1}$. That $\mathcal{K}_1$ is an $(N_1, q^{\ell-1})$-arc is clear. To see its completeness, suppose that

$P \in \mathrm{PG}(2,q^\ell) \setminus \mathcal{K}_1$. Let $P = (A : B : 1)$ and let $\mathcal{L}$ be the line $y + bx + c = 0$ with $c = -bA - B$ so that $P \in \mathcal{L}$; if $\mathbf{T}(b) = 0$, then $\#\,\mathcal{K}_1 \cap \mathcal{L} = q^{\ell-1}$ by Lemma 5.1(1)(i). Now let $P = (1 : B : 0)$ with $\mathbf{T}(B) = 0$; here we let $\mathcal{L}$ be the line $y - Bx = 0$, and the result follows by Lemma 5.1(1)(i) again.

Case E. Let $p \geq 2$ be a prime and ℓ be even with $\ell \geq 4$ and $\ell \equiv 0 \pmod 4$. Here the answer to Question 5.3 is also negative.

In fact, set $f(x) = x^{q^{2r}} + x$ and let H be the set of elements $B \in \mathbb{F}_{q^\ell}$ such that the equation $f(x) = B^{q^r}$ has a solution in $\mathbb{F}_{q^\ell}$. Let us fix a set $H_1 \subseteq \mathbb{F}_{q^\ell} \setminus H$ with $\#\,H_1 = q^{\ell-1} + q^{r-1} - 1$; this selection of H_1 is possible since $\#\,H \leq q^{\ell-2}$. Then the pointset

$$\mathcal{K}_2 := \mathcal{K} \cup \{(1 : B : 0) \in \mathrm{PG}(2,q^\ell) : B \in H_1\}$$

is a complete (N_2, d)-arc, with $N_2 = N + \#\,H_1 = q^{2\ell-1} + q^{\ell-1} + q^{r-1}$.

Arguing as in Case C, it is easy to see that $\mathcal{K}_2$ is in fact an (N_2, d)-arc. To derive its completeness, let $P \in \mathrm{PG}(2,q^\ell) \setminus \mathcal{K}_2$. If $P = (A : B : 1)$, we proceed as in Case C by means of Remark 5.2 and Lemma 5.1(2)(ii). Let now $P = (1 : B : 0)$ with $B \in H$, and $x_0 \in \mathbb{F}_{q^\ell}$ a solution of $f(x) = B^{q^r}$. Let $c \in \mathbb{F}_{q^\ell}$ be such that $\mathbf{T}(x_0^{q^r+1} - c) \neq 0$ and consider the line $y - Bx + c = 0$; the result follows.

Case F. Let $p = 2$ and ℓ be even with $\ell \geq 4$ and $\ell \equiv 2 \pmod 4$. In this case, the answer to Question 5.3 is also negative.

In fact, let H be the set defined in Case E and fix a set $H_2 \subseteq \mathbb{F}_{q^\ell} \setminus H$ such that $\#\,H_2 = q^{\ell-1} + q^{r-2}(q-1) - 1$. Then the pointset

$$\mathcal{K}_3 := \mathcal{K} \cup \{(1 : B : 0) : B \in H_2\}$$

is a complete (N_3, d_2)-arc with

$$N_3 = N + \#\,H_2 = q^{2\ell-1} + q^{\ell-1} + q^{r-2}(q-1), \qquad d_2 = q^{\ell-1} + q^{r-2}(q-1).$$

The proof of this case is analogous to Case E by using Lemma 5.1(2)(ii) once again. ∎

We summarize the above computations in the following.

Theorem 5.4. *Let $\mathcal{H}$ be the plane curve over $\mathbb{F}_{q^\ell}$ defined in Section 2, where $q = p^n$ is a power of a prime $p \geq 2$ and ℓ is an integer with $\ell \geq 3$. Let $\mathcal{K} = \mathcal{H}(\mathbb{F}_{q^\ell}) \subseteq \mathrm{PG}(2,q^\ell)$ be the set of $\mathbb{F}_{q^\ell}$-rational points of $\mathcal{H}$. Let $N = \#\,\mathcal{H}(\mathbb{F}_{q^\ell}) = q^{2\ell-1} + 1$ and $d = q^{\ell-1} + q^{r-1}$ be, respectively, the number of $\mathbb{F}_{q^\ell}$-rational points and the degree of $\mathcal{H}$, where r is the integer defined in* (2.1).

(1) *If $p > 2$ and ℓ is odd, then $\mathcal{K}$ is a complete (N, d)-arc in* $\mathrm{PG}(2,q^\ell)$.
(2) *If $p > 2$ and ℓ is even with $\ell \equiv 2 \pmod 4$, then $\mathcal{K}$ is a complete (N, d_1)-arc in* $\mathrm{PG}(2,q^\ell)$ *with* $d_1 = q^{\ell-1} + q^{r-3}$.

(3) *Let $p = 2$ and ℓ be odd. Suppose that n is even or $\ell \equiv \pm 1 \pmod 8$. Set $\bar{\mathcal{K}} := \{(1 : B : 0) \in \mathrm{PG}(2, q^\ell) : \mathbf{T}(B) = 0\}$, where $\mathbf{T} : \mathbb{F}_{q^\ell} \to \mathbb{F}_q$ is the trace map. Then the pointset*

$$\mathcal{K}_1 := \mathcal{K} \cup \bar{\mathcal{K}}$$

is a complete (N_1, d)-arc with $N_1 = N + q^{\ell-1}$.

(4) *Let $p = 2$ and ℓ be odd. Suppose that n is odd and $\ell \equiv \pm 3 \pmod 8$. Set $\bar{\mathcal{K}} := \{(1 : B : 0) \in \mathrm{PG}(2, q^\ell) : \mathbf{T}(B) \neq 0\}$, where $\mathbf{T} : \mathbb{F}_{q^\ell} \to \mathbb{F}_q$ is the trace map. Then the pointset*

$$\mathcal{K}_1 := \mathcal{K} \cup \bar{\mathcal{K}}$$

is a complete $(N_1, q^{\ell-1})$-arc with $N_1 = N + q^\ell - q^{\ell-1}$.

Set $H := \{B \in \mathbb{F}_{q^\ell} : x^{q^{2r}} + x = B^{q^r}$ has a solution in $\mathbb{F}_{q^\ell}\}$.

(5) *Let $p \geq 2$ and ℓ be even with $\ell \equiv 0 \pmod 4$. Let H_1 be a subset of the complement of H in $\mathbb{F}_{q^\ell}$ whose size is $q^{\ell-1} + q^{r-1} - 1$. Then the pointset*

$$\mathcal{K}_2 = \mathcal{K} \cup \{(1 : B : 0) : B \in H_1\}$$

is a complete $(q^{2\ell-1} + q^{\ell-1} + q^{r-1}, d)$-arc.

(6) *Let $p = 2$, and ℓ be even with $\ell \equiv 2 \pmod 4$. Let H_2 be a subset of the complement of H in $\mathbb{F}_{q^\ell}$ whose size is $q^{\ell-1} + q^{r-2}(q-1) - 1$. Then the pointset*

$$\mathcal{K}_3 = \mathcal{K} \cup \{(1 : B : 0) : B \in H_2\}$$

is a complete $(q^{2\ell-1} + q^{\ell-1} + q^{r-2}(q-1), q^{\ell-1} + q^{r-2}(q-1))$-arc.

Remark 5.5. Let q be a power of an odd prime and ℓ be a positive even integer. Let B be a subset of $\mathbb{F}^*_{q^{\ell/2}}$ of size b with $1 \leq b \leq b^{\ell/2-1}$. In [12] the following union of Hermitian curves over $\mathbb{F}_{q^\ell}$ is considered:

$$\mathcal{X}_B : \prod_{\lambda \in B} (\lambda X^{q^{\ell/2}+1} + XY^{q^{\ell/2}} + X^{q^{\ell/2}}Y + Z^{q^{\ell/2}+1}) = 0.$$

The pointset $\mathcal{X}_B(\mathbb{F}_{q^\ell})$ is a complete $(q^\ell q^{\ell/2} b + 1, b(q^{\ell/2}+1))$-arc; in particular, if $b = q^{\ell/2-1}$ we obtain a complete $(q^{2\ell-1}+1, q^{\ell-1}+q^{\ell/2-1})$-arc in $\mathrm{PG}(2, q^\ell)$. For $\ell \geq 6$ and $\ell \equiv 2 \pmod 4$, this arc has the same parameters as the arc $\mathcal{K} = \mathcal{H}(\mathbb{F}_{q^\ell})$ in Theorem 5.4(2). However, these arcs are not isomorphic. In fact, if they were, there would exist a collineation T on $\mathrm{PG}(2, q^\ell)$ such that $T(\mathcal{K}) = \mathcal{X}_B(\mathbb{F}_{q^\ell})$. By Bézout's Theorem there are at most $(q^{\ell-1} + q^{r-1})(q^{\ell-1} + q^{r-3})$ points in the intersection of $\mathcal{H}$ and $\mathcal{X}_B$, which is a contradiction as $\#\,\mathcal{K} = q^{2\ell-1} + 1$.

Remark 5.6. The construction of the arcs in Theorem 5.4(5),(6) seems not to be canonical in the sense that it might depend on the selection of certain subsets of $\mathbb{F}_{q^\ell}$. As a matter of fact, we do not even know if the

smallest case $q = 2$ and $\ell = 4$ would provide at least two nonisomorphic complete $(140, 12)$-arcs in $\mathrm{PG}(2, 16)$.

Acknowledgments. We thank M. Giulietti, J. W. P. Hirschfeld, G. Korchmáros, J. Moyano-Fernández, and D. Panario for useful comments. H. Borges was partially supported by FAPESP-Brazil Grant 2011/19446-3, B. Motta was partially supported by CAPES-Brazil, CNPq-Brazil and FAPEMIG-Brazil, and F. Torres was partially supported by CNPq-Brazil Grant 306324/2011-3.

References

[1] H. Borges Filho, *On complete (N, d)-arcs derived from plane curves*, Finite Fields Appl. 15 (2009), 82–96.

[2] H. Borges Filho and R. Conceição, *Minimal value set polynomials and a generalization of the Hermitian curve*, preprint, 2013.

[3] S. V. Bulygin, *Generalized Hermitian codes over* $\mathrm{GF}(2^r)$, IEEE Trans. Inform. Theory 52 (2006), 4664–4669.

[4] E. Çakçak and F. Özbudak, *Curves related to Coulter's maximal curves*, Finite Fields Appl. 14 (2008), 209–220.

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

[6] R. S. Coulter, *Further evaluations of Weil sums*, Acta Arith. 86 (1998), 217–226.

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

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

[9] A. Garcia and F. Özbudak, *Some maximal function fields and additive polynomials*, Comm. Algebra 35 (2007), 1553–1566.

[10] A. Garcia and H. Stichtenoth, *A class of polynomials over finite fields*, Finite Fields Appl. 5 (1999), 424–435.

[11] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. 343 (2009), 229–245.

[12] M. Giulietti, F. Pambianco, F. Torres and E. Ughi, *On complete arcs arising from plane curves*, Des. Codes Cryptogr. 25 (2002), 237–246.

[13] A. Hefez and J. F. Voloch, *Frobenius nonclassical curves*, Arch. Math. (Basel) 54 (1990), 263–273; Correction, ibid. 57 (1991), 416.

[14] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed., Oxford Univ. Press, Oxford, 1998.

[15] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton Univ. Press, Princeton, 2008.

[16] J. W. P. Hirschfeld and J. F. Voloch, *The characterization of elliptic curves over finite fields*, J. Austral. Math. Soc. Ser. A 45 (1988), 275–286.

[17] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, Reading, MA, 1983.

[18] C. Munuera, A. Sepúlveda and F. Torres, *Algebraic geometry codes from Castle curves*, in: Lecture Notes in Comput. Sci. 5228, Springer, Berlin, 2008, 117–127.

[19] C. Munuera, A. Sepúlveda and F. Torres, *Generalized Hermitian codes*, Des. Codes Cryptogr. 69 (2013), 123–130.
[20] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[21] S. Tafazolian, *A note on certain maximal hyperelliptic curves*, Finite Fields Appl. 18 (2012), 1013–1016.
[22] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.
[23] J. Wolfmann, *The number of points on certain algebraic curves over finite fields*, Comm. Algebra 17 (1989), 2055–2060.

Herivelto Borges
Instituto de Ciências Matemáticas
e de Computação
Universidade de São Paulo
13560-970, São Carlos, SP, Brazil
E-mail: hborges@icmc.usp.br

Fernando Torres
Institute of Mathematics, Statistics
and Computer Science (IMECC)
University of Campinas (UNICAMP)
R. Sérgio Buarque de Holanda, 651
Cidade Universitária "Zeferino Vaz"
13083-059, Campinas, SP, Brazil
E-mail: ftorres@ime.unicamp.br

Beatriz Motta
Departamento de Matemática
Instituto de Ciências Exatas
Universidade Federal de Juiz de Fora
Rua José Lourenço Kelmer s/n
Campus Universitário
Bairro São Pedro
36036-900, Juiz de Fora, MG, Brazil
E-mail: beatriz@ice.ufjf.br

Received on 9.4.2013
and in revised form on 7.1.2014 (7404)