ON THE REE CURVE

SAEED TAFAZOLIAN AND FERNANDO TORRES

ABSTRACT. We point out a characterization of the Ree curve which involves the number of rational points, the genus, and the shape of two elements of the Weierstrass semigroup at a rational point.

1. Introduction

There are three outstanding examples of algebraic curves defined over a finite field $\mathbb{F}_q$ of order q; that is, the Deligne-Lusztig varieties associated respectively to a connected, reductive, algebraic simple groups of type

- ${}_2A^2(q)$, where q is a square;
- ${}_2B^2(q)$, where $q = 2q_0^2$, $q_0 = 2^s > 1$;
- ${}_2G^2(q)$, where $q = 3q_0^2$, $q_0 = 3^s > 1$.

For instance, these curves are *optimal* in the sense that their number of $\mathbb{F}_q$-rational points coincides with the maximum number of $\mathbb{F}_q$-rational points that curves of their genus can have. Concrete examples of such Deligne-Lusztig varieties are respectively the so-called Hermitian curve, the Suzuki curve and the Ree curve [4, 1] (see also [9, Ch. 12]) which can be defined respectively by the affine equations

- $y^{\sqrt{q}+1} + x^{\sqrt{q}+1} + 1 = 0$, q a square;
- $y^q - y = x^{q_0}(x^q - x)$, $q = 2q_0^2$, $q_0 = 2^s > 1$;
- For $q = 3q_0^2$, $q_0 = 3^s > 1$,

$$y^q - y = x^{q_0}(x^q - x)\,, \quad z^q - z = x^{2q_0}(x^q - x)\,. \tag{1.1}$$

As a matter of fact, the nonsingular model of these curves can be characterized by the data [5]: (A) Number of $\mathbb{F}_q$-rational points, (B) The genus, (C) The automorphism group (over $\mathbb{F}_q$). It turns out that condition (C) can be overlooked for both the Hermitan curve and the Suzuki curve [16, 3]. This observation is the main stimulus for this paper, namely to elucidate whether or not the Ree curve would also be characterized by means of its number of rational points and genus only. So far the Ree curve is characterized by the following data [5]:

2010 Math. Subj. Class.: Primary 05B, Secondary 14H.
Keywords: finite field, optimal curve, Ree curve, Weierstrass semigroup.
April 14, 2018.

(I) Number of $\mathbb{F}_q$-rational points: $\tilde{N} = q^3 + 1$;
(II) Genus: $\tilde{g} = \frac{3}{2}q_0(q-1)(q+q_0+1)$;
(III) Automorphism group equals to the Ree group over q.

Let $\mathcal{X}$ be a curve over $\mathbb{F}_q$, $q = 3q_0^2$, $q_0 = 3^s > 1$, satisfying conditions (I) and (II) above. We summarize the content of this paper. In Section 3 we introduce two linear series on $\mathcal{X}$, $\mathcal{D}$ and $\mathcal{E}$ (Definitions 3.2, 3.6). In order to do that we first compute the zeta function of $\mathcal{X}$ over $\mathbb{F}_q$ by following Pedersen [15] via Weil explicit formulas, see Proposition 3.1 here. This is the starting point to consider the definition of $\mathcal{D}$ which in fact becomes a very ample linear series (Theorem 3.11). Then $\mathcal{E}$ is a sublinear series of $\mathcal{D}$ and hence some information on the Weierstrass semigroup $H(P)$, $P \in \mathcal{X}(\mathbb{F}_q)$, can be obtained from both $\mathcal{D}$ and $\mathcal{E}$; see Proposition 3.4, Proposition 3.7, Corollary 3.8 and Proposition 3.10(2). In particular, this curve becomes an example of a Castle curve in the sense of Munuera et al. [14] and thus it is of interest for Coding Theory purposes cf. Munuera et al. [14, 13].

Theorem 4.6 is the main result of this paper. By considering a further geometrical property (Lemma 4.3) of linear series which are closely related to the aforementioned $\mathcal{D}$, for $q_0 \geq 9$, we characterize the Ree curve by means of conditions (I) and (II) above and

$\text{(III)}'$: There exists $P_0 \in \mathcal{X}(\mathbb{F}_q)$ such that $q + q_0q$, $q + 2q_0q$ are non-gaps at P_0.

Our approach in this article follows closely the paper [3, Sect. 5]; in particular, we use as a key tool the Stöhr-Voloch theory [19] which consider ways on improvement on the number of rational point of curves over finite fields. We recall some basic facts on this theory in Section 2. A suitable reference for the background on curves that we assume is in fact the aforementioned book [9].

Notation. By $\mathbb{P}^N$ we denote the N-dimensional projective space over the algebraic closure $\bar{\mathbf{F}}$ of a ground field $\mathbf{F}$.

2. Basic facts on the Stöhr-Voloch theory

Stöhr and Voloch [19] development a geometrical way to bound the number of rational points of curves over finite fields. In this section we subsume some very basic results from this theory. Let $\mathcal{X}$ be a (nonsingular, projective, geometrically irreducible, algebraic) curve defined over a finite field $\mathbf{F} := \mathbb{F}_q$ of order q. Let $\mathcal{D}$ be a base-point-free linear series on $\mathcal{X}$ of (projective) dimension $r \geq 1$ and degree d and also defined over $\mathbf{F}$. Thus there exist a divisor $E \in \mathrm{Div}(\mathcal{X})$ and a $(r+1)$-dimensional vector sub-space $\mathcal{L}$ of the Riemann-Roch space $\mathcal{L}(E)$ such that

$$\mathcal{D} = \{E + \mathrm{div}(f) : f \in \mathcal{L} \setminus \{0\}\}\,.$$

Let $\pi := (f_0 : f_1 : \ldots : f_r) : \mathcal{X} \to \mathbb{P}^r$ be the morphism defined by a $\mathbf{F}$-base $\{f_0, f_1, \ldots, f_r\}$ of $\mathcal{L}$. This morphism is (up to coordinates) uniquely defined by $\mathcal{D}$. For $P \in \mathcal{X}$ and $i \geq 0$ an integer, we define sub-sets of $\mathcal{D}$ which will provide with geometric information on $\mathcal{X}$.

Let $\mathcal{D}_i(P) := \{D \in \mathcal{D} : v_P(D) \geq i\}$ (here $D = \sum_P v_P(D)P$). We have $\mathcal{D}_i(P) = \emptyset$ for $i > d$,

$$\mathcal{D} \supseteq \mathcal{D}_0(P) \supseteq \mathcal{D}_1(P) \supseteq \ldots \supseteq \mathcal{D}_{d-1}(P) \supseteq \mathcal{D}_d(P)\,,$$

and each $\mathcal{D}_i(P)$ is a sub-linear series of $\mathcal{D}$ such that the codimension of $\mathcal{D}_{i+1}(P)$ in $\mathcal{D}_i(P)$ is at most one. If $\mathcal{D}_i(P) \supsetneqq \mathcal{D}_{i+1}(P)$, the integer i is called a $(\mathcal{D}, P)$-*order*; thus by Linear Algebra we have a sequence of $(r+1)$-orders at P:

$$0 = j_0(P) < j_1(P) < \ldots < j_r(P) \leq d\,.$$

Here $\mathcal{D} = \mathcal{D}_0(P)$ since $\mathcal{D}$ is base-point-free by hypothesis. We describe now the linear series $\mathcal{D}_{j_i}(P)$ by using a very special set of coordinates. There exists $D \in \mathcal{D}$ such that $v_P(D) = j_i(P)$. Choose the coordinates f_i's in such a way that

$$v_P(E) + v_P(f_i) = j_i(P)\,.$$

Set $\mathcal{L}_i(P) := \langle f_i, \ldots, f_r\rangle$. Thus

$$\mathcal{D}_{j_i}(P) = \{E + \mathrm{div}(f) : f \in \mathcal{L}_i(P)\}\,.$$

We have the following linear sub-spaces in $\mathbb{P}^r$:

$T_{r-1}(P) : X_r = 0$ (the osculating hyperplane); $T_{r-2}(P) : X_r = X_{r-1} = 0; \ldots;$
$T_2(P) : X_r = X_{r-1} = \ldots X_3 = 0; T_1(P) : X_r = X_{r-1} = \ldots = X_2 = 0$ (the tangent line).

The space $T_{r-1}(P)$ is defined by the equation

$$\det \begin{pmatrix} X_0 & X_1 & \ldots & X_r \\ D_t^{j_0} g_0(P) & D_t^{j_0} g_1(P) & \ldots, & D_t^{j_0} g_r(P) \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ D_t^{j_{r-1}} g_0(P) & D_t^{j_{r-1}} g_1(P) & \ldots & D_t^{j_{r-1}} g_r(P)) \end{pmatrix} = 0\,, \tag{2.1}$$

where t is a separating element of the function field $\bar{\mathbf{F}}(\mathcal{X})$ of $\mathcal{X}$ over $\bar{\mathbf{F}}$, the operators $D_t^{j_i}$'s are the Hasse derivatives of order j_i (see e.g. [8]) and $g_i := t^{-e_P} f_i$ with $e_P := \min\{v_P(f_i)\}$. (Hürwitz's Wronskian method). It is a fundamental result the fact that the sequence $(j_i(P))$ is the same for all but finitely many points P of $\mathcal{X}$. The generic sequence $\bar{\epsilon}$ is called the *order sequence* of $\mathcal{D}$ and will be denoted by

$$0 = \epsilon_0 < \epsilon_1 < \ldots < \epsilon_r \quad (\epsilon_i = \epsilon_i(\mathcal{D}))\,.$$

We can characterize $\bar{\epsilon}$ as follows. For a sequence $\bar{\delta} : 0 = \delta_0 < \delta_1 < \ldots < \delta_r$, let

$$\Delta^{\bar{\delta}} := \begin{pmatrix} D_t^{\delta_0} f_0, & D_t^{\delta_0} f_1 & \ldots & D_t^{\delta_0} f_r \\ D_t^{\delta_1} f_0, & D_t^{\delta_1} f_1 & \ldots & D_t^{\delta_1} f_r \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ D_t^{\delta_r} f_0 & D_t^{\delta_r} f_1 & \ldots & D_t^{\delta_r} f_r \end{pmatrix}\,.$$

Then the sequence $\bar\epsilon$ is the minimum (in the lexicographically order) among the sequences $\bar\delta$ such that $\det(\Delta^{\bar\delta}) \neq 0$. There are finitely many points P where exceptional $(\mathcal{D}, P)$-orders occur; these are called the *$\mathcal{D}$-Weierstrass points* of $\mathcal{X}$. If $\mathcal{D}$ is the canonical linear series, the $\mathcal{D}$-Weierstrass points are the usual *Weierstrass points* of the curve. There is a divisor $R = R(\mathcal{D})$, the so-called *Ramification Divisor* of $\mathcal{D}$, whose support is the set of $\mathcal{D}$-Weierstrass points, namely

$$R = \mathrm{div}(\Delta^{\bar\epsilon}) + (\sum_{i=0}^{r} \epsilon_i)dt + (r+1)E\,.$$

Lemma 2.1. (1) *$j_i(P) \geq \epsilon_i$ for each i, for each $P \in \mathcal{X}$;*

(2) *$v_P(R) \geq \sum_{i=1}^{r}(j_i(P) - \epsilon_i)$;*

(3) *(p-adic criterion) Let p be the characteristic of $\mathbf{F}$. If ϵ is an order and $\binom{\epsilon}{\eta} \not\equiv 0 \pmod p$, then η is also an order.*

Now we deal with the set $\mathcal{X}(\mathbf{F})$ of $\mathbf{F}$-rational points of $\mathcal{X}$. Let $\mathbf{\Phi} : \mathcal{X} \to \mathcal{X}$ be the $\mathbf{F}$-Frobenius morphism on $\mathcal{X}$. Let $T_{r-1}(P)$ be the hyperplane in (2.1) at a generic point P of $\mathcal{X}$; i.e. P is not a $\mathcal{D}$-Weierstrass point.

(SV0) If $\pi(\mathbf{\Phi}(P)) \notin T_{r-1}(P)$ we let

$$\bar\nu : \epsilon_0 < \epsilon_1 < \ldots < \epsilon_{r-1}\,.$$

(SV1) If $\pi(\mathbf{\Phi}(P)) \in T_{r-1}(P)$, then there exists an integer $1 \leq I \leq r-1$ such that $\pi(\mathbf{\Phi}(P)) \in T_I(P) \setminus T_{I-1}(P)$. Define $\bar\nu : \nu_0 < \ldots < \nu_{r-1}$ with $\nu_j := \epsilon_j$ for $0 \leq j \leq I-1$ and $\nu_j = \epsilon_{j+1}$ for $j = I, \ldots, r-1$.

The sequence $\bar\nu$ in (SV0) or (SV1) is called the $\mathbf{F}$-*Frobenius order* sequence of $\mathcal{D}$. We can characterize the ν_j's as follows. For a sequence $\bar\mu : 0 = \mu_0 < \mu_1 < \ldots < \mu_{r-1}$, let

$$\Gamma^{\bar\mu} := \begin{pmatrix} f_0^q & f_1^q & \ldots & f_r^q \\ D_t^{\mu_0} f_0, & D_t^{\mu_0} f_1 & \ldots & D_t^{\mu_0} f_r \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ D_t^{\mu_{r-1}} f_0 & D_t^{\mu_{r-1}} f_1 & \ldots & D_t^{\mu_{r-1}} f_r \end{pmatrix}.$$

Then the sequence $\bar\nu = (\nu_j)$ is the minimum (in the lexicographically order) among the sequences $\bar\mu = (\mu_j)$ such that $\det(\Gamma^{\bar\mu}) \neq 0$. Observe that $\det(\Gamma^{\bar\mu})(P) = 0$ for $P \in \mathcal{X}(\mathbb{F}_q)$.

(SV2) There exists a divisor $S = S(q, \mathcal{D})$ on $\mathcal{X}$, the so-called $\mathbb{F}_q$-*Frobenius Divisor* associated to $\mathcal{D}$, which will allow to bound $\#\mathcal{X}(\mathbb{F}_q)$:

$$S = \mathrm{div}(\det(\Gamma^{\bar\nu}) + (\sum_{i=0}^{r-1} \nu_i)\mathrm{div}(\mathrm{dt}) + (q+r)E\,.$$

Lemma 2.2. *Let $P \in \mathcal{X}(\mathbb{F}_q)$.*

(1) $v_P(S) \geq (j_r(P) - \nu_{r-1}) + \ldots + (j_1(P) - \nu_0)$;

(2) $\nu_i \le j_{i+1}(P) - j_1(P)$ *for* $i = 0, \ldots, r-1$.

Thus $v_P(S) \ge r$ *so that* $\#\mathcal{X}(\mathbb{F}_q) \le \deg(S)/r$.

3. On certain linear series

In the remaining part of this paper, we let $\mathbf{F} = \mathbb{F}_q$ be the finite field of order q with $q := 3q_0^2$, $q_0 := 3^s > 1$. Let $\mathcal{X}$ be a curve over $\mathbf{F}$ whose number $\#\mathcal{X}(\mathbb{F}_q)$ of $\mathbf{F}$-rational points and genus $g(\mathcal{X})$ satisfy (I) and (II) in the Introduction, namely:

(I)) $\#\mathcal{X}(\mathbb{F}_q) := \tilde{N} = q^3 + 1$;
(II) $g(\mathcal{X}) := \tilde{g} = \frac{3}{2}q_0(q-1)(q+q_0+1)$.

We shall investigate certain linear series on $\mathcal{X}$ (Definitions 3.2, 3.6 below) which, by means of the approach in [3, §3], will reveal outstanding geometrical properties of $\mathcal{X}$. We start by collecting some information on the zeta function $Z(t) = Z_{\mathcal{X},q}(t)$ of $\mathcal{X}$ over $\mathbf{F}$. Let N_i be the number of $\mathbf{F}_{q^i}$-rational points of $\mathcal{X}$, where $\mathbf{F}_{q^i}$ is the unique extension of $\mathbf{F} = \mathbb{F}_q$ of degree i. Thus

$$Z(t) = \exp(\sum_{i=1}^{\infty} N_i t^i/i)\,.$$

The following properties hold true, see e.g. [18, Thm. 5.1.15]:

- By the Riemann-Roch theorem, there exists a polynomial $L(t) = L_{\mathcal{X},q}(t) \in \mathbb{Z}[t]$ of degree $2\tilde{g}$ such that $L(t) = Z(t)(1-t)(1-qt)$.
- $L(t) = \prod_{j=1}^{2\tilde{g}}(1-\alpha_j t)$, where the α_j's are algebraic integers which can be arranged in such a way that $\alpha_j\bar{\alpha}_j = q$ for $j = 1, \ldots, \tilde{g}$ (Riemann hypothesis on curves over finite fields).

Set

$$h(t) = h_{\mathcal{X},q}(t) := t^{2\tilde{g}}L(t^{-1}) = \prod_{j=1}^{\tilde{g}}(t-\alpha_j)(t-\bar{\alpha}_j)\,. \tag{3.1}$$

The following result can be read off from [15]; for the sake of completeness we write a proof.

Proposition 3.1. *Let* $\mathcal{X}$ *be a curve over* $\mathbb{F}_q$ *with* $\#\mathcal{X}(\mathbb{F}_q)$ *and* $g(\mathcal{X})$ *as above. Let*

$$a := \frac{1}{2}q_0(q-1)(q+3q_0+1)\,, \quad b := q_0(q^2-1)\,.$$

(1) *The polynomial in (3.1) is given by* $h(t) = (t^2+q)^a(t^2+3q_0t+q)^b$;
(2) *For* $i \ge 1$, $N_i = q^i + 1 - 2\sqrt{q^i}(a\cos(i\pi/2) + b\cos(5i\pi/6))$.

In particular, $N_5 = N_4 = N_3 = N_2 = N_1 = \tilde{N} = q^3+1$ *and the curve* $\mathcal{X}$ *is* $\mathbf{F}_{q^6}$*-maximal.*

Proof. (1) By the Riemann hypothesis we can write, $\alpha_j = \sqrt{q}\exp(\sqrt{-1}\theta_j)$ for some θ_j. Now we use the Weil explicit formulas with

$$\begin{aligned} f(\theta) =& \frac{1}{3}(1+\sqrt{3}\cos\theta+\cos 2\theta)^2 \\ =& 1+\sqrt{3}\cos\theta+\frac{7}{6}\cos 2\theta+\frac{\sqrt{3}}{3}\cos 3\theta+\frac{1}{6}\cos 4\theta\,; \end{aligned}$$

if we write $f(\theta) = 1 + 2\sum_{n\geq 1} c_n \cos n\theta$, for $d \geq 1$ define $\phi_d(t) := \sum_{n\geq 1} c_{nd}t^{nd}$. Then

$$N_1 = \frac{\tilde{g}}{\phi_1(q^{-1/2})} + 1 + \frac{\phi_1(q^{1/2})}{\phi_1(q^{-1/2})} \tag{3.2}$$

if and only if

$$\sum_{j=1}^{\tilde{g}} f(\theta_j) = 0 \quad \text{and} \quad \sum_{d\geq 2} d a_d \phi(q^{-1/2}) = 0\,,$$

where a_d is the number of points of degree d. After some computations we check that (3.2) holds true. In particular,

$$1+\sqrt{3}\cos\theta_j+\cos 2\theta_j = 0 \quad \text{for} \quad j = 1,\ldots,\tilde{g}\,.$$

Since $\cos 2\theta_j = 2\cos^2\theta_j - 1$, we have that $\cos\theta_j = 0$ $(\alpha_j + \bar{\alpha}_j = 0)$ or $\cos\theta_j = -\sqrt{3}/2$ $(\alpha_j + \bar{\alpha}_j = -3q_0)$. Thus

$$h(t) = (t^2+q)^a(t^2+3q_0t+q)^b$$

with $2a + 2b = 2\tilde{g}$. By the relation between $L(t)$ and $Z(t)$ we get

$$N_i = q^i + 1 - \sum_{j=1}^{\tilde{g}}(\alpha_j^i + \bar{\alpha}_j^i)\,.$$

In particular, $N_1 = q + 1 + 3q_0b$ and the computation of $h(t)$ follows.

(2) The formula for N_i holds from Item (1) and the definition of $Z(t)$. □

Let $\mathbf{\Phi}$ be the $\mathbf{F}$-Frobenius morphism on the curve $\mathcal{X}$, and $\mathbf{\Phi}_{\mathcal{J}}$ the corresponding morphism induced by $\mathbf{\Phi}$ on the Jacobian variety $\mathcal{J}$ over $\mathbb{F}_q$ of $\mathcal{X}$. The map $\mathbf{\Phi}_{\mathcal{J}}$ acts on the Tate module of $\mathcal{X}$ so that the polynomial $h(t)$ in Proposition 3.1(1) becomes a multiple of the characteristic polynomial of $\mathbf{\Phi}_{\mathcal{J}}$. Now since $\mathbf{\Phi}_{\mathcal{J}}$ is semisimple and the representation of endomorphisms of $\mathcal{J}$ on the Tate module is faithfully [20, Thm. 2], [11, VI§3], we have that

$$(\mathbf{\Phi}_{\mathcal{J}}^2 + qI_{\mathcal{J}})(\mathbf{\Phi}_{\mathcal{J}}^2 + 3q_0\mathbf{\Phi}_{\mathcal{J}} + qI_{\mathcal{J}}) = 0\,, \tag{3.3}$$

where $I_{\mathcal{J}}$ is the identity morphism on $\mathcal{J}$. Fix $P_0 \in \mathcal{X}(\mathbb{F}_q)$ and embed $\mathcal{X}$ into $\mathcal{J}$ via the natural morphism $f(P) = [P - P_0]$; since the following diagram is commutative

$$\begin{array}{ccc}
\mathcal{X} & \xrightarrow{f} & \mathcal{J} \\
\Big\downarrow{\scriptstyle\mathbf{\Phi}} & & \Big\downarrow{\scriptstyle\mathbf{\Phi}_{\mathcal{J}}} \\
\mathcal{X} & \xrightarrow{f} & \mathcal{J}\,,
\end{array}$$

then for any $P \in \mathcal{X}$, (3.3) implies the following linear equivalence of divisors on $\mathcal{X}$ (cf. [9, Sect. 9.8]):

$$q^2P + 3q_0q\mathbf{\Phi}(P) + 2q\mathbf{\Phi}^2(P) + 3q_0\mathbf{\Phi}^3(P) + \mathbf{\Phi}^4(P) \sim (q+1)(q+3q_0+1)P_0\,. \tag{3.4}$$

Motivated by this equivalence, we introduce the following linear series on $\mathcal{X}$.

Definition 3.2. Let $q_0 = 3^s > 1$, $q = 3q_0^2$, $\mathcal{X}$ be as above. For a fixed $P_0 \in \mathcal{X}(\mathbb{F}_q)$, we let $\mathcal{D} := |mP_0|$ with $m = (q+1)(q+3q_0+1) = q^2 + 3q_0q + 2q + 3q_0 + 1$.

By (3.4) we observe that the definition of $\mathcal{D}$ is independent of the selection of P_0, and that $\mathcal{D}$ is indeed base-point-free. For a point $P \in \mathcal{X}$, let us denote by

$$0 = m_0(P) < m_1(P) < m_2(P) < \ldots$$

the increasing sequence that enumerates the Weierstrass semigroup $H(P)$ at P. Let r be the (projective) dimension of $\mathcal{D} = |mP_0|$.

Lemma 3.3. *For $P \in \mathcal{X}(\mathbb{F}_q)$ we have*

(1) $m_r(P) = m$;
(2) $\tilde{N} = (q - 3q_0 + 1)m_r(P)$;
(3) $2\tilde{g} - 2 = (3q_0 - 2)m_r(P)$.

Proof. Item (1) follows from (3.4); Items (3) and (4) follow after some computations. ☐

Proposition 3.4. *Let $\mathcal{X}$ and q be as above. For all $P \in \mathcal{X}$, $q^2 \in H(P)$ and $m_1(P) = q^2$ whenever $P \in \mathcal{X}(\mathbb{F}_q)$.*

Proof. We apply $\mathbf{\Phi}_*$ in (3.4) and find

$$q^2\mathbf{\Phi}(P) + 3q_0q\mathbf{\Phi}^2(P) + 2q\mathbf{\Phi}^3(P) + 3q_0\mathbf{\Phi}^4(P) + \mathbf{\Phi}^5(P) \sim m_rP_0 \sim$$
$$q^2P + 3q_0q\mathbf{\Phi}(P) + 2q\mathbf{\Phi}^2(P) + 3q_0\mathbf{\Phi}^3(P) + \mathbf{\Phi}^4(P)\,.$$

Thus if $P \notin \mathcal{X}(\mathbb{F}_q)$ and since $\tilde{N} = N_1 = N_2 = N_3 = N_4 = N_5$ (Proposition 3.1), $q^2 \in H(P)$. Now let $P \in \mathcal{X}(\mathbb{F}_q)$. As q^2 is in particular a generic non-gap of $\mathcal{X}$, then $m_1(P) \le q^2$ (to see this, we apply the p-adic criterion in Lemma 2.1 to the canonical linear series of the curve). Finally by Lewittes bound [12, Thm. 1(b)] $\tilde{N} = q^3 + 1 \le qm_1(P) + 1$ so that $m_1(P) = q^2$. ☐

Remark 3.5. Under conditions (I), (II), (III) in the Introduction; i.e., if $\mathcal{X}$ is the Ree curve, it has been shown in [5] that $m = (q+1)(q+3q_0+1)$ and q^2 belong to the Weierstrass semigroup at some rational point of $\mathcal{X}$.

Now we consider a sublinear series of $\mathcal{D} = |mP_0|$. Let $\mathcal{X}$ and q be as above.

Definition 3.6. Let $x, f \in \mathbb{F}_q(\mathcal{X})$ such that $\operatorname{div}_\infty(x) = m_1(P_0)P_0$ and $\operatorname{div}_\infty(f) = mP_0$. We let $\mathcal{E}$ be the linear series defined by the morphism $\pi_{0,1,r} = (1 : x : f) : \mathcal{X} \to \mathbb{P}^2$.

Notice that $x : \mathcal{X} \to \mathbb{P}^1$ is a separable morphism.

Proposition 3.7. *The linear series $\mathcal{E}$ above is $\mathbb{F}_q$-Frobenius non-classical; i.e,*

$$f^q - f = (x^q - x)D_x^1 f\,.$$

Proof. Let $S = S(q, \mathcal{E})$ (resp. $0 < \nu$) be the $\mathbb{F}_q$-Frobenius divisor (resp. the $\mathbb{F}_q$-Frobenius sequence) associated to $\mathcal{E}$. We have to show that $\nu > 1$. In fact, by Lemma 2.2

$$\deg(S) = \nu(2\tilde{g} - 2) + (q+2)m \geq 2\tilde{N}$$

and from Lemma 3.3

$$\nu(3q_0 - 2)m + (q+2)m \geq 2(q - 3q_0 + 1)m$$

so that $\nu \geq (q - 6q_0)/(3q_0 - 2) \geq q_0 - 1 > 1$. Therefore the following matrix has rank two

$$\begin{pmatrix} 1 & x^q & f^q \\ 1 & x & f \\ 0 & 1 & D_x^1 f \end{pmatrix},$$

and the proof follows. □

The following result has been already noticed in [14, Prop. 3]. For the sake of completeness we state a proof.

Corollary 3.8. *Let $\mathcal{X}$ and q be as above and let $P \in \mathcal{X}(\mathbb{F}_q)$. Then the divisor $(2\tilde{g} - 2)P$ is canonical; in particular, the Weierstrass semigroup $H(P)$ at P is symmetric.*

Proof. By (3.4) and Lemma 3.3 we can assume $P = P_0$, where $\mathcal{D} = |mP_0|$. Let $\mathcal{E}$ be defined by $(1 : x : f)$ as above. Let v and t be respectively the valuation and a local parameter at P_0. We shall show that $v(D_t^1 x) = 2\tilde{g} - 2$.; from Proposition 3.7 we get

$$-qm = v(D_t^1 f) - v(D_t x) - qm_1(P_0)\,.$$

Since $v(D_t^1 f) = -m-1$, after some computations we indeed obtain $v(D_t^1 x) = (3q_0-2)m = 2\tilde{g} - 2$ by Lemma 3.3. □

Corollary 3.9. *Let $\mathcal{X}$ and q be as above. Let $P \in \mathcal{X}(\mathbf{F})$ and $x : \mathcal{X} \to \mathbb{P}^1$ be the morphism such that $\operatorname{div}_\infty(x) = m_1(P)P$. Then x is unramified outside P. Moreover, $x^{-1}(\alpha) \subseteq \mathcal{X}(\mathbf{F})$ for all $\alpha \in \mathbb{F}_q$.*

Proof. It follows from $\mathrm{div}(dx) = (2\tilde{g}-2)P$, $\#x^{-1}(\alpha) \le q^2$ for any $\alpha \in \mathbf{F}$, and $\tilde{N} = q^3+1$. □

We show next some properties of $\mathcal{D} = |mP_0|$. Let us recall that $m = m_r(P)$ for any $P \in \mathcal{X}(\mathbb{F}_q)$.

Proposition 3.10. *Let $\mathcal{X}$ and q be as above.*

(1) *The $(\mathcal{D}, P)$-order sequence at $P \in \mathcal{X}(\mathbf{F})$ is given by*

$$j_0(P) = 0 < j_1(P) = m - m_{r-1}(P) < \ldots < j_{r-1}(P) = m - m_1(P) < j_r(P) = m\,;$$

(2) $j_1(P) = 1$ *(or equivalently $m_{r-1}(P) = m-1$) at $P \in \mathcal{X}(\mathbb{F}_q)$;*
(3) *The numbers $1, 3q_0, 2q, 3q_0q$ and q^2 are $(\mathcal{D}, P)$-orders at $P \in \mathcal{X} \setminus \mathcal{X}(\mathbb{F}_q)$;*
(4) *The numbers $1, 3q_0, q, 2q, 3q_0q$ and q^2 are orders of $\mathcal{D}$;*
(5) $j_{r-1}(P) < q^2$ *at $P \in \mathcal{X}(\mathbf{F})$; in particular, $\nu_{r-1} = \epsilon_r = q^2$ being $\nu_0 < \ldots < \nu_{r-1}$ (resp. $\epsilon_0 < \ldots < \epsilon_r$) the $\mathbf{F}$-Frobenius orders (resp. orders) of $\mathcal{D}$.*

Proof. (1) Let $P \in \mathcal{X}(\mathbb{F}_q)$. For $i = 1, \ldots, r$ let $f_i \in \mathbf{F}(\mathcal{X})$ be such that $\mathrm{div}(f_i) = D_i - m_i(P)P$ with $P \notin \mathrm{Supp}(D_i)$. Then $\mathrm{div}(f_i) + mP = D_i + (m - m_i(P))P$ and (1) follows since $mP \sim mP_0$ by (3.4).

(2) Let $P \in \mathcal{X}(\mathbb{F}_q)$, $P \neq P_0$. By taking $x : \mathcal{X} \to \mathbb{P}^1$ with $\mathrm{div}_\infty(x) = m_1(P_0)P_0$, from Corollary 3.9 we have that $\mathrm{div}(x) = P + D - m_1(P_0)P_0$ and hence $j_1(P) = 1$. For $P = P_0$ we apply this argument by taking $\mathcal{D} = |mP_1|$ with $P_1 \in \mathcal{X}(\mathbb{F}_q) \setminus \{P_0\}$.

(3) Let $P \notin \mathcal{X}(\mathbf{F})$ and $Q \in \mathcal{X}$ such that $P = \mathbf{\Phi}^4(Q)$. From (3.4)

$$q^2Q + 3q_0q\mathbf{\Phi}(Q) + 2q\mathbf{\Phi}^2(Q) + 3q_0\mathbf{\Phi}^3(Q) + P \sim m_rP_0\,.$$

We have $\mathbf{\Phi}^i(Q) \neq P$ for $i = 0, 1, 2, 3$ as $N_1 = N_2 = N_3 = N_4$ by Proposition 3.1 so that $j_1(P) = 1$. In a similar way we prove that $3q_0$, $2q$, $3q_0q$ and q^2 are also $(\mathcal{D}, P)$-orders.

(3) In view of Item (3) we just need to show that q is an order. This follows from the p-adic criterion: $\binom{2q}{q} \not\equiv 0 \pmod 3$ (cf. Lemma 2.1(3)).

(4) Let $P \in \mathcal{X}(\mathbb{F}_q)$; then $\epsilon_{r-1} \le j_{r-1}(P) = m - m_1(P) = 3q_0q + 2q + 3q_0 + 1$ by Proposition 3.4. It follows that $\epsilon_{r-1} < q^2$ and hence $\epsilon_r = q^2$ since q^2 is an order of $\mathcal{D}$ (Item 3). By definition of $\mathcal{D}$, $\mathbf{\Phi}(Q)$ belongs to the osculating hyperplane at Q and so $\nu_{r-1} = \epsilon_r$. □

Next we show that the linear series $\mathcal{D}$ in Definition 3.2 is very ample.

Theorem 3.11. *Let $\mathcal{X}$ be the curve as above. The linear series $\mathcal{D}$ in Definition 3.2 is very ample; i.e., the morphism associated to $\mathcal{D}$ is an embedding.*

Proof. We have to show that $\mathcal{D}$ separates tangent vectors and points; cf. Hartshorne [6, p. 108]. The first condition was already proved in Proposition 3.10, namely $j_1(P) = 1$

for all $P \in \mathcal{X}$. Now we have to show that the morphism π associated to $\mathcal{D}$ is injective. If $\pi(P) = \pi(Q)$, then by (3.4)

$$\{P, \mathbf{\Phi}(P), \mathbf{\Phi}^2(P), \mathbf{\Phi}^3(P), \mathbf{\Phi}^4(P)\} = \{Q, \mathbf{\Phi}(Q), \mathbf{\Phi}^2(Q), \mathbf{\Phi}^3(Q), \mathbf{\Phi}^4(Q)\}\,.$$

Let $P = \mathbf{\Phi}^i(Q)$ with $i = 1, \ldots, 4$. We have

$$\mathbf{\Phi}^{i-1}(Q) \in \{\mathbf{\Phi}^i(Q), \mathbf{\Phi}^{i+1}(Q), \mathbf{\Phi}^{i+2}(Q), \mathbf{\Phi}^{i+3}(Q), \mathbf{\Phi}^{i+4}(Q)\}$$

so that $\mathbf{\Phi}^j(Q) = Q$ for some $1 \le j \le 5$. Proposition 3.1 implies $P = Q$. □

Remark 3.12. If $\mathcal{X}$ were the Ree curve, Theorem 3.11 was already shown by Eid and Duursma in [2, Prop. 5.4.]. In this case they also consider a sublinear series $\mathcal{D}_1$ of $\mathcal{D}$ which also define an embedding $\mathcal{X} \to \mathbb{P}^{13}$. The geometry $\mathcal{D}_1$ was further studied by Skabelund [17] who, among other things, computed its order sequence and showed that the set of $\mathcal{D}_1$-Weirstrass points coincides with the set of $\mathbf{F}$-rational points of $\mathcal{X}$. Related results can be found in Kane's paper [10].

4. Defining Equations

Let $\mathcal{X}$ be a curve over $\mathbb{F}_q$ satisfying (I) and (II) in Introduction. We let r be the (projective) dimension of the linear series $\mathcal{D} = |mP_0|$, $m = m_r = q^2 + 3q_0q + 2q + 3q_0 + 1$, which was introduced in Definition 3.2 (notice that $r \ge 6$ by Proposition 3.10(4)). The key point in this section is the study of a generalization of the linear series $\mathcal{E}$ in Definition 3.6.

Throughout, we let $f_0 = 1, f_1 = x, f_2, \ldots, f_r$ be the coordinates of the morphism π associated to $\mathcal{D}$. For $0 \le i < j < k \le r$, let $\mathcal{E}_{i,j,k}$ be the linear series defined by the morphism $\pi_{i,j,k} := (f_i : f_j : f_k)$; i.e.,

$$\mathcal{E}_{i,j,k} = \{E_{i,j,k} + \mathrm{div}(f) : f \in \langle f_i, f_j, f_k\rangle\}\,,$$

where $E_{i,j,k} = \sum_P e_P P$, $e_P = -\min\{v_P(f) : f \in \langle f_i, f_j, f_k\rangle\}$. Thus $E_{i,j,k} = m_k P_0 - D$ for certain positive divisor D with $P_0 \notin \mathrm{Supp}(D)$; notice that $D = 0$ for $i = 0$ and that $\mathcal{E}_{0,1,r} = \mathcal{E}$.

Proposition 4.1. *The linear series $\mathcal{E}_{i,j,k}$ above is $\mathbb{F}_q$-Frobenius non-classical; i.e.,*

$$\det\begin{pmatrix} f_i^q & f_j^q & f_k^q \\ f_i & f_j & f_k \\ D_x^1 f_i & D_x^1 f_j & D_x^1 f_k \end{pmatrix} = 0\,.$$

Proof. Similar to the proof of Proposition 3.7, by taking into consideration that $\deg(\mathcal{E}_{i,j,k}) \le m_k \le m$. □

As above we let $\nu_0 = 0 < \nu_1 < \ldots < \nu_{r-1}$ (resp. $\epsilon_0 = 0 < \epsilon_1 = 1 < \ldots < \epsilon_r$) be the $\mathbf{F}$-Frobenius orders (resp. orders) of $\mathcal{D}$. In Proposition 3.10(5) we have already observed that $\nu_{r-1} = \epsilon_r$; indeed, a strongest result is true:

Corollary 4.2. *The linear series $\mathcal{D}$ is $\mathbf{F}$-Frobenius non-classical; i.e., $\nu_1 = \epsilon_2 > 1$ (and thus $\nu_2 = \epsilon_3, \ldots, \nu_{r-1} = \epsilon_r$.)*

Proof. By Proposition 4.1 the rank of the matrix

$$\begin{pmatrix} 1 & x^q & f_2^q & \ldots & f_r^q \\ 1 & x & f_2 & \ldots & f_r \\ 0 & 1 & D_x^1 f_2 & \ldots & D_x^1 f_r \end{pmatrix}$$

is two and so $\nu_1 > \epsilon_1 = 1$. □

Let $m_0 = 0 < m_1 < m_2 < \ldots < m_{r-1} = m - 1 < m_r = m < m_{r+1} < \ldots$ be the non-gaps at P_0, where $\mathcal{D} = |mP_0|$. Let $i = 2, \ldots, r$. From Corollary 4.2 we obtain equations of type

$$f_i^q - f_i = D_x^1 f_i (x^q - x)\,. \tag{4.1}$$

We notice that each function $D_x^1 f_i$ is regular outside P_0 by Corollary 3.9 so that

$$-v(D_x^1 f_i) = q(m_i - m_1) \in H(P_0)\,, \tag{4.2}$$

where as above v is the valuation at P_0. For $q_0 \geq 9$ we are able to improve (4.2). Let us recall the following result concerning Hasse derivatives.

Lemma 4.3. (Hasse-Schmidt [7]) *Let δ be a power of the characteristic of $\mathbf{F}$ and $f \in \mathbf{F}(\mathcal{X})$. If $D^j f = 0$ for $j = 1, \ldots, \delta - 1$, then there exists $g \in \mathbb{F}_q(\mathcal{X})$ such that $f = g^\delta$.*

Lemma 4.4. *Let $(0, 1, \epsilon)$ be the order sequence of $\mathcal{E}_{0,1,i}$. If $q_0 \geq 9$, then:*

1. *ϵ is a power of 3, and there exists $g_i \in \mathbb{F}_q(\mathcal{X})$ such that $D_x^1 f_i = g_i^\epsilon$;*
2. *$q(m_i - m_1)/\epsilon \in H(P_0)$;*
3. *$m_i \geq m_1 + \epsilon q$, where $\epsilon \in \{q_0, 3q_0\}$.*

Proof. (1) With $f = D_x^1 f_i$ and $\delta = \epsilon$ we shall apply Lemma 4.3. We first show that ϵ is in fact a power of 3. Let $(0, \nu)$ be the $\mathbf{F}$-Frobenius orders of $\mathcal{E}_{0,1,i}$. Then $\nu = \epsilon$ by Proposition 4.1; now, as $\nu \geq q_0 - 1 > 2$ by hypothesis on q_0, ϵ is a power of 3 by the p-adic criterion (Lemma 2.1(3)).

From (4.1) we have $D_x^1 f = 0$. Let $j = 2, \ldots, \epsilon - 1$. Then we also have that $D_x^j f_i = 0$ by the very definition of ϵ. Finally by applying the chain rule in (4.1), $D_x^j f = 0$ and Item (1) follows.

(2) It follows from Item (1) and (4.2).

(3) We have $q(m_i - m_1)/\epsilon \geq m_1 = q^2$ so that

$$m_1 + \epsilon q \leq m_i \leq m_r = m_1 + 3q_0 q + 2q + 3q_0 + 1\,;$$

in particular, $\epsilon \leq 3q_0$ since ϵ is a power of 3. On the other hand, we have that $\epsilon \geq q_0$ as in the proof of Item (1). This finishes the proof. □

Corollary 4.5. *If $q_0 \geq 9$, then $\epsilon_{r-1} = 3q_0 q$.*

Proof. Notation as above. From Lemma 4.4(3), $m_2 \geq q^2 + q_0 q$ so that

$$\epsilon_{r-2} \leq j_{r-2}(P_0) = m - m_2 \leq 2q_0 q + 2q + 3q_0 + 1 < 3q_0 q\,.$$

The result then follows from Proposition 3.10(4). ☐

Now we are able to prove the main result of this paper.

Theorem 4.6. *Let $q = 3q_0^2$, $q_0 = 3^s \geq 9$. Let $\mathcal{X}$ be a curve over $\mathbb{F}_q$. Suppose that*

(I) $\#\mathcal{X}(\mathbb{F}_q) = \tilde{N} = q^3 + 1$;
(II) $g(\mathcal{X}) = \tilde{g} = \frac{3}{2}q_0(q-1)(q+q_0+1)$;
(III) *There exists $P_0 \in \mathcal{X}(\mathbb{F}_q)$ such that $q^2 + q_0 q, q^2 + 2q_0 q \in H(P_0)$.*

Then $\mathcal{X}$ is isomorphic to the Ree curve.

Proof. Let $P_0 \in \mathcal{X}(\mathbb{F}_q)$ be as above and v the valuation at P_0. Let $x \in \mathbb{F}_q(\mathcal{X})$ such that $\text{div}(x) = q^2 P_0$; recall that $m_1(P_0) = q^2$ (cf. Proposition 3.4 above) and hence the extension $\mathbb{F}_q(\mathcal{X})|\mathbb{F}_q(x)$ is separable. Let $y, z \in \mathbb{F}_q(\mathcal{X})$ such that $\text{div}_\infty(y) = (q^2 + q_0 q)P_0$, $\text{div}_\infty(z) = (q^2 + 2q_0 q)P_0$. Then from (4.1) and Lemma 4.3(1) we have equations of type

$$y^q - y = g^\alpha(x^q - x)\,, \quad z^q - z = h^\beta(x^q - x)\,,$$

where $\alpha, \beta \geq q_0$. Then $-v(g) = q(q_0 q)/\alpha \geq q^2$, $-v(h) = q(2q_0 q)/\beta \geq q^2$ and so $\alpha = \beta = q_0$. In particular, $v(g) = -q^2$ and $v(h) = -2q^2$. This implies that $g = ax + b$ and $h = cx^2 + dx + e$ with $a, b, c, d, e \in \mathbb{F}_q$, $ac \neq 0$. After a change of coordinates we find that $\mathcal{X}$ is defined by equations of type (1.1); i.e, it is $\mathbb{F}_q$−isomorphic to the Ree curve. ☐

Remark 4.7. (1) Let $\mathcal{X}$ and q be as above, $q_0 \geq 9$ and suppose that $q^2 + q_0 q \in H(P_0)$ for $P_0 \in \mathcal{X}(\mathbb{F}_q)$, then $m_2(P_0) = q^2 + q_0 q$ by Lemma 4.4.

(2) The hypothesis concerning Weierstrass non-gaps in the main result is natural in the sense that they are closely related to the equations that define the Ree curve.

Remark 4.8. The case $q_0 = 3$ can be handle in a similar way if we could show that for any $i = 2, \ldots, r$, $\mathcal{E}_{0,1,i}$ is not classical.

Acknowledgment. The authors were partially supported respectively by FAPESP/SP-Brazil (Grant 2017/19190-5) and CNPq/Brazil (Grant 310623/2017-0).

References

[1] P. Deligne and G. Lusztig, *Representations of reductive groups over finite fields*, Ann. of Math. **103** (1976), 103–161.
[2] A. Eid and I. Duursma, *Smooth embeddings for the Suzuki and Ree curves*, Algorithmic arithmetic, geometry, and coding theory, Contemp. Math., **637**, Amer. Math. Soc., Providence, RI, 2015, 251–291,

[3] R. Fuhrmann and F. Torres, *On Weierstrass points and optimal curves*, Rend. Circ. Mat. Palermo Suppl. **51** (1998), 25–46.

[4] J.P. Hansen, *Deligne-Lusztig varieties and group codes*, Lect. Notes Math. **1518** (1992), 63–81.

[5] J.P. Hansen and J.P. Pedersen, *Automorphism group of Ree type, Deligne-Lusztig curves and function fields*, J. reine angew. Math. **440** (1993), 99–109.

[6] R. Hartshorne, "Algebraic Geometry", Grad. Texts in Maths. 52, Springer, New York, 1977.

[7] H. Hasse and F.K. Schmidt, *Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten*, J. reine angew. Math. **177** (1937), 215–237.

[8] A. Hefez, *Reflexive curves*, Compositio Math. **69** (1989), 3–25.

[9] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, "Algebraic Curves over a Finite Field", Princenton Univ. Press 2008.

[10] D.M. Kane, *Canonical Projective Embedding of the Deligne-Lusztig Curves Associated to $^2A_2$, $^2B_2$ and $^2G_2$*, Int, Math. Res. Not. **4** (2016), 1158–1189.

[11] S. Lang, Abelian Varieties, Interscience Pub., New York 1959.

[12] Lewittes, J., *Places of degree one in function fields over finite fields*, J. Pure Appl. Alg. **69** (1990), 177–183.

[13] C. Munuera, A. Sepúlveda and F. Torres, *Castle curves and codes*, Adv. Math. Commun. **3**(4) (2009), 399–408.

[14] C. Munuera, A. Sepúlveda and F. Torres, *Algebraic Geometry codes from Castle curves*, Lect. Notes in Comput. Sci. **5228** (2008), 128–126.

[15] J.P. Pedersen, *A function field related to the Ree group*, Lect. Notes Math. **1518** (1992), 122–131.

[16] H.G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. reine angew. Math. **457** (1994), 185–188.

[17] D. C. Skabelund, *On the order sequence of an embedding of the Ree curve*, arXiv: 1705.04268v3.

[18] H. Stichtenoth, "Algebraic Function Fields and Codes", Second Edition, Springer-Verlag, Berlin Heildelberg, 2009.

[19] K.O. Stöhr and J.F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), 1–19.

[20] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones Math. **2** (1966), 134–144.

IMECC/UNICAMP, R. Sérgio Buarque de Holanda, 651, Cidade Universitária "Zeferino Vaz", 13083-859, Campinas, SP, Brazil

E-mail address: tafazolian@ime.unicamp.br

E-mail address: ftorres@ime.unicamp.br