ON WEIERSTRASS POINTS AND OPTIMAL CURVES

RAINER FUHRMANN AND FERNANDO TORRES

Abstract. We show some properties of maximal curves and give a characterization of the Suzuki curve by means of its genus and the number of its rational points only.

1. Introduction

Let X be a (non-singular, projective, geometrically irreducible, algebraic) curve of genus g defined over the finite field $\mathbb{F}_\ell$ of order ℓ. The curve is called (ℓ, g)-*optimal* if

$$\#X(\mathbb{F}_\ell) = N_\ell(g) := \max\{\#Y(\mathbb{F}_\ell) : Y \text{ a curve of genus } g \text{ defined over } \mathbb{F}_\ell\}\,.$$

These curves are very important in several areas of mathematics such as Coding Theory after Goppa's work [10]. The Hasse-Weil bound gives $N_\ell(g) \leq \ell+1+2g\sqrt{\ell}$. If $\#X(\mathbb{F}_\ell) = \ell + 1 + 2g\sqrt{\ell}$, the curve is called *maximal*. Arithmetical and geometrical properties of maximal curves have been pointed out in [7] and [8] by using the geometrical approach of Stöhr-Voloch theory [26] to the Hasse-Weil bound. In Section 4 we compute the Frobenius order sequence of a natural linear series associated to these curves as well as some properties concerning Weierstrass semigroups. Ihara [17] showed that the genus g of a maximal curve satisfies $g \leq g_1 := \sqrt{\ell}(\sqrt{\ell}-1)/2$ and Rück and Stichtenoth [23] proved that the Hermitian curve: $x^{\sqrt{\ell}+1} + y^{\sqrt{\ell}+1} + 1 = 0$ is the unique maximal curve of genus g_1. In [20, Sect. 6] one can find another proof of this result.

Let $\ell_0 = 2^s > 2$ be a power of two and set $\ell := 2\ell_0^2$. In Section 5 we give a characterization of the Deligne-Lusztig variaty associated to a connected reductive algebraic group of type ${}^2B_2$ over $\mathbb{F}_\ell$; such a variaty is a curve of genus $\tilde{g} = \ell_0(\ell - 1)$, number of $\mathbb{F}_\ell$-rational points equals $\tilde{N} = \ell^2+1$ whose $\mathbb{F}_\ell$-automorphism group is the Suzuki group, cf. [4], [11], [12], [21]. This curve is the so-called *Suzuki curve* and it is $(\ell, \tilde{g})$-optimal, loc. cit.. The main result of this section is to show that the Suzuki curve is the unique curve defined over $\mathbb{F}_\ell$ with the parameters $\tilde{g}$ and $\tilde{N}$ above, see Theorem 5.1.

In Section 2 we recall some basic results from [26]. In Section 3 we notice an interplay between Zeta functions and linear series on curves over finite fields.

This paper was partially written while the second author was visiting the University of Essen (supported by the Graduiertenkolleg "Theoretische und experimentelle Methoden der Reinen Mathematik"); ICTP, Trieste -Italy (supported by ICTP) and IMPA, Rio de Janeiro-Brazil (supported by CNPq).

Rend. Circ. Mat. Palermo Suppl. 51 (1998), 25–46.

Revised version: January, 2008.

2. On the Stöhr-Voloch theory

In this section we recall some results of Stöhr-Voloch paper [26] concerning Weierstrass points and Frobenius orders.

Let $\mathcal{D} \subseteq |E|$ be a base-point-free linear series of dimension N and degree d on a curve X of genus g. For $P \in X$ and $i \geq 0$ an integer, we define sub-sets of $\mathcal{D}$ which will provide with geometric information on 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 $i > d$,

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

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 $\mathcal{D}_i(P) \supsetneqq \mathcal{D}_{i+1}(P)$, then the integer i is called a $(\mathcal{D}, P)$-*order*; thus by Linear Algebra we have a sequence of $(N+1)$ orders at P:

$$0 = j_0(P) < j_1(P) < \cdots < j_N(P) \leq d\,.$$

Notice that $\mathcal{D} = \mathcal{D}_0(P)$ since $\mathcal{D}$ is base-point-free by hypothesis. It is a fundamental result the fact that the sequence above is the same for all but finitely many points P of X, see [26, Thm. 1.5]. This constant sequence is called the *order sequence* of $\mathcal{D}$ and will be denoted by

$$0 = \epsilon_0 < \epsilon_1 < \cdots < \epsilon_N\,.$$

The finitely many points P, where exceptional $(\mathcal{D}, P)$-orders occur, are called the $\mathcal{D}$-*Weierstrass points* of X. There exists a divisor R on X, the *ramification divisor* of $\mathcal{D}$, whose support is exactly the set of $\mathcal{D}$-Weierstrass points:

$$R = \operatorname{div}(\det(D_t^{\epsilon_i} f_j)) + (\sum_{i=0}^{N} \epsilon_i)\operatorname{div}(\mathrm{dt}) + (N+1)E\,,$$

where $\pi = (f_0 : f_1 : \cdots : f_N)$ is the morphism defined by $\mathcal{D}$ (up to equivalence), t a separating element of $\bar{\mathbb{F}}_\ell(X)|\bar{\mathbb{F}}_\ell$ and the operators $D_t^{\epsilon_i}$'s are the Hasse derivaties (properties of these operators can be found in Hefez's paper [15]). Moreover, the number of $\mathcal{D}$-Weierstrass points of X (counted with multiplicity) is the degree of R.

Now to deal with rational points over $\mathbb{F}_\ell$ we require that both X and $\mathcal{D}$ be defined over $\mathbb{F}_\ell$. Choose the coordenates f_i's above in such a way that $v_P(f_i) + v_P(E) = j_i(P)$, where v_P denotes the valuation at P. Set $L_i(P) = \langle f_i, \cdots, f_N\rangle$. Thus

$$\mathcal{D}_i(P) = \{\operatorname{div}(f) + E : f \in L_i(P)\}\,.$$

For $i = 0, \cdots, N-1$ set

$$S_i(P) := \mathcal{D}_{j_{i+1}}(P) \cap \cdots \cap \mathcal{D}_{j_N}(P) \quad \text{and}$$

$$T_i(P) := \cap_{D \in S_i} \operatorname{Supp}(D)\,.$$

This is a subspaces of the dual of $\mathbb{P}^N(\bar{\mathbb{F}}_\ell)$ whose projective dimension is i. Notice that

$$\{P\} = T_0(P) \subsetneq T_1(P) \subsetneq \cdots \subsetneq T_{N-1}(P)\,.$$

The spaces $T_{N-1}(P)$ and $T_1(P)$ are usually called the $\mathcal{D}$-*osculating hyperplane* and the $\mathcal{D}$-*tangent line* at P respectively.

Let $\mathbf{\Phi} : X \to X$ be the Frobenius morphism on X. Suppose that for a generic P, $\mathbf{\Phi}(P) \in T_{N-1}(P)$. Then there exists an integer $1 \le I \le N-1$ such that $\phi(P) \in T_I(P) \setminus T_{I-1}(P)$. Define $\nu_j := \epsilon_j$ for $0 \le j \le I-1$ and $\nu_j = \epsilon_{j+1}$ for $j = I, \cdots, N-1$. The sequence $0 = \nu_0 < \nu_1 < \cdots < \nu_{N-1}$ is called the *Frobenius order sequence* of $\mathcal{D}$ (with respect to $\mathbb{F}_\ell$; cf. [26, Sect. 2]). The key property related with rational points in [26] is the existence of a divisor S, *the Frobenius divisor* of X (over $\mathbb{F}_\ell$) satisfying Lemma 2.1(3)(4)(5)(6) below. This divisor is defined as follows. Let $\tilde{L}$ denote the determinant of the matrix whose rows are:

$$(f_0^\ell, f_1^\ell, \cdots, f_N^\ell)\,, \quad (D_t^{\nu_i} f_0, D_t^{\nu_i} f_1, \cdots, D_t^{\nu_i} f_N)\,, \quad i = 0, 1, \cdots, N-1\,.$$

Then

$$S := \mathrm{div}(\tilde{L}) + (\sum_{i=0}^{N-1} \nu_i)\mathrm{div}(\mathrm{dt}) + (\ell + N)E\,.$$

We notice that $X(\mathbb{F}_\ell) \subseteq \mathrm{Supp}(S)$ and $v_P(S) \ge N$ for $P \in X(\mathbb{F}_\ell)$ (Lemma below). Thus

$$\#X(\mathbb{F}_\ell) \le \deg(S)/N\,.$$

We subsume some properties of the ramification divisor and Frobenius divisor of $\mathcal{D}$.

Lemma 2.1. *Let $P \in X$ and ℓ be a power of a prime p.*

1. *For each i, $j_i(P) \ge \epsilon_i$;*
2. $v_P(R) \ge \sum_{i=0}^{N}(j_i(P) - \epsilon_i)$; *equality holds if and only if* $\det\left(\binom{j_i(P)}{\epsilon_j}\right) \not\equiv 0 \pmod p$;
3. *If $P \in X(\mathbb{F}_\ell)$, then for each i, $\nu_i \le j_{i+1}(P) - j_1(P)$;*
4. *If $P \in X(\mathbb{F}_\ell)$, then $v_P(S) \ge \sum_{i=0}^{N-1}(j_{i+1}(P) - \nu_i)$; equality holds if and only if* $\det\left(\binom{j_{i+1}(P)}{\nu_j}\right) \not\equiv 0 \pmod p$;
5. *If $P \in X(\mathbb{F}_\ell)$, then $v_P(S) \ge N j_1(P)$;*
6. *If $P \notin X(\mathbb{F}_\ell)$, then $v_P(S) \ge \sum_{i=0}^{N-1}(j_i(P) - \nu_i)$.*

3. Z-functions and Linear Series

Let X be a curve of genus g defined over $\mathbb{F}_\ell$ with $\#X(\mathbb{F}_\ell) > 0$. Let $h(t) := t^{2g}L(t^{-1})$, where $L(t)$ is the enumerator of the Zeta function of X. Then $h(t)$ is monic, of degee $2g$ whose independent term is non-zero, see e.g. [25]; moreover, $h(t)$ is the characteristic polynomial of the Frobenius morphism $\mathbf{\Phi}_{\mathcal{J}}$ on the Jacobian $\mathcal{J}$ of X (by considering $\mathbf{\Phi}_{\mathcal{J}}$ as an endomorphism on a Tate module). Let $h(t) = \prod_i h_i^{r_i}(t)$ be the factorization of $h(t)$ in $\mathbb{Z}[t]$. Since $\mathbf{\Phi}_{\mathcal{J}}$ is semisimple and the representation of endomorphisms of $\mathcal{J}$ on the Tate module is faithfully, see [27, Thm. 2], [19, VI§3], it follows that

$$\prod_i h_i(\mathbf{\Phi}_{\mathcal{J}}) = 0\,. \tag{3.1}$$

Let $\mathbf{\Phi}$ denote the Frobenious morphism on X. Let $\pi : X \to \mathcal{J}$ be the natural morphism $P \mapsto [P - P_0]$, where $P_0 \in X(\mathbb{F}_\ell)$. We have $\pi \circ \mathbf{\Phi} = \mathbf{\Phi}_{\mathcal{J}} \circ \pi$ and thus (3.1) implies the following linear equivalence of divisors

$$\prod_i h_i(\mathbf{\Phi}(P)) \sim mP_0\,, \quad \text{where } P \in X \text{ and } m = \prod_i h_i(1)\,. \tag{3.2}$$

This suggests the study of the linear series

$$\mathcal{D} := |mP_0|\,.$$

Let us write

$$\prod_i h_i(t) = t^U + \alpha_1 t^{U-1} + \alpha_2 t^{U-2} + \cdots + \alpha_{U-1} t + \alpha_U\,.$$

We assume:

(A) $\alpha_1 \geq 1$
(B) $\alpha_{i+1} \geq \alpha_i$ for $i = 1, \cdots, U-1$.

Remark 3.1. There are curves which do not satisfy conditions (A) and (B) above. For example, if X is a *minimal* curve of genus g; i.e., $\#X(\ell) = \ell + 1 - 2\sqrt{\ell}g$, then $h(t) = (t - \sqrt{\ell})^{2g}$. Further examples can be found in [2].

Next we compute some invariants of the linear series $\mathcal{D}$ above according to the results in Section 2; we use the notation of that section. Let N be the dimention of $\mathcal{D}$. For $P \in X(\mathbb{F}_\ell)$ we have the following sequence of non-gaps at P:

$$0 = m_0(P) < m_1(P) < \cdots < m_{N-1}(P) < m_N(P) = m\,.$$

Lemma 3.2. (1) *If $P \in X(\mathbb{F}_\ell)$, then the $(\mathcal{D}, P)$-orders are*

$$0 = m - m_N(P) < m - m_{N-1}(P) < \cdots < m - m_1(P) < m - m_0(P)\,;$$

(2) *If $P \notin X(\mathbb{F}_\ell)$, then $j_1(P) = 1$;*
(3) *The numbers $1, \alpha_1, \cdots, \alpha_U$ are orders of $\mathcal{D}$;*
(4) *If $\mathbf{\Phi}^i(P) \neq P$ for $i = 1, 2, \cdots, U+1$, then α_U is a non-gap at P. In particular, α_U is a generic non-gap of X;*
(5) *If $\mathbf{\Phi}^i(P) \neq P$ for $i = 1, 2, \cdots, U$ and $\mathbf{\Phi}^{U+1}(P) = P$, then $\alpha_U - 1$ is also a non-gap at P;*
(6) *If $g \geq \alpha_U$, then the curve is non-classical with respect to the canonical linear series.*

Proof. The proof of (1), (2) or (3) is similar to [8, Thm. 1.4, Prop. 1.5]. To show the other statements, let us apply $\mathbf{\Phi}_*$ in (3.2); thus

$$\alpha_U P \sim \mathbf{\Phi}^{U+1}(P) + (\alpha_1 - 1)\mathbf{\Phi}^U(P) + (\alpha_2 - \alpha_1)\mathbf{\Phi}^{U-1}(P) + \cdots + (\alpha_U - \alpha_{U-1})\mathbf{\Phi}(P)\,.$$

Then (4) and (5) follow from hypothesis (A) and (B) above. Finally, a non-classical curve of genus g is characterized for having a generic non-gap $n \le g$; hence (4) implies (6). □

We finish this section with some properties involving the number of rational points.

Proposition 3.3. *Suppose that* $\mathrm{char}(\mathbb{F}_\ell)$ *does not divide* m.

(1) *If* $\#X(\mathbb{F}_\ell) \ge 2g+3$, *then there exists* $P \in X(\mathbb{F}_\ell)$ *such that* $(m-1)$ *and* m *are non-gaps at* P;
(2) *The linear series* $\mathcal{D}$ *is simple*; *i.e., the morphism* $\pi : X \to \pi(X) \subseteq \mathbb{P}^N(\bar{\mathbb{F}}_\ell)$ *defined by* $\mathcal{D}$ *is birational.*

Proof. (1) (Following [28]) Let $P \ne P_0$ be a rational point. We have $mP \sim mP_0$ by (3.2). Let $x : X \to \mathbb{P}^1(\bar{\mathbb{F}}_\ell)$ be a rational function with $\mathrm{div}(x) = mP - mP_0$. Let n be the number of rational points wchich are unramified for x. Then by Riemann-Hurwitz $2g-2 \ge m(-2) + 2(m-1) + (\#X(\mathbb{F}_\ell) - n - 2)$ so that $n \ge \#X(\mathbb{F}_\ell) - (2g+2) \ge 1$. Thus there exists $Q \in X(\mathbb{F}_\ell)$, $Q \ne P, P_0$ such that $\mathrm{div}(x-a) = Q + D - mP_0$ with $D \in \mathrm{Div}(X)$, $P_0, Q \notin \mathrm{Supp}(D)$. Let y be a rational function such that $\mathrm{div}(y) = mP_0 - mQ$. Then $\mathrm{div}((x-a)y) = D - (m-1)Q$ and the proof is complete.

(2) Let $Q \in X(\mathbb{F}_\ell)$ be the point in (1) and $x, y \in \mathbb{F}_\ell(X)$ such that $\mathrm{div}_\infty(x) = (m-1)Q$ and $\mathrm{div}_\infty(y) = mQ$. Then $\mathbb{F}_\ell(X) = \mathbb{F}_\ell(x,y)$ and we are done. □

Proposition 3.4. (1) $\epsilon_N = \nu_{N-1}$;
(2) *Let* $P \in X(\mathbb{F}_\ell)$ *and suppose that* $\#X(\mathbb{F}_\ell) \ge \ell(m-\alpha_U)+2$. *Then* $j_{N-1}(P) < \alpha_U$; *in particular,* $\epsilon_N = \alpha_U$ *and* P *is a* $\mathcal{D}$*-Wierstrass point*;
(3) *If* $\#X(\mathbb{F}_\ell) \ge \ell\alpha_U + 1$, *then* $\#X(\mathbb{F}_\ell) = \ell\alpha_U + 1$ *and* $m_1(P) = \alpha_U$ *for any* $P \in X(\mathbb{F}_\ell)$.

Proof. (1) Definition of $\mathcal{D}$.

(2) We have that $\#X(\mathbb{F}_\ell) \le \ell m_1(P) + 1$ by Lewittes [18, Thm. 1(b)]. Then the result follows from Lemma 3.2.

(3) Let $P \in X(\mathbb{F}_\ell)$. We have $m_1(P) \le m_1(Q)$ where Q is a generic point of X (apply Section 2 to the canonical linear series on X). Therefore, $m_1(Q) \le \alpha_U$ by Lemma 3.2 and hence $\ell\alpha_U + 1 \le \#X(\mathbb{F}_\ell) \le \ell m_1(P) + 1 \le \ell\alpha_U + 1$. □

4. Maximal Curves: Frobenius orders and Weierstrass semigroups

Notation as in Sections 2 and 3. Throughout X will denote a maximal curve of genus g defined over $\mathbb{F}_{q^2}$. Let $\mathbf{\Phi} : X \to X$ denote the Frobenius morphism on X. The characteristic polynomial of its Jacobian $\mathcal{J}$ is $h(t) = (t+q)^{2g}$. Thus X is equipped with the linear series $\mathcal{D} = |(q+1)P_0|$, where $P_0 \in X(\mathbb{F}_{q^2})$ and $(q+1)P_0 \sim qP + \mathbf{\Phi}(P)$ for any $P \in X$. If N denotes the dimention of $\mathcal{D}$, for $P \in X$ we have the following sequence of non-gaps at P:

$$0 = m_0(P) < m_1(P) < \cdots < m_{N-1}(P) \leq q < m_N(P)\,.$$

A. The Frobenius orders of a maximal curve. We are interested in computing the Frobenius orders of the linear series $\mathcal{D}$. Let us recall the following result from [8]. For the sake of completeness we give a proof. Let

$$0 = \tilde{m}_0 < \tilde{m}_1 < \tilde{m}_2 < \tilde{m}_3 < \cdots$$

be the sequence of generic non-gaps of X.

Proposition 4.1. *If $P \not\in X(\mathbb{F}_\ell)$, then the numbers $0, 1, q - m_{N-1}(P), \cdots, q - m_1(P), q$ are $(\mathcal{D}, P)$-orders. In particular, the numbers $0, 1, q - \tilde{m}_{N-1}, \cdots, q - \tilde{m}_1, q$ are orders of $\mathcal{D}$.*

Proof. By Lemma 3.2, 1 is an $(\mathcal{D}, P)$-order. Set $m_i = m_i(P)$. Let v and u_i, $i = 0, \cdots, N-1$, be rational functions such that $\mathrm{div}(v) = qP + \mathbf{\Phi}(P) - (q+1)P_0$ and $\mathrm{div}(u_i) = D_i - m_iP$ with $P \not\in \mathrm{Supp}(D_i)$. Thus $\mathrm{div}(vu_i) = D_i + \mathbf{\Phi}(P) + (q - m_i)P - (q+1)P_0$ and the assertion follows. □

We recall that $\tilde{m}_{N-1} = q$ and $\tilde{m}_{N-2} = q - 2$ for $N \geq 3$ (see [8, Prop. 1.5(v)]). Thus if $N = 2$, the orders of $\mathcal{D}$ are $0, 1, q$. If $N \geq 3$ we only get $N - 1$ orders, namely

$$0 = q - \tilde{m}_{N-1} < 1 = q - \tilde{m}_{N-2} < \cdots < q - \tilde{m}_1 < q - \tilde{m}_0\,. \tag{4.1}$$

Theorem 4.2. *If $N \geq 3$, then the Frobenius orders of $\mathcal{D}$ are precisely the orders of $\mathcal{D}$ listed in* (4.1).

Proof. (Notation as in the proof of Proposition 4.1) We have seen that $\mathrm{div}(vu_i) = D_i + \mathbf{\Phi}(P) + (q - \tilde{m}_i)P - (q+1)P_0$. Let ϵ_I be the missing order of $\mathcal{D}$ in (4.1). We put $\epsilon_{I-1} = q - \tilde{m}_{J-1} < \epsilon_I < \epsilon_{I+1} = q - \tilde{m}_J$. Thus $\mathbf{\Phi}(P) \in T_I(P)$. We claim that $\mathbf{\Phi}(P) \not\in T_{I-1}$, otherwise $q - \epsilon_I \in H(P)$ which is a contradiction. □

B. Canonical Weierstrass semigroups on maximal curve. We know that $m_N(P) = q + 1$ for any $P \in X(\mathbb{F}_{q^2})$. In particular, $g \geq q + 1 - N$ and

$$g = q + 1 - N \quad \Leftrightarrow \quad \{q+1, q+2, \cdots,\} \subseteq H(P) \quad \text{for any } P \in X\,.$$

Since q is a non-gap at a non-Weiersstrass point (Lemma 3.2) we also have

$$X \text{ classical} \quad \Rightarrow \quad g = q + 1 - N\,.$$

The reciprocal assertion is not true (see e.g. [8, Prop. 1.8]); we remark that the term "classical" is with respect to the canonical linear series of the curve. The following results are contained in the proof of [6, Satz II.2.5].

Lemma 4.3. *Let X be a maximal curve of genus g over $\mathbb{F}_{q^2}$ and P a non-Weierstrass point of X. If $q+1 \in H(P)$, then $q+1, \cdots, 2q \in H(P)$. In particular, as $q \in H(P)$, $\{q+1, q+2, \cdots\} \subseteq H(P)$ and $g = q+1-N$.*

Proof. Let $i \in \{1, \cdots, q\}$ such that $q+i \notin H(P)$; then $\binom{q+i-1}{q} \not\equiv 0 \pmod{\mathrm{char}(\mathbb{F}_{q^2})}$. Hence, by the p-adic criterion [26, Cor. 1.9], $q+1 \notin H(P)$. □

Corollary 4.4. *$g = q+1-N$ if and only if $q+1$ is a non-gap at a non-Weierstrass point of X.*

Corollary 4.5. *If $g > q+1-N$, then each $\mathbb{F}_{q^2}$-rational point of X is a Weierstrass point.*

Remark 4.6. Corollary 4.5 is false if $g = q+1-N$; see e.g. [8, Ex. 1.6].

5. The Suzuki curve

Througout this section we let $\ell_0 = 2^s > 2$ be a power of two and set $\ell := 2\ell_0^2$. As we already mentioned in the introduction, the Suzuki curve is the Deligne-Lusztig curve defined over $\mathbb{F}_\ell$ associated to a grupo of type ${}^2B_2$. It is characterized by the following data (see e.g. [12], [11]):

(I) genus: $\tilde{g} = \ell_0(\ell - 1)$;
(II) number of $\mathbb{F}_\ell$-rational points: $\tilde{N} = \ell^2 + 1$;
(III) $\mathbb{F}_\ell$-automorphism group equals the Suzuki group.

In this section we prove the following.

Theorem 5.1. *The Suzuki curve is the unique curve that satisfies both properties (I) and (II) above.*

Let us fix a curve X of genus $\tilde{g} = \ell_0(\ell - 1)$ over $\mathbb{F}_\ell$ having $\tilde{N} = \ell^2 + 1$ number of $\mathbb{F}_\ell$-rational points. The starting point of the proof is the fact that the characteristic polynomial of the Frobenius morphism of the Jacobian of X is given by [12]

$$h(t) = (t^2 + 2\ell_0 t + \ell)^g\,.$$

Let $\mathbf{\Phi} : X \to X$ be the Frobenius morphism on X. From Section 3 we conclude that X is equipped with the linear series $\mathcal{D} := |(1+2\ell_0+\ell)P_0|$, $P_0 \in X(\mathbb{F}_\ell)$, where for any $P \in X$

$$\mathbf{\Phi}^2(P) + 2\ell_0\mathbf{\Phi}(P) + \ell P \sim (1+2\ell_0+\ell)P_0\,. \tag{5.1}$$

Let N denote the dimention of $\mathcal{D}$. We already know that $m = m_N(P) = 1+2\ell_0+\ell$ for any $P \in X(\mathbb{F}_\ell)$. Lemma 3.2 and Propotition 3.4 imply the following properties of X:

(a) $m_1(P) = \ell$ and $j_{N-1}(P) = 1+2\ell_0$ for any $P \in X(\mathbb{F}_\ell)$;
(b) $\epsilon_1 = 1$ and $\epsilon_N = \nu_{N-1} = \ell$.

Lemma 5.2. *$N \geq 3$ and $\epsilon_{N-1} = 2\ell_0$.*

Proof. By Lemma 3.2 the numbers 1, $2\ell_0$ and ℓ are orders of $\mathcal{D}$ and thus $N \geq 3$. Since $\epsilon_{N-1} \leq j_{N-1}(P) = 1+2\ell_0$ (Lemma 2.1) and $\epsilon_N = \ell$ we have that

$$2\ell_0 \leq \epsilon_{N-1} \leq 1+2\ell_0\,.$$

Suppose that $\epsilon_{N-1} = 1+2\ell_0$ (observe that $2\ell_0$ is also an order of $\mathcal{D}$). Let $P \in X(\mathbb{F}_\ell)$. By Lemma 2.1

$$\nu_{N-2} \leq j_{N-1}(P) - j_1(P) \leq \epsilon_{N-2} = 2\ell_0\,.$$

Thus the sequence of Frobenius order of $\mathcal{D}$ would be $\epsilon_0, \epsilon_1, \cdots, \epsilon_{N-2}, \epsilon_N$. Now for any $P \in X(\mathbb{F}_\ell)$ (Lemma 2.1)

$$v_P(S) \geq \sum_{i=0}^{N-1}(j_{i+1}(P)-\nu_i) = \sum_{i=0}^{N-2}(j_{i+1}(P)-\nu_i)+(j_N(P)-\nu_{N-1}) \geq (N-1)j_1(P)+1+2\ell_0$$

so that

$$\deg(S) \geq (N+2\ell_0)\tilde{N}\,. \tag{5.2}$$

From the following identities

- $2\tilde{g}-2 = (2\ell_0-2)(1+2\ell_0+\ell) = (2\ell_0-2)m_N(P)$ and
- $\tilde{N} = (1-2\ell_0+\ell)(1+2\ell_0+\ell) = (1-2\ell_0+\ell)m_N(P)$,

inequality (5.2) becomes

$$(2\ell_0-2)\sum_{i=0}^{N-1}\nu_i + (N+\ell) \geq (N+2\ell_0)(1-2\ell_0+\ell)\,.$$

Since $\nu_{N-1} = \ell$ it follows that

$$\sum_{i=0}^{N-2}\epsilon_i = \sum_{i=0}^{N-2}\nu_i \geq (N-1)\ell_0\,.$$

Next we use a property involving the orders of $\mathcal{D}$ (see [5]): $\epsilon_i + \epsilon_j \le \epsilon_{i+j}$ for $i + j \le N$. We apply this in the form $\epsilon_i + \epsilon_j \le \epsilon_{N-2}$ with $i + j = N - 2$. Thus

$$2\sum_{i=0}^{N-2} \epsilon_i \le (N-1)\epsilon_{N-2} = (N-1)2\ell_0\,.$$

From the last two inequalities we conclude that $\epsilon_i + \epsilon_{N-2-i} = \epsilon_{N-2}$ for $i = 0, 1, \cdots, N-2$. In particular, $\epsilon_{N-3} = 2\ell_0 - 1$ and the p-adic criterion (cf. [26, Cor. 1.9]) would imply $\epsilon_i = i$ for $i = 0, 1, \cdots, N-3$. These facts imply $N = 2q_0 + 2$. Finally, we are going to see that this is a contradiction according to Castelnuovo's genus bound (see e.g. [3], [1, p. 116], [22, Cor. 2.8]). Castelnuovo's formula applied to $\mathcal{D}$ implies

$$2\tilde{g} = 2\ell_0(\ell-1) \le \frac{(\ell + 2\ell_0 - (N-1)/2)^2}{N-1}\,.$$

For $N = 2\ell_0 + 2$ this gives $2\ell_0(\ell-1) < (\ell+\ell_0)^2/2\ell_0 = \ell_0\ell + \ell/2 + \ell_0/2$, a contradiction. □

Remark 5.3. Here we write a more simple proof of the previous lemma. We have $2\ell_0 \le \epsilon_{N-1} \le j_{N-1}(P) = 1 + 2\ell_0$. Suppose $\ell_{N-1} = 1 + 2\ell_0$ and thus $\ell_{N-2} = 2\ell_0$. For any $P \in X(\mathbb{F}_\ell)$ $\ell_{N-2} \le j_{N-2}(P) < j_{N-1}(P) = 1 + 2\ell_0$. Thus for any $P \in X(\mathbb{F}_\ell)$ $j_{N-2}(P) = 2\ell_0$ and $1 + \ell \in H(P)$. If we take $\tilde{P} \in X(\mathbb{F}_\ell)$ such that $1 + 2\ell_0 + \ell, 2\ell_0 + \ell \in H(\tilde{P})$ (Proposition 3.3) we find that $H(\tilde{P})$ contains the semigroup

$$H := \langle \ell, \ell+1, 2\ell_0 + \ell, 1 + 2\ell_0 + \ell \rangle$$

and hence $\tilde{g} \le g(H) := (\mathbb{N}_0 \setminus H)$. However one shows that $\tilde{g} > g(H)$, cf. Remark 5.6 below.

Lemma 5.4. *There exists $P \in X(\mathbb{F}_\ell)$ such that the following properties hold true*:

(1) $j_1(P) = 1$;
(2) $j_i(P) = \nu_{i-1} + 1$ *for* $i = 2, \cdots, N-1$.

Proof. Let $P \in X(\mathbb{F}_\ell)$. In the proof of Lemma 5.2 we obtained the following inequality

$$v_P(S) \ge \sum_{i=0}^{N-2} (j_{i+1}(P) - \nu_i) + 1 + 2\ell_0 \ge (N-1)j_1(P) + 1 + 2\ell_0 \ge N + 2\ell_0\,.$$

Thus it is enough to show that $v_P(S) = N + 2\ell_0$ for some point $P \in X(\mathbb{F}_\ell)$. Suppose on the contrary that $v_P(S) \ge N + 2q_0 + 1$ for any $P \in X(\mathbb{F}_\ell)$. Then arguing as in the proof of Lemma 5.2 we would have

$$\sum_{i=0}^{N-2} \nu_i \ge N\ell_0 + 1\,.$$

As $\nu_i \le \epsilon_{i+1}$, then

$$1+\sum_{i=0}^{N-2}\nu_i \le \sum_{i=0}^{N-1}\epsilon_i \le N\epsilon_{N-1}/2;$$

thus

$$N\ell_0+2\le N\epsilon_{N-1}/2$$

so that $\epsilon_{N-1} > 2\ell_0$ which is a contradiction according to Lemma 5.2. □

Lemma 5.5. (1) ϵ_2 *is a power of two*;
(2) $\nu_1 > \epsilon_1 = 1$.

Proof. (1) It is a consequence of the p-adic criterion [26, Cor. 1.9].

(2) Suppose that $\nu_1 = 1$. Let P be a $\mathbb{F}_\ell$-rational point satisfying Lemma 5.4. Then $j_2(P) = 2$ and thus by Lemma 3.2 the Weierstrass semigroup $H(P)$ at P contains the semigroup

$$H := \langle \ell, -1+2\ell_0+\ell, 2\ell_0+\ell, 1+2\ell_0+\ell\rangle\,.$$

Therefore $\tilde{g} \le g(H) := \#(\mathbb{N}_0 \setminus H)$. This is a contradiction as we will see in the remark below. □

Remark 5.6. Let H be the semigroup defined above. We are going to show that $g(H) = \tilde{g} - \ell_0^2/4$. To begin with we notice that $L := \cup_{i=1}^{2\ell_0-1} L_i$ is a complete system of residues module ℓ, where

$$\begin{array}{lcl}
L_i & = & \{i\ell + i(2\ell_0-1)+j : j=0,\cdots,2i\} \quad \text{if } \ 1\le i\le \ell_0-1,\\
L_{\ell_0} & = & \{\ell_0\ell+\ell-\ell_0+j : j=0,\cdots,\ell_0-1\},\\
L_{\ell_0+1} & = & \{(\ell_0+1)\ell+1+j : j=0,\cdots,\ell_0-1\},\\
L_{\ell_0+i} & = & \{(\ell_0+i)\ell+(2i-3)\ell_0+i-1+j : j=0,\cdots,\ell_0-2i+1\}\cup\\
 & & \{(\ell_0+i)\ell+(2i-2)\ell_0+i+j : j=0,\cdots \ell_0-1\} \quad \text{if } \ 2\le i\le \ell_0/2,\\
L_{3q_0/2+i} & = & \{(3\ell_0/2+i)\ell+(\ell_0/2+i-1)(2\ell_0-1)+\ell_0+2i-1+j :\\
 & & j=0,\cdots,\ell_0-2i-1\} \quad \text{if } \ 1\le i\le \ell_0/2-1.
\end{array}$$

Moreover, for each $m \in L$, $m \in H$ and $m-\ell \notin H$. Hence $g(H)$ can be computed by summing up the coefficients of ℓ from the above list (see e.g. [24, Thm. p.3]); i.e.

$$\begin{array}{lcl}
g(H) & = & \sum_{i=1}^{\ell_0-1} i(2i+1)+\ell_0^2+(\ell_0+1)\ell_0+\sum_{i=2}^{\ell_0/2}(\ell_0+i)(2\ell_0-2i+2)+\\
 & & \sum_{i=1}^{\ell_0/2-1}(3\ell_0/2+i)(\ell_0-2i) = \ell_0(\ell-1)-\ell_0^2/4\,.
\end{array}$$

In the remaining part of this paper we let P_0 be a point satisfying Lemma 5.4. We set $m_i := m_i(P_0)$ and denote by $v = v_{P_0}$ the valuation at P_0.

By Lemma 5.5 the Frobenius orders of $\mathcal{D}$ are $\nu_0 = 0, \nu_1 = \epsilon_2, \cdots, \nu_{N-1} = \epsilon_N$ and thus

$$\begin{cases} m_i = 2\ell_0+\ell-\epsilon_{N-i} \quad \text{if } i=1,\cdots,N-2,\\ m_{N-1} = 2\ell_0+\ell,\\ m_N = 1+2\ell_0+\ell. \end{cases} \tag{5.3}$$

Let $x, y_2, \cdots, y_N \in \mathbb{F}_\ell(X)$ be rational functions such that $\operatorname{div}_\infty(x) = m_1 P_0$, and $\operatorname{div}_\infty(y_i) = m_i P_0$ for $i = 2, \cdots, N$. The fact that $\nu_1 > 1$ means that the following matrix

$$\begin{pmatrix} 1 & x^\ell & y_2^\ell & \cdots & y_N^\ell \\ 1 & x & y_2 & \cdots & y_N \\ 0 & 1 & D_x^1 y_2 & \cdots & D_x^1 y_N \end{pmatrix}.$$

has rank two (cf. [26, Sect. 2]). In particular,

$$y_i^\ell - y_i = D_x^1 y_i (x^\ell - x) \quad \text{for } i = 2, \cdots, N\,. \tag{5.4}$$

Lemma 5.7. (1) *For $P \in X(\mathbb{F}_\ell)$, the divisor $(2g-2)P$ is canonical; in particular, the Weierstrass semigroup at P is symmetric;*

(2) *Let $n \in H(P_0)$. If $n < 2\ell_0 + \ell$, then $n \le \ell_0 + \ell$;*

(3) *For $i = 2, \cdots, N$ there exists $g_i \in \mathbb{F}_\ell(X)$ such that $D_x^1 y_i = g_i^{\epsilon_2}$. Furthermore, $\operatorname{div}_\infty(g_i) = \frac{\ell m_i - \ell^2}{\epsilon_2} P_o$.*

Proof. (1) Let $P \in X(\mathbb{F}_\ell)$. We have $m_N P \sim m_N P_0$ by (5.1) and $2\tilde{g} - 2 = (2\ell_0 - 2)m_N$. Thus we can assume $P = P_0$. Let t be a local parameter at P_0. We show that $v(\frac{dx}{dt}) = 2\tilde{g} - 2$. The equation $i = N$ in (5.4) by $\frac{dx}{dt}$ and the product rule give

$$\frac{dx}{dt}(y_N^\ell - y_N) = \frac{dy_N}{dt}(x^\ell - x)\,;$$

from properties of valuations: $v(\frac{dx}{dt}) - \ell m_N = -m_N - (\ell^2 + 1)$; i.e.,

$$v(\frac{dx}{dt}) = (\ell - 1)m_N - (1 - 2\ell_0 + \ell)m_N = (2\ell_0 - 2)m_N = 2\tilde{g} - 2\,.$$

(2) We know that the elements ℓ, $2\ell_0 + \ell$ and $1 + 2\ell_0 + \ell$ belong to the Weierstrass semigroup $H(P_0)$ at P_0. Then the numbers

$$k\ell + j(2\ell_0 + \ell) + i(1 + 2\ell_0 + \ell) = (k + j + i)\ell + (j + i)2\ell_0 + i$$

are also non-gaps at P_0 where $k, j, i \in \mathbb{N}_0$. Let $k = 2\ell_0 - 2$, $j + i = \ell_0 - 2$. Thus the numbers

$$(2\ell_0 - 2)\ell + \ell - 4\ell_0 + j \quad j = 0, \cdots, \ell_0 - 2$$

are also non-gaps at P_0. Therefore, by the symmetry of $H(P_0)$, the elements below

$$1 + \ell_0 + \ell + j \quad j = 0, \cdots, \ell_0 - 2$$

are gaps at P_0; now the proof follows.

(3) Set $f_i := D_x^1 y_i$. We notice that $D_x^1 f_i = 0$ and $D_x^j(x^\ell - x) = 0$ for $j \ge 2$. Now we apply the product rule to (5.4),

$$0 = D_x^j y_i = D_x^j f_i (x^\ell - x) \quad \text{for } 2 \le j < \epsilon_2\,.$$

because the matrices

$$\begin{pmatrix} 1 & x & y_2 & \cdots & y_N \\ 0 & 1 & D^1_x y_2 & \cdots & D^1_x y_N \\ 0 & 0 & D^j_x y_2 & \cdots & D^j_x y_N \end{pmatrix}, \quad 2 \leq j < \epsilon_2$$

have all rank two (cf. [26, Sect. 1]). Consequently $D^j f_i = 0$ for $1 \leq j < \epsilon_2$. By Hasse and Schmidt [14, Satz 10],

$$f_i = g_i^{\epsilon_2} \quad \text{for some } g_i \in \mathbb{F}_\ell(X)\,.$$

From the computations $v(g_i) = v(f_i)/\epsilon_2$ and $-\ell m_i = v(f_i) - \ell^2$ by (5.4) we find $v(f_i) = -\ell m_i + \ell_0$. If $P \neq P_0$, $\frac{\mathrm{df_i}}{\mathrm{dt}} = \frac{\mathrm{dy_i}}{\mathrm{dt}}$ where $t = x - x(P)$ is a local parameter at P by Item (1). □

Lemma 5.8. $\epsilon_2 = \ell_0$ *and* $N = 4$.

Proof. By Lemma 5.2 $N \geq 3$ We claim that $N \geq 4$; otherwise let g_2 be the rational function in Lemma 5.7(3). We have $v(g_2) = -\ell$ since $m_2 = 2\ell_0 + \ell$ and $\epsilon_2 = 2\ell_0$. Therefore there exists $a \neq 0, b \in \mathbb{F}_\ell$ such that $x = ag_2 + b$ (notice that $v(x) = \ell$). The case case $i = 2$ in (5.4) reads

$$(y_2/a)^\ell - y_2/a = g_2^{2\ell_0}(g_2^\ell - g_2)$$

and we can assume that X is defined by $v^\ell - v = u^{2\ell_0}(u^\ell - u)$. Now the function $w := v^{\ell_0} - u^{\ell_0+1}$ satisfies $w^\ell - w = u^{\ell_0}(u^\ell - u)$ and we find that $\ell_0 + \ell$ is a non-gap at P_0 (cf. [13, Lemma 1.8]). This contradiction eliminates the case $N = 3$.

Let $N \geq 4$. The element $(\ell m_{N-2} - \ell^2)/\epsilon_2$ is a positive non-gap at P and hence at least $m_1 = \ell$. Thus $m_{N-2} - \ell \geq \epsilon_2$ $(*)$ and $2\ell_0 - \epsilon_2 \geq \epsilon_2$ (5.3) so that $\ell_0 \geq \epsilon_2$. Now by Lemma 5.7(2) $m_{N-2} \leq \ell_0 + \ell$; since $m_{N-2} = 2\ell_0 + \ell - \epsilon_2$ we find $\ell_0 \leq \epsilon_2$.

Finally we show that $N = 4$. As in $(*)$ $m_2 - \ell \geq \epsilon_2$ and from (5.3) $2\ell_0 - \epsilon_{N-2} \geq \epsilon_2 = \ell_0$. Thus $\ell_0 \geq \epsilon_{N-2} \geq \epsilon_2 = \ell_0$. □

Proof of Theorem 5.1. Let $P_0 \in X(\mathbb{F}_\ell)$ be as above. The case $i = 2$ in (5.4) and Lemma 5.7 give

$$y_2^\ell - y_2 = g_2^{\ell_0}(x^\ell - x)\ ,$$

Moreover $m_2 = \ell_0 + \ell$ and so $v(g_2) = -\ell$. Thus $x = ag_2 + b$ with $a, b \in \mathbb{F}_\ell$, $a \neq 0$ so that $(y_2^\ell/a) - (y_2/a) = g^{\ell_0}(g_2^\ell - g_2)$. We see that X is defined by the plane equation

$$v^\ell - v = u^{\ell_0}(u^\ell - u)\,.$$

Henn [16] showed that the automorphism group of the curve X above is the Suzuki group (The automorphisms of the curve are defined over $\mathbb{F}_\ell$ because the Suzuki group is simple.) Thus the curve X is isomorphimc to the Suzuki curve by the statements (I), (II) and (III) stated at the begining of this section.

Recall that the $\mathcal{D}$-invariantes and Frobenius orders of the Susuki curve are respectively $0, 1, \ell_0, 2\ell_0, \ell$ and $0, \ell_0, 2\ell_0, \ell$. Let X be the Suzuki curve.

Remark 5.9. For any $P \in X(\mathbb{F}_\ell)$ the $(\mathcal{D}, P)$-order sequence is

$$0, 1, 1+\ell_0, 1+2\ell_0, 1+2\ell_0+\ell\,.$$

To see let us compute

$$\deg(S) = (3\ell_0+\ell)(2g-2) + (\ell+4)(1+2\ell_0+\ell) = (4+2\ell_0)\#X(\mathbb{F}_\ell)\,.$$

We conclude that $v_P(S) = \sum_{i=0}^{3}(j_{i+1}(P) - \nu_i) = 4 + 2\ell_0$ and follows the assertion.

Remark 5.10. Let $P \in X$. By the previous remark, $H(P)$ contains the semigroup

$$H := \langle \ell, \ell_0+\ell, 2\ell_0+\ell, 1+2\ell_0+\ell \rangle\,.$$

We can prove that $\tilde{g} = g(H)$ as in Remark 5.6 or see [13, Appendix].

Remark 5.11. We claim that the set of $\mathcal{D}$-Weierstrass points is precisaly the set of $\mathbb{F}_\ell$-rational points. It follows from the facts that $v_P(R) = 2\ell_0 + 3$ for any $\in X(\mathbb{F}_\ell)$ and

$$\deg(R) = \sum_{i=0}^{4} \epsilon_i(2g-2) + 5(1+2\ell_0+\ell) = (2\ell_0+3)\#X(\mathbb{F}_\ell)\,.$$

In particular, the $(\mathcal{D}, P)$-orders for $P \notin X(\mathbb{F}_\ell)$ are $0, 1, \ell_0, 2\ell_0$ and ℓ.

Remark 5.12. We can use the previous remark to obtain orders for the canonical morphism on the curve. By using the fact that $(2\ell_0 - 2)\mathcal{D}$ is the canonical linear series (Lemma 5.7(1)) on X, we see that the eleements of the set

$$\{a + \ell_0 b + 2\ell_0 c + \ell d : a+b+c+d \leq 2\ell_0 - 2\}$$

are canonical orders of X. By using first order differentials this remark was first noticed in [9, Sect. 4].

Remark 5.13. The Suzuki curve X is non-classical for the canonical morphism: we have two different proofs for this fact: Garcia-Stichtenoth [9] and Lemma 3.2(6) here.

References

[1] Arbarello, E.; Cornalba, M.; Griffiths, P.A.; Harris, J.: Geometry of algebraic curves, Vol I, Springer Verlag, New York 1985.

[2] Carbonne, P.; Henocq, T.: *Décomposition de la Jacobienne sur les corps finis*, Bull. Polish Acad. Sci. Math. **42**(3), 207–215 (1994).

[3] Castelnuovo, G.: *Ricerche di geometria sulle curve algebriche*, Atti. R. Acad. Sci. Torino **24**, 196–223 (1889).

[4] Deligne, P.; Lusztig, G.: *Representations of reductive groups over finite fields*, Ann. of Math. **103**, 103–161 (1976).

[5] Esteves, E.: *A geometric proof of an inequality of order sequences*, Comm. Algebra **21**(1), 231–238 (1993).

[6] Fuhrmann, R.: Algebraische Funktionenkörper über endlichen Körpern mit maximaler Anzahl rationaler Stellen, Dissertation, Universität GH Essen 1995.

[7] Fuhrmann, R.; Torres, F.: *The genus of curves over finite fields with many rational points*, Manuscripta Math. **89**, 103–106 (1996).

[8] Fuhrmann, R.; Garcia, A.; Torres, F.: *On maximal curves*, J. Number Theory. **67**(1), 29–51 (1997).

[9] Garcia, A.; Stichtenoth, H.: *Elementary abelian p-extensions of algebraic functions fields*, Manuscripta Math. **72**, 67–79 (1991).

[10] Goppa, V.D.: Geometry and Codes, Mathematics and its applications, Vol 24, Kluwer Academic Publiisher, Dordreet, Boston, London 1988.

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

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

[13] Hansen, J.P.; Stichtenoth, H.: *Group codes on certain algebraic curves with many rational points*, AAECC **1**, 67–77 (1990).

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

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

[16] Henn H.W.; *Funktionenkörper mit großer Automorphismengruppe*, J. reine angew. Math. **302**, 96–115 (1978).

[17] Ihara, Y.: *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokio **28**, 721–724 (1981).

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

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

[20] Munuera, C.; Torres, F.: *Sobre curvas algebraicas y códigos correctores*, La Gaceta de la RSME **9**(1), 203–222 (2006).

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

[22] Rathmann, J.: *The uniform position principle for curves in characteristic p*, Math. Ann. **276**, 565–579 (1987).

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

[24] Selmer, E.S.: *On the linear diophantine problem of Frobenius*, J. reine angew. Math. **293/294**, 1–17 (1977).

[25] Stichtenoth, H,: Algebraic Function Fields and Codes, Springer, New York-Berlin, 1993.

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

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

[28] Xing, C.; Stichtenoth, H.: *The genus of maximal functions fields*, Manuscripta Math. **86**, 217–224 (1995).

Universität GH Essen, FB 6 Mathematik und Informatik, D-45117 Essen, Germany

IMECC-UNICAMP, Cx. 6055, 13083-970, Campinas SP-Brazil

E-mail address: RAINER.FUHRMANN@ZENTRALE.DEUTSCHE-BANK.dbp.de

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