# ALGEBRAIC CURVES WITH MANY POINTS OVER FINITE FIELDS

FERNANDO TORRES

As long as Algebra and Geometry proceeded along separate paths, their advance was slow and their applications limited.

But when these sciences joined company they drew from each other fresh vitality and thenceforward marched on at a rapid pace towards perfection.

J.L. Lagrange
(Cited in Goppa's book [38])

## Contents

## Introduction

The purpose of this paper is to survey some results concerning the number of rational points of curves over finite fields. A remarkable motivation which is intimately related to mathematicians like Fermat, Euler, Lagrange, Legengre, Gauss, Jacobi, ... is the following question (cf. [17], [85], [81]). Let $p$ be a prime and $m \geq 2$ an integer such that $p$ does

Many thanks to P.C. Oliveira for point out some misprints on the July 2014 version of this paper.

Advances in Algebraic Geometry Codes
Series on Coding Theory and Cryptology
World Scientific Home, 2008, 221–256.

**Revised version: August 10, 2014.**

not divide $m$. Let $\mathbb{F}_p$ denote the finite field with $p$ elements. How many solutions in the projective plane $\mathbb{P}^2(\mathbb{F}_p)$ exist for the curve

$$X^m + Y^m + Z^m = 0?$$

In the early years of the 19th century, Gauss considered finite sums of powers of $p$th root of unity (now known as *Gauss sums*) to give a proof of one of the great theorems in mathematics: the Quadratic Reciprocity Law (cf. $m = 2$); the proof suggests an approach to Higher Reciprocity Law (cf. $m > 2$). Let $N$ be the number of $\mathbb{F}_p$-solutions of the curve above. It turns out that $N$ is a *Jacobi sum*; i.e., a finite sum of sums closely related to Gauss sums. Gauss calculated $N$ for $m = 2$ and $m = 3$; see e.g. [81, Ch. 6]. If $m > 3$ however, things get progressively more complicated and in general there is only an estimate, namely

$$|N - (p+1)| \le \lfloor 2g\sqrt{p} \rfloor ,$$

where $g = (m-1)(m-2)/2$ is the genus of the curve, see Weil [102]. This result is indeed a particular case of a deep result in Algebraic Curve Theory, namely the so-called *Hasse-Weil bound* (HW-bound) (or the *Riemann-Hypothesis*) for curves over finite fields. Throughout, let $\mathcal{X}$ be a curve (nonsingular, projective, geometrically irreducible) of genus $g$ over the finite field $\mathbb{F}_q$ with $q$ elements. The HW-bound assert that

$$|\#\mathcal{X}(\mathbb{F}_q) - (q+1)| \le \lfloor 2g\sqrt{q} \rfloor ;$$

Hasse (around 1932) showed the case $g = 1$ via complex multiplication on elliptic curves and Weil (around 1940) showed the general case via the theory of the correspondences [101]. The key starting point was a conjecture of Artin (Ph.D. thesis, 1924) on the complex module of the zeroes of a *zeta-function* of a curve, see Theorem 1.2. Such a function was introduced by Artin himself in analogy with Dedekind's zeta-function of numerical fields and the aforementioned conjecture was inspired by the well-known classical Riemann hypothesis.

Bombieri [8] gave an elementary proof of the HW-bound by following ideas of Stepanov, Postnikov, Stark and Manin; his proof uses the Riemann-Roch theorem only. Now, once the HW-bound was available, some sharp upper bounds were obtained in the context of questions associated to curves; e.g. exponential sums [89], [70] and the number of elements of plane arcs [49], [50] and [48] (see also the references therein).

Let $N_q(g)$ be the maximal number of rational points that a curve of genus $g$ over $\mathbb{F}_q$ can have. In the last years, due mainly to applications in Coding Theory and Cryptography, there has been considerable interest in computing the actual value of $N_q(g)$. It is a classical result that $N_q(0) = q+1$. Deuring [16] and Serre [88] computed $N_q(1)$ and $N_q(2)$; we quote these computations in Example 1.5. For $g = 3$ we have the Voloch's bound which says that $N_q(3) \le 2q+6$ whenever $q \ne 8, 9$, see Example 1.6. Serre computed $N_q(3)$ for $q < 25$ [88] and Top [94] extended these computations to $q < 100$; see Remarks 1.7, 1.8. The tables in [34] describe what is known about $N_q(g)$ for $g \le 50$ and $q \in \{2, 3, 4, 8, 9, 16, 27\}$.

By using narrow ray class extensions, Niederreiter and Xing found bounds on $N_q(g)$ for $q = 2, 3, 4, 5, 8, 16$ and $1 \leq g \leq 50$ [75]; see also [76] and the references therein.

In general, a closed formula for $N_q(g)$ seems still to be a long way off. An upper bound on $N_q(g)$ is clearly the HW-bound; Serre [87] observed that this bound may be sharpened in several cases via the HWS-bound in (1.4) or the "explicit formulas" method in Proposition 1.9. Osterlé used tools from linear programing to optimize this method [88] by selecting the "best" trigonometric polynomial in (1.6); this is called the Osterlé bound. Currently, powerful tools related to Abelian Varieties are used to investigate $N_q(g)$; cf. Howe, Lauter, Serre [59], [60], [61], [62], [63], [64], [65]; we will not survey these results here.

In order to find lower bounds on $N_q(g)$ we look for curves $\mathcal{X}$ "with many points" in the sense that $\#\mathcal{X}(\mathbb{F}_q)$ has to be as close as possible to the best upper bound known on $N_q(g)$. In most cases, the best known bound comes from Osterlé's (cf. [62]). If $\#\mathcal{X}(\mathbb{F}_q) = N_q(g)$, the curve is called *Optimal*. In Section 5 we investigate a particular family of optimal curves, the so-called *Maximal Curves*; i.e., those whose number of rational points attains the upper HW-bound. A distinguished example here is the *Hermitian curve* which is intrinsically determined by its genus and number of rational points [82]; see Theorem 5.3 here. There are also two important families of optimal curves, namely the *Suzuki curves* and the *Ree curves*; each curve in each family is intrinsically determined by the data: (1) the genus, (2) the number of rational points and (3) the automorphism group (see Hansen [39], Hansen-Pedesrsen [40], Hansen-Stichtenoth, [41], Heen [46]). An important result is Theorem 4.1, where we show that the Suzuki curve is characterized by properties (1) and (2) only; it seems that this property is an open problem for the Ree curve. It is worthwhile to point out that the Hermitian curve, the Suzuki curve and the Ree curve are respectively the Deligne-Lusztig varieties of positive genus associated to connected reduction algebraic group of type ${}_2A^2$, ${}_2B^2$ and ${}_2R^2$ [15].

Apart from Bombieri's work in simplifying the proof of the HW-bound and the bounds on exponential sums and plane arcs mentioned above, qualitative aspects of the study of the HW-bound in 1940 was similar to that in 1977. The interest on this matter was renewed after Goppa (around 1977) constructed error-correcting codes from linear series on curves, the so-called *Geometric Goppa Codes* (GG-codes) (as they currently are known); see [37], [38]. These codes generalize the well-known Reed-Solomon codes, BCH-codes and the "classical" Goppa codes (see van Lint [67], van Lint-van der Geer [68]). Goppa's idea showed for the first time how two totally different areas of mathematics: Algebraic Curve Theory ("pure" subject) and Coding Theory ("applied" subject) can be related to each other.

Next we briefly describe (the dual construction) of a GG-code. Let $g^r_e$ be a $r$-dimencional linear series on $\mathcal{X}$ of degree $e$ defined over $\mathbb{F}_q$ and whose sections are contained in a Riemann-Roch space $\mathcal{L}(G)$. For simplicity we shall assume that $g^r_e = |G|$ is complete. Let $P_1, \ldots, P_n$ be pairwise distinct $\mathbb{F}_q$-rational points of the curve such that $P_i \notin \mathrm{Supp}(G)$ for any $i$. Consider the $\mathbb{F}_q$-linear map

$$\mathrm{e_v} : f \in \mathcal{L}(G) \mapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n\,.$$

Then the following $q$-ary linear code, namely

$$C_{\mathcal{X}}(G, D) := \mathrm{e_v}(\mathcal{L}(G))$$

is the Goppa code defined by the triple $(\mathcal{X}, G, D)$, where $D := P_1 + \ldots + P_n$. Let $k$ and $d$ be respectively the dimension and minimum distance of the code. Then

(1) $k = \ell(G) - \ell(G - D)$, where $\ell(.)$ denotes the $\mathbb{F}_q$-dimension of the corresponding Riemann-Roch space;
(2) $d \geq n - \deg(G)$.

We observe that $k$ and $d$ can be handled by means of the Riemann-Roch theorem. In addition, (2) is only meaningful, if (fixed $\deg(G)$), $\mathcal{X}$ is a curve with many points. With respect to the dimension $k$, if $n > \deg(G)$, then

$$k = \ell(G) = \deg(G) + 1 - g + \ell(K - G) \geq \deg(G) + 1 - g\,,$$

where $K$ is a canonical divisor on $\mathcal{X}$; in particular,

$$(*) \qquad n + 1 \geq k + d \geq n + 1 - g\,.$$

Thus we are ready to appreciate an amazing asymptotic property of families of GG-codes and to understand the first remarkable application of these codes in the context of asymptotic problems in Coding Theory. As a matter of fact, Tsfasman, Vlăduţ and Zink [97] (see also [96], [70]) showed that, for $q \geq 49$ a square, the Gilbert-Varshamov bound can be improved via a sequence of GG-codes; roughly speaking, this is done as follows:

(A) They show that there is a family of GG-codes $(\mathcal{X}_i)$ such that the sequence of their relative parameters $(r_i, \delta_i)$ has a limit point $(R, \delta)$. Here the sequence of genus $g_i \to \infty$ and $\lim\mathrm{supp}_i \frac{n_i}{g_i} = \sqrt{q} - 1$;
(B) Then inequality $(*)$ implies $R + \delta = 1 - 1/(\sqrt{q} - 1)$; this improves the Gilbert-Varshamov.

For Items (A) and (B) above, one studies values $N_q(g)$ of $q$-ary GG-codes based on curves of genus $g$ over $\mathbb{F}_q$ ($q$ fixed and $g$ large enough) and ask for the limit

$$A(q) := \lim\sup_g \frac{N_q(g)}{g}$$

to be as large as possible. We consider this question in Section 2, where our main references were the papers by Kresch et al. [56] and Elkies et al. [19].

Coming back to the study of the HW-bound for a single curve, Stöhr and Voloch (around 1982) development a geometric method to bound $\#\mathcal{X}(\mathbb{F}_q)$ based on $\mathbb{F}_q$-linear series on the curve [91]; such a bound will be denoted by SV-bound. We report some features on this theory in the Appendix. The SV-bound gives a new proof of the HW-bound and improvements in several cases. For example, via the SV-bound, Voloch obtained the best upper bound known so far on the order of complete arcs in projective planes over prime fields [99], [100].

There is a natural link between the arithmetic and geometry of a curve which comes from a linear series naturally defined from the zeta-function of the curve (see Section 3). This linear series is simple and its existence implies the uniqueness of the Suzuki curve. In the case of maximal curves, the linear series is very ample (Theorem 5.1) and thus we can study maximal curves embedded in projective spaces and apply classical results from Algebraic Curve Theory or Finite Geometry such as:

- The Castelnuovo genus bound for curves in projective spaces [10], [6], [78], [42];
- Halphen's bound on the genus of the curve taking into consideration the degree of a surface where the curve is contained [11];
- Properties of quadratic surfaces in $\mathbb{P}^3(\bar{\mathbb{F}}_q)$ [48].

We recall that Castelnuovo and Halphen bounds are valid in positive characteristic by Hartshorne [42] (space curves) and Rathmann [78].

From the interplay of these properties with the Stöhr-Voloch theory (Appendix) we deduce quantitave and qualitative properties of maximal curves (see Hirschfeld et al. [51]); we will mention a few of them in Section 5.

Tafasolian [92] (Ph. D. Thesis, 2008) investigated properties of maximal curves via Cartier Operators; among other things, he characterized certain HWS-maximal curves, HW-maximal Fermat curves and HW-maximal Artin-Schreier curves. His results improve on previous work in [2], [5], [3], [1], [22].

Standard references are the books by Fulton [25], Arbarello et al. [6], Hartshorne [42], Namba [73], Stichtenoth [90], Moreno, [70], Stepanov [89], Goldschmidt [36], Goppa [38], Tsfasman and Vladut [96], Hirschfeld et all. [51]. For the convenience of the reader we include an Appendix on the Theory of Stöhr-Voloch [91].

Throughout this paper, by a curve over $\mathbb{F}_q$ (the finite field with $q$ elements) we mean a nonsingular, projective, geometrically irreducible algebraic curve defined over $\mathbb{F}_q$.

## 1. The function $N_q(g)$

In this section we discuss curves with many points. Our references on zeta-functions are e.g. the books [90], [89] or [70]. Let $\mathcal{X}$ be a curve of genus $g$ over $\mathbb{F}_q$. Let $N_i = \#\mathcal{X}(\mathbb{F}_{q^i})$ be the number of $\mathbb{F}_{q^i}$-rational points of $\mathcal{X}$. Thanks to Riemann, Dedekind, Artin, Hasse, Weil, ... all the information about the $N_i$ is contained in the zeta-function

$$Z(t) = Z(\mathcal{X}, q; t) := \exp(\sum_{i=1}^{\infty} N_i t^i / i) \tag{1.1}$$

of $\mathcal{X}$ over $\mathbb{F}_q$. By the Riemann-Roch theorem, there is a polynomial $L(t) = L(\mathcal{X}, q; t)$ of degree $2g$ satisfying:

**Proposition 1.1.** (1) $L(t) = Z(t)(1-t)(1-qt)$;

(2) $L(t) = \pi_{j=1}^{2g}(1-\alpha_j t)$ *where the* $\alpha_j$ *are algebraic integers which can be arranged in such a way that* $\alpha_j\bar{\alpha}_j = q$.

Thus from (1.1) we obtain

$$N_i = q^i + 1 - \sum_{j=1}^{2g}\alpha_j^i = q^i + 1 - \sum_{j=1}^{g}(\alpha_j^i + \bar{\alpha}_j^i)\,. \tag{1.2}$$

The main result to bound $\#\mathcal{X}(\mathbb{F}_q)$ is the following.

**Theorem 1.2.** (Riemann hypothesis) *The complex value of each* $\alpha_j$ *is* $\sqrt{q}$.

Therefore (1.2) implies the Hasse-Weil bound (HW-bound) mentioned in the introduction (for $i=1$), namely

$$|\#\mathcal{X}(\mathbb{F}_{q^i}) - (q^i + 1)| \le \lfloor 2g\sqrt{q^i}\rfloor\,. \tag{1.3}$$

**Example 1.3.** (The Hermitian curve) If $q = \ell^2$, the HW-bound is sharp as the following curve, known as *the Hermitian curve*

$$\mathcal{H}: \quad X^{\ell+1} + Y^{\ell+1} + Z^{\ell+1} = 0$$

shows. The genus of $\mathcal{H}$ is $g = \ell(\ell-1)/2$ and $\#\mathcal{H}(\mathbb{F}_{\ell^2}) = \ell^3+1$. Rück and Stichtenoth [82] noticed that $\mathcal{H}$ is the unique curve having these properties; we will improve this result in Theorem 5.3.

**Example 1.4.** (The Klein quartic over $\mathbb{F}_8$) In general the HW-bound is not sharp: Consider the curve

$$\mathcal{K}: \quad X^3Y + Y^3Z + Z^3X = 0\,,$$

known as *the Klein quartic.* If $q = 8$, the curve is nonsingular of genus $g = 3$. The HW-bound is 25; however, $\#\mathcal{K}(\mathbb{F}_8) = 24$.

In Remark 5.4 we will see that the HW-bound is not necessarily sharp even if $q$ is a square. Set

$$N_q(g) := \max\{\#\mathcal{Y}(\mathbb{F}_q) : \mathcal{Y} \text{ a curve of genus } g \text{ defined over } \mathbb{F}_q\}\,.$$

**Example 1.5.** (Deuring [16], Serre [88]) Write $q = p^\alpha$ and $m = \lfloor 2\sqrt{q}\rfloor$. Thus

- $N_q(1) = q + 1 + m$ except when $\alpha \ge 3$ is odd, and $p$ divides $m$; in this case, $N_q(1) = q + m$.
- $N_q(2) = q + 1 + 2m$ except in the following cases: (1) $N_4(2) = 10$, $N_9(2) = 20$; (2) $\alpha$ is odd, $p$ divides $m$; (3) $\alpha$ is odd and $q$ of the form $x^2+1$, $x^2+x+1$ or $x^2+x+2$ ($x \in \mathbb{Z}$).

In cases (2) and (3) above we have $N_q(2) = q + 2m$ if $2\sqrt{q} - m > (\sqrt{5} - 1)/2$ or $N_q(2) = q + 2m - 1$ otherwise.

As a nice application of the Appendix we prove the Voloch's bound for curves of genus 3; cf. Serre [88], Top [94, Prop.1].

**Example 1.6.** For $q \neq 8, 9$, $N_q(3) \leq 2q + 6$. Indeed, let $\mathcal{X}$ be a curve of genus 3 over $\mathbb{F}_q$ with $\#\mathcal{X}(\mathbb{F}_q) > 2q + 6$. Then $\mathcal{X}$ is nonhyperelliptic. We apply the Appendix to the canonical linear series $\mathcal{D}$. Let $0 = \nu_0 < \nu_1$ be the $\mathbb{F}_q$-Frobenius orders and $S$ the $\mathbb{F}_q$-divisor of $\mathcal{D}$ respectively. Thus

$$2q + 6 < \deg(S)/2 = (4\nu_1 + (q + 2)4)/2$$

so that $\nu_1 > 1$. Thus the order sequence of $\mathcal{D}$ is $0, 1, \nu_1$ and $j_2(P) \geq \nu_1 + 1$ for any $P \in \mathcal{X}(\mathbb{F}_q)$. The Hefez-Voloch theorem (Appendix) gives $\#\mathcal{X}(\mathbb{F}_q) = 4(q - 2)$ and thus

$$\deg(R) = (1 + \nu_1)4 + 12 \geq \#\mathcal{X}(\mathbb{F}_q) = 4(q - 2)\,,$$

and hence $q < \nu_1 + 6$; i.e. $q \in \{2, 3, 4, 5, 7, 8, 9\}$ as $\nu_1 \leq 4$. On the other hand, $\#\mathcal{X}(\mathbb{F}_q) = 4q - 8 > 2q + 6$ so that $q = 8, 9$.

*Remark* 1.7. We have that $28 \leq N_9(3)$ and $24 \leq N_8(3)$ due to the Hermitian curve and the Klein quartic above.

**Case:** $q = 9$**.** Following the example above we find that $\nu_1 = 3$ whenever $\#\mathcal{X}(\mathbb{F}_9) \leq \deg(S)/2 = 28$ In particular, $N_9(3) = 28$. We observe that there is just one curve of genus $g = 3$ over $\mathbb{F}_9$ with 28 rational points, namely the Hermitian $X^4 + Y^4 + Z^4 = 0$, cf. [82].

**Case.** $q = 8$**.** As in Case 1 we find that $\nu_1 = 2$ and $N_8(3) = 24$. From [94, Prop1.1(a)] the Klein quartic over $\mathbb{F}_8$ is the unique curve of genus 3 with 24 rational points.

*Remark* 1.8. From the table in [94] we observe that Voloch's bound is sharp for $q = 4, 5, 7, 11, 13, 16, 17, 19, 25$. Let $q = p^{2a}$ with $p$ an odd prime and $a \geq 1$ an integer. Ibukiyama [52] showed that there exist a curve of genus 3 over $\mathbb{F}_q$ whose number of rational points attains the HW-bound. Thus $N_q(3) = p^{2a} + 1 + 6p^a$.

Serre [87] noticed that the HW-bound (1.3) may be improved to the following HWS-bound:

$$|\#\mathcal{X}(\mathbb{F}_{q^i}) - (q^i + 1)| \leq g\lfloor 2\sqrt{q} \rfloor\,. \tag{1.4}$$

This bound is sharp as Example 1.4 above shows. Now we remark the Serre "explicit formulas" method; cf. [88], [39].

From Theorem 1.2 we can write $\alpha_j = \sqrt{q}\exp(\sqrt{-1}\theta_j)$. From (1.2)

$$N_i = q^i + 1 - 2\sqrt{q}^i \sum_{j=1}^{g} \cos i\theta_j\,. \tag{1.5}$$

Let $f(\theta)$ be a trigonometric polynomial of the form

$$f(\theta) = 1 + 2\sum_{n\geq 1} c_n \cos n\theta\,.$$

Set

$$\psi_d(t) := \sum_{n\geq 1} c_{nd}t^{nd} \quad d \geq 1\,.$$

After some computation, (1.5) implies

$$\sum_{j=1}^{g} f(\theta_j) + + \sum_{d\geq 1} da_d\psi_d(q^{-1/2}) = g + \psi_1(q^{-1/2}) + \psi_1(q^{1/2})\,, \tag{1.6}$$

where $a_d$ is the number of points of degree $d$. Notice that $N_i = \sum_{d|i} da_d$. Whence we obtain the following.

**Proposition 1.9.** *Suppose that the $c_i$'s are non-negative real number not all zero. Suppose that $f(\theta) \geq 0$ for all $\theta$. Then*

$$N_1 = \#\mathcal{X}(\mathbb{F}_q) \leq \frac{g}{\psi_1(q^{-1/2})} + 1 + \frac{\psi_1(q^{1/2})}{\psi_1(q^{-1/2})}\,;$$

*equality holds if and only if*

$$\sum_{j=1}^{g} f(\theta_j) = 0\,, \quad \textit{and} \quad \sum_{d\geq 2} da_d\psi_d(q^{-1/2}) = 0\,.$$

Set

$$h(t) = h(\mathcal{X}, q; t) := t^{2g}L(\mathcal{X}, q; t^{-1})\,. \tag{1.7}$$

The following result is the key starting point for the characterization of the Suzuki curve given in Section 4.

**Proposition 1.10.** (cf. [88]) *Let $q = 2q_0^2$ with $q_0$ a power of two. Let $\mathcal{X}$ be a curve of genus $g = q_0(q-1)$ with $N_1 = q^2+1$ rational points. Then*

$$h(t) = (t^2 + 2q_0t + q)^g\,.$$

*Proof.* Let $h(t) = \prod_{j=1}^{g}(t-\alpha_j)(t-\bar{\alpha}_j)$ with $\alpha_j = \exp(\sqrt{-1}\theta_j)$. We let

$$f(\theta) := 1 + \sqrt{2}\cos\theta + \frac{1}{2}\cos 2\theta = \frac{1}{2}(1+\sqrt{2}\cos\theta)^2\,.$$

Thus $\psi_1(t) = \frac{\sqrt{2}}{2}t + \sqrt{1}4t^2$ and $\psi_2(t) = \frac{1}{4}t^2$. After some computations from Proposition 1.9 we have $\sum_{j=1}^{g} f(\theta_j) = 0$. It follows that $\cos\theta_j = -\frac{1}{\sqrt{2}}$ and hence $\alpha_j + \bar{\alpha}_j = -2q_0$; the result follows. □

## 2. Asymptotic Problems

In this section we survey a few results related to Tsfasman-Vlăduţ-Zink improvement on the Gilbert-Varshamov bound. The key matter is to find a family of curves $(\mathcal{X}_g)$ (indexed by its genus and defined over a fixed field $\mathbb{F}_q$) such that

$$A(q) := \limsup_g \frac{N_q(g)}{g}$$

be as large as possible. This number was introduced by Ihara [53] (and the inverse value was considered by Manin, loc. cit.). Ihara showed

$$N_q(g) \leq q + 1 + \frac{1}{2}\sqrt{(8q+1)g^2 + 4(q^2-q)g} - g$$

and thus if $g > \sqrt{q}(\sqrt{q}-1)/2$, $N_q(g)$ is less than the HW-bound. From the upper bound on $N_q(g)$ above it follows that

$$A(q) \leq \frac{1}{2}(\sqrt{8q+1} - 1)\,.$$

Vlăduţ and Drinfeld [98] improve this bound and show that indeed

$$A(q) \leq \sqrt{q} - 1\,.$$

To find lower bounds on $A(q)$ one needs to produce families of curves with many points. Serre used class field theory [87], [88] to show that $A(q) \geq \gamma_q$ with $\gamma_q$ a positive constant depending of $q$ (see also [74]). We have a stronger result, namely $N_q(g) > \gamma_q g$ for any $g$ (see Elkies et al. [19]). Ihara used supersingular points on a family of modular curves $(\mathcal{X}_g)$ to show that, when $q$ is an square, one can take $\gamma_q = \sqrt{q} - 1$ and hence

$$A(q) = \sqrt{q} - 1\,. \tag{2.1}$$

The GG-codes constructed on the respective curves $(\mathcal{X}_g)$ above have the best asymptotic parameters that can be constructed so far; for practical applications one needs an explicit description of the aforementioned codes; this task seems to be very hard in the case of modular curves. Garcia and Stichtenoth proved (2.1) via curves defined by "explicit equations" (see [26], [27]). It is an intrigued fact that Garcia and Stichtenoth curves are also modular curves (see Elkies [18]).

For $q = p^{2m+1}$, it seems that the true value of $A(q)$ is unknown. Zink showed $A(p^3) \geq 2(p^2-1)/(p+2)$ (curves with no explicit equations). van der Geer and van der Vlugt [33] for $q = 8$ and Bezerra et al. [7] for any $q$ as above generalized Zink's bound (curves with explicit equations).

Further asymptotic results on $N_q(g)$ which implies consequence both for $A(q)$ and $A^{-}(q) := \liminf_g N_q(g)/g$ can be found in the quite nice references [56] and [19] (see also the references therein).

## 3. Zeta-functions and Linear Series

Let $\mathcal{X}$ be a curve of genus $g$ over $\mathbb{F}_q$ such that $\#\mathcal{X}(\mathbb{F}_q) > 0$. Let $L(t) = L(\mathcal{X}, q; t)$ be the enumerator of the zeta-function of $\mathcal{X}$ over $\mathbb{F}_q$. We consider the function $h(t)$ defined in (1.7), namely

$$h(t) = t^{2g}L(t^{-1}) = \prod_{j=1}^{g}(t-\alpha_j)(t-\bar{\alpha}_j)\,,$$

where the $\alpha_j$ are defined in Proposition 1.1. Then $h(t)$ is monic, of degree $2g$ whose independent term is non-zero; moreover, $h(t)$ is the characteristic polynomial of the Frobenius morphism $\mathbf{\Phi}_{\mathcal{J}}$ on the Jacobian $\mathcal{J}$ of the curve $\mathcal{X}$ (here we consider $\mathbf{\Phi}_{\mathcal{J}}$ as an endomorphism on a Tate module). Let

$$h(t) = \prod_j h_j^{r_j}(t)$$

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 [93, Thm. 2], [58, VI§3], it follows that

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

Let $\mathbf{\Phi}$ denote the Frobenius morphism on $\mathcal{X}$. Let $\pi : \mathcal{X} \to \mathcal{J}$ be the natural morphism $P \mapsto [P - P_0]$, where $P_0 \in \mathcal{X}(\mathbb{F}_q)$. We have

$$\pi \circ \mathbf{\Phi} = \mathbf{\Phi}_{\mathcal{J}} \circ \pi$$

and thus (3.1) implies the following linear equivalence of divisors on $\mathcal{X}$

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

This suggests the study of the linear series

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

Let us write

$$\prod_j h_j(t) = t^U + \alpha_1 t^{U-1} + \alpha_2 t^{U-2} + \ldots + \alpha_{U-1}t + \alpha_U\,.$$

We assume:

(A) $\alpha_1 \geq 1$, (we already known that $\alpha_U \mid q$);
(B) $\alpha_{j+1} \geq \alpha_j$ for $j = 1, \ldots, U-1$.

*Remark* 3.1. There are curves which do not satisfy conditions (A) and (B) above; cf. [9].

Next we compute some invariants of the linear series $\mathcal{D}$ above according to the results in the Appendix; we use the notation of that Appendix. Let $r$ be the dimension of $\mathcal{D}$. For $P \in \mathcal{X}(\mathbb{F}_q)$ we have the following sequence of non-gaps at $P$:

$$0 = m_0(P) < m_1(P) < \ldots < m_{r-1}(P) < m_r(P) = m\,.$$

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

$$0 = m - m_r(P) < m - m_{r-1}(P) < \ldots < m - m_1(P) < m - m_0(P)\,;$$

(2) *If $P \notin \mathcal{X}(\mathbb{F}_q)$, then $j_1(P) = 1$;*

(3) *The numbers $1, \alpha_1, \ldots, \alpha_U$ are orders of $\mathcal{D}$;*

(4) *If $\mathbf{\Phi}^{U+1}(P) \neq P$, then $\alpha_U$ is a non-gap at P. In particular, $\alpha_U$ is a generic non-gap of $X$;*

(5) *If $\mathbf{\Phi}^{U}(P) \neq P$ and $\mathbf{\Phi}^{U+1}(P) = P$, then $\alpha_U - 1$ is a non-gap at P.*

*Proof.* The proof of (1), (2) or (3) is similar to [22, Thm. 1.4, Prop. 1.5]. To show the other statements, let us apply $\mathbf{\Phi}_*$ in (3.2); thus

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

Then (4) and (5) follow from hypothesis (A) and (B) above. □

We finish this section with some properties involving rational points.

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

(1) *If $\#\mathcal{X}(\mathbb{F}_q) \geq 2g + 3$, then there exists $P \in \mathcal{X}(\mathbb{F}_q)$ such that $(m-1)$ and $m$ are non-gaps at $P$;*

(2) *The linear series $\mathcal{D}$ is simple; i.e., the morphism $\pi : \mathcal{X} \to \pi(\mathcal{X}) \subseteq \mathbb{P}^r(\bar{\mathbb{F}}_q)$ defined by $\mathcal{D}$ is birational.*

*Proof.* (1) Following [103], let $P \neq P_0$ be a rational point. We have $mP \sim mP_0$ by (3.2). Let $x : \mathcal{X} \to \mathbb{P}^1(\bar{\mathbb{F}}_q)$ 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 $2g-2 \geq m(-2) + 2(m-1) + (\#\mathcal{X}(\mathbb{F}_q) - n - 2)$ so that $n \geq \#\mathcal{X}(\mathbb{F}_q) - (2g+2) \geq 1$. Thus there exists $Q \in \mathcal{X}(\mathbb{F}_q)$, $Q \neq P, P_0$ such that $\mathrm{div}(x-a) = Q + D - mP_0$ with $D \in \mathrm{Div}(\mathcal{X})$, $P_0, Q \notin \mathrm{Supp}(D)$. 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 $Q \in \mathcal{X}(\mathbb{F}_q)$ be the point in (1) and $x, y \in \mathbb{F}_q(X)$ be such that $\mathrm{div}_\infty(x) = (m-1)Q$ and $\mathrm{div}_\infty(y) = mQ$. Then $\mathbb{F}_q(\mathcal{X}) = \mathbb{F}_q(x, y)$ and we are done. □

**Proposition 3.4.** (1) $\epsilon_r = \nu_{r-1}$;

(2) *Let $P \in \mathcal{X}(\mathbb{F}_q)$ and suppose that $\#\mathcal{X}(\mathbb{F}_q) \geq q(m - \alpha_U) + 2$. Then $j_{r-1}(P) < \alpha_U$; in particular, $\epsilon_r = \alpha_U$ and $P$ is a $\mathcal{D}$-Weierstrass point;*

(3) *If $\#\mathcal{X}(\mathbb{F}_q) \geq q\alpha_U + 1$, then $\#\mathcal{X}(\mathbb{F}_q) = q\alpha_U + 1$ and $m_1(P) = \alpha_U$ for any $P \in \mathcal{X}(\mathbb{F}_q)$.*

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

(2) We have $\#\mathcal{X}(\mathbb{F}_q) \leq qm_1(P) + 1$ by Lewittes [66, Thm. 1(b)]. Then the result follows from Lemma 3.2.

(3) Let $P \in \mathcal{X}(\mathbb{F}_q)$. We have $m_1(P) \leq m_1(Q)$, where $Q$ is a generic point of $\mathcal{X}$ (apply the Appendix to the canonical linear series on $\mathcal{X}$). Therefore, $m_1(Q) \leq \alpha_U$ by Lemma 3.2 and hence $q\alpha_U + 1 \leq \mathcal{X}(\mathbb{F}_q) \leq qm_1(P) + 1 \leq q\alpha_U + 1$. □

## 4. A characterization of the Suzuki curve

This section is based on [24]; it is a nice application of the interplay of Section 3 and the Appendix. Throughout, we let $q_0 = 2^s > 2$ be a power of two and set $q := 2q_0^2$. As we mentioned in the Introduction, the Suzuki curve $\mathcal{S}$ is the unique curve over $\mathbb{F}_q$ defined by the following data:

(I) genus: $g = q_0(q-1)$;
(II) number of $\mathbb{F}_q$-rational points: $N_1 = q^2 + 1$;
(III) $\mathbb{F}_q$-automorphism group equals the Suzuki group.

Our aim is to show the following.

**Theorem 4.1.** *Let $\mathcal{X}$ be a curve of genus $g = q_0(q-1)$ over $\mathbb{F}_q$ such that $N_1 = \#\mathcal{X}(\mathbb{F}_q) = q^2 + 1$. Then $\mathcal{X}$ is isomorphic to the Suzuki curve $\mathcal{S}$.*

We first show some lemmas. The reference "Lemma A" below is placed in the Appendix.

Let $\mathcal{X}$ be as in the theorem. Let $h(t) = t^{2g}L(t^{-1})$ be the polynomial defined in (1.7). The starting point of the proof is Proposition 1.10; thus

$$h(t) = (t^2 + 2q_0t + q)^g \,.$$

Let $\mathbf{\Phi} : \mathcal{X} \to \mathcal{X}$ be the Frobenius morphism on $\mathcal{X}$. From Section 3 we conclude that $\mathcal{X}$ is equipped with the linear series

$$\mathcal{D} := |(1 + 2q_0 + q)P_0| \,, \quad P_0 \text{ a rational point}$$

such that for any $P \in \mathcal{X}$

$$\mathbf{\Phi}^2(P) + 2q_0\mathbf{\Phi}(P) + qP \sim (1 + 2q_0 + q)P_0 \,. \tag{4.1}$$

Let $r$ denote the dimension of $\mathcal{D}$. We already know that $m = m_r(P) = 1 + 2q_0 + q$ for any $P \in \mathcal{X}(\mathbb{F}_q)$. Lemma 3.2 and Proposition 3.4 imply the following properties:

(1) $m_1(P) = q$ and $j_{r-1}(P) = 1 + 2q_0$ for any $P \in \mathcal{X}(\mathbb{F}_q)$;
(2) $\epsilon_1 = 1$ and $\epsilon_r = \nu_{r-1} = q$.

**Lemma 4.2.** $r \geq 3$ *and* $\epsilon_{r-1} = 2q_0$.

*Proof.* By Lemma 3.2 the numbers 1, $2q_0$ and $q$ are orders of $\mathcal{D}$ and thus $r \geq 3$. Since $\epsilon_{r-1} \leq j_{r-1}(P) = 1 + 2q_0$ (Lemma A) and $\epsilon_r = q$ we have

$$2q_0 \leq \epsilon_{r-1} \leq 1 + 2q_0\,.$$

Suppose that $\epsilon_{r-1} = 1 + 2q_0$ (observe that $2q_0$ is also an order of $\mathcal{D}$). Let $P \in \mathcal{X}(\mathbb{F}_q)$. By Lemma A

$$\nu_{r-2} \leq j_{r-1}(P) - j_1(P) \leq \epsilon_{r-2} = 2q_0\,.$$

Thus the sequence of Frobenius orders of $\mathcal{D}$ would be $\epsilon_0, \epsilon_1, \ldots, \epsilon_{r-2}, \epsilon_r$. Now for any $P \in \mathcal{X}(\mathbb{F}_q)$ (Lemma A)

$$v_P(S) \geq \sum_{i=0}^{r-1}(j_{i+1}(P) - \nu_i) = \sum_{i=0}^{r-2}(j_{i+1}(P) - \nu_i) + (j_r(P) - \nu_{r-1}) \geq (r-1)j_1(P) + 1 + 2q_0$$

so that

$$\deg(S) \geq (r + 2q_0)N_1\,. \tag{4.2}$$

From the following identities

- $2g - 2 = (2q_0 - 2)(1 + 2q_0 + q) = (2q_0 - 2)m_r(P)$,
- $N_1 = (1 - 2q_0 + q)(1 + 2q_0 + q) = (1 - 2q_0 + q)m_r(P)$,

inequality (4.2) becomes

$$(2q_0 - 2)\sum_{i=0}^{r-1}\nu_i + (r + q) \geq (r + 2q_0)(1 - 2q_0 + q)\,.$$

Since $\nu_{r-1} = q$ it follows that

$$\sum_{i=0}^{r-2}\epsilon_i = \sum_{i=0}^{r-2}\nu_i \geq (r-1)q_0\,.$$

Now we use a property involving the orders of $\mathcal{D}$ (see [20]): $\epsilon_i + \epsilon_j \leq \epsilon_{i+j}$ for $i + j \leq r$. We apply this in the form $\epsilon_i + \epsilon_j \leq \epsilon_{r-2}$ with $i + j = r - 2$. Thus

$$2\sum_{i=0}^{r-2}\epsilon_i \leq (r-1)\epsilon_{r-2} = (r-1)2q_0\,.$$

We conclude that $\epsilon_i + \epsilon_{r-2-i} = \epsilon_{r-2}$ for $i = 0, 1, \ldots, r-2$. In particular, $\epsilon_{r-3} = 2q_0 - 1$ and the $p$-adic criterion (cf. [91, Cor. 1.9]) would imply $\epsilon_i = i$ for $i = 0, 1, \ldots, r-3$. These facts imply $r = 2q_0 + 2$. Finally, we are going to see that this is a contradiction according to Castelnuovo's genus bound applied to $\mathcal{D}$; we must have

$$2g = 2q_0(q-1) \leq \frac{(q + 2q_0 - (r-1)/2)^2}{r-1}\,.$$

For $r = 2q_0 + 2$ this gives $2q_0(q-1) < (q+q_0)^2/2q_0 = q_0q + q/2 + q_0/2$, a contradiction. □

*Remark* 4.3. We write an alternative proof of the previous lemma. We have $2q_0 \le \epsilon_{r-1} \le j_{r-1}(P) = 2q_0 + 1$. Suppose $\epsilon_{r-1} = 2q_0 + 1$ and thus $\epsilon_{r-2} = 2q_0$. For any $P \in \mathcal{X}(\mathbb{F}_q)$, $\epsilon_{r-2} \le j_{r-2}(P) < j_{r-1}(P) = 1 + 2q_0$; thus $j_{r-2}(P) = 2q_0$ and $1 + q \in H(P)$. If we take $\tilde{P} \in \mathcal{X}(\mathbb{F}_q)$ such that $1 + 2q_0 + q, 2q_0 + q \in H(\tilde{P})$ (Proposition 3.3), $H(\tilde{P})$ contains the semigroup

$$H := \langle q, q+1, 2q_0 + q, 1 + 2q_0 + q \rangle$$

and hence $g \le g(H) := (\mathbb{N}_0 \setminus H)$. However, one shows that $g > g(H)$ as in Remark 4.6 below.

**Lemma 4.4.** *There exists $P \in \mathcal{X}(\mathbb{F}_q)$ such that the following properties hold true*:

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

*Proof.* Let $P \in \mathcal{X}(\mathbb{F}_q)$. In the proof of Lemma 4.2 we obtained the following inequality

$$v_P(S) \ge \sum_{i=0}^{r-2} (j_{i+1}(P) - \nu_i) + 1 + 2q_0 \ge (r-1)j_1(P) + 1 + 2q_0 \ge r + 2q_0\,.$$

Thus it is enough to show that $v_P(S) = r + 2q_0$ for some point $P \in \mathcal{X}(\mathbb{F}_q)$. Suppose on the contrary that $v_P(S) \ge r + 2q_0 + 1$ for any $P \in \mathcal{X}(\mathbb{F}_q)$. Then arguing as in the proof of Lemma 4.2 we would have

$$\sum_{i=0}^{r-2} \nu_i \ge rq_0 + 1\,.$$

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

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

and thus

$$rq_0 + 2 \le r\epsilon_{r-1}/2$$

so that $\epsilon_{r-1} > 2q_0$ which is a contradiction according to Lemma 4.2. □

**Lemma 4.5.** (1) $\epsilon_2$ *is a power of two*;
(2) $\nu_1 > \epsilon_1 = 1$.

*Proof.* (1) It is a consequence of the $p$-adic criterion [91, Cor. 1.9].

(2) Suppose that $\nu_1 = 1$. Let $P$ be a $\mathbb{F}_q$-rational point satisfying Lemma 4.4. Then $j_2(P) = 2$ and thus by Lemma 3.2 the Weierstrass semigroup $H(P)$ at $P$ contains the semigroup

$$H := \langle q, -1 + 2q_0 + q, 2q_0 + q, 1 + 2q_0 + q \rangle\,.$$

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

*Remark* 4.6. Let $H$ be the semigroup defined above. We are going to show that $g(H) = g - q_0^2/4$. To begin with we notice that $L := \cup_{i=1}^{2q_0-1} L_i$ is a complete system of residues module $q$, where

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

Moreover, for each $\ell \in L$, $\ell \in H$ and $\ell - q \notin H$. Hence $g(H)$ can be computed by summing up the coefficients of $q$ from the above list (see e.g. [86, Thm. p.3]); i.e.

$$\begin{array}{lcl} g(H) & = & \sum_{i=1}^{q_0-1} i(2i+1) + q_0^2 + (q_0+1)q_0 + \sum_{i=2}^{q_0/2} (q_0+i)(2q_0 - 2i + 2) + \\ & & \sum_{i=1}^{q_0/2-1} (3q_0/2 + i)(q_0 - 2i) = q_0(q-1) - q_0^2/4 \, . \end{array}$$

In the remaining part of this paper we let $P_0$ be a point satisfying Lemma 4.4. We set $m_i := m_i(P_0)$ and denote by $v = v_{P_0}$ the valuation at $P_0$.

By Lemma 4.5 the Frobenius orders of $\mathcal{D}$ are $\nu_0 = 0, \nu_1 = \epsilon_2, \ldots, \nu_{r-1} = \epsilon_r$ and thus

$$\text{(4.3)} \qquad \begin{cases} m_i = 2q_0 + q - \epsilon_{r-i} & \text{if } i = 1, \ldots, r-2, \\ m_{r-1} = 2q_0 + q, \\ m_r = 1 + 2q_0 + q. \end{cases}$$

Let $x, y_2, \ldots, y_r \in \mathbb{F}_q(\mathcal{X})$ be rational functions such that $\mathrm{div}_\infty(x) = m_1 P_0$, and $\mathrm{div}_\infty(y_i) = m_i P_0$ for $i = 2, \ldots, r$. The fact $\nu_1 > 1$ means that the following matrix

$$\begin{pmatrix} 1 & x^q & y_2^q & \ldots & y_r^q \\ 1 & x & y_2 & \ldots & y_r \\ 0 & 1 & D_x^1 y_2 & \ldots & D_x^1 y_r \end{pmatrix}$$

has rank two (cf. [91, Sect. 2]). Here $D_x^j y_i$ denotes the $j$th Hasse derivative (see e.g. [83], [84], [44]). In particular,

$$\text{(4.4)} \qquad y_i^q - y_i = D_x^1 y_i (x^q - x) \quad \text{for } i = 2, \ldots, r \, .$$

**Lemma 4.7.** (1) *For $P \in \mathcal{X}(\mathbb{F}_q)$, the divisor $(2g-2)P$ is canonical; in particular, the Weierstrass semigroup at $P$ is symmetric;*

(2) *Let $n \in H(P_0)$. If $n < 2q_0 + q$, then $n \le q_0 + q$;*

(3) *For $i = 2, \ldots, r$ there exists $g_i \in \mathbb{F}_q(\mathcal{X})$ such that $D_x^1 y_i = g_i^{\epsilon_2}$. Furthermore,* $\mathrm{div}_\infty(g_i) = \frac{q m_i - q^2}{\epsilon_2} P_0$.

*Proof.* (1) Let $P \in \mathcal{X}(\mathbb{F}_q)$. We have $m_r P \sim m_r P_0$ by (4.1) and $2g-2 = (2q_0-2)m_r$. Thus we can assume $P = P_0$. Let $t$ be a local parameter at $P_0$. We shall show that $v(\frac{dx}{dt}) = 2g-2$. The equation $i = r$ in (4.4) by $\frac{dx}{dt}$ and the product rule give

$$\frac{dx}{dt}(y_r^q - y_r) = \frac{dy_r}{dt}(x^q - x)\,;$$

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

$$v(\frac{dx}{dt}) = (q-1)m_r - (1-2q_0+q)m_r = (2q_0-2)m_r = 2g-2\,.$$

(2) We know that the elements $q$, $2q_0+q$ and $1+2q_0+q$ belong to the Weierstrass semigroup $H(P_0)$ at $P_0$. Then the numbers

$$kq + j(2q_0+q) + i(1+2q_0+q) = (k+j+i)q + (j+i)q_0 + i$$

are also non-gaps at $P_0$ where $k, j, i \in \mathbb{N}_0$. Let $k = 2q_0-2$, $j+i = q_0-2$. Hence,

$$(2q_0-2)q + q - 4q_0 + j \quad \text{for } j = 0, \dots, q_0-2$$

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

$$1 + q_0 + q + j \quad \text{with } j = 0, \dots, q_0-2$$

are gaps at $P_0$ and the proof follows.

(3) Set $f_i := D_x^1 y_i$. By Hasse-Schmidt [43, Satz 10] it is enough to show that

$$D_x^j f_i = 0 \ \ , \quad \text{for } 1 \le j < \epsilon_2\,.$$

From Eqs 4.4 it is clear that $D_x^1 f_i = 0$. Now as $\epsilon_2 > 2$ each matrix below has rank two (cf. [91, Sect. 1])

$$\begin{pmatrix} 1 & x & y_2 & \dots & y_r \\ 0 & 1 & D_x^1 y_2 & \dots & D_x^1 y_r \\ 0 & 0 & D_x^j y_2 & \dots & D_x^j y_r \end{pmatrix}\ , \quad 2 \le j < \epsilon_2\,;$$

consequently $D_x^j f_i = 0$ for $2 \le j < \epsilon_2$. Finally from the computations $v(g_i) = v(f_i)/\epsilon_2$ and $-qm_i = v(f_i) - q^2$ by (4.4) we find $v(f_i) = -qm_i + q^2$. If $P \ne P_0$, $\frac{\mathrm{d}f_i}{\mathrm{d}t} = \frac{\mathrm{d}y_i}{\mathrm{d}t}$, where $t = x - x(P)$ is a local parameter at $P$ by Item (1). □

**Lemma 4.8.** *$\epsilon_2 = q_0$ and $r = 4$.*

*Proof.* By Lemma 4.2, $r \ge 3$. We claim that $r \ge 4$; otherwise, let $g_2$ be the rational function in Lemma 4.7(3). We have $v(g_2) = -q$ since $m_2 = 2q_0 + q$ and $\epsilon_2 = 2q_0$. Therefore there exist elements $a \ne 0$ and $b$ in $\mathbb{F}_q$ such that $x = ag_2 + b$ (notice that $v(x) = -q$). The case $i = 2$ in (4.4) reads

$$\frac{y_2}{a}^q - \frac{y_2}{a} = g_2^{2q_0}(g_2^q - g_2)\,;$$

let $v := y_2/a$, $u := g_2$ and set $w := v^{q_0} - u^{q_0+1}$. Thus

$$w^q - w = u^{q_0}(u^q - u)$$

and we find that $q_0 + q$ is a non-gap at $P_0$ (cf. [41, Lemma 1.8]). This contradiction eliminates the case $r = 3$.

Let $r \geq 4$ and $2 \leq i < r$. We show that $\epsilon_2 = q_0$. The element $(qm_{r-2} - q^2)/\epsilon_2$ is a positive non-gap at $P_0$ and hence at least $m_1 = q$. Thus $m_{r-2} - q \geq \epsilon_2$ $(*)$ and $2q_0 - \epsilon_2 \geq \epsilon_2$ by (4.3); it follows that $q_0 \geq \epsilon_2$. Now by Lemma 4.7(2) $m_{r-2} \leq q_0 + q$; from $m_{r-2} = 2q_0 + q - \epsilon_2$, $q_0 \leq \epsilon_2$.

Finally we show that $r = 4$. As in $(*)$ we deduce that $m_2 - q \geq \epsilon_2$ and from (4.3) $2q_0 - \epsilon_{r-2} \geq \epsilon_2 = q_0$; i.e, $q_0 \geq \epsilon_{r-2} \geq \epsilon_2 = q_0$ so that $\epsilon_{r-2} = \epsilon_2$ and the proof follows. □

**Proof of Theorem 4.1.** Let $P_0 \in \mathcal{X}(\mathbb{F}_q)$ be as above. The case $i = 2$ in (4.4) and Lemma 4.7 give

$$y_2^q - y_2 = g_2^{q_0}(x^q - x)\ ;$$

moreover, $m_2 = q_0 + q$ and so $v(g_2) = -q$. Thus $x = ag_2 + b$ with $a$ and $b$ in $\mathbb{F}_q$, $a \neq 0$; in particular,

$$\frac{y_2}{a}^q - \frac{y_2}{a} = g_2^{q_0}(g_2^q - g_2)\,.$$

It follows that $\mathcal{X}$ is defined by the plane equation

$$v^q - v = u^{q_0}(u^q - u)\,,$$

where $v := y_2/a$ and $u := g_2$, and thus its automorphism group (over $\bar{\mathbb{F}}_q$) is the Suzuki group (Henn [46]). As the Suzuki group is simple it follows that it is also defined over $\mathbb{F}_q$. We conclude that $\mathcal{X}$ is isomorphic to the Suzuki curve by the statements (I), (II) and (III) stated at the beginning of this section.

## 5. Maximal Curves

Let $\mathcal{X}$ be a curve of genus $g > 0$ over $\mathbb{F}_q$ with $q = \ell^2$. The curve is called *maximal* if its number of rational points attains the HW-bound. By (1.2), the $\alpha_j$'s in Proposition 1.1 satisfies $\alpha_j = -\ell$ for any $j$. Thus the polynomial $h(t)$ in (1.7) is of the form

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

Let $\mathbf{\Phi} : \mathcal{X} \to \mathcal{X}$ be the Frobenius morphism over $\mathbb{F}_q$. By Section 3 the curve $\mathcal{X}$ is equipped with the linear series

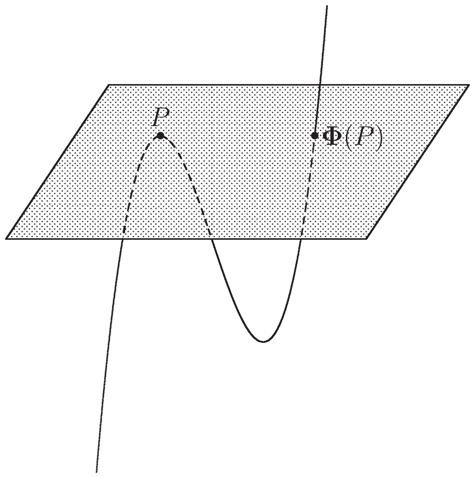
$$\mathcal{D} = |(1 + \ell)P_0|\,, \quad P_0 \text{ a rational point}$$

such that

$$\mathbf{\Phi}(P) + \ell P \sim (1 + \ell)P_0 \tag{5.1}$$

for any $P \in \mathcal{X}$; see the picture below

We already know that the Hermitian curve $\mathcal{H}$ is maximal. We can obtain many examples of maximal curves by taking into consideration the following Serre's remark (cf. [57]). Let $\mathcal{Y}$ be a curve over $\mathbb{F}_{\ell^2}$ and $\mathcal{X} \to \mathcal{Y}$ a non-constant morphism over $\mathbb{F}_{\ell^2}$; then $P(\mathcal{Y}, \ell^2; t)$



divides $P(\mathcal{X},\ell^2;t)$. In particular, if $\mathcal{X}$ is maximal, $\mathcal{Y}$ is so. Therefore if $G$ is a subgroup of the automorphisms group of $\mathcal{H}$, the quotiont curve $\mathcal{H}/G$ is also maximal; we remark that there exists maximal curves which are not covered by the Hermitian curve (see Example 5.9). van der Geer and van der Vlught constructed maximal curves via methods coming from linear codes. See Hirschfeld et al. [51] for a complete bibliography on maximal curves.

**5.1 The linear series $\mathcal{D}$.** Let $r$ and

$$\pi = (f_0 : f_1 : \ldots : f_r)$$

be respectively the dimension and the morphism defined by $\mathcal{D}$. We use the notation of the Appendix. Set $\mathbb{P}^r := \mathbb{P}^r(\bar{\mathbb{F}}_{\ell^2})$, $\mathbb{P}^M := \mathbb{P}^M(\bar{\mathbb{F}}_{\ell^2})$.

By Proposition 3.4, $\epsilon_r = \ell$ which is equivalent (see e.g. [31]) to the existence of rational functions $w_0, w_1, \ldots, w_r$ (not all zero) such that

$$w_0^\ell f_0 + w_1^\ell f_1 + \ldots + w_r^\ell f_r = 0\,. \tag{5.2}$$

For $P \in \mathcal{X}$ let $v = v_P$ and $t = t_P$ denote respectively the valuation and a local parameter at $P$. We let $e = e_P := \min\{v(w_0), v(w_1), \ldots, v(w_r)\}$ and $z_i := t^{-e}w_i$.

Then for any $P \in \mathcal{X}$, the $\mathcal{D}$-osculating hyperplane at $P$ is defined by

$$(z_0^\ell(P), z_1^\ell(P), \ldots, z_r^\ell(P))\,.$$

Hence from (5.1) and (5.2) we obtain the following dual relation

$$z_0 f_0^\ell + z_1 f_1^\ell + \ldots + z_r f_r^\ell = 0\,. \tag{5.3}$$

A natural question is the following: Is $\pi$ an embedding?. Since $j_1(P) = 1$ for any $P$ we have just to investigate whether or not $\pi$ is injective. Let us consider the morphism

$$\phi := (w_0 : w_1 : \ldots : w_r) = (z_0 : z_1 : \ldots : z_r)\,.$$

Let $M$ be the dimension of the linear series $\mathcal{D}'$ associated to $\phi$. By (5.3) $\mathcal{D}'$ satisfies (5.1) in the sense that all the divisor of type $\mathbf{\Phi}(P) + qP \in \mathcal{D}'$; we notice that we may have

$M < r$ since the $w_i$'s may be linearly dependent. We obtain the following qualitative properties of maximal curves [54].

**Theorem 5.1.** (1) *The morphism $\pi : \mathcal{X} \to \mathbb{P}^r$ is an embedding;*

(2) *The morphism $\phi : \mathcal{X} \to \mathbb{P}^r$ is an embedding; thus $\mathcal{X}$ is isomorphic to $\phi(\mathcal{X}) \subseteq \mathbb{P}^M$;*

(3) *Let us identify the curve $\mathcal{X}$ with its image $\pi(\mathcal{X}) \subseteq \mathbb{P}^r$. The curve is contained in an Hermitian variety;*

(4) *Let $\mathcal{Y} \subseteq \mathbb{P}^r$ be a curve of degree $\ell + 1$ over $\mathbb{F}_q$. If $\mathcal{Y}$ is contained in an Hermitian variety, then $\mathcal{Y}$ is a maximal curve.*

*Proof.* (sketch) (1) If $\pi(P) = \pi(Q)$, by (5.1) $\{P, \mathbf{\Phi}(P)\} = \{Q, \mathbf{\Phi}(Q)\}$. Let $P = \mathbf{\Phi}(Q)$ (and one shows that $Q$ is rational). Let $\tilde{\mathbf{\Phi}} : \mathbb{P} \to \mathbb{P}$ denote the Frobenius morphism on $\mathbb{P}^r$. We have $\pi \circ \mathbf{\Phi} = \tilde{\mathbf{\Phi}} \circ \pi$ and hence $\pi(P)$ is rational; that is $\tilde{\mathbf{\Phi}}(\pi(P)) = \pi(P)$. After a change of coordinates we can assume $\pi(P) = (1 : 0 : \ldots : 0)$ with $f_0 = 1$ and $v(f_i) \geq 1$. Let $z_i(t) = z_i(P) + a_i^{(1)} t + \ldots$ for $i = 0, 1, \ldots, r$. From (5.2):

$$D = (z_0(P) f_0 + z_1(P) f_1 + \ldots + z_r(P) f_r) = -\sum_{i=0}^{r} f_i((a_i^1)^\ell t^\ell + \ldots)$$

We have to show that $v_P(D) = \ell + 1$. From the equation above,

$$v_(D) = \ell + v(\sum_{i=0}^{r} f_i(((a_i^{(1)})^\ell + (a_i^{(2)})^\ell t + \ldots) \,.$$

As $v_P(f_i) \geq 1$ for $i \geq 1$ we just have to check that $a_0^{(1)} = 0$. This comes from (5.3).

(2) The proof is similar to (1).

(3) The linear series $\mathcal{D}'$ is a sub linear series of $\mathcal{D}$; in particular each $z_j$ is a $\mathbb{F}_{\ell^2}$-linear combination of type $z_j = \sum_{i=1}^{r} a_{ij} f_i$. After some linear computations, the result follows from (5.3).

(4) See [54, Thm. 4.1]. □

*Remark* 5.2. The minimum dimension of the Hermitian variety which contains a maximal curve is $M = \dim(\mathcal{D}')$.

**5.2 The Hermitian Curve.** Notation as above. We notice that $r \geq 2$ by (5.1). We shall prove the following. We recall that the Hermitian curve can be also defined by the equation $y^\ell + y = x^{\ell+1}$.

**Theorem 5.3.** ([24], [72]) *Let $\mathcal{X}$ be a maximal curve over $\mathbb{F}_{\ell^2}$ of genus $g > 0$. The following statements are equivalent:*

(1) *$\mathcal{X}$ is the Hermitian curve;*

(2) $g > (\ell - 1)^2/4$;

(3) $r = 2$.

*Proof.* The genus in (1) is $\ell(\ell-1)/2$ and (2) follows. Assume (2). Since $\mathcal{D}$ is simple we apply Castelnuovo's genus bound; i.e.,

$$2g \le (2\ell - r + 1)^2/4(r-1)\,.$$

If $r \ge 3$, then $2g \le (\ell-1)^2/4$, a contradiction. Now assume (3). To proof (1) we proceed as in Theorem 4.1. Let $x, y \in \mathbb{F}_{\ell^2}(\mathcal{X})$ whose pole divisor are respectively $\mathrm{div}_\infty(x) = \ell P_0$ and $\mathrm{div}_\infty y = (\ell+1)P_0$ (Lemma 3.2). Since $\nu_1 = \ell$ we have a relation of type

$$(y^{\ell^2} - y)D^1_x x = (x^{\ell^2} - x)D^1_x y\,, \tag{5.4}$$

Let $f := D^1_x y$. Then $D^1_x f = 0$. Now since $\epsilon_2 = \nu_1 = \ell$ (Proposition 3.4), for $i = 2, \ldots, < \epsilon_2 = \ell$ the rank of the following matrices is two:

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & f \\ 0 & 0 & D^i_x y \end{pmatrix}.$$

Thus $D^i_x y = 0$ for $i = 2, \ldots, \ell$ and from (5.4), $D^i_x f = 0$ for $i = 1, \ldots, \ell - 1$. So by [43, Satz 10], $f$ is a $\ell$-th power, says $f = f_1^\ell$. From (5.4), $v_{P_0}(f) = -\ell^2$ and so $v_{P_0}(f_1) = -\ell$; thus $f_1 = ax + b$ with $a, b \in \mathbb{F}_{\ell^2}$, $a \ne 0$. If $x_1 := ax + b$ and $y_1 := ay$, the equation (5.4) becomes

$$y_1^{\ell^2} - y_1 = x_1^\ell(x_1^{\ell^2} - x_1);$$

therefore

$$(y_1^\ell + y_1 - x_1^{\ell+1})^\ell = y_1^\ell + y_1 - x_1^{\ell+1}$$

and the proof is complete. □

**5.3. The genus.** Here we discuss some properties concerning the genus $g$ of a maximal curve over $\mathbb{F}_{\ell^2}$. First of all we notice that Theorem 5.3 implies the following restriction on $g$ which was conjectured by Xing and Stichtenoth [103]; see [21], [23]. (This gives a partial answer of a question of Serre [88].) We have

$$g \le g_2 := \lfloor (\ell-1)^2/4 \rfloor\,, \quad \text{or} \quad g = g_1 = \ell(\ell-1)/2\,. \tag{5.5}$$

*Remark* 5.4. Thus $N_{\ell^2}(g) < \ell^2 + 1 + 2\ell g$ for $g_2 < g < g_1$ (cf. Lauter [59]).

We already know that $g = g_1$ occurs only for the Hermitian curve. A similar property holds for $g = g_2$: the unique maximal curves of genus $g_2$ is the quotient of the Hermitian curve by certain involutions; these curves are defined by the following plane curves [22], [2], [55]

- $y^q + y = x^{(q+1)/2}$ if $q$ is odd;
- $y^{q/2} + \ldots + y^2 + y = x^{q+1}$ if $q$ is even.

We can improve (5.5) as follows. Let $g_3 := h(\ell+1,3) = \lfloor(\ell^2-\ell+4)/6\rfloor$ denote the Halphen's number which asserts that any non-degenerate curve in $\mathbb{P}^3(\bar{\mathbb{F}}_{\ell^2})$ of degree $\ell+1$ of genus $g > g_3$ is contained in a quadratic surface. Thus, as the curve has many rational points, $g \geq g_2$.

**Theorem 5.5.** ([55]) *The genus $g$ of a maximal curve over $\mathbb{F}_{\ell^2}$ satisfies*

$$g \leq g_3 = \lfloor(\ell^2-\ell+4)/6\rfloor\,, \quad \textit{or} \quad g = g_2 = \lfloor(\ell-1)^2/4\rfloor \quad \textit{or} \quad g = g_1 = \ell(\ell-1)/2\,.$$

There exist examples of maximal curves of $g = g_3$: for example the quotient curves of the Hermitian curve by certain subgroups of order three; they are defined by the following plane equations [28], [13], [14]

- $x^{(\ell+1)/3} + x^{2(\ell+1)/3} + y^{\ell+1} = 0$ if $\ell \equiv 2 \pmod 3$;
- $\omega x^{(\ell-1)/3} - yx^{2(\ell-1)/3} + y^\ell = 0$ if $\ell \equiv 1 \pmod 3$, where $\omega \in \mathbb{F}_{\ell^2}$ such that $\omega^{\ell-1} = -1$;
- $y^\ell + y = (\sum_i^t x^{\ell/3})^2$ if $\ell = 3^t$.

**Question 5.6.** There is a unique maximal curve of genus $g_3$ which is Galois covered by the Hermitian curve, namely the examples above [14, Prop. 2.1]. Is there exist a maximal curve of genus $g_3$ which is not covered by the Hermitian curve?

For $\ell \not\equiv 0 \pmod 3$, we can improve Theorem 5.5 as follows.

**Theorem 5.7.** ([95]) *Let $\mathcal{X}$ be a maximal curve over $\mathbb{F}_{\ell^2}$ of genus $g$. Assume $\ell \not\equiv 0 \pmod 3$ and $r = 3$. If $(4\ell-1)(2g-2) > (\ell+1)(\ell^2-5\ell-2)$, then*

$$g \geq (\ell^2-2\ell+3)/6\,.$$

*Proof.* First we show that $\epsilon_2 = 2$; on the contrary, $\epsilon_3 \geq 4$, by the $p$-adic criterion (here we use the hypothesis on $\ell$). Let $R$ and $S$ be the ramification and $\mathbb{F}_{\ell^2}$-Frobenius divisor of $\mathcal{D}$ respectively. We have (Lemma A)

$$v_P(S) \geq j_2(P) + (j_3(P) - \epsilon_2) \geq 5 \quad \text{for any } P \in \mathcal{X}(\mathbb{F}_{\ell^2})$$

and so the maximality of $\mathcal{X}$ implies

$$\deg(S) = (\ell+1)(2g-2) + (\ell^2+3)(\ell+1) \geq 5(\ell+1)^2 + 5\ell(2g-2)\,.$$

It follows that

$$(\ell+1)(\ell^2-5\ell-2) \geq (4\ell-1)(2g-2)\,,$$

a contradiction. Now we use the ramification divisor $R$:

$$\deg(R) = (\ell+2+1)(2g-2) + 4(\ell+1) \geq (\ell+1)^2 + \ell(2g-2)$$

and thus $g \geq (\ell^2-2\ell+3)/6$. □

**Corollary 5.8.** *Let $\mathcal{X}$, $g$ and $\ell$ be as in the theorem above. If $g > (\ell-1)(\ell-2)/6$, then*

$$g \geq (\ell^2-2\ell+3)/6\,.$$

*Proof.* The hypothesis on $g$ implies $r \le 3$. If $r = 2$, then $g = \ell(\ell-1)/2$ by Theorem 5.3. Let $r = 3$; the hypothesis on $g$ is equivalent to $(2g-2) > (\ell+1)(\ell-4)/3$ and hence

$$(4\ell-1)(2g-2) > (4\ell-1)(\ell+1)(\ell-4)/3 > (\ell+1)(\ell^2-5\ell-2)$$

and the result follows. □

**5.4 Examples.** Throughout, by a maximal curve we mean a maximal curve over $\mathbb{F}_{\ell^2}$.

**Example 5.9.** (Curves covered by the Hermitian curve, I) We have already noticed that any curve covered by the Hermitian curve is also maximal. However, there exist maximal curves that cannot arise in this way. The first example of such a situation was given by Giulietti and Korchmáros [35]; their example is the case $m = 3$ of the nonsingular model of the curve defined in $\mathbb{P}^3(\bar{\mathbb{F}}_{\ell^{2m}})$ ($m$ odd) by the equations

$$\begin{cases} z^{(\ell^m+1)/(\ell+1)} = yh(x) \\ (x^\ell + x)^{N/\ell} = y^{\ell+1} \end{cases}$$

where $h(x) = \sum_{i=0}^{N}(-1)^{i+1}x^{(\ell-1)i}$ and $N(\ell-1)+1 = (\ell^m+1)/(\ell+1)$. After some computations one shows that the curve is contained in an Hermitian variety and that any irreducible component is defined over $\mathbb{F}_{\ell^{2m}}$; it follows that each irreducible component is maximal according to Theorem 5.1. In addition the genus of such components is $(\ell^m+1)(N\ell-2)/2+1$. By using the Riemann-Hurwitz genus formula and by counting rational points one concludes that such components cannot be covered by the Hermitian curve. We should say that we have no a theoretically explanation on the existence of these examples. We shall start with the question below.

**Example 5.10.** (Curves covered by the Hermitian curve, II) Let $\mathcal{X}$ be a maximal of genus $g$. By Theorem 5.5, $\mathcal{X}$ is covered by the Hermitian curve provided that

$$g > c(\ell) = (\ell^2 - \ell + 4)/6\,.$$

**Question 5.11.** Shall we improve the bound $c(\ell)$?

Notice that $c(\ell)$ is the Halphen's bound related to quadratic surfaces in $\mathbb{P}^3$; we may obtain further improvements on $c(\ell)$ by taking into considerations constraints that curves with many rational points may impose on surface of arbitrary degree.

**Example 5.12.** (On the uniqueness of maximal curves, I) Let $\mathcal{X}$ be a maximal curve of genus $g$. Let $d$ be a divisor of $\ell+1$. Let $\ell+1 = dn$. The curve is defined by the plane curve

$$y^\ell + y = x^n$$

whenever there exists a rational point $P$ of $\mathcal{X}$ whose Weierstrass semigroup is generated by $n$ and $q$ [22] (see also [1], [3] for analogous results).

**Example 5.13.** (On the uniqueness of maximal curves, II) Let $d$ be a divisor of $\ell+1$. The previous example suggests to consider the uniqueness of maximal curves $\mathcal{X}$ of genus

$$g = \frac{1}{2}(\ell-1)(\frac{\ell+1}{d}-1)\,.$$

If $d=2$, $g$ coincides with Castelnuos genus bound. In this case, the geometry of the curve equipped with the linear series $|2\mathcal{D}|$ implies the hypothesis on non-gaps above; thus there is a unique maximal curve of genus $(\ell-1)^2/4$ as we have pointed out above.

If $d=3$, $g$ also coincides with Castelnuovo genus bound and as in the case above, the hypothesis on non-gaps hold true and there exists a unique maximal curve of genus $(\ell-1)(\ell-2)/6$.

Now observe that $g=(\ell-1)(\ell-2)/6$ is an integer for $\ell \equiv 1 \pmod 3$. However, for $\ell \geq 13$, there is no maximal curves having such a genus [55]. Here one uses a beautiful theorem due to Accola [4] concerning further constraints on curves whose genus equals Castelnuovo's genus bound.

**Question 5.14.** Shall we exclude the hypothesis on non-gaps in Example 5.12?

**Example 5.15.** (On the uniqueness of maximal curves, III) A maximal curve is not necessarily characterized via its genus.

(1) Let $\ell \equiv 3 \mod 4$. Consider the maximal curve $\mathcal{X}$ and $\mathcal{Y}$ defined respectively by the plane curves:

$$x^{(\ell+1)/2} + y^{(\ell+1)/2} + 1 = 0\,, \quad \text{and} \quad y^\ell + y = x^{(\ell+1)/4}\,.$$

They have the same genus $g=(\ell-1)(\ell-3)/8$ but they are not isomorphic because the semigroup $\langle(\ell-1)/2,,(\ell+1)/2\rangle$ is a Weierstrass semigroup at some point of $\mathcal{X}$ but there is no point on $\mathcal{Y}$ satisfying this property [30], [12]. Moreover, in the last reference it is shown that the unique plane maximal curve of degree $(\ell+1)/2$ ($\ell \geq 11$ odd) is the curve $\mathcal{X}$ above.

(2) Let us consider maximal curves over $\mathbb{F}_{64}$. Let $\epsilon$ be a primitive 3th-root of unity.

Curve $\mathcal{X}$: The Hermitian curve is given by $x^9+y^9+1=0$. Consider $T_1 : (x,y) \mapsto (x,\epsilon y)$. Thus the quotient curve $\mathcal{X}_1 := \mathcal{H}/ < T_1 >$ is defined by $u^9+v^3+1=0\,(*)$. Now consider $T_2 : (u,v) \mapsto (\epsilon u, \epsilon^{-1} v)$. Then $\mathcal{X}_1/\langle T_2\rangle$ is defined by $z^4+z=w^3$ (to see this we just multiply $(*)$ by $u^3$); clearly its genus is $g=3$ and it is maximal since it is covered by the Hermitian curve (cf. Rodriguez [79], Luengo et all. [80]).

Curve $\mathcal{Y}$: Consider the maximal curve $\mathcal{Y}_1 : x^4+x^2+x=y^9$. We can use the automorphism $T_1 : (x,y) \to (x,\epsilon y)$ to obtain the maximal curve $\mathcal{Y} := \mathcal{Y}_1/\langle T_1\rangle$ of genus 3 defined by $u^4+u^2+u=w^3$.

**Claim.** The curves $\mathcal{X}$ and $\mathcal{Y}$ above are non-isomorphic over $\bar{\mathbb{F}}_{64}$ (cf. [29], [95]). There is just one point $P_0$ over $x=\infty$ or $u=\infty$. The number 5 does not belong to the Weierstrass semigroup at $P_0$ and so for both curves $\mathcal{D}=4P_0$ is the canonical linear series. We apply the Appendix to $\mathcal{D}$ and one shows that the curve $\mathcal{X}$ and $\mathcal{Y}$ have 5 and 17 Weierstrass points respectively.

Let $\ell \not\equiv 0 \pmod 3$. Then by Corollary 5.8 the genus $g$ of a maximal curve does not belong to the interval

$$[\lfloor\frac{1}{6}(\ell-1)(\ell-2)\rfloor+1, \lceil\frac{1}{6}(\ell^2-2\ell+3)\rceil-1]\,. \tag{5.6}$$

Let $S(\ell)$ be the set of numbers that arise as the genus of maximal curves over $\mathbb{F}_{\ell^2}$. For $\ell \le 5$, the set $S(\ell)$ is complete determined [28, Remark 6.1]; by taking into consideration such a remark we work out the following.

**Example 5.16.** Case $\ell = 7$. $g \le g_3 = 7$ or $\{0,1,2,3,5,7,9,21\} \subseteq S(7)$; $6 \not\in S(7)$ by (5.6).

Case $\ell = 8$. $g \le g_3 = 10$ or $\{0,1,2,3,4,6,7,9,10,12,28\} \subseteq S(8)$; $8 \not\in S(8)$ by (5.6),

Case $\ell = 11$. $g \le g_3 = 19$ or $\{0,1,2,3,4,5,7,9,10,11,13,15,18,19,25,55\} \subseteq S(11)$; $16 \not\in S(11)$ by (5.6),

Case $\ell = 13$. $g \le g_3 = 26$ or $\{0,1,2,3,6,9,12,15,18,26,36,78\} \subseteq S(13)$; $23, 24 \not\in S(13)$ by (5.6). Moreover, $22 \not\in S(13)$ (cf. Example 5.13).

Case $\ell = 16$. $g \le g_3 = 40$ or $\{0,1,2,4,6,8,12,24,28,56,120\} \subseteq S(16)$; $36, 37 \not\in S(16)$ by (5.6. Moreover, $35 \not\in S(16)$ (cf. Example 5.13).

**Question 5.17.** (1) Does 4 (resp. 5) belong to $S(7)$ (resp. $S(8)$)?

(2) Does $g = g_4 := \lceil\frac{1}{6}(\ell^2-2\ell+3)\rceil$ belong to $S(\ell)$ for infinitely many $\ell$? (In each case above such a $g$ exists).

(3) What about the genus of a maximal curves in the interval $[g_4, g_3-1]$?

**Example 5.18.** (Plane maximal curves) Here we consider (nonsingular) plane maximal curves (over $\mathbb{F}_{\ell^2}$)

(1) Fermat curves: $X^m + Y^m + Z^m = 0$. Clearly the curve is maximal if $m \mid (\ell+1)$. Tafazolian [92] proved that in fact the curve is maximal only if this condition holds.

(2) Hurwitz curves (cf. [5], [29]). Let $\mathcal{H}_n : X^nY + Y^nZ + Z^nX = 0$. This curve is covered by the Fermat curve

$$U^{n^2-n+1} + V^{n^2-n+1} + W^{n^2-n+1} = 0$$

(via an unramified morphism). In particular, if $(n^2-n+1) \mid (\ell+1)$, $\mathcal{H}_n$ is maximal. Conversely, if $\mathcal{H}_n$ is maximal, $\ell+1$ belongs to the Weierstrass semigroup at any rational point. After some computations via the Weierstrass semigroup at $P = (0:1:0)$, which is generated by the set

$$S = \{s(n-1)+1 : s = 1, \ldots, n\}\,,$$

one shows that $(q+1)$ is a multiple of $(n^2-n+1)$. As a numerical example we choose $n = 3$ and conclude that the Klein curve is maximal over $\mathbb{F}_{\ell^2}$ if and only if $\ell \equiv 6 \pmod 7$.

**Appendix: On the Stöhr-Voloch theory.**

In this appendix, we recall some results of Stöhr-Voloch paper [91] concerning Weierstrass points and Frobenius orders. Let $\mathcal{X}$ be a curve of genus $g$ defined over $\bar{\mathbb{F}}_q$.

Let $\mathcal{D} \subseteq |E|$ be a base-point-free linear series of dimension $r$ and degree $D$ on $\mathcal{X}$. 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 $\mathcal{D}_i(P) \supsetneqq \mathcal{D}_{i+1}(P)$, then the integer $i$ is called a $(\mathcal{D}, P)$-*order*; thus by Linear Algebra we have a sequence of $(N+1)$ orders at $P$:

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

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 $\mathcal{X}$, see [91, Thm. 1.5]. This constant sequence is called the *order sequence* of $\mathcal{D}$ and will be denoted by

$$0 = \epsilon_0 < \epsilon_1 < \ldots < \epsilon_r\,.$$

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

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

where $\pi = (f_0 : f_1 : \ldots : f_r)$ is the morphism defined by $\mathcal{D}$, $t$ a separating element of $\bar{\mathbb{F}}_\ell(\mathcal{X})|\bar{\mathbb{F}}_\ell$ and the operator $D_t^i$ is the $i$th Hasse derivative (properties of these operators can be seen in Hefez's paper [44]). Moreover, the number of $\mathcal{D}$-Weierstrass points of $\mathcal{X}$ (counted with multiplicity) is the degree of $R$.

Now to deal with rational points over $\mathbb{F}_q$ we require that both $\mathcal{X}$ and $\mathcal{D}$ be defined over this field. Choose the coordinates $f_i$'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 $L_i(P) = \langle f_i, \ldots, f_r \rangle$. Thus

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

For $i = 0, \ldots, r-1$ set

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

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

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

$$\{P\} = T_0(P) \subsetneqq T_1(P) \subsetneqq \ldots \subsetneqq T_{r-1}(P)\,.$$

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

Let $\mathbf{\Phi} : \mathcal{X} \to \mathcal{X}$ be the Frobenius morphism on $\mathcal{X}$. Suppose that for a generic $P$, $\mathbf{\Phi}(P) \in T_{N-1}(P)$. Then there exists an integer $1 \leq I \leq r-1$ such that $\phi(P) \in T_I(P) \setminus T_{I-1}(P)$. Define $\nu_j := \epsilon_j$ for $0 \leq j \leq I-1$ and $\nu_j = \epsilon_{j+1}$ for $j = I, \ldots, r-1$. The sequence $0 = \nu_0 < \nu_1 < \ldots < \nu_{N-1}$ is called the *Frobenius order sequence* of $\mathcal{D}$ (with respect to $\mathbb{F}_q$; cf. [91, Sect. 2]). The key property related with rational points in [91] is the existence of a divisor $S$, *the Frobenius divisor* of $\mathcal{X}$ (over $\mathbb{F}_q$) satisfying Lemma A(3)(4)(5)(6) below. This divisor is defined as follows. Let $\tilde{L}$ denote the determinant of the matrix whose rows are:

$$(f_0^\ell, f_1^\ell, \ldots, f_r^\ell)\,, \quad (D_t^{\nu_i} f_0, D_t^{\nu_i} f_1, \ldots, D_t^{\nu_i} f_r)\,, \quad i = 0, 1, \ldots, r-1\,.$$

Then

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

We notice that $\mathcal{X}(\mathbb{F}_q) \subseteq \mathrm{Supp}(S)$ and $v_P(S) \geq r$ for $P \in \mathcal{X}(\mathbb{F}_q)$ (Lemma below). Thus

$$\#\mathcal{X}(\mathbb{F}_q) \leq \deg(S)/r\,.$$

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

**Lemma A.** Let $P \in \mathcal{X}$ and $q$ be a power of a prime $p$.

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

**Frobenius non classical plane curves.** (Hefez-Voloch [45]) Let $\mathcal{X}$ be a plane curve of degree $d$ defined over $\mathbb{F}_q$. We consider the linear series $\mathcal{D} := g_d^2$ (whose elements cuts out the curve by lines). Let $0 < \nu$ be the $\mathbb{F}_q$-Frobenius order sequence of $\mathcal{D}$. Assume that $\nu > 1$ (one usually says that $\mathcal{X}$ *is non-classical*). Thus the order sequence of $\mathcal{D}$ is $0 < 1 < \nu$ and hence

$$\deg(R) = (1+\nu)(2g-2) + 3d\,, \quad \text{and} \quad \deg(S) = \nu(2g-2) + (q+2)d\,.$$

The Hefez-Voloch used in this paper affirm

$$\#\mathcal{X}(\mathbb{F}_q) = \deg(S) - \deg(R) = d(q-d+2)\,.$$

## References

[1] M. Abdón and A. Garcia, "On a characterization of certain maximal curves", Finite Fields Appl. **10**(2) (2004), 133–158).

[2] M. Abdón and F. Torres, "On maximal curves in characteristic two", Manuscripta Math. **99** (1999), 39–53.

[3] M. Abdón and F. Torres, "On $\mathbb{F}_{q^2}$-maximal curves of genus $(q-3)q/6$", Beitr. Algebra Geom., **46**(1) (2005), 241–260.

[4] R.D. Accola, "On Castelnuovo's inequality for algebraic curves I", Trans. Amer. Math. Soc. **251** (1979), 357–373.

[5] A. Aguglia, G. Korchmáros and F. Torres, "Plane maximal curves", Acta Arithm. **98**(2) (2001), 165–179.

[6] E. Arbarello, M. Cornalba, P.A. Griffiths and J. Harris, "Geometry of Algebraic Curves", Vol I. Springer-Verlag, New York, 1985.

[7] J. Bezerra, A. Garcia and H. Stichtenoth, "An explicit tower on function fields over cubic finite fields and Zink's lower bound", J. Reine Angew. Math. **589** (2005), 159–199.

[8] E. Bombieri, "Hilbert's 8th problem: An analogue", Proc. Symp. Pure Math. **28** (1976), 269–274.

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

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

[11] L. Chiantini, C. Ciliberto, "Towards a Halphen theory of linear series on curves", Trans. Amer. Math. Soc. **356**(6) (1999), 2197–2212.

[12] A. Cossidente, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, "On plane maximal curves", Compos. Math. **121** (2000), 163–181.

[13] A. Cossidente, G. Korchmáros and F. Torres, "On curves covered by the Hermitian curve", J. Algebra **216** (1999), 56–76.

[14] A. Cossidente, G. Korchmáros and F. Torres, "Curves of large genus covered by the Hermitian curve", Comm. Algebra **28**(10) (2000), 4707–4728.

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

[16] M. Deuring, "Die Typen der Multiplicatorenringe elliptishher Funktionen Körper", Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272.

[17] L.E. Dickson, "History of the Theory of Numbers", Vol. II, Chelsea Publ. Comp., New York 1971.

[18] N.D. Elkies, "Explicit modular towers", Proceeding of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing , Univ. of Illinois at Urbana -Champaign, E.T. Basar and A. Vardy Eds. (1998), 23–32.

[19] N.D. Elkies, E.W. Howe, A. Kresch, B. Poonen, J.L. Wetherell and M.E. Zieve, "Curves of every genus with many points, II: Asymptotically good families", Duke Math. J. **122**(2) (2004), 399–421.

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

[21] R. Fuhrmann, "Algebraische Funktionenkörper über endlichen Körpern mit maximaler Anzahl rationaler Stellen, Disseration, Universität GH Essen, 1995.

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

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

[24] R. Fuhrmann and F. Torres, “On Weierstrass points and optimal curves”, Rend. Circ. Mat. Palermo, Suppl. **51** (Recent Progress in Geometry, E. Ballico and G. Korchmáros Eds.) (1998), 25–46,

[25] W. Fulton, “Algebraic Curves”, Benjamin, New York, 1969.

[26] A. Garcia and H. Stichtenoth, “A tower of Artin-Schreier extensions of functions fields attaining the Drinfeld-Vlăduţ bound”, Invent. Math. **121**(1) (1995), 211–233.

[27] A. Garcia and H. Stichtenoth, “On the asymptotic behavior of some towers of function fields over finite fields”, J. Number Theory **6** (1996), 248–273.

[28] A. Garcia, H. Stichtenoth and C.P. Xing, “On subfields of the Hermitian function field”, Compos. Math. **120** (2000), 137–170.

[29] A. Garcia and F. Torres“On unramified coverings of maximal curves”, Proceedings AGCT-10, to appear.

[30] A. Garcia and P. Viana, “Weierstrass points on certain non-classical curves”, Arch. Math. **46** (1986), 315–322.

[31] A. Garcia and J.F. Voloch, “Wronskians and linear independence in fields of prime characteristic”, Manuscripta Math. **59** (1987), 457–469.

[32] G. van der Geer, “Error-Correcting Codes and Curves over Finite Fields”, Mathematics Unlimited - 2001 and Beyond, Springer, 1115–1138, 2000.

[33] G. van der Geer and M. van der Vlugt, “An asymptotically good tower of curves over the finite field with eight elements”, Bull. London Math. **24** (2002), 291–300.

[34] G. van der Geer and M. van der Vlugt, “Tables of curves with many points”, Math. Comp. **69** (2000), 797–810. Updates of these tables are found in, Tables for the function $N_q(g)$, available from http://www.wins.uva.nl/ geer.

[35] M. Giulietti and G. Korchmáros, “A new family of $\mathbb{F}_{q^2}$-maximal curves”, preprint, 2007.

[36] D.M. Goldschmidt, “Algebraic Functions and Projective Curves”, Springer-Verlag, New York, 2003.

[37] V.D. Goppa, “Codes associated with divisors”, Problems of Information Transmition **I**, 1977.

[38] V.D. Goppa, “Geometry and Codes”, Mathematics and its applications, Vol. 24, Kluwer Academic Publisher, Dordrecht-Boston-London, 1988.
curves”, Regional Conference Series in Math.

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

[40] 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.

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

[42] R. Hartshorne, “Algebraic Geometry”, Grad. Texts in Math. Vol. 52, Springer-Verlag, New York/Berlin, 1977.

[43] H. Hasse and F.K. Schmidt, “Noch eine Begründung der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten; Zusatz bei der Korrektur”, J. Reine Angew. Math. **177** (1937), 215–237.

[44] A. Hefez, “Non reflexive curves”, Compos. Math. **69** (1989), 3–35.

[45] A. Hefez and J.F. Voloch, “Frobenius non classical curves”, Arch. Math. **54** (1990), 263–273.

[46] H.W. Henn, “Funktionenkörper mit gro$\beta$er Automorphismengruppe”, J. Reine Angew. Math. **302** (1978), 96–115.

[47] A. Hefez and J.F. Voloch, “”Frobenius non classical curves”, Arch. Math. **71** (1990), 263–273.

[48] J.P.W. Hirschfeld, “Projective Geometries Over Finite Spaces”, 2nd ed. Oxford University Press, Oxford,1998.

[49] J.W.P. Hirschfeld and G. Korchmáros, “On the embedding of an arc into a conic in a finite plane”, Finite Fields Appl. **2** (1996), 274–292.

[50] J.W.P. Hirschfeld and G. Korchmáros, "Arcs and curves over a finite field", Finite Fields Appl. **5** (1999), 393–408.

[51] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, "Algebraic Curves Over a Finite Field", Princenton University Press, Princenton and Oxford, 2008.

[52] T. Ibukiyama, "On rational points of curves of genus 3 over finite fields", Tôhuku Math. J. **45** (1993), 311–329.

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

[54] G. Korchmáros and F. Torres, "Embedding of a maximal curve in a Hermitian variety", Compos. Math. **128** (2001), 95–113.

[55] G. Korchmáros and F. Torres, "On the genus of a maximal curve", Math. Ann. **323**(3) (2002), 589–608.

[56] A. Kresch, J.L. Wetherell and M. Zieve, "Curves of every genus with many points, I: Abelian and toric families", J. Algebra **250** (2002), 353–370.

[57] G. Lachaud, "Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis", C.R. Acad. Sci. Paris **305** Série I (1987), 729–732.

[58] S. Lang, "Abelian Varieties", Interscience Pub., New York, 1950.

[59] K. Lauter, "Improved upper bounds for the number of rational points on algebraic curves over finite fields", C.R. Acad. Sci. Paris **328**(12) Série I (1999), 1181–1185.

[60] K. Lauter, "A formula for constructing curves over finite fields with many points", J. Number Theory **74** (1999), 56–72.

[61] K. Lauter, "Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points", Proc. Amer. Math. Soc. **128** (2000), 369–374.

[62] K. Lauter, "Zeta-functions of curves over finite fields with many rational points", Buchmann, Johannes (ed.) et al., Coding Theory, Cryptography and Related Areas. Proceedings of an international conference, Guanajuato, Mexico, April 1988. Berlin: Springer 167–174 (2000).

[63] K. Lauter (with an Appendix by J.P. Serre), "Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields", J. Alg. Geometry **10**(1) (2001), 19–36.

[64] K. Lauter, "The maximum or minimum number of rational points on curves of genus three over finite fields (with an appendix by J.P. Serre)", Compos. Math. **134** (2002), 87–111.

[65] E.W. Howe and K. Lauter, "Improved upper bounds for the number of points on curves over finite fields", Ann. Inst. Fourier **53**(6) (2003), 1677–1737.

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

[67] J.H. van Lint, "Introduction to Coding Theory", Springer-Verlag, third edition, 1999.

[68] J.H. van Lint and G. van der Geer, "Introduction to Coding Theory and Algebraic Geometry, Birkhäuser, 1988.

[69] J.S. Milne, Abelian Varieties, "Arithmetic Geometry" (G. Cornell and J.H. Silverman Eds.), 103–150, Springer-Verlag, New York, 1986.

[70] C. Moreno, "Algebraic curves over finite fields", Cambridge Tracts in Math. Vol. 97, Cambridge Univ. Press, Cambridge, 1991.

[71] D. Mumford, "Abelian Varieties", Tata Inst. Fund. Res., Oxford University Press, Bombay, 1994.

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

[73] N. Namba, "Geometry of projective algebraic curves", Marcel Dekkers INC, New York and Basel, 1984.

[74] H. Niederreited and C. Xing,“Towers of global function fields with asymptotically many rational places and an improvement of the Gilbert-Varshamov bound”, Math. Nachr. **195** (1998), 171–186.

[75] H. Niederreited and C. Xing,“Global function fields with many rational places and their applications”, Contemporary Math. **225** (1999), 87–111.

[76] H. Niederriter and C. Xing,“Rational Points on Curves over Finite Fields: Theory and Applications”, London Mathematical Society Lecture Notes, London Mathematical Society Lecture Note Series **285**, Cambridge Univ. Press, Cambridge, 2001.

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

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

[79] M.C. Rodriguez-Palánquex, “Arithmética de curvas quasihermíticas. Aplicaciones a los códigos geométricos de Goppa”, Ph.D. Thesis, UCM, 2000.

[80] M.C. Rodriguez-Palánquex, I.J. García-Villalba and L. Luengo-Velasco, “Computing the genus of a class of curves”, Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Lectures Notes in Comput. Sci. **2227**, Springer, Berlin, 2001.

[81] H.E. Rosen, “A course in Number Theory”, Clarendon Press - Oxford, 1988.

[82] H.G. Rück and H. Stichtenoth, “A characterization of Hermitian function fields over finite fields”, J. Reine Angew. Math. **457** (1994), 185–188.

[83] F.K. Schmidt, “Die Wronskisch Determinante in belebigen differenzierbaren Funktionenkörpern”, Math. Z. **45** (1939), 62–74.

[84] F.K. Schmidt, “Zur arithmetischen Theorie der algebraischen Funktionen II, Allgemeine Theorie der Weierstrasspunkte”,

[85] W. Scharlau and H. Opolka, “From Fermat to Minkowski: Lectures on the Theory of Numbers and Its Historical Development”, Springer-Verlag, New York, 1985.

[86] E.S. Selmer, “On the linear diophantine problem of Frobenius”, J. Reine Angew. Math. **293/294** (1977), 1–17.

[87] J.P. Serre, “Sur le nombre des points rationnels d’une courbe algébrique sur un corps fini”, C.R. Acad. Sci. Paris **296** Série I, (1983), 397–402. (Oeuvres III, 128, 658–663).

[88] J.P. Serre, “Rational points on curves over finite fields”, Notes by F. Gouvea of lectures at Harvard University, 1985.

[89] S.A. Stepanov, “Arithmetic of Algebraic Curves”, Monographs in Contemporary Mathematics, Consultans Bureau, New York - London, 1994.

[90] H. Stichtenoth, “Algebraic function fields and codes”, Springer-Verlag, Berlin, 1993.

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

[92] S. Tafazolian, “On Supersingular Curves Over Finite Fields”, Ph. D., IMPA. 2008.

[93] J. Tate, “Endomorphisms of abelian varieties over finite fields”, Invent. Math. **2** (1966), 134–144.

[94] J. Top, “Curves of genus 3 over small finite fields”, Indag. Mathem. N.S. **14**(2) (2003), 275–283.

[95] F. Torres, “Maximal curves over $\mathbb{F}_{64}$”, (2007), preprint.

[96] M.A. Tsfasman and S.G. Vlăduţ, “Algebraic-Geometric Codes”, Mathematics and its applications, Vol. 58, Kluwer Academic Publisher, Dordrecht-Boston-London, 1991.

[97] M.A. Tsfasman, S.G. Vlăduţ and T. Zink, “On Goppa codes which are better than the Varshamov-Gilbert bound”, Math. Nachr. **109** (1982), 21–28.

[98] S.G. Vlăduţ and V.G. Drinfeld, “Number of points of an algebraic curve”, Funct. Anal. **17**(1) (1983), 68–69.

[99] J.F. Voloch, “Arcs in projective planes over prime fields”, J. Geom. **38** (1990), 198–200.

[100] J.F. Voloch, "Complete arcs in Galois planes of non square order", Advances in Finite Geometries and Designs, (J.W.P. Hirschfeld et al., Eds.) Oxford Univ. Press, Oxford, 401–405, 1991.

[101] A. Weil, "Courbes Algébriques et Variétés Abeliennes", Hermann, Paris, 1971.

[102] A. Weil, *Number of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.

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

Institute of Mathematics, Statistics and Computer Science, P.O. Box 6065, University of Campinas, 13083-970, Campinas, SP, Brazil