The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs

Fernando Torres

THE APPROACH OF STÖHR-VOLOCH TO THE HASSE-WEIL BOUND WITH APPLICATIONS TO OPTIMAL CURVES AND PLANE ARCS

FERNANDO TORRES

Contens.

Introduction

The objective of this paper is to report applications of the approach of Stöhr-Voloch to the Hasse-Weil bound [99], to the investigation of the uniqueness of certain optimal curves, as well as to the search of upper bounds for the second largest size that a complete plane arc (in a projective plane of odd order) can have.

Author's address: IMECC-UNICAMP, Cx. P. 6065, Campinas, 13083-970-SP-Brazil.
ftorres@ime.unicamp.br.

Let $\mathcal{X}$ be a (projective, geometrically irreducible, non-singular algebraic) curve of genus g defined over a finite field $\mathbf{F}_q$ of q elements. Weil [108] showed that

$$(*) \qquad |\#\mathcal{X}(\mathbf{F}_q) - (q+1)| \leq 2\sqrt{q}g\,,$$

being this bound sharp as Example 4.4 here shows. Goppa [37] constructed linear codes from curves defined over $\mathbf{F}_q$. These codes were used by Tsfasman, Vladut and Zink [105] to show that the Gilbert-Varshamov bound can be improved whenever q is a square and $q \geq 49$. This was an unexpected result for coding theorist.

The length and the minimum distance of Goppa codes are related with the number of $\mathbf{F}_q$-rational points in the underlying curve. Then Goppa's construction provided motivation and in fact reawakened the interest in the study of rational points of curves which, despite of this motivation, is an interesting mathematical problem by its own.

Serre [93] noticed that $(*)$ can be improved by replacing $2\sqrt{q}$ by $\lfloor 2\sqrt{q} \rfloor$. A refined version of Ihara [58] shows that

$$g > \frac{q^2-q}{2\sqrt{q}^2 + 2\sqrt{q} - 2q} \quad \Rightarrow \quad \#\mathcal{X}(\mathbf{F}_q) < q + 1 + \lfloor 2\sqrt{q} \rfloor g\,,$$

and in this case Serre [93], [95] upper bounded $\#\mathcal{X}(\mathbf{F}_q)$ via explicit formulae.

A geometric point of view to bound $\#\mathcal{X}(\mathbf{F}_q)$ was introduced by Stöhr and Voloch [99]: Suppose that $\mathcal{X}$ admits a base-point-free linear series g^r_d defined over $\mathbf{F}_q$; then

$$\#\mathcal{X}(\mathbf{F}_q) \leq \frac{\sum_{i=0}^{r-1} \nu_i(2g-2) + (q+r)d}{r}\,,$$

where $\nu_0, \ldots, \nu_{r-1}$ are certain $\mathbf{F}_q$-invariants associated to g^r_d (see Theorem 3.13 here). By an appropriate choice of g^r_d this result implies $(*)$ [99, Cor. 2.14], and in several cases one obtains improvements on $(*)$. We write an exposition of Stöhr-Voloch's approach in Sect. 3. For the sake of completeness we include an expository account on Weierstrass point theory of linear series on curves: Sects. 1, 2.

Next we discuss two applications of [99] studied here. The first one is concerning the uniqueness of certain optimal curves. The most well known example of a $\mathbf{F}_q$-maximal curve is the *Hermitian curve* (Example 4.4 here) whose genus is $\sqrt{q}(\sqrt{q}-1)/2$; i.e., the biggest one that a $\mathbf{F}_q$-maximal curve can have according to the aforementioned Ihara's result. Rück and Stichtenoth [87] showed that this property characterize Hermitian curves up to $\mathbf{F}_q$-isomorphic. In Sect. 4.1 we equip the curve $\mathcal{X}$ with a linear series $\mathcal{D}_{\mathcal{X}}$ obtained from its Zeta Function provided that $\mathcal{X}(\mathbf{F}_q) \neq \emptyset$. It turns out that $\mathcal{D}_{\mathcal{X}} = |(\sqrt{q}+1)P_0|$, $P_0 \in \mathcal{X}(\mathbf{F}_q)$, whenever $\mathcal{X}$ is $\mathbf{F}_q$-maximal. Then applying [99] to $\mathcal{D}_{\mathcal{X}}$ we prove a stronger version of Rück-Stichtenoth's result; see Theorem 4.24 here. Further properties of $\mathbf{F}_q$-maximal were proved via an interplay of Stöhr-Voloch's paper [99], and results on linear series such as Castelnuovo's genus bound and Halphen's theorem applied to $\mathcal{D}_{\mathcal{X}}$; see [24], [26],[67],[68]. A characterization result is also proved

for the Suzuki curve (Theorem 4.27), which in fact is optimal with genus $q_0(q-1)$ and (q^2+1) $\mathbf{F}_q$-rational points.

The second application of [99] studied here is the bounding of the size k of a complete plane arc $\mathcal{K}$ in $\mathbf{P}^2(\mathbf{F}_q)$ which indeed is a basic problem in Finite Geometry. What it makes this possible is the fact that associated to $\mathcal{K}$ there is a (possible singular) plane curve $\mathcal{C}$. A fundamental result of B. Segre [90] (see Theorem 5.2 here for the odd case) allows then to upper bound k via [99] applied to certain linear series defined on the non-singular model of an irreducible component of $\mathcal{C}$. Details of the following discussion can be seen in Sect. 5. The largest k is already well known and so the problem is concerning the second largest size $m_2'(2,q)$. Let q be a square. If q is even, then $m'(2,q) = q - \sqrt{q} + 1$ and a similar result is expected for q odd, $q \geq 49$. Let q be odd. Applying $(*)$ B. Segre showed that $m'(2,q) \leq q - \sqrt{q}/4 + 7/4$. One obtains the same bound by using [99]; see Proposition 5.11 here. If in addition, for q large, one takes into consideration a bound for the number of $\mathbf{F}_q$-rational of plane curves due to Hirschfeld and Korchmáros [68] (see Theorem 5.24 here) one finds the currently best upper bound for $m'(2,q)$, namely

$$m'(2,q) \leq q - \frac{\sqrt{q}}{2} + \frac{5}{2}\,.$$

So far, for $\sqrt{q} \notin \mathbf{N}$, the best upper bound for $m'(2,q)$ is due to Voloch [106], [107]; see Lemmas 5.17, 5.19 here.

This paper is an outgrowth and a considerable expanded of lectures given at the University of Essen in April 1997 and the University of Perugia in February 1998.

Convention. The word *curve* will mean a projective, irreducible, non-singular algebraic curve.

1. Linear series on curves

The purpose of this section is to summarize relevant material regarding linear series on curves. Standard references are Arbarello-Cornalba-Griffiths-Harris [3], Griffiths [39], Griffiths-Harris [40], Hartshorne [45], Namba [79], Seidenberg [91], Stichtenoth [96].

Let $\mathcal{X}$ be a curve over an algebraically closed field $\mathbf{F}$; set $\mathbf{P}^r := \mathbf{P}^r(\mathbf{F})$.

1.1. Terminology and notation.

We start by fixing some terminology and notation.

1.1.1. We denote by $\mathrm{Div}(\mathcal{X})$ the group of *divisors* on $\mathcal{X}$; i.e., the $\mathbf{Z}$-free abelian group generated by the points of $\mathcal{X}$. Let $D = \sum n_P P \in \mathrm{Div}(\mathcal{X})$. The *multiplicity* of D at P is $v_P(D) := n_P$. The divisor D is called *effective* (notation: $D \succeq 0$) if $v_P(D) \geq 0$ for each P. For $D, E \in \mathrm{Div}(\mathcal{X})$, we write $D \succeq E$ if $D - E \succeq 0$. The *degree* of D is the number $\deg(D) := \sum v_P(D)$, and the *support* of D is the set $\mathrm{Supp}(D) := \{P \in X : v_P(D) \neq 0\}$.

1.1.2. Let $\mathbf{F}(\mathcal{X})$ denote the field of rational functions on $\mathcal{X}$. Associated to $f \in \mathbf{F}(\mathcal{X})^* := \mathbf{F}(\mathcal{X}) \setminus \{0\}$ we have the divisor

$$\mathrm{div}(f) := \sum v_P(f)P\,,$$

where v_P stands for the *valuation* at $P \in \mathcal{X}$. Recall that v_P satisfies: $v_P(0) := +\infty$, $v_P(f+g) \geq \min(v_P(f), v_P(g))$, and $v_P(fg) = v_P(f) + v_P(g)$ for $f, g \in \mathbf{F}(\mathcal{X})$.

For $f \in \mathbf{F}^* := \mathbf{F} \setminus \{0\}$, $\mathrm{div}(f) = 0$ and for $f \in \mathbf{F}(\mathcal{X}) \setminus \mathbf{F}$, $\mathrm{div}(f) = \mathrm{div}_0(f) - \mathrm{div}_\infty(f)$, where $\mathrm{div}_0(f) := \sum_{v_P(f)>0} v_P(f)P$ and $\mathrm{div}_\infty(f) := \sum_{v_P(f)<0}(-v_P(f))P$ are respectively the *zero* and the *polar* divisor of f. Moreover, $\deg(\mathrm{div}(f)) = 0$ and $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$.

Associated to $D \in \mathrm{Div}(\mathcal{X})$ we have the $\mathbf{F}$-linear space

$$L(D) := \{f \in \mathbf{F}(\mathcal{X})^* : D + \mathrm{div}(f) \succeq 0\} \cup \{0\}\,,$$

where $\ell(D) := \dim_{\mathbf{F}} L(D) \leq \deg(D) + 1$. For $D, E \in \mathrm{Div}(\mathcal{X})$ such that $L(D) \subseteq L(E)$, we have

$$\ell(E) - \ell(D) \leq \deg(E) - \deg(D)\,.$$

The Riemann-Roch theorem computes $\ell(D)$: If C is a canonical divisor on $\mathcal{X}$ and g is the genus of $\mathcal{X}$, then

$$\ell(D) = \deg(D) + 1 - g + \ell(C - D)\,.$$

In particular, C is characterized by the properties: $\deg(C) = 2g - 2$ and $\ell(C) \geq g$.

A *local parameter* at $P \in \mathcal{X}$ is a rational function $t \in \mathbf{F}(\mathcal{X})$ such that $v_P(t) = 1$. Associated to $f \in \mathbf{F}(\mathcal{X})^*$ we have its *local expansion at* P, $\sum_{i=v_P(f)}^{\infty} a_i t^i$, where $a_{v_P(f)} \neq 0$. Let $f \in \mathbf{F}(\mathcal{X})$ be a *separating variable of* $\mathbf{F}(\mathcal{X})|\mathbf{F}$; i.e., let the field extension $\mathbf{F}(\mathcal{X})|\mathbf{F}(f)$ be separable. Then we have the divisor of the *differential of* f, namely $\mathrm{div}(df)$ where $v_P(\mathrm{div}(df))$ equals the minimum integer i such that $ia_i \neq 0$. It holds that $\deg(\mathrm{div}(f)) = 2g - 2$.

1.1.3. Two divisors $D, E \in \mathrm{Div}(\mathcal{X})$ are called *linearly equivalent* (notation: $D \sim E$) if there exists $f \in \mathbf{F}(\mathcal{X})^*$ such that $D = E + \mathrm{div}(f)$. In this case, $\deg(D) = \deg(E)$ and $L(D)$ is $\mathbf{F}$-isomorphic to $L(E)$ via the map $g \mapsto fg$. For $E \in \mathrm{Div}(\mathcal{X})$, let

$$|E| := \{D \in \mathrm{Div}(\mathcal{X}) : D \succeq 0,\ D \sim E\}\,;$$

i.e.,

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

Since, for $f, g \in \mathbf{F}(X)^*$, $\mathrm{div}(f) = \mathrm{div}(g)$ if and only if there exists $a \in \mathbf{F}^*$ such that $f = ag$, the set $|E|$ is equipped with a structure of projective space by means of the map $E + \mathrm{div}(f) \in |E| \mapsto [f] \in \mathbf{P}(L(E))$; notation: $|E| \cong \mathbf{P}(L(E))$.

A *linear series* $\mathcal{D}$ on $\mathcal{X}$ is a subset of some $|E|$, of type

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

with $\mathcal{D}'$ being a $\mathbf{F}$-linear subspace of $L(E)$. The numbers $d = \deg(\mathcal{D}) := \deg(E)$ and $r = \dim(\mathcal{D}) := \dim_{\mathbf{F}}(\mathcal{D}') - 1$ are called respectively the *degree* and the (projective) *dimension* of $\mathcal{D}$. We say that $\mathcal{D}$ is a g^r_d on $\mathcal{X}$. $\mathcal{D}$ is called *complete* if $\mathcal{D} = |E|$. Observe that, under the identification $|E| \cong \mathbf{P}(L(E))$, $\mathcal{D}$ corresponds to $\mathbf{P}(\mathcal{D}')$; notation: $\mathcal{D} \cong \mathbf{P}(\mathcal{D}') \subseteq |E|$. A linear series $\mathcal{D}_1 \cong \mathbf{P}(\mathcal{D}'_1) \subseteq |E_1|$ will be called a *subspace* of $\mathcal{D} \cong \mathbf{P}(\mathcal{D}') \subseteq |E|$ if $L(E_1) \subseteq L(E)$ and $\mathcal{D}'_1 \subseteq \mathcal{D}'$.

1.1.4. Let $P \in \mathcal{X}$ and $f \in \mathbf{F}(\mathcal{X})$ *regular* at P; i.e., $v_P(f) \geq 0$. Then there exists a unique $a_f \in \mathbf{F}$ such that $v_P(f - a_f) > 0$. We set $f(P) := a_f$. For $f, g \in \mathbf{F}(\mathcal{X})$ regular at P, $(f+g)(P) = f(P) + g(P)$ and $(fg)(P) = f(P)g(P)$. A point of the r-projective space $\mathbf{P}^r$ will be denoted by $(a_0 : \cdots : a_r)$.

Let $\phi : \mathcal{X} \to \mathbf{P}^r$ be a morphism; i.e., let $f_0, \ldots, f_r \in \mathbf{F}(\mathcal{X})$, not all zero, such that

$$\phi(P) = ((t^{e_P} f_0)(P) : \ldots : (t^{e_P} f_r(P)) \,,$$

where t is a local parameter at P, and

$$e_P := -\min\{v_P(f_0), \ldots, v_P(f_r)\} \,.$$

Observe that each $t^{e_P} f_i$ is regular at P. The rational functions $f_0, \ldots, f_r$ are called (homogeneous) *coordinates* of ϕ. We set

$$\phi = (f_0 : \ldots : f_r) \,.$$

The coordinates $f_0, \ldots, f_r$ are uniquely determinated by ϕ up to a factor in $\mathbf{F}(\mathcal{X})^*$; so ϕ corresponds to a point of $\mathbf{P}^r(\mathbf{F}(\mathcal{X}))$. If ϕ is non-constant, the image $\phi(\mathcal{X})$ is a (possible singular) algebraic curve in $\mathbf{P}^r$ whose function field is $\mathbf{F}(\phi(\mathcal{X})) = \mathbf{F}(f_0, \ldots, f_r)$. The curve $\mathcal{X}$ can be thought as a parametrized curve in $\mathbf{P}^r$, or $\phi(\mathcal{X})$ as being a concrete manifestation of $\mathcal{X}$ in $\mathbf{P}^r$. For $Q \in \phi(\mathcal{X})$, the points of the fiber $\phi^{-1}(Q)$ will be called the *branches* of $\phi(\mathcal{X})$ centered at Q. The *degree* of ϕ is $\deg(\phi) := [\mathbf{F}(\mathcal{X}) : \mathbf{F}(\phi(\mathcal{X}))]$.

Example 1.1. Each rational function $f \in \mathbf{F}(\mathcal{X})$ can be seen as a morphism $f : \mathcal{X} \to \mathbf{P}^1 = \mathbf{F} \cup \{\infty\}$, such that $P \mapsto f(P)$ if $P \notin \mathrm{div}_\infty(f)$; $P \mapsto \infty$ otherwise. If $f \notin \mathbf{F}$, we have $d := \deg(f) = [\mathbf{F}(\mathcal{X}) : \mathbf{F}(f)] = \deg(\mathrm{div}_\infty(f))$. Moreover, if $\mathbf{F}(\mathcal{X})|\mathbf{F}(f)$ is separable, the genus g of $\mathcal{X}$ can be computed via the so-called Riemann-Hurwitz formula:

$$2g - 2 = d(-2) + \deg(R_f) \,,$$

where $R_f = \mathrm{div}(df) + 2\mathrm{div}_\infty(f)$ is the ramification divisor of f. If $\mathrm{char}(\mathbf{F})$ does not divide the ramification index e_P of P over $f(P)$, then $v_P(R_f) = e_P - 1$ otherwise $v_P(R_f) > e_P - 1$. We have the product formula

$$\sum_{P \in f^{-1}(f(P))} e_P = d \,.$$

For all but finitely many $Q \in \phi(\mathcal{X})$, $\#\phi^{-1}(Q)$ equals the separable degree of $\mathbf{F}(\mathcal{X})|\mathbf{F}(\phi(\mathcal{X}))$. ϕ is called *birational* (resp. *embedding*) if $\deg(\phi) = 1$ (resp. $\mathcal{X}$ is $\mathbf{F}$-isomorphic to $\phi(\mathcal{X})$); in both cases, $\mathcal{X}$ is a (the) non-singular model of $\phi(\mathcal{X})$.

Let H be a hyperplane in $\mathbf{P}^r$ such that $\phi(\mathcal{X}) \not\subseteq H$. Then $\#\phi(\mathcal{X}) \cap H$ is finite. To each $P \in \mathcal{X}$ one associates a number $I_P(H) = I(\phi(\mathcal{X}), H; P)$, called the *intersection multiplicity* of $\phi(\mathcal{X})$ and H at P, in such a way that $I_P = 0 \Leftrightarrow P \notin \phi(\mathcal{X}) \cap H$ and that $\sum I_P(H)$ is independent of H; i.e., if H' is another hyperplane in $\mathbf{P}^r$ such that $\phi(\mathcal{X}) \not\subseteq H'$, then $\sum I_P(H) = \sum I_P(H')$. This number is called the *degree* $\deg(\phi(\mathcal{X}))$ of $\phi(\mathcal{X})$. If $\phi(\mathcal{X}) \subseteq \mathbf{P}^2$, the degree of $\phi(\mathcal{X})$ equals the degree of the polynomial that defines $\phi(\mathcal{X})$.

A morphism $\phi : \mathcal{X} \to \mathbf{P}^r$ is called *non-degenerate* if $\phi(\mathcal{X}) \not\subseteq H$ for each hyperplane H in $\mathbf{P}^r$. A curve $\mathcal{X} \subseteq \mathbf{P}^r$ is called *non-degenerate* if the inclusion morphism $\mathcal{X} \hookrightarrow \mathbf{P}^r$ is so.

Lemma 1.2. *A morphism $\phi = (f_0 : \ldots : f_r) : \mathcal{X} \to \mathbf{P}^r$ is non-degenerate if and only if $f_0, \ldots, f_r$ are $\mathbf{F}$-linearly independent.*

Proof. There exists a hyperplane H in $\mathbf{P}^r$ such that $\phi(\mathcal{X}) \subseteq H$ if and only if there exist $a_0, \ldots, a_r \in \mathbf{F}$, not all zero, such that $\sum_i a_i f_i(P) = 0$ for all but finitely many $P \in \mathcal{X}$. The last condition is equivalent to $\sum_i a_i f_i = 0$, as a non-zero rational function has only finitely many zeros (cf. Sect. 1.1.2); now the result follows. □

For $V \subseteq \mathbf{F}(\mathcal{X})$, $\langle V \rangle$ stands for the $\mathbf{F}$-vector space in $\mathbf{F}(\mathcal{X})$ generated by V.

1.2. Morphisms from linear series; Castelnuovo's genus bound. Let $\mathcal{D}$ be a r-dimensional linear series on $\mathcal{X}$, say $\mathcal{D} \cong \mathbf{P}(\mathcal{D}') \subseteq |E|$. The following subsets will provide information on the geometry of $\mathcal{X}$.

Definition. For $P \in \mathcal{X}$ and $i \in \mathbf{N}_0$,

$$\mathcal{D}_i(P) := \{D \in \mathcal{D} : D \succeq iP\}\,.$$

Clearly $\mathcal{D}_i(P) \supseteq \mathcal{D}_{i+1}(P)$ and $\mathcal{D}_i(P) = \emptyset$ if $i > d$.

Lemma 1.3. (1) *$\mathcal{D}_i(P)$ is a linear series*;
(2) *$\mathcal{D}_i(P)$ is a subspace of $\mathcal{D}$*;
(3) $\dim(\mathcal{D}_i(P)) \leq \dim(\mathcal{D}_{i+1}(P)) + 1$.

Proof. Set $\mathcal{D}_j := \mathcal{D}_j(P)$ and let $f \in \mathcal{D}' \setminus \{0\}$. Then $E + \operatorname{div}(f) \in \mathcal{D}_i$ if and only if $v_P(E) + v_P(f) \geq i$; i.e., $\mathcal{D}_i \cong \mathbf{P}(\mathcal{D}'_i)$, where

$$\mathcal{D}'_i := \mathcal{D}' \cap L(E - iP)\,.$$

This shows parts (1) and (2). Now $\mathcal{D}'_i/\mathcal{D}'_{i+1}$ is $\mathbf{F}$-isomorphic to a $\mathbf{F}$-subspace of $\mathcal{L} := L(E - iP)/L(E - (i+1)P)$. Since $\dim_{\mathbf{F}} \mathcal{L} \leq 1$ (see Sect. 1.1.2), part (3) follows. □

Definition. The *multiplicity* of $\mathcal{D}$ at $P \in \mathcal{X}$ is defined by

$$b(P) := \min\{v_P(D) : D \in \mathcal{D}\}\,.$$

We have $b(P) > 0$ if and only if $P \in \mathrm{Supp}(D)$ for all $D \in \mathcal{D}$; so $b(P) \neq 0$ for finitely many $P \in X$. Consequently, we can define the effective divisor $B = B^{\mathcal{D}}$ on $\mathcal{X}$ by setting

$$v_P(B) := b(P)\,.$$

Definition. The divisor B is called the *base locus of* $\mathcal{D}$. A point $P \in \mathrm{Supp}(B)$ is called a *base point of* $\mathcal{D}$. If $B = 0$, $\mathcal{D}$ is called *base-point-free*.

Thus $\mathcal{D}$ is base-point-free if and only if for each $P \in \mathcal{X}$ there exists $f \in \mathcal{D}' \setminus \{0\}$ such that $v_P(E + \mathrm{div}(f)) = 0$. Now, since $D \succeq B$ for each $D \in \mathcal{D}$, $\mathcal{D}' \subseteq L(E - B)$ and

$$\mathcal{D}^B := \{D - B : D \in \mathcal{D}\} \subseteq |E - B|$$

is a subspace of $\mathcal{D}$ such that $\mathcal{D}^B \cong \mathbf{P}(\mathcal{D}') \subseteq |E - B|$. We have $B^{\mathcal{D}^B} = 0$; i.e., $\mathcal{D}^B$ is a $g^r_{d-\deg(B)}$ base-point-free on $\mathcal{X}$.

Lemma 1.4. *Let $\mathcal{D} \cong \mathbf{P}(\mathcal{D}') \subseteq |E|$ be a linear series, where $\mathcal{D}' = \langle f_0, \ldots, f_s\rangle$. Then E is determinated by $\mathcal{D}$; i.e,*

$$v_P(E) = b(P) - \min\{v_P(f_0), \ldots, v_P(f_s)\}\,.$$

Proof. Since $\mathcal{D}' \subseteq L(E - B)$, $v_P(E) - b(P) + v_P(f_i) \geq 0$ for each i and each P so that $v_P(E) \geq b(P) - \min\{v_P(f_0), \ldots, v_P(f_s)\}$. On other hand, as $\mathcal{D}^B$ is base-point-free, for each P there exists $(a_0 : \ldots : a_s) \in \mathbf{P}^s(\mathbf{F})$ such that $v_P(E - B + \mathrm{div}(\sum_i a_i f_i)) = 0$; now the result follows. □

Next we associate a morphism to $\mathcal{D}$. For $P \in \mathcal{X}$ we have $\mathcal{D} = \mathcal{D}_{b(P)}(P) \supsetneqq \mathcal{D}_{b(P)+1}(P)$, so that $\dim(\mathcal{D}_{b(P)+1}) = \dim(\mathcal{D}) - 1$ by Lemma 1.3. Thus we have the following map

$$\phi_{\mathcal{D}} :\ \mathcal{X} \to \mathcal{D}^* \cong \mathbf{P}(\mathcal{D}')^*\,, \qquad P \mapsto \mathcal{D}_{b(P)+1}\,.$$

Homogeneous coordinates of $\phi_{\mathcal{D}}$ are given as follows. Let $\{f_0, \ldots, f_r\}$ be a $\mathbf{F}$-base of $\mathcal{D}'$, t a local parameter at P, and $f \in \mathcal{D}' \setminus \{0\}$. Then $v_P(t^{v_P(E)-b(P)} f) \geq 0$ and

$$E + \mathrm{div}(f) \in \mathcal{D}_{b(P)+1} \ \Leftrightarrow\ v_P(t^{v_P(E)-b(P)} f) \geq 1 \ \Leftrightarrow\ (t^{v_P(E)-b(P)} f)(P) = 0\,.$$

Since $f = \sum_i a_i f_i$ with $(a_0 : \ldots : a_r) \in \mathbf{P}^r$, we have

$$\begin{aligned}\mathcal{D}_{b(P)+1} &\cong \{(a_0 : \ldots : a_r) \in \mathbf{P}^r : \sum_{i=0}^{r} (t^{v_P(E)-b(P)} f_i)(P) a_i = 0\} \in \mathbf{P}^{r*} \\ &\cong ((t^{v_P(E)-b(P)} f_0)(P) : \ldots : (t^{v_P(E)-b(P)} f_r)(P)) \in \mathbf{P}^r\,.\end{aligned}$$

Hence from Lemma 1.4 the morphism $\phi_{f_0,\ldots,f_r} := (f_0 : \ldots : f_r)$ gives a coordinate description of $\phi_{\mathcal{D}}$, and it will be referred as *a morphism associated to* $\mathcal{D}$. If $\phi_{g_0,\ldots,g_r}$ is another morphism associated to $\mathcal{D}$, then $\phi_{g_0,\ldots,g_r} = T \circ \phi_{f_0,\ldots,f_r}$, with $T \in \mathrm{Aut}(\mathbf{P}^r(\mathbf{F}))$; i.e., a morphism associated to $\mathcal{D}$ is uniquely determinated by $\mathcal{D}$, up to projective equivalence. Observe that $\phi_{\mathcal{D}}$ and $\phi_{\mathcal{D}^B}$ have the same coordinate description. We summarize the above discussion as follows.

Lemma 1.5. *Let $\mathcal{D} \cong \mathbf{P}(\mathcal{D}')$ be a r-dimensional linear series on $\mathcal{X}$. Each $\mathbf{F}$-base $f_0, \ldots, f_r$ of $\mathcal{D}'$ defines a non-degenerate morphism $\phi_{f_0,\ldots,f_r} = (f_0 : \ldots : f_r) : \mathcal{X} \to \mathbf{P}^r$. If $g_0, \ldots, g_r$ is another $\mathbf{F}$-base of $\mathcal{D}'$, then there exists $T \in \mathrm{Aut}(\mathbf{P}^r)$ such that $\phi_{g_0,\ldots,g_r} = T \circ \phi_{f_0,\ldots,f_r}$.*

At this point we recall Castelnuovo's genus bound. Let g be the genus of $\mathcal{X}$.

Definition. A linear series $\mathcal{D}$ is called *simple* if a (any) morphism associated to $\mathcal{D}$ is birational.

Let $\mathcal{D}$ be a simple g^r_d, $r \geq 2$, on $\mathcal{X}$. Let $d' := d - \deg(B^{\mathcal{D}})$, and let ϵ be the unique integer with $0 \leq \epsilon \leq r-2$ and $d' - 1 \equiv \epsilon \pmod{(r-1)}$. Define Castelnuovo's number $c_0(d', r)$ by

$$c_0(d', r) = \frac{d' - 1 - \epsilon}{2(r-1)}(d' - r + \epsilon)\,.$$

Lemma 1.6. (Castelnuovo's genus bound for curves in projective spaces, [10], [3, p. 116], [45, IV, Thm. 6.4], [86, Cor. 2.8])

$$g \leq c_0(d', r)\,.$$

Remark 1.7.

$$c_0(d', r) \leq \begin{cases} (d' - 1 - (r-1)/2)^2/2(r-1) & \text{for } r \text{ odd,} \\ (d' - 1 - (r-1)/2)^2 - 1/4)2/(r-1) & \text{for } r \text{ even.} \end{cases}$$

Remark 1.8. Any curve $\mathcal{X}$ of genus g admits a simple g^2_d (i.e., a birational plane model) such that

$$g = d(d-1)/2 - \sum_P \delta_P\,,$$

where the δ_P's are the δ-invariants of the plane curve $\phi(\mathcal{X})$ with ϕ being a morphism associated to g^2_d. We have that $\delta_P > 0$ if and only if $\phi(\mathcal{X})$ is singular at P. A nice method to compute δ_P was recently noticed by Beelen and Pellikaan [4].

1.3. Linear series from morphisms. Let $\phi = (f_0 : \ldots : f_r) : \mathcal{X} \to \mathbf{P}^r$ be a morphism on $\mathcal{X}$. In Sect. 1.1.4 we defined

$$e_P = -\min\{v_P(f_0), \ldots, v_P(f_r)\}\,, \qquad P \in \mathcal{X}\,.$$

Then $e_P \neq 0$ for finitely many $P \in \mathcal{X}$, and so we have a divisor $E = E_{f_0,\ldots,f_r}$ defined by

$$v_P(E) := e_P\,.$$

Observe that $f_i \in L(E)$ for each i. Let

$$\mathcal{D}' := \langle f_0, \ldots, f_r \rangle \subseteq L(E)\,.$$

Then we have the following linear series on $\mathcal{X}$

$$\mathcal{D}_{f_0,\ldots,f_r} := \{E + \mathrm{div}(f) : f \in \mathcal{D}' \setminus \{0\}\} \subseteq |E|\,,$$

which is base-point-free. Indeed, $v_P(E + \mathrm{div}(f_{i_0})) = 0$ where i_0 is defined by $e_P = -v_P(f_{i_0})$. In addition, if $\phi_1 = (g_0 : \ldots : g_r) = T \circ \phi$ with $T \in \mathrm{Aut}(\mathbf{P}^r)$, then

$$\min\{v_P(g_0), \ldots, v_P(g_r)\} = \min\{v_P(f_0), \ldots, v_P(f_r)\}\,,$$

and hence $\mathcal{D}_{g_0,\ldots,g_r} = \mathcal{D}_{f_0,\ldots,f_r}$. Moreover, if $h \in \mathbf{F}(\mathcal{X})^*$, then

$$E_{f_0h,\ldots,f_rh} = E_{f_0,\ldots,f_r} - \mathrm{div}(h)$$

and so

$$\mathcal{D}_{f_0h,\ldots,f_rh} = \mathcal{D}_{f_0,\ldots,f_r}\,.$$

Consequently, the linear series $\mathcal{D}_\phi := \mathcal{D}_{f_0,\ldots,f_r}$ is uniquely determinated by ϕ and it is invariant under projective equivalence of morphisms. Summarizing we have the following.

Lemma 1.9. *Associated to a morphism $\phi = (f_0 : \ldots : f_r) : X \to \mathbf{P}^r$, there exists a base-point-free linear series $\mathcal{D}_\phi \subseteq |E|$, where E is defined by*

$$v_P(E) := -\min\{v_P(f_0), \ldots, v_P(f_r)\}\,.$$

If ϕ is non-degenerate, then $\dim(\mathcal{D}_\phi) = r$. If $\phi_1 = T \circ \phi$, $T \in \mathrm{Aut}(\mathbf{P}^r)$, then $\mathcal{D}_{\phi_1} = \mathcal{D}_\phi$.

In the remaining part of this subsection, we let $\phi = (f_0 : \ldots : f_r)$ be a non-degenerate morphism on $\mathcal{X}$. Then $\mathcal{D}_\phi$ is given by

$$\mathcal{D}_\phi = \{E + \mathrm{div}(\sum_{i=0}^{r} a_i f_i) : (a_0 : \ldots : a_r) \in \mathbf{P}^r\}\,,$$

because $\sum_i a_i f_i = 0 \Leftrightarrow a_i = 0$ for each i by Lemma 1.2. Therefore, since the point $(a_0 : \ldots : a_r)$ can be identify with the hyperplane H of equation $\sum_i a_i X_i = 0$,

$$\mathcal{D}_\phi = \{\phi^*(H) : H \text{ hyperplane in } \mathbf{P}^r\}\,, \tag{1.1}$$

where $\phi^*(H) = E + \mathrm{div}(\sum_i a_i f_i)$ is the pull-back of H by ϕ.

Lemma 1.10. *We have $\phi^*(H) = (T \circ \phi)^*(T(H))$, where $T \in \mathrm{Aut}(\mathbf{P}^r)$ and H is a hyperplane in $\mathbf{P}^r$.*

Proof. The result follows from the facts that $E_\phi = E_{T\circ\phi}$ and that $T(H) : \sum_i b_i Y_i = 0$, where $(b_0, \ldots, b_r) = (a_0, \ldots, a_r)A^{-1}$, A being the matrix defining T and $H : \sum_i a_i X_i = 0$. □

Lemma 1.11. *With the aforementioned notation,*

(1) *$P \in \mathrm{Supp}(\phi^*(H)) \Leftrightarrow \phi(P) \in H$; i.e, $\mathrm{Supp}(\phi^*(H)) = \phi^{-1}(\phi(\mathcal{X}) \cap H)$;*
(2) *For $P_1 \in \phi^{-1}(\phi(P))$, $P_1 \in \mathrm{Supp}(\phi^*(H)) \Leftrightarrow \phi^{-1}(\phi(P)) \subseteq \mathrm{Supp}(\phi^*(H))$;*
(3) *$d := \deg(\mathcal{D}) = \deg(\phi)\deg(\phi(\mathcal{X}))$.*

Proof. Let t be a local parameter at $P \in \mathcal{X}$.

(1) The proof follows from the equivalences

$$P \in \mathrm{Supp}(\phi^*(H)) \Leftrightarrow v_P(\mathrm{div}(\sum_i a_i t^{e_P} f_i)) \geq 1 \Leftrightarrow (\sum_i a_i t^{e_P} f_i)(P) = 0\,.$$

(2) The implication ($\Leftarrow$) is trivial. ($\Rightarrow$): Let $P_2 \in \phi^{-1}(\phi(P))$. Then $\phi(P_1) = \phi(P_2)$ which belong to H by part (1). Thus, once again by (1) we conclude that $P_2 \in \mathrm{Supp}(\phi^*(H))$.

(3) Let H_1 be a hyperplane in $\mathbf{P}^r$ such that $\phi(\mathcal{X}) \cap H \cap H_1 = \emptyset$. Denote by h/h_1 the rational function on $\mathbf{P}^r$, obtained by dividing the equation of H by the one of H_1. Then we obtain a rational function on $\mathcal{X}$, namely $\varphi := (h/h_1) \circ \phi$ (i.e., the pull-back of h/h_1 by ϕ). The function h/h_1 is regular on $\mathbf{P}^r \setminus H_1$ and hence φ is regular on $\phi^{-1}(\mathbf{P}^r \setminus H_1)$. Moreover, by the election of H_1, we have that $v_P(\varphi) \geq 1 \Leftrightarrow \phi(P) \in H$ and therefore from part (1) we conclude that $v_P(\varphi) \geq 1 \Leftrightarrow P \in \mathrm{Supp}(\phi^*(H))$. From the definition of φ we even conclude that $\phi^*(H) = \mathrm{div}_0(\varphi)$.

Now suppose that $\phi(P) = Q \in \phi(\mathcal{X}) \cap H$ is non-singular; let u be a local parameter at Q and set $i_P := v_P(u)$ (the ramification index at P). By considering h/h_1 as a function on $\phi(\mathcal{X})$ we have $v_P(\phi^{-1}(H)) = v_P(\varphi) = i_P v_Q(h/h_1)$, and by the product formula we also have

$$\sum_{P \in \phi^{-1}(Q)} v_P(\phi^{-1}(H)) = \deg(\phi) v_Q(h/h_1)\,.$$

Now take H such that every point in $\phi(X) \cap H$ is non-singular (this is possible because $\phi(\mathcal{X})$ has a finite number of singular points and so we can apply Bertini's theorem). Then from the above equation,

$$d = \deg(\phi) \sum_{Q \in \phi(\mathcal{X}) \cap H} v_Q(h/h_1)\,.$$

It turns out that $v_Q(h/h_1) = I(\phi(\mathcal{X}), H; Q)$ (cf. [45, Ex.6.2]), and the result follows. □

From this lemma and its proof we obtain:

Corollary 1.12. *Let $\phi : \mathcal{X} \to \mathbf{P}^r$ be a non-degenerate morphism.*

(1) *If ϕ is birational; i.e.,* $\deg(\phi) = 1$, *then* $\deg(\mathcal{D}_\phi) = \deg(\phi(\mathcal{X}))$.
(2) *If $\mathcal{X} \subseteq \mathbf{P}^r$ and ϕ is the inclusion morphism, then*

$$\mathcal{D}_\phi = \{\mathcal{X} \cdot H : H \text{ hyperplane in } \mathbf{P}^r\}\,,$$

where $\mathcal{X} \cdot H = \sum_P I(\mathcal{X}, H; P)$ is the intersection divisor of $\mathcal{X}$ and H.

1.4. Relation between linear series and morphisms. Define the following sets:

- $\mathcal{L} = \mathcal{L}_r := \{\mathcal{D}^B : \mathcal{D} \text{ linear series with } \dim(\mathcal{D}) = r\}$;
- $\mathcal{M} = \mathcal{M}_r := \{\langle\phi\rangle : \phi : \mathcal{X} \to \mathbf{P}^r \text{ non-degenerate morphism}\}$, where $\langle\phi\rangle := \{T \circ \phi : T \in \mathrm{Aut}(\mathbf{P}^r)\}$ denotes the projective equivalent class of ϕ.

From Sects. 1.2 and 1.3 we have two maps, namely

$$M = M_r : \mathcal{L} \to \mathcal{M}; \qquad \mathcal{D}^B \mapsto \langle \text{coordinate representation of } \phi_{\mathcal{D}^B} \rangle\,,$$

and

$$L = L_r : \mathcal{M} \to \mathcal{L}; \qquad \langle\phi\rangle \mapsto \mathcal{D}_\phi\,.$$

We have $M \circ L = \mathrm{id}_{\mathcal{M}}$ by definition, and $L \circ M = \mathrm{id}_{\mathcal{L}}$ by Lemma 1.4. Therefore,

Lemma 1.13. *The set of base-point-free linear series of dimension r is equivalent to the set of projective equivalent class of non-degenerate morphism from $\mathcal{X}$ to $\mathbf{P}^r$.*

Remark 1.14. The fact that $(L \circ M)(\mathcal{D}^B) = \mathcal{D}^B$ means that

$$\mathcal{D}^B = \{\phi^*(H) : H \text{ hyperplane in } \mathbf{P}^r\} \subseteq |E - B|\,,$$

where $\phi : \mathcal{X} \to \mathbf{P}^r$ is the non-degenerate morphism determinated, up to an automorphism of $\mathbf{P}^r$, by a base of $\mathcal{D}'$.

1.5. Hermitian invariants; Weierstrass semigroups I. Let $\mathcal{D}$ be a g^r_d on $\mathcal{X}$, say $\mathcal{D} \cong \mathbf{P}(\mathcal{D}') \subseteq |E|$, and $P \in \mathcal{X}$. We continue the study of the linear series $\mathcal{D}_i(P)$ started in Sect. 1.2. Recall that $\mathcal{D}_i(P)' = \mathcal{D}' \cap L(E - iP)$ and that $\mathcal{D}_i(P) \supseteq \mathcal{D}_{i+1}(P)$.

Definition. A non-negative integer j is called a $(\mathcal{D}, P)$-*order* (or an *Hermitian P-invariant*), if $\mathcal{D}_j(P) \supsetneqq \mathcal{D}_{j+1}(P)$.

From Lemma 1.3, there exist $r+1$ $(\mathcal{D}, P)$-orders, say

$$j_0(P) = j_0^{\mathcal{D}}(P) < \ldots < j_r(P) = j_r^{\mathcal{D}}(P)\,.$$

For $i = 0, \ldots, r$,

$$j_i(P) = \min\{v_P(E) + v_P(f) : f \in \mathcal{D}_{j_i(P)}(P)'\}\,,$$

and thus $\mathcal{D}_{j_i}(P)$ is a g^{r-i}_d on $\mathcal{X}$.

Lemma 1.15. (Esteves-Homma [21, Lemma 1]) *For $P, Q \in \mathcal{X}$, $P \neq Q$,*

$$j_i(P) + j_{r-i}(Q) \leq d\,.$$

Proof. Since $\dim(\mathcal{D}_{j_i(P)}(P) \cap \mathcal{D}_{j_{r-i}(Q)}(Q)) \geq 0$, there exists $D \in \mathcal{D}_{j_i(P)}(P) \cap \mathcal{D}_{j_{r-i}(Q)}(Q)$ and the result follows. □

This result will be complemented by Corollary 2.14.

Remark 1.16. (i) Since $j_0(P)$ equals $b(P)$, $\mathcal{D}$ is base-point-free if and only if $j_0(P) = 0$ for each $P \in \mathcal{X}$. Moreover, j is a $(\mathcal{D}, P)$-order if and only if $j - b(P)$ is a $(\mathcal{D}^B, P)$-order.

(ii) $j_r(P) \leq d$ as $\mathcal{D}_i(P) = \emptyset$ for $i > d$.

(iii) Let $j \in \mathbf{N}_0$. From Lemma 1.3, the following statements are equivalent:

(1) j is a $(\mathcal{D}, P)$-order;
(2) $\exists\ D \in \mathcal{D}$ such that $v_P(D) = j$;
(3) $\exists\ f \in \mathcal{D}'$ such that $v_P(E) + v_P(f) = j$;
(4) $\exists\ f \in \mathcal{D}'$ such that $f \in L(E - jP) \setminus L(E - (j+1)P)$;
(5) $\dim_{\mathbf{F}}(\mathcal{D}'_j(P)) = \dim_{\mathbf{F}}(\mathcal{D}'_{j+1}(P)) + 1$;
(6) $\dim(\mathcal{D}_j(P)) = \dim(\mathcal{D}_{j+1}(P)) + 1$.

(iv) Let $\mathcal{D} = |E|$; i.e., $\mathcal{D}' = L(E)$, C a canonical divisor on $\mathcal{X}$, and $j \in \mathbf{N}_0$. From $\mathcal{D}'_j(P) = L(E - jP)$, the Riemann-Roch theorem, and part(iii)(5) above, the following statements are equivalent:

(1') j is a $(|E|, P)$-order;
(2') $\exists\ f \in L(E)$ such that $v_P(E) + v_P(f) = j$;
(3') $\exists\ f \in L(E - jP) \setminus L(E - (j+1)P)$;
(4') $L(C - E + (j+1)P) = L(C - E + jP)$;
(5') $\nexists\ f \in L(C - E + (j+1)P)$ such that $v_P(C - E) + v_P(f) = -(j+1)$.

Example 1.17. Let g be the genus of $\mathcal{X}$, and $\mathcal{D} := |E|$ with $d = \deg(E) \geq 2g$. For $P \in \mathcal{X}$, we compute some $(\mathcal{D}, P)$-orders. We have $j_i(P) = i$ for $0 \leq i \leq d - 2g$. Indeed for such an i, $\deg(C - E + (i+1)P) < 0$ and then Remark 1.16(iv(4')) is trivially satisfied. In particular, $\mathcal{D}$ is base-point-free.

Example 1.18. We claim that for a given sequence of non-negative integers $\ell_0 < \ldots < \ell_r$, there exists a curve $\mathcal{Y}$, a point $P_0 \in \mathcal{Y}$, and a linear series $\mathcal{F}$ on $\mathcal{Y}$ such that the sequence equals the $(\mathcal{F}, P_0)$-orders. Indeed, let $\mathcal{Y} := \mathbf{P}^1(\mathbf{F})$ and x a transcendental element over $\mathbf{F}$. Set $P_\infty := (0 : 1)$, and $P_a := (1 : a)$ for $a \in \mathbf{F}$. We assume $\mathrm{div}(x) = P_0 - P_\infty$, $v_{P_a}(x - a) = 1$ for $a \in \mathbf{F}$. Define

$$E := \ell_r P_\infty, \qquad \text{and} \qquad \mathcal{F}' := \langle x^{\ell_0}, \ldots, x^{\ell_r} \rangle \subseteq \mathbf{F}(x)\,.$$

Then $\mathcal{F} := \{E + \mathrm{div}(f) : f \in \mathcal{F}'\}$ is a $g^r_{\ell_r}$ on $\mathcal{Y}$. We have $E + \mathrm{div}(x^{\ell_i}) = \ell_i P_0 + (\ell_r - \ell_i) P_\infty$ and hence the $(\mathcal{F}, P_0)$-orders are $\ell_0, \ldots, \ell_r$. In addition, we have that $j_0^{\mathcal{F}}(P) = 0$ for $P \neq P_0$; i.e., the base locus of $\mathcal{F}$ is $B^{\mathcal{F}} = \ell_0 P_0$. Moreover, for the morphism associated to $\mathcal{F}$ $\phi = (x^{\ell_0} : \ldots : x^{\ell_r})$ we have $E_\phi = \ell_r P_\infty - \ell_0 P_0$. If $\ell_r = r$, then $\mathcal{F}$ is complete and base-point-free, and the curve $\phi(\mathcal{Y})$ is the so-called rational normal curve in $\mathbf{P}^r$. Conversely, if $\mathcal{F}$ is complete, say $\mathcal{F} = |E_1|$, then $E_1 = E$ by Lemma 1.4, and so $\ell = r$.

We will introduce next the so-called Weierstrass semigroup. To begin with we state a definition which is motivated by Remark 1.16(iv)(5').

Definition. Let $D \in \mathrm{Div}(\mathcal{X})$ and $\ell \in \mathbf{N}_0$. We say that ℓ is a (D,P)-*gap* if does not exist $f \in L(D+\ell P)$ such that $v_P(D) + v_P(f) = -\ell$.

We have that

$$\ell \text{ is a } (D,P)\text{-gap} \quad \text{if and only if} \quad \ell - 1 \text{ is a } (|C-D|,P)\text{-order}\,,$$

where C is a canonical divisor on $\mathcal{X}$. Denote by $\mathcal{K} = \mathcal{K}_{\mathcal{X}} := |C|$ the canonical linear series on $\mathcal{X}$.

Definition. The $(0,P)$-gaps are called the *Weierstrass gaps* at P. The *Weierstrass semigroup* at P is the set

$$H(P) := \mathbf{N}_0 \setminus G(P)\,,$$

where

$$G(P) := \{\ell \in \mathbf{Z}^+ : \ell \text{ Weierstrass gap at } P\}\,.$$

The elements of $H(P)$ are called *Weierstrass non-gaps* at P.

Lemma 1.19. *Let g be the genus of $\mathcal{X}$. Then*

(1) $\#G(P) = g$ *(Weierstrass gap theorem)*;
(2) *For $h \in \mathbf{N}_0$, the following statements are equivalent*:
  (i) $h \in H(P)$;
  (ii) $\exists\ f_h \in L(hP)$ such that $v_P(f_h) = -h$;
  (iii) $\exists\ f_h \in k(X)$ such that $\mathrm{div}_\infty(f_h) = hP$;
  (iv) $\ell(hP) = \ell((h-1)P) + 1$.

Proof. Since $\dim(\mathcal{K}) = g-1$ and

$$G(P) = \{j_0^{\mathcal{K}}(P)+1, \ldots, j_{g-1}^{\mathcal{K}}(P)+1\}\,,$$

part (1) follows. Remark 1.16(iv) implies part (2). □

We see now that $H(P)$ is indeed a semigroup.

Corollary 1.20. *The set $H(P)$ is a sub-semigroup of $(\mathbf{N}_0, +)$ such that*

$$H(P) \supseteq \{2g, 2g+1, 2g+2, \ldots\}\,,$$

where g is the genus of $\mathcal{X}$.

Proof. It follows from Lemma 1.19(2.(iii)) and $j_{g-1}^{\mathcal{K}}(P) \leq \deg(\mathcal{K}) = 2g-2$. □

Let $(n_i(P) : i = 0, 1, \ldots)$ denote the strictly increasing sequence that enumerates the Weierstrass semigroup $H(P)$. From Lemma 1.19(2)(iv), $\ell(n_i(P)P) = i+1$ and from Corollary 1.20, $n_i(P) = g+i$ for $i \geq g$.

Remark 1.21. For $g = 0$, $\mathcal{K} = \emptyset$ and hence $H(P) = \mathbf{N}_0$ for any $P \in \mathcal{X}$. If $g = 1$, then $\dim(\mathcal{K}) = 0$ and hence $H(P) = \{0, 2, 3, \ldots\}$ for any $P \in \mathcal{X}$.

Corollary 1.22. *If $\mathcal{X}$ is a curve of genus $g \geq 1$, then $\mathcal{K}$ is base-point-free.*

Proof. We have to show that $j_0(P) := j_0^{\mathcal{K}}(P) = 0$ for each $P \in \mathcal{X}$. Suppose that $j_0(P_0) \geq 1$ for some $P_0 \in \mathcal{X}$. Then $1 \in H(P_0)$ and hence $H(P_0) = \mathbf{N}_0$. This implies $g = 0$. □

Example 1.23. We consider complete linear series on $\mathcal{X}$ arising from Weierstrass non-gaps which will be useful for applications to optimal curves. Let $P \in \mathcal{X}$, set $n_i := n_i(P)$ and consider $\mathcal{D} := |n_r P|$. Then

(1) $\mathcal{D}$ is a $g^r_{n_r}$ base-point-free on $\mathcal{X}$;
(2) The $(\mathcal{D}, P)$-orders are $n_r - n_i$, $i = 0, \ldots, r$.

In fact, we already noticed that $\dim(\mathcal{D}) = r$; P cannot be a base point of $\mathcal{D}$ by Lemma 1.19(2)(iv); if $Q \neq P$, then $D := n_r P + \mathrm{div}(1) \in \mathcal{D}$ and $v_Q(D) = 0$. This prove (1). To see (2), let $f_i \in \mathbf{F}(\mathcal{X})$ such that $\mathrm{div}(f_i) = \mathrm{div}_0(f_i) - n_i P$; cf. Lemma 1.19(2)(iii). Then

$$n_r P + \mathrm{div}(f_i) = (n_r - n_i)P + \mathrm{div}_0(f_i)\,,$$

and the result follows.

Lemma 1.24. *Let $f \in \mathbf{F}(\mathcal{X})$ such that $\mathrm{div}_\infty(f) = n_1(P)P$. Then f is a separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$.*

Proof. If $\mathbf{F}(\mathcal{X})|\mathbf{F}(f)$ were not separable, then $f = g^p$, $g \in \mathbf{F}(\mathcal{X})$ by [96, Prop. III.9.2]. Then $n_1(P)/p$ would be a non-gap at P, a contradiction. □

By definition, a Weierstrass semigroup $H(P)$ belongs to the class of *numerical semigroup*; i.e., it is a sub-semigroup H of $(\mathbf{N}_0, +)$ whose complement in $\mathbf{N}_0$, $G(H) := \mathbf{N}_0 \setminus H$, is finite. For such a semigroup H, $g(H) := \#(\mathbf{N}_0 \setminus H)$ is called the *genus* of H. We let $(n_i(H) : i \in \mathbf{N})$ (resp. $(\ell_i(H) : i = 1, \ldots, g(H))$) denote the strictly increasing sequence that enumerates H (resp. $G(H)$). Clearly $n_i(H) = g(H) + i$ for $i \geq g(H)$, and $n_i(H) = 2i$ for $i = 1, \ldots, g(H)$ whenever $n_1(H) = 2$. H is called *hyperellitpic* if $2 \in H$ (note that $2 \in H$ if and only if $n_1(H) = 2$, whenever $g(H) \geq 1$). This definition is motivated by the so-called *hyperelliptic curves*, namely those curves admitting a g^1_2, or equivalently those admitting rational functions of degree two. Indeed, $\mathcal{X}$ is hyperelliptic if and only if there exists $P \in \mathcal{X}$ such that $2 \in H(P)$ (see Example 2.28).

Lemma 1.25. (Buchweitz [7, I.3], Oliveira [81, Thm. 1.1]) *If $n_1(H) \geq 3$, then $n_i(H) \geq 2i + 1$ for $i = 1, \ldots, g(H) - 2$. In particular, $n_{g-1}(H) \geq 2g(H) - 2$.*

The *weight* of H is $w(H) := \sum_{i=1}^{g(H)} (\ell_i(H) - i)$. It is easy to see that

$$w(H) = (3g(H)^2 + g(H))/2 - \sum_{i=1}^{g(H)} n_i(H)\,, \tag{1.2}$$

and that $w(H) = g(H)(g(H) - 1)/2$ if H is hyperelliptic. Now Lemma 1.25 and (1.2) imply:

Corollary 1.26. (1) $0 \leq w(H) \leq g(H)(g(H)-1)/2$;
(2) $w(H) = g(H)(g(H)-1)/2$ *if and only if* H *is hyperelliptic*;
(3) $w(H) \leq (g(H)^2 - 3g(H) + 4)/2$ *if* $n_1(H) \geq 3$.

Remark 1.27. (Kato [59]) If $n_1(H) \geq 3$, we indeed have $w(H) \leq g(H)(g(H)-1)/3$, for $g(H) = 3, 4, 6, 7, 9, 10$ and $w(H) \leq (g(H)^2 - 5g(H) + 10)/2$, otherwise.

Definition. A numerical semigroup H is called *Weierstrass* if there exist a curve $\mathcal{X}$ and a point $P \in \mathcal{X}$ such that H equals the Weierstrass semigroup $H(P)$ at P.

Remark 1.28. If H is Weierstrass, say $H = H(P)$ on a curve $\mathcal{X}$ of genus $g = g(H)$, then Lemma 1.25 follows from Castelnuovo's genus bound (Lemma 1.6): We want to show that $n_i := n_i(P) \geq 2i+1$ provided that $n_1 := n_1(P) \geq 3$ and $1 \leq i \leq g-2$. Let i be the least integer for which $n_i \leq 2i$. Then $i \geq 2$, $n_{i-1} = 2i-1$, and $n_i = 2i$. Thus $\mathcal{D} := |n_i P|$ is a simple $g^i_{n_i}$ on $\mathcal{X}$; therefore Castelnuovo's genus bound implies $g \leq i+1$, a contradiction.

A numerical semigroup H is Weierstrass if any of the following conditions hold:

- either $g(H) \leq 7$, or $g(H) = 8$ and $2n_1(H) > \ell_g(H)$; see Komeda [63];
- $n_1(H) \leq 5$; see Komeda [61], [64], Maclachlan [75, Thm. 4];
- either $w(H) \leq g(H)/2$ or $g(H)/2 < w(H) \leq g(H) - 1$ and $2n_1(H) > \ell_g(H)$; see Eisenbud-Harris [19], Komeda [62];

We remark that the underlying curve in these examples is defined over the complex numbers.

In 1893, Hurwitz [57] asked about the characterization of Weierstrass semigroups; see [8, p. 32] and [19, p. 499] for further historical information. Long after that, in 1980 Buchweitz (see Corollary 1.30) showed the existence of a non-Weierstrass semigroup as a consequence of the following.

Lemma 1.29. (Buchweitz's necessary condition, [8, p. 33]) *Let H be a numerical semigroup. For an integer $n \geq 2$, let $nG(H)$ be the set of all sums of n elements of $G(H)$. If H is Weierstrass, then*

$$\#nG(H) \leq (2n-1)(g(H)-1)\,. \tag{1.3}$$

Proof. We have that $g := g(H)$ is the genus of the underlying curve, say $\mathcal{X}$. For a canonical divisor C on $\mathcal{X}$, we observe that $\ell(nC) = (2n-1)(g-1)$ by the Riemann-Roch theorem. Let $\ell := \ell_1 + \ldots + \ell_n \in nG(H)$. From Remark 1.16(iv)(2'), there exists $f_i \in L(C)$ such that $v_P(C) + v_P(f_i) = \ell_i - 1$ for $i = 1, \ldots, n$. Then $f_\ell := f_1 \ldots f_n \in L(nC)$ and being the map $\ell \mapsto f_\ell$ injective, the result follows. □

Corollary 1.30. ([8, p. 31]) $\{1, \ldots, 12, 19, 21, 24, 25\}$ *is the set of gaps of a numerical semigroup H of genus 16 which is not Weierstrass.*

Proof. We apply the case $n = 2$ in Lemma 1.29. An easy computations shows that $2G(H) = [2, 50] \setminus \{39, 41, 47\}$. Then $\#2G(H) = 46 > 3g - 3 = 45$ and so H cannot be Weierstrass. □

In addition, Buchweitz (loc. cit.) showed that for every integer $n \geq 2$ there exist numerical semigroups which do not satisfy (1.3). Further examples of such semigroups were given in [104, Sect. 4.1] and Komeda [65]. On the other hand, what can we say about semigroups H that satisfy (1.3) for each $n \geq 2$? In fact, there exist at least two classes of such semigroups, namely *symmetric semigroups* (resp. *quasi-symmetric semigroups*); i.e., those H with $\ell(H) = 2g(H) - 1$ (resp. $\ell(H) = 2g(H) - 2$). Indeed, equality in (1.3) for each n characterize symmetric semigroups (see Oliveira [81, Thm. 1.5]), and Oliveira and Stöhr [82, Thm. 1.1] noticed that $\#nG(H) = (2n-1)(g-1)-(n-2)$ whenever H is quasi-symmetric. In 1993, Stöhr [103, Scholium 3.5] constructed symmetric semigroups which are not Weierstrass. Indeed, symmetric non-Weierstrass semigroups of any genus larger than 99 can be constructed (loc. cit.) by using the Buchweitz's semigroup (Corollary 1.30) as a building block. A similar result was obtained for quasi-symmetric semigroups [82, Thm. 5.1] and these examples were generalized in [104, Sect. 4.2]. We stress that any symmetric (resp. quasi-symmetric) semigroup is a Weierstrass semigroup on a Gorenstein (resp. reducible Gorenstein) curve; see [98] (resp. [82]).

Finally, we mention that Hurwitz's question for numerical semigroups that satisfy (1.3) for each $n \geq 2$ is currently an open problem.

2. Weierstrass point theory

In this section we study Weierstrass Point Theory of linear series on curves from Stöhr-Voloch's paper [99, §1]. Other references are Farkas-Kra [22, III.5], Homma [54, Sects. 1,2], Laksov [71], F.K. Schmidt [88], [89].

Let $\mathcal{X}$ be a curve over an algebraically closed field $\mathbf{F}$ of characteristic $p \geq 0$. Let $\mathcal{D}$ be a g^r_d on $\mathcal{X}$, say $\mathcal{D} \cong \mathbf{P}^r(\mathcal{D}') \subseteq |E|$.

In Sect. 1.5, to any point $P \in \mathcal{X}$ we have assigned a sequence of $(r + 1)$ integers, namely the $(\mathcal{D}, P)$-orders. Here we study the behaviour of such sequences for general points of $\mathcal{X}$; i.e, for points in an open Zariski subset of $\mathcal{X}$. In order to do that we use "wronskians" on $\mathcal{X}$; i.e., certain functions in $\mathbf{F}(\mathcal{X})$ defined via derivatives. To avoid restrictions on the characteristic p, we use Hasse derivatives.

2.1. Hasse derivatives. Let x be a trascendental element over $\mathbf{F}$. For $i, j \in \mathbf{N}_0$, set

$$D^i_x x^j := \binom{j}{i} x^{j-i},$$

and extend it $\mathbf{F}$-linearly on $\mathbf{F}[x]$. The $\mathbf{F}$-linear map D_x^i is called the *i-th Hasse derivative* on $\mathbf{F}[x]$. $i!\,D_x^i x^j$ is the usual i-th derivative $\frac{d^i}{dx^i}$, and $D_x^i \neq 0$, as $D_x^i x^i = 1$, but $\frac{d}{d^i x} = 0$ for $i \geq p > 0$.

Remark 2.1. For $f(x) \in \mathbf{F}[x]$, $D_x^i f(x)$ is the coefficient of u^i in the expansion of $f(x+u)$ as a polynomial in u.

The $\mathbf{F}$-linear maps D_x^i, $i \in \mathbf{N}_0$, satisfy the following four properties:

(H1) $D_x^0 = \mathrm{id}$;
(H2) $D_{x|\mathbf{F}}^i = 0$ for $i \geq 1$;
(H3) $D_x^i(fg) = \sum_{j=0}^i D_x^j f D_x^{i-j} g$ (Product Rule);
(H4) $D_x^i \circ D_x^j = \binom{i+j}{i} D_x^{i+j}$.

Properties (H1), (H2) and (H4) easily follow from the definition of D_x^i, while (H3) follows by comparing the coefficients of $(fg)(x+u)$ and $f(x+u)g(x+u)$.

Next one extends D_x^i to $\mathbf{F}(x)$ and then to each finite separable extension of $\mathbf{F}(x)$. This is done in just one way; moreover, the extended map remains $\mathbf{F}$-linear and still satisfies the four aforementioned properties. The extension on $\mathbf{F}(x)$ is constructed as follows. By (H1) and (H3) it is enough to define $D_x^i(1/f)$ for $i \geq 1$ and $f \neq 0$. From $f(1/f) = 1$, (H2) and (H3) one finds the following recursive formula:

$$\sum_{j=0}^{i} D_x^j(1/f) D_x^{i-j} f = 0\,.$$

For $i = 1$ one obtains the expected relation $D_x^1(1/f) = -(D_x^1 f)/f^2$, and in general [38, p. 119]

$$D_x^i(1/f) = \sum_{j=1}^{i} \frac{(-1)^j}{f^{j+1}} \sum_{i_1,\ldots,i_j \geq 1;\ i_1+\ldots+i_j=i} D_x^{i_1} f \ldots D_x^{i_j} f\,.$$

Remark 2.2. The maps D_x^i on $\mathbf{F}(x)$, $i \in \mathbf{N}_0$, are characterized by the following four properties:

(i) they are $\mathbf{F}$-linear;
(ii) they satisfy (H1) and (H3) above;
(iii) $D_x^1 x = 1$;
(iv) $D_x^i x = 0$ for $i \geq 2$.

To see this, let η_i, $i \in \mathbf{N}_0$, be maps on $\mathbf{F}(x)$ satisfying (i), (ii), (iii) and (iv). From the formula for $D_x^i(1/f)$ above, is enough to show that $\eta_i(x^j) = D_x^i x^j$ $(*)$ for $i, j \in \mathbf{N}_0$. Now, since the η_i's satisfy (H3), it follows [47, Lemma 3.11]

$$\eta_i(x^j) = j x^{j-1} \eta_i(x) + \sum_{\ell=2}^{j} \sum_{m=1}^{i-1} x^{j-\ell}(\eta_m(x))(\eta_{i-m}(x^{\ell-1}))\,, \tag{2.1}$$

and we obtain $(*)$ by induction on i and j.

Remark 2.3. The maps D^i_x, $i \in \mathbf{N}_0$, on $\mathbf{F}(x)$ have also a unique extension to the Laurent series $\mathbf{F}((x))$ which satisfy (H1), (H2), (H3), and (H4) above. One sets $D^i_x(\sum_j a_j x^j) := \sum_j \binom{j}{i} a_j x^{i-j}$, see [47, p. 12].

Next we extend D^i_x to a finite separable extension $\mathbf{K}|\mathbf{F}(x)$. Let $y \in \mathbf{K}$ be such that $\mathbf{K} = \mathbf{F}(x,y)$, and $F(x)[Y]$ the minimal polynomial of y over $\mathbf{F}(x)$. Then we define $D^i_x y^m$ by using $F(x,y) = 0$ and (2.1). For example, for $i = 1$ we obtain

$$F_Y(x,y) D^1_x y + \sum_j (D^1_x a_j(x)) y^j = 0\,, \tag{2.2}$$

so that $D^1_x y$ is well defined as $F_Y(x,y) \neq 0$. Notice that these extensions satisfy (H1), (H2), (H3) and (H4) above and depend on the element y. However, it is a matter of fact that the $\mathbf{F}$-linear maps D^i_x on $\mathbf{F}(x)$ admit a unique extension to $\mathbf{F}$-linear maps on $\mathbf{K}$ satisfying the aforementioned (H1), (H2), (H3), and (H4); see [46].

Therefore, $\mathbf{F}(\mathcal{X})$ is equipped with $\mathbf{F}$-linear maps D^i_x such that (H1), (H2), (H3) and (H4) above hold true, with x being a separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$. If y is another separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$, relations among the D^i_x's and the D^j_y's are given by the so called *chain rule*; see (2.3) and (2.4).

Remark 2.4. For $i \in \mathbf{N}_0$, let D^i be $\mathbf{F}$-linear maps on a $\mathbf{F}$-algebra $\mathbf{K}$ satisfying (H1), (H2), (H3) and (H4) above. From (H4),

$$i!\, D^i = (D^1)^i := D^1 \circ \ldots \circ D^1 \quad i \text{ times}\,,$$

so that each D^i is determinated by D^1 provided that $p = 0$. Suppose now $p > 0$.

Claim. Let $0 \leq a, b < p$, $\alpha,\ \beta \in \mathbf{N}$. Then

(1) $D^{ap^\alpha + bp^\beta} = D^{ap^\alpha} \circ D^{bp^\beta}$.
(2) $D^{ap^\alpha} = (D^{p^\alpha})^a / a!$.

Proof. The statements are consequence of (H4) and the following property of binomial numbers: if $i = \sum_\alpha a^\alpha p^\alpha$, $j = \sum_\alpha b^\alpha p^\alpha$ are the p-adic expansion of $i, j \in \mathbf{N}$, then $\binom{i}{j} = \prod_\alpha \binom{a_\alpha}{b_\alpha}$. □

Therefore in positive characteristic the D^i's are determinated by $D^1, D^p, D^{p^2}, \ldots$.

A $\mathbf{F}$-linear map D on $\mathbf{F}(\mathcal{X})$ satisfying $D(fg) = fD(g) + gD(f)$, is called a $\mathbf{F}$-*derivation* on $\mathbf{F}(\mathcal{X})$. For example, D^1_x is a derivation on $\mathbf{F}(\mathcal{X})$, where x is a separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$. From (2.1) follows that two $\mathbf{F}$-derivations δ_1 and δ_2 on $\mathbf{F}(\mathcal{X})$ are equal if $\delta_1(x) = \delta_2(x)$.

Now let y be another separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$. Since the $\mathbf{F}$-derivations $\delta_1 := D^1_y$ and $\delta_2 := D^1_y(x) D^1_x$ satisfy $\delta_1(x) = \delta_2(x)$, we obtain the usual chain rule, namely

$$D^1_y \;=\; D^1_y(x) D^1_x\,. \tag{2.3}$$

To generalize this relation to higher derivatives, let T be a trascendental element over $\mathbf{F}(\mathcal{X})$. The maps D_x^i and D_y^j can be read off from the homomorphisms of $\mathbf{F}$-algebras $\eta_x, \eta_y\colon \mathbf{F}(X) \to \mathbf{F}(X)[[T]]$ defined respectively by

$$\eta_x(f) := \sum_{i\geq 0} D_x^i(f)T^i\,, \quad \text{and} \quad \eta_y(f) := \sum_{i\geq 0} D_y^i(f)T^i\,.$$

Let $h : \mathbf{F}(\mathcal{X})[[T]] \to \mathbf{F}(\mathcal{X})[[T]]$ be the $\mathbf{F}$-homomorphism defined by $h_{|\mathbf{F}(\mathcal{X})} = \mathrm{id}_{|\mathbf{F}(\mathcal{X})}$ and $h(T) := \sum_{i\geq 1} D_y^i(x)T^i$. Since $D_y^1(x) \neq 0$ by (2.3), h is an automorphism of $\mathbf{F}(\mathcal{X})[[T]]$. Consider the $\mathbf{F}$-homomorphism $\eta : \mathbf{F}(X) \to \mathbf{F}(X)[[T]]$ given by $\eta := h^{-1} \circ \eta_y$. For $f \in \mathbf{F}(\mathcal{X})$, set $\eta(f) := \sum_{i\geq 0} \eta_i(f)T^i$. Then the maps η_i are $\mathbf{F}$-linear on $\mathbf{F}(\mathcal{X})$ and satisfy properties (H1) and (H3) above. Write $h(T) = TU$, $U = D_y^1(x) + D_y^2(x)T + \ldots$.

Claim. Let $i \in \mathbf{N}_0$ and $f \in \mathbf{F}(\mathcal{X})$. Then $\eta_0(f) = D_y^0(f)$ and for $i \geq 1$ the following holds

$$D_y^i(f) = \sum_{j=1}^{i} a_j \eta_j(f)\,,$$

where a_j is the coefficient of T^{i-j} in U^j. In particular, $a_1 = D_y^i(x)$, $a_i = (D_y^1 x)^i$.

Proof. Write $\eta_y = h \circ \eta$. The coefficient of T^i in $(h \circ \eta)(f)$ can be read off from $\sum_{j=0}^{i} a_j(f)(TU)^j$, and the claim follows. □

Then we have $\eta_1(x) = 1$ and $\eta_i(x) = 0$ for $i \geq 2$. Therefore from Remark 2.2, $\eta_i = D_x^i$ on $\mathbf{F}(x)$ and hence also on $\mathbf{F}(\mathcal{X})$. This implies the generalized chain rule:

$$\eta_y = h \circ \eta_x\,,$$

or equivalently

$$D_y^i = \sum_{j=1}^{i} f_j D_x^j\,, \qquad i = 1, 2 \ldots, \tag{2.4}$$

where $f_j \in \mathbf{F}(\{D_y^m(x) : m = 1, 2, \ldots\})$. Observe that $f_1 = D_y^i(x)$ and $f_i = (D_y^1 x)^i$.

Remark 2.5. We mention two further properties of Hasse derivatives regarding prime powers of rational functions. Let $f \in \mathbf{F}(\mathcal{X})$, x a separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$, and q a power of $p = \mathrm{char}(\mathbf{F}) > 0$. We have

(i) $D_x^i f^q = (D_x^{i/q} f)^q$ if q divides i, and $D_x^i f^q = 0$ otherwise;
(ii) ([46, Satz 10]) $\exists\ g \in \mathbf{F}(\mathcal{X})$ such that $f = g^q$ if and only if $D_x^i(f) = 0$ for $i = 1, \ldots, q-1$.

Definition. A *wronskian* on $\mathcal{X}$ is a rational function of type

$$W_{f_0,\ldots,f_r;x}^{\ell_0,\ldots,\ell_r} := \det((D_x^{\ell_i} f_j))\,,$$

where $\ell_0 < \ldots < \ell_r$ is a sequence of non-negative integers, x is a separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$, and $f_0, \ldots, f_r \in \mathbf{F}(\mathcal{X})$. We set

$$\mathcal{A}(f_0, \ldots, f_r; x) := \{(m_0, \ldots, m_r) \in \mathbf{N}_0^{r+1} : m_0 < \ldots < m_r;\ W_{f_0,\ldots,f_r;x}^{m_0,\ldots,m_r} \neq 0\}\,.$$

2.2. Order sequence; Ramification divisor. Let $P \in \mathcal{X}$ and t be a local parameter at P. Let

$$j_0 = j_0(P) < \ldots < j_r = j_r(P)$$

denote the $(\mathcal{D}, P)$-orders. From Remark 1.16(iii)(3) there exists $f_\ell \in \mathbf{F}(\mathcal{X})$ such that

$$v_P(t^{v_P(E)} f_\ell) = j_\ell\,, \qquad \ell = 0, \ldots, r\,.$$

Claim. $\{f_0, \ldots, f_r\}$ is a $\mathbf{F}$-base of $\mathcal{D}'$.

Proof. If there exists a non-trivial relation $\sum_i a_i f_i = 0$ with $a_i \in \mathbf{F}$, then we would have $v_P(f_i) = v_P(f_\ell)$ for $i \neq \ell$ and so $j_i = j_\ell$, a contradiction. □

Definition. The aforementioned $\mathbf{F}$-base $\{f_0, \ldots, f_r\}$ is called a $(\mathcal{D}, P)$-*base* (or $(\mathcal{D}, P)$-*Hermitian base*).

Remark 2.6. Let $\{f_0, \ldots, f_r\}$ be a $(\mathcal{D}, P)$-base. For $i = 0, \ldots, r$, $\mathcal{D}_i'(P) = \mathcal{D}' \cap L(E - j_i P)$ so that

$$\mathcal{D}_{j_i}'(P) = \langle f_i, \ldots, f_r \rangle\,,$$

or equivalently

$$\mathcal{D}_{j_i}(P) = \{E + \operatorname{div}(\sum_{\ell=i}^{r} a_\ell f_\ell) : (a_i : \ldots : a_r) \in \mathbf{P}^{r-i}(\mathbf{F})\}\,.$$

Thus

$$j_i(P) = \min\{v_P(\sum_{\ell=i}^{r} a_\ell f_\ell t^{v_P(E)}) : (a_i : \ldots : a_r) \in \mathbf{P}^{r-i}(\mathbf{F})\}\,.$$

Let $\{f_0, \ldots, f_r\}$ be a $(\mathcal{D}, P)$-base. Set $g_\ell := t^{v_P(E)} f_\ell$.

Lemma 2.7. *If $m_0 < \ldots < m_r$ is a sequence of non-negative integers such that $\det(\binom{j_\ell}{m_i}) \not\equiv 0 \pmod p$, then $(m_0, \ldots, m_r) \in \mathcal{A}(g_0, \ldots, g_r; t)$. In particular, $(j_0, \ldots, j_r) \in \mathcal{A}(g_0, \ldots, g_r; t)$.*

Proof. Let $g_\ell = \sum_{s=j_\ell}^{\infty} c_s^\ell t^s$, $c_{j_\ell}^\ell \neq 0$, be the local expansion of g_ℓ at P. Set $C := \prod_{\ell=0}^r c_{j_\ell}^\ell$. Then

$$\begin{aligned} W_{g_0,\ldots,g_r;t}^{m_0,\ldots,m_r} &= \det\Big(\sum_{s=j_\ell}^{\infty} \binom{s}{m_i} c_s^\ell t^{s-m_i}\Big) \\ &= Ct^{-\sum_i m_i} \det\Big(\sum_{s=j_\ell}^{\infty} \binom{s}{m_i} \frac{c_s^\ell}{c_{j_\ell}^\ell} t^s\Big) \\ &= C\det\Big(\binom{j_\ell}{m_i}\Big) t^{\sum_i (j_i - m_i)} + \ldots \neq 0\,, \end{aligned}$$

and the result follows. □

For $\ell \in \mathbf{N}_0$, set $D_x^\ell \phi := (D_x^\ell g_0, \ldots, D_x^\ell g_r)$. Since each coordinate of this vector is regular at P, we also set $D_x^\ell \phi(P) := (D_x^\ell g_0(P), \ldots, D_x^\ell g_r(P))$.

Then, for $0 \leq m_0 < \ldots < m_r$, $(m_0, \ldots, m_r) \in \mathcal{A}(g_0, \ldots, g_r; t)$ if and only if $D_t^{m_0}\phi, \ldots, D_t^{m_r}\phi$ are $\mathbf{F}(\mathcal{X})$-linearly independent.

Scholium 2.8. (1) *Set $j_{-1} := 0$. For $i = 0, \ldots, r$,*

$$j_i = j_i^{\mathcal{D}}(P) = \min\{s > j_{i-1} : (D_t^{j_0}\phi)(P), \ldots, (D_t^{j_{i-1}}\phi)(P), (D_t^s\phi)(P) \text{ are } \mathbf{F}\text{-l.i.}\}\,;$$

(2) *Let $m_0 < \ldots < m_{r'}$ be non-negative integers, with $r' \leq r$, such that the vectors $(D_t^{m_0}\phi)(P), \ldots, (D_t^{m_{r'}}\phi)(P)$ are $\mathbf{F}$-linearly independent. Then $j_i \leq m_i$ for $i = 0, \ldots, r'$.*

Proof. (1) From Lemma 2.7 and its proof, the vectors $(D_t^{j_0}\phi)(P), \ldots, (D_t^{j_i}\phi)(P)$ are $\mathbf{F}$-linearly independent and

$$D_t^{j_i} g_\ell(P) = \begin{cases} 0 & \text{if } \ell > i\,, \\ c_{j_\ell}^\ell & \text{if } \ell = i\,, \\ c_{j_i}^\ell & \text{if } \ell < i\,. \end{cases}$$

Let $j_{i-1} < s < j_i$. For $\ell = 0, \ldots, i-1$, we have vectors of type

$$(D_t^{j_\ell}\phi)(P) = (*, \ldots, *, c_{j_\ell}^\ell, 0, \ldots, 0)\,,$$

with $(r-\ell)$ zeros and where $*$ denotes an element of $\mathbf{F}$. Since the last $(r-i+1)$ entries of the vector $(D_t^s\phi)(P)$ are zeroes, (1) follows.

(2) From (1), $\dim_{\mathbf{F}}\langle\{(D^s\phi)(P) : s = 0, \ldots, j_i - 1\}\rangle = i$ so that $j_i - 1 < m_i$. □

In $\mathbf{Z}^{r+1}$ we have a partial order given by the so-called *lexicographic order* $<$. For $\alpha, \beta \in \mathbf{Z}^{r+1}$, $\alpha < \beta$ if in the vector $\beta - \alpha$ the left most non-zero entry is positive. This order is a well-ordering on $\mathbf{N}^{r+1}$, see e.g. [16, p. 55]. Let

$$\mathcal{E} := (\epsilon_0, \ldots, \epsilon_r)$$

be the minimum (in the lexicographic order) of $\mathcal{A}(g_0, \ldots, g_r; t)$.

Lemma 2.9. (1) $\epsilon_0 = 0$;

(2) $\epsilon_1 = 1$ *whenever* p *does not divide* $\deg(\mathcal{D}) - \deg(B^{\mathcal{D}})$;

(3) *For* $i = 1, \ldots, r$,

$$\epsilon_i = \min\{s > \epsilon_{i-1} : D_t^{\epsilon_0}\phi, \ldots, D_t^{\epsilon_{i-1}}\phi, D_t^s\phi \text{ are } \mathbf{F}(\mathcal{X})\text{-}l.i.\}\,.$$

Proof. (1) Suppose that $\epsilon_0 > 0$. Then $D_t^0\phi = \sum_{j=1}^r h_j D_t^{\epsilon_j}\phi$ with some $h_{j_0} \in \mathbf{F}(\mathcal{X})^*$, because $(0, \epsilon_1, \ldots, \epsilon_r) < \mathcal{E}$. Then we replace the row $D_t^{\epsilon_{j_0}}\phi$ by $D_t^0\phi$ in $W^{\epsilon_0,\ldots,\epsilon_r}_{g_0,\ldots,g_r;t}$ so that $(0, \epsilon_0, \ldots, \epsilon_{j_0-1}, \epsilon_{j_0+1}, \ldots, \epsilon_r) \in \mathcal{A}(g_0, \ldots, g_r; t)$, a contradiction to the minimality of $\mathcal{E}$.

(2) As in part (1) we have that $\epsilon_1 = 0$ if and only if $D_t^1 g_\ell = 0$ (or equivalently $D_t^i g_\ell = 0$ for $1 \le i < p$) for any $\ell = 0, \ldots, r$. Then each g_ℓ is a p-power by Remark 2.5(ii), and so p divides $v_P(E) - b(P)$ by Lemma 1.4; i.e., p divides $\deg(\mathcal{D}) - \deg(B^{\mathcal{D}})$.

(3) Clearly $D_t^{\epsilon_0}\phi, \ldots, D_t^{\epsilon_i}\phi$ are $\mathbf{F}(\mathcal{X})$-linearly independent. Let $\epsilon_{i-1} < s < \epsilon_i$. Since $(\epsilon_0, \ldots, \epsilon_{i-1}, s, \epsilon_{i+1}, \ldots, \epsilon_r) < \mathcal{E}$, there exists a relation of type

$$D_t^s\phi = \sum_{j=0}^{i-1} h_j D_t^{\epsilon_j}\phi + \sum_{j=i+1}^{r} h_j D_t^{\epsilon_j}\phi\,,$$

with $h_j \in \mathbf{F}(\mathcal{X})$. We claim that $h_j = 0$ for $j \ge i+1$. Indeed, suppose that $h_{j_0} \ne 0$ for some $j_0 \ge i+1$. Then by replacing $D_t^{\epsilon_{j_0}}\phi$ by $D_t^s\phi$ in $W^{\epsilon_0,\ldots,\epsilon_r}_{g_0,\ldots,g_r;t}$ we would have that $(\epsilon_0, \ldots, \epsilon_{i-1}, s, \epsilon_i, \ldots, \epsilon_{j_0-1}, \epsilon_{j_0+1}, \ldots, \epsilon_r) \in \mathcal{A}(g_0, \ldots, g_r; t)$, a contradiction to the minimality of $\mathcal{E}$. This finish the proof. □

Corollary 2.10. (1) *Let* $(m_0, \ldots, m_r) \in \mathcal{A}(g_0, \ldots, g_r; t)$. *Then for each* i, $\epsilon_i \le m_i$. *In particular,* $\epsilon_i \le j_i = j_i(P)$;

(2) *If* $0 \le m_0 < \ldots < m_r$ *are integers such that* $\det(\binom{j_i}{m_\ell}) \not\equiv 0 \pmod p$, *then* $\epsilon_i \le m_i$ *for each* i.

Proof. From Lemma 2.9,

$$\langle\{D_t^\ell\phi : \ell = 0, \ldots, \epsilon_i - 1\}\rangle = \langle\{D_t^{\epsilon_j}\phi : j = 0, \ldots, i-1\}\rangle\,. \tag{2.5}$$

If $\epsilon_i > m_i$, we would have

$$\dim_{\mathbf{F}(\mathcal{X})}(\{D_t^\ell\phi : \ell = 0, \ldots, \epsilon_i - 1\}) \ge \dim_{\mathbf{F}(\mathcal{X})}(\{D_t^{m_\ell}\phi : \ell = 0, \ldots, i\}) \ge i + 1\,,$$

a contradiction. This proves (1). Now (2) follows from Lemma 2.7 and (1). □

Proposition 2.11. (1) *If* $h_i = \sum a_{ij} g_j$ *with* $(a_{ij}) \in M_{r+1}(\mathbf{F})$, *then*

$$W^{\epsilon_0,\ldots,\epsilon_r}_{h_0,\ldots,h_r;t} = \det((a_{ij}))W^{\epsilon_0,\ldots,\epsilon_r}_{g_0,\ldots,g_r;t}\,;$$

(2) *If* $f \in \mathbf{F}(\mathcal{X})$, *then*

$$W^{\epsilon_0,\ldots,\epsilon_r}_{fg_0,\ldots,fg_r;t} = f^{r+1}W^{\epsilon_0,\ldots,\epsilon_r}_{g_0,\ldots,g_r;t}\,;$$

(3) *Let* x *be any separating variable of* $\mathbf{F}(\mathcal{X})|\mathbf{F}$. *Then*

$$W^{\epsilon_0,\ldots,\epsilon_r}_{g_0,\ldots,g_r;x} = (D_x^1 t)^{\sum_i \epsilon_i} W^{\epsilon_0,\ldots,\epsilon_r}_{g_0,\ldots,g_r;t}\,.$$

Proof. (1) It follows from $D_t^{\epsilon_\ell} h_i = \sum a_{ij} D_t^{\epsilon_\ell} g_j$. Note that this result does not depend on the minimality of $\mathcal{E}$.

(2) By the product rule (cf. Sect. 2.1), we have

$$D_t^{\epsilon_i}(fg_j) = \sum_{\ell=0}^{\epsilon_i} D_t^\ell f D_t^{\epsilon_i - \ell} g_j \,.$$

Then

$$(D_t^{\epsilon_i} fg_0, \ldots, D_t^{\epsilon_i} fg_r) = fD_t^{\epsilon_i}\phi + \sum_{\ell=1}^{\epsilon_i} D_t^\ell f D_t^{\epsilon_i-\ell}\phi \,.$$

By (2.5) we can factor out f in each row of $W^{\epsilon_0,\ldots,\epsilon_r}_{fg_0,\ldots,fg_r;t}$, and (2) follows.

(3) The proof is similar to (2) but here we use the chain rule (2.4) instead of the product rule. We have

$$D_x^{\epsilon_i} g_j = \sum_{\ell=1}^{\epsilon_i} f_\ell D_t^\ell g_j \,,$$

where $f_\ell \in \mathbf{F}(\mathcal{X})$ and $f_{\epsilon_i} = (D_x^1 t)^{\epsilon_i}$. Hence

$$D_x^{\epsilon_i}\phi = (D_x^1 t)^{\epsilon_i} D_t^{\epsilon_i}\phi + \sum_{\ell=1}^{\epsilon_i - 1} f_\ell D_t^\ell \phi \,,$$

and again by (2.5) we can factor out $(D_x^1 t)^{\epsilon_i}$ in each row of $W^{\epsilon_0,\ldots,\epsilon_r}_{g_0,\ldots,g_r;x}$. □

Now we see that $\mathcal{E}$ depends only on $\mathcal{D}$: Let $f_0', \ldots, f_r'$ be any $\mathbf{F}$-base of $\mathcal{D}'$ and x any separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$; since $g_\ell = t^{v_P(E)} f_\ell$, from Proposition 2.11(1)(2) $\mathcal{E}$ is the minimum for $\mathcal{A}(f_0', \ldots, f_r'; t)$. Moreover by part (3) of that proposition, $\mathcal{E}$ is also the minimum for $\mathcal{A}(g_0, \ldots, g_r; x)$. Finally, from part (2), $\mathcal{E}$ is also the minimum for $\mathcal{A}(f_0', \ldots, f_r'; x)$.

Definition. $\mathcal{E} = \mathcal{E}_\mathcal{D}$ is called the *order sequence* of $\mathcal{D}$. The *order sequence* of a morphism ϕ is the order sequence of $\mathcal{D}_\phi$.

Remark 2.12. Let $m_0 < \ldots < m_r$ be a sequence of non-negative integers such that $\det(\binom{j_\ell}{m_i}) \not\equiv 0 \pmod p$. Then $\epsilon_i \le m_i$ for each i by Corollary 2.10(2). We shall discuss the best election of the m_i's. In Example 1.18 we have seen that the $(\mathcal{D}, P)$-orders $j_0 < \ldots < j_r$ are the $(\mathcal{D}_\phi, P_0)$-orders for $\phi = (x^{j_0} : \ldots : x^{j_r}) : \mathbf{P}^1(\mathbf{F}) \to \mathbf{P}^{j_r}$ and $P_0 = (1:0)$. Observe that

$$W^{n_0,\ldots,n_r}_{x^{j_0},\ldots,x^{j_r};x} = \det\left(\binom{j_\ell}{n_i}\right) x^{\sum_i (j_i - n_i)} \,. \tag{2.6}$$

Let $\eta_0, \ldots, \eta_r$ be the $\mathcal{D}_\phi$-orders. Then

(1) $\det(\binom{j_i}{\eta_\ell}) \not\equiv 0 \pmod p$ by (2.6) with $n_i = \eta_i$, and the definition of $\mathcal{D}_\phi$-orders;
(2) $\eta_\ell \le m_\ell$ for each ℓ by (2.6) with $n_i = m_i$, and Corollary 2.8(2).

This shows that the best way to upper bound the ϵ_i's is by means of the sequence $\eta_0, \ldots, \eta_r$. In addition, from (2.6) and Lemma 2.9 applied to $\mathcal{D}_\phi$, we obtain the following.

Corollary 2.13. *Let $i \in \{0, \ldots, r\}$ and let $m_0 < \ldots < m_i$ be non-negative integers, such that the vectors $(\binom{j_0}{m_\ell}, \ldots, \binom{j_r}{m_\ell})$, $\ell = 0, \ldots, i$ are $\mathbf{F}_p$-linearly independent. Then $\epsilon_\ell \leq m_\ell$ for $\ell = 0, \ldots, i$.*

Corollary 2.14. (Esteves, [20])

$$\epsilon_i + j_\ell(P) \leq j_{i+\ell}(P)\,, \qquad i + \ell \leq r\,.$$

Proof. (Following Homma [56]) By means of suitable central projections [20, Lemma 2] one can assume that $i + \ell = r$. Let $\mathcal{D}_\phi$ be the linear series on $\mathbf{P}^1(\mathbf{F})$ in Remark 2.12, and $\eta_0, \ldots, \eta_r$ the $\mathcal{D}_\phi$-orders. By Example 1.18, $j_r - j_r, j_r - j_{r-1}, \ldots, j_r - j_0$ are the $(\mathcal{D}_\phi, (0:1))$-orders. Then, for each i, $j_r - j_{r-i} \geq \eta_i \geq \epsilon_i$ by Corollary 2.10(1) and Remark 2.12, and the result follows. □

Remark 2.15. Corollary 2.14 was first noticed by Homma [55] for $\mathcal{D}$-orders; see also [28] and [56].

Now we define the so-called ramification divisor of $\mathcal{D}$. Let $f_0', \ldots, f_r'$ be any base of $\mathcal{D}'$ and x any separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$. As before let $P \in \mathcal{X}$, t a local parameter at P, $\{f_0, \ldots, f_r\}$ a $(\mathcal{D}, P)$-base; set $g_\ell = t^{v_P(E)} f_\ell$. We have a matrix $(a_{ij}) \in GL(r+1, \mathbf{F})$ such that $f_i' = \sum_j a_{ij} f_j$ for each i. Proposition 2.11 implies

$$\begin{aligned} W^{\epsilon_0,\ldots,\epsilon_r}_{f_0',\ldots,f_r';x} &= \det(a_{ij}) W^{\epsilon_0,\ldots,\epsilon_r}_{f_0,\ldots,f_r;x} = \det(a_{ij}) t^{-(r+1)v_P(E)} W^{\epsilon_0,\ldots,\epsilon_r}_{g_0,\ldots,g_r;x} \\ &= \det(a_{ij}) t^{-(r+1)v_P(E)} (D^1_x t)^{\sum_i \epsilon_i} W^{\mathcal{E}}_{g_0,\ldots,g_r;t}\,; \end{aligned}$$

i.e.,

$$W^{\epsilon_0,\ldots,\epsilon_r}_{f_0',\ldots,f_r';x} (D^1_t x)^{\sum_i \epsilon_i} t^{(r+1)v_P(E)} = \det(a_{ij}) W^{\epsilon_0,\ldots,\epsilon_r}_{g_0,\ldots,g_r;t}\,. \tag{2.7}$$

Thus the divisor

$$R = R^{\mathcal{D}} := \mathrm{div}(W^{\epsilon_0,\ldots,\epsilon_r}_{f_0',\ldots,f_r';x}) + (\sum_{i=0}^{r} \epsilon_i)\mathrm{div}(dx) + (r+1)E\,,$$

just depends on $\mathcal{D}$ and locally is given by (2.7).

Definition. R is called the *ramification divisor* of $\mathcal{D}$. The *ramification divisor* of a morphism ϕ is the ramification divisor of $\mathcal{D}_\phi$.

Example 2.16. Let x be a separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$ and consider the morphism $\phi = (1:x) : \mathcal{X} \to \mathbf{P}^1(\mathbf{F})$. Then $E_\phi = \mathrm{div}_\infty(x)$; moreover, as $\#x^{-1}(x(P)) = \deg(\mathrm{div}_\infty(x))$ for infinitely many $P \in \mathcal{X}$, the $\mathcal{D}_\phi$-orders are 0,1. Then

$$R^{\mathcal{D}_\phi} = \mathrm{div}(dx) + 2\mathrm{div}_\infty(x)\,;$$

i.e., it coincides with the ramification divisor R_x of x, see Example 1.1.

Lemma 2.17. (Garcia-Voloch [33, Thm. 1]) *Let $\phi = (f_0 : \ldots : f_r)$ be a morphism associated to $\mathcal{D}$, and q' a power of* $\mathrm{char}(\mathbf{F}) > 0$. *Then $\epsilon_r \geq q'$ if and only if there exist $z_0, \ldots, z_r \in \mathbf{F}(\mathcal{X})$, not all zero, such that*

$$z_0^{q'} f_0 + \ldots + z_r^{q'} f_r = 0\,.$$

Corollary 2.18. *Let $P \in \mathcal{X}$. Under the hypothese of the previous lemma, there exist $i, \ell \in \{0, \ldots, r\}$, $i \neq \ell$, such that $j_i(P) \equiv j_\ell(P) \pmod{q'}$.*

Proof. We can assume that $f_0, \ldots . f_r$ is a $(\mathcal{D}, P)$-base. Now there exist $0 \leq i < \ell \leq r$ such that $v_P(z_i^{q'} f_i) = v_P(z_\ell^{q'} f_\ell)$ and the result follows. □

2.3. $\mathcal{D}$-Weierstrass points. Let us keep the notation of the previous subsection. Now we study R locally at P via (2.7); i.e., we study

$$v_P(R) = v_P(W_{g_0,\ldots,g_r;t}^{\epsilon_0,\ldots,\epsilon_r})\,.$$

We observe that $v_P(R) \geq 0$ since g_ℓ is regular at P for each ℓ.

Theorem 2.19. (1) $v_P(R) \geq \sum_{i=0}^r (j_i(P) - \epsilon_i)$;
(2) $v_P(R) = \sum_{i=0}^r (j_i(P) - \epsilon_i) \;\Leftrightarrow\; \det(\binom{j_\ell(P)}{\epsilon_i}) \not\equiv 0 \pmod{p}$.

Proof. Set $j_i := j_i(P)$. From the proof of Lemma 2.7 with $m_i = \epsilon_i$ we have a local expansion of type

$$W_{g_0,\ldots,g_r;t}^{\epsilon_0,\ldots,\epsilon_r} = C\det(\binom{j_\ell}{\epsilon_i}) t^{\sum_i (j_i - \epsilon_i)} + \ldots\,,$$

with $C \in \mathbf{F}^*$ and the result follows. □

We have already observed that R is an effective divisor which also follows from $j_i(P) \geq \epsilon_i$ (cf. Corollary 2.10(1)). Moreover, the following is clear from the theorem.

Corollary 2.20. *$v_P(R) = 0$ if and only if $j_i(P) = \epsilon_i$ for each i. In particular, for all but finitely many $P \in \mathcal{X}$, the $(\mathcal{D}, P)$-orders equal $\epsilon_0, \ldots, \epsilon_r$.*

Definition. The *$\mathcal{D}$-Weierstrass points* of $\mathcal{X}$ are those of $\mathrm{Supp}(R)$. The *$\mathcal{D}$-weight* of P is $v_P(R)$.

Thus the number of $\mathcal{D}$-Weierstrass points of $\mathcal{X}$, counted with their weighs, equals

$$\deg(R) = (\sum_{i=0}^r \epsilon_i)(2g-2) + (r+1)d\,.$$

Lemma 2.21. (p-adic criterion) *Let ϵ be a $\mathcal{D}$-order and let μ be an integer such that $\binom{\epsilon}{\mu} \not\equiv 0 \pmod{p}$. Then μ is also a $\mathcal{D}$-order. In particular, $0, 1, \ldots, \epsilon - 1$ are $\mathcal{D}$-orders provided that $p > \epsilon$.*

Proof. Let $\ell \in \{0, \ldots, r-1\}$ be such that $\epsilon_\ell < \mu \leq \epsilon_{\ell+1} \leq \epsilon$. We apply Corollary 2.13 to a point $P \notin \mathrm{Supp}(R)$; i.e., such that $j_i(P) = \epsilon_i$ for each i. Let $m_0 = \epsilon_0, \ldots, m_\ell = \epsilon_\ell, m_{\ell+1} := \mu$. Then the vectors $(\binom{\epsilon_0}{m_s}, \ldots, \binom{\epsilon_r}{m_s})$, $s = 0 \ldots, \ell+1$, are $\mathbf{F}_p$-linearly independent and the result follows. □

Definition. The curve $\mathcal{X}$ is called *classical with respect to* $\mathcal{D}$, or the linear series $\mathcal{D}$ is called *classical*, if the $\mathcal{D}$-orders are $0, \ldots, r$. A morphism ϕ is called *classical* if $\mathcal{D}_\phi$ is classical.

Lemma 2.22. *Suppose that* $\prod_{i>\ell} \frac{j_i(P)-j_\ell(P)}{i-\ell} \not\equiv 0 \pmod{p}$. *Then*

(1) $\mathcal{D}$ *is classical*;
(2) $v_P(R) = \sum_{i=0}^{r}(j_i(P) - i)$.

Proof. (1) Set $j_i = j_i(P)$. We have

$$\det(\binom{j_i}{\ell}) = \prod_{i>\ell} \frac{j_i - j_\ell}{i-\ell} \not\equiv 0 \pmod{p},$$

by hypothesis. Then $\epsilon_i \leq i$ by Corollary 2.10(2); i.e, $\epsilon_i = i$ for each i.

(2) Follows from Theorem 2.19(2). □

In particular, as $j_r(P) \leq d = \deg(\mathcal{D})$, we obtain:

Corollary 2.23. *If* $p = 0$ *or* $p > d = \deg(\mathcal{D})$, *then*

(1) $\mathcal{D}$ *is classical*;
(2) *For each* $P \in \mathcal{X}$, $v_P(R) = \sum_i (j_i(P) - i)$.

2.4. $\mathcal{D}$-osculating spaces. Assume that $\mathcal{D}$ is base-point-free, $\mathcal{D} = g^r_d \cong \mathbf{P}^r(\mathcal{D}') \subseteq |E|$. From Remark 1.14,

$$\mathcal{D} = \{\phi^*(H) : H \text{ hyperplane in } \mathbf{P}^r\},$$

where $\phi = (f_0 : \ldots : f_r)$, and where $\{f_0, \ldots, f_r\}$ is a $\mathbf{F}$-base of $\mathcal{D}'$. Let $P \in \mathcal{X}$ with $(\mathcal{D}, P)$-orders $j_0 < \ldots < j_r$. From Lemma 1.4,

$$v_P(E) = -\min\{v_P(f_0), \ldots, v_P(f_r)\}.$$

For $i = 0, \ldots, r-1$, let $L_i^{f_0,\ldots,f_r}(P)$ be the intersection of the hyperplanes H in $\mathbf{P}^r$ such that $v_P(\phi^*(H)) \geq j_{i+1}$. If $g_0, \ldots, g_r$ is another base of $\mathcal{D}'$, there exists $T \in \mathrm{Aut}(\mathbf{P}^r(\mathbf{F}))$ such that $\phi_1 := (g_0 : \ldots : g_r) = T \circ \phi$; thus

$$L_i^{g_0,\ldots,g_r}(P) = T(L_i^{f_0,\ldots,f_r}(P)). \tag{2.8}$$

We conclude then that $L_i^{f_0,\ldots,f_r}(P)$ is uniquely determinated by $\mathcal{D}$ up to projective equivalence.

Definition. $L_i(P) = L_i^{f_0,\ldots,f_r}(P)$ is called the *i-th osculating space* at P (with respect to the base $\{f_0, \ldots, f_r\}$).

Clearly we have:

$$L_0(P) \subseteq \ldots \subseteq L_{r-1}(P)\,.$$

Lemma 2.24. *$L_i^{f_0,\ldots,f_r}(P)$ is an i-dimensional space generated by the vectors $(D_t^{j_s}\phi')(P)$, $s = 0, \ldots, i$, where $\phi' = (t^{v_P(E)}f_0 : \ldots : t^{v_P(E)}f_r)$.*

Proof. From Lemma 1.10 and (2.8) we can assume that $f_0, \ldots, f_r$ is a $(\mathcal{D}, P)$-base. Let H_i be the hyperplane corresponding to $X_i = 0$, where $X_0, \ldots, X_r$ are homogeneous coordinates of $\mathbf{P}^r$. Let $H : \sum_i a_i X_i = 0$ be a hyperplane. Then $v_P(\phi^*(H)) \geq j_{i+1}$ if and only if $a_0 = \ldots a_i = 0$, since $v_P(t^{v_P(E)}f_\ell) = j_\ell$ for each ℓ. Thus

$$L_i^{f_0,\ldots,f_r}(P) = H_{i+1} \cap \ldots \cap H_r\,;$$

i.e., it has dimension i. In addition, it is generated by the vectors $(D_t^{j_s}\phi')(P)$ by the proof of Scholium 2.8 □

From the proof above we obtain:

Scholium 2.25. *$H \supseteq L_i(P)$ if and only if $v_P(\phi^*(H)) \geq j_{i+1}$.*

Remark 2.26. If $\mathcal{D}$ has base points, the i-osculating spaces for $\mathcal{D}$ are, by definition, those of $\mathcal{D}^B$.

Definition. The 1-osculating (resp. $(r-1)$-osculating) space at P is called the *tangent line* (resp. *osculating hyperplane*) at P.

A consequence of Lemma 2.24 is the following.

Corollary 2.27. *The osculating hyperplane at P (with respect to the base $\{f_0, \ldots, f_r\}$) is given by the equation*

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

where $g_\ell := t^{v_P(E)}f_\ell$, $\ell = 0, \ldots, r$.

2.5. Weierstrass points; Weierstrass semigroups II. In this sub-section we consider Weierstrass Point Theory for the canonical linear series $\mathcal{K} = \mathcal{K}^{\mathcal{X}}$ on the curve $\mathcal{X}$ of genus g. By Remark 1.21 we can assume $g \geq 2$. The special feature in the canonical case is the existence of a (numerical) semigroup, namely the Weierstrass semigroup $H(P)$ at $P \in \mathcal{X}$ (cf. Sect. 1.5) which is closely related to the $(\mathcal{K}, P)$-orders. We stress the following.

Definition. (1) The *Weierstrass points* of the curve $\mathcal{X}$ is the set $\mathcal{W} = \mathcal{W}_{\mathcal{X}}$ of its $\mathcal{K}$-Weierstrass points; i.e., $\mathcal{W} = \mathrm{Supp}(R^{\mathcal{K}})$. The $\mathcal{K}$-weight of P is called the *Weierstrass weight* ω_P of P; i.e., $\omega_P = v_P(R^{\mathcal{K}})$.

(2) We set $w_P := \sum_{i=0}^{g-1}(j_i^{\mathcal{K}}(P) - i)$; i.e., w_P is the weight of the Weierstrass semigroup $H(P)$ at P.

(3) The curve $\mathcal{X}$ is called *classical* if it is classical with respect to the canonical linear series $\mathcal{K}$.

In particular, since $\mathcal{K}$ has dimension $g-1$ and degree $2g-2$, the number of Weierstrass points $P \in \mathcal{W}$ counted with their weights ω_P equals

$$\deg(R^{\mathcal{K}}) = (\sum_{i=0}^{g-1} \epsilon_i)(2g-2) + g(2g-2)\,, \tag{2.9}$$

where $\epsilon_0 < \ldots < \epsilon_{g-1}$ are the $\mathcal{K}$-orders. From Theorem 2.19(1) we have

$$\omega_P \geq \sum_{i=0}^{g-1}(j_i^{\mathcal{K}}(P) - \epsilon_i)\,.$$

In general, $\omega_P > \sum_i (j_i^{\mathcal{K}}(P) - \epsilon_i)$ and $\omega_P \neq w_P$ (see Example 2.28); however, if either $p = 0$ or $p > 2g-2$, then the curve is classical and $\omega_P = \sum_i (j_i^{\mathcal{K}}(P) - i) = w_P$ by Corollary 2.23; in this case the curve has $g(g^2-1)$ Weierstrass points (counted with their weights) by (2.9).

Example 2.28. (Hyperelliptic curves) Let $\mathcal{X}$ be hyperelliptic with $g_2^1 = |\mathrm{div}_\infty(f)|$, $f \in \mathbf{F}(\mathcal{X})$ of degree two. Note that f is a separating variable since $g > 0$. We have $\mathcal{K} = |(g-1)\mathrm{div}_\infty(f)|$, where $\mathcal{K}'$ is generated by $1, f, \ldots, f^{g-1}$. Then $W^{0,1,\ldots,g-1}_{1,f,\ldots,f^{g-1};f} = 1$; i.e., $\mathcal{X}$ is classical.

The ramification divisor of $\mathcal{K}$ is thus

$$R^{\mathcal{K}} = \frac{g(g-1)}{2}\mathrm{div}(df) + g(g-1)\mathrm{div}_\infty(f)\,,$$

so that $R^{\mathcal{K}} = \frac{g(g-1)}{2}R_f$ by Example 2.16. Note that f has $\deg(R_f) = 2g+2$ ramifications points (counted with multiplicity), and that $P \in \mathrm{Supp}(R_f)$ if and only if $e_P = 2$; see Example 1.1. Therefore the following conditions are equivalent:

- $P \in \mathcal{W}$;
- $P \in \mathrm{Supp}(R_f)$;
- $e_P = 2$;
- $2 \in H(P)$;
- the $(\mathcal{K}, P)$-orders are $0, 2, \ldots, 2g-2$.

If $P \notin \mathcal{W}$, then the $(\mathcal{K}, P)$-orders are $0, 1, \ldots, g-1$; i.e., $H(P) = \{0, g+1, \ldots\}$. In particular, a hyperellitpic curve has only two types of Weierstrass semigroups.

If $p = 0$ or $p > 2$, and $P \in \mathrm{Supp}(R_f)$, then $v_P(R_f) = 1$ and hence $\mathcal{X}$ has $2g+2$ Weierstrass points P such that $\omega_P = g(g-1)/2$. In particular, here we have $\omega_P = \sum_i (j_i^{\mathcal{K}} - i) = w_P$ $(*)$.

If $p = 2$, then $(*)$ is in general not true as the following example shows. Let $\mathcal{X}$ be the non-singular model of the plane curve of equation

$$y^2 + y = x^{q+1},$$

over $\mathbf{F}$ of characteristic two, and where $q = 2^a$, $a \geq 2$. Then $x \in \mathbf{F}(\mathcal{X})$ has degree two an so $\mathcal{X}$ is hyperellitpic. There are two different points in $\mathcal{X}$ over each $a \in \mathbf{F}$, since $Y^2 + Y = a$ has two different solutions. Let P over $x = \infty$. Then $2v_P(y) = -(q+1)e_P$ so that $e_P = 2$; hence there is just one point P_∞ over $x = \infty$; i.e., $\#\mathrm{Supp}(R_x) = 1$. In particular, P_∞ is the only Weierstrass point of $\mathcal{X}$ and thus its weight is $\omega_P = \deg(R^{\mathcal{K}}) = g(g^2-1) > \sum_i (j_i^{\mathcal{K}}(P) - i) = w_P = g(g-1)/2$ because $g > 1$ as we see below.

To compute the genus of $\mathcal{X}$ we use the fact that P_∞ is the only ramified point for x: We have $2g - 2 = \deg(dx) = v_{P_\infty}(dx) = q - 2$ and so $g = q/2 > 1$.

Lemma 2.29. *Let $\mathcal{X}$ be a classical curve of genus g such that $\omega_P = w_P$ for each P (e.g. if $p = 0$ or $p > 2g-2$). Then*

(1) $2g + 2 \leq \#\mathcal{W} \leq g(g^2-1)$;
(2) $\#\mathcal{W} = 2g+2$ *if and only if $\mathcal{X}$ is hyperelliptic*;
(3) $\#\mathcal{W} = g(g^2-1)$ *if and only if $\omega_P = 1$ for any $P \in \mathcal{X}$.*

Proof. We have $g(g^2-1) = \deg(R^{\mathcal{K}}) = \sum_P w_P \leq \#\mathcal{W} g(g-1)/2$ by Corollary 1.26(1). This proves (1). (2) follows from Corollary 1.26(2)(3) and Example 2.28. (3) is trivial. □

Lemma 2.30. *Let $(\tilde{n}_i : i \in \mathbf{N})$ be the Weierstrass semigroup at non-Weierstrass points. Then $n_i(P) \leq \tilde{n}_i$ for each P and each i.*

Proof. Let i be the minimum positive integer such that $n_i(P) > \tilde{n}_i$. Then $i \geq 2$ and $n_{i-1}(P) \leq \tilde{n}_{i-1}$ so that $n_{i-1}(P) \leq \tilde{n}_{i-1} < \tilde{n}_i < n_i(P)$. Now we have $\tilde{n}_i = \ell_{\tilde{n}_i - i + 1} \geq \tilde{\ell}_{\tilde{n}_i - i + 1}$ by Corollary 2.10(1), where $\tilde{\ell}_1 < \tilde{\ell}_2 < \ldots$ are the gaps at non-Weierstrass points. Since $\ell_{\tilde{n}_i - i + 1} \geq \tilde{n}_i + 1$ we have a contradiction and the result follows. □

Lemma 2.31. *The largest $\mathcal{K}$-order ϵ_{g-1} is less than* $\deg(\mathcal{K}) = 2g - 2$.

Proof. (Garcia [27, p. 235]) Suppose $\epsilon_{g-1} = 2g-2$. Then for $P \notin \mathcal{W}$, $(2g-2)P$ is a canonical divisor. In particular, $(2g-2)P \sim (2g-2)P_0$ for $P, P_0 \notin \mathcal{W}$ $(*)$. We consider the isogeny $i : D \mapsto (2g-2)D$ on the Jacobian variety $\mathcal{J}$ associated to $\mathcal{X}$, and the natural map $\mathcal{X} \to \mathcal{J}$, $P \mapsto [P - P_0]$. Note that $[P - P_0] = [Q - P_0]$ if and only $P = Q$

since $g > 0$. Then $(*)$ says that there are infinitely points in $\mathcal{J}$ belonging to the kernel of i, a contradiction since this kernel is finite [77, p. 62]. □

Example 2.32. (The non-classical curve of genus 3) It is easy to see that the only semigroups of genus two are $\{0, 3, 4, 5, \ldots\}$ and $\{0, 2, 4, 5, \ldots\}$. Since a curve of genus two must have at least one Weierstrass points, then such a curve is hyperelliptic and hence classical.

Now let $\mathcal{X}$ be a curve of genus three. We shall show a result due to Komiya [66]: $\mathcal{X}$ is non-classical if and only if $p = 3$ and $\mathcal{X}$ is $\mathbf{F}$-isomorphic to the non-singular plane curve of equation $y^3 + y = x^4$. If $\mathcal{X}$ is non-classical, then $0 < p < 2g - 2 = 4$ by Corollary 2.23 so that $p = 2, 3$. We have $\epsilon_0 = 0, \epsilon_1 = 1$ and $\epsilon_2 = 3$. Then $p = 3$ by the 2-adic criterion. We have $P \in \mathcal{W} \Leftrightarrow j_0^{\mathcal{K}}(P) = 0, j_1^{\mathcal{K}}(P) = 1, j_2^{\mathcal{K}}(P) = 4 \Leftrightarrow H(P) = \{0, 3, 4, 6, \ldots\}$; then $\omega_P = 1$ and $\mathcal{X}$ has $\deg(R^{\mathcal{K}}) = 28$ Weierstrass points (note that a classical curve of genus 3 has $3 \times (3^2 - 1) = 24$ Weierstrass points counted with their weights). Let $P_0 \in \mathcal{W}, x, y \in \mathbf{F}(\mathcal{X})$ such that $\mathrm{div}_\infty(x) = 3P_0$ and $\mathrm{div}_\infty(y) = 4P_0$. We see that $4P_0$ is a canonical divisor and so $\mathcal{K} = |4P_0|$. We also see that x is a separating variable of $\mathbf{F}(\mathcal{X})|\mathbf{F}$ so that $W^{0,1,2}_{1,x,y;x} = D_x^2 y = 0$ as $\epsilon_2 > 2$. Now the eleven functions $1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, x^4, y^3$ belong to $L(12P_0)$ which has dimension 10. Therefore there is a non-trivial relation over $\mathbf{F}$ of type

$$a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{40}x^4 + a_{03}y^3 = 0\,.$$

Since $v_P(x^i y^j) < 12$ for $3i + 4j < 12$ we must have $a_{40} \neq 0$ and $a_{03} \neq 0$. In particular we can assume $a_{40} = 1$. Next we apply D_x^2 to the equation above; using the fact that $D_x^2 y = 0$ we find:

$$a_{20} + a_{11}D_xy + a_{02}(D_xy)^2 + a_{21}(y + 2xD_xy) + a_{12}(2xyD_xy + x(D_xy)^2) = 0\,.$$

Let $v_P(D_xy) = a$. Then the valuation at P of the functions

$$1, D_xy, (D_xy)^2, y, xD_xy, xyD_xy, x(D_xy)^2$$

are respectively

$$0, a, 2a, -4, -3 + a, -7 + a, -3 + 2a\,;$$

we see that they are pairwise different and hence $a_{20} = a_{11} = a_{02} = a_{21} = a_{12} = 0$; i.e., we have

$$a_{00} + a_{10}x + a_{01}y + a_{30}x^3 + x^4 + a_{03}y^3 = 0\,.$$

By means of $x \mapsto (x - a_{30})$ and $y \mapsto -(a_{03})^{1/3}y$ we can assume $a_{30} = 0$ and $a_{03} = -1$. Now as $[\mathbf{F}(\mathcal{X}) : \mathbf{F}(x)] = 3$ the above equation is irreducible and hence $a_{01} \neq 0$ because x is a separating variable. Then by means of $x \mapsto a_{01}^{3/8}x$ and $y \mapsto -a_{01}^{1/2}y$ we can assume $a_{01} = 1$. So we have an equation of type

$$y^3 + y = x^4 + a_{10}x + a_{00}\,.$$

Finally let P_1 be another Weierstrass point. Then $4P_1 \sim 4P_0$ as both divisor are canonical. So we can choose y such that $\mathrm{div}(y) = 4P_1 - 4P_0$. Then $4 = v_{P_1}(y) = v_{P_1}(x^4 + a_{10}x + a_{00})$ implies $a_{00} = a_{10} = 0$.

Conversely if $\mathcal{X}$ is defines by $y^3 + y = x^4$, we have that $\mathcal{X}$ is a non-singular plane curve of genus three. Moreover there is just one point P_∞ over $x = \infty$ and $H(P_\infty) = \{0, 3, 4, 6, \ldots\}$. This implies that x is a separating variable and we have $D_x^2 y = 0$; i.e., $\mathcal{X}$ is non-classical.

Further examples of non-classical linear series can be found in Neeman [80]. Finally we mention that Weierstrass Point Theory on schemes was considered by Laksov and Thorup [72]; see the introduction there for further references.

3. Frobenius orders

Let $\mathcal{X}$ be a curve defined over $\mathbf{F}_q$, a finite field with q elements; i.e., $\mathcal{X}$ is a curve over the algebraic closure $\bar{\mathbf{F}}_q$ of $\mathbf{F}_q$, equipped with the action of the Frobenius morphism $\mathbf{\Phi}_q$ relative to $\mathbf{F}_q$. Let $\mathcal{D} \cong \mathbf{P}(\mathcal{D}') \subseteq |E|$ be a base-point-free g^r_d on $\mathcal{X}$. Assume that $\mathcal{D}$ is also defined over $\mathbf{F}_q$; i.e., for any $D = \sum_P n_P P \in \mathcal{D}$, $(\mathbf{\Phi}_q)_*(D) := \sum_P n_P \mathbf{\Phi}_q(P) = D$. Let $\phi = (f_0 : \ldots : f_r)$ be a morphism over $\mathbf{F}_q$ associated to $\mathcal{D}$; i.e., its coordinates belong to $\mathbf{F}_q(\mathcal{X})$ and they form a $\mathbf{F}_q$-base of $\mathcal{D}'$.

The starting point of Stöhr-Voloch's approach to the Hasse-Weil bound is to look at points P of $\mathcal{X}$ such that $\phi(\mathbf{\Phi}_q(P))$ belongs to the osculating hyperplane $L_{r-1}^{f_0,\ldots,f_r}(P)$ at P. Then Corollary 2.27 leads to the consideration of rational functions of type

$$V^{\ell_0,\ldots,\ell_{r-1}}_{f_0,\ldots,f_r;x} := \det \begin{pmatrix} f_0 \circ \mathbf{\Phi}_q & \ldots & f_r \circ \mathbf{\Phi}_q \\ D_x^{\ell_0} f_0 & \ldots & D_x^{\ell_0} f_r \\ \vdots & \vdots & \vdots \\ D_x^{\ell_{r-1}} f_0 & \ldots & D_x^{\ell_{r-1}} f_r \end{pmatrix},$$

where x is a separating variable of $\bar{\mathbf{F}}_q(\mathcal{X})|\bar{\mathbf{F}}_q$. We set

$$\mathcal{B}(f_0, \ldots, f_r; x) := \{(m_0, \ldots, m_{r-1}) \in \mathbf{N}_0^r : m_0 < \ldots < m_{r-1};\ V^{m_0,\ldots,m_{r-1}}_{f_0,\ldots,f_r;x} \neq 0\}.$$

Lemma 3.1. *Let $(m_0, \ldots, m_r) \in \mathcal{A}(f_0, \ldots, f_r; x)$ with $m_0 = 0$. Then there exists $0 < I \leq r$ such that $(m_0, \ldots, m_{I-1}, m_{I+1}, \ldots, m_r) \in \mathcal{B}(f_0, \ldots, f_r; x)$.*

Proof. Let I be the smallest integer such that $\phi \circ \mathbf{\Phi}_q := (f_0 \circ \mathbf{\Phi}_q, \ldots, f_r \circ \mathbf{\Phi}_q)$ is a $\mathbf{F}(\mathcal{X})$-linear combination of $D_x^{m_0}\phi, \ldots, D_x^{m_I}\phi$. Since $f_0, \ldots, f_r$ is a $\mathbf{F}_q$-base of $\mathcal{D}'$, then $I > 0$ and the result follows. □

Since the $\mathcal{D}$-order sequence $(\epsilon_0, \ldots, \epsilon_r)$ belongs to $\mathcal{A}(f_0, \ldots, f_r; x)$ (cf. Proposition 2.11), $\mathcal{B}(f_0, \ldots, f_r; x) \neq \emptyset$. Let

$$\mathcal{V} := (\nu_0, \ldots, \nu_{r-1})$$

be the minimum (in the lexicographic order) of $\mathcal{B}(f_0,\dots,f_r;x)$.

Lemma 3.2. (1) $\nu_0 = 0$;

(2) *For* $i = 1,\dots,r-1$,

$$\nu_i = \min\{s > \nu_{i-1} : \phi\circ\mathbf{\Phi}_q, D_x^{\nu_0}\phi,\dots,D_x^{\nu_{i-1}}\phi, D_x^s\phi \text{ are } \bar{\mathbf{F}}_q(\mathcal{X})\text{-}l.i\}\ ;$$

(3) *Let* $(m_0,\dots,m_{r-1}) \in \mathcal{B}(f_0,\dots,f_r;x)$. *Then* $\nu_i \le m_i$ *for each* i.

Proof. Similar to the proofs of Lemma 2.9 and Corollary 2.10(1). □

Corollary 3.3. *There exists* $0 < I \le r$ *such that*

$$\nu_i = \begin{cases} \epsilon_i & \text{if } i < I, \\ \epsilon_{i+1} & \text{if } i \ge I. \end{cases}$$

Proof. From Proposition 2.11(3) and Lemma 3.1, there exists $0 < I \le r$ such that $(\epsilon_0,\dots,\epsilon_{I-1},\epsilon_{I+1},\dots,\epsilon_r) \in \mathcal{B}(f_0,\dots,f_r;x)$. Hence from Lemma 3.2, $\nu_i \le \epsilon_i$ for $i < I$ and $\nu_i \le \epsilon_{i+1}$ for $i \ge I$. Since $D_x^{\nu_0}\phi,\dots,D_x^{\nu_{I-1}}\phi$ are $\mathbf{F}(\mathcal{X})$-l.i, from Lemma 2.9(3) follows that $\epsilon_i \le \nu_i$ for $i = 0,\dots,I-1$; thus $\nu_i = \epsilon_i$ for $i = 0,\dots,I-1$. The same argument yields $\epsilon_I \le \nu_I$; in fact, $\epsilon_I < \nu_I$ by the definition of I in the proof of Lemma 3.1. Suppose that $\nu_I < \epsilon_{I+1}$. Then by Lemma 2.9(3) the vectors $D_x^{\nu_0}\phi,\dots,D_x^{\nu_{I-1}}\phi, D_x^{\epsilon_I}\phi, D_x^{\nu_I}\phi$ would be linearly dependent over $\mathbf{F}(\mathcal{X})$ so that $D^{\nu_I} \in \langle D_x^{\nu_0}\phi,\dots,D_x^{\nu_{I-1}}\phi, D_x^{\epsilon_I}\phi\rangle$. This is a contradiction because $\phi\circ\mathbf{\Phi}_q, D_x^{\nu_0}\phi,\dots,D_x^{\nu_{I-1}}\phi, D_x^{\nu_I}\phi$ are $\bar{\mathbf{F}}_q(\mathcal{X})$-linearly independent. A similar argument shows that $\nu_i = \epsilon_{i+1}$ if $i > I$. □

We remark the following computation regarding change of basis. Let $g_i = \sum a_{ij} f_j$ with $(a_{ij}) \in M_{r+1}(\bar{\mathbf{F}}_q)$. Then

$$\det\begin{pmatrix} \tilde{g}_0 & \dots & \tilde{g}_r \\ D_x^{\ell_0} g_0 & \dots & D_x^{\ell_0} g_r \\ \vdots & \vdots & \vdots \\ D_x^{\ell_{r-1}} g_0 & \dots & D_x^{\ell_{r-1}} g_r \end{pmatrix} = \det(a_{ij}) V_{f_0,\dots,f_r;x}^{\ell_0,\dots,\ell_{r-1}}\ , \tag{3.1}$$

where $\tilde{g}_j = \sum_i a_{ij} f_i \circ \mathbf{\Phi}_q$. The following is analogous to Proposition 2.11.

Proposition 3.4. (1) *If* $g_i = \sum_j a_{ij} f_j$ *with* $(a_{ij}) \in M_{r+1}(\mathbf{F}_q)$, *then*

$$V_{g_0,\dots,g_r;x}^{\nu_0,\dots,\nu_{r-1}} = \det((a_{ij})) V_{f_0,\dots,f_r;x}^{\nu_0,\dots,\nu_{r-1}}\ ;$$

(2) *If* $f \in \bar{\mathbf{F}}_q(\mathcal{X})$, *then*

$$V_{ff_0,\dots,ff_r;x}^{\nu_0,\dots,\nu_{r-1}} = f^{q+r} V_{f_0,\dots,f_r;x}^{\nu_0,\dots,\nu_{r-1}}\ ;$$

(3) *Let* y *be any separating variable of* $\bar{\mathbf{F}}_q(\mathcal{X})|\bar{\mathbf{F}}_q$. *Then*

$$V_{f_0,\dots,f_r;y}^{\nu_0,\dots,\nu_{r-1}} = (D_y^1 x)^{\sum_i \nu_i} V_{f_0,\dots,f_r;x}^{\nu_0,\dots,\nu_{r-1}}\ .$$

Proof. (1) follows from (3.1) taking into consideration that $a_{ij}^q = a_{ij}$. (2) and (3) follow as in Proposition 2.11. □

Now we show that $\mathcal{V}$ just depend on $\mathcal{D}$ and q. Let $\{f_0', \dots, f_r'\} \subseteq \mathbf{F}_q(\mathcal{X}$ be another $\mathbf{F}_q$-base of $\mathcal{D}'$ and y another separating variable of $\bar{\mathbf{F}}_q(\mathcal{X})|\bar{\mathbf{F}}_q$. From part (1) above, $\mathcal{V}$ is the minimum for $\mathcal{B}(f_0', \dots, f_r'; x)$ and from part (3) it is also the minimum for $\mathcal{B}(f_0', \dots, f_r'; y)$.

Definition. $\mathcal{V} = (\nu_0, \dots, \nu_{r-1})$ is called the $\mathbf{F}_q$-*Frobenius orders* of $\mathcal{D}$. If $\nu_i = i$ for each i, $\mathcal{D}$ is called $\mathbf{F}_q$-*Frobenius classical*.

Now let $P \in \mathcal{X}$. We have that $v_P(E) = -\min(v_P(f_0), \dots, v_P(f_r))$ because $\mathcal{D}$ is base-point-free, cf. Lemma 1.4. In addition, the rational functions $g_i := t^{v_P(E)} f_i$ are regular at P for each i, where t is a local parameter at P. Let $\{f_0', \dots, f_r'\}$ and y be as above. Let $f_i' = \sum_j a_{ij} f_j$, $a_{ij} \in \mathbf{F}_q$. Applying Proposition 3.4 we have

$$\begin{aligned} V^{\nu_0,\dots,\nu_{r-1}}_{f_0',\dots,f_r';y} &= \det(a_{ij}) V^{\nu_0,\dots,\nu_{r-1}}_{f_0,\dots,f_r;y} \\ &= \det(a_{ij})(D^1_y t)^{\sum_i \nu_i} V^{\nu_0,\dots,\nu_{r-1}}_{f_0,\dots,f_r;t} \\ &= \det(a_{ij})(D^1_y t)^{\sum_i \nu_i} t^{-(q+r)v_P(E)} V^{\nu_0,\dots,\nu_{r-1}}_{g_0,\dots,g_r;t} ; \end{aligned}$$

i.e.,

$$V^{\nu_0,\dots,\nu_{r-1}}_{f_0',\dots,f_r';y} (\frac{dy}{dt})^{\sum_i \nu_i} t^{(q+r)v_P(E)} = \det(a_{ij}) V^{\nu_0,\dots,\nu_{r-1}}_{g_0,\dots,g_r;t} . \tag{3.2}$$

Therefore the divisor

$$S = S^{\mathcal{D},q} := \operatorname{div}(V^{\nu_0,\dots,\nu_{r-1}}_{f_0',\dots,f_r';y}) + (\sum_{i=0}^{r-1} \nu_i)\operatorname{div}(dy) + (q+r)E ,$$

just depend on $\mathcal{D}$ and q and locally at P is given by (3.2).

Definition. S is called the $\mathbf{F}_q$-*Frobenius divisor* of $\mathcal{D}$.

The divisor S is effective because, as we already noticed, each g_ℓ is regular at P. Note that

$$\deg(S) = (\sum_{i=0}^{r-1} \nu_i)(2g-2) + (q+r)d .$$

Next we study $v_P(S)$ by means of (3.2); i.e. we study

$$v_P(S) = v_P(V^{\nu_0,\dots,\nu_{r-1}}_{g_0,\dots,g_r;t}) .$$

We consider two cases according as P is $\mathbf{F}_q$-rational or not.

Case I: $P \in \mathcal{X}(\mathbf{F}_q)$. Here we can assume that $f_0, \dots, f_r$ is a $(\mathcal{D}, P)$-base; i.e, $v_P(g_\ell) = j_\ell$ for $\ell = 0, \dots, r$. By Proposition 3.4(2)

$$v_P(S) = v_P(g_0^{q+r} V^{\nu_0,\dots,\nu_{r-1}}_{h_0,\dots,h_r;t}) = v_P(V^{\nu_0,\dots,\nu_{r-1}}_{h_0,\dots,h_r;t}) ,$$

where $h_\ell := g_\ell/g_0$. Note that $h_0 = 1$ and that $v_p(h_\ell) = j_\ell$. In particular,

$$V^{\nu_0,\ldots,\nu_{r-1}}_{h_0,\ldots,h_{r-1};t} = \det \begin{pmatrix} h_1 - h_1^q & \ldots & h_r - h_r^q \\ D_t^{\nu_1} h_1 & \ldots & D_t^{\nu_1} h_r \\ \vdots & \vdots & \vdots \\ D_t^{\nu_{r-1}} h_1 & \ldots & D_t^{\nu_{r-1}} h_r \end{pmatrix}, \tag{3.3}$$

and we can made similar computations as in the proof of Lemma 2.7: Expand h_ℓ at P, $h_\ell = \sum_{s=j_\ell}^{\infty} c_s^\ell t^s$, set $C := \prod_{\ell=1}^{r} c_{j_\ell}^\ell$; then

$$V^{\nu_0,\ldots,\nu_{r-1}}_{h_0,\ldots,h_r;t} = C\det(\binom{j_\ell}{\nu_i}) t^{\sum_{i=i}^{r-1}(j_i - \nu_{i-1})} + \ldots, \tag{3.4}$$

where $i = 0, \ldots, r-1; \ell = 1, \ldots, r$ in the matrix above involving the binomial operator. Now $v_P(S)$ can be estimated via this local expansion.

Case II: $P \notin \mathcal{X}(\mathbf{F}_q)$. Let $h_0, \ldots, h_r$ be a $(\mathcal{D}, P)$-base. Then there exists $(a_{ij}) \in M_{r+1}(\bar{\mathbf{F}}_q)$ such that $h_i' := t^{v_P(E)} h_i = \sum_j a_{ij} g_j$. Then from (3.1)

$$v_P(S) = v_P(\sum_{i=0}^{r} (-1)^i \tilde{h}_i' d_i),$$

where the d_i's are the determinants obtained by Cramer's rule. Clearly $v_P(\tilde{h}_i') \geq 0$ and so

$$v_P(S) \geq \min\{v_P(d_0), \ldots, v_P(d_r)\}.$$

Once again we can expand each d_i at P as in the proof of Lemma 2.7: Let $M := (\binom{j_\ell}{\nu_k})_{k=0,\ldots,r-1;\ell=0,\ldots,r}$ and let M_i be the matrix obtained from M by deleting the ith column. Then

$$d_i = C_i \det(M_i) t^{\sum_{k=0}^{r} j_k - j_i - \sum_{k=0}^{r-1} \nu_k} + \ldots, \tag{3.5}$$

where $C_i \in \bar{\mathbf{F}}_q^*$. Thus (3.4) and (3.5) imply the following.

Proposition 3.5. (1) *For $P \in \mathcal{X}(\mathbf{F}_q)$, $v_P(S) \geq \sum_{i=1}^{r}(j_i(P) - \nu_{i-1})$; equality holds if and only if $\det(\binom{j_\ell(P)}{\nu_i})_{i=0,\ldots,r-1;\ell=1,\ldots,r} \not\equiv 0 \pmod p$;*

(2) *For $P \notin \mathcal{X}(\mathbf{F}_q)$, $v_P(S) \geq \sum_{i=1}^{r-1}(j_i(P) - \nu_i)$; if $\det(\binom{j_\ell(P)}{\nu_i})_{i,\ell=0,\ldots,r-1} \equiv 0 \pmod p$, then the stric inequality holds.*

Proposition 3.6. *Let ν be a $\mathbf{F}_q$-Frobenius order such that $\nu < q$. Let μ an integer such that $\binom{\nu}{\mu} \not\equiv 0 \pmod p$. Then μ is also an $\mathbf{F}_q$-Frobenius order. In particular, if $\nu_i < p$ then $(\nu_0, \ldots, \nu_i) = (0, \ldots, i)$.*

Proof. Let $\nu = \nu_i$. For $j \leq i$, we have $D_t^{\nu_j}(f^q) = 0$ by Remark 2.5. So $\nu_0, \ldots, \nu_i$ are the first $i+1$ orders of the morphism $(h_1 - h_1^q : \ldots : h_r - h^q)$, where $h_1, \ldots, h_r$ are as in (3.3). Then the resul follows from the p-adic criterion (Lemma 2.21). □

Next we study relations between the $\mathbf{F}_q$-Frobenius orders and $(\mathcal{D}, P)$-orders at $\mathbf{F}_q$-rational points P.

Proposition 3.7. *Let $P \in \mathcal{X}(\mathbf{F}_q)$ and $m_0 < \ldots < m_{r-1}$ be a sequence of non-negative integers such that $\det(\binom{j_\ell(P)-j_1(P)}{m_i})_{i=0,\ldots,r-1;\ell=1,\ldots,r} \not\equiv 0 \pmod p$. Then $\nu_i \le m_i$ for each i.*

Proof. Set $j_i = j_i(P)$ and let $\phi := (1 : x^{j_2-j_1} : \ldots : x^{j_r-j_1})$, where x is a separating variable of $\bar{\mathbf{F}}_q(\mathcal{X})|\bar{\mathbf{F}}_q$. Let $\eta_0 < \ldots < \eta_{r-1}$ be the orders of ϕ. Then $\eta_i \le m_i$ for each i by (2.6), hypothesis and Corollary 2.10(1). Then, as $\phi = (x^{j_1} : \ldots : x^{j_r})$, $\det((\binom{j_i}{\eta_\ell})) \not\equiv 0 \pmod p$, and the result follows from (3.4). □

Remark 3.8. From the proof above follows that the best election of the m_i's in Proposition 3.7 are the orders of the morphism $\phi = (x^{j_1(P)} : \ldots : x^{j_r(P)})$.

Corollary 3.9. *Let $P \in \mathcal{X}(\mathbf{F}_q)$.*

(1) *$\nu_i \le j_{i+1}(P) - j_1(P)$ for $i = 0, \ldots, r-1$, and so $v_P(S) \ge r j_1(P)$;*
(2) *Suppose $a := \prod_{1\le i<\ell\le r}(j_\ell(P) - j_i(P))/(\ell - i) \not\equiv 0 \pmod p$. Then $\mathcal{D}$ is $\mathbf{F}_q$-Frobenius classical and $v_P(S) = r + \sum_{i=1}^{r}(j_i(P) - i)$.*

Proof. Note that $a = \det(\binom{j_\ell(P)}{i})_{i=0,\ldots,r-1;\ell=1,\ldots,r}$. Then (1) (resp. (2)) follows from Proposition 3.7 with $m_i = j_i(P) - j_1(P)$ (resp. from the proof of Proposition 3.7 with $m_i = i$, and Proposition 3.5(1)). □

Remark 3.10. The criterion of Corollary 3.9(2) is satisfied if $j_\ell(P) - j_i(P) \not\equiv 0 \pmod p$ for $1 \le i < \ell \le r$. In particular, the criterion is satisfied if $p \ge j_r(P)$.

Corollary 3.11. (1) *If $P \in \mathcal{X}(\mathbf{F}_q)$ and $\det(\binom{j_\ell(P)-j_1(P)}{\epsilon_j})_{j=0,\ldots,r-1;\ell=1,\ldots,r} \not\equiv 0 \pmod p$, then $\nu_i = \epsilon_i$ for $i = 0, \ldots, r-1$;*
(2) *If $\mathcal{D}$ is not $\mathbf{F}_q$-Frobenius classical, then $j_r(P) > r$ for any $P \in \mathcal{X}(\mathbf{F}_q)$;*
(3) *If $(\nu_0, \ldots, \nu_{r-1}) \ne (\epsilon_0, \ldots, \epsilon_{r-1})$, then $\mathcal{X}(\mathbf{F}_q) \subseteq \mathrm{Supp}(R)$.*

Proof. (1) follows from Proposition 3.7 with $m_i = \epsilon_i$.

(2) If there exists $P \in \mathcal{X}(\mathbf{F}_q)$ such that $j_r(P) = r$, then $\nu_i = i$ for each i by Corollary 3.9(1).

(3) Suppose that there exists $P \in \mathcal{X}(\mathbf{F}_q) \setminus \mathrm{Supp}(R)$. Then $j_i(P) = \epsilon_i$ for each i and hence $\nu_i \le \epsilon_{i+1} - \epsilon_1$ by Corollary 3.9(1); i.e. $\nu_i = \epsilon_i$ for each i, a contradiction. □

Remark 3.12. If we choose i such that $\mathcal{X}(\mathbf{F}_{q^i}) \not\subseteq \mathrm{Supp}(R)$, then from Corollary 3.11(3) we see that the $\mathbf{F}_{q^i}$-order sequence of $\mathcal{D}$ coincide with $(\epsilon_0, \ldots, \epsilon_{r-1})$.

Theorem 3.13. *Let $\mathcal{X}$ be a curve defined over $\mathbf{F}_q$ that admits a base-point-free linear series $\mathcal{D} = g^r_d$ defined over $\mathbf{F}_q$. Let $\nu_0 < \ldots < \nu_{r-1}$ be the $\mathbf{F}_q$-Frobenius orders of $\mathcal{D}$. Then*

$$\#\mathcal{X}(\mathbf{F}_q) \le \frac{\sum_{i=0}^{r-1} \nu_i(2g-2) + (q+r)d}{r}.$$

Proof. Let S be the $\mathbf{F}_q$-Frobenius divisor of $\mathcal{D}$. Then $v_P(S) \geq r$ for each $P \in \mathcal{X}(\mathbf{F}_q)$ by Corollary 3.9(1), and so $\#\mathcal{X}(\mathbf{F}_q) \leq \deg(S)/r$. □

Example 3.14. (The Hermitian curve over $\mathbf{F}_9$) We are looking for a curve $\mathcal{X}$ of genus 3 defined over $\mathbf{F}_q$ such that $\#\mathcal{X}(\mathbf{F}_q) > 2q + 8$. Let $\epsilon_0 = 0 < \epsilon_1 = 1 < \epsilon_2$ (resp. $\nu_0 = 0 < \nu_1$) be the canonical orders (resp. canonical $\mathbf{F}_q$-orders).

Claim. $\mathcal{X}$ is non-classical; i.e., $\epsilon_2 > 2$.

Indeed, if $\epsilon_2 = 2$, then $\nu_1 \leq 2$ by Corollary 3.3 and Theorem 3.13 gives $\#\mathcal{X}(\mathbf{F}_q) \leq 2q+8$.

Therefore from Example 2.32 we conclude that q is a power of three, $\epsilon_2 = 3$, and that $\mathcal{X}$ is given by $y^3 + a_{01}y = x^4$, with $a_{01} \in \bar{\mathbf{F}}_q$ (notice that the change of coordinates involving a_{01} in Example 2.32 is not defined over $\mathbf{F}_q$). Moreover, the proof above also shows that $\nu_1 > 1$; i.e $\nu_1 = 3$.

Claim. $q = 9$ and $\mathcal{X}$ is $\mathbf{F}_9$-isomorphism to the Hermitian curve $y^3 + y = x^4$. In addition, $\mathcal{X}(\mathbf{F}_9) = \mathcal{W}$ (so that $\#\mathcal{X}(\mathbf{F}_9) = 28 > 2 \times 9 + 8$).

Let x and y be as in Example 2.32. Then $V^{0,1}_{1,x,y;x} = 0$ or equivalently $y - y^q = (x - x^q)D_x y$ $(*)$. Then taking valuation at P we have $-4q = -3q - 9$ so that $q = 9$. Moreover from $(*)$ and the equation defining $\mathcal{X}$ we have $(1 - a_{01}^3)y^3 + (a_{10} - 1)y^9 = 0$ so that $a_{01} = 1$. That $\mathcal{X}(\mathbf{F}_9) \subseteq \mathcal{W}$ follows from Corollary 3.11(3) and equality holds since $\#\mathcal{X}(\mathbf{F}_9) = 28$ (see Sect. 4.2).

Finally, observe that $\#\mathcal{X}(\mathbf{F}_9)$ attains the bound in Theorem 3.13.

Example 3.15. (The Hermitian curve, I) Let ℓ be a power of a prime and $\mathcal{H}$ the plane curve of equation

$$Y^\ell Z + Y Z^\ell = X^{\ell+1}. \tag{3.6}$$

It is easy to see that $\mathcal{H}$ is non-singular so that it has genus $g = \ell(\ell-1)/2$ by Remark 1.8.

Claim. $\#\mathcal{H}(\mathbf{F}_{\ell^2}) = \ell^3 + 1$.

Indeed, we have $\mathcal{H} \cap (Z = 0) = \{(0 : 1 : 0)\}$; in $Z \neq 0$ we look for points $(x : y : 1)$ such that $y^\ell + y = x^{\ell+1}$. It follows that $x \in \mathbf{F}_{\ell^2} \Rightarrow y \in \mathbf{F}_{\ell^2}$ and since $Y^\ell + Y = x^{\ell+1}$ has ℓ different solutions for Y we conclude that there are ℓ^3 such $(x : y : 1)$ points.

Now over $x := X/Z = \infty$ there is just one point say P_∞ such that $H(P_\infty) \subseteq \langle \ell, \ell+1 \rangle$. Since $\#(\mathbf{N} \setminus \langle \ell, \ell+1 \rangle) = \ell(\ell-1)/2 = g$, $H(P_\infty) = \langle \ell, \ell+1 \rangle$. Next we consider $\mathcal{D} := |(\ell+1)P_\infty|$ which is a $g^2_{\ell+1}$ base-point-free on $\mathcal{H}$. Since $L((\ell+1)P_\infty) = \langle 1, x, y \rangle$, where $y^\ell + y = x^{\ell+1}$ we see that $\mathcal{D}$ is just the linear series cut out by lines on $\mathcal{H}$. Let $\epsilon_0 = 0, \epsilon_1 = 1, \epsilon_2$ (resp. $\nu_0 = 0, \nu_1 \in \{1, \epsilon_2\}$) denote the $\mathcal{D}$-orders (resp. $\mathbf{F}_{\ell^2}$-Frobenius orders) of $\mathcal{H}$.

Claim. (1) $\epsilon_2 = \nu_1 = \ell$;

(2) $j_2(P) = \ell + 1$ if $P \in \mathcal{H}(\mathbf{F}_{\ell^2})$; $j_2(P) = \ell$ otherwise.

In fact, $2\#\mathcal{H}(\mathbf{F}_{\ell^2}) \leq \nu_1(2g-2) + (\ell^2+2)(\ell+1)$ by Theorem 3.13 so that $\nu_1 \geq \ell$. Then $\ell \leq \nu_1 = \epsilon_2 \leq \ell+1$ and so $\ell = \nu_1 = \epsilon_2$ by Lemma 2.21 (p-adic criterion). That $j_2(P) = \ell+1$ whenever $P \in \mathcal{H}(\mathbf{F}_{\ell^2})$ follows from Corollary 3.9(1) and part (1). In particular for such points P, $v_P(R) = 1$. Now we have $\deg(R^{\mathcal{D}}) = \ell^3+1$ and therefore $j_2(P) = \ell$ for $P \not\in \mathcal{H}(\mathbf{F}_{\ell^2})$.

We can write a direct proof of part (2) as follows. Let $a, b \in \bar{\mathbf{F}}_\ell$ such that $b^\ell + b = a^{\ell+1}$. It is easy to see that $(x-a)$ is a local parameter at $(a:b:1) \in \mathcal{H}$ so that $(y-b) = a^\ell(x-a) + (a-a^\ell)(x-a)^\ell + (x-a)^{\ell+1} + \ldots$. Let

$$f := (y-b) - a^\ell(x-a)\,.$$

Then

$$\operatorname{div}(f) = \ell(a:b:1) + (a^{\ell^2}:b^{\ell^2}:1) - (\ell+1)P_\infty$$

and part (2) follows.

Further arithmetical and geometrical properties of Frobenius orders can be read in Garcia-Homma [29]. From that paper we mention the following.

Lemma 3.16. ([29, Cor. 3]) *Let $\mathcal{V} = \mathcal{E} \setminus \{\epsilon_I\}$ and suppose that $I < r$. Then* $\operatorname{char}(\mathbf{F}_q)$ *divides ϵ_{I+1}.*

4. Optimal curves

Let $\mathcal{X}$ be a curve defined over $\mathbf{F}_q$ of genus g. To study quantitative results on the number of $\mathbf{F}_q$-rational points of $\mathcal{X}$ it is convenient to form a formal power series, the so-called *Zeta Function* of $\mathcal{X}$ relative to $\mathbf{F}_q$:

$$Z_{\mathcal{X},q}(t) := \exp\Big(\sum_{i=1}^{\infty} \frac{\#\mathcal{X}(\mathbf{F}_{q^i})}{i} t^i\Big)\,.$$

By the Riemann-Roch theorem there exists a polynomial $P(t)$ of degree $2g$ with integer coefficients, such that (see e.g. [78, Thm. 3.2], [96, Thm. V.1.15])

$$Z_{\mathcal{X},q}(t) = \frac{P(t)}{(1-t)(1-qt)}\,. \tag{4.1}$$

Remark 4.1. ([96, Thm. V.1.15])

(i) Let $P(t) = \sum_{i=0}^{2g} a_i t^i$. Then $a_0 = 1$, $a_{2g} = q$, and $a_{2g-i} = q^{g-i}a_i$ for $i = 0, \ldots, g$.

(ii) Set

$$h(t) = h_{\mathcal{X},q}(t) := t^{2g}P(t^{-1})\,;$$

then the $2g$ roots (counted with multiplicity) $\alpha_1, \ldots, \alpha_{2g}$ of $h(t)$ can be arranged in such a way that $\alpha_j\alpha_{g+j} = q$ for $j = 1, \ldots, g$. Note that $a_1 = -\sum_{j=1}^{2g}\alpha_j$.

Now (4.1) implies $\#\mathcal{X}(\mathbf{F}_q) = q + 1 + a_1$ and hence that

$$\#\mathcal{X}(\mathbf{F}_q) = q + 1 - \sum_{j=1}^{2g} \alpha_j \,,$$

by Remark 4.1(ii). Furthermore [96, Cor. V.1.16],

$$\#\mathcal{X}(\mathbf{F}_{q^i}) = q^i + 1 - \sum_{j=1}^{2g} \alpha_j^i \,.$$

By analogy with the Riemann hypothesis E. Artin conjectured that the absolute value of each α_i equals $\sqrt{q}$. This result was showed by Hasse for $g = 1$ and for A. Weil for arbitrary g [108] (see also [99, Cor. 2.14], [78], [96, Thm. V.2.3]). In particular, we obtain the Hasse-Weil bound on the number of $\mathbf{F}_q$-rational points of $\mathcal{X}$, namely

$$|\#\mathcal{X}(\mathbf{F}_q) - (q+1)| \leq 2\sqrt{q}g \,.$$

If $\mathcal{X}$ attains the upper bound above, it is called $\mathbf{F}_q$-*maximal*; in this case q must be a square.

Lemma 4.2. *Let $q = \ell^2$. The following statements are equivalent:*

(1) *$\mathcal{X}$ is $\mathbf{F}_{\ell^2}$-maximal;*
(2) *$\alpha_i = -\ell$ for $i = 1, \ldots, 2g$;*
(3) *$h_{\mathcal{X},\ell^2}(t) = (t + \ell)^{2g}$.*

If any of these conditions hold and $\mathcal{X}$ is defined over $\mathbf{F}_\ell$, then

$$\#\mathcal{X}(\mathbf{F}_{\ell^i}) = \begin{cases} \ell^i + 1 & \text{if } i \equiv 1 \pmod 2, \\ \ell^i + 1 + 2\sqrt{\ell^i}g & \text{if } i \equiv 2 \pmod 4, \\ \ell^i + 1 - 2\sqrt{\ell^i}g & \text{if } i \equiv 0 \pmod 4. \end{cases}$$

Proof. $\mathcal{X}$ is $\mathbf{F}_{\ell^2}$-maximal if and only if $\sum_{i=1}^{2g} \alpha_i = \sum_{i=1}^{g} (\alpha_i + \bar{\alpha}_i) = -2\ell g$. By the Riemann-hypothesis, this is the case if and only if $\alpha_i = -\ell$ for each i and the equivalences follow. Now we show the formulae on the number of rational points. Let $\#\mathcal{X}(\mathbf{F}_\ell) = \ell + 1 - \sum_{j=1}^{2g} \beta_j$. Then $\beta_j^2 = -\ell$ for each j so that $\beta_j^i + \bar{\beta}_j^i = 0$ for $i \equiv 1 \pmod 2$; i.e., $\#\mathcal{X}(\mathbf{F}_{\ell^i}) = \ell^i + 1$. If $i \equiv 2 \pmod 4$, $\beta_j^i = -\sqrt{\ell^i}$ and follows the formula for such i's. Finally, if $i \equiv 0 \pmod 4$, $\beta_j = \sqrt{\ell^i}$ and the proof is complete. □

Corollary 4.3. (Ihara [58]) *If $\mathcal{X}$ is $\mathbf{F}_{\ell^2}$-maximal, then $g \leq \ell(\ell-1)/2$.*

Proof. We have $\mathcal{X}(\mathbf{F}_{\ell^2}) \subseteq \mathcal{X}(\mathbf{F}_{\ell^4})$. Then from the lemma above, $\ell^2 + 1 + 2\ell g \leq \ell^4 + 1 - 2\ell^2 g$, and the result follows. □

Example 4.4. (The Hermitian curve, II) The curve $\mathcal{H}$ in Example 3.15 has genus $\ell(\ell-1)/2$ and $\ell^3 + 1$ $\mathbf{F}_{\ell^2}$-rational points. Hence it is $\mathbf{F}_{\ell^2}$-maximal and attains the bound in Corollary 4.3.

This curve is called *the Hermitian curve* and it is the most fancy example of a maximal curve. By Lachaud [70, Prop. 6] any curve $\mathbf{F}_{\ell^2}$-covered by a $\mathbf{F}_{\ell^2}$-maximal curve is also $\mathbf{F}_{\ell^2}$-maximal. Then one obtains further examples of $\mathbf{F}_{\ell^2}$-maximal curves by e.g. considering suitable quotient curves $\mathcal{H}/G$, whit G a subgroup of $\mathrm{Aut}_{\mathbf{F}_{\ell^2}}(\mathcal{H})$; see Garcia-Stichtenoth-Xing [31], and [14], [15]. As a matter of fact, all the known examples of $\mathbf{F}_{\ell^2}$-maximal curves arise in this way.

Problem 4.5. Is any $\mathbf{F}_{\ell^2}$-maximal curve $\mathbf{F}_{\ell^2}$-covered by $\mathcal{H}$?

Further properties of maximal curves can be found in [24], [26], [67], [68] and the references therein.

If q is not a square, the Hasse-Weil bound was improved by Serre [93, Thm. 1] as follows (see also [96, Thm. V.3.1])

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

Lemma 4.6. *The following statements are equivalent:*

(1) $\mathcal{X}$ *is maximal with respect to Serre's bound*;
(2) $\alpha_i + \bar{\alpha}_i = -\lfloor 2\sqrt{q} \rfloor$ *for* $i = 1, \dots g$;
(3) $h_{\mathcal{X},q}(t) = (t^2 + \lfloor 2\sqrt{q} \rfloor t + q)^g$.

Proof. $\mathcal{X}$ is maximal with respect to Serre's bound if and only if $\sum_{i=1}^{g}(\alpha + \bar{\alpha}_i) = -\lfloor 2\sqrt{q} \rfloor g$ if and only if $\alpha_i + \bar{\alpha}_i = -\lfloor 2\sqrt{q} \rfloor$. Now, as we can assume $\alpha_i \bar{\alpha}_i = q$ by Remark 4.1(ii) so that $h_{\mathcal{X},q}(t) = \prod_{i=1}^{g}(t - \alpha_i)(t - \bar{\alpha}_i)$, the result follows. □

Corollary 4.7. *We have* $g \le (q^2 - q)/(\lfloor 2\sqrt{q} \rfloor^2 + \lfloor 2\sqrt{q} \rfloor - 2q)$ *whenever* $\mathcal{X}$ *is maximal with respect to Serre's bound.*

Proof. As in the proof of Corollary 4.3 we use $\mathcal{X}(\mathbf{F}_q) \subseteq \mathcal{X}(\mathbf{F}_{q^2})$. We have $\alpha_i + \bar{\alpha}_i = -\lfloor 2\sqrt{q} \rfloor$ and $\alpha_i \bar{\alpha}_i = q$ so that $\alpha_i^2 + \bar{\alpha}_i^2 = \lfloor 2\sqrt{q} \rfloor^2 - 2q$; hence

$$\#\mathcal{X}(\mathbf{F}_q) = q + 1 + \lfloor 2\sqrt{q} \rfloor \le \#\mathcal{X}(\mathbf{F}_{q^2}) = q^2 + 1 - (\lfloor 2\sqrt{q} \rfloor^2 - 2q)g\,,$$

and the result follows. □

Remark 4.8. The proofs of the following statements are similar to the proofs of Lemmas 4.2 and 4.6.

(i) A curve $\mathcal{X}$ defined over $\mathbf{F}_{\ell^2}$ is $\mathbf{F}_{\ell^2}$*-minimal*; i.e., $\#\mathcal{X}(\mathbf{F}_{\ell^2}) = \ell^2 + 1 - 2\ell g$ if and only if $h_{\mathcal{X},\ell^2}(t) = (t - \ell)^{2g}$.
(ii) A curve $\mathcal{X}$ defined over $\mathbf{F}_q$ is minimal with respect to Serre's bound; i.e., $\#\mathcal{X}(\mathbf{F}_q) = q + 1 - \lfloor 2\sqrt{q} \rfloor g$ if and only if $h_{\mathcal{X},q}(t) = (t^2 - \lfloor 2\sqrt{q} \rfloor t + q)^g$.

Example 4.9. (The Klein quartic) Let $\mathcal{X}$ be the plane curve over $\mathbf{F}$ defined by

$$X^3Y + Y^3Z + Z^3X = 0\,.$$

It is easy to see that $\mathcal{X}$ is non-singular if and only if $\mathrm{char}(\mathbf{F}) \neq 7$; in this case $\mathcal{X}$ has genus 3. This curve was considered by many authors since the time of Klein who showed that $\mathrm{Aut}(\mathcal{X})$ reaches the Hurwitz bound for the number of automorphism of curves of genus 3 whenever $\mathrm{char}(\mathbf{F}) = 0$. A connection with the Fano plane was noticed by Pellikaan [84].

Claim. $\mathcal{X}$ defined over $\mathbf{F}_8$ reachs the Serre's bound; i.e, $\#\mathcal{X}(\mathbf{F}_8) = 1+9+\lfloor 2\sqrt{8}\rfloor 3 = 24$.

To see this we first notice that $(1:0:0), (0:1:0), (0:0:1)$ are $\mathbf{F}_8$-rational points (this is true for any field where $\mathcal{X}$ is defined). Now (cf. [84, p. 10]) we look for $(x:y:1) \in \mathcal{X}$ such that $x \neq 0, y \neq 0$ and such that $x^7 = 1$. We have

$$0 = x^3y + +y^3 + x = x^3y + x^7y^3 + x = x(x^2y + (x^2y)^3 + 1)\,;$$

i.e., $t^3 + t + 1 = 0$ $(*)$ with $t = x^2y$ $(*_1)$. Conversely, it is easy to see that equation $(*)$ is irreducible over $\mathbf{F}_2$ and hence its three roots are in $\mathbf{F}_8$. Then once $x \in \mathbf{F}_8^*$ we have $y \in \mathbf{F}_8^*$ by $(*_1)$. Therefore we have 21 such points $(x:y:1)$ and the claim follows.

Then $h_{\mathcal{X},8}(t) = (t^2 + 5t + 8)^3$ by Lemma 4.6.

Claim. $h_{\mathcal{X},2}(t) = t^6 + 5t^3 + 8$; in particular $\#\mathcal{X}(\mathbf{F}_2) = 3$.

Let $h_{\mathcal{X},2}(t) = \prod_{i=1}^{3}(t-\beta_i)(t-\bar{\beta}_i)$. Then $\beta_i^3 + \bar{\beta}_i^3 = -5$ (cf. Lemma 4.6) so that β_i^3 and $\bar{\beta}_i^3$ are roots of $T^2+5T+8 = 0$; then $h_{\mathcal{X},2}(t) = t^6+5t^3+8$ so that $\#\mathcal{X}(\mathbf{F}_2) = 2+1-0 = 3$.

Finally, we mention that $\mathcal{X}$ is $\mathbf{F}_{\ell^2}$-maximal if and only if either $\ell = p^{6v+1}$ and $p \equiv 6 \pmod 7$, or $\ell = p^{6v+3}$ and $p \equiv 3, 5, 6 \pmod 7$, or $\ell = p^{6v+5}$ and $p \equiv 6 \pmod 7$; see [2, Cor. 3.7(2)].

Remark 4.10. (Lewittes [74, Thm. 1(b)]) Let $P \in \mathcal{X}(\mathbf{F}_q)$ and $f : \mathcal{X} \to \mathbf{P}^1(\bar{\mathbf{F}}_q)$ be the $\mathbf{F}_q$-rational function on $\mathcal{X}$ such that $\mathrm{div}_\infty(f) = n_1(P)P$. Then $\mathcal{X}(\mathbf{F}_q) \subseteq f^{-1}(\mathbf{P}^1(\mathbf{F}_q)) = \{P_1\} \cup f^{-1}(\mathbf{F}_q)$ and hence

$$\#\mathcal{X}(\mathbf{F}_q) \leq 1 + qn_1(P)\,.$$

Now from Corollaries 4.3 and 4.7 we see that neither the Hasse-Weil bound nor Serre's bound is effective to estimate $\#\mathcal{X}(\mathbf{F}_q)$ whenever g is large with respect to q. So in general one studies the number

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

For instance $N_q(0) = q + 1$, and Example 4.9 shows that $N_8(3) = 24$. The study of the actual value of $N_q(g)$ was initiated by Serre [93] who computed $N_q(1)$ and $N_q(2)$. Further properties were proved by Serre himself [94], Lauter [73], and Kresh-Wetherell-Zieve [69]. Tables for $N_q(g)$ with q and g small can be found in van der Geer-van der Vlugt [34].

Definition. A curve $\mathcal{X}$ of genus g and defined over $\mathbf{F}_q$ is called *optimal* (with respect to g and q) if $\#\mathcal{X}(\mathbf{F}_q) = N_q(g)$.

If $q = \ell^2$ and $\mathcal{X}$ is $\mathbf{F}_{\ell^2}$-maximal then $\mathcal{X}$ is certainly optimal. We already noticed (Example 4.4) that the Hermitian curve $\mathcal{H}$ is $\mathbf{F}_{\ell^2}$-maximal whose genus attains the bound in Corollary 4.3. Indeed, this property characterizes Hermitian curves:

Theorem 4.11. (Rück-Stichtenoth [87]) *A $\mathbf{F}_{\ell^2}$-maximal curve $\mathcal{X}$ has genus $\ell(\ell-1)/2$ if and only if $\mathcal{X}$ is $\mathbf{F}_{\ell^2}$-isomorphic to the Hermitian curve of equation (3.6).*

This result follows from Theorem 4.24.

Next we discuss optimal curves for $\sqrt{q} \notin \mathbf{N}$. Besides some curves of small genus (see above), the only known examples of optimal curves are the Deligne-Lusztig curves $\mathcal{S}$ and $\mathcal{R}$ associated to the Suzuki group $Sz(q)$, $q = 2^{2s+1}$, $s \geq 1$, and to the Ree group $R(q)$, $q = 3^{2s+1}$, $s \geq 1$, respectively [17, Sect. 11]. As a matter of terminology, $\mathcal{S}$ (resp. $\mathcal{R}$) will be call *the Suzuki curve* (resp. *the Ree curve*). After the work of Hansen-Stichtenoth [43], Hansen [41], Pedersen [83], Hansen-Pedersen [42], the curves $\mathcal{S}$ and $\mathcal{R}$ can be characterized as follows.

Theorem 4.12. *The curves $\mathcal{S}$ and $\mathcal{R}$ are the unique curves (up to $\mathbf{F}_q$-isomorphic) $\mathcal{X}$ defined over $\mathbf{F}_q$ such that the following three conditions hold:*

(1) $\#\mathcal{X}(\mathbf{F}_q) = q^2 + 1$ *(resp.* $\#\mathcal{X}(\mathbf{F}_q) = q^3 + 1$*);*
(2) $\mathcal{X}$ *has genus* $q_0(q-1)$ *(resp.* $3q_0(q-1)(q+q_0+1)/2$*), where* $q_0 := 2^s$ *(resp.* 3^s*);*
(3) $\mathrm{Aut}_{\mathbf{F}_q}(\mathcal{X}) = Sz(q)$ *(resp.* $\mathrm{Aut}_{\mathbf{F}_q}(\mathcal{X}) = R(q)$*).*

Moreover, the Suzuki curve $\mathcal{S}$ (resp. the Ree curve $\mathcal{R}$) is the non-singular model of

$$Y^q Z^{q_0} - Y Z^{q+q_0-1} = X^{q_0}(X^q - X Z^{q-1}),$$

(resp.

$$\begin{cases} Y^q W^{q_0} - Y W^{q+q_0-1} = X^{q_0}(X^q - X W^{q-1}) \\ Z^q W^{2q_0} - Y W^{q+2q_0-1} = X^{2q_0}(x^q - X W^{q-1})). \end{cases}$$

In Sect. 4.3 we prove a stronger version of this theorem for the Suzuki curve.

Lemma 4.13. *Let $\mathcal{X}$ be a curve defined over $\mathbf{F}_q$ such that (1) and (2) in Theorem 4.12 hold. Then $\mathcal{X}$ is optimal; moreover:*

(1) *If* $q = 2^{2s+1}$, $h_{\mathcal{X},q}(t) = (t^2 + 2q_0 t + q)^{q_0(q-1)}$;
(2) *If* $q = 3^{2s+1}$, $h_{\mathcal{X},q}(t) = (t^2 + 3q_0 t + q)^{q_0(q^2-1)}(t^2+q)^{q_0(q-1)(q+3q_0+1)/2}$.

Proof. It is easy to see that Serre's bound is not effective to bound $\#\mathcal{X}(\mathbf{F}_q)$; in this case one uses the so-called "explicit formula" (4.2) of Weil [93]: (following Stichtenoth [96, p. 183]) Let $h_{\mathcal{X},q}(t) = \prod_{i=1}^{g}(t-\alpha_i)(t-\bar{\alpha}_i)$, $\alpha_i = \sqrt{q}e^{\sqrt{-1}\theta_i}$, and write

$$q^{-i/2}\#\mathcal{X}(\mathbf{F}_{q^i}) = q^{i/2} + q^{-i/2} - q^{-i/2}\sum_{j=1}^{g}(\alpha_j^i + \bar{\alpha}_j^i);$$

this equation can we rewritten as

$$\#\mathcal{X}(\mathbf{F}_q)c_iq^{-i/2} = c_iq^{i/2} + c_iq^{-i/2} + c_iq^{-i/2}\sum_{j=1}^{g}(\alpha_j^i + \bar{\alpha}_j^i) - (\#\mathcal{X}(\mathbf{F}_{q^i}) - \#\mathcal{X}(\mathbf{F}_q)c_iq^{-i/2}\,,$$

where $c_i \in \mathbf{R}$. Now suppose that $c_1, \ldots, c_m$ are given real numbers. Then from the above equation we obtain:

$$\begin{aligned}\#\mathcal{X}(\mathbf{F}_q)\lambda_m(q^{-1/2}) = \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) + g - \sum_{j=1}^{g} f_m(q^{-1/2}\alpha_j) - \\ \sum_{i=1}^{m}(\#\mathcal{X}(\mathbf{F}_{q^i}) - \#\mathcal{X}(\mathbf{F}_q))c_iq^{-i/2}\,,\end{aligned} \tag{4.2}$$

where $\lambda_m(t) := \sum_{i=1}^{m} c_it^i$ and $f_m(t) := 1 + \lambda_m(t) + \lambda_m(t^{-1})$. Note that $f_m(t) \in \mathbf{R}$ whenever $t \in \mathbf{C}$ and $|t| = 1$.

Case $q = 2^{2s+1}$ and $g = q_0(q-1)$. Here we choose $m = 2$, $c_1 = \sqrt{2}/2$, $c_2 = 1/4$. Then $f_2(e^{\sqrt{-1}\theta}) = 1 + \sqrt{2}cos\theta + cos(2\theta)/2 = (cos\theta + \sqrt{2}/2)^2 \geq 0$. Then from (4.2) we have

$$\#\mathcal{X}(\mathbf{F}_q)\lambda_2(q^{-1/2}) \leq \lambda_2(q^{1/2}) + \lambda_2(q^{-1/2}) + g\,,$$

so that $\#\mathcal{X}(\mathbf{F}_q) \leq q^2 + 1$, and hence $\mathcal{X}$ is optimal. Moreover, as $\#\mathcal{X}(\mathbf{F}_q) = q^2 + 1$ we must have $f_2(q^{-1/2}\alpha_j) = 0$ by (4.2) so that $cos\theta_j = -\sqrt{2}/2$. Then $\alpha_j + \bar{\alpha}_j = -2q_0$ and the result on $h_{\mathcal{X},q}(t)$ follows.

Case $q = 3^{2s+1}$ and $g = 3q_0(q-1)(q+q_0+1)/2$. Here we use $m = 4$, $c_1 = \sqrt{3}/2$, $c_2 = 7/12$, $c_3 = \sqrt{3}/6$, $c_4 = 1/12$. Then $f_4(e^{\sqrt{-1}\theta}) = 1 + \sqrt{3}cos\theta + 7cos(2\theta)/6 + \sqrt{3}cos(3\theta)/3 + cos(4\theta)/6 = (1 + \sqrt{3}cos\theta + cos2\theta)^2/3 \geq 0$. Then from (4.2)

$$\#\mathcal{X}(\mathbf{F}_q)\lambda_4(q^{-1/2}) \leq \lambda_4(q^{1/2}) + \lambda_4(q^{-1/2}) + g\,,$$

so that $\mathcal{X}(\mathbf{F}_q) \leq q^3 + 1$. Moreover, $1 + \sqrt{3}cos\theta_j + cos2\theta_j = 0$ whenever $\mathcal{X}(\mathbf{F}_q) = q^3 + 1$. Hence $cos\theta_j = 0$ or $cos\theta_j = -\sqrt{3}/2$ so that

$$h_{\mathcal{X},t}(t) = (t^2 + 3q_0t + q)^A(t^2 + q)^{g-A}\,,$$

where A is the number of j's such that $cos\theta_j = -\sqrt{3}/2$. To compute A we use the facts that $a_1 = \#\mathcal{X}(\mathbf{F}_q) - (q+1) = q^3 - q$ and $a_{2g-1} = q^{g-1}a_1$. We have $a_{2g-1} = h'_{\mathcal{X},q}(0) = 3q_0q^{g-1}A$ and hence that $A = q_0(q^2-1)$. □

4.1. A $\mathbf{F}_q$-divisor from the Zeta Function. Assume now that $\mathcal{X}(\mathbf{F}_q) \neq \emptyset$, and fix a $\mathbf{F}_q$-rational point $P_0 \in \mathcal{X}$. Let $f = f^{P_0} : P \to [P - P_0]$ be the canonical map from $\mathcal{X}$ to its Jacobian over $\mathbf{F}_q$, $\mathcal{J} \cong \{D \in \mathrm{Div}(\mathcal{X}) : \deg(D) = 0\}/\{\mathrm{div}(x) : x \in \bar{\mathbf{F}}_q(\mathcal{X})^*\}$. Let ${\mathbf{\Phi}_q}'$ be the Frobenius morphism on $\mathcal{J}$ induced by $\mathbf{\Phi}_q$.

We recall some facts concerning the characteristic polynomial of ${\mathbf{\Phi}_q}'$ which in fact turns out to be the polynomial $h(t) = h_{\mathcal{X},q}(t)$ which was defined in Remark 4.1; see e.g. [77, p. 205], or [76, proof of Thm. 19.1].

For a prime ℓ different from $\mathrm{char}(\mathbf{F}_q)$, let $\mathcal{J}_{\ell^i}$ denote the kernel of the isogeny $\mathcal{J} \to \mathcal{J}$, $P \mapsto \ell^i P$. Then one defines the *Tate modulo* associated to $\mathcal{J}$ as the inverse limit of the groups $\mathcal{J}_{\ell^i}$, $i \geq 1$, with respect to the maps $\mathcal{J}_{\ell^{i+1}} \to \mathcal{J}_{\ell^i}$, $P \mapsto \ell P$. We have that $\#\mathcal{J}_{\ell^i} = (\ell^i)^{2g}$ [77, p. 62] so that $\mathcal{J}_{\ell^i}$ is a finite abelian group such that for all j, $1 \leq j \leq i$ it contains exactly $(\ell^j)^{2g}$ elements of order ℓ^j. Therefore

$$\mathcal{J}_{\ell^i} \cong (\mathbf{Z}/\ell^i\mathbf{Z})^{2g} \qquad \text{and hence} \qquad T_\ell(\mathcal{J}) \cong \mathbf{Z}_\ell^{2g}\,,$$

where $\mathbf{Z}_\ell$ denotes the ℓ-adic integers. Thus $T_\ell(\mathcal{J})$ is a free $\mathbf{Z}_\ell$-module of rank $2g$. Now clearly ${\boldsymbol{\Phi}_q}'(\mathcal{J}_{\ell^i}) \subseteq \mathcal{J}_{\ell^i}$ and hence ${\boldsymbol{\Phi}_q}'$ gives rise to a $\mathbf{Z}_\ell$-linear map $T_\ell({\boldsymbol{\Phi}_q}')$ on $T_\ell(\mathcal{J})$. Let π be the characteristic polynomial of $T_\ell({\boldsymbol{\Phi}_q}')$. A priory we have that π is a polynomial of degree $2g$ with coefficients in $\mathbf{Z}_\ell$. As a matter of fact, $\pi \in \mathbf{Z}[t]$ [77, proof of Ch. IV, Thm. 4], and $\pi = h$ as we mentioned before. In particular, the minimal polynomial m of $T_\ell({\boldsymbol{\Phi}_q}')$ has integral coefficients. We claim that

$$m({\boldsymbol{\Phi}_q}') = 0 \qquad \text{on } \mathcal{J}\,. \tag{4.3}$$

To see this, notice that any endomorphism $\alpha \in \mathrm{End}(\mathcal{J}) : \mathcal{J} \mapsto \mathcal{J}$ acts on $T_\ell(\mathcal{J})$ giving rise to a $\mathbf{Z}_\ell$-linear map $T_\ell(\alpha)$. This action is injective because $\mathrm{End}(\mathcal{J})$ is torsion free and because of [77, Ch. IV, Thm. 3]. Now, as $m({\boldsymbol{\Phi}_q}') \in \mathrm{End}(\mathcal{J})$, we have

$$0 = m(T_\ell({\boldsymbol{\Phi}_q}')) = T_\ell(m({\boldsymbol{\Phi}_q}'))$$

and (4.3) follows. Moreover, it is known that $\mathbf{Q} \otimes \mathrm{End}(\mathcal{J})$ is a finite dimensional semisimple algebra over $\mathbf{Q}$ whose center is $\mathbf{Q}[{\boldsymbol{\Phi}_q}']$ [77, Ch. IV, Cor. 3], [100, Thm. 2(a)]. In particular, $\mathbf{Q}[{\boldsymbol{\Phi}_q}']$ is semisimple and it is not difficult to see that $T_\ell({\boldsymbol{\Phi}_q}')$ is semisimple; cf. [77, p. 251]. This means that

$$m(t) = \prod_{i=1}^{T} h_i(t)\,,$$

where $h_1(t), \ldots, h_T(t)$ are the irreducibles $\mathbf{Z}$-factors of $h(t)$. Let U be the degree of $m(t)$ and let $b_1, \ldots, b_U \in \mathbf{Z}$ be the coefficients of $m(t) - t^U$; i.e,

$$m(t) = t^U + \sum_{i=1}^{U} b_i t^{U-i}\,.$$

Thus $({\boldsymbol{\Phi}_q}')^U + \sum_{i=1}^{U} b_i({\boldsymbol{\Phi}_q}')^{U-i} = 0$ by (4.3). Now we evaluate the left hand side of this equality at $f(P) = [P - P_0]$, and by using the fact that ${\boldsymbol{\Phi}_q}' \circ f = f \circ \boldsymbol{\Phi}_q$ we find that

$$f({\boldsymbol{\Phi}_q}^U(P)) + \sum_{i=1}^{U} a_i f({\boldsymbol{\Phi}_q}^{U-i}(P)) = 0\,, \qquad P \in \mathcal{X}\,;$$

$$\text{i.e.,} \quad {\boldsymbol{\Phi}_q}^U(P) + \sum_{i=1}^{U} b_i {\boldsymbol{\Phi}_q}^{U-i}(P) \sim (1 + \sum_{i=1}^{U} b_i)P_0 = m(1)P_0\,. \tag{4.4}$$

This equivalence is the motivation to define on $\mathcal{X}$ the linear series

$$\mathcal{D}_{\mathcal{X}} := ||m(1)|P_0|\,, \tag{4.5}$$

which is clearly independent of P_0 being $\mathbf{F}_q$-rational.

Problem 4.14. For a curve $\mathcal{X}$ over $\mathbf{F}_q$, how is the interplay among its $\mathbf{F}_q$-rational points, its Weierstrass points, its $\mathcal{D}_{\mathcal{X}}$-Weierstrass points, and the support of the $\mathbf{F}_q$-Frobenius divisor of $\mathcal{D}_{\mathcal{X}}$.

Next we discuss some properties of $\mathcal{D}_{\mathcal{X}}$.

Lemma 4.15. (1) *If $P, Q \in \mathcal{X}(\mathbf{F}_q)$, then $m(1)P \sim m(1)Q$; in particular, $|m(1)|$ is a Weierstrass non-gap at each $P \in \mathcal{X}(\mathbf{F}_q)$.*

(2) *If $\#\mathcal{X}(\mathbf{F}_q) \geq 2g+3$, then there exists $P_1 \in \mathcal{X}(\mathbf{F}_q)$ such that $|m(1)|-1$ and $|m(1)|$ are Weierstrass non-gaps at P_1.*

Proof. (1) It follows immediately from (4.4).

(2) (Following Stichtenoth-Xing [97, Prop. 1]) Let $Q \in \mathcal{X}(\mathbf{F}_q) \setminus \{P_0\}$. From (1), there exists a morphism $x : \mathcal{X} \to \mathbf{P}^1(\bar{\mathbf{F}}_q)$ with $\mathrm{div}(x) = |m(1)|P_0 - |m(1)|Q$. Let n be the number of $\mathbf{F}_q$-rational points of $\mathcal{X}$ which are unramified for x. Let $x^s : \mathcal{X} \to \mathbf{P}^1(\bar{\mathbf{F}}_q)$ be the separable part of x. We have that $\mathrm{div}(x^s) = |m(1)|'P_0 - |m(1)|'Q$ (here $|m(1)|'$ is the separable degree of x) and from the Riemman-Hurwitz applied to x^s we find that

$$2g-2 \geq |m(1)|'(-2) + 2(|m(1)|'-1) + (\#\mathcal{X}(\mathbf{F}_q) - n - 2)\,,$$

so that $n \geq \#\mathcal{X}(\mathbf{F}_q) - 2g - 2$. Thus $n \geq 1$ by hypothesis, and hence there exists $\alpha \in \mathbf{F}_q$, $P_1 \in \mathcal{X}(\mathbf{F}_q) \setminus \{P_0, Q\}$ such that $\mathrm{div}(x-\alpha) = P_1 + D - mQ$ with $P_1, Q \notin \mathrm{Supp}(D)$. Let $y \in \bar{\mathbf{F}}_q(\mathcal{X})$ be such that $\mathrm{div}(y) = |m(1)|Q - |m(1)|P_1$ (cf. (1)). Then $\mathrm{div}(y(x-\alpha)) = D - (|m(1)|-1)P_1$ and (2) follows. □

Corollary 4.16. (1) *$\mathcal{D}_{\mathcal{X}}$ is base-point-free;*

(2) *If $\#\mathcal{X}(\mathbf{F}_q) \geq 2g+3$, then $\mathcal{D}_{\mathcal{X}}$ is simple.*

Proof. (1) follows by Lemma 4.15 and Example 1.23

(2) Let P_1 be as in Lemma 4.15(2), ϕ a morphism associated to $\mathcal{D}_{\mathcal{X}}$, $f_1, f_2 \in \bar{\mathbf{F}}_q(\mathcal{X})$ such that $\mathrm{div}_\infty(f_1) = (|m(1)|-1)P_1$ and $\mathrm{div}_\infty(f_2) = |m(1)|P_1$. Then $[\bar{\mathbf{F}}_q(\mathcal{X}) : \bar{\mathbf{F}}_q(f_i)]$, $i = 1, 2$, divides $[\bar{\mathbf{F}}_q(\mathcal{X}) : \bar{\mathbf{F}}_q(\phi(\mathcal{X}))]$ and the result follows. □

Now we study $(\mathcal{D}_{\mathcal{X}}, P)$-orders. We let $\epsilon_0 = 0 < \epsilon_1 = 1 < \ldots < \epsilon_N$ (resp. $\nu_0 = 0 < \ldots < \nu_{N-1}$) denote the $\mathcal{D}_{\mathcal{X}}$-orders (resp. the $\mathbf{F}_q$-Frobenius orders) of $\mathcal{D}_{\mathcal{X}}$, where $N := \dim(\mathcal{D}_{\mathcal{X}})$. Notice that $n_N(P) = |m(1)|$ for any $P \in \mathcal{X}(\mathbf{F}_q)$ by Lemma 4.15(1). From Example 1.23 we obtain:

Lemma 4.17. *For $P \in \mathcal{X}(\mathbf{F}_q)$, the $(\mathcal{D}_{\mathcal{X}}, P)$-orders are*

$$j_{N-i}(P) = n_N(P) - n_i(P)\,, \qquad i = 0, 1, \ldots, N\,.$$

This result (for $i = 1$) and Remark 4.10 yield the following.

Corollary 4.18. *Let $P \in \mathcal{X}(\mathbf{F}_q)$. If $\#\mathcal{X}(\mathbf{F}_q) > q(|m(1)| - b_U) + 1$, then $j_{N-1}(P) < b_U$.*

Lemma 4.19. *Suppose*

$$b_i \geq 0\,, \quad i = 1, \ldots, U\,, \tag{4.6}$$

and let $P \in \mathcal{X}$ such that ${\mathbf{\Phi}_q}^i(P) \neq P$ for $i = 1, \ldots, U$. Then:

1. *The numbers $1, b_1, \ldots, b_U$ are $(\mathcal{D}_\mathcal{X}, P)$-orders;*
2. *If in addition*

$$b_1 \geq b_0 := 1 \quad \textit{and} \quad b_{i+1} \geq b_i, \ \textit{for } i = 1, \ldots, U-1\,, \tag{4.7}$$

then b_U (resp. $b_U - 1$) is a Weierstrass non-gap at P whenever ${\mathbf{\Phi}_q}^{U+1}(P) \neq P$ (resp. ${\mathbf{\Phi}_q}^{U+1}(P) = P$).

Proof. (1) Fix $j \in \{0, 1, \ldots, U\}$, and let $Q \in \mathcal{X}$ such that ${\mathbf{\Phi}_q}^{U-j}(Q) = P$ $(*)$. From (4.4) we have

$$\sum_{i \in \{0,1,\ldots,U\} \setminus \{j\}} b_i {\mathbf{\Phi}_q}^{U-i}(Q) + b_j P \sim m(1) P_0\,.$$

We claim that ${\mathbf{\Phi}_q}^{U-i}(Q) \neq P$; otherwise from $(*)$ we would have ${\mathbf{\Phi}_q}^{i-j}(P) = P$, a contradiction. This shows (1).

(2) Applying $\mathbf{\Phi}_{q_*}$ to (4.4) we have

$$ {\mathbf{\Phi}_q}^{U}(P) + \sum_{i=1}^{U} b_i {\mathbf{\Phi}_q}^{U-i}(P) \sim m(1) P_0 \sim {\mathbf{\Phi}_q}^{U+1}(P) + \sum_{i=1}^{U} b_i {\mathbf{\Phi}_q}^{U-i+1}(P)\,,$$

so that

$$b_U P \sim {\mathbf{\Phi}_q}^{U+1}(P) + \sum_{i=1}^{U} (b_i - b_{i-1}) {\mathbf{\Phi}_q}^{U-i+1}(P)\,,$$

and (2) follows. □

Remark 4.20. (i) Minimal curves as well as minimal curves with respect to Serre's bound (Remark 4.8) do not satisfy (4.6).

(ii) The Klein curve (Example 4.9) defined over $\mathbf{F}_2$ satisfies (4.6) but not (4.7).

(iii) Other examples as in (i) and (ii) can be found in Carbonne-Henocq [9].

Corollary 4.21. *Assume (4.6).*

1. *If $P \notin \mathcal{X}(\mathbf{F}_q)$ and $\mathcal{X}(\mathbf{F}_q) = \ldots = \mathcal{X}(\mathbf{F}_{q^U})$, then $1, b_1, \ldots, b_U$ are $(\mathcal{D}_\mathcal{X}, P)$-orders.*
2. *The numbers $1, b_1, \ldots, b_U$ are $\mathcal{D}_\mathcal{X}$-orders. In particular, $\dim(\mathcal{D}_\mathcal{X}) \geq U + 1$ provided that $b_i \neq b_j$ for $i \neq j$;*
3. *If in addition (4.7) holds and $g \geq b_U$, then $\mathcal{X}$ is non-classical.*

Proof. Lemma 4.19(1) implies (1) and (2) since there are infinitely many points P such that ${\mathbf{\Phi}_q}^i(P) \neq P$ for $i = 1, \ldots, U$. To see (3) we take $P \in \mathcal{X}$ such that ${\mathbf{\Phi}_q}^{U+1}(P) \neq P$. Then $b_U \in H(P)$ by Lemma 4.19(2). If $\mathcal{X}$ were classical then $n_1(P) = g + 1$ so that $g < b_U$, a contradiction. □

Corollary 4.22. *Assume (4.6).*

(1) $\epsilon_N = \nu_{N-1} = b_U$;
(2) $\mathcal{X}(\mathbf{F}_q) \subseteq \mathrm{Supp}(R^{\mathcal{D}})$.

Proof. (1) We have $\epsilon_{N-1} \leq j_{N-1}(P)$ for any P by Corollary 2.10(1); thus $\epsilon_{N-1} < b_U$ by Corollary 4.18. Therefore $\epsilon_N = b_U$ by Corollary 4.21(2), and so

$$\phi^*(L_{N-1}(P)) = {\mathbf{\Phi}_q}^U(P) + \sum_{I=1}^{U} b_i {\mathbf{\Phi}_q}^{U-i}(P)$$

by (4.4), where ϕ is a morphism associated to $\mathcal{D}_{\mathcal{X}}$. It follows that $\phi(\mathbf{\Phi}_q(P)) \in L_{N-1}(P)$ so that $\nu_{N-1} = \epsilon_N$.

(2) By Lemma 4.17 $j_N(P) = n_N(P) = m(1)$ for each $P \in \mathcal{X}(\mathbf{F}_q)$. Since $m(1) = 1 + \sum_{i=1}^{U} b_i > b_U = \epsilon_N$ (cf. (1)), the result follows. □

Corollary 4.23. *Assume (4.7). Then $n_1(P) \leq b_U$ for each $P \in \mathcal{X}(\mathbf{F}_q)$, and equality holds provided that $\#\mathcal{X}(\mathbf{F}_q) \geq q b_U + 1$.*

Proof. Let $P \in \mathcal{X}(\mathbf{F}_q)$. By Lemma 2.30 $n_1(P) \leq n_1(Q)$ where $Q \notin \mathcal{W}$. Therefore $n_1(P) \leq b_U$ by Lemma 4.19(2). Now if $\#\mathcal{X}(\mathbf{F}_q) \geq q b_U + 1$, then $1 + q n_1(P) \geq q b_U + 1$ by Remark 4.10 and the result follows. □

4.2. The Hermitian curve. Let $\mathcal{X}$ be a $\mathbf{F}_{\ell^2}$-maximal curve of genus g. Recall that $g \leq \ell(\ell+1)/2$ by Corollary 4.3 and that the Hermitian curve is $\mathbf{F}_{\ell^2}$-maximal of genus $\ell(\ell-1)/2$ (cf. Example 3.15). From Lemma 4.2 and (4.5), $\mathcal{X}$ is equipped with the linear series $\mathcal{D}_{\mathcal{X}} := |(\ell+1)P_0|$. By Corollary 4.16, $\mathcal{D}_{\mathcal{X}}$ is simple and base-point-free. We see that $\mathcal{X}$ satisfies (4.7) (and hence (4.6)); in particular $1, \ell$ are $\mathcal{D}_{\mathcal{X}}$ orders so that $N := \dim(\mathcal{D}_{\mathcal{X}}) \geq 2$.

Theorem 4.24. ([26, Thm. 2.4]) *Let $\mathcal{X}$ be a $\mathbf{F}_{\ell^2}$-maximal curve of genus g. The following statements are equivalent:*

(1) *$\mathcal{X}$ is $\mathbf{F}_{\ell^2}$-isomorphic to the Hermitian curve $\mathcal{H}$ of equation (3.6)*;
(2) $g > (\ell-1)^2/4$;
(3) $N = 2$.

Proof. (1) implies (2) because the genus of $\mathcal{H}$ is $\ell(\ell-1)/2$. Assume (2) and suppose that $N \geq 3$. Then Castelnuovo's genus bound (Remark 1.7) applied to $\mathcal{D}_{\mathcal{X}}$ would yield $g \leq (\ell-1)^2/4$, a contradiction. Finally let $N = 2$. By (4.4) $(\ell+1)P \sim (\ell+1)P_0$ for

any $P \in \mathcal{X}(\mathbf{F}_{\ell^2})$ and hence we can assume that $\ell, \ell+1 \in H(P_0)$ by Lemma 4.15(2); in this case, as $N = 2$, $n_1(P_0) = \ell$ and $n_2(P_0) = \ell+1$. Let $\epsilon_0 = 0 < \epsilon_1 = 1 < \epsilon_2$ (resp. $\nu_0 = 0 < \nu_1$) denote the $\mathcal{D}_{\mathcal{X}}$-orders (resp. $\mathbf{F}_{\ell^2}$-orders) of $\mathcal{X}$. Then $\epsilon_2 = \nu_1 = \ell$ by Corollary 4.22. Let $x, y \in \mathbf{F}_{\ell^2}(\mathcal{X})$ such that $\mathrm{div}_\infty(x) = \ell P_0$ and $\mathrm{div}_\infty(y) = (\ell+1)P_0$. We have that$x$ is a separating variable (Lemma 1.24) and therefore

$$(*) \qquad V^{0,1}_{1,x,y,;x} = \det \begin{pmatrix} 1 & x^{\ell^2} & y^{\ell^2} \\ 1 & x & y \\ 0 & 1 & D^1_x y \end{pmatrix} = (x - x^{\ell^2}) D^1_x y - (y - y^{\ell^2}) = 0\,.$$

Claim. There exists $f \in \mathbf{F}^-_{\ell^2}(\mathcal{X})$ such that $D^1_x y = f^\ell$.

To proof this we have to show that $D^i_x(D^1_x y) = 0\,(*_1)$ for $1 \le i < \ell$ by Remark 2.5(ii). We apply D^1_x to $(*)$: $(x - x^{\ell^2}) D^1_x(D^1_x y) = 0$ and so $(*_1)$ holds for $i = 1$. Suppose that $(*_1)$ is true for $i = 1, \ldots, j$, $1 \le j \le \ell - 2$. We apply D^{j+1}_x to $(*)$ and using the inductive hypothesis and Remark 2.5(i) we find that $(x - x^{\ell^2}) D^{j+1}_x(D^1_x y) = D^{j+1}_x y$. It turns out that

$$W^{0,1,j+1}_{1,x,y;x} = \begin{pmatrix} 1 & x & y \\ 0 & 1 & D^1_x y \\ 0 & 0 & D^{j+1}_x y \end{pmatrix} = D^{j+1}_x y = 0\,,$$

since $\epsilon_2 = \ell$, and the claim follows.

Claim. $\#x^{-1}(x(P)) = \ell$ for $P \neq P_0$.

From $(*)$ $v_{P_0}(D^1_x y) = -\ell^2$. Let t be a local parameter at P_0. Then $v_{P_0}(D^1_t x) = \ell^2 - l - 2$ since $D^1_t y = D^1_t x D^1_x y$ by the chain rule (2.3). We have that $\deg(dx) = 2g - 2$ (see Example 1.1) and that $v_P(x) \ge 0$ for $P \neq P_0$. Therefore $2g - 2 \ge \ell^2 - l - 2$; i.e., $g \ge l(l-2)/2$; i.e. $g = \ell(\ell-1)/2$ by Corollary 4.3. It follows that $v_P(dx) = 0$ for $P \neq P_0$ and so the claim.

We conclude that $D^1_x y = f^\ell$ with $\mathrm{div}_i nftyf = \ell P_0$; moreover $f \in \mathbf{F}_q(\mathcal{X})$ since $D^1_x y \in \mathbf{F}_q(\mathcal{X})$. Then $f = a + bx$ with $a, b \in \mathbf{F}_{\ell^2}$ and $(*)$ gives a relation of type

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

Finally we have that $y_1^\ell + y_1 - x_1^{\ell+1} = c \in \mathbf{F}_\ell$ and with $y_2 := y_1 + \lambda$, $\lambda^\ell + \lambda = a$, we have that (3.6) holds; i.e., $\mathcal{X}$ is $\mathbf{F}_{\ell^2}$-isomorphic to $\mathcal{H}$. □

Corollary 4.25. ([25]) *The genus g of a $\mathbf{F}_{\ell^2}$-maximal curve satisfies*

$$\textit{either} \qquad g \le (\ell-1)^2/4 \qquad \textit{or} \qquad g = \ell(\ell-1)/2\,.$$

Remark 4.26. This result was improved in [68] where it is shown that $g \le (\ell^2 - \ell + 1)/6$ whenever $g < (\ell-1)^2/4$.

4.3. The Suzuki curve. Set $q_0 := 2^s$, $s \in \mathbf{N}$, $q := 2q_0^2$. Let $\mathcal{X}$ be a curve defined over $\mathbf{F}_q$ of genus g such that

$$g = q_0(q-1) \qquad \text{and} \qquad \#\mathcal{X}(\mathbf{F}_q) = q^2 + 1\,. \tag{4.8}$$

The main result of this sub-section is the following theorem which improves Theorem 4.12 for the Suzuki curve $\mathcal{S}$.

Theorem 4.27. *A curve $\mathcal{X}$ defined over $\mathbf{F}_q$ is $\mathbf{F}_q$-isomorphic to the Suzuki curve $\mathcal{S}$ if and only if (4.8) hold true.*

If (4.8) hold, then $h_{\mathcal{X},q}(t) = (t^2 + 2q_0t + q)^g$ by Lemma 4.13(1), and from (4.5) we see that $\mathcal{X}$ is equipped with the linear series

$$\mathcal{D}_{\mathcal{X}} = |(q + 2q_0 + 1)P_0|\,, \qquad P_0 \in \mathcal{X}(\mathbf{F}_q)\,.$$

The results of Sect. 4.1 applied to this case are summarized in the following proposition. Let $N := \dim(\mathcal{D}_{\mathcal{X}})$, $\epsilon_0 = 0 < \epsilon_1 = 1 < \ldots < \epsilon_N$ (resp. $\nu_0 = 0 < \ldots < \nu_{N-1}$) be the $\mathcal{D}_{\mathcal{X}}$-orders (resp. $\mathbf{F}_q$-Frobenius orders) of $\mathcal{X}$.

Proposition 4.28. (1) *$j_N(P) = n_N(P) = q + 2q_0 + 1$ for any $P \in \mathcal{X}(\mathbf{F}_q)$; in addition, there exists $P_1 \in \mathcal{X}(\mathbf{F}_q)$ such that $n_{N-1}(P_1) = q + 2q_0$;*

(2) *$\mathcal{D}_{\mathcal{X}}$ is simple and base-point-free;*

(3) *$2q_0$ and q are $\mathcal{D}_{\mathcal{X}}$-orders so that $N \geq 3$;*

(4) *$\epsilon_N = \nu_{N-1} = q$;*

(5) *$n_1(P) = q$ for any $P \in \mathcal{X}(\mathbf{F}_q)$.*

From (5) and (1) above and Lemma 4.17, $j_{N-1}(P) = j_N(P) - n_1(P) = 2q_0 + 1$ for any $P \in \mathcal{X}(\mathbf{F}_q)$ so that

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

Lemma 4.29. $\epsilon_{N-1} = 2q_0$.

Proof. Suppose that $\epsilon_{N-1} > 2q_0$. Then $\epsilon_{N-2} = 2q_0$ and $\epsilon_{N-1} = 2q_0 + 1$. By Corollary 3.9(1) $\nu_{N-2} \leq j_{N-1}(P) - j_1(P) \leq 2q_0 = \epsilon_{N-2}$, and thus the $\mathbf{F}_q$-Frobenius orders of $\mathcal{D}_{\mathcal{X}}$ would be $\epsilon_0, \epsilon_1, \ldots, \epsilon_{N-2}$, and ϵ_N. Now from Proposition 3.5(1)

$$v_P(S) \geq \sum_{i=1}^{N} (j_i(P) - \nu_{i-1}) \geq (N-1)j_1(P) + 1 + 2q_0 \geq N + 2q_0\,, \tag{4.9}$$

for $P \in \mathcal{X}(\mathbf{F}_q)$ so that $\deg(S) = (\sum_i \nu_i)(2g-2) + (q+N)(q+2q_0+1) \geq (N + 2q_0)\#\mathcal{X}(\mathbf{F}_q)$. From the identities $2g - 2 = (2q_0 - 2)(q + 2q_0 + 1)$ and $\#\mathcal{X}(\mathbf{F}_q) = (q - 2q_0 + 1)(q + 2q_0 + 1)$ we would have

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

Now, as $\epsilon_i + \epsilon_j \leq \epsilon_{i+j}$ for $i + j \leq N$ by Corollary 2.14,

$$(N-1)2q_0 = (N-1)\epsilon_{N-2} \geq 2\sum_{i=0}^{N-2} \epsilon_i \geq 2(N-1)q_0\,,$$

and hence $\epsilon_i + \epsilon_{N-2-i} = \epsilon_{N-2}$ for $i = 0, \ldots, N-2$. In particular, $\epsilon_{N-3} = 2q_0 - 1$ and by the p-adic criterion (Lemma 2.21) we would have $\epsilon_i = i$ for $i = 0, 1, \ldots, N-3$. Then $N = 2q_0 + 2$. Now from Castelnuovo's genus bound (Remark 1.7)

$$2g = 2q_0(q-1) \leq (q + 2q_0 - (N-1)/2)^2)/(N-1)\,;$$

i.e., $2q_0(q-1) < (q+q_0)^2/2q_0 = q_0 q + q/2 + q_0/2$, a contradiction. □

Corollary 4.30. *There exists $P_1 \in \mathcal{X}(\mathbf{F}_q)$ such that*

$$\begin{cases} j_1(P_1) = 1 \\ j_i(P_1) = \nu_{i-1} + 1 \quad \textit{if } i = 2, \ldots, N-1. \end{cases}$$

Proof. Since we already observed that $v_P(S) \geq (N-1)j_1(P) + 2q_0 + 1 \geq N + 2q_0$ for $P \in \mathcal{X}(\mathbf{F}_q)$, it is enough to show that there exists $P_1 \in \mathcal{X}(\mathbf{F}_q)$ such that $v_{P_1}(S) = N + 2q_0$. Suppose that $v_P(S) \geq N + 2q_0 + 1$ for any $P \in \mathcal{X}(\mathbf{F}_q)$. Then by Theorem 3.13

$$\sum_{i=0}^{N-1} \nu_i \geq q + Nq_0 + 1\ ,$$

so that

$$\sum_{i=0}^{N-1} \epsilon_i \geq Nq_0 + 2\,,$$

because $\epsilon_1 = 1$, $\nu_{N-1} = q$ and $\nu_i \leq \epsilon_{i+1}$. Then from Corollary 2.14 we would have $N\epsilon_{N-1} \geq 2Nq_0 + 4$; i.e., $\epsilon_{N-1} > 2Nq_0$, a contradiction by Lemma 4.29. □

Lemma 4.31. (1) $\nu_1 > \epsilon_1 = 1$;
(2) ϵ_2 *is a power of two.*

Proof. If $\nu_1 > \epsilon_1 = 1$, then $\nu_1 = \epsilon_2$ and it must be a power of two by the p-adic criterion (Lemma 2.21): i.e., (1) implies (2). Suppose now that $\nu_1 = 1$. Then from Corollary 4.30 there exists a point $P_1 \in \mathcal{X}(\mathbf{F}_q)$ such that $j_1(P_1) = 1, j_2(P_1) = 2$; thus

$$H(P_1) \subseteq H := \langle q, q + 2q_0 - 1, q + 2q_0, q + 2q_0 + 1\rangle\,,$$

by Proposition 4.28(1)(5) and Lemma 4.17. In particular $g = q_0(q-1) \leq \tilde{g} := \#(\mathbf{N}_0 \setminus H)$. This is a contradiction as follows immediately from the claim below.

Claim. $\tilde{g} = g - q_0^2/4$.

In fact, $L := \cup_{i=1}^{2q_0-1} L_i$ is a complete system of residues module q, where

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

Moreover, for each $\ell \in L$, $\ell \in H$ and $\ell - q \notin H$. Hence $\tilde{g}$ can be computed by summing up the coefficients of q from the above list (see e.g. [92, Thm. p.3]); i.e.,

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

□

In the remaining part of this sub-section we let $P_0 = P_1$ be a $\mathbf{F}_q$-rational point satisfying Corollary 4.30; we set $n_i := n_i(P_1)$ and $v := v_{P_1}$.

Lemma 4.31(1) implies $\nu_i = \epsilon_{i+1}$ for $i = 1, \ldots, N-1$. Therefore from Corollary 4.30 and Lemma 4.17 we have

$$\text{(4.10)} \qquad \begin{cases} n_i = 2q_0 + q - \epsilon_{N-i} & \text{if } i = 1, \ldots N-2 \\ n_{N-1} = 2q_0 + q, \quad n_N = 1 + 2q_0 + q. \end{cases}$$

Let $x, y_2, \ldots, y_N \in \mathbf{F}_q(\mathcal{X})$ be such that $\mathrm{div}_\infty(x) = n_1 P_1$, and $\mathrm{div}_\infty(y_i) = n_i P_1$ for $i = 2, \ldots, N$. The fact that $\nu_1 > 1$ means that the following matrix has rank two (see Sect. 3)

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

In particular,

$$\text{(4.11)} \qquad y_i^q - y_i = D_x^1 y_i (x^q - x) \qquad \text{for } \ i = 2, \ldots, N\,.$$

Lemma 4.32. (1) *$(2g-2)P$ is canonical for any $P \in \mathcal{X}(\mathbf{F}_q)$; i.e., the Weierstrass semigroup at such a P is symmetric*;

(2) *Let $m \in H(P_1)$ such that $m < q + 2q_0$. Then $m \le q + q_0$*;

(3) *There exists $g_i \in \mathbf{F}_q(\mathcal{X})$ such that $D_x^1 y_i = g_i^{\epsilon_2}$ for $i2, \ldots, N$. Furthermore,* $\mathrm{div}_\infty(g_i) = \frac{qm_i - q^2}{\epsilon_2} P_1$.

Proof. (1) By the identity $2g - 2 = (2q_0 - 2)(q + 2q_0 + 1)$ and (4.4) we can assume $P = P_1$. Now the case $i = N$ of Eqs. (4.11) implies $v(dx) = 2g - 2$ and the result follows since $v_P(dx) \ge 0$ for $P \ne P_1$.

(2) From (4.10), $q, q+2q_0$ and $q+2q_0+1 \in H(P_1)$. Then the numbers

$$(2q_0-2)q+q-4q_0+j \qquad j=0,\dots,q_0-2$$

are also non-gaps at P_1. Therefore, by the symmetry of $H(P_1)$,

$$q+q_0+1+j \qquad j=0,\dots,q_0-2$$

are gaps at P_1 and the proof follows.

(3) Set $f_i := D^1_x y_i$. We have $D^j_x y_i = (x^q-x)D^j_x f_i + D^{(j-1)}_x f_i$ for $1 \le j < q$ by the product rule applied to (4.11). Then, $D^j_x f_i = 0$ for $1 \le j < \epsilon_2$, because the matrices

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

have rank two (see Sect. 2.2). Consequently, as ϵ_2 is a power of two by Lemma 4.31(2)), from Remark 2.5(2), $f_i = g_i^{\epsilon_2}$ for some $g_i \in \mathbf{F}_q(\mathcal{X})$. Finally, from the proof of (1) we have that $x - x(P)$ is a local parameter at P if $P \neq P_1$. Then, by the election of the y_i's, g_i has no pole but in P_1, and from (4.11), $v(g_i) = -(qm_i - q^2)/\epsilon_2$. □

Lemma 4.33. *$N = 4$ and $\epsilon_2 = q_0$.*

Proof. We know that $N \ge 3$. We claim that $N \ge 4$ otherwise we would have $\epsilon_2 = 2q_0$, $n_1 = q$, $n_2 = q+2q_0$, $n_3 = q+2q_0+1$, and hence $v(g_2) = -q$ (with g_2 being as in Lemma 4.32(3)). Therefore, after some $\mathbf{F}_q$-linear transformations, the case $i = 2$ of (4.11) reads

$$y_2^q - y_2 = x^{2q_0}(x^q - x)\,.$$

Now the function $z := y_2^{q_0} - x^{q_0+1}$ satisfies $z^q - z = x^{q_0}(x^q - x)$ and we find that $q_0 + q$ is a non-gap at P_1 (cf. [43, Lemma 1.8]). This contradiction eliminates the possibility $N = 3$.

Let $N \ge 4$ and $2 \le i \le N$. By Lemma 4.32(3) $(qn_i - q^2)/\epsilon_2 \in H(P_1)$, and since $(qn_i - q^2)/\epsilon_2 \ge n_{i-1} \ge q$, by (4.10) we have

$$2q_0 \ge \epsilon_2 + \epsilon_{N-i} \qquad \text{for } i = 2,\dots,N-2\,.$$

In particular, $\epsilon_2 \le q_0$. On the other hand, by Lemma 4.32(2) we must have $n_{N-2} \le q + q_0$ and so, by (4.10) we find that $\epsilon_2 \ge q_0$; i.e., $\epsilon_2 = q_0$.

Finally we show that $N = 4$. $\epsilon_2 = q_0$ implies $\epsilon_{N-2} \le q_0$. Since $n_2 \le q + q_0$ (cf. Lemma 4.32(2)), by (4.10), we have $\epsilon_{N-2} \ge q_0$. Therefore $\epsilon_{N-2} = q_0 = \epsilon_2$ so that $N = 4$. □

Proof of Theorem 4.27. Let $P_1 \in \mathcal{X}(\mathbf{F}_q)$ be as above. By (4.11), Lemma 4.32(3) and Lemma 4.33 we have the following equation

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

where g_2 has no pole except at P_1. Moreover, by (4.10), $n_2 = q_0 + q$ and so $v(g_2) = -q$ (cf. Lemma 4.32(3)). Thus $g_2 = ax + b$ with $a, b \in \mathbf{F}_q$, $a \neq 0$, and after some $\mathbf{F}_q$-linear transformations (as those in the proof of Theorem 4.24) the result follows.

Remark 4.34. (i) From the above computations we conclude that the Suzuki curve $\mathcal{S}$ is equipped with a complete, simple and base-point-free $g^4_{q+2q_0+1}$, namely $\mathcal{D}_{\mathcal{S}} = |(q + 2q_0 + 1)P_0|$, $P_0 \in \mathcal{S}(\mathbf{F}_q)$. Such a linear series is an $\mathbf{F}_q$-invariant. The orders of $\mathcal{D}_{\mathcal{S}}$ (resp. the $\mathbf{F}_q$-Frobenius orders) are $0, 1, q_0, 2q_0$ and q (resp. $0, q_0, 2q_0$ and q).

(ii) There exists $P_1 \in \mathcal{S}(\mathbf{F}_q)$ such that the $(\mathcal{D}_{\mathcal{S}}, P_1)$-orders are $0, 1, q_0 + 1, 2q_0 + 1$ and $q + 2q_0 + 1$ (Corollary 4.30). Now we show that the above sequence is, in fact, the $(\mathcal{D}_{\mathcal{S}}, P)$-orders for each $P \in \mathcal{S}(\mathbf{F}_q)$. To see this, notice that

$$\deg(S) = (3q_0 + q)(2g - 2) + (q + 4)(q + 2q_0 + 1) = (4 + 2q_0)\#\mathcal{S}(\mathbf{F}_q).$$

Let $P \in \mathcal{S}(\mathbf{F}_q)$. By (4.9) we conclude that $v_P(S^{\mathcal{D}}) = \sum_{i=1}^{4}(j_i(P) - \nu_{i-1}) = 4 + 2q_0$ and so, by Proposition 3.5(1) that $j_1(P) = 1$, $j_2(P) = q_0 + 1$, $j_3(P) = 2q_0 + 1$, and $j_4(P) = q + 2q_0 + 1$.

(iii) Then, by Lemma 4.17 $H(P)$ contains the semigroup $H := \langle q, q + q_0, q + 2q_0, q + 2q_0 + 1\rangle$ whenever $P \in \mathcal{S}(\mathbf{F}_q)$. Indeed $H(P) = H$ since $\#(\mathbb{N}_0 \setminus H) = g = q_0(q-1)$ (this can be proved as in the claim in the proof of Lemma 4.31(1); see also [43, Appendix]).

(iv) We have

$$\deg(R) = \sum_{i=0}^{4} \epsilon_i(2g - 2) + 5(q + 2q_0 + 1) = (2q_0 + 3)\#\mathcal{S}(\mathbf{F}_q)\,,$$

and $v_P(R) = 2q_0 + 3$ for $P \in \mathcal{S}(\mathbf{F}_q)$ as follows from (i), (ii) and Sect. 2.2. Therefore the set of $\mathcal{D}_{\mathcal{S}}$-Weierstrass points of $\mathcal{S}$ is equal to $\mathcal{S}(\mathbf{F}_q)$. In particular, the $(\mathcal{D}, P)$-orders for $P \notin \mathcal{S}(\mathbf{F}_q)$ are $0, 1, q_0, 2q_0$ and q.

(v) We can use the above computations to obtain information on orders for the canonical morphism on $\mathcal{S}$. By using the fact that $(2q_0 - 2)\mathcal{D}_{\mathcal{S}}$ is canonical (cf. Lemma 4.32(1)) and (iv), we see that the set $\{a + q_0 b + 2q_0 c + qd : a + b + c + d \leq 2q_0 - 2\}$ is contained in the set of orders of $\mathcal{K}_{\mathcal{S}}$ at non-rational points. (By considering first order differentials on $\mathcal{S}$, similar computations were obtained in [30, Sect. 4].)

(vi) Finally, we remark that $\mathcal{S}$ is non-classical for the canonical morphism: We have two different proofs for this fact: loc. cit. and Corollary 4.21(3).

Remark 4.35. (A. Cossidente) Recall that an *ovoid* in $\mathbf{P}^N(\mathbf{F}_q)$ is a set of points P no three of which are collinear and such that for each P the union of the tangent lines at P is a hyperplane; see [49]. We are going to related the Suzuki-Tits ovoid $\mathcal{O}$ in $\mathbf{P}^4(\mathbf{F}_q)$ with the $\mathbf{F}_q$-rational points of the Suzuki curve $\mathcal{S}$.

It is known that any ovoid in $\mathbf{P}^4(\mathbf{F}_q)$ that contains the point $(0 : 0 : 0 : 0 : 1)$ can be defined by

$$\{(1 : a : b : f(a, b) : af(a, b) + b^2) : a, b \in \mathbf{F}_q\} \cup \{(0 : 0 : 0 : 0 : 1)\},$$

where $f(a,b) := a^{2q_0+1} + b^{2q_0}$; cf. [102], [85, p.3].

Let $\phi = (1 : x : y : z : w)$ be the morphism associated to $\mathcal{D}_{\mathcal{S}}$ such that $\mathrm{div}_\infty(x) = qP_0$, $\mathrm{div}_\infty(y) = (q+q_0)P_0$, $\mathrm{div}_\infty(z) = (q+2q_0)P_0$ and $\mathrm{div}_\infty(w) = q+2q_0+1$; see Remark 4.34(iii).

Claim. $\mathcal{O} = \phi(\mathcal{S}(\mathbf{F}_q))$.

Indeed we have $\phi(P_0) = (0:0:0:0:1)$; in addition the coordinates of ϕ can be choosen such that $y^q - y = x^{q_0}(x^q - x)$, $z := x^{2q_0+1} + y^{2q_0}$, and $w := xy^{2q_0} + z^{2q_0} = xy^{2q_0} + x^{2q+2q_0} + y^{2q}$ (see [43, Sect. 1.7]). For $P \in \mathcal{S}(\mathbf{F}_q)\setminus\{P_0\}$ set $a := x(P)$, $b := y(P)$, and $f(a,b) := z(a,b)$. Then $w(a,b) = af(a,b) + b^2$ and the claim follows.

Remark 4.36. The morphism ϕ in the previous remark is an embedding. To see this, as $j_1(P) = 1$ for any $P \in \mathcal{S}$ (Remarks 4.34(ii)(iv)), it is enough to show that ϕ is injective. We have

$$(q+2q_0+1)P_0 \sim q{\boldsymbol{\Phi}_q}^2(P) + 2q_0\boldsymbol{\Phi}_q(P) + P \tag{4.12}$$

so that the points $P \in \mathcal{S}$ where ϕ could not be injective satisfy either $P \notin \mathcal{S}(\mathbf{F}_q)$, or ${\boldsymbol{\Phi}_q}^3(P) = P$ or ${\boldsymbol{\Phi}_q}^2(P) = P$. Now from the Zeta function of $\mathcal{S}$ one sees that $\#\mathcal{S}(\mathbb{F}_{q^3}) = \#\mathcal{S}(\mathbb{F}_{q^2}) = \#\mathcal{S}(\mathbf{F}_q)$, and the remark follows.

Remark 4.37. From the claim in Remark 4.35, (4.12) and [48] we have

$$\mathrm{Aut}_{\overline{\mathbf{F}}_q}(\mathcal{S}) = \mathrm{Aut}_{\mathbf{F}_q}(\mathcal{S}) \cong \{A \in \mathrm{PGL}(5,q) : A\mathcal{O} = \mathcal{O}\}\,.$$

5. Plane arcs

In this section we show how to apply Sections 2 and 3 to study the size of plane arcs. The approach is from Hirschfeld-Korchmáros [50], [51] and Voloch [106], [107]. Our exposition follows [36].

A *k-arc* in $\mathbf{P}^2(\mathbf{F}_q)$ is a set $\mathcal{K}$ of k points no three of which are collinear. It is *complete* if it is not properly contained in another arc. For a given q, a basic problem in Finite Geometry is to find the values of k for which a complete k-arc exists. Bose [6] showed that

$$k \le m(2,q) := \begin{cases} q+1 & \text{if } q \text{ is odd}\,, \\ q+2 & \text{otherwise}\,. \end{cases}$$

For q odd the bound $m(2,q)$ is attained if and only if $\mathcal{K}$ is an irreducible conic [90], [49, Thm. 8.2.4]. For q even the bound is attained by the union of an irreducible conic and its nucleus, and not every $(q+2)$-arc arises in this way; see [49, Sect. 8.4]. Let $m'(2,q)$ denote the second largest size that a complete arc in $\mathbf{P}^2(\mathbf{F}_q)$ can have. Segre [90], [49, Sect. 10.4] showed that

$$m'(2,q) \le \begin{cases} q - \frac{1}{4}\sqrt{q} + \frac{7}{4} & \text{if } q \text{ is odd,} \\ q - \sqrt{q} + 1 & \text{otherwise.} \end{cases} \tag{5.1}$$

Besides small q, namely $q \leq 29$ [11], [49], [53], the only case where $m'(2,q)$ has been determined is for q an even square. Indeed, for q square, examples of complete $(q - \sqrt{q}+1)$-arcs [5], [12], [18], [23], [60] show that

$$m'(2,q) \geq q - \sqrt{q} + 1\,, \tag{5.2}$$

and so the bound (5.1) for an even q square is sharp. This result has been recently extended by Hirschfeld and Korchmáros [52] who showed that the third largest size that a complete arc can have is upper bounded by $q - 2\sqrt{q} + 6$.

If q is not a square, Segre's bounds were notably improved by Voloch [106], [107].

If q is odd, Segre's bound was slightly improved to $m'(2,q) \leq q - \sqrt{q}/4 + 25/16$ by Thas [101]. If q is an odd square and large enough, Hirschfeld and Korchmáros [51] significantly improved the bound to

$$m'(2,q) \leq q - \frac{1}{2}\sqrt{q} + \frac{5}{2}\,. \tag{5.3}$$

Inequalities (5.2) and (5.3) suggest the following problem, which seems to be difficult and has remained open since the 60's.

Problem 5.1. For q an odd square, is it true that $m'(2,q) = q - \sqrt{q} + 1$?

The answer is negative for $q = 9$ and affirmative for $q = 25$ [11], [49], [53]. So Problem 5.1 is indeed open for $q \geq 49$.

5.1. B. Segre's fundamental theorem: Odd case. We recall a fundamental theorem of Segre which is the link between arcs and curves.

Let $\mathcal{K}$ be an arc in $\mathbf{P}^2(\mathbf{F}_q)$. Segre associates to $\mathcal{K}$ a plane curve $\mathcal{C}$ in the dual plane of $\mathbf{P}^2(\bar{\mathbf{F}}_q)$. This curve is defined over $\mathbf{F}_q$ and it is called *the envelope of* $\mathcal{K}$. For $P \in \mathbf{P}^2(\bar{\mathbf{F}}_q)$, let ℓ_P denote the corresponding line in the dual plane. A line ℓ in $\mathbf{P}^2(\mathbf{F}_q)$ is called an *i-secant* of $\mathcal{K}$ if $\#\mathcal{K} \cap \ell = i$. The following result summarizes the main properties of $\mathcal{C}$ for the odd case.

Theorem 5.2. (B. Segre [90], [49, Sect. 10]) *If q is odd, then the following statements hold:*

1. *The degree of $\mathcal{C}$ is $2t$, with $t = q - k + 2$ being the number of 1-secants through a point of $\mathcal{K}$.*
2. *All kt of the 1-secants of $\mathcal{K}$ belong to $\mathcal{C}$.*
3. *Each 1-secant ℓ of $\mathcal{K}$ through a point $P \in \mathcal{K}$ is counted twice in the intersection of $\mathcal{C}$ with ℓ_P; i.e., $I(\mathcal{C}, \ell_P; \ell) = 2$.*
4. *The curve $\mathcal{C}$ contains no 2-secant of $\mathcal{K}$.*
5. *The irreducible components of $\mathcal{C}$ have multiplicity at most two, and $\mathcal{C}$ has at least one component of multiplicity one.*

(6) *For $k > (2q+4)/3$, the arc $\mathcal{K}$ is incomplete if and only if $\mathcal{C}$ admits a linear component over $\mathbf{F}_q$. For $k > (3q+5)/4$, the arc $\mathcal{K}$ is a conic if and only if it is complete and $\mathcal{C}$ admits a quadratic component over $\mathbf{F}_q$.*

Next we show some properties of $\mathcal{C}$. Recall that a non-singular point P of a plane curve $\mathcal{A}$ is called an *inflexion point of* $\mathcal{A}$ if $I(\mathcal{A}, \ell; P) > 2$, with ℓ being the tangent line of $\mathcal{A}$ at P.

Definition. A point P_0 of $\mathcal{C}$ is called *special* if the following conditions hold:

(i) it is non-singular;
(ii) it is $\mathbf{F}_q$-rational;
(iii) it is not an inflexion point of $\mathcal{C}$.

Then, by (i), a special point P_0 belongs to an unique irreducible component of the envelope which will be called *the irreducible envelope* associated to P_0 or *an irreducible envelope of* $\mathcal{K}$.

Lemma 5.3. *Let $\mathcal{C}_1$ be an irreducible envelope of $\mathcal{K}$. Then*

(1) *$\mathcal{C}_1$ is defined over $\mathbf{F}_q$;*
(2) *if q is odd and the k-arc $\mathcal{K}$, with $k > (3q+5)/4$, is complete and different from a conic, then the degree of $\mathcal{C}_1$ is at least three.*

Proof. (1) Let $\mathcal{C}_1$ be associated to P_0, let $\mathbf{\Phi}$ be the Frobenius morphism (relative to $\mathbf{F}_q$) on the dual plane of $\mathbf{P}^2(\bar{\mathbf{F}}_q)$, and suppose that $\mathcal{C}_1$ is not defined over $\mathbf{F}_q$. Then, since the envelope is defined over $\mathbf{F}_q$ and P_0 is $\mathbf{F}_q$-rational, P_0 would belong to two different components of the envelope, namely $\mathcal{C}_1$ and $\mathbf{\Phi}(\mathcal{C}_1)$. This is a contradiction because the point is non-singular.

(2) This follows from Theorem 5.2(6). □

The next result will show that special points do exist provided that q is odd and the arc is large enough.

Proposition 5.4. *Let $\mathcal{K}$ be an arc in $\mathbf{P}^2(\mathbf{F}_q)$ of size k such that $k > (2q+4)/3$. If q is odd, then the envelope $\mathcal{C}$ of $\mathcal{K}$ has special points.*

Remark 5.5. The hypothesis $k > (2q+4)/3$ in the proposition is equivalent to $k > 2t$, with $t = q - k + 2$. Also, under this hypothesis, the envelope $\mathcal{C}$ is uniquely determined by $\mathcal{K}$, see [49, Thm. 10.4.1(i)].

To prove Proposition 5.4 we need the following lemma.

Lemma 5.6. *Let $\mathcal{A}$ be a plane curve defined over $\bar{\mathbf{F}}_q$ and suppose that it has no multiple components. Let α be the degree of $\mathcal{A}$ and s the number of its singular points. Then,*

$$s \leq \binom{\alpha}{2},$$

and equality holds if $\mathcal{A}$ consists of α lines no three concurrent.

Proof. That a set of α lines no three concurrent satisfies the bound is trivial. Let $G = 0$ be the equation of $\mathcal{A}$, let $G = G_1 \dots G_r$ be the factorization of G in $\bar{\mathbf{F}}_q[X, Y]$, and let $\mathcal{A}_i$ be the curve given by $G_i = 0$. For simplicity we assume α even, say $\alpha = 2M$. Setting $\alpha_i := \deg(G_i)$, $i = 1, \dots, r$ and $I := \sum_{i=1}^{r-1} \alpha_i$ we have $\alpha_r = 2M - I$. The singular points of $\mathcal{A}$ arise from the singular points of each component and from the points in $\mathcal{A}_i \cap \mathcal{A}_j$, $i \neq j$. Recall that an irreducible plane curve of degree d has at most $\binom{d-1}{2}$ singular points, and that $\#\mathcal{A}_i \cap \mathcal{A}_j \leq a_i a_j$, $i \neq j$ (Bézout's Theorem). So

$$
\begin{aligned}
s &\leq \sum_{i=1}^{r-1} \binom{\alpha_i - 1}{2} + \binom{2M - I - 1}{2} + \sum_{1 \leq i_1 < i_2 \leq r-1} \alpha_{i_1} \alpha_{i_2} + \sum_{i=1}^{r-1} (2M - I)\alpha_i \\
&= \sum_{i=1}^{r-1} \frac{\alpha_i^2 - 3\alpha_i + 2}{2} + \frac{4M^2 - 4MI + I^2 - 6M + 3I + 2}{2} + \sum_{1 \leq i_1 < i_2 \leq r-1} \alpha_{i_1} \alpha_{i_2} + (2M - I)I \\
&= \frac{1}{2}[\sum_{i=1}^{r-1} \alpha_i^2 - 3I + 2(r-1) + 4M^2 - 4MI + I^2 - 6M + 3I + 2 + \\
&\quad 2 \sum_{1 \leq i_1 < i_2 \leq r-1} \alpha_{i_1} \alpha_{i_2} + 4MI - 2I^2] \\
&\leq 2M^2 - 3M + \alpha = 2M^2 - M \,.
\end{aligned}
$$

□

Proof. (*Proposition 5.4*) Let $F = 0$ be the equation of $\mathcal{C}$ over $\mathbf{F}_q$. By Theorem 5.2(5), F admits a factorization in $\bar{\mathbf{F}}_q[X, Y, Z]$ of type

$$G_1 \dots G_r H_1^2 \dots H_s^2 \,,$$

with $r \geq 1$ and $s \geq 0$. Let $\mathcal{A}$ be the plane curve given by

$$G := G_1 \dots G_r = 0 \,.$$

Then $\mathcal{A}$ satisfies the hypothesis of Lemma 5.6 and it has even degree by Theorem 5.2(1). From Theorem 5.2(3) and Bézout's theorem, for each line ℓ_P (in the dual plane) corresponding to a point $P \in \mathcal{K}$, we have

$$\#(\mathcal{A} \cap \ell_P) \geq M \,,$$

where $2M = \deg(G)$, and so at least kM points corresponding to unisecants of $\mathcal{K}$ belong to $\mathcal{A}$. Since $k > 2t$ (see Remark 5.5) and $2t \geq 2M$, then $kM > 2M^2$ and from Lemma 5.3 we have that at least one of the unisecant points in $\mathcal{A}$, says P_0, is non-singular. Suppose that P_0 passes through $P \in \mathcal{K}$. The point P_0 is clearly $\mathbf{F}_q$-rational and P_0 is not a point of the curve of equation $H = 0$: otherwise $I(P_0, \mathcal{C} \cap \ell_P) > 2$ (see Theorem 5.2(3)). Then, $I(P_0, \mathcal{C} \cap \ell_P) = I(P_0, \mathcal{A} \cap \ell_P) = 2$ and so ℓ_P is the tangent of $\mathcal{C}$ at P_0. Therefore P_0 is not an inflexion point of $\mathcal{C}$, and the proof of Proposition 5.4 is complete. □

Let $\mathcal{C}_1$ be an irreducible envelope associated to a special point P_0, and

$$\pi : \mathcal{X} \to \mathcal{C}_1 ,$$

the non-singular model of $\mathcal{C}_1$. Then by Lemma 5.3(1) we can assume that $\mathcal{X}$ and π are both defined over $\mathbf{F}_q$. In particular, the linear series Σ_1 cut out by lines of $\mathbf{P}^2(\bar{\mathbf{F}}_q)^*$ on $\mathcal{X}$ is $\mathbf{F}_q$-rational. Also, there is just one point $\tilde{P}_0 \in \mathcal{X}$ such that $\pi(\tilde{P}_0) = P_0$.

Lemma 5.7. *Let q be odd. Then,*

(1) *the $(\Sigma_1, \tilde{P}_0)$-orders are $0, 1, 2$;*
(2) *the curve $\mathcal{X}$ is classical with respect to Σ_1.*

Proof. (1) follows from the proof of Proposition 5.4 while (2) from (1) and Corollary 2.10(1). □

Remark 5.8. The hypothesis q odd in Lemma 5.7 (as well as in Proposition 5.4) is necessary. In fact, from [23] and [101] follow that the envelope associated to the cyclic $(q - \sqrt{q} + 1)$-arc, with q an even square, is irreducible and $\mathbf{F}_q$-isomorphic to the curve of equation $XY^{\sqrt{q}} + X^{\sqrt{q}}Z + YZ^{\sqrt{q}} = 0$. It is not difficult to see that this curve is $\bar{\mathbf{F}}_q$-isomorphic to the Hermitian curve $\mathcal{H}$ in Example 3.15 (see e.g. [15, p. 4711]) so that it is Σ_1 non-classical.

Next consider the following sets:

$$\begin{aligned}
\mathcal{X}_1(\mathbf{F}_q) &:= \{P \in \mathcal{X} : \pi(P) \in \mathcal{C}_1(\mathbf{F}_q)\} , \\
\mathcal{X}_{11}(\mathbf{F}_q) &:= \{P \in \mathcal{X}_1(\mathbf{F}_q) : j_2^1(P) = 2j_1^1(P)\} , \\
\mathcal{X}_{12}(\mathbf{F}_q) &:= \{P \in \mathcal{X}_1(\mathbf{F}_q) : j_2^1(P) \neq 2j_1^1(P)\} ,
\end{aligned}$$

and the following numbers:

$$M_q = M_q(\mathcal{C}_1) := \sum_{P \in \mathcal{X}_{11}(\mathbf{F}_q)} j_1^1(P) , \qquad M'_q = M'_q(\mathcal{C}_1) := \sum_{P \in \mathcal{X}_{12}(\mathbf{F}_q)} j_1^1(P) , \tag{5.4}$$

where $0 < j_1^1(P) < j_2^1(P)$ denotes the (Σ_1, P)-order sequence. We have that

$$M_q + M'_q \geq \#\mathcal{X}_1(\mathbf{F}_q) \geq \#\mathcal{X}(\mathbf{F}_q) \qquad \text{and} \qquad \#\mathcal{X}_1(\mathbf{F}_q) \geq \#\mathcal{C}_1(\mathbf{F}_q) .$$

Proposition 5.9. *Let $\mathcal{K}$ be an arc of size k and d the degree of an irreducible envelope of $\mathcal{K}$. For M_q and M'_q as above we have*

$$2M_q + M'_q \geq kd .$$

To prove this proposition we first prove the following lemma.

Lemma 5.10. *Let $\mathcal{K}$ be an arc and $\mathcal{C}_1$ an irreducible envelope of $\mathcal{K}$. Let $Q \in \mathcal{K}$ and $\mathcal{A}_Q$ be the set of points of $\mathcal{C}_1$ corresponding to unisecants of $\mathcal{K}$ passing through Q. Let $u := \#\mathcal{A}_Q$ and v be the number of points in $\mathcal{A}_Q$ which are non-singular and inflexion points of $\mathcal{C}_1$. Then*

$$2(u - v) + v \geq d ,$$

where d is the degree of $\mathcal{C}_1$.

Proof. Let $P' \in \mathcal{A}_Q$. Suppose that it is non-singular and an inflexion point of $\mathcal{C}_1$. Then, from Theorem 5.2(3) and the definition of $\mathcal{A}_Q$, we have that ℓ_Q is not the tangent line of $\mathcal{C}_1$ at P', i.e. we have that $I(P', \mathcal{C}_1 \cap \ell_Q) = 1$. Now suppose that P' is either singular or a non-inflexion point of $\mathcal{C}_1$. Then from Theorem 5.2(3) we have $I(P', \mathcal{C}_1 \cap \ell_Q) \leq 2$ and the result follows from Bézout's theorem applied to $\mathcal{C}_1$ and ℓ_Q. □

Proof of Proposition 5.9. Let $Q \in \mathcal{K}$ and $\mathcal{A}_Q$ be as in Lemma 5.10. Set

$$\mathcal{Y}_Q := \{P \in \mathcal{X}_1(\mathbf{F}_q) : \pi(P) \in \mathcal{A}_Q\}\,,$$

and

$$m(Q) := 2 \sum_{P \in \mathcal{X}_{11}(\mathbf{F}_q) \cap \mathcal{Y}_Q} j_1^1(P) + \sum_{P \in \mathcal{X}_{12}(\mathbf{F}_q) \cap \mathcal{Y}_Q} j_1^1(P)\,.$$

We claim that $m(Q) \geq d$. Indeed, this claim implies the proposition since, from Theorem 5.2(4),

$$\mathcal{Y}_Q \cap \mathcal{Y}_{Q_1} = \emptyset \qquad \text{whenever} \qquad Q \neq Q_1\,.$$

To prove the claim we distinguish four types of points in $\mathcal{Y}_Q$, namely

$$\begin{aligned}
\mathcal{Y}_Q^1 :=& \{P \in \mathcal{Y}_Q : \pi(P) \text{ is non-singular and non- inflexion point of } \mathcal{C}_1\}\,,\\
\mathcal{Y}_Q^2 :=& \{P \in \mathcal{Y}_Q : \pi(P) \text{ is a non-singular inflexion point of } \mathcal{C}_1\}\,,\\
\mathcal{Y}_Q^3 :=& \{P \in \mathcal{Y}_Q : \pi(P) \text{ is a singular point of } \mathcal{C}_1 \text{ such that } \#\pi^{-1}(\pi(P)) = 1\}\,,\\
\mathcal{Y}_Q^4 :=& \{P \in \mathcal{Y}_Q : \pi(P) \text{ is a singular point of } \mathcal{C}_1 \text{ such that } \#\pi^{-1}(\pi(P)) > 1\}\,.
\end{aligned}$$

Observe that $\mathcal{Y}_Q^1 \subseteq \mathcal{X}_{11}(\mathbf{F}_q)$ and so

$$m(Q) \geq 2 \sum_{P \in \mathcal{Y}_Q^1} j_1^1(P) + \sum_{P \in \mathcal{Y}_Q^2} j_1^1(P) + \sum_{P \in \mathcal{Y}_Q^3} j_1^1(P) + \sum_{P \in \mathcal{Y}_Q^4} j_1^1(P)\,.$$

Since $j_1^1(P) > 1$ for all $P \in \mathcal{Y}_Q^4$, the above inequality becomes

$$m(Q) \geq 2\#\mathcal{Y}_Q^1 + 2\#\mathcal{Y}_Q^4 + \#\mathcal{Y}_Q^3 + \#\mathcal{Y}_Q^2\,.$$

Therefore, as to each singular non-cuspidal point of $\mathcal{C}_1$ in $\mathcal{A}_Q$ corresponds at least two points in $\mathcal{Y}_Q^3$, it follows that

$$\begin{aligned}
m(Q) \geq 2\#\{P' \in \mathcal{A}_Q : P' \text{ is either singular or not an inflexion point of } \mathcal{C}_1\} +\\
\#\{P' \in \mathcal{A}_Q : P' \text{ is a nonsingular inflexion point of } \mathcal{C}_1\}\,.
\end{aligned}$$

Then the claim follows from Lemma 5.10 and the proof of Proposition 5.9 is complete.

5.2. The work of Hirschfeld, Korchmáros and Voloch. Throughout the whole subsection we fix the following notation:

- q is a power of an odd prime p;
- $\mathcal{K}$ is a complete arc of size k such that $(3q+5)/4 < k \leq m'(2,q)$; therefore the degree of any irreducible envelope of $\mathcal{K}$ is at least three by Theorem 5.2(6);
- P_0 is a special point of the envelope $\mathcal{C}$ of $\mathcal{K}$ and the plane curve $\mathcal{C}_1$ of degree d is an irreducible envelope associated to P_0;
- $\pi : \mathcal{X} \to \mathcal{C}_1$ is the normalization of $\mathcal{C}_1$ which is defined over $\mathbf{F}_q$; as a matter of terminology, $\mathcal{X}$ will be also called an irreducible envelope of $\mathcal{K}$.
- $\tilde{P}_0$ is the only point in $\mathcal{X}$ such that $\pi(\tilde{P}_0) = P_0$; g is the genus of $\mathcal{X}$ (so that $g \leq (d-1)(d-2)/2$);
- The symbols M_q and M'_q are as in Sect. 5.1;
- Σ_1 is the linear series g^2_d cut out by lines of $\mathbf{P}^2(\bar{\mathbf{F}}_q)^*$ on $\mathcal{X}$; Σ_2 is the linear series g^5_{2d} cut out by conics of $\mathbf{P}^2(\bar{\mathbf{F}}_q)^*$ on $\mathcal{X}$; then $\Sigma_2 = 2\Sigma_1$. Notice that $\dim(\Sigma_2) = 5$ because $d \geq 3$ and that Σ_1 and Σ_2 are base-point-free;
- S is the $\mathbf{F}_q$-Frobenius divisor associated to Σ_2;
- $j_5(\tilde{P}_0)$ is the 5th positive $(\Sigma_2, \tilde{P}_0)$-order; ϵ_5 is the 5th positive Σ_2-order; ν_4 is the 4th positive $\mathbf{F}_q$-Frobenius order of Σ_2.

We apply the results in Sects. 2 and 3 to Σ_1 and Σ_2. We have already noticed that the $(\Sigma_1, \tilde{P}_0)$-orders, as well as the Σ_1-orders, are 0,1 and 2; see Lemma 5.7. Then, the $(\Sigma_2, \tilde{P}_0)$-orders are 0,1,2,3,4 and $j_5(\tilde{P}_0)$, with $5 \leq j_5(\tilde{P}_0) \leq 2d$, and the Σ_2-orders are 0,1,2,3,4 and ϵ_5 with $5 \leq \epsilon_5 \leq j_5(\tilde{P}_0)$.

Then, we compute the $\mathbf{F}_q$-Frobenius orders of Σ_2. We apply Proposition 3.5(1) to $\tilde{P}_0$ and infer that this sequence is 0,1,2,3 and ν_4, with

$$\nu_4 \in \{4, \epsilon_5\}\,.$$

Therefore

$$\deg(S) = (6+\nu_4)(2g-2) + (q+5)2d\,,$$

and

$$v_P(S) \geq 5j^2_1(P), \qquad \text{for each } P \in \mathcal{X}_1(\mathbf{F}_q)\,,$$

where $j^2_1(P)$ stands for the first positive (Σ_2, P)-order.
Claim. $j^2_1(P)$ equals $j^1_1(P)$ (the first positive (Σ_1, P)-order).

Proof. Let $\Sigma_1 = \{E + \mathrm{div}(f) : f \in \Sigma'_1 \setminus \{0\}\}$. From Sect. 2.2 we can assume that $\Sigma'_1 = \langle 1, x, y\rangle$ where

$$(*) \qquad j^1_1(P) = v_P(E) + v_P(x) \qquad \text{and} \qquad j^1_2(P) = v_P(E) + v_P(y)\,.$$

Now $\Sigma_2 = \{2E + \mathrm{div}(f) : f \in \Sigma_2' \setminus \{0\}\}$, where $\Sigma_2' = \langle 1, x, y, xy, x^2, y^2\rangle$, and there exists $f \in \Sigma_2'$ such that

$$j_1^2(P) = v_P(2E) + v_P(f)\,.$$

Let $f = a_0 + a_1x + a_2y + a_3x^2 + a_4xy + a_5y^2$. From Lemma 1.4,

$$v_P(2E) = -\min\{v_P(1), v_P(x), v_P(y), v_P(x^2), v_P(xy), v_P(y^2)\}\,.$$

Suppose that $0 \le v_P(x)$ and $0 \le v_P(y)$. Then $v_P(2E) = 0$ so that $v_P(f) = j_1^2(P) > 0$ and hence $a_0 = 0$. Then the result follows from $(*)$. Now suppose that $0 > v_P(x)$ or $0 > v_P(y)$. Then $v_P(2E) < 0$ and hence $a_i \neq 0$ for some $i \in \{1, \ldots, 5\}$. Then the result follows from $(*)$ and the fact that $v_P(f) \ge \min\{v_P(x), v_P(y), v_P(x^2), v_P(xy), v_P(y^2)\}$. □

We then have

$$\deg(S) \ge 5(M_q + M_q')\,,$$

where M_q and M_q' were defined in (5.4).

Proposition 5.11. *Let $\mathcal{K}$ be a complete arc of size k such that $(3q+5)/4 < k \le m'(2,q)$. Then*

$$k \le \min\{q - \frac{1}{4}\nu_4 + \frac{7}{4}\,,\ \frac{28+4\nu_4}{29+4\nu_4}q + \frac{32+2\nu_4}{29+4\nu_4}\}\,,$$

where ν_4 is the 4th positive $\mathbf{F}_q$-Frobenius order of the linear series Σ_2 defined on an irreducible envelope of $\mathcal{K}$.

Proof. From the computations above and Proposition 5.9,

$$\deg(S) = (6+\nu_4)(2g-2) + (q+5)2d \ge 5(M_q + M_q') \ge \frac{5}{2}kd\,.$$

Now $d(d-3) \ge 2g-2$ and $d \le 2t = 2(q+2-k)$ (Theorem 5.2(1)). Then $k(29+\nu_4) \le (28+4\nu_4)q + (32+2\nu_4)$. On the other hand, $\nu_4 \le j_5(\tilde{P}_0) - 1 \le 2d-1$ (Proposition 3.5(1)) and hence $k \le q - \nu_4/4 + 7/4$. □

Next we consider separately the cases $\nu_4 = 4$ and $\nu_4 = \epsilon_5$.

Case $\nu_4 = 4$. In this case, the corresponding irreducible envelope will be called *Frobenius classical*. Proposition 5.11 becomes the following.

Corollary 5.12. *Let $\mathcal{K}$ be a complete arc of size k such that $(3q+5)/4 < k \le m'(2,q)$. Suppose that $\mathcal{K}$ admits a Frobenius classical irreducible envelope. Then*

$$k \le \frac{44}{45}q + \frac{40}{45}\,.$$

The bound in the corollary holds in the following cases:

(A) (Voloch [107]) Whenever $q = p$ is an odd prime;

(B) (Giulietti [35]) The arc is cyclic of Singer type whose size k satisfies $2k \not\equiv -2, 1, 2, 4 \pmod p$, where $p > 5$.

For the sake of completeness let us prove (A): Let $\mathcal{C}_1$ be an irreducible envelope of $\mathcal{K}$ and d the degree of $\mathcal{C}_1$. If $p < 2d$, then $p < 4t = 4(p+2-k)$ so that $k < (3p+8)/4$ and the result follows. So let $p \geq 2d$. Then from Remark 3.10 we have that $\mathcal{C}_1$ is Frobenius classical and (A) follows from Proposition 5.11.

Next we show that, for q square and $k = m'(2,q)$, Corollary 5.12 can only hold for q small.

Corollary 5.13. *Let $\mathcal{K}$ be an arc of size $m'(2,q)$ and suppose that q is a square. Then,*

(1) *if $q > 9$, $\mathcal{K}$ has irreducible envelopes;*
(2) *if $q > 43^2$, any irreducible envelope of $\mathcal{K}$ is Frobenius non-classical.*

Proof. (1) As we mentioned in (5.2), $m'(2,q) \geq q - \sqrt{q} + 1$. Since $q - \sqrt{q} + 1 > (2q+4)/3$ for $q > 9$, (1) follows from Proposition 5.4.

(2) If existed a Frobenius classical irreducible envelope of $\mathcal{K}$, then from Lemma 5.14 and (5.2) we would have

$$q - \sqrt{q} + 1 \leq m'(2,q) \leq 44q/45 + 40/45\,.$$

so that $q \leq 43^2$. □

Case $\nu_4 = \epsilon_5$. Here, from Lemma 3.16 we have that p divides ϵ_5. More precisely we have the following result.

Lemma 5.14. *Either ϵ_5 is a power of p or $p = 3$ and $\epsilon_5 = 6$.*

Proof. We can assume $\epsilon_5 > 5$. If ϵ_5 is not a power of p, by the p-adic criterion (Lemma 2.21) we have $p \leq 3$ and $\epsilon = 6$. □

From Proposition 5.11, the case $\nu_4 = \epsilon_5 = 6$ provides the following bound:

Lemma 5.15. *Let $\mathcal{K}$ be a complete arc of size k such that $(3q+5)/4 < k \leq m'(2,q)$. Suppose that $\mathcal{K}$ admits an irreducible envelope such that $\nu_4 = \epsilon_5 = 6$. Then $p = 3$ and*

$$k \leq \frac{52}{53}q + \frac{44}{53}\,.$$

As in the case $\nu_4 = 4$, for q an even power of 3 and $k = m'(2,q)$ the case $\nu_4 = \epsilon_5 = 6$ occur only for q small. More precisely, we have the following result.

Corollary 5.16. *Let $\mathcal{K}$ be an arc of size $m'(2,q)$. Suppose that q is an even power of p and that $\mathcal{K}$ admits an irreducible envelope with $\nu_4 = \epsilon_5 = 6$. Then $p = 3$ and $q \leq 3^6$.*

Proof. From the p-adic criterion (Lemma 2.21), $p = 3$. Then from Proposition 5.11 and (5.2) we have

$$q - \sqrt{q} + 1 \leq m'(2,q) \leq 52q/53 + 44/53\,,$$

and the result follows. □

From now on we assume

$$\nu_4 = \epsilon_5 = \text{a power of } p\,.$$

Then, the bound

$$k \le q - \frac{1}{4}\nu_4 + \frac{7}{4} \tag{5.5}$$

in Proposition 5.11 and Segre's bound (5.1) provide motivation to consider three cases according as $\nu_4 > \sqrt{q}$, $\nu_4 < \sqrt{q}$, or $\nu_4 = \sqrt{q}$.

Case $\nu_4 > \sqrt{q}$. Since ν_4 is a power of p, here we have that $\nu^2 \ge pq$ and so from (5.5) the following holds:

Lemma 5.17. *Let $\mathcal{K}$ be a complete arc of size k such that $(3q+5)/4 < k \le m'(2,q)$. Suppose that $\mathcal{K}$ admits an irreducible envelope such that ν_4 is a power of p and that $\nu_4 > \sqrt{q}$. Then*

$$k \le \begin{cases} q - \frac{1}{4}\sqrt{pq} + \frac{7}{4} & \text{if } q \text{ is not a square}\,, \\ q - \frac{1}{4}p\sqrt{q} + \frac{7}{4} & \text{otherwise}\,. \end{cases}$$

If q is a square and $k = m'(2,q)$, then $\nu_4 > \sqrt{q}$ can only occur in characteristic 3:

Corollary 5.18. *Let $\mathcal{K}$ be an arc of size $m'(2,q)$. Suppose that q is an even power of p and that $\mathcal{K}$ admits an irreducible envelope with ν_4 a power of p and $\nu_4 > \sqrt{q}$. Then $p = 3$, $\nu_4 = 3\sqrt{q}$, and*

$$k \le q - \frac{3}{4}\sqrt{q} + \frac{7}{4}\,.$$

Proof. From Lemma 5.17 and (5.2) follow that $\sqrt{q}(p-4) \le 3$ and so that $p = 3$. From $\nu_4 \le 2d - 1$ and $2d \le 4t = 4(q + 2 - m'(2,q)) \le 4\sqrt{q} + 4$ we have that $\nu_4 \le 4\sqrt{q} + 3$ and it follows the assertion on ν_4. The bound on k follows from Lemma 5.17. □

Case $\nu_4 < \sqrt{q}$. Let

$$F(x) := (2x + 32 - q)/(4x + 29)\,.$$

Then the bound

$$k \le \frac{28 + 4\nu_4}{29 + 4\nu_4}q + \frac{32 + 2\nu_4}{29 + 4\nu_4}$$

in Proposition 5.11 can be written as

$$k \le q + F(\nu_4)\,. \tag{5.6}$$

For $x > 0$, $F(x)$ is an increasing function so that

$$F(\nu_4) \le \begin{cases} F(\sqrt{q/p}) = -\frac{1}{4}\sqrt{pq} + \frac{29}{16}p + \frac{1}{2} + R & \text{if } q \text{ is not a square}\,, \\ F(\sqrt{q}/p) = -\frac{1}{4}p\sqrt{q} + \frac{29}{16}p^2 + \frac{1}{2} + R & \text{otherwise}\,, \end{cases}$$

where

$$R = \begin{cases} -\frac{841p - 280}{16(4\sqrt{q/p} + 29)} & \text{if } q \text{ is not a square}\,, \\ -\frac{841p^2 - 280}{16(4\sqrt{q}/p + 29)} & \text{otherwise}\,. \end{cases}$$

Then from (5.6) and since $R < 0$ we have the following result.

Lemma 5.19. *Let $\mathcal{K}$ be a complete arc of size k such that $(3q+5)/4 < k \leq m'(2,q)$. Suppose that $\mathcal{K}$ admits an irreducible envelope such that ν_4 is a power of p and that $\nu_4 < \sqrt{q}$. Then*

$$k < \begin{cases} q - \frac{1}{4}\sqrt{pq} + \frac{29}{16}p + \frac{1}{2} & \text{if } q \text{ is not a square}, \\ q - \frac{1}{4}p\sqrt{q} + \frac{29}{16}p^2 + \frac{1}{2} & \text{otherwise}. \end{cases}$$

Corollary 5.20. *Let $\mathcal{K}$ be a complete arc of size $m'(2,q)$. Suppose that q is an even power of p and that $\mathcal{K}$ admits an irreducible envelope with ν_4 a power of p and $\nu_4 < \sqrt{q}$. Then one of the following statements holds:*

(1) *$p = 3$, $\nu_4 = \sqrt{q}/3$, and $m'(2,q)$ satisfies Lemma 5.19.*
(2) *$p = 5$, $q = 5^4$, $\nu_4 = 5$, and $m'(2,5^4) \leq 613$;*
(3) *$p = 5$, $q = 5^6$, $\nu_4 = 5^2$, and $m'(2,5^6) \leq 15504$;*
(4) *$p = 7$, $q = 7^4$, $\nu_4 = 7$, and $m'(2,7^4) \leq 2359$.*

Proof. Let $q = p^{2e}$; so $e \geq 2$ as $p \leq \nu_4 < p^e$. From (5.2) and Lemma 5.19 we have that

$$(p-4)p^e/4 < 29p^2/16 - 0.5\,,$$

so that $p \in \{3,5,7,11\}$.

Let $p = 3$. If $\nu_4 \leq \sqrt{q}/9$ (so $e \geq 4$), then from (5.2) and $m'(2,q) \leq q + F(\sqrt{q}/9)$ we would have that

$$q - \sqrt{q} + 1 \leq q - 9\sqrt{q}/4 + 2357/16 - 67841/16(43^{e-2} + 29)\,,$$

which is a contradiction for $e \geq 4$.

Let $p = 11$. Then $p^e \leq 125$ and $e = 2$ and $\nu_4 = 11$. Thus from Proposition 5.11 we have $m'(2,11^4) \leq 11^4 + F(11)$, i.e. $m'(2,11^4) \leq 14441$. This is a contradiction since by (5.2) we must have $m'(2,11^4) \geq 14521$. This eliminates the possibility $p = 11$.

The other cases can be handled in an analogous way. □

Case $\nu_4 = \sqrt{q}$. In this case, according to (5.5), we just obtain Segre's bound (5.1).

Next we study geometrical properties of irreducible envelopes associated to large complete arcs in $\mathbf{P}^2(\mathbf{F}_q)$, q odd. In doing so we use the bounds obtained above and divide our study in two cases according as q is a square or not.

Case q square. Let $\mathcal{X}$ be an irreducible envelope associated to an arc of size $m'(2,q)$. Then from Lemma 5.7, and Corollaries 5.13, 5.16, 5.18, 5.20, we have the following result.

Proposition 5.21. *If q is an odd square and $q > 43^2$, then $\mathcal{X}$ is Σ_1-classical. The Σ_2-orders are $0,1,2,3,4,\epsilon_5$ and the $\mathbf{F}_q$-Frobenius Σ_2-orders are $0,1,2,3,\nu_4$, with $\epsilon_5 = \nu_4$, where also one of the following holds:*

(1) $\nu_4 \in \{\sqrt{q}/3, 3\sqrt{q}\}$ *for* $p = 3$;
(2) $(\nu_4, q) \in \{(5, 5^4), (5^2, 5^6), (7, 7^4)\}$;
(3) $\nu_4 = \sqrt{q}$ *for* $p \geq 5$.

Case q non-square. In this case there is no analogue to bound (5.2). From Corollary 5.12 and Lemmas 5.15, 5.17, 5.19, and taking into consideration (5.6) we have the following result.

Proposition 5.22. *Let $q > 43^2$ and $q = p^{2e+1}$, $e \geq 1$. Then, apart from the values on ν_4, the curve $\mathcal{X}$, ν_4 and ϵ_5 are as in Proposition 5.21. In this case*

$$m'(2, q) > q - 3\sqrt{pq}/4 + 7/4$$

implies

(1) $\nu_4 = \sqrt{q/p}$;
(2) $m'(2, q) < q - \sqrt{pq}/4 + 29p/16 + 1/2$.

In particular, our approach just gives a proof of Segre's bound (5.1) and Voloch's bound [107]. However, both propositions above show the type of curves associated to large complete arcs. The study of such curves, for q square and large enough, allowed Hirschfeld and Korchmáros [50], [51] to improve Segre's bound (5.1) to the bound in (5.3).

Next we stress here the main ideas from [51] necessary to deal with Problem 5.1. Due to Proposition 5.9, the main strategy is to bound from above the number $2M_q + M'_q$ (which is defined via (5.4)). For instance, if one could prove that

$$2M_q + M'_q \leq d(q - \sqrt{q} + 1)\,, \tag{5.7}$$

where d is the degree of the irreducible envelope whose normalization is $\mathcal{X}$, then from Proposition 5.9 would follow immediately an affirmative answer to Problem 5.1. However, since we know the answer to be negative for $q = 9$ and $d \leq 2t = 2(q+2-m'(2,q))$, then one can assume that d is bounded by a linear function on $\sqrt{q}$ and should expect to prove (5.7) only under certain conditions on q.

Lemma 5.23. *Let q be an odd square. If (5.7) holds true for $d \leq 2\sqrt{q} - \alpha$ with $\alpha \geq 0$, then $m'(2, q) < q - \sqrt{q} + 2 + \alpha/2$. In particular, if (5.7) holds true for $d \leq 2\sqrt{q}$, then the answer to Problem 5.1 is positive; i.e,, $m'(2, q) = q - \sqrt{q} + 1$.*

Proof. If $m'(2, q) \geq q - \sqrt{q} + 2 + \alpha/2$, then from $d \leq 2(q + 2 - m'(2, q))$ we would have that $d \leq 2\sqrt{q} - \alpha$ and so, from Proposition 5.9 and (5.7), that $m'(2, q) \leq q - \sqrt{q} + 1$, a contradiction. □

Now, in [50], (5.7) is proved for $d \leq \sqrt{q} - 3$ and q large enough, and so (5.3) follows. More precisely we have the following.

Theorem 5.24. (Hirschfeld-Korchmáros [51, Thm. 1.3]) *Let q be a square, $q > 23^2$, $q \neq 3^6$. Let $3 \leq d \leq \sqrt{q} - 3$. Suppose that Σ_1 is classical, that $0, 1, 2, 3, 4, \sqrt{q}$ are the Σ_2-orders, and that $0, 1, 2, 3, \sqrt{q}$ are the $\mathbf{F}_q$-Frobenius orders of Σ_2. Then (5.7) holds.*

Proof. (Sketch) Suppose that $2M_q + M_q' \geq d(q - \sqrt{q} + 1)$. We are going to show that $2M_q + M_q' = d(q - \sqrt{q} + 1)$. Notice that $d \geq (\sqrt{q} + 1)/2$ by Corollary 3.9(1). Let $\phi = (f_0 : \ldots : f_5)$ be a morphism associated to Σ_2. From Lemma 2.9 there exist $z_0, \ldots, z_5 \in \bar{\mathbf{F}}_q(\mathcal{X})$, not all zero, such that $\sum_{i=0}^{5} z_i^{\sqrt{q}} f_i = 0$. Set

$$\mathcal{Z} := (z_0 : \ldots : z_5)(\mathcal{X}) .$$

(This curve is related to the dual curve of $\phi(\mathcal{X})$ since it is easy to see that $\sum_{i=0}^{5} z_i^{\sqrt{q}}(P) X_i = 0$ is the hyperplane tangent at P for infinitely many P's.)

We have [51, Props. 8.3, 8.4, 8.5]

(I) $\sqrt{q}\deg(\mathcal{Z}) \leq d(2d + q + 3) - (2M_q + M_q')$;
(II) $\deg(\mathcal{Z}) \geq \sqrt{q} j_1(P)$ for any $P \in \mathcal{X}$;
(III) $\deg(\mathcal{Z}) \geq 2\sqrt{q}$ whenever $\mathcal{C}_1$ is singular.

It follows from (I) and (II) that $j_1(P) \leq 2$ since $d \leq \sqrt{q} - 3$. Now from Corollary 2.18 and the hypothesis on d there are three possibilities for (Σ_1, P)-orders:

(A) $j_2(P) = 2j_1(P)$;
(B) $j_2(P) = (\sqrt{q} + j_1(P))/2$;
(C) $j_2(P) = \sqrt{q} - j_1(P)$.

We see that points of type (C) cannot occur since $j_1(P) \leq 2$ and $d \leq \sqrt{q} - 3$. Now from the proof of [51, Prop. 9.4] we have that

$$\sqrt{q}\deg(\mathcal{Z}) = 2(dq + d - 2M_q - M_q') \leq 2d\sqrt{q}, ,$$

so that $\deg(\mathcal{Z}) < 2\sqrt{q}$ as $d \leq \sqrt{q} - 3$. It follows from (III) that $\mathcal{C}_1$ is non-singular; i.e., $\mathcal{X} = \mathcal{C}_1$. In particular the Σ_1-Weierstrass points are of type (B) and we have

$$\deg(R_1) = 3d(d-2) = (\sqrt{q} - 3)/3\tau ,$$

where R_1 is the ramification divisor of Σ_1 and τ is the number of points of type (B). Now we use the following relation between $\deg(\mathcal{Z})$ and τ [51, Prop. 9.3]:

(IV) $3\deg(\mathcal{Z}) = 2\tau$.

Since we already notice that $\deg(\mathcal{Z}) \leq 2d$ it follows that $d \leq (\sqrt{q} + 1)/2$; i.e., $d = (\sqrt{q} + 1)/2$. Next we show that $\tau = M_q'$. For P of type (B), the (Σ_2, P)-orders are $0, 1, 2, (\sqrt{q} + 1)/2, (\sqrt{q} + 3)/2, \sqrt{q} + 1$. Suppose that $P \notin \mathcal{X}(\mathbf{F}_q)$. Then $2\ell_P$ is the tangent hyperplane $L_4(P)$ at P with respect to Σ_2, where ℓ_P is the tangent line at P

with respect to Σ_1. It is easy to see that $\mathbf{\Phi}_q(P) \in L_4(P)$ so that $\mathbf{\Phi}_q(P) \in \ell_P$. This implies $d > (\sqrt{q}+1)/2$, a contradiction. Thus $M'_q = 3(\sqrt{q}+1)/2$. Finally by means of

$$\deg(S_1) = d(q+d-1) = 2M_q + \frac{\sqrt{q}+1}{2} M'_q \,,$$

where S_1 is the $\mathbf{F}_q$-Frobenius divisor associated to Σ_1, we find that $M_q = (\sqrt{q}+1)(q-\sqrt{q}-2)/4$, and one easily checks that $2M_q + M'_q = d(q-\sqrt{q}+1)$. □

Remark 5.25. The plane curve $\mathcal{X}$ of degree $d = (\sqrt{q}+1)/2$ in the above proof satisfies

$$\#\mathcal{X}(\mathbf{F}_q) = M_q + M'_q = q + 1 + \sqrt{q}(d-1)(d-2)\,;$$

i.e, it is $\mathbf{F}_q$-maximal. If $q \geq 121$, such a curve is $\mathbf{F}_q$-isomorphic to the Fermat curve $X^{(\sqrt{q}+1)/2} + Y^{(\sqrt{q}+1)/2} + Z^{(\sqrt{q}+1)/2} = 0$; see [13].

Recently, Aguglia and Korchmáros [1] proved a weaker version of (5.7) for $d = \sqrt{q} - 2$ and q large enough, namely

$$2M_q + M'_q \leq d(q - \sqrt{q}/2 - 9/2) - 3\,.$$

From this inequality and Proposition 5.9 one slightly improves (5.3) to $m'(2,q) \leq q - \sqrt{q}/2 - 11/2$ whenever $d = \sqrt{q} - 2$ and q is large enough. Therefore the paper [1], as well as [50] or [51], is a good guide toward the proof of (5.7) for $\sqrt{q} - 2 \leq d \leq 2\sqrt{q}$.

References

[1] A. Aguglia and G. Korchmáros, *On algebraic curves over a finite field with many rational points*, to appear in Bull. Belg. Math. Soc. Simon Stevin.

[2] A. Aguglia, G. Korchmáros and F. Torres, *Plane maximal curves*, to appear in Acta Arithm.

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

[4] P. Beelen and R. Pellikaan, *The Newton polygon of plane curves with many rational points*, to appear in Des. Codes Cryptogr.

[5] E. Boros and T. Szönyi, *On the sharpeness of a theorem of B. Segre*, Combinatorica **6** (1986), 261–268.

[6] R.C. Bose, *Mathematical theory of the symmetrical factorial design*, Sankhya **8** (1947), 107–166.

[7] R.O. Buchweitz, "Über Deformationen monomialer Kurvensingularitäten und Weiertrasspunkte auf Riemannschen Flächen", Thesis, Hannover, 1976.

[8] R.O. Buchweitz, "On Zariski's criterion for equisingularity and non-smoothable monomial curves", Thése, Paris VII, 1981.

[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] J.M. Chao and H. Kaneta, *Classical arcs in $PG(2,q)$ for $23 \leq q \leq 27$*, to appear in Discrete Math.

[12] A. Cossidente, *New proof of the existence of (q^2-q+1)-arcs in $PG(2,q^2)$*, J. Geometry **53** (1995), 37–40.

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

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

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

[16] D. Cox, J. Little and D. O'Shea, "Ideal, varieties and algorithms", Undergrad. Texts in Math., second edition, Springer, 1997.

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

[18] G.L. Ebert, *Partitioning projective geometries into caps*, Canad. J. Math. **37** (1985), 1163–1175.

[19] D. Eisenbud and J. Harris, *Existence, decomposition and limits of certain Weierstrass points*, Invent. Math. **87** (1987), 495–515.

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

[21] E. Esteves and M. Homma, Order sequences and rational curves, "Projective geometry with applications" (E. Ballico Ed.), Lecture Notes in Pure and Appl. Math. Vol. 166, Dekker, New York, 27–42, 1994

[22] H.M. Farkas and I. Kra, "Riemann Surfaces", Grad. Texts in Math. Vol. 71, second edition, Springer Verlag, New York/Berlin, 1992.

[23] J.C. Fisher, J.W.P. Hirschfeld and J.A. Thas, *Complete arcs in planes of square order*, Ann. Discrete Math. **30**, North Holland, 243–250, 1986.

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

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

[26] 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,

[27] A. Garcia, *Some arithmetic properties of order-sequences of algebraic curves*, J. Pure Appl. Algebra **85** (1993), 259–269.

[28] A. Garcia, *On Weierstrass points on Artin-Schreier extensions of* $k(x)$, Math. Nachr. **144** (1989), 233–239.

[29] A. Garcia and M. Homma, Frobenius order-sequences of curves, "Algebra and Number Theory" (G. Frey and J. Ritter Eds.), de Gruyter, Berlin, 27–41, 1994.

[30] A. Garcia and H. Stichtenoth, *Elementary abelian p-extensions of algebraic function fields*, Manuscripta Math. **72** (1991), 67–79.

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

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

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

[34] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, July 2000, http://www.wins.uva.nl/ geer.

[35] M. Giulietti, *On cyclic k-arcs of Singer type in* $PG(2, q)$, to appear in Discrete Math.

[36] M. Giulietti, F. Pambianco, F. Torres and E. Ughi, *On large complete arcs: odd case*, to appear in Discrete Math.

[37] V.D. Goppa, "Geometry and codes", Mathematics and its applications, Vol. 24, Kluwer Academic Publisher, Dordrecht-Boston-London, 1988.

[38] R. Göttfert and H. Niederreiter, *Hasse-Teichmüller derivatives and products of linear recurring sequences*, (G.L. Mullen et al. Eds.) Finite fields: theory, applications and algorithms (Las Vegas, USA, 1993), Contemp. Math. **168** (1994), 117–125.

[39] P.A. Griffiths, "An introduction to the theory of special divisors on algebraic curves", Regional Conference Series in Math. Vol. 44, Amer. Math. Soc., Providence, RI, 1980.

[40] P.A. Griffiths and J. Harris, "Principles of Algebraic Geometry", Wiley-Interscience, New York, 1992.

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

[42] 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.

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

[44] J. Harris, "Algebraic Geometry, A first course", Grad. Texts in Math. Vol. 133, Springer-Verlag, New York/Berlin 1992.

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

[46] 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.

[47] A. Hefez, *Non-reflexive curves*, Compositio Math. **69** (1989), 3–35.

[48] H.W. Henn, *Funktionenkörper mit großer Automorphismengruppe*, J. Reine Angew. Math. **302** (1978), 96–115.

[49] J.W.P. Hirschfeld, "Projective Geometries Over Finite Fields", second edition, Oxford University Press, Oxford, 1998.

[50] 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.

[51] J.W.P. Hirschfeld and G. Korchmáros, *On the number of points on an algebraic curve over a finite field*, Bull. Belg. Math. Soc. Simon Stevin **5** (1998), 313–340.

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

[53] J.W.P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces*, J. Statist. Plann. Inference **72** (1988), 275–286.

[54] M. Homma, *Funny plane curves in characteristic $p > 0$*, Comm. Algebra **15**(7) (1987), 1469–1501.

[55] M. Homma, *Linear systems on curves with no Weierstrass points*, Bol. Soc. Bras. Mat. **23**(1-2) (1992), 93–108.

[56] M. Homma, *On Esteves' inequality of order sequences of curves*, Comm. Algebra **21**(10) (1993), 3685–3689.

[57] A. Hurwitz, *Über algebraische Gebilde mit eindeutigen Transformationen in sich*. Math. Ann. **41** (1893), 403–442.

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

[59] T. Kato, *Non-hyperelliptic Weierstrass points of maximal weight*, Math. Ann. **239** (1979), 141–147.

[60] B. Kestenband, *Unital intersections in finite projective planes*, Geom. Dedicata **11** (1981), 107–117.

[61] J. Komeda, *On Weierstrass points whose first non-gaps are four*, J. Reine Angew. Math. **341** (1983), 237–270.
[62] J. Komeda, *On primitive Schubert indices of genus g and weight $g-1$*, J. Math. Soc. Japan **43**(3) (1991), 437–445.
[63] J. Komeda, *On the existence of Weierstrass gap sequences on curves of genus ≤ 8*, J. Pure Appl. Algebra **97** (1994), 51–71.
[64] J. Komeda, *On the existence of Weierstrass points whose first non-gaps are five*, Manuscripta Math. **76**(2) (1992), 193–211.
[65] J. Komeda, *Non-Weierstrass numerical semigroups*, Semigroup Forum **57**(2) (1998), 157–185.
[66] K. Komiya, *Algebraic curves with non-classical types of gap sequences for genus three and four*, Hiroshima Math. J. **8** (1978), 371–400.
[67] G. Korchmáros and F. Torres, *Embedding of a maximal curve in a Hermitian variety*, to appear in Compositio Math.
[68] G. Korchmáros and F. Torres, *On the genus of a maximal curve*, arXiv: math.AG/0008202.
[69] A. Kresh, J.L. Wetherell and M. Zieve, *Curves of every genus with many points, I: Abelian and toric families*, arXiv: math.AG/9912069.
[70] 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.
[71] D. Laksov, *Weierstrass points on curves*, Astérisque 87-88 (Societé Mathématique de France, Paris) (1981), 221–247.
[72] D. Laksov and A. Thorup, *Weierstrass points on schemes*, J. Reine Angew. Math. **460** (1995), 127–164.
[73] 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.
[74] J. Lewittes, *Places of degree one in function fields over finite fields*, J. Pure Appl. Alg. **69** (1990), 177–183.
[75] C. Maclachlan, *Weierstrass points on compact Riemann surfaces*, J. London Math. Soc. (2) **3** (1971), 722–724.
[76] J.S. Milne, Abelian Varieties, "Arithmetic Geometry" (G. Cornell and J.H. Silverman Eds.), 103–150, Springer-Verlag, New York, 1986.
[77] D. Mumford, "Abelian Varieties", Tata Inst. Fund. Res., Oxford University Press, Bombay, 1994.
[78] C. Moreno, "Algebraic curves over finite fields", Cambridge Tracts in Math. Vol. 97, Cambridge Univ. Press, Cambridge, 1991.
[79] N. Namba, "Geometry of algebraic projective curves", Marcel Dekkers INC, New York and Basel, 1984.
[80] A. Neeman, *Weierstrass points in characteristic p*, Invent. Math. **75** (1984), 359–376.
[81] G. Oliveira, *Weierstrass semigroups and the canonical ideal of non-trigonal curves*, Manuscripta Math. **71** (1991), 431–450.
[82] G. Oliveira and K.O. Stöhr, *Gorenstein curves with quasi-symmetric Weierstrass semigroups*, Geom. Dedicata **67**(1) (1997), 45–63.
[83] J.P. Pedersen, *A function field related to the Ree group*, Lect. Notes Math. **1518** (1992), 122–131.
[84] R. Pellikaan, The Klein quartic, the Fano plane and curves representing designs, *Codes, Curves and Signals: Common Threads in Communications* (A. Verdy Ed.), 9–20, Kluwer Acad. Publ., Dordrecht, 1998.
[85] T. Penttila and B. Williams, *Ovoids of parabolic spaces*, Geom. Dedicata **82**(1-3) (2000), 1–19.
[86] J. Rathmann, *The uniform position principle for curves in characteristic p*, Math. Ann. **276**, (1987), 565–579.

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

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

[89] F.K. Schmidt, *Zur arithmetischen Theorie der algebraischen Funktionen II, Allgemeine Theorie der Weierstrasspunkte*, Math. Z. **45** (1939), 75–96.

[90] B. Segre, *Ovals in a finite projective plane*, Canad. J. Math. **7** (1955), 414–416.

[91] A. Seidenberg, "Elements of the theory of algebraic curves", Addison Wesley, Reading, Mass., 1969.

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

[93] 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.

[94] J.P. Serre, "Rational points on curves over finite fields, Part I: q large", Notes by F. Gouvea of lectures at Harvard University, 1985.

[95] J.P. Serre, "Rational points on curves over finite fields, Part I: g large", Notes by F. Gouvea of lectures at Harvard University, 1985.

[96] H. Stichtenoth, "Algebraic function fields and codes", Springer-Verlag Berlin, 1993.

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

[98] K.O. Stöhr, *On the moduli spaces of Gorenstein curves with symmetric Weierstrass semigroups*, J. Reine Angew. Math. **441** (1993), 189–213.

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

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

[101] J.A. Thas, *Complete arcs and algebraic curves in $PG(2,q)$*, J. Algebra **106** (1987), 451–464.

[102] J. Tits, *Ovoïdes et groupes de Suzuki*, Arch. Math. **13** (1962), 187–198.

[103] F. Torres, *Weierstrass points and double coverings of curves with applications: Symmetric numerical semigroups which cannot be realized as Weierstrass semigroups*, Manuscripta Math. **83** (1994), 39–58.

[104] F. Torres, *On certain N-sheeted coverings of curves and numerical semigroups which cannot be realized as Weierstrass semigroups*, Comm. Algebra **23**(11) (1995), 4211–4228.

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

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

[107] 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.

[108] A. Weil, "Courbes algébriques et variétés abeliennes", Hermann, Paris, 1971.