WEIERSTRASS POINTS AND CURVES OVER FINITE FIELDS

KARL-OTTO STÖHR *and* JOSÉ FELIPE VOLOCH

[Received 5 February 1985]

ABSTRACT

For any projective embedding of a non-singular irreducible complete algebraic curve defined over a finite field, we obtain an upper bound for the number of its rational points. The constants in the bound are related to the Weierstrass order-sequence associated with the projective embedding. The bounds obtained lead to a proof of the Riemann hypothesis for curves over finite fields and yield several improvements on it.

0. *Introduction*

Let X be a curve of genus g defined over a field k with q elements, and let N be the number of rational points of X.

In 1948 Weil [12] proved the Riemann hypothesis for curves over finite fields which states that

$$|N-(q+1)| \leqslant 2gq^{\frac{1}{2}},$$

and, in particular, that

$$N \leqslant q+1+2gq^{\frac{1}{2}}. \qquad (*)$$

Fixing g and making extensions of the constant field, we know that the above bound is the best possible in the sense that $2g$ cannot be replaced by a smaller constant.

On the other hand, there are several instances in which (*) can be improved. The first result along these lines is due to Stark [10] in the hyperelliptic case, using Stepanov's method. Afterwards, Drinfeld-Vladut and Serre obtained improvements on (*) when $g > \frac{1}{2}(q-q^{\frac{1}{2}})$, using 'explicit formulae' (see [9] and the references therein). Serre also remarked that Weil's bound can be improved in general to

$$|N-(q+1)| \leqslant g[2q^{\frac{1}{2}}],$$

where $[\cdot]$ denotes the integral part.

The purpose of this paper is to give a general approach to the problem of improving (*). The idea is as follows. Consider X as embedded in some projective space. Using the equations for the osculating hyperplanes at the points on the curve, we define a function which vanishes at those points P whose images under the Frobenius map lie on the osculating hyperplane at P. This function will have zeros of high order at the rational points of X and a controlled number of poles. We thus get an upper bound for N which depends on q, g, the dimension of the ambient projective space, the degree of X, and on the Weierstrass order-sequence of the embedding. By

The research of the second author is supported by CNPq (Brazil), Grant No. 200.916/82, and by ORS (England).

A.M.S. (1980) subject classification: 14G15.

Proc. London Math. Soc. (3), 52 (1986), 1–19.

an appropriate choice of the embedding, we prove the Riemann hypothesis and, in several cases, we obtain improvements on (*).

Our approach has some similarities with Stepanov's method (see [1, 7]). The fundamental difference is that, instead of obtaining an auxiliary function by solving linear equations, we give it explicitly in a conceptual way as a sort of wronskian determinant.

Our approach has an interesting connection with Weil's original approach. This is explained in the appendix to this paper.

The prototype of our results is the following rather simple theorem for plane algebraic curves.

THEOREM 0.1 *Let k be a finite field with q elements of characteristic different from 2. Let $f(x,y)$ be an absolutely irreducible polynomial of degree d with coefficients in k. Then the number of solutions, say N, of the equation $f(x,y)=0$ in k^2 satisfies*

$$N \leqslant \tfrac{1}{2}d(d+q-1)$$

if f does not divide $f_{xx}(f_y)^2-2f_{xy}f_xf_y+f_{yy}(f_x)^2$.

Proof. Let $h=(x-x^q)f_x+(y-y^q)f_y$. Then h, as a function on the curve $f(x,y)=0$, has zeros at the rational points, and their orders are at least 2, because the differential dh also vanishes there. In fact,

$$dh=(x-x^q)\,df_x+(y-y^q)\,df_y+f_x\,dx+f_y\,dy,$$

and $f_x\,dx+f_y\,dy=df=0$. So if h does not vanish identically on the curve, then Bezout's theorem implies that $2N \leqslant d(d+q-1)$.

Now suppose that $h=0$, that is,

$$(x-x^q)\frac{dy}{dx}-(y-y^q)=0.$$

Differentiating this equation with respect to x gives $(x-x^q)d^2y/dx^2=0$, so that $d^2y/dx^2=0$, which by implicit differentiation means that $f_{xx}(f_y)^2-2f_{xy}f_xf_y+f_{yy}(f_x)^2$ vanishes identically on the curve.

The criterion $d^2y/dx^2 \neq 0$ means that not every point of the algebraic curve $f(x,y)=0$ is a flex. The opposite can only happen if the curve is a line or if the characteristic is a prime not larger than d (see § 1).

The contents of the paper are as follows. The first section contains an exposition of Weierstrass order-sequences associated to projective embeddings. The idea occurs naturally when one writes out the arithmetic approach of F. K. Schmidt [6] in a geometric and more general setting. It seems that some aspects and some proofs are new. In any case the exposition is rather different from other publications on these topics (see [4, 11] and the references therein).

The heart of the paper is § 2. There we state and prove our main result (Theorem 2.13), and relate the invariants of the bound with the Weierstrass order-sequences.

In § 3 we give some applications of our main result to obtain bounds which are better than the Riemann hypothesis in certain cases.

The second author would like to acknowledge the stimulating conversations he had with Professor J. W. S. Cassels on the subject of this paper.

1. *Projective embeddings and Weierstrass points*

Let X be an irreducible non-singular projective algebraic curve of genus g defined over an algebraically closed field k of characteristic p, and let $k(X)$ be the field of rational functions on X. We denote by $v_P(h)$ the order of a rational function h at a point P of X.

Let $f\colon X \to \mathbb{P}^n(k)$ be a morphism, say $f=(f_0:\ldots:f_n)$, where $f_0,\ldots,f_n \in k(X)$. Since the functions f_i are uniquely determined by f up to a proportionality factor in $k(X)^*$, the morphism f corresponds to a point of $\mathbb{P}^n(k(X))$. For each $P \in X$ we have

$$f(P)=((t^{e_P}f_0)(P):\ldots:(t^{e_P}f_n)(P))$$

where $e_P := -\min\{v_P(f_0),\ldots,v_P(f_n)\}$ and where t is a local parameter of X at P.

We will consider $f\colon X \to \mathbb{P}^n(k)$ as a parametrized curve in $\mathbb{P}^n(k)$, and the points P of X will be viewed as its branches. We will always assume that $f(X)$ is not contained in a hyperplane of $\mathbb{P}^n(k)$. A hyperplane H, consisting of the points $(x_0:\ldots:x_n) \in \mathbb{P}^n(k)$ satisfying the equation $\sum_{i=0}^n a_ix_i=0$, intersects the branch $P \in X$ with multiplicity $v_P(\sum_{i=0}^n a_if_i)+e_P$. So the intersection divisor $f^{-1}(H)$ of the parametrized curve f and the hyperplane H is given by

$$f^{-1}(H)=\operatorname{div}\left(\sum_{i=0}^n a_if_i\right)+E$$

where $E := \sum e_PP$. If X is contained in $\mathbb{P}^n(k)$ and f is the identity map then this is the intersection divisor of X and H. If the morphism $X \to f(X)$ is birational then the degree of $f^{-1}(H)$ is equal to the degree of the algebraic curve $f(X)$ in $\mathbb{P}^n(k)$. Let

$$\mathscr{D} := \{f^{-1}(H) \mid H \text{ hyperplane in } \mathbb{P}^n(k)\}$$

be the linear system of hyperplane sections. Clearly $\mathscr{D}$ is base-point-free, that is, there is no $P \in X$ such that $P \leqslant D$ for each $D \in \mathscr{D}$.

Conversely, each base-point-free linear system $\mathscr{D}$ of divisors of X is associated to a morphism $X \to \mathbb{P}^n(k)$ uniquely determined up to projective equivalence, which in coordinate-invariant description is the map $X \to \{\text{hyperplanes in } \mathscr{D}\}$ given by $P \to \{D \in \mathscr{D} \mid D \geqslant P\}$.

Let $P \in X$. An integer j is called a *hermitian P-invariant* of $\mathscr{D}$ or simply a *$(\mathscr{D},P)$-order* if there exists $D \in \mathscr{D}$ such $v_P(D)=j$; this means that there exists a hyperplane intersecting the branch P with multiplicity j.

If $\mathscr{D}$ is the canonical linear system then it follows from the Riemann–Roch theorem that j is a $(\mathscr{D},P)$-order if and only if $j+1$ is a Weierstrass gap at P, that is, there is no rational function on X, regular outside P, and having a pole of order $j+1$ at P.

For each integer i we consider the space $\mathscr{D}_i := \{D \in \mathscr{D} \mid D \geqslant iP\}$, which is isomorphic to the space of all hyperplanes in $\mathbb{P}^n(k)$ intersecting the branch P with multiplicity at least i. We have $\mathscr{D}=\mathscr{D}_0 \supseteq \mathscr{D}_1 \supseteq \mathscr{D}_2 \supseteq \ldots$. An integer j is a $(\mathscr{D},P)$-order if and only if $\mathscr{D}_j \neq \mathscr{D}_{j+1}$, in which case $\mathscr{D}_{j+1}$ has codimension 1 in $\mathscr{D}_j$. It is obvious that $\mathscr{D}_i$ is empty whenever $i>d$, where d is the degree of $\mathscr{D}$. Hence there are exactly $n+1$ $(\mathscr{D},P)$-orders, say $j_0<j_1<\ldots<j_n$, and we have $j_n \leqslant d$. Since P is not a base-point of $\mathscr{D}$ we get $j_0=0$. Note that $j_1=1$ if and only if the branch P is non-singular.

If the linear system $\mathscr{D}$ is complete then, by the Riemann–Roch theorem, we get $n=d-g$ if $d>2g-2$, and $\dim \mathscr{D}_i=d-i-g$ if $i \leqslant d-2g+1$, and hence $j_i=i$ whenever $i \leqslant d-2g$.

Let L_i be the intersection of all hyperplanes in $\mathbb{P}^n(k)$ which intersect the branch P with multiplicity at least j_{i+1}. Clearly L_0 is just a point, namely $f(P)$, and L_1 is the tangent line at P. We call L_i the *ith osculating plane* at P, and L_{n-1} the *osculating hyperplane* at P. The flag $L_0 \subset L_1 \subset \ldots \subset L_{n-1} \subset \mathbb{P}^n$ can be seen as the algebraic analogue of the Frenet frame in differential geometry.

We are looking for a description of the osculating planes in terms of the projective coordinate functions f_i. To avoid vanishing of higher derivatives if the characteristic is prime, we will use the Hasse derivatives (see [7]). Recall that $D_t^{(i)}$ is defined on $k[t]$ by

$$D_t^{(i)}\left(\sum c_j t^j\right) := \sum \binom{j}{i} c_j t^{j-i},$$

and naturally extends to $k(t)$ and to each finite separable field extension of $k(t)$. Multiplying $D_t^{(i)}$ by $i!$ one gets the usual higher derivatives.

THEOREM 1.1. *Let t be a local parameter at P, and suppose (after dividing the f_i by t^{e_P}) that $e_P = 0$. Assume that the first i $(\mathscr{D}, P)$-orders $j_0, \ldots, j_{i-1}$ are known. Then j_i is the smallest integer such that the points $((D_t^{(j_i)}f_0)(P) : \ldots : (D_t^{(j_i)}f_n)(P))$ with $r = 0, \ldots, i$ are independent, and the i-th osculating plane at P is spanned by these points.*

Proof. After a projective transformation we may assume that

$$L_i = \{(x_0 : \ldots : x_n) \mid x_{i+1} = \ldots = x_n = 0\}$$

for each $i = 0, \ldots, n-1$. Then,

$$j_{i+1} = \min\{v_P(a_{i+1}f_{i+1} + \ldots + a_nf_n) \mid a_{i+1}, \ldots, a_n \in k\}.$$

Hence $j_n = v_P(f_n)$, $j_{n-1} = v_P(f_{n-1})$, $\ldots$, $j_0 = v_P(f_0)$. Thus the matrix

$$((D_t^{(j_r)}f_i)(P))_{0 \leqslant r \leqslant n,\, 0 \leqslant i \leqslant n}$$

is triangular and has non-zero elements on the diagonal. Hence L_i is spanned by the points $((D_t^{(j_r)}f_0)(P) : \ldots : (D_t^{(j_r)}f_n)(P))$ with $r = 0, \ldots, i$.

The minimality of the j_i holds even in a stronger sense.

SCHOLIUM 1.2. *If $m_0, m_1, \ldots, m_r$ are non-negative integers with $m_0 < m_1 < \ldots < m_r$ such that the points $((D_t^{(m_i)}f_0)(P) : \ldots : (D_t^{(m_i)}f_n)(P))$ with $i = 0, \ldots, r$ are independent, then $j_i \leqslant m_i$ for each $i = 0, \ldots, r$.*

Proof. Since the vectors $((D_t^{(s)}f_0)(P), \ldots, (D_t^{(s)}f_n)(P))$ with $s = 0, 1, \ldots, j_i - 1$ span a space of dimension i, and the $i+1$ vectors with $s = m_0, m_1, \ldots, m_i$ are linearly independent, we get $j_i - 1 < m_i$, that is, $j_i \leqslant m_i$.

COROLLARY 1.3. *The osculating hyperplane at P is given by the equation*

$$\det\begin{pmatrix} X_0 & \ldots & X_n \\ (D_t^{(j_0)}f_0)(P) & \ldots & (D_t^{(j_0)}f_n)(P) \\ \vdots & & \vdots \\ (D_t^{(j_{n-1})}f_0)(P) & \ldots & (D_t^{(j_{n-1})}f_n)(P) \end{pmatrix} = 0.$$

We call $P \in X$ an *osculation point* (or more precisely a $\mathscr{D}$-osculation point) if $j_n > n$, that is, if there is a hyperplane intersecting the branch P with multiplicity greater than n.

Now we will study the parametrized curve at a general point. Thus t will be a separating variable but not necessarily a local parameter. By Theorem 1.1 we are led to consider generalized wronskian determinants. As we will prove in a moment, there exist integers $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n$ with $0 \leqslant \varepsilon_0 < \varepsilon_1 < \ldots < \varepsilon_n$ such that the wronskian

$$\det(D_t^{(\varepsilon_i)}f_j)_{i,j=0,\ldots,n}$$

does not vanish identically. We will choose $\varepsilon_0, \ldots, \varepsilon_n$ minimally in the lexicographic order, that is, $\varepsilon_0 = 0$ and if $\varepsilon_0, \ldots, \varepsilon_{i-1}$ are chosen by induction then we choose ε_i minimal such that the rows $(D_t^{(\varepsilon_r)}f_0, \ldots, D_t^{(\varepsilon_r)}f_n)$ with $r = 0, \ldots, i$ are linearly independent over $k(X)$. Like the j_i in the scholium to Theorem 1.1 the ε_i are minimal in an even stronger sense: if $m_0, \ldots, m_r$ are integers with $0 \leqslant m_0 < \ldots < m_r$ such that the vectors $(D_t^{(m_i)}f_0, \ldots, D_t^{(m_i)}f_n)$, with $i = 0, \ldots, r$, are linearly independent, then $\varepsilon_i \leqslant m_i$ for each $i = 0, \ldots, r$.

PROPOSITION 1.4. (a) *If $g_i = \sum a_{ij}f_j$ with $(a_{ij}) \in \mathrm{GL}_{n+1}(k)$, then*

$$\det(D_t^{(\varepsilon_i)}g_j) = \det(a_{ij})\det(D_t^{(\varepsilon_i)}f_j).$$

(b) *If $h \in k(X)$, then*

$$\det(D_t^{(\varepsilon_i)}(hf_j)) = h^{n+1}\det(D_t^{(\varepsilon_i)}f_j).$$

(c) *If x is another separating variable, then*

$$\det(D_x^{(\varepsilon_i)}f_j) = \left(\frac{dt}{dx}\right)^{\varepsilon_0 + \ldots + \varepsilon_n}\det(D_t^{(\varepsilon_i)}f_j).$$

Proof. (a) This is trivial and does not depend on the fact that the ε_i are minimal.
(b) By the product rule for the Hasse derivatives we have

$$D_t^{(\varepsilon_i)}(hf_j) = \sum_{s=0}^{\varepsilon_i}(D_t^{(s)}h)(D_t^{(\varepsilon_i - s)}f_j) = hD_t^{(\varepsilon_i)}f_j + \ldots.$$

We factor out h in the first row of the wronskian. In the second row $(hD_t^{(\varepsilon_0)}f_0 + \ldots, \ldots, hD_t^{(\varepsilon_0)}f_n + \ldots)$ the correction term is a linear combination of the vectors $(D_t^{(r)}f_0, \ldots, D_t^{(r)}f_n)$ with $0 \leqslant r < \varepsilon_1$ and hence, by the minimality of ε_1, a multiple of $(D_t^{(\varepsilon_0)}f_0, \ldots, D_t^{(\varepsilon_0)}f_n)$. Thus we can factor out h again and proceeding inductively in this way, we see that the result follows.

(c) This is similar to (b). We use again the minimality of the ε_i and replace the application of the product rule by the chain rule:

$$\det(D_x^{(\varepsilon_i)}f_j) = \det\left(\left(\frac{dt}{dx}\right)^{\varepsilon_i}(D_t^{(\varepsilon_i)}f_j) + \ldots\right)$$
$$= \left(\frac{dt}{dx}\right)^{\varepsilon_0 + \ldots + \varepsilon_n}\det(D_t^{(\varepsilon_i)}f_j).$$

It follows from the proposition that $\varepsilon_0, \ldots, \varepsilon_n$ depend only on the linear system $\mathscr{D}$ and so we call them the *$\mathscr{D}$-orders* or the *orders* of the morphism f.

To prove their existence, by the proposition we may suppose that t is a local parameter at a point $P \in X$ and that $e_P = 0$. Then the existence follows from Theorem 1.1. Moreover, because of their minimality, one gets

$$\varepsilon_i \leqslant j_i \quad \text{for each } i.$$

As the main application of Proposition 1.4 we obtain that the divisor

$$R := \operatorname{div}(\det(D_t^{(\varepsilon_i)} f_j)) + (\varepsilon_1 + \ldots + \varepsilon_n)\operatorname{div}(dt) + (n+1)E$$

depends only on the linear system $\mathscr{D}$. The divisor R is called the *ramification divisor* of $\mathscr{D}$. Note that

$$\deg(R) = (\varepsilon_1 + \ldots + \varepsilon_n)(2g-2) + (n+1)d.$$

Now we will study the coefficient $v_P(R)$ of the divisor R at a point P.

THEOREM 1.5. *Let $P \in X$ and let $j_0, \ldots, j_n$ be the $(\mathscr{D}, P)$-orders. Then*

$$v_P(R) \geqslant \sum_{i=0}^{n} (j_i - \varepsilon_i)$$

and equality holds if and only if

$$\det\left(\binom{j_i}{\varepsilon_r}\right) \not\equiv 0 \pmod{p}.$$

Proof. We may assume that $e_P = 0$. Let t be a local parameter at P. Then

$$v_P(R) = v_P(\det(D_t^{(\varepsilon_i)} f_j)).$$

After a projective transformation, as in the proof of Theorem 1.1, we may assume that $f_i = t^{j_i} + \ldots$ for each i, where the dots indicate terms of higher orders. Then

$$\begin{aligned}\det(D_t^{(\varepsilon_i)} f_j) &= \det\left(\binom{j_i}{\varepsilon_r} t^{j_i - \varepsilon_r} + \ldots\right) \\ &= \det\left(\binom{j_i}{r} t^{j_i} + \ldots\right) t^{-\varepsilon_0 - \ldots - \varepsilon_n} \\ &= \det\left(\binom{j_i}{\varepsilon_r}\right) t^{j_0 + \ldots + j_n - \varepsilon_0 - \ldots - \varepsilon_n} + \ldots.\end{aligned}$$

Thus

$$v_P(\det(D_t^{(\varepsilon_i)} f_j)) \geqslant \sum (j_i - \varepsilon_i)$$

and equality holds if and only if

$$\det\left(\binom{j_i}{\varepsilon_r}\right) \not\equiv 0 \pmod{p}.$$

By the theorem the ramification divisor R is positive and we have $v_P(R) = 0$ if and only if $j_i = \varepsilon_i$ for each i. Hence $\varepsilon_0, \ldots, \varepsilon_n$ are the $(\mathscr{D}, P)$-orders for almost all $P \in X$. Such a point is called *$\mathscr{D}$-ordinary*. The finitely many points where $(j_0, \ldots, j_n) \neq (\varepsilon_0, \ldots, \varepsilon_n)$ are called the *$\mathscr{D}$-Weierstrass points* and $v_P(R)$ is called the *weight* of P. Thus the number of $\mathscr{D}$-Weierstrass points, counted with their weight, equals $(\varepsilon_1 + \ldots + \varepsilon_n)(2g-2) + (n+1)d$.

When $\mathscr{D}$ is the canonical linear system, we speak simply of Weierstrass points. This coincides with the definition in [6].

When the sequence $\varepsilon_0, \ldots, \varepsilon_n$ is the *classical sequence* $0, \ldots, n$, then the $\mathscr{D}$-Weierstrass points are exactly the $\mathscr{D}$-osculation points. In this case $\mathscr{D}$ is called *classical*. If $\mathscr{D}$ is non-classical then every point is a $\mathscr{D}$-osculation point. The existence of non-classical linear systems is somewhat rare. We will give an example in §3, but see [5] for a lengthier discussion.

We are now looking for criteria to decide whether the linear system $\mathscr{D}$ is classical. For this we will state a refinement of the estimative $\varepsilon_i \leqslant j_i$.

PROPOSITION 1.6. *Let $P \in X$ and let $j_0, \ldots, j_n$ be the $(\mathscr{D}, P)$-order sequence. If $m_0, \ldots, m_n$ are integers such that $0 \leqslant m_0 < \ldots < m_n$ and $\det\left(\binom{j_i}{m_r}\right) \not\equiv 0 \pmod{p}$, then $\varepsilon_i \leqslant m_i$ for each i.*

Proof. As in the proof of Theorem 1.5 we have

$$\det(D_t^{(m_i)} f_j) = \det\left(\binom{j_i}{m_r}\right) t^{\Sigma(j_i - m_i)} + \ldots \neq 0.$$

Hence $\varepsilon_i \leqslant m_i$, by the minimality of the ε_i.

REMARK. The best choice for the integers $m_0, \ldots, m_n$ in Proposition 1.6 are the orders of the morphism $\mathbf{P}^1 \to \mathbf{P}^n$ given by $(1:x) \mapsto (x^{j_0}: \ldots : x^{j_n})$, that is, $m_0 = 0$ and if $m_0, \ldots, m_{i-1}$ are chosen then we choose m_i minimal such that the vectors $\left(\binom{j_0}{m_r}, \ldots, \binom{j_n}{m_r}\right)$ with $r = 0, \ldots, i$ are linearly independent over the prime field $\mathbf{F}_p$.

COROLLARY 1.7. *Let $P \in X$ and let $j_0, \ldots, j_n$ be the $(\mathscr{D}, P)$-orders. If the integer $\prod_{i>s}(j_i - j_s)/(i-s)$ is not divisible by p then $\mathscr{D}$ is classical and the weight of P is equal to $\sum(j_i - i)$.*

Proof. We have

$$\det\left(\binom{j_i}{r}\right) = \det((f_i^{(r)}/i!) + \ldots) = \det(f_i^{(r)})/(1!2!\ldots n!) = \prod_{i>s}(j_i - j_s)/(i-s).$$

Thus $\varepsilon_i = i$ by Proposition 1.6 and $v_P(R) = \sum(j_i - i)$ by Theorem 1.5.

The criterion of the corollary is satisfied if $j_i \not\equiv j_s \pmod{p}$ whenever $i \neq s$. In particular, since $j_n \leqslant d$, we obtain:

COROLLARY 1.8. *If $p > d$ or $p = 0$, then $\mathscr{D}$ is classical and $v_P(R) = \sum(j_i - i)$.*

Applying Proposition 1.6 to a $\mathscr{D}$-ordinary point we obtain:

COROLLARY 1.9. *Let ε be some $\mathscr{D}$-order and let μ be an integer such that*

$$\binom{\varepsilon}{\mu} \not\equiv 0 \pmod{p}.$$

Then μ is also a $\mathscr{D}$-order.

In particular, if ε is a $\mathscr{D}$-order less than p then the integers $0, 1, \ldots, \varepsilon - 1$ are also $\mathscr{D}$-orders.

Proof. Since $\binom{\varepsilon}{\mu} \neq 0$ we have $0 \leqslant \mu \leqslant \varepsilon$. We may suppose that $\mu > 0$. Let r be the

largest integer such that $\varepsilon_r < \mu$. The matrix

$$\begin{pmatrix} \binom{\varepsilon_0}{\varepsilon_0} & \dots & \binom{\varepsilon_r}{\varepsilon_0} & \binom{\varepsilon}{\varepsilon_0} \\ \vdots & & \vdots & \vdots \\ \binom{\varepsilon_0}{\varepsilon_r} & \dots & \binom{\varepsilon_r}{\varepsilon_r} & \binom{\varepsilon}{\varepsilon_r} \\ \binom{\varepsilon_0}{\mu} & \dots & \binom{\varepsilon_r}{\mu} & \binom{\varepsilon}{\mu} \end{pmatrix}$$

is triangular with diagonal entries $1, \dots, 1, \binom{\varepsilon}{\mu}$ and hence its rows are linearly independent over the prime field $\mathbf{F}_p$. So $\varepsilon_{r+1} \leqslant \mu$ by Proposition 1.6. Hence $\mu = \varepsilon_{r+1}$, by the definition of r.

REMARK. It is easy to show that $\binom{\varepsilon}{\mu} \not\equiv 0 \pmod p$ if and only if $\mu \geqslant 0$ and μ is *p-adically smaller* than ε, that is, each coefficient of the p-adic expansion of μ is less than or equal to the corresponding one of ε.

2. *The main result*

Let k be a finite field with q elements and let $\bar{k}$ be its algebraic closure. Let X be an irreducible non-singular projective algebraic curve of genus g defined over k. We simply consider X as the algebraic curve $X(\bar{k})/\bar{k}$ equipped with the action of the Frobenius map. A point $P \in X(\bar{k})$ is rational if and only if it is a fixed point of the Frobenius map. A divisor D of $X(\bar{k})$ is defined over k if and only if it is invariant under the Frobenius action.

Let $f: X \to \mathbf{P}^n$ be a k-morphism, say $f = (f_0 : \dots : f_n)$, where $f_0, \dots, f_n$ are k-rational functions on X. We keep the notations of the first paragraph, except that k is replaced by $\bar{k}$. Note that the divisor E and the linear system $\mathscr{D}$ are defined over k.

To get an upper bound for the number of rational points of X, we look at the possibly larger set of all points P of X such that the image of $f(P)$ under the Frobenius map of $\mathbf{P}^n$ is contained in the osculating hyperplane at P. By Corollary 1.3 a point P of X with $e_P = 0$ belongs to this set if and only if

$$\det \begin{pmatrix} f_0(P)^q & \dots & f_n(P)^q \\ (D_t^{(j_0)} f_0)(P) & \dots & (D_t^{(j_0)} f_n)(P) \\ \vdots & & \vdots \\ (D_t^{(j_{n-1})} f_0)(P) & \dots & (D_t^{(j_{n-1})} f_n)(P) \end{pmatrix} = 0,$$

where t is a local parameter at P and the j_i are the $(\mathscr{D}, P)$-orders. This motivates the study of the determinants

$$W_t^{\nu_0, \dots, \nu_{n-1}}(f_0, \dots, f_n) := \det \begin{pmatrix} f_0^q & \dots & f_n^q \\ D_t^{(\nu_0)} f_0 & \dots & D_t^{(\nu_0)} f_n \\ \vdots & & \vdots \\ D_t^{(\nu_{n-1})} f_0 & \dots & D_t^{(\nu_{n-1})} f_n \end{pmatrix},$$

where t is a separating variable of $k(X)/k$ and $\nu_0, \dots, \nu_{n-1}$ are non-negative integers.

PROPOSITION 2.1. *There exist integers $\nu_0, \dots, \nu_{n-1}$ with $0 \leqslant \nu_0 < \dots < \nu_{n-1}$ such that $W_t^{\nu_0, \dots, \nu_{n-1}}(f_0, \dots, f_n) \neq 0$. Choose them minimally in the lexicographic order. Then there exists an integer I with $0 < I \leqslant n$ such that*

$$\nu_i = \begin{cases} \varepsilon_i & \text{whenever } i < I, \\ \varepsilon_{i+1} & \text{whenever } i \geqslant I. \end{cases}$$

Proof. Let I be the smallest integer such that the row $(f_0^q, \dots, f_n^q)$ is a linear combination of the vectors $(D_t^{(\varepsilon_i)} f_0, \dots, D_t^{(\varepsilon_i)} f_n)$ with $i = 0, \dots, I$. Then it is clear that $\{\nu_0, \dots, \nu_{n-1}\} = \{\varepsilon_0, \dots, \varepsilon_n\} \setminus \{\varepsilon_I\}$. Since f is non-constant, we have $\nu_0 = 0$, that is, $I > 0$.

We will always choose the ν_i minimally in the lexicographic order. The minimality also holds in a stronger sense: if $m_0, \dots, m_r$ are integers with $0 \leqslant m_0 < \dots < m_r$ such that the rows of the matrix

$$\begin{pmatrix} f_0^q & \dots & f_n^q \\ D_t^{(m_0)} f_0 & \dots & D_t^{(m_0)} f_n \\ \vdots & & \vdots \\ D_t^{(m_r)} f_0 & \dots & D_t^{(m_r)} f_n \end{pmatrix}$$

are linearly independent, then $\nu_i \leqslant m_i$ for each $i = 0, \dots, r$. Indeed, the matrix

$$\begin{pmatrix} f_0^q & \dots & f_n^q \\ D_t^{(0)} f_0 & \dots & D_t^{(0)} f_n \\ \vdots & & \vdots \\ D_t^{(\nu_r - 1)} f_0 & \dots & D_t^{(\nu_r - 1)} f_n \end{pmatrix}$$

has rank $r+1$, whence $\nu_r - 1 < m_r$, that is, $\nu_r \leqslant m_r$.

PROPOSITION 2.2. (a) *If $g_i = \sum a_{ij} f_j$ with $(a_{ij}) \in \mathrm{GL}_{n+1}(k)$, then*

$$W_t^{\nu_0, \dots, \nu_{n-1}}(g_0, \dots, g_n) = \det(a_{ij}) W_t^{\nu_0, \dots, \nu_{n-1}}(f_0, \dots, f_n).$$

(b) *If $h \in k(X)$, then*

$$W_t^{\nu_0, \dots, \nu_{n-1}}(hf_0, \dots, hf_n) = h^{q^n} W_t^{\nu_0, \dots, \nu_{n-1}}(f_0, \dots, f_n).$$

(c) *If x is another separating variable of $k(X)/k$, then*

$$W_x^{\nu_0, \dots, \nu_{n-1}}(f_0, \dots, f_n) = \left(\frac{dt}{dx}\right)^{\nu_0 + \dots + \nu_{n-1}} W_t^{\nu_0, \dots, \nu_{n-1}}(f_0, \dots, f_n).$$

We may omit the proof of the proposition since it is analogous to Proposition 1.4. For Part (a), note that $a_{ij}^q = a_{ij}$ since $a_{ij} \in k$.

By Proposition 2.2, the integers $\nu_0, \dots, \nu_{n-1}$ and the divisor

$$S := \operatorname{div}(W_t(f_0, \dots, f_n)) + (\nu_1 + \dots + \nu_{n-1}) \operatorname{div}(dt) + (q+n)E$$

depend only on the linear system $\mathscr{D}$. We call $\nu_0, \dots, \nu_{n-1}$ the *Frobenius orders* of $\mathscr{D}$. Note that

$$\deg(S) = (\nu_1 + \dots + \nu_{n-1})(2g-2) + (q+n)d.$$

Dividing the projective coordinate functions $f_0, \ldots, f_n$ by f_0, we may assume that $f_0 = 1$, and $f_1, \ldots, f_n$ may be considered as affine coordinate functions. Since $v_0 = 0$, we get

$$W_t(1, f_1, \ldots, f_n) = \det\begin{pmatrix} f_1 - f_1^q & \ldots & f_n - f_n^q \\ D_t^{(v_1)} f_1 & \ldots & D_t^{(v_1)} f_n \\ \vdots & & \vdots \\ D_t^{(v_{n-1})} f_1 & \ldots & D_t^{(v_{n-1})} f_n \end{pmatrix}.$$

Note that $D_t^{(v_i)}(f_j^q) = 0$ if v_i is not a multiple of q. Hence, if $v_i < q$, then $v_0, \ldots, v_i$ are the first $i+1$ orders of the morphism

$$((f_1 - f_1^q) : \ldots : (f_n - f_n^q)) : X \to \mathbf{P}^{n-1}.$$

So we may apply Corollary 1.9 and obtain

PROPOSITION 2.3. *If v is a Frobenius order of $\mathscr{D}$ less than q, then each non-negative integer p-adically smaller than v is also a Frobenius order of $\mathscr{D}$.*

In particular, if $v_i < p$ then $(v_0, \ldots, v_i) = (0, \ldots, i)$.

Now we will study the divisor S locally at a point $P \in X$. Let $t \in k(X)$ be a local parameter at P. Dividing the projective coordinate functions $f_0, \ldots, f_n$ by t^{e_P}, we may suppose that $e_P = 0$. Thus

$$v_P(S) = v_P(W_t(f_0, \ldots, f_n)) \geqslant 0.$$

In particular, we get the important result that S is a positive divisor. The point P is in the support of S if and only if $W_t(f_0, \ldots, f_n)(P) = 0$. In particular, if $(v_0, \ldots, v_{n-1}) = (j_0, \ldots, j_{n-1})$ (where $j_0, \ldots, j_n$ are the $(\mathscr{D}, P)$-orders), then P is in the support of S if and only if the image of $f(P)$ under the Frobenius map is contained in the osculating hyperplane at P. If $v_i < j_i$ for some i, then P is in the support of S. Since for $P \in X(k)$ the first two rows of $W_t(f_0, \ldots, f_n)$ coincide, we conclude that all rational points are in the support of S. Now we will look for quantitative results.

PROPOSITION 2.4. (a) *If P is a rational point of X with the $(\mathscr{D}, P)$-orders $j_0, \ldots, j_n$ then*

$$v_P(S) \geqslant \sum_{i=1}^{n} (j_i - v_{i-1})$$

and equality holds if and only if

$$\det\left(\binom{j_i}{v_r}\right)_{0 \leqslant r \leqslant n-1,\ 1 \leqslant i \leqslant n} \not\equiv 0 \pmod{p}.$$

(b) *If P is an arbitrary point of X then*

$$v_P(S) \geqslant \sum_{i=1}^{n-1} (j_i - v_i),$$

and, if

$$\det\left(\binom{j_i}{v_r}\right)_{r,i=0,\ldots,n-1} \equiv 0 \pmod{p},$$

then the strict inequality holds.

Proof. (a) Since P is rational, the osculating planes at P are defined over k. So, after a projective transformation with coefficients in k, we may assume that $f_i = t^{j_i} + \ldots$ for each i. Dividing by f_0 we may also assume that $f_0 = 1$. Thus

$$W_t^{v_0, \ldots, v_{n-1}} = \det\begin{pmatrix} f_1 - f_1^q & \ldots & f_n - f_n^q \\ D_t^{(v_1)} f_1 & \ldots & D_t^{(v_1)} f_n \\ \vdots & & \vdots \\ D_t^{(v_{n-1})} f_1 & \ldots & D_t^{(v_{n-1})} f_n \end{pmatrix}.$$

Since $v_0 = 0$ and $j_i > 0$ for $i = 1, \ldots, n$, we get

$$W_t^{v_0, \ldots, v_{n-1}} = \det\left(\binom{j_i}{v_r} t^{j_i - v_r} + \ldots\right)$$

$$= \det\left(\binom{j_i}{v_r}\right) t^{j_1 + \ldots + j_n - v_0 - \ldots - v_{n-1}} + \ldots.$$

Now the result follows.

(b) Applying a projective transformation with coefficients in the algebraically closed field $\bar{k}$, we obtain $\bar{k}$-rational functions $g_i = \sum_{j=0}^{n} a_{ij} f_j$ where $(a_{ij}) \in \mathrm{GL}_{n+1}(\bar{k})$ such that $g_i = t^{j_i} + \ldots$ for each i. Let $h_i := \sum a_{ij} f_j^q$. In contrast to Part (a), we cannot affirm that $h_i = g_i^q$. But it is clear that $v_P(h_i) \geqslant 0$ for each i. We have

$$W_t(f_0, \ldots, f_n)\det(a_{ij}) = \det\begin{pmatrix} h_0 & \ldots & h_n \\ D_t^{(v_0)} g_0 & \ldots & D_t^{(v_0)} g_n \\ \vdots & & \vdots \\ D_t^{(v_{n-1})} g_0 & \ldots & D_t^{(v_{n-1})} g_n \end{pmatrix}$$

$$= \sum_{i=0}^{n} (-1)^i h_i d_i,$$

where the d_i are the determinants obtained by Cramér's rule. Thus

$$v_P(S) \geqslant \min_i \{v_P(d_0), \ldots, v_P(d_n)\}.$$

Now, by the usual local computations, we obtain that

$$v_P(d_i) \geqslant j_0 + \ldots + j_n - j_i - v_0 - \ldots - v_{n-1}.$$

If

$$\det\left(\binom{j_i}{v_r}\right)_{i,r=0,\ldots,n-1} \equiv 0 \pmod{p},$$

then $v_P(d_n) > j_0 + \ldots + j_{n-1} - v_0 - \ldots - v_{n-1}$. This proves Part (b).

Now we are looking for relations between the Frobenius orders $v_0, \ldots, v_{n-1}$ and the hermitian invariants $j_0, \ldots, j_n$ of a rational point.

PROPOSITION 2.5. *Let P be a rational point of X and let $j_0, \ldots, j_n$ be the $(\mathscr{D}, P)$-order-sequence. If $m_0, \ldots, m_{n-1}$ are integers such that $0 \leqslant m_0 < \ldots < m_{n-1}$ and*

$$\det\left(\binom{j_i - j_1}{m_r}\right)_{0 \leqslant r \leqslant n-1,\ 1 \leqslant i \leqslant n} \not\equiv 0 \pmod{p},$$

then $v_i \leqslant m_i$ for each i.

Proof. The best choices for the integers m_i are the orders of the morphism $\mathbb{P}^1 \to \mathbb{P}^{n-1}$ defined by

$$(1:x) \mapsto (1:x^{j_2-j_1}:\ldots:x^{j_n-j_1}) = (x^{j_1}:x^{j_2}:\ldots:x^{j_n}).$$

So we may suppose that $m_0 = 0$ and

$$\det\left(\binom{j_i}{m_r}\right)_{0\leqslant r\leqslant n-1,\,1\leqslant i\leqslant n} \not\equiv 0 \pmod{p}.$$

We may assume again that $f_0 = 1$ and $f_i = t^{j_i} + \ldots$ for each i. Thus, as in the proof of Proposition 2.4(a), we get

$$W_t^{m_0,\ldots,m_{n-1}}(f_0,\ldots,f_n) = \det\left(\binom{j_i}{m_r}\right) t^{j_1+\ldots+j_n-m_0-\ldots-m_{n-1}} + \ldots \neq 0.$$

Hence $v_i \leqslant m_i$, by the minimality of the v_i.

As an immediate consequence of Propositions 2.5 and 2.4(a) we obtain:

COROLLARY 2.6. *If $P \in X(k)$ and if $j_0,\ldots,j_n$ are the $(\mathscr{D},P)$-orders then*

$$v_i \leqslant j_{i+1} - j_1 \quad \text{for each } i,$$

$$v_P(S) \geqslant nj_1.$$

In the case where $m_i = i$, we obtain

COROLLARY 2.7. *Let $P \in X(k)$ and let $j_0,\ldots,j_n$ be the $(\mathscr{D},P)$-orders. If the integer $\prod_{1\leqslant i<r\leqslant n}(j_r-j_i)/(r-i)$ is not divisible by p, then $v_i = i$ for each i and*

$$v_P(S) = n + \sum_{i=1}^{n}(j_i - i).$$

Note that the criterion of the corollary is satisfied if $j_i \not\equiv j_r \pmod{p}$ whenever $1 \leqslant i < r \leqslant n$. In particular, the Frobenius order-sequence $v_0,\ldots,v_{n-1}$ is classical whenever $p \geqslant d$.

Applying Proposition 2.5 in the case where $m_i = \varepsilon_i$, we get

COROLLARY 2.8. *If*

$$\det\left(\binom{j_i - j_1}{\varepsilon_r}\right)_{0\leqslant r\leqslant n-1,\,1\leqslant i\leqslant n} \not\equiv 0 \pmod{p},$$

where $j_0,\ldots,j_n$ are the hermitian invariants at some rational point, then $v_i = \varepsilon_i$ for each i.

COROLLARY 2.9. *If the Frobenius order-sequence $v_0,\ldots,v_{n-1}$ is non-classical, then each rational point of X is a $\mathscr{D}$-osculation point.*

Proof. Suppose contrariwise that there is a rational point with the order-sequence $0,\ldots,n$. Then, by Corollary 2.6 we obtain that $v_i = i$ for each i.

COROLLARY 2.10. *If the Frobenius order-sequence $v_0,\ldots,v_{n-1}$ differs from the sequence $\varepsilon_0,\ldots,\varepsilon_{n-1}$, then each rational point of X is a $\mathscr{D}$-Weierstrass point.*

Proof. If there is a $\mathscr{D}$-ordinary rational point, then $v_i \leqslant \varepsilon_{i+1} - \varepsilon_1$ by Corollary 2.6, and hence $v_i = \varepsilon_i$ by Proposition 2.1.

Thus, by an extension of the constant field k, we may always arrange that the Frobenius order-sequence $v_0,\ldots,v_{n-1}$ coincides with the sequence $\varepsilon_0,\ldots,\varepsilon_{n-1}$. In particular, we see that the Frobenius orders may not be invariant under constant field extensions.

COROLLARY 2.11. *If $\mathscr{D}$ is complete and if there exists a rational point, then $v_i = i$ whenever $i < d-2g$.*

Proof. Let $P \in X(k)$ with the $(\mathscr{D},P)$-orders $j_0,\ldots,j_n$. Since $\mathscr{D}$ is complete it follows, as observed in § 1, that $j_i = i$ whenever $i \leqslant d-2g$. Hence, by Corollary 2.6, we obtain that $v_i = i$ when $i < d-2g$.

COROLLARY 2.12. *If there exists a rational point on X, then $v_i \leqslant i+d-n$ for each i.*

Proof. Since $j_n \leqslant d$ we have $j_i \leqslant i+d-n$ for each i, and Corollary 2.6 applies.

Now we state the main result of this paper.

THEOREM 2.13. *Let X be an irreducible non-singular projective algebraic curve of genus g defined over a finite field k with q elements, and let N be the number of its rational points. If there exists on X a base-point-free linear system defined over k of degree d, dimension n, and with the Frobenius order-sequence $v_0, v_1, \ldots, v_{n-1}$, then*

$$N \leqslant ((v_1 + \ldots + v_{n-1})(2g-2) + (q+n)d)/n.$$

Proof. By Corollary 2.6 we have $v_P(S) \geqslant n$ for each $P \in X(k)$. Since S is positive we conclude that $N \leqslant \deg(S)/n$.

As the first consequence of this theorem we will prove the Riemann hypothesis for curves over finite fields.

COROLLARY 2.14 (Weil [12]). *Let X be an irreducible non-singular projective algebraic curve of genus g defined over a finite field with q elements, and let N be the number of its rational points. Then*

$$q+1-2gq^{\frac{1}{2}} \leqslant N \leqslant q+1+2gq^{\frac{1}{2}}.$$

Proof. Suppose first that X has a rational point P. Let d be an integer such that $d \geqslant 2g$ and let $\mathscr{D}$ be a complete linear system defined over k of degree d (for example, $\mathscr{D} = |dP|$). Then, by the Riemann–Roch theorem, $n = d-g$ and $\mathscr{D}$ is base-point-free. By Corollaries 2.11 and 2.12 we obtain that $v_i = i$ whenever $i < n-g$ and $v_i \leqslant i+g$ for each $i = n-g,\ldots,n-1$. Thus it follows from Theorem 2.13 that

$$N \leqslant q+1+(n+(q/n))g + 2g^2(g-1)/n$$

for each integer n such that $n \geqslant g$. If q is a square such that $q > 4g^4(g-1)^2$, then we take $n = q^{\frac{1}{2}}$ and obtain that $N \leqslant q+1+2gq^{\frac{1}{2}}$. Now the Riemann hypothesis follows by a standard argument (see, for example, [1]).

Now we will state some remarkable consequences of the theorem for curves with a ge number of rational points.

COROLLARY 2.15. *If $N > (n-1)(g-1)+(q+n)d/n$, then each rational point is a $\mathscr{D}$-culation point.*

Proof. If N is as large as assumed, then by Theorem 2.13 the sequence $\nu_0, \ldots, \nu_{n-1}$ is ion-classical, and hence by Corollary 2.9 each rational point is a $\mathscr{D}$-osculation point.

COROLLARY 2.16. *If $N > ((\varepsilon_1 + \ldots + \varepsilon_{n-1})(2g-2)+(q+n)d)/n$, then each rational point is a $\mathscr{D}$-Weierstrass point.*

Proof. If N is as large as assumed, then it follows from Theorem 2.13 that $(\nu_0, \ldots, \nu_{n-1}) \neq (\varepsilon_0, \ldots, \varepsilon_{n-1})$, and hence by Corollary 2.10 each rational point is a $\mathscr{D}$-Weierstrass point.

COROLLARY 2.17. *If $N > ((n^2+n-2p+2)(g-1)+(q+n)d)/n$ and $p \leqslant n+1$ (or $N > ((n^2-n)(g-1)+(q+n)d)/n$ and $p \geqslant n+1$), then $\mathscr{D}$ is non-classical, that is, each point (rational or non-rational) of X is a $\mathscr{D}$-osculation point.*

Proof. Suppose contrariwise that $\varepsilon_i = i$ for each i. Then it follows from Proposition 2.1, that $\nu_i \leqslant i+1$ for each i and, by Proposition 2.3, that $\nu_i = i$ whenever $i \leqslant p-2$. So by Theorem 2.13 we get a contradiction.

Thus, roughly speaking, an excessive number of rational points implies a strange geometric behaviour of the curve.

3. *Improvements on the Riemann hypothesis*

If the linear system $\mathscr{D}$ in Theorem 2.13 is complete (whence $d \leqslant n+g$) and if the Frobenius order-sequence $\nu_0, \ldots, \nu_{n-1}$ is classical, then

$$N \leqslant q+1+g(n+(q/n)),$$

and in the case where $n = q^1$ this gives exactly the upper bound of the Riemann hypothesis. There are several ways to sharpen the upper bound. If $\mathscr{D}$ is special with the speciality index $\delta := n+g-d$, then one may subtract $(q+n)\delta/n$ from the above upper bound.

If there exists a non-rational point P in the support of S (see Proposition 2.4(b)), then we may subtract $v_P(S)/n$ from the upper bound of Theorem 2.13.

Likewise, when there exists a rational point P with $v_P(S) > n$ (see Proposition 2.4(a)), then we may subtract $(v_P(S)-n)/n$ from the upper bound.

We will illustrate this in the case where $\mathscr{D} = |dP|$, $d \geqslant 2g$, and $P \in X(k)$. Then $\mathscr{D}$ is base-point-free and $n = d-g$. An integer j with $0 \leqslant j \leqslant d$ is a $(\mathscr{D}, P)$-order if and only if there exists $f \in k(X)$ such that $\operatorname{div}(f)+dP \geqslant 0$ and $v_P(f)+d = j$, that is, $d-j$ is not a Weierstrass gap at P. Thus, denoting by $\alpha_1, \ldots, \alpha_g$ the Weierstrass gaps at P, the set of $(\mathscr{D}, P)$-orders equals $\{0, \ldots, d\} \setminus \{d-\alpha_1, \ldots, d-\alpha_g\}$. Suppose now that the sequence $\nu_0, \ldots, \nu_{n-1}$ is classical (see, for example, Corollary 2.7). Then it follows from Proposition 2.4(a) that $v_P(S)-n \geqslant g+\sum_{i=1}^{g-1}(\alpha_i - i)$, and hence that

$$N \leqslant q+1+ng+\frac{1}{n}\left(gq-g-\sum_{i=1}^{g}(\alpha_i - i)\right).$$

Now take $\mathscr{D} = |K+sP|$, where K is a canonical divisor defined over k, $s \geqslant 2$, and $P \in X(k)$. Then, $d = 2g-2+s \geqslant 2g$ and $n = d-g$. A non-negative integer j is a $(\mathscr{D}, P)$-order if and only if $j-s+1$ is a Weierstrass gap at P or it is negative. Thus $\{0, \ldots, s-2\} \cup \{\alpha_1+s-1, \ldots, \alpha_g+1-1\}$ is the set of $(\mathscr{D}, P)$-orders. If we suppose that the sequence $\nu_0, \ldots, \nu_{n-1}$ is classical, we will again obtain the above inequality.

Applying these considerations to hyperelliptic curves one may deduce the bounds of Stark **[10]**.

In a similar way, one may refine Corollaries 2.15, 2.16, and 2.17 about curves with a large number of rational points, if the hermitian invariants of some rational points are known.

Now, we will apply Theorem 2.13 to a few complete special linear systems.

PROPOSITION 3.1. *Let X be an irreducible non-singular projective algebraic curve of genus g defined over a finite field of characteristic p with q elements, and let N be the number of its rational points. If $p \geqslant g \geqslant 3$ and if the Weierstrass gap-sequence at an ordinary point of X is the classical gap-sequence $1, \ldots, g$, then*

$$N \leqslant 2q+g(g-1).$$

Proof. Let $\mathscr{D}$ be the canonical linear system. Since $g \neq 0$, it is base-point-free. By the Riemann–Roch Theorem, we obtain that $n = g-1$ and $d = 2g-2$. By hypothesis, the $\mathscr{D}$-order-sequence is the classical sequence $0, \ldots, g-1$. Thus $\nu_{n-1} \leqslant g-1$, by Proposition 2.1. Hence $\nu_{n-1} < p$. So, by Proposition 2.3, the Frobenius order-sequence $\nu_0, \ldots, \nu_{n-1}$ is classical. Now the proposition follows from Theorem 2.13.

The hypothesis on the gap-sequence is satisfied whenever $p \geqslant 2g-1$ (see Corollary 1.8).

The bound of Proposition 3.1 is better than the upper bound of the Riemann hypothesis if $|q^{\frac{1}{2}} - g| < (g+1)^{\frac{1}{2}}$.

When $g = 3$, Theorem 0.1 and Proposition 3.1 yield the same result. This is not surprising once one realizes that the canonical embedding of a non-hyperelliptic curve of genus 3 is a plane embedding of degree 4. J.-P. Serre has communicated to us that the corresponding result is the best possible for $q = 5, 7, 11, 13, 17$, and 19.

PROPOSITION 3.2. *If $3 \leqslant g \leqslant \frac{1}{2}(p+3)$ and X is not hyperelliptic, then*

$$N \leqslant \frac{2g-3}{g-2}q+g(g-2).$$

Proof. We may suppose that there exists a rational point P in X. Let $\mathscr{D}$ be the complete linear system $|K-P|$, where K is a canonical divisor defined over k. (Geometrically, the corresponding curve is the image of the canonical curve of X under a projection centred in a rational point of it.) Since X is non-hyperelliptic of genus at least 3, the canonical linear system $|K|$ is very ample, and hence $\mathscr{D}$ is base-point-free and $n = g-2$. Since $d = 2g-3$, we have $d \leqslant p$. Thus, by Corollary 2.12 and Proposition 2.3, we obtain that $\nu_i = i$ for each i. Now the proposition follows from Theorem 2.13.

Proposition 3.2 is better than the Riemann hypothesis if

$$|q^{\frac{1}{2}} - g(g-2)(g-1)^{-1}| < ((g-2)(g^2-g-1))^{\frac{1}{2}}(g-1)^{-1},$$

and better than Proposition 3.1 if $q < g(g-2)$. As a numerical example we take $g = 4$ and $q = 7$. Then, the Riemann hypothesis gives $N \leqslant 29$, Serre's improvement mentioned in the introduction yields $N \leqslant 28$, Proposition 3.1 gives $N \leqslant 26$, and Proposition 3.2 yields $N \leqslant 25$.

We close this section with an example. We are looking for a curve X such that $p \geqslant g = 3$ and $N > 2q + g(g-1)$. By Proposition 3.1, the order-sequence $\varepsilon_0, \varepsilon_1, \varepsilon_2$ of the canonical linear system is non-classical. So, Corollary 1.8 implies that $p = 3$. Let j_0, j_1, j_2 be the orders of a Weierstrass point. Since the canonical morphism is non-singular, we have $\varepsilon_1 = j_1 = 1$. Since $j_2 \leqslant d = 4$, we conclude that $(j_0, j_0, j_2) = (0, 1, 4)$ and that $(\varepsilon_0, \varepsilon_1, \varepsilon_2) = (0, 1, 3)$. Thus by Theorem 1.5, each Weierstrass point has weight 1, and therefore the number of Weierstrass points is equal to $(\sum \varepsilon_i)(2g-2) + (n+1)d = 28$. By Theorem 2.13, the sequence v_0, v_1 is non-classical. Thus, Proposition 2.1 gives $(v_0, v_1) = (0, 3)$.

Let P be a rational point of X. By Corollary 2.16, P is a Weierstrass point. Hence 3 and 4 are non-gaps at P. So, there exists a k-rational function x, respectively y, regular outside P and having at P a pole of order 3, respectively of order 4. Thus $[k(X):k(x)] = 3$ and $[k(X):k(y)] = 4$. Hence $k(X) = k(x, y)$. Since, by the Riemann–Roch theorem, the space of k-rational functions which are regular outside P and have at P at most a pole of order 12 has dimension 10, there is a polynomial equation with coefficients in k of the form

$$a_0 y^3 + a_1 y^2 + a_2 xy^2 + a_3 y + a_4 xy + a_5 x^2 y + a_6 + a_7 x + a_8 x^2 + a_9 x^3 + a_{10} x^4 = 0,$$

where $a_0 \neq 0$ and $a_{10} \neq 0$. Since $K = k(x, y)$ and $g = 3$, the corresponding projective plane quartic curve is non-singular and isomorphic to X.

Since the sequence $\varepsilon_0, \varepsilon_1, \varepsilon_2$ is non-classical, we have $\det(D_x^{(i)} f_j) = 0$, where $f_0 = 1$, $f_1 = x, f_2 = y$. Thus $D_x^{(2)} y = 0$. This implies by a straightforward computation that the coefficients a_2, a_1, a_5, a_4, a_8 are all equal to zero. The non-singularity of the projective quartic curve means that $a_3 \neq 0$. By an affine transformation, we may assume that $a_0 = a_{10} = 1$ and that $a_6 = a_7 = a_9 = 0$. Thus, $y^3 + a_3 y + x^4 = 0$.

Since the sequence v_0, v_1 is non-classical, we have $W_x^{0,1}(1, x, y) = 0$, that is, $(x - x^q)x^4 + a_3(y - y^q) = 0$. This implies that $q = 9$ and that $a_3 = 1$. Thus $k = \mathbf{F}_9$ and

$$y^3 + y + x^4 = 0.$$

It is now easy to check that $N = 28$. By Proposition 3.1, a classical curve of genus 3 defined over $\mathbf{F}_9$ has at most 24 rational points. Thus, the curve we are looking for does exist and it is unique up to isomorphisms. Their rational points are exactly their Weierstrass points. Their number coincides with the upper bound given by the Riemann hypothesis (and by Theorem 2.13).

This curve also gives counter-examples, showing that the following four affirmations are not always true: $v_i = \varepsilon_i$, $v_i \leqslant \varepsilon_{i+1} - \varepsilon_1$, $v_i \leqslant j_i$, $v_P(S) > n$ for each rational Weierstrass point P.

Up to an isomorphism defined over an algebraically closed field of characteristic 3, the above curve is the only curve of genus 3 with a non-classical canonical linear system (see [3]).

The results of this last section should be considered as prototypes of a vast theory. Exploring systematically the existence of special divisors, one should expect improvements for the upper bound of the Riemann hypothesis when, roughly, the genus is larger than the square root of the number of elements of the constant field, and if a small number of curves with non-classical Frobenius order-sequences is excluded.

This seems compatible with the results recently obtained by several authors exploring the connection with coding theory (see [2, 8] and the references therein).

Appendix

As was remarked in the introduction, there is an obvious connection between our method and that of Stepanov. Here we demonstrate a less obvious link with that of Weil [12].

Notations and assumptions are as at the beginning of § 2. To fix ideas we suppose furthermore that $\mathscr{D}$ is complete non-special (that is, $d = n + g$) and classical, that its Frobenius order-sequence is classical, and that there exists a rational point P_0 in X. We study the divisor

$$C = S - n \sum_{P \in X(k)} P$$

which is positive by Corollary 2.6.

Let F be the Frobenius map of X.

LEMMA A.1. *A point $P \in X$ is in the support of C if and only if there is some $D \in \mathscr{D}$ such that*

$$nP + F(P) \leqslant D$$

Proof. If P is a rational point (that is, $F(P) = P$) then, by Proposition 2.4 (a), P is in the support of C if and only if P is a $\mathscr{D}$-osculation point that is, $(n+1)P \leqslant D$ for some $D \in \mathscr{D}$.

Now suppose that P is non-rational. If $j_i(P) = i$ for each $i = 0, \ldots, n-1$, then the result is clear by the preliminary remarks to Proposition 2.4. If $j_i(P) > i$ for some $i < n$, then P is in the support of C and, on the other hand, the divisors $D \in \mathscr{D}$ with $D \geqslant nP$ form a linear system of dimension at least 1, and so we can pick up D such that $D \geqslant F(P)$.

Since $\deg \mathscr{D} = n + g$, we obtain

COROLLARY A.2. *A point $P \in X$ is in the support of C if and only if there is a positive divisor M of degree $g - 1$ such that*

$$nP + F(P) + M \in \mathscr{D}.$$

We now interpret this condition in terms of the jacobian variety $J(X)$. Let Φ be the canonical map from divisors on X to $J(X)$ with base point P_0, where P_0 is the rational point of X whose existence was assumed above. We define also a map λ from X to $J(X)$ by

$$\lambda(P) = \Phi(nP + F(P)).$$

In this terminology Corollary A.2 is equivalent to

LEMMA A.3. *A point $P \in X$ is in the support of C if and only if*

$$\lambda(P) \in \theta + \kappa$$

where θ is the theta divisor on $J(X)$ and $\kappa = \Phi(E) - \Phi(K)$ for a canonical divisor K on X.

Proof. This is clear once one observes that $-\theta = \theta - \Phi(K)$.

We also need

LEMMA A.4. *We have*

$$\deg(C) = gn^2 + an + gq$$

where a is defined by

$$N = q + 1 - a.$$

Proof. This follows at once from the formula for the degree of S in § 2.

We now compare with Weil's approach. By [12, Chapitre 3, n° 48, Théorème 25], the intersection number

$$\lambda(X).\theta = \lambda(X).(\theta + \kappa)$$

is half the trace of the correspondence $n\Delta + \Gamma \subset X^2$, where Δ is the diagonal and Γ the graph of F. It follows that

$$\lambda(X).\theta = gn^2 + an + gq$$

by the results of [12, Chapitre 2, n° 21]. The coincidence with Lemma A.4 makes it reasonable to conclude not merely that the sets Supp(C) and $\{P \in X \mid \lambda(P) \in \theta + \kappa\}$ are identical but also that their elements have the same multiplicity.

Weil argues as follows. Castelnuovo's inequality, which asserts the positivity of the trace of any correspondence, implies that

$$gx^2 + axy + gqy^2 \geqslant 0 \qquad (*)$$

for all integers x and y. Hence the discriminant $4g^2q - a^2$ is non-negative, that is, $|a| \leqslant 2gq^{\frac{1}{2}}$.

What we have done is to remark that the positivity of C implies that (*) holds for $x = n$, $y = 1$. As we saw at the end of § 2 the Riemann hypothesis can be deduced on taking $n = [q^{\frac{1}{2}}]$.

References

1. E. BOMBIERI, 'Hilbert's 8th problem: an analogue', Proceedings of Symposia in Pure Mathematics 28 (ed. F. Browder, American Mathematical Society, Providence, R.I., 1976), pp. 269–274.
2. V. D. GOPPA, 'Algebraico-geometric codes', *Math. USSR-Izv.*, 21 (1983), 75–91.
3. K. KOMIYA, 'Algebraic curves with non-classical types of gap sequences for genus three and four', *Hiroshima Math. J.*, 8 (1978), 371–400.
4. D. LAKSOV, 'Weierstrass points on curves', Astérisque 87–88 (Société Mathématique de France, Paris, 1981), pp. 221–247.
5. A. NEEMAN, 'Weierstrass points in characteristic p', *Invent. Math.*, 75 (1984), 359–376.
6. F. K. SCHMIDT, 'Zur arithmetischen Theorie der algebraischen Funktionen II. Allgemeine Theorie der Weierstrasspunkte', *Math. Z.*, 45 (1939), 75–96.
7. W. M. SCHMIDT, *Equations over finite fields, an elementary approach*, Lecture Notes in Mathematics 536 (Springer, Berlin, 1976).
8. J.-P. SERRE, *Nombres de points des courbes algébriques sur* F_q, Séminaire de Théorie des Nombres de Bordeaux, Année 1982–1983, exposé n° 22.
9. J.-P. SERRE, 'Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini', *C. R. Acad. Sci. Paris Sér. I Math.*, 296 (1983), 397–402.

10. H. STARK, 'On the Riemann hypothesis in hyperelliptic function fields', Proceedings of Symposia in Pure Mathematics 24 (ed. F. Browder, American Mathematical Society, Providence, R.I., 1973), pp. 285–302.
11. H. STICHTENOTH, *Algebraische Funktionenkörper einer Variablen*, Vorlesungen aus dem Fachbereich Mathematik der Universität Essen 1 (1978).
12. A. WEIL, *Courbes algébriques et variétés abéliennes* (Hermann, Paris, 1971).

Instituto de Matemática Pura e Aplicada
Estrada Dona Castorina 110
22460 *Rio de Janeiro*
Brazil

Department of Pure Mathematics and Mathematical Statistics
16 *Mill Lane*
Cambridge CB2 1SB