J. Eur. Math. Soc. 15, 1927–1942

DOI 10.4171/JEMS/409

Pietro Corvaja · Umberto Zannier

Greatest common divisors of $u - 1, v - 1$ in positive characteristic and rational points on curves over finite fields

Received November 4, 2011

Abstract. In our previous work [4] we proved a bound for $\gcd(u - 1, v - 1)$, for S-units u, v of a function field in characteristic zero. This generalized an analogous bound holding over number fields, proved in [3]. As pointed out by Silverman [15], the exact analogue does not work for function fields in positive characteristic. In the present work, we investigate possible extensions in that direction; it turns out that under suitable assumptions some of the results still hold. For instance we prove Theorems 2 and 3 below, from which we deduce in particular a new proof of Weil's bound for the number of rational points on a curve over finite fields (see §4). When the genus of the curve is large compared to the characteristic, we can even go beyond it.

What seems a new feature is the analogy with the characteristic zero case, which admitted applications to apparently distant problems.

1. Introduction

The purpose of this work is to extend to positive characteristic certain results which we shall soon recall. We shall also deduce several consequences, including a new proof of Weil's bound for the number of rational points on a curve over finite fields; in some special cases, our estimates will go even beyond Weil's bounds (see §4).

In the paper [4], as an analogue of a previous result in arithmetic [3], we proved the following (Corollary 2.3 in [4]):

Theorem 1. *Let κ be an algebraically closed field of characteristic zero, X be a smooth projective curve over κ, $u, v \in \kappa(X)$ non-constant multiplicatively independent rational functions, and $S \subset X(\kappa)$ their set of zeros and poles. Then*

$$\sum_{v \in X(\kappa) \setminus S} \min\{v(1-u), v(1-v)\} \leq 3\sqrt[3]{2}(\deg(u)\deg(v)\chi)^{1/3}. \tag{1}$$

In the above sum, $\chi = |S| + 2g - 2$ is the Euler characteristic of the affine curve $X \setminus S$ (and g its genus); v runs over the points of the curve $X \setminus S$, viewed as places of the function field $\kappa(X)/\kappa$; in other words $v(f)$ denotes the multiplicity of vanishing of f at the point v.

P. Corvaja: Dipartimento di Matematica e Informatica, Via delle Scienze, 33100 Udine, Italy;
e-mail: pietro.corvaja@dimi.uniud.it

U. Zannier: Scuola Normale Superiore, Piazza dei Cavalieri, 7, 56100 Pisa, Italy;
e-mail: u.zannier@sns.it

Note that the left-hand side may be trivially bounded by $\min(\deg(u), \deg(v))$, whereas the theorem in particular gives for the same quantity the upper bound $\ll_\chi \max(\deg(u), \deg(v))^{2/3}$.

Theorem 1 was proved as a corollary of a more general inequality with parameters to which we shall return. The arguments were on the same lines as the alluded arithmetic results, but in place of the difficult Subspace Theorem of Schmidt it used rather elementary and self-contained considerations using Wronskians.

To give some alternative views of this result, let us now consider the image of $X \setminus S$ in $\mathbb{G}_{\mathrm{m}}^2$ given by the map $p \mapsto (u(p), v(p))$; this is an affine curve. Then the left-hand side in the above formula represents the multiplicity of such a curve at the origin $(1, 1)$ of $\mathbb{G}_{\mathrm{m}}^2$. Still another point of view is to interpret the left-hand side as a gcd of $u-1$, $v-1$, viewed as functions on $X \setminus S$; in turn, Silverman [14] interpreted it as a height, with respect to the exceptional divisor in a blow-up of $\mathbb{G}_{\mathrm{m}}^2$.

Theorem 1 admits various applications, for instance to a special case of a conjecture of Vojta concerning integral points for the complement in $\mathbb{P}_2$ of certain curves (see [4], [7]) and to rational curves on projective surfaces [6].

Another application occurs when X, u, v are defined over a number field k, and we take $\kappa = \bar{\mathbb{Q}}$. If $x \in \mathcal{X}(\bar{\mathbb{Q}})$ is a common zero of $u-1$, $v-1$, all the conjugates x^σ of x over k contribute to $\gcd(u-1, v-1)$, whence

$$[k(x) : k] \leq 3\sqrt[3]{2}(\deg(u)\deg(v)\chi)^{1/3}. \tag{2}$$

In turn, this was applied in [5] to obtain a new bound for the maximal order of a torsion point on a curve in $\mathbb{G}_{\mathrm{m}}^n$.

The inequality in Theorem 1 is often useful when u, v have few zeros and poles compared to their degree. A significant and illustrative instance of this occurs when $u = a^n$, $v = b^n$ for fixed non-constant multiplicatively independent polynomials $a(t), b(t) \in k[t]$. In this case, on taking $X = \mathbb{P}_1$ and S to be exactly the set of zeros of $a(t)b(t)$ plus the point at infinity, we deduce from (2) that the degree over k of any common zero of a^n-1, b^n-1 is $\ll n^{2/3}$. Recalling that the degree of n-th roots of unity is $\phi(n) \gg n/\log n$, we conclude that in fact

$$\deg(\gcd(a^n(t) - 1, b^n(t) - 1)) = O_{a,b}(1),$$

as was proved by Ailon and Rudnick [1].

Let us now consider the case when κ has positive characteristic. As proved by Silverman, even in the special case $u = a^n$, $v = b^n$, the analogue of Theorem 1 does not hold; in fact, an immediate consequence of his Theorem 4 in [15] is that *for every pair of non-constant polynomials $a(t), b(t) \in \mathbb{F}_q[t]$ there exists a positive constant $c = c(a, b) > 0$ such that for infinitely many n*,

$$\deg(\gcd(a^n(t) - 1, b^n(t) - 1)) \geq cn. \tag{3}$$

Taking into account this counter-example, we still want to explore further what can be proved in positive characteristic, in the direction of (1). We shall see for instance that

something remains true if the degrees involved are "small" with respect to the characteristic: see Theorem 2 below.

Remaining in the context of Silverman's counter-example, we also observe that if we take an arbitrary curve X over $\mathbb{F}_q$, a, b non-constant rational functions in $\mathbb{F}_q(X)$ and u, v of the form $u = a^{q^m-1}$ then $v = b^{q^m-1}$, the gcd in question is at least the number of points defined over the field $\mathbb{F}_{q^m}$ on the curve $X \setminus S$. In fact, at any such point of the curve both functions a, b take values in $\mathbb{F}_{q^m}^*$, so their q^m-1-th power equals 1.

On the one hand this justifies at once the lower bound (3), at least for n of the form q^m-1.

On the other hand, taking into account this link with rational points over finite fields, we might ask whether some modification of the proof of the above theorem continues to work, producing some upper bounds concerning rational points.

In fact, suppose that X is defined over a prime field $\mathbb{F}_p$ and that its degree is small enough with respect to p. Then it turns out that the proof method of Theorem 1 may be suitably enriched with further arguments, producing a bound of the "correct" magnitude for the number of rational points. In particular this applies if we start with an absolutely irreducible curve defined over $\mathbb{Q}$ and consider its reduction modulo p, for p tending to infinity. The bound then takes the shape $p + O(\sqrt{p})$, as predicted by Weil's Theorem.

The purpose of this paper is to detail this argument and actually to produce an analogue for arbitrary finite fields. In this extension, Wronskians will be replaced by hyper-Wronskians (which are constructed out of Hasse hyperderivatives); see §3, Theorem 3 for the details of this extension and the formulation of an analogue of the estimates in [4]. See also §4 for the deduction from this results of the full Weil bound, namely

$$\big||X(\mathbb{F}_q)| - q - 1\big| \le 2g\sqrt{q}.$$

Here, q is an arbitrary power of a prime p, and no hypothesis on X or p is required.

We mention that other authors, like Schmidt, Stöhr, Voloch, ..., have already recognised the usefulness of hyperderivatives in the context of rational points over finite fields; actually the paper [13] recovers the full Weil bound in this way. However, the present method is definitely different in other respects, and also shows the link of this topic with the gcd estimates, which have already allowed many different applications. We stress that our gcd-method has its origin in characteristic zero, while Weil's and Stepanov's have no known analogue in characteristic zero.

We now state a version of Theorem 1 in positive characteristic, whose corollaries sometimes go beyond what follows from Weil's bounds. More precisely, we have the following

Theorem 2. *Let X be a smooth projective absolutely irreducible curve over a field κ of characteristic p. Let $u, v \in \kappa(X)$ be rational functions, multiplicatively independent modulo κ^*, and with non-zero differentials; let S be the set of their zeros and poles; and let $\chi = |S| + 2g - 2$ be the Euler characteristic of $X \setminus S$. Then*

$$\sum_{\nu \in X(\overline{\kappa})\setminus S} \min\{\nu(1-u), \nu(1-v)\} \le \max\left(3\sqrt[3]{2}(\deg u \deg v \chi)^{1/3}, 12\frac{\deg u \deg v}{p}\right).$$

Observe that we recover the same bound of Theorem 1 when

$$32(\deg u \deg v)^2 \le p^3 \chi .$$

Note also that the estimate is non-trivial only if $\max(\deg u, \deg v) < p/12$; in fact the gcd (i.e. the left side of the displayed inequality) is in any case bounded by $\min(\deg u, \deg v)$.

We give some simple corollaries of this theorem; it will be clear that much more general statements can be obtained, but we limit ourselves to simple choices just for the sake of illustration.

Corollary 1. *Let X be a curve defined over a finite field κ of characteristic p. Let x_1, x_2, y_1, y_2 be rational functions on X, S the set of their zeros and poles, and χ the Euler characteristic of $X \setminus S$. Let a_1, a_2, b_1, b_2 be integers. Then either $x_1^{a_1} x_2^{a_2}$ and $y_1^{b_1} y_2^{b_2}$ are multiplicatively dependent, or the number N of points $z \in X(\overline{\kappa})$ such that*

$$x_1^{a_1} x_2^{a_2} = y_1^{b_1} y_2^{b_2} = 1$$

satisfies

$$N \le \max\left(3\sqrt[3]{2}[(\deg x_1^{a_1} x_2^{a_2})(\deg y_1^{b_1} y_2^{b_2})\chi]^{1/3}, 12\frac{(\deg x_1^{a_1} x_2^{a_2})(\deg y_1^{b_1} y_2^{b_2})}{p} \right).$$

For another corollary, let us take $x_2 = y_2 = 1$. Dropping the indices and denoting by μ_n the set of n-th roots of unity, we obtain:

Corollary 2. *Let $X \subset \mathbb{G}_{\mathrm{m}}^2$ be an absolutely irreducible plane curve of Euler characteristic χ, not the translate of a subtorus. Suppose it is defined by an equation $f(x, y) = 0$ of bidegree (d_1, d_2). Then*

$$|X \cap (\mu_{m_1} \times \mu_{m_2})| \le \max\left(3\sqrt[3]{2}(m_1 m_2 d_1 d_2 \chi)^{1/3}, 12\frac{m_1 m_2 d_1 d_2}{p} \right).$$

On taking further the curve X to be the line $x + y = c$, for some $c \in \mathbb{F}_p^*$, and $m_1 = m_2 = m$ a divisor of $p - 1$, we find that the number of solutions in m-th roots of unity to the equation $x + y = c$ is bounded by $\max(3\sqrt[3]{2}\, m^{2/3}, 12m^2/p)$.

Up to a constant, the same bound was obtained by Garcia and Voloch [9] by different methods. Also, this is essentially the case $T = 1$ (but our method too could handle the case of arbitrary values of T, with similar estimates) of Lemma 5 in the paper by Heath-Brown and Konyagin [10]. (They give the estimate only for $m < p^{3/4}$, but on the other hand, for $m \gg p^{3/4}$ our bound can also be deduced from Weil's theorem.)

Note that for every m dividing $p - 1$, the expected number of solutions should be about m^2/p (in fact, for a given value of $x \in \mu_m$, the probability that $c - x$ belongs to μ_m is $m/(p - 1)$). Also, taking the average over $c \in \mathbb{F}_p^*$, it is clear that our estimate $12m^2/p$ is, up to a constant, best possible.

We also note that writing $p - 1 = ml$ this yields an upper bound for the number of points on the Fermat curve $x^l + y^l = 1$; when $m \ll p^{3/4}$, this bound goes beyond what can be deduced from Weil's bound in the same range. (See [10] for applications to

exponential sums.) As we have already remarked, it is peculiar that our result comes from an analogue in zero characteristic.

Another instance occurs when the curve X is defined over $\mathbb{F}_p$. In the same way as Theorem 1 leads to (2), Theorem 2 gives a bound for the degree over $\mathbb{F}_p$ of the common zeros of $u-1$, $v-1$. In fact, suppose that X contains a point $(\xi_1, \xi_2) \in \overline{\mathbb{F}}_p^2$ with ξ_1 of order m_1 and ξ_2 of order m_2. Then the degree of this point over $\mathbb{F}_p$ is the multiplicative order of p modulo the l.c.m. m of m_1, m_2. Then, since also the conjugate points lie on X, we obtain the bound $\ll (m_1 m_2)^{1/3}$ for the order of p modulo m.

This argument can in fact be carried out as in the paper [5], using Corollary 1 above. We only sketch the idea. Let X be defined by $f(x_1, x_2) = 0$ of bidegree (d_1, d_2). Via geometry of numbers one constructs two multiplicatively independent monomials $u = x_1^{a_1} x_2^{a_2}$, $v = x_1^{b_1} x_2^{b_2}$ such that $(\deg u)(\deg v) \le 2md_1d_2$ and with the value 1 at (ξ_1, ξ_2). Then the monomials continue to take the value 1 at all the conjugate points. Thus Corollary 1 yields

$$\operatorname{ord}(p, \bmod m) = [\mathbb{F}_p(\xi_1, \xi_2) : \mathbb{F}_p] \le \max\left(3\sqrt[3]{4}(md_1d_2\chi)^{1/3}, 24\frac{md_1d_2}{p}\right).$$

This is useless if m is "large", but in that case one can still use the trivial estimate for the gcd leading to the bound $\sqrt{2md_1d_2}$. This shows that if we have a torsion point of prime order l on X, then p must have a "small" multiplicative order modulo l.

For further results on torsion points on curves over finite fields, going in another direction, see [16].

2. Review of auxiliary tools

Let $\kappa \subset \mathbb{F}_q$ be a finite field of characteristic p. Let $\mathcal{X}$ be an absolutely irreducible smooth projective curve over κ and denote by $L = \kappa(\mathcal{X})$ its function field. We let x, y be separating elements generating L over κ.

Let L^q denote the subfield of L formed by the q-th powers in L.

Lemma 1. $[L : L^q] = q$.

Proof. This is well known. □

Lemma 2. *Let $z \in L$ be a separating element; then z generates L over L^q. Assume also that z is a local parameter, so that L embeds into $\kappa((z))$. Then $L \cap \kappa((z^q)) = L^q$ and the fields L and $\kappa((z^q))$ are linearly disjoint over L^q.*

Proof. The extension $L/L^q(z)$ is both separable and purely inseparable, so it has degree one.

Put $E = L \cap \kappa((z^q))$. Note that E contains L^q. On the other hand $[\kappa((z)) : \kappa((z^q))] = q$: Clearly $1, z, \ldots, z^{q-1}$ is a basis for $\kappa((z))$ as a $\kappa((z^q))$-vector space. Hence $[E(z) : E] \ge q$. Since $[L : L^q] = q$, by the previous lemma, we obtain $E = L^q$. Also a basis of L over L^q is again $1, z, \ldots, z^{q-1}$ and these elements are linearly independent over $\kappa((z^q))$. □

Let us now recall a few elementary facts on the zeta function of a curve. We take $\kappa = \mathbb{F}_q$ and the curve $\mathcal{X}$ defined over $\mathbb{F}_q$, of genus g. The zeta function $\zeta_{\mathcal{X}}(s)$ is defined either by a sum over the effective divisors on $\mathcal{X}$ or by an Euler product, ranging over the prime divisors on $\mathcal{X}$, as

$$\zeta_{\mathcal{X}}(s) = \sum_D q^{-s \deg D} = \prod_P (1 - q^{-s \deg P})^{-1}.$$

Note that a prime divisor P is the sum of the conjugates of a single point defined over an extension $\mathbb{F}_{q^r}$; if r is minimal, P is the sum of r points, so $\deg P = r$.

Putting $t = q^{-s}$, we can write

$$\zeta_{\mathcal{X}}(s) = \prod_P (1 - t^{\deg P})^{-1}.$$

The Riemann–Roch theorem implies that $\zeta_{\mathcal{X}}$ is a rational function in t of the shape

$$\zeta_{\mathcal{X}}(s) = \frac{L_{\mathcal{X}}(t)}{(1-t)(1-qt)},$$

where $L_{\mathcal{X}}(T) \in \mathbb{Z}[T]$ is a polynomial of degree $2g$ (actually a reciprocal polynomial). By logarithmic differentiation with respect to t one finds, after easy manipulations,

$$t \cdot \frac{\zeta'_{\mathcal{X}}(s)}{\zeta_{\mathcal{X}}(s)} = \sum_{m=1}^{\infty} |\mathcal{X}(\mathbb{F}_{q^m})| t^m.$$

As a consequence, the expression for the number of points on $\mathcal{X}$ over $\mathbb{F}_{q^m}$ takes the form

$$|\mathcal{X}(\mathbb{F}_{q^m})| = q^m + 1 - \sum_{i=1}^{2g} \alpha_i^m$$

for suitable complex numbers $\alpha_1, \ldots, \alpha_{2g}$.

The Riemann hypothesis reduces to proving that $|\alpha_i| \le q^{1/2}$ for each $i = 1, \ldots, 2g$. Let us observe the following fact:

Lemma 3. *The following are equivalent:*

(i) $|\alpha_i| \le q^{1/2}$ *for every* $i = 1, \ldots, 2g$.
(ii) $\big||\mathcal{X}(\mathbb{F}_{q^m})| - q^m - 1\big| \le 2g q^{m/2}$ *for every* $m \ge 1$.
(iii) *There exists a positive integer* r *such that* $|\mathcal{X}(\mathbb{F}_{q^{rm}})| = q^{rm} + O(q^{rm/2})$ *as* $m \to \infty$.

Proof. It is clear that (i)⇒(ii)⇒(iii). Let us now assume (iii), which amounts to $|\sum_i \alpha_i^{rm}| = O(q^{rm/2})$. There are several ways to deduce from this asymptotic estimate that $|\alpha_j| \le q^{1/2}$ for each $j = 1, \ldots, 2g$. We shall give the following argument.

We shall prove more generally that if $c_1, \ldots, c_l$ are non-zero complex numbers, $\beta_1, \ldots, \beta_l$ are distinct complex numbers and $|\sum_{i=1}^{l} c_i \beta_i^m| = O(\rho^m)$, then $\max_i |\beta_i| \le \rho$.

For this we can argue by induction on l, the assertion being clear for $l = 1$. Suppose $l > 1$ and write $f(m) = \sum_{i=1}^{l} c_i \beta_i^m$. Then $|f(m+1) - \beta_1 f(m)| = O(\rho^m)$. On the other hand, $f(m+1) - \beta_1 f(m) = \sum_{i=2}^{l} c_i (\beta_i - \beta_1) \beta_i^m$. By induction we easily conclude. □

3. GCD-estimates in arbitrary characteristic

Let $\kappa \subset \mathbb{F}_q$, and let L be a 1-dimensional function field over κ. Let x, y be separating elements in L. Let $f(x, y) = 0$ be the minimal relation bewteen x and y, with coefficients in κ, where $f(X, Y) \in \kappa[X, Y]$ is supposed to be absolutely irreducible. Let $\mathcal{C}$ be a smooth projective model of the function field L and let $S \subset \mathcal{C}$ be a finite set containing all the zeros and poles of x, y; we denote by χ the Euler characteristic of $\mathcal{C} \setminus S$. Let $a = \deg_X f$ and $b = \deg_Y f$.

Theorem 3. *Let h, k be positive integers with*

$$ah + bk < q. \tag{4}$$

Put $u = xz^q$ and $v = yw^q$ for some S-units $z, w \in L^*$. Then at least one of the two alternatives holds: either

- *$a \leq k$ and $b \leq h$, or*
- $\displaystyle\sum_{v \notin S} \min(v(1-u), v(1-v)) \leq \frac{q+k-hk}{q} \deg(v) + \frac{k}{q} \deg(u) + \frac{q-1}{2}\chi.$

Proof. Let h, k be positive integers as in the statement. Suppose that the first alternative of the theorem does not hold, so that either $k \leq a-1$ or $h \leq b-1$.

Define $n = hk+h+k$, and put $u = xz^q$, $v = yw^q$, $\rho = (1-u)/(1-v)$. Let us define the functions $f_1, \ldots, f_n$ as follows: for $i = 1, \ldots, k$ put $f_i = u^{i-1}\rho$, while $f_{k+1}, \ldots, f_n$ are the functions $u^r v^s$ for $r = 0, \ldots, k$, $s = 0, \ldots, h-1$.

Proposition 1. *The functions $f_1, \ldots, f_n \in L$ are linearly independent over L^q.*

Proof. Any dependence relation leads to an identity

$$P_1(u)(1-u) + P_2(u, v)(1-v) = 0 \tag{5}$$

for some polynomials $P_1 \in L^q[U]$, $P_2 \in L^q[U, V]$ not both zero and with $\deg P_1 \leq k-1$, $\deg_U P_2 \leq k$ and $\deg_V P_2 \leq h-1$.

Let us define the polynomial $P(X, Y) \in L^q[X, Y]$ by setting $P(X, Y) = P_1(Xz^q)(1 - Xz^q) + P_2(Xz^q, Yw^q)(1 - Yw^q)$. Then $\deg_X P \leq k$, $\deg_Y P \leq h$.

Observe that $P(X, Y)$ is not identically zero: otherwise in the first place P_1 would be identically zero (since $P_1(Xz^q)(1 - Xz^q)$ would be divisible by the polynomial $1 - Yw^q$, which is non-constant in Y) and in turn P_2 would also have to vanish, which is a contradiction.

Replacing $u = xz^q$, $v = yw^q$ in (5) we find $P(x, y) = 0$. Let $R(Y) \in L^q[Y]$ be the resultant with respect to X between $f(X, Y)$ and $P(X, Y)$.

Suppose first that $R(Y)$ vanishes identically. Observe that $f(X, Y)$ is absolutely irreducible, so it is irreducible viewed as a polynomial in $L^q[X, Y]$ and *a fortiori* is irreducible as a polynomial in X over the field $L^q(Y)$. Therefore f must divide P in $L^q(Y)[X]$, because f and P, as polynomials in X, must have a common root in an algebraic closure of L^q. By Gauss' Lemma, f divides P in $L^q[X, Y]$. Therefore in particular $k \geq a$, $h \geq b$, which is excluded.

Hence $R(Y) \neq 0$.

Note that by the standard expression of the resultant as a determinant (see e.g. [12, Chap. IV, §8]) we find $\deg R \leq ah + bk$.

On the other hand the polynomials $f(X, y)$ and $P(X, y)$ have the common root x and hence $R(y) = 0$. In particular, we find $[L^q(y) : L^q] \leq \deg R \leq ah + bk < q$. By Lemma 2, $L^q(y) = L$, but $[L : L^q] = q$ and we have a contradiction. □

Now the proof will proceed by taking suitable hyper-Wronskians. We follow the treatment of Garcia–Voloch [8] and Hsia–Wang [11]. For a separating element $t \in L$, we define as in §1 of [8] a sequence of differential operators $D_{n,t} = D_n$, for $n = 0, 1, 2, \ldots$, with the following properties: D_0 is the identity operator on L and

- $D_i(zw) = \sum_{j=0}^{i} D_j(z) D_{i-j}(w)$ for all $z, w \in L$;
- $D_i \circ D_j = \binom{i+j}{i} D_{i+j}$.

We choose once and for all a separating element $t \in L$, which is moreover a local parameter at some point; also, for every place ν of L/κ, we choose a local parameter t_ν at ν. It follows from Remark 1 of [8] that for integers $i \geq j > 0$,

$$\nu(D_{i,t_\nu}(t_\nu^j)) = j - i.$$

We now continue with the proof of Theorem 3. Since the first alternative does not hold, i.e. either $h < b$ or $k < a$, by Proposition 1 the functions $f_1, \ldots, f_n$ are linearly independent over L^q. Hence, by Lemma 2, they are linearly independent over $\kappa((t))$. In turn, by Theorem 1 of [8], there exist integers $0 = \epsilon_1 < \cdots < \epsilon_n < q$ such that the corresponding hyper-Wronskian with respect to t,

$$\omega = W_t(f_1, \ldots, f_n) = \det(D_{\epsilon_j,t} f_i)_{1 \leq i,j \leq n},$$

does not vanish. We take the minimal such ϵ (in the lexicographic order), called the orders (see [8, p. 461]).

Observe that the inequality $n < q$ is indeed implied directly. In fact, $ah + bk < q$ by assumption. Moreover, if for instance $k \leq a - 1$ (the other case being similar) we have $n = h(k + 1) + k \leq ah + k \leq ah + bk < q$.

Here and in what follows the sequence of ϵ_j is fixed, so the reference to the ϵ_j is omitted.

We also denote by $\omega_\nu = W_{t_\nu}(f_1, \ldots, f_n)$ the local hyper-Wronskian at ν.

By Proposition 2.1 in [11], for two local parameters t, u, we have a formula

$$D_{m,t} = \left(\frac{du}{dt}\right)^m D_{m,u} + \text{linear combination of } D_{l,u},\ l < m.$$

Using this formula and taking into account that $(\epsilon_1, \ldots, \epsilon_n)$ is a minimal sequence with linearly independent rows, the residual terms in the formula do not matter in the determinant, leading to the identity

$$\omega_\nu = \left(\frac{dt}{dt_\nu}\right)^\sigma \omega, \tag{6}$$

where

$$\sigma = \sum_j \epsilon_j. \tag{7}$$

We go on by estimating $v(\omega_v)$ and for this we shall distinguish several cases, as in [4].

Case (i): $v \notin S$, $v(\rho) \leq 0$. As in [4] we first make a simple observation: Suppose that two functions f_i, f_j, $i \neq j$, have a pole at v of the same order > 0. Then by subtracting from the i-th column a constant multiple of the j-th column, we may suppose in calculating the hyper-Wronskian that f_i has a pole of smaller order than f_j at v. Therefore, by repeating this procedure we may assume that the functions f_i which have a pole at v have in fact poles of pairwise distinct orders, not exceeding the original maximal order.

In the present Case (i) the only functions which (may) have a pole at v are $f_1, \ldots, f_k$, because $v \notin S$, so the remaining f_i's are units at v by assumption. Hence, the only poles we shall possibly find in ω_v will come from the first k columns. However by the above observation we may change the actual f_i's, $i = 1, \ldots, k$, to assume that the negative ones among $v(f_1), \ldots, v(f_k)$ are all distinct and $\geq v(\rho)$. Suppose that after such column operations and a suitable renumbering, only $f_1, \ldots, f_r$ have a pole at v and $v(f_1) < \cdots < v(f_r) < 0$. Plainly we will have $v(\rho) \leq v(f_1)$ and $r \leq k$, so $r \leq \min(k, -v(\rho))$. Also, observe that the hyper-derivation D_s with respect to t_v increases the order of a pole by at most s and leaves regular a regular function at v.

In conclusion, by looking at the individual terms obtained in the expansion of the determinant (after having performed the column operations), a simple inspection shows that

$$v(\omega_v) \geq v(f_1) + \cdots + v(f_r) - \epsilon_n - \epsilon_{n-1} - \cdots - \epsilon_{n-r+1}.$$

Also, we are assuming the $v(f_i)$ to be distinct and all $\geq v(\rho)$; then letting $\epsilon = \epsilon_n \leq q-1$ denote the maximum of the ϵ_j, we have $\epsilon_n + \epsilon_{n-1} + \cdots + \epsilon_{n-r+1} \leq r\epsilon - \binom{r}{2}$. Then we obtain

$$v(\omega_v) \geq rv(\rho) + \binom{r}{2} - r\epsilon + \binom{r}{2} = rv(\rho) + r(r-1-\epsilon).$$

Using $-r \geq v(\rho)$ we have $r(r-1-\epsilon) \geq -v(\rho)(\epsilon + 1 - r)$, whence

$$v(\omega_v) \geq v(\rho)(\epsilon+1) \geq v(\rho) \cdot q. \tag{8}$$

Case (ii): $v \notin S$, $v(\rho) \geq 0$. Now every element of the local Wronskian matrix is v-integral, so the same holds for the determinant, i.e., $v(\omega_v) \geq 0$ in this case.

Case (iii): $v \in S$, $v(v) > 0$. This case contains the crucial point. As in [4], we consider the identity

$$u^j\rho - u^j(1-u)(1+v+\cdots+v^{h-1}) = u^j v^h \rho. \tag{9}$$

This will be useful to approximate $u^j\rho$ with a polynomial in u, v, at the places under consideration.

In fact, we may use the identity to replace, via suitable column operations, the function f_i, for $i = 1, \ldots, k$, with the left side of (9), with $j = i-1$, which by (9) equals $u^{i-1}v^h\rho$. Observe that this corresponds to subtracting from f_i a certain κ-linear combination of $f_{k+1}, \ldots, f_n$, and thus the value of ω_v is unchanged.

Denoting $g_i = u^{-1}v^h\rho$, we have $\nu(g_i) = (i-1)\nu(u) + h\nu(v) + \nu(\rho)$.

Since $\nu(D_{\epsilon_l} f) \geq \nu(f) - \epsilon_l$, we easily find, on looking again at the individual terms in the determinant expansion, that

$$\nu(\omega_\nu) \geq \frac{k(k-1)}{2}\nu(u) + hk\nu(v) + k\nu(\rho) + \sum_{i=k+1}^{n} \nu(f_i)) - \sigma.$$

Case (iv): $\nu \in S$, $\nu(v) \leq 0$. We now argue directly with the terms in the determinant expansion (that is, we do not perform any column operation). Since $\nu(f_i) = (i-1)\nu(u) + \nu(\rho)$ for $i = 1, \ldots, k$, we find as in the previous case that

$$\nu(\omega_\nu) \geq \frac{k(k-1)}{2}\nu(u) + k\nu(\rho) + \sum_{i=k+1}^{n} \nu(f_i) - \sigma.$$

Summing over all places ν of L/κ, taking into account the estimates obtained in the four cases, and recalling that $\sum_{\nu\in S} \nu(u) = \sum_{\nu\in S} \nu(v) = \sum_{\nu\in S} \nu(f_i) = 0$ for $i > k$, because u, v are S-units, we thus get

$$\sum_{\nu} \nu(\omega_\nu) \geq \sum_{\nu\notin S,\, \nu(\rho)<0} q\nu(\rho) + hk \sum_{\nu\in S,\, \nu(v)>0} \nu(v) + k\sum_{\nu\in S} \nu(\rho) - \sigma|S|. \tag{10}$$

Now, $\sum_{\nu\in S,\, \nu(v)>0} \nu(v) = \sum_{\nu(v)>0} \nu(v)$, because v is an S-unit; also, $\sum_{\nu(v)>0} \nu(v) = -\sum_{\nu(v)<0} \nu(v) = \deg(v)$.

Moreover, (6) shows that $\nu(\omega_\nu) = \sigma\nu(dt/dt_\nu) + \nu(\omega)$. On summing over ν this yields

$$\sum_{\nu} \nu(\omega_\nu) = \sigma \sum_{\nu} \nu\left(\frac{dt}{dt_\nu}\right) + \sum_{\nu} \nu(\omega) = \sigma(2g-2),$$

the last equality holding because of the product formula (since ω does not vanish) and because $2g-2$ is the degree of any canonical divisor (recall that t is a separating element). Comparing with the above yields

$$\sigma\chi - \sum_{\nu\notin S,\, \nu(\rho)<0} q\nu(\rho) \geq hk\deg(v) + k\sum_{\nu\in S} \nu(\rho). \tag{11}$$

Finally, $-\sum_{\nu\in S} \nu(\rho) \leq H(\rho) \leq \deg(u) + \deg(v)$, whence

$$\sigma\chi + qH_S(\rho) \geq (hk-k)\deg(v) - k\deg(v). \tag{12}$$

Now note that by definition,

$$H_S\left(\frac{1-u}{1-v}\right) = \sum_{\nu\notin S,\, \nu(1-v)>\nu(1-u)} \min(\nu(1-v) - \nu(1-u)). \tag{13}$$

In turn the right side may be replaced by

$$\sum_{\nu\notin S} (\nu(1-v) - \min(\nu(1-u), \nu(1-v))). \tag{14}$$

Now $\sum_{v\notin S} \nu(1-v) \le H(1-v) = \deg(v)$ whence

$$H_S(\rho) \le \deg(v) - \sum_{v\notin S} \min(\nu(1-u), \nu(1-v)). \tag{15}$$

Now, putting all together and using that $\sigma \le q(q-1)/2$, we obtain

$$\sum_{v\notin S} \min(\nu(1-u), \nu(1-v)) \le \frac{q+k-hk}{q}\deg(v) + \frac{k}{q}\deg(u) + \frac{q-1}{2}\chi. \tag{16}$$

□

4. Deduction of Weil's bound

We start by deducing from Theorem 3 an upper bound for the number of rational points on the non-singular model $\mathcal{C}$ of the curve defined by $f(x,y)=0$. We recall that we put $a = \deg_X f$, $b = \deg_Y f$ and S is the set formed by the zeros and the poles of x and y on $\mathcal{C}$.

Corollary 3. *The number $N := |\mathcal{C}(\mathbb{F}_{q^2})|$ satisfies the inequality*

$$N \le q^2 - 1 + \frac{q^2-1}{q}[a + (b+ab+a)(a-1)] + \frac{q-1}{2}\chi + |S|. \tag{17}$$

Proof. The estimate is trivial if $f(X,Y)$ is linear in some variable, so we may suppose for instance $b \ge a \ge 2$. We may also suppose that $q > a+b(a-1)$. We let $L = \mathbb{F}_q(\mathcal{C}) = \mathbb{F}_q(x,y)$ be the function field generated by x, y over $\mathbb{F}_q$. Take $z = x^{-q}$, $w = y^{-q}$ and $k = a-1$ in Theorem 3. We take for h the largest integer such that (4) holds; by our assumption, $h \ge 1$.

Then, by construction, the first alternative in Theorem 3 is not satisfied, so the second one holds. The left side of the inequality in Theorem 3 is at least $N - |S|$. Also $\deg(v) = (q^2-1)a$ and $\deg(u) = (q^2-1)b$. So

$$N \le |S| + \frac{q+(a-1)(1-h)}{q}(q^2-1)a + \frac{a-1}{q}(q^2-1)b + \frac{q-1}{2}\chi.$$

Now, $q+(a-1)(1-h) = (q-ah)+(a-1)+h$; also from (4) we have $q-ah \le a+b(a-1)$ and $a-1+h \le (a-1)(b/a)+h = k(b/a)+h < q/a$. Inserting these estimates in the above inequality we obtain the corollary. □

Note that for $q\to\infty$ the inequality (17) is of the shape $|\mathcal{C}(\mathbb{F}_{q^2})| \le q^2 + O(q)$.

It is well known that this estimate is itself sufficient to derive Riemann's hypothesis from other more elementary properties of the zeta function of the curve. This was first shown in Bombieri's elementary proof [2], in which among other things the upper bound was shown to imply a corresponding lower bound. Here we could invoke this procedure, but we prefer to carry out explicitly the arguments, which are particularly simple in this case due to the shape of our Theorem 3.

We shall use Theorem 3 in the form of the following

Corollary 4. *Let $\mathcal{X}$ be a smooth complete absolutely irreducible curve over $\mathbb{F}_q$ of genus g, $x, y \in \mathbb{F}_q(\mathcal{X})$ be non-constant rational functions, and σ be an automorphism of $\mathbb{F}_q(\mathcal{X})/\mathbb{F}_q$. There exists a number $c_1 = c_1(g, \deg x, \deg y)$ such that for all integers $n \geq 1$ the number $N_n(\sigma)$ of points $\xi \in \mathcal{X}(\overline{\mathbb{F}}_q)$ such that*

$$x^\sigma(\xi) = x(\xi)^{q^{2n}}, \qquad y^\sigma(\xi) = y(\xi)^{q^{2n}} \tag{18}$$

satisfies the upper bound

$$N_n(\sigma) \leq [\mathbb{F}_q(\mathcal{X}) : \mathbb{F}_q(x, y)] \cdot q^{2n} + c_1 q^n. \tag{19}$$

Proof. The proof is very similar to that of Corollary 3. Let $L = \mathbb{F}_q(\mathcal{X}) \supset \mathbb{F}_q(x, y, x^\sigma, y^\sigma)$. We let $f(x, y) = 0$ be a minimal algebraic relation between x and y, of bidegree (a, b), where we suppose that $b \geq a$. If $a = 1$ then x is a rational function of y, and (18) reduces to the right equality $y^\sigma(\xi) = y(\xi)^{q^{2n}}$. Now, the rational function $y^\sigma - y^{q^{2n}}$ satisfies $\deg(y^\sigma - y^{q^{2n}}) = q^{2n} \deg y + O(1)$ and this bounds the number of its zeros over $\overline{\mathbb{F}}_q$, proving (19) in a sharpened form. So let us assume $a \geq 2$. We apply Theorem 3, with q^n in place of q, taking the functions x^σ (resp. y^σ) in place of x (resp. y) and taking $z = x^{-q^n}$, $w = y^{-q^n}$.

We have $u = x^\sigma x^{-q^{2n}}$ and $v = y^\sigma y^{-q^{2n}}$, so, as $n \to \infty$, $\deg(u) = q^{2n} H(x) + O(1) = bq^{2n}[L : \mathbb{F}_q(x, y)] + O(1)$, $\deg(v) = q^{2n} H(y) + O(1) = aq^{2n}[L : \mathbb{F}_q(x, y)] + O(1)$.

As in Corollary 3, with the same choices for h, k (i.e. $k = a - 1$, h the largest integer such that $ah + bk < q^n$) we obtain the inequality (19). □

Deduction of the Riemann Hypothesis. Let $\mathcal{C}$ be a smooth complete irreducible algebraic curve over a finite field κ of characteristic p. Let $f(x, y) = 0$ be the equation for a plane model of $\mathcal{C}$, with x separating.

Let $\mathcal{X} \to \mathbb{P}_1$ be the Galois closure of $x : \mathcal{C} \to \mathbb{P}_1$: $\mathcal{X}$ is the smooth model of the function field obtained as Galois closure of the extension $\kappa(\mathcal{C})/\kappa(x)$. We may assume that $\mathcal{X}$ is absolutely irreducible and κ is a finite field $\mathbb{F}_q$ so that the morphism $x : \mathcal{C} \to \mathbb{P}_1$, the Galois closure $\mathcal{X} \to \mathbb{P}_1$ of $\mathcal{C} \to \mathbb{P}_1$ and its Galois group Γ are all defined over $\mathbb{F}_q$.

Let $L = \mathbb{F}_q(\mathcal{X})$ so that by our choice of q, $L/\mathbb{F}_q(x)$ is a regular Galois extension with Galois group Γ.

Let $\Omega \subset \Gamma$ be a system of representatives for the left cosets of the subgroup of Γ fixing $\mathcal{C}$. Observe that the y^σ for $\sigma \in \Omega$ are the conjugates of y over $\mathbb{F}_q(x)$ and in particular $|\Omega| = [\mathbb{F}_q(x, y) : \mathbb{F}_q(x)]$. Hence, for each $\xi \in \mathcal{X}$ with $x(\xi) \in \mathbb{F}_{q^{2n}}$, the value $y(\xi)$ must satisfy one relation of the form $y(\xi)^{q^{2n}} = y^\sigma(\xi)$ for some $\sigma \in \Omega$, since $x(\xi)^{q^{2n}} = x(\xi)$. Then

$$|\{\xi \in \mathcal{X} : x(\xi) \in \mathbb{F}_{q^{2n}}\}| = \sum_{\sigma \in \Omega} N_n(\sigma) + O(1).$$

On the other hand, the left-hand side satisfies

$$|\{\xi \in \mathcal{X} \,:\, x(\xi) \in \mathbb{F}_{q^{2n}}\}| = q^{2n}[L : \mathbb{F}_q(x)] = q^{2n}[L : \mathbb{F}_q(x, y)] \cdot |\Omega|.$$

Let us denote by $E_n(\sigma)$ the error term $N_n(\sigma) - q^{2n}[\mathbb{F}_q(\mathcal{X}) : \mathbb{F}_q(x, y)]$. By the above identity we have

$$\sum_{\sigma \in \Omega} E_n(\sigma) = O(1),$$

whereas by Corollary 4 we have, for every σ,

$$N_n(\sigma) = [\mathbb{F}_q(\mathcal{X}) : \mathbb{F}_q(x, y)] \cdot q^{2n} + O(q^n).$$

Therefore for each $\sigma_0 \in \Omega$,

$$E_n(\sigma_0) \geq -(|\Omega| - 1)c_1 q^n + O(1).$$

In particular, denoting by 1 the identity of the Galois group Γ, we have

$$N_n(1) = [\mathbb{F}_q(\mathcal{X}) : \mathbb{F}_q(x, y)] \cdot q^{2n} + O(q^n).$$

Now, $N_n(1) = [\mathbb{F}_q(\mathcal{X}) : \mathbb{F}_q(x, y)] \cdot |\mathcal{C}(\mathbb{F}_{q^{2n}})| + O(1)$, so

$$|\mathcal{C}(\mathbb{F}_{q^{2n}})| = q^{2n} + O(q^n).$$

This is known to be equivalent to Riemann's hypothesis (see Lemma 3 for the details on this last deduction).

5. On Theorem 2 and its corollaries

The aim of this section is to prove Theorem 2.

We start with an intermediate statement with parameters, which is the analogue in positive characteristic of Proposition 2.2 in [4].

Proposition 2. *Let X be a smooth projective curve over a finite field of characteristic p. Let $u, v \in \kappa(X)$ be rational functions, multiplicatively independent modulo constants, and let S be the set of their zeros and poles. Suppose that $\kappa(X) = \kappa(u, v)$ and put $a = \deg(v)$ and $b = \deg(u)$. Let h, k be integers ≥ 0 such that*

$$ah + bk < p. \tag{20}$$

Finally, denote by $\chi = |S| + 2g - 2$ the Euler characteristic of the curve $X \setminus S$. Then either

$$a \leq k, \quad b \leq h, \tag{21}$$

or

$$\sum_{v \in X \setminus S} \min\{v(u-1), v(v-1)\} \leq \frac{h+2k}{hk+h+k} a + \frac{k}{hk+h+k} b + \frac{hk+h+k-1}{2} \chi. \tag{22}$$

Note that both inequalities (21) and (22) coincide with those in Proposition 2.2 of [4]. As explained in [4], the assumption that $\kappa(u, v) = \kappa(X)$ is not restrictive, but in the general case the right-hand sides of (21) should be multiplied by $[\kappa(X) : \kappa(u, v)]$.

Proof. We follow the proof of Proposition 2.2 in [4] and of Theorem 3 in the present paper. We let $n = hk + h + k$ and define rational functions $f_1, \dots, f_n$, regular outside S. For $i = 1, \dots, k$, we put $f_i = u^{i-1}(u-1)/(v-1)$ while $f_{k+1}, \dots, f_n$ are the functions $u^r v^s$, $0 \le r \le k$, $0 \le s < h$, in some order.

These functions are linearly independent over $\kappa(X)^p$, by Proposition 1 (applied in the case $z = w = 1$). The proof now proceeds by taking the usual Wronskian of $f_1, \dots, f_n$ and using the fact that $\kappa(X)^p$ is the constant field with respect to a non-trivial derivation. Now hyperderivatives do not appear at all, so the sequence $\epsilon_1, \dots, \epsilon_n$ appearing in the proof of Theorem 3 will now be simply $0, 1, \dots, n-1$. The same estimates as in the proof of Proposition 2.2 in [4] give the result. □

Theorem 4. *Let X be a smooth projective absolutely irreducible curve over a finite field κ of characteristic p. Let $u, v \in \kappa(X)$ be separating rational functions, multiplicatively independent modulo κ, and let S be the set of their zeros and poles. Let χ be the Euler characteristic of $X \setminus S$. Let $t > 0$ be a real number. Suppose that*

$$(\deg(u)\deg(v))^2 < \frac{1}{8t^3}(p + \deg u + \deg v)^3 \chi.$$

Then

$$\sum_{v \in X(\overline{\kappa}) \setminus S} \min\{v(1-u), v(1-v)\} \le \left(\frac{4}{t} + \frac{t^2}{2}\right)(\deg u \deg v \chi)^{1/3}.$$

The minimum in t of the factor $4/t + t^2/2$ appearing on the right is attained at $t = \sqrt[3]{4}$. However, it may be convenient to increase this factor by other choices of t, in order to weaken the assumptions.

Proof of Theorem 4. By symmetry, we can and will suppose that $\deg(u) \ge \deg(v)$. For consistency with the previous notation we put $b = \deg(u)$ and $a = \deg(v)$, so $b \ge a$ (note that if $f(u, v) = 0$ is the irreducible equation relating u, v over κ, then $\deg u = \deg_Y f$ and $\deg v = \deg_X f$).

If $\chi \le 0$, the result is trivial since u, v will be necessarily multiplicatively dependent modulo constants, so we suppose from now on that $\chi \ge 1$. Let us denote by G the left-hand side term in (22):

$$G := \sum_{v \in X \setminus S} \min\{v(u-1), v(v-1)\}.$$

Note the trivial bound

$$G \le \min\{\deg(u), \deg(v)\} = a.$$

We have to prove that

$$G \le \left(\frac{4}{t} + \frac{t^2}{2}\right) \cdot (ab\chi)^{1/3}. \tag{23}$$

Let us choose the parameters h, k in order to apply Proposition 2. Put

$$h = \left[t \frac{b^{2/3}}{(a\chi)^{1/3}} \right] - 1, \qquad k = \left[t \frac{a^{2/3}}{(b\chi)^{1/3}} \right] - 1$$

where $[\cdot]$ denotes the integral part. Note that $h \geq k$.

Suppose first that $k < 1$. Then $t^3 a^2/(b\chi) < 8$, so $a^3 < (8/t^3)ab\chi$, and the trivial inequality $G \leq a$ implies

$$G \leq \frac{2}{t}(ab\chi)^{1/3},$$

which is stronger than (23). So (23) is proved in this case.

From now on we shall suppose $h \geq k \geq 1$.

We proceed to verify the inequality (20). We have

$$ah + bk \leq 2t \frac{(ab)^{2/3}}{\chi^{1/3}} - a - b.$$

This in turn implies (20) provided $8t^3 a^2 b^2 < (p + a + b)^3 \chi$, which we are assuming.

We can now apply Proposition 2, which guarantees the validity of either the inequalities (21) or the inequality (22).

Suppose first that the inequalities (21) both hold. Then in particular $b \leq h$, so

$$b^3 < (h+1)^3 \leq t^3 \frac{b^2}{a\chi},$$

so $(ab\chi) \leq t^3$. Since $a \leq b$ and $\chi \geq 1$ we deduce $a^2 \leq t^3$ and from the trivial inequality $G \leq a$ it follows that $G \leq t^{3/2}$. Since $\deg u \deg v \chi \geq 1$, the sought-for result will follow if we prove that $(4/t + t^2/2) > t^{3/2}$ for all positive t. This can be easily checked by standard calculations.

Let us now suppose that the second alternative (22) holds. Since $h \geq k$, we have

$$\frac{h+2k}{hk+h+k} \leq \frac{3}{k+2} \quad \text{and} \quad \frac{k}{hk+h+k} \leq \frac{1}{h+2},$$

and inequality (22) gives

$$G \leq \frac{3}{k+2}a + \frac{1}{h+2}b + \frac{(h+1)(k+1)-2}{2}\chi.$$

Now

$$k+2 \geq t \frac{a^{2/3}}{(b\chi)^{1/3}}, \qquad h+2 \geq t \frac{b^{2/3}}{(a\chi)^{1/3}},$$

while

$$(h+1)(k+1) \leq t^2 \frac{(ab)^{1/3}}{\chi^{2/3}}.$$

Then

$$G \leq \left(\frac{3}{t} + \frac{1}{t} \right)(ab\chi)^{1/3} + \frac{t^2}{2}(ab\chi)^{1/3},$$

and we obtain the desired inequality (23).

Proof of Theorem 2. We distinguish two cases, according to the value of the quotient $Q := p^3\chi/(\deg u \deg v)^2$. In case $Q \geq 4$, the choice $t = \sqrt[3]{4}$ satisfies the assumption of Theorem 4. The estimate for the gcd coincides with the first upper bound in Theorem 2.

In the case $Q \leq 4$, we choose $t = Q^{1/3} \leq \sqrt[3]{4}$. In this case it is immediately checked that $4/t + t^2/2 \leq 6/t$. Again, substituting, Theorem 4 yields the bound $12(\deg u \deg v)/p$.

Acknowledgments. We are pleased to thank E. Bombieri, D. R. Heath-Brown, J. Silverman, J. F. Voloch and A. Wigderson for their interest in this work and some useful remarks and references. We are also grateful to an anonymous referee for his fast and precise report.

References

[1] Ailon, N., Rudnick, Z.: Torsion points on curves and common divisors of $a^k - 1$, $b^k - 1$. Acta Arith. **113**, 31–38 (2004) Zbl 1057.11018 MR 12046966

[2] Bombieri, E.: Counting points on curves over finite fields (d'après S. A. Stepanov). Sém. Bourbaki (1972/1973), exp. 430, Lecture Notes in Math. 383, Springer, 234–241 (1974) Zbl 0307.14011 MR 0429903

[3] Corvaja, P., Zannier, U.: A lower bound for the height of a rational function at S-unit points. Monatsh. Math. **144**, 203–224 (2005) Zbl 1086.11035 MR 2130274

[4] Corvaja, P., Zannier, U.: Some cases of Vojta's conjecture on integral points over function fields. J. Algebraic Geom. **17**, 295–333 (2008); Addendum, Asian J. Math. **14**, 581–584 (2010) Zbl 1221.11146 MR 2369088

[5] Corvaja, P., Zannier, U.: On the maximal order of a torsion point on a curve in $\mathbb{G}_{\mathrm{m}}^n$. Rend. Lincei Mat. Appl. **19**, 73–78 (2008) Zbl 1150.11023 MR 2383563

[6] Corvaja, P., Zannier, U.: An *abcd* theorem over function fields and applications. Bull. Soc. Math. France **139**, 437–454 (2011) Zbl 1252.11031 MR 2869299

[7] Corvaja, P., Zannier, U.: Algebraic hyperbolicity of ramified covers of $\mathbb{G}_{\mathrm{m}}^2$ (and integral points on affine subsets of $\mathbb{P}_2$). J. Differential Geom. **93**, 355–377 (2013) MR 3024299

[8] Garcia, A., Voloch, J. F.: Wronskians and linear independence in fields of prime characteristic. Manuscripta Math. **59**, 457–469 (1987) Zbl 0637.12015 MR 0915997

[9] Garcia, A., Voloch, J. F.: Fermat curves over finite fields. J. Number Theory **30**, 345–356 (1988) Zbl 0671.14012 MR 0966097

[10] Heath-Brown, D. R., Konyagin, S.: New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum. Quart. J. Math. **51**, 221–235 (2000) Zbl 0983.11052 MR 1765792

[11] Hsia, L.-C., Wang, J. T.-Y.: The ABC theorem for higher-dimensional function fields. Trans. Amer. Math. Soc. **356**, 2871–2887 (2004) Zbl 1067.11038 MR 2052600

[12] Lang, S.: Algebra. Rev. 3rd ed., Springer (2002) Zbl 0984.00001 MR 1878556

[13] Stöhr, K. O., Voloch, J. F.: Weierstrass points on curves over function fields. Proc. London Math. Soc. **52**, 1–19 (1986) Zbl 0593.14020 MR 0812443

[14] Silverman, J. H.: Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups. Monatsh. Math. **145**, 333–350 (2005) Zbl 1197.11070 MR 2162351

[15] Silverman, J.: Common divisors of $a^n - 1$ and $b^n - 1$ over function fields. New York J. Math. **10**, 37–43 (2004) Zbl 1120.11045 MR 2052363

[16] Voloch, J. F.: On the order of torsion points on curves over finite fields. Integers **7**, A49, 4 pp. (2007) MR 2373111