On a variant of the Ailon-Rudnick theorem in finite characteristic

D. Ghioca, L.-C. Hsia and T. J. Tucker

Abstract. Let L be a field of characteristic p, and let $a, b, c, d \in L(T)$. Assume that a and b are algebraically independent over $\mathbb{F}_p$. Then for each fixed positive integer n, we prove that there exist at most finitely many $\lambda \in \overline{L}$ satisfying $f(a(\lambda)) = c(\lambda)$ and $g(b(\lambda)) = d(\lambda)$ for some polynomials $f, g \in \mathbb{F}_{p^n}[Z]$ such that $f(a) \neq c$ and $g(b) \neq d$. Our result is a characteristic p variant of a related statement proven by Ailon and Rudnick.

1. Introduction

We prove the following result.

Theorem 1.1. *Let L be a field of characteristic $p > 0$, let $a, b, c, d \in L(T)$, and let q be a power of p. Suppose that a and b are algebraically independent over $\mathbb{F}_p$. Then there are finitely many $\lambda \in \overline{L}$ such that there exist some $f, g \in \mathbb{F}_q[Z]$ satisfying the following two properties:*

(i) *$f(a(\lambda)) = c(\lambda)$ and $g(b(\lambda)) = d(\lambda)$; but*
(ii) *$f(a) \neq c$ and $g(b) \neq d$.*

It is immediate to see that the hypothesis in Theorem 1.1 is essential, as shown by the following example and also by the examples referenced in [Sil04a] (where $a, b \in \overline{\mathbb{F}}_p[T]$ and $c = d = 1$).

Example 1.2. Assume $a, b \in L \setminus \overline{\mathbb{F}}_p$ such that $a + b = 1$; also, assume $c(T) = d(T) = T$. Then for each $n \in \mathbb{N}$, letting $F_n(Z) = Z^{p^n}$ and $G_n(Z) = 1 - Z^{p^n}$, we have that

$$F_n(a) - c(T) = a^{p^n} - T = G_n(b) - d(T);$$

so, there exist infinitely many $t \in \overline{L}$ satisfying conditions (i)-(ii) in Theorem 1.1.

The following result is an immediate corollary of Theorem 1.1.

Corollary 1.3. *Let L be a field of characteristic $p > 0$ and let $a, b, c, d \in L[T]$ such that a and b are algebraically independent over $\mathbb{F}_p$. Then the following*

$$S := \bigcup_{\substack{m,n \geq 1 \\ a^m \neq c, b^n \neq d}} \left\{\lambda \in \overline{L} \,:\, (T - \lambda) \mid \gcd(a^m - c, b^n - d)\right\}$$

is a finite set.

2010 AMS Subject Classification: Primary 11G50; Secondary 11G35, 14G25. The research of the first author was partially supported by an NSERC Discovery grant. The second author was supported by MOST grant 104-2115-M-003-004-MY2. The third author was partially supported by NSF Grant DMS-1501515.

Remark 1.4. In the special case $c = d = 1$, we note that Corollary 1.3 also follows easily from the fact that if a curve defined over an extension of $\mathbb{F}_p$ has infinitely many $\overline{\mathbb{F}}_p$-points, then the curve itself is defined over $\overline{\mathbb{F}}_p$. However, for the full statement of Corollary 1.3 (or more generally, Theorem 1.1) which allows for arbitrarily polynomials c and d, the points $(a(\lambda), b(\lambda))$ (for $\lambda \in S$) need not lie in $\overline{\mathbb{F}_p}^2$, and our proof requires information about points of small height, which is supplied by [Ghi14].

On the other hand, one cannot expect in Corollary 1.3 (nor in the similar statement from Theorem 1.1) that $\gcd(a^m - c, b^n - d)$ has bounded degree, as we can see from the following construction.

Example 1.5. Let $a, b \in L[T]$ such that $a(0) = b(0) = 1$, but there is no nonzero $F \in \overline{\mathbb{F}}_p[X, Y]$ such that $F(a, b) = 0$. Clearly, $\gcd\left(a^{p^n} - 1, b^{p^n} - 1\right)$ has the root $\lambda = 0$ with multiplicity at least equal to p^n.

If one restricts in Corollary 1.3 to computing $\gcd(a^m - 1, b^n - 1)$ for positive integers m and n which are coprime to p, then an argument similar to [Sil04b, Theorem 8 part (b)] yields the uniform boundedness of the degree of this greatest common divisor as we vary among all $m, n \in \mathbb{N}$ coprime with p. As shown in [Sil04b], the key fact is that for any positive integer n not divisible by p, the endomorphism of $\mathbb{G}_m$ given by the map $x \mapsto x^n$ (defined over $\mathbb{F}_p$) is étale. Furthermore, strengthening the hypotheses in Theorem 1.1, we can prove the uniform boundedness of the degree of $\gcd(f(a) - c, g(b) - d)$, as we let f and g vary in $\mathbb{F}_q[Z]$; we state the next result only for polynomials $a, b, c, d \in L[T]$, though an appropriate modification (with a similar proof) holds for rational functions as well.

Theorem 1.6. *Let p be a prime number, let $n \in \mathbb{N}$, let L be a field of characteristic $p > 0$ and let $a, b, c, d \in L[T]$ with the property that there is no $\lambda \in \overline{L}$ such that both $a(\lambda)$ and $b(\lambda)$ are contained in $\overline{\mathbb{F}}_p$. Then there exists a nonzero polynomial $D \in L[T]$ with the property that for any $f, g \in \mathbb{F}_{p^n}[Z]$ such that $f(a) \neq c$ and $g(b) \neq d$, we have that* $\gcd(f(a(T)) - c(T), g(b(T)) - d(T)) \mid D(T)$.

Corollary 1.3 (along with Theorem 1.6) is in the spirit of the main result of Ailon-Rudnick [AR04], who proved that if $a, b \in \mathbb{C}[T]$ are multiplicatively independent, then there exists a nonzero polynomial $c \in \mathbb{C}[t]$ such that $\gcd(a^k - 1, b^k - 1) \mid c$ for all $k \in \mathbb{N}$. In turn, the result of Ailon-Rudnick was motivated by the work of Bugeaud-Corvaja-Zannier [BCZ03] who established an upper bound for $\gcd(a^k - 1, b^k - 1)$ (as k varies in $\mathbb{N}$) for given $a, b \in \overline{\mathbb{Q}}$. We also mention that this problem of bounding the greatest common divisor has been studied in several other directions as well: for elements close to S-units (see [CZ13b, Luc05]), for elliptic divisibility sequences (see [Sil04b]), and also for compositional iterates of complex polynomials (see [HT]). Furthermore, we note that the result of [CZ13b] extends in arbitrary characteristic the main theorem of [CZ08], which in turn had interesting applications to a special case of a conjecture of Vojta concerning integral points for the complement in $\mathbb{P}^2$ of certain curves (see [CZ13a]) and to rational curves on projective surfaces (see [CZ11]). We also mention that our Theorem 1.1 bears resemblance to [Mas14, Theorem 1.1]; one of the differences is that our result holds in the absence of an algebraic group, even though, a special case of our result (when a, b and c are algebraically independent over $\mathbb{F}_p$ and $d = 1$) can be recovered from the main theorem of [Mas14]. Finally, we note that our Theorem 1.1 answers in the affirmative the following special case of [HT, Question 17].

Corollary 1.7. *Let p be a prime number, let $f, g \in \overline{\mathbb{F}}_p[Z]$, let L be a field of characteristic p, and let $a, b, c, d \in L[T]$ such that a and b are algebraically independent over $\mathbb{F}_p$. Then there exist at most finitely many $\lambda \in \overline{L}$ with the property that for some $m, n \in \mathbb{N}$ we have that $f^{\circ m}(a(\lambda)) = c(\lambda)$ (but $f^{\circ m}(a) \neq c$) and $g^{\circ n}(b(\lambda)) = d(\lambda)$ (but $g^{\circ n}(b) \neq d$).*

On the other hand, Silverman [Sil04a] showed that for nonconstant $a, b \in \overline{\mathbb{F}}_p[T]$, there exist infinitely many $\lambda \in \overline{\mathbb{F}}_p$ which are roots of $\gcd(a^m - 1, b^n - 1)$. Actually, the same analysis as in [Sil04a] suggests that more generally, when the polynomials a, b, c and d are all defined over a finite field $\mathbb{F}_q$, the polynomials $\gcd(a^m - c, b^n - d)$ may have infinitely many distinct roots as we vary m and n. Indeed, if a and b were primitive roots for infinitely many distinct prime ideals $\mathfrak{p}$ of $\mathbb{F}_q[T]$ (i.e., that both a and b modulo $\mathfrak{p}$ generate the cyclic group $(\mathbb{F}_q[T]/\mathfrak{p})^*$, which often times happens, as it is shown in [PS95]), then there exist $m, n \in \mathbb{N}$ such that $\gcd(a^m - c, b^n - d) \in \mathfrak{p}$, thus showing that there are infinitely many roots of these gcd-polynomials as we vary m and n.

In Corollary 1.3 (and more generally, in Theorem 1.1) we show that if a and b are algebraically independent over $\mathbb{F}_p$ (which is the same as algebraic independence over $\overline{\mathbb{F}}_p$), then $\gcd(a^m - c, b^n - d)$ has at most finitely many distinct roots as we vary m and n. As an aside, note that in Corollary 1.3, if L is a finite field, as it is the case in Silverman's examples from [Sil04a], then a and b must be algebraically dependent over $\mathbb{F}_p$ (and then also $\gcd(a^m - 1, b^n - 1)$ may have arbitrarily many distinct roots).

We also note (see the next example) that it is essential in Theorem 1.1 to restrict ourselves to polynomials $f, g \in \mathbb{F}_q[Z]$, rather than considering all polynomials in $\overline{\mathbb{F}}_p[Z]$.

Example 1.8. Let $L = \mathbb{F}_p(t)$, let $a, b \in L(T)$ such that there is no $F \in \overline{\mathbb{F}}_p[X, Y]$ so that $F(a, b) = 0$, and let $c(T) := a(T) - T$ and $d(T) := b(T) - T$. Then, for any $\lambda \in \overline{\mathbb{F}}_p$, letting $f(Z) := Z - \lambda$, we have that

$$f(a) - c = f(b) - d = T - \lambda,$$

thus showing that in the conclusion of Theorem 1.1 we have to restrict ourselves to the case when $f, g \in \mathbb{F}_q[Z]$ for some given prime power q.

Our Theorem 1.1 can also be interpreted from the point of view of the principle of *unlikely intersections* in arithmetic geometry (for a comprehensive discussion on this topic, see [Zan12]). Indeed, let L be a field of characteristic p, and let $a, b, c, d \in L(T)$; then these rational functions parametrize a (rational) curve C defined over L inside $(\mathbb{P}^1)^4$. More precisely, C consists of all points of the form

$$\left\{(a(t), b(t), c(t), d(t)) : t \in \overline{L}\right\}. \tag{1.9}$$

Then for a given q (which is a power of p), and for any $f, g \in \mathbb{F}_q[Z]$, we define the surface $Y_{f,g} \subset (\mathbb{P}^1)^4$ given by the equations

$$x_3 = f(x_1) \text{ and } x_4 = g(x_2),$$

where (x_1, x_2, x_3, x_4) are the coordinates of $(\mathbb{P}^1)^4$. In Theorem 1.1, we prove that if C is not contained in a hypersurface of $(\mathbb{P}^1)^4$ defined by an equation of the form

$$F(x_1, x_2) = 0 \text{ for some nonzero } F \in \overline{\mathbb{F}}_p[Z_1, Z_2], \tag{1.10}$$

then $C(\overline{L}) \cap \left(\bigcup_{f,g\in\mathbb{F}_q[Z]} Y_{f,g}(\overline{L})\right)$ is finite. This geometric reformulation is similar to [CGMM13, Theorem 1.2], which is a function field version of the classical Pink-Zilber conjecture; in the same spirit, see also [GMZ15] for partial results on the Bounded Height Conjecture for function fields formulated in [CGMM13]. Indeed, a special case of [CGMM13, Theorem 1.2] yields that as long as the curve C from (1.9) is not contained in a proper subvariety of $(\mathbb{P}^1)^4$ defined over $\overline{\mathbb{F}}_p$ (which is a significantly stronger hypothesis than (1.10)), then the intersection of C with the union of all surfaces $S \subset (\mathbb{P}^1)^4$ defined over $\overline{\mathbb{F}}_p$ is finite. Actually, the result from [CGMM13, Theorem 1.2] is stated for affine subvarieties, but the exact same proof works for subvarieties of $(\mathbb{P}^1)^n$. The following result (which is in the same spirit as [Ost16, Theorem 1.3]) is an immediate consequence of [CGMM13, Theorem 1.2] (for fields of arbitrary characteristic).

Corollary 1.11. *Let L be a function field over an algebraically closed field K, let $m, k, n, \ell \in \mathbb{N}$, and let*

$$a_1, \dots, a_m, b_1, \dots, b_k, c_1, \dots, c_n, d_1, \dots, d_\ell \in L(T)$$

with the property that there exists no nonzero $F \in K[X_1, \dots, X_{m+n+k+\ell}]$ such that $F(a_1, \dots, a_m, b_1, \dots, b_k, c_1, \dots, c_n, d_1, \dots, d_\ell) = 0$. Then there exist at most finitely many $t \in \overline{L}$ with the property that there exist some $f \in K[X_1, \dots, X_m]$ and $h \in K[Z_1, \dots, Z_n]$ (not both constant) and some $g \in K[Y_1, \dots, Y_k]$ and $j \in K[W_1, \dots, W_\ell]$ (not both constant) such that

$$f(a_1(t), \dots, a_m(t)) = h(c_1(t), \dots, c_n(t)) \text{ and} \tag{1.12}$$

$$g(b_1(t), \dots, b_k(t)) = j(d_1(t), \dots, d_\ell(t)). \tag{1.13}$$

Indeed, the hypothesis from Corollary 1.11 yields that the curve C in $(\mathbb{P}^1)^{m+k+n+\ell}_{\overline{L}}$, given by the parametrization

$$(a_1(t), \dots, a_m(t), b_1(t), \dots, b_k(t), c_1(t), \dots, c_n(t), d_1(t), \dots, d_\ell(t))$$

is not contained in any proper subvariety defined over K, and therefore [CGMM13, Theorem 1.2] yields that its intersection with the union of all subvarieties of $(\mathbb{P}^1)^{m+nk+\ell}$ of codimension 2 is finite. Conditions (1.12)-(1.13) in Corollary 1.11 simply tell us that we intersect the curve C with all codimension-2 subvarieties of $(\mathbb{P}^1)^{m+k+n+\ell}$ given by equations of the form

$$f(x_1, \dots, x_m) = h(x_{m+k+1}, \dots, x_{m+k+n}) \text{ and}$$

$$g(x_{m+1}, \dots, x_{m+k}) = j(x_{m+k+n+1}, \dots, x_{m+k+n+\ell}),$$

for (non-constant) polynomials f, g, h, j with coefficients in K, and therefore the intersection must be finite.

In Corollary 1.11, if $K = \overline{\mathbb{F}}_p$ then we recover a result similar to our Theorem 1.1. However, the difference is that in Corollary 1.11 we have a stronger hypothesis, i.e., with the notation as in Theorem 1.1, we would have to ask that a, b, c, d are algebraically independent over $\mathbb{F}_p$, while in Theorem 1.1 we only ask that a and b are algebraically independent over $\mathbb{F}_p$.

We present now the plan for our paper. We start in Section 2 by introducing the necessary notation for our paper. In Section 3 we prove various results which we will use later in order to establish the conclusion of Theorem 1.1. In Section 3, we also state (see Theorem 3.6) a result from [Ghi14] (which, in turn, generalizes [Ghi09]) regarding points of small height on curves. We discuss next these results and their connection to our problem in the special case when $\mathrm{trdeg}_{\mathbb{F}_p} L = 1$. So, in [Ghi09, Theorem 2.2] it is proven that if $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ is a curve defined over $\overline{\mathbb{F}_p(t)}$, but which is not defined over $\overline{\mathbb{F}}_p$, then there exists a positive constant c_0 such that for all but finitely many points $(x, y) \in C\left(\overline{\mathbb{F}_p(t)}\right)$, we have that

$$\max\{h(x), h(y)\} \ge c_0,$$

where $h(\cdot)$ is the usual Weil height on $\mathbb{P}^1$ corresponding to the function field $\mathbb{F}_p(t)$ (for more details regarding heights on function fields, see Section 2).

Now, we note that we may assume in Theorem 1.1 that L is finitely generated; thus, assuming further that $\mathrm{trdeg}_{\mathbb{F}_p} L = 1$, we have that L is a finite extension of $\mathbb{F}_p(t)$. Our hypothesis from Theorem 1.1 yields that if at least one of a or b is in $L(T) \setminus L$, then the rational curve

$$\left\{(a(t), b(t)) \colon t \in \overline{L}\right\} \subset \mathbb{P}^1_{\overline{L}} \times \mathbb{P}^1_{\overline{L}}$$

is not defined over $\overline{\mathbb{F}}_p$. However, as shown by our Lemma 3.1, if $a, b \in L(T)\setminus L$, then the existence of infinitely many λ_i satisfying the conditions (i)-(ii) from Theorem 1.1 yields that

$$\max\left\{h(a(\lambda_i)), h(b(\lambda_i))\right\} \to 0,$$

contradicting thus Theorem 3.6 (in the special case when $\mathrm{trdeg}_{\mathbb{F}_p} L = 1$). In Section 4, we finish the proof of Theorem 1.1; we also note that the case when a (or b) is in L requires a different argument than the general case (see Claim 4.1). The conclusion in Theorem 1.6 follows then easily from Theorem 1.1.

Acknowledgments. We thank Joe Silverman, Alina Ostafe, and the anonymous referee for their useful comments and suggestions which improved our presentation.

2. Preliminaries

In this section, we set up our notation and recall facts from the theory of height functions and specializations that will be used in this paper.

2.1. Global (function) fields. A *product formula field* L is a field equipped with a set of inequivalent absolute values (places) Ω_L, normalized so that the product formula holds (see (2.1)); the corresponding absolute value to a place $v \in \Omega_L$ is denoted by $|\cdot|_v$. More precisely, for each $v \in \Omega_L$ there exists a positive integer N_v such that for all $\alpha \in L^*$ we have the *product formula*:

$$\prod_{v\in\Omega_L} |\alpha|_v^{N_v} = 1. \tag{2.1}$$

Examples of product formula fields (or *global fields*) are number fields and function fields of projective varieties which are regular in codimension 1 over another field k (see [Lan83, § 2.3] or [BG06, § 1.4.6]). We remark that if $L = k(V)$ is a function field of a projective variety which is regular in codimension 1, then each place in Ω_L corresponds to an irreducible subvariety of codimension one in V; also, as proven in [deJ96, Remark 4.2], at the expense of replacing L by a finite extension, we may even assume that it is the function field of an irreducible, smooth, projective variety defined over a finite extension of k.

2.2. Weil height. Let L' be a finite extension of L, and let $\Omega_{L'}$ be the set of all absolute values of L' which extend the absolute values in Ω_L. For each $w \in \Omega_{L'}$ extending some $v \in \Omega_L$ we let $N_w := N_v \cdot [L'_w : L_v]$, where L_v and L'_w are the corresponding completions of L and L' with respect to $|\cdot|_v$ and $|\cdot|_w$. The (naive) *Weil height* of any point $x \in L'$ is defined as

$$h(x) = \frac{1}{[L' : L]} \sum_{w \in \Omega_{L'}} N_w \cdot \log \max\{1, |x|_w\}.$$

As shown in [Lan83] (see also [BG06]), the above definition of the height $h(x)$ is independent of the field L' containing x. Since we will work with heights on $\mathbb{P}^1$, we simply define $h([x : 1]) := h(x)$ for any $x \in \overline{L}$, and also define $h([1 : 0]) := 0$.

In our paper we will often use height functions relative to different global (function) fields; therefore, to avoid confusion, we will use the notation $h^{(L)}$ to indicate that the height is computed with respect to the global field (L, Ω_L). Furthermore, if the places in Ω_L correspond to viewing L as a function field over (a finite exension of) the field k, we will use the notation $h^{(L/k)}$. An important property for the Weil height $h^{(L/k)}$ is that if $\alpha \in \overline{L}$, then

$$h^{(L/k)}(\alpha) = 0 \text{ if and only if } \alpha \in \overline{k}. \tag{2.2}$$

2.3. Properties of the Weil height. Let L be a product formula field and let $f \in L(x) \setminus L$. We will often use the following standard fact (see [Lan83, Theorem 1.8, p. 81])

$$h^{(L)}(f(x)) = \deg(f) \cdot h^{(L)}(x) + O(1), \tag{2.3}$$

i.e., there is a positive constant C (depending on f, but independent of $x \in \overline{L}$) such that

$$\left| h^{(L)}(f(x)) - \deg(f) \cdot h^{(L)}(x) \right| \le C.$$

Now, assume L is a function field over some other field k, let $x \in \overline{L}$ and let $f \in k[T] \setminus k$. Then we will often use the following easy fact (which strengthens (2.3) under our assumption that each coefficient of f is in k)

$$h^{(L/k)}(f(x)) = \deg(f) \cdot h^{(L/K)}(x). \tag{2.4}$$

Indeed, formula (2.4) follows from the fact that for each $v \in \Omega_L$, if $|x|_v \le 1$ then also $|f(x)|_v \le 1$, while if $|x|_v > 1$ then $|f(x)|_v = |x|_v^{\deg(f)}$ since each coefficient of f belongs to the constants field k.

3. Some useful results

The following result is crucial in the proof of Theorem 1.1.

Lemma 3.1. *Let L be a global field of characteristic p, let q be a power of p, let $a \in L(T) \setminus L$, let $c \in L(T)$, and let $(\lambda_i)_{i=1}^{\infty} \subset \overline{L}$ be a nonrepeating sequence such that for each i, there is a polynomial $f_i \in \mathbb{F}_q[Z]$ with the property that $f_i(a(\lambda_i)) = c(\lambda_i)$, but $f_i(a) \neq c$. Then $\lim_{i \to \infty} h^{(L)}(a(\lambda_i)) = 0$.*

Proof. We let a sequence $\{\lambda_i\} \subset \overline{L}$ satisfying the above hypotheses with respect to some polynomials $f_i \in \mathbb{F}_q[Z]$. Since there are finitely many polynomials in $\mathbb{F}_q[Z]$ of any given degree, we may assume each f_i is nonconstant, and furthermore, $\deg(f_i) \to \infty$. Then for each i, we have

$$h^{(L)}(f_i(a(\lambda))) = (\deg f_i) h^{(L)}(a(\lambda_i)) \text{ (by (2.4))} \tag{3.2}$$

and

$$h^{(L)}(c(\lambda_i)) \leq (\deg c) h^{(L)}(\lambda_i) + O(1) \text{ (by (2.3))}. \tag{3.3}$$

Combining (3.2) with (3.3), along with the fact that $f_i(a(\lambda_i)) = c(\lambda_i)$, we obtain

$$h^{(L)}(a(\lambda_i)) \leq \frac{1}{\deg f_i} \cdot \Big(\deg c \cdot h^{(L)}(\lambda_i) + O(1)\Big) \tag{3.4}$$

On the other hand,

$$(\deg a) h^{(L)}(\lambda_i) \leq h^{(L)}(a(\lambda_i)) + O(1) \text{ (by (2.3))}; \tag{3.5}$$

so, combining (3.4) with (3.5), along with the fact that $\deg(f_i) \to \infty$ and $\deg(a) \geq 1$, we obtain that the heights of the λ_i must be bounded. Then (3.4) finishes the proof of Lemma 3.1 because $\deg(f_i) \to \infty$. ☐

We will also use the following result from [Ghi14, Theorem 1.4] (see also [Ghi14, Remark 1.5]).

Theorem 3.6. *Let L be a function field of transcendence degree 1 over another field k, and let C be an irreducible curve in $\mathbb{P}^1 \times \mathbb{P}^1$ defined over $\overline{L}$. If C is not defined over $\overline{k}$, then there is an $\epsilon > 0$ such that there are at most finitely many $(x, y) \in C(\overline{L})$ for which $\max\left\{h^{(L/k)}(x), h^{(L/k)}(y)\right\} < \epsilon$.*

4. Proof of our main results

Proof of Theorem 1.1. Without loss of generality (at the expense of replacing L with a suitable subfield), we may assume L is finitely generated. Indeed, for any field L_0 such that $a, b, c, d \in L_0(T)$, then any λ satisfying conditions (i)-(ii) from Theorem 1.1 must be algebraic over the field L_0. So, from now on, we assume L is finitely generated.

First we prove that it suffices to assume that both a and b are non-constant in $L(T)$.

Claim 4.1. *If $a \in L$ or $b \in L$, then Theorem 1.1 holds.*

Proof. Without loss of generality, we may assume $a \in L$. We argue by contradiction and thus assume there exist infinitely many $\lambda_i \in \overline{L}$ satisfying conditions (i)-(ii) corresponding to some polynomials $f_i, g_i \in \mathbb{F}_q[Z]$. An important observation throughout our proof of Theorem 1.1 is that $\deg(f_i) \to \infty$ and also $\deg(g_i) \to \infty$, since for any given $d \in \mathbb{N}$, there exist finitely many polynomials of degree d with coefficients in $\mathbb{F}_q$.

We have two cases: either $b \in L$ as well, or $b \in L(T) \setminus L$.

Case 1. Assume first that $b \in L$. In this case, we immediately get that $c, d \in L(T) \setminus L$ since otherwise conditions (i) and (ii) of Theorem 1.1 can not be satisfied simultaneously. By assumption $\mathrm{trdeg}_{\overline{\mathbb{F}}_p}(\overline{\mathbb{F}}_p(a, b)) = 2$, therefore we may view L as a function field over $L_1 := \mathbb{F}_p(a)$. Because $b \notin \overline{L_1}$, then (2.2) yields that

$$h^{(L/L_1)}(b) > 0. \tag{4.2}$$

Using that $g_i \in \mathbb{F}_q[Z]$, then (2.4) yields that

$$h^{(L/L_1)}(d(\lambda_i)) = h^{(L/L_1)}(g_i(b)) = \deg(g_i) \cdot h^{(L/L_1)}(b) \to \infty \text{ as } i \to \infty, \tag{4.3}$$

since $\deg(g_i) \to \infty$ as $i \to \infty$. Equation (4.3) combined with equation (2.3) yields that

$$h^{(L/L_1)}(\lambda_i) \to \infty \quad \text{as } i \to \infty. \tag{4.4}$$

On the other hand, since $f_i(a) \in \overline{L_1}$ for each i and thus $h^{(L/L_1)}(f_i(a)) = 0$, we also get that $h^{(L/L_1)}(c(\lambda_i)) = 0$ (because $f_i(a) = c(\lambda_i)$). Again using equation (2.3) (note that $c \in L(T) \setminus L$), we obtain that

$$h^{(L/L_1)}(\lambda_i) \text{ is bounded.} \tag{4.5}$$

Equations (4.4) and (4.5) yield a contradiction; therefore, there are at most finitely many $\lambda \in \overline{L}$ satisfying both conditions (i)-(ii) from the conclusion of Theorem 1.1.

Case 2. Now, assume $b(T) \in L(T) \setminus L$. We may assume $a \notin \overline{\mathbb{F}}_p$ because otherwise, $\operatorname{trdeg}_{\overline{\mathbb{F}}_p}(\overline{\mathbb{F}}_p(a, b)) \le 1 < 2$ which is not the case. Because $a \notin \overline{\mathbb{F}}_p$, its height $h^{(L/\mathbb{F}_p)}(a)$ is positive (where the height $h^{(L/\mathbb{F}_p)}(\cdot)$ is constructed by viewing L as a finite transcendence degree function field over a finite extension of $\mathbb{F}_p$). Then, as shown by Lemma 3.1 (note that $b \in L(T) \setminus L$), for any infinite sequence $\lambda_i \in \overline{L}$ with the property that there exist some $g_i \in \mathbb{F}_q[T]$ for which $g_i(b) \ne d$ but $g_i(b(\lambda_i)) = d(\lambda_i)$ we have

$$h^{(L/\mathbb{F}_p)}(b(\lambda_i)) \to 0. \tag{4.6}$$

Using (2.3) and (4.6) (note that b is not a constant function in $L(T)$), we get that

$$h^{(L/\mathbb{F}_p)}(\lambda_i) \text{ is bounded.} \tag{4.7}$$

On the other hand, if $f_i(a) \ne c$ but $f_i(a) = c(\lambda_i)$ for some $f_i \in \mathbb{F}_q[Z]$, then (arguing as in the previous **Case 1**) we have

$$h^{(L/\mathbb{F}_p)}(c(\lambda_i)) = h^{(L/\mathbb{F}_p)}(f_i(a)) = \deg(f_i) \cdot h^{(L/\mathbb{F}_p)}(a) \to \infty. \tag{4.8}$$

Then using (2.3) and (4.8) yields

$$h^{(L/\mathbb{F}_p)}(\lambda_i) \to \infty. \tag{4.9}$$

Equations (4.7) and (4.9) are contradictory, thus proving that there is no infinite set of $\lambda \in \overline{L}$ satisfying conditions (i)-(ii) in Theorem 1.1; this concludes the proof of Claim 4.1. $\square$

So, from now on, we assume that $a, b \in L(T) \setminus L$. We argue by contradiction, and so, we suppose that we have an infinite sequence $\{\lambda_i\} \subset \overline{L}$ satisfying conditions (i)-(ii) in Theorem 1.1 corresponding to some polynomials $f_i, g_i \in \mathbb{F}_q[Z]$.

If L is algebraic over $\mathbb{F}_p$, then clearly, $\operatorname{trdeg}_{\overline{\mathbb{F}}_p}(\overline{\mathbb{F}}_p(a, b)) \le 1 < 2$. So, from now on, we assume that L has positive transcendence degree over $\mathbb{F}_p$.

Let $\operatorname{trdeg}_{\overline{\mathbb{F}}_p}(L) = n \ge 1$ and let K be any finitely generated subfield of L of transcendence degree $n - 1$ over $\mathbb{F}_p$. As above, we let $h^{(L/K)}$ denote the Weil height function corresponding to the function field L/K (of transcendence degree 1). Lemma 3.1 applied to a and c, respectively to b and d (note that $a, b \in L(T) \setminus L$) yields that

$$\lim_{i\to\infty} \max\left\{h^{(L/K)}(a(\lambda_i)), h^{(L/K)}(b(\lambda_i))\right\} \to 0. \tag{4.10}$$

Hence, by Theorem 3.6, the curve C parametrized by $(a(t), b(t))$ over all $t \in \overline{L}$ must be defined over $\overline{K}$. However, we can repeat this argument for *any* finitely generated subfield K of L such that $\operatorname{trdeg}_K L = 1$. Since the intersection (inside $\overline{L}$) of all algebraic closures of such subfields equals $\overline{\mathbb{F}}_p$, we conclude that C is defined over $\overline{\mathbb{F}}_p$. Hence there exists a nonzero polynomial $F \in \overline{\mathbb{F}}_p[X, Y]$ such that $F(a, b) = 0$, contradicting our hypothesis. This concludes the proof of Theorem 1.1. □

Proof of Theorem 1.6. We first note that the hypothesis that there is no $\lambda \in \overline{L}$ such that both $a(\lambda)$ and $b(\lambda)$ are contained in $\overline{\mathbb{F}}_p$ is actually stronger than the hypothesis from Theorem 1.1 that a and b are algebraically independent over $\mathbb{F}_p$. Indeed, the hypothesis of Theorem 1.6 yields that the L-rational curve in $\mathbb{P}^1 \times \mathbb{P}^1$ parametrized by $(a(t), b(t))$ is not defined over $\overline{\mathbb{F}}_p$; hence a and b are algebraically independent over $\mathbb{F}_p$. So, Theorem 1.1 yields the existence of only finitely many $\lambda \in \overline{L}$ which are roots of the greatest common divisors of the nonzero polynomials $f(a)(T) - c(T)$ and $g(b)(T) - d(T)$ for some $f, g \in \mathbb{F}_{p^n}$. Hence, all we have left to prove is that for each of these finitely many λ's, their corresponding multiplicity in $\gcd(f(a)(T)-c(T), g(b)(T)-d(T))$ is uniformly bounded independent of $f, g \in \mathbb{F}_{p^n}$ (as long as $f(a) \neq c$ and $g(b) \neq d$). The desired conclusion follows from the following easy claim.

Claim 4.11. *Let $f_1, f_2, g_1, g_2 \in \overline{\mathbb{F}}_p[Z]$ such that $f_1 \neq f_2$ and $g_1 \neq g_2$. Then the polynomials $f_1(a) - c$, $g_1(b) - d$, $f_2(a) - c$ and $g_2(b) - d$ are coprime.*

Proof of Claim 4.11. Assume there exists some $\lambda \in \overline{L}$ such that

$$f_1(a(\lambda)) = c(\lambda) = f_2(a(\lambda)) \text{ and } g_1(b(\lambda)) = d(\lambda) = g_2(b(\lambda)).$$

Thus, letting $f_0 := f_1 - f_2$ and $g_0 := g_1 - g_2$ (which are both nonzero polynomials according to our hypotheses), we get that

$$f_0(a(\lambda)) = g_0(b(\lambda)) = 0,$$

which yields that $a(\lambda), b(\lambda) \in \overline{\mathbb{F}}_p$. This contradicts the hypothesis of Theorem 1.6, thus proving Claim 4.11. □

Claim 4.11 yields that for each of the finitely many λ which is a root of some $\gcd(f_1(a)(T) - c(T), g_1(b)(T) - d(T))$ (for some $f_1, g_1 \in \mathbb{F}_{p^n}$), its multiplicity in *any* of the greatest common divisors of $f(a) - c$ and of $g(b) - d$ as we vary $f, g \in \mathbb{F}_{p^n}$ is uniformly bounded in terms of the maximum of the multiplicity of λ as a root either of $f_1(a)(T) - c(T)$ or of $g_1(b)(T) - d(T)$. This concludes the proof of Theorem 1.6. □

References

[AR04] Ailon, N.; Rudnick, Z. Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$, *Acta Arith.* **113** (2004), no. 1, 31–38. MR2046966 (2004m:11045), Zbl 1057.11018.

[BG06] Bombieri, E.; Gubler, W. Heights in Diophantine Geometry *New Mathematical Monograph* **3**, *Cambridge Univ. Press, Cambridge*, 2006. MR2216774 (2007a:11092), Zbl 1115.11034.

[BCZ03] Bugeaud, Y.; Corvaja, P.; Zannier, U. An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$, *Math. Z.* **243** (2003), 79–84. MR1953049 (2004a:11064), Zbl 1021.11001.

[CGMM13] Chatzidakis, Z.; Ghioca, D.; Masser, D.; Maurin, G. Unlikely, likely, and impossible intersections without algebraic groups, *Rend. Lincei Mat. Appl.* **24** (2013), 485–501. MR3129750, Zbl 1320.11060.

[CZ08] Corvaja, P.; Zannier, U. Some cases of Vojta's conjecture on integral points over function fields, *J. Algebraic Geom.* **17** (2008), 295?333. MR2369088, Zbl 1221.11146; Addendum, Asian J. Math. **14**, 581-?84 (2010) MR2774278.

[CZ11] Corvaja, P.; Zannier, U. An *abcd* theorem over function fields and applications, *Bull. Soc. Math. France* **139** (2011), 437?454. MR2869299, Zbl 1252.11031.

[CZ13a] Corvaja, P.; Zannier, U. Algebraic hyperbolicity of ramified covers of $\mathbb{G}_m^2$ (and integral points on affine subsets of $\mathbb{P}^2$), *J. Differential Geom.* **93** (2013), 355-?77. MR3024299.

[CZ13b] Corvaja, P.; Zannier, U. Greatest common divisors of $u-1$, $v-1$ in positive characteristic and rational points on curves over finite fields, *J. Eur. Math. Soc. (JEMS)* **15** (2013), no. 5, 1927–1942. MR3082249, Zbl 1325.11060.

[deJ96] de Jong, A. J. Smoothness, semi-stability and alterations, *Inst. Hautes Études Sci. Publ. Math.* **83** (1996), 51–93. MR1423020 (98e:14011), Zbl 0916.14005.

[Ghi09] Ghioca, D. Points of small height on varieties defined over a function field, *Canad. Math. Bull.* **52** (2009), no. 2, 237–244. MR2512312 (2010e:11061), Zbl 1196.11092.

[Ghi14] Ghioca, D. A Bogomolov type statement for function fields, *Bull. Inst. Math. Acad. Sin. (N.S.)* **9** (2014), no. 4, 641–656. MR3309945, Zbl 1320.11059.

[GMZ15] Ghioca, D.; Masser, D.; Zannier, U. Bounded height conjecture for function fields, New York J. Math. **21** (2015), 837–846. MR3425624, Zbl 06498841.

[HT] Hsia, L.-C.; Tucker, T. J. A variant in characteristic p of a theorem of Ailon-Rudnick, preprint, https://arxiv.org/abs/1611.04115.

[Lan83] Lang, S. Fundamentals of Diophantine geometry, *Springer-Verlag*, New York, 1983, xviii+370 pp. MR0715605 (85j:11005).

[Luc05] Luca, F. On the greatest common divisor of $u-1$ and $v-1$ with u and v near S-units, *Monatsh. Math.* **146** (2005), no. 3, 239–256. MR2184226 (2006f:11079), Zbl 1107.11029.

[Mas14] Masser, D. Unlikely intersections for curves in multiplicative groups over positive characteristic, *Q. J. Math.* **65** (2014), no. 2, 505?515. MR3230373, Zbl 1317.11067.

[Ost16] Ostafe, A. On some extensions of the Ailon-Rudnick theorem, *Monatsh. Math.* **181** (2016), no. 2, 451–471. MR3539944, Zbl 06641474.

[PS95] Pappalardi, F.; Shparlinski, I. On Artin's conjecture over function fields, *Finite Fields Appl.* **1** (1995), no. 4, 399-404. MR1353988 (97g:11132).

[Sil04a] Silverman, J. H. Common divisors of $a^n - 1$ and $b^n - 1$ over function fields, *New York J. Math.* **10** (2004), 37–43. MR2052363, Zbl 1120.11045.

[Sil04b] Silverman, J. H. Common divisors of elliptic divisibility sequences over function fields, *Manuscripta Math.* **114** (2004), no. 4, 431–446. MR2081943 (2005d:11096), Zbl 1128.11015.

[Zan12] Zannier, U. Some problems of unlikely intersections in arithmetic and geometry. With appendixes by David Masser. *Annals of Math. Studies* **181**, Princeton, NJ, 2012, xiv+160 pp. MR2918151, Zbl 1246.14003.

Dragos Ghioca, Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
dghioca@math.ubc.ca

Liang-Chung Hsia, Department of Mathematics, National Taiwan Normal University, Taipei, Taiwan, ROC
hsia@math.ntnu.edu.tw

Thomas J. Tucker, Department of Mathematics, University of Rochester, Rochester, NY 14627, USA
ttucker@math.rochester.edu