ORDER OF TORSION FOR REDUCTION OF LINEARLY INDEPENDENT POINTS FOR A FAMILY OF DRINFELD MODULES

DRAGOS GHIOCA AND IGOR E. SHPARLINSKI

ABSTRACT. Let q be a power of the prime number p, let $K = \mathbb{F}_q(t)$, and let $r \geqslant 2$ be an integer. For points $\mathbf{a}, \mathbf{b} \in K$ which are $\mathbb{F}_q$-linearly independent, we show that there exist positive constants N_0 and c_0 such that for each integer $\ell \geqslant N_0$ and for each generator τ of $\mathbb{F}_{q^\ell}/\mathbb{F}_q$, we have that for all except N_0 values $\lambda \in \overline{\mathbb{F}_q}$, the corresponding specializations $\mathbf{a}(\tau)$ and $\mathbf{b}(\tau)$ cannot have orders of degrees less than $c_0 \log \log \ell$ as torsion points for the Drinfeld module $\Phi^{(\tau,\lambda)} : \mathbb{F}_q[T] \longrightarrow \mathrm{End}_{\overline{\mathbb{F}_q}}(\mathbb{G}_a)$ (where $\mathbb{G}_a$ is the additive group scheme), given by $\Phi_T^{(\tau,\lambda)}(x) = \tau x + \lambda x^q + x^{q^r}$.

1. INTRODUCTION

1.1. **Notation.** Let q a power of a prime number p. Consequently, we denote by $\mathbb{F}_q$ the finite field with q elements and also, let $\overline{\mathbb{F}_q}$ be its algebraic closure. We let $K = \mathbb{F}_q(t)$ be the rational function field of transcendence degre 1 over $\mathbb{F}_q$. Then each $\mathbf{a} \in K$ can be written as a quotient $P(t)/Q(t)$ for relatively prime polynomials $P, Q \in \mathbb{F}_q[t]$ (with $Q \neq 0$); so, for all but finitely many $\tau \in \overline{\mathbb{F}_q}$ (as long as $Q(\tau) \neq 0$), the specialization map $t \mapsto \tau$ yields a specialization $\mathbf{a} \mapsto \mathbf{a}(\tau) \in \overline{\mathbb{F}_q}$. Furthermore, for any polynomial $f \in K[x]$, then for all but finitely many $\tau \in \overline{\mathbb{F}_q}$ the specialization $t \mapsto \tau$ is well-defined for each coefficient of $f(x)$; in this case, we denote by $f(\tau; x) \in \overline{\mathbb{F}_q}[x]$ the corresponding specialization of $f(x)$.

An ($\mathbb{F}_q[T]$-)Drinfeld module Φ defined over any field L containing $\mathbb{F}_q$ is given by a non-linear action of $\mathbb{F}_q[T]$ on the additive group scheme $\mathbb{G}_a$, that is, it is an endomorphism $\Phi : \mathbb{F}_q[T] \longrightarrow \mathrm{End}_L(\mathbb{G}_a)$ where not all of the maps $\Phi_{P(T)} := \Phi(P(T))$ are linear. In particular, each such Drinfeld module is uniquely defined by an *additive polynomial* (of degree larger than 1) with coefficients in L corresponding to Φ_T. We recall thar a polynomial $f(x)$ is called *additive* if $f(x + y) = f(x) + f(y)$ for all x and y. These are linear polynomials in characteristic zero and polynomials with monomial terms of degrees which are powers of p in positive characteristic p. A point $\mathbf{c} \in \overline{L}$ is a torsion point for Φ if there exists a nonzero polynomial $P(T) \in \mathbb{F}_q[T]$ such

that $\Phi_{P(T)}(\mathbf{c}) = 0$; the *monic* polynomial $P(T)$ of minimal degree for which $\Phi_{P(T)}(\mathbf{c}) = 0$ is called the *order* of $\mathbf{c}$. For more details on Drinfeld modules, we refer the reader to [Gos96].

1.2. **Unlikely intersections.** Inspired by the classical unlikely intersection problems in arithmetic geometry (for example, see [Hab09] and the references therein), Masser and Zannier [MZ10, MZ12] have proved a remarkable result: there exist finitely many $\lambda \in \mathbb{C}$ such that both the points $\left(2, \sqrt{2(2 - \lambda)}\right)$ and $\left(3, \sqrt{6(3 - \lambda)}\right)$ are torsion on the corresponding elliptic curve E_λ from the Legendre family given by the equation $y^2 = x(x-1)(x-\lambda)$. The results from [MZ10,MZ12] have been the starting point of a very intense research campaign in arithmetic dynamics, which emulates the classical unlikely intersection problems from arithmetic geometry, but this time, the unlikely intersection taking place in an algebraic dynamics setting (for example, see [BD11,GHT13,GKN17]). In this spirit, the first author and Hsia have proved in [GH13, Theorem 1.5] the following result.

Theorem A. *Let $r > 1$ be an integer, let q be a power of the prime number p, and let $K = \mathbb{F}_q(t)$. We consider the family of Drinfeld modules $\Phi^{(z)}$ (parametrized by $z \in \overline{K}$) such that*

$$\Phi_T^{(z)}(x) = tx + zx^q + x^{q^r}.$$

Let $\mathbf{a}, \mathbf{b} \in K$. Then there exist infinitely many $z \in \overline{K}$ such that both $\mathbf{a}$ and $\mathbf{b}$ are torsion points for the Drinfeld module $\Phi^{(z)}$ if and only if $\mathbf{a}$ and $\mathbf{b}$ are $\mathbb{F}_q$-linearly dependent.

Remark 1.1. In [GH13, Theorem 1.5], the above conclusion in Theorem A has been stated under the assumption that there exist infinitely many λ in the separable closure K^{sep} of K. On the other hand, we observe that the main technical ingredient used in the proof of [GH13, Theorem 1.5] comes from the equidistribution theorem of Baker and Rumely [BR10, Theorem 7.52], which is stated for product formula fields. So, in [GH13, Theorem 2.6] (which provides the key step in proving [GH13, Theorem 1.5]), one could work instead with the perfect closure $K^{\mathrm{per}} := \mathbb{F}_q\left(t^{1/p^n} : n \geqslant 1\right)$, which is a product formula field since each valuation on K has a unique extension to K^{per} and thus, the hypotheses (1)-(4) from [BR10, Definition 7.51, p. 185] are met for K^{per}. Then since $(K^{\mathrm{per}})^{\mathrm{sep}} = \overline{K}$, one obtains our Theorem A with an identical proof as in [GH13, Theorem 1.5].

Remark 1.2. We also note that if $\mathbf{b} = \zeta \cdot \mathbf{a}$ for some $\zeta \in \mathbb{F}_q$, then $\Phi_{P(T)}^{(z)}(\mathbf{b}) = \zeta \cdot \Phi_{P(T)}^{(z)}(\mathbf{a})$ for *each* $z \in \overline{K}$; therefore, we have that $\mathbf{a}$ is torsion for $\Phi^{(z)}$ if and only if $\mathbf{b}$ is torsion for $\Phi^{(z)}$, and moreover, they both have the same order as torsion points for $\Phi^{(z)}$.

One of the unlikely intersection results inspired by [MZ10, MZ12] is the result of Habegger [Hab13] that there exist finitely many pairs $(a, b) \in \mathbb{C}^2$

with the property that *each* of the three points

(1.1) $\left(1, \sqrt{1+a+b}\right), \quad \left(2, \sqrt{8+2a+b}\right), \quad \left(3, \sqrt{27+3a+b}\right)$

are torsion points for the elliptic curve $y^2 = x^3 + ax + b$. This motivated the second author to prove the following result (see [Shp20, Theorem 1.1]).

Theorem B. *There is an absolute constant M_0 such that for all primes p and for all but at most M_0 pairs $(a, b) \in \overline{\mathbb{F}_p}^2$ with $4a^3 + 27b^2 \neq 0$ at least one of the points from (1.1) is of order at least $(\log p)^{1/33+o(1)}$.*

Theorem B is proven in [Shp20] by employing both the result of Habegger [Hab13], but also using in an essential way [D'AOSS19, Theorem 2.1] which provides a way to control the number of solutions to polynomial equations when they are reduced modulo primes.

1.3. **Our results.** Here we prove the following result which is a counterpart for Drinfeld modules of Theorem B (also, note that as observed in [Gos96, Chapter 3], the family of Drinfeld modules $\Phi^{(z)}$ which plays the counterpart role of elliptic curves is the one for which $\Phi_T^{(z)}(x) = tx + zx^q + x^{q^2}$, as we vary z in $\overline{K}$).

In order to state our result, we define for each $\tau \in \overline{\mathbb{F}_q}$ its degree (over $\mathbb{F}_q$) as $\deg \tau := [\mathbb{F}_q(\tau) : \mathbb{F}_q]$.

Theorem 1.3. *Let $r \geqslant 2$ be an integer, let q be a power of the prime p, and let $K = \mathbb{F}_q(t)$. We let $\mathbf{a}, \mathbf{b} \in K$ be two $\mathbb{F}_q$-linearly independent points. Then there exist positive constants N_0 and c_0 (depending only on q, r and the degrees of $\mathbf{a}$ and $\mathbf{b}$) such that for each $\ell \geqslant N_0$ and for each $\tau \in \overline{\mathbb{F}_q}$ such that $\deg \tau = \ell$, we have that for all except N_0 values of $\lambda \in \overline{\mathbb{F}_q}$, at least one of the two points $\mathbf{a}(\tau)$ or $\mathbf{b}(\tau)$ is a torsion point whose order has degree at least $c_0 \log \log(\ell)$ for the Drinfeld module $\Phi^{(\tau, \lambda)} \in \mathrm{End}_{\overline{\mathbb{F}_q}}(\mathbb{G}_a)$ given by $\Phi_T^{(\tau, \lambda)}(x) := \tau x + \lambda x^q + x^{q^r}$.*

Remark 1.4. In Theorem 1.3, the family of Drinfeld modules $\Phi^{(\tau, \lambda)}$ given by $\Phi_T^{(\tau, \lambda)}(x) := \tau x + \lambda x^q + x^{q^r}$ varies with respect to both parameters τ and λ in $\overline{\mathbb{F}_q}$. Note that for any given $\tau \in \overline{\mathbb{F}_q}$, one could easily find $\lambda \in \overline{\mathbb{F}_q}$ such that $\mathbf{a}(\tau)$ is killed by Φ_T, say, and therefore $\mathbf{a}(\tau)$ could be a torsion point of order of a very small degree for the Drinfeld module $\Phi^{(\tau, \lambda)}$; but then the conclusion of our Theorem 1.3 yields that $\mathbf{b}(\tau)$ cannot be a torsion point whose order has also very small degee compared to $[\mathbb{F}_q(\tau) : \mathbb{F}_q]$. Again, just like it has been observed in Remark 1.2, the fact that $\mathbf{a}$ and $\mathbf{b}$ are $\mathbb{F}_q$-linearly independent is paramount since otherwise, if $\mathbf{b}/\mathbf{a} \in \mathbb{F}_q^*$ (for example) then for any suitable specialization $t \mapsto \tau$, we would have that also $\mathbf{a}(\tau)$ and $\mathbf{b}(\tau)$ are $\mathbb{F}_q$-linearly dependent and therefore, they are torsion points for any Drinfeld module $\Phi^{(\tau, \lambda)}$ of the same order (which thus could be very small relative to $[\mathbb{F}_q(\tau) : \mathbb{F}_q]$).

Remark 1.5. The fact that in the conclusion of our Theorem 1.3 we ask that $\ell \geqslant N_0$ is merely for guaranteeing that the specialization $\mathbf{a} \mapsto \mathbf{a}(\tau)$ (resp. $\mathbf{b} \mapsto \mathbf{b}(\tau)$) is well-defined for each generator τ for the extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$ (note that there are only finitely many $\tau \in \overline{\mathbb{F}_q}$ for which the above specializations do not make sense).

Remark 1.6. The extra logarithm appearing in $c_0 \log \log \ell$ from the conclusion of our Theorem 1.3 comes form the fact that we insist that for *each* specialization $t \mapsto \tau$ where τ *generates* the extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$ our desired conclusion regarding the orders of the torsion points $\mathbf{a}(\tau)$ and $\mathbf{b}(\tau)$ must hold. Our proof could be easily modified to show that there exists *some* τ generating the extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$ with the property that the specialization $t \mapsto \tau$ yields that at least one of $\mathbf{a}(\tau)$ or $\mathbf{b}(\tau)$ would be a torsion point for $\Phi^{(\tau,\lambda)}$ (for each $\lambda \in \overline{\mathbb{F}_q}$ apart from some N_0 values λ) whose order has degree at least $c_1 \log(\ell)$ (for some positive constant c_1 depending only on q, r and the degrees of $\mathbf{a}$ and $\mathbf{b}$).

We also note that our Theorem 1.3 (similar to Theorem B of [Shp20]) fits into a more general program of obtaining results for specialization over finite fields for certain global results stemming from arithmetic dynamics (see also [AG09, BCMOS20, Cha13, CKSZ14, D'AOSS19, KMS21, Mel21, Shp18]). Also, strictly in the context of Drinfeld modules, there has been interest in the past for considering Drinfeld modules defined over finite fields, either for studying some of their intrinsic arithmetic properties (as in [Ghi08]), or for infering aritmetic properties of Drinfeld modules of generic characteristic after considering their reductions at various places (see [GT08, Hsi08]). Furthermore, our results provide additional evidence that Drinfeld modules are the right vehicle in positive characteristic for formulating questions which are analogue to classical arithmetic problems in the context of abelian varieties (see [Bre12, Ghi05, Sca02] for results in the context of Drinfeld modules, which are analogues of the classical André-Oort, Mordell-Lang, respectvely Manin-Mumford conjectures).

We also note that [AG09, Theorem 5.2] provides a somewhat related result to our Theorem 1.3; however, there are some significant differences between that result and ours. The result from [AG09, Theorem 5.2] refers to reductions at various places of a *given* Drinfeld module, while in our result we vary both the specialization $t \mapsto \tau$ but also vary λ in $\overline{\mathbb{F}_q}$; in other words, $\left\{ \Phi^{(\tau,\lambda)} \right\}$ is a two-dimensional family of Drinfeld modules defined over $\overline{\mathbb{F}_q}$. Finally, we refer to our Section 4 for a discussion regarding further research in the direction set by our paper.

We sketch briefly the plan for our paper. The approach to our Theorem 1.3 follows the general direction set in [Shp20] for the case of elliptic curves. So, we need to establish a technical result (which is our Lemma 2.4) regarding the preservation of the number of zeros in specializations of polynomials over a function field. Then using also a couple of technical results (see Lemmas 2.7 and 2.5) regarding the growth of heights and of degrees

of the iterates of a given point under polynomials in a family of Drinfeld modules, we obtain the desired technical ingredients for finishing the proof of our Theorem 1.3, which is completed Section 3. We conclude with a discussion in Section 4 of further research in the direction opened up by our article.

2. Preliminary results

2.1. **Greatest common divisors of polynomials.** We recall that a greatest common divisor of polynomials $f_1, \ldots, f_s \in \mathbb{L}[x]$ over a field $\mathbb{L}$ is any polynomial $d \in \mathbb{L}[x]$ such that any other common divisor e of $f_1, \ldots, f_s$ divides d (clearly d is defined up to a nonzero scalar multiple). In particular, we can define the degree $\deg \gcd(f_1, \ldots, f_s)$, which does not depend on a particular choice of a greatest common divisor.

We need the following special case of [vzGKS97, Lemma 4.8].

Lemma 2.1. *Let $\mathbb{L}$ be a field and let $f_1, \ldots, f_s \in \mathbb{L}[x]$ be $s \geqslant 2$ polynomials of degree at most D. For any finite set $\mathcal{A} \subseteq \mathbb{L}$, uniformly chosen random elements $\alpha_3, \ldots, \alpha_s \in \mathcal{A}$ and*

$$f_0 = f_2 + \sum_{3 \leqslant i \leqslant s} \alpha_i f_i \in \mathbb{L}[x].$$

we have

$$\mathrm{Prob}_{\alpha_3, \ldots, \alpha_s \in \mathcal{A}} \left[\deg \gcd(f_1, \ldots, f_s) = \deg \gcd(f_0, f_1) \right] \geq 1 - D/\#\mathcal{A}.$$

We can now estimate the degree of the coefficients in the Bézout identity for relatively prime polynomials.

Lemma 2.2. *Let $\mathbb{L}$ be a field and let $f_1, \ldots, f_s \in \mathbb{L}[x]$ be $s \geqslant 2$ relatively prime polynomials of degree at most D. There are polynomials $b_1, \ldots, b_s \in \mathbb{L}[x]$ of degree less than D such that*

$$(2.1) \qquad\qquad b_1 f_1 + \ldots + b_s f_s = 1.$$

Proof. Taking the algebraic closure $\overline{\mathbb{L}}$ of $\mathbb{L}$ (which is not necessary if $\mathbb{L}$ is infinite, or even finite but satisfying $\#\mathbb{L} > D$), we see from Lemma 2.1 that there are some $\alpha_3, \ldots, \alpha_s \in \overline{\mathbb{L}}$ such that f_1 and f_0, defined as in Lemma 2.1 are relatively prime. Note that $\deg f_0 \leqslant D$ and hence using the standard Euclidean algorithm we see that there are $b_0, b_1 \in \overline{\mathbb{L}}[x]$ of degrees at most $D - 1$ such that

$$b_0 f_0 + b_1 f_1 = 1$$

and we obtain (2.1) with $b_1, b_2 = b_0, b_3 = \alpha_3 b_0, \ldots, b_s = \alpha_s b_0 \in \overline{\mathbb{L}}[x]$.

We now observe that (2.1) defines a system of linear equations for Ds coefficients of polynomials $b_1, \ldots, b_s$. The above argument shows that that system is compatible over $\overline{\mathbb{L}}$, and since the coefficients of this system are defined over $\mathbb{L}$, then this means that the system is compatible over $\mathbb{L}$ as well. Hence we can find polynomials $b_1, \ldots, b_s \in \mathbb{L}[x]$ satisfying (2.1). $\qquad\square$

2.2. Preserving number of common zeros in specializations of polynomials over a function field.

Definition 2.3. *For a polynomial $f \in \mathbb{F}_q[t][x]$, we define its height $\mathfrak{h}(f)$ as the maximum degree of the coefficients of f, which are themselves polynomials in $\mathbb{F}_q[t]$. (Note that for any element in $\mathbb{F}_q(t)$, its Weil height is simply its degree as a rational function.)*

One of our main tools is the following result. Note that in our proof of Theorem 1.3, we only employ Lemma 2.4 for two polynomials (that is, $s = 2$ with the notation as in Lemma 2.4); however, we include this more general version of Lemma 2.4 which may be useful beyond our current application. For further generalisations see Section 4.

Lemma 2.4. *Let $f_1, \ldots, f_s \in \mathbb{F}_q[t][x]$ be polynomials of degrees at most D and of heights at most H. Assume that there exist at most N_0 common zeros in $\overline{\mathbb{F}_q(t)}$ of the polynomials $f_1(x), \ldots, f_s(x)$. Then there exists a nonzero polynomial $\mathcal{T} \in \mathbb{F}_q[T]$ of degree at most $2DH$ with the property that for each $\tau \in \overline{\mathbb{F}_q}$ such that $\mathcal{T}(\tau) \neq 0$, for the specialization polynomials $f_i(x) \mapsto f_i(\tau; x)$, $i = 1, \ldots, s$, corresponding to the specialization $t \mapsto \tau$, we have that the polynomials*

$$f_1(\tau; x), \ldots, f_s(\tau; x) \in \overline{\mathbb{F}_q}[x]$$

have at most N_0 common zeros in $\overline{\mathbb{F}_q}$.

Proof. Let $h \in \mathbb{F}_q[t][x]$ be the greatest primitive common divisor of $f_1, \ldots, f_s$, that is, the coefficients of h are relatively prime as polynomials in t. We first claim that considering $f_1, \ldots, f_s, h$ as bivariate polynomials in $\mathbb{F}_q[t, x]$ we still have the divisibility $h \mid f_i$, $i = 1, \ldots, s$ (this is a consequence of Gauss' Lemma, as pointed out by the referee, whom we thank once again for their useful comments and suggestions). Indeed, we know that h divides f_i, $i = 1, \ldots, s$, in the ring $\mathbb{F}_q(t)[x]$ and so there are $g_i \in \mathbb{F}_q[t][x]$ and $b \in \mathbb{F}_q[t]$ such that b is relatively prime to $g_1, \ldots, g_s$ as polynomials in $\mathbb{F}_q[t, x]$ and

$$f_i = (g_i/b) \cdot h$$

that is

$$b f_i = h g_i$$

Since h is primitive and $\mathbb{F}_q[t, x]$ is a unique factorisation domain, we deduce that $b \in \mathbb{F}_q$.

Hence for $g_i := f_i/h$ we have $g_i \in \mathbb{F}_q[t][x]$, $i = 1, \ldots, s$. Furthermore, we see that $g_1, \ldots, g_s$ have no common zeros in $\overline{\mathbb{F}_q(t)}$ and hence by Lemma 2.2 there are for some $b_1, \ldots, b_s \in \mathbb{F}_q(t)[x]$ of degree at most $D - 1$ such that

$$(2.2) \qquad\qquad b_1 g_1 + \ldots + b_s g_s = 1.$$

We now see that (2.2) can be rewritten as a system of at most $2D$ linear equations over $\mathbb{F}_q(t)$ in Ds variables. Choosing that largest nonsingular submatrix of the matrix defining this system, from the Cramer rule we see

that (2.2) has a solution in $b_i = c_i/\Delta$ where $c_i \in \mathbb{F}_q[t][x]$, $i = 1, \ldots, s$ and $\Delta \in \mathbb{F}_q[t]$ is a polynomial of degree (in t)

$$\deg \Delta \leqslant 2DH.$$

We now write (2.2) as $c_1 g_1 + \ldots + c_s g_s = \Delta$ or

(2.3) $$c_1 f_1 + \ldots + c_s f_s = \Delta h.$$

Therefore, for any $\tau \in \overline{\mathbb{F}_q}$ which is not a root of $\Delta(t)$ we derive from (2.3) that

$$c_1(\tau; x) f_1(\tau; x) + \ldots + c_s(\tau; x) f_s(\tau; x) = \Delta(\tau) h(\tau; x).$$

By our assumption, $h(x)$ has at most N_0 roots in $\overline{\mathbb{F}_q(t)}$; hence, unless $h(\tau; x)$ is identically equal to zero, then it must have at most N_0 roots in $\overline{\mathbb{F}_q}$. On the other hand, we know that $h(\tau; x)$ is never identically equal to 0 since h is a primitive polynomial and therefore, its coefficients (as polynomials in $\mathbb{F}_q[t]$) never vanish simultaneously at the point $\tau \in \overline{\mathbb{F}_q}$. Hence, letting $\mathcal{T}(t) := \Delta(t)$, we obtain a nonzero polynomial in $\mathbb{F}_q[t]$ of degree at most $2DH$ which satisfies the desired conclusion from Lemma 2.4. $\qquad\square$

2.3. **Technical background on Drinfeld modules.** In this Section we derive some basic results regarding the growth of the heights of the polynomials in a family of Drinfeld modules; for more results regarding heights for Drinfeld modules, we refer the reader to [Den92, Ghi07, GH13, GT08].

Let $r \geqslant 2$ be an integer, and let $K := \mathbb{F}_q(t)$. We consider the family of Drinfeld modules $\Phi^{(z)} : \mathbb{F}_q[T] \longrightarrow \mathrm{End}_{K(z)}(\mathbb{G}_a)$ given by $\Phi_T^{(z)}(x) := tx + zx^q + x^{q^r}$ parametrized by $z \in \overline{K}$.

Let $\mathbf{a} \in K$ be a nonzero point; we write $\mathbf{a} = \mathbf{a}_1/\mathbf{a}_2$ with (nonzero) relatively prime polynomials $\mathbf{a}_1, \mathbf{a}_2 \in \mathbb{F}_q[t]$. Let $D := \deg \mathbf{a}$ (or equivalently, D is the height of $\mathbf{a}$, as defined in [Ghi07]), that is, $D := \max\{\deg_t \mathbf{a}_1, \deg_t \mathbf{a}_2\}$. Then for each positive integer n, we have that $\Phi_{T^n}^{(z)}(\mathbf{a})$ is a polynomial in $K[z]$; for more details, see [GH13, Section 4].

More precisely, let

$$f_n(z) := \Phi_{T^n}^{(z)}(\mathbf{a}),$$

then as proven in [GH13, Lemma 4.2], we have that $\deg_z f_n(z) = q^{r(n-1)}$ (since $f_1(z) = \mathbf{a}^q \cdot z + t\mathbf{a} + \mathbf{a}^{q^r}$ is a linear polynomial in z). Also, the leading coefficient of $f_n(z)$ is $\mathbf{a}^{q^{1+r(n-1)}}$. Furthermore, for each $P(T) \in \mathbb{F}_q[T]$, we may consider the polynomial in z given by $z \mapsto \Phi_{P(T)}^{(z)}(\mathbf{a})$, which is a polynomial with coefficients in K. In particular, we have the following immediate corollary of [GH13, Lemma 4.2].

Lemma 2.5. *Let $0 \neq \mathbf{a} \in K$ and let $P(T) \in \mathbb{F}_q[T]$ be a non-constant polynomial. Then the map $z \mapsto \Phi_{P(T)}^{(z)}(\mathbf{a})$ is a polynomial in $K[z]$ of degree $q^{r(\deg T - 1)}$.*

In our proof of Theorem 1.3 we also need the following result, which gives us control on the heights of the coefficients of $f_n(z)$.

Lemma 2.6. *Let $\mathbf{a} := \mathbf{a}_1/\mathbf{a}_2 \in K = \mathbb{F}_q(t)$, where $\mathbf{a}_1$ and $\mathbf{a}_2$ are nonzero coprime polynomials in $\mathbb{F}_q[t]$. As before, we let $f_n(z) := \Phi_{T^n}^{(z)}(\mathbf{a}) \in K[z]$ for each positive integer n. Then $g_n(z) := \mathbf{a}_2^{q^{rn}} \cdot f_n(z) \in \mathbb{F}_q[t][z]$ and moreover,*

$$\mathfrak{h}(g_n) \leqslant (2 + \deg \mathbf{a})^{q^{rn}}.$$

Proof. We have that $f_1(z) = \mathbf{a}^q z + t\mathbf{a} + \mathbf{a}^{q^r}$ and so,

$$g_1(z) = \mathbf{a}_2^{q^r} \cdot f_1(z) = \mathbf{a}_1^q \mathbf{a}_2^{q^r - q} z + t\mathbf{a}_1 \mathbf{a}_2^{q^r - 1} + \mathbf{a}_1^{q^r} \in \mathbb{F}_q[t][z];$$

furthermore, $\mathfrak{h}(g_1) \leqslant 1 + (\deg \mathbf{a})^{q^r} < (2 + \deg \mathbf{a})^{q^r}$. Also, we have that for each positive integer n,

$$f_{n+1}(z) = f_n(z)^{q^r} + z f_n(z)^q + t f_n(z)$$

and so,

$$(2.4) \quad \begin{aligned} g_{n+1}(z) &= \mathbf{a}_2^{q^{r(n+1)}} f_{n+1}(z) \\ &= g_n(z)^{q^r} + \mathbf{a}_2^{q^{r(n+1)} - q^{1+rn}} z g_n(z)^q + t \mathbf{a}_2^{q^{r(n+1)} - q^{rn}} g_n(z). \end{aligned}$$

Therefore, an easy induction yields that $g_n(z) \in \mathbb{F}_q[t][z]$ and furthermore, $\mathfrak{h}(g_n(z)) \leqslant (2 + \deg \mathbf{a})^{rn}$ for all $n \in \mathbb{N}$; note that since $\deg \mathbf{a}_2 \leqslant \deg \mathbf{a}$, then the contribution to the height of $g_{n+1}(z)$ of the last term in (2.4) is at most equal to

$$1 + (\deg \mathbf{a})^{q^{r(n+1)} - q^{rn}} \cdot (2 + \deg \mathbf{a})^{q^{rn}} \leqslant (2 + \deg \mathbf{a})^{q^{r(n+1)}}.$$

This concludes our proof of Lemma 2.6. $\qquad\qquad\qquad\square$

Finally, the next result is an immediate consequence of Lemma 2.6.

Lemma 2.7. *Let $\mathbf{a} := \mathbf{a}_1/\mathbf{a}_2$ for some nonzero coprime polynomials $\mathbf{a}_1, \mathbf{a}_2 \in \mathbb{F}_q[t]$. Then for each non-constant polynomial $P(T) \in \mathbb{F}_q[T]$, the map*

$$z \mapsto \mathbf{a}_2^{q^{r \deg_T P(T))}} \cdot \Phi_{P(T)}^{(z)}(\mathbf{a})$$

is a polynomial in $\mathbb{F}_q[t][z]$ of height at most $(2 + \deg \mathbf{a})^{q^{r \deg_T P(T)}}$.

3. Proof of Theorem 1.3

3.1. **Bounds on degree and height of some polynomials.** So, we have $\mathbf{a}, \mathbf{b} \in K = \mathbb{F}_q(t)$ which are $\mathbb{F}_q$-linearly independent, and we write

$$\mathbf{a} := \frac{\mathbf{a}_1}{\mathbf{a}_2} \qquad \text{and} \qquad \mathbf{b} := \frac{\mathbf{b}_1}{\mathbf{b}_2}$$

with nonzero relatively prime polynomials $\mathbf{a}_1, \mathbf{a}_2 \in \mathbb{F}_q[t]$ (resp. $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{F}_q[t]$). Then $D := \max\{\deg \mathbf{a}, \deg \mathbf{b}\}$ is a positive integer since otherwise, we would have that both $\mathbf{a}$ and $\mathbf{b}$ are elements of $\mathbb{F}_q$ and thus, they would be $\mathbb{F}_q$-linearly dependent, contradicting our hypothesis.

According to Theorem A, there exist at most N_0 points $z \in \overline{K}$ such that both $\mathbf{a}$ and $\mathbf{b}$ are torsion points for the Drinfeld module $\Phi^{(z)} : \mathbb{F}_q[T] \longrightarrow \mathrm{End}_{K(z)}(\mathbb{G}_a)$ given by $\Phi_T^{(z)}(x) = tx + zx^q + x^{q^r}$. At the expense of replacing

N_0 by a larger positive integer, we may also assume that neither $\mathbf{a}_2$ nor $\mathbf{b}_2$ has a root τ generating an extension of $\mathbb{F}_q$ of degree at least equal to N_0.

Now, let $\ell \geqslant N_0$ and let τ be a generator for the finite fields extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$. Then we can specialize both $\mathbf{a}$ and $\mathbf{b}$ as $t \mapsto \tau$ (since $\mathbf{a}_2(\tau)$ and $\mathbf{b}_2(\tau)$ are both nonzero).

Let $\lambda_0 \in \overline{\mathbb{F}_q}$. Then both $\mathbf{a}(\tau)$ and $\mathbf{b}(\tau)$ are torsion points for the Drinfeld module $\Phi^{(\tau,\lambda_0)} : \mathbb{F}_q[T] \longrightarrow \operatorname{End}_{\overline{\mathbb{F}_q}}(\mathbb{G}_a)$ given by

$$\Phi_T^{(\tau,\lambda_0)}(x) = \tau x + \lambda_0 x^q + x^{q^r}$$

since each element in $\overline{\mathbb{F}_q}$ would be torsion for the Drinfeld module $\Phi^{(\tau,\lambda_0)}$ (which is itself defined over $\overline{\mathbb{F}_q}$). Now, assume their respective orders $P(T)$ and $Q(T)$ are both of degree at most M (in T) for some real number $M > 1$.

For each non-constant polynomial $R(T) \in \mathbb{F}_q[T]$, we let

$$g_{\mathbf{a},R(T)}(z) := \mathbf{a}_2^{q^{r \deg_T R}} \cdot \Phi_{R(T)}^{(z)}(\mathbf{a}),$$

$$g_{\mathbf{b},R(T)}(z) := \mathbf{b}_2^{q^{r \deg_T R}} \cdot \Phi_{R(T)}^{(z)}(\mathbf{b}).$$

Then

$$g_{\mathbf{a},R(T)}(z), g_{\mathbf{b},R(T)}(z) \in \mathbb{F}_q[t][z]$$

are polynomials of height at most $(2+D)^{q^{r \deg_T R}}$ (according to Lemma 2.7) and of degree $q^{r(\deg_T(R)-1)}$ (according to Lemma 2.5). Then let

$$\tilde{g}_{\mathbf{a},M}(z) := \prod_{\substack{1 \leqslant \deg_T R \leqslant M \\ R \text{ is monic}}} g_{\mathbf{a},R(T)}(z)$$

$$\tilde{g}_{\mathbf{b},M}(z) := \prod_{\substack{1 \leqslant \deg_T R \leqslant M \\ R \text{ is monic}}} g_{\mathbf{b},R(T)}(z).$$

The following two results are immediate consequences of Lemmas 2.5 and 2.7.

Lemma 3.1. *With the above notation, both $\tilde{g}_{\mathbf{a},M}(z)$ and $\tilde{g}_{\mathbf{b},M}(z)$ have degree less than $q^{(M+1)(r+1)}$.*

Proof. For each $s = 1, \ldots, M$, we have q^s monic polynomials $R(T) \in \mathbb{F}_q[T]$ of degree s. Since for each monic polynomial $R(T) \in \mathbb{F}_q[T]$ of degree s, we have $\deg_z g_{\mathbf{a},R(T)}(z) = q^{r(s-1)}$ (according to Lemma 2.5), then we obtain the desired conclusion from Lemma 3.1. $\square$

Lemma 3.2. *With the above notation, we have that $\mathfrak{h}(\tilde{g}_{\mathbf{a},M}), \mathfrak{h}(\tilde{g}_{\mathbf{b},M}) \leqslant c_2(2+D)^{q^{(r+1)(M+1)}}$ for some constant c_2 depending only on D, q and r.*

Proof. Again using that we have q^s monic polynomials of degree s in $\mathbb{F}_q[T]$ along with Lemma 2.7, we derive that both $\mathfrak{h}(\tilde{g}_{\mathbf{a},M}(z))$ and $\mathfrak{h}(\tilde{g}_{\mathbf{b},M}(z))$ are

bounded above by

$$\sum_{s=1}^{M} q^s \cdot (2+D)^{q^{rs}} \ll (2+D)^{q^{(r+1)(M+1)}},$$

where the implied constant depends only on D, q and r. This concludes our proof of Lemma 3.2. $\qquad\square$

3.2. **Concluding the proof.** As previously noted, due to Theorem A (because $\mathbf{a}$ and $\mathbf{b}$ are $\mathbb{F}_q$-inearly independent), we know that there exist at most N_0 solutions in $\overline{K}$ for the system:

$$\tilde{g}_{\mathbf{a},M}(z) = \tilde{g}_{\mathbf{b},M}(z) = 0.$$

Then, by Lemma 2.4 (see also Lemmas 3.2 and 3.1), we know that there exists a nonzero polynomial $\mathcal{T} \in \mathbb{F}_q[t]$ of degree at most

$$(3.1) \qquad 2q^{(M+1)(r+1)} \cdot c_2(2+D)^{q^{(M+1)(r+1)}} < c_3(5+2D)^{q^{(M+1)(r+1)}},$$

(for another constant c_3 depending only on D, q and r) such that for each $\tau \in \overline{\mathbb{F}_q}$ such that $\mathcal{T}(\tau) \neq 0$, then the specialization $t \mapsto \tau$ yields polynomials $\tilde{g}_{\mathbf{a},M}(\tau; x), \tilde{g}_{\mathbf{b},M}(\tau; x) \in \overline{\mathbb{F}_q}[x]$ which have at most N_0 common roots $\lambda \in \overline{\mathbb{F}_q}$. So, as long as τ generates a finite field extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$ of degree larger than $\deg \mathcal{T}$, then we are guaranteed that the system of equations

$$(3.2) \qquad\qquad \tilde{g}_{\mathbf{a},M}(\tau; \lambda) = \tilde{g}_{\mathbf{b},M}(\tau; \lambda) = 0$$

has at most N_0 solutions $\lambda \in \overline{\mathbb{F}_q}$. Hence, we may take $M := c_0 \log\log(\ell)$ for some absolute constant $c_0 > 0$, which depends only on q, r and $D = \max\{\deg \mathbf{a}, \deg \mathbf{b}\}$, so that ℓ is larger than the bound from (3.1). Therefore, in this case, for each $\lambda \in \overline{\mathbb{F}_q}$ other than the N_0 common solutions to the system (3.2), we obtain that not both $\mathbf{a}(\tau)$ and $\mathbf{b}(\tau)$ are torsion points under the action of $\Phi^{(\tau,\lambda)}$ of orders of degrees less than $M = c_0 \log\log \ell$. This concludes our proof of Theorem 1.3.

4. COMMENTS

In [GH13, Theorem 1.5], a slightly more general result has been proven than the stated Theorem A. More precisely, the same conclusion as in Theorem A holds if $\mathbf{a}$ and $\mathbf{b}$ are $\mathbb{F}_q$-linearly independent elements of $\overline{\mathbb{F}_q}(t)$. The exact same proof that we used for our Theorem 1.3 could be applied for $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{q^s}(t)$ (for some given $s \in \mathbb{N}$); the only difference is that in Theorem A we would need to replace $\mathbb{F}_q$ by $\mathbb{F}_{q^s}$ and $\mathbb{F}_{q^\ell}$ by $\mathbb{F}_{q^{s\ell}}$.

Furthermore, in [GH13, Theorem 1.4], a similar result as Theorem A is proven for the same family of Drinfeld modules but replacing $\mathbb{F}_q(t)$ with any function field K in which $\mathbb{F}_q$ is algebraically closed. Once again, a similar result as the one from Theorem 1.3 can be derived when starting with two $\mathbb{F}_q$-linearly independent points $\mathbf{a}, \mathbf{b} \in K$. Indeed, for all but finitely many specializations $t \mapsto \tau$ (where $\tau \in \overline{\mathbb{F}_q}$) we have well defined specializations $\mathbf{a} \mapsto \mathbf{a}(\tau)$ and $\mathbf{b} \mapsto \mathbf{b}(\tau)$ and the rest of the argument follows after

replacing the technical statements from Subsection 2.3 with similar results inferring heights (for more details regarding heights for Drinfeld modules, see [Ghi07]). Now, in order to extend the result of our Theorem 1.3 to arbitrary $\mathbb{F}_q$-linearly independent points in $\overline{\mathbb{F}_q(t)}$ (or more generally, to arbitrary one-dimensional families of Drinfeld modules), the same strategy from this paper applies as along as one would find a strengthening of [GH13, Theorems 1.4 and 1.5]; however, this last part seems very difficult at this moment since the conclusions in [GH13, Theorems 1.4 and 1.5] are obtained through some nontrivial arguments using valuation theory, which do not seem amenable to generalizations.

Finally, one could consider a higher-dimensional variant of our Theorem 1.3 by studying a family of Drinfeld modules parametrized by more than one variable. So, for example, letting once again $K := \mathbb{F}_q(t)$, a natural question would be to consider the 2-dimensional family of Drinfeld modules $\Psi^{(z_1,z_2)} : \mathbb{F}_q[T] \longrightarrow \mathrm{End}_{K(z_1,z_2)}(\mathbb{G}_a)$ given by

$$\Psi_T^{(z_1,z_2)}(x) := tx + z_1 x^q + z_2 x^{q^2} + x^{q^3}$$

along with three $\mathbb{F}_q$-linearly independent points $\mathbf{a}, \mathbf{b}, \mathbf{c} \in K$. Then the *expectation* is that there are only finitely many pairs of $(z_1, z_2) \in \overline{K}^2$ such that $\mathbf{a}, \mathbf{b}, \mathbf{c}$ are simultaneously torsion points for the corresponding Drinfeld module $\Psi^{(z_1,z_2)}$. Even though proving this expectation is beyond the known methods in arithmetic dynamics, once such a result would be established, then our current proof strategy would still apply verbatim to this more general setting using a suitable multi-variables generalization of Lemma 2.4 (note that Lemmas 2.5 and 2.7 easily extend to higher-dimensional families of Drinfeld modules).

There are two possible approaches to such generalizing Lemma 2.4 to the multivariate setting of polynomials $f_1, \ldots, f_s \in \mathbb{F}_q[t][\mathbf{x}]$ where $\mathbf{x} = (x_1, \ldots, x_n)$. The first approach, which is perhaps rather elaborate, is to follow the argument of [D'AOSS19] and establish an analogue of [D'AOSS19, Theorem 2.1], in the function field case. In this case one can use the machinery of heights in function fields, and for example, rely on the *effective Hilbert Nullstellensatz* given by [DKS13, Theorem 5] (rather than on its number field counterpart [DKS13, Theorem 5] as in [D'AOSS19]). The second way is a little simpler and shorter, but may lead to weaker results. For this we observe that if the system of equations

$$f_1(\mathbf{x}) = \ldots = f_s(\mathbf{x}) = 0$$

has at most N_0 solutions in $\mathbf{x} \in \overline{\mathbb{F}_q(t)}^n$, then the polynomial

$$F(\mathbf{x}_1, \ldots, \mathbf{x}_{N_0+1}) := \prod_{j=1}^{N_0} (x_{j,1} - x_{N_0+1,1})$$

vanishes identically on the variety

$$(4.1) \qquad f_1(\mathbf{x}_j) = \ldots = f_s(\mathbf{x}_j) = 0, \qquad j = 1, \ldots, N_0 + 1.$$

Hence the $s(N_0 + 1) + 1$ polynomials $f_i(\mathbf{x}_j)$, $i = 1, \ldots s$, $j = 1, \ldots, N_0 + 1$ and $1 - zF(\mathbf{x}_1, \ldots, \mathbf{x}_{N_0+1})$ in $n(N_0 + 1) + 1$ variables do not have common zeros. Now we are under the conditions of [DKS13, Theorem 5] which leads us to a multivariate analogue of the relation (2.2) and thus allows us to estimate the number of specialisations $t \mapsto \tau \in \overline{\mathbb{F}_q}$ for which the corresponding polynomials $f_1(\tau; \mathbf{x}), \ldots, f_s(\tau; \mathbf{x})$ have more that N_0 common zeros.

Acknowledgements

References

[AG09]   A. Akbary and D. Ghioca, *Periods of orbits modulo primes*, J. Number Theory, **129** (2009), 2831–2842. 4

[BD11]   M. Baker and L. DeMarco, *Preperiodic points and unlikely intersections*, Duke Math. J., **159** (2011), 1–29. 2

[BR10]   M. Baker and R. Rumely, *Potential theory and dynamics on the Berkovich projective line*, Math. Surveys Monogr. **159**, Amer. Math. Soc., Providence, RI, 2010. 2

[BCMOS20]   F. Barroero, L. Capuano, L. Mérai, A. Ostafe and M. Sha, *Multiplicative and linear dependence in finite fields and on elliptic curves modulo primes*, *Preprint*, 2020, (available from http://arxiv.org/abs/2008.00389). 4

[Bre12]   F. Breuer, *Special subvarieties of Drinfeld modular varieties*, J. Reine Angew. Math. **668** (2012), 35–57. 4

[Cha13]   M.-C. Chang, *Elements of large order in prime finite fields*, Bull. Aust. Math. Soc., **88** (2013), 169–176. 4

[CKSZ14]   M.-C. Chang, B. Kerr, I. E. Shparlinski, and U. Zannier, *Elements of large order on varieties over prime finite fields*, J. Théor. Nombres Bordeaux, **26** (2014), 579–594. 4

[DKS13]   C. D'Andrea, T. Krick and M. Sombra, *Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze*, Ann. Sci. Éc. Norm. Supér., **46** (2013), 549–627. 11, 12

[D'AOSS19] C. D'Andrea, A. Ostafe, I. E. Shparlinski, and M. Sombra, *Reductions modulo primes of systems of polynomial equations and algebraic dynamical systems*, Trans. Amer. Math. Soc., **371** (2019), 1169–1198. 3, 4, 11

[Den92]   L. Denis, *Hauteurs canoniques et modules de Drinfeld*, Math. Ann., **294** (1992), 213–223. 7

[vzGKS97]   J. von zur Gathen, M. Karpinski and I. E. Shparlinski, *Counting points on curves over finite fields*, Comp. Compl., **6** (1997), 64–99. 5

[Ghi05]   D. Ghioca, *The Mordell-Lang theorem for Drinfeld modules*, Int. Math. Res. Not. **2005** (2005), 3273–3307. 4

[Ghi07]   D. Ghioca, *The Lehmer inequality and the Mordell-Weil theorem for Drinfeld modules*, J. Number Theory, **122** (2007), 37–68. 7, 11

[Ghi08]   D. Ghioca, *The isotrivial case in the Mordell-Lang theorem*, Trans. Amer. Math. Soc., **360** (2008), 3839–3856. 4

[GH13] D. Ghioca and L.-C. Hsia, *Torsion points in families of Drinfeld modules*, Acta Arith., **161** (2013), 219–240. 2, 7, 10, 11

[GHT13] D. Ghioca, L.-C. Hsia, and T. J. Tucker, *Preperiodic points for families of polynomials*, Algebra Number Theory, **7** (2013), 701–732. 2

[GKN17] D. Ghioca, H. Krieger, and D. K. Nguyen, *The dynamical Andre-Oort conjecture: Unicritical polynomials*, Duke Math. J., **166** (2017), 1–25. 2

[GT08] D. Ghioca and T. J. Tucker, *Equidistribution and integral points for Drinfeld modules*, Trans. Amer. Math. Soc., **360** (2008), 4863–4887. 4, 7

[Gos96] D. Goss, *Basic Structure of Function field Arithmetic*, Springer-Verlag, Berlin, 1996. 2, 3

[Hab09] P. Habegger, *Intersecting subvarieties of abelian varieties with algebraic subgroups of complementary dimension*, Invent. Math., **176** (2009), 405–447. 2

[Hab13] P. Habegger, *Torsion points on elliptic curves in Weierstrass form*, Ann. Sc. Norm. Super. Pisa Cl. Sci.,**12** (2013), 687–715. 2, 3

[Hsi08] L.-C. Hsia, *On the reduction of a non-torsion point of a Drinfeld module*, J. Number Theory, **128** (2008), 1458–1484. 4

[KMS21] B. Kerr, J. Mello and I. E. Shparlinski, *On elements of large order of elliptic curves and multiplicative dependent images of rational functions over finite fields*, Illinois J. Math., (to appear). 4

[MZ10] D. Masser and U. Zannier, *Torsion anomalous points and families of elliptic curves*, Amer. J. Math., **132** (2010), 1677–1691. 2

[MZ12] D. Masser and U. Zannier, *Torsion points on families of squares of elliptic curves*, Math. Ann., **352** (2012), 453–484. 2

[Mel21] J. Mello, *On semigroup orbits of polynomials and multiplicative orders*, Bull. Aust. Math. Soc., (to appear). 4

[Sca02] T. Scanlon, *Diophantine geometry of the torsion of a Drinfeld module*, J. Number Theory **97** (2002), 10–25. 4

[Shp18] I. E. Shparlinski, *Multiplicative orders in orbits of polynomials over finite fields*, Glasgow Math. J., **60** (2018), 487–493. 4

[Shp20] I. E. Shparlinski, *Orders of points in families of elliptic curves*, Proc. Amer. Math. Soc., **148** (2020), 2371–2377. 3, 4

DRAGOS GHIOCA, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BC V6T 1Z2, CANADA

E-mail address: dghioca@math.ubc.ca

IGOR E. SHPARLINSKI, SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY NSW 2052, AUSTRALIA

E-mail address: igor.shparlinski@unsw.edu.au