HAL
open science

LOWER BOUNDS FOR THE CANONICAL HEIGHT ON DRINFELD MODULES

Vincent Bosser, Aurélien Galateau

To cite this version:

Vincent Bosser, Aurélien Galateau. LOWER BOUNDS FOR THE CANONICAL HEIGHT ON DRINFELD MODULES. International Mathematics Research Notices, 2019, 2019 (1), pp.165-200. 10.1093/imrn/rnx112 . hal-02151916

HAL Id: hal-02151916

https://normandie-univ.hal.science/hal-02151916v1

Submitted on 10 Jun 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

LOWER BOUNDS FOR THE CANONICAL HEIGHT ON DRINFELD MODULES

VINCENT BOSSER AND AURÉLIEN GALATEAU

Abstract. We use diophantine approximation to bound from below the canonical height on a Drinfeld module. We first give a positive answer to the Lehmer problem in the case of purely inseparable extensions on Drinfeld modules with at least one supersingular prime. We also revisit the CM case, where we improve the estimates already known, and we finally give a bound of polynomial strength in the general case.

1. Introduction

This article is devoted to the study of points with small canonical height on Drinfeld modules through diophantine approximation. This problem finds its origin in the number field setting and a famous question raised by Lehmer.

Small values of the Weil height on number fields. Let h be the (logarithmic, absolute) Weil height on $\bar{\mathbb{Q}}^*$. A classical theorem of Kronecker states that the zero locus of h is the group of roots of unity. Lehmer's problem amounts to finding an optimal lower bound for h when this function does not vanish. With time, it turned out to be stated as a conjecture (see [22], §13, p. 476 for the original version).

Conjecture 1.1 (Lehmer)**.** *If $x \in \bar{\mathbb{Q}}^*$ is not a root of unity:*

$$h(x) \gg \frac{1}{[\mathbb{Q}[x] : \mathbb{Q}]}.$$

The notation $\gg$ means that the inequality is true after possibly multiplying the right-hand side by a positive number. This problem has been solved in many instances, but it is still open in general. The best unconditional estimate so far is due to Dobrowolski ([11]).

Theorem 1.2 (Dobrowolski)**.** *For all $x \in \bar{\mathbb{Q}}^*$ of degree $D := [\mathbb{Q}(x) : \mathbb{Q}]$ not a root of unity:*

$$h(x) \gg \frac{1}{D}\left(\frac{\log\log(3D)}{\log(2D)}\right)^3.$$

This theorem has been extended in greater dimension by Amoroso and David ([1], or [3] for sharper estimates). There can also be an absolute lower bound for the height on some particular subfields of $\bar{\mathbb{Q}}$ (see [2] for the abelian closure $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$, [28] for the field $\mathbb{Q}^{\mathrm{tr}}$ of totally real numbers, or [18] for the field generated by torsion points of an elliptic curve defined over $\mathbb{Q}$).

The same questions arise if one considers the Néron-Tate height on an elliptic curve, or more generally an abelian variety (over a number field). The equivalent of Dobrowolski's estimate is known to hold for CM abelian varieties (see [21] on elliptic

curves or [6] in greater dimension). For arbitrary abelian varieties, an estimate of polynomial strength has been proved by Masser ([23] or [24]).

The canonical height on Drinfeld modules. We can also consider the analogous problems on Drinfeld modules. Let A be the ring of polynomials on a finite field $\mathbb{F}_q$, k its fraction field and $\bar{k}$ an algebraic closure of k. Let ϕ be an A-Drinfeld module of rank $r \geq 1$ over $\bar{k}$. We denote by $h(\phi)$ the height of ϕ, and by D_ϕ the degree of the field of definition of ϕ. There is a Weil height h on $\bar{k}$, and a canonical height $\hat{h}_\phi$ constructed out of h by a limit process.

Now, it is easy to see that the Lehmer conjecture is true for the Weil height, but it is still open for $\hat{h}_\phi$. Denis proved a Dobrowolski-type estimate for separable extensions in the Carlitz case ([9]).

Theorem 1.3 (Denis)**.** *Let ϕ be the Carlitz module. For all $x \in \bar{k}$ not torsion for ϕ such that $k(x)/k$ is separable of degree D:*

$$\hat{h}_\phi(x) \gg_{\mathcal{C}} \frac{1}{D}\left(\frac{\log\log(3D)}{\log(2D)}\right)^3.$$

The notation $\gg_\phi$ means that the inequality is true after possibly multiplying the right-hand side by a positive number that depends on ϕ. This result was extended to a wider class of Drinfeld modules (including many CM modules) by Demangos, who also tackled inseparable extensions ([8]).

Theorem 1.4 (Demangos)**.** *Suppose that there is a positive density of supersingular primes for ϕ. Then for all $x \in \bar{k}$ not torsion of degree D and inseparable degree D_{i}:*

$$\hat{h}_\phi(x) \gg_\phi \frac{1}{D}\left(\frac{\log\log(3D)}{D_{\mathrm{i}}\log(2D)}\right)^{3rD_\phi h(\phi)+1}.$$

Ghioca proved an unconditional lower bound for the canonical height of a non torsion $x \in \bar{k}$, which is exponential in the number of places of $K(x)$ with bad reduction (see [15], Theorem 4.5). He also found a conditional polynomial lower bound ([16], Theorem 1.4); his assumption concerns the local height $\hat{h}_{\phi,v}$ associated to a place v not above the place $\infty := \left(\frac{1}{t}\right)$ of $k(t)$.

Theorem 1.5 (Ghioca)**.** *Let $x \in \bar{k}$ of degree D and suppose that there is a place $v \nmid \infty$ such that $\hat{h}_{\phi,v}(x) > 0$. Then:*

$$\hat{h}_\phi(x) \gg_\phi \frac{1}{D^{r^4+r}}.$$

It is possible to find some large subfield K of $\bar{k}$ for which there is an even better estimate than the Lehmer bound. In certain cases, the dependence on D can be removed, and we say that K satisfies the property (B_ϕ). A first interesting instance is that of the abelian closure of k, which has been dealt with by David and Pacheco (see [7]). For ϕ a CM module, Bauchère finds a broad class of fields which satisfy (B_ϕ) (see [4]). If ϕ has rank 2 and is not exceptional, the field generated by the whole torsion of ϕ also satisfies (B_ϕ) (see [13]). In contrast with the number field setting, the bounds here are not absolute and depend on ϕ.

New bounds for purely inseparable extensions and in the general case. Our first result concerns purely inseparable extensions. Remark that it is useless here to exclude points of finite order, since they generate separable extensions.

Theorem 1.6. *Let ϕ be the Carlitz module. For all $x \in \bar{k}$ such that $k(x)/k$ is purely inseparable:*

$$\hat{h}_\phi(x) \geq \frac{(4q)^{-2}}{[k(x):k]}.$$

This is a slight improvement of Ghioca's estimate ([15], Theorem 4.5). Indeed, the Carlitz module has bad reduction only at ∞ and this place is totally ramified in any inseparable extension. Under the assumptions of Theorem 1.6, Ghioca's bound thus yields:

$$\hat{h}_\phi(x) \geq \frac{q^{-4}}{[k(x):k]}.$$

Our method naturally extends to a Drinfeld module with at least one prime of supersingular reduction, whereas Ghioca's theorem provides a bound of Lehmer strength in the purely inseparable case for all Drinfeld modules.

In the case of Drinfeld modules with complex multiplication, we can also consider morel general extensions. Unfortunately, we are not able to extend the Dobrowolski estimate to mixed extensions. We prove a variant of the theorem of Demangos in which the exponents are improved and the assumption on the Dirichlet density of the set of primes of supersingular reduction is removed.

Theorem 1.7. *Suppose that ϕ is of CM type. For all $x \in \bar{k}$ which are not torsion elements of ϕ, say with degree D and inseparable degree D_{i}, we have the following inequality:*

$$\hat{h}_\phi(x) \gg_\phi \frac{1}{D\big(D_{\mathrm{i}} \log(2D)\big)^{2r+1}}.$$

We finally turn to the case of Drinfeld modules without any further assumptions, and we show that there exists a lower bound for the canonical height of non-torsion elements for ϕ of polynomial type in the rank of ϕ.

Theorem 1.8. *For all $x \in \bar{k}$ non torsion for ϕ, say of degree D, the following inequality holds:*

$$\hat{h}_\phi(x) \gg_\phi \frac{1}{D^{4r^2+5}}.$$

The proofs of these theorems are all about diophantine approximation. In Section 2, we will start by recalling basic material about Drinfeld modules, their reductions and Tate modules. We will also discuss classical results about the distribution of supersingular places. At the end of this section, we will describe the properties of the canonical height.

In Section 3, we will then look at purely inseparable extensions, for which there is a specific ramification property that will be very useful here. Besides, the proof of Theorem 1.6 involves an "acceleration of convergence" trick and v-adic estimates at a place v of supersingular reduction.

The last two theorems need a heavier diophantine process. In Section 4, we will recall Siegel's lemma for function fields proved by Denis, and use it first to tackle

the CM case. The idea here is to exploit a standard v-adic property at a suitable place v in order to extrapolate the zeros of a well-chosen auxiliary polynomial.

Our lower bound in the general case will be proved in Section 5 following a similar method. The new ingredients here will be a weaker v-adic estimate and some combinatorial tools, that both reflect fine properties of the characteristic polynomial of the Frobenius morphism.

Acknowledgement. We would like to warmly thank Cécile Armana for her interest in this work as well as for the many inspiring discussions we had with her.

2. Drinfeld modules and canonical heights

We start by recalling classical facts about Drinfeld modules, their Tate modules, and supersingularity which plays a specific role in this work. We finally explain how to construct the canonical height on a Drinfeld module and describe its well-known properties.

For the sequel, we fix $\mathbb{F}_q$ a finite field with $q := p^\nu$ elements (where p is a prime number). Let $A := \mathbb{F}_q[t]$ be the ring of polynomials in one indeterminate over $\mathbb{F}_q$, embedded in its fraction field $k := \mathbb{F}_q(t)$, and let $\bar{k}$ be a fixed algebraic closure of k. The degree of a polynomial $a \in A \setminus \{0\}$ is denoted by $\deg(a)$; any ideal I of A is principal, and we let $\deg(I)$ be the degree of any generator of I.

2.1. Preliminaries on Drinfeld modules.

Let us first give basic definitions on Drinfeld modules and morphisms between them. For further details, we refer to [17], Chapter 4.

Let L be an A-field, i.e. a field endowed with a ring homomorphism $\iota : A \to L$. If ι is not injective, the kernel of ι is called the *A-characteristic of L*. Otherwise, the field L is said to have *generic characteristic*. This is the case when L is an extension of k, with ι being the inclusion map. Let $L\{\tau\}$ be he ring of twisted polynomials with coefficients in L. Recall that the multiplication in $L\{\tau\}$ is non-commutative and given on monomials by:

$$\forall \lambda, \mu \in L, \forall k, \ell \in \mathbb{N} : \quad \lambda\tau^k \mu\tau^\ell = \lambda\mu^{q^k}\tau^{k+\ell}.$$

For $P \in L\{\tau\}$, let $\deg_\tau(P)$ be the degree of P as a polynomial in τ. The map that sends τ to the q-th power Frobenius morphism: $X \mapsto X^q$ defines an isomorphism between $L\{\tau\}$ and the ring of $\mathbb{F}_q$-linear endomorphisms of the additive group $\mathbb{G}_a$ over L, where the multiplication is given by composition. If P belongs to $L\{\tau\}$, we will write $P(X)$ for the polynomial deduced from P when τ is replaced by X^q.

A *Drinfeld module* (or A-Drinfeld module) over L is an $\mathbb{F}_q$-algebra homomorphism ϕ:

$$\begin{array}{ccc} A & \longrightarrow & L\{\tau\} \\ a & \longmapsto & \phi_a \end{array}$$

such that the constant coefficient of ϕ_a is equal to $\iota(a)$ for any $a \in A$, and the image of ϕ contains at least one non-constant twisted polynomial. Because $A = \mathbb{F}_q[t]$, the Drinfeld module ϕ is uniquely determined by $\phi_t \in L\{\tau\}$. The *rank* r of ϕ is defined by: $r := \deg_\tau(\phi_t)$. We have the following property:

$$\forall a \in A : \deg_\tau(\phi_a) = r \deg(a).$$

In the sequel, we will usually write:

$$\phi_t := a_0\tau^0 + \cdots + a_r\tau^r,$$

where $a_i \in L$ for $0 \leq i \leq r$.

The simplest example of a Drinfeld module is the *Carlitz module* $\mathcal{C} : A \to k\{\tau\}$ given by $\mathcal{C}_t = t\tau^0 + \tau^1$, with rank equal to one.

If ϕ is a Drinfeld module over $\bar{k}$, the field k_ϕ generated over k by the coefficients of ϕ_t is a finite extension of k, called the *field of definition* of ϕ. For any $a \in A$, the polynomial ϕ_a has coefficients in k_ϕ; and k_ϕ is the minimal field with this property. Let B be the integral closure of A in k_ϕ and $D_\phi := [k_\phi : k]$.

For an ideal I of A, the set of *I-torsion points* for the Drinfeld module ϕ over L is

$$\phi[I] = \{x \in \bar{L}, \forall a \in I, \phi_a(x) = 0\}$$

and the set of *torsion points* for ϕ is:

$$\phi_{\text{tor}} := \bigcup_{I \lhd A} \phi[I].$$

Since ϕ_a is a separable polynomial, $\phi[I]$ is contained in a separable closure L^{s} of L. If the intersection between I and the A-characteristic of L is trivial, then $\phi[I]$ is an A-module isomorphic to $(A/I)^r$.

For two Drinfeld modules ϕ and ψ over L, a *morphism* from ϕ to ψ is an element $P \in L\{\tau\}$ such that:

$$\forall a \in A : P\phi_a = \psi_a P.$$

Since $A = \mathbb{F}_q[t]$, it is enough to check this property for $a = t$. The degree of P is its degree as a polynomial in τ. A non zero morphism is called an *isogeny*. An *isomorphism* is a morphism $P \in L^*$. Let $\text{End}(\phi)$ be the ring of endomorphisms of ϕ over $\bar{L}$.

Assume that ϕ is defined over $\bar{k}$. Then $\text{End}(\phi)$ is a finitely generated projective A-module of rank at most r. One can identify A with a subring of $\text{End}(\phi)$ by the map $a \mapsto \phi_a$. The case where the endomorphism ring has maximal rank will play a specific role in the sequel.

Definition 2.1. *We say that ϕ has complex multiplication (CM) if* $\text{End}(\phi)$ *has rank r over A.*

Let ϕ be a Drinfeld module of rank $r \geq 1$ over an A-field L, and $\mathfrak{l} := \lambda A$ be a prime ideal of A.

Definition 2.2. *The $\mathfrak{l}$-adic Tate module of ϕ is the projective limit:*

$$T_{\mathfrak{l}}(\phi) := \varprojlim \phi[\lambda^n].$$

The Tate module $T_{\mathfrak{l}}(\phi)$ is a module of rank $t \leq r$ over the completion $A_{\mathfrak{l}}$ of A at $\mathfrak{l}$. If L has generic characteristic (or if $L = A/\mathfrak{p}$, where $\mathfrak{p} \neq \mathfrak{l}$ is a prime ideal of A), the rank of $T_{\mathfrak{l}}(\phi)$ is exactly r. If $L = A/\mathfrak{l}$ the rank always drops because of inseparability (see [17], 4.5).

Let L^{s} be a separable closure of L. There is a linear action of the Galois group $\text{Gal}(L^{\text{s}}/L)$ on ϕ_{tor}, which yields a representation :

$$\rho_{\mathfrak{l}^\infty} : \text{Gal}(L^{\text{s}}/L) \longrightarrow \text{GL}_t(A_{\mathfrak{l}}).$$

Considering the $\mathfrak{l}$-torsion, we get another representation :

$$\rho_{\mathfrak{l}} : \mathrm{Gal}(L^{\mathrm{s}}/L) \longrightarrow \mathrm{GL}_t(\mathbb{F}_{\mathfrak{l}}),$$

where $\mathbb{F}_{\mathfrak{l}} = A/\mathfrak{l}$ is the residue field with $q_{\mathfrak{l}} := q^{\deg(\mathfrak{l})}$ elements.

2.2. **Supersingularity.** We continue with a review of supersingularity for Drinfeld modules over a finite field, reduction of Drinfeld modules, and what is known about places of supersingular reduction.

Let $\mathfrak{p}$ be a prime ideal in A of degree d and $\mathbb{F}_{\mathfrak{p}}$ the finite field $A/\mathfrak{p}$. We consider an extension L of $\mathbb{F}_{\mathfrak{p}}$ of degree m and a Drinfeld module ψ over L of rank r.

Definition 2.3. *The module ψ is said to be supersingular if $\psi[\mathfrak{p}] = \{0\}$.*

The module ψ is supersingular if and only if $T_{\mathfrak{p}}(\psi) = \{0\}$. Let $n := dm$. The Frobenius morphism

$$F := \tau^n : X \mapsto X^{q^n}$$

is an element of $L\{\tau\}$. Since the morphism F is the identity on L, it commutes with $\psi(A)$ and $F \in \mathrm{End}(\psi)$.

Proposition 2.4. *The module ψ is supersingular if and only some power of F belongs to $\psi(A)$.*

Proof. See [14] Proposition 4.1 or [17] Proposition 4.12.17, which also give other equivalent definitions of supersingularity. □

Remark. If ψ is supersingular, there is $\mathcal{P} \in A$ and a positive integer α such that: $F^\alpha = \phi_{\mathcal{P}}$. By comparing degrees in τ, we find that: $n\alpha = r\deg(\mathcal{P})$. Furthermore, since the Frobenius is inseparable, the ideal $\mathcal{P}A$ must be a power of $\mathfrak{p}$.

We now consider a Drinfeld module ϕ of rank r over $\bar{k}$ and a prime ideal $\mathfrak{P}$ of B. Let $B_{\mathfrak{P}}$ be the local ring of B at $\mathfrak{P}$ and $\mathbb{F}_{\mathfrak{P}}$ the residue field $B/\mathfrak{P}$.

Definition 2.5. *The module ϕ has good reduction at $\mathfrak{P}$ if it is isomorphic over k_ϕ to a Drinfeld module ϕ' such that the coefficients of ϕ'_t belong to $B_{\mathfrak{P}}$, and the leading coefficient of ϕ'_t is a unit of $B_{\mathfrak{P}}$.*

The last condition is equivalent to requiring that the map $\psi : A \to \mathbb{F}_{\mathfrak{P}}\{\tau\}$, obtained from ϕ' by reducing modulo $\mathfrak{P}$, is a Drinfeld module over $\mathbb{F}_{\mathfrak{P}}$ of rank exactly r. The module ϕ has good reduction at all but a finite number of primes. We say that $\mathfrak{P}$ is a *supersingular prime* for ϕ if ϕ has good reduction at $\mathfrak{P}$ and the reduced Drinfeld module ψ is supersingular over $\mathbb{F}_{\mathfrak{P}}$.

Remark. The Carlitz module $\mathcal{C}$ has good reduction at any prime ideal $\mathfrak{p}$ in A. Furthermore, the rank of the $\mathfrak{p}$-torsion drops modulo $\mathfrak{p}$ and the reduction is always supersingular at $\mathfrak{p}$ (see [17], Example 4.5.9).

Some facts are known about the distribution of supersingular primes. Let us start with the CM case (which covers the Carlitz module). We let ϕ be a CM Drinfeld module over $\bar{k}$ and $E := \mathrm{End}(\phi) \otimes_A k$, which is an extension of degree r of k, with ring of integers $\mathcal{O}_E$. We denote by H_E^+ the "normalizing field" of E. This is the field of definition of any $\mathcal{O}_E$-module ψ which is "sign normalized": the leading coefficient of ψ_x as a function of $x \in \mathcal{O}_E$ is given by a twisting of a sign function (see [20], 12 and 14). Let d_E be the degree of the constant field of H_E^+ over $\mathbb{F}_q$.

Let $\mathcal{P}_\phi$ be the set of primes $\mathfrak{p}$ of $\mathcal{O}_E$ completely split in H_E^+ for which there exists $F_\mathfrak{p} \in \mathrm{End}(\phi)$ such that $\deg_\tau(F_\mathfrak{p}) = \deg(\mathfrak{p})$, and for every prime ideal $\mathfrak{P}$ of B above $\mathfrak{p}$, we have the congruence in $B_\mathfrak{P}\{\tau\}$:

$$F_\mathfrak{p} \equiv \tau^{\deg(\mathfrak{p})} \pmod{\mathfrak{P}}.$$

The following result will be useful in the sequel.

Proposition 2.6. *There is a Drinfeld module ψ isogeneous to ϕ with* $\mathrm{End}(\psi) = \mathcal{O}_E$ *and such that for all positive integers P with $d_E \mid P$:*

$$\left|\{\mathfrak{p} \in \mathcal{P}_\psi, \deg(\mathfrak{p}) = P\}\right| \gg_\psi \frac{q^P}{P}.$$

Proof. By the theory of Hayes, there exists a Drinfeld module ψ isogeneous to ϕ with $\mathrm{End}(\psi) = \mathcal{O}_E$, which is sign-normalized (see [20], Theorem 12.3, as well as [19], 3 and [4], 1.6). Remark that ψ can be seen as an $\mathcal{O}_E$-module of rank 1, and that $k_\psi = H_E^+$.

Let P be a multiple of d_E. We take a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_E$ of degree P, and a prime $\mathfrak{P} \subset \mathcal{O}_{k_\psi}$ such that $\mathfrak{P} \mid \mathfrak{p}$. The module ψ has good reduction at $\mathfrak{P}$, and by Corollary 5.9 of [20], there exists an element $\psi_\mathfrak{p} \in k_\psi\{\tau\}$ such that:

$$\psi_\mathfrak{p} \equiv \tau^{\deg \mathfrak{p}} \pmod{\mathfrak{P}}.$$

By [20], Lemma 4.4, if $\mathfrak{p} = \mathcal{P}\mathcal{O}_E$ with $\mathrm{sgn}(\mathcal{P}) = 1$, then $\psi_\mathfrak{p} = \psi_\mathcal{P} \in \mathrm{End}(\psi)$.

Denote by $\mathcal{I}(\mathcal{O}_E)$ the group of fractional ideals and $\mathcal{P}^+(\mathcal{O}_E)$ its subgroup of principal ideals generated by elements $a \in E$ satisfying $\mathrm{sgn}(a) = 1$. Let

$$\mathcal{P}' := \left\{\mathfrak{p} \in \mathcal{P}^+(\mathcal{O}_E), \mathfrak{p} \text{ is prime}\right\},$$

and

$$\mathrm{Pic}^+(\mathcal{O}_E) := \mathcal{I}(\mathcal{O}_E)/\mathcal{P}^+(\mathcal{O}_E).$$

By Theorem 14.7 of [20], the Artin map induces an isomorphism:

$$\mathrm{Pic}^+(\mathcal{O}_E) \simeq \mathrm{Gal}(H_E^+/E).$$

Via this isomorphism, the set $\mathcal{P}'$ corresponds to the set of primes $\mathfrak{p}$ such that:

$$\left(\frac{H_E^+/E}{\mathfrak{p}}\right) = 1.$$

This means that the primes of $\mathcal{P}'$ are completely split in H_E^+, so that: $\mathcal{P}' \subset \mathcal{P}_\psi$. By the assumption on P, we can apply the Chebotarev density theorem ([12], Proposition 6.4.8), and the proof of the proposition is complete. □

Remark. There are variants of this statement. See [4], Proposition 1.6 where the restriction on the prime ideals is relaxed by considering a suitable power of the Frobenius, or [7], Proposition 2.5.1. Note that if the prime ideals of prescribed degree are counted in the normalizing field, we get a set of density 1.

Proposition 2.7. *If E/k is cyclic, there are infinitely many primes of supersingular reduction for ϕ.*

Proof. Let $(\mathcal{P})$ be a prime ideal of A that stays inert in E and $\mathfrak{p} \mid \mathcal{P}$ a prime of $\mathcal{O}_{k_\phi}$ such that ϕ has good reduction $\tilde{\phi}$ at $\mathfrak{p}$. Then Corollary 5.9 of [20] shows that $\tilde{\phi}_\mathcal{P}$ is purely inseparable, so the reduction is supersingular. The proposition follows from the Chebotarev density theorem applied to E/k. □

Away from the CM case, supersingularity should happen less often. On the one hand, the equivalent of a famous theorem of Elkies has been settled by Brown ([5]). If ϕ has rank 2, one can define its j-invariant $j(\phi) \in k_\phi$, which classifies ϕ up to $\bar{k}$-isomorphism. We say that ϕ is *exceptional* if $tj(\phi)$ is a square in the completion at infinity of k_ϕ (see the remarks following Proposition 1 of [25] for the correct assumption in Brown's theorem).

Theorem 2.8 (Brown)**.** *Suppose that $\mathbb{F}_q$ has characteristic > 2. If ϕ has rank 2 and is not exceptional, there are infinitely many primes of supersingular reduction for ϕ.*

On the other hand, Poonen has found many examples of Drinfeld modules of any rank $r \geq 2$ without a supersingular place (see [26]). Therefore, the estimates proven below under the existence of a supersingular prime cannot cover all Drinfeld modules.

2.3. **Heights and Drinfeld modules.** Let K be a finite extension of k and $M(K)$ denote the set of places of K. For $v \in M(K)$ we denote again by v the corresponding valuation

$$v : K \to \mathbb{Z} \cup \{\infty\},$$

which is normalized by taking $v(K^*) = \mathbb{Z}$. Let $\mathbb{F}_v$ be the residue field at v and $f_v := [\mathbb{F}_v \colon \mathbb{F}_q]$ be the residual degree at v. For any $x \in K^*$, there are finitely many places $v \in M(K)$ with $v(x) \neq 0$, and we have the *product formula*:

$$\sum_{v \in M(K)} f_v v(x) = 0. \tag{1}$$

If $x \in \bar{k}$, we can define its (absolute, logarithmic) Weil height $h(x)$ by the following formula:

$$h(x) := \frac{1}{[K:k]} \sum_{v \in M(K)} f_v \max\{0, -v(x)\},$$

where K is a field containing x (the height does not depend on the choice of such a field). The Weil height takes values in $\mathbb{R}^+$ and satisfies:

$$\forall n \in \mathbb{Z} : h(x^n) = |n| h(x).$$

Like in the number field setting, it has the Northcott property which is characteristic of height functions: for all real numbers D and H, the set of $x \in \bar{k}$ with $[k(x) : k] \leq D$ and $h(x) \leq H$ is finite. The height vanishes exactly on the field of constants of $\bar{k}$, and the Lehmer conjecture is trivially true in this case.

We will also use the notation $h(x_1, \ldots, x_n)$ for an n-tuple $(x_1, \ldots, x_n) \in \bar{k}^n$. By definition, if K is any field containing $x_1, \ldots, x_n$, we let:

$$h(x_1, \ldots, x_n) := \frac{1}{[K:k]} \sum_{v \in M(K)} f_v \max\{0, -v(x_1), \ldots, -v(x_n)\}.$$

Now, let ϕ be a Drinfeld module of rank r over $\bar{k}$. There is a notion of canonical height on $\bar{k}$ attached to ϕ, inspired by the Néron-Tate height and introduced by Denis (see [9]). This height is obtained from the Weil height h by a limit process. For any $x \in \bar{k}$, let:

$$\hat{h}_\phi(x) := \lim_{n \to +\infty} \frac{h(\phi_{t^n}(x))}{q^{rn}}.$$

The function $\hat{h}_\phi$ takes values in $\mathbb{R}^+$ and it is compatible with the action of ϕ in the following sense:

$$\forall a \in A, \forall x \in \bar{k} : \hat{h}_\phi(\phi_a(x)) = q^{r\deg(a)}\hat{h}_\phi(x). \tag{2}$$

More generally, if $F \in \bar{k}\{\tau\}$ is an isogeny from ϕ to ψ, we have (see [25], Proposition 2) :

$$\forall x \in \bar{k},\ \hat{h}_\psi(F(x)) = q^{\deg_\tau F}\hat{h}_\phi(x). \tag{3}$$

It is also possible to compare the canonical height with the Weil height; indeed, there exists a positive real number $c(\phi)$ such that:

$$\forall x \in \bar{k}, \quad \left|h(x) - \hat{h}_\phi(x)\right| \leq c(\phi). \tag{4}$$

From this inequality and the fact that h satisfies the Northcott property, it follows that $\hat{h}_\phi$ also satisfies the Northcott property.

We finally define the height of ϕ to be the naive height of the polynomial $\phi_t = \sum_{i=0}^r a_i\tau^i$, with coefficients in k_ϕ:

$$h(\phi) := \frac{1}{D_\phi}\sum_{v\in M(k_\phi)} f_v \max_{0\leq i\leq r}\{0, -v(a_i)\}.$$

The height of ϕ appears naturally while bounding the canonical height from below; we will not be very precise here about this dependence.

3. The Lehmer problem in the inseparable case

In this section, we slightly improve the bound given by Ghioca in [15], which solves the Lehmer problem for purely inseparable extensions and the Carlitz module. We first give a few useful lemmas, then we prove Theorem 1.6, and we finally generalise our estimate to Drinfeld modules with at least one prime of supersingular reduction. In the sequel, we let ϕ be a Drinfeld module of rank $r \geq 1$ defined over $\bar{k}$.

3.1. Preliminary lemmas.

We start with a classical reduction of the Lehmer problem to the case of integers. Let $x \in \bar{k}$ and recall that:

$$\phi_t := a_0\tau^0 + \cdots + a_r\tau^r,$$

where $a_i \in k_\phi$ for all $0 \leq i \leq r$.

Lemma 3.1. *Suppose that v is a valuation of $k_\phi(x)$ such that $v(x) < 0$, $v(a_r) = 0$ and $v(a_i) \geq 0$ for all $0 \leq i \leq r-1$. Then:*

$$\hat{h}_\phi(x) \geq \frac{D_\phi^{-1}}{[k(x):k]}.$$

Proof. This is Lemma 4.10 of [15]. For the sake of completeness, let us give a short proof here. The valuation v is normalized so that: $v(K^*) = \mathbb{Z}$, hence $v(x) \leq -1$. It follows from the assumption of the lemma that:

$$v\big(a_i x^{q^i}\big) > v\big(a_r x^{q^r}\big)$$

for all $0 \leq i \leq r-1$, and we get:

$$v(\phi_t(x)) = q^r v(x).$$

A straightforward induction yields, for any integer $n \geq 0$:

$$v(\phi_{t^n}(x)) = q^{rn} v(x) \leq -q^{rn}.$$

We thus derive the following bound:

$$\begin{aligned} h(\phi_{t^n}(x)) &= \frac{1}{[k_\phi(x):k]} \sum_{w \in M(k_\phi(x))} f_w \max\{0, -w(\phi_{t^n}(x))\} \\ &\geq \frac{q^{rn}}{[k_\phi(x):k]} \geq q^{rn} \frac{D_\phi^{-1}}{[k(x):k]}. \end{aligned}$$

Dividing both sides by q^{rn} and taking the limit when n goes to infinity, we obtain the inequality of the lemma. □

Remark. Suppose for instance that $a_r = 1$, the coefficients a_i of ϕ_t are in A and x is not an algebraic integer. Then there exists a valuation v that satisfies the assumption of the lemma, and the Lehmer conjecture is true for x. This is the case for a non-integral x in the Carlitz module.

One of the main ingredients in the proof of Theorem 1.6 is the following result concerning the decomposition of primes in purely inseparable extensions.

Lemma 3.2. *Let L/K be a finite and purely inseparable extension. Then every prime ideal of K is totally ramified in L.*

Proof. See [27], Proposition 7.5. □

3.2. **Purely inseparable extensions in the Carlitz case.** We now give a proof of Theorem 1.6. We let $\mathcal{C}$ be the Carlitz module and remark that $k_\phi = k$.

Proof of Theorem 1.6. We fix $x \in \bar{k}$ such that the extension $k(x)/k$ is purely inseparable. We let $L := k(x)$, with degree D over k and ring of integers $\mathcal{O}_L$, and denote by $\mathfrak{p} := tA$ the prime ideal of A generated by the polynomial t. By Lemma 3.2, the ideal $\mathfrak{p}$ is totally ramified in L, so there exists a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ such that:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^D.$$

In particular, the corresponding residual extension is trivial:

$$\mathcal{O}_L/\mathfrak{P} \simeq A/\mathfrak{p} \simeq \mathbb{F}_q.$$

Let v be the valuation on L associated to $\mathfrak{P}$, normalized as before. If $v(x) < 0$, the announced bound is a consequence of Lemma 3.1. So let us assume that $v(x) \geq 0$. Since $\mathcal{O}_L/\mathfrak{P} \simeq \mathbb{F}_q$, we have:

$$v(x^q - x) \geq 1,$$

and besides:

$$v\big(\phi_t(x) - x^q\big) = v(tx) \geq v(t) = D.$$

We let $y := \phi_t(x) - x$ and derive: $v(y) \geq 1$. Since $v(t) = D$, a straightforward induction yields, for all $m \geq 1$:

$$v\big(\phi_{t^m}(y)\big) \geq \min\left\{D + v\big(\phi_{t^{m-1}}(y)\big), qv(\phi_{t^{m-1}}(y))\right\} \geq \min\left\{D, q^m v(y)\right\}.$$

We now choose $m \geq 1$ to be the only positive integer such that:

$$q^{m-1} \leq D < q^m.$$

We thus have $v\big(\phi_{t^m}(y)\big) \geq D$. For all $n \geq m$, we obtain by induction:

$$v(\phi_{t^n}(y)) \geq (n - m + 1)D.$$

Fix $n := m + \alpha_q$, with $\alpha_2 = 4$, $\alpha_3 = 1$, and $\alpha_q = 0$ if $q > 3$. We get:

$$v\big(\phi_{t^n}(y)\big) \geq (1 + \alpha_q)D.$$

Remark now that x is not a torsion point for the Carlitz module, since x is purely inseparable over k and torsion points are separable. We can thus apply the product formula (1) to:

$$z := \phi_{t^n}(y) = \phi_{t^n(t-1)}(x) \in k(x),$$

which is not zero. We get :

$$(1 + \alpha_q)D \leq f_v v(z) = -\sum_{w \neq v} f_w w(z) \leq [k(x) : k]h(z) = Dh(z).$$

By (4), there exists a real number $c(\mathcal{C}) > 0$ such that:

$$\big|h(z) - \hat{h}_{\mathcal{C}}(z)\big| \leq c(\mathcal{C}),$$

and by [10], Theorem 4, we can take:

$$c(\mathcal{C}) = c_q = \frac{2q}{(q-1)^2}.$$

Applying (2), we obtain:

$$1 + \alpha_q \leq h(z) \leq \hat{h}_{\mathcal{C}}(z) + c(\mathcal{C}) = q^{n+1}\hat{h}_{\mathcal{C}}(x) + c_q,$$

from which we finally deduce:

$$\hat{h}_{\mathcal{C}}(x) \geq \frac{1 + \alpha_q - c_q}{q^{n+1}} = \frac{1 + \alpha_q - c_q}{q^{m+1+\alpha_q}} \geq \beta_q \frac{q^{-2}}{D},$$

where:

$$\beta_q = \frac{1 + \alpha_q - c_q}{q^{\alpha_q}}.$$

Now, a quick computation shows that $\beta_2 = 16^{-1}$, $\beta_3 = 6^{-1}$ and $\beta_q \geq 9^{-1}$ for $q > 3$ so that the expected inequality holds. □

Remark. We easily see that $(4q)^{-2}$ can be replaced by $2^{-1}q^{-2}$ for $q \geq 7$.

3.3. **An explicit estimate within a good model.** We now extend Theorem 1.6 to Drinfeld modules with at least one prime of supersingular reduction. The strategy is the same but some technical complications arise. A first problem comes from the degree of the supersingular prime, which may be greater than one. We also have to take care of the fact that ϕ is defined over k_ϕ.

We take a Drinfeld module ϕ of rank r defined over a field K with $[K : k] = d$. We also suppose that there exists a prime $\mathfrak{p}$ of $B := \mathcal{O}_K$ of supersingular reduction for ϕ. As usual, we denote:

$$\phi_t = a_0\tau^0 + \cdots + a_r\tau^r.$$

We first assume that:

$$\forall 0 \leq i \leq r : a_i \in B_{\mathfrak{p}}, \text{ and } a_r \in B_{\mathfrak{p}}^{\times},$$

and that the Drinfeld module obtained after reducing ϕ mod $\mathfrak{p}$ is supersingular. By Proposition 2.4, there exists a polynomial $\mathcal{P} \in A$ such that the following congruence holds in $B_{\mathfrak{p}}\{\tau\}$:

$$\phi_{\mathcal{P}} \equiv \tau^{r \deg(\mathcal{P})} \pmod{\mathfrak{p}}. \tag{5}$$

We get the following explicit lower bound.

Proposition 3.3. *For all $x \in \bar{k}$ such that $K(x)/K$ is purely inseparable:*

$$\hat{h}_\phi(x) \geq \frac{q^{-rd\deg(\mathfrak{p})(c(\phi)+3)}}{[k(x):k]}.$$

Proof. We consider $x \in \bar{k}$ such that $K(x)/K$ is purely inseparable. Let $L := K(x)$ with ring of integers $\mathcal{O}_L$ and

$$D := [L:K] \leq [k(x):k].$$

Lemma 3.2 says that $\mathfrak{p}$ is totally ramified in L, hence there exists a prime $\mathfrak{P}$ of $\mathcal{O}_L$ such that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^D$. Moreover, the associated residual extension is trivial:

$$\mathcal{O}_L/\mathfrak{P} \simeq B/\mathfrak{p} \simeq \mathbb{F}_{q_\mathfrak{p}},$$

where by definition: $q_\mathfrak{p} = q^{\deg(\mathfrak{p})}$.

Let now v denote the valuation of L associated to $\mathfrak{P}$, normalized as usual by $v(L^*) = \mathbb{Z}$. If $v(x) < 0$, by the assumption made on the coefficients of ϕ_t, we can apply Lemma 3.1 and get a bound even stronger than expected here. So we assume that $v(x) \geq 0$. Let

$$\mathcal{O}_\mathfrak{P} := \{\alpha \in L \mid v(\alpha) \geq 0\}$$

be the valuation ring of $\mathfrak{P}$. Since $\mathcal{O}_\mathfrak{P}/\mathfrak{P}\mathcal{O}_\mathfrak{P} \simeq \mathcal{O}_L/\mathfrak{P}$, we have the following congruence in the ring $\mathcal{O}_\mathfrak{P}$:

$$x^{q_\mathfrak{p}} \equiv x \pmod{\mathfrak{P}\mathcal{O}_\mathfrak{P}}.$$

By the remark following Proposition 2.4, we see that: $\deg(\mathfrak{p}) \mid r\deg(\mathcal{P})$. From the congruence above and (5), we derive:

$$\phi_\mathcal{P}(x) \equiv x^{q^{r\deg(\mathcal{P})}} \equiv x \pmod{\mathfrak{P}\mathcal{O}_\mathfrak{P}}.$$

Let $y := \phi_\mathcal{P}(x) - x$, so that: $v(y) \geq 1$. If we write:

$$\phi_\mathcal{P} := b_0\tau^0 + \cdots + b_{r\deg(\mathcal{P})}\tau^{r\deg(\mathcal{P})},$$

the combination of (5) and Lemma 3.2 shows that:

$$\forall 0 \leq i \leq r\deg(\mathcal{P}) - 1 : v(b_i) \geq D.$$

Let $m \geq 1$. By an easy induction, we deduce that:

$$\begin{aligned} v(\phi_{\mathcal{P}^m}(y)) &\geq \min\left\{D, q^{r\deg(\mathcal{P})}v(\phi_{\mathcal{P}^{m-1}}(y))\right\} \\ &\geq \min\left\{D, q^{mr\deg(\mathcal{P})}v(y)\right\}. \end{aligned}$$

We choose for m the only positive integer such that:

$$q^{(m-1)r\deg(\mathcal{P})} \leq D < q^{mr\deg(\mathcal{P})}.$$

We thus have $v(\phi_{\mathcal{P}^m}(y)) \geq D$, and by another quick induction, for all $n \geq m$:

$$v(\phi_{\mathcal{P}^n}(y)) \quad \geq \quad (n-m+1)D.$$

We take:

$$n := m - 1 + ([c(\phi)] + 2)d,$$

so that:

$$v(\phi_{\mathcal{P}^n}(y)) \geq ([c(\phi)] + 2)dD \geq (c(\phi) + 1)dD.$$

Let us apply the product formula (1) to

$$z := \phi_{\mathcal{P}^n}(y) = \phi_{\mathcal{P}^n(\mathcal{P}-1)}(x) \in L.$$

Remark that x is not torsion for ϕ because of inseparability, so z is not zero. We get :

$$(c(\phi)+1)dD \leq f_v v(z) = -\sum_{w\neq v} f_w w(z) \leq [L:k]h(z),$$

hence

$$c(\phi)+1 \leq h(z) \leq \hat{h}_\phi(z) + c(\phi) = q^{(n+1)r\deg(\mathcal{P})}\hat{h}_\phi(x) + c(\phi),$$

from which we deduce

$$\begin{aligned}\hat{h}_\phi(x) &\geq \frac{1}{q^{(n+1)r\deg(\mathcal{P})}} \geq \frac{q^{-rd(c(\phi)+3)\deg(\mathcal{P})}}{q^{(m-1)r\deg(\mathcal{P})}} \\ &\geq \frac{q^{-rd(c(\phi)+3)\deg(\mathcal{P})}}{D} \geq \frac{q^{-rd(c(\phi)+3)\deg(\mathcal{P})}}{[k(x):k]}.\end{aligned}$$

□

Remarks. Using [10] Theorem 4, it is possible to bound $c(\phi)$ explicitly in terms of $h(\phi)$. Compared to [15] Theorem 4.5, our method needs a place of supersingular reduction. But if such a place is given, our bound is stronger in the rank of the module.

3.4. **The general situation.** We can now prove an estimate of Lehmer strength in the inseparable case, when ϕ has at least one prime of supersingular reduction. This is done by handling the changes produced by an isomorphism.

Proposition 3.4. *Suppose that there exists a prime of supersingular reduction for ϕ. Then for all $x \in \bar{k}$ such that $k(x)/k$ is purely inseparable:*

$$\hat{h}_\phi(x) \gg_\phi \frac{1}{[k(x):k]}.$$

Proof. Let ϕ be a Drinfeld module with a supersingular prime. The module ϕ is isomorphic to a Drinfeld module ψ that satisfies the assumption made before Proposition 3.3. The isomorphism is multiplication by an element $u \in \bar{k}^*$. The module $\psi = u^{-1}\phi u$ is defined over $K = k_\phi(u)$ and for all $x \in \bar{k}^*$ (see [9], Corollaire 2):

$$\hat{h}_\phi(x) = \hat{h}_\psi(u^{-1}x).$$

Now, if x is purely inseparable over k, the number $u^{-1}x$ is purely inseparable over K and:

$$[k(u^{-1}x):k] \leq [k(x):k][k(u):k],$$

so the theorem follows from Proposition 3.3. □

Remarks. It is possible to cover the case where $k(x)/k$ is no longer purely inseparable by taking K large enough so as to contain the separable closure of k in $k(x)$. The dependence on the separable degree is exponential.

The same strategy might be applied without any supersingularity assumption. If ϕ is a Drinfeld module of rank r and $k(x)/k$ is purely inseparable of degree D, it should yield:

$$\hat{h}_\phi(x) \gg_\phi \frac{1}{D^r},$$

which is better than our general bound below (but this method gives a weaker lower bound in terms of the separable degree of the extension $k(x)/k$).

4. The canonical height on CM modules

In this section, we focus on CM Drinfeld modules, for which an estimate of Dobrowolski strength on the canonical height has been given by Demangos.

We fix $x \in \bar{k}$ not torsion for ϕ. It will be more natural in this section to consider the degree of x over k_ϕ (and it will be of no effect on the bound we want to prove), so we set $D := [k_\phi(x) : k_\phi]$. We also write $D = D_{\mathrm{s}} D_{\mathrm{i}}$, where D_{s} (resp. D_{i}) is the separable (resp. inseparable) degree of $k_\phi(x)/k_\phi$.

4.1. **Siegel's lemma for function fields.** We start by recalling Siegel's lemma in the function field case. This is a statement about systems of linear equations with coefficients in $\bar{k}$. Provided that there are sufficiently many unknowns (compared to the number of equations), we can get a solution with height explicitly bounded in terms of the linear system. We let m and n be two positive integers.

Lemma 4.1. *Let K be a finite extension of k with degree d and $a_{i,j} \in K$, for $1 \leq i \leq m$, $1 \leq j \leq n$. If $m > nd$, there is a non-zero element $(x_1, \ldots, x_m)$ in A^m such that:*

$$\forall 1 \leq j \leq n : \sum_{1 \leq i \leq m} a_{i,j} x_i = 0,$$

and:

$$\forall\, 1 \leq i \leq m : \; h(x_i) \leq \frac{d}{m - nd} \sum_{1 \leq j \leq n} h(a_{1,j}, \ldots, a_{m,j}).$$

Proof. See [9] Lemme 5, and remark that the regularity assumption on the field of definition is not used in the proof of the lemma. □

This result is very important in diophantine approximation. As we will see, it can be used to construct "auxiliary" polynomials (with coefficients of bounded height) that vanish on a given $x \in \bar{k}$ with prescribed multiplicity.

If G is a polynomial of $\bar{k}[X]$ and $\ell \geq 0$ is an integer, denote by $\partial_\ell G(X)$ the coefficient in Y^ℓ of the polynomial $G(X+Y) \in \bar{k}[X, Y]$. We will need the following interpretation of inseparability (see [8], the proof of Proposition 4).

Lemma 4.2. *Let G be a polynomial of $k_\phi[X]$ and $n \geq 0$ an integer. The following conditions are equivalent:*

(i) $\forall 0 \leq m < n, \; \partial_{mD_{\mathrm{i}}} G(x) = 0$
(ii) $\forall 0 \leq m < nD_{\mathrm{i}}, \; \partial_m G(x) = 0.$

Proof. It is immediate that *(ii)* is stronger than *(i)*. In order to prove the other implication, we proceed by induction on n. If $n = 0$, there is nothing to prove, so we let $n \geq 1$ and suppose that *(i)* holds. By the induction hypothesis, we have

$$\forall 0 \leq m \leq (n-1)D_{\mathrm{i}} : \partial_m G(x) = 0,$$

so that G vanishes at x with multiplicity $> (n-1)D_{\mathrm{i}}$.

Let $\Delta \in k_\phi[X]$ be the minimal polynomial of x over k_ϕ, and write $G := \Delta^\ell H$, where $H \in k_\phi[X]$ and $\Delta \nmid H$ in $k_\phi[X]$. Since x is a root of Δ of multiplicity D_{i}, we have: $\ell > n - 1$, so $\ell \geq n$ and it follows that G vanishes at x with multiplicity $\geq nD_{\mathrm{i}}$. □

Due to the gap between the Weil height and the canonical height, we apply Philippon's "stretched embedding" trick, and consider polynomials in two variables.

The following corollary of Siegel's lemma will be used as an interpolation step in the sequel.

Corollary 4.3. *Let $\mathcal{N} \in A$ of degree N, and L, T two positive integers such that T is a multiple of D_{i} and:*

$$L^2 \geq 2D_\phi D_{\mathrm{s}} T. \tag{6}$$

Then there is a non-zero polynomial:

$$F(X,Y) := \sum_{0 \leq i,j < L} f_{i,j} X^i Y^j \in A[X,Y]$$

such that $F(X, \phi_{\mathcal{N}}(X))$ vanishes at x with multiplicity $\geq T$ and:

$$h(F) := \max_{i,j} h(f_{i,j}) \ll_\phi \frac{D_{\mathrm{s}} T}{L^2} \left(L q^{rN} \hat{h}_\phi(x) + L + TN \right).$$

Proof. Let:

$$F(X,Y) := \sum_{0 \leq i,j < L} f_{i,j} X^i Y^j, \text{ and } G(X) := F(X, \phi_{\mathcal{N}}(X)).$$

We apply Siegel's lemma to the system:

$$\forall\, 0 \leq \ell < T : \partial_\ell G(x) = 0.$$

This system is defined over the field $K := k_\phi(x)$, and it is linear in the unknown variables $(f_{i,j})_{0 \leq i,j < L}$. We may rewrite it under the following form:

$$\forall\, 0 \leq \ell < T : \sum_{0 \leq i,j < L} a_{i,j,\ell} f_{i,j} = 0,$$

where for all $0 \leq i, j < L$ and $0 \leq \ell < T$:

$$a_{i,j,\ell} = \partial_\ell \left(X^i \phi_{\mathcal{N}}(X)^j \right)(x).$$

The number of unknown variables is:

$$m = \left| \{(i,j), 0 \leq i,j < L\} \right| = L^2.$$

Thanks to Lemma 4.2, it is sufficient to consider the previous equations for $0 \leq \ell < T$ a multiple of D_{i}. Thus, the number of equations is:

$$n = \frac{T}{D_{\mathrm{i}}}.$$

Now, denote by d the degree of K over k. We have:

$$nd = D_\phi D_{\mathrm{s}} T \leq \frac{L^2}{2} < m,$$

so we are in a position to use Siegel's lemma. The height of the coefficients $a_{i,j,\ell}$ is classically bounded by considering formal series (see [8], Proof of Proposition 7; or [9], p. 221 in the Carlitz case). For $0 \leq \ell < T$, we get:

$$h\big((a_{i,j,\ell})_{0 \leq i,j < L}\big) \leq Lh(x) + Lh(\phi_{\mathcal{N}}(x)) + h(\phi)TN, \tag{7}$$

so that:

$$\begin{aligned} h\big((a_{i,j,\ell})_{0 \leq i,j < L}\big) &\ll_\phi L\hat{h}_\phi(x) + L\hat{h}_\phi(\phi_{\mathcal{N}}(x)) + L + TN \\ &\ll_\phi L q^{rN} \hat{h}_\phi(x) + L + TN. \end{aligned}$$

By Lemma 4.1, there exists a solution $(f_{i,j})_{0\leq i,j<L}$ such that:

$$\begin{aligned} h(f_{i,j}) &\leq \frac{nd}{m-nd}\max_{0\leq \ell<T} h\big((a_{i,j,\ell})_{0\leq i,j\leq L}\big) \\ &\ll_\phi \frac{nd}{m}\big(Lq^{rN}\hat{h}_\phi(x)+L+TN\big) \\ &\ll_\phi \frac{D_{\mathrm{s}}T}{L^2}\left(Lq^{rN}\hat{h}_\phi(x)+L+TN\right). \end{aligned}$$

□

4.2. **The extrapolation step.** In [8], Demangos extends the theorem proved by Denis in the Carlitz case to Drinfeld modules of CM type. In fact, his result holds in a slightly different setting. He also considers inseparable extensions and finds a lower bound for the canonical height which is polynomial in the inseparable degree.

The method used in the previous section to tackle purely inseparable extensions does not extend well as soon as the separable degree grows. This is mainly because our strategy relies on the triviality of the residue field. Thus, we do not manage to extend Dobrowolski's bound to arbitrary extensions for Drinfeld modules of CM type.

We now revisit the method used by Demangos and focus on the CM case. We get a lower bound estimate where the exponents are improved and depend only on the rank r of ϕ.

For the remaining of this section, we suppose that ϕ is of CM type. Using (3), we see that it suffices to prove Theorem 1.7 for any Drinfeld module ψ over $\bar{k}$ isogeneous to ϕ. We will thus assume in the sequel that ϕ satisfies the properties of the module ψ of Proposition 2.6; in particular, the field E of CM is contained in k_ϕ. We pick $\mathcal{N}\in A$ of degree $N\geq 1$, and L,T two positive integers such that T is a multiple of D_i and such that (6) holds. Our Corollary 4.3 yields a non-zero polynomial $F\in A[X,Y]$ of controlled degree with vanishing properties and height precisely bounded. Again, we let

$$G(X):=F(X,\phi_{\mathcal{N}}(X)).$$

The following result shows that the vanishing properties of G can be extended to $F_{\mathfrak{p}}(x)$, for a prime $\mathfrak{p}$ well chosen in $\mathcal{O}_E$ (recall that $F_{\mathfrak{p}}$ is a lifting of the Frobenius morphism, see Proposition 2.6, and above for the definition of $\mathcal{P}_\phi$).

Proposition 4.4. *Let P be an integer large enough with respect to ϕ, and $T'\geq 1$ such that:*

$$h(F)+2L\big(q^{r(N+P)}\hat{h}_\phi(x)+c(\phi)\big)+T'Nh(\phi)<\frac{P}{D_\phi}\left(\frac{T-T'}{D_{\mathrm{i}}}\right). \tag{8}$$

For any place $\mathfrak{p}\in\mathcal{P}_\phi$ of degree P such that x is $\mathfrak{P}$-integral for all $\mathfrak{P}\mid\mathfrak{p}$, the polynomial G vanishes at $F_{\mathfrak{p}}(x)$ with multiplicity $>T'$.

Proof. Let us proceed by contradiction. We suppose that there is a prime $\mathfrak{p}$ with prescribed properties as well as $0\leq k\leq T'$ such that:

$$y:=\partial_k G(F_{\mathfrak{p}}(x))\neq 0.$$

We want to apply the product formula to $y \in \bar{k}$. We start with finite places above $\mathfrak{p}$ and take $\mathfrak{p}' \mid \mathfrak{p}$ a prime of B. Let:

$$\Delta := \sum_{0 \le i \le D} \delta_i X^i$$

be the minimal polynomial of x over k_ϕ. By definition, the order of Δ at x is D_{i}. Now, the polynomial $\partial_k G \in B_{\mathfrak{p}'}[X]$ (for P large enough) vanishes at x with multiplicity at least $T-k$, so there is $\ell \ge \frac{T-k}{D_{\mathrm{i}}}$ such that:

$$\Delta^\ell \mid \partial_k G \text{ in } B_{\mathfrak{p}'}[X].$$

By construction of $\mathcal{P}_\phi$, the residual degree $f_{\mathfrak{p}'|\mathfrak{p}}$ is 1. So $|B/\mathfrak{p}'B| = q^P$, and for $0 \le i \le D$:

$$\delta_i \equiv \delta_i^{q^P} \pmod{\mathfrak{p}'B}.$$

Let $\mathfrak{P} \mid \mathfrak{p}'$ a prime in $\mathcal{O}_{k_\phi(x)}$. Using the properties of characteristic p, we derive the following congruence in the valuation ring $\mathcal{O}_{\mathfrak{P}}$ (at least for P large enough):

$$\Delta(F_{\mathfrak{p}}(x)) \equiv \sum_{0 \le i \le D} \delta_i x^{iq^P} \equiv \sum_{0 \le i \le D} \delta_i^{q^P} x^{iq^P} \equiv \Delta(x)^{q^P} \equiv 0 \pmod{\mathfrak{p}'\mathcal{O}_{\mathfrak{P}}}.$$

If v is the valuation corresponding to $\mathfrak{P}$, we deduce that: $v(y) \ge \ell e_{\mathfrak{P}|\mathfrak{p}'}$. By the product formula (1):

$$\begin{aligned} 0 &= \sum_{v \in M(k_\phi(x))} f_v v(y) \\ &\ge \sum_{v|\mathfrak{p}'} f_v e_{v|\mathfrak{p}'} \ell - \sum_{v \nmid \mathfrak{p}'} f_v \max\{0, -v(y)\}, \end{aligned}$$

and therefore:

$$[k_\phi(x) : k_\phi] P \ell \le [k_\phi(x) : k] h(y).$$

The height of y is bounded using (7), and we get:

$$\begin{aligned} \frac{T-k}{D_{\mathrm{i}}} P \le \ell P &\le D_\phi\Big(h(F) + Lh(F_{\mathfrak{p}}(x)) + Lh(\phi_{\mathcal{N}}(F_{\mathfrak{p}}(x))) + h(\phi)kN\Big) \\ &\le D_\phi\Big(h(F) + 2L\big(q^{r(N+P)}\hat{h}_\phi(x) + c(\phi)\big) + T'Nh(\phi)\Big), \end{aligned}$$

so that:

$$h(F) + 2L\big(q^{r(N+P)}\hat{h}_\phi(x) + c(\phi)\big) + T'Nh(\phi) \ge \frac{P}{D_\phi}\Big(\frac{T-T'}{D_{\mathrm{i}}}\Big),$$

which is a contradiction. □

4.3. **The lemma of zeros.** The next step is to count the number of zeros of G with multiplicity and then compare this with $\deg(G)$. We fix positive integers P and T' as in Proposition 4.4.

Lemma 4.5. *Suppose that $d_E \mid P$ and that for any prime $\mathfrak{p} \in \mathcal{P}_\phi$ with $\deg(\mathfrak{p}) = P$, x is $\mathfrak{P}$-integral for all $\mathfrak{P} \mid \mathfrak{p}$. If $q^{rN} \ge L$ and $q^P \gg_\phi \log(D_{\mathrm{s}})^2$, then:*

$$T' D_{\mathrm{s}} \frac{q^P}{P} \ll_\phi q^{rN} L. \tag{9}$$

Proof. We observe that:

$$\deg\left(\phi_{\mathcal{N}}(X)\right) = q^{rN},$$

and $G(X) = F(X, \phi_{\mathcal{N}}(X))$ with $\deg_X(F) < L$, $\deg_Y(F) < L$. So we get:

$$\deg(G) < L(q^{rN} + 1).$$

Further, the polynomial G is not zero. Indeed, otherwise we would have:

$$\left(Y - \phi_{\mathcal{N}}(X)\right) \mid F(X, Y) \text{ in } k_\phi[X, Y],$$

and considering the degrees with respect to X, we derive: $q^{rN} < L$, which contradicts the assumption of the lemma.

There remains to count the number of roots of the polynomial G, with multiplicity. By Proposition 4.4, this polynomial vanishes on

$$\{F_{\mathfrak{p}}(x), \mathfrak{p} \in \mathcal{P}_\phi, \deg(\mathfrak{p}) = P\}$$

with multiplicity $> T'$. Since G is defined over k_ϕ, it also vanishes at each Galois conjugate over k_ϕ. The point x is not torsion for ϕ, so by a classical combinatorial argument (see [8], Lemma 3, Dobrowolski's original result [11], Lemma 3, or its adaptation to CM abelian varieties [6], Proposition 2.7), for all $\mathfrak{p}, \mathfrak{q}$ distinct primes, the elements $F_{\mathfrak{p}}(x)$ and $F_{\mathfrak{q}}(x)$ are not conjugates over k_ϕ, and furthermore we have an inequality:

$$\left|\left\{\mathfrak{p}, [k_\phi(F_{\mathfrak{p}}(x)) : k_\phi]_s < D_{\mathrm{s}}\right\}\right| \leq \frac{\log(D_{\mathrm{s}})}{\log(2)}.$$

Now, let M_P be the number of prime ideals in $\mathcal{P}_\phi$ of degree P. By Proposition 2.6, we get:

$$M_P \gg_\phi \frac{q^P}{P}.$$

Therefore, if we let $|Z|$ the number of zeros of G counted with multiplicity, we have:

$$|Z| \geq T' D_{\mathrm{s}} \left(M_P - \frac{\log(D_{\mathrm{s}})}{\log(2)}\right) \gg_\phi T' D_{\mathrm{s}} \frac{q^P}{P}.$$

The lemma follows immediately from this estimate and the upper bound on $\deg(G)$. □

4.4. **A bound for the canonical height in the CM case.** We are ready to bound from below the canonical height associated to a CM module. Let us first explain how the parameters ought to be determined.

Start by remarking that in order to get an inverse polynomial bound in D, we have to choose L, T, T', q^N, q^P to be at most polynomial in D. The major constraint concerning N is the assumption of Lemma 4.5. Considering that we need to ensure:

$$q^{r(N+P)} \hat{h}_\phi(x) \ll_\phi 1,$$

we will fix N in terms of L as small as possible in order to get a sharp lower bound for the height. The integer N also appears in (8), but it will be sufficient to remark that it is logarithmic in D.

We know that the "Dirichlet quotient"

$$\frac{D_{\mathrm{s}} T}{L^2}$$

is bounded, so the only dangerous contribution in the bound for $h(F)$ comes from TN. If we want (8) to hold, we have to compensate the N factor; this can be done by forcing:

$$\frac{P}{D_{\mathrm{i}}\log(D)\log(P)} \ll_\phi \frac{D_{\mathrm{s}}T}{L^2} \ll_\phi \frac{P}{D_{\mathrm{i}}\log(D)\log(P)} \tag{10}$$

Using this and choosing T' as big as possible in terms of T so as to satisfy (8), we find how to fix q^P in order to get a final negation of (9). Now, the inequality in (8) implies a precise bound for L in terms of T. Injecting this in (10), we get L (and T) in terms of D.

Let us now state our lower bound in the CM case. In order to avoid heavy computations, we do not optimize our method (this would bring a power of $\log(D_{\mathrm{i}})\log\log(D)$ at the numerator) or specify the dependence on ϕ except for the exponents.

Proposition 4.6. *Let $x \in \bar{k}$ not torsion for ϕ and of degree $D = D_{\mathrm{s}}D_{\mathrm{i}} \geq 2$. Then:*

$$\hat{h}_\phi(x) \gg_\phi \frac{1}{D\big(D_{\mathrm{i}}\log(D)\big)^{2r+1}}.$$

Proof. We may assume that the degrees are taken over k_ϕ and that D is large enough in terms of ϕ. Let us proceed by contradiction. Choose $P \in \mathbb{N}$ such that:

$$D_{\mathrm{i}}^2\log(D)^2 \ll_\phi q^P \ll_\phi D_{\mathrm{i}}^2\log(D)^2;$$

this is possible for D large enough, and we may also assume that $d_E \mid P$. Let:

$$L := DD_{\mathrm{i}}\left[\frac{\log(D)\log(P)^2}{P^2}\right],\ T := DD_{\mathrm{i}}^2\left[\frac{\log(D)\log(P)^3}{P^3}\right],\ N \in \mathbb{N} \text{ with } L \leq q^{rN} \ll_\phi L,$$

the last condition being easy to ensure for D large enough; also fix $\mathcal{N} \in A$ of degree N. The assumption (6) is valid, so we have a polynomial $F \in A[X,Y]$ such that $G(X) := F(X, \phi_{\mathcal{N}}(X))$ vanishes at x with order $\geq T$, and:

$$\begin{aligned} h(F) &\ll_\phi \frac{D_{\mathrm{s}}T}{L^2}\Big(Lq^{Nr}\hat{h}_\phi(x) + L + TN\Big) \\ &\ll_\phi \frac{P}{D_{\mathrm{i}}\log(D)\log(P)}\left(L + T\log(D)\right) \ll_\phi \frac{TP}{D_{\mathrm{i}}\log(P)}. \end{aligned}$$

We apply Proposition 4.4 with

$$T' := \left[\frac{TP}{D_{\mathrm{i}}\log(D)\log(P)}\right] \leq \frac{T}{2},$$

where the inequality holds for D large enough. We check that:

$$h(F) + 2L\big(q^{r(N+P)}\hat{h}_\phi(x) + c(\phi)\big) + T'Nh(\phi) \ll_\phi \frac{T}{D_{\mathrm{i}}}\frac{P}{\log(P)},$$

so for D (and thus P) large enough:

$$h(F) + 2L\big(q^{r(N+P)}\hat{h}_\phi(x) + c(\phi)\big) + T'Nh(\phi) < \frac{P}{D_\phi}\left(\frac{T-T'}{D_{\mathrm{i}}}\right).$$

Thus, condition (8) holds and G vanishes at $F_{\mathfrak{p}}(x)$ with multiplicity $> T'$ for $\mathfrak{p}$ as in Proposition 4.4. Remark that we may assume that x has non-negative valuation above all primes of $\mathcal{P}_\phi$ with degree P (large enough). Otherwise, Lemma 3.1 yields

an even stronger bound for $\hat{h}_\phi(x)$. The assumptions of Lemma 4.5 are satisfied and we have:

$$q^{rN} L \ll_\phi L^2 = D^2 D_{\mathrm{i}}^2 \frac{\log(D)^2 \log(P)^4}{P^4},$$

whereas:

$$T' D_{\mathrm{s}} \frac{q^P}{P} \gg_\phi D^2 D_{\mathrm{i}}^2 \frac{\log(D)^2 \log(P)^2}{P^3}.$$

This contradicts (9) for D and thus P large enough, so the proof of the theorem is complete. □

Remark. This result is close to the main theorem of [8]. Our proof follows a similar strategy, except that we use a lifting of the Frobenius instead of the properties of supersingular primes. On the one hand, our exponents are a bit better, and they do not depend on $h(\phi)$ and D_ϕ. On the other hand, part of the work of Demangos was to compute the constant in the bound, which we have not done here.

5. A polynomial bound for general Drinfeld modules

We are now going to prove an estimate for the canonical height in general Drinfeld modules. Without any specific assumption on our Drinfeld module ϕ, we give a lower bound for the height, with a power of the degree at the denominator. Furthermore, this power only depends on the rank r of ϕ. In the sequel, since the result we have in view is already known in rank 1, we will suppose that $r \geq 2$.

We fix $x \in \bar{k}$ not torsion for ϕ. As in the previous section we will consider degrees over the field of definition k_ϕ of the Drinfeld module ϕ; this has no effect on the lower bound we are going to prove. Let us set: $D := [k_\phi(x) : k_\phi] = D_{\mathrm{s}} D_{\mathrm{i}}$, where D_{s} (resp. D_{i}) is the separable (resp. inseparable) degree of $k_\phi(x)/k_\phi$.

5.1. **Characteristic polynomial of the Frobenius and extrapolation.** Like in the previous section, we use diophantine approximation. The first step is the construction of an auxiliary polynomial.

Let $\mathcal{N} \in A$ of degree N, and L, T two positive integers with $D_{\mathrm{i}} \mid T$ such that (6) holds. By Corollary 4.3, there is a non-zero polynomial $F \in A[X, Y]$ of controlled degree with vanishing properties and height precisely bounded. We still let:

$$G(X) := F(X, \phi_{\mathcal{N}}(X)).$$

We take a prime $\mathfrak{p}$ of the ring of integers B of k_ϕ where ϕ has good reduction. Let $P_{\mathfrak{p}} \in A[X]$ be the characteristic polynomial of the $\mathfrak{p}$-Frobenius on the $\mathfrak{l}$-adic Tate module, where $\mathfrak{l}$ is a prime ideal of A with $\mathfrak{p} \nmid \mathfrak{l}$ (this polynomial is independent of the choice of $\mathfrak{l}$). Write:

$$P_{\mathfrak{p}}(X) := \sum_{0 \leq i \leq r} p_{\mathfrak{p},i} X^i = X^r - Q_{\mathfrak{p}}(X),$$

where $\deg(Q_{\mathfrak{p}}) < r$. Let $p_{\mathfrak{p}} := p_{\mathfrak{p},0} \in A$, which satisfies:

$$\deg(p_{\mathfrak{p}}) = \deg(\mathfrak{p}).$$

Let k_ϕ^{s} be the separable closure of k_ϕ and for a place $\mathfrak{P}' \mid \mathfrak{p}$ in k_ϕ^{s}, let $\sigma_{\mathfrak{P}'} \in \mathrm{Gal}(k_\phi^{\mathrm{s}}/k_\phi)$ a Frobenius element associated to $\mathfrak{P}'$. Now, if we let $\mathfrak{P} \mid \mathfrak{p}$ in $\bar{k_\phi}$, the prime $\mathfrak{P}$ is totally ramified over a prime $\mathfrak{P}'$ of k^{s}, and we define $\sigma_{\mathfrak{P}}$ to be the unique extension of $\sigma_{\mathfrak{P}'}$ to the field of definition of $\mathfrak{P}$.

The next proposition shows how to extrapolate the vanishing properties of G in the general case. The main idea is that $P_{\mathfrak{p}}$ vanishes on a conjugate of x modulo a prime above $\mathfrak{p}$ (by Cayley-Hamilton), providing a useful metric estimate.

Proposition 5.1. *Let P an integer large enough in terms of ϕ, and T' such that:*

$$h(F) + 2L\big(q^{r(N+P)}\hat{h}_\phi(x) + c(\phi)\big) + T'Nh(\phi) < \frac{P}{DD_\phi}\left(\frac{T-T'}{D_{\mathrm{i}}}\right). \tag{11}$$

For any prime $\mathfrak{p} \subset B$ of good reduction with $\deg(\mathfrak{p}) = P$ and for any place $\mathfrak{P} \mid \mathfrak{p}$ such that x is integral at $\mathfrak{P}$, the polynomial G vanishes at $\psi_{\mathfrak{P}}(x) := Q_{\mathfrak{p}}(\sigma_{\mathfrak{P}})(x)$ with multiplicity $\geq T'$.

Proof. We proceed by contradiction, following lines similar to the proof of Proposition 4.4. Suppose that there is a place $\mathfrak{P}$ of $k_\phi(x)$ above a good prime $\mathfrak{p}$ of B with stated degree as well as $0 \leq k \leq T'$ such that:

$$y := \partial_k G(\psi_{\mathfrak{P}}(x)) \neq 0.$$

The minimal polynomial Δ of x over k_ϕ has order D_{i} at x. Once again, there is $\ell \geq \frac{T-k}{D_{\mathrm{i}}}$ such that:

$$\Delta^\ell \mid \partial_k G \text{ in } B_{\mathfrak{p}}(X).$$

If x is separable over k_ϕ, we have the following congruence in the localization $\mathcal{O}_{\mathfrak{P}}$ of $\mathcal{O}_{k_\phi(x)}$ at $\mathfrak{P}$ (by the theorem of Cayley-Hamilton and [17], Theorem 4.12.12):

$$P_{\mathfrak{p}}(\sigma_{\mathfrak{P}})(x) \equiv 0 \pmod{\mathfrak{P}}.$$

For general x, the same equality holds with x replaced by x^α, where α is the smallest power of q^{D_ϕ} such that x^α is separable over k_ϕ, and $\mathfrak{P}$ replaced by $\mathfrak{P}^{D_{\mathrm{i}}}$ (by Lemma 3.2). We use the properties of characteristic p and remark that the valuation v corresponding to $\mathfrak{P}$ takes integral values to find once again:

$$P_{\mathfrak{p}}(\sigma_{\mathfrak{P}})(x) \equiv 0 \pmod{\mathfrak{P}},$$

which in turn implies:

$$\psi_{\mathfrak{P}}(x) \equiv \sigma_{\mathfrak{P}}^r(x) \pmod{\mathfrak{P}}.$$

The polynomial Δ also vanishes at the conjugate $\sigma_{\mathfrak{P}}^r(x)$ of x; therefore:

$$\Delta(\psi_{\mathfrak{P}}(x)) \equiv \Delta(\sigma_{\mathfrak{P}}^r(x)) \equiv 0 \pmod{\mathfrak{P}},$$

and we see that $v(y) \geq \ell$. By the product formula (1):

$$\begin{aligned} 0 &= \sum_{w \in M(k_\phi(x))} f_w w(y) \\ &\geq f_v \ell - \sum_{v \nmid \mathfrak{p}} f_v \max\{0, -v(y)\}, \end{aligned}$$

and thus:

$$\deg(\mathfrak{p})\ell \leq [k_\phi(x) : k]h(y).$$

Using classical bounds on the zeros of $P_{\mathfrak{p}}$ (see [7], 4.2, p. 1063) and the invariance of the canonical height under conjugation, we get:

$$\hat{h}_\phi(\psi_{\mathfrak{P}}(x)) \leq \sum_{i=0}^{r-1} q^{r\deg(p_{\mathfrak{p},i})}\hat{h}_\phi(x) \leq \sum_{i=0}^{r-1} q^{i\deg(\mathfrak{p})}\hat{h}_\phi(x) \leq q^{r\deg(\mathfrak{p})}\hat{h}_\phi(x).$$

The height of y is bounded using (7), and we derive:

$$\begin{aligned}\left(\frac{T-k}{D_{\mathrm{i}}}\right)P \leq \deg(\mathfrak{p})\ell &\leq DD_\phi\Big(h(F)+2L\big(q^{rN}\hat{h}_\phi(\psi_{\mathfrak{P}}(x))+c(\phi)\big)+T'Nh(\phi)\Big)\\ &\leq DD_\phi\Big(h(F)+2L\big(q^{r(N+P)}\hat{h}_\phi(x)+c(\phi)\big)+T'Nh(\phi)\Big),\end{aligned}$$

so:

$$h(F)+2L\big(q^{r(N+P)}\hat{h}_\phi(x)+c(\phi)\big)+T'Nh(\phi) \geq \frac{P}{DD_\phi}\left(\frac{T-T'}{D_{\mathrm{i}}}\right),$$

which is a contradiction. □

5.2. **Counting the roots.** The last step in the diophantine process is to count the roots of G as deduced from the previous proposition, and to compare this result to the estimate for the degree of G that was found earlier. We combine a box principle with the classical estimates on the roots of the characteristic polynomial of the Frobenius in order to show that the extrapolation set is big enough. Again, we fix P and T' as in Proposition 5.1.

Lemma 5.2. *Suppose that $D_\phi \mid P$ and that $q^{rN} \geq L$. Then:*

$$q^{\frac{P}{r}}\frac{T'}{P} \quad \ll_\phi \quad Lq^{rN}. \tag{12}$$

Proof. Again, the polynomial G is not zero, and:

$$\deg(G) < L(q^{rN}+1).$$

We can therefore focus on the number of roots of G (with multiplicity). For P a multiple of D_ϕ large enough, the set S_P of primes in B with good reduction and degree P satisfies (see [27], Theorem 5.12):

$$M_P := |S_P| \gg_\phi \frac{q^P}{P}.$$

Let $S'_P := \{p_{\mathfrak{p}}, \mathfrak{p} \in S_P\}$. There are at most D_ϕ prime ideals in B above a prime of A, so we get:

$$|S'_P| \geq \frac{|S_P|}{D_\phi}.$$

Now, the number of elements of A with degree

$$< \left[\frac{(r-1)P+\log_q(2r)}{r}\right]+1$$

is bounded by:

$$q^{\left[\frac{(r-1)P+\log_q(2r)}{r}\right]+1}.$$

If we let:

$$M := \left[M_P q^{-1-\left[\frac{(r-1)P+\log_q(2r)}{r}\right]}D_\phi^{-1}\right],$$

Dirichlet's box principle shows that there exist $\mathfrak{p}_1,\ldots,\mathfrak{p}_M \in S_P$ such that:

$$\forall\, 1 \leq i < j \leq M \ : \ \deg(p_{\mathfrak{p}_i}-p_{\mathfrak{p}_j}) \geq \left[\frac{(r-1)P+\log_q(2r)}{r}\right]+1.$$

For $1 \leq i \leq M$, we let $\mathfrak{P}_i | \mathfrak{p}_i$ be a place of $k_\phi(x)$. We claim that the $(\psi_{\mathfrak{P}_i}(x))_{1 \leq i \leq M}$ are pairwise distinct. If not, let $i \neq j$ such that $\psi_{\mathfrak{P}_i}(x) = \psi_{\mathfrak{P}_j}(x)$. Then:

$$\phi_{p_{\mathfrak{p}_i} - p_{\mathfrak{p}_j}}(x) = \sum_{1 \leq k \leq r-1} \phi_{p_{\mathfrak{p}_j}, k}\big(\sigma^k_{\mathfrak{P}_j}(x)\big) - \phi_{p_{\mathfrak{p}_i}, k}\big(\sigma^k_{\mathfrak{P}_i}(x)\big).$$

We compute the canonical height on both sides and deduce (by [7], 4.2, p. 1063 once again):

$$\begin{aligned} q^{r \deg(p_{\mathfrak{p}_i} - p_{\mathfrak{p}_j})} \hat{h}_\phi(x) &\leq 2\hat{h}_\phi(x) \sum_{1 \leq k \leq r-1} q^{kP} \\ &\leq 2(r-1) q^{(r-1)P} \hat{h}_\phi(x). \end{aligned}$$

Since x is not torsion, we get:

$$q^{r \deg(p_{\mathfrak{p}_i} - p_{\mathfrak{p}_j})} \leq q^{(r-1)P + \log_q(2(r-1))},$$

which is a contradiction. We can now compare the degree of G with the number of its roots with multiplicity, which yields:

$$q^{\frac{P}{r}} \frac{T'}{P} \ll_\phi T'M \leq 2Lq^{rN},$$

so the announced inequality holds. □

5.3. **Bounding the height in the general case.** Let us finally state and prove our lower bound for the canonical height in general Drinfeld modules. The parameters are chosen following a procedure close to that of the CM case. The main difference is that the $\mathfrak{p}$-adic properties at finite places $\mathfrak{p}$ are much weaker.

In order to ensure (11), we have to take T large enough. In fact, the quotient $T/(DD_{\mathrm{i}})$ should dominate L as well as the contribution $D_{\mathrm{s}}T^2/L^2$ from $h(F)$. This determines L and T in terms of D and D_{i}, and then T' so as to satisfy (11). Again, the parameter N is chosen according to the condition in Lemma 5.2. We finally take P large enough to invalidate (12).

Proposition 5.3. *Let $x \in \bar{k}$ not torsion with degree $D := D_{\mathrm{s}}D_{\mathrm{i}}$. Then:*

$$\hat{h}_\phi(x) \gg_\phi \frac{1}{(D^3 D_{\mathrm{i}})^{r^2+1} \log(D)^{2r^2+r}}.$$

Proof. We suppose as usual that the degrees are taken over k_ϕ and that D is large enough in terms of ϕ. Let us proceed by contradiction. We set:

$$L := D^3 D_{\mathrm{i}}\ ,\ T := D_{\mathrm{i}}^2 \left[\frac{D^4}{\sqrt{\log(D)}} \right],\ \text{and } N \in \mathbb{N} \text{ such that } L \leq q^{rN} \ll_\phi L;$$

this last condition is satisfied for D large enough. Also fix $\mathcal{N} \in A$ such that $\deg(\mathcal{N}) = N$. The assumption (6) holds, so there is $F \in A[X, Y]$ such that

$$G(X) := F(X, \phi_{\mathcal{N}}(X))$$

vanishes at x with order T, and:

$$\begin{aligned} h(F) &\ll_\phi \frac{D_{\mathrm{s}}T}{L^2} \Big(Lq^{Nr} \hat{h}_\phi(x) + L + TN \Big) \\ &\ll_\phi \frac{DT}{D_{\mathrm{i}}L^2} \left(L + T\log(D) \right) \ll_\phi \frac{T\sqrt{\log(D)}}{DD_{\mathrm{i}}}. \end{aligned}$$

We want to apply Proposition 5.1 with:

$$T' := \left[\frac{T}{DD_{\mathrm{i}}\sqrt{\log(D)}}\right] \leq \frac{T}{2},$$

this inequality being true at least for D large enough, and $P \in \mathbb{N}$ a multiple of D_ϕ such that:

$$L^r \log(D)^{2r+1} \ll_\phi q^P \leq L^r \log(D)^{2r+1}.$$

Because P is supposed to be large enough in terms of ϕ, we can assume x to have non-negative valuation above all places of B with degree P. Otherwise, Lemma 3.1 yields an even better lower bound for $\hat{h}_\phi(x)$. We have:

$$h(F) + 2L\big(q^{r(N+P)}\hat{h}_\phi(x) + c(\phi)\big) + T'Nh(\phi) \quad \ll_\phi \quad \frac{T}{DD_{\mathrm{i}}}\sqrt{\log(D)},$$

so for D, and thus P, large enough:

$$h(F) + 2L\big(q^{r(N+P)}\hat{h}_\phi(x) + c(\phi)\big) + T'Nh(\phi) \quad < \quad \frac{P}{DD_\phi}\left(\frac{T-T'}{D_{\mathrm{i}}}\right).$$

Therefore, condition (11) holds and G vanishes at $\psi_{\mathfrak{P}}(x)$ with multiplicity $\geq T'$ for any prime $\mathfrak{P}|\mathfrak{p}$ in $k_\phi(x)$ and $\mathfrak{p}$ a prime in B of good reduction with $\deg(\mathfrak{p}) = P$. The assumption of Lemma 5.2 is satisfied and we have:

$$q^{rN}L \ll_\phi L^2,$$

whereas:

$$T'\frac{q^{\frac{P}{r}}}{P} \gg_\phi T'L\log(D)^{1+\frac{1}{r}} \gg_\phi \frac{TL\log(D)^{1+\frac{1}{r}}}{DD_{\mathrm{i}}\sqrt{\log(D)}} \gg_\phi L^2\log(D)^{\frac{1}{r}}.$$

This contradicts (12) for D large enough, and the theorem is completely proved. □

Remark. An analogous bound has been found by Masser for the canonical height on abelian varieties, as a consequence of his counting theorem for points of small height (see [23]). An adaptation of this counting result to Drinfeld modules might bring a bound of the same kind, but with exponents possibly improved.

References

1. F. Amoroso and S. David, *Le problème de Lehmer en dimension supérieure*, J. Reine Angew. Math. **513** (1999), 145–179.
2. F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), 260–272.
3. F. Amoroso and E. Viada, *Small points on rational subvarieties of tori*, Comment. Math. Helv. **87** (2012), no. 2, 355–383.
4. H. Bauchère, *Minoration de la hauteur canonique pour les modules de Drinfeld à multiplications complexes*, J. Number Theory **157** (2015), 291–328.
5. M. Brown, *Singular moduli and supersingular moduli of Drinfeld modules*, Invent. Math. **110** (1992), 419–439.
6. S. David and M. Hindry, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C.M.*, J. Reine Angew. Math. **529** (2000), 1–74.
7. S. David and A. Pacheco, *Le problème de Lehmer abélien pour un module de Drinfeld*, Int. J. Number Theory **4** (2008), no. 6, 1043–1067.
8. L. Demangos, *Lehmer problem and Drinfeld modules*, Preprint (2015), 52 pages.
9. L. Denis, *Hauteurs canoniques et modules de Drinfeld*, Math. Ann. **294** (1992), 213–223.
10. ———, *Problèmes diophantiens sur les t-modules*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 97–110.

11. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.
12. M. D. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, 2008.
13. A. Galateau and A. Pacheco, *Hauteur et torsion des modules de Drinfeld de rang* 2, Preprint (2015), 27 pages.
14. E.-U. Gekeler, *On finite Drinfeld modules*, J. Algebra **141** (1991), no. 1, 187–203.
15. D. Ghioca, *The Lehmer inequality and the Mordell-Weil theorem for Drinfeld modules*, J. Number Theory **122** (2007), no. 1, 37–68.
16. ———, *The local Lehmer inequality for Drinfeld modules*, J. Number Theory **123** (2007), no. 2, 426–455.
17. D. Goss, *Basic structures of function field arithmetic*, Springer Verlag, 1998.
18. P. Habegger, *Small height and infinite nonabelian extensions*, Duke Math. J. **162** (2013), no. 11, 2027–2076.
19. D. R. Hayes, *Explicit class field theory in global function fields*, Studies in algebra and number theory, Adv. in Math. Suppl. Stud., vol. 6, Academic Press, 1979, pp. 173–217.
20. D.R. Hayes, *A brief introduction to Drinfeld modules*, The Arithmetic of Function Fields. Ohio State Univ. Math. Res. Inst. Publ. **2** (1992), 1–32.
21. M. Laurent, *Minoration de la hauteur de Néron-Tate*, Séminaire de théorie des nombres de Paris, 1981-1982, Progr. Math. **38** (1983), 137–152.
22. D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461–479.
23. D. Masser, *Small values of the quadratic part of the Néron-Tate height on an abelian variety*, Compos. Math. **53** (1984), 153–170.
24. ———, *Letter to Daniel Bertrand*, (1986).
25. B. Poonen, *Local height functions and the Mordell-Weil theorem for Drinfeld modules*, Compositio Math. **97** (1995), no. 3, 349–368.
26. ———, *Drinfeld modules with no supersingular primes*, Int. Math. Res. Not. **3** (1998), 151–159.
27. M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.
28. A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399.

Université de Caen
E-mail address: vincent.bosser@unicaen.fr

Université de Franche-Comté
E-mail address: aurelien.galateau@univ-fcomte.fr