EXPLICIT ISOGENY THEOREMS FOR DRINFELD MODULES

IMIN CHEN* AND YOONJIN LEE**

Abstract. Let $F = \mathbb{F}_q(T)$, $A = \mathbb{F}_q[T]$. Given two non-isogenous rank r Drinfeld A-modules ϕ and ϕ' over K, where K is a finite extension of F, we obtain a partially explicit upper bound (dependent only on ϕ and ϕ') on the degree of primes $\wp$ of K such that $P_\wp(\phi) \neq P_\wp(\phi')$, where $P_\wp(*)$ denotes the characteristic polynomial of Frobenius at $\wp$ on a Tate module of $*$. The bounds are completely explicit in terms of the defining coefficients of ϕ and ϕ', except for one term, which can be made explicit in the case of $r = 2$. An ingredient in the proof of the partially explicit isogeny theorem for general rank is an explicit bound for the different divisor of torsion fields of Drinfeld modules which detects primes of potentially good reduction.

Our results are a Drinfeld module analogue of [16], but the results we obtain are unconditional because GRH for function fields holds.

1. Introduction

Let $A = \mathbb{F}_q[T]$, $F = \mathbb{F}_q(T)$, $\overline{F}$ be a fixed algebraic closure of F, K a finite extension of F in $\overline{F}$, $\overline{K}$ the algebraic closure of K in $\overline{F}$, $\mathcal{O}$ the ring of integers of K, and $\mathbb{F}_q$ a finite field of order q.

By a prime $\wp$ (or place) of K, we mean a discrete valuation ring R with field of fractions K and maximal ideal $\wp$, and v denotes the discrete valuation associated to a prime $\wp$ of K. For each place v of K, we fix a choice of $\overline{K}_v$, and extend v to $\overline{K}_v$, which by abuse of notation, we also call v. Also, when we speak of a finite extension of K_v, we assume they are initially given as subfields of $\overline{K}_v$.

Let ∞ be the infinite prime of F with corresponding discrete valuation $v_\infty(f/g) = \deg g - \deg f$, where $f, g \in A$. Let S_∞^K be the set of the infinite primes of K lying over ∞, and let $\bar{\infty} \in S_\infty^K$ have corresponding discrete valuation $v_{\bar{\infty}}$.

Let τ be the map which raises an element to its q-th power. A *Drinfeld A-module ϕ over K* is given by an $\mathbb{F}_q$-algebra homomorphism $i : A \to K$ and an $\mathbb{F}_q$-algebra

2000 *Mathematics Subject Classification.* Primary: 11G09, Secondary: 11R58.

Key words and phrases. Drinfeld modules, Galois representations, Chebotarev Density Theorem, Isogeny Theorem, Different, Ramification.

The author* was supported by NSERC and the author** is the corresponding author and supported by Priority Research Centers Program through the NRF funded by the Ministry of Education, Science and Technology(2010-0028298) and by the NRF grant funded by the Korea government(MEST)(2011-0015684).

homomorphism

$$\phi : A \to K\{\tau\}$$

such that ϕ_a has constant term $i(a)$ for any $a \in A$, and the image of ϕ is not contained in K.

A rank r Drinfeld A-module ϕ over K is completely determined by

$$\phi_T = i(T) + a_1(\phi)\tau + \cdots + a_{r-1}(\phi)\tau^{r-1} + \Delta(\phi)\tau^r,$$

where $a_i(\phi), a_r = \Delta(\phi) \in K$ for $1 \le i \le r-1$. We call $\Delta(\phi)$ the *discriminant* of ϕ.

For any *monic* $a \in \mathbb{F}_q[T]$, we have

$$\phi_a = i(a) + \sum_{i=1}^{M-1} a_i(\phi, a)\tau^i + \Delta(\phi)^{(q^M-1)/(q^r-1)}\tau^M, \tag{1}$$

for some $a_i(\phi, a) \in K$, where $M = r \deg_K a$.

For any $a \in A, a \neq 0$, we define the A-module of *a-torsion points* as

$$\phi[a] = \{\lambda \in \overline{K} \mid \phi_a(\lambda) = 0\}.$$

If I is a non-zero ideal of A, we similarly define the A-module of *I-torsion points*

$$\phi[I] = \{\lambda \in \overline{K} \mid \phi_a(\lambda) = 0 \text{ for every } a \in I\}.$$

We have that $\phi[a] \simeq (A/aA)^r$ if ϕ is of rank r [13, Prop. 12.4]. Let $K_{\phi,a} := K(\phi[a])$ be the field obtained by adjoining a-torsion points of ϕ to K and let $K_{\phi,I} := K(\phi[I])$.

In the following, we briefly explain the definition of good reduction of a Drinfeld module. For more details, refer to [9, 21]. Let ϕ be a rank r Drinfeld A-module over K and let $\wp$ be a prime of K. Let $\mathcal{O}_\wp$ be the valuation ring of $\wp$ with the maximal ideal $\wp$ and residue field $\mathbb{F}_\wp := \mathcal{O}_\wp/\wp$. We say that ϕ has *integral coefficients* at $\wp$ if ϕ_a has coefficients in $\mathcal{O}_\wp$ for all $a \in A$ and the reduction modulo $\wp$ of these coefficients defines a Drinfeld module over $\wp$. The reduced Drinfeld module is denoted by $\phi^\wp$.

We say that ϕ has *good reduction* at $\wp$ if there exists a Drinfeld module ψ over K which is isomorphic to ϕ over K and ψ has integral coefficients at $\wp$, and $\psi^\wp$ is a Drinfeld module of rank r.

By [20] (cf. [9, Theorem 4.10.5], cf. also [10, Theorem 3.2.3] for one direction), we have that ϕ has good reduction at $\wp$ if and only if the G_K-module $\phi[\mathfrak{L}^\infty] := \cup_{m\ge1}\phi[\mathfrak{L}^m]$ is unramified at $\wp$, where G_K is the absolute Galois group of K and $\mathfrak{L}$ is a prime ideal of A different from $\wp$. This is the analog for Drinfeld modules of the classical result of Ogg-Néron-Shafarevich in the theory of abelian varieties.

If ϕ is a Drinfeld A-module defined over K, and all its defining coefficients $a_i(\phi)$ lie in $\mathcal{O}$, then we say that ϕ *integral over* $\mathcal{O}$. If ϕ is integral over $\mathcal{O}$, then it has good reduction outside any set of primes S of K which includes the primes lying over ∞

and the primes dividing the discriminant $\Delta(\phi)$ of ϕ. In particular, the G_K-modules $\phi[\mathfrak{L}^\infty]$ and $\phi[\mathfrak{L}]$ are unramified outside $S \cup \{\text{primes of } K \text{ lying over } \mathfrak{L}\}$.

Let $\wp$ be a finite prime of K. The $\wp$-torsion points of ϕ in $\overline{K}$ give rise to a representation

$$\rho_{\phi,\wp} : G_K \to \mathrm{Aut}_{A/\wp}(\phi[\wp]) \cong \mathrm{GL}_r(A/\wp A)$$

where G_K is the absolute Galois group of K. Let $\mathrm{Frob}_\wp \in \mathrm{Gal}(\overline{K}/K)$ denote a Frobenius conjugacy class at an unramified prime $\wp$ of K. If ϕ has good reduction at $\wp$, then the $\mathfrak{L}$-adic Tate module $T_{\mathfrak{L}}(\phi)$ of ϕ is unramified at $\wp$ if $\wp \neq \mathfrak{L}$. Let $a_\wp(\phi)$ denote the trace of $\mathrm{Frob}_\wp$ on the $T_{\mathfrak{L}}(\phi)$, and more generally, let $P_\wp(\phi)(X)$ be the characteristic polynomial of $\mathrm{Frob}_\wp$ on the $T_\ell(\phi)$. It is known that $a_\wp(\phi)$ and $P_\wp(\phi)(X)$ are independent of $\mathfrak{L}$ [9, Theorem 4.12.12].

The following is the Tate conjecture for rank r Drinfeld A-modules over K which is proven in [18].

Theorem 1.1. *Let ϕ, ϕ' be rank r Drinfeld A-modules over K and $A_{\mathfrak{L}}$ be the $\mathfrak{L}$-adic completion of A. Then the natural homomorphism*

$$\mathrm{Hom}_K(\phi, \phi') \otimes_A A_{\mathfrak{L}} \to \mathrm{Hom}_{A_{\mathfrak{L}}[G_K]}(T_{\mathfrak{L}}(\phi), T_{\mathfrak{L}}(\phi'))$$

is an isomorphism, where $T_{\mathfrak{L}}(*)$ is the $\mathfrak{L}$-adic Tate module of $*$.

A consequence of the Tate conjecture is the isogeny theorem which states that two Drinfeld A-modules ϕ, ϕ' over K are K-isogenous if and only if $P_\wp(\phi)(X) = P_\wp(\phi')(X)$ for all but finitely many primes $\wp$ [17, Proposition 3.1].

We prove the following partially explicit and effective version of the isogeny theorem for rank r Drinfeld A-modules over K. For a Drinfeld A-module ϕ and a place $\wp$ of K, define

$$\tau_{K,\wp}(\phi) = \inf \left\{ \frac{v_\wp(a_i(\phi))}{q^i - 1} : i = 1, \ldots, r \right\}.$$

For any extension L/F, let $\gamma_L = [\mathbb{F}_L : \mathbb{F}_q]$. It is known that the constant field of $K_{\phi,\mathrm{tor}} := K(\phi[a] : a \in A \text{ non-zero})$ is finite over $\mathbb{F}_q$ (cf. [4, Lemma 3.2]) so we may define $\gamma_\phi = \gamma_{K_{\phi,\mathrm{tor}}}$. More precisely, let $g_{\phi,\bar\infty} = [K_{\bar\infty}(\Lambda_{\phi,\bar\infty}) : K_{\bar\infty}]$, where $\Lambda_{\phi,\bar\infty}$ is the lattice associated to the uniformization of ϕ over $C_{\bar\infty}$. Then we have that

$$\gamma_\phi \leq g_\phi = min \left\{ g_{\phi,\bar\infty} : \bar\infty \mid \infty \right\}.$$

One can bound $g_{\phi,\bar\infty}$ using knowledge of the successive minima of the lattices $\Lambda_{\phi,\bar\infty}$ associated to ϕ [6, Proposition 4(i)]. Unfortunately, an explicit bound for these successive minima is not currently known except in the case of rank ≤ 2 [2], so this term is currently inexplicit in general.

Throughout, $\ln x$ denotes the natural logarithm of x, $\log_q x$ the logarithm of x to base q, and $\log_q^* x = \log_q \max\{x, 1\}$.

Theorem 1.2. *Let ϕ_1, ϕ_2 be rank r Drinfeld A-modules which are integral over $\mathcal{O}$ and not K-isogenous. Let S be the set consisting of the primes of K lying over the prime ∞ and the primes dividing $\Delta(\phi_1)\Delta(\phi_2)$. Suppose $\wp \notin S$ is a prime of K of least degree such that $P_\wp(\phi_1) \neq P_\wp(\phi_2)$. Then*

$$(2)\qquad \deg_K \wp \leq \max\left\{\frac{4}{m_0}\left(C_{q,r} + W + c_r s_{q,r} \log_q W\right),\ s \max\left\{1 + 2\log_q s, 7\right\}\right\},$$

where

$$\begin{aligned}
s &= \text{ the geometric extension degree of } K/F \\
m_0 &= \gamma_K \\
c_r &= 2r^2 + r + 1 \\
d_r &= c_r + \log_q 86rs^2(g+1) \\
s_{q,r} &= \frac{\ln(qd_r)}{\ln(qd_r) - 1} \\
C_{q,r} &= \log_q 86rs^2(g+1) + c_r\left(1 + s_{q,r}\log_q \frac{4}{m_0} + \log_q d_r\right) + c_r s_{q,r} \log_q \log_q d_r \\
a_r(\phi_i) &= \Delta(\phi_i), i = 1, 2 \\
W &= \log_q^* \left(\Lambda_K(\phi_1, \phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2)\right) + g_{\phi_1} g_{\phi_2} m_0 \\
\Lambda_K(\phi_1, \phi_2) &= -\sum_v \tau_{K,v}(\phi_1) \deg_K v - \sum_v \tau_{K,v}(\phi_2) \deg_K v \\
\deg_K \operatorname{rad}_K x &= \sum_{v(x)\neq 0} \deg_K v
\end{aligned}$$

(the sums are over every place v of K).

Note that any Drinfeld A-module defined over K is isomorphic over K to a Drinfeld A-module which is integral over $\mathcal{O}$. In order to reduce the bounds given by the above theorem, in particular the quantity $\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2)$, one should use minimal models of ϕ_1 and ϕ_2 (cf. [19, Section 2]).

The proof follows the strategy in [16] as adapted to the Drinfeld module situation with the notable difference that the effective Chebotarev Density Theorem we use [12] is stronger and unconditional because GRH holds for function fields. Also, unlike the number field case, it is necessary to deal with wild ramification when bounding the different divisor. The bound we obtain on the different divisor is completely explicit in terms of the defining coefficients of the Drinfeld modules involved, unlike the results in [6], which are effective but not explicit. In addition, the bounds are sensitive to primes of potentially good reduction, unlike the bounds in [17].

We discuss some of the differences between our method and [6] in more detail later in Section 7. In the rank 2 case, it is possible to make explicit the quantities involved in Gardeyn's bounds for the different divisor of torsion fields, by determining the Newton polygons of exponential functions attached to Drinfeld modules [2]. However, the computation of Newton polygons grows in complexity for higher rank, so new techniques using weaker information will likely be required to obtain explicit bounds for successive minima so we can apply the bounds of [6] for the different divisor and g_ϕ. Further remarks about this will be made in the concluding section 7.

2. Preliminaries

Let L be a finite extension of K, and $\mathcal{O}_L$ be the maximal order of L, i.e. the integral closure of $\mathcal{O}$ in L. The *constant field* $\mathbb{F}_L$ of L is the algebraic closure of $\mathbb{F}_q$ in L. The *geometric extension degree* of L/K is the degree of L/K', where K' is the maximal constant field extension of K in L (i.e. $[L : K]/[\mathbb{F}_L : \mathbb{F}_K]$). We say L/K is a *geometric extension* if $K = K'$.

For a prime ideal $\mathfrak{B}$ of $\mathcal{O}_L$, we let $\deg_L \mathfrak{B}$ be the $\mathbb{F}_L$-dimension of the residue class field $\mathbb{F}_{L,\mathfrak{B}} := \mathcal{O}_L/\mathfrak{B}$ of $\mathfrak{B}$, extending this to a general ideal I of $\mathcal{O}_L$ by additivity on products. For a in $\mathcal{O}_L$, we define the degree of a by $\deg_L a := \deg_L(a)$, where (a) is the principal ideal of $\mathcal{O}_L$ generated by a.

More generally, let $\mathfrak{B}$ be a prime of L, $\mathcal{O}_{L,\mathfrak{B}}$ the valuation ring of $\mathfrak{B}$, and $\mathbb{F}_{L,\mathfrak{B}} := \mathcal{O}_{L,\mathfrak{B}}/\mathfrak{B}$ the residue class field of $\mathfrak{B}$. Then the *degree* of $\mathfrak{B}$ is defined to be $\deg_L \mathfrak{B} := [\mathbb{F}_{L,\mathfrak{B}} : \mathbb{F}_L]$, the $\mathbb{F}_L$-dimension of $\mathbb{F}_{L,\mathfrak{B}}$. We extend the definition by linearity to a divisor $\mathfrak{D} = \sum_{\mathfrak{B}} n_{\mathfrak{B}}\mathfrak{B}$ of L by $\deg_L \mathfrak{D} = \sum_{\mathfrak{B}} n_{\mathfrak{B}} \deg_L \mathfrak{B}$. The *finite part* $\mathfrak{D}_0$ of a divisor $\mathfrak{D} = \sum_{\mathfrak{B}} n_{\mathfrak{B}}\mathfrak{B}$ is the divisor $\sum_{\mathfrak{B}\nmid\infty} n_{\mathfrak{B}}\mathfrak{B}$.

Let $i_{L/K} : \mathrm{Div}(K) \to \mathrm{Div}(L)$ be the *conorm map* from divisors on K to divisors on L, defined by

$$i_{L/K}(\wp) = \sum_{\mathfrak{B}|\wp} e(\mathfrak{B}/\wp)\mathfrak{B}$$

for every prime $\wp$ of K, and then extended by linearity, where $e(\mathfrak{B}/\wp)$ denotes the *ramification index* of $\mathfrak{B}$ over $\mathfrak{B}$.

For $\mathfrak{B}$ a prime of L lying over the prime $\wp$ of K, denote by $f(\mathfrak{B}/\wp)$ the inertia degree of $\mathfrak{B}$ over $\wp$.

Lemma 2.1. *Let L/K be a finite extension, $\mathfrak{D}$ a divisor of K, and $\mathfrak{B}$ is a prime of L lying over the prime $\wp$ of K. Then*

$$\deg_L i_{L/K}\mathfrak{D} = n' \deg_K \mathfrak{D},$$
$$\deg_L \mathfrak{B} = \frac{f(\mathfrak{B}/\wp)}{[\mathbb{F}_L : \mathbb{F}_K]} \deg_K \wp$$

where n' is the geometric extension degree of L/K.

Proof. cf. [13, Proposition 7.7] □

Let L/K be a finite extension. Writing divisors in terms of places instead of primes, the *different divisor* $\mathfrak{D}(L/K)$ of L/K is defined as

$$\mathfrak{D}(L/K) = \sum_w w(D(L_w/K_v))w,$$

and its degree is given by

$$\deg_L \mathfrak{D}(L/K) = \sum_w w(D(L_w/K_v)) \deg_L w,$$

where w ranges through all normalized places of L, and $D(L_w/K_v)$ is the *different ideal* of L_w/K_v.

For convenience, we also define *the degree with respect to* K of $\mathfrak{D}(L/K)$ as

$$\deg_K \mathfrak{D}(L/K) = \sum_v \max\{v(D(L_w/K_v)) : w|v\} \deg_K v,$$

where v ranges through all normalized places of K. Similarly, we define the degree with respect to K of $\mathfrak{D}_0(L/K)$ as

$$\deg_K \mathfrak{D}_0(L/K) = \sum_{v \nmid \infty} \max\{v(D(L_w/K_v)) : w|v\} \deg_K v.$$

Lemma 2.2. *Let L/K be a finite extension. Then*

$$\deg_L \mathfrak{D}(L/K) \leq n' \deg_K \mathfrak{D}(L/K),$$

where n' is the geometric extension degree of L/K.

Proof. By the definition, we have

$$\begin{aligned}
\deg_L \mathfrak{D}(L/K) &= \sum_w w(D(L_w/K_v)) \deg_L w \\
&= \sum_v \sum_{w|v} w(D(L_w/K_v)) \deg_L w \\
&= \sum_v \sum_{w|v} v(D(L_w/K_v))e(w/v)f(w/v) \frac{1}{[\mathbb{F}_L : \mathbb{F}_K]} \deg_K v \\
&\leq \frac{1}{[\mathbb{F}_L : \mathbb{F}_K]} \sum_v \max\{v(D(L_w/K_v)) : w|v\} \sum_{w|v} e(w/v)f(w/v) \deg_K v \\
&= n' \sum_v \max\{v(D(L_w/K_v)) : w|v\} \deg_K v = n' \deg_K \mathfrak{D}(L/K),
\end{aligned}$$

where $\mathbb{F}_L$ and $\mathbb{F}_K$ are the constant fields of L and K respectively, $f(w/v)$ denotes the *relative degree* of w over v, and we use the identity

$$[L : K] = \sum_{w|v} e(w/v)f(w/v),$$

which is valid as our constant fields are finite and hence perfect [13, Proposition 7.4]. □

Lemma 2.3. *Let $M/L/K$ be a tower of finite separable extensions. Then the different divisor satisfies the following transitivity relation,*

$$\mathfrak{D}(M/K) = \mathfrak{D}(M/L) + i_{M/L}\mathfrak{D}(L/K).$$

Proof. Refer to [15, Proposition 8, Chapter III.4]. □

Lemma 2.4. *Let K be a local field with ring of integers $\mathcal{O}$ and L/K be a finite extension of K with ring of integers $\mathcal{O}_L$. Let $\alpha \in \mathcal{O}_L$ be such that $L = K(\alpha)$ and suppose $f(X) \in \mathcal{O}[X]$ is the minimal polynomial of α over K. Then the different ideal $D(\mathcal{O}_L/\mathcal{O})$ divides the ideal $(f'(\alpha))$, with equality holding if and only if $\mathcal{O}_L = \mathcal{O}[\alpha]$. Furthermore, we may replace $f(X)$ by any monic polynomial $g(X)$ in $\mathcal{O}[X]$ which α satisfies.*

Proof. cf. [15, Corollary 2, III.6]. For the final remark, we note that $g(X) = f(X)h(X)$ for some $g(X) \in \mathcal{O}[X]$ so that $(g'(\alpha)) = (f'(\alpha)h(\alpha)) \subseteq (f'(\alpha))$. □

Lemma 2.5. *Let E/K and L/K be finite extensions of local fields, with $\mathcal{O}$ the ring of integers of K, $\mathcal{O}_E$ the ring of integers of E, $\mathcal{O}_{EL}$ the ring of integers of EL, $\mathcal{O}_L$ the ring of integers of L.*

Then the different ideals satisfy $D(EL/L) \mid \mathcal{O}_{EL} \cdot D(E/K)$.

Proof. Suppose that $\mathcal{O}_E = \mathcal{O}_K[x]$ for some $x \in B$ so that $E = K(x)$ (cf. [15, Proposition 12, III.6]). Let $f \in \mathcal{O}_K[X]$ be the minimal polynomial of x over K.

Now $EL = K(x)L = K(x)$ and $x \in \mathcal{O}_{EL}$.

As $f \in \mathcal{O}[X]$ is monic and $x \in \mathcal{O}_{EL}$ is a root of f, we may apply Lemma 2.4 to get that $D(EL/L) \mid \mathcal{O}_{EL} \cdot f'(x)$. But as $\mathcal{O}_E = \mathcal{O}[x]$, we have that $D(E/K) = \mathcal{O}_E \cdot f'(x)$. Hence, $\mathcal{O}_{EL} \cdot f'(x) = \mathcal{O}EL \cdot \mathcal{O}_E \cdot f'(x) = \mathcal{O}_{EL} \cdot D(E/K)$. The result thus follows. □

Lemma 2.6. *Let E/K and L/K be finite extensions of global fields. Then*

$$\mathfrak{D}(EL/K) \leq i_{EL/E}\mathfrak{D}(E/K) + i_{EL/L}\mathfrak{D}(L/K).$$

Proof. This follows by localization and applying Lemma 2.3 and Lemma 2.5. □

3. Effective Chebotarev Density Theorem

Lemma 3.1. *Let K be a finite extension of $F = \mathbb{F}_q(T)$ with constant field $\mathbb{F}_q$, where $\mathbb{F}_q$ is a finite field of order q, and let g be the genus of K. Let $S(N)$ be the number of primes $\wp$ of K with $\deg_K \wp = N$. Then*

$$\mid S(N) - \frac{q^N}{N} \mid \leq \left(2g + 1 + \left(2g + \frac{3}{2}\right)\frac{4}{q}\right)\frac{q^{\frac{N}{2}}}{N}.$$

Proof. From the Prime Number Theorem for L [13, Theorem 5.12], we have that

$$S(N) = \frac{q^N}{N} + O\left(\frac{q^{\frac{N}{2}}}{N}\right).$$

We recall the proof in loc. cit. to make the constant explicit.

Let $Z_K(u)$ be the zeta function of K. Using the Euler product decomposition of $Z_K(u)$ and [13, Theorem 5.9], we obtain

$$Z_K(u) = \frac{\prod_{i=1}^{2g}(1 - \pi_i u)}{(1-u)(1-qu)} = \prod_{d=1}^{\infty}(1 - u^d)^{-S(d)}.$$

Taking the logarithmic derivative of both sides, multiplying by u, and equating coefficients of u^N yields the relation:

$$q^N + 1 - \sum_{i=1}^{2g} \pi_i^N = \sum_{d|N} dS(d).$$

Using the Möbius inversion formula yields

$$NS(N) = \sum_{d|N} \mu(d) q^{\frac{N}{d}} + 0 - \sum_{d|N} \mu(d) \left(\sum_{i=1}^{2g} \pi_i^{\frac{N}{d}} \right).$$

Following the argument in [13, Theorem 2.2], we obtain

$$\left| \sum_{d|N} \mu(d) q^{\frac{N}{d}} - q^N \right| \leq q^{\frac{N}{2}} + N q^{\frac{N}{3}}.$$

Similarly, using the Riemann Hypothesis [13, Theorem 5.10], we obtain

$$\left| \sum_{d|N} \mu(d) \left(\sum_{i=1}^{2g} \pi_i^{\frac{N}{d}} \right) \right| \leq 2g q^{\frac{N}{2}} + 2gN q^{\frac{N}{4}}.$$

It follows that

$$\left| NS(N) - q^N \right| \leq (2g+1) q^{\frac{N}{2}} + N q^{\frac{N}{3}} + 2gN q^{\frac{N}{4}}$$

so

$$\left| S(N) - \frac{q^N}{N} \right| \leq \frac{2g+1}{N} q^{\frac{N}{2}} + q^{\frac{N}{3}} + 2g q^{\frac{N}{4}} \leq \frac{q^{\frac{N}{2}}}{N} \left(2g + 1 + \frac{N}{q^{\frac{N}{6}}} + 2g \frac{N}{q^{\frac{N}{4}}} \right). \tag{3}$$

Since $\frac{x}{q^x} \leq \frac{1}{q}$ for $x \geq 1$, (3) is less than or equal to

$$\frac{q^{\frac{N}{2}}}{N} \left(2g + 1 + \left(2g + \frac{3}{2} \right) \frac{4}{q} \right).$$

□

The next theorem follows from the effective Chebotarev Density Theorem in [12, Theorem 1].

Theorem 3.2. *Let K be a finite extension of $F = \mathbb{F}_{q_0}(T)$ with constant field $\mathbb{F}_q$ and the genus g, where $q = q_0^{m_0}$. Let E be a finite Galois extension of K with Galois group G, $\mathbb{F}_{q^m}$ the algebraic closure of $\mathbb{F}_q$ in E, and $K' = \mathbb{F}_{q^m} K$ be the maximal constant field extension of K in E.*

Let $\mathcal{C} \subseteq G = \mathrm{Gal}(E/K)$ be a non-empty conjugacy class in G whose restriction to $\mathbb{F}_{q^m}/\mathbb{F}_q \cong K'/K$ is τ^k, where τ is the Frobenius map $\tau(x) = x^q$, and $\mathfrak{D}$ be the different divisor of E/K'. Let Σ be the divisor of K which is the sum of the primes of K which are ramified in E, and suppose Σ' is a divisor of K such that $\Sigma' \geq \Sigma$. Let $B = \max\{\deg_K \Sigma',\ \deg_E \mathfrak{D},\ 2|\mathrm{Gal}(E/K')| - 2,\ 1\}$.

If $N \geq \frac{2}{m_0} \log_{q_0} \frac{4}{3} \left(B^2 + B\left(2g + \frac{g}{m} + 3\right) + 2(5g + \frac{g}{m} + 3)\right)$ *and* $N \equiv k \pmod{m}$*, there is a prime* $\wp \notin \Sigma'$ *of* K *such that* $\deg_K \wp = N$ *and* $\mathrm{Frob}_\wp = \mathcal{C}$*.*

Proof. The situation at the outset is that we start with $F = \mathbb{F}_{q_0}(T)$ and K a finite extension of F with possibly larger constant field $\mathbb{F}_q$, where $q = q_0^n$. Next, we replace $F = \mathbb{F}_{q_0}(T)$ by $F = \mathbb{F}_q(T)$ so that K is a geometric extension of $F = \mathbb{F}_q(T)$. This allows us to use Lemma 3.1 without modification, but now q_0 is replaced by q.

Another remark is that if there exists a prime $\wp \notin \Sigma'$ of K such that $\deg_K \wp = N$ and $\mathrm{Frob}_\wp = \mathcal{C}$, then it follows that $\mathcal{C}$ restricted to $K'/K \cong \mathbb{F}_{q^m}/\mathbb{F}_q$ is τ^N by [12, Lemma 1]. Since $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ cyclic of order m, we have that $\tau^N = \tau^k$ in $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ if and only if $N \equiv k \pmod{m}$.

Let $\mathbb{F}_{q^m}$ be the algebraic closure of $\mathbb{F}_q$ in E so $K' := \mathbb{F}_{q^m}K$ and E/K' is a geometric extension. Let $\mathcal{D} := \deg_E \mathfrak{D}$ and $\delta' = \deg_K \Sigma'$. Let $\pi(N, \Sigma')$ be the number of primes $\wp \notin \mathrm{Supp}\, \Sigma'$ of K with $\deg_K \wp = N$ and $\pi_{\mathcal{C}}(N, \Sigma')$ be the number of primes $\wp \notin \mathrm{Supp}\, \Sigma'$ of K such that $\deg_K \wp = N$ and $\mathrm{Frob}_\wp = \mathcal{C}$.

It suffices to find a lower bound N_0 for N such that for $N \geq N_0$, $\pi_{\mathcal{C}}(N, \Sigma')$ is positive.

In fact, the genus g of K over $\mathbb{F}_q$ is the same as that of K' over $\mathbb{F}_{q^m}$ (refer to [13, Prop. 8.9]). We know that the genus of K' over $\mathbb{F}_{q^m}$ and the genus of E over $\mathbb{F}_{q^m}$ are related by the Riemann-Hurwitz Theorem [13, Theorem 7.16]. Thus, letting g_E be the genus of E, we have

$$g_E = 1 + |\,\mathrm{Gal}(E/K')|(g-1) + \frac{1}{2}\mathcal{D}. \tag{4}$$

The effective Chebotarev Density Theorem in [12, Theorem 1] gives

$$\frac{m|\mathcal{C}|}{|G|}\pi(N, \Sigma') - \alpha \leq \pi_{\mathcal{C}}(N, \Sigma') \leq \frac{m|\mathcal{C}|}{|G|}\pi(N, \Sigma') + \alpha,$$

where

$$\alpha = \frac{|\mathcal{C}|}{N} q^{N/2} \left(2g_E \frac{1}{|G|} + 2(2g+1) + \frac{1 + \frac{N}{|\mathcal{C}|}}{q^{N/2}} \delta' \right). \tag{5}$$

The condition $N \equiv r \pmod{m}$ ensures $\mathcal{C}$ restricted to $\mathbb{F}_{q^m}/\mathbb{F}_q$ is τ^N.

Remark 3.3. When $\Sigma' = \Sigma$, this is what is proved in [12, Theorem 1]. However, the proof carries over with Σ replaced by Σ'. In particular, the key identity (2.1) still holds with $y \in Y_r$ unramified replaced by $y \in Y_r$ not in the support of $\Sigma' \geq \Sigma$.

We have that

$$\pi(N, \Sigma') \geq S(N) - \frac{\deg_K \Sigma'}{N}.$$

Thus,

$$\frac{m|\mathcal{C}|}{|G|}\left(S(N)-\frac{\deg_K \Sigma'}{N}\right)-\alpha \le \pi_{\mathcal{C}}(N,\Sigma')$$

It is therefore enough to find a lower bound for N such that

$$\frac{m|\mathcal{C}|}{|G|}\left(S(N)-\frac{\deg_K \Sigma'}{N}\right)-\alpha > 0. \tag{6}$$

From Lemma 3.1 we have

$$\frac{q^N}{N}-\left(2g+1+\left(2g+\frac{3}{2}\right)\frac{4}{q}\right)\frac{q^{N/2}}{N} \le S(N) \le \frac{q^N}{N}+\left(2g+1+\left(2g+\frac{3}{2}\right)\frac{4}{q}\right)\frac{q^{N/2}}{N}. \tag{7}$$

Since $\frac{|G|}{m}=|\operatorname{Gal}(E/L')|$ and $\frac{1+N/|\mathcal{C}|}{q^{N/2}}\le 2$, from (5) we have

$$\alpha \ \le\ \frac{2m|\mathcal{C}|}{N|G|}\, q^{N/2}(|\operatorname{Gal}(E/K')|(2g+1+\delta')+\frac{g_E}{m}). \tag{8}$$

Therefore, combining (6) through (8), we obtain

$$\frac{m|\mathcal{C}|}{|G|}\left(S(N)-\frac{\deg_K \Sigma'}{N}\right)-\alpha \ \ge\ \frac{m|\mathcal{C}|}{N|G|}\, q^{N/2}\left(q^{N/2}-\left(c_0+\frac{\deg_K \Sigma'}{q^{N/2}}+2|\operatorname{Gal}(E/K')|(2g+1+\delta')+2\frac{g_E}{m}\right)\right), \tag{9}$$

where $c_0=2g+1+\left(2g+\frac{3}{2}\right)\frac{4}{q}$.

We thus need to find a lower bound of N such that the right hand side of the inequality of (9) is positive, or equivalently

$$q^{N/2} > c_0+\frac{\deg_K \Sigma'}{q^{N/2}}+2|\operatorname{Gal}(E/K')|(2g+1+\delta')+2\frac{g_E}{m} \tag{10}$$

$$= c_0+\frac{\deg_K \Sigma'}{q^{N/2}}+2|\operatorname{Gal}(E/K')|(2g+1+\delta')+\frac{2}{m}\left(1+|\operatorname{Gal}(E/K')|(g-1)+\frac{1}{2}\mathcal{D}\right) \tag{11}$$

$$= c_0+\frac{\deg_K \Sigma'}{q^{N/2}}+2|\operatorname{Gal}(E/K')|\left(2g+1+\delta'+\frac{g-1}{m}\right)+\frac{2}{m}\left(1+\frac{1}{2}\mathcal{D}\right) \tag{12}$$

using (4).

Let $1\le B$, $\delta'\le B$, $\mathcal{D}\le B$, and $|\operatorname{Gal}(E/K')|\le \frac{1}{2}B+1$. Note if $g=0$, it suffices to take $\delta'\le B$ and $\mathcal{D}\le B$ only, as it is then automatic that $|\operatorname{Gal}(E/K')|\le \frac{1}{2}\mathcal{D}+1\le$

$\frac{1}{2}B+1$. Therefore, we have that

$$\begin{aligned}
&c_0 + \frac{\deg_K \Sigma'}{q^{N/2}} + 2|\operatorname{Gal}(E/K')|\left(2g+1+\delta'+\frac{g-1}{m}\right) + \frac{2}{m}\left(1+\frac{1}{2}\mathcal{D}\right) \\
&\le c_0 + \frac{B}{q^{N/2}} + (B+2)\left(2g+1+B+\frac{g-1}{m}\right) + \frac{2}{m}\left(1+\frac{1}{2}B\right) \\
&\le 2g+1+\left(2g+\frac{3}{2}\right)\frac{4}{q} + \frac{B}{q^{N/2}} + (B+2)\left(2g+1+B+\frac{g-1}{m}\right) + \frac{2}{m}\left(1+\frac{1}{2}B\right) \\
&\le B^2 + B\left(2g+3+\frac{g}{m}\right) + 6g+3+\frac{2g}{m} + \left(2g+\frac{3}{2}\right)\frac{4}{q} + \frac{B}{q^{N/2}} \\
&\le B^2 + B\left(2g+3+\frac{g}{m}\right) + 10g+6+\frac{2g}{m} + \frac{B}{q^{N/2}},
\end{aligned}$$

where the last inequality uses $\frac{4}{q} \le 2$. Therefore, it suffices to have

$$q^{N/2} > \left(B^2 + B\left(2g+3+\frac{g}{m}\right) + 10g+6+\frac{2g}{m}\right) + \frac{B}{q^{N/2}}.$$

This can be satisfied if the following two inequalities hold,

$$\alpha q^{N/2} \ge B^2 + B\left(2g+3+\frac{g}{m}\right) + 10g+6+\frac{2g}{m} \text{ and}$$
$$(1-\alpha)q^{N/2} > \frac{B}{q^{N/2}},$$

where $0<\alpha<1$, or equivalently,

$$N \ge 2\log_q \frac{1}{\alpha}\left(B^2 + B\left(2g+3+\frac{g}{m}\right) + 10g+6+\frac{2g}{m}\right) \text{ and}$$
$$N > \log_q \frac{1}{1-\alpha}B.$$

Taking $\alpha = \frac{3}{4}$, the required inequalities become

$$N \ge 2\log_q \frac{4}{3}\left(B^2 + B\left(2g+3+\frac{g}{m}\right) + 10g+6+\frac{2g}{m}\right) \text{ and}$$
$$N > \log_q 4B.$$

So if $N \ge \frac{2}{m_0}\log_{q_0}\frac{4}{3}\left(B^2 + B\left(2g+3+\frac{g}{m}\right) + 2\left(5g+3+\frac{g}{m}\right)\right)$ and $N \equiv k \pmod m$, then there is a prime $\wp \notin \Sigma'$ of K such that $\deg_K \wp = N$ and $\operatorname{Frob}_\wp = \mathcal{C}$. □

Corollary 3.4. *Let the notation and hypotheses be as in Theorem 3.2. Then there exists a prime $\wp \notin \Sigma'$ of K such that $\operatorname{Frob}_\wp = \mathcal{C}$ and*

$$\deg_K \wp \le \frac{4}{m_0}\log_{q_0}\frac{4}{3}(B+3g+3) + m.$$

Proof. Let M be the integer such that

$$M = \frac{2}{m_0} \log_{q_0} \frac{4}{3} \left(B^2 + B \left(2g + \frac{g}{m} + 3 \right) + 2(5g + \frac{g}{m} + 3) \right) + \delta,$$

where $0 \leq \delta < 1$. Let $N = M + k'$, where $0 \leq k' \leq m - 1$ is chosen so that $N \equiv k \pmod{m}$. Then $N \geq \frac{2}{m_0} \log_{q_0} \frac{4}{3} \left(B^2 + B \left(2g + \frac{g}{m} + 3 \right) + 2(5g + \frac{g}{m} + 3) \right)$ and $N \equiv k \pmod{m}$. By Theorem 3.2, there exists a prime $\wp \notin \Sigma'$ of K such that $\deg_K \wp = N$ and $\mathrm{Frob}_\wp = \mathcal{C}$. Now,

$$\begin{aligned}
\deg_K \wp &= N = M + k' \\
&\leq \frac{2}{m_0} \log_{q_0} \frac{4}{3} \left(B^2 + B \left(2g + 3 + \frac{g}{m} \right) + 10g + 6 + \frac{2g}{m} \right) + m \\
&\leq \frac{2}{m_0} \log_{q_0} \frac{4}{3} \left(B + 2g + 3 + \frac{g}{m} \right)^2 + m \\
&\leq \frac{4}{m_0} \log_{q_0} \frac{4}{3} (B + 3g + 3) + m.
\end{aligned}$$

□

4. Bounds for the different divisor

Proposition 4.1. *Let ϕ be a rank r Drinfeld A-module which is integral over K and let $\mathfrak{L} = (a)$ be a finite prime of A with a monic. Let $\mathfrak{D}_0(K_{\phi,\mathfrak{L}}/K)$ be the finite part of the different divisor $\mathfrak{D}(K_{\phi,\mathfrak{L}}/K)$. Then we have*

$$\deg_K \mathfrak{D}_0(K_{\phi,\mathfrak{L}}/K) \leq r \left(\deg_K a + \frac{(\ell^r - 2)(\ell^r - 1)}{q^r - 1} \deg_K \Delta(\phi) \right),$$

where $\ell = q^{\deg_F \mathfrak{L}}$. In addition, if $v(a\Delta(\phi)) = 0$ for a finite place v of K, then

$$v(D(K_{\phi,\mathfrak{L},w}/K_v)) = 0,$$

where $D(K_{\phi,\mathfrak{L},w}/K_v)$ is the different ideal of $K_{\phi,\mathfrak{L},w}/K_v$, and $w \mid v$ is a place of $K_{\phi,\mathfrak{L},w}$.

Proof. This is a slightly modified version of [4, Lemma 4.2] which is derived from [17].

Let $\alpha \in \overline{K}$ be a root of a separable polynomial $f(X) = b_0 X + b_1 X^q + \ldots + b_m X^{q^m}$ with $b_i \in \mathcal{O}$ and $b_0 b_m \neq 0$. Then $h(X) = b_m^{q^m - 1} f(X/b_m) = b_0 b_m^{q^m - 2} X + b_1 b_m^{q^m - 1 - q} X^q + \ldots + b_{m-1} b_m^{q^m - 1 - q^{m-1}} X^{q^{m-1}} + X^{q^m} \in \mathcal{O}[X]$ is monic. Since $h(b_m \alpha) = 0$ and $K(\alpha) = K(b_m \alpha)$, we may apply Lemma 2.4 to $b_m \alpha$ and $h(X)$ to show the *different ideal* $D(K(\alpha)/K)$ divides the principal ideal $(b_0 b_m^{q^m - 2})$.

Let $\mathfrak{L} = (a)$ and $f(X) = \phi_a(X)$. Then $f(X) = aX + \ldots + \Delta(\phi)^{(q^m - 1)/(q^r - 1)} X^{q^m}$ where $m = r \deg_F a$ (cf. [13, Proposition 13.8]). There are r roots $\beta_1, \ldots, \beta_r$ of $\phi_a(X)$

which generate $K_{\phi,\mathfrak{L}}$ over K. Using the transitivity of the different (cf. Lemma 2.3), it follows that

$$D(K_{\phi,\mathfrak{L}}/K) \mid \left(b_0 b_m^{q^m-2}\right)^r = \left(a\,(\Delta(\phi))^{(q^m-2)(q^m-1)/(q^r-1)}\right)^r. \tag{13}$$

This shows that if $v(a\Delta(\phi)) = 0$ for a finite place v, then $v(D(K_{\phi,\mathfrak{L},w}/K_v)) = 0$. Furthermore, taking the degree with respect to K of (13), we obtain

$$\deg_K \mathfrak{D}_0(K_{\phi,\mathfrak{L}}/K) \le r(\deg_K a + \frac{(\ell^r-2)(\ell^r-1)}{q^r-1}\deg_K \Delta(\phi)).$$

□

Although it is possible to obtain a bound on $\deg_K \mathfrak{D}(K_{\phi,\mathfrak{L}}/K)$ based on Proposition 4.1 and Lemma 4.2, we shall give a slightly more refined bound in Proposition 4.3, using additional techniques.

Lemma 4.2. *Let $\bar{\infty}$ be an infinite prime of K, $K_{\bar{\infty}}$ be the completion of K at $\bar{\infty}$, $\mathcal{O}_{\bar{\infty}}$ the valuation ring of $\bar{\infty}$, $v_{\bar{\infty}}$ the valuation associated to $\bar{\infty}$, and e be the ramification index of $\bar{\infty}$ over ∞.*

Let $\phi_T(X) = TX + a_1X^q + \cdots + a_iX^{q^i} + \cdots + a_rX^{q^r}$ be a rank r Drinfeld A-module defined over K, and write $\phi_{T^n}(X) = T^nX + b_1X^q + \ldots + b_iX^{q^i} + \ldots + b_{rn}X^{q^{rn}}$ where $n \ge 1$.

Let $\omega_1 = \max\left\{e, -\frac{v_{\bar{\infty}}(a_i)}{q^i},\ i = 1,\ldots,r\right\}$ and $\omega_n = n\omega_1$. Then

$$\omega_n \ge \max\left\{ne, -\frac{v_{\bar{\infty}}(b_i)}{q^i} : i = 1,\ldots,rn\right\}.$$

Proof. We use induction on n. First note that

$$\phi_{T^n}(\lambda_nX) = T^n\lambda_nX + b_1\lambda_n^qX^q + \ldots + b_i\lambda_n^{q^i}X^{q^i} + \ldots + b_{rn}\lambda_n^{q^{rn}}X^{q^{rn}},$$

so taking $\lambda_n \in K$ with $v_{\bar{\infty}}(\lambda_n) = \omega_n \ge \max\left\{ne, -\frac{v_{\bar{\infty}}(b_i)}{q^i} : i = 1,\ldots,rn\right\}$ implies that $\phi_{T^n}(\lambda_nX) \in \mathcal{O}_{\bar{\infty}}[X]$.

The result is true for $n = 1$ as $\omega_1 = \max\left\{e, -\frac{v_{\bar{\infty}}(a_i)}{q^i},\ i = 1,\ldots,r\right\}$.

Assume $\omega_n = n\omega_1 \ge \max\left\{ne, -\frac{v_{\bar{\infty}}(b_i)}{q^i} : i = 1,\ldots,rn\right\}$. Now, consider the terms in the product

$$\phi_{T^{n+1}} = \phi_{T^n} \circ \phi_T = (T^n + b_1\tau + \ldots + b_{rn}\tau^{rn}) \circ (T + a_1\tau + \cdots + a_r\tau^r),$$

where there are $2(r+1)$ types of terms to consider:

$$\begin{aligned} b_i\tau^i T =& b_i T^{q^i}\tau^i, \qquad 1 \le i \le rn, \\ b_i\tau^i a_1\tau =& b_i a_1^{q^i}\tau^{i+1}, \quad 1 \le i \le rn, \\ & \vdots \\ b_i\tau^i a_r\tau^r =& b_i a_r^{q^i}\tau^{i+r}, \quad 1 \le i \le rn, \\ T^{n+1},\ T^n a_1\tau,\ & T^n a_2\tau^2,\ \cdots,\ T^n a_r\tau^r \end{aligned}$$

We need to show $\omega_{n+1} \ge$ the valuations of the coefficients of each type of term, namely, that for each i with $1 \le i \le rn$,

$$\omega_{n+1} \ge -\frac{v_{\bar\infty}(b_i)}{q^i} + e \tag{14}$$

$$\omega_{n+1} \ge -\frac{v_{\bar\infty}(b_i)}{q^{i+j}} - \frac{v_{\bar\infty}(a_j)}{q^j}, \quad 1 \le j \le r, \tag{15}$$

$$\omega_{n+1} \ge ne + 1 \tag{16}$$

$$\omega_{n+1} \ge ne - \frac{v_{\bar\infty}(a_j)}{q^j}, \quad 1 \le j \le r. \tag{17}$$

As $\omega_n \ge -\frac{v_{\bar\infty}(b_i)}{q^i}$ for $1 \le i \le 2n$, we have that $\omega_{n+1} = \omega_n + \omega_1 \ge \frac{\omega_n}{q^j} + \omega_1 \ge -\frac{v_{\bar\infty}(b_i)}{q^{i+j}} + \omega_1$ for $j = 0, 1, \cdots, r$ and $i = 1, 2, \ldots, rn$, so (14) and (15) are satisfied. Since $\omega_1 = \max\left\{e, -\frac{v_{\bar\infty}(a_j)}{q^j},\ j = 1, \ldots, r\right\}$,

$$\omega_{n+1} = (n+1)\omega_1 = n\omega_1 + \omega_1 \ge ne + \omega_1 \ge \max\left\{(n+1)e,\ ne - \frac{v_{\bar\infty}(a_j)}{q^j},\ j = 1, \ldots, r\right\},$$

so the last inequalities in (16) and (17) are satisfied. □

In the following proposition, we obtain an upper bound on the degree of the different divisor of $K_{\phi,\mathfrak{L}}/K$, which uses mild information from the Newton polygons of $\phi_a(X)$, and takes into account primes of potentially good reduction.

Proposition 4.3. *Let ϕ be a rank r Drinfeld A-module which is integral over K and let $\mathfrak{L} = (a)$ be a finite prime of A with a monic. Let $\mathfrak{D}(K_{\phi,\mathfrak{L}}/K)$ be the different divisor of $K_{\phi,\mathfrak{L}}/K$. Then we have*

$$\deg_K \mathfrak{D}(K_{\phi,\mathfrak{L}}/K) \le r\left(\frac{\ell^r - 1}{q-1}(s\deg_K a + \Lambda(\phi)) + 2\deg_K a \operatorname{rad}_K \Delta(\phi)\right),$$

where s denotes the geometric extension degree of K/F, $\ell = q^{\deg_F \mathfrak{L}}$, $\Lambda(\phi) = -\sum_v \tau_v(\phi) \deg_K v$, and for $x \in K$, we let $\deg_K \operatorname{rad}_K x := \sum_{v(x)\neq 0} \deg_K v$ (the sums are over every place v of K).

Proof. Let $\phi_T(X) = TX + a_1X^q + \ldots + a_rX^{q^r}$ where $a_i \in \mathcal{O}$. Let

$$\begin{aligned} f(X) = \phi_a(X) &= b_0X + b_1X^q + \ldots + b_{rn}X^{q^{rn}} \\ &= b_{rn}\prod_{i=1}^{q^{rn}}(X - \alpha_i), \end{aligned}$$

where $b_0 = a$, $b_{rn} = a_r^{\frac{q^{rn}-1}{q^r-1}}$, and $n = \deg_K a = \deg_K \mathfrak{L}$. Let α be any one of the α_i.

Let $\wp$ be a finite place of K with corresponding discrete valuation $v_\wp$, and let $\tau_\wp = \inf\left\{\frac{v_\wp(a_i)}{q^i-1} : i = 1, \ldots, r\right\}$. Note $\tau_\wp \geq 0$. Let $K_\wp$ be the completion of K at $\wp$, and ${K_\wp}'/K_\wp$ be a totally tamely ramified extension with ramification index $\frac{1}{q^{rn}-1}$, and ring of integers $\mathcal{O}'_\wp$.

Over ${K_\wp}'$, ϕ_T is isomorphic to a Drinfeld A-module $\phi'_T(X) = TX+a'_1X^q+\ldots+a'_rX^{q^r}$, where $a'_i = a_i/\lambda^{q^i-1}$, $v_\wp(a'_i) \geq 0$, for $1 \leq i \leq r$, $v_\wp(\lambda) = \tau_\wp$, and $\lambda \in {K_\wp}'$.

Let $\phi'_a(X) = b'_0X + b'_1X^q + \ldots + b'_{rn}X^{q^{rn}}$. As $b'_i = b_i/\lambda^{q^i-1}$, we have that

$$\begin{aligned} v_\wp(b_i) &\geq (q^i - 1)v_\wp(\lambda) \\ &= (q^i - 1)\tau_\wp. \end{aligned}$$

From the Newton polygon of $f(X)$, we have that

$$v_\wp(\alpha) \geq -\frac{v_\wp(a_r)\frac{q^{rn}-1}{q^r-1} - (q^{rn-1} - 1)\tau_\wp}{q^{rn} - q^{rn-1}} := -\delta.$$

Pick a $\mu \in {K_\wp}'$ such that $v_\wp(\mu) = \delta + \epsilon$ where $0 \leq \epsilon < \frac{1}{q^{rn}-1}$. Now,

$$f(X/\mu) = b_{rn}/\mu^{q^{rn}}\prod_{i=1}^{q^{rn}}(X - \mu\alpha_i),$$

and we know that $g(X) = \prod_i (X - \mu\alpha_i)$ is monic and lies in $\mathcal{O}'_\wp[X]$, where $\mathcal{O}'_\wp$ is the ring of integers of $K_\wp{}'$. Thus, $g'(X) = \mu^{q^{rn}-1} a/b_{rn}$. Hence,

$$\begin{aligned} v_\wp(g'(\mu\alpha)) &= v_\wp(\mu)(q^{rn}-1) + v_\wp(a) - v_\wp(b_{rn}) \\ &\leq \delta(q^{rn}-1) + 1 + v_\wp(a) - v_\wp(a_r)\frac{q^{rn}-1}{q^r-1} \\ &\leq v_\wp(a_r)\frac{q^{rn}-1}{q^r-1}\left(\frac{q^{rn}-1}{q^{rn}-q^{rn-1}} - 1\right) - \frac{(q^{rn-1}-1)(q^{rn}-1)}{q^{rn}-q^{rn-1}}\tau_\wp + 1 + v_\wp(a) \\ &\leq v_\wp(a_r)\frac{q^{rn}-1}{q^r-1}\cdot\frac{1-q^{1-rn}}{q-1} - \frac{q^{2rn-1}-q^{rn}-q^{rn-1}+1}{q^{rn}-q^{rn-1}}\tau_\wp + 1 + v_\wp(a) \\ &= v_\wp(a_r)\frac{q^{rn}-1}{(q^r-1)(q-1)} - \frac{q^{rn}-q-1+q^{1-rn}}{q-1}\tau_\wp + 1 + v_\wp(a). \end{aligned}$$

It follows that

$$v_\wp(D(K_\wp{}'(\mu\alpha)/K_\wp{}')) \leq v_\wp(a_r)\frac{q^{rn}-1}{(q^r-1)(q-1)} - \frac{q^{rn}-q-1+q^{1-rn}}{q-1}\tau_\wp + 1 + v_\wp(a)$$

and

$$\begin{aligned} v_\wp(D(K_\wp(\alpha)/K_\wp)) &\leq v_\wp(D(K_\wp{}'(\mu\alpha)/K_\wp{}')) + v_\wp(D(K_\wp{}'/K_\wp)) \\ &\leq v_\wp(a_r)\frac{q^{rn}-1}{(q^r-1)(q-1)} - \frac{q^{rn}-q-1+q^{1-rn}}{q-1}\tau_\wp + 2 + v_\wp(a). \end{aligned}$$

Since $\tau_\wp \leq \frac{v_\wp(a_r)}{q^r-1}$, we have that

$$\begin{aligned} & v_\wp(a_r)\frac{q^{rn}-1}{(q^r-1)(q-1)} - \frac{q^{rn}-q-1+q^{1-rn}}{q-1}\tau_\wp + 2 + v_\wp(a) \\ &\geq v_\wp(a_r)\frac{q^{rn}-1}{(q^r-1)(q-1)} - \frac{q^{rn}-q-1+q^{1-rn}}{q-1}\frac{v_\wp(a_r)}{q^r-1} + 2 + v_\wp(a) \\ &= v_\wp(a_r)\frac{q-q^{1-rn}}{(q^r-1)(q-1)} + 2 + v_\wp(a) \\ &\geq 2. \end{aligned}$$

From Proposition 4.1, we know for a finite place $v_\wp$ of K, $v_\wp(D(K(\alpha)/K)) = 0$ if $v_\wp(aa_r) = 0$. It follows that we in fact have that

$$v_\wp(D(K_\wp(\alpha)/K_\wp)) \leq v_\wp(a_r)\frac{q^{rn}-1}{(q^r-1)(q-1)} - \frac{q^{rn}-q-1+q^{1-rn}}{q-1}\tau_\wp + 2\nu + v_\wp(a) \tag{18}$$

where $\nu = 1$ if $v_\wp(aa_r) > 0$ and $\nu = 0$ if $v_\wp(aa_r) = 0$.

Let $\bar{\infty} \in S_\infty^K$ be an infinite prime of K with corresponding valuation $v_{\bar{\infty}}$, and let $K'_{\bar{\infty}}/K_{\bar{\infty}}$ be a totally tamely ramified extension with ramification index $\frac{1}{q^{rn}-1}$, and ring of integers $\mathcal{O}'_{\bar{\infty}}$.

Let $\tau_{\bar{\infty}}(\phi) = \inf \left\{ \frac{v_{\bar{\infty}}(a_i)}{q^i-1} : i = 1, \ldots, r \right\}$. Note $\tau_{\bar{\infty}} \leq 0$.

Over $K'_{\bar{\infty}}$, ϕ_T is isomorphic to a Drinfeld A-module $\phi'_T(X) = TX + a'_1 X^q + \ldots + a'_r X^{q^r}$, where $a'_i = a_i/\lambda^{q^i-1}$, $v_{\bar{\infty}}(a'_i) \geq 0$, for $1 \leq i \leq r$, $v_{\bar{\infty}}(\lambda) = \tau_{\bar{\infty}}$, and $\lambda \in K'_{\bar{\infty}}$.

Let $\phi'_a(X) = b'_0 X + b'_1 X^q + \ldots + b'_{rn} X^{q^{rn}}$. Set $\omega_1 = \max \left\{ e, -\frac{v_{\bar{\infty}}(a'_i)}{q^i} : i = 1, \ldots, r \right\} = 1$. From Lemma 4.2, we know that $\omega_n = n\omega_1 \geq \max \left\{ ne, -\frac{v_{\bar{\infty}}(b'_i)}{q^i} : i = 1, \ldots, rn \right\}$. Thus, $v_{\bar{\infty}}(b'_i) \geq -q^i ne$ for $i = 1, \ldots, rn$. As $b'_i = b_i/\lambda^{q^i-1}$, we have that

$$\begin{aligned} v_{\bar{\infty}}(b_i) &\geq -q^i ne + (q^i - 1) v_{\bar{\infty}}(\lambda) \\ &= -q^i ne + (q^i - 1)\tau_{\bar{\infty}}. \end{aligned}$$

From the Newton polygon of $f(X)$, it follows that

$$v_{\bar{\infty}}(\alpha) \geq -\frac{v_{\bar{\infty}}(a_r)\frac{q^{rn}-1}{q^r-1} + neq^{rn-1} - (q^{rn-1}-1)\tau_{\bar{\infty}}}{q^{rn} - q^{rn-1}} := -\delta_{\bar{\infty}}.$$

Let $\mu_{\bar{\infty}}$ be such that $v_{\bar{\infty}}(\mu_{\bar{\infty}}) = \delta_{\bar{\infty}} + \epsilon_\infty$, where $0 \leq \epsilon_\infty < \frac{1}{q^{rn}-1}$. Now,

$$f(X/\mu_{\bar{\infty}}) = b_{rn}/\mu_{\bar{\infty}}^{q^{rn}} \prod_{i=1}^{q^{rn}} (X - \mu_{\bar{\infty}}\alpha_i),$$

and we know that $g(X) = \prod_{i=1}^{q^{rn}} (X - \mu_{\bar{\infty}}\alpha_i)$ is monic and lies in $\mathcal{O}'_{\bar{\infty}}[X]$, where $\mathcal{O}'_{\bar{\infty}}$ is the ring of integers of $K'_{\bar{\infty}}$. Thus, $g'(X) = \mu_{\bar{\infty}}^{q^{rn}-1} a/b_{rn}$. Hence,

$$\begin{aligned} &v_{\bar{\infty}}(g'(\mu_{\bar{\infty}}\alpha)) = v_{\bar{\infty}}(\mu_{\bar{\infty}})(q^{rn} - 1) + v_{\bar{\infty}}(a) - v_{\bar{\infty}}(b_{rn}) \\ &\leq \delta_{\bar{\infty}}(q^{rn} - 1) + 1 + v_{\bar{\infty}}(a) - v_{\bar{\infty}}(a_r)\frac{q^{rn}-1}{q^r-1} \\ &\leq v_{\bar{\infty}}(a_r)\frac{q^{rn}-1}{q^r-1}\left(\frac{q^{rn}-1}{q^{rn}-q^{rn-1}} - 1\right) + ne\frac{q^{rn}-1}{q-1} - \frac{(q^{rn-1}-1)(q^{rn}-1)}{q^{rn}-q^{rn-1}}\tau_{\bar{\infty}} + 1 + v_{\bar{\infty}}(a) \\ &= v_{\bar{\infty}}(a_r)\frac{q^{rn}-1}{q^r-1} \cdot \frac{1-q^{1-rn}}{q-1} + ne\frac{q^{rn}-1}{q-1} - \frac{q^{2rn-1} - q^{rn} - q^{rn-1} + 1}{q^{rn} - q^{rn-1}}\tau_{\bar{\infty}} + 1 + v_{\bar{\infty}}(a) \\ &= v_{\bar{\infty}}(a_r)\frac{q^{rn}-1}{(q^r-1)(q-1)} + ne\frac{q^{rn}-1}{q-1} - \frac{q^{rn} - q - 1 + q^{1-rn}}{q-1}\tau_{\bar{\infty}} + 1 + v_{\bar{\infty}}(a). \end{aligned}$$

It follows that
(19)

$$v_{\bar\infty}(D(K_{\bar\infty}(\alpha)/K_{\bar\infty})) \leq v_{\bar\infty}(a_r)\frac{q^{rn}-1}{(q^r-1)(q-1)}+ne\frac{q^{rn}-1}{q-1}-\frac{q^{rn}-q-1+q^{1-rn}}{q-1}\tau_{\bar\infty}+2+v_{\bar\infty}(a).$$

Let $\mathfrak{D}(K(\alpha)/K)$ be the different divisor of $K(\alpha)$ over K, and Ω_P be the set of conjugates of α over K_P. Using (18) and (19), we obtain

$$\begin{aligned}
\deg_K \mathfrak{D}(K(\alpha)/K) &= \sum_P \max\left\{v_P(D(K_P(\alpha)/K_P)) : \alpha \in \Omega_P\right\} \deg_K P \\
&\leq n\frac{q^{rn}-1}{q-1}\sum_{\bar\infty\in S_\infty^K} e(\bar\infty/\infty)\deg_K \bar\infty - \frac{q^{rn}-q-1+q^{1-rn}}{q-1}\sum_v \tau_P \deg_K P \\
&+ 2\deg_K \operatorname{rad}_K aa_r, \\
&= n\frac{q^{rn}-1}{q-1}\sum_{\bar\infty\in S_\infty^K} e(\bar\infty/\infty)\frac{f(\bar\infty/\infty)}{[\mathbb{F}_K:\mathbb{F}_F]}\deg_F \infty \\
&- \frac{q^{rn}-q-1+q^{1-rn}}{q-1}\sum_v \tau_P \deg_K P + 2\deg_K \operatorname{rad}_K aa_r, \\
&\leq n\frac{q^{rn}-1}{q-1}s - \frac{q^{rn}-q-1+q^{1-rn}}{q-1}\sum_v \tau_P \deg_K P + 2\deg_K \operatorname{rad}_K aa_r,
\end{aligned}$$

where the summation runs through all the primes P of K, s is the geometric extension degree of K/F, and we use the fact that $\sum_P v_P(x)\deg_K P = 0$ for $x \in K$. Remark that $\sum_P \tau_P \deg_K P \leq 0$, so we finally get

$$\begin{aligned}
\deg_K \mathfrak{D}(K(\alpha)/K) &\leq ns\frac{q^{rn}-1}{q-1} + \frac{q^{rn}-q-1+q^{1-rn}}{q-1}\left(-\sum_v \tau_P \deg_K P\right) + 2\deg_K \operatorname{rad}_K aa_r \\
&\leq ns\frac{q^{rn}-1}{q-1} + \frac{q^{rn}-1}{q-1}\left(-\sum_P \tau_P \deg_K P\right) + 2\deg_K \operatorname{rad}_K aa_r \\
&\leq \frac{q^{rn}-1}{q-1}\left(ns - \sum_v \tau_P \deg_K P\right) + 2\deg_K \operatorname{rad}_K aa_r \\
&\leq \frac{\ell^r-1}{q-1}(ns + \Lambda(\phi)) + 2\deg_K \operatorname{rad}_K aa_r \\
&\leq \frac{\ell^r-1}{q-1}(s\deg_K a + \Lambda(\phi)) + 2\deg_K \operatorname{rad}_K a\Delta(\phi)
\end{aligned}$$

Using transitivity of the different (cf. Lemma 2.3), and the fact that $K_{\phi,\mathfrak{L}}$ is generated by r of the roots α_i, the result follows. □

Corollary 4.4. *Assume the notation of Proposition 4.3. Let* ϕ_1 *and* ϕ_2 *be rank* r *Drinfeld* A*-modules which are integral over* $\mathcal{O}$*. Let* $\mathfrak{D}(\tilde{K}/K)$ *be the different divisor of* $\tilde{K}/K$*, where* $\tilde{K} = K_{\phi_1,\mathfrak{L}}K_{\phi_2,\mathfrak{L}}$*. Then we have*

$$\deg_K \mathfrak{D}(\tilde{K}/K) \leq r\left(\frac{\ell^r - 1}{q-1}(2s\deg_K a + \Lambda(\phi_1,\phi_2)) + 2\deg_K \mathrm{rad}_K \Delta(\phi_1)\Delta(\phi_2) + 4\deg_K a\right),$$

where $\Lambda(\phi_1,\phi_2) = \Lambda(\phi_1) + \Lambda(\phi_2)$*.*

Proof. The result follows from Lemma 2.6 and Proposition 4.3. □

5. Proof of Theorem 1.2

We first recall some intermediate results which are function field analogues of those found in [16] (cf. [6]).

Lemma 5.1. *We have that*

$$\sum_{1\leq \deg_F \mathfrak{L} \leq N} \deg_F \mathfrak{L} \geq q^N$$

for all positive integers N*, where the sum is over finite primes* $\mathfrak{L}$ *of* F*.*

Proof. The product of all finite primes $\mathfrak{L}$ of F such that $\deg \mathfrak{L}$ divides N is equal to $T^{q^N} - T$, so the inequality follows. □

Lemma 5.2. *For any non-zero* $n \in A$*, there exists a finite prime* $\mathfrak{L}$ *of* F *such that* $n \not\equiv 0 \pmod{\mathfrak{L}}$ *with* $\deg_F \mathfrak{L} \leq 1 + \log_q \deg_F n$*.*

Proof. Suppose $n \equiv 0 \pmod{\mathfrak{L}}$ for all the primes $\mathfrak{L}$ such that $1 \leq \deg_F \mathfrak{L} \leq 1 + \log_q \deg_F n$.

Choose $k := \lfloor 1 + \log_q \deg_F n \rfloor$, so that $k - 1 \leq \log_q \deg_F n < k$, and hence $q^{k-1} \leq \deg_F n < q^k$

Then $\prod_{1\leq \deg_F \mathfrak{L} \leq k}$ divides n, thus $q^k \leq \deg_F n$ by Lemma 5.1. But, $\deg_F n < q^k$, which is a contradiction. □

For the proof of Theorem 1.2, we will require an estimate of the form

$$\gamma x^t \leq \frac{x}{1 + \log_q x}, \tag{20}$$

for $x \geq C$.

Lemma 5.3. *Let* $c^* \geq 1$ *be given and set* $t^* = 1 - \frac{1}{\ln(qc^*)}$. *Then we have*

$$\gamma x^{t^*} \leq \frac{x}{1 + \log_q x}, \tag{21}$$

for $x \geq c^*$, *where* $\gamma = \frac{(c^*)^{1-t^*}}{1+\log_q c^*} = \frac{(c^*)^{\frac{1}{\ln(qc^*)}}}{1+\log_q c^*}$.

Proof. The inequality

$$\gamma x^t \leq \frac{x}{1 + \log_q x}$$

is equivalent to

$$f(x,t) = \frac{x^{1-t}}{1 + \log_q x} \geq \gamma.$$

For a fixed t, taking the derivative of f with respect to x,

$$f'(x,t) = x^{-t}\left((1-t)(1+\log_q x) - \frac{1}{\ln q}\right)/*^2,$$

where $* = (1+\log_q x)$. Hence, $f'(x,t) \geq 0$ is equivalent to $(1-t)(1+\log_q x) - \frac{1}{\ln q} \geq 0$, equivalently,

$$(1-t)(\ln q + \ln x) \geq 1. \tag{22}$$

Assuming $t < 1$, (22) is equivalent to $x \geq \frac{e^{\frac{1}{1-t}}}{q} := \beta(t)$. Thus, for a fixed $t < 1$, $f(x,t)$ is increasing with respect to x, when $x \geq \beta(t)$; that is, $f(x,t) \geq f(\beta(t),t)$ if $x \geq \beta(t)$. Now, $\beta(t^*) = c^*$ and $t^* < 1$, so we obtain

$$x^{t^*} f(c^*, t^*) \leq \frac{x}{1 + \log_q x},$$

for $x \geq c^*$. □

Lemma 5.4.

$$\log_q(x+y) \leq \max\{\log_q(2x),\ \log_q(2y)\} \tag{23}$$

$$\log_q(x+y) \leq \log_q x + \log_q y \text{ if } x, y \geq 2. \tag{24}$$

Proof. In order to have $z \geq \log_q(x+y)$, it suffices to have

$$\frac{1}{2}q^z \geq x \quad \text{and} \quad \frac{1}{2}q^z \geq y,$$

which is equivalent to

$$z \geq \log_q(2x) \quad \text{and} \quad z \geq \log_q(2y).$$

Thus, taking $z = \max\{\log_q(2x),\ \log_q(2y)\}$, we have $\log_q(x+y) \leq \max\{\log_q(2x),\ \log_q(2y)\}$. □

Conclusion of the proof of Theorem 1.2

Let $\wp \notin S$ be a prime of K with least degree such that $P_\wp(\phi_1) \neq P_\wp(\phi_2)$, where S is the given finite set of primes of K outside of which both ϕ_1 and ϕ_2 have good reduction. Let α_0 be a non-zero coefficient of $P_\wp(\phi_1) - P_\wp(\phi_2)$.

It is known that a root γ of $P_\wp(\phi_1)$ or $P_\wp(\phi_2)$ satisfies

$$v_\infty(\gamma) = -\frac{1}{r} \deg_K \wp,$$

(cf. [10, Theorem 3.2.3(c)(d)], [6, Proposition 9]). This implies that each coefficient β of $P_\wp(\phi_1)$ and $P_\wp(\phi_2)$ satisfies $\deg_F \beta \leq \deg_K \wp$ and hence each coefficient α of $P_\wp(\phi_1) - P_\wp(\phi_2)$ also satisfies $\deg_F \alpha \leq \deg_K \wp$, in particular $\deg_F \alpha_0 \leq \deg_K \wp$.

We choose a finite prime $\mathfrak{L}$ of F by Lemma 5.2 such that

$$\alpha_0 \not\equiv 0 \pmod{\mathfrak{L}} \quad \text{and} \quad \deg_F \mathfrak{L} \leq 1 + \log_q \deg_K \wp, \tag{25}$$

and write $\mathfrak{L} = (a)$, where a is monic in A.

Suppose $\wp$ lies above the prime $\mathfrak{p}$ of F. For $x \geq 7$, we have that $\log_q x < \frac{1}{2}(x-1)$ (since if we let $f(x) = \frac{1}{2}(x-1) - \log_q x$, then $f'(x) > 0$ for $x \geq 7$ and $f(7) > 0$). Hence, we obtain that $x < q^{\frac{1}{2}(x-1)}$, so $\frac{q^{\frac{1}{2}(x-1)}}{x} > 1$; hence, $\frac{q^{x-1}}{x} > q^{\frac{1}{2}(x-1)}$ for $x \geq 7$. Thus, noting $s \geq \frac{f(\wp/\mathfrak{p})}{[\mathbb{F}_K:\mathbb{F}_F]}$, if $x \geq \max\left\{1 + 2\log_q s, 7\right\}$, we get that $\frac{q^{x-1}}{x} > q^{\frac{1}{2}(x-1)} \geq s \geq \frac{f(\wp/\mathfrak{p})}{[\mathbb{F}_K:\mathbb{F}_F]}$. But then if $\mathfrak{L} = \wp$, we would have that

$$\begin{aligned} \deg_F \mathfrak{p} &\leq 1 + \log_q \deg_K \wp \\ &= 1 + \log_q \frac{f(\wp/\mathfrak{p})}{[\mathbb{F}_K : \mathbb{F}_F]} \deg_F \mathfrak{p}, \end{aligned}$$

in other words,

$$\frac{q^{x-1}}{x} \leq \frac{f(\wp/\mathfrak{p})}{[\mathbb{F}_K : \mathbb{F}_F]},$$

where $x = \deg_F \mathfrak{p} = \deg_F \mathfrak{L}$. Therefore, we either have that $\deg_F \mathfrak{p} \leq \max\left\{1 + 2\log_q s, 7\right\}$ or $\mathfrak{L} \neq \mathfrak{p}$ by the above inequality. In the former case, it follows that $\deg_K \wp \leq s \max\left\{1 + 2\log_q s, 7\right\}$.

Suppose we are now in the latter case where $\mathfrak{L} \neq \mathfrak{p}$. Consider the representation

$$\psi_\mathfrak{L} : G_K \to \mathrm{Aut}_{A/\mathfrak{L}}(\phi_1[\mathfrak{L}]) \times \mathrm{Aut}_{A/\mathfrak{L}}(\phi_2[\mathfrak{L}]) \cong \mathrm{GL}_2(A/\mathfrak{L}) \times \mathrm{GL}_2(A/\mathfrak{L})$$

where $\psi_\mathfrak{L} = \rho_{\phi_1,\mathfrak{L}} \times \rho_{\phi_2,\mathfrak{L}}$. Let $G_\mathfrak{L}$ be the image of this homomorphism. Let $C_\mathfrak{L}$ be the subset of $G_\mathfrak{L}$ consisting of pairs (a,b) such that the characteristic polynomials of a and b are not equal. Note that $C_\mathfrak{L}$ is invariant under conjugation so it is a union of conjugacy classes in $G_\mathfrak{L}$. Since $\mathfrak{L} \neq \mathfrak{p}$, we have that $C_\mathfrak{L} \neq \emptyset$, in particular, there is some conjugacy class $\mathcal{C} \subseteq C_\mathfrak{L}$ in $G_\mathfrak{L}$ with $\mathcal{C} \neq \emptyset$.

Let $S_{\mathfrak{L}} = S \cup \{\text{primes } \mathfrak{l} \text{ of } K \text{ lying over } \mathfrak{L}\}$. Then the Galois representation $\psi_{\mathfrak{L}}$ is unramified outside $S_{\mathfrak{L}}$. We have that $A/\mathfrak{L} \cong \mathbb{F}_\ell$ where $\ell = q^{\deg_F \mathfrak{L}}$.

Let $\tilde{K}/K$ be the field extension associated to $\psi_{\mathfrak{L}}$ and let n (resp. n') be its degree (resp. geometric extension degree). Applying Corollary 3.4 to $\tilde{K}/K$, and using Lemma 2.2 together with the bound for the degree with respect to K of $\mathfrak{D} = \mathfrak{D}(\tilde{K}/K)$ given in Corollary 4.4, we deduce that there is a prime $P \notin S_{\mathfrak{L}}$ such that $\mathrm{Frob}_P = \mathcal{C} \subseteq C_{\mathfrak{L}}$ and

$$\deg_K P \leq \frac{4}{m_0} \log_q \frac{4}{3} (B + 3g + 3) + m,$$

where

$$\begin{aligned}
&\Sigma' = \sum_{\mathfrak{p} \in S_{\mathfrak{L}}} \mathfrak{p} \geq \Sigma = \sum_{\mathfrak{p} \in S} \mathfrak{p}, \\
&\deg_K \Sigma' = \deg_K \mathrm{rad}_K \Delta(\phi_1)\Delta(\phi_2) + \deg_K \mathfrak{L}, \\
&B = \max\left\{\deg_K \Sigma', \deg_{\tilde{K}} \mathfrak{D}, 2\left|\mathrm{Gal}(E/K')\right| - 2, 2\right\}, \\
&\deg_{\tilde{K}} \mathfrak{D} \leq rn' \left(\frac{\ell^r - 1}{q - 1} (2s \deg_K a + \Lambda(\phi_1, \phi_2)) + 2 \deg_K \mathrm{rad}_K \Delta(\phi_1)\Delta(\phi_2) + 4 \deg_K a \right) \\
&m = [\mathbb{F}_{\tilde{K}} : \mathbb{F}_K], m_0 = [\mathbb{F}_K : \mathbb{F}_F].
\end{aligned}$$

Then

$$\begin{aligned}
\deg_K P &\leq \frac{4}{m_0} \log_q \frac{4}{3} (B + 3g + 3) + m, \\
&\leq \frac{4}{m_0} \left(\log_q \frac{4}{3} B + \log_q 4(g + 1) \right) + m, \qquad (26)
\end{aligned}$$

using $B \geq 2$ and Lemma 5.4. Note that regarding B, the terms $\deg_K \Sigma'$ and $2\left|\mathrm{Gal}(E/K')\right| - 2$ are less than the bound we use for $\deg_{\tilde{K}} \mathfrak{D}$, so we can ignore them later on when we bound B.

Using Lemma 5.4, we obtain

$$\begin{aligned}
&\log_q \deg_{\tilde{K}} \mathfrak{D} \\
&= \log_q rn' \left(\frac{\ell^r - 1}{q - 1} \Lambda(\phi_1, \phi_2) + 2 \deg_K \mathrm{rad}_K \Delta(\phi_1)\Delta(\phi_2) + \left(2s \frac{\ell^r - 1}{q - 1} + 4 \right) \deg_K a \right) \\
&\leq \log_q rn' + \log_q \left(\frac{\ell^r - 1}{q - 1} \left(\Lambda(\phi_1, \phi_2) + 2 \deg_K \mathrm{rad}_K \Delta(\phi_1)\Delta(\phi_2) \right) + \left(2s \frac{\ell^r - 1}{q - 1} + 4 \right) \deg_K a \right) \\
&\leq \log_q rn' + \max\left\{V_1,\ V_2\right\},
\end{aligned}$$

where

$$\begin{aligned}
V_1 &:= \log_q 2\frac{\ell^r - 1}{q-1}\left(\Lambda(\phi_1, \phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2)\right) \\
&= \log_q 2 + \log_q \frac{\ell^r - 1}{q-1} + \log_q\left(\Lambda(\phi_1, \phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2)\right), \\
\text{and}\ \ V_2 &:= \log_q 2\left(2s\frac{\ell^r - 1}{q-1} + 4\right)\deg_K a \\
&\leq \log_q 2 + \log_q 8s + \log_q \frac{\ell^r - 1}{q-1} + \log_q \deg_K a \\
&\leq V_1 + \log_q 8s + \log_q \deg_K a.
\end{aligned}$$

Thus,

$$\begin{aligned}
\log_q B &\leq \log_q rn' + V_1 + \log_q 8s + \log_q \deg_K a \\
&= \log_q rn' + \log_q 16s + \log_q \frac{\ell^r - 1}{q-1} + \log_q \deg_K a + \log_q\left(\Lambda(\phi_1, \phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2)\right).
\end{aligned}$$

Since $n' \leq n = |G_{\mathfrak{L}}| < \ell^{2r^2}$, $\log_q \ell = \deg_F \mathfrak{L} = \deg_F a$, and $\deg_K a \leq s\deg_F a = s\log_q \ell$, we finally obtain

(27)
$$\log_q B \leq \log_q 16rs^2 + (2r^2 + r)\log_q \ell + \log_q \log_q \ell + \log_q\left(\Lambda(\phi_1, \phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2)\right).$$

Note that if $\log_q\left(\Lambda(\phi_1, \phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2)\right) = 0$, the derivation of the bound (27) above can be modified so as to obtain

$$\log_q B \leq \log_q 16rs^2 + (2r^2 + r)\log_q \ell + \log_q \log_q \ell. \tag{28}$$

Thus, we have that

(29)
$$\log_q \frac{4}{3}B \leq \log_q \frac{64}{3}rs^2 + (2r^2 + r + 1)\log_q \ell + \log_q^*\left(\Lambda(\phi_1, \phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2)\right).$$

Returning to (26), we obtain

$$\deg_K P \leq \frac{4}{m_0}\Big(\log_q 86rs^2(g+1) + (2r^2 + r + 1)\log_q \ell \tag{30}$$

$$+ \log_q^*\left(\Lambda(\phi_1, \phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2)\right)\Big) + m. \tag{31}$$

By construction of $C_{\mathfrak{L}}$, we have that $P_P(\phi_1) \not\equiv P_P(\phi_2) \pmod{\mathfrak{L}}$. Thus, $\deg_K \wp \leq \deg_K P$, and from (25), it follows that

$$\begin{aligned}\deg_K \wp &\leq \frac{4}{m_0}(\log_q 86rs^2(g+1) + (2r^2+r+1)\log_q \ell \\ &+ \log_q^* (\Lambda(\phi_1,\phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2))) + m \\ &\leq \frac{4}{m_0}(\log_q 86rs^2(g+1) + (2r^2+r+1)(1+\log_q \deg_K \wp) \\ &+ \log_q^* (\Lambda(\phi_1,\phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2))) + m.\end{aligned} \tag{32}$$

As $1+\log_q x \geq 1$, $\frac{\log_q x}{x} \leq 1$, we have that

$$\frac{\deg_K \wp}{1+\log_q(\deg_K \wp)} \leq \frac{4}{m_0}(d_r + W),$$

where $c_r = 2r^2+r+1$, $d_r := c_r + \log_q 86rs^2(g+1)$, and

$$W := \log_q^* (\Lambda(\phi_1,\phi_2) + 2\deg_K \operatorname{rad}_K \Delta(\phi_1)\Delta(\phi_2)) + mm_0.$$

If $x \geq d_r$, then using Lemma 5.3 with $c^* = d_r$ and $x = \deg_K \wp$, we obtain

$$\gamma x^{t^*} \leq \frac{x}{1+\log_q x} \leq \frac{4}{m_0}(d_r + W),$$

where γ is as in Lemma 5.3. This implies that

$$x^{t^*} \leq \frac{4}{m_0}\frac{(d_r + W)}{\gamma},$$

so that

(33)

$$\begin{aligned}\log_q \deg_K \wp = \log_q x &\leq \frac{1}{t^*}\log_q \frac{4}{m_0}(d_r+W) \cdot \frac{1+\log_q d_r}{(d_r)^{\frac{1}{\ln(qd_r)}}} \\ &\leq s^*\left(\log_q \frac{4}{m_0} + \log_q(d_r+W) + \log_q(1+\log_q d_r) - \frac{1}{\ln(qd_r)}\log_q d_r\right) \\ &\leq s^*\left(\log_q \frac{4}{m_0} + \log_q d_r + \log_q W + \log_q(1+\log_q d_r) - \frac{1}{\ln(qd_r)}\log_q d_r\right) \\ &\leq s^*\left(\log_q \frac{4}{m_0} + \log_q W + \log_q \log_q d_r\right) + \log_q d_r,\end{aligned}$$

using $d_r, W \geq 2$, and where $t^* = \frac{\ln(qd_r)-1}{\ln(qd_r)}$ and $s^* = s^*_{q,r} = \frac{1}{t^*} = \frac{\ln(qd_r)}{\ln(qd_r)-1}$. We note when q or r is large, $s^*_{q,r}$ tends to 1 from above.

Substitution of (33) into (32) yields

(34)

$$\begin{aligned}
\frac{1}{4}\deg_K \wp &\le \log_q 86rs^2(g+1) + c_r(1+\log_q \deg_K \wp) + W \\
&\le \log_q 86rs^2(g+1) + c_r\left(1 + s^*\left(\log_q \frac{4}{m_0} + \log_q W + \log_q \log_q d_r\right) + \log_q d_r\right) + W \\
&= \log_q 86rs^2(g+1) + c_r\left(1 + s^* \log_q \frac{4}{m_0} + \log_q d_r\right) + c_r s^* \log_q \log_q d_r \\
&+ W + c_r s^* \log_q W \\
&= C_{q,r} + W + c_r s^*_{q,r} \log_q W,
\end{aligned}$$

where

$$C_{q,r} = \log_q 86rs^2(g+1) + c_r\left(1 + s^*_{q,r} \log_q \frac{4}{m_0} + \log_q d_r\right) + c_r s^*_{q,r} \log_q \log_q d_r.$$

Therefore, we either have the above upper bound (34) on $\deg_K \wp$ or $\deg_K \wp \le d_r \le C_{q,r}$, so in the end, we get

$$\deg_K \wp \le \frac{4}{m_0}\left(C_{q,r} + W + c_r s_{q,r} \log_q W\right). \tag{35}$$

Finally, we note from the discussion in the introduction that $m \le g_{\phi_1} g_{\phi_2}$.

6. The case of rank 2

In this section, we consider the case of rank 2 and $K = F$, and explain how to make all the terms explicit in our isogeny theorem.

For a Drinfeld A-module ϕ of rank 2 over $K = F = \mathbb{F}_q(T)$, the successive minima of the lattices associated to the uniformizations of ϕ are determined in [2] and this is used to obtain an explicit bound for the valuation $v_\infty(D(K_\infty(\phi[a])/K_\infty))$ of the different of $K_{\phi,a} = K(\phi[a])$ over K at the infinite prime ∞ of K and $v_\mathfrak{p}(D(K_\mathfrak{p}(\phi[a])/K_\mathfrak{p}))$ at a finite prime $\mathfrak{p}$ of K, following the work of [9].

The infinite prime case is obtained using the explicit information about the Newton polygon of the exponential map $e_{\phi,\infty}$ attached to ϕ from its uniformization over C_∞.

Assume the same notation as in the proof and statement of Proposition 4.3, taking $K = F = \mathbb{F}_q(T)$ and $\bar{\infty} = \infty$, the explicit bounds given in [2] are as follows.

Let $\phi_T = T + a_1\tau + a_2\tau^2$, $j(\phi) = a_1^{q+1}/a_2$, and m be the least positive integer such that $-v_\infty(j(\phi)) \le q^{m+1}$. Then we have

$$v_\infty(D(K_\infty(\phi[a])/K_\infty)) \le \begin{cases} 1 & \text{if } -v_\infty(j(\phi)) \le q \\ 1 + \kappa\left(q^{\kappa+1} - 1\right) & \text{if } q < -v_\infty(j(\phi)) \le q^{m+1}, \end{cases}$$

where $\kappa = \frac{-v_\infty(j(\phi)) - q^m}{q^m(q-1)} + m - 1$, and

$$v_\mathfrak{p}(D(K_\mathfrak{p}(\phi[a])/K_\mathfrak{p})) \le \begin{cases} 2v_\mathfrak{p}(a) & \text{if } \phi \text{ has good reduction over } K_\mathfrak{p}, \\ 2v_\mathfrak{p}(a) + 1 & \text{if } v_\mathfrak{p}(j(\phi)) \ge 0 \text{ and } \phi \text{ has} \\ & \text{bad reduction over } K_\mathfrak{p}, \\ 2v_\mathfrak{p}(a) + 1 - \frac{2}{q-1}v_\mathfrak{p}(j(\phi)) & \text{if } v_\mathfrak{p}(j(\phi)) < 0. \end{cases}$$

Putting this together yields the following explicit bound on the different divisor of $F(\phi[a])/F$ when ϕ has rank 2, which can be used in place of the more general bound that we use in this paper. See Section 7 for a comparison of the two bounds in the context of our application.

Theorem 6.1. *Let ϕ be a Drinfeld A-module of rank 2 over F, and let $\mathfrak{D}(F(\phi[a])/F)$ be the different divisor of $F(\phi[a])/F$. Then*

$$\deg_F \mathfrak{D}(F(\phi[a])/F) \le 2\deg_F a + \deg_F \eta + \frac{2}{q-1}\deg_F \delta + v_\infty(D(F_\infty(\phi[a])/F_\infty))$$

where δ is the (monic) denominator of $j(\phi)$ as represented by a fraction in reduced form, and η is the product of finite primes $\mathfrak{p}$ such that ϕ has bad reduction over $F_\mathfrak{p}$.

Concerning the term g_ϕ, we have from [6] that

$$g_\phi = g_{\phi,\infty} \le (q^2-1)(q^2-q)\nu_{2,\phi,\infty}/\nu_{1,\phi,\infty}$$

where $\nu_{i,\phi,\infty}$ is the i-th successive minima of ϕ associated to its uniformization over C_∞. In [2], the $\nu_{i,\phi,\infty}$ are determined as follows.

Case 1: If $-v(j(\phi)) \le q$, then $\nu_{1,\phi,\infty} = \nu_{2,\phi,\infty} = -s_1$,

Case 2: If $q < -v(j(\phi)) \le q^{m+1}$, then $\nu_{1,\phi,\infty} = -s_1$, $\nu_{2,\phi,\infty} = -s_1 - \kappa$,

where $s_1 = \frac{v(a_2)+q^2}{q^2-1}$ in Case 1 and $s_1 = \frac{v(a_1)+q}{q-1}$ in Case 2, and m, κ are as above.

7. Comparison with work of Gardeyn

In this section, we make some detailed comparisons with the work in [6], where an effective isogeny theorem is proven.

For the proof of our Theorem 1.2, an essential ingredient is the bound on the different divisor given in Proposition 4.3,

(36)
$$\deg_K \mathfrak{D}(K_{\phi,\mathfrak{L}}/K) \le r\left(\frac{\ell^r-1}{q-1}(s\deg_K a+\Lambda(\phi))+2\deg_K \operatorname{rad}_K \Delta(\phi)+2\deg_K a\right),$$

where we recall $\Lambda(\phi) = -\sum_v \tau_v(\phi)\deg_K v$. The counterpart of (36) in [6] is

$$\deg_K \mathfrak{D}(K_{\phi,\mathfrak{L}}/K) \le r\deg_K a+\deg_K \Delta_\phi \tag{37}$$

where Δ_ϕ is a divisor of K which is determined from the Newton polygons of the exponential functions associated to uniformizations of ϕ over $C_\wp$, where $\wp$ is a prime of K.

Although there is a larger dependence on ℓ in our different bounds when we take degrees with respect to K, what is required in the application is the degree with respect to $K_{\phi,\mathfrak{L}}$, which necessitates multiplying the degree with respect to K by $n' < \ell^{r^2}$. This means both bounds end up being comparable in their dependence on ℓ, as we later take the $\log_q$ of this degree with respect to $K_{\phi,\mathfrak{L}}$.

The quantity Δ_ϕ is more difficult to make explicit and compare, as we saw in Section 6, where its determination in the case of rank 2 and $K = F = \mathbb{F}_q(T)$ is recalled from [2]. The method in [2] yields the entire Newton polygon and uses Gekeler's theory of Drinfeld modular forms as well as Rosen's theory of formal Drinfeld modules. It may be possible to obtain weaker information using the more elementary approach of [3] in the infinite prime case, and to generalize Rosen's work to higher rank in the finite prime case, in such a way that Gardeyn's bounds can be made explicit.

As for the terms g_ϕ, it would seem that this also requires some knowledge relating to the successive minima of the lattices associated to the uniformization of ϕ over infinite primes.

Finally, two other places of difference are in our use of [12] for the Chebotarev Density Theorem instead of [8], and in our analytic estimation methods, which differ slightly from both [6, 16], because we have attempted to reduce the size of the constants in the different divisor bound, especially in front of the dominating terms.

Acknowledgements. We would like to thank A. Cojocaru and C. David for useful discussions pertaining to the subject of this paper.

References

[1] A. Cojocaru and C. Hall, Uniform results for Serre's theorem for elliptic curves, Int. Math. Res. Not. no. 50 (2005) 3065–3080.

[2] I. Chen and Y. Lee, Newton polygons, successive minima, and different bounds for Drinfeld modules of rank 2, to appear in Proc. Amer. Math. Soc.

[3] I. Chen and Y. Lee, Coefficients of exponential functions attached to Drinfeld modules of rank 2, Manuscripta Math., DOI: 10.1007/s00229-011-0505-2, 2012.
[4] C. David, Frobenius distributions of Drinfeld modules of any rank, J. Number Theory 90 (2001), no. 2, 329–340.
[5] F. Gardeyn, t-motives and Galois representations, PhD thesis, ETH Zurich, 2001.
[6] F. Gardeyn, Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld, Arch. Math. 79 (2002), 241–251.
[7] E.-U. Gekeler, On finite Drinfeld modules, J. Algebra 141 (1991), 167–182.
[8] W.D. Geyer and M. Jarden, Bounded realization of ℓ-groups over global fields, Nagoya Math. J. 150 (1998), 13–62.
[9] D. Goss, Basic structures of function field arithmetic, Springer-Verlag, Berlin, 1996.
[10] D. Goss, L-series of t-motives and Drinfeld modules. In: The Arithmetic of Function Fields. D. Goss et al., eds., Proceedings of the workshop at Ohio State Univ. 1991. Berlin-New York, 313-402, 1992.
[11] A. Kraus, Une remarque sur les points de torsion des courbes elliptiques, C. R. Acad. Sci. Paris Sr. I Math. 321 (1995), no. 9, 1143–1146.
[12] V.K. Murty and J. Scherk, Effective versions of the Chebotarev density theorem for function fields, C. R. Acad. Sci. Paris Sr. I Math. 319 (1994), no. 6, 523–528.
[13] M. Rosen, Number Theory in Function Fields, Springer, 2002.
[14] J-P. Serre, Propriétés galoisiennes des points d'order fini des courbes elliptiques, Invent. Math. 15 (1972), 259-331.
[15] J-P. Serre, Local Fields, Graduate Texts in Math., Springer-Verlag, New York, 1979.
[16] J-P. Serre, Quelques applications du théorème de densité de Chebotarev, Inst. Hautes Etudes Sci. Publ. Math. No. 54 (1981), 323–401.
[17] Y. Taguchi, Ramifications arising from Drinfeld modules, in *The arithmetic of function fields* (Columbus, OH, 1991), 171–187, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992.
[18] Y. Taguchi, On ϕ-modules, J. Number Theory 60 (1996), 124–141.
[19] Y. Taguchi, Semi-simplicity of the Galois representations attached to Drinfeld modules over fields of "infinite characteristics", J. Number Theory, 44, no. 3 (1993), 292–314.
[20] T. Takahashi, Good reduction of elliptic modules, J. Math. Soc. Japan 34 (1982), 475–487.
[21] D.S. Thakur, Function field arithmetic, World Scientific Publishing Co., Inc., 2004.

Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, CANADA V5A 1S6, E-mail: ichen@math.sfu.ca

Department of Mathematics, Ewha Womans University, 11-1 Daehyun-Dong, Seodaemun-Gu, Seoul, 120-750, S. Korea, E-mail: yoonjinl@ewha.ac.kr