# CYCLICITY OF FINITE DRINFELD MODULES

WENTANG KUO AND YU-RU LIU

ABSTRACT. Let $A = \mathbb{F}_q[T]$ be the polynomial ring over the finite field $\mathbb{F}_q$, $k = \mathbb{F}_q(T)$ the rational function field, and $K$ a finite extension of $k$. For a prime $\mathfrak{P}$ of $K$, we denote by $\mathcal{O}_\mathfrak{P}$ the valuation ring of $\mathfrak{P}$, by $\mathcal{M}_\mathfrak{P}$ the maximal ideal of $\mathcal{O}_\mathfrak{P}$, and by $\mathbb{F}_\mathfrak{P}$ the residue field $\mathcal{O}_\mathfrak{P}/\mathcal{M}_\mathfrak{P}$. Let $\phi$ be a Drinfeld $A$-module over $K$ of rank $r$. If $\phi$ has good reduction at $\mathfrak{P}$, let $\phi \otimes \mathbb{F}_\mathfrak{P}$ denote the reduction of $\phi$ at $\mathfrak{P}$, and let $\phi(\mathbb{F}_\mathfrak{P})$ denote the $A$-module $(\phi \otimes \mathbb{F}_\mathfrak{P})(\mathbb{F}_\mathfrak{P})$. If $\phi$ is of rank 2 with $\mathrm{End}_{\bar{K}}(\phi) = A$, we obtain an asymptotic formula for the number of primes $\mathfrak{P}$ of $K$ of degree $x$ for which $\phi(\mathbb{F}_\mathfrak{P})$ is cyclic. This result can be viewed as a Drinfeld module analogue of Serre's cyclicity result on elliptic curves. We also show that when $\phi$ is of rank $r \geq 3$, a similar result follows.

## 1. INTRODUCTION

Let $A = \mathbb{F}_q[T]$ be the polynomial ring over the finite field $\mathbb{F}_q$ and $k = \mathbb{F}_q(T)$ the rational function field. An *$A$-field* $L$ is a field $L$ equipped with a morphism $\iota : A \to L$. The prime ideal $\mathfrak{w}$ which is the kernel of $\iota$ is called the *$A$-characteristic* of $L$. We say that $L$ has *generic $A$-characteristic* if $\mathfrak{w} = (0)$; otherwise we say $L$ has *finite $A$-characteristic*.

Let $L$ be an $A$-field, and let $\tau$ be the Frobenius endomorphism relative to $\mathbb{F}_q$, i.e., $\tau(X) = X^q$. In the ring $\mathrm{End}_L(\mathbb{G}_a)$ of all $L$-endomorphisms of the additive group scheme $\mathbb{G}_a|L$, by identifying the element $b \in L$ with the endomorphism defined by multiplication by $b$, $\tau$ generates a subalgebra $L\{\tau\}$. It is a non-commutative polynomial algebra in $\tau$ subject to the rule $\tau b = b^q \tau$ for all $b \in L$. We have two homomorphisms, $\epsilon : L \to L\{\tau\}$ defined by $\epsilon(b) = b$ and $D : L\{\tau\} \to L$ defined by $D(\sum_{i=0}^n b_i \tau^i) = b_0$.

A *Drinfeld $A$-module $\phi$ over $L$* is an algebra homomorphism

$$\phi : A \longrightarrow L\{\tau\} \subseteq \mathrm{End}_L(\mathbb{G}_a), \quad a \mapsto \phi_a$$

such that $\iota = D \circ \phi$ and $\phi \neq \epsilon \circ \iota$. Let $\deg_\tau \phi_a$ denote the degree of $\phi_a$ in $\tau$ and $\deg a$ the degree of $a$ in $T$. There exists a unique positive integer $r$ such that $\deg_\tau \phi_a = r \cdot \deg a$ for all $a \in A$ with $a \neq 0$ (see [4, Proposition 2.1]). The integer $r$ is called the *rank* of $\phi$. Let $B$ be an $L$-algebra. Then the composition

$$A \to \mathrm{End}_L(\mathbb{G}_a) \to \mathrm{End}(\mathbb{G}_a(B))$$

gives $B$ another $A$-module structure, which we denote by $\phi(B)$.

*Date*: September 24, 2023.

2000 *Mathematics Subject Classification.* Primary 11G09; Secondary 11R45, 11N36.

*Key words and phrases.* Drinfeld modules, cyclic components.

The research of the first author was supported by an NSERC discovery grant.

The research of the second author was supported by an NSERC discovery grant.

We now consider an $A$-field $K$, which is a finite extension of $k$ of degree $d$. Let $\mathbb{F}_K$ be the constant field of $K$, which is of degree $d_K$ over $\mathbb{F}_q$. Given a prime $\mathfrak{P}$ of $K$, let $\mathcal{O}_{\mathfrak{P}}$ be the valuation ring of $\mathfrak{P}$ and $\mathcal{M}_{\mathfrak{P}}$ the maximal ideal of $\mathcal{O}_{\mathfrak{P}}$. Let $\mathbb{F}_{\mathfrak{P}}$ denote the residue field $\mathcal{O}_{\mathfrak{P}}/\mathcal{M}_{\mathfrak{P}}$. Throughout this paper, we use "primes" to denote monic irreducible polynomials of $A$ and "primes" to denote discrete valuations of $K$.

Let $\phi$ be a Drinfeld $A$-module over $K$ of rank $r$. For all but finitely many primes $\mathfrak{P}$ of $K$, $\phi$ has good reduction at $\mathfrak{P}$ (see [10, Definition 4.10.1, p88]). Let $\mathcal{P}_\phi$ be the set of primes of $K$ at which $\phi$ has good reduction. For a prime $\mathfrak{P} \in \mathcal{P}_\phi$, we can consider $\phi \otimes \mathbb{F}_{\mathfrak{P}}$, *the reduction of* $\phi$ *at* $\mathfrak{P}$. Then we write $\phi(\mathbb{F}_{\mathfrak{P}})$ to denote the $A$-module $(\phi \otimes \mathbb{F}_{\mathfrak{P}})(\mathbb{F}_{\mathfrak{P}})$.

Since $\phi(\mathbb{F}_{\mathfrak{P}})$ is a finite $A$-module and $A$ is a principal ideal domain, we have

$$\phi(\mathbb{F}_{\mathfrak{P}}) \simeq A/w_1A \times A/w_2A \times \cdots \times A/w_sA, \tag{1}$$

where $w_i \in A \setminus \mathbb{F}_q$ $(1 \le i \le s)$ satisfy $w_i | w_{i-1}$ $(2 \le i \le s)$. We call each $A/w_iA$ a *cyclic component* of $\phi(\mathbb{F}_{\mathfrak{P}})$. The Euler-Poincaré characteristic $\chi_\phi(\mathfrak{P})$ of $\phi(\mathbb{F}_{\mathfrak{P}})$ is the ideal of $A$ equal to

$$\chi_\phi(\mathfrak{P}) = w_1 w_2 \cdots w_s A$$

in this case. In the following, we will abuse notation by using $\chi_\phi(\mathfrak{P})$ to denote both the ideal $\chi_\phi(\mathfrak{P})$ and its monic generator in $A$.

Given the finite $A$-module $\phi(\mathbb{F}_{\mathfrak{P}})$, one can consider the number of its cyclic components. For $m \in A$ with $m \neq 0$, let $\phi_{\mathfrak{P}}[m]$ denote the $m$-division points of $\phi \otimes \mathbb{F}_{\mathfrak{P}}$ in the algebraic closure $\bar{\mathbb{F}}_{\mathfrak{P}}$ of $\mathbb{F}_{\mathfrak{P}}$. Let $\mathfrak{p} = \mathfrak{P} \cap A$ and let $p \in A$ be the prime with $pA = \mathfrak{p}$. If $\phi$ is of rank $r$ and $(m, p) = 1$, we have [4, Proposition 2.2]

$$\phi_{\mathfrak{P}}[m] \simeq (A/mA)^r.$$

Since $\phi(\mathbb{F}_{\mathfrak{P}})$ is finite, there exists a polynomial $m \in A$ with $m \neq 0$ such that $\phi(\mathbb{F}_{\mathfrak{P}}) \subseteq \phi_{\mathfrak{P}}[m]$. It follows that $s \le r$ in (1).

Consider the special case when $K = k$ and $\phi = C$, the Carlitz $A$-module over $k$ (i.e., $\phi_T = T\tau^0 + \tau$ and $r = 1$). For a prime $l \in A$ and $\mathfrak{l} = lA$, we see from (1) that $C(\mathbb{F}_{\mathfrak{l}})$ is cyclic. One can indeed show that [9, Theorem 5.1]

$$C(\mathbb{F}_{\mathfrak{l}}) \simeq A/(l-1)A.$$

Although the structure of $C(\mathbb{F}_{\mathfrak{l}})$ is well-understood, for a general $\phi$ and a prime $\mathfrak{P} \in \mathcal{P}_\phi$, it is difficult to write down explicitly the cyclic components of $\phi(\mathbb{F}_{\mathfrak{P}})$. In the case that $\phi$ is of rank $r = 2$, $\phi(\mathbb{F}_{\mathfrak{P}})$ contains at most two cyclic components. One may ask how often $\phi(\mathbb{F}_{\mathfrak{P}})$ is a cyclic module. Define

$$f(x, \phi) = f^K(x, \phi) = \#\left\{\mathfrak{P} \in \mathcal{P}_\phi \;\middle|\; \deg_K \mathfrak{P} = x \text{ and } \phi(\mathbb{F}_{\mathfrak{P}}) \text{ is cyclic}\right\},$$

where $\deg_K \mathfrak{P} = [\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} : \mathbb{F}_K]$. Note that when there is no ambiguity, we will drop the superscript $K$ for $f^K(x, \phi)$ as above. In this paper, we will provide an asymptotic formula for the quantity $f(x, \phi)$.

Our estimate for $f(x, \phi)$ can be generalized to any $\phi$ of rank $r \ge 2$. In general, if $\phi$ is of rank $r \ge 2$ and $\phi(\mathbb{F}_{\mathfrak{P}})$ can be decomposed as in (1) with $s < r$, we say $\phi(\mathbb{F}_{\mathfrak{P}})$ *has at most*

$(r-1)$ *cyclic components*. For $x \in \mathbb{N}$, we consider the quantity

$$f(x,\phi) = \#\Big\{\mathfrak{P} \in \mathcal{P}_\phi \,\Big|\, \deg_K \mathfrak{P} = x \text{ and } \phi(\mathbb{F}_\mathfrak{P}) \text{ has at most } (r-1) \text{ cyclic components}\Big\}.$$

Let $\mathrm{End}_{\bar{K}}(\phi)$ denote the endomorphism ring of $\phi$ over the algebraic closure $\bar{K}$ of $K$. Let $\phi[m]$ be the $m$-division points of $\phi$ in the algebraic closure $\bar{K}$ of $K$. By adjoining to $K$ the $m$-division points of $\phi$, we obtain $K(\phi[m])$, the $m$-division field of $\phi$. We write $r_m$ to denote the degree of the constant field of $K(\phi[m])$ over $\mathbb{F}_K$, i.e., $r_m = [K(\phi[m]) \cap \bar{\mathbb{F}}_K : \mathbb{F}_K]$, where $\bar{\mathbb{F}}_K$ is the algebraic closure of $\mathbb{F}_K$. Let $\pi_K(x)$ denote the number of primes of $K$ of degree $x$. We will prove that

**Theorem 1.** *Let $\phi$ be a Drinfeld $A$-module over $K$ of rank $r \geq 2$ with $\mathrm{End}_{\bar{K}}(\phi) = A$. For $x \in \mathbb{N}$, we have*

$$f(x,\phi) = c_\phi(x)\,\pi_K(x) + O_\phi\big((q^{d_K x})^{\Delta_r}\big),$$

*where*

$$\Delta_r = \begin{cases} \frac{r^2+4r-2}{2r^2+2r} & \text{if } r = 2,3, \\ \frac{r+2}{2r} & \text{if } r \geq 4, \end{cases} \tag{2}$$

*and*

$$c_\phi(x) = c_\phi^K(x) = \sum_{\substack{m \in A \\ m \text{ is monic}}} \frac{\mu_q(m)\, r_m(x)}{[K(\phi[m]) : K]} \tag{3}$$

*with $\mu_q(\cdot)$ denoting the Möbius function in $A$ and*

$$r_m(x) = \begin{cases} r_m & \text{if } r_m | x, \\ 0 & \text{otherwise.} \end{cases}$$

Note that when there is no ambiguity, we will drop the superscript $K$ for $c_\phi^K$ as above. As a direct consequence of Theorem 1, we have

**Corollary 2.** *Let $\phi$ be a Drinfeld $A$-module over $K$ of rank $r \geq 2$ with $\mathrm{End}_{\bar{K}}(\phi) = A$. Suppose that all division fields of $\phi$ are geometric. For $x \in \mathbb{N}$, we have*

$$f(x,\phi) = c_\phi\,\pi_K(x) + O_\phi\big((q^{d_K x})^{\Delta_r}\big),$$

*where $\Delta_r$ is defined as in* (2) *and*

$$c_\phi = \sum_{\substack{m \in A \\ m \text{ is monic}}} \frac{\mu_q(m)}{[K(\phi[m]) : K]}.$$

Let $E$ be an elliptic curve of conductor $N$ defined over $\mathbb{Q}$. For a rational prime $p$ with $p \nmid N$, let $E(\mathbb{F}_p)$ denote the set of rational points on $E$ defined over the finite field $\mathbb{F}_p$. Define

$$g(x,E) = \#\Big\{p \,\Big|\, p \leq x,\, p \nmid N, \text{ and } E(\mathbb{F}_p) \text{ is cyclic}\Big\}.$$

Let $\operatorname{li} x = \int_2^x \frac{dt}{\log t}$ and

$$c_E = \sum_{n \in \mathbb{N}} \frac{\mu(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q})]}, \tag{4}$$

where $\mu(\cdot)$ denotes the Möbius function in $\mathbb{Z}$ and $\mathbb{Q}(E[n])$ denotes the $n$-division field of $E$. In [17] (see also [12, Theorem 2]), Serre proved that if $E$ is an elliptic curve without complex multiplication, assuming the generalized Riemann hypothesis (GRH), we have

$$g(x, E) = c_E \operatorname{li} x + \operatorname{error}(x, E),$$

where

$$\operatorname{error}(x, E) = o\Big(\frac{x}{\log x}\Big).$$

The error term in Serre's estimate has recently been improved by Cojocaru and R. Murty in [2, Theorem 1.1], where they obtained

$$\operatorname{error}(x, E) = O_E\Big(x^{5/6} (\log x)^{2/3}\Big).$$

Let $\phi$ be a Drinfeld $A$-module over $K$ of rank 2 with $\operatorname{End}_{\bar{K}}(\phi) = A$. Suppose that all division fields of $\phi$ are geometric. From Corollary 2, we have

$$\begin{aligned} f(x, \phi) &= \#\Big\{\mathfrak{P} \in \mathcal{P}_\phi \,\Big|\, \deg_K \mathfrak{P} = x \text{ and } \phi(\mathbb{F}_\mathfrak{P}) \text{ is cyclic}\Big\} \\ &= c_\phi\, \pi_K(x) + O_\phi\big((q^{d_K x})^{5/6}\big). \end{aligned}$$

Hence, this special case of Theorem 1 provides an unconditional Drinfeld module analogue of Serre's cyclicity result on elliptic curves. Due to a better version of the Chebotarev density theorem for function fields, the above error term is modestly sharper than the result of Cojocaru and R. Murty

For an elliptic curve $E/\mathbb{Q}$, Serre proved that the constant $c_E$ defined in (4) is positive whenever $\mathbb{Q}(E[2]) \neq \mathbb{Q}$ (see [2, Section 6]). One could consider the positivity of the value $c_\phi(x)$ defined in (3). Since $c_\phi(x)$ depends on the field $K$, the number $x$, and the division fields of $\phi$, it seems difficult to give a general solution to this problem. However, in the special case when $K = k$, the rational function field, and all division fields of $\phi$ are geometric, we have a definite answer to this question.

**Theorem 3.** *Let $\phi$ be a Drinfeld $A$-module over $k$ of rank $r \geq 2$ with $\operatorname{End}_{\bar{k}}(\phi) = A$. Suppose that all division fields of $\phi$ are geometric. Let $c_\phi$ be defined as in Corollary 2. Then $c_\phi$ is positive if and only if $k(\phi[a]) \neq k$ for all $a \in A$ of degree 1.*

Despite the similarity amongst elliptic curves and Drinfeld modules, there are still several intrinsic differences between their structures. For example, an elliptic curve $E$ over $\mathbb{Q}$ corresponds to a Drinfeld $A$-module $\phi$ over $k$ of rank $r = 2$, whose division fields are all geometric. Theorem 1 holds for any Drinfeld $A$-module $\phi$ over a finite extension $K$ of $k$, $\phi$ can be of any rank $r \geq 2$, and the division fields of $\phi$ are not necessarily geometric. Thus modifications of the proofs of Serre and Cojocaru-Murty are required in order to derive this more general result. Furthermore, for an elliptic curve $E/\mathbb{Q}$, to prove the positivity of the constant $c_E$, one utilizes the relation between division fields of $E$ and cyclotomic number fields to estimate certain quantities. For a general Drinfeld $A$-module $\phi$ over $K$, its associated rank 1 $A$-module over $K$ is not necessarily the Carlitz $A$-module $C$. Hence we can not apply analogous properties of cyclotomic function fields (i.e., division fields of $C$) in our proof. To overcome this difficulty, we axiomatize the proof of [2, Corollary 6.2] to obtain the result in a more abstract setting (see Lemma 14), and this allows us to prove Theorem 3.

In the next section, we state a theorem on the adelic openness for Drinfeld modules and recall the Chebotarev density theorem for function fields. In Section 3, we prove some results concerning division fields of $\phi$ which are required in the proof of Theorem 1. We prove Theorem 1 in Section 4, and we conclude this paper by proving Theorem 3 in Section 5.

In this paper, we only consider a Drinfeld $A$-module $\phi$ over $K$, where $\mathrm{End}_{\bar{K}}(\phi) = A$ and the $A$-field $K$ is of generic characteristic. One could also estimate the quantity $f(x, \phi)$ when $\mathrm{End}_{\bar{K}}(\phi) \neq A$ or when $K$ is of finite characteristic. Moreover, Serre's cyclicity result can be viewed as a subproblem of a conjecture of Lang and Trotter on primitive points on elliptic curves. Thus one could ask an analogous question for Drinfeld modules. We intend to return to these matters in future papers.

**Notation** For $x \in \mathbb{N}$, let $f(x)$ and $g(x)$ be functions of $x$. If $g(x)$ is positive and there exists a constant $c > 0$ such that $|f(x)| \leq cg(x)$, we write either $f(x) \ll g(x)$ or $f(x) = O(g(x))$. If $\lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 0$, we write $f(x) = o(g(x))$. We will take the convention here that when we write $\ll$ or $O$, the implicit constant depends only on the field $K$. If the implicit constant also depends on the module $\phi$, then we write $\ll_\phi$ or $O_\phi$.

## 2. Preliminaries

The most important ingredients in our proof are the theorem of Pink and Rütsche on the adelic openness for Drinfeld modules and the Chebotarev density theorem for function fields. In this section, we recall some related results.

Let $L$ be an $A$-field with $A$-characteristic $\mathfrak{w}$, and let $\phi$ be a Drinfeld $A$-module over $L$ of rank $r$. For $m \in A$ with $m \neq 0$ and $m$ is coprime to $\mathfrak{w}$, we denote by $\phi[m]$ the $m$-division points of $\phi$ in the algebraic closure $\bar{L}$ of $L$. By adjoining to $L$ the $m$-division points, we obtain $L(\phi[m])$, the $m$-division field of $\phi$, which is a finite Galois extension of $L$. We have [4, Proposition 2.2]

$$\phi[m] \simeq (A/mA)^r.$$

By choosing a basis, we have a natural injection

$$\Phi_m : \mathrm{Gal}(L(\phi[m])/L) \hookrightarrow \mathrm{Aut}(\phi[m]) \simeq \mathrm{GL}_r(A/mA).$$

For a prime $l \in A$ coprime to $\mathfrak{w}$, let

$$\phi[l^\infty] = \bigcup_{n\in\mathbb{N}} \phi[l^n],$$

be the direct limit of the $l^n$-division points of $\phi$. Let $A_l$ and $k_l$ be the completion of $A$ and $k$ at $l$ respectively. The *$l$-adic Tate module of $\phi$*, $T_l(\phi)$, is defined to be

$$T_l(\phi) = \mathrm{Hom}_{A_l}(k_l/A_l, \phi[l^\infty]),$$

which is a free $A_l$-module of rank $r$. By choosing a basis, we have the *$l$-adic representation $\rho_{l,\phi}$ of $\phi$* defined by

$$\rho_{l,\phi} : \mathrm{Gal}(L^{\mathrm{sep}}/L) \to \mathrm{Aut}(T_l(\phi)) \simeq \mathrm{GL}_r(A_l),$$

where $L^{\text{sep}}$ is the maximal separable extension of $L$. By putting together the $l$-adic representations $\rho_l$, we obtain a continuous representation

$$\rho_\phi = \prod_l \rho_{l,\phi} : \text{Gal}(L^{\text{sep}}/L) \to \text{GL}_r(\hat{A}),$$

where $\hat{A}$ is the profinite completion of $A$. The following theorem is about the openness of $\rho_\phi$. The case $r = 2$ is proved by Gardeyn and Pink, and the general case is recently obtained by Pink and Rütsche.

**Theorem 4.** (Gardeyn[7, Remark 3.15] [8, Remark 1.16], Pink [13, Theorem 0.1], Pink and Rütsche [14, Theorem 0.1]) *Let $L$ be a finitely generated $A$-field of generic $A$-characteristic, and let $\phi$ be a Drinfeld $A$-module over $L$ $\text{End}_{\bar{L}}(\phi) = A$. Then the image of $\rho_\phi$ is open.*

Now we come back to our original setting. Let $A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$. Consider the $A$-field $K$, which is a finite extension of $k$ of degree $d$. Let $\mathbb{F}_K$ be the constant field of $K$, which is of degree $d_K$ over $\mathbb{F}_q$ . Let $\phi$ be a Drinfeld $A$-module over $K$, and let $\mathcal{P}_\phi$ be the set of primes of $K$ at which $\phi$ has good reduction.

The following lemma is a direct consequence of Theorem 4.

**Proposition 5.** *Let $\phi$ be a Drinfeld $A$-module over $K$ with $\text{End}_{\bar{K}}(\phi) = A$ and of rank $r \geq 2$. There exists $B(\phi) \in A$ (depending only on $\phi$) such that for every $m \in A$ with $(m, B(\phi)) = 1$, the map $\Phi_m$ is an isomorphism.*

For a prime $\mathfrak{P}$ of $K$, let $\mathfrak{p} = \mathfrak{P} \cap A$ and let $p \in A$ be the prime with $pA = \mathfrak{p}$. Let $l \in A$ be a prime with $(l, p) = 1$. By the work of Drinfeld [4] on the theory of good reduction, which is analogous to the classical result of Ogg-Néron-Shafarevich for elliptic curves, $\phi$ has good reduction at $\mathfrak{P}$ if and only if $K(\phi[l^\infty])/K$ is unramified at $\mathfrak{P}$ for all primes $l \in A$ with $(l, p) = 1$. In this case, let $\sigma_\mathfrak{P}$ be the Artin symbol of $\mathfrak{P}$ in $\text{Gal}(K(\phi[l^\infty])/K)$, and let $\phi \otimes \mathbb{F}_\mathfrak{P}$ be the Drinfeld module over $\mathbb{F}_\mathfrak{P}$ which is the reduction of $\phi$ at $\mathfrak{P}$. Then one can identify $T_l(\phi)$ and $T_l(\phi \otimes \mathbb{F}_\mathfrak{P})$, and the action of $\sigma_\mathfrak{P}$ is the same as that of the Frobenius of $\mathbb{F}_\mathfrak{P}$. Moreover, the characteristic polynomial of $\sigma_\mathfrak{P}$ on $T_l(\phi)$ is independent of $l$ (see [9, Corollary 3.4] and [19, Theorem 2(b)]), and we denoted it by $P_{\mathfrak{P},\phi}(X)$.

**Proposition 6.** ([9, Theorem 5.1]) *Let $\mathfrak{P}$ be a prime in $\mathcal{P}_\phi$. Then as ideals of $A$,*

$$\mathfrak{p}^{m_\mathfrak{P}} = P_{\mathfrak{P},\phi}(0)A \qquad \text{and} \qquad \chi_\phi(\mathfrak{P}) = P_{\mathfrak{P},\phi}(1)A,$$

*where $m_\mathfrak{P} = [\mathbb{F}_\mathfrak{P} : A/\mathfrak{p}]$.*

We remark here that by Proposition 6, $p^{m_\mathfrak{P}}$ (resp. $\chi_\phi(\mathfrak{P})$) and $P_{\mathfrak{P},\phi}(0)$ (resp. $P_{\mathfrak{P},\phi}(1)$) differ by at most an element of $\mathbb{F}_q^*$ as polynomials of $A$. Also, since $|\phi(\mathbb{F}_\mathfrak{P})|$, the cardinality of $\phi(\mathbb{F}_\mathfrak{P})$, is equal to $|\mathbb{F}_\mathfrak{P}|$, $\deg_K \mathfrak{P} = [\mathbb{F}_\mathfrak{P} : \mathbb{F}_K]$, and $[\mathbb{F}_K : \mathbb{F}_q] = d_K$, we have

$$d_K \deg_K \mathfrak{P} = \deg \chi_\phi(\mathfrak{P}) = \deg P_{\mathfrak{P},\phi}(1), \tag{5}$$

where $\deg \chi_\phi(\mathfrak{P})$ and $\deg P_{\mathfrak{P},\phi}(1)$ are the degrees of $\chi_\phi(\mathfrak{P})$ and $P_{\mathfrak{P},\phi}(1)$ in $T$, respectively.

We now state the Chebotarev density theorem for function fields. For a finite Galois extension $L/K$, we denote by $G$ the Galois group of $L/K$ and by $\mathcal{C}$ a union of conjugacy

classes of $G$. For $x \in \mathbb{N}$, define

$$\pi_{\mathcal{C}}\big(x, L/K\big) = \#\Big\{\mathfrak{P} \;\Big|\; \deg_K \mathfrak{P} = x,\ \mathfrak{P} \text{ is a prime unramified in } L/K, \text{ and } \sigma_{\mathfrak{P}} \subseteq \mathcal{C}\Big\},$$

where $\sigma_{\mathfrak{P}}$ is the Artin symbol of $\mathfrak{P}$ in $\mathrm{Gal}(L/K)$. Let $r_L = [L \cap \bar{\mathbb{F}}_K : \mathbb{F}_K]$.

**Theorem 7.** ([5, Proposition 6.4.8]) *Let $L/K$ be a finite Galois extension with Galois group $G$. Let $\mathcal{C} \subseteq G$ be a conjugacy class whose restriction to $\mathbb{F}_L$ is the $a$-th power of the Frobenius automorphism of $\mathbb{F}_K$. Then for $x \in \mathbb{N}$, if $x \not\equiv a \pmod{r_L}$, we have*

$$\pi_{\mathcal{C}}(x, L/K) = 0.$$

*If $x \equiv a \pmod{r_L}$, we have*

$$\begin{aligned}\Big|\pi_{\mathcal{C}}\big(x, L/K\big) - r_L \frac{|\mathcal{C}|}{|G|}\frac{q^{d_K x}}{x}\Big| &\\ \leq \frac{2|\mathcal{C}|}{x|G|}\Big((|G| + g_L r_L)(q^{d_K x})^{1/2} + |G|(2g_K+1)(q^{d_K x})^{1/4} + g_L r_L + |G|d/d_K\Big),&\end{aligned}$$

*where $g_L$ and $g_K$ are the genus of $L$ and $K$, respectively.*

Let $\pi_K(x)$ denote the number of primes of $K$ of degree $x$. Applying Theorem 7 with $L = K$, we get

$$\pi_K(x) = \frac{q^{d_K x}}{x} + O\bigg(\frac{(q^{d_K x})^{1/2}}{x}\bigg).$$

Moreover, in the special case when $\mathcal{C}$ consists only of the identity element in $\mathrm{Gal}(L/K)$, we have $a = 0$ and $\pi_{\mathcal{C}}(x, L/K)$ counts the number of primes $\mathfrak{P}$ of $K$ of degree $x$ which split completely in $L$. As a direct consequence of Theorem 7, we have

**Theorem 8.** *Given a Drinfeld $A$-module $\phi$ over $K$, let $\pi_1(x, L/K)$ denote the number of primes $\mathfrak{P} \in \mathcal{P}_\phi$ such that $\deg_K \mathfrak{P} = x$ and $\mathfrak{P}$ splits completely in $L$. Then for $x \in \mathbb{N}$, if $r_L \nmid x$, we have*

$$\pi_1(x, L/K) = 0.$$

*If $r_L | x$, we have*

$$\Big|\pi_1\big(x, L/K\big) - r_L \frac{1}{|G|}\pi_K(x)\Big| \ll \bigg(\frac{g_L r_L}{|G|} + 1\bigg)\frac{(q^{d_K x})^{1/2}}{x},$$

*where the implicit constant depends only on $K$.*

In order to estimate the error term in Theorem 8 when $L = K(\phi[m])$, we need the following result.

**Proposition 9.** ([6, Corollary 7]) *There exists a constant $D(\phi)$ (depending only on $\phi$) such that for each $m \in A \setminus \mathbb{F}_q$,*

$$g_{K(\phi[m])} \ll D(\phi) \cdot [K(\phi[m]) : K] \cdot \deg m,$$

*where the implicit constant depends only on the field $K$.*

The following proposition shows that the degrees over $\mathbb{F}_K$ of the constant fields of $K(\phi[m])$ are bounded absolutely.

**Proposition 10.** ([3, Lemma 3.2]), [10, Remark 7.1.9]) *Let $\phi$ be a Drinfeld $A$-module over $K$, and let $K_\phi$ be the field obtained by adjoining to $K$ all division points of $\phi$. Then we have*

$$E(\phi) = [K_\phi \cap \bar{\mathbb{F}}_K : \mathbb{F}_K] < \infty.$$

We remark that although in [3, Lemma 3.2] Gekeler proved the above result only for $K = k$, his argument can be extended to a finite extension $K$ of $k$ without modification.

## 3. Division fields of $\phi$

Let $\phi$ be a Drinfeld $A$-module over $K$, and let $\mathcal{P}_\phi$ be the set of primes of $K$ at which $\phi$ has good reduction. In this section, we prove some properties about division fields of $\phi$. We will need these results later in our proof of Theorem 1. For a prime $\mathfrak{P} \in \mathcal{P}_\phi$, write

$$\phi(\mathbb{F}_\mathfrak{P}) \simeq A/w_1A \times A/w_2A \times \cdots \times A/w_sA,$$

where $w_i \in A \setminus \mathbb{F}_q$ $(1 \le i \le s)$ satisfy $w_i | w_{i-1}$ $(2 \le i \le s)$. For $m \in A$ and $n \in \mathbb{N}$ with $n \le s$, if $m | w_n$, then

$$(A/mA)^n \times (A/A)^{s-n} \subseteq A/w_1A \times \cdots \times A/w_nA \times A/w_{n+1}A \times \cdots \times A/w_sA.$$

In this case, we say that $\phi(\mathbb{F}_\mathfrak{P})$ *contains an $(A/mA)^n$-type submodule.*

**Proposition 11.** *Let $K$ be a finite extension of $k$ of degree $d$, and let $\mathbb{F}_K$ be the constant field of $K$, which is of degree $d_K$ over $\mathbb{F}_q$. Let $\phi$ be a Drinfeld $A$-module over $K$ of rank $r \ge 2$. For a prime $\mathfrak{P} \in \mathcal{P}_\phi$, let $\mathfrak{p} = \mathfrak{P} \cap A$ and let $p \in A$ be the prime with $pA = \mathfrak{p}$.*
(i) *For $m \in A$ with $(m, p) = 1$, the finite $A$-module $\phi(\mathbb{F}_\mathfrak{P})$ contains an $(A/mA)^r$-type submodule if and only if $\mathfrak{P}$ splits completely in $K(\phi[m])$.*
(ii) *The module $\phi(\mathbb{F}_\mathfrak{P})$ contains at most $(r-1)$ cyclic components if and only if $\mathfrak{P}$ does not split completely in $K(\phi[l])$ for all primes $l \in A$ with $l \ne p$.*
(iii) *Let $P_{\mathfrak{P},\phi}(X)$ be the characteristic polynomial of $\mathfrak{P}$ with respect to $\phi$. If $\mathfrak{P}$ splits completely in $K(\phi[m])$, then $m^r | P_{\mathfrak{P},\phi}(1)$.*

*Proof:* (i) For a prime $\mathfrak{P} \in \mathcal{P}_\phi$, let

$$\tau_\mathfrak{P} : \phi(\bar{F}_\mathfrak{P}) \longrightarrow \phi(\bar{F}_\mathfrak{P})$$

be the Frobenius of $\mathbb{F}_\mathfrak{P}$; thus the kernel $\ker(\tau_\mathfrak{P} - 1) = \phi(\mathbb{F}_\mathfrak{P})$. Since $(m, p) = 1$, we have $\phi_\mathfrak{P}[m] \simeq (A/mA)^r$ [4, Proposition 2.2]. Hence $\phi(\mathbb{F}_\mathfrak{P})$ contains an $(A/mA)^r$-type submodule if and only if its $m$-division points $\phi_\mathfrak{P}[m]$ are contained in $\phi(\mathbb{F}_\mathfrak{P}) = \ker(\tau_\mathfrak{P} - 1)$. In other words,

$$(A/mA)^r \subseteq \phi(\mathbb{F}_\mathfrak{P}) \iff \tau_\mathfrak{P} \text{ acts trivially on } \phi_\mathfrak{P}[m]. \tag{6}$$

For a prime $\mathfrak{P} \in \mathcal{P}_\phi$ with $(m, p) = 1$, $\mathfrak{P}$ is unramified in $K(\phi[m])$ and we write $\sigma_\mathfrak{P}$ to denote the Artin symbol of $K(\phi[m])/K$. From the work of Drinfeld [4] on Drinfeld module analogues of the classical results of Ogg-Néron-Shafarevich for elliptic curves, $\tau_\mathfrak{P}$ acts trivially on $\phi_\mathfrak{P}[m]$ if and only $\sigma_\mathfrak{P}$ acts trivially on $\phi[m]$, i.e.,

$$\tau_\mathfrak{P} \text{ acts trivially on } \phi_\mathfrak{P}[m] \iff \mathfrak{P} \text{ splits completely in } K(\phi[m]). \tag{7}$$

Combining (6) and (7), Statement (i) follows.
(ii) Note that the subscheme of $p$-torsion points is non-reduced, and hence the $p$-torsion of

$\phi(F)$ is of rank at most $r-1$ for any $A$-field $F$ of characteristic $p$. Hence, to conclude that $\phi(\mathbb{F}_{\mathfrak{P}})$ has at most $(r-1)$ cyclic components, it is equivalent to have $(A/lA)^r \not\subseteq \phi(\mathbb{F}_{\mathfrak{P}})$ for all primes $l \in A$ with $(l,p)=1$. Then (ii) follows from (i).
(iii) From (i), if $\mathfrak{P}$ splits completely in $K(\phi[m])$, then $m^r$ divides $\chi_\phi(\mathfrak{P})$. By Proposition 6, (iii) follows.

**Proposition 12.** *Let $\phi$ be a Drinfeld $A$-module over $K$ of rank $r \geq 2$ with $\mathrm{End}_{\bar{K}}(\phi) = A$, and let $B(\phi)$ be defined as in Proposition 5. For a monic polynomial $m \in A$, we can write it uniquely as $m = m_1 m_2$, where $m_1, m_2 \in A$ are monic, $m_1$ composed of primes which are divisors of $B(\phi)$, and $m_2$ composed of primes which are coprime to $B(\phi)$. Let $n(m)$ denote the cardinality of the Galois group $\mathrm{Gal}(K(\phi[m])/K)$. We have*

$$n(m) \gg \varphi(m_2)\, q^{(r^2-1)\deg m_2},$$

*where $\varphi(m_2) = \left|(A/m_2A)^*\right|$ is the Euler $\varphi$-function of $m_2 \in A$.*

*Proof:* We first note that $K(\phi[m_2]) \subseteq K(\phi[m])$. Since $(m_2, B(\phi)) = 1$, by Proposition 5, we have $n(m_2) = \left|\mathrm{GL}_r(A/m_2A)\right|$. Hence we have

$$\begin{aligned} n(m) \geq n(m_2) &= q^{r^2 \deg m_2} \prod_{l \mid m_2} \Big(1 - \frac{1}{q^{\deg l}}\Big)\Big(1 - \frac{1}{q^{2\deg l}}\Big)\cdots\Big(1 - \frac{1}{q^{r\deg l}}\Big) \\ &= \varphi(m_2)\, q^{(r^2-1)\deg m_2} \prod_{l \mid m_2} \Big(1 - \frac{1}{q^{2\deg l}}\Big)\cdots\Big(1 - \frac{1}{q^{r\deg l}}\Big), \end{aligned}$$

where the product is over distinct primes $l | m_2$. Since

$$\prod_{l \mid m_2} \Big(1 - \frac{1}{q^{2\deg l}}\Big)\cdots\Big(1 - \frac{1}{q^{r\deg l}}\Big) \gg \prod_{l:\,\text{prime}} \Big(1 - \frac{1}{q^{2\deg l}}\Big)\cdots\Big(1 - \frac{1}{q^{r\deg l}}\Big) \gg 1,$$

the proposition follows.

## 4. Proof of Theorem 1

Let $K$ be a finite extension of $k$ of degree $d$, and let $\mathbb{F}_K$ be the constant field of $K$, which is of degree $d_K$ over $\mathbb{F}_q$. Given a Drinfeld $A$-module $\phi$ over $K$, in this section, we provide a proof of Theorem 1 for it. Although the error term which we state in Theorem 1 depends on $\phi$, it can be made more precise in our proof. In the following, we will prove:

**Theorem 1'.** *Let $\phi$ be a Drinfeld $A$-module over $K$ of rank $r \geq 2$ with $\mathrm{End}_{\bar{K}}(\phi) = A$, and let $B(\phi)$, $D(\phi)$, and $E(\phi)$ be defined as in Propositions 5, 9, and 10. For $x \in \mathbb{N}$, we have*

$$f(x,\phi) = c_\phi(x)\,\pi_K(x) + \mathrm{error}(x,\phi),$$

*where*

$$c_\phi(x) = \sum_{\substack{m \in A \\ m \text{ is monic}}} \frac{\mu_q(m)\, r_m(x)}{[K(\phi[m]) : K]}$$

*and*

$$\mathrm{error}(x,\phi) \ll D(\phi)E(\phi)(q^{d_K x})^{\Delta_r} \;+\; E(\phi)\, x^{-1} \log x (q^{d_K x})^{\delta_r} q^{r^2 \deg B(\phi)}.$$

*Here, the implicit constant depends only on $K$, $\Delta_r$ is defined as in* (2)*, and*

$$\delta_r = \begin{cases} \frac{-3r^2+7r-2}{2r} & \text{if } r = 2, 3, \\ \frac{-r^2+r+1}{r} & \text{if } r \geq 4. \end{cases} \tag{8}$$

Before starting the proof of Theorem 1', we need to introduce more notation. Let $K\{\tau\}$ be the non-commutative polynomial algebra in $\tau$ defined by $\tau b = b^q \tau$ for all $b \in K$. Let $\phi$ be a Drinfeld $A$-module over $K$ of rank $r$, and let $M(\phi)$ be the A-motive associated to $\phi$ as defined in [18, Definition 2.1]. In [18, Corollary 3.2.3], van der Heiden showed that there exists an $A$-module $\psi_\phi$ over $K$ of rank 1 such that as $K\{\tau\}[T]$-modules, the exterior product $\Lambda^r_{k[T]} M(\phi)$ is isomorphic to the A-motive $M(\psi_\phi)$. Using the existence of $\psi_\phi$, he constructed a "Weil paring" - an $r$-multilinear map like a determinant object - for $\phi$ (see [18, Section 5]).

For $m \in A$ with $m \neq 0$, by using the Galois-invariance of the Weil pairing, one can derive from [18, Theorem 5.3] that the $m$-division field of $\psi_\phi$, $K(\psi_\phi[m])$, is contained in $K(\phi[m])$. Thus, given a Drinfeld $A$-module $\phi$ of rank $r$, we can associate to it a Drinfeld $A$-module $\psi_\phi$ of rank 1 satisfying

$$K(\psi_\phi[m]) \subseteq K(\phi[m])$$

for all $m \in A$ with $m \neq 0$. As a consequence, if $\phi$ has good reduction at a prime $\mathfrak{P}$ of $K$, then $\psi_\phi$ also has good reduction at $\mathfrak{P}$. For $\mathfrak{P} \in \mathcal{P}_\phi$, we denote by $P_{\mathfrak{P},\phi}(X)$ and $P_{\mathfrak{P},\psi_\phi}(X)$ the characteristic polynomials of the Frobenius of $\mathbb{F}_\mathfrak{P}$ acting on the Tate modules of $\phi$ and $\psi_\phi$, respectively.

For a finite extension $L/K$, let

$$\pi_1\big(x, L/K\big) = \#\Big\{\mathfrak{P} \in \mathcal{P}_\phi \;\Big|\; \deg_K \mathfrak{P} = x \text{ and } \mathfrak{P} \text{ splits completely in } L/K\Big\}$$

be defined as in Theorem 8. Also, for a monic polynomial $m \in A$, we denote by $n(m)$ the cardinality of the Galois group $\mathrm{Gal}(K(\phi[m])/K)$ and by $g(m)$ the genus of the field $K(\phi[m])$. We recall that if $r_m = [K(\phi[m]) \cap \overline{\mathbb{F}}_K : \mathbb{F}_K]$, then

$$r_m(x) = \begin{cases} r_m & \text{if } r_m | x, \\ 0 & \text{otherwise.} \end{cases}$$

Now, we are ready to prove Theorem 1'.

*Proof:* We recall that $[K : k] = d$. Let $\sum$ denote a sum over monic polynomials $m$ of $A$. By Proposition 11(ii) and the inclusion-exclusion principle, we have

$$f(x, \phi) = \sum_{m \in A} \mu_q(m)\, \pi_1\big(x, K(\phi[m])/K\big).$$

By Proposition 11(iii), a prime $\mathfrak{P}$ splits completely in $K(\phi[m])$ implies that $m^r | P_{\mathfrak{P},\phi}(1)$. Since $\deg P_{\mathfrak{P},\phi}(1) = d_K \deg_K \mathfrak{P} = d_K x$ (see (5) in Section 2), it suffices to consider $m \in A$ with $\deg m \leq d_K x/r$. Let $y = y(x) \in \mathbb{N}$ with $y \leq d_K x/r$ (a choice of $y$ will be made later).

Then we can write

(9)
$$\begin{aligned} f(x,\phi) &= \sum_{\deg m \le d_K x/r} \mu_q(m)\,\pi_1\big(x, K(\phi[m])/K\big) \\ &= \sum_{\deg m \le y} \mu_q(m)\,\pi_1\big(x, K(\phi[m])/K\big) + \sum_{y<\deg m \le d_K x/r} \mu_q(m)\,\pi_1\big(x, K(\phi[m])/K\big) \\ &= \text{main} + \text{error} \qquad \text{(say)}. \end{aligned}$$

The first sum in (9) will be the dominant term. From Theorem 8, we have

$$\text{main} = \sum_{\deg m \le y} \mu_q(m) \left( \frac{\pi_K(x)\, r_m(x)}{n(m)} + O\Big( \Big( \frac{g(m) r_m(x)}{n(m)} + 1 \Big) \frac{(q^{d_K})^{x/2}}{x} \Big) \right).$$

By Propositions 9 and 10, since $y < d_K x/r \ll x$, we have

$$\sum_{\deg m \le y} \left( \frac{g(m) r_m(x)}{n(m)} + 1 \right) \ll \sum_{\deg m \le y} D(\phi)\, E(\phi)\, \deg m \ll D(\phi)\, E(\phi)\, x\, q^y.$$

Hence, it follows that

$$\text{main} = \pi_K(x) \left( \sum_{\deg m \le y} \frac{\mu_q(m)\, r_m(x)}{n(m)} \right) + O\Big( D(\phi)\, E(\phi)\, q^{\frac{d_K x}{2} + y} \Big). \tag{10}$$

We now estimate the error term in (9). Let $\mathfrak{p} = \mathfrak{P} \cap A$ and let $p \in A$ be the prime with $pA = \mathfrak{p}$. By Proposition 6, we have

$$P_{\mathfrak{P},\phi}(X) = X^r + a_{r-1,\phi}(\mathfrak{P}) X^{r-1} + \cdots + a_{1,\phi}(\mathfrak{P}) X + u_{\mathfrak{P}} p^{m_{\mathfrak{P}}}$$

and

$$P_{\mathfrak{P},\psi_\phi}(X) = X + v_{\mathfrak{P}} p^{m_{\mathfrak{P}}},$$

where $a_{i,\phi}(\mathfrak{P}) \in A$ $(1 \le i \le r-1)$ and $u_{\mathfrak{P}}, v_{\mathfrak{P}} \in \mathbb{F}_q^*$. Let

$$b_\phi(\mathfrak{P}) = a_{r-1,\phi}(\mathfrak{P}) + \cdots + a_{1,\phi}(\mathfrak{P}).$$

For a fixed $m \in A$, $u, v \in \mathbb{F}_q^*$, and $b \in A$, define

$$\begin{aligned} S_{u,v,b}(m,x) = \Big\{ \mathfrak{P} \in \mathcal{P}_\phi \;\big|\; & \deg_K \mathfrak{P} = x,\ u_{\mathfrak{P}} = u,\ v_{\mathfrak{P}} = v,\ b_\phi(\mathfrak{P}) = b, \\ & \text{and } \mathfrak{P} \text{ splits completely in } K(\phi[m])/K \Big\}. \end{aligned}$$

Since $\deg_K \mathfrak{P} = x$ and $[\mathbb{F}_K : \mathbb{F}_q] = d_K$, from [9, Theorem 5.1], we have $\deg b_\phi(\mathfrak{P}) \le \frac{r-1}{r} d_K x$. Also, since $K(\psi_\phi[m]) \subseteq K(\phi[m])$, if $\mathfrak{P}$ splits completely in $K(\phi[m])$, then it also splits completely in $K(\psi_\phi[m])$. By Proposition 11(iii), we have $m^r | P_{\mathfrak{P},\phi}(1)$ and $m | P_{\mathfrak{P},\psi_\phi}(1)$. Hence, if $\mathfrak{P} \in S_{u,v,b}(m,x)$, we have $m^r | (1 + b + u p^{m_{\mathfrak{P}}})$ and $m | (1 + v p^{m_{\mathfrak{P}}})$. It follows that $m | (1 + b - uv^{-1})$, where $v^{-1}$ is the inverse of $v$ in $\mathbb{F}_q^*$. Let $\sum'$ denote a sum over monic

polynomials $m$ of $A$ which are square-free. Then we have

$$\begin{aligned}
\text{error} &\le \sideset{}{'}\sum_{y<\deg m\le d_Kx/r}\ \sum_{u,v\in\mathbb{F}_q^*}\ \sum_{\deg b\le(r-1)d_Kx/r} \#\big(S_{u,v,b}(m,x)\big)\\
&\le \sideset{}{'}\sum_{y<\deg m\le d_Kx/r}\ \sum_{u,v\in\mathbb{F}_q^*}\ \sum_{\substack{\deg b\le(r-1)d_Kx/r\\ m|(1+b-uv^{-1})}}\ \sum_{\substack{\deg_K\mathfrak{P}=x\\ u_{\mathfrak{P}}=u,\,v_{\mathfrak{P}}=v,\,b_\phi(\mathfrak{P})=b\\ m^r|(1+b+up^{m_{\mathfrak{P}}})}} 1\\
&\le \sideset{}{'}\sum_{y<\deg m\le d_Kx/r}\ \sum_{u,v\in\mathbb{F}_q^*}\ \sum_{\substack{\deg b\le(r-1)d_Kx/r\\ m|(1+b-uv^{-1})\\ 1+b-uv^{-1}\neq0}}\ \sum_{\substack{\deg_K\mathfrak{P}=x\\ u_{\mathfrak{P}}=u,\,v_{\mathfrak{P}}=v,\,b_\phi(\mathfrak{P})=b\\ m^r|(1+b+up^{m_{\mathfrak{P}}})}} 1\\
&\quad+\sideset{}{'}\sum_{y<\deg m\le d_Kx/r}\ \sum_{u,v\in\mathbb{F}_q^*}\ \sum_{\substack{\deg b\le(r-1)d_Kx/r\\ 1+b-uv^{-1}=0}}\ \sum_{\substack{\deg_K\mathfrak{P}=x\\ u_{\mathfrak{P}}=u,\,v_{\mathfrak{P}}=v,\,b_\phi(\mathfrak{P})=b\\ m^r|(1+b+up^{m_{\mathfrak{P}}})}} 1\\
&= \text{error 1} + \text{error 2} \qquad \text{(say)}.
\end{aligned}$$

Consider the innermost sum in error 1. Since $\deg_K(\mathfrak{P})=x$ and $m_{\mathfrak{P}}=[\mathbb{F}_{\mathfrak{P}}:A/\mathfrak{p}]$, we have $\deg p^{m_{\mathfrak{P}}}=d_Kx$. For fixed $b\in A$ and $u\in\mathbb{F}_q^*$, there are at most $q^{d_Kx-r\deg m}$ primes $p\in A$ of degree $d_Kx$ such that $m^r|(1+b+up^{m_{\mathfrak{P}}})$. Moreover, for each fixed prime $p\in A$, there are at most $d$ primes $\mathfrak{P}$ of $K$ such that $\mathfrak{P}\cap A=\mathfrak{p}=pA$. It follows that

$$\sum_{\substack{\deg_K\mathfrak{P}=x,\\ u_{\mathfrak{P}}=u,\,v_{\mathfrak{P}}=v,\,b_\phi(\mathfrak{P})=b\\ m^r|(1+b+up^{m_{\mathfrak{P}}})}} 1 \le dq^{d_Kx-r\deg m} \ll q^{d_Kx-r\deg m}.$$

Thus we have

$$\begin{aligned}
\text{error 1} &\ll \sideset{}{'}\sum_{y<\deg m\le d_Kx/r}\ \sum_{u,v\in\mathbb{F}_q^*}\Big(q^{\frac{r-1}{r}\,d_Kx-\deg m}\Big)\Big(q^{d_Kx-r\deg m}\Big)\\
&\ll \sideset{}{'}\sum_{y<\deg m\le d_Kx/r} q^{\frac{d_K(2r-1)}{r}\,x-(r+1)\deg m} \qquad (11)\\
&\le q^{\frac{d_K(2r-1)}{r}\,x}\sum_{y<n\le d_Kx/r} q^{-(r+1)n}\cdot q^n \ll q^{\frac{d_K(2r-1)}{r}\,x-ry}.
\end{aligned}$$

Also,

$$\begin{aligned}
\text{error 2} &= \sideset{}{'}\sum_{y<\deg m\le d_Kx/r}\ \sum_{u,v\in\mathbb{F}_q^*}\ \sum_{\substack{\deg_K\mathfrak{P}=x\\ u_{\mathfrak{P}}=u,\,v_{\mathfrak{P}}=v,\,b_\phi(\mathfrak{P})=uv^{-1}-1\\ m^r|(uv^{-1}+up^{m_{\mathfrak{P}}})}} 1\\
&\ll \sideset{}{'}\sum_{y<\deg m\le d_Kx/r}\Big(q^{d_Kx-r\deg m}\Big) \qquad (12)\\
&\ll q^{d_Kx-(r-1)y}.
\end{aligned}$$

Comparing the error terms in (10), (11), and (12), there are two cases:
(i) If $r = 2, 3$, we choose $y$ such that $q^{\frac{d_K x}{2}+y} = q^{\frac{d_K(2r-1)}{r}\,x - ry}$, i.e.,

$$y = \frac{3r-2}{2r(r+1)}\, d_K x. \tag{13}$$

(ii) If $r \geq 4$, we take

$$y = \frac{1}{r}\, d_K x; \tag{14}$$

thus the error term in (9) becomes trivial.
Combining (9), (10), (11), and (12) with this choice of $y$, we obtain

$$f(x,\phi) = \pi_K(x) \Bigg( \sum_{\deg m \leq y} \frac{\mu_q(m)\, r_m(x)}{n(m)} \Bigg) + O\Big( D(\phi) E(\phi) (q^{d_K x})^{\Delta_r} \Big), \tag{15}$$

where $\Delta_r$ is defined as in (2).

To prove the theorem, it remains to consider

$$\pi_K(x) \Bigg( \sum_{\deg m \leq y} \frac{\mu_q(m)\, r_m(x)}{n(m)} \Bigg) = c_\phi(x)\, \pi_K(x) - \pi_K(x) \Bigg( \sum_{\deg m > y} \frac{\mu_q(m)\, r_m(x)}{n(m)} \Bigg). \tag{16}$$

For $m \in A$, write $m = m_1 m_2$ as in Proposition 12. We note that if $m$ is square-free, so is $m_1$. Applying Propositions 10, 12, and the fact $\varphi(m_2) \gg q^{\deg m_2} / \log \deg m_2$, we have

$$\begin{aligned} \sum_{\substack{\deg m > y \\ m = m_1 m_2}}{}' \frac{r_m(x)}{n(m)} &\ll \sum_{m_1}{}' \sum_{\deg m_2 > (y - \deg m_1)} \frac{E(\phi)}{\varphi(m_2)\, q^{(r^2-1)\deg m_2}} \\ &\ll \sum_{m_1}{}' \sum_{\deg m_2 > (y - \deg m_1)} \frac{E(\phi) \log \deg m_2}{q^{r^2 \deg m_2}}. \end{aligned}$$

Consider the innermost sum in the above expression. We have

$$\begin{aligned} \sum_{\deg m_2 > (y - \deg m_1)} \frac{E(\phi) \log \deg m_2}{q^{r^2 \deg m_2}} &\ll \sum_{n > (y - \deg m_1)} \frac{E(\phi) \log n}{q^{(r^2-1)n}} \\ &\leq \frac{E(\phi) \log y}{q^{(r^2-2)(y - \deg m_1)}} \sum_{n > (y - \deg m_1)} \frac{1}{q^n} \\ &\ll \frac{E(\phi) \log y}{q^{(r^2-1)(y - \deg m_1)}}. \end{aligned}$$

Combining the above two inequalities, we obtain

$$\begin{aligned} \sum_{\substack{\deg m > y \\ m = m_1 m_2}}{}' \frac{r_m(x)}{n(m)} &\ll \frac{E(\phi) \log y}{q^{(r^2-1)y}} \sum_{m_1}{}' q^{(r^2-1)\deg m_1} \\ &= \frac{E(\phi) \log y}{q^{(r^2-1)y}} \prod_{l \mid B(\phi)} \Big( 1 + q^{(r^2-1)\deg l} \Big), \end{aligned}$$

where the product is over primes $l \in A$ with $l|B(\phi)$. Note that

$$\begin{aligned} 1+q^{(r^2-1)\deg l} &= q^{(r^2-1)\deg l}\left(1+\frac{1}{q^{(r^2-1)\deg l}}\right) \\ &\le q^{(r^2-1)\deg B(\phi)}\left(1+\frac{1}{q^{(r^2-1)\deg l}}\right). \end{aligned}$$

Thus, using the fact that $1+y \le q^y$ for $y>0$, we have

$$\begin{aligned} \sum_{\substack{\deg m>y \\ m=m_1m_2}}{}' \frac{r_m(x)}{n(m)} &\le \frac{E(\phi)\log y}{q^{(r^2-1)y}}\, q^{(r^2-1)\deg B(\phi)} \prod_{l|B(\phi)}\left(1+\frac{1}{q^{(r^2-1)\deg l}}\right) \\ &\ll \frac{E(\phi)\log y}{q^{(r^2-1)y}}\, q^{(r^2-1)\deg B(\phi)}\, q^{\sum_{l|B(\phi)} q^{-(r^2-1)\deg l}} \\ &\ll \frac{E(\phi)\log y}{q^{(r^2-1)y}}\, q^{r^2\deg B(\phi)}. \end{aligned}$$

The last inequality follows from the facts that $q^{-(r^2-1)\deg l} \le 1$ and the number of primes $l \in A$ with $l|B(\phi)$ is bounded by $\deg B(\phi)$. Thus from (16), we have

$$\pi_K(x)\left(\sum_{\deg m\le y}\frac{\mu_q(m)\, r_m(x)}{n(m)}\right) = c_\phi(x)\,\pi_K(x) + O\left(\frac{E(\phi)\, q^{d_K x}\,\log x}{x\, q^{(r^2-1)y}}\, q^{r^2\deg B(\phi)}\right). \tag{17}$$

Plugging the choice of $y$ in (13) or in (14) into the above equation, we obtain

$$\begin{aligned} &\pi_K(x)\left(\sum_{\deg m\le y}\frac{\mu_q(m)\, r_m(x)}{n(m)}\right) \\ &= c_\phi(x)\,\pi_K(x) + O\left(E(\phi)\, x^{-1}\,\log x\,\left(q^{d_K x}\right)^{\delta_r}\, q^{r^2\deg B(\phi)}\right), \end{aligned} \tag{18}$$

where $\delta_r$ is defined as in (8). Combining (15) and (18), Theorem 1' follows.

## 5. Proof of Theorem 3

In this section, we will prove Theorem 3. We begin by stating a theorem of Poonen, which is an analogue of Mazur's result on the torsion subgroup of elliptic curves over $\mathbb{Q}$.

**Theorem 13.** ([15, Theorem 1 & Theorem 9]) *Let $K$ be a finite extension of $k$ and $\psi$ a Drinfeld $A$-module over $K$. Define*

$$\psi(K)_{\mathrm{tors}} = \big\{\alpha \in K \,|\, \psi_a(\alpha) = 0 \text{ for some nonzero } a \in A\big\}.$$

*For any fixed positive integer $d$, there is a uniform bound on $\#\psi(K)_{\mathrm{tors}}$ as $K$ ranges over extensions of $k$ with $[K:k] \le d$ and $\psi$ ranges over rank 1 Drinfeld $A$-modules over $K$. As a consequence, there exists a positive constant $C_K$ (depending only on $[K:k]$) such that for all $a \in A$ with $\deg a > C_K$, $K(\psi[a]) \ne K$. In the special case when $K = k$ and $a$ are primes, the constant $C_k$ can be taken to be 1.*

The main goal of this section is to prove the following theorem, which is a generalization of Theorem 3.

**Theorem 3'.** *Let $K$ be a finite extension of $k$ and $\phi$ a Drinfeld $A$-module over $K$ of rank $r \geq 2$. Let $c_\phi(x) = c_\phi^K(x)$ be defined as in Theorem 1.*
*(1) If $K(\phi[a]) = K$ for some non-constant $a \in A$, then $c_\phi(x) = 0$.*
*(2) Let $C_K$ be defined as in Theorem 13. Suppose that $\mathrm{End}_{\bar{K}}(\phi) = A$ and all division fields of $\phi$ are geometric, i.e., do not contain non-trivial constant field extensions. Suppose further that $K(\phi[a]) \neq K$ for all non-constant $a \in A$ with $\deg a \leq C_K$. Then $c_\phi(x)$ is positive.*

Note that if all division fields of $\phi$ are geometric, $c_\phi(x)$ is independent from $x$. Thus we can write $c_\phi = c_\phi(x)$ as in Corollary 2. In addition, when $K = k$, we have seen in Theorem 13 that $C_k = 1$. Thus Theorem 3 is a direct consequence of Part (2) of Theorem 3'.

In order to prove Theorem 3', we need the following result from [2, Lemma 6.1]. We note that although the statement in [2, Lemma 6.1] is for number fields, by making typographical changes, we can extend that result to the following setting.

**Lemma 14.** ([2, Lemma 6.1]) *Let $\mathcal{L}$ and $\mathcal{L}'$ be sets of primes in $A$ with $\mathcal{L}' \subseteq \mathcal{L}$. Let $\mathcal{K} = (K_l)_{l\in\mathcal{L}}$ and $\mathcal{K}' = (K'_{l'})_{l'\in\mathcal{L}'}$ be two families of finite geometric Galois extensions of $K$ indexed over primes $l \in \mathcal{L}$ and $l' \in \mathcal{L}'$, respectively. For monic square-free polynomials $m$ and $m'$ composed of primes of $\mathcal{L}$ and $\mathcal{L}'$, respectively, let $K_m$ and $K'_{m'}$ be the compositum of $K_l$ with $l|m$ and $l \in L$ and of $K'_{l'}$ with $l'|m'$ and $l' \in L'$ respectively. Also, let $s(m) = [K_m : K]$, $s'(m') = [K'_{m'} : K]$,*

$$\delta(\mathcal{K}) = \sum_{\substack{m \\ l|m \Rightarrow l\in\mathcal{L}}} \frac{\mu_q(m)}{s(m)}, \qquad \text{and} \qquad \delta(\mathcal{K}') = \sum_{\substack{m' \\ l'|m' \Rightarrow l'\in\mathcal{L}'}} \frac{\mu_q(m')}{s'(m')},$$

*where $s(1) = s'(1') = 1$. Suppose that*
*(1) $\mathcal{K}$ covers $\mathcal{K}'$, that is, for any $l' \in \mathcal{L}'$, there exists $l \in \mathcal{L}$ such that $K'_{l'} \subseteq K_l$, and for any $l \in \mathcal{L}$, there exists $l' \in \mathcal{L}'$ such that $K'_{l'} \subseteq K_l$.*
*(2) We have*

$$\sum_{\substack{m \\ l|m \,\Rightarrow\, l\in\mathcal{L}}}{}' \frac{1}{s(m)} < \infty \qquad \text{and} \qquad \sum_{\substack{m' \\ l'|m' \,\Rightarrow\, l'\in\mathcal{L}'}}{}' \frac{1}{s'(m')} < \infty,$$

*where $\sum'$ denotes a sum over monic square-free polynomials in $A$.*
*Then it follows that*

$$\delta(\mathcal{K}) \geq \delta(\mathcal{K}').$$

*In particular, if the fields $K'_{l'}$ in $\mathcal{K}'$ are mutually independent (i.e., $K'_{l'_1} \cap K'_{l'_2} = K$ for any $l'_1, l'_2 \in \mathcal{L}'$ with $l'_1 \neq l'_2$), then*

$$\delta(\mathcal{K}) \geq \prod_{l'\in\mathcal{L}'} \Big(1 - \frac{1}{s'(l')}\Big).$$

To prove Theorem 3', we also need the following lemma.

**Lemma 15.** *Let $\mathcal{L}$ be a set of primes in $A$, and let $\mathcal{K} = \{K_l\}_{l\in\mathcal{L}}$ be a family of non-trivial finite (geometric) Galois extensions of $K$. Suppose that all but finitely many fields $K_l$ in $\mathcal{K}$*

*are mutually independent. Then there exists a set of primes $\mathcal{L}'$ in $A$ and a corresponding family $\mathcal{K}' = \{K'_{l'}\}_{l' \in \mathcal{L}'}$ of non-trivial finite (geometric) Galois extensions of $K$ such that $\mathcal{L}' \subseteq \mathcal{L}$, $\mathcal{K}$ covers $\mathcal{K}'$, and all fields $K'_{l'}$ in $\mathcal{K}'$ are mutually independent.*

*Proof:* Write $\mathcal{L} = \mathcal{G} \sqcup \mathcal{E}$, a disjoint union of $\mathcal{G}$ and $\mathcal{E}$, where $\mathcal{G}$ is an index set whose indexed fields are mutually independent and $\mathcal{E}$ is the exceptional set. Since all but finitely many fields $K_l$ in $\mathcal{K}$ are mutually independent, without loss of generality, we can assume that $|\mathcal{E}|$, the cardinality of $\mathcal{E}$, is finite.

We will construct $\mathcal{L}'$ and $\mathcal{K}'$ by induction on the cardinality of $\mathcal{E}$. If $|\mathcal{E}| = 0$, we can take $\mathcal{L}' = \mathcal{L}$ and $\mathcal{K}' = \mathcal{K}$, and then the result follows. Now suppose $|\mathcal{E}| \geq 1$. For a prime $e \in \mathcal{E}$, there are two possibilities for $K_e$.
(1) Suppose that $K_e$ is mutually independent from all fields indexed by primes in $\mathcal{G}$. Then we can write $\tilde{\mathcal{L}} = \tilde{\mathcal{G}} \sqcup \tilde{\mathcal{E}}$, where $\tilde{\mathcal{G}} = \mathcal{G} \cup \{e\}$ and $\tilde{\mathcal{E}} = \mathcal{E} \backslash \{e\}$. Since $|\tilde{\mathcal{E}}| = |\mathcal{E}| - 1$, by induction, there exist $\mathcal{L}'$ and $\mathcal{K}'$ satisfying the required conditions. Thus the result follows.
(2) Suppose that $K_e$ is not mutually independent from all fields indexed by $\mathcal{G}$. Then there exists a prime $g \in \mathcal{G}$ such that $K_e \cap K_g \neq K$. Note that $K_e \cap K_g$ is a non-trivial finite (geometric) Galois extension of $k$. For $h \in \mathcal{G} \setminus \{g\}$, since $K_g$ is mutually independent from $K_h$, it follows that $K_e \cap K_g$ is mutually independent from $K_h$. In this case, we take $\tilde{\mathcal{L}} = \mathcal{G} \sqcup \tilde{\mathcal{E}}$ with $\tilde{\mathcal{E}} = \mathcal{E} \backslash \{e\}$, and we construct a new family $\tilde{\mathcal{K}} = (\tilde{K}_{\tilde{l}})_{\tilde{l} \in \tilde{L}}$ of non-trivial finite (geometric) Galois extensions of $k$ as follows:
- Define $\tilde{K}_g = K_e \cap K_g$.
- For $h \in \mathcal{G} \setminus \{g\}$, define $\tilde{K}_h = K_h$.
- For $i \in \tilde{\mathcal{E}}$, define $\tilde{K}_i = K_i$.
Then all but finitely many $\tilde{K}_{\tilde{l}}$ in $\tilde{\mathcal{K}}$ are mutually independent. Now, since $|\tilde{\mathcal{E}}| = |\mathcal{E}| - 1$, it follows by induction that there exist $\mathcal{L}'$ and $\mathcal{K}'$ satisfying the required conditions with respect to $\tilde{\mathcal{K}}$. Since $\tilde{\mathcal{L}} \subseteq \mathcal{L}$ and $\mathcal{K}$ covers $\tilde{\mathcal{K}}$, we have $\mathcal{L}' \subseteq \mathcal{L}$ and $\mathcal{K}$ covers $\mathcal{K}'$. Thus the lemma follows.

**Remark** We note that from the above construction, if $\mathcal{L} = \mathcal{G} \sqcup \mathcal{E}$, we can take $\mathcal{L}' = \mathcal{G}' \sqcup \mathcal{E}_1 \sqcup \mathcal{E}_2$, where $\mathcal{G}' \subseteq \mathcal{G}$, $\mathcal{E}_1 \sqcup \mathcal{E}_2 = \mathcal{E}$, and $\mathcal{E}_1$ and $\mathcal{E}_2$ are the sets of primes from possibilities (1) and (2) of the proof of Lemma 15, respectively. In particular, the sets $\mathcal{E}_1$ and $\mathcal{E}_2$ are not canonical; they depend on the choices made in the proof. Now we have that $K'_{l'} = K_{l'}$ for $l' \in \mathcal{G}'$, that $K'_{l'_1} = K_{l'_1}$ for $l'_1 \in \mathcal{E}_1$, and that $K'_{l'_2} \neq K$ for $l'_2 \in \mathcal{E}_2$. Since $\mathcal{G}' \subseteq \mathcal{G}$ and $[K'_{l'} : K] \geq 2$ for $l' \in \mathcal{E}_1 \sqcup \mathcal{E}_2$, by Lemmas 14 and 15, we have

$$\delta(\mathcal{K}) \geq \Big(\frac{1}{2}\Big)^{|\mathcal{E}|} \prod_{l' \in \mathcal{G}'} \Big(1 - \frac{1}{s'(l')}\Big) \geq \Big(\frac{1}{2}\Big)^{|\mathcal{E}|} \prod_{l \in \mathcal{G}} \Big(1 - \frac{1}{s(l)}\Big).$$

Now, we are ready to prove Theorem 3'.

*Proof:* (1) Suppose that $K(\phi[a]) = K$ for some non-constant $a \in A$. Since $\phi[a] \simeq (A/aA)^r$ [4, Proposition 2.2], it follows that $\phi(K)_{\text{tor}}$ contains a subgroup of the form $(A/aA)^r$. Since $\phi(K)_{\text{tor}} \subseteq \phi(\mathbb{F}_{\mathfrak{P}})$ for all but finitely many primes $\mathfrak{P}$ of $K$, there are only finitely many $\phi(\mathbb{F}_{\mathfrak{P}})$ which have at most $(r-1)$ cyclic components. Thus we have $c_\phi(x) = 0$.
(2) Suppose that $\phi$ satisfies all conditions stated in (2). We recall that since all division fields of $\phi$ are geometric, $c_\phi(x)$ is independent from $x$. In the following, we will write $c_\phi =$

$c_\phi(x)$. To apply Lemma 14, let $\mathcal{L}$ be the set of all primes of $A$ and $\mathcal{K} = (K_l = K(\phi[l]))_{l\in\mathcal{L}}$. Since the fields $K(\phi[l])$ are finite geometric Galois extensions of $K$, we have

$$c_\phi = \delta(\mathcal{K}).$$

Let $B(\phi)$ be defined as in Proposition 5 and $l_1, l_2 \in \mathcal{L}$ be distinct primes with $(l_1, B(\phi)) = 1 = (l_2, B(\phi))$. By Proposition 5,

$$\begin{aligned}[K(\phi[l_1l_2]) : K] &= \big|\mathrm{GL}_r(A/l_1l_2A)\big| = \big|\mathrm{GL}_r(A/l_1A)\big| \cdot \big|\mathrm{GL}_r(A/l_2A)\big| \\ &= [K(\phi[l_1]) : K] \cdot [K(\phi[l_2]) : K].\end{aligned}$$

It follows that $K(\phi[l_1l_2]) = K(\phi[l_1], \phi[l_2])$. Thus the division fields $K(\phi[l])$ are mutually independent for primes $l \in \mathcal{L}$ with $l \nmid B(\phi)$. Also, they are non-trivial extensions of $K$.

For a prime $l \in \mathcal{L}$ with $l|B(\phi)$, we will now show that $K(\phi[l])$ is also a non-trivial extension of $K$. Let $\psi_\phi$ be the rank 1 Drinfeld $A$-module associated to $\phi$ via Weil's paring. By Theorem 13, $K(\psi_\phi[l])$ are non-trivial extensions of $K$ for primes $l$ with $\deg l > C_K$. Since $K(\psi_\phi[l]) \subseteq K(\phi[l])$ and $K(\phi[a]) \neq K$ for all non-constant $a \in A$ with $\deg a \leq C_K$, it follows that $K(\phi[l]) \neq K$ for all primes $l \in \mathcal{L}$.

Now, we have $\mathcal{K} = (K(\phi[l]))_{l\in\mathcal{L}}$, a family of non-trivial finite geometric Galois extensions of $K$. Since the division fields $K(\phi[l])$ are mutually independent for primes $l$ with $l \nmid B(\phi)$, we can take $\mathcal{L} = \mathcal{G} \sqcup \mathcal{E}$, where

$$\mathcal{G} = \Big\{ l \in \mathcal{L} \,\Big|\, l \nmid B(\phi) \Big\} \qquad \text{and} \qquad \mathcal{E} = \Big\{ l \in \mathcal{L} \,\Big|\, l \,|B(\phi) \Big\}.$$

We note that for primes $l$ with $l \nmid B(\phi)$,

$$s(l) = [K(\phi[l]) : K] = |\mathrm{GL}_r(A/lA)| \gg q^{r^2 \deg l}.$$

Thus we have

$$\prod_{l\nmid B(\phi)} \left(1 - \frac{1}{s(l)}\right) \gg 1.$$

Also, for a monic square-free polynomial $m \in A$, we write $m = m_1m_2$ as in Proposition 12. Then $s(m) \geq s(m_2)$, and it follows that

$$\sum_{\substack{m \\ l|m \Rightarrow l\in\mathcal{L}}}{}' \frac{1}{s(m)} \leq \sum_{\substack{m=m_1m_2 \\ l|m \Rightarrow l\in\mathcal{L}}}{}' \frac{1}{s(m_2)} \leq \prod_{l|B(\phi)} (1+1) \prod_{l\nmid B(\phi)} \left(1 + \frac{1}{s(l)}\right) < \infty.$$

Let $\mathcal{K}' = (K'_{l'})_{l'\in\mathcal{L}'}$ be the family associated to $\mathcal{K}$ as defined in Lemma 15. Since the fields $K'_{l'}$ are mutually independent for primes $l' \in \mathcal{L}'$ and $s'(l') = s(l) \gg q^{r^2 \deg l}$ for all but finitely many primes $l'$, we have

$$\sum_{\substack{m' \\ l'|m' \Rightarrow l'\in\mathcal{L}'}}{}' \frac{1}{s'(m')} = \prod_{l'\in\mathcal{L}'} \left(1 + \frac{1}{s'(l')}\right) < \infty.$$

Moreover, since $|\mathcal{E}| \leq \deg B(\phi)$, by the remark after Lemma 15, we have

$$c_\phi = \delta(\mathcal{K}) \geq \left(\frac{1}{2}\right)^{\deg B(\phi)} \prod_{l\nmid B(\phi)} \left(1 - \frac{1}{s(l)}\right) \gg 1.$$

This completes the proof of Theorem 3'.

In the remaining part of the paper, we will discuss the case when division fields of $\phi$ are not all geometric. We need the following proposition to prove our result.

**Proposition 16.** ([16, Proposition 8.13]) *Let $K$ be a finite extension of $k$ and $\mathfrak{P}$ a prime of $K$. Let $L$ be the constant field extension of $K$ with $[L:K]=n$. Then $\mathfrak{P}$ splits into $(n, \deg_K \mathfrak{P})$ primes in $L$. In particular, if $n | \deg_K \mathfrak{P}$, then $\mathfrak{P}$ splits completely in $L$. In addition, if $\mathcal{P}$ is a prime of $L$ lying over $\mathfrak{P}$, then $\deg_L \mathcal{P} = \deg_K \mathfrak{P}/(n, \deg_K \mathfrak{P})$.*

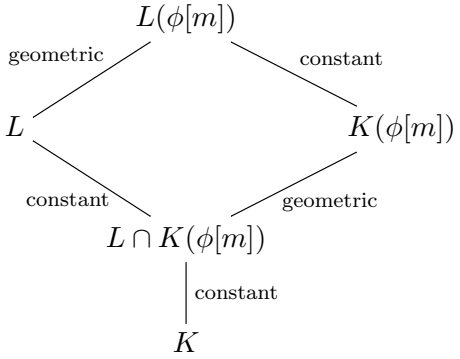
**Theorem 17.** *Let $K$ be a finite extension of $k$ and let $\phi$ be a Drinfeld $A$-module over $K$ of rank $r \geq 2$ with $\mathrm{End}_{\bar{K}}(\phi) = A$. Let $E(\phi)$ be defined as in Proposition 10 and define $E(\phi)^* = \prod_{p:\text{prime}, p|E(\phi)} p$, the squarefree kernel of $E(\phi)$. Let $L$ be the constant field extension of $K$ with $[L:K] = E(\phi)$ and let $C_L$ be defined as in Theorem 13. Suppose that $L(\phi[a]) \neq L$ for all non-constant $a \in A$ with $\deg a \leq C_L$. Then for all $x \in \mathbb{N}$ with $(E(\phi)\cdot E(\phi)^*)|x$, $c_\phi^K(x)$ is positive.*

*Proof:* By the construction of $L$, all of its division fields are geometric. Thus, by Theorem 3'(2), there is a positive constant $c_\phi^L$ such that for any $y \in \mathbb{N}$,

$$f^L(y,\phi) = \sum_{m\in A} \mu_q(m)\pi_1(y, L(\phi[m])/L) = c_\phi^L \pi_L(y) + o\big(\pi_L(y)\big),$$

where $\pi_1(y, L(\phi[m])/L)$ is the number of primes of $L$ which are of good reduction, of degree $y$, and splitting completely in $L(\phi[m])$.

For every $m \in A$, we have the following diagram.




Consider only the constant field extensions. We have

$$[L(\phi[m]) : K(\phi[m])] \cdot [L \cap (\phi[m]) : K] = [L:K] = E(\phi).$$

*Claim 1*: Let $\mathfrak{P}$ be a prime of $K$ of degree $E(\phi)y$ for some $y \in \mathbb{N}$. Then $\mathfrak{P}$ splits completely in $K(\phi[m])$ if and only if every prime of $L$ lying over $\mathfrak{P}$, which is of degree $y$, splits completely in $L(\phi[m])$.

*Proof of Claim 1*: Since $[L\cap K(\phi[m]) : K] \,|\, E(\phi)$, $\deg_K \mathfrak{P}$ is divisible by $[L\cap K(\phi[m]) : K]$. By Proposition 16, $\mathfrak{P}$ splits completely in $L \cap K(\phi[m])$, and the primes of $L \cap K(\phi[m])$ lying above $\mathfrak{P}$ are of degree $E(\phi)y/[L\cap K(\phi[m]) : K]$. Similarly, since $\deg_K \mathfrak{P}$ is divisible by $E(\phi)$, $\mathfrak{P}$ splits completely in $L$, and the primes of $L$ lying above $\mathfrak{P}$ are of degree $y$. Suppose that $\mathfrak{P}$ splits completely in $K(\phi[m])$. Let $\tilde{\mathcal{P}}$ be a prime in $L\cap K(\phi[m])$ lying above

$\mathfrak{P}$, and $\mathcal{P}$ a prime in $K(\phi[m])$ lying above $\tilde{\mathcal{P}}$. Since $K(\phi[m])/L \cap K(\phi[m])$ is a geometric extension, we have

$$\deg_{K(\phi[m])} \mathcal{P} = \deg_{L\cap K(\phi[m])} \tilde{\mathcal{P}} = E(\phi)y/[L \cap K(\phi[m]) : K] = [L(\phi[m]) : K(\phi[m])]\, y.$$

Since $\deg_{K(\phi[m])} \mathcal{P}$ is divisible by $[L(\phi[m]) : K(\phi[m])]$, by Proposition 16, $\mathcal{P}$ splits completely in $L(\phi[m])$. We now see that $\mathfrak{P}$ splits completely in $K(\phi[m])$ if and only if $\mathfrak{P}$ splits completely in $L(\phi[m])$, if and only if every prime $\mathcal{P}$ of $L$ lying over $\mathfrak{P}$ splits completely in $L(\phi[m])$. This completes the proof of Claim 1.

*Claim 2*: Every prime $\mathcal{P}$ of $L$, which is of degree $y$ with $E(\phi)^*|y$, lies over a prime $\mathfrak{P}$ of $K$ which is of degree $E(\phi)y$.

*Proof of Claim 2*: To show that $\deg_K \mathfrak{P} = E(\phi)y$, by Proposition 16, it suffices to show that $\deg_K \mathfrak{P}$ is divisible by $E(\phi)$. Let $p$ be a rational prime divisor of $E(\phi)$. If the exponent of $p$ in $\deg_K \mathfrak{P}$ is less than or equal to that in $E(\phi)$, by Proposition 16, $y = \deg_L \mathcal{P}$ has no $p$ factor, which contradicts the fact that $E(\phi)^*|y$. Thus the exponent of $p$ in $\deg_K \mathfrak{P}$ must be greater than that in $E(\phi)$ and it follows that $E(\phi)|\deg_K \mathfrak{P}$. This completes the proof of Claim 2.

Combining the above two claims, for $x = E(\phi)y$ with $E(\phi)^*|y$, we have

$$E(\phi) \cdot \pi_1(x, K(\phi[m])/K) = \pi_1(y, L(\phi[m])/L).$$

It follows that

$$\begin{aligned} f^K(x,\phi) &= \sum_{m\in A} \mu_q(m)\pi_1(x, K(\phi[m])/K) \\ &= \frac{1}{E(\phi)} \sum_{m\in A} \mu_q(m)\pi_1(y, L(\phi[m])/L) \\ &= \frac{1}{E(\phi)} c_\phi^L \pi_L(y) + o\big(\pi_L(y)\big) \\ &= c_\phi^K \pi_K(x) + o\big(\pi_K(x)\big). \end{aligned}$$

In particular, $c_\phi^K(x) = c_\phi^L/E(\phi)$ is positive. This completes the proof of Theorem 17.

**Acknowledgement** The authors are grateful to Chantal David for mentioning to us that Theorem 4 was true in the case of rank 2 before the paper of Pink and Rütsche was published. The authors also would like to thank Gert-Jan van der Heiden for answering questions related to this paper, and to Jiu-Kang Yu for many useful discussions about this work. Finally, the authors are grateful to the referees for their detailed comments and many valuable suggestions about this paper, including the partial result on removing the geometric condition, and referring to us the recent theorem of Pink and Rütsche on the adelic openness for Drinfeld modules.

## References

[1] D. A. Clark & M. Kuwata, *Generalized Artin's Conjecture for primitive roots and cyclicity mod* $\mathfrak{p}$ *of elliptic curves over function fields*, Canad. Math. Bull. Vol 38(2), 1995, 167–173.

[2] A. C. Cojocaru & M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, Math. Ann. 330 (2004), 601-625.
[3] C. David, *Frobenius distributions of Drinfeld modules of any rank*, Journal of Number Theory 90 (2001), 329–340.
[4] V.G. Drinfeld, *Elliptic modules*, Math. Sbornik 94 (1974), 594–627, English transl.: *Math. U.S.S.R. Sbornik* 23 (1976), 561–592.
[5] M. Fried & M. Jarden, *Field Arithmetic (Second Edition)*, A Series of Modern Surveys in Mathematics, Vol. 11, Springer (2005).
[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] F. Gardeyn, *t-Motives and Galois representations*, Ph.D. Thesis, Universiteit Gent, 2002.
[8] F. Gardeyn, *Openness of the Galois image for $\tau$-modules of dimension 1*, J. Number Theory 102 (2003), 306–338.
[9] E.-U. Gekeler, *On Finite Drinfeld Modules*, J. of Algebra 141 (1991), 187–203.
[10] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse 35, Springer, Berlin (1996).
[11] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. 189 (1974), 77-91.
[12] M. R. Murty, *On Artin's conjecture*, J. Number Theory 16 (1983), 147-168.
[13] R. Pink, *The Mumford-Tate conjecture for Drinfeld modules*, Publ. RIMS, Kyoto University 33 (1997), 393-425.
[14] R. Pink & E. Rütsche, *Adelic openness for Drinfeld modules in generic characteristic*, J. Number Theory 129 (2009), 882-907.
[15] B. Poonen, *Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture*, Math. Ann. 308 (1997), 571-586.
[16] M. Rosen, *Number theory in function fields*, GTM 210, Springer (2002).
[17] J.-P. Serre, *Résumé des cours de 1977-1978*, Annuaire de Collège de France (1978), 67-70.
[18] G.-J. van der Heiden, *Weil pairing for Drinfeld modules*, Monatsh. Math. 143 (2004), 115-143.
[19] J.-K. Yu, *Isogenies of Drinfeld modules*, J. Number Theory 54 (1995), 161–171.

Wentang Kuo, Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

*E-mail address*: wtkuo@math.uwaterloo.ca

Yu-Ru Liu, Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

*E-mail address*: yrliu@math.uwaterloo.ca