GAUSSIAN LAWS ON 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. Let ϕ be a Drinfeld A-module over K of rank r. For a place \mathfrak{P} of K of good reduction, write $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}}/\mathcal{M}_{\mathfrak{P}}$, where $\mathcal{O}_{\mathfrak{P}}$ is the valuation ring of \mathfrak{P} and $\mathcal{M}_{\mathfrak{P}}$ its maximal ideal. Let $P_{\mathfrak{P},\phi}(X)$ be the characteristic polynomial of the Frobenius automorphism of $\mathbb{F}_{\mathfrak{P}}$ acting on a Tate module of ϕ . Let $\chi_{\phi}(\mathfrak{P}) = P_{\mathfrak{P},\phi}(1)$, and let $\nu(\chi_{\phi}(\mathfrak{P}))$ be the number of distinct primes diving $\chi_{\phi}(\mathfrak{P})$. If ϕ is of rank 2 with $\operatorname{End}_{\overline{K}}(\phi) = A$, we prove that there exists a normal distribution for the quantity

$$\frac{\nu(\chi_{\phi}(\mathfrak{P})) - \log \deg \mathfrak{P}}{\sqrt{\log \deg \mathfrak{P}}}.$$

For $r \geq 3$, we show that the same result holds under the open image conjecture for Drinfeld modules. We also study the number of distinct prime divisors of the trace of the Frobenius automorphism of $\mathbb{F}_{\mathfrak{P}}$ acting on a Tate module of ϕ and obtain similar results.

1. INTRODUCTION

For $n \in \mathbb{N} := \{1, 2, 3, \dots\}$, let $\omega(n)$ denote the number of distinct rational primes dividing n. For $x \in \mathbb{R}$ with $x \ge 1$, a theorem of Turán [28] states that

$$\sum_{n \le x} \left(\omega(n) - \log \log n \right)^2 \ll x \log \log x,$$

from which we can derive the earlier result of Hardy and Ramanujan [14] that the normal order of $\omega(n)$ is $\log \log n$. In 1940, Erdős and Kac [5] gave a remarkable refinement of Turán's Theorem by showing the existence of a normal distribution for $\omega(n)$. More precisely, they proved that for $\gamma \in \mathbb{R}$,

$$\lim_{x \to \infty} \frac{1}{x} \# \Big\{ n \, \big| \, n \leq x \text{ and } \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} \leq \gamma \Big\} = G(\gamma) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{\frac{-t^2}{2}} dt.$$

Instead of the sequence of natural numbers, we now consider the sequence of rational primes p. Since $\omega(p) = 1$, to obtain results analogous to those of Turán and Erdős-Kac, we estimate $\omega(f(p))$, where f is a function from the set of primes to \mathbb{N} . In the case that

Date: September 24, 2023.

²⁰⁰⁰ Mathematics Subject Classification. Primary 11G09; Secondary 11K36, 11N36.

 $K\!ey\ words\ and\ phrases.$ Drinfeld modules, normal distribution.

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.

f(p) = p - 1, Erdős [4] proved that

$$\sum_{p \le x} \left(\omega(p-1) - \log \log p \right)^2 \ll \pi(x) \log \log x,$$

where $\pi(x)$ is the number of rational primes p with $p \leq x$. Thus the normal order of $\omega(p-1)$ is $\log \log p$. In 1955, Halberstam [13] improved Erdős's result and showed that the quantity

$$\frac{\omega(p-1) - \log\log p}{\sqrt{\log\log p}}$$

distributes normally. One can also take $f(p) = \tau(p)$, where $\tau(n)$ denotes the Ramanujan τ -function. Assuming the GRH (i.e. the Riemann hypothesis for all Dedekind zeta functions of number fields), R. Murty and K. Murty [23] proved that

$$\sum_{\substack{p \le x \\ (p) \ne 0}} \left(\omega(\tau(p)) - \log \log p \right)^2 \ll \pi(x) \log \log x.$$

Under the GRH, they [24] also proved that the quantity

$$\frac{\omega(\tau(p)) - \log \log p}{\sqrt{\log \log p}}$$

distributes normally. Their general theorem is applicable to a wide class of functions arising as Fourier coefficients of modular forms.

Let E be an elliptic curve of conductor N defined over \mathbb{Q} . For a rational prime pwith $p \nmid N$, we denote by $\#E(\mathbb{F}_p)$ the cardinality of the set of rational points on Edefined over the finite field \mathbb{F}_p . One can consider $\omega(f(p))$ with $f(p) = \#E(\mathbb{F}_p)$. Note that $\#E(\mathbb{F}_p) = P_{p,E}(1)$, where $P_{p,E}(X)$ is the characteristic polynomial of the Frobenius automorphism of \mathbb{F}_p acting on a Tate module of E. In [22], Miri and K. Murty proved that if E is without complex multiplication (non-CM), assuming the GRH, we have

$$\sum_{\substack{p \le x \\ p \nmid N}} \left(\omega(\#E(\mathbb{F}_p)) - \log\log p \right)^2 \ll \pi(x) \log\log x$$

If E is with complex multiplication, the second author [20] proved that the above inequality holds unconditionally. She [21] also proved that for $\gamma \in \mathbb{R}$ (assuming the GRH if E is non-CM),

(1)
$$\lim_{x \to \infty} \frac{1}{\pi(x)} \# \left\{ p \mid p \le x, p \nmid N, \text{ and } \frac{\omega(\# E(\mathbb{F}_p)) - \log \log p}{\sqrt{\log \log p}} \le \gamma \right\} = G(\gamma).$$

This provides us an elliptic analogue of the Erdős-Kac theorem.

It is natural to ask if a function field analogue of the above result holds unconditionally. 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. Let K be a finite extension of k and \mathbb{F}_K the constant field of K. Given a place \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 $\mathcal{O}_{\mathfrak{P}}/\mathcal{M}_{\mathfrak{P}}$ and deg $\mathfrak{P} = [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_K]$. Throughout this paper, we use "primes" to denote monic irreducible polynomials of A and "places" to denote discrete valuations of K. To consider a function field analogue of the above result, one may ask, for a given elliptic curve E_q/K , if the quantity

$$\frac{\omega(\#E_q(\mathbb{F}_{\mathfrak{P}})) - \log \deg \mathfrak{P}}{\sqrt{\log \deg \mathfrak{P}}}$$

distributes normally. At this point, we encounter a difficulty in establishing such a result. The main obstacle is that the estimate involves the quantity $\sum_{n \leq x} \omega(q^n - 1)$, and it is difficult to obtain an asymptotic formula for this sum (see [16, Section 1] for further discussion of this issue). Thus we consider a function field analogue of (1) in a different formulation.

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 ι 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 τ be the Frobenius endomorphism relative to \mathbb{F}_q , i.e., $\tau(X) = X^q$. In the ring $\operatorname{End}_L(\mathbb{G}_a)$ 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, τ generates a subalgebra $L\{\tau\}$. It is a non-commutative polynomial algebra in τ 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 ϕ over L is an algebra homomorphism

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

such that $\iota = D \circ \phi$ and $\phi \neq \epsilon \circ \iota$. Let $\deg_{\tau} \phi_a$ denote the degree of ϕ_a in τ 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 [3, Proposition 2.1]). The integer r is called the *rank* of ϕ . Let B be an L-algebra. Then the composition

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

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

Now, we 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 ϕ be a Drinfeld A-module over K of rank r. For all but finitely many places \mathfrak{P} of K, ϕ has good reduction at \mathfrak{P} (see [12, Definition 4.10.1, p88]). Let \mathcal{P}_{ϕ} be the set of places of K at which ϕ has good reduction. For a place $\mathfrak{P} \in \mathcal{P}_{\phi}$, we can consider $\phi \otimes \mathbb{F}_{\mathfrak{P}}$, the reduction of ϕ at \mathfrak{P} . Then we write $\phi(\mathbb{F}_{\mathfrak{P}})$ to denote the A-module $(\phi \otimes \mathbb{F}_{\mathfrak{P}})(\mathbb{F}_{\mathfrak{P}})$.

To consider an analogue of $\#E(\mathbb{F}_p)$ in the Drinfeld module setting, let $P_{\mathfrak{P},\phi}(X)$ be the characteristic polynomial of the Frobenius of $\mathbb{F}_{\mathfrak{P}}$ acting on a Tate module of $\phi \otimes \mathbb{F}_{\mathfrak{P}}$ (see the next section for the definition). Write

$$\chi_{\phi}(\mathfrak{P}) = P_{\mathfrak{P},\phi}(1).$$

Since the ideal $\chi_{\phi}(\mathfrak{P})A$ is the Euler-Poincaré characteristic of $\phi(\mathbb{F}_{\mathfrak{P}})$ [11, Theorem 5.1], and $|\phi(\mathbb{F}_{\mathfrak{P}})|$, the cardinality of $\phi(\mathbb{F}_{\mathfrak{P}})$, is equal to $|\mathbb{F}_{\mathfrak{P}}|$, we have

(2)
$$\deg \chi_{\phi}(\mathfrak{P}) = d_K \deg \mathfrak{P},$$

where deg $\chi_{\phi}(\mathfrak{P})$ is the degree of $\chi_{\phi}(\mathfrak{P}) \in A$ in T and deg $\mathfrak{P} = [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_K]$.

For $m \in A$ with $m \neq 0$, let $\nu(m)$ denote the number of distinct primes dividing m. One can consider the distribution of $\nu(\chi_{\phi}(\mathfrak{P}))$ over the places $\mathfrak{P} \in \mathcal{P}_{\phi}$. In the special case that ϕ is the Carlitz module (i.e., $\phi_T = T\tau^0 + \tau$ and r = 1) and K = k, for a prime $l \in A$ and $\mathfrak{l} = lA$, we have $\chi_{\phi}(\mathfrak{l}) = l - 1$ [11, Theorem 5.1]. In [18], the second author proved that

$$\sum_{\deg l=x} \left(\nu(l-1) - \log \deg l\right)^2 \ll \pi_k(x) \log x,$$

where $\pi_k(x)$ is the number of primes $l \in A$ of degree x. From which we can conclude that the normal order of $\nu(l-1)$ is log deg l. She also showed that the quantity

$$\frac{\nu(l-1) - \log \deg l}{\sqrt{\log \deg l}}$$

distributes normally.

In this paper, we study analogous questions for $\nu(\chi_{\phi}(\mathfrak{P}))$ when ϕ is of rank r = 2 and K is a finite extension of k. What distinguishes the case r = 2 from r = 1 is its "non-abelian character." For r = 1 and K = k, divisibility properties of (l - 1) depend only on primes in arithmetic progressions. In other words, what is latent in this case is the distribution of primes in cyclotomic function fields, which are abelian extensions of k. However, in the case when r = 2, divisibility properties of $\chi_{\phi}(\mathfrak{P})$ are in the intervention of the distribution of primes in the division fields of ϕ , and they are no longer abelian. This difference makes the study of $\nu(\chi_{\phi}(\mathfrak{P}))$ much more difficult than that of $\nu(l-1)$.

Our estimate for $\nu(\chi_{\phi}(\mathfrak{P}))$ can be generalized to any ϕ of rank $r \geq 2$ provided that the open image conjecture for ϕ is satisfied. We will discuss this conjecture in more detail in Section 2. Let $\operatorname{End}_{\bar{K}}(\phi)$ denote the endomorphism ring of ϕ over the algebraic closure \bar{K} of K, and let $\pi_K(x)$ be the number of places \mathfrak{P} of K of degree x. We now state the major results of this paper.

Theorem 1. (i) Let ϕ be a Drinfeld A-module over K of rank 2 with $\operatorname{End}_{\overline{K}}(\phi) = A$. For $x \in \mathbb{N}$,

$$\sum_{\substack{\deg \mathfrak{P}=x\\ \mathfrak{P}\in\mathcal{P}_{\phi}}} \left(\nu(\chi_{\phi}(\mathfrak{P})) - \log \deg \mathfrak{P}\right)^2 \ll \pi_K(x) \log x.$$

(ii) Let ϕ be a Drinfeld A-module over K of rank $r \geq 3$ with $\operatorname{End}_{\bar{K}}(\phi) = A$. Assuming the open image conjecture for ϕ , the above inequality holds.

This theorem can be viewed as a Drinfeld module analogue of the result of Miri and K. Murty in [22, Theorem 2]. As a direct consequence of Theorem 1, we have

Corollary 2. Let ϕ be a Drinfeld A-module over K of rank $r \geq 2$ with $\operatorname{End}_{\bar{K}}(\phi) = A$. Assume the open image conjecture for ϕ when $r \geq 3$. Then the normal order of $\nu(\chi_{\phi}(\mathfrak{P}))$ is $\log \deg \mathfrak{P}$.

We can also consider the distribution of $\nu(\chi_{\phi}(\mathfrak{P}))$. The following theorem is analogous to [21, Theorem 1].

Theorem 3. (i) Let ϕ be a Drinfeld A-module over K of rank 2 with $\operatorname{End}_{\overline{K}}(\phi) = A$. For $x \in \mathbb{N}$ and $\gamma \in \mathbb{R}$,

$$\lim_{x \to \infty} \frac{1}{\pi_K(x)} \# \left\{ \mathfrak{P} \in \mathcal{P}_\phi \mid \deg \mathfrak{P} = x \text{ and } \frac{\nu(\chi_\phi(\mathfrak{P})) - \log \deg \mathfrak{P}}{\sqrt{\log \deg \mathfrak{P}}} \le \gamma \right\} = G(\gamma).$$

(ii) Let ϕ be a Drinfeld A-module over K of rank $r \geq 3$ with $\operatorname{End}_{\bar{K}}(\phi) = A$. Assuming the open image conjecture for ϕ , the above equality holds.

For a place $\mathfrak{P} \in \mathcal{P}_{\phi}$, the *exponent* $\lambda_{\phi}(\mathfrak{P})$ of $\phi(\mathbb{F}_{\mathfrak{P}})$ is defined to be the monic polynomial of A which generates the ideal containing the polynomials that annihilate all elements of $\phi(\mathbb{F}_{\mathfrak{P}})$. By the definitions of $\lambda_{\phi}(\mathfrak{P})$ and $\chi_{\phi}(\mathfrak{P})$, we have

$$\nu(\lambda_{\phi}(\mathfrak{P})) = \nu(\chi_{\phi}(\mathfrak{P})).$$

Hence, as a direct consequence of Theorems 1 and 3, we have

Corollary 4. Let ϕ be a Drinfeld A-module over K of rank $r \geq 2$ with $\operatorname{End}_{\bar{K}}(\phi) = A$. Assume the open image conjecture for ϕ when $r \geq 3$. (i) For $x \in \mathbb{N}$, we have

$$\sum_{\substack{\deg \mathfrak{P}=x\\ \mathfrak{P}\in\mathcal{P}_{\phi}}} \left(\nu(\lambda_{\phi}(\mathfrak{P})) - \log \deg \mathfrak{P}\right)^2 \ll \pi_K(x) \log x.$$

Thus the normal order of $\nu(\lambda_{\phi}(\mathfrak{P}))$ is $\log \deg \mathfrak{P}$. (ii) For $x \in \mathbb{N}$ and $\gamma \in \mathbb{R}$, we have

$$\lim_{x \to \infty} \frac{1}{\pi_K(x)} \# \left\{ \mathfrak{P} \in \mathcal{P}_\phi \mid \deg \mathfrak{P} = x \text{ and } \frac{\nu(\lambda_\phi(\mathfrak{P})) - \log \deg \mathfrak{P}}{\sqrt{\log \deg \mathfrak{P}}} \le \gamma \right\} = G(\gamma).$$

For a place $\mathfrak{P} \in \mathcal{P}_{\phi}$, let $a_{\phi}(\mathfrak{P}) \in A$ be the trace of the Frobenius of $\mathbb{F}_{\mathfrak{P}}$ acting on a Tate module of $\phi \otimes \mathbb{F}_{\mathfrak{P}}$ (see the next section for the definition). We can also consider the quantity $\nu(a_{\phi}(\mathfrak{P}))$ provided that $a_{\phi}(\mathfrak{P}) \neq 0$. The following theorems can be viewed as Drinfeld module analogues of the results of R. Murty and K. Murty in [23] and [24].

Theorem 5. Let ϕ be a Drinfeld A-module over K of rank $r \geq 2$ with $\operatorname{End}_{\bar{K}}(\phi) = A$. Assume the open image conjecture for ϕ when $r \geq 3$. For $x \in \mathbb{N}$, we have

$$\sum_{\substack{\deg \mathfrak{P}=x\\\mathfrak{P}\in\mathcal{P}_{\phi}\\a_{\phi}(\mathfrak{P})\neq 0}} \left(\nu(a_{\phi}(\mathfrak{P})) - \log \deg \mathfrak{P}\right)^{2} \ll \pi_{K}(x) \log x$$

Thus the normal order of $\nu(a_{\phi}(\mathfrak{P}))$ is $\log \deg \mathfrak{P}$.

Theorem 6. Let ϕ be a Drinfeld A-module over K of rank $r \geq 2$ with $\operatorname{End}_{\overline{K}}(\phi) = A$. Assume the open image conjecture for ϕ when $r \geq 3$. For $x \in \mathbb{N}$ and $\gamma \in \mathbb{R}$, we have

$$\lim_{x \to \infty} \frac{1}{\pi_K(x)} \# \left\{ \mathfrak{P} \in \mathcal{P}_\phi \, \big| \, \deg \mathfrak{P} = x, \, a_\phi(\mathfrak{P}) \neq 0, \text{ and } \frac{\nu(a_\phi(\mathfrak{P})) - \log \deg \mathfrak{P}}{\sqrt{\log \deg \mathfrak{P}}} \leq \gamma \right\} = G(\gamma).$$

Let $a \in A$ be a fixed polynomial. As we will see from our proofs of Theorems 5 and 6, the above two statements are also valid if we replace $a_{\phi}(\mathfrak{P})$ by $(a_{\phi}(\mathfrak{P}) - a)$. Moreover, for $m \in A$ with $m \neq 0$, let $\mathcal{V}(m)$ denote the number of primes dividing m, counted with

WENTANG KUO AND YU-RU LIU

multiplicity. Since the difference between $\nu(m)$ and $\mathcal{V}(m)$ is small on average, all the results in this paper hold when ν is replaced by \mathcal{V} . In Section 2, we state the open image conjecture for Drinfeld modules and discuss some of its consequences. We also recall the Chebotarev density theorem for function fields. In Section 3, we review the basic results in probability theory which are required in our proofs of Theorems 3 and 6. We prove Theorems 1 and 3 in Sections 4 and 5, and we conclude this paper by proving Theorems 5 and 6 in Section 6.

In this paper, we only consider a Drinfeld A-module ϕ over K, where $\operatorname{End}_{\bar{K}}(\phi) = A$ and the A-field K is of generic characteristic. One could ask questions analogous to these in the paper when $\operatorname{End}_{\bar{K}}(\phi) \neq A$ or when K is of finite characteristic. 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)). In this paper, all the implicit constants depend only on the Drinfeld A-module ϕ over K.

2. Preliminaries

The most important ingredients in our proof are the open image conjecture 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 ϕ be a Drinfeld A-module over L of rank r. For $m \in A$ with $m \neq 0$, we denote by $\phi[m]$ the m-division points of ϕ in the algebraic closure \overline{L} of L. By adjoining to L the m-division points, we obtain $L(\phi[m])$, the m-division field of ϕ , which is a finite Galois extension of L. If m is coprime to \mathfrak{w} , we have [3, Proposition 2.2]

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

By choosing a basis, we have a natural injection

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

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

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

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

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

GAUSSIAN LAWS ON DRINFELD MODULES

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

$$\rho_{\phi} = \prod_{l} \rho_{l,\phi} : \operatorname{Gal}(L^{\operatorname{sep}}/L) \to \operatorname{GL}_{r}(\hat{A}),$$

where \hat{A} is the profinite completion of A. The open image conjecture for ϕ concerns the nature of the map ρ_{ϕ} . The following statement is a special case of the general conjecture.

Conjecture 7. (Open image conjecture for Drinfeld modules) Let L be an A-field of generic A-characteristic, and let ϕ be a Drinfeld A-module over L of rank $r \geq 2$ with $\operatorname{End}_{\overline{L}}(\phi) = A$. Then the image of ρ_{ϕ} is open.

Although the general open image conjecture remains unsolved, exciting progress has recently been made. In particular, by the work of Gardeyn [9, Remark 3.15] [10, Remark 1.15] and Pink [26, Theorem 0.1], we now know that this conjecture holds for r = 2.

Now we come back to our original setting. Write $A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$. Let K be a finite extension of k, and let \mathbb{F}_K be the constant field of K. Let ϕ be a Drinfeld A-module over K, and let \mathcal{P}_{ϕ} be the set of places of K at which ϕ has good reduction. The following properties of Φ_m and $K(\phi[m])$ are consequences of the open image conjecture.

Proposition 8. Let ϕ be a Drinfeld A-module over K of rank $r \geq 2$ with $\operatorname{End}_{\bar{K}}(\phi) = A$. Assume Conjecture 7 holds for ϕ if $r \geq 3$. Then there exists $B(\phi) \in A$ (depending only on ϕ) such that for every $m \in A$ with $(m, B(\phi)) = 1$,

(i) the map Φ_m is an isomorphism.

(ii) $K(\phi[m])/K$ is a geometric extension.

Proof: We note that (i) is a direct consequence of the openness of the image of ρ_{ϕ} and the Chinese remainder theorem. Hence, it remains to prove (ii). The following argument has been implicitly discussed by David in [2]. For the completeness of the paper, we include a proof here following an idea from [2].

Let $B_1(\phi)$ be the product of all primes l such that ρ_l is not an isomorphism. For distinct primes $l_1, l_2 \in A$ with $(l_1 l_2, B_1(\phi)) = 1$, since Φ_{l_1} and Φ_{l_2} are isomorphisms, we have

$$\operatorname{Gal}(K(\phi[l_1l_2])/K)) = |\operatorname{Gal}(K(\phi[l_1])/K)| \cdot |\operatorname{Gal}(K(\phi[l_2])/K)|.$$

Hence the fields $K(\phi[l_1])$ and $K(\phi[l_2])$ are disjoint. Let K_{ϕ} be the field obtained by adjoining to K all division points of ϕ , and let $\overline{\mathbb{F}}_K$ be the algebraic closure of \mathbb{F}_K . For K = k, it was proved by Gekeler in [2, Lemma 3.2] that

$$[k_{\phi} \cap \mathbb{F}_k : \mathbb{F}_k] < \infty.$$

One can generalize his argument to a finite extension K of k and obtain

$$[K_{\phi} \cap \overline{\mathbb{F}}_K : \mathbb{F}_K] < \infty.$$

Therefore, by the disjoint property of $K(\phi[l])$, there are only finitely many primes $l \in A$ such that $K(\phi[l]) \cap \overline{\mathbb{F}}_K \neq \mathbb{F}_K$. Let $B_2(\phi)$ be the product of such exceptional primes. By taking $B(\phi) = B_1(\phi) \cdot B_2(\phi)$, Statement (ii) follows. This completes the proof of Proposition 8. For a place \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 [3] on the theory of good reduction, which is analogous to the classical result of Ogg-Néron-Shafarcvich for elliptic curves, ϕ has a 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 $\operatorname{Gal}(K(\phi[l^{\infty}])/K)$, and let $\phi \otimes \mathbb{F}_{\mathfrak{P}}$ be the Drinfeld module over $\mathbb{F}_{\mathfrak{P}}$, which is the reduction of ϕ at \mathfrak{P} . Then one can identify $T_l(\phi)$ and $T_l(\phi \otimes \mathbb{F}_{\mathfrak{P}})$, and the action of $\sigma_{\mathfrak{P}}$ on $T_l(\phi)$ is independent frobenius of $\mathbb{F}_{\mathfrak{P}}$. Moreover, the characteristic polynomial of $\sigma_{\mathfrak{P}}$ on $T_l(\phi)$ is independent of l (see [11, Corollary 3.4] and [29, Theorem 2(b)]) and we denoted it by $P_{\mathfrak{P},\phi}(X)$. Thus we have

Proposition 9. Let $\mathfrak{P} \in \mathcal{P}_{\phi}$ and $m \in A$ with (m, p) = 1. (i) The characteristic polynomial of $\Phi_m(\sigma_{\mathfrak{P}})$ is equal to $P_{\mathfrak{P},\phi}(X) \pmod{m}$. (ii) If $a_{\phi}(\mathfrak{P})$ is the trace of the Frobenius of $\mathbb{F}_{\mathfrak{P}}$ on $T_l(\phi \otimes \mathbb{F}_{\mathfrak{P}})$, then

 $\operatorname{tr}\left(\Phi_m(\sigma_{\mathfrak{P}})\right) = a_\phi(\mathfrak{P}) \,(\operatorname{mod} m).$

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 C a union of conjugacy classes of G. For $x \in \mathbb{N}$, define

$$\pi_C(x, L/K) = \# \Big\{ \mathfrak{P} \, \big| \, \deg \mathfrak{P} = x, \, \mathfrak{P} \text{ is a place unramified in } L/K, \text{ and } \sigma_{\mathfrak{P}} \subseteq C \Big\},\$$

where $\sigma_{\mathfrak{P}}$ is the Artin symbol of \mathfrak{P} in $\operatorname{Gal}(L/K)$. The following result of Ishibashi provides an estimate for $\pi_C(x, L/K)$.

Theorem 10. (Ishibashi [15, p 55]) If L/K is a geometric extension, then for $x \in \mathbb{N}$,

$$\pi_C(x, L/K) = \frac{|C|}{|G|} \pi_K(x) + O\Big((q^{d_K})^{x/2} |G| d(L/K)\Big),$$

where $\pi_K(x)$ is the number of places \mathfrak{P} of K of degree x, and d(L/K) is the degree of the different of L over K.

We remark here that the error term we state above has been improved by K. Murty and Scherk in [25] and M. Fried and M. Jarden in [7].

In order to estimate the error term in Theorem 10 when $L = K(\phi[m])$, one can apply the following result of Gardeyn.

Proposition 11. (Gardeyn [8, Proposition 6]) For $m \in A \setminus \mathbb{F}_q$, there exists a constant $C(\phi)$ (depending only on ϕ) such that

$$d(K(\phi[m])/K) \le C(\phi) \cdot [K(\phi[m]):K] \cdot \deg m.$$

In order to estimate $\nu(a_{\phi}(\mathfrak{P}))$, we need to exclude places $\mathfrak{P} \in \mathcal{P}_{\phi}$ with $a_{\phi}(\mathfrak{P}) = 0$. The following result of David [2] provides an upper bound for such \mathfrak{P} .

Theorem 12. (David [2, Theorem 1.1]) Let ϕ be a Drinfeld A-module over K of rank $r \geq 2$ with $\operatorname{End}_{\bar{K}}(\phi) = A$, and let $a \in A$ be fixed. For $x \in \mathbb{N}$, there exists a constant $D(\phi)$

(depending only on ϕ) such that

$$\# \left\{ \mathfrak{P}_{\phi} \mid \deg \mathfrak{P} = x \text{ and } a_{\phi}(\mathfrak{P}) = a \right\} \leq D(\phi) \cdot \frac{(q^{d_{K}})^{\theta(r)x}}{x},$$

where $\theta(r) = 1 - \frac{1}{2(r^{2}+2r)}.$

We remark here that although in [2] David only stated the result for K = k, her argument can be extended to a finite extension K of k without modification.

3. Review of probability theory

To prove Theorem 3, we need the following results from the probability theory; their proofs can be found in [1] and [6]. For $x \in \mathbb{N}$, let V_x be a real-valued random variable with a probability measure P_x . Let F_x be its associated distribution function and $E_x\{V_x\}$ the expectation of V_x with respect to F_x .

Definition Given a sequence of random variables $\{V_x\}$ and $\alpha \in \mathbb{R}$, we say $\{V_x\}$ converges in probability to α if for any $\epsilon > 0$,

$$\lim_{x \to \infty} \Pr_x \{ |V_x - \alpha| > \epsilon \} = 0.$$

We denote it by

$$V_x \xrightarrow{p} \alpha.$$

Proposition 13. ([1, p 134]) Given a sequence of random variables $\{V_x\}$, if

$$\lim_{x \to \infty} \mathbf{E}_x \big\{ |V_x| \big\} = 0,$$

then we have

$$V_x \xrightarrow{p} 0.$$

Proposition 14. ([1, p 134-135], [6, p.247]) Let $\{V_x\}, \{W_x\}$, and $\{U_x\}$ be sequences of random variables with the same probability measure P_x . Let F be a distribution function. Suppose that

$$V_x \xrightarrow{p} 1$$
 and $W_x \xrightarrow{p} 0.$

Then for all $\gamma \in \mathbb{R}$, we have

$$\lim_{x \to \infty} \mathbf{P}_x \big\{ U_x \le \gamma \big\} = F(\gamma)$$

if and only if

$$\lim_{x \to \infty} \mathbf{P}_x \{ (V_x U_x + W_x) \le \gamma \} = F(\gamma).$$

For $\gamma \in \mathbb{R}$, let $G(\gamma)$ denote the Gaussian normal distribution, i.e.,

$$G(\gamma) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{\frac{-t^2}{2}} dt.$$

For $s \in \mathbb{N}$, the s-th moment μ_s of G is defined by

$$\mu_s = \int_{-\infty}^{\infty} t^s dG(t)$$

The following proposition shows that G is uniquely determined by these moments.

Proposition 15. ([6, p 262-263]) Let $\{F_x\}$ be a sequence of distribution functions. Suppose that for all $s \in \mathbb{N}$,

$$\lim_{x \to \infty} \int_{-\infty}^{\infty} t^s dF_x(t) = \mu_s.$$

Then for all $\gamma \in \mathbb{R}$, we have

$$\lim_{x \to \infty} F_x(\gamma) = G(\gamma).$$

This next proposition is an analogue of the Lebesgue Dominated Convergence Theorem.

Proposition 16. ([6, p 244-245]) Let $s \in \mathbb{N}$ and $\{F_x\}$ a sequence of distribution functions. Suppose that for all $\gamma \in \mathbb{R}$,

$$\lim_{x \to \infty} F_x(\gamma) = G(\gamma),$$

and for some $\delta = \delta(s) > 0$,

$$\sup_{x} \left\{ \int_{-\infty}^{\infty} |t|^{s+\delta} dF_x(t) \right\} < \infty.$$

Then we have

$$\lim_{x \to \infty} \int_{-\infty}^{\infty} t^s dF_x(t) = \mu_s.$$

The next proposition is a special case of the Central Limit Theorem.

Proposition 17. ([6, p 256-258]) Let $V_1, V_2, \dots, V_i, \dots$ be a sequence of independent random variables with a probability measure P, and let $E\{V_i\}$ and $Var\{V_i\}$ be the expectation and the variance of V_i , respectively. Also, we denote by $Im V_i$ the image of V_i . Suppose that

(1) $\sup_{i} \{\operatorname{Im} V_{i}\} < \infty,$ (2) $\operatorname{E} \{V_{i}\} = 0 \quad and \quad \operatorname{Var} \{V_{i}\} < \infty \quad for \ all \ i \in \mathbb{N}.$

For $x \in \mathbb{N}$, let G_x be the normalization of V_1, V_2, \cdots, V_x , i.e.,

$$G_x = \left(\sum_{i=1}^x V_i\right) / \left(\sum_{i=1}^x \operatorname{Var}\{V_i\}\right)^{\frac{1}{2}}.$$

If $\sum_{i=1}^{\infty} \operatorname{Var}\{V_i\}$ diverges, we have

$$\lim_{x \to \infty} \mathbf{P} \big\{ G_x \le \gamma \big\} = G(\gamma).$$

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 ϕ over K of rank $r \geq 2$ with

GAUSSIAN LAWS ON DRINFELD MODULES

 $\operatorname{End}_{\bar{K}}(\phi) = A$, let \mathcal{P}_{ϕ} be the set of places of K at which ϕ has good reduction. In this section, we provide a proof of Theorem 1, which states that for $x \in \mathbb{N}$,

$$\sum_{\substack{\deg \mathfrak{P}=x\\ \mathfrak{P}\in \mathcal{P}_{\phi}}} \left(\nu(\chi_{\phi}(\mathfrak{P})) - \log \deg \mathfrak{P}\right)^2 \ll \pi_K(x) \log x.$$

To prove this inequality, we need the following lemma, which can be derived from the result of Lang and Weil in [17, Theorem 1].

Lemma 18. For $r \in \mathbb{N}$, $r \geq 2$, and $l \in A$ a prime, define

$$C_{l,r} = \Big\{ g \in \operatorname{GL}_r(A/lA) \, \big| \, \det \left(g - I_r \right) \equiv 0 \pmod{l} \Big\},$$

where GL_r is the general linear group of dimension r and I_r the $r \times r$ identity matrix. Then we have

$$|C_{l,r}| = q^{(r^2-1)\deg l} + O(q^{(r^2-2)\deg l}),$$

which implies that

$$\frac{|C_{l,r}|}{|\operatorname{GL}_r(A/lA)|} = \frac{1}{q^{\deg l}} + O\left(1/q^{2\deg l}\right).$$

Now, we are ready to prove Theorem 1. We remark here that the following proof works for any ϕ of rank $r \geq 2$ provided that when $r \geq 3$, the open image conjecture for ϕ is satisfied.

Proof: (of Theorem 1) Given a Drinfeld A-module ϕ over K of rank $r \geq 2$ with $\operatorname{End}_{\bar{K}}(\phi) = A$, let $B(\phi) \in A$ be defined as in Proposition 8. We denote by \sum^* the sum over places \mathfrak{P}_{ϕ} , and by \sum^{**} the sum over primes $l \in A$ with $(l, B(\phi)) = 1$. For $x \in \mathbb{N}$, we consider

(3)

$$\sum_{\deg \mathfrak{P}=x}^{*} \left(\nu(\chi_{\phi}(\mathfrak{P})) - \log \deg \mathfrak{P}\right)^{2} \\
= \sum_{\deg \mathfrak{P}=x}^{*} \nu^{2}(\chi_{\phi}(\mathfrak{P})) - 2\log x \sum_{\deg \mathfrak{P}=x}^{*} \nu(\chi_{\phi}(\mathfrak{P})) + (\log x)^{2} \sum_{\deg \mathfrak{P}=x}^{*} 1.$$

Since all but finitely many places \mathfrak{P} satisfying $\mathfrak{P} \in \mathcal{P}_{\phi}$, we have

(4)
$$\sum_{\deg \mathfrak{P}=x}^{*} 1 = \pi_K(x) + O(1),$$

where

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

Let $\delta \in \mathbb{R}$ with $0 < \delta < 1/d$ (a choice of δ will be made later). We have seen in (2) that $\deg \chi_{\phi}(\mathfrak{P}) = d_K \deg \mathfrak{P} = d_K x$. Thus there are at most O(1) many primes l with $l|\chi_{\phi}(\mathfrak{P})$ and $\deg l > \delta x$. Also, there are at most O(1) many primes l with $(l, B(\phi)) \neq 1$. Hence,

the second sum in (3) can be written as

$$\sum_{\deg \mathfrak{P}=x}^{*} \nu(\chi_{\phi}(\mathfrak{P})) = \sum_{\deg \mathfrak{P}=x}^{*} \sum_{\substack{\deg l \le \delta x \\ l \mid \chi_{\phi}(\mathfrak{P})}} 1 + \sum_{\deg \mathfrak{P}=x}^{*} \sum_{\substack{\deg l > \delta x \\ l \mid \chi_{\phi}(\mathfrak{P})}} 1$$
$$= \sum_{\deg l \le \delta x} \sum_{\substack{\deg \mathfrak{P}=x \\ l \mid \chi_{\phi}(\mathfrak{P})}}^{*} 1 + O(\pi_{K}(x)).$$

Let $\mathfrak{p} = \mathfrak{P} \cap A$ and let $p \in A$ be the prime with $pA = \mathfrak{p}$. Since [K : k] = d and $[\mathbb{F}_K : \mathbb{F}_q] = d_K$ we have

 $[\mathbb{F}_{\mathfrak{P}}: A/\mathfrak{p}] \leq d,$ and $\deg p \cdot [\mathbb{F}_{\mathfrak{P}}: A/\mathfrak{p}] = [\mathbb{F}_{\mathfrak{P}}: \mathbb{F}_q] = \deg \mathfrak{P} \cdot d_K.$

Therefore, we have

 $\deg p \ge (\deg \mathfrak{P} \cdot d_K)/d \ge x/d.$

We note that since $\delta < 1/d$, if l is a prime with deg $l \leq \delta x$, we have (l, p) = 1. Since $l \mid \chi_{\phi}(\mathfrak{P})$ if and only if $P_{\mathfrak{P},\phi}(1) \equiv 0 \pmod{l}$, by Proposition 9(i), this is equivalent to say that $\Phi_l(\sigma_{\mathfrak{P}})$ has an eigenvalue 1, i.e., $\Phi_l(\sigma_{\mathfrak{P}})$ belongs to one of the conjugacy classes of $C_{l,r}$ as defined in Lemma 18. Applying Theorem 10, Propositions 8, 11, and Lemma 18, we have

$$\sum_{\deg l \le \delta x} \sum_{\substack{\deg \mathfrak{P}=x \\ l \mid \chi_{\phi}(\mathfrak{P})}}^{**} 1 = \sum_{\deg l \le \delta x} \left(\left(\frac{1}{q^{\deg l}} + O(1/q^{2 \deg l}) \right) \pi_{K}(x) + O\left((q^{d_{K}})^{x/2} q^{2r^{2} \deg l} \deg l \right) \right)$$
$$= \pi_{K}(x) \sum_{\deg l \le \delta x} \frac{1}{q^{\deg l}} + O(\pi_{K}(x)) + O\left((q^{d_{K}})^{x/2} \sum_{\deg l \le \delta x} \left(q^{2r^{2} \deg l} \deg l \right) \right)$$
$$= \pi_{K}(x) \log x + O(\pi_{K}(x)) + O\left(q^{((2r^{2}+2)\delta + d_{K}/2)x} \right).$$

The last equality follows from the prime number theory for polynomials. Hence, if $(2r^2 + 2)\delta < d_K/2$, we obtain

(5)
$$\sum_{\deg \mathfrak{P}=x}^{*} \nu(\chi_{\phi}(\mathfrak{P})) = \pi_{K}(x) \log x + O(\pi_{K}(x)).$$

Now, we consider

$$\sum_{\deg \mathfrak{P}=x}^{*} \nu^2(\chi_{\phi}(\mathfrak{P})).$$

Let $\delta \in \mathbb{R}$ with $0 < \delta < 1/(2d)$. Since $\chi_{\phi}(\mathfrak{P})$ has at most O(1) many prime divisors l satisfying either deg $l > \delta x$ or $(l, B(\phi)) \neq 1$, using the estimate in (5), we have

$$\sum_{\deg \mathfrak{P}=x}^{*} \nu^2(\chi_{\phi}(\mathfrak{P})) = \sum_{\deg \mathfrak{P}=x}^{*} \left(\sum_{\substack{\deg l \le \delta x \\ l \mid \chi_{\phi}(\mathfrak{P})}}^{**} 1 + O(1) \right)^2$$
$$= \sum_{\substack{\deg l_1, \deg l_2 \le \delta x \\ l_1 \neq l_2}}^{**} \sum_{\substack{\deg \mathfrak{P}=x \\ l_1 l_2 \mid \chi_{\phi}(\mathfrak{P})}}^{*} 1 + O\left(\pi_K(x) \log x\right).$$

For distinct primes l_1, l_2 with deg $l_1 \leq \delta x$ and deg $l_2 \leq \delta x$, since $\delta < 1/(2d)$ and deg $p \geq x/d$, we have $(l_1l_2, p) = 1$. Since $l_1l_2 | \chi_{\phi}(\mathfrak{P})$ if and only if $P_{\mathfrak{P},\phi}(1) \equiv 0 \pmod{l_1l_2}$, by Proposition 9(i), this is equivalent to say that $\Phi_{l_1l_2}(\sigma_{\mathfrak{P}})$ belongs to one of the conjugacy classes of $C_{l_1l_2,r}$, where

$$C_{l_1 l_2, r} = \Big\{ g \in \operatorname{GL}_r(A/l_1 l_2 A) \, \big| \, \det (g - I_r) = 0 \Big\}.$$

Since $l_1 \neq l_2$, by the Chinese remainder theorem, we have

$$|C_{l_1 l_2, r}| = |C_{l_1, r}| |C_{l_2, r}| \quad \text{and} \quad |\operatorname{GL}_r(A/l_1 l_2 A)| = |\operatorname{GL}_r(A/l_1 A)| |\operatorname{GL}_r(A/l_2 A)|.$$

Combining this with Theorem 10, Propositions 8, 11, and Lemma 18, we get

$$\sum_{\substack{d \in g \ l_1, d \in g \ l_2 \le \delta x \\ l_1 \neq l_2}} \sum_{\substack{d \in g \ \mathfrak{P} = x \\ l_1 l_2 \mid \chi_{\phi}(\mathfrak{P})}}^{*} 1 = \pi_K(x) \sum_{\substack{d \in g \ l_1, d \in g \ l_2 \le \delta x \\ l_1 \neq l_2}}^{**} \frac{1}{q^{\deg l_1} q^{\deg l_2}} + O(\pi_K(x)) + O\left(\pi_K(x) \log l_2 \log l_2 \log l_1 \log l_2 \log l_2 \log l_2 \log l_2 \log l_2 \log l_2 \log l_2\right) \\ = \pi_K(x) (\log x)^2 + O\left(\pi_K(x) \log x\right) + O\left(q^{(2(2r^2 + 2)\delta + d_K/2)x}\right).$$

Hence, if $2(2r^2+2)\delta < d_K/2$, we have

(6)
$$\sum_{\deg \mathfrak{P}=x}^{*} \nu^2(\chi_{\phi}(\mathfrak{P})) = \pi_K(x)(\log x)^2 + O\big(\pi_K(x)\log x\big).$$

Combining (3), (4), (5), and (6), by choosing δ such that

$$0 < \delta < \min\left\{\frac{1}{2d}, \frac{d_K}{4(2r^2+2)}\right\},$$

we obtain

$$\sum_{\deg \mathfrak{P}=x}^{*} \left(\nu(\chi_{\phi}(\mathfrak{P})) - \log \deg x\right)^{2} \ll \pi_{K}(x) \log x.$$

This completes the proof of Theorem 1.

5. Proof of Theorem 3

In this section, we provide a proof of Theorem 3. For $x \in \mathbb{N}$ and $\gamma \in \mathbb{R}$, let

$$P_x \Big\{ \mathfrak{P} \, \big| \, \mathfrak{P} \text{ satisfies } \frac{\nu(\chi_\phi(\mathfrak{P})) - \log \deg \mathfrak{P}}{\sqrt{\log \deg \mathfrak{P}}} \leq \gamma \Big\}$$

denote the quantity

$$\frac{1}{\pi_K(x)} \# \Big\{ \mathfrak{P} \in \mathcal{P}_\phi \mid \deg \mathfrak{P} = x \text{ and } \frac{\nu(\chi_\phi(\mathfrak{P})) - \log \deg \mathfrak{P}}{\sqrt{\log \deg \mathfrak{P}}} \leq \gamma \Big\}.$$

Our goal is to prove that

$$\lim_{x \to \infty} \Pr_x \left\{ \mathfrak{P} \, \big| \, \mathfrak{P} \text{ satisfies } \frac{\nu(\chi_\phi(\mathfrak{P})) - \log \deg \mathfrak{P}}{\sqrt{\log \deg \mathfrak{P}}} \le \gamma \right\} = G(\gamma).$$

We remark here that P_x is the probability measure that places weights $1/\pi_K(x)$ at each place \mathfrak{P} of K of degree x. Following the approach in [19, Theorem 1], which is based

on the idea of Billingsley in [1], we divide our proof into four lemmas. Again, under the assumption of the open image conjecture for Drinfeld modules, our proof holds for any rank $r \geq 2$.

Given a Drinfeld A-module ϕ over K, let $B(\phi)$ be defined as in Proposition 8. Let \sum^* and \sum^{**} be defined as in the proof of Theorem 1. For $x \in \mathbb{N}$ with $x \geq 3$, let $y = y(x) = [x/\log x]$. For $m \in A$, let $\nu_y(m)$ denote the number of distinct primes l dividing m, which satisfy deg $l \leq y$ and $(l, B(\phi)) = 1$. It is a truncation function of $\nu(m)$. The following lemma shows that we can replace ν by ν_y in Theorem 3.

Lemma 19. For $\gamma \in \mathbb{R}$, we have

$$\lim_{x \to \infty} \Pr_x \left\{ \mathfrak{P} \mid \mathfrak{P} \text{ satisfies } \frac{\nu(\chi_\phi(\mathfrak{P})) - \log x}{\sqrt{\log x}} \le \gamma \right\} = G(\gamma)$$

if and only if

$$\lim_{x \to \infty} \Pr_x \left\{ \mathfrak{P} \, \big| \, \mathfrak{P} \text{ satisfies } \frac{\nu_y(\chi_\phi(\mathfrak{P})) - \log x}{\sqrt{\log x}} \le \gamma \right\} = G(\gamma).$$

Proof: Since

$$\frac{\nu_y(\chi_\phi(\mathfrak{P})) - \log x}{\sqrt{\log x}} = \frac{\nu(\chi_\phi(\mathfrak{P})) - \log x}{\sqrt{\log x}} + \frac{\nu_y(\chi_\phi(\mathfrak{P})) - \nu(\chi_\phi(\mathfrak{P}))}{\sqrt{\log x}}$$

by Propositions 13 and 14, to prove this lemma, it suffices to prove that

$$\lim_{x \to \infty} \mathbf{E}_x \left\{ \left| \frac{\nu(\chi_\phi(\mathfrak{P})) - \nu_y(\chi_\phi(\mathfrak{P}))}{\sqrt{\log x}} \right| \right\} = 0.$$

Let $\delta \in \mathbb{R}$ with $0 < \delta < 1$. Since there are at most O(1) many primes l with deg $l > \delta x$ which satisfy either $l|B(\phi)$ or $l|\chi_{\phi}(\mathfrak{P})$, we have

$$\sum_{\deg \mathfrak{P}=x}^{*} \left| \nu(\chi_{\phi}(\mathfrak{P})) - \nu_{y}(\chi_{\phi}(\mathfrak{P})) \right| = \sum_{\substack{y < \deg l \le \delta x \\ l \mid \chi_{\phi}(\mathfrak{P})}}^{**} \sum_{\substack{\chi_{\phi}(\mathfrak{P}) \\ l \mid \chi_{\phi}(\mathfrak{P})}}^{*} 1 + O(\pi_{K}(x)).$$

Also, by Theorem 10, Propositions 8, 9(i), 11, and Lemma 18, if $\delta < 1/d$ and $(2r^2+2)\delta < d_K/2$, we have

$$\sum_{\substack{y < \deg l \le \delta x \\ l \mid \chi_{\phi}(\mathfrak{P})}}^{**} \sum_{\substack{q < \deg l \le \delta x \\ k \mid \chi_{\phi}(\mathfrak{P})}}^{*} 1 = \sum_{\substack{y < \deg l \le \delta x \\ q^{\deg l} = k}}^{**} \left(\frac{\pi_K(x)}{q^{\deg l}} + O\left(\frac{\pi_K(x)}{q^{2\deg l}}\right) + O\left((q^{d_K})^{x/2} q^{2r^2 \deg l} \deg l\right) \right)$$
$$\ll \pi_K(x) \log \log x.$$

Thus by choosing δ such that

$$0 < \delta < \min\left\{\frac{1}{d}, \frac{d_K}{2(2r^2 + 2)}\right\},$$

we have

$$\sum_{\deg \mathfrak{P}=x}^{*} \left| \nu(\chi_{\phi}(\mathfrak{P})) - \nu_{y}(\chi_{\phi}(\mathfrak{P})) \right| \ll \pi_{K}(x) \log \log x.$$

It follows that as $x \to \infty$,

$$\mathbf{E}_x\Big\{\Big|\frac{\nu(\chi_\phi(\mathfrak{P}))-\nu_y(\chi_\phi(\mathfrak{P}))}{\sqrt{\log x}}\Big|\Big\}\ll \frac{\pi_K(x)\log\log x}{\pi_K(x)\sqrt{\log x}} ~\longrightarrow~ 0.$$

This completes the proof of Lemma 19.

In order to apply the central limit theorem, we now associate ν_y to a sum of independent random variables. For a prime $l \in A$, define an independent random variable V_l by

$$P\{V_l = 1\} = \frac{1}{q^{\deg l}}$$
 and $P\{V_l = 0\} = 1 - \frac{1}{q^{\deg l}}$.

Let S_y be a random variable defined by

$$S_y = \sum_{\deg l \le y}^{**} V_l.$$

Since $y = [x/\log x]$, we have

$$\mathbb{E}\left\{S_y\right\} = \sum_{\deg l \le y}^{**} \frac{1}{q^{\deg l}} = \log x + O\left(\log\log x\right)$$

and

$$\operatorname{Var}\left\{S_{y}\right\} = \sum_{\deg l \leq y}^{**} \frac{1}{q^{\deg l}} \left(1 - \frac{1}{q^{\deg l}}\right) = \log x + O\left(\log \log x\right).$$

The following lemma shows that the log x term in Lemma 19 can be replaced by $E\{S_y\}$ and $Var\{S_y\}$.

Lemma 20. For $\gamma \in \mathbb{R}$, we have

$$\lim_{x \to \infty} \mathcal{P}_x \Big\{ \mathfrak{P} \, \big| \, \mathfrak{P} \text{ satisfies } \frac{\nu_y(\chi_\phi(\mathfrak{P})) - \log x}{\sqrt{\log x}} \le \gamma \Big\} = G(\gamma)$$

if and only if

$$\lim_{x \to \infty} \Pr_x \left\{ \mathfrak{P} \, \big| \, \mathfrak{P} \text{ satisfies } \frac{\nu_y(\chi_\phi(\mathfrak{P})) - \mathrm{E}\{S_y\}}{\sqrt{\mathrm{Var}\{S_y\}}} \le \gamma \right\} = G(\gamma).$$

Proof: Write

$$\frac{\nu_y(\chi_\phi(\mathfrak{P})) - \mathrm{E}\{S_y\}}{\sqrt{\mathrm{Var}\{S_y\}}} = \frac{\nu_y(\chi_\phi(\mathfrak{P})) - \log x}{\sqrt{\log x}} \cdot \frac{\sqrt{\log x}}{\sqrt{\mathrm{Var}\{S_y\}}} + \frac{\log x - \mathrm{E}\{S_y\}}{\sqrt{\mathrm{Var}\{S_y\}}}.$$

The above computations of $E\{S_y\}$ and $Var\{S_y\}$ imply that

$$\frac{\sqrt{\log x}}{\sqrt{\operatorname{Var}\{S_y\}}} \xrightarrow{p} 1 \quad \text{and} \quad \frac{\log x - \operatorname{E}\{S_y\}}{\sqrt{\operatorname{Var}\{S_y\}}} \xrightarrow{p} 0.$$

By Proposition 14, the lemma follows.

Now, for a prime $l \in A$, let $\delta_l : A \to \{0, 1\}$ be a random variable defined by

$$\delta_l(m) = \begin{cases} 1 & \text{if } l \mid m, \\ 0 & \text{otherwise.} \end{cases}$$

Hence, we can write

$$\nu_y(\chi_\phi(\mathfrak{P})) = \sum_{\deg l \le y}^{**} \delta_l(\chi_\phi(\mathfrak{P})).$$

By Theorem 10, Propositions 8, 9(i), 11, and Lemma 18, we have

$$P_x\left\{\mathfrak{P} \mid \mathfrak{P} \text{ satisfies } \delta_l(\chi_\phi(\mathfrak{P})) = 1\right\} = \frac{1}{q^{\deg l}} + O\left(1/q^{2 \deg l}\right).$$

Hence, the expectations of random variables V_l and δ_l are close. Thus the sum S_y of V_l is a good approximation of the sum ν_y of δ_l . Indeed, the s-th moments of their normalizations are equal as $x \to \infty$.

Lemma 21. For $s \in \mathbb{N}$, we have

$$\lim_{x \to \infty} \left| \mathbf{E} \left\{ \left(\frac{S_y - \mathbf{E} \{S_y\}}{\sqrt{\operatorname{Var} \{S_y\}}} \right)^s \right\} - \mathbf{E}_x \left\{ \left(\frac{\nu_y(\chi_\phi(\mathfrak{P})) - \mathbf{E} \{S_y\}}{\sqrt{\operatorname{Var} \{S_y\}}} \right)^s \right\} \right| = 0.$$

Proof: For an integer t with $0 \le t \le s$, write

$$\mathbf{E}\{S_{y}^{t}\} = \sum_{u=1}^{t} \sum_{u=1}^{t} \sum_{u=1}^{t} \frac{t!}{t_{1}!\cdots t_{u}!} \sum_{u=1}^{t} \mathbf{E}\{V_{l_{1}}^{t_{1}}\cdots V_{l_{u}}^{t_{u}}\},$$

where \sum' denotes the sum over all *u*-tuples (t_1, t_2, \dots, t_u) of positive integers such that $t_1 + t_2 + \dots + t_u = t$, and \sum'' denotes the sum over all *u*-tuples of distinct primes (l_1, l_2, \dots, l_u) with deg $l_i \leq y$ and $(l_i, B(\phi)) = 1$ $(1 \leq i \leq u)$. Since V_{l_i} take only values 0 or 1 and they are independent, we have

$$\mathbf{E}\{V_{l_1}^{t_1}\cdots V_{l_u}^{t_u}\}=\mathbf{E}\{V_{l_1}\cdots V_{l_u}\}=\prod_{i=1}^u \frac{1}{q^{\deg l_u}}.$$

Similarly, if we abbreviate $\nu_y(\chi_\phi(\mathfrak{P}))$ and $\delta_l(\chi_\phi(\mathfrak{P}))$ by ν_y and δ_l , respectively, we have

$$E_x\{\nu_y^t\} = \sum_{u=1}^t \sum_{u=1}^t t! \frac{t!}{t_1! \cdots t_u!} \sum_{u=1}^t E_x\{\delta_{l_1}^{t_1} \cdots \delta_{l_u}^{t_u}\}.$$

Since δ_{l_i} take only values 0 or 1, combining the Chinese remainder theorem with Theorem 10, Propositions 8, 9(i), 11, and Lemma 18, we obtain

$$E_{x}\left\{\delta_{l_{1}}^{t_{1}}\cdots\delta_{l_{u}}^{t_{u}}\right\} = E_{x}\left\{\delta_{l_{1}}\cdots\delta_{l_{u}}\right\}$$

= $\frac{1}{\pi_{K}(x)}\sum_{\substack{\deg\mathfrak{P}=x\\l_{1}l_{2}\cdots l_{u}\mid\chi_{\phi}(\mathfrak{P})}}^{*}1$
= $\prod_{i=1}^{u}\frac{1}{q^{\deg l_{u}}} + O\left(x(q^{d_{K}})^{-x/2}q^{2r^{2}\deg l_{1}+\cdots+2r^{2}\deg l_{u}}\deg l_{1}\cdots l_{u}\right).$

It follows that

$$\left| \mathbf{E} \{ V_{l_1}^{t_1} \cdots V_{l_u}^{t_u} \} - \mathbf{E}_x \{ \delta_{l_1}^{t_1} \cdots \delta_{l_u}^{t_u} \} \right| \ll x (q^{d_K})^{-x/2} q^{(2r^2+1) \deg l_1 + \dots + (2r^2+1) \deg l_u}.$$

Thus

$$\begin{split} \left| \mathbf{E} \{ S_y^t \} - \mathbf{E}_x \{ \nu_y^t \} \right| &\ll \sum_{u=1}^t \sum' \frac{t!}{t_1! t_2! \cdots t_u!} \sum'' x(q^{d_K})^{-x/2} q^{(2r^2+1) \deg l_1 + \cdots + (2r^2+1) \deg l_u} \\ &\ll x(q^{d_K})^{-x/2} \left(\sum_{\deg l \le y} q^{(2r^2+1) \deg l} \right)^t \\ &\ll xq^{-d_K x/2 + (2r^2+2)ty}. \end{split}$$

Write

$$\mathbf{E}\left\{\left(S_y - \mathbf{E}\left\{S_y\right\}\right)^s\right\} = \sum_{t=0}^s \binom{s}{t} \mathbf{E}\left\{S_y^t\right\} \mathbf{E}\left\{S_y\right\}^{s-t}$$

and

$$\mathbf{E}_x\left\{\left(\nu_y - \mathbf{E}\left\{S_y\right\}\right)^s\right\} = \sum_{t=0}^s \binom{s}{t} \mathbf{E}_x\left\{\nu_y^t\right\} \mathbf{E}\left\{S_y\right\}^{s-t}.$$

Since $E\{S_y\} = \log x + O(\log \log x)$ and $y = [x/\log x] \gg \log x$, we have

$$\left| \mathbf{E} \{ \left(S_y - \mathbf{E} \{ S_y \} \right)^s \} - \mathbf{E}_x \{ \left(\nu_y - \mathbf{E} \{ S_y \} \right)^s \} \right| \ll \sum_{t=0}^s \binom{s}{t} x q^{-d_K x/2 + (2r^2 + 2)ty} (\log x)^{s-t}$$
$$\ll x q^{-d_K x/2} \left(q^{(2r^2 + 2)y} + \log x \right)^s$$
$$\ll x q^{-d_K x/2 + (2r^2 + 2)sy}.$$

Since $y < \epsilon x$ for any $\epsilon > 0$, as $x \to \infty$,

$$\left| \mathrm{E}\left\{ \left(S_y - \mathrm{E}\left\{ S_y \right\} \right)^s \right\} - \mathrm{E}_x\left\{ \left(\nu_y - \mathrm{E}\left\{ S_y \right\} \right)^s \right\} \right| \longrightarrow 0.$$

Thus the lemma follows.

By combining Lemmas 19, 20, and 21, we have reduced Theorem 3 into a purely probabilistic problem which is about a normal distribution of the quantity

$$\frac{S_y - \mathrm{E}\{S_y\}}{\sqrt{\mathrm{Var}\{S_y\}}}.$$

Hence, the remaining proof follows in the same way as the one in [19, Theorem 1]. More precisely, as in [19, Lemma 7], we have the following lemma about the s-th moment of S_y .

Lemma 22. For $s \in \mathbb{N}$, we have

$$\sup_{y} \left| \mathbf{E} \left\{ \left(\frac{S_y - \mathbf{E} \{S_y\}}{\sqrt{\operatorname{Var} \{S_y\}}} \right)^s \right\} \right| < \infty.$$

Combining Lemmas 19, 20, 21, 22 with Propositions 15, 16, and 17, the same argument as the one in [19, Section 4] gives us

$$\lim_{x \to \infty} \Pr_x \left\{ \mathfrak{P} \, \big| \, \mathfrak{P} \text{ satisfies } \frac{\nu(\chi_\phi(\mathfrak{P})) - \log \deg \mathfrak{P}}{\sqrt{\log \deg \mathfrak{P}}} \le \gamma \right\} = G(\gamma).$$

This completes the proof of Theorem 3.

WENTANG KUO AND YU-RU LIU

6. Proofs of Theorems 5 and 6

In this section, we consider $\nu(a_{\phi}(\mathfrak{P}))$. In order to prove Theorems 5 and 6, we need the following result, which is similar to Lemma 18.

Lemma 23. For $r \in \mathbb{N}$, $r \geq 2$, and $l \in A$ a prime, define

$$D_{l,r} = \Big\{ g \in \operatorname{GL}_r(A/lA) \, \big| \operatorname{tr} g \equiv 0 \pmod{l} \Big\}.$$

Then we have

$$|D_{l,r}| = q^{(r^2-1)\deg l} + O(q^{(r^2-2)\deg l}),$$

which implies that

$$\frac{|D_{l,r}|}{|\operatorname{GL}_r(A/lA)|} = \frac{1}{q^{\deg l}} + O\left(1/q^{2\deg l}\right).$$

Now, we are ready to prove Theorems 5 and 6. Since our approaches are similar to those of Theorems 1 and 3, we will only sketch their proofs. In the following, let \sum^* and \sum^{**} be defined as in the proof of Theorem 1.

Proof: (of Theorem 5) Using the same principle as the one in the proof of Theorem 1, to prove Theorem 5, it suffices to estimate the sums

$$\sum_{\substack{\deg \mathfrak{P}=x\\a_{\phi}(\mathfrak{P})\neq 0}}^{*} \nu(a_{\phi}(\mathfrak{P})) \quad \text{and} \quad \sum_{\substack{\deg \mathfrak{P}=x\\a_{\phi}(\mathfrak{P})\neq 0}}^{*} \nu^{2}(a_{\phi}(\mathfrak{P})).$$

Let $\delta \in \mathbb{R}$ with $0 < \delta < 1$. We have

$$\sum_{\substack{\deg \mathfrak{P}=x\\a_{\phi}(\mathfrak{P})\neq 0}}^{*} \nu(a_{\phi}(\mathfrak{P})) = \sum_{\substack{\deg \mathfrak{P}=x\\a_{\phi}(\mathfrak{P})\neq 0}}^{*} \sum_{\substack{\deg l \leq \delta x\\l \mid a_{\phi}(\mathfrak{P})}}^{1 + O(\pi_{K}(x))}$$
$$= \sum_{\substack{\deg l \leq \delta x\\l \mid a_{\phi}(\mathfrak{P}), a_{\phi}(\mathfrak{P})\neq 0}}^{**} \sum_{\substack{\deg \mathfrak{P}=x\\l \mid a_{\phi}(\mathfrak{P}), a_{\phi}(\mathfrak{P})\neq 0}}^{*} 1 + O(\pi_{K}(x)).$$

By Theorem 12,

$$\sum_{\deg l \le \delta x}^{**} \sum_{\substack{\deg \mathfrak{P}=x\\l|a_{\phi}(\mathfrak{P}), a_{\phi}(\mathfrak{P}) \neq 0}}^{*} 1 = \sum_{\deg l \le \delta x}^{**} \sum_{\substack{\deg \mathfrak{P}=x\\l|a_{\phi}(\mathfrak{P})}}^{*} 1 + O\left(q^{(\delta+d_{K}\theta(r))x}\right).$$

Let $\mathfrak{p} = \mathfrak{P} \cap A$ and let $p \in A$ be the prime with $pA = \mathfrak{p}$. If $\delta < 1/d$, we have (l, p) = 1. Then by Proposition 9(ii), we have $l \mid a_{\phi}(\mathfrak{P})$ if and only if $\Phi_l(\sigma_{\mathfrak{P}})$ belongs to one of the conjugacy classes of $D_{l,r}$ as defined in Lemma 23. Applying Theorem 10, Propositions 8, 11, and Lemma 23, we have

$$\sum_{\deg l \le \delta x} \sum_{\substack{\deg \mathfrak{P}=x \\ l \mid a_{\phi}(\mathfrak{P})}}^{**} 1 = \sum_{\deg l \le \delta x} \left(\left(\frac{1}{q^{\deg l}} + O(1/q^{2 \deg l}) \right) \pi_{K}(x) + O\left((q^{d_{K}})^{x/2} q^{2r^{2} \deg l} \deg l \right) \right)$$
$$= \pi_{K}(x) \log x + O\left(\pi_{K}(x) \right) + O\left(q^{((2r^{2}+2)\delta + d_{K}/2)x} \right).$$

18

Combining the above estimates, if $\delta < 1/d$, $\delta + d_K \theta(r) < d_K$, and $(2r^2 + 2)\delta < d_K/2$, we obtain

(7)
$$\sum_{\substack{\deg \mathfrak{P}=x\\a_{\phi}(\mathfrak{P})\neq 0}}^{*} \nu(a_{\phi}(\mathfrak{P})) = \pi_{K}(x) \log x + O(\pi_{K}(x)).$$

Similarly, by Theorem 12, we have

$$\sum_{\substack{\deg \mathfrak{P}=x\\a_{\phi}(\mathfrak{P})\neq 0}}^{*} \nu^{2}(a_{\phi}(\mathfrak{P})) = \sum_{\substack{\deg l_{1},\deg l_{2}\leq\delta x\\l_{1}\neq l_{2}}}^{**} \sum_{\substack{\deg \mathfrak{P}=x\\l_{1}l_{2}\mid a_{\phi}(\mathfrak{P}),a_{\phi}(\mathfrak{P})\neq 0}}^{*} 1 + O\left(\pi_{K}(x)\log x\right)$$
$$= \sum_{\substack{\deg l_{1},\deg l_{2}\leq\delta x\\l_{1}\neq l_{2}}}^{**} \sum_{\substack{\deg \mathfrak{P}=x\\l_{1}\neq l_{2}}}^{*} 1 + O\left(q^{(2\delta+d_{K}\theta(r))x}\right) + O\left(\pi_{K}(x)\log x\right).$$

Combining the Chinese remainder theorem with Theorem 10, Propositions 8, 9(ii), 11, and Lemma 23, if $\delta < 1/(2d)$, we have

$$\sum_{\substack{\deg l_1, \deg l_2 \le \delta x \\ l_1 \ne l_2}}^{**} \sum_{\substack{\deg \mathfrak{P}=x \\ l_1 l_2 \mid a_{\phi}(\mathfrak{P})}}^{*} 1 = \pi_K(x)(\log x)^2 + O\left(\pi_K(x)\log x\right) + O\left(q^{(2(2r^2+2)\delta + d_K/2)x}\right).$$

Hence, if $\delta < 1/(2d)$, $2\delta + d_K \theta(r) < d_K$, and $2(2r^2 + 2)\delta < d_K/2$,

(8)
$$\sum_{\substack{\deg \mathfrak{P}=x\\a_{\phi}(\mathfrak{P})\neq 0}}^{*} \nu^{2}(a_{\phi}(\mathfrak{P})) = \pi_{K}(x)(\log x)^{2} + O(\pi_{K}(x)\log x).$$

Combine (3) (with $\chi_{\phi}(\mathfrak{P})$ replaced by $a_{\phi}(\mathfrak{P})$), (4), (7), and (8). Since $\theta(r) = 1 - \frac{1}{2(r^2+2r)}$, by choosing δ such that

$$0 < \delta < \min\left\{\frac{1}{2d}, \frac{d_K}{4(r^2 + 2r)}, \frac{d_K}{4(2r^2 + 2)}\right\},$$

it follows that

$$\sum_{\deg \mathfrak{P}=x}^{*} \left(\nu(a_{\phi}(\mathfrak{P})) - \log \deg x\right)^{2} \ll \pi_{K}(x) \log x$$

This completes the proof of Theorem 5.

Proof: (of Theorem 6) Let ν_y , S_y , E, and E_x be defined as in the proof of Theorem 3. Suppose that we have

(9)
$$\sum_{\deg \mathfrak{P}=x}^{*} \left| \nu(a_{\phi}(\mathfrak{P})) - \nu_{y}(a_{\phi}(\mathfrak{P})) \right| \ll \pi_{K}(x) \log \log x,$$

and as $x \to \infty$,

(10)
$$\left| \mathbf{E}\left\{ \left(S_y - \mathbf{E}\left\{ S_y \right\} \right)^s \right\} - \mathbf{E}_x \left\{ \left(\nu_y - \mathbf{E}\left\{ S_y \right\} \right)^s \right\} \right| \longrightarrow 0.$$

Then we can establish the normal distribution for $\nu(a_{\phi}(\mathfrak{P}))$ as the remaining proof is the same as that of Theorem 3 (i.e., Lemmas 19 to 22).

To obtain (9), let $\delta \in \mathbb{R}$ with $0 < \delta < 1$. For a place $\mathfrak{P} \in \mathcal{P}_{\phi}$, by Theorem 12, we have

$$\begin{split} \sum_{\deg \mathfrak{P}=x}^{*} \left| \nu(a_{\phi}(\mathfrak{P})) - \nu_{y}(a_{\phi}(\mathfrak{P})) \right| &= \sum_{y < \deg l \le \delta x}^{**} \sum_{\substack{\deg \mathfrak{P}=x\\l \mid a_{\phi}(\mathfrak{P}), a_{\phi}(\mathfrak{P}) \neq 0}}^{*} 1 + O\left(\pi_{K}(x)\right) \\ &= \sum_{y < \deg l \le \delta x} \sum_{\substack{\deg \mathfrak{P}=x\\l \mid a_{\phi}(\mathfrak{P})}}^{**} 1 + O\left(q^{(\delta + d_{K}\theta(r))x}\right) + O\left(\pi_{K}(x)\right). \end{split}$$

Then by Theorem 10, Propositions 8, 9(ii), 11, and Lemma 23, if $\delta < 1/d$ and $(2r^2+2)\delta < d_K/2$, we have

$$\sum_{\substack{y < \deg l \le \delta x \\ l \mid a_{\phi}(\mathfrak{P})}}^{**} \sum_{\substack{q < \deg l \le \delta x \\ l \mid a_{\phi}(\mathfrak{P})}}^{*} 1 = \sum_{\substack{y < \deg l \le \delta x \\ q \deg l}}^{**} \left(\frac{\pi_K(x)}{q^{\deg l}} + O\left((q^{d_K})^{x/2} q^{2r^2 \deg l} \deg l \right) \right)$$
$$\ll \pi_K(x) \log \log x.$$

Combine the above two estimates. By choosing δ such that

$$0 < \delta < \min\left\{\frac{1}{d}, \ \frac{d_K}{2(r^2 + 2r)}, \ \frac{d_K}{2(2r^2 + 2r)}\right\},$$

the inequality (9) follows.

To obtain (10), let

$$S_y = \sum_{\deg l \le y}^{**} V_l, \quad \text{and} \quad \nu_y(a_\phi(\mathfrak{P})) = \sum_{\deg l \le y}^{**} \delta_l(a_\phi(\mathfrak{P}))$$

be defined as in the proof of Theorem 3. For an integer t with $0 \le t \le s$, we have

$$\mathbf{E}\{S_y^t\} = \sum_{u=1}^t \sum_{u=1}^t t' \frac{t!}{t_1! \cdots t_u!} \sum_{u=1}^t \mathbf{E}\{V_{l_1}^{t_1} \cdots V_{l_u}^{t_u}\}$$

and

$$\mathbf{E}\{V_{l_1}^{t_1}\cdots V_{l_u}^{t_u}\} = \prod_{i=1}^u \frac{1}{q^{\deg l_u}},$$

where \sum', \sum'' are defined as in the proof of Lemma 21. Similarly, if we abbreviate $\nu_y(a_\phi(\mathfrak{P}))$ and $\delta_l(a_\phi(\mathfrak{P}))$ by ν_y and δ_l , respectively, we have

$$E_x\{\nu_y^t\} = \sum_{u=1}^t \sum_{u=1}^t t! \sum_{u=1}^t t' \frac{t!}{t_1! \cdots t_u!} \sum_{u=1}^t E_x\{\delta_{l_1}^{t_1} \cdots \delta_{l_u}^{t_u}\}.$$

Combining the Chinese remainder theorem with Theorems 10, 12, Propositions 8, 9(ii), 11, and Lemma 18, we get

$$\begin{split} & \operatorname{E}_{x}\left\{\delta_{l_{1}}^{t_{1}}\cdots\delta_{l_{u}}^{t_{u}}\right\} \\ &= \frac{1}{\pi_{K}(x)}\sum_{\substack{\deg\mathfrak{P}=x\\l_{1}l_{2}\cdots l_{u}\mid a_{\phi}(\mathfrak{P}), a_{\phi}(\mathfrak{P})\neq 0}^{*}1 \\ &= \prod_{i=1}^{u}\frac{1}{q^{\deg l_{u}}} + O\left(xq^{d_{K}(\theta(r)-1)x}\right) + O\left(x(q^{d_{K}})^{-x/2}q^{2r^{2}\deg l_{1}+\cdots+2r^{2}\deg l_{u}} \deg l_{1}\cdots l_{u}\right). \end{split}$$

It follows that

$$\left| \mathbf{E} \{ V_{l_1}^{t_1} \cdots V_{l_u}^{t_u} \} - \mathbf{E}_x \{ \delta_{l_1}^{t_1} \cdots \delta_{l_u}^{t_u} \} \right| \\ \ll x q^{d_K(\theta(r)-1)x} + x (q^{d_K})^{-x/2} q^{(2r^2+1) \deg l_1 + \dots + (2r^2+1) \deg l_u}.$$

Thus

$$\begin{aligned} \left| \mathbf{E} \{ S_y^t \} - \mathbf{E}_x \{ \nu_y^t \} \right| \\ \ll \sum_{u=1}^t \sum_{l=1}^t \sum_{l=1}^t \frac{t!}{t_1! t_2! \cdots t_u!} \sum_{l=1}^t \left(x q^{d_K(\theta(r)-1)x} + x (q^{d_K})^{-x/2} q^{(2r^2+1) \deg l_1 + \cdots + (2r^2+1) \deg l_u} \right) \\ \ll x q^{d_K(\theta(r)-1)x} \left(\sum_{\deg l \le y} 1 \right)^t + x (q^{d_K})^{-x/2} \left(\sum_{\deg l \le y} q^{(2r^2+1) \deg l} \right)^t \\ \ll x q^{d_K(\theta(r)-1)x + ty} + x q^{-d_K x/2 + (2r^2+2) ty}. \end{aligned}$$

Write

$$\mathbf{E}\left\{\left(S_{y} - \mathbf{E}\left\{S_{y}\right\}\right)^{s}\right\} = \sum_{t=0}^{s} {\binom{s}{t}} \mathbf{E}\left\{S_{y}^{t}\right\} \mathbf{E}\left\{S_{y}\right\}^{s-t}$$

and

$$\mathbf{E}_x\left\{\left(\nu_y - \mathbf{E}\left\{S_y\right\}\right)^s\right\} = \sum_{t=0}^s \binom{s}{t} \mathbf{E}_x\left\{\nu_y^t\right\} \mathbf{E}\left\{S_y\right\}^{s-t}.$$

Since $\mathbb{E}\left\{S_y\right\} = \log x + O(\log \log x)$ and $y = [x/\log x] \gg \log x$, we have

$$\begin{aligned} \left| \mathbf{E} \{ \left(S_y - \mathbf{E} \{ S_y \} \right)^s \} - \mathbf{E}_x \{ \left(\nu_y - \mathbf{E} \{ S_y \} \right)^s \} \right| \\ \ll \sum_{t=0}^s \binom{s}{t} \left(x q^{d_K(\theta(r)-1)x+ty} + x q^{-d_K x/2 + (2r^2+2)ty} \right) (\log x)^{s-t} \\ \ll x q^{d_K(\theta(r)-1)x} \left(q^y + \log x \right)^s + x (q^{d_K})^{-x/2} \left(q^{(2r^2+2)y} + \log x \right)^s \\ \ll x q^{d_K(\theta(r)-1)x+sy} + x q^{-d_K x/2 + (2r^2+2)sy}. \end{aligned}$$

Since $y < \epsilon x$ for any $\epsilon > 0$, as $x \to \infty$,

$$\left| \mathbf{E} \{ \left(S_y - \mathbf{E} \{ S_y \} \right)^s \} - \mathbf{E}_x \{ \left(\nu_y - \mathbf{E} \{ S_y \} \right)^s \} \right| \longrightarrow 0.$$

Hence, (10) is satisfied. This completes the proof of Theorem 6.

For a fixed polynomial $a \in A$ and a prime $l \in A$, define

$$D_{l,r,a} = \left\{ g \in \operatorname{GL}_r(A/lA) \, \big| \, \operatorname{tr} g \equiv a \, (\operatorname{mod} l) \right\}.$$

Note that the statement of Lemma 23 is also valid with $|D_{l,r}|$ replaced by $|D_{l,r,a}|$. We recall that the result of David in Proposition 12 works for any $a_{\phi}(\mathfrak{P}) = a$. Thus by adapting the approach in this section (with $a_{\phi}(\mathfrak{P})$ replaced by $a_{\phi}(\mathfrak{P}) - a$), we can state Theorems 5 and 6 in a more general way. More precisely, let ϕ be a Drinfeld A-module over K of rank r with $\operatorname{End}_{\bar{K}}(\phi) = A$, and let $a \in A$ be a fixed polynomial. Assuming the open image conjecture for ϕ when $r \geq 3$, we have

$$\sum_{\substack{\mathfrak{P} \in \mathfrak{P}_{\phi} \\ \mathfrak{P} \in \mathcal{P}_{\phi} \\ u_{\phi}(\mathfrak{P}) \neq a}} \left(\nu(a_{\phi}(\mathfrak{P}) - a) - \log \deg \mathfrak{P} \right)^{2} \ll \pi_{K}(x) \log x.$$

Also, for $\gamma \in \mathbb{R}$, we have

$$\lim_{x \to \infty} \frac{1}{\pi_K(x)} \# \left\{ \mathfrak{P} \in \mathcal{P}_\phi \mid \deg \mathfrak{P} = x, \ a_\phi(\mathfrak{P}) \neq a, \text{ and } \frac{\nu(a_\phi(\mathfrak{P}) - a) - \log \deg \mathfrak{P}}{\sqrt{\log \deg \mathfrak{P}}} \leq \gamma \right\} = G(\gamma)$$

Acknowledgement The authors would like to thank Prof. Chantal David for mentioning to us that by combining the work of Gardeyn and Pink, the open image conjecture for Drinfeld modules has been established in the case of rank 2. We also want to thank Prof. Jiu-Kang Yu for many useful discussion about this work. Finally, we are grateful to the referee for valuable suggestions about this paper.

Remark Pink and Rütsche have recently announced a proof of the open image conjecture [27]. Hence, Theorems 1,3, 5,6 and Corollaries 2, 4 now do not rely on any unproved conjectures.

References

- P. Billingsley, On the central limit theorem for the prime divisor functions, Amer. Math. Monthly, 76 (1969), 132-139.
- [2] C. David, Frobenius distributions of Drinfeld modules of any rank, Journal of Number Theory 90 (2001), 329–340.
- [3] V.G. Drinfeld, *Elliptic modules*, Math. Sbornik 94 (1974), 594–627, English transl.: Math. U.S.S.R. Sbornik 23 (1976), 561–592.
- [4] P. Erdős, On the normal order of prime factors of (p-1) and some related problems concerning Euler's ϕ -functions, Quart. J. Math.(Oxford), 6 (1935), 205-213.
- [5] P. Erdős & M. Kac, The Gaussian law of errors in the theory of additive number theoretic functions, Amer. J. Math., 62 (1940), 738-742.
- [6] W. Feller, An introduction to probability theory and its applications, Vol. II, Wiley (1966).
- [7] M. Fried & M. Jarden, Fields Arithmetics (Second Edition), A Series of Modern Surveys in Mathematics, Vol. 11, Springer (2005).
- [8] 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.
- [9] F. Gardeyn, t-Motives and Galois representations, Ph.D. Thesis, Universiteit Gent, 2002.
- [10] F. Gardeyn, Openness of the Galois image for τ-modules of dimension 1, J. Number Theory 102 (2003), 306–338.
- [11] E.-U. Gekeler, On Finite Drinfeld Modules, J. of Algebra 141 (1991), 187-203.

22

GAUSSIAN LAWS ON DRINFELD MODULES

- [12] D. Goss, Basic structures of function field arithmetic, Ergebnisse 35, Springer, Berlin (1996).
- [13] H. Halberstam, On the distribution of additive number theoretic functions, I., II., & III., J. London Math. Soc., 30 (1955), 43-53; 31 (1956), 1-14, 15-27.
- [14] G. H. Hardy & S. Ramanujan, The normal number of prime factors of a number n, Quar. J. Pure. Appl. Math., 48 (1917), 76-97.
- [15] M. Ishibashi, Effective version of the Tschebotareff density theorem in function fields over finite fields, Bull. London Math. Soc. 24 (1992), 52-56.
- [16] W. Kuo & Y.-R. Liu, A Carlitz module analogue of a conjecture of Erdős and Pomerance, to appear in Trans. Amer. Math. Soc.
- [17] S. Lang & A. Weil, Number of points of varieties in finite fields, Amer. J. Math. 76 (1954), 819-829.
- [18] Y.-R. Liu, The Erdős theorem and the Halberstam theorem in function fields, Acta. Arith. 114 (2004), 323-330.
- [19] Y.-R. Liu, A generalization of the Erdős-Kac Theorem and its applications, Canad. Math. Bull. 47 (2004), 589-606.
- [20] Y.-R. Liu, Prime divisors of the number of rational points on elliptic curves with complex multiplication, Bull. London Math. Soc. 37 (2005), 658-664.
- [21] Y.-R. Liu, Prime analogues of the Erdős-Kac Theorem for elliptic curves, J. Number Theory 119 (2006), 155-170.
- [22] S. A. Miri & V. K. Murty, An application of sieve methods to elliptic curves, Progress in Cryptology —INDOCRYPT, Lecture Notes in Comput. Sci. 2247, Springer, Berlin (2001), 91-98.
- [23] M.R. Murty & V.K. Murty, Prime divisors of Fourier coefficients of modular forms, Duke. Math. J., 51 (1984), 57-76.
- [24] M. R. Murty & V. K. Murty, An analogue of the Erdős-Kac theorem for Fourier coefficients of modular forms, Indian J. Pure App. Math., 15 (1984), 1090-1101.
- [25] V. K. Murty & J. Scherk, Effective versions of the Chebotarev density theorem for function fields, C. R. Acad. Sci. Paris, t. 319, Série I (1994), 523-528.
- [26] R. Pink, The Mumford-Tate conjecture for Drinfeld modules, Publ. RIMS, Kyoto University 33 (1997), 393-425.
- [27] R. Pink and E. Rütsche, Adelic openness for Drinfeld modules in generic characteristic, J. Number Theory 129 (2009), 882-907.
- [28] P. Turán, On a theorem of Hardy and Ramanujan, J. London Math. Soc. 9 (1934), 274-276.
- [29] J.-K. Yu, Isogenies of Drinfeld modules, J. Number Theory 54 (1995), 161–171.

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

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

Y.-R. LIU, DEPARTMENT OF PURE MATHEMATICS, FACULTY OF MATHEMATICS, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, CANADA N2L 3G1

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