FROBENIUS DISTRIBUTIONS OF DRINFELD MODULES OF ANY RANK

HRISHABH MISHRA

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. Let A be the polynomial ring $\mathbb{F}_q[T]$ and F be its fraction field $\mathbb{F}_q(T)$. We fix a separable closure F^{sep} of F once and for all. Given any field K, let G_K denote the absolute Galois group $Gal(K^{sep}/K)$ of K. We now give a quick overview of Drinfeld modules and associated Galois representations.

1.1. **Drinfeld modules.** Let K be an extension of $\mathbb{F}_q$ and $\gamma : A \to K$ an $\mathbb{F}_q$-algebra homomorphism. Hence, K is an A-field. Let $\mathrm{char}_A(K) := ker(\gamma) \subset A$, we call it the A-characteristic of K. We denote by $K\{\tau\}$ the ring of *skew polynomials*, the non-commutative ring with underlying abelian group $K[\tau]$ and twisted multiplication given by $\tau a = a^q \tau$ for all $a \in K$.

Definition 1.1. *A Drinfeld A-module ϕ of rank $r \geq 1$ over K is an $\mathbb{F}_q$-algebra homomorphism*

$$\phi : A \to K\{\tau\},$$
$$a \mapsto \phi_a = \gamma(a) + g_1(a)\tau + \cdots + g_n(a)\tau^n,$$

such that for $a \neq 0$ we have $n = \deg_T(a)r$ and $g_n(a) \neq 0$.

We note that a Drinfeld A-module ϕ is completely determined by ϕ_T and we call $g_r(T)$ the discriminant of the Drinfeld module. We obtain an A-module structure on K^{sep} given by $a \cdot m = \phi_a(m)$ for $a \in A$ and $m \in K^{sep}$. Let $\mathfrak{a} \subset A$ be a non-zero ideal, we define the $\mathfrak{a}$-torsion of ϕ,

$$\phi[\mathfrak{a}] := \{x \in K^{sep} : \phi_a(x) = 0 \text{ for all } a \in \mathfrak{a}\}.$$

It is well-known that if $\mathfrak{a}$ and $\mathrm{char}_A(K)$ are co-prime then $\phi[\mathfrak{a}]$ is a free $A/\mathfrak{a}$ module of rank r. Further the Galois group G_K acts on the set $\phi[\mathfrak{a}]$ and this action respects the module structure. Therefore, we obtain the representations

$$\rho_{\phi,\mathfrak{a}} : G_K \to \mathrm{Aut}(\phi[\mathfrak{a}]) \simeq \mathrm{GL}_r(A/\mathfrak{a}),$$

for each $\mathfrak{a} \subset A$ co-prime to $\mathrm{char}_A(K)$. In particular, for any non-zero prime $\mathfrak{l} \neq \mathrm{char}_A(K)$ we have the Galois representations,

$$\rho_{\phi,\mathfrak{l}^n} : G_K \to \mathrm{Aut}(\phi[\mathfrak{l}^n]) \simeq \mathrm{GL}_r(A/\mathfrak{l}^n),$$

for each $n \geq 1$. Note that we have the multiplication map $\phi[\mathfrak{l}^{n+1}] \xrightarrow{\phi_{\mathfrak{l}}} \phi[\mathfrak{l}^n]$ for $n \geq 1$. Let $T_{\mathfrak{l}}(\phi) := \varprojlim_i \phi[\mathfrak{l}^i]$ be the $\mathfrak{l}$-*adic Tate module*. We take the inverse limit to construct the following Galois representation,

$$\overline{\rho}_{\phi,\mathfrak{l}} : G_K \to \mathrm{Aut}_{A_{\mathfrak{l}}}(T_{\mathfrak{l}}(\phi)) \simeq \mathrm{GL}_r(A_{\mathfrak{l}}).$$

Here $A_{\mathfrak{l}}$ denotes the $\mathfrak{l}$-adic completion of A. If K is a finite field then the Galois group G_K is generated by the Frobenius element $\mathrm{Frob}_K : K^{sep} \to K^{sep}$ given by $x \mapsto x^{\#K}$. Let P_ϕ be the characteristic polynomial of $\overline{\rho}_{\phi,\mathfrak{l}}(\mathrm{Frob}_K) \in \mathrm{GL}_r(A_{\mathfrak{l}})$, which means that $P_\phi = det(x - \overline{\rho}_{\phi,\mathfrak{l}}(\mathrm{Frob}_K))$. The polynomial P_ϕ has coefficients in A and is independent of the prime $\mathfrak{l}$. The theory of Drinfeld A-modules is very similar to elliptic curves over $\mathbb{Q}$ and analogs of various problems for the Elliptic curves have been studied for Drinfeld modules. One such problem is the Lang-Trotter conjecture. We describe the analogous problem in more detail.

1.2. **Lang-Trotter Conjecture.** Let E be a non-CM elliptic curve over $\mathbb{Q}$ and $p \in \mathbb{N}$ a non-zero prime of good reduction and E_p the elliptic curve over $\mathbb{F}_p$ obtained by reducing E modulo p. Let ℓ be a prime different from p then we have the associated Galois representation,

$$\overline{\rho}_{E_p,\ell} : G_{\mathbb{F}_p} \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Let $P_{E,p}$ denote the characteristic polynomial of the image of Frobenius automorphism under this representation, the polynomial $P_{E,p}$ has coefficients in $\mathbb{Z}$ and is independent of prime ℓ. We denote by $a_p(E)$ the trace of the polynomial $P_{E,p}$. Given any $t \in \mathbb{N}$, the Lang-Trotter conjecture predicts the asymptotics of the following quantity,

$$\pi_t(x) := \#\{p \leq x : p \text{ prime of good reduction and } a_p(E) = t\}$$

Conjecture 1.2 (Lang-Trotter, [LT76])**.** *Let E be a non-CM elliptic curve over $\mathbb{Q}$ and $t \in \mathbb{N}$ then we have that*

$$\pi_t(x) \sim C_{E,t} \frac{\sqrt{x}}{\log x},$$

the constant $C_{E,t}$ depends only on E and t.

We note that $i : A \hookrightarrow F$, hence F is an A-field with characteristic zero. Let ϕ be a Drinfeld A-module of rank r over F without complex multiplication. For any prime $\mathfrak{p} \subset A$ of good reduction, we consider the Drinfeld A-module $\phi_{\mathfrak{p}}$ over $\mathbb{F}_{\mathfrak{p}} := A/\mathfrak{p}$ and for any prime $\mathfrak{l} \neq \mathfrak{p}$ we have the associated representation,

$$\overline{\rho}_{\phi_{\mathfrak{p}},\mathfrak{l}} : G_{\mathbb{F}_{\mathfrak{p}}} \to \mathrm{GL}_r(A_{\mathfrak{l}}).$$

Let $P_{\phi,\mathfrak{p}}$ be the characteristic polynomial of the image of Frobenius automorphism under the above Galois representation and let $a_{\mathfrak{p}}(\phi) \in A$ denote the trace of the polynomial $P_{\phi,\mathfrak{p}}$. For a fixed $t \in A$ and $k > 0$ we consider the following set

$$\mathcal{P}_{t,k} := \{\deg(\mathfrak{p}) = k : \mathfrak{p} \text{ prime of good reduction and } a_{\mathfrak{p}}(\phi) = t\},$$

and let $\pi_t(k) := \#\mathcal{P}_{t,k}$. The following upper bound for $\pi_t(k)$ is due to C. David ([Dav01]).

Theorem 1.3 (Theorem 1.1, [Dav01])**.** *Let ϕ be a Drinfeld module over F of any rank $r \geq 2$ without complex multiplication. Then, for any $t \in A$ and any integer k,*

$$\pi_t(k) \ll r \frac{q^{k\theta(r)}}{k}$$

where $\theta(r) := 1 - \frac{1}{2(r^2+2r)}$, and the constant depends only on ϕ.

We remark that similar results on the distribution of $\pi_t(k)$ are obtained by A.C. Cojocaru, C. David and, D. Zywina in [Dav96], [CD08], [Zyw16]. We end this section by stating the following analogue of Lang-Trotter conjecture for Drinfeld modules.

Conjecture 1.4. *There exists a positive integer M_ϕ such that*

$$\pi_t(k) \sim C_{\phi,t}(k)\frac{q^{k/2}}{k}$$

as $k \to \infty$, where $C_{\phi,t}(k)$ are constants whose value depend only on k modulo M_ϕ.

1.3. **Notation and Organization.** Given a finite Galois extension E/F we denote by $g(E)$ the genus and we let L_E denote the subfield of L consisting of elements in L algebraic over $\mathbb{F}_q$, we also write N_E for the degree $[L_E F : F]$. The write-up consists of three sections including the Introduction, we discuss some preliminary results in Section 2 and proceed to complete the proof of Theorem 1.3 in the next section.

2. Preliminaries

In this section, we state the results we will use to prove Theorem 1.3 in Section 3 and we provide proofs for some of these results. We obtain theorem 1.3 by relating the distribution of trace of Frobenius to the distribution of Artin symbols and use the Chebotarev density theorem to obtain the desired bound. Let ϕ be a Drinfeld A-module over F of rank $r \geq 2$ without complex multiplication. We fix a prime $\mathfrak{l}$ of A. Let $E_n := F(\phi[\mathfrak{l}^n])$ and $G_n := Gal(E_n/F)$. We write $|\mathfrak{l}|$ for $q^{\deg(\mathfrak{l})}$.

2.1. **Open Image Theorem.** The following open image theorem was proved by R. Pink and E. Rütsche in [PR09].

Theorem 2.1. *Let ψ be a Drinfeld module of rank r over a finite extension K of F. Assume that $End_{\overline{K}}(\psi) = A$. Then there exists a constant $N(\psi, K)$ such that*

$$[GL_r(A/\mathfrak{a}) : \rho_{\psi,\mathfrak{a}}(G_K)] \leq N(\psi, K),$$

for all $\mathfrak{a} \subset A$.

Now, given ϕ as above we note that $|G_n| \leq |M_r(A/\mathfrak{l}^n)|$. Hence, $|G_n| \leq |\mathfrak{l}|^{r^2 n}$. Next, it immediately follows from the above theorem that $|\mathfrak{l}|^{r^2 n} \ll |G_n|$ for some constant depending only on ϕ and $\mathfrak{l}$.

2.2. **Chebotarev Density Theorem.** Suppose E/F is finite Galois with Galois group G. If $\mathfrak{p}$ is unramified in E/F, we define $\sigma_\mathfrak{p}$ to be the Artin symbol at $\mathfrak{p}$. Let C be a conjugacy class in G and k a positive integer, we define,

$$S_k(E/F, C) := \{\sigma_\mathfrak{p} = C : \deg(\mathfrak{p}) = k, \mathfrak{p} \text{ is unramified in } E/F\}.$$

We have the following bound on the size of the set $S_k(E/F, C)$.

Theorem 2.2. *(Chebotarev Density Theorem) We have that,*

$$|S_k(E/F, C)| \ll \frac{N_E|C|}{|G|}\frac{q^k}{k} + |C|q^{k/2} + \frac{N_E|C|}{|G|}\frac{q^{k/2}}{k}g(E),$$

with an absolute constant.

We will apply the above theorem to a family of extensions, E_n, $n \geq 1$. We prove that $\{N_{E_n}\}_{n\geq 1}$ is bounded and as a consequence, we will obtain a bound on $|S_k(E_n/F, C)|$ which will only depend on the genus of E_n/F for $n \geq 1$. Let us consider the field F_{tors} generated by all torsion points of ϕ. We prove the following.

Proposition 2.3. *For ϕ as above, $N_{F_{tors}}$ is finite.*

Proof. Using analytic theory, let Λ_ϕ be the lattice associated with ϕ. Now, considering the Newton polygon of the associated exponential e_ϕ and using the Weierstrass preparation theorem we conclude that all elements of lattice Λ_ϕ are algebraic over $F_\infty = \mathbb{F}_q((1/T))$. Let F_{Λ_ϕ} be the field generate by lattice elements, then $F_{\Lambda_\phi}/F_\infty$ is finite. We also note that F_{Λ_ϕ} contains all the elements of the form $e_\phi(a\lambda)$ for $a \in F$, $\lambda \in \Lambda_\phi$. Hence, again using analytic theory we conclude that,

$$F_{tors} \subset F_{\Lambda_\phi}.$$

Now as F_∞/F is geometric therefore, $L_{F_{\Lambda_\phi}}$ is a finite extension because $F_{\Lambda_\phi}/F_\infty$ is finite. □

As an immediate corollary of the last two results we deduce the following,

Corollary 2.4. *For any $n \geq 1$ and U a union of conjugacy classes in G_n the following holds,*

$$|S_k(E_n/F, U)| \ll \frac{|U|}{|G_n|}\frac{q^k}{k} + |U|q^{k/2} + \frac{|U|}{|G_n|}\frac{q^{k/2}}{k}g(E_n).$$

The associated constant depends only on ϕ.

We will also need the following bound on $g(E_n)$ in the next section. We state the upper bound without proof. The proof follows at once from the Riemann-Hurwitz formula once we obtain a bound on the degree of the different $\mathfrak{D}(E_n/F)$ for $n \geq 1$.

Lemma 2.5. *We have that,*

$$g(E_n) \ll r[E_n : F]|\mathfrak{l}|^{2nr}$$

with the constant only depending on ϕ.

3. Proof of the Main Theorem

We begin by noting that for any $n \geq 1$,

$$\begin{aligned}\pi_t(k) &:= \#\{\deg(\mathfrak{p}) = k : a_\mathfrak{p}(\phi) = t\} \\ &\leq \{\deg(\mathfrak{p}) = k : a_\mathfrak{p}(\phi) = t \mod \mathfrak{l}^n\}.\end{aligned}$$

Now, suppose $\mathfrak{p}$ is a prime of a good reduction, then using the analogue of the Néron–Ogg –Shafarevich criterion we conclude that for any prime $\mathfrak{l} \neq \mathfrak{p}$, the Tate module $T_\mathfrak{l}(\phi)$ is unramified. Hence, in other words, the Galois representation,

$$\rho_{\phi,\mathfrak{l}} : G_F \to GL_r(A_\mathfrak{l}).$$

is unramified at the prime $\mathfrak{p}$. Now, considering the decomposition group $G_\mathfrak{p}$, we have following maps,

$$\begin{array}{ccccccc} I_\mathfrak{p} & \hookrightarrow & G_\mathfrak{p} & \hookrightarrow & G_F & \xrightarrow{\rho_{\phi,\mathfrak{l}}} & GL_r(A_\mathfrak{l}) \\ & & \downarrow & & & & \\ & & G_{\mathbb{F}_\mathfrak{p}} & & & & \end{array}$$

Next, consider an element in the decomposition group that induces the Frobenius element of $G_{\mathbb{F}_\mathfrak{p}}$ and suppose that $a_\mathfrak{p}(\phi) = t \mod \mathfrak{l}^n$ then the trace of that corresponding element is also $t \mod \mathfrak{l}^n$. Hence, $\sigma_\mathfrak{p}$ has trace t in $M_r(A/\mathfrak{l}^n)$. Now, the number of trace t elements in $M_r(A/\mathfrak{l}^n)$ is a union of conjugacy classes. Let this union be C_t, note $|C_t| \leq |\mathfrak{l}|^{(r^2-1)n}$, then we conclude that,

$$\pi_t(k) \leq S_k(E_n/F, C_t).$$

Using corollary 2.4 and the bound on the genus, we obtain that,

$$\pi_t(k) \ll \frac{1}{|\mathfrak{l}|^n}\frac{q^k}{k} + |\mathfrak{l}|^{(r^2-1)n}q^{k/2} + r|\mathfrak{l}|^{(r^2+2r-1)n}\frac{q^{k/2}}{k}.$$

Choosing n suitably such that,

$$q^{k/2(r^2+2r)} \ll |\mathfrak{l}|^n \ll q^{k/2(r^2+2r)},$$

with constants depending only on $|\mathfrak{l}|$ we obtain Theorem 1.3.

References

[CD08] Alina Carmen Cojocaru and Chantal David. Frobenius fields for drinfeld modules of rank 2. *Compositio Mathematica*, 144(4):827–848, 2008.

[Dav96] Chantal David. Average distribution of supersingular Drinfeld modules. *J. Number Theory*, 56(2):366–380, 1996.

[Dav01] Chantal David. Frobenius distributions of Drinfeld modules of any rank. *J. Number Theory*, 90(2):329–340, 2001.

[LT76] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions*, volume Vol. 504 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[PR09] Richard Pink and Egon Rütsche. Adelic openness for drinfeld modules in generic characteristic. *Journal of Number Theory*, 129(4):882–907, 2009.

[Zyw16] David Zywina. The Sato-Tate law for Drinfeld modules. *Trans. Amer. Math. Soc.*, 368(3):2185–2222, 2016.

(H. Mishra) Chennai Mathematical Institute, H1, SIPCOT IT Park, Kelambakkam, Siruseri, Tamil Nadu 603103, India

Email address: hrishabh@cmi.ac.in