Frobenius distributions of Drinfeld modules of any rank

Chantal David, Concordia University

January 23, 2001

Abstract

Let $A = \mathbb{F}_q[T]$, and let ϕ be a Drinfeld A-module of rank $r \geq 2$ over $\mathbb{F}_q(T)$. For each prime $\mathfrak{p} \in A$ which is a prime of good reduction for ϕ, let $a_\mathfrak{p}(\phi)$ be the trace of the Frobenius endomorphism at $\mathfrak{p}$. We study in this paper the distribution of the traces $a_\mathfrak{p}(\phi)$, and we show that for any $t \in A$ and any positive integer k, the set of primes $\mathfrak{p} \in A$ of degree k such that $a_\mathfrak{p}(\phi) = t$ has density 0. Our proof is based on a similar result that was obtained by Serre [16] for elliptic curves over $\mathbb{Q}$.

1 Introduction

In all this paper, let $A = \mathbb{F}_q[T]$ and $F = \mathbb{F}_q(T)$. This is a particular case of F being any function field over $\mathbb{F}_q$, and A being the ring of functions regular away from a fixed place of F denoted ∞. As $A = \mathbb{F}_q[T]$, the fixed place corresponds to the valuation $v_\infty(f) = -\deg f$ on F. Then, $|f|_\infty = q^{\deg f}$, and we will denote this absolute value by $|f|$ as there is no possible confusion. Let ϕ be a Drinfeld A-module of rank r over F, i.e. an A-module structure on the additive group of the field F. Drinfeld modules, and particularly Drinfeld modules of rank 2, offer striking analogies with elliptic curves over the rationals.

For any prime $\mathfrak{p}$ of good reduction of ϕ, let $P_\mathfrak{p}(x)$ be the characteristic polynomial of the Frobenius endormorphism at $\mathfrak{p}$ (see section 2). As in the case of elliptic curves, this polynomial characterises the isogeny class of $\phi_\mathfrak{p}$, the reduction of the Drinfeld module ϕ over the finite field $A/\mathfrak{p}A$. We study in this paper the distribution of the traces $a_\mathfrak{p}(\phi) = \mathrm{tr}\,(P_\mathfrak{p}(x))$. This is a generalisation of the distribution of traces for elliptic curves over $\mathbb{Q}$. In this classical case, there is a precise conjecture made by Lang and Trotter, based on a probabilistic model for the distribution of the traces [12]. Those distribution questions were also studied for elliptic curves over number fields [11], modular curves [1] and forms of higher weight [9]. In all those cases, proving an exact asymptotic result seems to be beyond the actual knowledge of the subject. In the case of Drinfeld modules, the only existing results are lower bounds for the number of supersingular primes (the case $a_\mathfrak{p}(\phi) = 0$) of certain rank 2 Drinfeld modules due to Brown [2] and David [3]. This followed the work of Elkies [5], who showed that every elliptic curve $E/\mathbb{Q}$ has infinitely many supersingular primes. But the analogous statement for Drinfeld modules over $\mathbb{F}_q(T)$ is false: there are Drinfeld modules having no supersingular primes, as Poonen showed in [14]. If $t \in A$ is non-zero, it is not even known that there are Drinfeld modules ϕ over $\mathbb{F}_q(T)$ with infinitely many primes $\mathfrak{p}$ such that $a_{\mathfrak{p}}(\phi) = t$.

Fix $t \in A$, k a positive integer. We show in this paper that the number of primes of A of degree k such that $a_{\mathfrak{p}}(\phi) = t$ has density 0. More precisely, let

$$\pi_t(k) = \#\left\{\text{primes } \mathfrak{p} \in A \text{ of degree } k \text{ such that } a_{\mathfrak{p}}(\phi) = t\right\}.$$

Theorem 1.1 *Let ϕ be a Drinfeld module over F of rank $r \geq 2$, and 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 $\theta(r) = 1 - \dfrac{1}{2(r^2+2r)}$, and the the constant depends only on ϕ.

We prove this result following the general lines of the work of Serre [16], who obtained such upper bounds for elliptic curves. The main idea is to apply the Chebotarev Density Theorem to certain finite Galois extensions obtained by adding torsion points of ϕ to F. This argument requires some knowledge on the size of those extensions, i.e., some equivalent of Serre's Theorem [15] for the case of Drinfeld modules. As explained in the next section, this is not known yet, but there are now partial results in this direction that were obtained by Pink [13] recently. We are then using those results to prove Theorem 1.1 along the lines of the proof of Serre in [16]. In the case of Drinfeld modules, we get unconditional results, as the Riemann Hypothesis holds for function fields.

For Drinfeld modules of rank 2, which are the function field analogue of elliptic curves, we have from Theorem 1.1 that $\theta(r) = 15/16$. One should note that in the case of elliptic curves, Serre obtained (under the Generalised Riemann Hypothesis) an upper bound with $\theta = 7/8$ [16, Corollary 1, p. 174]. We obtain a weaker bound in the case of function fields because the upper bounds on the discriminants are weaker in that case.

In section 2, we collect the facts about Drinfeld modules that will be needed in this paper. Section 3 contains the statement of the Chebotarev Density Theorem for function fields that we will need for our application to Galois representations of Drinfeld modules. Section 4 contains the estimates on the different and genus of our field extensions, and we prove Theorem 1.1 in Section 5.

2 Drinfeld modules

Let K be an A-field, i.e., a field equipped with a ring homomorphism $\iota : A \to K$. Let K^+ be the additive group of K, and let τ be the Frobenius element of the finite field $\mathbb{F}_q$. The (non-commutative) ring $\mathrm{End}(K^+)$ is isomorphic to the ring $K\{\tau\}$ of formal polynomials $f(\tau) = \sum_{i=0}^{n} a_i\tau^i$ with $a_i \in K$ under the twisted multiplication

$$a^q\tau = \tau a \tag{1}$$

for all $a \in K$.

Definition 2.1 *A Drinfeld A-module ϕ over K is a ring homomorphism*

$$\begin{aligned} \phi : A &\to End(K^+) \simeq K\{\tau\} \\ a &\mapsto \phi_a = \sum_{i=0}^{N_a} a_i\tau^i \end{aligned}$$

such that

> *(i) for all $a \in A$, ϕ_a has constant term $\iota(a)$;*
>
> *(ii) there is a positive integer r such that for all $a \in A$, $N_a = r\,deg(a)$.*

The integer r is called the rank of the Drinfeld module ϕ.

In the special case $A = \mathbb{F}_q[T]$, a Drinfeld A-module ϕ is completely determined by

$$\phi_T = T + c_1(\phi)\tau + \ldots + c_{r-1}(\phi)\tau^{r-1} + \Delta(\phi)\tau^r.$$

We call $\Delta(\phi)$ the discriminant of ϕ.

Drinfeld modules offer a striking analogy with elliptic curves. This analogy is best seen throught the complex theory. We review here the results about the complex theory that will be needed in this paper. For a complete account of those results, we refer the reader to [8, Chapter 4] or [10].

Let $F_\infty = \mathbb{F}_q((\frac{1}{T}))$ be the completion of F at the prime at infinity, and let C_∞ be the completion of the algebraic closure of F_∞. Then, C_∞ is complete and algebraically closed, and will play the role of the usual complex field $\mathbb{C}$ in our setting. Let Λ be a lattice of C_∞ of rank r_Λ, i.e., a discrete A-submodule of C_∞ such that $F_\infty\Lambda$ has finite F_∞-dimension r_Λ. Since C_∞ is an infinite dimensional F_∞-vector space, lattices of every positive rank exist.

The exponential function associated to the lattice Λ is

$$e_\Lambda(z) = z \prod_{\lambda\in\Lambda-\{0\}} \left(1 - \frac{z}{\lambda}\right).$$

Then, e_Λ is entire $\mathbb{F}_q$-linear, and the map

$$e_\Lambda : C_\infty/\Lambda \to C_\infty$$

is an isomorphism. Furthermore, for each $a \in A$, there is a polynomial $\phi_a^\Lambda \in C_\infty\{\tau\}$ such that

$$e_\Lambda(az) = \phi_a^\Lambda(e_\Lambda(z))$$

for all $z \in C_\infty$, and the map $a \to \phi_a^\Lambda$ is a Drinfeld module of rank r_Λ over C_∞.

We now state the analytic uniformisation theorem for Drinfeld modules.

Theorem 2.2 *[8, Theorem 4.6.9] Let ϕ be a Drinfeld A-module of rank $r > 0$ defined over F_∞. Then, there is a lattice Λ such that ϕ is the Drinfeld module associated with Λ as described above. Furthermore, the lattice elements are the roots of a power series*

$$e_\phi = \sum_{i=0}^{\infty} c_i \tau^i \in F_\infty\{\{\tau\}\}$$

with $c_0 = 1$.

For each $a \in A$, the a-torsion points of ϕ are the roots of the multiplication-by-a polynomial ϕ_a, which is a separable polynomial of degree $q^{r \deg(a)}$. Let $\phi[a]$ be the A-module of a-torsion points of ϕ. From the analytic uniformisation, $\phi_a(e_\Lambda(z)) = 0$ if and only if $e_\Lambda(az) = 0$ if and only if $z \in \frac{1}{a}\Lambda$. It then follows that $\phi[a] \simeq (A/aA)^r$. Then, by letting $\mathrm{Gal}(F^{sep}/F)$ act on the a-torsion points of ϕ, we get Galois representations

$$\rho_a : \mathrm{Gal}(F^{sep}/F) \to \mathrm{Aut}\,(\phi([a])) \simeq \mathrm{GL}_r(A/aA),$$

as in the case of elliptic curves.

Let $\mathfrak{L} \in A$ be a prime. Let $\phi[\mathfrak{L}^n]$ be the A-module of $\mathfrak{L}^n$-torsion points, and let $\phi[\mathfrak{L}^\infty]$ be the direct limit of the $\phi[\mathfrak{L}^n]$. Let $A_\mathfrak{L}$ and $F_\mathfrak{L}$ be the $\mathfrak{L}$-completions of A and F, respectively. We define the $\mathfrak{L}$-adic Tate module of ϕ by

$$T_\mathfrak{L}(\phi) = \mathrm{Hom}_{A_\mathfrak{L}}\left(F_\mathfrak{L}/A_\mathfrak{L}, \phi[\mathfrak{L}^\infty]\right).$$

It is a free $A_\mathfrak{L}$-module of dimension r, and $\mathrm{Gal}(F^{sep}/F)$ acts continuously on $T_\mathfrak{L}(\phi)$, giving raise to a representation

$$\rho_{\mathfrak{L}^\infty} : \mathrm{Gal}(F^{sep}/F) \to \mathrm{Aut}(T_\mathfrak{L}(\phi) \simeq \mathrm{GL}_r(A_\mathfrak{L}).$$

For any unramified prime $\mathfrak{p}$ of $\rho_{\mathfrak{L}^\infty}$, let $\sigma_\mathfrak{p}$ be the Artin symbol at $\mathfrak{p}$. Let $P_\mathfrak{p}(x)$ and $a_\mathfrak{p}(\phi)$ be the characteristic polynomial and the trace of $\rho_{\mathfrak{L}^\infty}(\sigma_\mathfrak{p})$ respectively. $P_\mathfrak{p}(x)$ is a polynomial of degree r in $A[x]$, i.e., it is independent of $\mathfrak{L}$ [8, Theorem 4.12.12]. $P_\mathfrak{p}(x)$ is the characteristic polynomial of the Frobenius endomorphism of $\phi_\mathfrak{p}$, the reduction of ϕ over the finite field $A/\mathfrak{p}A$. From the theory of Drinfeld modules over finite fields (see [7] or [19]),

$$P_\mathfrak{p}(x) = x^r + a_1 x^{r-1} + \ldots + a_{r-1}x + u\mathfrak{p}$$

for some $u \in \mathbb{F}_q^*$, and for each root π of $P_\mathfrak{p}(x)$, we have $|\pi| = |\mathfrak{p}|^{1/r}$. Then,

$$|a_\mathfrak{p}(\phi)| \leq |\mathfrak{p}|^{1/r}. \tag{2}$$

For $r = 2$, this is similar to the situation of elliptic curves over finite fields, but the cases of higher rank are not analogous to abelian varieties over finite fields as the size of the roots of $P_\mathfrak{p}(x)$ depends on the rank r. From that point of view, the situation of Drinfeld modules of rank $r \geq 3$ has no analogue in the classical case. By the analytic uniformisation, those Drinfeld modules are associated to lattices of rank ≥ 3 in C_∞, and there are no such lattices in $\mathbb{C}$.

Fix a Drinfeld A-module ϕ of rank $r \geq 2$, $t \in A$, and a positive integer k. By (2), the "probability" that $a_\mathfrak{p}(\phi) = t$ is proportional to $1/|\mathfrak{p}|^{1/r}$. This suggests the following upper bound

$$\pi_t(k) \ll \frac{q^{k(1-1/r)}}{k}.$$

This conjectural upper bound is stronger than the result of Theorem 1.1.

By analogy with the case of elliptic curves [15], we would expect that the Galois representation

$$\rho_\phi : \mathrm{Gal}(F^{sep}/F) \to \prod_{\mathfrak{L}} \mathrm{Aut}(T_\mathfrak{L}(\phi)) \simeq \prod_{\mathfrak{L}} \mathrm{GL}_r(A_\mathfrak{L}),$$

describing the action of Galois on the full A-module of torsion points of ϕ, has open image. This result is not known yet for Drinfeld modules. It would imply that for all but a finite number of primes $\mathfrak{L}$, the representations $\rho_\mathfrak{L}$ are surjective, and we could use those representations with $\mathfrak{L}$ appropriately chosen to prove Theorem 1.1 following the proof of Serre [16] for elliptic curves. As this general result is not known yet for Drinfeld modules, we will prove Theorem 1.1 using the result of Pink stated below. Then, we will fix a prime $\mathfrak{L}$ and use $\rho_{\mathfrak{L}^n}$ for n appropriately chosen.

Theorem 2.3 *[13, Theorem 0.2] Suppose that ϕ does not have complex multiplication, and let $\mathfrak{L}$ be a prime of A. Then, the Galois representation*

$$\rho_{\mathfrak{L}^\infty} : Gal(F^{sep}/F) \to Aut(T_\mathfrak{L}(\phi)) \simeq GL_r(A_\mathfrak{L})$$

has open image in $GL_r(A_\mathfrak{L})$.

For any positive integer n, let $\rho_{\mathfrak{L}^n}$ be the reduction of $\rho_{\mathfrak{L}^\infty}$ modulo $\mathfrak{L}^n$. The representation $\rho_{\mathfrak{L}^n}$ gives the action of $\mathrm{Gal}(F^{sep}/F)$ on the module $\phi[\mathfrak{L}^n]$ of $\mathfrak{L}^n$-torsion points of ϕ. Then, $\rho_{\mathfrak{L}^n}$ is a Galois representation

$$\rho_{\mathfrak{L}^n} : \mathrm{Gal}(F^{sep}/F) \to \mathrm{Aut}(\phi[\mathfrak{L}^n]) \simeq \mathrm{GL}_r(A/\mathfrak{L}^n A). \tag{3}$$

In the following, let $E_n = F(\phi[\mathfrak{L}^n])$ be the field obtained by adjoining the $\mathfrak{L}^n$-torsion of ϕ to F, and let $G_n = \mathrm{Gal}(E_n/F)$. Then, quotienting by the kernel in (3), we get an injection of G_n into $\mathrm{GL}_r(A/\mathfrak{L}^n A)$. In the following, we identify G_n with the corresponding subgroup of $\mathrm{GL}_r(A/\mathfrak{L}^n A)$.

3 Chebotarev Density Theorem

Let E be a finite Galois extension of $F = \mathbb{F}_q(T)$, with Galois group $G = \mathrm{Gal}(E/F)$ and genus $g(E)$. Let L be the algebraic closure of $\mathbb{F}_q$ in E, and let $N_E = [LF : F]$. Let τ be the Frobenius map of $\mathbb{F}_q$. For each prime $\mathfrak{p}$ which is unramified in E/F, let $\sigma_{\mathfrak{p}}$ be the Artin symbol at $\mathfrak{p}$. For k a positive integer, and C a conjugacy class in G, let $S_k(E/F, C)$ be the set of unramified primes of F of degree k and such that $\sigma_{\mathfrak{p}} = C$. Let a_C be a positive integer such that

$$\mathrm{res}_L\, \sigma = \mathrm{res}_L\, \tau^{a_C}$$

for all $\sigma \in C$.

Theorem 3.1 *[6, Proposition 5.16] If $k \not\equiv a_C$ mod N_E, then $S_k(E/F, C)$ is empty. If $k \equiv a_C$ mod N_E, then*

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

with an absolute constant.

Fix a prime $\mathfrak{L}$ of A. We want to show that the degree of the non-geometric part of $F(\phi[\mathfrak{L}^n])$ is bounded by a constant independent of n. This follows from the more general result:

Lemma 3.2 *Let F_{tors} be the field obtained by adding all torsion points of ϕ to F, and let L be the algebraic closure of $\mathbb{F}_q$ in F_{tors}. Then, $N_\phi = [LF : F]$ is finite.*

Proof: (from E.-U. Gekeler) Let Λ be the lattice corresponding to ϕ by Theorem 2.2. Then, the lattice elements are algebraic over F_∞ [8, Proposition 2.9], and the field F_Λ generated by the lattice elements is finite over F_∞, being finitely generated by algebraic elements. But F_Λ also contains all the points

$$\{e_\Lambda(b\alpha) : b \in F \text{ and } \alpha \in \Lambda\}.$$

These are precisely the torsion points of ϕ, i.e., $F_{tors} \subseteq F_\Lambda$ [8, Remark 4.3.6.2]. But the algebraic closure of $\mathbb{F}_q$ in F_Λ is a finite extension, because F_Λ is finite over F_∞, and $F_\infty = \mathbb{F}_q((\frac{1}{T}))$ is geometric over F. QED.

Remark: Let ϕ be a Drinfeld module over F. From the last lemma, $N_\phi < \infty$, but one does not know when F_{tors} is geometric (i.e., $N_\phi = 1$). Is it true for "most" Drinfeld modules ϕ? One can find Drinfeld modules ϕ over F where $N_\phi > 1$, but it does not seem to be the general behavior. For example, consider the Drinfeld module given by $\phi_T = T(\tau-1)^2 = T - 2T\tau + T\tau^2$ of [14] (this is a Drinfeld module without any supersingular primes). The T-torsion of ϕ is the 2-dimensional $\mathbb{F}_q$-vector space $\ker((1-\tau)^2)$, which lies in $\overline{\mathbb{F}_q}$.

We now state the version of the Chebotarev Density Theorem that we will use to obtain Theorem 1.1. As above, let $E_n = F(\phi[\mathfrak{L}^n])$ and $G_n = \mathrm{Gal}(E_n/F)$. Let N_n be the degree of the constant extension part of E_n. Then, E_n is a function field over the finite field with q^{N_n} elements. We also put $\ell = |\mathfrak{L}| = q^{\deg \mathfrak{L}}$.

Corollary 3.3 *Let n be any positive integer, and let C be a union of conjugacy classes in G_n. Then,*

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

with a constant depending only on the Drinfeld module ϕ.

Proof: Let $C = C_1 \cup \ldots \cup C_s$, where each C_i is a conjugacy class in G_n. From the above lemma, $N_n \leq N_\phi < \infty$ for all n, and for each conjugacy class C_i, we have from Theorem 3

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

with a constant depending only on ϕ, and not on n. The lemma follows from there. QED.

4 Ramification in torsion fields

Let E/F be a finite field extension. Then, E is a function field over the finite field with q^{N_E} elements. Let $g(E)$ and $\mathfrak{D}(E/F)$ be the genus and the different of E respectively. Let $\mathfrak{O}_E$ be the integral closure of A in E, and for any ideal $\mathfrak{a}$ of $\mathfrak{O}_E$, we define the degree of $\mathfrak{a}$ as

$$\deg_E(\mathfrak{a}) = \log_{q^{N_E}} |\mathfrak{O}_E/\mathfrak{a}|\,.$$

From the Riemann-Hurwitz formula,

$$2g(E) - 2 = -2[E : F] + \deg_E \mathfrak{D}(E/F). \tag{4}$$

We want an upper bound on the degree of the different $\mathfrak{D}(E_n/F)$ for E_n as above. This was obtained by Taguchi in [18] for the differents $\mathfrak{D}(F(\phi[a])/F)$ for any $a \in A$. The situation is simpler in our case, as we have $A = \mathbb{F}_q[T]$ anf $F = \mathbb{F}_q(T)$, and Taguchi was working with the general case. We outline his argument here, and we refer the reader to [18] for the missing details.

From classical results [17, Corollary 2, III.6], if $\alpha \in E$ is a root of a separable polynomial $f(x) = \sum_{i=0}^{M} a_i x^{p^i} \in A[x]$ with $a_0 a_M \neq 0$, then $\mathfrak{D}(F(\alpha)/F)$ divides the principal ideal $(a_0 a_M^{p^M - 2})$. In our case, $f(x)$ is the multiplication-by-a polynomial ϕ_a. We then need the following result:

Lemma 4.1 *Let ϕ be a Drinfeld module over $\mathbb{F}_q(T)$ with*

$$\phi_T = T + c_1(\phi)\tau + \ldots + c_{r-1}(\phi)\tau^{r-1} + \Delta(\phi)\tau^r.$$

Then, for any $a \in \mathbb{F}_q[T]$,

$$\phi_a = \sum_{i=0}^{M=r\deg a} a_i\tau^i$$

with $a_0 = a$ and $a_M = \Delta(\phi)^{(q^M-1)/(q^r-1)}$.

Proof: Let $a = \sum_{i=0}^{\deg a} b_i T^i$ be a monic polynomial in $\mathbb{F}_q[T]$. Then,

$$\phi_a = \sum_{i=0}^{\deg a} b_i \left(T + c_1(\phi)\tau + \ldots + c_{r-1}\tau^{r-1} + \Delta(\phi)\tau^r\right)^i = \sum_{i=0}^{r\deg a} a_i\tau^i$$

with $a_0 = \sum_{i=0}^{\deg a} b_i T^i = a$. The term of highest τ-degree has degree $r\deg a$, and multiplying in the non-commutative ring $F\{\tau\}$ according to (1), we get

$$\begin{aligned} a_{r\deg a}\tau^{r\deg a} &= (\Delta(\phi)\tau^r)^{\deg a} = \Delta(\phi)^{1+q^r+q^{2r}+\ldots+q^{(\deg a-1)r}}\tau^{r\deg a} \\ &= \Delta(\phi)^{(q^{r\deg a}-1)/(q^r-1)}\tau^{r\deg a} \end{aligned}$$

as claimed. QED.

Recall that $F(\phi[a]) = F(\alpha_1, \ldots, \alpha_r)$ for any A-basis of the a-torsion module $\phi[a] \simeq (A/aA)^r$. Then using the transitivity property of the discriminant, it follows from Lemma 4.1 that $\mathfrak{D}(F(\phi[a])/F)$ divides the principal ideal

$$\left(a\ \Delta(\phi)^{(q^M-2)(q^M-1)/(q^r-1)}\right)^r \tag{5}$$

where $M = r\deg a$. Finally, applying those results to the extension E_n/F, we get:

Lemma 4.2

$$\deg_{E_n} \mathfrak{D}(E_n/F) \ll r\,[E_n : F]\,\ell^{2nr}$$

where the constant depends only on ϕ.

Proof: From (5),

$$\deg_{E_n} \mathfrak{D}(E_n/F) \leq r\left(\deg_{E_n} \mathfrak{L}^n + \ell^{2nr}\deg_{E_n}\Delta(\phi)\right).$$

The result now follows from

$$\begin{aligned} \deg_{E_n} \mathfrak{L} &= \frac{1}{N_n}[E_n : F]\ \deg_F \mathfrak{L} \leq [E_n : F]\ \log_q \ell \\ \deg_{E_n} \Delta(\phi) &= \frac{1}{N_n}[E_n : F]\ \deg_F \Delta(\phi) \ll [E_n : F] \end{aligned}$$

where the constant depends only on ϕ. QED.

Corollary 4.3

$$g(E_n) \ll r\,[E_n : F]\,\ell^{2nr}$$

where the constant depends only on ϕ.

Proof: Immediate from the Riemann-Hurwitz formula and Lemma 4.2. QED.

5 Proof of Theorem 1.1

We now complete the proof of Theorem 1.1 by applying Corollary 3.3 to the extension E_n/F. Let $C_n(t)$ be the set of elements of G_n of trace t. Then, $C_n(t)$ is a union of conjugacy classes.

Lemma 5.1

$$\ell^{r^2 n} \ll |G_n| \leq \ell^{r^2 n}$$

for some constant depending only on ϕ and $\mathfrak{L}$.

Proof: The upper bound is trivial, as

$$|G_n| \leq |\mathrm{M}_r(A/\mathfrak{L}^n A)| = \ell^{r^2 n}.$$

The lower bound follows from Theorem 2.3. Because the image of $\rho_{\mathfrak{L}^\infty}$ is open in $\mathrm{GL}_r(A_{\mathfrak{L}})$, $\mathrm{Gal}(F(\phi[\mathfrak{L}^\infty])/F)$ contains the principal congruence subgroup $\mathrm{GL}_r(A_{\mathfrak{L}})(M)$, for some level M depending only on ϕ and $\mathfrak{L}$. Then, G_n contains $\mathrm{GL}_r(A/\mathfrak{L}^{\mathrm{n}}A)(M)$, and the result follows. QED.

Lemma 5.2

$$|C_n(t)| \leq \ell^{(r^2-1)n}.$$

Proof: This is a trivial bound as $|C_n(t)|$ is smaller than the number of elements of trace t in $\mathrm{M}_r(A/\mathfrak{L}^n A)$. QED.

Proof of Theorem 1.1: Let $\mathfrak{L}$ be a prime of A, and n be a positive integer. Trivially, we have

$$\begin{aligned}
\pi_t(k) &= \#\,\{\text{primes } \mathfrak{p} \text{ of degree } k \text{ such that } a_{\mathfrak{p}}(\phi) = t\} \\
&\leq \#\,\{\text{primes } \mathfrak{p} \text{ of degree } k \text{ such that } a_{\mathfrak{p}}(\phi) \equiv t \text{ modulo } \mathfrak{L}^n\}.
\end{aligned}$$

By definition, $a_{\mathfrak{p}}(\phi) \equiv t$ modulo $\mathfrak{L}^n$ if and only if $\sigma_{\mathfrak{p}} \in C_n(t)$ in the Galois group $G_n \leq \mathrm{GL}_r\,(A/\mathfrak{L}^n A)$. Then, with the notation of Section 3

$$\pi_t(k) \leq |S_k(E_n/F, C_n(t)|.$$

Using the estimates of Lemmas 4.3, 5.1 and 5.2 in Corollary 3.3, we get that

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

We choose n such that

$$q^{k/2(r^2+2r)} \ll \ell^n \ll q^{k/2(r^2+2r)} \tag{6}$$

with constants depending only on ℓ. This gives

$$\pi_t(k) \ll r\,\frac{q^{k(1-1/2(r^2+2r))}}{k}.$$

QED.

Acknowledgments: The author would like to thank E.-U. Gekeler for helpful discussions, and for providing the proof of Lemma 3.2.

References

[1] P. Bayer and J. Gonzáles, On the Hasse-Witt Invariants of modular curves, *Experimental Math.* **6** (1997), 57–76.

[2] M. Brown, Singular moduli and supersingular moduli of Drinfeld modules, *Invent. Math.* **110** (1992), 419–439.

[3] C. David, Supersingular reduction of Drinfeld modules, *Duke Math. J.* **78** (1995), 399–412.

[4] C. David, Average distribution of supersingular Drinfeld modules, *J. Number Theory* **56** (1996), 366–380.

[5] N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, *Invent. Math.* **89** (1987), 561–567.

[6] M. D. Fried and M. Jarden, "Field arithmetic", Springer–Verlag, Berlin-New York, 1986.

[7] E.-U. Gekeler, On finite Drinfeld modules, *J. Algebra* **141** (1991), 167–182.

[8] D. Goss, "Basic structures of function field arithmetic", Springer–Verlag, Berlin, 1996.

[9] F. Gouvêa, Non-ordinary primes: a story, *Experimental Math.* **6** (1997), 195–205.

[10] D. Hayes, A brief introduction to Drinfeld modules, *in* "The arithmetic of function fields" (D. Goss et al., Eds.), pp. 1–32, de Gruyter, 1992.

[11] V. K. Murty, Frobenius distributions and Galois representations, *Proc. Sympos. Pure Math.* **66**, (1999), 193–211.

[12] H. Trotter and S. Lang, "Frobenius distributions in GL_2 extensions", Lecture Notes in Math., **504**, Springer–Verlag, Berlin, 1976.

[13] R. Pink, The Mumford-Tate conjecture for Drinfeld modules, *Publ. Res. Inst. Math.Sci. Kyoto Univ.* **33** (1997), 393-425.

[14] B. Poonen, Drinfeld modules with no supersingular primes, *Internat. Math. Res. Notices* **No. 3** (1998), 151–159.

[15] J-P. Serre Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[16] J-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Inst. Hautes Études Sci. Publ. Math.* **No. 54** (1981), 323–401.

[17] J-P. Serre, "Local fields", Graduate Texts in Math., Springer–Verlag, New York, 1979.

[18] Y. Taguchi, Ramifications arising from Drinfeld modules, *in* "The arithmetic of function fields" (D. Goss et al., Eds.), pp. 171–188, de Gruyter, 1992.

[19] J.-K. Yu, Isogenies of Drinfeld modules over finite fields, *J. Number Theory* 54 (1995), 161–171.

Concordia University, Department of Mathematics, 1455 de Maisonneuve Blvd. West, Montréal, Quebec H3G 1M8, CANADA
E–mail: chantal@cicma.concordia.ca