ACTA ARITHMETICA
131.4 (2008)

The Erdős and Halberstam theorems for Drinfeld modules of any rank

by

Alina Carmen Cojocaru (Chicago, IL, and Bucharest)
with an appendix by Hugh Thomas (Fredericton)

1. INTRODUCTION

Let $\omega(n)$ denote the number of distinct prime factors of a positive integer n. A natural question to consider is how the function $\omega(n)$ behaves as n varies. In 1917, Hardy and Ramanujan [HaRa] answered this by showing that $\omega(n)$ has normal order $\log\log n$, meaning that for every $\varepsilon > 0$,

$$\#\{n \le x : |\omega(n) - \log\log n| > \varepsilon \log\log n\} = \mathrm{o}(x) \tag{1}$$

as $x \to \infty$. A simpler proof of this result was given by Turán in 1934 [Tu], who showed that

$$\sum_{n \le x} (\omega(n) - \log\log n)^2 \ll x \log\log x. \tag{2}$$

A precise asymptotic formula for the second moment of $\omega(n)$ was obtained by Saidak [Sa]:

$$\sum_{n \le x} (\omega(n) - \log\log n)^2 = x \log\log x + cx + \mathrm{O}\left(\frac{x \log\log x}{\log x}\right).$$

In 1940, thanks to the development of probabilistic ideas, Erdős and Kac [ErKa] obtained a remarkable refinement of (1) by showing that

$$\frac{\omega(n) - \log\log n}{\sqrt{\log\log n}}$$

is distributed normally, that is, for every $\alpha < \beta$,

2000 *Mathematics Subject Classification*: 11G09, 11N05, 11K31.
Key words and phrases: Drinfeld modules, normal order, Chebotarev density theorem.
ACC supported in part by NSF grant DMS-0636750.
HT supported by an NSERC Discovery Grant.

$$\#\left\{n \le x : \alpha \le \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} \le \beta\right\} \sim \Phi(\alpha,\beta)x, \tag{3}$$

where

$$\Phi(\alpha,\beta) := \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\beta} e^{-t^2/2}\, dt.$$

In the 1950s and 1960s, further generalizations of (3) were developed by Kubilius and Shapiro to the wider class of strongly additive functions, leading to what is now known as probabilistic number theory (see [El] and the references therein).

For example, a simple variation of the problem of studying $\omega(n)$ is that of studying $\omega(p-1)$, where p denotes a rational prime. Erdős [Er] proved that

$$\sum_{p \le x} (\omega(p-1) - \log\log x)^2 \ll \pi(x)\log\log x, \tag{4}$$

where $\pi(x)$ denotes the number of rational primes up to x. As with Turán's result, (4) implies that the normal order of $\omega(p-1)$ is $\log\log p$. In 1955, Halberstam [Hal] considered a prime analogue of (3); namely, he showed that for every $\alpha < \beta$,

$$\#\left\{p \le x : \alpha \le \frac{\omega(p-1) - \log\log p}{\sqrt{\log\log p}} \le \beta\right\} \sim \Phi(\alpha,\beta)\pi(x). \tag{5}$$

In the early 1980s, K. Murty and R. Murty [MuMu] explored higher-dimensional analogues of the results of Erdős and Halberstam by replacing the sequence $(p-1)_{p \le x}$ with the sequence $(a_p)_{p \le x}$ of Fourier coefficients of eigenforms. More recently, A. Miri and K. Murty [MiMu] and the author [Co] explored analogues of (4) for the sequence $(p+1-a_p)_{p \le x}$ arising by looking at the reductions modulo p of an elliptic curve over $\mathbb{Q}$. All these variations may be viewed as non-abelian generalizations of the Erdős and Halberstam theorems, since their proofs involve the use of certain non-abelian extensions of $\mathbb{Q}$, containing cyclotomic fields, while the proofs of (4) and (5) involve the use of cyclotomic fields (which are abelian extensions of $\mathbb{Q}$).

The purpose of this paper is to explore higher-dimensional analogues of the Erdős and Halberstam theorems in the context of function fields. This was already started by Liu [Li2], who studied the behaviour of

$$\omega(\mathfrak{f}) := \#\{\mathcal{L} \in \mathbb{F}_q[T] : \mathcal{L} \text{ monic, irreducible, } \mathcal{L} \mid \mathfrak{f}\}$$

for polynomials $\mathfrak{f} \in \mathbb{F}_q[T]$, where q denotes an odd prime power and $\mathbb{F}_q$ denotes the finite field with q elements. More precisely, she showed that

$$\sum_{\substack{P \in \mathbb{F}_q[T] \\ \deg P \le n}} (\omega(P - \mathfrak{f}) - \log n)^2 \ll \pi(n)\log n \tag{6}$$

and, for every $\alpha < \beta$,

$$(7) \qquad \#\left\{P \in \mathbb{F}_q[T] : \deg P \le n,\ \alpha \le \frac{\omega(P-\mathfrak{f}) - \log\deg P}{\sqrt{\log\deg P}} \le \beta\right\} \sim \Phi(\alpha,\beta)\pi(n)$$

as $n \to \infty$, where $P \in \mathbb{F}_q[T]$ denotes monic, irreducible polynomials of degree $\deg P$, $\mathfrak{f} \in \mathbb{F}_q[T]$ is fixed, and

$$\pi(n) := \#\{P \in \mathbb{F}_q[T] : \deg P \le n\}.$$

As in the rational case, it is of interest to explore if analogues of (6) and (7) hold in higher dimensions. As such, one needs to understand what "higher dimensions" might mean. We propose to answer this by looking at analogues of the results of [MuMu], [MiMu] and [Co] for Drinfeld modules, as explained in what follows.

Let $A := \mathbb{F}_q[T]$ and $F := \mathbb{F}_q(T)$. This is a particular case of F being a function field over $\mathbb{F}_q$ and A being the ring of fractions regular away from a fixed place of F, denoted ∞, and called the *place at infinity*. This place corresponds to the valuation $v_\infty(\mathfrak{f}) = -\deg\mathfrak{f}$ on F, and so $|\mathfrak{f}|_\infty = q^{\deg\mathfrak{f}}$ for $0 \ne \mathfrak{f} \in F$ and $|0|_\infty = 0$. Our main results are:

THEOREM 1. *Let ϕ be a Drinfeld A-module over F, of rank $r \ge 1$. Assume that ϕ has trivial endomorphism ring. For a prime $P \in A$ of good reduction for ϕ, let $\mathbf{P}_{P,\phi}(X) \in A[X]$ be the characteristic polynomial of the Frobenius automorphism at P and let $a_P(\phi)$ be the trace of the Frobenius automorphism at P (see Section 2 for more explanations). If $r \ge 3$, assume the validity of the Mumford–Tate conjecture for ϕ (again, see Section 2). Then*:

$$\text{(i)} \quad \sum_{\substack{P\in A\\ \deg P\le n}} (\omega(\mathbf{P}_{P,\phi}(1)) - \log n)^2 \ll_\phi \pi(n)\log n,$$

$$\text{(ii)} \quad \sum_{\substack{P\in A\\ \deg P\le n}} (\omega(a_P(\phi)) - \log n)^2 \ll_\phi \pi(n)\log n,$$

as $n \to \infty$. The implied $\ll_\phi$-constants depend on ϕ.

COROLLARY 2. *We keep the setting and assumptions of Theorem 1. Let $(g_n)_n$ be a sequence of real numbers with $\lim_{n\to\infty} g_n = \infty$. Then*

$$\#\left\{P \in A : \deg P \le n,\ \left|\frac{\omega(\mathbf{P}_{P,\phi}(1)) - \log\deg P}{\sqrt{\log\deg P}}\right| > g_n\right\} = \mathrm{o}(\pi(n)),$$

$$\#\left\{P \in A : \deg P \le n,\ \left|\frac{\omega(a_P(\phi)) - \log\deg P}{\sqrt{\log\deg P}}\right| > g_n\right\} = \mathrm{o}(\pi(n)).$$

In particular, for any $\varepsilon > 0$ *we have*

$$\#\{P \in A : \deg P \le n,\ |\omega(\mathbf{P}_{P,\phi}(1)) - \log\deg P| > \varepsilon \log\deg P\} = \mathrm{o}(\pi(n)),$$
$$\#\{P \in A : \deg P \le n,\ |\omega(a_P(\phi)) - \log\deg P| > \varepsilon \log\deg P\} = \mathrm{o}(\pi(n)).$$

Thus the sequences $\omega(\mathbf{P}_{P,\phi}(1))$ *and* $\omega(a_P(\phi))$ *have normal order* $\log\deg P$.

THEOREM 3. *We keep the setting and assumptions of Theorem* 1. *Then for every* $\alpha < \beta$ *we have*

$$\#\left\{P \in A : \deg P \le n,\ \alpha \le \frac{\omega(\mathbf{P}_{P,\phi}(1)) - \log\deg P}{\sqrt{\log\deg P}} \le \beta\right\} \sim \Phi(\alpha,\beta)\pi(n),$$
$$\#\left\{P \in A : \deg P \le n,\ \alpha \le \frac{\omega(a_P(\phi)) - \log\deg P}{\sqrt{\log\deg P}} \le \beta\right\} \sim \Phi(\alpha,\beta)\pi(n),$$

as $n \to \infty$.

2. DRINFELD MODULES

2.1. Generalities. In this section we shall record basic facts about Drinfeld modules needed in our proofs. For proofs or more results on Drinfeld modules, the reader is referred to [Dr1], [Dr2], [Ge1], [Ge2], [Go], or [Hay]. We keep the notation A, F introduced in Section 1, and we let $\overline{F}$ and F^{sep} denote an algebraic closure and a separable closure of F. Also, we let $\tau : x \mapsto x^q$ denote the qth power Frobenius automorphism, and $F\{\tau\}$ the twisted polynomial ring in τ, where the multiplication law is $\alpha^q\tau = \tau\alpha$ for every $\alpha \in F$.

We recall that a *Drinfeld* A*-module over* F*, of rank* r, is a ring homomorphism

$$\phi : A \to F\{\tau\}, \qquad a \mapsto \phi_a := \sum_{i=0}^{r\deg a} a_i\tau^i,$$

such that $a_0 = a$. Clearly, ϕ is completely determined by

$$\phi_T = T + c_1(\phi)\tau + \cdots + c_{r-1}(\phi)\tau^{r-1} + \Delta(\phi)\tau^r \in F\{\tau\},$$

where $\Delta(\phi)$ is called the *discriminant* of ϕ.

Drinfeld modules may be viewed as function field analogues of elliptic curves. This analogy is not visible from the above definition, but from the (equivalent) definition based on the complex theory of F. Even without much digression in that direction, we can still see the similarity with elliptic curves by looking at the Galois representations associated to ϕ, as follows.

For each prime $\mathcal{L} \in A$ and positive integer n, let

$$\phi[\mathcal{L}^n] := \{\lambda \in \overline{F} : \phi_{\mathcal{L}^n}(\lambda) = 0\}$$

be the $\mathcal{L}^n$-torsion points of ϕ. It is known that $\phi[\mathcal{L}^n] \simeq (A/\mathcal{L}^n A)^r$, and that $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ acts continuously on $\phi[\mathcal{L}^n]$, giving rise to a Galois representation

$$\bar{\varrho}_{\mathcal{L}^n} : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{Aut}_{A/\mathcal{L}^n A}\, \phi\,[\mathcal{L}^n] \simeq \mathrm{GL}_r(A/\mathcal{L}^n A).$$

Moreover, by taking

$$\phi[\mathcal{L}^\infty] := \varinjlim_n \phi\,[\mathcal{L}^n]$$

and

$$T_{\mathcal{L}}(\phi) := \mathrm{Hom}_{A_{\mathcal{L}}}(F_{\mathcal{L}}/A_{\mathcal{L}}, \phi[\mathcal{L}^\infty]) \simeq A_{\mathcal{L}}^r,$$

where $A_{\mathcal{L}}$ and $F_{\mathcal{L}}$ are the $\mathcal{L}$-completions of A and F, we obtain the $\mathcal{L}$-adic Galois representation

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

Also, if $\mathcal{L}_1, \dots, \mathcal{L}_u \in A$ are distinct primes, we can talk about the $\mathcal{L}_1 \dots \mathcal{L}_u$-torsion points of ϕ,

$$\phi[\mathcal{L}_1 \dots \mathcal{L}_u] := \{\lambda \in \overline{F} : \phi_{\mathcal{L}_1 \dots \mathcal{L}_u}(\lambda) = 0\},$$

and the associated Galois representation

$$\bar{\varrho}_{\mathcal{L}_1 \dots \mathcal{L}_u} : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{Aut}_{A/\mathcal{L}_1 \dots \mathcal{L}_u A}\, \phi[\mathcal{L}_1 \dots \mathcal{L}_u] \simeq \mathrm{GL}_r(A/\mathcal{L}_1 \dots \mathcal{L}_u A).$$

From results of Drinfeld and Gekeler we know that the $(\varrho_{\mathcal{L}^\infty})_{\mathcal{L}}$ form a *strictly compatible system of representations* in the sense that for all primes $P \nmid \Delta(\phi)\mathcal{L}$ of A, $\varrho_{\mathcal{L}^\infty}$ is unramified at P and the characteristic polynomial at P,

$$\mathbf{P}_{P,\phi}(X) := \det(X - \varrho_{\mathcal{L}^\infty}(\mathrm{Frob}_P)) \in F_{\mathcal{L}}[X],$$

of the Artin symbol Frob_P at P does not depend on $\mathcal{L}$ and has coefficients in A. Thus we can write

$$\mathbf{P}_{P,\phi}(X) = X^r - a_P(\phi)X^{r-1} + a_2 X^{r-2} + \dots + a_{r-1}X + \mu_P P \in A[X] \tag{8}$$

for some $\mu_P \in \mathbb{F}_q^*$.

If we let $\pi_P(\phi)$ be one of the roots of $\mathbf{P}_{P,\phi}(X)$ in $\overline{F}$, we also know that

$$|\pi_P(\phi)|_\infty = |P|_\infty^{1/r}.$$

Therefore

$$|a_P(\phi)|_\infty \le |P|_\infty^{1/r},$$

a result which reminds us of Hasse's bound for elliptic curves.

As in the case of elliptic curves, there is a notion of isogenies between Drinfeld modules, thus we can talk about the endomorphism ring $\mathrm{End}_{\overline{F}}(\phi)$ of ϕ. If the rank r of ϕ is 1, then $\mathrm{End}_{\overline{F}}(\phi) \simeq A$. If $r = 2$, then $\mathrm{End}_{\overline{F}}(\phi)$ is isomorphic either to A or to an order in an imaginary quadratic extension of F. If $r \ge 3$, then $\mathrm{End}_{\overline{F}}(\phi)$ may be isomorphic to A or several other rings; in general, it is a projective A-module of rank $\le r^2$. In this paper we shall

consider only the case when $\mathrm{End}_{\overline{F}}(\phi) \simeq A$, and relegate the other cases to future research.

2.2. Connection with the Erdős and Halberstam theorems. Before moving on, let us recall that our ultimate goal in this paper is to study higher-dimensional versions of the Erdős and Halberstam theorems in the context of function fields. A first simple observation which we can make is that if ϕ has rank 1, then the study of $\omega(\mathbf{P}_{P,\phi}(1))$, as $P \in A$ varies over primes, provides us with the first instance of (4) and (5) for function fields, and is nothing else but what was obtained in [Li2]. Indeed, when $r = 1$,

$$\mathbf{P}_{P,\phi}(X) = X + \mu_P P \in A[X],$$

and so

$$\omega(\mathbf{P}_{P,\phi}(1)) = \omega(1 + \mu_P P).$$

This coincidence is not at all surprising, since Drinfeld modules of rank 1 (introduced by Carlitz in 1938) lead to the function field analogue of cyclotomic fields, and the latter are precisely the fields playing the key role in the proofs of (4) and (5).

A second observation which we can make concerns the case when $r \geq 2$. If $r = 2$, say, then the primes $\mathcal{L} \,|\, \mathbf{P}_{P,\phi}(1)$ enumerated by $\omega(\mathbf{P}_{P,\phi}(1))$ are the ones for which

$$\mathcal{L} \,|\, \pi_P(\phi) - 1 \quad \text{or} \quad \mathcal{L} \,|\, \overline{\pi_P(\phi)} - 1 \quad \text{in } F(\pi_P(\phi)),$$

where $\overline{\pi_P(\phi)}$ denotes the conjugate of $\pi_P(\phi)$ in F^{sep}. In other words, we are concerned with primes $\mathcal{L}$ enumerated by $\omega(\pi_P(\phi) - 1)$ or $\omega(\overline{\pi_P(\phi)} - 1)$ in $F(\pi_P(\phi))$. Since $\pi_P(\phi)$ and $\overline{\pi_P(\phi)}$ are primes in $F(\pi_P(\phi))$, we see that the study of $\omega(\mathbf{P}_{P,\phi}(1))$ is indeed a natural generalization of that of $\omega(P-1)$.

The study of the sequence $\omega(a_P(\phi))$ does not generalize that of $\omega(P-1)$; however, it is the direct analogue of the study made in [MuMu], hence worth considering.

2.3. Division fields of Drinfeld modules. With these observations in mind, we may now move on and discuss the objects which will play a fundamental role in the proofs of our main results; these are the division fields of a Drinfeld module, defined as follows. For a prime $\mathcal{L} \in A$, we define the *$\mathcal{L}$-division field* of a Drinfeld module ϕ as the field obtained by adjoining to F the $\mathcal{L}$-torsion points of ϕ:

$$F[\mathcal{L}] := F(\phi[\mathcal{L}]).$$

It is a finite Galois extension of F such that $\mathrm{Ker}\, \bar{\varrho}_{\mathcal{L}} = \mathrm{Gal}(\overline{\mathbb{Q}}/F[\mathcal{L}])$. Thus we have an injective representation

$$\bar{\varrho}_{\mathcal{L}} : \mathrm{Gal}(F[\mathcal{L}]/F) \to \mathrm{GL}_r(A/\mathcal{L}A),$$

and so

$$[F[\mathcal{L}] : F] \leq |\mathrm{GL}_r(A/\mathcal{L}A)| = \prod_{i=0}^{r-1}(\ell^r - \ell^i) \ll \ell^{r^2},$$

where $\ell := |\mathcal{L}|_\infty$.

If ϕ has rank 1, then the above map is, in fact, an isomorphism. Furthermore, thanks to important work of Gardeyn and Pink, this also holds if ϕ has rank 2 and trivial endomorphism ring, for all but finitely many primes $\mathcal{L}$. In the case of higher rank, such a statement is conjectured to be true, though it has not yet been proven, and is part of the Mumford–Tate conjecture for Drinfeld modules. We record all these statements below:

THEOREM 4.

(i) (Carlitz). *Let ϕ be a rank 1 Drinfeld A-module over F. Then*

$$\mathrm{Gal}(F[\mathcal{L}]/F) \simeq (A/\mathcal{L}A)^*$$

for all primes $\mathcal{L} \in A$.

(ii) (Gardeyn and Pink). *Let ϕ be a rank 2 Drinfeld A-module over F, with $\mathrm{End}_{\overline{F}}(\phi) \simeq A$. Let $\widehat{A}$ be the ring of adeles of A. Then the action of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ on the set of all torsion points of ϕ has open image in $\mathrm{GL}_2(\widehat{A})$. In particular,*

$$\mathrm{Gal}(F[\mathcal{L}]/F) \simeq \mathrm{GL}_2(A/\mathcal{L}A)$$

for all but finitely many primes $\mathcal{L} \in A$.

Proof. For (i), see [Ro, p. 206]. (ii) is a consequence of the results in [Ga1] and [Pi] (see [CoDa, Thm. 11], for example, for more precise references). ∎

CONJECTURE 5 (The Mumford–Tate conjecture for Drinfeld modules). *Let ϕ be a rank r Drinfeld A-module over F, with $\mathrm{End}_{\overline{F}}(\phi) \simeq A$. As above, let $\widehat{A}$ be the ring of adeles of A. Then the action of the Galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ on the set of all torsion points of ϕ has open image in $\mathrm{GL}_r(\widehat{A})$. In particular,*

$$\mathrm{Gal}(F[\mathcal{L}]/F) \simeq \mathrm{GL}_r(A/\mathcal{L}A)$$

for all but finitely many primes $\mathcal{L} \in A$.

Important results towards this general conjecture were obtained by Pink [Pi], however the conjecture is still open at the moment. We record Pink's main result below:

THEOREM 6 (Pink [Pi, Thm. 0.1]). *Let ϕ be a rank r Drinfeld A-module over F, with $\mathrm{End}_{\overline{F}}(\phi) \simeq A$. Then for any finite set Λ of primes $\mathcal{L} \neq \infty$ of A, the image of the representation*

$$(\varrho_{\mathcal{L}^\infty})_{\mathcal{L}\in\Lambda} : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \prod_{\mathcal{L}\in\Lambda} \mathrm{GL}_r(A_{\mathcal{L}})$$

is open.

The division fields of ϕ have the following additional properties:

PROPOSITION 7. *Let ϕ be a rank r Drinfeld A-module over F. Let $\mathcal{L}, \mathcal{L}_1, \ldots, \mathcal{L}_u$ denote mutually distinct primes in A. Let K, K_u be the algebraic closures of $\mathbb{F}_q$ in $F[\mathcal{L}]$ and $F[\mathcal{L}_1 \ldots \mathcal{L}_u]$, respectively, and let $N_{\mathcal{L}} := [KF : F]$ and $N_{\mathcal{L}_1 \ldots \mathcal{L}_u} := [K_u F : F]$. Let $g_{\mathcal{L}}$ and $\mathcal{D}(F[\mathcal{L}]/\mathcal{F})$ be the genus of $F[\mathcal{L}]$ and the different of the extension $F[\mathcal{L}]/F$, respectively. Similarly, let $g_{\mathcal{L}_1 \ldots \mathcal{L}_u}$ and $\mathcal{D}(F[\mathcal{L}_1 \ldots \mathcal{L}_u]/F)$ be the genus of $F[\mathcal{L}_1 \ldots \mathcal{L}_u]$ and the different of $F[\mathcal{L}_1 \ldots \mathcal{L}_u]/F$, respectively.*

(i) *Assume that $\mathrm{End}_{\overline{F}}(\phi) \simeq A$. Then, for all but finitely many primes $\mathcal{L}, \mathcal{L}_1, \ldots, \mathcal{L}_u \in A$, $F[\mathcal{L}]$ and $F[\mathcal{L}_1 \ldots \mathcal{L}_u]$ are geometric extensions of F, i.e. $N_{\mathcal{L}} = N_{\mathcal{L}_1 \ldots \mathcal{L}_u} = 1$.*

(ii) *We have*

$$g_{\mathcal{L}} \ll_\phi r|\mathrm{GL}_r(A/\mathcal{L}A)| \deg \mathcal{L} \ll_\phi r\ell^{r^2} \deg \mathcal{L}$$

and

$$\begin{aligned} g_{\mathcal{L}_1 \ldots \mathcal{L}_u} &\ll_\phi r|\mathrm{GL}_r(A/\mathcal{L}_1 \ldots \mathcal{L}_u A)| \deg(\mathcal{L}_1 \ldots \mathcal{L}_u) \\ &\ll_\phi r\ell_1^{r^2} \ldots \ell_u^{r^2} \deg(\mathcal{L}_1 \ldots \mathcal{L}_u), \end{aligned}$$

where $\ell := |\mathcal{L}|_\infty$, $\ell_1 := |\mathcal{L}_1|_\infty, \ldots, \ell_u := |\mathcal{L}_u|_\infty$. The implied $\ll_\phi$-constants depend on ϕ.

Proof. From Theorem 6 it follows that the fields $F[\mathcal{L}]$ are disjoint. Now we recall from [Da, Lem. 3.2, p. 335] that the degree of the algebraic closure of $\mathbb{F}_q$ in the extension of F obtained by adding all the torsion points of ϕ is finite. The assertion of (i) now follows. For (ii), see [Ga2, p. 246]. ∎

3. THE PRIME NUMBER THEOREM AND THE CHEBOTAREV DENSITY THEOREM

Of interest to us are applications of the prime number theorem and the Chebotarev density theorem (over function fields) to the division fields of a Drinfeld module. We recall these results below.

THEOREM 8. *Let $A := \mathbb{F}_q[T]$, as before. Let n be a positive integer and let $\pi(n)$ be the number of primes $\mathcal{L} \in A$ with $\deg \mathcal{L} = n$. Then*

$$\pi(n) = \frac{q^n}{n} + \mathrm{O}\left(\frac{q^{n/2}}{n}\right).$$

For a proof, see [Ro, Thm. 2.2, p. 14].

THEOREM 9. *Let $F := \mathbb{F}_q(T)$, as before, and let $F \subseteq E$ be a finite Galois extension, of genus g_E and Galois group G. Let K be an algebraic closure of $\mathbb{F}_q$ in E, and let $N_E := [KF : F]$. Let $\tau : x \mapsto x^q$ be the qth power Frobenius automorphism. For an unramified prime P in E/F, let Frob_P be the Artin*

symbol in E/F. Let $C \subseteq G$ be a union of conjugacy classes in G, and for a positive integer n, let

$$S_n(E/F, C) := \{P : \deg P = n, \operatorname{Frob}_P \subseteq C\}.$$

Let a_C be a positive integer such that

$$\operatorname{Res}_K \sigma = \operatorname{Res}_K \tau^{a_C} \quad \forall \sigma \in C.$$

(i) *If $n \not\equiv a_C \pmod{N_E}$, then $S_n(E/F, C) = \emptyset$.*
(ii) *If $n \equiv a_C \pmod{N_E}$, then*

$$|S_n(E/F, C)| = N_E \frac{|C|}{|G|} \cdot \frac{q^n}{n} + \mathrm{O}\bigg(|C| q^{n/2} + N_E \frac{|C|}{|G|} \cdot \frac{q^{n/2}}{n} g_E\bigg),$$

where the implied O*-constant is absolute.*

For a proof, see [FrJa, Prop. 5.16].

An immediate consequence of this theorem, combined with Proposition 7, is:

Corollary 10. *Let A, F be as in Section* 1. *Let ϕ be a rank r Drinfeld A-module over F. Assume that $\operatorname{End}_{\overline{F}}(\phi) \simeq A$. Let $\mathcal{L}, \mathcal{L}_1, \dots, \mathcal{L}_u \in A$ be mutually distinct primes and let k be a positive integer. Let C, C_u be unions of conjugacy classes in $\operatorname{Gal}(F[\mathcal{L}]/F)$ and $\operatorname{Gal}(F[\mathcal{L}_1 \dots \mathcal{L}_u]/F)$, respectively. Then*

$$|S_n(F[\mathcal{L}]/F, C)| = \frac{|C|}{[F[\mathcal{L}] : F]} \cdot \frac{q^n}{n} + \mathrm{O}_\phi\bigg(|C| q^{n/2} + |C| \frac{q^{n/2}}{n} r \deg \mathcal{L}\bigg)$$

and

$$|S_n(F[\mathcal{L}_1 \dots \mathcal{L}_u]/F, C_u)| = \frac{|C_u|}{[F[\mathcal{L}_1 \dots \mathcal{L}_u] : F]} \cdot \frac{q^n}{n} + \mathrm{O}_\phi\bigg(|C_u| q^{n/2} + |C_u| \frac{q^{n/2}}{n} r(\deg \mathcal{L}_1 \dots \mathcal{L}_u)\bigg),$$

where the implied O_ϕ-constants depend on ϕ.

4. PROOF OF THEOREM 1

The proof of Theorem 1 is based on a very simple method due to Paul Turán, which we follow closely.

We first make the observation that for any $0 < \delta < 1$ and any $\mathfrak{f} \in A$ of degree n, we have

$$\omega(\mathfrak{f}) = \omega_\delta(\mathfrak{f}) + \mathrm{O}\bigg(\frac{1}{\delta}\bigg), \tag{9}$$

where

$$\omega_\delta(\mathfrak{f}) := \sum_{\substack{\mathcal{L}\mid\mathfrak{f}\\ \deg\mathcal{L}\le\delta n}} 1.$$

Here and throughout the paper, $\mathcal{L}$ denotes a prime in A, that is, a monic irreducible polynomial.

Using (9) and the prime number theorem (Thm. 8), we see that

$$\sum_{\deg P=n} \omega(\mathbf{P}_{P,\phi}(1)) = \sum_{\deg P=n} \omega_\delta(\mathbf{P}_{P,\phi}(1)) + \mathrm{O}\left(\frac{q^n}{n}\right) \tag{10}$$

and

$$\begin{aligned}\sum_{\deg P=n} \omega^2(\mathbf{P}_{P,\phi}(1))&\\ = \sum_{\deg P=n} \omega_\delta^2(\mathbf{P}_{P,\phi}(1)) + \mathrm{O}\left(\frac{1}{\delta}\sum_{\deg P=n} \omega_\delta(\mathbf{P}_{P,\phi}(1))\right) + \mathrm{O}\left(\frac{q^n}{n}\right).\end{aligned} \tag{11}$$

Similarly,

$$\sum_{\deg P=n}{}' \omega(a_P(\phi)) = \sum_{\deg P=n}{}' \omega_\delta(a_P(\phi)) + \mathrm{O}\left(\frac{q^n}{n}\right) \tag{12}$$

and

$$\begin{aligned}\sum_{\deg P=n}{}' \omega^2(a_P(\phi))&\\ = \sum_{\deg P=n}{}' \omega_\delta^2(a_P(\phi)) + \mathrm{O}\left(\frac{1}{\delta}\sum_{\deg P=n}{}' \omega_\delta(a_P(\phi))\right) + \mathrm{O}\left(\frac{q^n}{n}\right),\end{aligned} \tag{13}$$

where $\sum'$ means that we are summing over primes $P \in A$ with $a_P(\phi) \neq 0$.

Let us introduce the notation:

$$\Pi_\phi^{\mathrm{char}}(n,\mathcal{L}) := \#\{P \in A : \deg P = n,\ P\nmid\Delta(\phi),\ \mathcal{L} \mid \mathbf{P}_{P,\phi}(1)\}, \tag{14}$$

$$\Pi_\phi^{\mathrm{char}}(n,\mathcal{L}_1\mathcal{L}_2) := \#\{P \in A : \deg P = n,\ P\nmid\Delta(\phi),\ \mathcal{L}_1\mathcal{L}_2 \mid \mathbf{P}_{P,\phi}(1)\}, \tag{15}$$

$$\begin{aligned}\Pi_\phi^{\mathrm{tr}}(n,\mathcal{L}) := \#\{P \in A : \deg P = n,\ a_P(\phi)\neq 0,&\\ P\nmid\Delta(\phi),\ \mathcal{L} \mid a_P(\phi)\}&,\end{aligned} \tag{16}$$

$$\begin{aligned}\Pi_\phi^{\mathrm{tr}}(n,\mathcal{L}_1\mathcal{L}_2) := \#\{P \in A : \deg P = n,\ a_P(\phi)\neq 0,&\\ P\nmid\Delta(\phi),\ \mathcal{L}_1\mathcal{L}_2 \mid a_P(\phi)\}&.\end{aligned} \tag{17}$$

We note that the primes P enumerated above are distinct from the primes $\mathcal{L}, \mathcal{L}_1, \mathcal{L}_2$, since $\deg P = n$ and $\deg\mathcal{L}, \deg\mathcal{L}_1, \deg\mathcal{L}_2 \le \delta n$ with $\delta < 1$. This observation will be necessary later.

By writing $\omega_\delta(\cdot)$ as a sum and interchanging summations, the identities (10)–(13) become:

$$\sum_{\deg P=n} \omega(\mathbf{P}_{P,\phi}(1)) = \sum_{\deg \mathcal{L}\le \delta n} \Pi_\phi^{\mathrm{char}}(n,\mathcal{L}) + \mathrm{O}\Big(\frac{q^n}{n}\Big), \tag{18}$$

$$\sum_{\deg P=n} \omega^2(\mathbf{P}_{P,\phi}(1)) = \sum_{\substack{\mathcal{L}_1\ne\mathcal{L}_2\\ \deg\mathcal{L}_1,\deg\mathcal{L}_2\le\delta n}} \Pi_\phi^{\mathrm{char}}(n,\mathcal{L}_1\mathcal{L}_2) + \mathrm{O}\Big(\sum_{\deg\mathcal{L}\le\delta n} \Pi_\phi^{\mathrm{char}}(n,\mathcal{L})\Big) + \mathrm{O}\Big(\frac{q^n}{n}\Big), \tag{19}$$

and similarly,

$$\sum_{\deg P=n}{}' \omega(a_P(\phi)) = \sum_{\deg \mathcal{L}\le \delta n} \Pi_\phi^{\mathrm{tr}}(n,\mathcal{L}) + \mathrm{O}\Big(\frac{q^n}{n}\Big), \tag{20}$$

$$\sum_{\deg P=n}{}' \omega^2(a_P(\phi)) = \sum_{\substack{\mathcal{L}_1\ne\mathcal{L}_2\\ \deg\mathcal{L}_1,\deg\mathcal{L}_2\le\delta n}} \Pi_\phi^{\mathrm{tr}}(n,\mathcal{L}_1\mathcal{L}_2) + \mathrm{O}\Big(\sum_{\deg\mathcal{L}\le\delta n} \Pi_\phi^{\mathrm{tr}}(n,\mathcal{L})\Big) + \mathrm{O}\Big(\frac{q^n}{n}\Big). \tag{21}$$

In order to finish the proof of Theorem 1, it remains to estimate the quantities described in (14)–(17). This is where the core of the proof lies and, as we shall see, using the $\mathcal{L}$-adic representations associated to ϕ, the whole problem translates into applications of the Chebotarev density theorem.

Let us note that so far we have not used the structure of $\mathrm{End}_{\overline{F}}(\phi)$; thus the above analysis holds in general.

4.1. Drinfeld modules of rank 1. If $r = 1$, then it only makes sense to discuss $\omega(\mathbf{P}_{P,\phi}(1))$ (as P varies). As pointed out in Section 2.2, the situation reduces to the one already investigated in [Li2], and relies on estimates for primes P in arithmetic progressions, i.e. nothing else but Corollary 10 for the division fields $F[\mathcal{L}]$ and $F[\mathcal{L}_1\mathcal{L}_2]$, with $C = 1$.

4.2. Drinfeld modules of rank 2. Let us consider the case when ϕ is a Drinfeld module of rank 2, with trivial endomorphism ring. Important consequences of these assumptions are the surjectivity of the mod $\mathcal{L}$ and mod $\mathcal{L}_1\mathcal{L}_2$ Galois representations associated to ϕ, and the geometricity of the associated division fields, for all but finitely many primes $\mathcal{L}, \mathcal{L}_1, \mathcal{L}_2 \in A$ (see part (ii) of Theorem 4 and part (i) of Proposition 7).

Now let us remark that, thanks to property (8) of the characteristic polynomial $\mathbf{P}_{P,\phi}(X)$, we have

$$\mathcal{L} \,|\, \mathbf{P}_{P,\phi}(1) \;\Leftrightarrow\; \bar{\varrho}_{\mathcal{L}}(\mathrm{Frob}_P) \subseteq C^{\mathrm{char}}_{\mathcal{L}},$$
$$\mathcal{L}_1\mathcal{L}_2 \,|\, \mathbf{P}_{P,\phi}(1) \;\Leftrightarrow\; \bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2}(\mathrm{Frob}_P) \subseteq C^{\mathrm{char}}_{\mathcal{L}_1\mathcal{L}_2},$$

where

$$C^{\mathrm{char}}_{\mathcal{L}} := \{g \in \operatorname{Im} \bar{\varrho}_{\mathcal{L}} : \det g + 1 - \operatorname{tr} g = 0\},$$
$$C^{\mathrm{char}}_{\mathcal{L}_1\mathcal{L}_2} := \{g \in \operatorname{Im} \bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2} : \det g + 1 - \operatorname{tr} g = 0\}.$$

Similarly,

$$\mathcal{L} \,|\, a_P(\phi) \;\Leftrightarrow\; \bar{\varrho}_{\mathcal{L}}(\mathrm{Frob}_P) \subseteq C^{\mathrm{tr}}_{\mathcal{L}}, \quad \mathcal{L}_1\mathcal{L}_2 \,|\, a_P(\phi) \;\Leftrightarrow\; \bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2}(\mathrm{Frob}_P) \subseteq C^{\mathrm{tr}}_{\mathcal{L}_1\mathcal{L}_2},$$

where

$$C^{\mathrm{tr}}_{\mathcal{L}} := \{g \in \operatorname{Im} \bar{\varrho}_{\mathcal{L}} : \operatorname{tr} g = 0\}, \quad C^{\mathrm{tr}}_{\mathcal{L}_1\mathcal{L}_2} := \{g \in \operatorname{Im} \bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2} : \operatorname{tr} g = 0\}.$$

Here is where we are using the fact that the primes P are different from the primes $\mathcal{L}, \mathcal{L}_1, \mathcal{L}_2$.

Put together and combined with Corollary 10, these remarks give:

$$\begin{aligned}
\Pi^{\mathrm{char}}_{\phi}(n,\mathcal{L}) &= \frac{|C^{\mathrm{char}}_{\mathcal{L}}|}{|\mathrm{GL}_2(A/\mathcal{L}A)|}\cdot\frac{q^n}{n} \\
&\quad + \mathrm{O}_{\phi}\bigg(|C^{\mathrm{char}}_{\mathcal{L}}|q^{n/2} + |C^{\mathrm{char}}_{\mathcal{L}}|\,\frac{q^{n/2}}{n}\deg\mathcal{L}\bigg), \\
\Pi^{\mathrm{char}}_{\phi}(n,\mathcal{L}_1\mathcal{L}_2) &= \frac{|C^{\mathrm{char}}_{\mathcal{L}_1\mathcal{L}_2}|}{|\mathrm{GL}_2(A/\mathcal{L}_1\mathcal{L}_2A)|}\cdot\frac{q^n}{n} \\
&\quad + \mathrm{O}_{\phi}\bigg(|C^{\mathrm{char}}_{\mathcal{L}_1\mathcal{L}_2}|q^{n/2} + |C^{\mathrm{char}}_{\mathcal{L}_1\mathcal{L}_2}|\,\frac{q^{n/2}}{n}\deg(\mathcal{L}_1\mathcal{L}_2)\bigg), \\
\Pi^{\mathrm{tr}}_{\phi}(n,\mathcal{L}) &= \frac{|C^{\mathrm{tr}}_{\mathcal{L}}|}{|\mathrm{GL}_2(A/\mathcal{L}A)|}\cdot\frac{q^n}{n} + \mathrm{O}_{\phi}\bigg(|C^{\mathrm{tr}}_{\mathcal{L}}|q^{n/2} + |C^{\mathrm{tr}}_{\mathcal{L}}|\,\frac{q^{n/2}}{n}\deg\mathcal{L}\bigg), \\
\Pi^{\mathrm{tr}}_{\phi}(n,\mathcal{L}_1\mathcal{L}_2) &= \frac{|C^{\mathrm{tr}}_{\mathcal{L}_1\mathcal{L}_2}|}{|\mathrm{GL}_2(A/\mathcal{L}_1\mathcal{L}_2A)|}\cdot\frac{q^n}{n} \\
&\quad + \mathrm{O}_{\phi}\bigg(|C^{\mathrm{tr}}_{\mathcal{L}_1\mathcal{L}_2}|q^{n/2} + |C^{\mathrm{tr}}_{\mathcal{L}_1\mathcal{L}_2}|\,\frac{q^{n/2}}{n}\deg(\mathcal{L}_1\mathcal{L}_2)\bigg),
\end{aligned}$$

for all but finitely many primes $\mathcal{L}, \mathcal{L}_1, \mathcal{L}_2 \in A$ (with $\mathcal{L}_1 \neq \mathcal{L}_2$).

We set

$$\ell := |\mathcal{L}|_\infty, \quad \ell_1 := |\mathcal{L}_1|_\infty, \quad \ell_2 := |\mathcal{L}_2|_\infty.$$

Simple calculations in GL_2 show that:

$$|\mathrm{GL}_2(A/\mathcal{L}A)| = (\ell^2-1)(\ell^2-\ell),$$
$$|\mathrm{GL}_2(A/\mathcal{L}_1\mathcal{L}_2A)| = (\ell_1^2-1)(\ell_1^2-\ell_1)(\ell_2^2-1)(\ell_2^2-\ell_2),$$

and

$$|C^{\mathrm{char}}_{\mathcal{L}}| = \ell^3 + \mathrm{O}(\ell^2), \qquad |C^{\mathrm{tr}}_{\mathcal{L}}| = \ell^3 + \mathrm{O}(\ell^2),$$
$$|C^{\mathrm{char}}_{\mathcal{L}_1\mathcal{L}_2}| = \ell_1^3\ell_2^3 + \mathrm{O}(\ell_1^2\ell_2^2), \quad |C^{\mathrm{tr}}_{\mathcal{L}_1\mathcal{L}_2}| = \ell_1^3\ell_2^3 + \mathrm{O}(\ell_1^2\ell_2^2).$$

Thus for all but finitely many primes $\mathcal{L}, \mathcal{L}_1, \mathcal{L}_2 \in A$ with $\mathcal{L}_1 \neq \mathcal{L}_2$, we have:

$$\Pi_\phi^{\mathrm{char}}(n,\mathcal{L}) = \frac{\ell^2}{(\ell^2-1)\,(\ell-1)} \cdot \frac{q^n}{n} + \mathrm{O}_\phi\bigg(\ell^3 q^{n/2} + \ell^3\,\frac{q^{n/2}}{n}\log_q \ell\bigg), \tag{22}$$

$$\begin{aligned}\Pi_\phi^{\mathrm{char}}(n,\mathcal{L}_1\mathcal{L}_2) &= \frac{\ell_1^2\ell_2^2}{(\ell_1^2-1)(\ell_2^2-1)(\ell_1-1)(\ell_2-1)} \cdot \frac{q^n}{n} \\ &\quad + \mathrm{O}_\phi\bigg(\ell_1^3\ell_2^3 q^{n/2} + \ell_1^3\ell_2^3\,\frac{q^{n/2}}{n}\log_q(\ell_1\ell_2)\bigg),\end{aligned} \tag{23}$$

$$\Pi_\phi^{\mathrm{tr}}(n,\mathcal{L}) = \frac{\ell^2}{(\ell^2-1)(\ell-1)} \cdot \frac{q^n}{n} + \mathrm{O}_\phi\bigg(\ell^3 q^{n/2} + \ell^3\,\frac{q^{n/2}}{n}\log_q \ell\bigg), \tag{24}$$

$$\begin{aligned}\Pi_\phi^{\mathrm{tr}}(n,\mathcal{L}_1\mathcal{L}_2) &= \frac{\ell_1^2\ell_2^2}{(\ell_1^2-1)(\ell_2^2-1)(\ell_1-1)(\ell_2-1)} \cdot \frac{q^n}{n} \\ &\quad + \mathrm{O}_\phi\bigg(\ell_1^3\ell_2^3 q^{n/2} + \ell_1^3\ell_2^3\,\frac{q^{n/2}}{n}\log_q(\ell_1\ell_2)\bigg).\end{aligned} \tag{25}$$

Now we plug (22)–(25) into (18)–(21), respectively, and obtain

$$\begin{aligned}\sum_{\deg P=n} \omega(\mathbf{P}_{P,\phi}(1)) &= \sum_{\deg \mathcal{L}\le \delta n} \frac{\ell^2}{(\ell^2-1)(\ell-1)} \cdot \frac{q^n}{n} \\ &\quad + \sum_{\deg \mathcal{L}\le \delta n} \mathrm{O}_\phi\bigg(\ell^3 q^{n/2} + \ell^3\,\frac{q^{n/2}}{n}\log_q \ell\bigg) + \mathrm{O}\bigg(\frac{q^n}{n}\bigg) \\ &= \frac{q^n}{n} \sum_{k\le \delta n} \frac{q^{2k}}{(q^{2k}-1)(q^k-1)} \sum_{\deg \mathcal{L}=k} 1 \\ &\quad + \mathrm{O}_\phi\bigg(q^{n/2} \sum_{k\le \delta n} q^{3k} \sum_{\deg \mathcal{L}=k} 1 + \frac{q^{n/2}}{n} \sum_{k\le \delta n} q^{3k} \sum_{\deg \mathcal{L}=k} k\bigg) \\ &\quad + \mathrm{O}\bigg(\frac{q^n}{n}\bigg) \\ &= \frac{q^n}{n} \sum_{k\le \delta n} \frac{q^{2k}}{(q^{2k}-1)\,(q^k-1)} \bigg[\frac{q^k}{k} + \mathrm{O}(q^{k/2})\bigg] \\ &\quad + \mathrm{O}_\phi\bigg(q^{n/2} \sum_{k\le \delta n} q^{3k}\,\frac{q^k}{k} + \frac{q^{n/2}}{n} \sum_{k\le \delta n} q^{3k}\,\frac{q^k}{k}\,k\bigg) + \mathrm{O}\bigg(\frac{q^n}{n}\bigg) \\ &= \frac{q^n}{n} \sum_{k\le \delta n} \frac{q^{3k}}{k(q^{2k}-1)(q^k-1)} + \mathrm{O}\bigg(\frac{q^n}{n} \sum_{k\le \delta n} \frac{1}{q^{k/2}}\bigg) \\ &\quad + \mathrm{O}_\phi\bigg(q^{n/2} \sum_{k\le \delta n} \frac{q^{4k}}{k} + \frac{q^{n/2}}{n} \sum_{k\le \delta n} q^{4k}\bigg) + \mathrm{O}\bigg(\frac{q^n}{n}\bigg)\end{aligned}$$

$$= \frac{q^n}{n}\log(\delta n) + \mathrm{O}\bigg(\frac{q^n}{n}\sum_{k\le\delta n}\frac{1}{q^{k/2}}\bigg) + \mathrm{O}_\phi(q^{n/2+4\delta n}(\log(\delta n)+\delta)) + \mathrm{O}\bigg(\frac{q^n}{n}\bigg).$$

If we choose $\delta < 1/8$, then

$$\sum_{\deg P=n}\omega(\mathbf{P}_{P,\phi}(1)) = \frac{q^n}{n}\log n + \mathrm{O}_\phi\bigg(\frac{q^n}{n}\bigg). \tag{26}$$

Similarly,

$$\sum_{\deg P=n}{}'\,\omega(a_P(\phi)) = \frac{q^n}{n}\log n + \mathrm{O}\bigg(\frac{q^n}{n}\bigg). \tag{27}$$

Along the same lines, we obtain

$$\sum_{\deg P=n}\omega^2(\mathbf{P}_{P,\phi}(1)) = \frac{q^n}{n}(\log n)^2 + \mathrm{O}_\phi\bigg(q^n\,\frac{\log n}{n}\bigg), \tag{28}$$

$$\sum_{\deg P=n}{}'\,\omega^2(a_P(\phi)) = \frac{q^n}{n}(\log n)^2 + \mathrm{O}_\phi\bigg(q^n\,\frac{\log n}{n}\bigg), \tag{29}$$

this time provided that $\delta < 1/16$. Thus we choose

$$\delta < 1/16$$

and combine the above estimates to deduce

$$\sum_{\deg P=n}(\omega(\mathbf{P}_{P,\phi}(1)) - \log n)^2 \ll_\phi q^n\,\frac{\log n}{n},$$

$$\sum_{\deg P=n}{}'\,(\omega(a_P(\phi)) - \log n)^2 \ll_\phi q^n\,\frac{\log n}{n}.$$

We recall from [Da, Thm. 1.1, p. 330] that

$$\#\{P\in A : a_P(\phi)=0\} \ll_\phi \frac{q^{n(1-1/2(r^2+r))}}{n};$$

hence

$$\sum_{\deg P=n}(\omega(a_P(\phi)) - \log n)^2 \ll_\phi q^n\,\frac{\log n}{n}.$$

Finally, we have

$$\begin{aligned}
&\sum_{\deg P\le n} (\omega(\mathbf{P}_{P,\phi}(1)) - \log n)^2 \\
&\quad = \sum_{k\le n} \sum_{\deg P=k} (\omega(\mathbf{P}_{P,\phi}(1)) - \log k + \log k - \log n)^2 \\
&\quad \ll \sum_{k\le n} \sum_{\deg P=k} (\omega(\mathbf{P}_{P,\phi}(1)) - \log k)^2 + \sum_{k\le n} \sum_{\deg P=k} (\log k - \log n)^2 \\
&\quad \ll_\phi \sum_{k\le n} q^k \frac{\log k}{k} + \sum_{1\le k\le n/2} \sum_{\deg P=k} (\log n)^2 + \sum_{n/2<k\le n} \sum_{\deg P=k} (\log k - \log n)^2 \\
&\quad \ll_\phi \pi(n)\log n + (\log n)^2\pi(n/2) + \pi(n) \ll_\phi \pi(n)\log n,
\end{aligned}$$

where we used, once again, the prime number theorem (Thm. 8). Similarly,

$$\sum_{\deg P\le n} (\omega(a_P(\phi)) - \log n)^2 \ll_\phi \pi(n)\log n.$$

This completes the proof of Theorem 1 for rank 2 Drinfeld modules.

4.3. Drinfeld modules of rank ≥ 3. Let us consider the case when ϕ is a Drinfeld module of rank ≥ 3, with trivial endomorphism ring. This time we also assume the validity of the Mumford–Tate conjecture for ϕ.

As in the rank 2 case, we can use property (8) to reinterpret the divisibility conditions

$$\mathcal{L} \,|\, \mathbf{P}_{P,\phi}(1), \quad \mathcal{L}_1\mathcal{L}_2 \,|\, \mathbf{P}_{P,\phi}(1), \quad \mathcal{L} \,|\, a_P(\phi), \quad \mathcal{L}_1\mathcal{L}_2 \,|\, a_P(\phi)$$

as Chebotarev conditions. We introduce the notation

$$\begin{aligned}
C_{\mathcal{L}}^{\mathrm{char}} &:= \{g \in \operatorname{Im}\bar{\varrho}_{\mathcal{L}} : \operatorname{Char}_g(1) = 0\}, \\
C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{char}} &:= \{g \in \operatorname{Im}\bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2} : \operatorname{Char}_g(1) = 0\},
\end{aligned}$$

where $\operatorname{Char}_g(X)$ is the characteristic polynomial of g, and

$$C_{\mathcal{L}}^{\mathrm{tr}} := \{g \in \operatorname{Im}\bar{\varrho}_{\mathcal{L}} : \operatorname{tr} g = 0\}, \quad C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{tr}} := \{g \in \operatorname{Im}\bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2} : \operatorname{tr} g = 0\}.$$

Then:

$$\Pi_\phi^{\mathrm{char}}(n,\mathcal{L}) = \frac{|C_{\mathcal{L}}^{\mathrm{char}}|}{|\operatorname{Im}\bar{\varrho}_{\mathcal{L}}|}\cdot\frac{q^n}{n} + \mathrm{O}_\phi\Big(|C_{\mathcal{L}}^{\mathrm{char}}|q^{n/2} + |C_{\mathcal{L}}^{\mathrm{char}}|\,\frac{q^{n/2}}{n}\deg\mathcal{L}\Big), \tag{30}$$

$$\begin{aligned}
\Pi_\phi^{\mathrm{char}}(n,\mathcal{L}_1\mathcal{L}_2) &= \frac{|C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{char}}|}{|\operatorname{Im}\bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2}|}\cdot\frac{q^n}{n} \\
&\quad + \mathrm{O}_\phi\Big(|C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{char}}|q^{n/2} + |C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{char}}|\,\frac{q^{n/2}}{n}\deg(\mathcal{L}_1\mathcal{L}_2)\Big),
\end{aligned} \tag{31}$$

$$\Pi_\phi^{\mathrm{tr}}(n,\mathcal{L}) = \frac{|C_{\mathcal{L}}^{\mathrm{tr}}|}{|\mathrm{Im}\,\bar{\varrho}_{\mathcal{L}}|}\cdot\frac{q^n}{n} + \mathrm{O}_\phi\bigg(|C_{\mathcal{L}}^{\mathrm{tr}}|q^{n/2} + |C_{\mathcal{L}}^{\mathrm{tr}}|\,\frac{q^{n/2}}{n}\deg\mathcal{L}\bigg), \tag{32}$$

$$\begin{aligned}\Pi_\phi^{\mathrm{tr}}(n,\mathcal{L}_1\mathcal{L}_2) &= \frac{|C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{tr}}|}{|\mathrm{Im}\,\bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2}|}\cdot\frac{q^n}{n}\\ &\quad + \mathrm{O}_\phi\bigg(|C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{tr}}|q^{n/2} + |C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{tr}}|\,\frac{q^{n/2}}{n}\deg(\mathcal{L}_1\mathcal{L}_2)\bigg).\end{aligned} \tag{33}$$

Now we need precise formulae for the quantities

$$\frac{|C_{\mathcal{L}}^{\mathrm{char}}|}{|\mathrm{Im}\,\bar{\varrho}_{\mathcal{L}}|},\quad \frac{|C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{char}}|}{|\mathrm{Im}\,\bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2}|},\quad \frac{|C_{\mathcal{L}}^{\mathrm{tr}}|}{|\mathrm{Im}\,\bar{\varrho}_{\mathcal{L}}|},\quad \frac{|C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{tr}}|}{|\mathrm{Im}\,\bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2}|}.$$

We have (see Appendix for proofs of more precise formulae):

$$\frac{|C_{\mathcal{L}}^{\mathrm{char}}|}{|\mathrm{Im}\,\bar{\varrho}_{\mathcal{L}}|} = \frac{1}{\ell} + \mathrm{O}\bigg(\frac{1}{\ell^2}\bigg),\qquad \frac{C_{\mathcal{L}}^{\mathrm{tr}}}{|\mathrm{Im}\,\bar{\varrho}_{\mathcal{L}}|} = \frac{1}{\ell} + \mathrm{O}\bigg(\frac{1}{\ell^2}\bigg),$$

$$\frac{|C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{char}}|}{|\mathrm{Im}\,\bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2}|} = \frac{1}{\ell_1\ell_2} + \mathrm{O}\bigg(\frac{1}{\ell_1^2\ell_2^2}\bigg),\qquad \frac{|C_{\mathcal{L}_1\mathcal{L}_2}^{\mathrm{tr}}|}{|\mathrm{Im}\,\bar{\varrho}_{\mathcal{L}_1\mathcal{L}_2}|} = \frac{1}{\ell_1\ell_2} + \mathrm{O}\bigg(\frac{1}{\ell_1^2\ell_2^2}\bigg),$$

with absolute O-constants. Therefore

$$\begin{aligned}\Pi_\phi^{\mathrm{char}}(n,\mathcal{L}) &= \frac{1}{\ell}\cdot\frac{q^n}{n} + \mathrm{O}\bigg(\frac{1}{\ell^2}\cdot\frac{q^n}{n}\bigg)\\ &\quad + \mathrm{O}_\phi\bigg(\ell^{r^2-1}q^{n/2} + \ell^{r^2-1}\,\frac{q^{n/2}}{n}\log_q\ell\bigg),\\ \Pi_\phi^{\mathrm{char}}(n,\mathcal{L}_1\mathcal{L}_2) &= \frac{1}{\ell_1\ell_2}\cdot\frac{q^n}{n} + \mathrm{O}\bigg(\frac{1}{\ell_1^2\ell_2^2}\cdot\frac{q^n}{n}\bigg)\\ &\quad + \mathrm{O}_\phi\bigg(\ell_1^{r^2-1}\ell_2^{r^2-1}q^{n/2} + \ell_1^{r^2-1}\ell_2^{r^2-1}\,\frac{q^{n/2}}{n}\log_q(\ell_1\ell_2)\bigg),\\ \Pi_\phi^{\mathrm{tr}}(n,\mathcal{L}) &= \frac{1}{\ell}\cdot\frac{q^n}{n} + \mathrm{O}\bigg(\frac{1}{\ell^2}\cdot\frac{q^n}{n}\bigg)\\ &\quad + \mathrm{O}_\phi\bigg(\ell^{r^2-1}q^{n/2} + \ell^{r^2-1}\,\frac{q^{n/2}}{n}\log_q\ell\bigg),\\ \Pi_\phi^{\mathrm{tr}}(n,\mathcal{L}_1\mathcal{L}_2) &= \frac{1}{\ell_1\ell_2}\cdot\frac{q^n}{n} + \mathrm{O}\bigg(\frac{1}{\ell_1^2\ell_2^2}\cdot\frac{q^n}{n}\bigg)\\ &\quad + \mathrm{O}_\phi\bigg(\ell_1^{r^2-1}\ell_2^{r^2-1}q^{n/2} + \ell_1^{r^2-1}\ell_2^{r^2-1}\,\frac{q^{n/2}}{n}\log_q(\ell_1\ell_2)\bigg).\end{aligned}$$

Proceeding as in Section 4.2, we obtain

$$\sum_{\deg P=n}\omega(\mathbf{P}_{P,\phi}(1)) = \frac{q^n}{n}\log n + \mathrm{O}_\phi\bigg(\frac{q^n}{n}\bigg),$$

$$\sum_{\deg P=n}{}' \omega(a_P(\phi)) = \frac{q^n}{n}\log n + \mathrm{O}_\phi\Big(\frac{q^n}{n}\Big),$$

$$\sum_{\deg P=n} \omega^2(\mathbf{P}_{P,\phi}(1)) = \frac{q^n}{n}(\log n)^2 + \mathrm{O}_\phi\Big(\frac{q^n\log n}{n}\Big),$$

$$\sum_{\deg P=n}{}' \omega^2(a_P(\phi)) = \frac{q^n}{n}(\log n)^2 + \mathrm{O}_\phi\Big(\frac{q^n\log n}{n}\Big),$$

provided that

$$\delta < \frac{1}{4r^2}$$

and under the assumption that the Mumford–Tate conjecture holds for ϕ. Again as in Section 4.2, the above estimates lead to

$$\sum_{\deg P\le n} (\omega(\mathbf{P}_{P,\phi}(1)) - \log n)^2 \ll_\phi q^n \frac{\log n}{n},$$

$$\sum_{\deg P\le n} (\omega(a_P(\phi)) - \log n)^2 \ll_\phi q^n \frac{\log n}{n}.$$

This completes the proof of Theorem 1. ∎

Remark 11. The Mumford–Tate conjecture is too strong an assumption for what is needed in our proof. Instead, we could only assume the average estimates

$$\sum_{\deg \mathcal{L}\le \delta n} \frac{|C^{\mathrm{char}}_{\mathcal{L}}|}{|\mathrm{Im}\,\bar\varrho_{\mathcal{L}}|} = \frac{q^n}{n}\log n + \mathrm{O}\Big(\frac{q^n}{n}\Big),$$

$$\sum_{\substack{\mathcal{L}_1\ne\mathcal{L}_2\\ \deg\mathcal{L}_1,\deg\mathcal{L}_2\le\delta n}} \frac{|C^{\mathrm{char}}_{\mathcal{L}_1\mathcal{L}_2}|}{|\mathrm{Im}\,\bar\varrho_{\mathcal{L}_1\mathcal{L}_2}|} = \frac{q^n}{n}(\log n)^2 + \mathrm{O}\Big(\frac{q^n\log n}{n}\Big)$$

and their analogues for the trace problem, where $\delta < 1/4r^2$.

5. PROOF OF THEOREM 3

The proof of Theorem 3 is a consequence of a general result due to Liu and of the applications of the Chebotarev density theorem to the division fields of the Drinfeld module ϕ. We recall Liu's general result below:

Theorem 12 (Liu [Li2, Thm. 3, p. 328]). *Let $A = \mathbb{F}_q[T]$, $F = \mathbb{F}_q(T)$, as before. Let $S \subseteq F$ be a subset such that, for any positive integer n,*

$$\#\{\mathfrak{f}\in S : \deg\mathfrak{f}\le n/2\} = \mathrm{o}(\#\{\mathfrak{f}\in S : \deg\mathfrak{f}\le n\}).$$

Let $h : S \to A$ be a map and let $\mathcal{L}, \mathcal{L}_1, \dots, \mathcal{L}_u \in A$ denote mutually distinct

monic irreducible polynomials. For a positive integer n, write

$$\frac{\#\{\mathfrak{f} \in S : \deg \mathfrak{f} \le n, h(\mathfrak{f}) \equiv 0 \pmod{\mathcal{L}}\}}{\#\{\mathfrak{f} \in S : \deg \mathfrak{f} \le n\}} = \lambda_{\mathcal{L}} + e_{\mathcal{L}}(n),$$

$$\frac{\#\{\mathfrak{f} \in S : \deg \mathfrak{f} \le n, h(\mathfrak{f}) \equiv 0 \pmod{\mathcal{L}_1 \dots \mathcal{L}_u}\}}{\#\{\mathfrak{f} \in S : \deg \mathfrak{f} \le n\}} = \lambda_{\mathcal{L}_1 \dots \mathcal{L}_u} + e_{\mathcal{L}_1 \dots \mathcal{L}_u}(n)$$

for some $\lambda_{\mathcal{L}}, \lambda_{\mathcal{L}_1 \dots \mathcal{L}_u}$ and $e_{\mathcal{L}}(n), e_{\mathcal{L}_1 \dots \mathcal{L}_u}(n)$. Assume that for every positive integer n there exist a constant $0 < \beta \le 1$ and a positive integer $m < n\beta$ such that the following conditions hold:

(i) *for all $\mathfrak{f} \in S$ with $\deg \mathfrak{f} \le n$,*

$$\#\{\mathcal{L} \in A : \deg \mathcal{L} > n\beta,\ h(\mathfrak{f}) \equiv 0 \pmod{\mathcal{L}}\} = \mathrm{O}(1);$$

(ii) $$\sum_{\substack{\mathcal{L} \in A \\ m < \deg \mathcal{L} \le n\beta}} \lambda_{\mathcal{L}} = \mathrm{o}((\log\log q^n)^{1/2});$$

(iii) $$\sum_{\substack{\mathcal{L} \in A \\ m < \deg \mathcal{L} \le n\beta}} |e_{\mathcal{L}}(n)| = \mathrm{o}((\log\log q^n)^{1/2});$$

(iv) $$\sum_{\substack{\mathcal{L} \in A \\ \deg \mathcal{L} \le m}} \lambda_{\mathcal{L}} = \log\log q^n + \mathrm{o}((\log\log q^n)^{1/2});$$

(v) $$\sum_{\substack{\mathcal{L} \in A \\ \deg \mathcal{L} \le m}} \lambda_{\mathcal{L}}^2 = \mathrm{o}((\log\log q^n)^{1/2});$$

(vi) *for any positive integer R,*

$$\sum_{\substack{\mathcal{L}_1, \dots, \mathcal{L}_u \in A \\ \deg \mathcal{L}_1 \le m, \dots, \deg \mathcal{L}_u \le m}} |e_{\mathcal{L}_1 \dots \mathcal{L}_u}(n)| = \mathrm{o}((\log\log q^n)^{-R/2}),$$

where the sum runs over all u-tuples $(\mathcal{L}_1, \dots, \mathcal{L}_u)$ with $u = 1, \dots, R$.

Then, for $\alpha < \beta$, we have

$$\#\left\{\mathfrak{f} \in S : \deg \mathfrak{f} \le n,\ \alpha \le \frac{\omega(h(\mathfrak{f})) - \log\log|\mathfrak{f}|_\infty}{\sqrt{\log\log|\mathfrak{f}|_\infty}} \le \beta\right\} \sim \Phi(\alpha, \beta)\#\{\mathfrak{f} \in S : \deg \mathfrak{f} \le n\}$$

as $n \to \infty$.

Now let ϕ be a rank r Drinfeld A-module over F, with $\mathrm{End}_{\overline{F}}(\phi) \simeq A$. If $r \ge 3$, assume the Mumford–Tate conjecture for ϕ. We apply the above general result to the set S consisting of monic irreducible polynomials $P \in A$ and the maps

$$h^{\mathrm{char}} : S \to A, \quad h^{\mathrm{char}}(P) = \mathbf{P}_{P,\phi}(1), \qquad h^{\mathrm{tr}} : S \to A, \quad h^{\mathrm{tr}}(P) = a_P(\phi).$$

From Corollary 10 and calculations similar to those made in Section 4.3, we see that

$$\begin{aligned}
\lambda_{\mathcal{L}}^{\mathrm{char}} &= \frac{1}{\ell}, \qquad \lambda_{\mathcal{L}_1\dots\mathcal{L}_u}^{\mathrm{char}} = \frac{1}{\ell_1\dots\ell_u},\\
e_{\mathcal{L}}^{\mathrm{char}}(n) &= \mathrm{O}\Big(\frac{1}{\ell^2}\Big) + \mathrm{O}_\phi\Big(\ell^{r^2-1}\,\frac{n}{q^{n/2}} + \ell^{r^2-1}\,\frac{1}{q^{n/2}}\log_q \ell\Big),\\
e_{\mathcal{L}_1\dots\mathcal{L}_u}^{\mathrm{char}}(n) &= \mathrm{O}\Big(\frac{1}{\ell_1^2\dots\ell_u^2}\Big)\\
&\quad + \mathrm{O}_\phi\Big(\ell_1^{r^2-1}\dots\ell_u^{r^2-1}\frac{n}{q^{n/2}} + \ell_1^{r^2-1}\dots\ell_u^{r^2-1}\,\frac{1}{q^{n/2}}\log_q(\ell_1\dots\ell_u)\Big),
\end{aligned}$$

and similarly,

$$\begin{aligned}
\lambda_{\mathcal{L}}^{\mathrm{tr}} &= \frac{1}{\ell}, \qquad \lambda_{\mathcal{L}_1\dots\mathcal{L}_u}^{\mathrm{tr}} = \frac{1}{\ell_1\dots\ell_u},\\
e_{\mathcal{L}}^{\mathrm{tr}}(n) &= \mathrm{O}\Big(\frac{1}{\ell^2}\Big) + \mathrm{O}_\phi\Big(\ell^{r^2-1}\,\frac{n}{q^{n/2}} + \ell^{r^2-1}\,\frac{1}{q^{n/2}}\log_q \ell\Big),\\
e_{\mathcal{L}_1\dots\mathcal{L}_u}^{\mathrm{tr}}(n) &= \mathrm{O}\Big(\frac{1}{\ell_1^2\dots\ell_u^2}\Big)\\
&\quad + \mathrm{O}_\phi\Big(\ell_1^{r^2-1}\dots\ell_u^{r^2-1}\,\frac{n}{q^{n/2}} + \ell_1^{r^2-1}\dots\ell_u^{r^2-1}\,\frac{1}{q^{n/2}}\log_q(\ell_1\dots\ell_u)\Big),
\end{aligned}$$

where $\ell := |\mathcal{L}|_\infty$, $\ell_1 := |\mathcal{L}_1|_\infty, \dots, \ell_u := |\mathcal{L}_u|_\infty$.

What remains to be done is the verification of the hypotheses of Theorem 12 in these two settings. We will only do it for h^{char}, as the situation for h^{tr} is the same.

By the prime number theorem (Thm. 8), the condition on the set S is satisfied. To verify conditions (i)–(vi), let n be a fixed positive integer and let

$$\beta < \frac{1}{2r^2} \quad \text{and} \quad m := \frac{n}{\log\log q^n}.$$

Condition (i) is an immediate consequence of the remark that if $P \in A$ satisfies $\deg P \le n$, then $\deg h^{\mathrm{char}}(P) \le n/r$, where we are using the important result that the roots of $\mathbf{P}_{P,\phi}$ have absolute value $|P|_\infty^{1/r}$.

To verify conditions (ii), (iv) and (v) we make use of the estimates

$$\sum_{\substack{\mathcal{L}\in A\\ \deg\mathcal{L}\le n}} \frac{1}{\ell} = \log\log q^n + \mathrm{O}(1), \qquad \sum_{\substack{\mathcal{L}\in A\\ \deg\mathcal{L}\le n}} \frac{1}{\ell^2} = \mathrm{O}(1),$$

obtained in [Li1, Lem. 1, 2, p. 575].

To verify condition (iii) we make use of the above and of our choice of β:

$$\begin{aligned}\sum_{\substack{\mathcal{L}\in A\\ m<\deg\mathcal{L}\le n\beta}} |e_{\mathcal{L}}^{\mathrm{char}}(n)| &\ll_\phi \frac{n}{q^{n/2}} \sum_{m<k\le n\beta} \sum_{\substack{\mathcal{L}\in A\\ \deg\mathcal{L}=k}} q^{k(r^2-1)}\\ &\quad + \frac{1}{q^{n/2}} \sum_{m<k\le n\beta} \sum_{\substack{\mathcal{L}\in A\\ \deg\mathcal{L}=k}} kq^{k(r^2-1)}\\ &\ll_\phi \frac{n}{q^{n/2}}\, q^{r^2 n\beta} \log\frac{n\beta}{m} + \frac{1}{q^{n/2}}\, q^{r^2 n\beta} n\beta\\ &= \mathrm{o}((\log\log q^n)^{1/2}).\end{aligned}$$

To verify condition (vi) we proceed as above and make use of our choice of m. This completes the proof of Theorem 3. ∎

6. CONCLUDING REMARKS

As already clear from [MuMu], the higher-dimensional analogues of the Erdős and Halberstam theorems, in both the rational and function field cases, may be interpreted as results about compatible systems of Galois representations. As such, one could prove similar results for abelian varieties (under suitable hypotheses, such as the generalized Riemann hypothesis and an open image conjecture, for the cases when this is not known) [nb. Drinfeld modules are function field analogues only of elliptic curves, not also of higher-dimensional abelian varieties]. As illustrated in [MuMu, Section 6], one could then use these results to obtain non-trivial lower bounds for $\mathbf{P}_{P,\phi}(1), a_P(\phi)$ and their other analogues. We relegate this work to future projects.

7. APPENDIX: ENUMERATION OF MATRICES
by Hugh Thomas

Fix a prime power q and a positive integer n. We consider the problems of counting matrices $A \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $\mathrm{Char}_A(1) = 0$, where Char_A is the characteristic polynomial of A, and of counting matrices $A \in \mathrm{GL}_n(\mathbb{F}_q)$ with $\mathrm{tr}\, A = 0$.

We will write g_n for $|\mathrm{GL}_n(\mathbb{F}_q)|$. We recall the well-known formula

$$g_n = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}).$$

The terms in the product count the number of ways of selecting a first non-zero column, a second non-zero column linearly independent from the first, etc.

7.1. The $\mathrm{Char}_A(1) = 0$ condition

PROPOSITION 13. *The number of invertible $n \times n$ matrices A over $\mathbb{F}_q$ satisfying $\mathrm{Char}_A(1) = 0$ is*

$$\left(\frac{1}{q-1} - \frac{1}{(q^2-1)(q-1)} + \frac{1}{(q^3-1)(q^2-1)(q-1)} + \cdots + \frac{(-1)^{n-1}}{(q^n-1)\cdots(q-1)}\right) g_n.$$

Proof. The condition that $\mathrm{Char}_A(1) = 0$ is equivalent to requiring that A has an eigenvector with eigenvalue 1. We will perform our counting of such matrices by means of an inclusion-exclusion argument. Let us write P_A for the 1-eigenspace of A.

Consider the number of ways to choose $A \in \mathrm{GL}_n(\mathbb{F}_q)$ together with a specified 1-dimensional 1-eigenspace. We can count this by choosing an eigenvector v in $q^n - 1$ ways, and forgetting the scalar multiple by dividing by $q - 1$. Now, with respect to some fixed basis $y_1, \ldots, y_{n-1}$ that does not include v, the matrix consists of an invertible $(n-1) \times (n-1)$ matrix (on the y_i) together with $n - 1$ matrix entries which are free, representing the component of v in Ay_i.

Thus, the number of choices is

$$\frac{(q^n-1)q^{n-1}}{q-1}\, g_{n-1} = \frac{g_n}{q-1}.$$

However, this has overcounted matrices A with $\dim_{\mathbb{F}_q} P_A > 1$.

Let us correct our count to consider properly those matrices for which $\dim_{\mathbb{F}_q} P_A = 2$. The number of such matrices is given by choosing a 2-dimensional subspace (the eigenspace), and then filling in the rest of the matrix. By an argument like the previous one, the number of such matrices is

$$\frac{(q^n-1)(q^n-q)}{(q^2-1)(q^2-q)}\, q^{2(n-2)} g_{n-2}.$$

Here the fraction counts the 2-dimensional subspaces (which we count by choosing a basis and then forgetting which basis we chose).

How many times was such a matrix counted in our original counting? Once for each linear subspace in the 2-dimensional subspace. We want to count it only once. Thus the correction factor is

$$1 - \frac{q^2-1}{q-1} = -q.$$

Thus the correction to the sum is

$$\frac{(q^n-1)(q^n-q)}{(q^2-1)(q^2-q)}\, q^{2(n-2)} g_{n-2}\left(1 - \frac{q^2-1}{q-1}\right) = \frac{-g_n}{(q^2-1)(q-1)}.$$

Now we will make an induction argument as to how many times we will have over- or under-counted the invertible matrices A with $\dim_{\mathbb{F}_q} P_A = k$, after we have correctly counted the matrices with $\dim_{\mathbb{F}_q} P_A < k$. Our induction claim is that we should add in the matrices A satisfying $\dim_{\mathbb{F}_q} P_A = k$ with multiplicity $(-1)^{k-1}q^{\binom{k}{2}}$.

As we have already seen, this is correct for $k = 1$ and $k = 2$. Assume it is true up to $k-1$, and let A be an invertible matrix with $\dim_{\mathbb{F}_q} P_A = k$. How many times has it been counted? At the dimension 1 stage, it was counted $(q^k - 1)/(q - 1)$ times. At the dimension 2 stage, it was subtracted off $q(q^k - 1)(q^{k-1} - 1)/(q^2 - 1)(q - 1)$ times (not forgetting the fact that we counted each occurrence with multiplicity q). In total, the multiplicity with which we have counted A is

$$\frac{q^k - 1}{q - 1} - q\,\frac{(q^k - 1)(q^{k-1} - 1)}{(q^2 - 1)(q - 1)} + \cdots + (-1)^{k-1}q^{\binom{k-1}{2}}\,\frac{(q^k - 1)\cdots(q^2 - 1)}{(q^{k-1} - 1)\cdots(q - 1)}.$$

We want to count A exactly once; the correction term is then $(-1)^{k-1}q^{\binom{k}{2}}$. This follows from substituting $z = 1$ into [GoJa, Identity 2.6.12(1)]:

$$\prod_{i=0}^{k-1}(z - q^i) = \sum_{i=0}^{k}(-1)^i\,\frac{(q^k - 1)(q^{k-1} - 1)\cdots(q^{k-i+1} - 1)}{(q^i - 1)(q^{i-1} - 1)\cdots(q - 1)}\,q^{\binom{i}{2}}z^{k-i}.$$

This proves the proposition. ∎

7.2. The $\operatorname{tr} A = 0$ condition. Let f_n be the number of matrices in $\mathrm{GL}_n(\mathbb{F}_q)$ which have trace zero. We prove that:

Proposition 14. *The numbers f_n satisfy the following recursion for $n \geq 2$:*

$$f_n = q^{n-1}(q^n - q)\cdots(q^n - q^{n-1}) - q^{n-1}f_{n-1}.$$

Plugging the upper bound on f_{n-1} provided by the proposition back into the proposition, we obtain the following approximation for f_n:

Corollary 15.

$$f_n = q^{n-1}(q^n - q)\cdots(q^n - q^{n-1}) + \mathrm{O}(q^{n^2-n-1}).$$

Proof. We are going to count invertible matrices $A = (a_{ij})$ satisfying the trace condition. Start by choosing the first $n - 1$ columns of A. We distinguish two cases. The first case is the very special case in which the last entry of each of these columns is zero; otherwise, we are in the second case.

In the first case, choosing the first $n - 1$ columns of A really amounted to choosing an invertible $(n-1) \times (n-1)$ matrix, so there are g_{n-1} ways to do this. Now consider the final column. The invertibility condition precisely amounts to the condition that $a_{nn} \neq 0$. The trace condition determines a_{nn}. It will be possible to satisfy both conditions precisely if the trace of

the principal $(n-1)\times(n-1)$ minor is non-zero. The number of invertible $(n-1)\times(n-1)$ matrices with non-zero trace is $g_{n-1}-f_{n-1}$. We now fill in the rest of the final column, which is arbitrary, and can therefore be done in q^{n-1} ways. Thus, the first case contributes $q^{n-1}(g_{n-1}-f_{n-1})$.

In the second case, the number of ways to choose the first $n-1$ columns is $(q^n-1)\cdots(q^n-q^{n-2})-g_{n-1}$. Here, the invertibility condition requires precisely that the final column does not lie in some hyperplane H (that spanned by the other columns), and this hyperplane is not parallel to the hyperplane $a_{nn}=-\sum_{i=1}^{n-1}a_{ii}$. Thus, the locus satisfying both the trace condition and the invertibility condition consists of the points on a hyperplane in $(\mathbb{F}_q)^n$ avoiding a hyperplane within that hyperplane. There are $q^{n-2}(q-1)$ such points. The proposition follows by adding together the contributions from the two cases. ∎

Acknowledgments. We would like to thank Nantel Bergeron for his contributions to the initial discussions surrounding the work contained in the Appendix. We would also like to thank the Fields Institute (Toronto) and MSRI (Berkeley), where some of this work was carried out, for their hospitality.

References

[Co] A. C. Cojocaru, *Reductions of an elliptic curve with almost prime orders*, Acta Arith. 119 (2005), 265–289.

[CoDa] A. C. Cojocaru and C. David, *Frobenius fields for Drinfeld modules of rank* 2, Compos. Math., to appear.

[Da] C. David, *Frobenius distributions of Drinfeld modules of any rank*, J. Number Theory 90 (2001), 329–340.

[Dr1] V. G. Drinfeld [V. G. Drinfel'd], *Elliptic modules I*, Mat. Sb. 94 (1974), 594–627 (in Russian); English transl.: Math. USSR-Sb. 23 (1974), 561–592.

[Dr2] —, *Elliptic modules II*, ibid. 102 (1977), 182–194 (in Russian); English transl.: ibid. 31 (1977), 159–170.

[El] P. D. T. A. Elliott, *Probabilistic Number Theory I, II*, Springer, New York, 1979.

[Er] P. Erdős, *On the normal number of prime factors of* $p-1$ *and some related problems concerning Euler's* φ*-function*, Quart. J. Math. Oxford Ser. 6 (1935), 205–213.

[ErKa] P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. 62 (1940), 738–742.

[FrJa] M. Fried and M. Jarden, *Field Arithmetic*, Springer, New York, 1986.

[Ga1] F. Gardeyn, *t-Motives and Galois representations*, PhD thesis, 2001.

[Ga2] —, *Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld*, Arch. Math. (Basel) 79 (2002), 241–251.

[Ge1] E.-U. Gekeler, *Zur Arithmetik von Drinfeld-Moduln*, Math. Ann. 262 (1983), 167–182.

[Ge2] —, *On finite Drinfeld modules*, J. Algebra 141 (1991), 187–203.

[Go] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergeb. Math. Grenzgeb. 35, Springer, Berlin, 1996.

[GoJa] I. Goulden and D. Jackson, *Combinatorial Enumeration*, Wiley, New York, 1983.

[Hal] H. Halberstam, *On the distribution of additive number-theoretic functions I*, J. London Math. Soc. 30 (1955), 43–53.

[HaRa] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. 48 (1917), 76–92.

[Hay] D. Hayes, *A brief introduction to Drinfeld modules*, in: The Arithmetic of Function Fields, D. Goss *et al.* (eds.), de Gruyter, Berlin, 1992, 1–32.

[Li1] Y.-R. Liu, *A generalization of the Turán theorem and its applications*, Canad. Math. Bull. 47 (2004), 573–588.

[Li2] —, *The Erdős theorem and the Halberstam theorem in function fields*, Acta Arith. 114 (2004), 323–330.

[MiMu] S. A. Miri and V. K. Murty, *An application of sieve methods to elliptic curves*, in: Progress in Cryptology—Indocrypt 2001, Lecture Notes in Comput. Sci. 2247, Springer, Berlin, 2001, 91–98.

[MuMu] M. R. Murty and V. K. Murty, *Prime divisors of Fourier coefficients of modular forms*, Duke Math. J. 51 (1984), 57–76.

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

[Ro] M. Rosen, *Number Theory in Function Fields*, Grad. Texts in Math. 201, Springer, New York, 2002.

[Sa] F. Saidak, *An elementary proof of a theorem of Delange*, C. R. Math. Acad. Sci. Soc. R. Can. 24 (2002), 144–151.

[Tu] P. Turán, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. 9 (1934), 274–276.

Department of Mathematics, Statistics
and Computer Science
University of Illinois at Chicago
322 SEO, 851 S. Morgan Street
Chicago, IL 60607-7045, U.S.A.
E-mail: cojocaru@math.uic.edu
and
Institute of Mathematics
Romanian Academy
Calea Grivitei 21
010702, Bucharest, Romania

Department of Mathematics and Statistics
University of New Brunswick
Fredericton, NB Canada E3B 5A3
E-mail: hugh@math.unb.ca

Received on 17.8.2006
and in revised form on 16.10.2007 (5261)