ARTIN'S CONJECTURE FOR DRINFELD MODULES

WENTANG KUO AND DAVID TWEEDLE

Abstract. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of rank 2 with generic characteristic, and suppose that the endomorphism ring of ϕ induces a Drinfeld module $\psi : B \to K\{\tau\}$ of rank 1. Let $a \in K$. We prove that the set of places $\wp$ of K for which a generates $\phi(\mathbb{F}_\wp)$ as an A-module has a density. Furthermore, we show that this density is positive unless there is a good reason.

We also revisit Artin's problem for Drinfeld modules of rank 1, first considered by Hsu and Yu. A key point is that our methods do not require that A be a principal ideal domain. We are also able to generalize a Brun-Titchmarsh theorem for function fields proved by Hsu.

1. Introduction

Let $a \in \mathbb{Z}$ and let p be a prime. Denote the residue class of a modulo p by $\overline{a}$. We say that a is a primitive root modulo p if $\overline{a}$ generates the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. A conjecture of Artin states that if $a \neq 0, \pm 1$ or any perfect square, then the density of primes for which a is a primitive root is positive. In this introduction, we want to give an overview of the results in this area. We wish to show that our results naturally arise when thinking of Artin's conjecture.

We use the notation that if X is a finite set then $|X|$ is the number of elements of X.

In 1967, Hooley [Hoo67, Theorem, p. 219] proved that if a is not equal to $0, \pm 1$ or any perfect square, then the density of primes for which a is a primitive root is positive conditional on the generalized Riemann hypothesis. Bilharz solved an analogous problem for function fields in [Bil37], thirty years prior to Hooley. His thesis showed, conditional on the Riemann Hypothesis for function fields later proved by Weil, that if K is a function field with constant field $\mathbb{F}_q$ and a is a non-zero, geometric element of K which is not an l-th power for any prime divisor l of $q-1$ then a is a primitive root modulo P for infinitely many primes P of K. Not everything is perfect when we translate to the world of function fields – in Bilharz's result a Dirichlet density is obtained.

We see that by replacing $\mathbb{Q}$ with a function field, we can sometimes obtain unconditional results which can be compared to the conditional results in the classical setting. We do not have to stop with replacing the field $\mathbb{Q}$ with a function field K, we can also replace the multiplicative structure of $\mathbb{Q}$ with other structures. By replacing the structure of the rationals with other nice structures over global fields, we can ask new questions.

We can replace rational numbers under multiplication with an elliptic curve E defined over $\mathbb{Q}$ and replace $a \in \mathbb{Q}^\times$ with a point $a \in E(\mathbb{Q})$. Let E be an elliptic curve defined over $\mathbb{Q}$ and $a \in E(\mathbb{Q})$ be a point of infinite order.

2010 *Mathematics Subject Classification.* 11G09 (primary), and 11G15, 11R45 (secondary).
The research of the first author was supported by an NSERC discovery grant.

Definition 1.1. The point $a \in E(\mathbb{Q})$ is a primitive point for E modulo p if E has good reduction at p and the residue of a in E modulo p generates the finite group E modulo p.

Lang and Trotter conjectured that there is a density of primes p for which a is a primitive point modulo p, and that this density can be seen to be positive under certain conditions.

Gupta and Murty were able to gain traction on this problem by assuming that E has complex multiplication by the full ring of integers $\mathcal{O}_L$ in an imaginary quadratic extension $L/\mathbb{Q}$. As E is defined over $\mathbb{Q}$, the class number of $\mathcal{O}_L$ is 1.

The prime counting function $M_a(x)$ is defined to be the number of primes $p \leq x$, such that p splits in L, and a is a primitive point modulo p.

Theorem 1.2 ([GM86, Theorem 1])**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by the ring of integers in a quadratic imaginary extension L of $\mathbb{Q}$. Let $a \in E(\mathbb{Q})$ be a point of infinite order. Assuming the generalized Riemann hypothesis, we have the estimate*

$$M_a(x) = C_E(a)\,\mathrm{li}(x) + \mathbf{O}\left(\frac{x \log\log x}{(\log x)^2}\right) \text{ as } x \to \infty,$$

and $C_E(a) > 0$ if 2 and 3 are inert in L or $L = \mathbb{Q}(\sqrt{-11})$.

So far the literature can treat the classical case under GRH, the case of elliptic curves under certain special conditions and the GRH, and the function field analogue unconditionally. Furthermore, if we only require infinitely many primes (instead of a set of primes of positive density), then there are some unconditional results available.

There are still more questions that we can consider. We can replace the structure of an elliptic curve or the rational numbers by the structure of a function field given by a Drinfeld module ϕ. Briefly, a Drinfeld module ϕ equips a function field with a non-trivial A-module structure, where A is the subset of the function field regular outside of a fixed place. If one thinks of an elliptic curve as equipping its rational points with the structure of a $\mathbb{Z}$-module, then the similarities are especially striking.

By considering Drinfeld modules of rank 1, Hsu [Hsu97, Theorem 4.6], and later, Hsu and Yu [HY01, Theorem 4.6] proved Drinfeld module analogues of Hooley's original result. To give some more perspective, we now state Hsu and Yu's result.

Theorem 1.3 ([HY01, Theorem 4.6])**.** *Let k be a global function field with constant field $\mathbb{F}_r$, ∞ a place of k of degree 1, and A the ring of elements of k regular everywhere except possibly ∞. Let H be the Hilbert class field of A, O the integral closure of A in H. Fix a sign function* $\mathrm{sgn} : k_\infty^* \to \mathbb{F}_r^*$*. Let $\psi : A \to O\{\tau\}$ be a* sgn*-normalized Drinfeld module of rank 1. Let $0 \neq a \in O$. Suppose that $r \neq 2$. Let $N_a(x)$ denote the number of primes $\mathfrak{p}$ of O of degree x for which $a + \mathfrak{p}$ generates $O/\mathfrak{p}$ as an A-module (the A-structure coming from the reduction of ψ). Then $N_a(x) = \delta_a r^x/x + \mathbf{o}(r^x/x)$ and furthermore, $\delta_a \neq 0$ is given by an Euler product.*

Notice that this result assumes that the degree of the point at infinity is 1, that the A-field is the Hilbert class field of A, and that the Drinfeld module is sign-normalized. We will prove a Drinfeld module analogue to Gupta and Murty's result, or if you wish, a rank 2 analogue of Hsu and Yu's result. Our result is

analogous to both Gupta and Murty's result and Hsu and Yu's result, but in order to get our results we need to express the Lang-Trotter condition in terms that are tractable for rings which are not principal ideal domains. The arguments in both Gupta and Murty's paper and Hsu and Yu's paper will not work for non-principal ideal domains. As a corollary of our proof, one can conclude Artin's conjecture for rank 1 Drinfeld modules $\psi : B \to K\{\tau\}$ where K is any finite extension of k and a is any non-torsion element of K for which the division fields $K(\mathfrak{q}^{-1}\langle a\rangle) =: L_{\mathfrak{q}}^{a} \neq K$ for every prime ideal $\mathfrak{q}$ of B. This seems to be about the strongest type of result one can expect in this generality.

Allow us now to try to describe how our results relate to both Gupta and Murty's work [GM86] and Hsu and Yu's work [HY01].

Let $A = \mathbb{Z}[i]$ and E be the elliptic curve $y^2 = x^3 - x$. Let $k = \mathbb{Q}(i)$, then $E(k)$ is an A-module, and A is a principal ideal domain. Let $a \in E(k)$ be non-torsion. We say that a is a primitive point modulo a place $\wp$ of k if $E(\mathbb{F}_\wp)$ is generated by a as an A-module. The methods of Gupta and Murty apply to tell us that if $L_{\mathfrak{q}} = k(\mathfrak{q}^{-1}a, E[\mathfrak{q}]) \neq k$ for each prime $\mathfrak{q}$ of A, then a is a primitive point modulo $\wp$ for infinitely many places $\wp$. This problem is analogous in some ways to Artin's original conjecture and Hsu's paper [Hsu99], one of the differences being that E does not have good reduction everywhere unlike G_m and the Carlitz module.

Let A be the ring of integers of a quadratic imaginary extension $k/\mathbb{Q}$ and suppose that A has class number one. Let E be an elliptic curve with complex multiplication by A so that $E(k)$ is an A-module. The methods of Gupta and Murty again apply to this case. This problem is analogous to Hsu and Yu's paper [HY01].

Now, suppose E/K is an elliptic curve with complex multiplication by the ring of integers $A \subseteq k$. Suppose that the endomorphisms of E are defined over K'. Then $E(K')$ is an A-module, and we can consider Artin's conjecture within this framework. But the methods of Gupta and Murty (and similarly, Hsu and Yu's methods) do not apply here. On the other hand, our methods can apply to this problem. This problem may be considered as a classical analogue to the problems considered in this paper. We will return to these ideas in the future.

We now state our main theorem.

Theorem 1.4. *Let F be a global function field over $\mathbb{F}_r$, ∞ a fixed place of F, A the ring of elements of F regular everywhere except possibly ∞, and K a finite extension of F.*

Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of generic characteristic and of rank 2. Let $B = \mathrm{End}(\phi)$, and suppose that B is the integral closure of A in a quadratic extension of F, and suppose the elements of B have coefficients in K.

Let $a \in K$ and define $N_a(x)$ to be the number of primes $\wp$ of K of degree equal to x such that the reduction of a generates $\mathbb{F}_\wp$ as an A-module.

Then there is a positive integer J and constants $\delta(0), \delta(1), \ldots, \delta(J-1)$, depending on ϕ and a, such that as $x \equiv i \mod J$ and $x \to \infty$ we have the estimate

$$N_a(x) = \delta(i)\frac{r^x}{x} + \mathbf{O}\left(\frac{r^x \log x}{x^2}\right).$$

We now describe the advances made in our work.

In Section 3, we formulate a Lang-Trotter type condition and in Section 4 make Galois theory calculations. It should be noted that we use Pink's work [Pin16] as a black box, and prove linear disjointness results based on Pink's open-image theorem.

We do so because working with Pink's results leads us to formulate the Lang-Trotter condition in terms of $\mathfrak{q}^{-1}W$, where W is the B-submodule of K generated by a and $\mathfrak{q}$ is a prime of B. This formulation leads to a fuller understanding of the Lang-Trotter condition. Also, the division modules $\mathfrak{q}^{-1}W$ behave nicely even when $\mathfrak{q}$ is not a principal ideal. This is not so in [HY01]. See, for example, the proof of [HY01, Proposition 2.3], in which it is claimed that

$$\phi_{\mathfrak{q}}(\overline{\alpha}) \equiv a \mod \mathfrak{P}'$$

implies that

$$\phi_{(p-1)\mathfrak{q}^{-1}}(a) \equiv 0 \mod \mathfrak{P}'$$

which requires us to accept that

$$\phi_{(p-1)\mathfrak{q}^{-1}}\phi_{\mathfrak{q}} = \phi_{(p-1)}$$

which does not necessarily hold if $\mathfrak{q}$ is not principal.

In Section 5, we calculate discriminant bounds in order to apply the Chebotarev density theorem. Our Theorem 5.11 may be viewed as a generalization of Gardeyn's discriminant calculations in [Gar02] and of the discriminant calculations in [HY01].

There are two difficulties to overcome in calculating discriminants of the division fields which are not addressed in [HY01]. First, our division fields are of the form $K(\mathfrak{q}^{-1}W)$, where $\mathfrak{q}^{-1}W = \{\alpha \in K^{\text{sep}} \mid \psi_t(\alpha) \in W \text{ for all } t \in \mathfrak{q}\}$, and W is the B-submodule of K generated by a. So the division field is not necessarily the splitting field of a single polynomial. To overcome this obstacle, we must estimate the discriminant locally. For each prime considered, we can choose a nice $t \in \mathfrak{q}$ so that $K(\mathfrak{q}^{-1}W) \subseteq K((t)^{-1}W)$ where now $K((t)^{-1}W)$ is the splitting field of $\psi_t(x) - a$.

There is another difficulty as well. We also do not assume that our Drinfeld module has good reduction at every prime. Similarly, we do not assume that a is integral at every prime of K. Adding these assumptions would simplify our calculations at the cost of less generality.

Proving the main theorem constitutes Section 6. This section is a straightforward combination of the analysis contained in [GM86], but worked out in the function field setting. The function field setting provides a few challenges which we are able to overcome.

In particular, we are able to remove any technical assumption about the division fields being geometric. Furthermore, we are able to prove a result which we summarize as "if the set of primes satisfying Artin's conjecture should not be finite, then the set of primes satisfying Artin's conjecture has positive density". This has its roots in the paper [KL09]. This happens in Section 7. We are also able to recover the results contained in [HY01], this deduction comprises Section 8. Furthermore, we are able to extend the Brun-Titchmarsh theorem proved by Hsu in [Hsu99] to include the case that $\deg \infty > 1$. To do this requires careful accounting of the original proof. We have included this accounting in Section 9. We hope that our presentation illuminates several key lemmas.

2. Notations and basic facts

We introduce some general notation and facts for Drinfeld modules. We will indicate when any additional assumptions are made on top of the standard definitions. The reader may consult Goss' book [Gos96] for a complete introduction to Drinfeld modules.

Let $\mathbb{F}_r$ be the finite field with r elements, where r is a power of a rational prime p.

A *global function field* with the constant field $\mathbb{F}_r$ is a field L over $\mathbb{F}_r$ with an element $T \in L$ such that L is a finite separable extension of the field $\mathbb{F}_r(T)$, where T is transcendental over $\mathbb{F}_r$, and the algebraic closure of $\mathbb{F}_r$ in L is equal to $\mathbb{F}_r$.

A *place* of L is a pair $P = (O_P, m_P)$ where $O_P \subset L$ is a discrete valuation ring with the maximal ideal $m_P \subset O_P$, and the quotient field of O_P is equal to L.

The *residue field* at a place P is $\mathbb{F}_P = O_P/m_P$.

The *degree of* P (for this paper we take the degree relative to $\mathbb{F}_r$), $\deg P$, is the degree of the extension $[\mathbb{F}_P : \mathbb{F}_r]$.

Each place induces a discrete valuation on the field L, the unique normalized discrete valuation corresponding to P will be denoted by v_P.

A *divisor* $\mathfrak{D}$ of L is a (finite and formal) sum over the places of L,

$$\mathfrak{D} = \sum v_P(\mathfrak{D}) \cdot P.$$

The *degree of a divisor* $\mathfrak{D}$ is

$$\deg \mathfrak{D} = \sum v_P(\mathfrak{D}) \deg P.$$

Now, let F be a global function field with a fixed place ∞.

The subring R of F of all elements of F which are integral at all places except at the place ∞ is a Dedekind domain. The place ∞ is called the infinite place and every other place is called a finite place. If $P = (O_P, m_P)$ is a finite place of F, then the ideal of R, $m_P \cap R$ is a prime ideal of R. By abuse of notation, this prime ideal is also called P. Ideals of R correspond to divisors of F supported on the finite places.

An R-field L is a field L equipped with an $\mathbb{F}_r$-morphism $\iota : R \to L$. The prime ideal $\mathfrak{w} = \ker(\iota)$ is called the R-characteristic of L. We say that L has generic R-characteristic if $\mathfrak{w} = (0)$; otherwise, we say that L has finite R-characteristic.

Let

$$F_{\mathfrak{w}} = \{x \in F \mid x = a/b, a, b \in R, b \notin \mathfrak{w}\}$$

and notice that ι extends to a map $\iota : F_{\mathfrak{w}} \to L$. If $\mathfrak{w} \neq 0$ then ι essentially embeds the residue field at $\mathfrak{w}$ into L. If, however, $\mathfrak{w} = 0$ then ι embeds F into L. Furthermore, if $\wp = (O_\wp, m_\wp)$ is a place of L, then there is a corresponding place of F, denoted by $\iota^*\wp = \mathfrak{p} = (O_\mathfrak{p}, m_\mathfrak{p})$

$$O_\mathfrak{p} = \{x \in F \mid \iota(x) \in O_\wp\}$$

$$m_\mathfrak{p} = \{x \in F \mid \iota(x) \in m_\wp\}.$$

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

A *Drinfeld R-module* ρ over L is an $\mathbb{F}_r$-algebra homomorphism

$$\rho : R \to L\{\tau\} \subset \mathrm{End}_L(\mathbb{G}_a), z \mapsto \rho_z,$$

such that $\iota = \mathcal{D} \circ \rho$ and $\rho \neq \epsilon \circ \iota$.

Let $\deg_\tau \rho_z$ denote the degree of ρ_z in τ and let $\deg(z)$ denote the degree of z. There exists a unique positive integer d, called the *rank* of ρ, such that $\deg_\tau \rho_z = d \deg(z)$.

For a finite place $\wp$ of L of good reduction (see [Gos96, Definition 4.10.1]) for ρ, denote by $\rho \otimes \mathbb{F}_\wp$ the Drinfeld module obtained by reducing the coefficients of ρ modulo $\wp$. Note that the definition of good reduction ensures that $\rho \otimes \mathbb{F}_\wp$ is a Drinfeld module of the same rank as ρ.

If the context is clear, we will use ρ to mean $\rho \otimes \mathbb{F}_\wp$.

Denote by $\rho(\mathbb{F}_\wp)$ the set $\mathbb{F}_\wp$ with R-action given by $(\rho \otimes \mathbb{F}_\wp)$ (this is the main place where we will use ρ to mean $\rho \otimes \mathbb{F}_\wp$). The R-characteristic of $\rho \otimes \mathbb{F}_\wp$ is seen to be $\iota^* \wp$.

An *endomorphism* of ρ is a polynomial $f \in \overline{L}\{\tau\}$ such that $f\rho_z = \rho_z f$ for all $z \in R$, where $\overline{L}$ is an algebraic closure of L. The set of all endomorphisms is denoted by $\mathrm{End}_{\overline{L}}(\rho)$. We say that ρ has *complex multiplication* if $\mathrm{End}_{\overline{L}}(\rho) \neq R$.

We have introduced some of the general concepts that we will be considering for Drinfeld modules. Let us now set up the specific situation for this paper. We will also compare our assumptions to some previous works.

Let F be a global function field with constant field $\mathbb{F}_r$. Let ∞ be a place of F. Let A be the ring of elements of F regular at all places except for possibly ∞. Let K be an A-field of generic characteristic (so that $\iota : A \to K$ has $\ker(\iota) = (0)$). Assume that $K/\iota(F)$ is a finite extension. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module and assume that ϕ is of rank 2. Let $B = \mathrm{End}_{K^{\mathrm{sep}}}(\phi)$ and assume that $B \neq A$. This implies that $\kappa = B \otimes_A F$ is a quadratic extension of F in which ∞ does not split.

Remark 2.1. In Hsu and Yu's work [HY01], it is assumed that $\deg \infty = 1$, that the A-field K is the Hilbert class field of A, and that the Drinfeld module in question is sign-normalized. We do not make these assumptions. In particular, we can drop the assumption that $\deg \infty = 1$ by adapting the proof of the Brun-Titchmarsh theorem for function fields in [Hsu99] to the case that $\deg \infty > 1$. See Section 9.

Also, assume that B is the integral closure of A in κ. This assumption is made for simplicity. In general B is an A-order in κ. Finally, assume that the elements of B are defined over K. That is, we assume

$$B = \mathrm{End}_{\overline{K}}(\phi) = \mathrm{End}_K(\phi).$$

Remark 2.2. How strong is this hypothesis that the endomorphisms of ϕ have coefficients in K? In general, we have $B = \mathrm{End}_{K'}(\phi)$ for some Galois extension K'/K. In fact, if we put $A' = \mathrm{End}_K(\phi)$, and F' the fraction field of A', then [KT20, Proposition 3.1] implies that $\mathrm{Gal}(\kappa/F') \cong \mathrm{Gal}(K'/K)$. Because κ/F' is either a quadratic extension or $\kappa = F'$, we have that K'/K is either a quadratic extension or $K' = K$. In the case that K'/K is a quadratic extension, when we replace K with K', we are essentially only considering primes $\wp$ of K which split completely in K'. This is the same tact as Gupta and Murty take in [GM86]. In fact, it is possible to prove a density theorem for the primes $\wp$ of K which are inert in K' using the techniques of [KT20], and we plan to carry out this strategy for elliptic curves with complex multiplication at a later time.

Now that we have considered the assumptions and limitations of our approach, let us finish setting up the notation for Theorem 1.4. Let $\psi : B \to K\{\tau\}$ be the Drinfeld B-module defined by $\psi_a = f(\tau)$, where $f \in \mathrm{End}_K(\phi)$ is associated to

$a \in B$ under $B \cong \mathrm{End}_K(\phi)$. This turns K into a B-field by the homomorphism (let us also call it ι) $\iota(a) = \mathcal{D}(f(\tau))$ where $f \mapsto a$ in $\mathrm{End}_K(\phi) \cong B$, as long as we remember that $\mathcal{D}$ is the function which gives us the constant term of an additive polynomial.

Let P_∞ be the set of places $\mathcal{Q}$ of K for which $\iota^*\mathcal{Q}$ corresponds to the place ∞ of F. All other places of K are called finite places. Let P_{good} be the set of finite places $\wp$ of K for which a is a unit modulo $\wp$ and for which the coefficients of ϕ_b are $\wp$-integers and the leading coefficients of ϕ_b are units modulo $\wp$ for all $b \in A$. This only excludes finitely many places which satisfy [Gos96, Definition 4.10.1]. The finite places which are not in P_{good} make up the set P_{bad}.

We say that a is a primitive point modulo $\wp$ if a is a unit modulo $\wp$ and ϕ has good reduction at $\wp$ (in other words, $\wp$ is in P_{good}) and the reduction of a modulo $\wp$ generates $\mathbb{F}_\wp$ as an A-module under the action of ϕ reduced modulo $\wp$. Let x be a positive integer and finally define the prime ideal counting function $N_a(x)$ by

$$N_a(x) = |\{\wp \in P_{good} \mid \deg \wp = x, a \text{ is a primitive point modulo } \wp\}|.$$

Remark 2.3. Note A is not assumed to have class number 1 We do not assume that $\deg \infty = 1$ and we do not make restrictions on the leading coefficient of the polynomials $\phi_b \in K\{\tau\}$.

We are able to recover the results of [HY01]. We only use the results of [HY01] on the degree and ramification of the extensions $K(\psi_m^{-1}(a), \psi[m])/K$ when $m \in B$, and we deduce the calculations when m is a non-principal ideal from these calculations.

It seems that we rely on the results of Pink [Pin16], but for our case, these results can be deduced without too much trouble from [HY01]. The real reason that we cite [Pin16] is to use the description of what "$\mathfrak{q}^{-1}a$" means when $\mathfrak{q}$ is not a principal ideal.

3. Reduction Theory for Drinfeld modules

Our goal in this section is to formulate a Lang-Trotter condition (as in [GM86]) for Drinfeld modules. The main difficulty is that the Lang-Trotter condition in [GM86] assumes that the endomorphism ring is a principal ideal domain (which happens naturally if one is interested in elliptic curves that are defined over $\mathbb{Q}$ with complex multiplication). This assumption seems rather unnatural for Drinfeld modules of rank 2. However, it is not necessary for us to assume that the endomorphism ring is a principal ideal domain. In this section we will prove that the Lang-Trotter condition can be formulated in terms of a set $\mathfrak{a}^{-1}W$, where W is the B-submodule of K generated by a. We can do this in such a way to take advantage of Pink's paper [Pin16]. Importantly, the terminology of Pink's paper gives a natural expression for a Lang-Trotter condition while the main result of Pink's paper lets us compute the degree of the various Kummer extensions. It should be noted that Pink's paper [Pin16] is important to this paper for its notation, and any generalization to the case where the rank of the Drinfeld module is greater than 1 will crucially rely on Pink's paper [Pin16]. Also note that the approach of considering $n^{-1}\langle a \rangle$ was taken by Kowalski [Kow03].

We summarize the arguments of this section. Recall that W is the B-submodule of K generated by a, and $\mathrm{red}(W) \subseteq \mathbb{F}_\wp$ its reduction modulo $\wp$ for primes $\wp$ in P_{good}. If $\mathfrak{q}$ is a prime ideal of B, the goal is to determine when the index of the reduction of W in $\mathbb{F}_\wp$ is divisible by $\mathfrak{q}$. The key is to look at $\mathfrak{q}^{-1}W = \{\alpha \in$

$K^{\text{sep}} \mid \psi_b(\alpha) \in W \text{ for all } b \in \mathfrak{q}\}$ and the splitting type of $\wp$ in $K(\mathfrak{q}^{-1}W)$, the smallest field containing all of $\mathfrak{q}^{-1}W$.

Our strategy is to follow the steps below.

(i) $\operatorname{red}(W) \neq \mathbb{F}_\wp$ if and only if $\mathfrak{q}^{-1}\operatorname{red}(W) \subseteq \mathbb{F}_\wp$ for some prime ideal $\mathfrak{q}$ of B.
(ii) There is an onto map from $\mathfrak{q}^{-1}W \to \mathfrak{q}^{-1}\operatorname{red}(W)$.
(iii) The Frobenius is trivial on $\mathfrak{q}^{-1}\operatorname{red}(W)$ if and only if it is trivial in $K(\mathfrak{q}^{-1}W)$
(iv) $K(q^{-1}W)$ is equal to $K(q^{-1}W/W)$ and the Galois group of the latter field can be calculated by the results of [Pin16].

Definition 3.1. Let M be a B-submodule of K and $\mathfrak{m}$ an ideal of B. Then define

$$\mathfrak{m}^{-1}M = \{x \in K^{\text{sep}} \mid \psi_m(x) \in M \text{ for all } m \in \mathfrak{m}\}.$$

If ψ has good reduction at a prime $\wp$ of K and M', is a B-submodule of $\mathbb{F}_\wp$, similarly define $\mathfrak{m}^{-1}M'$.

Proposition 3.2. *Let M' be any B-submodule of $\mathbb{F}_\wp$. Let $\mathfrak{p}$ be the B-characteristic of $\mathbb{F}_\wp$. Assume that $\mathfrak{p} \nmid \mathfrak{m}$. Then we have*

$$(\mathbb{F}_\wp/M')[\mathfrak{m}] \cong (B/\mathfrak{m})$$

if and only if

$$\mathfrak{m}^{-1}M' \subseteq \mathbb{F}_\wp.$$

Proof. Notice that because the reduction of ψ is rank 1, $\mathfrak{p}$ does not divide $\mathfrak{m}$, and M' is torsion, we get that

$$\mathfrak{m}^{-1}M'/M' \cong B/\mathfrak{m}.$$

If we now suppose that

$$\mathfrak{m}^{-1}M' \subseteq \mathbb{F}_\wp,$$

we get that the $\mathfrak{m}$-torsion of $\mathbb{F}_\wp/M'$ is isomorphic to $B/\mathfrak{m}$.

Suppose $\mathbb{F}_\wp/M'[\mathfrak{m}] \cong B/\mathfrak{m}$. Since

$$B/\mathfrak{m} \cong \mathbb{F}_\wp/M'[\mathfrak{m}] \subseteq \mathfrak{m}^{-1}M'/M' \cong B/\mathfrak{m}$$

it follows that $\mathbb{F}_\wp/M'[\mathfrak{m}] = \mathfrak{m}^{-1}M'/M'$ and therefore $\mathfrak{m}^{-1}M' \subseteq \mathbb{F}_\wp$. □

Proposition 3.3. *Let M be a B-submodule of a field L. Suppose $\wp$ is a prime of L, with local ring $\mathcal{O}_\wp$, maximal ideal $m_\wp$ and residue field $\mathbb{F}_\wp = \mathcal{O}_\wp/m_\wp$. If $M \subseteq \mathcal{O}_\wp$ and ψ has good reduction at $\wp$ then $\operatorname{red}(M) = (M + m_\wp)/m_\wp$ is a B-submodule of $\mathbb{F}_\wp$, and the reduction map*

$$M \to \operatorname{red}(M)$$

is onto.

Proof. We only need to check that $\operatorname{red}(M)$ is a B-submodule of $\mathbb{F}_\wp$. First, notice that $M \subseteq \mathcal{O}_\wp$ and ψ has good reduction at $\wp$. Since ψ has good reduction at $\wp$, we have that $\psi_b(m_\wp) \subseteq m_\wp$ for all $b \in B$. Now, we can conclude that $\operatorname{red}(M)$ is a B-submodule of $\mathbb{F}_\wp$. □

Now, let W be the B-submodule of K generated by the non-torsion element $a \in K$. Fix a separable closure K^{sep} of K. Let $G_K = \operatorname{Gal}(K^{\text{sep}}/K)$. Let $\mathfrak{m}$ be an ideal of B. Then $\mathfrak{m}^{-1}W$ and $\mathfrak{m}^{-1}W/W$ are both G_K modules.

Proposition 3.4. *Let $\mathfrak{m}$ be an ideal of B. Then for all $\sigma \in G_K$, σ is the identity on $\mathfrak{m}^{-1}W$ if and only if σ is the identity on $\mathfrak{m}^{-1}W/W$.*

Proof. This is essentially [Pin16, Proposition 2.13]. The "only if" part is clear. Suppose σ is the identity on $\mathfrak{m}^{-1}W/W$. Then let $\lambda \in \mathfrak{m}^{-1}W$ and suppose $\sigma(\lambda)-\lambda \in W$. By definition, $\psi_m(\lambda) \in W$ for each $m \in \mathfrak{m}$. Since ψ_m has coefficients in K, we obtain that $\psi_m(\sigma(\lambda)) = \psi_m(\lambda)$ which implies $\sigma(\lambda)-\lambda \in \psi[\mathfrak{m}]$. But $\psi[\mathfrak{m}] \cap W = \{0\}$ since W is torsion-free. So σ fixes $\mathfrak{m}^{-1}W$. □

Definition 3.5. Now, let $L^a_{\mathfrak{m}}$ be the fixed field of the subgroup

$$\{\sigma \in G_K \mid \sigma \text{ is trivial on } \mathfrak{m}^{-1}W\}$$

of G_K. In other words, $L^a_{\mathfrak{m}} = K(\mathfrak{m}^{-1}W)$. We have that $L^a_{\mathfrak{m}}/K$ is a finite Galois extension. If s is an ideal of B then put $K_s = K(\psi[s])$. Also, put $L^a_{\mathfrak{m},s} = L^a_{\mathfrak{m}} \cdot K_s$.

The following is essentially [Hsu97, Proposition 1.1].

Proposition 3.6. *Let $m \in B$ and put $\mathfrak{m} = (m)$. Then $L^a_{\mathfrak{m}}$ is the splitting field of $\psi_m(X) - a$.*

Proof. Choose α such that $\psi_m(\alpha) = a$. Then any element of $\mathfrak{m}^{-1}W$ can be represented as $\psi_b(\alpha)+\lambda$ where $\lambda \in \psi[\mathfrak{m}]$. But any element of $\psi[\mathfrak{m}]$ is a difference of roots of $\psi_m(X)-a$. This tells us that $L^a_{\mathfrak{m}}$ is contained in the splitting field of $\psi_m(X)-a$ and the converse is obvious. □

We need to know that $L^a_{\mathfrak{m}}/K$ is unramified above $\wp$ almost always.

Proposition 3.7. *Suppose that ψ has good reduction at $\wp$ and that $W \subseteq \mathcal{O}_\wp$. In particular, this only excludes finitely many primes $\wp$. Suppose that $\mathfrak{p}$ is the B-characteristic of $\mathbb{F}_\wp$ as a B-module. Suppose that $\mathfrak{m}$ is an ideal of B such that $\mathfrak{p} \nmid \mathfrak{m}$. Then $L^a_{\mathfrak{m}}/K$ is unramified above $\wp$.*

Proof. Let $\mathfrak{b} = \operatorname{lcm}(\mathfrak{a}, sB)$ and let $\mathfrak{m} = \mathfrak{b}^h$ where h is the class number of B. Then $\mathfrak{m} = (m)$ for some $m \in B$. So $L^a_{\mathfrak{a},s}$ is contained in the splitting field of $\psi_m(X) - a$. It is standard (see [Gos96, Theorem 4.10.5]) that $K(\psi[m])/K$ is unramified above $\wp$ if $\mathfrak{p}$ is coprime to (m). The field $L_{\mathfrak{m}}/K(\psi[\mathfrak{m}])$ is generated by any root α of $\psi_m(X) - a$. Furthermore, if $f(X) = \psi_m(X) - a$ then $f'(X) = \iota(m)$ which has zero valuation at $\wp$ since $\mathfrak{p}$ does not divide $\mathfrak{m}$. This implies that $L_{\mathfrak{m}}/K(\psi[\mathfrak{m}])$ is unramified above $\wp$. □

Proposition 3.8. *Let $\wp$ be a prime of K, let $\mathfrak{m}$ be an ideal of B and suppose that $\mathfrak{p} \nmid \mathfrak{m}$ where $\mathfrak{p}$ is the B-characteristic of $\mathbb{F}_\wp$. Suppose that ψ has good reduction at $\wp$ and that $W \subseteq \mathcal{O}_\wp$. Let $\sigma \in \operatorname{Gal}(L^a_{\mathfrak{m}}/K)$ be a Frobenius automorphism corresponding to $\wp$. Then $\sigma = 1$ if and only if $\mathfrak{m}^{-1}\operatorname{red}(W) \subseteq \mathbb{F}_\wp$.*

Proof. Let σ be a Frobenius automorphism for $\wp$, and let $n(\wp)$ be the number of elements of $\mathbb{F}_\wp$. That means that $\sigma(x) \equiv x^{n(\wp)} \mod \wp$ for all $x \in \mathfrak{m}^{-1}W$.

Suppose now that $\sigma = 1$. That implies that $\mathfrak{m}^{-1}\operatorname{red}(W) \subseteq \mathbb{F}_\wp$, since the reduction map $\mathfrak{m}^{-1}W \to \mathfrak{m}^{-1}\operatorname{red}(W)$ is onto.

Suppose that $\mathfrak{m}^{-1}\operatorname{red}(W) \subseteq \mathbb{F}_\wp$. Then $\sigma(x) \equiv x \mod \wp$ for all $x \in \mathfrak{m}^{-1}W$. But $L^a_{\mathfrak{m}}$ is unramified at $\wp$, so this implies that $\sigma = 1$. □

We are now able to establish a Lang-Trotter criterion which we will use to detect whether a modulo $\wp$ generates $\mathbb{F}_\wp$ as an A-module.

Proposition 3.9. *Let $\wp$ be a prime of K, let $\mathfrak{a}$ and s be ideals of B and suppose that $\mathfrak{p} \nmid \mathfrak{a}$ and $\mathfrak{p} \nmid s$ where $\mathfrak{p}$ is the B-characteristic of $\mathbb{F}_\wp$. Suppose that ψ has good reduction at $\wp$ and that $W \subseteq \mathcal{O}_\wp$. Let $\sigma \in \mathrm{Gal}(L^a_{\mathfrak{a},s}/K)$ be a Frobenius automorphism corresponding to $\wp$. Then $\sigma = 1$ if and only if $\mathfrak{a}^{-1}\operatorname{red}(W) \subseteq \mathbb{F}_\wp$ and $s^{-1}0 \subseteq \mathbb{F}_\wp$.*

Proof. Notice that $\wp$ splits completely in $L^a_{\mathfrak{a},s}$ if and only if $\wp$ splits completely in both $L^a_{\mathfrak{a}}$ and $K(\psi[s])$ since $L^a_{\mathfrak{a},s} = L^a_{\mathfrak{a}} \cdot K(\psi[s])$. That $\wp$ splits completely in $L^a_{\mathfrak{a}}$ if and only if $\mathfrak{a}^{-1}\operatorname{red}(W) \subseteq \mathbb{F}_\wp$ is the previous proposition. That $\wp$ splits completely in $K(\psi[s])$ if and only if $s^{-1}0 = \psi[s] \subseteq \mathbb{F}_\wp$ follows by taking $W = 0$. □

4. Application of Pink's Open Image Theorem

Suppose that $\{H_{\mathfrak{a}}\}_{\mathfrak{a}}$ is an inverse system of groups (where $\mathfrak{a}$ runs over ideals of B). Suppose that for any pair of ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that $\mathfrak{a}$ divides $\mathfrak{b}$, there exists a surjective homomorphism $\pi_{\mathfrak{a},\mathfrak{b}} : H_{\mathfrak{b}} \to H_{\mathfrak{a}}$. Suppose that if $\mathfrak{a}$ and $\mathfrak{a}'$ are coprime then the natural map

$$H_{\mathfrak{a}\mathfrak{a}'} \to H_{\mathfrak{a}} \times H_{\mathfrak{a}'}$$

is an isomorphism.

Suppose that L is a field, and L^{sep} a separable closure of L, and suppose there exists a homomorphism $\rho : G_L \to H$ where $G_L = \mathrm{Gal}(L^{\mathrm{sep}}/L)$.

Suppose that $\pi_{\mathfrak{a}} : H \to H_{\mathfrak{a}}$ is the natural projection. Define $\rho_{\mathfrak{a}} : G_L \to H_{\mathfrak{a}}$ to be the composition $\pi_{\mathfrak{a}} \circ \rho$.

Let $X = H/\rho(G_L)$, the set of cosets of $\rho(G_L)$ in H. Applying the propositions [BK72, Chapter IX, Propositions 2.3 and 2.4] to our situation gives that

$$H/\rho(G_L) \cong \lim_{\mathfrak{a}} H_{\mathfrak{a}}/\rho_{\mathfrak{a}}(G_L), \tag{1}$$

as long as $\{\rho_{\mathfrak{a}}(G_L)\}$ satisfies the Mittag-Leffler condition.

If in addition, we assume that $H/\rho(G_L)$ is finite, then we conclude that there exists $M \in B$ such that

$$H/\rho(G_L) \cong H_M/\rho_M(G_L)$$

and further that

$$H_{M\mathfrak{a}}/\rho_{M\mathfrak{a}}(G_L) \cong H_M/\rho_M(G_L)$$

for any ideal $\mathfrak{a}$ of B.

Note that the above holds if M is replaced by M' with $M|M'$.

Now assume that $\mathfrak{a}$ is an ideal that is coprime to $M \cdot B$, the ideal generated by M. Suppose that $\mathfrak{b}$ is an ideal, all of whose prime factors divide M (so clearly, $\mathfrak{b}$ is coprime to $\mathfrak{a}$). Then $\mathfrak{b}$ divides M^k for some positive integer k, and

$$H_{M^k\mathfrak{a}}/\rho_{M^k\mathfrak{a}}(G_L) \cong H_{M^k}/\rho_{M^k}(G_L)$$

by Equation 1. But also $H_{M^k\mathfrak{a}} \cong H_{M^k} \times H_{\mathfrak{a}}$ and the kernel of the composition

$$H_{M^k\mathfrak{a}} \to H_{M^k} \times H_{\mathfrak{a}} \to H_{M^k}/\rho_{M^k}(G_L) \times H_{\mathfrak{a}}/\rho_{\mathfrak{a}}(G_L)$$

contains $\rho_{M^k\mathfrak{a}}(G_L)$ giving a homomorphism

$$H_{M^k\mathfrak{a}}/\rho_{M^k\mathfrak{a}}(G_L) \to H_{M^k}/\rho_{M^k}(G_L) \times H_{\mathfrak{a}}/\rho_{\mathfrak{a}}(G_L)$$

But the first coordinate is an isomorphism by Equation 1. As both sides are finite groups, we have that $H_{\mathfrak{a}} = \rho_{\mathfrak{a}}(G_L)$ and $\rho_{M^k\mathfrak{a}}(G_L) \cong \rho_{M^k}(G_L) \times \rho_{\mathfrak{a}}(G_L)$

Let us define the necessary homomorphisms. Let $T_{\mathrm{ad}}(\psi) = \mathrm{Hom}(k/B, \mathrm{Div}_{K^{\mathrm{sep}}}(0))$. Notice that this is the limit of $\mathrm{Hom}(\mathfrak{a}^{-1}/B, \mathrm{Div}_{K^{\mathrm{sep}}}(0))$. Then the action of G_K on T_{ad} defines a homomorphism $\rho_1 : G_K \to \mathrm{Aut}_{B_{\mathrm{ad}}}(T_{\mathrm{ad}}(\psi))$ and denote by Γ the image of ρ_1. Let $L = K(\mathrm{Div}_{K^{\mathrm{sep}}}(0)$ and consider the homomorphism $\rho_2 : G_L \to \mathrm{Hom}(W, T_{\mathrm{ad}}(\psi))$ as well (see [Pin16] for details). Let Δ be the image of ρ_2.

The theorems by Pink and Rutsche [PR09, Theorem 0.1] and Pink [Pin16, Theorem 5.1] tell us the homomorphisms ρ_1 and ρ_2 have open images. Since the groups $\mathrm{Aut}_{B_{\mathrm{ad}}}(T_{\mathrm{ad}}(\psi))$ and $\mathrm{Hom}_B(W, T_{\mathrm{ad}}(\psi))$ satisfy the Mittag-Leffler condition, we can obtain M_1 satisfying the following property.

Corollary 4.1. *Suppose that $\mathfrak{a}$, $\mathfrak{a}'$, s, and s' are ideals of B such that $\mathfrak{a}$ and s are coprime to M_1 and the prime factors of $\mathfrak{a}'$ and s' divide M_1. Define $n(\mathfrak{a}, s) = [L^a_{\mathfrak{a},s} : K]$. Then*

$$n(\mathfrak{a}\mathfrak{a}', ss') = n(\mathfrak{a}, s)n(\mathfrak{a}', s')$$

and

$$n(\mathfrak{a}, s) = |B/\mathfrak{a}| \cdot |(B/\mathfrak{b})^\times|$$

where

$$\mathfrak{b} = \mathrm{lcm}(s, \mathfrak{a}).$$

5. Ramification calculations

We recall the machinery of the different, for more details see [FJ08, Section 3.6].

The degree of the different appears in the Riemann-Hurwitz formula [Ros02, Theorem 7.16]. We need the Riemann-Hurwitz formula to determine the genus of L' in terms of the genus of L. The genera of L' and L both appear in an effective Chebotarev density theorem for L'/L, as such we must compute the differents of various fields. More specifically for fields L' over some fixed field L, we must determine a bound for $\deg \mathrm{Diff}(L'/L)/[L' : L]$.

The different $\mathrm{Diff}(L'/L)$ is defined to be the following divisor of L'

$$\mathrm{Diff}(L'/L) = \sum d_{L'/L}(\hat{\mathcal{Q}})\hat{\mathcal{Q}},$$

where the sum is over all places $\hat{\mathcal{Q}}$ of L', and $d_{L'/L}(\hat{\mathcal{Q}})$ is the different exponent of L'/L at $\hat{\mathcal{Q}}$. The different exponent is zero at all unramified places of L'. The degree of $\mathrm{Diff}(L'/L)$ is (relative to $\mathbb{F}_r$)

$$\deg \mathrm{Diff}(L'/L) = \sum d_{L'/L}(\hat{\mathcal{Q}}) \deg \hat{\mathcal{Q}},$$

where the degree $\deg \hat{\mathcal{Q}}$ is the degree of a place of L' relative to $\mathbb{F}_r$.

Remark 5.1. We now deal with a more general class of Drinfeld modules and submodules W of K. These assumptions will remain in place for the remainder of this section.

Let A be the ring of regular functions of a function field k, and K a A-field under the map $\iota : A \to K$, and let us assume that ι is injective. Let $\rho : A \to K\{\tau\}$ be a Drinfeld module of rank n and let $a_1, \ldots, a_t \in K$. Let $W = \langle a_1, \ldots, a_t \rangle$ be the A-submodule of K generated by $a_1, \ldots, a_t$.

Definition 5.2. Let W and ρ be as in Remark 5.1. Let $\mathfrak{a}$ be an ideal of A. Then put $\mathfrak{a}^{-1}W = \{x \in K^{\mathrm{sep}} \mid \rho_m(x) \in W \text{ for all } m \in \mathfrak{a}\}$ and put $L^W_{\mathfrak{a}}$ to be the smallest field which contains all of $\mathfrak{a}^{-1}W$.

Now consider $\rho_1 : G_K \to \mathrm{Aut}_{B_{\mathrm{ad}}}(T_{\mathrm{ad}}(\psi))$ and $\rho_2 : G_L \to \mathrm{Hom}_B(W, T_{\mathrm{ad}}(\psi))$.

Let w' be a place of $L_{\mathfrak{a}}^W$. Then there is a place w of K which lies below w'. Also, by using the structure map $\iota : k \to K$, there is a place v of k lying below w.

If v is not the infinite place of A, then v corresponds to an ideal $\mathfrak{q}$ of A, and we write $v(\mathfrak{a}) = j$ to mean that $\mathfrak{a} = \mathfrak{q}^j\mathfrak{a}'$ where $\mathfrak{a}'$ is coprime to $\mathfrak{q}$.

Let $e_{L_{\mathfrak{a}}^W/K}(w')$ and $e_{K/k}(w)$ denote the ramification indices of w' over w and w over v respectively.

For each place w of K, let $\mathcal{O}_w$ be the elements of K which are regular at w, and $\mathfrak{m}_w$ the maximal ideal of $\mathcal{O}_w$.

We now recall the definition of integral coefficients, good reduction, and stable reduction (see [Gos96, Definition 4.10.1]).

Definition 5.3. If for all $a \in A$, we have that $\rho_a \in \mathcal{O}_w\{\tau\}$ and the reduction of the coefficients modulo $\mathfrak{m}_w$ defines a Drinfeld module over $\mathcal{O}_w/\mathfrak{m}_w$ of rank n' with $0 < n' \leq n$, then we say that ρ has integral coefficients. If $\rho \cong \rho'$ (that is, there exists $u \in K$ with $\rho' = u^{-1}\rho u$) such that ρ' has integral coefficients and the reduction of the coefficients of ρ' defines a Drinfeld module of rank n, then we say that ρ has good reduction. If $\rho \cong \rho'$ and ρ' has integral coefficients then we say that ρ has stable reduction.

We now give two additional definitions. We say that if ρ has integral coefficients and the reduction of the coefficients of ρ defines a Drinfeld module of the same rank as ρ, then we say that ρ has good coefficients.

Let W be an A-submodule of K. If there exists $u \in K$ so that $\rho' = u^{-1}\rho u$ has good coefficients and so that $u^{-1}W \subseteq \mathcal{O}_w$, then we say that the pair (ρ, W) has good reduction.

Proposition 5.4. *Let L be an extension of K and suppose that $\rho : A \to L\{\tau\}$ is a Drinfeld module of rank n. Let $x \in A$ and suppose that $\rho[x] \subseteq L$. Let $a \in L$. Suppose w is a place of L. Let $L' = L(\alpha)$ where $\rho_x(\alpha) = a$. Let w' be a place of L' lying above w. Let e be the ramification index of w' over w. There exists constants $C_1(w, a, \rho)$ and $C_2(w, a, \rho)$ (depending on ρ and a) such that if $w(u) \geq C_1(w, a, \rho)$, then $u^{-1}\rho_y u \in \mathcal{O}_w$ and $u^{-1}a \notin \mathcal{O}_w$, and furthermore*

$$d_{L'/L}(w') \leq e(w(\iota(x)) + C_2(w, a, \rho))$$

Proof. Notice that since ρ is finitely generated, if we make $w(u)$ sufficiently large then $u^{-1}\rho_y u \in \mathcal{O}_w$ for all $y \in A$. Then by taking $w(u) > w(a)$, we then ensure that $w(u^{-1}a) < 0$. This gives us our constant $C_1(w, a, \rho)$ (which we assume to be an integer).

Now, let $u \in L$ be such that $w(u) = C_1(w, a, \rho)$. Then let $f(X) = u^{-1}\rho_x u(X) - u^{-1}a$, so that if $\rho_x(\alpha) = a$, then $f(u^{-1}\alpha) = 0$. Then let $g(X) = (u/a)X^{\deg f} f(1/X)$, so that $g(u/\alpha) = 0$.

Notice that $g(X) \in \mathcal{O}_w[X]$ and g is a monic polynomial.

We compute

$$g'(X) = ua^{-1} \deg f X^{\deg f - 1} f(1/X) + ua^{-1} X^{\deg f} f'(1/X) \cdot (-1/X^2)$$

and since $\deg f = r^{n \deg x} = 0$ in K, and $f'(1/X) = \iota(x)$ we have

$$g'(X) = -ua^{-1} X^{r^{n \deg x} - 2} \iota(x).$$

We want to apply [Ser79, Chapter III, Corollary 2 to Proposition 11]. We need to compute $w'(g'(u\alpha^{-1}))$.

We see that

$$w'(g'(u\alpha^{-1})) = w'(ua^{-1}) + (r^{n\deg x} - 2)w'(u\alpha^{-1}) + w'(\iota(x)).$$

But notice that $w'(ua^{-1}) = r^{n\deg x}w'(u\alpha^{-1})$, the reason being that the roots of $f(X)$ are of the form $u^{-1}\alpha+\lambda$ where $\rho'_x(\lambda) = 0$, and so $w'(u^{-1}\alpha+\lambda) = w'(u^{-1}\lambda)$ as $w'(\lambda) \geq 0 > w'(u^{-1}\alpha)$. This implies that $w'(u^{-1}a) = r^{n\deg x}w'(u^{-1}\alpha)$. Therefore,

$$\begin{aligned} w'(g'(u\alpha^{-1})) &\leq w'(ua^{-1}) + r^{n\deg x}w'(u\alpha^{-1}) + w'(\iota(x)) \\ &= 2w'(ua^{-1}) + w'(\iota(x)). \end{aligned}$$

As $w(u) > w(a)$ and $w(u) = C_1(w, a, \rho)$, writing $w'(y) = ew(y)$ for all $y \in L$, gives the result. □

Proposition 5.5. *Let L be an extension of K and suppose that $\rho : A \to L\{\tau\}$ is a Drinfeld module of rank n. Let $x \in A$ and suppose that $\rho[x] \subseteq L$. Let $a \in L$. Suppose w is a place of L, and suppose that there is $u \in K$ such that $\rho' = u^{-1}\rho u$ has good coefficients at w (so that ρ has good reduction at w). Let $L' = L(\alpha)$ where $\rho_x(\alpha) = a$, and suppose that $u^{-1}a \in \mathcal{O}_w$. Let w' be a place of L' lying above w. Then*

$$d_{L'/L}(w') \leq w'(\iota(x)).$$

Proof. Let $f(X) = \rho'_x(X) - u^{-1}a$. Then

$$\begin{aligned} f(u^{-1}\alpha) &= \rho'_x(u^{-1}\alpha)_u^{-1}a \\ &= u^{-1}\rho_x(uu^{-1}\alpha) - u^{-1}a \\ &= u^{-1}(\rho_x(\alpha) - a) \\ &= 0. \end{aligned}$$

Since $u^{-1}a \in \mathcal{O}_w$, $f(X)$ has coefficients in $\mathcal{O}_w$ and its leading coefficient is in $\mathcal{O}_w^\times$. Therefore, [Ser79, Chapter III, Corollary 2 to Proposition 11] applies to give

$$d_{L'/L}(w') \leq w'(\iota(x)).$$

□

Proposition 5.6 ([Gar02, Proposition 6])**.** *Let $\mathfrak{a}$ be an ideal of A, and let $L = K(\rho[\mathfrak{a}])$.*

Let w be a finite place of K, and let w' be a place of L lying above w.

If ρ has good reduction at w, then $d_{L/K}(w') \leq nv(\mathfrak{a})e_{L/K}(w')e_{K/k}(w)$.

There exists a constant $C(\rho)$ (only depending on ρ) such that if ρ does not have good reduction then

$$d_{L/K}(w') \leq (nv(\mathfrak{a}) + C(\rho))e_{L/K}(w')e_{K/k}(w).$$

Proof. Although the result in [Gar02] is proved for $A = \mathbb{F}_r[T]$, the result we stated can be proved in the same manner. □

Proposition 5.7. *Let $x \in A$ and let w' be a place of $L^W_{(x)}$ which lies above a place w of K.*

Then, there is a constant $C_3(w, W, \rho)$ such that for all $x \in A$,

$$d_{L^W_{(x)}/K}(w') \leq e_{L^W_{(x)}/K}(w')(e_{K/k}(w)v(x)(n + t) + C_3(w, W, \rho)).$$

Suppose that ρ has good reduction at w, $\rho' = u^{-1}\rho u$ has good coefficients at w, and $u^{-1}W \subseteq \mathcal{O}_w$, then

$$d_{L^W_{(x)}/K}(w') \leq e_{L^W_{(x)}/K}(w')e_{K/k}(w)v(x)(n+t).$$

Proof. Let $L_0 = K(\rho[x])$ and for each $i = 1, 2, \ldots, t$ let $L_i = L_{i-1}(\alpha_i)$ where $\rho_x(\alpha_i) = a_i$ and $a_1, \ldots, a_t$ generate W. Notice that $L^W_{(x)} = L_t$ and let w_t be the valuation w'. Then for $i = 0, 1, 2, \ldots, t-1$, let w_i be the valuation of L_i lying below w_t.

For each $i = 1, \ldots, t$, let d_i denote the different exponent of L_i over L_{i-1} at the place w_i, and let e_i denote the ramification index at w_i of L_i over L_{i-1}, and let d_0 and e_0 denote the different exponent and ramification index respectively of L_0/K at the place w_0. Then repeatedly applying [Ser79, Chapter III, Proposition 8], we see

$$d_{L_t/K}(w_t) = d_t + e_t d_{t-1} + e_t e_{t-1} d_{t-2} + \cdots + e_t \cdots e_2 d_1 + e_t \cdots e_2 e_1 d_0.$$

First, let us deal with the case of an arbitrary finite place w. We have by Proposition 5.6, that

$$d_0 \leq e_0(e_{K/k}v(x)n + C(\rho)).$$

By Proposition 5.4,

$$d_i \leq e_i(w_{i-1}(\iota(x)) + C(w, \rho, a_i)).$$

Now, recall that

$$e_t e_{t-1} \cdots e_{i+1} e_i w_{i-1}(\alpha) = e_t \cdots e_1 e_0 w(\alpha) = e_{L_t/K} w(\alpha)$$

for all $\alpha \in K$, and $i = 0, 1, \ldots, t$. Therefore,

$$\begin{aligned} d_{L_t/K}(w_t) &\leq e_{L_t/K}(w_t)(w(\iota(x) \cdot (n+t) + C(\rho) + \sum_{i=1}^{t} C(w, \rho, a_i)) \\ &= e_{L_t/K}(w_t)\left[e_{K/k}(w)v(x) \cdot (n+t) + C_3(w, W, \rho)\right] \end{aligned}$$

by taking $C_3(w, W, \rho) = C(\rho) + \sum_{i=1}^{t} C(w, \rho, a_i)$.

Suppose that there exists $u \in K$ such that $u^{-1}\rho u$ has good coefficients and $u^{-1}W \subseteq \mathcal{O}_w$.

We have that [Gar02, Proposition 6] (which can be generalized without much trouble) tells us that

$$d_0 \leq n w_0(\iota(x)).$$

Also, Proposition 5.5, implies that for each $i = 1, 2 \ldots, t$,

$$d_i \leq w_i(\iota(x)),$$

since $w_i(u^{-1}a_i) \geq 0$. Now, recall that

$$e_t e_{t-1} \cdots e_{i+1} w_i(\alpha) = e_t \cdots e_1 e_0 w(\alpha) = e_{L_t/K} w(\alpha)$$

for all $\alpha \in K$, and $i = 0, 1, \ldots, t$. Therefore,

$$d_{L_t/K}(w_t) = e_{L_t/K}(w_t)(w(\iota(x)) \cdot (n+t).$$

It remains to remark that $w(\iota(x)) = e_{K/k} \cdot v(x)$. □

Remark 5.8. The following proposition from [HY01] was stated for a specific class of Drinfeld modules, but may be generalized without problems.

Proposition 5.9 ([HY01, Proposition 3.2(4)])**.** *Let v be an infinite place of K, and K_v the completion of K at v. There exists a finite extension L/K_v such that*

$$\mathrm{Div}_{K^{\mathrm{sep}}}(W) \subseteq L.$$

Proposition 5.10. *There exists a finite set S_{bad} of finite places of K and constants C_4, C_5, and C_6 such that for each place w' of $L_{\mathfrak{a}}^W$*

(i) if $w \in S_{\mathrm{bad}}$, then $d_{L_{\mathfrak{a}}^W/K}(w') \leq (C_4 \cdot v(\mathfrak{a}) + C_5) e_{L_{\mathfrak{a}}^W/K}(w')$,
(ii) if w is an infinite place of K, then $d_{L_{\mathfrak{a}}^W/K}(w') \leq C_6$, and
(iii) otherwise, $d_{L_{\mathfrak{a}}^W/K}(w') \leq e_{L_{\mathfrak{a}}^W/K}(w') e_{K/k}(w) v(\mathfrak{a})(n+t)$.

Proof. We define the set S_{bad} of places of K to be the set of finite places for which the pair (ρ, W) does not have good reduction.

Since A is finitely generated as an algebra over $\mathbb{F}_r$, it is clear that S_{bad} is finite.

Suppose that $w \notin S_{\mathrm{bad}}$. Then let $\mathfrak{c}$ be the product of the all the prime ideals $\mathfrak{p}$ of A such that there is a place in S lying above $\mathfrak{p}$. Let $\mathfrak{q}$ be the prime ideal of A corresponding to w of K.

Let $x \in \mathfrak{a}$ be such that $(x) = \mathfrak{a}\mathfrak{b}$ where $\mathfrak{b}$ is coprime to $\mathfrak{a}\mathfrak{q}\mathfrak{c}$ (see [Mil14, Corollary 20.13] or slightly modify [DF04, Corollary 19]).

Then we have that $(x)^{-1}W = \mathfrak{a}^{-1}W + \mathfrak{b}^{-1}W$. This implies that $L_{(x)}^W = L_{\mathfrak{a}}^W L_{\mathfrak{b}}^W$. Furthermore, since $\mathfrak{q}$ does not divide $\mathfrak{b}$ and (ρ, W) has good reduction at all places lying above prime ideals dividing $\mathfrak{b}$, it follows that $L_{\mathfrak{b}}^W/K$ is unramified above w. Let w'' be a place of $L_{(x)}^W$ lying above w'.

Applying Proposition 5.7 gives the bound

$$d_{L_{\mathfrak{a}}^W/K}(w') \leq d_{L_{(x)}^W/K}(w'') \leq e_{L_{(x)}^W/K}(w'') \cdot e_{K/k}(w) \cdot v(x)(n+t)$$

since (ρ, W) has good reduction at w. But $e_{L_{(x)}^W/K}(w'') = e_{L_{\mathfrak{a}}^W/K}(w')$ since $L_{(x)}^W = L_{\mathfrak{a}}^W \cdot L_{\mathfrak{b}}^W$ and $L_{\mathfrak{b}}^W$ is unramified above w. Therefore,

$$d_{L_{\mathfrak{a}}^W/K}(w') \leq e_{L_{\mathfrak{a}}^W/K}(w') \cdot e_{K/k}(w) \cdot v(x)(n+t).$$

But, again, by choice of $\mathfrak{b}$, we have that $v(x) = v(\mathfrak{a})$. This gives the stated bound for $w \notin S_{\mathrm{bad}}$.

Suppose that w is an infinite place of K. Let K_w be the completion of K at w. Then Proposition 5.9 gives a finite extension L of K_w (not depending on $\mathfrak{a}$) such that $L_{\mathfrak{a}}^W \subseteq L$. To complete the proof of this case, we just take C_6 to be larger than the different exponent of L/K_w, which, again, does not depend on the ideal $\mathfrak{a}$.

The only remaining case is when (ρ, W) does not have good reduction at w, that is $w \in S_{\mathrm{bad}}$. Let $x \in \mathfrak{a}$ be such that $\deg x \leq \deg \mathfrak{a} + g - 1 + \deg \infty$ (choose x by applying the Riemann-Roch theorem to the divisor $D = N\infty - \mathfrak{a}$ where N is chosen so that $\deg \mathfrak{a} + g \leq N \deg \infty < \deg \mathfrak{a} + g + \deg \infty$).

Then $L_{\mathfrak{a}}^W \subseteq L_{(x)}^W$ and $[L_{(x)}^W : L_{\mathfrak{a}}^W]$ can be crudely bounded by $r^{(n+t)^2(g-1+\deg\infty)}$. Let w'' be a place of $L_{(x)}^W$ lying above the place w' of $L_{\mathfrak{a}}^W$.

We have

$$d_{L_{\mathfrak{a}}^W/K}(w') \leq d_{L_{(x)}^W/K}(w'') \leq e_{L_{(x)}^W/K}(w'')(e_{K/k} v(x)(n+t) + C(w, W, \rho))$$

by Proposition 5.7. But then since $e_{L_{(x)}^W/L_{\mathfrak{a}}^W}(w'')$ is bounded by $[L_{(x)}^W : L_{\mathfrak{a}}^W]$ which is bounded independently of $\mathfrak{a}$, and since $v(x) \leq v(\mathfrak{a}) + g - 1 + \deg\infty$, we can bound the above by

$$e_{L_{\mathfrak{a}}^W/K}(w')(C_4 v(\mathfrak{a}) + C_5).$$

□

Now, define two sets of places of k. Define S'_{bad} to be the set of places v of k, such that there is a place $w \in S_{\text{bad}}$ of K which lies above v. Define S'_{good} to be the set of places v of k, such that no places w of K lying above v has $w \in S_{\text{bad}}$.

For any divisor $D = \sum_v n_v \cdot v$ of k, we define $\deg_{\text{bad}}(D) = \sum_{v \in S'_{\text{bad}}} n_v \deg(v)$, and similarly define $\deg_{\text{good}}(D) = \sum_{v \in S'_{\text{good}}} n_v \deg(v)$. This can then be extended to define $\deg_{\text{bad}}(\mathfrak{a})$ and $\deg_{\text{good}}(\mathfrak{a})$ for ideals $\mathfrak{a}$ of A.

Combining the above bound and summing over all places w of K gives the following bound.

Theorem 5.11. *There exists constants C_7 and C_8 depending only on ρ and W such that for all ideals $\mathfrak{a}$ of A, we have*

$$\deg \operatorname{Diff}(L_{\mathfrak{a}}^W/K) \leq \left(\deg_{\text{good}}(\mathfrak{a})(n+t) + C_7 \deg_{\text{bad}}(\mathfrak{a}) + C_8\right)[L_{\mathfrak{a}}^W : K]$$

Proof. Write

$$\operatorname{Diff}(L_{\mathfrak{a}}^W/K) = \sum_v \sum_{w|v} \sum_{w'|w} d_{L_{\mathfrak{a}}^W/K}(w') \deg(w')$$

where the left-most sum is over all places v of k, the next sum is over places w of K lying over v, and the right most summation is over places w' of $L_{\mathfrak{a}}^W$ lying over w. Split the sum into $\Sigma_\infty + \Sigma_S + \Sigma'$ where Σ_∞ is the sum over the place $v = \infty$, Σ_{bad} is over $v \in S'_{\text{bad}}$, and Σ_{good} is the remaining places (those v in S'_{good}).

Recall that $\deg(w') = f_{L_{\mathfrak{a}}^W/K}(w') \deg(w)$ where w' is a place of $L_{\mathfrak{a}}^W$ lying above a place w of K, and $f_{L_{\mathfrak{a}}^W/K}(w')$ is the inertial degree of w' over w. Therefore, as we sum over places w' lying above a fixed place w, we have

$$\sum_{w'|w} e_{L_{\mathfrak{a}}^W/K}(w') \deg(w') = \sum_{w'|w} e_{L_{\mathfrak{a}}^W/K} f_{L_{\mathfrak{a}}^W/K}(w') \deg(w) = [L_{\mathfrak{a}}^W : K] \deg(w).$$

We have

$$\Sigma_\infty = \sum_{w|\infty} \sum_{w'|w} d_{L_{\mathfrak{a}}^W/K}(w') \deg(w') \leq C_6 \sum_{w'} \deg(w') \leq C_6 \sum_{w|\infty} \deg(w)[L_{\mathfrak{a}}^W : K]$$

We have

$$\begin{aligned}
\Sigma_{\text{bad}} &= \sum_{v \in S'_{\text{bad}}} \sum_{w|v} \sum_{w'|w} d_{L_{\mathfrak{a}}^W/K}(w') \deg(w') \leq \sum_v \sum_{w|v} \sum_{w'|w} e_{L_{\mathfrak{a}}^W/K}(C_4 v(\mathfrak{a}) + C_5) \deg(w') \\
&= \sum_{v \in S'_{\text{bad}}} \sum_{w|v} (C_4 v(\mathfrak{a}) + C_5)) \deg(w)[L_{\mathfrak{a}}^W : K] \\
&\leq \left(C_7 \deg_{\text{bad}}(\mathfrak{a})\right)[L_{\mathfrak{a}}^W : K] + C_5[L_{\mathfrak{a}}^W : K] \sum_{v \in S'_{\text{bad}}} \sum_{w|v} \deg(w).
\end{aligned}$$

Finally

$$\begin{aligned}\Sigma_{\text{good}} &= \sum_{v\in S'_{\text{good}}}\sum_{w|v}\sum_{w'|w} d_{L_{\mathfrak{a}}^W/K}(w')\deg(w')\\ &\leq \sum_{v\in S'_{\text{good}}}\sum_{w|v}\sum_{w'|w}(n+t)v(\mathfrak{a})e_{L_{\mathfrak{a}}^W/K}(w')e_{K/k}(w)\deg(w')\\ &= \sum_{v\in S'_{\text{good}}}\deg(v)(n+t)v(\mathfrak{a})[L_{\mathfrak{a}}^W:K]\\ &= (n+t)\deg_{\text{good}}(\mathfrak{a})[L_{\mathfrak{a}}^W:K]\end{aligned}$$

Putting $C_8 = C_5\sum_{v\in S'_{\text{bad}}}\sum_{w|v}\deg(w) + C_6\sum_{w|\infty}\deg(w)$ gives the result. □

Remark 5.12. If one assumes further that (ρ, W) has potentially stable reduction at every finite place w of K, then one is able to prove a result more in line with Gardeyn's work. If one assumes that for each finite place w of K, there exists $u \in K$ such that $u^{-1}\rho u$ has integral coefficients and $u^{-1}W \subseteq \mathcal{O}_w$, then one is able to leverage the existence of the exponential function in [Dri74, Proposition 7.2] to get a much cleaner bound than the one we have obtained. The crucial point is that one is able to extend the base field to reduce to the case of good reduction.

We now state the particular result we need. Recall that $L^a_{\mathfrak{a},s}$ is the extension defined in Definition 3.5.

Proposition 5.13.

$$\deg\operatorname{Diff}(L^a_{\mathfrak{a},s}/K)/n(\mathfrak{a},s) \ll \deg\mathfrak{a} + \deg s.$$

Proof. Now, working in the specific case that $\psi : B \to K\{\tau\}$ is a rank-1 Drinfeld module, $W = \langle a\rangle$ is the B-submodule of K generated by a, applying Theorem 5.11 gives that

$$\deg\operatorname{Diff}(L^a_{\mathfrak{a}}/K) \ll \deg\mathfrak{a}[L^a_{\mathfrak{a}}:K]$$

and

$$\deg\operatorname{Diff}(K_s/K) \ll \deg s[K_s:K].$$

But this is enough to get the stated bound, as

$$\operatorname{Diff}(L^a_{\mathfrak{a}}K_s/K) = \operatorname{Diff}(L^a_{\mathfrak{a}}K_s/K_s) + \operatorname{Diff}(K_s/K).$$

□

6. Analysis

The goal of this section is to prove Theorem 1.4. Note that our strategy essentially follows the work of Hooley [Hoo67] with minor modifications as necessary. Roughly speaking, in the function field setting r^x will stand in for the size of a prime of degree x, whereas in the classical setting we may consider primes $p \leq x$. Continuing the analogy, a term of the form r^x/x will correspond to $x/\log x$ in the classical setting, and $\log x$ in the function field setting will correspond to $\log\log x$ in the classical setting. In this way, one may trace through our work (and that of Hsu and Yu [HY01]) and (with minor exceptions) link it to its analogue in Hooley's work.

We need to estimate $N_a(x)$. To do this we need some notations. Recall that

$$P_{good} = \left\{ \wp \text{ a finite place of } K \;\middle|\; \begin{array}{l} \text{for all } b \in B, \\ \text{the coefficients of } \psi_b \text{ are in } O_\wp \text{ and} \\ \text{the leading coefficient of } \psi_b \text{ is in } O_\wp^*. \\ \text{Furthermore, } a \text{ is in } O_\wp^* \end{array} \right\}$$

and

$$N_a(x) = |\{\wp \in P_{good} \mid \deg \wp = x, a \text{ is a primitive point for } \phi \text{ modulo } \wp\}|.$$

We say that a prime ideal $\mathfrak{P}$ of B is of first degree if it lies above a prime ideal $\mathfrak{p}$ of A and the residue field extension is of degree 1 over $\mathbb{F}_\mathfrak{p}$.

Let

$$S = \{\mathfrak{q} \subset B \mid \mathfrak{q} \text{ is a prime ideal of } B \text{ of first degree}\},$$
$$T = \{q \subset A \mid q \text{ is a prime ideal of } A\},$$
$$N(x,y) = \left| \left\{ \wp \in \mathcal{P}_{good} \;\middle|\; \begin{array}{l} \deg \wp = x, \\ \wp \text{ does not split completely in any } L_\mathfrak{q}^a \\ \text{where } \mathfrak{q} \in S \text{ with } \deg \mathfrak{q} \leq y, \text{ and} \\ \wp \text{ does not split completely in any } K_q, \\ \text{where } q \in T, \deg q \leq y \end{array} \right\} \right|,$$

and

$$M_x(y_1,y_2) = \left| \left\{ \wp \in \mathcal{P}_{good} \;\middle|\; \begin{array}{l} \deg \wp = x, \\ \wp \text{ splits completely in some } L_\mathfrak{q}^a \text{ or } K_q, \\ \mathfrak{q} \in S, q \in T, y_1 \leq \deg q, \deg \mathfrak{q} \leq y_2 \end{array} \right\} \right|.$$

For the rest of the paper, the implied constants of $\mathbf{O}$ depend only on ϕ and a. Notice that as long as we have ϕ, all related subjects, such as F, κ, K, and ψ will be decided.

We are now able to estimate $N_a(x)$ by $N(x,y)$ with error term $\mathbf{O}(M_x(y,x))$. We will later choose an appropriate y as a function of x to control the main and error terms.

Proposition 6.1.

$$N_a(x) = N(x,y) + \mathbf{O}\left(M_x(y,x) + r^y\right),$$

as $x \to \infty$.

Proof. We will see that

$$N_a(x) \leq N(x,y) + \mathbf{O}(r^y),$$

and

$$N(x,y) \leq N_a(x) + M_x(y,x),$$

for x large enough.

First, suppose that $\wp$ is counted by $N_a(x)$. Then by Proposition 3.9, $\wp$ does not split completely in any extension K_q or $L_\mathfrak{q}^a$ where $q \neq P$ and $\mathfrak{q} \neq \mathfrak{p}$, where P is the A-characteristic of $\mathbb{F}_\wp$ and $\mathfrak{p}$ is not equal to the B-characteristic of $\mathbb{F}_\wp$.

If $\wp$ is not counted by $N(x,y)$, it can only mean that the degree of $\mathfrak{p}$ or P is less than y. The number of $\wp$ such that P or $\mathfrak{p}$ have degree less than y is $\mathbf{O}(r^y)$ by [Ros02, Theorem 5.12]. If you assume that $y/x \to 0$ you can reduce this error to zero for x large enough. This proves that

$$N_a(x) \leq N(x,y) + \mathbf{O}(r^y),$$

as $x \to \infty$.

Now, if a prime is counted by $N(x,y)$, either it does not split completely in any of the extensions K_q or $L^a_{\mathfrak{q}}$, or it is counted by $M_x(y,x)$. If it does not split completely in any K_q or $L^a_{\mathfrak{q}}$ then it is counted by $N_a(x)$. This is standard and follows from Proposition 3.9.

This proves that

$$N(x,y) \leq N_a(x) + M_x(y,x),$$

as $x \to \infty$ which completes the proof of the proposition. □

We use the principle of inclusion and exclusion to estimate $N(x,y)$ in terms of the number of places of K splitting completely in the extensions $L^a_{\mathfrak{a},s}/K$. This requires the Chebotarev Density theorem.

Let L and L' be two global function fields with $\mathbb{F}_r \subset L \subset L'$. Let $G = \mathrm{Gal}(L'/L)$. Let $\mathbb{F}_L, \mathbb{F}_{L'}$ denote the constant fields of L and L' respectively.

Let $\sigma_{\mathfrak{P}}$ be the Artin symbol (which denotes a conjugacy class of G) for $\mathfrak{P}$ with respect to L'/L, and $d_L = [\mathbb{F}_L : \mathbb{F}_r]$, and $r_{L'} = [\mathbb{F}_{L'} : \mathbb{F}_L]$. For a conjugacy class $\mathcal{C} \subset G$, define

$$\pi_{\mathcal{C}}(x) = \{\mathfrak{P} | \deg \mathfrak{P} = x, \mathfrak{P} \text{ is a prime unramified in } L'/L, \text{ and } \sigma_{\mathfrak{P}} \subset \mathcal{C}\}.$$

A final note, in the theorem cited below, the degree of a place of L'/L is relative to the constant field of L. When we apply this theorem later, the degree of a place will be relative to the field $\mathbb{F}_r$ instead.

Theorem 6.2 ([FJ08, Chebotarev Density Theorem, Chapter 6, Section 4])**.** *Let L'/L be a finite Galois extension with Galois group G. Let $\mathcal{C} \subset G$ be a conjugacy class whose restriction to $\mathbb{F}_{L'}$ is the h-th power of the Frobenius automorphism of $\mathbb{F}_L$. Then for $x \in \mathbb{N}$, if $x \not\equiv h \pmod{r_{L'}}$, we have*

$$\pi_{\mathcal{C}}(x) = 0.$$

If $x \equiv h \pmod{r_{L'}}$,

$$\left| \pi_{\mathcal{C}}(x) - r_{L'} \frac{|\mathcal{C}|}{|G|} \frac{r^{d_L x}}{x} \right|$$
$$\leq \frac{2|\mathcal{C}|}{x|G|}((|G| + g_{L'} r_{L'})(r^{d_L x})^{1/2} + |G|(2g_L + 1)(r^{d_L x})^{1/4} + g_{L'} r_{L'} + |G| d/d_L),$$

where $g_{L'}, g_L$ denote the genus of L' and L respectively, and d is a constant depending on a choice of T with $L/\mathbb{F}_r(T)$ algebraic (otherwise unrelated to the result).

Although the effective version is not explicitly listed as a theorem, one can trace through [FJ08, Chapter 6, Section 4] to find all the constants.

To estimate $N(x,y)$, which we expect to be the main term, we use Theorem 6.2.

Let us fix ideals s and $\mathfrak{a}$, where s is a square-free ideal of A and $\mathfrak{a}$ is a square-free ideal of B only divisible by prime ideals of first degree. Set $L' = L^a_{\mathfrak{a},s}$, $L = K$. Let us rename all constants in terms of $\mathfrak{a}$ and s, for ease of notation. The algebraic closure of $\mathbb{F}_r$ inside $L^a_{\mathfrak{a},s}$ is, say, $\mathbb{F}_{\mathfrak{a},s}$, and put $j(\mathfrak{a},s) = [\mathbb{F}_{\mathfrak{a},s} : \mathbb{F}_r]$. The genus of $L^a_{\mathfrak{a},s}$ is denoted $g(\mathfrak{a},s)$ and, recall that $n(\mathfrak{a},s) = [L^a_{\mathfrak{a},s} : K]$.

Since we are interested in the prime ideals which split completely, we let $\mathcal{C} = \{1\}$, and let $\pi_{\mathfrak{a},s}$ denote $\pi_{\mathcal{C}}$ for this particular choice of L' and L.

Proposition 6.3. *If* $x \equiv 0 \pmod{j(\mathfrak{a}, s)}$ *then*

$$\left|\pi_{\mathfrak{a},s}(x) - j(\mathfrak{a}, s)\frac{r^x}{n(\mathfrak{a}, s)x}\right| = \mathbf{O}\left(\frac{r^{x/2}}{x}\left(\deg \mathfrak{a} + \deg s\right)\right).$$

Otherwise, $\pi_{\mathfrak{a},s}(x) = 0$.

Proof. Applying Theorem 6.2 to our special case, if x is divisible by $j(\mathfrak{a}, s)$ then

$$\left|\pi_{\mathfrak{a},s}(x) - j(\mathfrak{a}, s)\frac{r^x}{n(\mathfrak{a}, s)x}\right| \leq$$
$$\frac{2}{xn(\mathfrak{a}, s)}\left((n(\mathfrak{a}, s) + g(\mathfrak{a}, s))r^{x/2} + n(\mathfrak{a}, s)(2g_K + 1)r^{x/4} + g(\mathfrak{a}, s) + n(\mathfrak{a}, s)d\right),$$

where $d = [H : \mathbb{F}_r(t)]$ for some fixed separating transcendence element t.

We can use the Riemann-Hurwitz formula [Ros02, Theorem 7.16] to bound the genus of $L^a_{\mathfrak{a},s}$ in terms of the different of $L^a_{\mathfrak{a},s}/K$ and g_K:

$$2g(\mathfrak{a}, s) - 2 = n(\mathfrak{a}, s)(2g_K - 2) + d(\mathfrak{a}, s).$$

Using this our formula becomes

$$\left|\pi_{\mathfrak{a},s}(x) - j(\mathfrak{a}, s)\frac{r^x}{n(\mathfrak{a}, s)x}\right|$$
$$\ll \frac{1}{xn(\mathfrak{a}, s)}\left((n(\mathfrak{a}, s) + d(\mathfrak{a}, s))r^{x/2} + n(\mathfrak{a}, s)r^{x/4} + d(\mathfrak{a}, s)\right).$$

Using Proposition 5.13, we get

$$\left|\pi_{\mathfrak{a},s}(x) - j(\mathfrak{a}, s)\frac{r^x}{n(\mathfrak{a}, s)x}\right| \ll \frac{r^{x/2}}{x}\left(\deg \mathfrak{a} + \deg s\right),$$

completing the bound. □

Now, we can prove that $N(x, y)$ is a constant times r^x/x. To make our summations clear, we introduce the following notations. Let

$$S_y = \{\mathfrak{q} \in S | \deg \mathfrak{q} \leq y\},$$
$$T_y = \{q \in T | \deg q \leq y\},$$

and let S^*_y denote all the ideals of $\mathcal{O}_\kappa$ which are square-free products of those in S_y. Similarly define S^*, T^*_y and T^*.

Proposition 6.4. *Let* $y = \frac{\log x - \log 2}{\log r}$ *and let* $x \to \infty$. *Then*

$$\left|N(x, y) - \frac{r^x}{x}\sum_{\mathfrak{a} \in S^*_y}\sum_{s \in T^*_y} f(\mathfrak{a}, s, x)\right| = \mathbf{O}\left(r^{(1/2+\epsilon)x}\right),$$

for any $\epsilon > 0$.

The function f *is defined as* $j(\mathfrak{a}, s)\mu(\mathfrak{a})\mu(s)n(\mathfrak{a}, s)^{-1}$ *if* $j(\mathfrak{a}, s)$ *divides* x *and* 0 *otherwise*

Proof. By the Lang-Trotter condition Proposition 3.9, a prime splits completely in the field

$$\prod_{q|s} K_q \prod_{\mathfrak{q}|\mathfrak{a}} L^a_{\mathfrak{q}}$$

if, and only if, it splits in the field

$$L^a_{\mathfrak{a},s}.$$

So the two fields are equal.

Therefore, by inclusion-exclusion,

$$N(x,y) = \sum_{\mathfrak{a}\in S_y^*, s\in T_y^*} \mu(s)\mu(\mathfrak{a})\pi_{\mathfrak{a},s}(x).$$

By Proposition 6.3,

$$\mu(s)\mu(\mathfrak{a})\pi_{\mathfrak{a},s}(x) = f(\mathfrak{a},s,x)\frac{r^x}{x} + \mathbf{O}\left(\frac{r^{x/2}}{x}(\deg\mathfrak{a}+\deg s)\right)$$

The last step in the proof is to bound

$$\sum_{\mathfrak{a}\in S_y^*, s\in T_y^*} (\deg\mathfrak{a}+\deg s),$$

which we will do crudely. First of all, we bound

$$|S_y^*| = 2^{|S_y|}, |T_y^*| = 2^{|T_y|}$$

and

$$|S_y| + |T_y| \leq Zr^y/y,$$

for some constant Z, depending on both A and B. It follows then that for $\mathfrak{a}\in S_y^*, s\in T_y^*$ we have

$$\deg\mathfrak{a}+\deg s \leq y2^{Zr^y/y},$$

and so

$$\sum_{\mathfrak{a}\in S_y^*, s\in T_y^*} (\deg\mathfrak{a}+\deg s) \leq y2^{Zr^y/y}2^{Zr^y/y},$$

and now since $y = (\log x - \log 2)/\log r$

$$\sum(\deg\mathfrak{a}+\deg s) \ll \log x r^{Z'x/y},$$

where Z' is another constant.

As x tends to infinity so too does y and so for x large enough, $Z'x/y \leq \epsilon x$. Also $\log x < r^{\epsilon x}$ as well. So far, the remainder term has been bounded as

$$r^{x/2}/x \sum_{\mathfrak{a}\in S_y^*,\ s\in T_y^*} (\deg\mathfrak{a}+\deg s) \ll r^{x/2}/x \cdot r^{\epsilon x},$$

as required. □

Let us now examine the coefficient of the main term of the estimate for $N(x,y)$.

Proposition 6.5. *The sum*

$$\delta(x) = \sum_{\mathfrak{a}\in S^*} \sum_{s\in T^*} f(\mathfrak{a},s,x)$$

converges absolutely. Furthermore, as $x\to\infty$ we have

$$\left|N(x,y) - \delta(x)\frac{r^x}{x}\right| = \mathbf{O}\left(\frac{r^x}{x^2}\right).$$

Finally, the value of $\delta(x)$ only depends on the congruence class of x modulo J where J is a fixed positive integer depending on ϕ and a.

Proof. First, we prove that $j(\mathfrak{a}, s)$ is bounded independently of $\mathfrak{a}$ and s, and further that $j(\mathfrak{a}, s) = 1$ if $\mathfrak{a}$ and s are prime to M_1. In fact, we may have to replace M_1 with a multiple of M_1 in order to achieve this. To see that $j(\mathfrak{a}, s)$ is bounded independently of $\mathfrak{a}$ and s, apply Proposition 5.9 ([HY01, Proposition 3.2(4)]), to see that there is a finite extension L/K_v containing $\mathrm{Div}_{K^{\mathrm{sep}}}(W)$ where K_v is the completion of K at an infinite place v. Since the algebraic closure of $\mathbb{F}_r$ in L will be a finite extension, this establishes that $j(\mathfrak{a}, s)$ is bounded. Let J be the maximum value of $j(\mathfrak{a}, s)$. Now, replace M_1 with a suitable multiple and such that the constant field of $L^a_{(M_1)}$ is equal to $\mathbb{F}_{r^J}$, in other words, $L^a_{(M_1)}$ contains the maximal constant field. Then for all $\mathfrak{a}$ and s prime to M_1 since $L^a_{\mathfrak{a},s}$ will be linearly disjoint from $L^a_{(M_1)}$ over K, the constant field of $L^a_{\mathfrak{a},s}$ must be equal to the constant field of K (else the constant field of $L^a_{(M_1)}$ would not be maximal). This establishes that $\delta(x)$ only depends on the congruence class of x modulo J, because each term $f(\mathfrak{a}, s, x)$ only depends on x modulo $j(\mathfrak{a}, s)$ which divides J.

Let us now analyze $\delta(x)$ by following the discussion on [GM86, p. 24],

$$f(\mathfrak{a}, s, x) = j(\mathfrak{a}, s)\mu(\mathfrak{a})\mu(s)n(\mathfrak{a}, s)^{-1},$$

if $j(\mathfrak{a}, s)$ divides x and is equal to zero otherwise.

Let $S_0 \subset S$ be the set of the primes of S which divide M_1 coming from Corollary 4.1, similarly let $T_0 \subseteq T$ be the set of primes of T which have a common factor with M_1. Let $S' = S \setminus S_0$ and $T' = T \setminus T_0$.

Then applying Corollary 4.1 implies the following factorization

$$n(\mathfrak{a}, s) = n(\mathfrak{a}_0, s_0)n(\mathfrak{a}', s') = n(\mathfrak{a}_0, s_0)|B/\mathfrak{m}'^{\times}| \cdot |B/\mathfrak{a}'|,$$

where $\mathfrak{a}_0 \in S_0^*$, $s_0 \in T_0^*$, $\mathfrak{a}' \in S'^*$ and $s' \in T'^*$ with

$$\mathfrak{a} = \mathfrak{a}_0\mathfrak{a}', s = s_0s'.$$

We can now bound $\delta(x)$.

$$|\delta(x)| \leq \sum_{\mathfrak{a}_0 \in S_0^*, s_0 \in T_0^*} n(\mathfrak{a}_0, s_0)^{-1} \sum_{\mathfrak{a}' \in S'^*, s \in T'^*} |B/\mathfrak{m}'^{\times}|^{-1}|B/\mathfrak{a}'|^{-1},$$

where $\mathfrak{m}' = \mathrm{lcm}(\mathfrak{a}', s')$ in the above sum.

So we check to see if the summation over S'^* and T'^* converges. We have

$$\begin{aligned}
\sum_{\mathfrak{a}', s'} |B/\mathfrak{m}'^{\times}|^{-1} \cdot |B/\mathfrak{a}'|^{-1} &= \sum_{\mathfrak{a}'} |B/\mathfrak{a}'|^{-1}|B/\mathfrak{a}'^{\times}|^{-1} \sum_{s'} \varphi((\mathfrak{a}', s'))|B/sB^{\times}|^{-1} \\
&\ll \sum_{\mathfrak{a}'} |B/\mathfrak{a}'^{\times}|^{-1}|B/\mathfrak{a}'| \prod_{q} (1 + \varphi(\mathfrak{a}', q)|B/qB^{\times}|^{-1}) \\
&\ll \prod_{\mathfrak{q}} (1 + 2|B/\mathfrak{q}|^{-1}|B/\mathfrak{q}^{\times}|^{-1})
\end{aligned}$$

which is a product that converges absolutely. □

Let $z = \frac{x}{2} - \nu \log x$, where ν is a constant to be chosen later such that $\nu \geq 1/\log r$. Recalling that $M_x(y, x)$ is the number of primes $\wp$ of degree x which split completely in some $L^a_{\mathfrak{q}}$ or K_q where $\mathfrak{q} \in S$ or $q \in T$ such that $y \leq \deg \mathfrak{q}, \deg q \leq x$, we have

$$M_x(y, x) \leq N_1 + M'(y, z) + M'(z, x/2 + \log x) + M'(x/2 + \log x, x),$$

where N_1 is the number of places of K of degree x which split completely in some $L^a_{1,q}$ with $y \leq \deg q \leq x/2$ and $M'(a,b)$ is the number of places of K of degree x which split completely in some $L^a_{\mathfrak{q},1}$ with $a \leq \deg \mathfrak{q} \leq b$.

Proposition 6.6. *We have the estimate*

$$N_1 + M'(y,z) = \mathbf{O}\left(\frac{r^x}{x^2}\right)$$

as x tends to infinity.

Proof. First,

$$\pi_{\mathfrak{q},1}(x) \leq r^x j(\mathfrak{q},1) n(\mathfrak{q},1)^{-1} x^{-1} + r^{x/2}(\deg \mathfrak{q})/x,$$

and

$$\pi_{1,q}(x) \leq r^x j(1,q) n(1,q)^{-1} x^{-1} + r^{x/2}(\deg q)/x,$$

by Proposition 6.3. Now, incorporating the range of summation, we have

$$\deg q, \deg \mathfrak{q} > (\log x - \log 2)/\log r,$$

and for x large enough we have

$$n(1,q) = r^{2\deg q} - 1,\ r^{\deg q}(r^{\deg q} - 1),\ \text{or}\ (r^{\deg q} - 1)^2,$$

and

$$n(\mathfrak{q},1) = r^{\deg \mathfrak{q}}(r^{\deg \mathfrak{q}} - 1),$$

by Corollary 4.1. Now, write

$$N_1 \leq \sum_{y \leq i \leq z} r^x x^{-1} (r^i - 1)^{-2} \cdot r^i/i$$

and

$$M'(y,z) \leq \sum_{y \leq i \leq z} r^{x/2} i/x.$$

Clearly, $M'(y,z)$ is within the stated error bound and we have

$$N_1 \leq r^x/x \sum_i (r^{-i}/i)(1 - r^{-i})^{-2} \ll (r^x/x)(r^{-y}/y) \ll r^x/x^2,$$

the second inequality coming from the fact that

$$\int_y^\infty \frac{r^{-z}}{1 - r^{-z}}^2\, dz = 1/\ln r \int_{1-r^{-y}}^1 1/u^2\ du$$

using the substitution $u = 1 - r^{-z}$, and $du = r^{-z} \ln r\ dz$, we get

$$\begin{aligned} &= -1/\ln r \left(1 - 1/(1 - r^{-y})\right) \\ &\to 0 \text{ as } y \to \infty, \end{aligned}$$

which completes the estimate. □

We are left with estimating $M'(z, x/2 + \log x) + M'(x/2 + \log x, x)$. We will estimate $M'(z, x/2 + \log x)$ by extending a Brun-Titchmarsh type result due to Hsu [Hsu99]. The sum $M'(x/2 + \log x, x)$ can be bounded by extending a result of Akbary and Ghioca [AG09].

First, consider $M'(z, x/2 + \log x)$ which is the sum over primes of K of degree x which split completely in some $L^a_{\mathfrak{q},1}$ with $z \leq \deg \mathfrak{q} \leq x/2 + \log x$. We will do this using a Brun-Titchmarsh theorem. The result we need is a slight generalization of [Hsu99, Theorem 4.3].

Proposition 6.7. *We have the bound*

$$M'(z, x/2 + \log x) = \mathbf{O}(r^x \ln x/x^2).$$

Proof. Let $\wp$ be a prime counted by $M'(z, x/2 + \log x)$. Applying [Gos96, Section 4.14], we can see that the characteristic polynomial of $\mathrm{Frob}_\wp$ is a degree one polynomial $X - b$ and furthermore,

$$B/(b-1) \cong \psi(\mathbb{F}_\wp)$$

and

$$(b) = (i^*\wp)^m,$$

for some integer m.

If $\mathfrak{p}$ is an ideal of B, then there are at most $[K : \iota(\kappa)]$ places of K whose reduction has characteristic $\mathfrak{p}$.

Therefore, the number of $\wp$ counted by $M'(z, x/2 + \log x)$ with $m \geq 2$ are at most a constant times the number of prime ideals $\mathfrak{p}$ of B with $\deg \mathfrak{p} \leq x/2$. By the prime number theorem for the ring B, this is $\mathbf{O}(r^{x/2}/x)$.

So we may assume that $m = 1$ and since $\wp$ is counted by $M'(z, x/2 + \log x)$ we have that there is an ideal $\mathfrak{a}$ such that

$$z < \deg \mathfrak{a} < x/2 + \log x$$

and $\mathfrak{a} = \mathfrak{q}$ is a prime ideal of B. We have that

$$\psi(\mathbb{F}_\wp)[\mathfrak{a}] \cong (B/\mathfrak{a}),$$

which implies that $\mathfrak{a}$ divides $(b-1)$. In other words,

$$b \equiv 1 \pmod{\mathfrak{a}},$$

and (b) is a prime ideal of B.

Now, let $\pi(x; 1, \mathfrak{a})$ denote the number of prime ideals of B of the form (b) with $b \equiv 1 \mod \mathfrak{a}$.

Then we have the estimate

$$M'(z, x/2 + \log x) = \sum{}' \pi(x; 1, \mathfrak{q}) + \mathbf{O}(r^{x/2}/x),$$

where the dash over the summation means that we sum over the primes $\mathfrak{q}$ of B with

$$x/2 - \nu \ln x < \deg \mathfrak{q} \leq x/2 + \log x.$$

For $\deg \mathfrak{q}$ in the range z to $x/2 + \log x$ we have

$$x - \deg \mathfrak{q} - 7g - 4D + 4 \geq x/2 - \log x - 7g - 4D + 4 > 0,$$

for x large enough. So Theorem 9.2, which we will prove in Section 9, applies and we have

$$x - \deg \mathfrak{q} - 7g - 4D + 6 \geq x/2 - \log x - 7D - 4D + 6 =\geq C'x,$$

for x large enough, where C' is a constant. So

$$\pi(x; 1, \mathfrak{q}) \ll r^x/(x\varphi(\mathfrak{q})) = r^x/x(r^{\deg \mathfrak{q}} - 1)$$

and summing over all $\mathfrak{q}$ with $\deg \mathfrak{q}$ in the range $z \leq \deg \mathfrak{q} < x/2 + \ln x$ can be bounded as

$$r^x/x \sum_{z \leq i < x/2 + \log x} r^i/i(r^i - 1) \ll r^x \ln x/x^2,$$

completing the estimate. □

Now, we have dealt with the middle range. The remainder can be dealt with by a technique from [AG09], which can be thought of as an analogue of Hooley's technique to deal with the tail end of the error.

We will introduce the result which is essentially [AG09, Proposition 5.1].

Proposition 6.8 ([AG09, Proposition 5.1])**.** *The number of places $\wp$ such that the reduction of a modulo $\wp$ generates a submodule of size at most q^ℓ is bounded by a constant times $q^{2\ell}$ and the constant is independent of ℓ.*

Remark 6.9. The result [AG09, Proposition 5.1] is only for $A = \mathbb{F}_q[T]$, but the result can be extended to our case using the Riemann-Roch theorem.

Proposition 6.10. *We have that*

$$M'(x/2 + \log x, x) = \mathbf{O}(r^x/x^2).$$

Proof. Suppose $\wp$ is a prime which splits completely in one of the fields $L^a_{\mathfrak{q},1}$ with $x/2 + \log x \leq \deg \mathfrak{q} \leq x$. Then the reduction of a modulo $\wp$ has size at most

$$r^{x-(x/2+\log x)} = r^{x/2-\log x}$$

and so by [AG09, Proposition 5.1], the number of such $\wp$ is at most a constant times

$$r^{x-2\ln x} = r^x/x^{2\log r}.$$

Since $r \geq 2$ the stated bound follows. □

On combining Propositions 6.1, 6.5, 6.6 and 6.10 we get the required estimate for $N_a(x)$.

Theorem 6.11. *We have the estimate*

$$N_a(x) = \delta(x)\frac{r^x}{x} + \mathbf{O}\left(\frac{r^x \log x}{x^2}\right),$$

as x lies in a fixed congruence class modulo J, and x tends to infinity.

We also get the following generalization of [HY01, Theorem 4.6].

Theorem 6.12. *Let κ be a global function field, with constant field $\mathbb{F}_r$, ∞ a fixed place of κ, B the ring of elements of κ regular everywhere except possibly ∞, K a global function field which is a B-field of generic characteristic, $\psi : B \to K\{\tau\}$ a Drinfeld module of rank 1, and $a \in K$ a non-torsion element for ψ. Let $N'_a(x)$ denote the number of primes $\wp$ of K for which a generates $\psi(\mathbb{F}_\wp)$ as a B-module. Then there is a fixed modulus $J \geq 1$ and constants $\delta(0), \ldots, \delta(J-1)$ such that as $x \equiv i \mod J$ and $x \to \infty$, we have*

$$N'_a(x) = \delta(i)\frac{r^x}{x} + \mathbf{O}\left(\frac{r^x \log x}{x^2}\right).$$

7. Positive density

If for some $\mathfrak{q} \in S$ we have $L^a_\mathfrak{q} = K$ or for some $q \in T$ we have $K_q = K$, then it follows that a is a primitive point for only finitely many primes $\wp$. In this section, we prove the converse to the above statement. That is, if K_q, $L^a_\mathfrak{q} \neq K$ for all $q \in T$, $\mathfrak{q} \in S$ then $\delta(x)$ is positive as x lies in some non-empty union of arithmetic progressions. Essentially, this will follow from a principal in [KL09], which we must combine with the reasoning of [GM86].

If all the extensions $L_{\mathfrak{q}}^a$ and K_q are geometric then we have the following result of Liu and the first author, which we have rewritten slightly for convenience. Essentially, it says that if a family of extensions are mostly linearly disjoint, then you can find a family of extensions in which distinct extensions are linearly disjoint.

Lemma 7.1 ([KL09, Lemma 15])**.** *Let $\mathcal{K}$ be a countable family of finite, separable, geometric extensions of K. Suppose that there is a subset $\mathcal{K}'$ such that $\mathcal{K}\backslash\mathcal{K}'$ is finite and distinct extensions in $\mathcal{K}'$ are linearly disjoint. Then there is a family of extensions $\mathcal{K}''$ such that distinct extensions in $\mathcal{K}''$ are linearly disjoint and $\mathcal{K}$ covers $\mathcal{K}''$. This means that if $L \in \mathcal{K}$ then there exists $L' \in \mathcal{K}''$ with $L' \subseteq L$ and if $L' \in \mathcal{K}''$ then there exists $L \in \mathcal{K}$ with $L' \subseteq L$.*

Using this lemma, one concludes that the density of primes that do not split completely in any $L' \in \mathcal{K}''$ is positive, and this is a lower bound for the density of primes that do not split completely in any $L \in \mathcal{K}$. For the proofs of the following theorems trace through the proof of [KL09, Theorem 3'].

Theorem 7.2. *Recall that for primes q of A, we have $K_q = K(\psi[q])$ and for primes $\mathfrak{q}$ of B, we have $L_{\mathfrak{q}}^a = K(\mathfrak{q}^{-1}\langle a\rangle)$.*

Put $\mathcal{K}_1 = \{K_q\} \cup \{L_{\mathfrak{q}}^a\}$ where q runs over primes of A and $\mathfrak{q}$ runs over primes of B of first-degree, and put $\mathcal{K}_2 = \{L_{\mathfrak{q}}^a\}$ where $\mathfrak{q}$ runs over all primes of B.

If $\mathcal{K}_i$ is a family of non-trivial, geometric extensions of K, then the density of primes that do not split completely in any member of $\mathcal{K}_i$ is $\delta_i > 0$.

By Theorems 6.11 and 6.12, we have

$$N_a(x) \sim \delta_1 \pi_K(x)$$

and

$$N_a'(x) \sim \delta_2(x)\pi_K(x),$$

where $\pi_K(x)$ is the number of primes of K of degree x.

Extending the ideas of [KL09], we are able to drop the assumption that all the extensions are geometric. We follow the proof of [KL09, Theorem 3'] with additional considerations for the case that not all of the extensions are geometric. We must also use the arguments of [GM86].

Let us review the key notations from the previous section.

(i) T (resp. T_0, resp. T') - the set of prime ideals of A, (resp. which divide M_1, resp. which are coprime to M_1)
(ii) T^*, (resp. T_0^*, resp. T'^*) - ideals of A which are square-free products of ideals in T (resp. T_0, resp. T').
(iii) S (resp. S_0, resp. S') - the set of prime ideals of B which are first-degree over A (resp. and which divide M_1, resp. and which are coprime to M_1)
(iv) S^* (resp. S_0^*, resp. S'^*) - the set of ideals of B which are square-free products of ideals in S (resp. S_0, resp. S'),
(v) $n(\mathfrak{a}, s)$ - the degree $[L_{\mathfrak{a},s}^a : K]$
(vi) $\mathbb{F}_{\mathfrak{a},s}$ - the algebraic closure of $\mathbb{F}_r$ inside $L_{\mathfrak{a},s}^a$
(vii) $j(\mathfrak{a}, s)$ - the degree $[\mathbb{F}_{\mathfrak{a},s} : \mathbb{F}_r]$
(viii) $f(\mathfrak{a}, s, x) = \begin{cases} j(\mathfrak{a}, s)\mu(\mathfrak{a})\mu(s)n(\mathfrak{a}, s)^{-1} & \text{if } j(\mathfrak{a}, s)|x \\ 0 & \text{otherwise} \end{cases}$
(ix) $\delta(x) = \sum_{\mathfrak{a},s} f(\mathfrak{a}, s, x)$

Lemma 7.3. *As $\mathfrak{a}$ runs over ideals of S^* and s runs over ideals of T^*, the degree $j(\mathfrak{a}, s)$ attains its maximum, say J, for some $\mathfrak{a} \in S_0^*$ and $s_0 \in T_0^*$, if we allow ourselves to add at most one exceptional prime to each of S_0 and T_0.*

Proof. To see this, we can appeal to the fact that the extensions $L_{\mathfrak{q}}^a$ for $\mathfrak{q}$ prime ideals of B coprime to M_1 are pairwise linearly disjoint over K by Corollary 4.1, so at most one has a non-trivial constant field extension. Similarly, the fields K_q as q runs over prime ideals of A coprime to M_1 are pairwise linearly disjoint. Letting these exceptions be absorbed by S_0 and T_0, we now assume the extensions $L_{\mathfrak{a}',s'}^a/K$ are geometric extensions of K for $\mathfrak{a}' \in S'^*$ and $s' \in T'^*$.

Alternatively, we can examine the constant fields of $L_{\mathfrak{a}',s'}^a$ and notice that all the division fields are contained in a finite extension of K_∞, by Proposition 5.9, and so the size of the constant field of $L_{\mathfrak{a}',s'}^a$ must be bounded independently of $\mathfrak{a}'$ and s'. By this argument, we only obtain that the constant field extensions are of bounded degree. □

We have the following theorem of Poonen.

Theorem 7.4 ([Poo95, Theorem 8])**.** *For fixed A, there is a constant $C > 0$ such that if ϕ is a rank 1 Drinfeld A-module over a global field L with $[L : K] = d$, then*

$$\#({}^{\phi}L)_{\text{tors}} \leq C \cdot d \log\log d.$$

For each A, this bound is best possible up to a constant factor.

Applying Poonen's result to our situation gives:

Corollary 7.5. *There exists a constant C' depending on B and $[K : \iota(\kappa)]$ such that if $L_{\mathfrak{q}}^a \neq K$ and $K_q \neq K$ for all primes $\mathfrak{q} \in S$ and primes $q \in T$ with $\deg \mathfrak{q} \leq C'$ and $\deg q \leq C'$ then $L_{\mathfrak{q}}^a \neq K$ and $K_q \neq K$ for all primes $\mathfrak{q} \in S$ and primes $q \in T$.*

We now give our positive density result. We may phrase the result as saying that the density of primes satisfying Artin's conjecture is positive, unless there is a good reason (read: K contains non-trivial division points of $\langle a \rangle$).

Theorem 7.6. *Suppose that $L_{\mathfrak{q}}^a \neq K$ for all primes $\mathfrak{q} \in S$ with $\deg \mathfrak{q} \leq C'$ and $K_q \neq K$ for all primes $q \in T$ with $\deg q \leq C'$. Then there is a non-empty set of conjugacy classes Z modulo J such that if $(x \pmod J) \in Z$ then $\delta(x) > 0$.*

If all the extensions K_q and $L_{\mathfrak{q}}^a$ are geometric and if $\mathbb{F}_K$ is the constant field of K, then we may take $J = [\mathbb{F}_K : \mathbb{F}_r]$ and $Z = \{0\}$ and $\delta(x) = \delta > 0$ for all $J|x$.

Proof. Following along with [KL09, Lemma 15 and Theorem 17] and the discussion after [GM86, Lemma 11], we will show that $\delta(x) = \delta_0(x)\delta_1$ where $\delta_0(x)$ only depends on the congruence class of x modulo J. Actually, $\delta_0(x)$ will be the density of primes of degree x that do not split completely in any of the fields $L_{\mathfrak{a}}^a$, K_q where $\mathfrak{q} \in S_0$ and $q \in T_0$.

By Corollary 4.1, if $\mathfrak{a} \in S^*$ and $s \in T^*$, then

$$n(\mathfrak{a}, s) = n(\mathfrak{a}_0, s_0)n(\mathfrak{a}', s')$$

where $\mathfrak{a}_0 \in S_0^*$ and $s_0 \in T_0^*$ and $\mathfrak{a}' \in S'^*$ and $s' \in T'^*$ Corollary 4.1 also gives that $n(\mathfrak{a}', s') = |\psi[\mathfrak{a}']| \cdot |(B/\mathfrak{b})^\times|$ where $\mathfrak{b} = \text{lcm}(\mathfrak{a}', s'B)$.

Furthermore, applying Lemma 7.3 gives that $L_{\mathfrak{a}',s'}^a/K$ is a geometric extension.

In any case, we have that

$$\begin{aligned}\delta(x) &= \sum_{\mathfrak{a},s} f(\mathfrak{a},s,x) \\ &= \sum\nolimits'_{\mathfrak{a}_0,s_0} f(\mathfrak{a}_0,s_0,x) \sum\nolimits''_{\mathfrak{a}',s'} f(\mathfrak{a}',s',x) \\ &= \delta_0(x)\cdot\delta_1.\end{aligned}$$

The first sum is taken over $\mathfrak{a}_0 \in S_0^*$ and $s_0 \in T_0^*$. The second sum is taken over $\mathfrak{a}' \in S'^*$ and $s' \in T'^*$ Notice that δ_1 does not depend on x since $f(\mathfrak{a}',s',x)$ corresponds only to geometric extensions of K. To see that $\delta_1 > 0$, let us expand δ_1 in a calculation similar to [GM86]. We have

$$\delta_1 = \sum_{s'} \mu(s')n(1,s')^{-1} \sum_{\mathfrak{a}'} \mu(\mathfrak{a}')\varphi((\mathfrak{a}',s'))/n(\mathfrak{a}',1),$$

and just as in [GM86]

$$= \sum_{s'} \mu(s')n(1,s')^{-1} \prod_{\mathfrak{q}} \left(1 - \frac{\varphi((\mathfrak{q},s'))}{n(\mathfrak{q},1)}\right).$$

Since $\varphi((\mathfrak{q},s')) = 1$ unless $\mathfrak{q}|s'$, we can bring most of the product over $\mathfrak{q} \in S$ to the front, and we leave behind a term in the sum over s',

$$= \prod_{\mathfrak{q}} \left(1 - n(\mathfrak{q},1)^{-1}\right) \sum_{s'} \mu(s')n(1,s')^{-1} \prod_{\mathfrak{q}|s'} \left(1 - r^{-\deg \mathfrak{q}}\right) \left(1 - n(\mathfrak{q},1)^{-1}\right)^{-1}.$$

Now, notice that the term in the sum over s' is multiplicative, and so

$$\begin{aligned}&= \prod_{\mathfrak{q}} \left(1 - n(\mathfrak{q},1)^{-1}\right) \\ &\prod_{q} \left(1 - n(1,q)^{-1}\right) \\ &\prod_{q} \left[1 - n(1,q)^{-1} \left(\frac{(1 - r^{-\deg \mathfrak{q}_1})(1 - r^{\deg \mathfrak{q}_2})}{(1 - n(\mathfrak{q}_1,1)^{-1})(1 - n(\mathfrak{q}_2,1)^{-1})}\right)\right] \\ &\prod_{q} \left[1 - n(1,q)^{-1} \left((1 - r^{-\deg \mathfrak{q}})(1 - n(\mathfrak{q},1)^{-1})^{-1}\right)\right]\end{aligned}$$

where the first product is over $\mathfrak{q} \in S'$, the second product is over $q \in T'$ which are inert in B, the second product is over primes $q \in T'$ such that qB factors as $\mathfrak{q}_1\mathfrak{q}_2$ with $\mathfrak{q}_1 \neq \mathfrak{q}_2$, and the third product is over primes $q \in T'$ with $qB = \mathfrak{q}^2$. Finally, bringing together the product over $\mathfrak{q} \in S'$ with the product over primes $q \in T'$ which are not inert in B gives

$$\begin{aligned}&= \prod_{q} \left(1 - (r^{2\deg q} - 1)^{-1}\right) \\ &\prod_{q} \left(1 - \frac{2}{(r^{\deg q} - 1)(r^{\deg q})} + \frac{1}{r^{2\deg q}(r^{\deg q} - 1)^2} - \frac{1}{r^{2\deg q}}\right) \\ &\prod_{q} \left(1 - \frac{1}{(r^{\deg q} - 1)r^{\deg q}} - \frac{1}{r^{2\deg q}}\right),\end{aligned}$$

the first product being over inert primes, the second over split primes, and the third over ramified primes.

This looks different than the infinite product in [GM86] (even after replacing $r^{\deg q}$ with q) but you can rearrange it to be sufficiently analogous. In particular $\delta_1 > 0$. We note that if κ/F is a separable extension then the product over ramified primes is a finite product. But if κ/F is inseparable, then all primes fall into the third category. In this case, the product looks different than the infinite product in [GM86].

Now onto δ_0 where we take the approach of Liu and the first author from [KL09]. It is not really possible to take the approach of [GM86], as we are examining a much broader collection of objects. First of all, note that if s divides t and $\mathfrak{a}$ divides $\mathfrak{b}$ then $j(\mathfrak{a}, s)$ divides $j(\mathfrak{b}, t)$. Let J be the maximum value of $j(\mathfrak{a}_0, s_0)$ as $\mathfrak{a}_0 \in S_0^*$ and $s_0 \in T_0^*$. Let $J' = [\mathbb{F}_K : \mathbb{F}_r]$. Then if we suppose $x \equiv 0 \pmod{J'}$ and $x/J' \equiv 1 \mod J/J'$, we have that

$$\delta_0(x) = \sum_{\mathfrak{a}_0, s_0} f(\mathfrak{a}_0, s_0, x),$$

where the sum is now over $\mathfrak{a}_0$ and s_0 such that $j(\mathfrak{a}_0, s_0) = J'$ (in other words, this sum is over the $\mathfrak{a}_0$ and s_0 which come from geometric extensions of K). This sum is non-empty because $j(1, 1) = J'$ refers to the constant field of K. By restricting to $x/J' \equiv 1 \mod J/J'$, we may consider only the geometric extensions. But now we can apply [KL09, Lemma 15] to see that as long as $L^a_{\mathfrak{q},1} \neq K$ and $K_q \neq K$ for all primes $q \in T$ and primes $\mathfrak{q} \in S$, we have $\delta(x) > 0$ for $x/J' \equiv 1 \pmod{J)/J'}$. In fact, this lemma requires that almost all the extensions be mutually linearly disjoint, but this condition trivially holds for a finite collection of fields. By Corollary 7.5 and the hypothesis of the theorem, we have that $K_q \neq K$ for all primes $q \in T$ and $L^a_{\mathfrak{q}} \neq K$ for all $\mathfrak{q} \in S$. This concludes the proof of the theorem. □

Remark 7.7. In fact the above analysis applies as long as $\gcd(J, x) = J'$. If not, write $J' < d = \gcd(J, x)$. Certainly $\delta(x) = \delta_0(x)\delta_1$ and $\delta_0(x)$ is the density of primes of K which do not split completely in any K_q or $L^a_{\mathfrak{q}}$ as the primes $q \in T_0$ and primes $\mathfrak{q} \in S_0$. But in this case the sum δ_1 is over $\mathfrak{a}_0$ and s_0 with $j(\mathfrak{a}_0, s_0)|d$. Now, even though we require that $L^a_{\mathfrak{q}} \neq K$ and $K_q \neq K$, it is possible that one of the extensions in question is exactly $L^a_{\mathfrak{q}} = K \cdot \mathbb{F}_{r^d}$, say. In this case we would have $\delta_0(x) = 0$. We cannot eliminate this case (in fact it is not hard to think of Drinfeld modules which have torsion that is a constant field extension), so we must conclude our analysis without saying anything further.

8. Examples

Here, we make a quick comparison to Artin's conjecture. Let $L_q = \mathbb{Q}(\sqrt[q]{a}, \sqrt[q]{1})$ and assume a is non-torsion (that is, $a \neq 0, \pm 1$). Then the condition that $L_q \neq \mathbb{Q}$ for all primes q is equivalent to the condition that a is not equal to a square. In this section, we give examples of Drinfeld modules for which all extensions $L^a_{\mathfrak{q}}$ and K_q are non-trivial. If we assume that $r \neq 2$, all the relevant extensions are non-trivial and geometric. This implies that the constant $\delta(x)$ is a positive constant as long as x is divisible by the degree of the constant field of K over $\mathbb{F}_r$. This family of examples includes those considered by Hsu and Yu in [HY01], but extends them by considering the case when $\deg \infty > 1$.

First we prove that the positivity results of [HY01] can be generalized to the situation when $\deg \infty > 1$. Let X be a smooth projective curve defined over $\mathbb{F}_r$ and ∞ a point of X of degree D. Let B be the ring of functions of X regular everywhere except possibly at ∞. Let κ be the fraction field of B.

Let κ_∞ be the completion of κ with respect to the valuation at ∞. Let $\mathbb{F}_\infty \subset \kappa_\infty$ be the residue field of κ_∞. Let $\operatorname{sgn} : \kappa_\infty^* \to \mathbb{F}_\infty^*$ be a sign function. That is, sgn is a group homomorphism and sgn restricts to the identity on $\mathbb{F}_\infty^*$. If $\sigma \in \operatorname{Gal}(\mathbb{F}_\infty/\mathbb{F}_r)$ then a twist of sgn is a function $\sigma \circ \operatorname{sgn}$.

Let H be the maximal unramified extension of κ which is completely split at ∞. That is, H is the Hilbert class field of B, and if $\mathcal{O}_H$ is the integral closure of B in H, then any principal ideal of B is the norm of an ideal in $\mathcal{O}_H$, and vice versa.

If C_∞ is the completion of an algebraic closure of κ_∞ and $L \subset C_\infty$. Then L is a B-field in a natural way using $B \subseteq \kappa \subseteq C_\infty$. If $\rho : B \to L\{\tau\}$ is a Drinfeld module then put $\mu_\rho(a)$ to be the leading coefficient of ρ_a for each $a \in B$ and ρ is called sgn-normalized if μ_ρ is a twist of sgn. Let $\phi : B \to L\{\tau\}$ be a sgn-normalized Drinfeld module of rank 1 and let H^+ be the field generated by κ and the coefficients of ψ. So in fact $\psi : B \to H^+\{\tau\}$.

Corollary 8.1 ([Gos96, Corollary 7.4.9])**.** *The Galois group* $\operatorname{Gal}(H^+/\kappa) \cong \mathcal{I}/\mathcal{P}^+$ *where* $\mathcal{I}$ *is the group of fractional ideals of* B *and* $\mathcal{P}^+$ *is the subgroup of principal fractional ideals generated by positive elements.*

So H^+ is the narrow class field of B relative to sgn.

Proposition 8.2 ([Gos96, Corollary 7.5.5])**.** $\operatorname{Gal}(H^+(\psi[\mathfrak{a}])/H^+) \cong (B/\mathfrak{a})^*$

Proposition 8.3 ([Gos96, Proposition 7.5.18])**.** *The extension* $H^+(\psi[\mathfrak{p}^m])/H^+$ *is totally ramified at all primes of* H^+ *lying above* $\mathfrak{p}$*.*

Let $K_\mathfrak{a} = H^+(\psi[\mathfrak{a}])$. Now let W be the B-submodule of H^+ generated by a. Put $L^a_\mathfrak{a}$ as in Definition 3.5.

If $r \neq 2$ or if $r = 2$ and $\mathfrak{a}$ is not divisible by any degree 1 prime, then $(B/\mathfrak{a})^*$ generates $B/\mathfrak{a}$ additively.

Recalling that $[\operatorname{Div}_{H^+}(W) : W]$ is finite, there is $c \in B$ such that $c \operatorname{Div}_{H^+}(W) \subseteq W$. Then if $r \neq 2$, applying [Pin16, Theorem 5.2], implies that $c \operatorname{Hom}_B(W, T_{\mathrm{ad}}) \subseteq \Delta$ where Δ is the image of the absolute Galois group.

If $\mathfrak{a}$ is such that $(B/\mathfrak{a})^*$ generates $B/\mathfrak{a}$ additively, then the proof of [HY01, Theorem 2.6(5)] tells us that $L^a_\mathfrak{a}/H^+$ is a geometric extension.

Combining this, if $r \neq 2$, the fields $L^a_\mathfrak{p}$ are linearly disjoint, geometric extensions of H^+ as $\mathfrak{p}$ runs over primes of B. If $r = 2$, we can say the same if we exclude degree 1 primes of B.

If we assume that $\operatorname{Div}_{H^+}(W)/(W)[\mathfrak{p}] \ncong (B/\mathfrak{p})^2$ if $r = 2$ and $\deg \mathfrak{p} = 1$, then $L^a_\mathfrak{p} \neq H^+$ for all $\mathfrak{p}$.

Applying Theorem 7.6 (or the analytic arguments of [HY01] combined with the new estimate Theorem 9.2) gives the following result. This is a generalization of Artin's conjecture for Drinfeld modules of rank 1 (cf. [HY01, Theorem 4.6]) to the case when $\deg \infty > 1$.

Theorem 8.4. *Suppose that* $\psi : B \to H^+\{\tau\}$ *is a* sgn*-normalized Drinfeld module of rank 1. Assume* $r \neq 2$*. Let* $N_a(x)$ *denote the number of primes* $\wp$ *of* H^+ *of degree* x *for which* a *modulo* $\wp$ *generates* $\mathbb{F}_\wp$ *as an* B*-module. Then there is a constant*

$\delta > 0$ such that

$$N_a(x) = \delta r^x/x + \mathbf{O}(r^x \log x/x^2)$$

as x tends to infinity, with $x \equiv 0 \mod D$.

Remark 8.5. If $r = 2$, then if we assume that $c\,\mathrm{Div}_{H^+}(W) \subseteq W$ and c has no prime divisor of degree 1, then it follows that every extension $L^a_{\mathfrak{q}}/K$ is non-trivial for all primes $\mathfrak{q}$ of A. But we cannot guarantee that the extensions are geometric in case $\mathfrak{q}$ is of degree 1. So in this case, the density of primes is still positive, but the constant is not so nice, and it depends on the congruence class of x modulo J for some J.

Now, suppose that $X, \infty, \kappa, B, \psi, H^+$ are as above and F is a subfield of κ such that $[\kappa : F] = 2$ such that there is a unique prime lying below ∞ (κ/F may be separable or inseparable). Let ∞' be the unique prime of F lying below ∞. Let A be $B \cap F$, so that B is the integral closure of A in κ.

Applying Theorems 1.4 and 7.6, we obtain examples of Drinfeld modules of rank 2 for which the density is positive.

Theorem 8.6. *Let $\phi : A \to H^+\{\tau\}$ be the restriction of ψ to $A = B \cap F$. Assume $r \neq 2$. Let $N_a(x)$ be the number of primes $\wp$ of H^+ of degree x such that a modulo $\wp$ generates $\mathbb{F}_\wp$ as an A-module under the action of ϕ.*

There exists $\delta > 0$ such that

$$N_a(x) = \delta r^x/x + \mathbf{O}(r^x \log x/x^2),$$

as x tends to infinity, with $x \equiv 0 \mod D$.

Remark 8.7. The case when $r = 2$ can be dealt with as in Remark 8.5.

9. Extension of the Brun-Titchmarsh theorem

We need to bound the number of primes of degree x congruent to 1 modulo $\mathfrak{q}$ where $\deg \mathfrak{q}$ is approximately $x/2$. As the degree of $\mathfrak{q}$ gets larger, this estimate becomes unnecessary. If the degree of $\mathfrak{q}$ is smaller the error term from the Chebotarev density theorem is manageable.

Let F be the function field of a curve X defined over $\mathbb{F}_r$ and ∞ a closed point of X of degree D and A be the ring of elements of F which are regular everywhere except possibly at ∞. In this section, we prove a Brun-Titchmarsh theorem for A, which extends the work of Hsu in [Hsu99], where it is assumed that $\deg \infty = 1$. We use Hsu's method to prove a version of the Brun-Titchmarsh theorem where $\deg \infty$ is not required to be 1.

Let $\mathfrak{a}$ be an ideal of A and $b \in A$ be coprime to $\mathfrak{a}$.

In the case that $\deg \infty = 1$, we have the following theorem of Hsu. In the statement of this theorem, g refers to the genus of X, h is the class number of A, $L(\cdot)$ is the L-function of X, N is a positive integer, H is the Hilbert class field of A, A' is the integral closure of A in H, and $\pi^H(N; b, \mathfrak{a})$ is the number of primes of $\wp$ of A', with $\mathrm{Norm}(\wp) = (P)$, (P) a principal ideal of A, $\deg P = N$, $\operatorname{sgn} P = 1$, and $P \equiv b \mod \mathfrak{a}$.

Theorem 9.1 ([Hsu99, Theorem 4.3])**.** *There exists effective constants C_1 and C_2 depending only on g and h such that if $N > \deg \mathfrak{a} + C_1 + C_2 \ln \deg \mathfrak{a}$ then we have*

$$\pi^H(N; b, \mathfrak{a}) \leq \frac{hr^N}{\varphi(\mathfrak{a}) \cdot (K_1 + 1 - 2g) \cdot L(1/r)}$$

where

$$K_1 = \min\left\{\left[\frac{N-1}{h}\right], \left[\frac{N-\deg\mathfrak{a}-C_1-C_2\ln\deg\mathfrak{a}+4g}{2}\right]\right\}.$$

We are able to adapt the arguments of Hsu to prove that a similar theorem holds when $D = \deg\infty \neq 1$. In the following theorem, $\pi(N; b, \mathfrak{a})$ is the number of principal prime ideals of A of the form (P) with $P \equiv b \mod \mathfrak{a}$, and $\deg P = N$. Notice that we count principal prime ideals of A while Hsu counts the primes of A' whose norm is principal and generated by a positive element in A

Theorem 9.2. *Suppose $N \geq \deg\mathfrak{a} + 4D + 7g - 4$ and N is larger than some fixed constant. Then*

$$\pi(N; b, \mathfrak{a}) \leq \frac{2(1-r^{-1})r^D r^N}{\varphi(\mathfrak{a})\cdot(N-\deg\mathfrak{a}-7g-4D+6)\cdot L(1/r)}.$$

One can also check that the arguments of [Hsu99] can be adapted to bound the number of prime ideals of the form (P) with $P \equiv b \mod \mathfrak{a}$ and $\operatorname{sgn}(P) = c$ where sgn is a sign function and c is an element of $\mathbb{F}_\infty$.

Fractional ideals of A correspond to divisors of X supported outside ∞. The degree function will be taken relative to $\mathbb{F}_r$. For an ideal I of A, put $\deg I = \log_r(|A/I|)$, for $a \in A$ put $\deg a = \log_r(|A/(a)|)$, for a prime $P = (O_P, m_P)$, an ordered pair of a discrete valuation ring and its corresponding maximal ideal put $\deg P = \log_r(|O_P/m_P|)$ and for a divisor $\mathfrak{D} = \sum_P n_P \cdot P$ put $\deg\mathfrak{D} = \sum_P n_P \deg P$. A divisor of X is effective if all $n_P \geq 0$. Recall the Riemann-Roch theorem.

Theorem 9.3 ([Ros02, Theorem 5.4])**.** *Let $\mathfrak{D}$ be a divisor on X and let $\mathcal{C}$ be a canonical divisor. Then*

$$\ell(\mathfrak{D}) - \ell(\mathcal{C}-\mathfrak{D}) = \deg\mathfrak{D} - g + 1,$$

where

$$\ell(\mathfrak{D}) = \dim_{\mathbb{F}_r}(L(\mathfrak{D})),$$

and

$$L(\mathfrak{D}) = \{x \in F \mid \operatorname{Div}(x) + \mathfrak{D} \geq 0\}.$$

In particular $L(\mathfrak{D}) \neq \emptyset$ if $\deg\mathfrak{D} \geq g$ and $\ell(\mathfrak{D}) = \deg\mathfrak{D} - g + 1$ if $\deg\mathfrak{D} \geq 2g-1$.

Let F_∞ be the completion of F with respect to the prime ∞. Then if $\mathbb{F}_\infty$ is the residue field at ∞, we have $\mathbb{F}_\infty \subseteq F_\infty$.

A sign function on F_∞ is a group homomorphism $\operatorname{sgn} : F_\infty^* \to \mathbb{F}_\infty^*$ which is the identity on $\mathbb{F}_\infty^*$. Given a sign function, sgn, a uniformizer can be chosen $\pi \in F_\infty$ with $\operatorname{sgn}(\pi) = 1$. To see this just choose $\pi \in m_\infty - m_\infty^2$ and scale by an element of $\mathbb{F}_\infty^*$ to obtain $\operatorname{sgn}(\pi) = 1$. Since sgn is trivial on $U_1 = \{x \in O_\infty \mid x \equiv 1 \mod m_\infty\}$ we may choose $\pi \in F$. Recall that the differential of π gives a divisor, see [Sti09, Chapter 4].

Taking $\mathcal{C} = \operatorname{Div}(d\pi)$ gives a canonical divisor class which is supported outside ∞ and so corresponds to a fractional ideal of A, which we also denote by $\mathcal{C}$. There is an isomorphism $F_\infty \cong \mathbb{F}_\infty((\pi))$.

Let $\operatorname{trace}_p^r : \mathbb{F}_r \to \mathbb{F}_p$ be the trace map where $p = \operatorname{Char}(\mathbb{F}_r)$. So, $\operatorname{trace}_r^{r^D} : \mathbb{F}_\infty \to \mathbb{F}_r$ and $\operatorname{trace}_p^{r^D} : \mathbb{F}_\infty \to \mathbb{F}_p$ will also be trace maps and clearly $\operatorname{trace}_p^r \circ \operatorname{trace}_r^{r^D} = \operatorname{trace}_p^{r^D}$. For $f \in F_\infty$, let $\operatorname{res}_\infty(f\, d\pi)$ be the residue of $f\, d\pi$ at ∞ as in [Tat68], see also [Sti09, Chapter 4]. In particular if $f = \sum_{n \geq N_f} c_n \pi^n$ then $\operatorname{res}_\infty(f\, d\pi) = \operatorname{trace}_r^{r^D}(c_{-1})$.

Define $E : \mathbb{F}_r \to \mathbb{C}^\times$ by $E(x) = \exp(\mathrm{trace}_p^r(x) \cdot 2\pi i/p)$. Define $T : F_\infty \to \mathbb{C}^\times$ by $T(f) = E(\mathrm{res}_\infty(f\, d\pi))$. Finally, define a bilinear form $B(x, f) = T_f(x) = T(fx)$ so $B : F_\infty \times F_\infty \to \mathbb{C}^\times$.

Let $I(y, N) = \{x \in F_\infty \mid \mathrm{ord}_\infty(x - y) \geq N\}$, which is an interval in F_∞ centred at y. We can define a Haar measure μ on F_∞ by putting $\mu(I(0, 0))(= \mu(O_\infty)) = 1$.

Let $\mathfrak{a}$ be a fractional ideal of A and k be an integer. Notice that

$$L(k\infty - \mathfrak{a}) \subseteq I(0, -k).$$

If

$$kD - \deg \mathfrak{a} \geq 2g - 1$$

then there is a $\mathbb{F}_r$-subspace $V \subseteq I(0, -k)$ with

$$I(0, -k) = L(k\infty - \mathfrak{a}) \oplus V.$$

Again, by the Riemann-Roch Theorem,

$$I(0, -n) = L(n\infty - \mathfrak{a}) \oplus V$$

for $n \geq k$.

In particular, $F_\infty = \mathfrak{a} \oplus V$. This implies that

$$\mu(F_\infty/\mathfrak{a}) = \mu(V) = r^{Dn} \cdot r^{-Dn + \deg \mathfrak{a} + g - 1} = r^{\deg \mathfrak{a} + g - 1}.$$

Also, if we write $\mathfrak{a} = U_k \oplus L(k\infty - \mathfrak{a})$ then

$$F_\infty = \mathfrak{a} \oplus V = U_k \oplus L(k\infty - \mathfrak{a}) \oplus V = U_k \oplus I(0, -k)$$

as long as $kD - \deg \mathfrak{a} \geq 2g - 1$.

Remark 9.4. Although, the lemmas and the general strategy for the proof come from [Hsu99], it should be noted that this result is for $\deg \infty \geq 1$ and the main result of [Hsu99] assumes $\deg \infty = 1$. For example, in the following lemma, the proof in [Hsu99] does not apply verbatim to the case $\deg \infty > 1$.

Lemma 9.5 ([Hsu99, Lemmas 2.1 and 2.2])**.** *Let $y \in F_\infty - F$ and $\mathfrak{b}$ be a fractional ideal of A. Then the closure of $\mathfrak{b}y + \mathfrak{b}$ is equal to F_∞.*

Proof. Fix k such that $kD - \deg \mathfrak{b} \geq 2g$. Then write $\mathfrak{b} = U_k \oplus L(k\infty - \mathfrak{b})$. Then we have a decomposition $F_\infty = U_k \oplus I(0, -k)$.

The pigeon hole principle implies that 0 is an accumulation point for $U_k + y\mathfrak{b}$ since $y \notin F$.

Now let $x \in F_\infty$. Write $x = u + x'$ with $x' \in I(0, -k)$, $u \in U_k$. Let $N > 0$ be given. There is an element $Y \in U_k + y\mathfrak{b}$ with $\mathrm{ord}_\infty(Y) \geq N + k$. Write $\mathrm{ord}_\infty(Y) = N' + k \geq N + k$. So if $a \in L((N' + 2k)\infty)$ then we have $\mathrm{ord}_\infty(aY) \geq -k$, that is $aY \in I(0, -k)$. Furthermore, $aY \in I(0, N')$ if and only if $\mathrm{ord}_\infty(a) + N' + k \geq +N'$ that is $a \in L(k\infty)$. By the Riemann-Roch theorem, the aY as a ranges over $L((N' + 2k)\infty)/L(k\infty)$ give distinct classes in $I(0, -k)/I(0, N')$. But both have the same dimension over $\mathbb{F}_r$, so there exists a such that $aY - x' \in I(0, N')$ which proves the result. □

Theorem 9.6 ([Hsu99, Theorem 2.3])**.** *Recall that $B : F_\infty \times F_\infty \to \mathbb{C}^\times$ is defined by*

$$B(f, g) = T(fg) = \exp(\mathrm{trace}_p^r(\mathrm{res}_\infty(fg\, d\pi))2\pi i/p).$$

Then, under B, F_∞ is identified with its Pontryagin dual, and the orthogonal complement of any fractional ideal $\mathfrak{a}$ of A, under B is $\mathfrak{a}^{-1}\mathcal{C}^{-1}$.

Proof. First let us prove that B is non-degenerate. Then the isomorphism

$$F_\infty \cong \mathbb{F}_\infty((\pi))$$

will show that the dual of F_∞ under B is F_∞.

Suppose that $x \in F_\infty$ is such that $B(x,y) = 1$ for all $y \in F_\infty$. That would mean that $\operatorname{trace}_p^r \operatorname{res}_\infty(xy\ d\pi) = 0$ for all y. Then writing $x = \sum x_i \pi^i$ and $y = \sum y_j \pi^j$, with $x_i, y_j \in \mathbb{F}_\infty$, we have

$$\operatorname{trace}_p^r(\operatorname{res}_\infty(xy\ d\pi)) = \sum \operatorname{trace}_p^r(x_j y_{-1-j}),$$

and by letting y vary over all F_∞, we see that $x_j = 0$ for all j, (remember that $\operatorname{trace}_p^r(xy)$ is non-degenerate on $\mathbb{F}_\infty$). So $x = 0$ and B is non-degenerate.

Let $a \in \mathfrak{a}$ and $x \in \mathfrak{a}^{-1}\mathcal{C}^{-1}$. Then the divisor of the differential $ax\ d\pi$ is effective which implies $\operatorname{res}_\infty(ax\ d\pi) = 0$ by the residue theorem. So $B(a,x) = 1$. This proves $\mathfrak{a}^{-1}\mathcal{C}^{-1} \subseteq \mathfrak{a}^\perp$.

Suppose that $x \in F_\infty$ with $B(a,x) = 1$ for all $a \in \mathfrak{a}$ (i.e., $x \in \mathfrak{a}^\perp$.) This implies that $\operatorname{res}_\infty(ax\ d\pi) = 0$. Suppose $x \notin F$. Then $x \cdot A + \mathfrak{a}^{-1}\mathcal{C}^{-1} \subseteq \mathfrak{a}^\perp$. Taking $\mathfrak{B} = A \cap \mathfrak{a}^{-1}\mathcal{C}^{-1}$ implies that $\mathfrak{B}x + \mathfrak{B} \subseteq \mathfrak{a}^\perp$ which implies that $\mathfrak{a}^\perp = F_\infty$ by Lemma 9.5, which is impossible.

So $x \in F$. Say $x \notin \mathfrak{a}^{-1}\mathcal{C}^{-1}$. We have $\mathfrak{a}^{-1}\mathcal{C}^{-1} \subseteq \mathfrak{a}^\perp \subseteq F$. In this case, there exists $f \in \mathfrak{a}$ such that $xf\ d\pi$ has order -1 at some prime of A and non-negative order at every other prime of A. By the residue theorem again, we have $\operatorname{res}_\infty(xf\ d\pi) \neq 0$, that is $x \notin \mathfrak{a}^\perp$. This proves that $\mathfrak{a}^\perp = \mathfrak{a}^{-1}\mathcal{C}^{-1}$. □

If $f : F_\infty \to \mathbb{C}$ is locally constant with compact support then define

$$\hat{f}(x) = \int_{F_\infty} f(y)\overline{T_x(y)}\ dy.$$

Lemma 9.7 ([Hsu99, Lemma 2.4])**.** *Define* $\Phi(x) = 1$ *if* $x \in O_\infty$ *and* 0 *otherwise. Then*

$$\widehat{\Phi} = \Phi, \quad \langle \Phi, \Phi \rangle = \int_{F_\infty} \Phi(y)\overline{\Phi(y)}\ dy = 1.$$

Proof. Consider

$$\begin{aligned}\widehat{\Phi}(x) &= \int_{O_\infty} \overline{T_x(y)}\ dy \\ &= \int_{O_\infty} \exp(-\operatorname{trace}(\operatorname{res}_\infty(xy\ d\pi))2\pi i/p)\ dy\end{aligned}$$

If $x \in O_\infty$ then $\operatorname{res}_\infty(xy\ d\pi) = 0$. If $x \notin O_\infty$ then write

$$x = x_{-k}\pi^{-k} + \cdots + x_{-1}\pi^{-1} + x' \neq x',$$

where $x' \in O_\infty$, and then

$$\begin{aligned}\widehat{\Phi}(x) &= \sum_{y_0, y_1, \ldots, y_{k-1}} e^{\operatorname{trace}(\sum_j x_{-j} y_{j-1})2\pi i/p} \mu(\pi^k O_\infty) \\ &= \prod_{j=1}^{k} \left(\sum_{y \in \mathbb{F}_\infty} e^{\operatorname{trace}(x_{-j} y)2\pi i/p} \right) r^{-Dk} \\ &= 0\end{aligned}$$

since at least one of $x_{-k}, \dots, x_{-1}$ is non-zero and $\operatorname{trace}(xy)$ is a non-degenerate bilinear form on $\mathbb{F}_\infty$. □

Fix a positive integers N and K, let $f \in F_\infty$ and let m_1 and m_2 be the least integers satisfying $m_1 \cdot D \geq K + 2g - 2$, and $m_2 \cdot D \geq N$. Put $m = \max\{m_1, m_2\}$. Define $\phi : F_\infty \to \mathbb{C}$ by

$$\phi(y) = r^{Dm} T_f(y) \Phi(y/\pi^m).$$

Lemma 9.8 ([Hsu99, Lemma 2.5])**.** *We have*

(i) $\phi(y) = 0$ *if* $\operatorname{ord}_\infty(y) < m_1$.
(ii) $\|\phi\|_2^2 = r^{Dm}$.
(iii) $\widehat{\phi}(x) = 1$ *if* $x \in I(f, -m_2)$.

Proof. If $\operatorname{ord}_\infty(y) < m_1$ then $\operatorname{ord}_\infty(y/\pi^m) < m_1 - m < 0$ so $\Phi(y/\pi^m) = 0$.

Consider

$$\begin{aligned}\|\phi\|_2^2 &= \int_{F_\infty} r^{2Dm} |T_f(y)|^2 \Phi(y/\pi^m)^2 \, dy \\ &= r^{2Dm} \int_{F_\infty} \Phi(y/\pi^m)^2 \, dy\end{aligned}$$

Substituting $x = y/\pi^m$ gives

$$\begin{aligned}&= r^{Dm} \int_{F_\infty} \Phi(x)^2 \, dx \\ &= r^{Dm}\end{aligned}$$

Finally, suppose that $x \in F_\infty$ and $\operatorname{ord}_\infty(x - f) \geq -m_2$ then

$$\begin{aligned}\widehat{\phi}(x) &= \int_{F_\infty} r^{Dm} T_f(y) \Phi(y/\pi^m) \overline{T_x(y)} \, dy \\ &= r^{Dm} \int_{F_\infty} T_{f-x}(y) \Phi(y/\pi^m) \, dy\end{aligned}$$

Substituting $z = y/\pi^m$ gives

$$\begin{aligned}&= \int_{F_\infty} \Phi(z) \overline{T_{(x-f)\pi^m}(z)} \, dz \\ &= \widehat{\Phi}((x - f)\pi^m)\end{aligned}$$

Finally, because $\operatorname{ord}_\infty((x - f)\pi^m) \geq -m_2 + m \geq 0$, we have

$$= 1,$$

proving the final statement. □

Let $\mathbb{T} = F_\infty / \mathcal{C}^{-1}$, and then [Hsu99, Theorem 2.3] implies that $\widehat{\mathbb{T}} \cong A$ under the bilinear form B. That is if $b \in A$, then define $f_b(x) = B(x, b)$ for all $x \in F_\infty$. By [Hsu99, Theorem 2.3], $f_b : F_\infty / \mathcal{C}^{-1} \to \mathbb{C}$ satisfies $f_b(x + y) = f_b(x) f_b(y)$. That is, $b \mapsto f_b$ defines a map $A \to \hat{\mathbb{T}}$, which must be onto.

Furthermore, using the canonical map $F_\infty \to \mathbb{T}$, we can define an interval in $\mathbb{T}$ to be the image of an interval in F_∞, and we can define a measure on $\mathbb{T}$ in a similar way.

That is, put

$$I_{\mathbb{T}}(u, M) = \{y + \mathcal{C}^{-1} \mid \operatorname{ord}_\infty(y + m - u) \geq M \text{ for some } m \in \mathcal{C}^{-1}\}.$$

Elements $u_1, \ldots, u_\ell$ of $\mathbb{T}$ are called an M-space if $I_{\mathbb{T}}(u_i, M)$ are mutually disjoint.

Let V be the integer defined by the inequality

$$2g - 2 < VD \leq 2g - 2 + D,$$

then

$$I(0, V) \cap \mathcal{C}^{-1} = L(\mathcal{C} - V\infty) = \{0\},$$

since $\deg \mathcal{C} - VD < 0$. So

$$I(0, V) \to I_{\mathbb{T}}(0, V)$$

is a bijection.

Define $\phi_1(x) = \phi(x)$ if $x + \mathcal{C}^{-1} \in I_{\mathbb{T}}(0, V)$ and 0 otherwise. Now, if $x \in I(f, -m_2) \cap A$ we have

$$\begin{aligned}
\hat{\phi_1}(x) &= \int_{\mathbb{T}} \phi_1(y)\overline{T_y(x)}\, dy \\
&= \int_{F_\infty} \phi(y)\overline{T_y(x)}\, dy \\
&\text{since } \phi_1(x + \alpha) = \phi(x) \text{ if } x \in I(0, V) \text{ and } \alpha \in \mathcal{C}^{-1} \\
&= \hat{\phi}(x) = 1.
\end{aligned}$$

Theorem 9.9. *Let N, K, m_1, and m_2 be positive integers with $Dm_1 \geq K + 2g - 2$, $Dm_2 \geq N$ and $f \in F_\infty$. Suppose $u_1, \ldots, u_\ell$ is a m_1-space in $\mathbb{T}$ and $S : \mathbb{T} \to \mathbb{C}$ such that*

$$S(y) = \sum_{x \in I(f, -m_2) \cap A} a_x T_x(y),$$

for each $y \in F_\infty$, where $a_x \in \mathbb{C}$. Then

$$\sum_{i=1}^{\ell} |S(u_i)|^2 \leq r^{D(m+1)} \sum_{x \in I(f, -m_2) \cap A} |a_x|^2,$$

where $m = \sup\{m_1, m_2\}$.

Proof. Notice that $\hat{S}\hat{\phi_1} = \hat{S}$ since $\hat{\phi_1}(x) = 1$ if $x \in I(f, -m_2)$ and $\hat{S}(x) = 0$ if $x \notin I(f, -m_2)$.

By the properties of convolution $S = \phi_1 * S$.

So

$$S(u) = \int_{\mathbb{T}} \phi_1(u - y)S(y)\, dy.$$

By the definition of ϕ_1, we get

$$S(u) = \int_{F_\infty} \phi(u - y)S(y)\, dy.$$

Substituting u_i for u gives,

$$S(u_i) = \int_{I(u_i, m_1)} \phi(u_i - y)S(y)\, dy,$$

since $\phi(u_i - y) = 0$ if $\operatorname{ord}_\infty(u_i - y) < m_1$.

Then

$$|S(u_i)^2| = r^{Dm} \int_{I(u_i,m_1)} |S(y)|^2 \, dy.$$

Finally since $\{u_i\}$ form an m_1-space, we can bound the sum of $|S(u_i)|^2$ by

$$\sum_i |S(u_i)|^2 \leq r^{Dm} \int_{I(0,-1)} |S(y)|^2 \, dy,$$

since each $u_i + \mathcal{C}^{-1}$ has a representative in $I(0,-1)$, by writing $I(0,-1) = L(\mathcal{C} + \infty) \oplus V$ and noticing that $I(0,-k) = L(\mathcal{C} + k\infty) \oplus V$ for each $k \geq 1$.

The integral can be bounded by

$$r^{D(m+1)} \sum |a_x|^2,$$

as required. □

Let $G_1, \ldots, G_n$ be a family of finite abelian groups, with character groups $\widehat{G_i}$, and put $G = \prod_{i=1}^n G_i$. Let $S : G \to \mathbb{C}$. An element of $(g_i) \in G$ is called primitive if $g_i \neq 0$ for each i. Let $\Omega_i \subseteq \widehat{G_i}$ and let α_i be such that

$$\#\Omega_i \leq \alpha_i \cdot \#\widehat{G_i}$$

and $0 < \alpha_i \leq 1$. Finally, assume that S is such that the Fourier coefficients of S are supported on $\prod_{i=1}^n \Omega_i$.

Lemma 9.10 ([Ser08, Lemma 10.2.1])**.** *We have*

$$\sum_{\substack{g \in G \\ g \text{ primitive}}} |S(g)|^2 \geq |S(0)|^2 \prod \left(\frac{1 - \alpha_i}{\alpha_i} \right),$$

where 0 *is the identity of* G*.*

Fix positive integers N and K and $f \in F_\infty$. Let X be a subset of A. Now take $m_1' D > 2K + 2g - 2$ and $m_2 D \geq N$.

For each prime ideal $\mathfrak{p}$ of A fix $\alpha_\mathfrak{p}$ such that

$$|X_\mathfrak{p}| \leq \alpha_\mathfrak{p} \cdot |A/\mathfrak{p}|,$$

$X_\mathfrak{p}$ being the image of the canonical map $X \hookrightarrow A \to A/\mathfrak{p}$. Let S_K denote set of square-free ideals in A which have degree at most K.

We have the following large sieve inequality.

Theorem 9.11 ([Hsu99, Theorem 3.2])**.**

$$|I(f, -m_2) \cap X| \cdot C_K \leq r^{D(m_0+1)},$$

where

$$m_0 = \sup\{m_1', m_2\},$$

and

$$C_K = 1 + \sum_{\mathfrak{a} \in S_K} \prod_{\mathfrak{p} | \mathfrak{a}} \left(\frac{1 - \alpha_\mathfrak{p}}{\alpha_\mathfrak{p}} \right).$$

Proof. For each ideal $\mathfrak{A}$ of A, denote by $\mathbb{T}[\mathfrak{A}]$, the $\mathfrak{A}$ torsion elements of $\mathbb{T}$. That is,

$$\mathbb{T}[\mathfrak{A}] = \mathfrak{A}^{-1}\mathcal{C}^{-1}/\mathcal{C}^{-1}.$$

Let $\{u_i\}$ be the union of $\mathbb{T}[\mathfrak{A}]$ as $\mathfrak{A} \in S_K$. If $u_i \neq u_j$ with $u_i \in \mathbb{T}[\mathfrak{A}]$ and $u_j \in \mathbb{T}[\mathfrak{B}]$ then

$$0 \neq u_i - u_j \in \mathbb{T}[\mathfrak{A}\mathfrak{B}] = (\mathfrak{A}\mathfrak{B}\mathcal{C})^{-1}/\mathcal{C}^{-1}$$

and so $u_i - u_j \in L(\mathfrak{A} + \mathfrak{B} + \mathcal{C} - n\infty)$ for some n with $\mathrm{ord}_\infty(u_i - u_j) = n$. Since $u_i - u_j \neq 0$ we have $\deg \mathfrak{A} + \deg \mathfrak{B} + \deg \mathcal{C} - nD \geq 0$ that is,

$$nD \leq 2K + 2g - 2.$$

This proves that $\{u_j\}$ is a m_1'-space.

Define

$$S(u) = \sum_{x \in I(f, -m_2) \cap X} T_x(u),$$

and by [Hsu99, Theorem 2.6], we get

$$\sum |S(u_i)|^2 \leq r^{D(m_0+1)} \cdot \#(I(f, -m_2) \cap X).$$

Now fix $\mathfrak{A} \in S_K$ and apply [Ser08, Lemma 10.2.1], to the following families

$$\{G_i\} = \{\mathbb{T}[\mathfrak{P}] \mid \mathfrak{P} \text{ prime }, \mathfrak{P}|\mathfrak{A}\}$$

$$\{\Omega_i\} = \{(I(f, -m_2) \cap X)_{\mathfrak{P}} \mid \mathfrak{P} \text{ prime}, \mathfrak{P}|\mathfrak{A}\}$$

$$\{\alpha_i\} = \{\alpha_{\mathfrak{P}} \mid \mathfrak{P} \text{ prime}, \mathfrak{P}|\mathfrak{A}\}.$$

So we get

$$\sum_{\substack{u \in \mathbb{T}[\mathfrak{A}] \\ u \text{ is primitive}}} |S(u)|^2 \geq |S(0)|^2 \prod_{\substack{\mathfrak{P} \text{ prime} \\ \mathfrak{P}|\mathfrak{A}}} \left(\frac{1 - \alpha_{\mathfrak{P}}}{\alpha_{\mathfrak{P}}}\right).$$

Summing over all possible $\mathfrak{A} \in S_K$ and noticing that each u_i is primitive for exactly one $\mathfrak{A}$ gives the formula

$$\sum |S(u_i)|^2 \geq |S(0)|^2 C_K = \#(I(f, -m_2) \cap X)^2 \cdot C_K.$$

Therefore,

$$C_K \cdot \#(I(f, -m_2) \cap X)^2 \leq \sum |S(u_i)|^2 \leq r^{D(m_0+1)} \#(I(f, -m_2) \cap X),$$

giving

$$C_K \cdot \#(I(f, -m_2) \cap X) \leq r^{D(m_0+1)},$$

as was to be shown. □

Put $\phi(\mathfrak{A}) = |(A/\mathfrak{A})^\times|$, and $\mu(\mathfrak{A}) = (-1)^n$ if $\mathfrak{A}$ is the product of n distinct prime ideals, and 0 otherwise. The zeta function of the curve X is the sum

$$Z(t) = \sum_{\mathfrak{D}} t^{\deg \mathfrak{D}} = \prod_{\mathfrak{P} \in X} (1 - t^{\deg \mathfrak{P}})^{-1},$$

taken over positive divisors of X. We have that

$$Z(t) = \frac{L(t)}{(1-t)(1-rt)},$$

where $L(t)$ is a polynomial of degree $2g$, see [Ros02].

Proposition 9.12 ([Hsu99, Lemmas 4.1 and 4.2])**.** *Suppose that $K \geq 2g + D - 1$. Then*

$$\sum_{\deg \mathfrak{a} \leq K} (|A/\mathfrak{a}|)^{-1} \geq (K - 2g - D + 2)L(1/r)(1 - r^{-D})/(1 - r^{-1}),$$

and

$$\sum_{\mathfrak{a} \in S_K} (\phi(\mathfrak{a}))^{-1} \geq (K - 2g - D + 2)L(1/r)(1 - r^{-D})/(1 - r^{-1}).$$

If $\mathfrak{U}$ is an ideal of A and $K + \deg \mathfrak{U} \geq 2g + D - 1$ then

$$\sum_{\substack{\mathfrak{a} \in S_K \\ (\mathfrak{a}, \mathfrak{U}) = 1}} \phi(\mathfrak{a})^{-1} \geq \frac{\phi(\mathfrak{U})}{|A/\mathfrak{U}|}(K + \deg \mathfrak{U} - 2g - D + 2)L(1/r)(1 - r^{-D})/(1 - r^{-1}).$$

Proof. The generating function for ideals of A is

$$\frac{(1 - t^D)L(t)}{(1 - t)(1 - rt)} = (1 + t + \cdots + t^{D-1})L(t)/(1 - rt) = F(t)/(1 - rt),$$

where F is a polynomial.

If the coefficient of t^j in $F(t)$ is f_j then the coefficient of t^j in $F(t)/(1 - rt)$ is

$$\sum_{k=0}^{j} f_k r^{j-k}.$$

If $j \geq \deg F$ then this coefficient becomes

$$r^j F(1/r).$$

As $\deg F = 2g + D - 1$, and taking $K \geq 2g + D - 1$

Therefore,

$$\begin{aligned}\sum_{\deg \mathfrak{a} \leq K} |A/\mathfrak{a}|^{-1} &\geq \sum_{j=2g+D-1}^{K} F(1/r) = (K - (2g + D - 1) + 1)F(1/r) \\ &= (K - 2g - D + 2)L(1/r)(1 - r^{-D})/(1 - r^{-1}).\end{aligned}$$

Since $\phi(\mathfrak{a}) \leq |A/\mathfrak{a}|$ we get

$$\sum_{\mathfrak{a} \in S_K} \frac{1}{\phi(\mathfrak{a})} \geq (K - 2g - D + 2)L(1/r)(1 - r^{-D})/(1 - r^{-1}).$$

Now,

$$\begin{aligned}\sum_{(\mathfrak{a}, \mathfrak{U}) = 1, \mathfrak{a} \in S_K} \frac{1}{\phi(\mathfrak{a})} \cdot \frac{|A/\mathfrak{a}|}{\phi(\mathfrak{A})} &\geq \sum_{\deg \mathfrak{a} \leq K} |A/\mathfrak{a}|^{-1} \\ &= L(1/r)(K - 2g - D + 2)(1 - r^{-D})/(1 - r^{-1}),\end{aligned}$$

as long as $K \geq D + 2g - 1$. □

Now, let $\mathfrak{U} = (u)$ be a principal ideal of A. Let $b \in A$ be such that $(b) + (u) = 1$. Let $\pi(N; b, \mathfrak{U})$ be the number of prime ideals of the form (P) such that $P \equiv b \bmod \mathfrak{U}$. Then let $S(N; b, \mathfrak{U})$ be the set of elements c of A such that $(cu + b)$ is prime and $\deg c = N - \deg \mathfrak{U}$. Notice that for this choice of $\mathfrak{U}$, we must have that $\deg \mathfrak{U}$ and $\deg P$ are multiples of D, and so N must also be a multiple of D if $S(N; b, \mathfrak{U})$ is to be non-empty. Therefore, put $N - \deg \mathfrak{U} = Dm_2$.

Now, we will establish Theorem 9.2 in the case where $\mathfrak{U}$ is a principal ideal.

Theorem 9.13. *Let $\mathfrak{U} = (u)$ be a principal ideal of A. Let $b \in A$ be such that $(b) + (u) = 1$. Suppose $N > \deg \mathfrak{U} + 3D + 6g - 2$, $N > \deg b$, then*

$$\pi(N; b, \mathfrak{U}) \leq \frac{2(1 - r^{-1})r^D r^N}{\phi(\mathfrak{U})(N - \deg \mathfrak{U} - 3D - 6g + 4)L(1/r)}.$$

Proof. As long as $\deg b < N$, we have $\pi(N; b, \mathfrak{U}) \leq |S(N; b, \mathfrak{U})|$. And there is a natural map

$$S(N; b, \mathfrak{U}) \to S(N; b, \mathfrak{U})_{\mathfrak{p}}$$

if $\mathfrak{p}$ is a prime of A with $\deg \mathfrak{p} < N$ and $\mathfrak{p} \nmid \mathfrak{U}$.

Furthermore, if $\mathfrak{p} \nmid \mathfrak{U}$ then $cu + b \neq 0$ modulo $\mathfrak{p}$ and so $c \neq -b/u$ modulo $\mathfrak{p}$ since $\mathfrak{p}$ is coprime to $\mathfrak{U}$. Therefore

$$|S(N; b, \mathfrak{U})_{\mathfrak{p}}| \leq \alpha_{\mathfrak{p}} |A/\mathfrak{p}|$$

with $\alpha_{\mathfrak{p}} = \phi(\mathfrak{p})/|A/\mathfrak{p}|$ for each $\mathfrak{p}$ with $\mathfrak{p} \nmid \mathfrak{U}$.

Now, notice that

$$S(N; b, \mathfrak{U}) \subseteq \bigcup_{\zeta \in \mathbb{F}_\infty^\times} I(\zeta \pi^{-m_2}, -m_2 + 1),$$

where $m_2 D = N - \deg \mathfrak{U}$.

So putting $Z = S(N; b, \mathfrak{U})$ we see

$$Z = \bigcup_{\zeta} (Z \cap I(\zeta \pi^{-m_2}, -m_2 + 1))$$

and so

$$|Z| \leq (r^D - 1)(r^{D(m_0+1)})/C_K$$

where

$$m_0 = \sup(m_1, m_2 - 1),$$

with

$$m_1 D > 2K + 2g - 2,$$
$$m_2 D = N - \deg \mathfrak{U}.$$

Recall that C_K satisfies

$$\begin{aligned} C_K &= 1 + \sum_{\mathfrak{a} \in S_K} \prod_{\mathfrak{p} | \mathfrak{a}} (1 - \alpha_{\mathfrak{p}})/\alpha_{\mathfrak{p}} \\ &= \sum_{\substack{\mathfrak{a} \in S_K \\ (\mathfrak{a}, \mathfrak{U}) = 1}} \frac{1}{\phi(\mathfrak{a})} \\ &\geq \frac{\phi(\mathfrak{U})}{|A/\mathfrak{U}|} (K - 2g - D + 2) L(1/r)(1 - r^{-D})/(1 - r^{-1}), \end{aligned}$$

for $K \geq 2g + D - 1$.

So choose K as large as possible under the restriction $m_1 \leq m_2 - 1$. That is,

$$D m_1 = D m_2 - D = N - \deg \mathfrak{U} - D$$

so take K such that

$$2K + 2g - 2 < N - \deg \mathfrak{U} - D,$$

or

$$\frac{N - \deg \mathfrak{U} - D - 2g}{2} \leq K < \frac{N - \deg \mathfrak{U} + 2 - D - 2g}{2}.$$

We also need $K \geq 2g + D - 1$ which implies that

$$2g + D - 1 \leq N/2 - \deg \mathfrak{U}/2 - D/2 - g$$

so

$$N \geq 6g + 3D + \deg \mathfrak{U} - 2.$$

Under these conditions

$$\begin{aligned}(K - 2g - D + 2) &= \frac{2K - 4g - 2D + 4}{2} \\ &\geq \frac{N - \deg \mathfrak{U} - D - 2g - 4g - 2D + 4}{2} \\ &= \frac{N - \deg \mathfrak{U} - 3D - 6g + 4}{2}\end{aligned}$$

And with this choice of K we have $D(m_0 + 1) = Dm_2 = N - \deg \mathfrak{U}$ so

$$\begin{aligned}|Z| &\leq \frac{2(1 - r^{-1})(r^D - 1)r^N}{\phi(\mathfrak{U})(N + \deg \mathfrak{U} - 3D - 6g + 4)(1 - r^{-D})L(1/r)} \\ &= \frac{2(1 - r^{-1})r^D r^N}{\phi(\mathfrak{U})(N - \deg \mathfrak{U} - 3D - 6g + 4)L(1/r)},\end{aligned}$$

as required. □

Now suppose $\mathfrak{a}$ is not principal. We will now prove the main theorem of the section.

Theorem 9.2. *Suppose $N \geq \deg \mathfrak{a} + 4D + 7g - 4$ and N is larger than some fixed constant. Then*

$$\pi(N; b, \mathfrak{a}) \leq \frac{2(1 - r^{-1})r^D r^N}{\varphi(\mathfrak{a}) \cdot (N - \deg \mathfrak{a} - 7g - 4D + 6) \cdot L(1/r)}.$$

Proof. The elements of $\mathfrak{a}$ correspond to $L(k\infty - \mathfrak{a})$ as k tends to infinity. By the Riemann-Roch theorem, there is an element $u \in \mathfrak{a}$ with $\deg u \leq \deg \mathfrak{a} + g + D - 2$. For each equivalence class b' modulo (u) with $b' \equiv b$ modulo $\mathfrak{a}$, the previous theorem tells us that

$$\pi(N; b', (u')) \leq \frac{2(1 - r^{-1})r^D r^N}{\phi((u))(N - \deg \mathfrak{U} - (g + D - 2) - 3D - 6g + 4)L(1/r)}.$$

There are $\phi((u))/\phi(\mathfrak{a})$ such equivalence classes, and as long as N is large enough any prime which satisfies $P \equiv b$ modulo $\mathfrak{a}$ also satisfies $P \equiv b'$ modulo (u) for some b'. This gives the bound

$$\pi(N; b, \mathfrak{a}) \leq \frac{2(1 - r^{-1})r^D r^N}{\phi(\mathfrak{a})(N - \deg \mathfrak{a} - 7g - 4D + 6)L(1/r)},$$

as required. □

Remark 9.14. This theorem is sufficient for our use, but one may further bound the number of prime ideals of the form (P) with $\operatorname{sgn}(P) = c$ and $P \equiv b \mod \mathfrak{a}$.

10. Further work

The following problems may be addressed in the future. We may consider trying to extend the main theorem of this paper to this case when $B = \mathrm{End}_{K^{\mathrm{sep}}}(\phi) \subsetneq \mathcal{O}_\kappa$. You may consider this as an analogue to the work of Chen and Yu [CY05].

We can also consider extending the work of Gupta and Murty in [GM86] to the case when E is an elliptic curve over a number field K with complex multiplication by an order B in a quadratic imaginary extension of $\mathbb{Q}$. In this case, the class number of B need not be 1. By letting K' be a field over which the elements of B are defined, $E(K')$ becomes a B-module, and considering the extensions $K'(\mathfrak{q}^{-1}\langle a\rangle)$ makes generalizing Gupta and Murty's results to this situation seem reasonable. There are, of course, other problems that need to be dealt with in this situation. This will be the topic of future work.

The focus of this paper is when ϕ is of rank 2. We may consider the case when the rank of ϕ is 3 or higher, and ϕ has endomorphism ring as large as possible. That is, $B = \mathrm{End}_{K^{\mathrm{sep}}}(\phi)$ and that is $\psi : B \to K\{\tau\}$ is of rank 1.

We can also try to generalize the work of the authors in [KT15] to the case when A is not the ring $\mathbb{F}_q[T]$. Particularly useful would be the Kummer theory results, discriminant bounds, and the Brun-Titchmarsh theorem. These could also be used to generalize the results obtained by Kuan, Yao, and the first author in [KKY15], or other similar theorems of this type.

Finally, one may work through Section 9 with the restriction $\mathrm{sgn}(P) = c$ (see Remark 9.14).

Acknowledgements

We thank the anonymous referee for their careful reading and helpful suggestions.

References

[AG09] Amir Akbary and Dragos Ghioca, *Periods of orbits modulo primes*, J. Number Theory **129** (2009), no. 11, 2831–2842.

[Bil37] Herbert Bilharz, *Primdivisoren mit vorgegebener Primitivwurzel*, Math. Ann. **114** (1937), no. 1, 476–492.

[BK72] A. K. Bousfield and D. M. Kan, *Homotopy limits, completions and localizations*, Lecture Notes in Mathematics, Vol. 304, Springer-Verlag, Berlin-New York, 1972.

[CY05] Yen-Mei J. Chen and Jing Yu, *On primitive points of elliptic curves with complex multiplication*, J. Number Theory **114** (2005), no. 1, 66–87.

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[Dri74] V. G. Drinfel′d, *Elliptic modules*, Mat. Sb. (N.S.) **94(136)** (1974), 594–627, 656.

[FJ08] Michael D. Fried and Moshe Jarden, *Field arithmetic*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008, Revised by Jarden.

[Gar02] Francis Gardeyn, *Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld*, Arch. Math. (Basel) **79** (2002), no. 4, 241–251.

[GM86] Rajiv Gupta and M. Ram Murty, *Primitive points on elliptic curves*, Compositio Math. **58** (1986), no. 1, 13–44.

[Gos96] David Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 35, Springer-Verlag, Berlin, 1996.

[Hoo67] Christopher Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[Hsu97] Chih-Nung Hsu, *On Artin's conjecture for the Carlitz module*, Compositio Math. **106** (1997), no. 3, 247–266.

[Hsu99] ———, *The Brun-Titchmarsh theorem in function fields*, J. Number Theory **79** (1999), no. 1, 67–82.

[HY01] Chih-Nung Hsu and Jing Yu, *On Artin's conjecture for rank one Drinfeld modules*, J. Number Theory **88** (2001), no. 1, 157–174.

[KKY15] Yen-Liang Kuan, Wentang Kuo, and Wei-Chen Yao, *On an Erdős-Pomerance conjecture for rank one Drinfeld modules*, J. Number Theory **157** (2015), 1–36.

[KL09] Wentang Kuo and Yu-Ru Liu, *Gaussian laws on Drinfeld modules*, Int. J. Number Theory **5** (2009), no. 7, 1179–1203.

[Kow03] E. Kowalski, *Some local-global applications of Kummer theory*, Manuscripta Math. **111** (2003), no. 1, 105–139.

[KT15] Wentang Kuo and David Tweedle, *Primitive submodules for Drinfeld modules*, Math. Proc. Cambridge Philos. Soc. **159** (2015), no. 2, 275–302.

[KT20] ———, *A prime analogue Erdős-Pomerance result for Drinfeld modules with arbitrary endomorphism rings*, Proc. Amer. Math. Soc. **148** (2020), no. 9, 3733–3747.

[Mil14] James S. Milne, *A primer of commutative algebra*, 2014, Available at www.jmilne.org/math/.

[Pin16] Richard Pink, *Kummer theory for Drinfeld modules*, Algebra Number Theory **10** (2016), no. 2, 215–234.

[Poo95] Bjorn Poonen, *Local height functions and the Mordell-Weil theorem for Drinfel′d modules*, Compositio Math. **97** (1995), no. 3, 349–368.

[PR09] Richard Pink and Egon Rütsche, *Adelic openness for Drinfeld modules in generic characteristic*, J. Number Theory **129** (2009), no. 4, 882–907.

[Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[Ser08] ———, *Topics in Galois theory*, second ed., Research Notes in Mathematics, vol. 1, A K Peters, Ltd., Wellesley, MA, 2008, With notes by Henri Darmon.

[Sti09] Henning Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

[Tat68] J. Tate, *Residues of differentials on curves.*, Ann. Sci. Éc. Norm. Supér. (4) **1** (1968), no. 1, 149–159 (English).

Email address: wtkuo@uwaterloo.ca

Department of Pure Mathematics, University of Waterloo, Waterloo, ON, Canada, N2L 3G1

Email address: david.tweedle@sta.uwi.edu

Department of Mathematics and Statistics, University of the West Indies, St. Augustine Campus, St. Augustine, Trinidad and Tobago, WI