Compositio Math. 144 (2008) 827–848
doi:10.1112/S0010437X07003387

Frobenius fields for Drinfeld modules of rank 2

Alina Carmen Cojocaru and Chantal David

Abstract

Let ϕ be a Drinfeld module of rank 2 over the field of rational functions $F = \mathbb{F}_q(T)$, with $\mathrm{End}_{\bar{F}}(\phi) = \mathbb{F}_q[T]$. Let K be a fixed imaginary quadratic field over F and d a positive integer. For each prime $\mathfrak{p}$ of good reduction for ϕ, let $\pi_{\mathfrak{p}}(\phi)$ be a root of the characteristic polynomial of the Frobenius endomorphism of ϕ over the finite field $\mathbb{F}_q[T]/\mathfrak{p}$. Let $\Pi_\phi(K; d)$ be the number of primes $\mathfrak{p}$ of degree d such that the field extension $F(\pi_{\mathfrak{p}}(\phi))$ is the fixed imaginary quadratic field K. We present upper bounds for $\Pi_\phi(K; d)$ obtained by two different approaches, inspired by similar ones for elliptic curves. The first approach, inspired by the work of Serre, is to consider the image of Frobenius in a mixed Galois representation associated to K and to the Drinfeld module ϕ. The second approach, inspired by the work of Cojocaru, Fouvry and Murty, is based on an application of the square sieve. The bounds obtained with the first method are better, but depend on the fixed quadratic imaginary field K. In our application of the second approach, we improve the results of Cojocaru, Murty and Fouvry by considering projective Galois representations.

Contents

1. Introduction

For q a power of an odd rational prime, let $\mathbb{F}_q$ denote the finite field with q elements, $\bar{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$, $A := \mathbb{F}_q[T]$ the polynomial ring over $\mathbb{F}_q$, and $F := \mathbb{F}_q(T)$ the field of fractions of A. Let $\bar{F}$ be an algebraic closure of F, and F^{sep} a separable closure of F. With this notation, the prime at infinity, ∞, of F is the fixed prime of F for which A is the ring of elements regular away from ∞. We set $|0| = |0|_\infty := 0$ and for an element $0 \neq a \in A$ of degree $\deg a$, we set $|a| = |a|_\infty := q^{\deg a}$.

Let ϕ be a *Drinfeld A-module of rank 2 over F*. That is, if $\tau : x \mapsto x^q$ is the qth power Frobenius

Received 3 August 2006, accepted in final form 5 October 2007.
2000 Mathematics Subject Classification 11G09.
Keywords: Lang–Trotter conjecture, Chebotarev density theorem, square sieve, Mumford–Tate conjecture for Drinfeld modules.
The first author is supported in part by NSF grant DMS-0636750, and the second author is supported in part by a NSERC Discovery Grant.

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

endomorphism, then ϕ is a ring homomorphism

$$\phi : A \longrightarrow F\{\tau\}, \quad a \mapsto \phi_a := \sum_{i=0}^{N_a} a_i \tau^i,$$

such that:

(1) for any $a \in A$, ϕ_a has constant term a; and

(2) for any $a \in A$, $N_a = 2 \deg a$.

Here $F\{\tau\}$ denotes the ring of twisted polynomials over F, where τ satisfies $\tau\alpha = \alpha^q\tau$ for all $\alpha \in F$. Notice that the Drinfeld module ϕ is completely determined by

$$\phi_T = T + c(\phi)\tau + \Delta(\phi)\tau^2,$$

where $c(\phi), \Delta(\phi) \in F$. The coefficient $\Delta(\phi)$ is called *the discriminant of* ϕ.

Now let $\mathcal{L} \in A$ be a prime (i.e. a monic irreducible polynomial) and $n \in \mathbb{N}^*$. We define the $\mathcal{L}^n$*-torsion points* and the $\mathcal{L}$*-adic Tate module* of ϕ as follows:

$$\begin{aligned} \phi[\mathcal{L}^n] &:= \{\lambda \in \bar{F} : \phi_{\mathcal{L}^n}(\lambda) = 0\}, \\ \phi[\mathcal{L}^\infty] &:= \lim_{\vec{n}} \phi[\mathcal{L}^n], \\ T_{\mathcal{L}} &:= \operatorname{Hom}_{A_{\mathcal{L}}}(F_{\mathcal{L}}/A_{\mathcal{L}}, \phi[\mathcal{L}^\infty]), \end{aligned}$$

where $A_{\mathcal{L}}$ and $F_{\mathcal{L}}$ are the $\mathcal{L}$-completions of A and F, respectively. From the theory of Drinfeld modules we know that

$$\begin{aligned} \phi[\mathcal{L}^n] &\simeq (A/\mathcal{L}^n A) \times (A/\mathcal{L}^n A), \\ T_{\mathcal{L}}(\phi) &\simeq A_{\mathcal{L}} \times A_{\mathcal{L}}, \end{aligned}$$

and that $\operatorname{Gal}(F^{\text{sep}}/F)$ acts continuously on $T_{\mathcal{L}}(\phi)$, giving rise to a representation

$$\rho_{\mathcal{L}^\infty,\phi} : \operatorname{Gal}(F^{\text{sep}}/F) \longrightarrow \operatorname{Aut}(T_{\mathcal{L}}(\phi)) \simeq \mathrm{GL}_2(A_{\mathcal{L}}). \tag{1}$$

For a prime $\mathfrak{p}$ of A, unramified for $\rho_{\mathcal{L}^\infty,\phi}$, let $\sigma_{\mathfrak{p}}$ denote the Frobenius at $\mathfrak{p}$ in F^{sep}/F. Let $P_{\mathfrak{p}}(x)$ be the characteristic polynomial of $\rho_{\mathcal{L}^\infty,\phi}(\sigma_{\mathfrak{p}})$ and $a_{\mathfrak{p}}(\phi)$ the trace of $\rho_{\mathcal{L}^\infty,\phi}(\sigma_{\mathfrak{p}})$. It is an important result that $P_{\mathfrak{p}}(x)$ does not depend on $\mathcal{L}$ and, furthermore, is the characteristic polynomial of the Frobenius endomorphism of the reduction $\phi_{\mathfrak{p}}$ of ϕ over the finite field $A/\mathfrak{p}A$. Thus

$$P_{\mathfrak{p}}(x) = x^2 - a_{\mathfrak{p}}(\phi)x + \mu_{\mathfrak{p}}\mathfrak{p} \in A[x] \tag{2}$$

for some $\mu_{\mathfrak{p}} \in \mathbb{F}_q^*$. If we let $\pi_{\mathfrak{p}}(\phi)$ denote one of the roots of $P_{\mathfrak{p}}(x)$ in $\bar{F}$, then we also know that

$$|\pi_{\mathfrak{p}}(\phi)| = |\mathfrak{p}|^{1/2}.$$

Therefore

$$|a_{\mathfrak{p}}(\phi)| \leqslant |\mathfrak{p}|^{1/2}, \tag{3}$$

a statement that has a striking resemblance with Hasse's bound for elliptic curves.

We recall that $\mathfrak{p}$ is called a *supersingular* prime for ϕ if the endomorphism ring $\operatorname{End}_{\bar{\mathbb{F}}_q}(\phi_{\mathfrak{p}})$ has rank 4 (see [Yu95, p. 166]), and an *ordinary* prime for ϕ otherwise. Then, for the ordinary primes $\mathfrak{p}$ we have that $F(\pi_{\mathfrak{p}}(\phi))$ is imaginary quadratic (see [Yu95, p. 167]). For the sake of completeness, we recall that a quadratic function field $K = F(\sqrt{g(T)})$ is called *real* if ∞ splits in K, and *imaginary* otherwise. It can be shown (see [Ros02, p. 248]) that if $g(T) \in A$ is squarefree, of degree d and leading coefficient a_d, then K is real if d is even and a_d is a square in $\mathbb{F}_q^*$, and K is imaginary if d is odd, or d is even and a_d is not a square in $\mathbb{F}_q^*$. For us, $K = F(\sqrt{g(T)})$ will be such that $g(T) \in A$ is always squarefree and with $\deg g(T) \geqslant 1$.

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

The purpose of this paper is to treat the following question.

Question 1. Let q, A, F be as above. Let ϕ be a Drinfeld A-module of rank 2 over F, with $\operatorname{End}_{\bar{F}}(\phi) = A$. Let K be an imaginary quadratic field over F, and let d be a positive integer. What is the asymptotic behaviour of the function

$$\Pi_\phi(K; d) := \#\{\mathfrak{p} \text{ prime of } A : \mathfrak{p} \text{ ordinary}, \deg \mathfrak{p} = d, F(\pi_\mathfrak{p}(\phi)) = K\},$$

as $d \to \infty$?

This question is analogous to a famous question posed by Lang and Trotter in 1976 in the context of elliptic curves (see [LT76]). In analogy with the Lang–Trotter conjecture, we predict the following.

CONJECTURE 2. Let q, A, F be as above. Let ϕ be a Drinfeld A-module of rank 2 over F, with $\operatorname{End}_{\bar{F}}(\phi) = A$. Let K be an imaginary quadratic field over F, and let d be a positive integer. There exists a constant $c(\phi, K)$, depending on ϕ and K, such that

$$\Pi_\phi(K; d) \sim c(\phi, K) \frac{q^{d/2}}{d},$$

as $d \to \infty$.

Remark 3. In the corresponding conjecture for an elliptic curve $E/\mathbb{Q}$ without complex multiplication and a quadratic imaginary extension K of $\mathbb{Q}$, formulated by Lang and Trotter [LT76, p. 69], it is predicted that the number of ordinary rational primes $p \leqslant x$ for which the Frobenius field of E at p is K is asymptotically $c(E, K)\sqrt{x}/\log x$ for a positive constant $c(E, K)$. Similarly, a related conjecture of Lang and Trotter coming from the same heuristics predicts that the number of supersingular primes less than or equal to x of $E/\mathbb{Q}$ should be asymptotically $c(E)\sqrt{x}/\log x$ for some positive constant $c(E)$. In the case of Drinfeld modules it was proven by Poonen [Poo98] that there are Drinfeld A-modules over F of rank 2 with no supersingular primes. This does not happen for elliptic curves, as proven by Elkies [Elk87]. One could then imagine that there exist special rank 2 Drinfeld A-modules ϕ with no primes $\mathfrak{p}$ such that $F(\pi_\mathfrak{p}(\phi)) = K$, and in this case the constant $c(\phi, K)$ would be 0. The authors have not yet addressed the question of trying to find those special Drinfeld modules, if any, which seems an interesting one in the light of Poonen's paper.

Our aim in this paper is to obtain upper bounds for $\Pi_\phi(K; d)$, and not an asymptotic formula. These upper bounds will be obtained by two different approaches, which both rely in some way on the application of the Chebotarev density theorem for function fields.

The first approach was communicated by Serre to the authors of [CFM05] (see § 6 of their paper) in the context of elliptic curves. In our paper we apply this approach to Drinfeld modules; namely, by building a mixed Galois representation associated to the Drinfeld module ϕ and the quadratic field K, we are able to find a union of conjugacy classes describing the primes $\mathfrak{p}$ such that $F(\pi_\mathfrak{p}(\phi)) = K$; then we use the Chebotarev density theorem to estimate the number of such $\mathfrak{p}$. A similar mixed Galois representation was also considered by Lang and Trotter in [LT76] to make their conjectures in the case of elliptic curves.

The second approach is based on the square sieve and was developed for elliptic curves by Cojocaru, Fouvry and Murty [CFM05]. Using the techniques of our paper, we can improve the results of [CFM05]. This will be included in [CD08].

The main results of this paper are as follows.

THEOREM 4. *Let q, A, F be as above. Let ϕ be a Drinfeld A-module of rank 2 over F, with $\operatorname{End}_{\bar{F}}(\phi) = A$. Let K be an imaginary quadratic field over F, and let d be a positive integer.*

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

Then, as $d \to \infty$,

$$\Pi_\phi(K;d) \ll_{\phi,K} \frac{q^{(4/5)d}}{d^{1/5}}.$$

The implied $\ll_{\phi,K}$-constant depends on both ϕ and K, and, more precisely, it depends on the class number and number of units of K.

Theorem 5. *Let q, A, F be as above. Let ϕ be a Drinfeld A-module of rank 2 over F, with $\mathrm{End}_{\bar{F}}(\phi) = A$. Let $K = F(\sqrt{g(T)})$ be an imaginary quadratic field over F, and let d be a positive integer. Then, as $d \to \infty$,*

$$\Pi_\phi(K;d) \ll_\phi q^{(7/8)d}[d + \deg g(T)] + q^{(3/4)d}[d + \deg g(T)]^2 d.$$

The implied $\ll_\phi$-constant depends only on ϕ.

Theorem 5, even though weaker than Theorem 4, is uniform in K. This uniformity is essential in applications of the method to other problems concerning the reductions of ϕ modulo $\mathfrak{p}$, though we will not touch upon this in the present paper. However, we record the following consequence of the uniformity in Theorem 5.

Corollary 6. *Let q, A, F be as above. Let ϕ be a Drinfeld A-module of rank 2 over F, with $\mathrm{End}_{\bar{F}}(\phi) = A$. Let d be a positive integer. We denote by $\mathcal{D}_\phi(d)$ the set of distinct fields $F(\pi_\mathfrak{p}(\phi))$ obtained by running over ordinary primes $\mathfrak{p} \in A$ with $\deg \mathfrak{p} = d$. Then, as $d \to \infty$,*

$$|\mathcal{D}_\phi(d)| \gg_\phi \frac{q^{(1/8)d}}{d^2}.$$

The implied $\gg_\phi$-constant depends on ϕ.

Remark 7. In Question 1 we need to restrict our attention to Drinfeld A-modules over F with trivial endomorphism ring, for otherwise the question is already understood using classical theory. Indeed, if ϕ is a Drinfeld A-module over F, of rank 2, with non-trivial endomorphism ring, then we know that $\mathrm{End}_{\bar{F}}(\phi) \otimes_A F =: K$ is an imaginary quadratic extension of F. This implies that we have an embedding

$$K \subseteq \mathrm{End}_{\overline{A/\mathfrak{p}}}(\phi_\mathfrak{p}) \otimes_A F,$$

which is in fact an isomorphism, since $\mathfrak{p}$ is an ordinary prime for ϕ. We also have

$$F(\pi_\mathfrak{p}(\phi)) \subseteq \mathrm{End}_{A/\mathfrak{p}}(\phi_\mathfrak{p}) \otimes_A F \subseteq \mathrm{End}_{\overline{A/\mathfrak{p}}}(\phi_\mathfrak{p}) \otimes_A F.$$

Then, as both K and $F(\pi_\mathfrak{p}(\phi))$ are degree 2 extensions of F, they must be equal.

Remark 8. In Question 1 we also need to restrict our attention to primes of ordinary reduction, for otherwise $a_\mathfrak{p}(\phi) = 0$ and so $F(\pi_\mathfrak{p}(\phi))$ is uniquely determined by $\mathfrak{p}$.

In the course of the proof of Theorem 5 we touch upon the question of the distribution of the Frobenius traces $a_\mathfrak{p}(\phi)$, which has been studied in more generality in [Dav01] (see also the references therein). In particular, we deduce the following improvement of Theorem 1.1 of [Dav01] in the case of rank 2 Drinfeld modules.

Theorem 9. *Let q, A, F be as above. Let ϕ be a Drinfeld A-module of rank 2 over F, with $\mathrm{End}_{\bar{F}}(\phi) = A$. Let d be a positive integer, and let $t \in A$. Then, as $d \to \infty$,*

$$\Pi_\phi(t;d) := \#\{\mathfrak{p} \text{ prime of } A : a_\mathfrak{p}(\phi) = t, \deg \mathfrak{p} = d\} \ll_\phi \begin{cases} q^{(3/4)d} & \text{if } t = 0, \\ \dfrac{q^{(4/5)d}}{d^{1/5}} & \text{otherwise.} \end{cases}$$

The implied $\ll_\phi$-constant depends on ϕ.

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

We remark that similar results should hold true for Drinfeld A-modules over general function fields F over $\mathbb{F}_q(T)$, though the proofs will be much more technical. Also, by exploiting in depth features of Drinfeld modules which are divergent from those of elliptic curves, such as the Sato–Tate law, one could shed more light on some of the big barriers in the Lang–Trotter conjecture for Frobenius fields for elliptic curves and improve upon the results above for Drinfeld modules. Our present paper is a first step in such investigations.

2. Heuristic for Conjecture 2

In this section we present a brief heuristic argument in support of Conjecture 2. We do not, however, develop any probability model for our reasoning, nor do we attempt to predict a formula for the constant $c(\phi, K)$ that appears in the conjecture.

Let q, A, F be as in § 1. Let ϕ be a Drinfeld A-module over F, of rank 2. Let $K = F(\sqrt{g(T)})$ be an imaginary quadratic extension of F, with $g(T) \in A$ squarefree. We denote by h_K the class number of K, by $\mathcal{O}_K$ the integral closure of A in K, by $N_{K/F}(\cdot)$ the norm of K/F, and by H_K the Hilbert class field of K. We recall that $\mathcal{O}_K = A + A\sqrt{g(T)}$ and, for $\alpha_1, \alpha_2 \in A$, that $N_{K/F}(\alpha_1 + \alpha_2\sqrt{g(T)}) = \alpha_1^2 - g(T)\alpha_2^2$.

Now let $\mathfrak{p} \in A$ be an ordinary prime for ϕ, of degree d, and such that $F(\pi_{\mathfrak{p}}(\phi)) = K$. Using the definition of $\pi_{\mathfrak{p}}(\phi)$, we see that this implies that

$$a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p} = g(T)h(T)^2$$

for some $h(T) \in A$, or, in other words, that

$$\mu_{\mathfrak{p}}\mathfrak{p} = N_{K/F}\left(\frac{a_{\mathfrak{p}}(\phi)}{2} + \frac{h(T)}{2}\sqrt{g(T)}\right).$$

The assertion that $\mathfrak{p}$ is a norm from K to F is equivalent to the assertion that $\mathfrak{p}$ splits completely in H_K; by the Chebotarev density theorem (see § 4), this event happens with probability $1/(2h_K)$. Furthermore, if $\mathfrak{p}$ is a norm from K to F, say

$$\mathfrak{p} = N_{K/F}(a(T) + b(T)\sqrt{g(T)}),$$

then the event $a(T) = a_{\mathfrak{p}}(\phi)/2$ for some non-zero $|a_{\mathfrak{p}}(\phi)| \leqslant |\mathfrak{p}|^{1/2}$ happens with probability proportional to $1/|\mathfrak{p}|^{1/2}$. Assuming that the above two events are independent, we obtain that the probability that $F(\pi_{\mathfrak{p}}(\phi)) = K$ should be of the order of magnitude

$$\frac{1}{h_K|\mathfrak{p}|^{1/2}}.$$

Therefore, combining the above with the prime number theorem for function fields, we obtain that, heuristically, as $d \to \infty$,

$$\Pi_\phi(K; d) \approx \sum_{\substack{\mathfrak{p} \in A \\ \mathfrak{p} \text{ ordinary prime}}} \frac{1}{h_K|\mathfrak{p}|^{1/2}} \sim \frac{c(\phi)}{h_K}\frac{q^{d/2}}{d}$$

for some constant $c(\phi)$, depending on ϕ.

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

3. Galois representations

3.1 Galois representations associated to Drinfeld modules

Let q, A, F be as in the introduction. Let ϕ be a Drinfeld A-module over F, of rank 2. For a prime $\mathcal{L} \in A$, let $\rho_{\mathcal{L}^\infty,\phi}$ be the $\mathcal{L}$-adic representation associated to ϕ. Let $\hat{A}$ denote the ring

$$\hat{A} = \varprojlim_{\mathfrak{a}} A/\mathfrak{a}A,$$

where the projective limit is taken over all ideals $\mathfrak{a}$ in A. By putting together the $\mathcal{L}$-adic representations $\rho_{\mathcal{L}^\infty,\phi}$, we obtain a continuous representation

$$\rho_\phi : \mathrm{Gal}(F^{\mathrm{sep}}/F) \longrightarrow \mathrm{GL}_2(\hat{A}).$$

More generally, if ϕ is a Drinfeld A-module over F of arbitrary rank r, then the action of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ on the set of all torsion points $F_{\mathrm{tors}} := F(\phi_{\mathrm{tors}})$ of ϕ gives rise to a continuous representation

$$\rho_\phi : \mathrm{Gal}(F^{\mathrm{sep}}/F) \longrightarrow \mathrm{GL}_r(\hat{A}).$$

Here, ϕ_{tors} is the set of elements $\lambda \in \bar{F}$ for which there exists $a \in A$ such that $\phi_a(\lambda) = 0$. The Mumford–Tate conjecture for Drinfeld modules of rank r with trivial endomorphism ring asserts that ρ_ϕ has *open* image in $\mathrm{GL}_r(\hat{A})$. This general conjecture is still open; however, in the case of rank 2 Drinfeld modules it has been recently proven by Gardeyn and Pink (see Theorem 11 below).

Remark 10. A prior result due to Pink [Pin97] asserts that, for a fixed prime $\mathcal{L} \in A$, the Galois representation $\rho_{\mathcal{L}^\infty,\phi}$ defined in (1) has open image in $\mathrm{GL}_r(\mathcal{A}_{\mathcal{L}})$. This result could be used in our treatment of Question 1, using an approach similar to the one in [Dav01] for a question concerning the distribution of the values $a_{\mathfrak{p}}(\phi)$ for a Drinfeld A-module ϕ over F, of arbitrary rank. However, such an argument would have to be modified in several places to make it work for Question 1, as it is more complicated to deal with the rings $A/\mathcal{L}^n A$ than with the fields $A/\mathcal{L}A$.

Theorem 11 (Gardeyn and Pink, 2005). *Let q, A, F be as in § 1. Let ϕ be a Drinfeld A-module over a finite extension of F, of rank 2. Assume that $\mathrm{End}_{\bar{F}}(\phi) = A$. Let $\hat{A}$ be the ring of adeles of A. Then the action of the Galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ on the set of all torsion points of ϕ has open image in $\mathrm{GL}_2(\hat{A})$.*

Proof. The proof follows by combining the work of Pink [Pin97] and Gardeyn [Gar02b], and was pointed out to the authors by Richard Pink. As mentioned in the remark above, it was proven in [Pin97] that the representation with image in $\prod_{\mathcal{L}} \mathrm{GL}_r(A_{\mathcal{L}})$ has open image in generic characteristic provided that the product is over a *finite* set of primes. In Chapter 3 of his thesis, Gardeyn states a residual version of the Mumford–Tate conjecture applicable to Drinfeld modules in generic characteristic, and can prove this conjecture when the rank is at most 2. He then uses this result, and the result of Pink mentioned above, to prove the Mumford–Tate conjecture for Drinfeld modules in general characteristic. □

Throughout the paper we will consider in parallel the Galois representations with image in GL_2 and PGL_2. The PGL_2 case leads to better estimates in the Chebotarev density theorem whenever it can be applied, that is, in all our applications except Theorem 9. We will use the following corollaries to Theorem 11. One should point out that the following two corollaries are really intermediate steps in the proof of Theorem 11, Corollary 12 being the hard part, and Corollary 13 following relatively easily from Corollary 12.

Corollary 12. *Let q, A, F be as in § 1. Let ϕ be a Drinfeld A-module over F, of rank 2. Assume that $\mathrm{End}_{\bar{F}}(\phi) = A$. Then the representation*

$$\rho_{\mathcal{L},\phi} : \mathrm{Gal}(F^{\mathrm{sep}}/F) \longrightarrow \mathrm{GL}_2(A/\mathcal{L}A),$$

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

and its projection in $\mathrm{PGL}_2(A/\mathcal{L}A)$,

$$\hat{\rho}_{\mathcal{L},\phi} : \mathrm{Gal}(F^{\mathrm{sep}}/F) \longrightarrow \mathrm{PGL}_2(A/\mathcal{L}A),$$

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

For any Drinfeld A-module ϕ, we denote by $\mathcal{S}(\phi)$ the finite set of primes of A such that $\mathcal{L} \notin \mathcal{S}(\phi)$ implies that $\rho_{\mathcal{L},\phi}$ is surjective, as given by Corollary 12. The explicit dependence of the set $\mathcal{S}(\phi)$ in terms of ϕ was studied by Chen and Lee, and their work will appear in a forthcoming paper.

Corollary 13. *Let* q, A, F *be as in § 1. Let* ϕ *be a Drinfeld* A*-module over* F*, of rank* 2*. Assume that* $\mathrm{End}_{\bar{F}}(\phi) = A$*. Then, for all distinct primes* $\mathcal{L}_1, \mathcal{L}_2 \notin \mathcal{S}(\phi)$*, the representation*

$$\rho_{\mathcal{L}_1\mathcal{L}_2,\phi} : \mathrm{Gal}(F^{\mathrm{sep}}/F) \longrightarrow \mathrm{GL}_2(A/\mathcal{L}_1\mathcal{L}_2A) \simeq \mathrm{GL}_2(A/\mathcal{L}_1A) \times \mathrm{GL}_2(A/\mathcal{L}_2A),$$

corresponding to the Galois action on the A*-module*

$$\phi[\mathcal{L}_1\mathcal{L}_2] := \{\lambda \in \bar{F} : \phi_{\mathcal{L}_1\mathcal{L}_2}(\lambda) = 0\},$$

and its projection in $\mathrm{PGL}_2(A/\mathcal{L}_1\mathcal{L}_2A)$,

$$\hat{\rho}_{\mathcal{L}_1\mathcal{L}_2,\phi} : \mathrm{Gal}(F^{\mathrm{sep}}/F) \longrightarrow \mathrm{PGL}_2(A/\mathcal{L}_1\mathcal{L}_2A) \simeq \mathrm{PGL}_2(A/\mathcal{L}_1A) \times \mathrm{PGL}_2(A/\mathcal{L}_2A),$$

are surjective.

Let $F_{\mathcal{L},\phi}, E_{\mathcal{L},\phi}, F_{\mathcal{L}_1\mathcal{L}_2,\phi}$ and $E_{\mathcal{L}_1\mathcal{L}_2,\phi}$ be the fixed fields of the kernels of $\rho_{\mathcal{L},\phi}$, $\hat{\rho}_{\mathcal{L},\phi}$, $\rho_{\mathcal{L}_1\mathcal{L}_2,\phi}$ and $\hat{\rho}_{\mathcal{L}_1\mathcal{L}_2,\phi}$ respectively. Note that $F_{\mathcal{L},\phi} = F(\phi[\mathcal{L}])$ and $F_{\mathcal{L}_1\mathcal{L}_2,\phi} = F(\phi[\mathcal{L}_1\mathcal{L}_2])$. The following is a restatement of Corollaries 12 and 13.

Corollary 14. *Let* q, A, F *be as in § 1. Let* ϕ *be a Drinfeld* A*-module over* F*, of rank* 2*. Assume that* $\mathrm{End}_{\bar{F}}(\phi) = A$*. Then the representations*

$$\begin{aligned}
\rho_{\mathcal{L},\phi} &: \mathrm{Gal}(F_{\mathcal{L},\phi}/F) \longrightarrow \mathrm{GL}_2(A/\mathcal{L}A),\\
\hat{\rho}_{\mathcal{L},\phi} &: \mathrm{Gal}(E_{\mathcal{L},\phi}/F) \longrightarrow \mathrm{PGL}_2(A/\mathcal{L}A),\\
\rho_{\mathcal{L}_1\mathcal{L}_2,\phi} &: \mathrm{Gal}(F_{\mathcal{L}_1\mathcal{L}_2,\phi}/F) \longrightarrow \mathrm{GL}_2(A/\mathcal{L}_1A) \times \mathrm{GL}_2(A/\mathcal{L}_2A),\\
\hat{\rho}_{\mathcal{L}_1\mathcal{L}_2,\phi} &: \mathrm{Gal}(E_{\mathcal{L}_1\mathcal{L}_2,\phi}/F) \longrightarrow \mathrm{PGL}_2(A/\mathcal{L}_1A) \times \mathrm{PGL}_2(A/\mathcal{L}_2A)
\end{aligned}$$

are isomorphisms for all primes $\mathcal{L} \notin \mathcal{S}(\phi)$ *and all distinct primes* $\mathcal{L}_1, \mathcal{L}_2 \notin \mathcal{S}(\phi)$.

Remark 15. We remark that the Galois representation modulo $\mathcal{L}$ transforms the relation about the characteristic polynomial of the Frobenius at $\mathfrak{p}$ described by (2) into the congruence conditions

$$\begin{aligned}
\mathrm{tr}\, \rho_{\mathcal{L},\phi}(\sigma_{\mathfrak{p}}) &\equiv a_{\mathfrak{p}}(\phi) \pmod{\mathcal{L}},\\
\det \rho_{\mathcal{L},\phi}(\sigma_{\mathfrak{p}}) &\equiv \mu_{\mathfrak{p}}\mathfrak{p} \pmod{\mathcal{L}}.
\end{aligned}$$

Similarly, $\rho_{\mathcal{L}_1\mathcal{L}_2,\phi}$ gives rise to congruences modulo $\mathcal{L}_1\mathcal{L}_2$. These important properties are at the basis of the proofs of Theorems 4 and 5.

Corollary 16. *Let* q, A, F *be as in § 1. Let* ϕ *be a Drinfeld* A*-module over* F*, of rank* 2*. Assume that* $\mathrm{End}_{\bar{F}}(\phi) = A$*. Let* K/F *be any finite extension. Then, there exists a finite set of primes* $\mathcal{T} \subset A$ *such that, for all primes* $\mathcal{L} \notin \mathcal{T}$*, and for all distinct primes* $\mathcal{L}_1, \mathcal{L}_2 \notin \mathcal{T}$*, we have:*

(1) $K \cap F_{\mathcal{L},\phi} = F$;

(2) $F_{\mathcal{L},\phi}/F$ *is a geometric extension (i.e. the algebraic closure of* $\mathbb{F}_q$ *in* $F_{\mathcal{L},\phi}$ *is* $\mathbb{F}_q$ *itself; also, see § 4 for a more general definition); and*

(3) $F_{\mathcal{L}_1\mathcal{L}_2,\phi}/F$ *is a geometric extension (in the above sense).*

Furthermore, the same assertions hold for $E_{\mathcal{L},\phi} \subset F_{\mathcal{L},\phi}$ *and* $E_{\mathcal{L}_1\mathcal{L}_2,\phi} \subset F_{\mathcal{L}_1\mathcal{L}_2,\phi}$.

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

Proof. It follows from Theorem 11 that the image of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ in $\mathrm{GL}_2(\hat{A})$ contains an open set of the form

$$U_S \times \prod_{\mathcal{L} \notin S} \mathrm{GL}_2(A_{\mathcal{L}}),$$

where S is a finite set of primes of A, and $U_S \subseteq \prod_{\mathcal{L}\in S} \mathrm{GL}_2(A_{\mathcal{L}})$. Then, all the fields $F_{\mathcal{L},\phi}$ are disjoint for $\mathcal{L} \notin S$, and then K intersects at most one of them. This shows part (1). For parts (2) and (3), it suffices to recall that the degree of the algebraic closure of $\mathbb{F}_q$ in the (infinite) extension of F obtained by adding all torsion points of ϕ is finite [Dav01, Lemma 3.2], and then the second and third assertions follow from the first. □

3.2 Galois representations associated to imaginary quadratic fields

Let q, A, F be as in the introduction. Let $K = F(\sqrt{g(T)})$ be an imaginary quadratic field with $g(T) \in A$ squarefree. Following standard notation, we let $\mathcal{O}_K = A + A\sqrt{g(T)}$ be the integral closure of A in K, $U_K := \mathcal{O}_K^*$ the group of units of $\mathcal{O}_K$, and $\mathrm{Cl}(\mathcal{O}_K)$ the ideal class group of $\mathcal{O}_K$, of cardinality $h = h_K$. We recall that $\mathcal{O}_K$ is a Dedekind domain whose non-zero prime ideals are in 1:1 correspondence with the primes $\mathfrak{P}$ of K for which $\mathfrak{P} \nmid \infty$, and that U_K is a finite group, as K is a quadratic imaginary extension of F. Consequently, the class number h and the number of units $w = w_K := |U_K|$ of K are finite (see [Ros02, Chapter 14]). We write $\mathrm{Gal}(K/F) := \{1, \mathfrak{c}\}$ for the Galois group of K/F, where $\mathfrak{c}$ is the complex conjugation automorphism given by $\mathfrak{c}(\sqrt{g(T)}) = -\sqrt{g(T)}$. Often, for an element or ideal X of K, we write $\mathfrak{c}(X) = \overline{X}$.

Now we let $\mathcal{L} \in A$ be a fixed prime satisfying the conditions of Corollaries 12 and 16, and which splits completely in K, say as

$$\mathcal{L}\mathcal{O}_K = \mathfrak{L}\overline{\mathfrak{L}}.$$

Note that

$$\mathcal{O}_K/\mathcal{L}\mathcal{O}_K \simeq \mathcal{O}_K/\mathfrak{L} \times \mathcal{O}_K/\overline{\mathfrak{L}} \simeq A/\mathcal{L}A \times A/\mathcal{L}A. \tag{4}$$

For any non-zero prime ideal $\mathfrak{P} \in \mathcal{O}_K$, $\mathfrak{P}^h$ is a principal ideal, say $\mathfrak{P}^h = (\alpha)$ for some $\alpha \in \mathcal{O}_K$. Thus we can define the quantity

$$\pi_{\mathfrak{P}}(K) := \alpha^w \in \mathcal{O}_K, \tag{5}$$

which is uniquely determined by $\mathfrak{P}$. This defines a group homomorphism

$$\begin{aligned} \chi_{\mathfrak{L}} : \mathrm{Gal}(K^{\mathrm{sep}}/K) &\longrightarrow (\mathcal{O}_K/\mathfrak{L})^*, \\ \sigma_{\mathfrak{P}} &\mapsto \pi_{\mathfrak{P}}(K) \pmod{\mathfrak{L}}, \end{aligned}$$

where K^{sep} denotes the separable closure of K and $\sigma_{\mathfrak{P}}$ the Frobenius at $\mathfrak{P}$ in K^{sep}/K.

We are interested in the representation induced from $H := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ to $G := \mathrm{Gal}(F^{\mathrm{sep}}/F)$. Since H is a subgroup of index 2 of G, we may write $G = H \oplus H\mathfrak{c}$. Then the induced representation is

$$\begin{aligned} \rho_{\mathcal{L},K} : \mathrm{Gal}(F^{\mathrm{sep}}/F) &\longrightarrow \mathrm{GL}_2(A/\mathcal{L}A) \\ \sigma &\mapsto \begin{pmatrix} \chi_{\mathfrak{L}}(\sigma) & 0 \\ 0 & \chi_{\mathfrak{L}}(\mathfrak{c}\sigma\mathfrak{c}) \end{pmatrix} \quad \text{if } \sigma \in H, \\ \sigma &\mapsto \begin{pmatrix} 0 & \chi_{\mathfrak{L}}(\sigma\mathfrak{c}) \\ \chi_{\mathfrak{L}}(\mathfrak{c}\sigma) & 0 \end{pmatrix} \quad \text{if } \sigma \notin H, \end{aligned}$$

where we have used the isomorphism $\mathcal{O}_K/\mathfrak{L} \simeq A/\mathcal{L}A$ to write the image in $\mathrm{GL}_2(A/\mathcal{L}A)$.

Let $N_{\mathcal{L}} \leqslant \mathrm{GL}_2(A/\mathcal{L}A)$ be the image of the representation $\rho_{\mathcal{L},K}$, and let $PN_{\mathcal{L}}$ be its projective image, i.e. $PN_{\mathcal{L}}$ is the quotient of $N_{\mathcal{L}}$ by the scalars in $N_{\mathcal{L}}$. Let $\hat{\rho}_{\mathcal{L},K}$ be the composition of $\rho_{\mathcal{L},K}$ with this quotient. Finally, let $F_{\mathcal{L},K}$ and $E_{\mathcal{L},K}$ be the fixed fields of the kernel of $\rho_{\mathcal{L},K}$ and $\hat{\rho}_{\mathcal{L},K}$,

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

respectively. We then have the isomorphisms

$$\begin{aligned}\rho_{\mathcal{L},K} &: \mathrm{Gal}(F_{\mathcal{L},K}/F) \longrightarrow N_{\mathcal{L}},\\ \hat{\rho}_{\mathcal{L},K} &: \mathrm{Gal}(E_{\mathcal{L},K}/F) \longrightarrow PN_{\mathcal{L}}.\end{aligned}$$

For primes $\mathfrak{p} \in A$ which split completely as $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}\overline{\mathfrak{P}}$ in K, the images of $\rho_{\mathcal{L},K}$ and $\hat{\rho}_{\mathcal{L},K}$ at the Frobenius elements are given by the conjugacy classes (denoted by [ ])

$$\rho_{\mathcal{L},K}(\sigma_{\mathfrak{p}}) = \left[\begin{pmatrix}\pi_{\mathfrak{P}}(K) \pmod{\mathfrak{L}} & 0 \pmod{\mathfrak{L}}\\ 0 \pmod{\mathfrak{L}} & \overline{\pi_{\mathfrak{P}}(K)} \pmod{\mathfrak{L}}\end{pmatrix}\right],$$

$$\hat{\rho}_{\mathcal{L},K}(\sigma_{\mathfrak{p}}) = \left[\widehat{\begin{pmatrix}\pi_{\mathfrak{P}}(K) \pmod{\mathfrak{L}} & 0 \pmod{\mathfrak{L}}\\ 0 \pmod{\mathfrak{L}} & \overline{\pi_{\mathfrak{P}}(K)} \pmod{\mathfrak{L}}\end{pmatrix}}\right],$$

where $\hat{g}$ denotes the coset of the matrix g in $PN_{\mathfrak{L}}$.

For future use, let us also denote $\pi_{\mathfrak{P}}(K)$ by

$$\pi_{\mathfrak{p}}(K). \tag{6}$$

If $\mathfrak{p}$ splits in K, then $\pi_{\mathfrak{p}}(K)$ is determined up to conjugation in K, and we will consider the two roots $\pi_{\mathfrak{p}}(K)$ and $\overline{\pi_{\mathfrak{p}}(K)}$ in pairs.

The following properties will be needed in the proof of our main results.

Lemma 17. *For all but finitely many primes $\mathcal{L} \in A$, the extensions $F_{\mathcal{L},K}/F$ and $E_{\mathcal{L},K}/F$ are geometric.*

Proof. We first consider the extension $F_{\mathcal{L},K}/K$. This is an abelian extension of K associated with the character $\chi_{\mathfrak{L}}$ as above. By the reciprocity map, it is contained in the ray class field of K at $\mathfrak{L}$. In the case of function fields, explicit class field theory is solved by adjoining torsion points of rank 1 Drinfeld modules (see for example [Hay92]). Then, $F_{\mathcal{L},K}/K$ is contained in the field of $\mathcal{L}$-torsion of a rank 1 Drinfeld module over K. Following the proof of Corollary 16, as the result [Dav01, Lemma 3.2] holds for Drinfeld modules of any rank (in particular, rank 1) over any function fields, we get that $F_{\mathcal{L},K}/K$ is a geometric extension of K for all but finitely many $\mathcal{L}$. Then, as K/F is geometric, the result of Lemma 17 follows. Finally, $E_{\mathcal{L},K} \subseteq F_{\mathcal{L},K}$ is also geometric. □

Lemma 18. *Let q, A, F be as in the introduction. Let K/F be an imaginary quadratic extension, of class number h and number of units w. Let $\mathcal{L}$ be a prime of A which splits completely in K. Let $\ell := |\mathcal{L}| = q^{\deg \mathcal{L}}$. Then*

$$\begin{aligned}|N_{\mathcal{L}}| &\gg_{h,w} \ell^2,\\ |PN_{\mathcal{L}}| &\gg_{h,w} \ell,\end{aligned}$$

where the implicit $\gg_{h,w}$-constant depends on h and w (and thus on K).

Proof. We shall need the following important result. Let $\mathrm{Cl}(\mathcal{L})$ be the ray class group modulo $\mathcal{L}\mathcal{O}_K$ of K, i.e. the set of classes of ideals I of $\mathcal{O}_K$, coprime to $\mathcal{L}\mathcal{O}_K$, under the equivalence relation

$$I \sim J \quad\Longleftrightarrow\quad \text{there exists } \alpha \in K^*, \alpha \equiv 1 \pmod{\mathcal{L}\mathcal{O}_K}, \text{ such that } I = (\alpha)J.$$

Then, for any $C \in \mathrm{Cl}(\mathcal{L})$, there exist infinitely many primes $\mathfrak{P} \in \mathcal{O}_K$ such that $\mathfrak{P} \in C$ (this follows, for example, from the Chebotarev density theorem). In particular, for any $\gamma \in (\mathcal{O}_K/\mathcal{L}\mathcal{O}_K)^*$, there exist infinitely many prime ideals $\mathfrak{P} \in \mathcal{O}_K$ such that

$$\mathfrak{P} \sim (\gamma) \quad\Rightarrow\quad \pi_{\mathfrak{P}}(K) \equiv \gamma^{hw} \pmod{\mathcal{L}\mathcal{O}_K}.$$

As $\mathcal{L}$ splits completely in K, $\mathcal{L}\mathcal{O}_K = \mathfrak{L}\overline{\mathfrak{L}}$ for some prime ideal $\mathfrak{L}$ in $\mathcal{O}_K$. Let (α, β) be any element of $(\mathcal{O}_K/\mathfrak{L})^* \times (\mathcal{O}_K/\overline{\mathfrak{L}})^*$. Let γ be the element of $(\mathcal{O}_K/\mathcal{L}\mathcal{O}_K)^*$ corresponding to $(\alpha, \overline{\beta})$ by the Chinese

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

remainder theorem. Then

$$\begin{aligned} &\pi_{\mathfrak{P}}(K) \equiv \gamma^{hw} \pmod{\mathcal{L}\mathcal{O}_K} \\ \iff &\quad \pi_{\mathfrak{P}}(K) \equiv \alpha^{hw} \pmod{\mathfrak{L}} \text{ and } \pi_{\mathfrak{P}}(K) \equiv \overline{\beta}^{hw} \pmod{\overline{\mathfrak{L}}}, \\ \iff &\quad \pi_{\mathfrak{P}}(K) \equiv \alpha^{hw} \pmod{\mathfrak{L}} \text{ and } \overline{\pi_{\mathfrak{P}}(K)} \equiv \beta^{hw} \pmod{\mathfrak{L}}. \end{aligned}$$

Thus, for any $(\alpha_0, \beta_0) \in (\mathcal{O}_K/\mathfrak{L})^* \times (\mathcal{O}_K/\overline{\mathfrak{L}})^*$ such that α_0 and β_0 are hwth powers, there exist infinitely many primes $\mathfrak{p} \in A$ such that

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}\bar{\mathfrak{P}},$$

and

$$\begin{aligned} \pi_{\mathfrak{P}}(K) &\equiv \alpha_0 \pmod{\mathfrak{L}}, \\ \overline{\pi_{\mathfrak{P}}(K)} &\equiv \beta_0 \pmod{\mathfrak{L}}. \end{aligned}$$

By the definition of $\rho_{\mathcal{L},K}$, we then deduce that

$$|N_{\mathcal{L}}| = \left(\frac{\ell - 1}{\gcd(\ell - 1, hw)}\right)^2 \gg_{h,w} \ell^2.$$

To prove the result for $PN_{\mathcal{L}}$, we use the fact proved above that $N_{\mathcal{L}}$ contains all matrices

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix},$$

where α, β are hwth powers in $(A/\mathcal{L}A)^*$. Then $PN_{\mathcal{L}}$ contains the distinct cosets

$$\widehat{\begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix}},$$

where β is any hwth power in $(A/\mathcal{L}A)^*$. This proves the desired lower bound for $PN_{\mathcal{L}}$. □

3.3 The mixed Galois representation

Let q, A, F be as in the introduction. Let ϕ be a Drinfeld A-module over F, of rank 2, such that $\mathrm{End}_{\bar{F}}(\phi) = A$. Let K/F be an imaginary quadratic extension, of class number h and number of units w. Let $\mathcal{L} \in A$ be a prime which splits completely in K, and which satisfies the hypotheses of Corollaries 12 and 16. We consider the composite fields

$$\begin{aligned} F_{\mathcal{L}} &:= F_{\mathcal{L},\phi} F_{\mathcal{L},K}, \\ E_{\mathcal{L}} &:= E_{\mathcal{L},\phi} E_{\mathcal{L},K}, \end{aligned}$$

and the product representations

$$\begin{aligned} \rho_{\mathcal{L}} := \rho_{\mathcal{L},\phi} \times \rho_{\mathcal{L},K} : \mathrm{Gal}(F_{\mathcal{L}}/F) &\hookrightarrow \mathrm{GL}_2(A/\mathcal{L}A) \times N_{\mathcal{L}}, \\ \sigma &\mapsto (\rho_{\mathcal{L},\phi}(\sigma), \rho_{\mathcal{L},K}(\sigma)) \end{aligned}$$

and

$$\begin{aligned} \hat{\rho}_{\mathcal{L}} := \hat{\rho}_{\mathcal{L},\phi} \times \hat{\rho}_{\mathcal{L},K} : \mathrm{Gal}(E_{\mathcal{L}}/F) &\hookrightarrow \mathrm{PGL}_2(A/\mathcal{L}A) \times PN_{\mathcal{L}}, \\ \sigma &\mapsto (\hat{\rho}_{\mathcal{L},\phi}(\sigma), \hat{\rho}_{\mathcal{L},K}(\sigma)). \end{aligned}$$

The aim of this section is to give lower bounds for the size of the images of the representations $\rho_{\mathcal{L}}$ and $\hat{\rho}_{\mathcal{L}}$. We will not use the lower bound for $\mathrm{Im}(\rho_{\mathcal{L}})$ in this paper, as in the proofs of Theorems 4 and 5 we are able to use the representation $\hat{\rho}_{\mathcal{L}}$ and then obtain better upper bounds than one would obtain using $\rho_{\mathcal{L}}$. Using the representation $\rho_{\mathcal{L}}$ would give an upper bound of $q^{(5/6)d}$ in Theorem 5 (and not $q^{(4/5)d}$), and an upper bound of $q^{(13/14)d}$ in Theorem 9 (and not $q^{(7/8)d}$). But it may not be possible to

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

use representations in PGL_2 for all applications, including further work on representations attached to Drinfeld modules that the authors are considering. Therefore we include the lower bound on the size of $\mathrm{Im}(\rho_{\mathcal{L}})$ for completeness and possible future applications.

Lemma 19. *Let $F_{\mathcal{L}} = F_{\mathcal{L},\phi}F_{\mathcal{L},K}$ be the composite field defined above. Let $\ell = |\mathcal{L}|$. Then*

$$[F_{\mathcal{L}} : F] = |\mathrm{Im}(\rho_{\mathcal{L}})| \gg_{h,w} \ell^5.$$

The implied $\gg_{h,w}$-constant depends on the class number h and the number of units w of K.

Proof. Since

$$[F_{\mathcal{L}} : F] = [F_{\mathcal{L},\phi}F_{\mathcal{L},K} : F] = \frac{[F_{\mathcal{L},\phi} : F][F_{\mathcal{L},K} : F]}{[F_{\mathcal{L},\phi} \cap F_{\mathcal{L},K} : F]} \gg_{h,w} \frac{\ell^6}{[F_{\mathcal{L},\phi} \cap F_{\mathcal{L},K} : F]}$$

by Corollary 14 and Lemma 18, we need to show that

$$[F_{\mathcal{L},\phi} \cap F_{\mathcal{L},K} : F] \ll \ell.$$

We first write

$$[F_{\mathcal{L},\phi} \cap F_{\mathcal{L},K} : F] \leqslant [KF_{\mathcal{L},\phi} \cap KF_{\mathcal{L},K} : F] = [KF_{\mathcal{L},\phi} \cap F_{\mathcal{L},K} : K][K : F]. \tag{7}$$

By the choice of $\mathcal{L}$, $K \cap F_{\mathcal{L},\phi} = F$, and then $\mathrm{Gal}(KF_{\mathcal{L},\phi}/K) \simeq \mathrm{Gal}(F_{\mathcal{L},\phi}/F) \simeq \mathrm{GL}_2(A/\mathcal{L}A)$ by Corollary 14. Let E be the fixed field of $\mathrm{SL}_2(A/\mathcal{L}A) \trianglelefteq \mathrm{GL}_2(A/\mathcal{L}A)$. Then, $K \subseteq E \subseteq KF_{\mathcal{L},\phi}$, and $\mathrm{Gal}(E/K) \simeq (A/\mathcal{L}A)^*$. We then have two extensions of the field E: $KF_{\mathcal{L},\phi}/E$, whose Galois group is $\mathrm{SL}_2(A/\mathcal{L}A)$, and $EF_{\mathcal{L},K}/E$, whose Galois group is abelian. As $\mathrm{SL}_2(A/\mathcal{L}A)$ has no abelian quotient, we have $KF_{\mathcal{L},\phi} \cap EF_{\mathcal{L},K} = E$, and then it follows from (7) that

$$[F_{\mathcal{L},\phi} \cap F_{\mathcal{L},K} : F] \leqslant 2[KF_{\mathcal{L},\phi} \cap F_{\mathcal{L},K} : K] \leqslant 2[KF_{\mathcal{L},\phi} \cap EF_{\mathcal{L},K} : E][E : K] \leqslant 2\ell,$$

which proves the lemma. □

Lemma 20. *Let $E_{\mathcal{L}} = E_{\mathcal{L},\phi}E_{\mathcal{L},K}$ be the composite field defined above. Let $\ell = |\mathcal{L}|$. Then*

$$[E_{\mathcal{L}} : F] = |\mathrm{Im}(\hat{\rho}_{\mathcal{L}})| \gg_{h,w} \ell^4.$$

The implied $\gg_{h,w}$-constant depends on the class number h and the number of units w of K.

Proof. Since

$$[E_{\mathcal{L}} : F] = [E_{\mathcal{L},\phi}E_{\mathcal{L},K} : E] = \frac{[E_{\mathcal{L},\phi} : E][E_{\mathcal{L},K} : E]}{[E_{\mathcal{L},\phi} \cap E_{\mathcal{L},K} : F]} \gg_{h,w} \frac{\ell^4}{[E_{\mathcal{L},\phi} \cap E_{\mathcal{L},K} : F]}$$

by Corollary 14 and Lemma 18, we need to show that

$$[E_{\mathcal{L},\phi} \cap E_{\mathcal{L},K} : F]$$

is bounded by an absolute constant. We first write

$$[E_{\mathcal{L},\phi} \cap E_{\mathcal{L},K} : F] \leqslant [KE_{\mathcal{L},\phi} \cap KE_{\mathcal{L},K} : F] = [KE_{\mathcal{L},\phi} \cap E_{\mathcal{L},K} : K][K : F].$$

By the choice of $\mathcal{L}$, $K \cap E_{\mathcal{L},\phi} = F$, and then $\mathrm{Gal}(KE_{\mathcal{L},\phi}/K) \simeq \mathrm{Gal}(E_{\mathcal{L},\phi}/F) \simeq \mathrm{PGL}_2(A/\mathcal{L}A)$ by Corollary 14. Furthermore, $\mathrm{Gal}(E_{\mathcal{L},K}/K)$ is abelian, as $K \subseteq E_{\mathcal{L},K} \subseteq F_{K,\mathcal{L}}$ and $\mathrm{Gal}(F_{\mathcal{L},K}/K)$ is abelian. But the only abelian quotients of $\mathrm{PGL}_2(A/\mathcal{L}A)$ are of order 1 or 2, as the commutator of $\mathrm{PGL}_2(A/\mathcal{L}A)$ is $\mathrm{PSL}_2(A/\mathcal{L}A)$, and this has index 2. Then

$$[E_{\mathcal{L},\phi} \cap E_{\mathcal{L},K} : F] \leqslant [KE_{\mathcal{L},\phi} \cap E_{\mathcal{L},K} : K][K : F] \leqslant 4,$$

which proves the lemma. □

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

4. The Chebotarev density theorem

Let F be a function field over $\mathbb{F}_q$, and let L/F be a finite Galois extension of function fields with Galois group $G := \mathrm{Gal}(L/F)$. Let g_F and g_L be the genus of F and L respectively. Let $\mathbb{F}_{q^m}$ be the algebraic closure of $\mathbb{F}_q$ in L. If $m = 1$, we say that L/F is a *geometric extension*.

In what follows, we recall effective versions of the Chebotarev density theorem for the extension L/F, with best error terms, as presented in [MS94]. We then apply this theorem to the fields associated to the Galois representations of the previous sections.

Let $C \subseteq G$ be a conjugacy class and let $d \in \mathbb{N}^*$. We set

$$\Pi_C(d; L/F) := \#\{\mathfrak{p} \in F \text{ unramified in } L/F \ : \deg \mathfrak{p} = d, \sigma_{\mathfrak{p}} = C\},$$

$$\Pi(d; L/F) := \#\{\mathfrak{p} \in F \text{ unramified in } L/F : \deg \mathfrak{p} = d\}.$$

We also need the following notation from [MS94]. Let

$$|D| = \sum_{\substack{\mathfrak{p} \in F \\ \mathfrak{p} \text{ ramified in } L/F}} \deg \mathfrak{p},$$

and let $\mathcal{D}_{L/F}$ be the different of the extension L/F. For each ramified prime $\mathfrak{p} \in F$ and $\mathfrak{P} \in L$ above $\mathfrak{p}$, let $\rho(\mathfrak{p})$ be such that

$$\nu_{\mathfrak{P}}(\mathcal{D}_{L/F}) \leqslant e(\mathfrak{P}/\mathfrak{p})(\rho(\mathfrak{p}) + 1).$$

Here $\nu_{\mathfrak{P}}(\cdot)$ denotes the valuation at $\mathfrak{P}$ and $e(\mathfrak{P}/\mathfrak{p})$ the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, as usual. In particular, if L/F is tamely ramified at $\mathfrak{p}$, one can take $\rho(\mathfrak{p}) = 0$. Finally, let

$$\rho_{L/F} = \max_{\mathfrak{p} \text{ ramified}} \rho(\mathfrak{p}).$$

Theorem 21 [MS94, p. 524]. *Let L/F be a finite Galois extension, with Galois group G. Let $\mathbb{F}_{q^m}$ be the algebraic closure of $\mathbb{F}_q$ in L. Let $C \subseteq G$ be a conjugacy class whose restriction to $\mathbb{F}_{q^m}$ is τ^{a_C} for some positive integer a_C. Let d be a positive integer. With the above notation, we have:*

(1) *if $d \not\equiv a_C \pmod m$, then $\Pi_C(d; L/F) = 0$; and*

(2) *if $d \equiv a_C \pmod m$, then*

$$\left|\Pi_C(d; L/F) - m\frac{|C|}{|G|}\Pi(d; L/F)\right| \leqslant 2g_L \frac{|C|}{|G|}\frac{q^{d/2}}{d} + 2(2g_F + 1)|C|\frac{q^{d/2}}{d} + \left(1 + \frac{|C|}{d}\right)|D|.$$

As the Riemann–Hurwitz formula gives

$$2g_L - 2 = (2g_F - 2)|G| + |D|, \tag{8}$$

the error terms above depend on $|C|$ and $|D|$. The following theorem improves the previous result to an error term depending on $|C|^{1/2}$ and $|D|$. In the case of number fields, such a theorem holds only under the Riemann hypothesis and the Artin conjecture (which were proven by Weil over function fields).

Theorem 22 [MS94, p. 525]. *Let L/F be a finite Galois extension, with Galois group G. Let $\mathbb{F}_{q^m}$ be the algebraic closure of $\mathbb{F}_q$ in L. Let $C \subseteq G$ be a conjugacy class whose restriction to $\mathbb{F}_{q^m}$ is τ^{a_C} for some positive integer a_C. Let d be a positive integer. With the above notation, we have:*

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

(1) *if* $d \not\equiv a_C \pmod{m}$, *then* $\Pi_C(d; L/F) = 0$; *and*

(2) *if* $d \equiv a_C \pmod{m}$, *then*

$$\left|\Pi_C(d; L/F) - m\frac{|C|}{|G|}\Pi(d; L/F)\right| \leqslant 2|C|^{1/2}\left((g_F - 1 + (\rho_{L/F} + 1)|D|)\frac{q^{d/2}}{d} + (2g_F + 1)\frac{q^{d/2}}{d} + \frac{|D|}{2d}\right) + |D|.$$

We now apply Theorem 22 for the Galois extensions $F_{\mathcal{L}}/\mathbb{F}_q(T)$ and $E_{\mathcal{L}}/\mathbb{F}_q(T)$, and we then need to understand the different of these extensions.

Proposition 23 [Gar02a, Proposition 6]. *Let* q, A, F *be as in* § *1. Let* ϕ *be a Drinfeld* A*-module of rank* 2 *over* F*. Let* $\mathfrak{a} \in A$ *be a polynomial of positive degree. Then*

$$\mathcal{D}_{F(\phi[\mathfrak{a}])/F} \supseteq (\mathfrak{a}^2\Delta_\phi),$$

where Δ_ϕ *depends only on the Drinfeld module* ϕ*, and not on* $\mathfrak{a}$*, and is defined in [Gar02a, p. 246].*

It follows from the above proposition that the extension $F_{\mathcal{L}} = F_{\mathcal{L},\phi}F_{\mathcal{L},K}$ is ramified only at $\mathcal{L}$ and at primes depending on the Drinfeld module ϕ and the quadratic extension K. In our applications, ramification at primes different from $\mathcal{L}$ is bounded by an absolute constant, and we are only interested in $\rho(\mathcal{L})$. Let $\mathcal{L}_1$ be a prime above $\mathcal{L}$ in $F_{\mathcal{L},\phi}$, let $\mathcal{L}_2$ be a prime above $\mathcal{L}$ in $F_{\mathcal{L},K}$, and let $\overline{\mathcal{L}}$ be a prime above $\mathcal{L}$ in $F_{\mathcal{L}}$. It follows from Proposition 23 that

$$\nu_{\mathcal{L}_1}(\mathcal{D}_{F_{\mathcal{L},\phi}/F}) \leqslant 2e(\mathcal{L}_1/\mathcal{L}).$$

The extension $F_{\mathcal{L},K}$ has degree dividing $(\ell-1)^2$ over the quadratic extension K, and there is then no wild ramification at $\mathcal{L}$ in $F_{\mathcal{L},K}/F$. Since

$$\mathcal{D}_{F_{\mathcal{L},\phi}/F}\mathcal{D}_{F_{\mathcal{L},K}/F} \subseteq \mathcal{D}_{F_{\mathcal{L}}/F},$$

this implies that

$$\nu_{\overline{\mathcal{L}}}(\mathcal{D}_{F_{\mathcal{L}}/F}) \leqslant 2e(\overline{\mathcal{L}}/\mathcal{L}),$$

and one can take $\rho_{F_{\mathcal{L}}/F} = 1$. As $E_{\mathcal{L}} \subseteq F_{\mathcal{L}}$, we can take the same bound for $E_{\mathcal{L}}/F$.

Then, applying Theorem 22, we get the following results.

Theorem 24. *Let* q, A, F *be as in* § 1*. Let* ϕ *be a Drinfeld* A*-module over* F*, of rank* 2*. Assume that* $\mathrm{End}_{\bar{F}}(\phi) = A$*. Let* d *be a positive integer. Suppose that* $\mathcal{L}, \mathcal{L}_1$ *and* $\mathcal{L}_2$ *are primes satisfying the hypotheses of Corollaries 12 and 16. If we fix a union of conjugacy classes* C *in* $\mathrm{Gal}(F_{\mathcal{L},\phi}/F)$, $\mathrm{Gal}(E_{\mathcal{L},\phi}/F)$ *or* $\mathrm{Gal}(E_{\mathcal{L}_1\mathcal{L}_2,\phi}/F)$*, respectively, we have as* $d \to \infty$ *that*

$$\Pi_C(d; F_{\mathcal{L},\phi}/F) = \frac{|C|}{(\ell^2-\ell)(\ell^2-1)}\,\Pi(d; F_{\mathcal{L},\phi}/F) + \mathrm{O}_\phi(|C|^{1/2}q^{d/2}\deg(\mathcal{L})),$$

$$\Pi_C(d; E_{\mathcal{L},\phi}/F) = \frac{|C|}{\ell(\ell^2-1)}\,\Pi(d; E_{\mathcal{L},\phi}/F) + \mathrm{O}_\phi(|C|^{1/2}q^{d/2}\deg(\mathcal{L}))$$

and

$$\Pi_C(d; E_{\mathcal{L}_1\mathcal{L}_2,\phi}/F) = \frac{|C|}{\ell_1(\ell_1^2-1)\ell_2(\ell_2^2-1)}\,\Pi(d; E_{\mathcal{L}_1\mathcal{L}_2,\phi}/F) + \mathrm{O}_\phi(|C|^{1/2}q^{d/2}\deg(\mathcal{L}_1\mathcal{L}_2)),$$

where $\ell := |\mathcal{L}|$, $\ell_1 := |\mathcal{L}_1|$ *and* $\ell_2 := |\mathcal{L}_2|$*. The implied* O_ϕ*-constants depend on* ϕ*.*

Theorem 25. *Let* q, A, F *be as in* § *1. Let* ϕ *be a Drinfeld* A*-module over* F*, of rank* 2*. Assume that* $\mathrm{End}_{\bar{F}}(\phi) = A$*. Let* K/F *be an imaginary quadratic extension. Let* d *be a positive integer. Then,*

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

for all but finitely many primes $\mathcal{L} \in A$, if we fix a union of conjugacy classes C in $\mathrm{Gal}(F_{\mathcal{L}}/F)$ *or* $\mathrm{Gal}(E_{\mathcal{L}}/F)$*, we have as $d \to \infty$,*

$$\Pi_C(d; F_{\mathcal{L}}/F) = \frac{|C|}{(\ell^2-1)(\ell^2-\ell)}\Pi(d; F_{\mathcal{L}}/F) + \mathrm{O}_{\phi,K}(|C|^{1/2} q^{d/2} \deg(\mathcal{L})),$$
$$\Pi_C(d; E_{\mathcal{L}}/F) = \frac{|C|}{\ell(\ell^2-1)}\Pi(d; E_{\mathcal{L}}/F) + \mathrm{O}_{\phi,K}(|C|^{1/2} q^{d/2} \deg(\mathcal{L})),$$

where $\ell = |\mathcal{L}|$, as usual. The implied $\mathrm{O}_{\phi,K}$-constant depends on ϕ and K.

5. Proof of Theorem 4

Let q, A, F be as in the introduction. Let ϕ be a Drinfeld A-module over F, of rank 2, such that $\mathrm{End}_{\bar{F}}(\phi) = A$. Let K/F be an imaginary quadratic extension, of class number h and number of units w. Let d be a positive integer. Our goal in this section is to derive an upper bound for $\Pi_\phi(K; d)$ of Theorem 4.

First, let us fix an arbitrary prime $\mathcal{L} \in A$ which satisfies Corollaries 12 and 16 and which splits completely in K. Let $\ell := |\mathcal{L}|$. We want to use the Chebotarev density theorem on the finite Galois extension $E_{\mathcal{L}} = E_{\mathcal{L},\phi}E_{\mathcal{L},K}/F$. In this section, we will write $G_{\mathcal{L}}$ for $\mathrm{Gal}(E_{\mathcal{L}}/F)$. We first find a conjugacy class of $G_{\mathcal{L}}$ describing the primes $\mathfrak{p} \in A$ such that $F(\pi_{\mathfrak{p}}(\phi)) = K$.

Lemma 26. *We keep the above setting. Let $\mathfrak{p} \in A$ be a prime which is unramified in $F_{\mathcal{L}}/F$. If $F(\pi_{\mathfrak{p}}(\phi)) = K$, then*

$$\pi_{\mathfrak{p}}(\phi)^{hw} = \pi_{\mathfrak{p}}(K),$$

with $\pi_{\mathfrak{p}}(\phi)$ and $\pi_{\mathfrak{p}}(K)$ as defined in §§ 1 and 3.2, respectively.

Proof. On the one hand, using (2) and the hypothesis of our lemma, we see that

$$\mu_{\mathfrak{p}}\mathfrak{p} = \pi_{\mathfrak{p}}(\phi)\overline{\pi_{\mathfrak{p}}(\phi)}$$

with $\pi_{\mathfrak{p}}(\phi), \overline{\pi_{\mathfrak{p}}(\phi)} \in K$, where the bar denotes the complex conjugation in K/F and where $\mu_{\mathfrak{p}} \in \mathbb{F}_q^*$, as in (2). Therefore

$$\mathfrak{p}\mathcal{O}_K = (\pi_{\mathfrak{p}}(\phi))(\overline{\pi_{\mathfrak{p}}(\phi)}). \tag{9}$$

In particular, $\mathfrak{p}$ splits completely in K.

On the other hand, using the definition of $\pi_{\mathfrak{p}}(K)$, we see that

$$\mathfrak{p}^{hw}\mathcal{O}_K = (\pi_{\mathfrak{p}}(K))(\overline{\pi_{\mathfrak{p}}(K)}). \tag{10}$$

From (9) and (10) it follows that $\pi_{\mathfrak{p}}(\phi)^{hw} = \pi_{\mathfrak{p}}(K)$ (after possibly renaming the roots). □

Lemma 27. *Let a, b be independent variables and n a positive integer. There exists a polynomial $P_n(x) \in \mathbb{Z}[x]$ such that*

$$\frac{(a^n+b^n)^2}{(ab)^n} = P_n\left(\frac{(a+b)^2}{ab}\right).$$

Proof. Observe that

$$\frac{(a+b)^2}{ab} = \frac{a}{b} + 2 + \frac{b}{a}$$

and

$$\frac{(a^n+b^n)^2}{a^nb^n} = \frac{a^n}{b^n} + 2 + \frac{b^n}{a^n}.$$

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

Thus, if we set $t := a/b$, we need to show that

$$t^n + 2 + \frac{1}{t^n} = P_n\left(t + 2 + \frac{1}{t}\right)$$

for some polynomial $P_n(x) \in \mathbb{Z}[x]$. It suffices to show that

$$\left(t + 2 + \frac{1}{t}\right)^n = t^n + 2 + \frac{1}{t^n} + Q_n\left(t + 2 + \frac{1}{t}\right) \tag{11}$$

for some polynomial $Q_n(x) \in \mathbb{Z}[x]$. Then we define $P_n(x) := x^n - Q_n(x)$.

We prove (11) by induction on n. Clearly, $Q_1(x) = 0$ and $Q_2(x) = 4x - 4$. Let us assume that (11) holds for each $k \leqslant n - 1$. Then for $k = n$ we have:

$$\begin{aligned}\left(t + 2 + \frac{1}{t}\right)^n &= \left(t^{n-1} + 2 + \frac{1}{t^{n-1}} + Q_{n-1}\left(t + 2 + \frac{1}{t}\right)\right)\left(t + 2 + \frac{1}{t}\right)\\ &= \left(t^n + 2 + \frac{1}{t^n}\right) + \left(t + 2 + \frac{1}{t}\right)Q_{n-1}\left(t + 2 + \frac{1}{t}\right)\\ &\quad + 2\left(t + 2 + \frac{1}{t}\right)^{n-1} - 2Q_{n-1}\left(t + 2 + \frac{1}{t}\right) + \left(t + 2 + \frac{1}{t}\right)^{n-2}\\ &\quad - Q_{n-2}\left(t + 2 + \frac{1}{t}\right) + 2\left(t + 2 + \frac{1}{t}\right) - 8.\end{aligned}$$

Now take

$$Q_n(x) := xQ_{n-1}(x) + 2x^{n-1} - 2Q_{n-1}(x) + x^{n-2} - Q_{n-2}(x) + 2x - 8.$$

This completes the proof of the lemma. □

Let g be a matrix in $\mathrm{GL}_2(A/\mathcal{L}A)$. Then the function

$$t(g) := \frac{\mathrm{tr}^2(g)}{\det(g)},$$

where det and tr denote the determinant and trace of a matrix, is well defined in $\mathrm{PGL}_2(A/\mathcal{L}A)$. We denote by $\hat{g}$ the projective image of g. Let

$$C_{\mathcal{L}} \subseteq \mathrm{PGL}_2(A/\mathcal{L}A) \times PN_{\mathcal{L}}$$

be the union of conjugacy classes of matrices defined by

$$C_{\mathcal{L}} := \{(\hat{g}_1, \hat{g}_2) \in \mathrm{PGL}_2(A/\mathcal{L}A) \times PN_{\mathcal{L}} : t(g_2) \equiv P_{hw}(t(g_1)) \pmod{\mathcal{L}}\}. \tag{12}$$

Lemma 28. *We keep the above setting and notation. Then*

$$\Pi_\phi(K; d) \leqslant \Pi_{C_{\mathcal{L}}}(d; E_{\mathcal{L}}/F),$$

where the quantity on the right-hand side was defined (in more generality) in § 5.

Proof. Let $\mathfrak{p} \in A$ be a prime of degree d, unramified in $F_{\mathcal{L}}$, such that $F(\pi_{\mathfrak{p}}(\phi)) = K$. In particular, $\mathfrak{p}$ splits in K. Then, from Lemma 26,

$$\pi_{\mathfrak{p}}(K) = \pi_{\mathfrak{p}}(\phi)^{hw},$$

and from Lemma 27,

$$\frac{(\pi_{\mathfrak{p}}(K) + \overline{\pi_{\mathfrak{p}}(K)})^2}{\pi_{\mathfrak{p}}(K)\overline{\pi_{\mathfrak{p}}(K)}} = \frac{(\pi_{\mathfrak{p}}(\phi)^{hw} + \overline{\pi_{\mathfrak{p}}(\phi)}^{hw})^2}{\pi_{\mathfrak{p}}(\phi)^{hw}\overline{\pi_{\mathfrak{p}}(\phi)}^{hw}} = P_{hw}\left(\frac{(\pi_{\mathfrak{p}}(\phi) + \overline{\pi_{\mathfrak{p}}(\phi)})^2}{\pi_{\mathfrak{p}}(\phi)\overline{\pi_{\mathfrak{p}}(\phi)}}\right).$$

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

Both sides of the above equality are elements of A. Reducing modulo $\mathcal{L}$ and using the definition of $\rho_{\mathcal{L},K}$ for split primes and Remark 15, this gives

$$t(\hat{\rho}_{\mathcal{L},K}(\sigma_{\mathfrak{p}})) \equiv P_{hw}(t(\hat{\rho}_{\mathcal{L},\phi}(\sigma_{\mathfrak{p}}))) \pmod{\mathcal{L}}$$

which is the defining property of $C_{\mathcal{L}}$. Thus $\hat{\rho}_{\mathcal{L}}(\sigma_{\mathfrak{p}}) \in C_{\mathcal{L}}$, as desired. □

Lemma 29. *Let $C_{\mathcal{L}} \subseteq \mathrm{PGL}_2(A/\mathcal{L}A) \times PN_{\mathcal{L}}$ be the union of conjugacy classes defined in (12). Then*

$$|C_{\mathcal{L}}| \ll_{h,w} \ell^3.$$

Proof. Let $\hat{g}_2 \in PN_{\mathcal{L}}$. There are two types of cosets in $PN_{\mathcal{L}}$, with representatives

$$\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix}$$

for $\alpha \in (A/\mathcal{L}A)^*$ (in fact, α is a hwth power in $(A/\mathcal{L}A)^*$, but we do not need to consider this to get the upper bound that we need). For a fixed $f \in (A/\mathcal{L}A)^*$, there are at most two cosets of $PN_{\mathcal{L}}$ of the first type such that

$$t\left(\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\right) = \frac{(1+\alpha)^2}{\alpha} = f.$$

Then, as $t(g_1)$ determines $t(g_2)$ by Lemma 27, the number of $(\hat{g}_1, \hat{g}_2) \in C_{\mathcal{L}}$ with $\hat{g}_2$ of the first type is at most

$$2|\,\mathrm{PGL}_2(A/\mathcal{L}A)| \ll \ell^3.$$

For cosets $\hat{g}_2 \in PN_{\mathcal{L}}$ of the second type, we always have $t(g_2) = 0$. The number of possible values of $t(g_1)$ such that $P_{hw}(t(g_1)) = 0$ is bounded by the degree of the polynomial P_{hw}, which depends only on hw (and not on $\mathcal{L}$). Then,

$$\#\{(\hat{g}_1, \hat{g}_2) \in C_{\mathcal{L}} : \hat{g}_2 \text{ is of the second type}\} \ll_{hw} \ell\, n(\ell),$$

where $n(\ell)$ is an upper bound for the number of cosets $\hat{g}_1$ in $\mathrm{PGL}_2(A/\mathcal{L}A)$ with $t(g_1) = f$ for any fixed value $f \in A/\mathcal{L}A$. It is an easy computation to see that $n(\ell) \ll \ell^2$, and this completes the proof. □

Finally, we are ready to prove Theorem 4. From Lemma 28 and Theorem 25 we see that

$$\Pi_\phi(K; d) \leqslant \Pi_{C_{\mathcal{L}}}(d; E_{\mathcal{L}}/F) = \frac{|C_{\mathcal{L}}|}{|G_{\mathcal{L}}|}\Pi(d; E_{\mathcal{L}}/F) + \mathrm{O}_{\phi,K}(|C_{\mathcal{L}}|^{1/2} q^{d/2} \deg(\mathcal{L})).$$

Combining this with the estimates of Lemmas 20 and 29, we deduce that

$$\Pi_\phi(K; d) \ll_{\phi,K} \frac{1}{\ell}\frac{q^d}{d} + \ell^{3/2} q^{d/2} \log_q \ell.$$

Now we choose the arbitrary prime $\mathcal{L} \in A$ such that

$$\ell = |\mathcal{L}| = \frac{q^{d/5}}{d^{4/5}}$$

and obtain the desired result. This completes the proof of Theorem 4.

6. Proof of Theorem 9

Let q, A, F be as in the introduction. Let ϕ be a Drinfeld A-module over F, of rank 2, and such that $\mathrm{End}_{\bar{F}}(\phi) = A$. Let d be a positive integer and $t \in A$. It is clear that

$$\#\{\mathfrak{p} \in A : \deg \mathfrak{p} = d,\ a_{\mathfrak{p}}(\phi) = t\} \leqslant \#\{\mathfrak{p} \in A : \deg \mathfrak{p} = d,\ a_{\mathfrak{p}}(\phi) \equiv t \pmod{\mathcal{L}}\} \qquad (13)$$

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

for any prime $\mathcal{L} \in A$. We choose a prime $\mathcal{L}$ which satisfies the hypotheses of Corollary 12. Using the observation of Remark 15 we obtain that

$$\#\{\mathfrak{p} \in A : \mathfrak{p} \nmid \mathcal{L}\Delta(\phi), \deg \mathfrak{p} = d, a_{\mathfrak{p}}(\phi) \equiv t \pmod{\mathcal{L}}\} = \Pi_{C_{\mathcal{L}}}(d; F_{\mathcal{L},\phi}/F),$$

where

$$C_{\mathcal{L}} := \{g \in \mathrm{GL}_2(A/\mathcal{L}A) : \operatorname{tr} g \equiv t \pmod{\mathcal{L}}\}$$

(note that this is different from the set $C_{\mathcal{L}}$ defined in (12)). It is easy to see that $|C_{\mathcal{L}}| = \ell^3 + \mathrm{O}(\ell^2)$, and so from Theorem 24 we deduce that

$$\Pi_{C_{\mathcal{L}}}(d; F_{\mathcal{L},\phi}/F) \ll_{\phi} \frac{1}{\ell}\frac{q^d}{d} + \ell^{3/2} q^{d/2} \deg \mathcal{L}.$$

We choose

$$\ell := \frac{q^{d/5}}{d^{4/5}}$$

and plug it back into (13) to obtain

$$\Pi_{\phi}(t; d) \ll_{\phi} \frac{q^{(4/5)d}}{d^{1/5}}.$$

To prove the stronger result for supersingular primes (or, equivalently, those primes $\mathfrak{p}$ with $a_{\mathfrak{p}}(\phi) = 0$), we work with the Galois representation $\hat{\rho}_{\mathcal{L},\phi} : \mathrm{Gal}(E_{\mathcal{L},\phi}/F) \to \mathrm{PGL}_2(A/\mathcal{L}A)$. Choosing $\mathcal{L}$ to satisfy Corollary 12, we have

$$|\mathrm{Gal}(E_{\mathcal{L},\phi}/F)| = |\mathrm{PGL}_2(A/\mathcal{L}A)| = \ell(\ell^2 - 1), \tag{14}$$

where $\ell := |\mathcal{L}|$, as usual. The condition $\operatorname{tr}(g) = 0$ is well defined for matrices $g \in \mathrm{PGL}_2(A/\mathcal{L}A)$, and we denote by $C^0_{\mathcal{L}}$ the union of conjugacy classes of these matrices. It is easy to see that $|C^0_{\mathcal{L}}| = \ell^2 + \mathrm{O}(\ell)$; thus, arguing as above, we obtain

$$\begin{aligned}\#\{\mathfrak{p} \in A : \deg \mathfrak{p} = d,\ a_{\mathfrak{p}}(\phi) = 0\} &\leqslant \#\{\mathfrak{p} \in A : \deg \mathfrak{p} = d,\ a_{\mathfrak{p}}(\phi) \equiv 0 \pmod{\mathcal{L}}\}\\ &\leqslant \#\{\mathfrak{p} \in A : \deg \mathfrak{p} = d,\ \hat{\rho}_{\mathcal{L},\phi}(\sigma_{\mathfrak{p}}) \in C^0_{\mathcal{L}}\}\\ &\ll_{\phi} \frac{1}{\ell}\frac{q^d}{d} + \ell q^{d/2} \deg \mathcal{L}.\end{aligned}$$

We choose

$$\ell := \frac{q^{d/4}}{d},$$

and replace in the above estimate to get the second part of Theorem 9.

7. The square sieve for function fields

Let q, A be as in the introduction. In this section we prove a function field analogue of the square sieve developed in [Hea84]. For this, we need to recall the definition of the quadratic symbol in A.

Let $\mathcal{L} \in A$ be a prime and let $a \in A$. We define

$$\left(\frac{a}{\mathcal{L}}\right) = \begin{cases} 0 & \text{if } \mathcal{L} \mid a;\\ 1 & \text{if } \mathcal{L} \nmid a \text{ and } x^2 \equiv a \pmod{\mathcal{L}} \text{ is solvable;}\\ -1 & \text{if } \mathcal{L} \nmid a \text{ and } x^2 \equiv a \pmod{\mathcal{L}} \text{ is not solvable.}\end{cases}$$

As in the rational case, it is easy to show that

$$a^{(|\mathcal{L}|-1)/2} \equiv \left(\frac{a}{\mathcal{L}}\right) \pmod{\mathcal{L}}.$$

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

From this we deduce the basic properties:

(1) if $a \equiv b \pmod{\mathcal{L}}$, then

$$\left(\frac{a}{\mathcal{L}}\right) = \left(\frac{b}{\mathcal{L}}\right);$$

(2) $\left(\frac{ab}{\mathcal{L}}\right) = \left(\frac{a}{\mathcal{L}}\right)\left(\frac{b}{\mathcal{L}}\right)$.

From the fact that $(A/\mathcal{L}A)^*$ is cyclic it follows easily that

$$\#\left\{a \in A/\mathcal{L}A : \left(\frac{a}{\mathcal{L}}\right) = 1\right\} = \#\left\{a \in A/\mathcal{L}A : \left(\frac{a}{\mathcal{L}}\right) = -1\right\} = \frac{|\mathcal{L}| - 1}{2}. \tag{15}$$

For proofs of these results and other properties, we refer the reader to [Ros02, p. 24].

With these definitions and remarks, we are now ready to state the following theorem.

Theorem 30 (The square sieve for function fields). *Let q, A be as in § 1. Let $\mathcal{A}$ be a finite set of (not necessarily distinct) non-zero elements of A. Let $\mathcal{P}$ be a finite set of primes of A. Set*

$$S(\mathcal{A}) := \{a \in \mathcal{A} : a = b^2 \text{ for some } b \in A\},$$

and for any $a \in A$ define

$$\nu_{\mathcal{P}}(a) := \#\{\mathcal{L} \in \mathcal{P} : \mathcal{L} | a\}.$$

Then

$$|S(\mathcal{A})| \leqslant \frac{|\mathcal{A}|}{|\mathcal{P}|} + \max_{\substack{\mathcal{L}_1, \mathcal{L}_2 \in \mathcal{P} \\ \mathcal{L}_1 \neq \mathcal{L}_2}} \left| \sum_{a \in \mathcal{A}} \left(\frac{a}{\mathcal{L}_1}\right)\left(\frac{a}{\mathcal{L}_2}\right) \right| + \frac{2}{|\mathcal{P}|} \sum_{a \in \mathcal{A}} \nu_{\mathcal{P}}(a) + \frac{1}{(|\mathcal{P}|)^2} \sum_{a \in \mathcal{A}} \nu_{\mathcal{P}}(a)^2.$$

Proof. The proof of this theorem is a straightforward function field analogue of the proof of the classical square sieve. For the sake of completeness, we include it here.

We note that if $a \in \mathcal{A}$ is a square, then

$$\sum_{\mathcal{L} \in \mathcal{P}} \left(\frac{a}{\mathcal{L}}\right) = \sum_{\substack{\mathcal{L} \in \mathcal{P} \\ \mathcal{L} \nmid a}} \left(\frac{a}{\mathcal{L}}\right) = |\mathcal{P}| - \nu_{\mathcal{P}}(a).$$

Therefore

$$\begin{aligned} |S(\mathcal{A})| &\leqslant \sum_{a \in \mathcal{A}} \frac{1}{|\mathcal{P}|^2} \left[\sum_{\mathcal{L} \in \mathcal{P}} \left(\frac{a}{\mathcal{L}}\right) + \nu_{\mathcal{P}}(a) \right]^2 \\ &\leqslant \frac{|\mathcal{A}|}{|\mathcal{P}|} + \frac{1}{|\mathcal{P}|^2} \sum_{\substack{\mathcal{L}_1, \mathcal{L}_2 \in \mathcal{P} \\ \mathcal{L}_1 \neq \mathcal{L}_2}} \sum_{a \in \mathcal{A}} \left(\frac{a}{\mathcal{L}_1}\right)\left(\frac{a}{\mathcal{L}_2}\right) + \frac{2}{|\mathcal{P}|} \sum_{a \in \mathcal{A}} \nu_{\mathcal{P}}(a) + \frac{1}{|\mathcal{P}|^2} \sum_{a \in \mathcal{A}} \nu_{\mathcal{P}}(a)^2, \end{aligned}$$

from which we deduce the result. □

8. Proof of Theorem 5 and Corollary 6

Let q, A, F be as in the introduction. Let ϕ be a Drinfeld A-module over F, of rank 2 and with $\mathrm{End}_{\bar{F}}(\phi) = A$. Let $K = F(\sqrt{g(T)})$ be an imaginary quadratic field over F, with $g(T) \in A$ squarefree. Finally, let d be a positive integer. We will use the square sieve to obtain upper bounds for the quantity $\Pi_\phi(K; d)$.

First, we observe that the condition $F(\pi_{\mathfrak{p}}(\phi)) = K$ given in the definition of $\Pi_\phi(K; d)$ implies that

$$a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p} = g(T)h(T)^2$$

for some $h(T) \in A$. Therefore, by multiplying both sides by $g(T)$, we see that our task is to count primes $\mathfrak{p}$ for which $g(T)\{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}\}$ is a square in A. We set

$$\mathcal{A} := \{g(T)\{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}\} : \mathfrak{p} \in A \text{ an ordinary prime for } \phi\,, \deg \mathfrak{p} = d\}$$

and

$$\mathcal{P} := \{\mathcal{L} \in A : \mathcal{L} \text{ prime}\,, \deg \mathcal{L} = \theta\}$$

for some parameter $\theta = \theta(d) \neq d$, to be chosen optimally later.

In this setting we apply the square sieve and obtain

$$\Pi_{\phi}(K; d) \leqslant \frac{|\mathcal{A}|}{|\mathcal{P}|} + \max_{\substack{\mathcal{L}_1, \mathcal{L}_2 \in \mathcal{P} \\ \mathcal{L}_1 \neq \mathcal{L}_2}} \left| \sideset{}{'}\sum_{\substack{\mathfrak{p} \in A \\ \deg \mathfrak{p} = d}} \left(\frac{g(T)\{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}\}}{\mathcal{L}_1}\right)\left(\frac{g(T)\{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}\}}{\mathcal{L}_2}\right)\right|$$
$$+ \frac{2}{|\mathcal{P}|}\sum_{a \in \mathcal{A}} \nu_{\mathcal{P}}(a) + \frac{1}{|\mathcal{P}|^2}\sum_{a \in \mathcal{A}} \nu_{\mathcal{P}}(a)^2,$$

where the prime on the summation signifies that we are summing over ordinary primes $\mathfrak{p}$ for ϕ. From the prime number theorem for function fields we deduce that

$$\frac{|\mathcal{A}|}{|\mathcal{P}|} \asymp q^{d-\theta}\frac{\theta}{d}. \tag{16}$$

By noting that

$$\nu_{\mathcal{P}}(a) \leqslant \deg a$$

and by using the bound (3) given in § 1, we see that for ordinary primes $\mathfrak{p}$ of degree d we have

$$\nu_{\mathcal{P}}(g(T)\{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}\}) \leqslant d + \deg g(T).$$

We infer the estimates

$$\frac{2}{|\mathcal{P}|}\sum_{a \in \mathcal{A}} \nu_{\mathcal{P}}(a) \ll q^{d-\theta}\frac{\theta}{d}\,[d + \deg g(T)], \tag{17}$$

$$\frac{1}{|\mathcal{P}|^2}\sum_{a \in \mathcal{A}} \nu_{\mathcal{P}}(a)^2 \ll q^{d-2\theta}\frac{\theta^2}{d}[d + \deg g(T)]^2. \tag{18}$$

It remains to evaluate

$$\max_{\substack{\mathcal{L}_1, \mathcal{L}_2 \in \mathcal{P} \\ \mathcal{L}_1 \neq \mathcal{L}_2}} \left| \sideset{}{'}\sum_{\substack{\mathfrak{p} \in A \\ \deg \mathfrak{p} = d}} \left(\frac{g(T)\{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}\}}{\mathcal{L}_1}\right)\left(\frac{g(T)\{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}\}}{\mathcal{L}_2}\right)\right|.$$

In doing so, we deviate from the proof in [CFM05] by making one simple (but important) observation and a reduction to PGL_2-extensions; these new ingredients lead to substantial savings in the final exponent of q. A more clear comparison with the method in [CFM05] is described in [CD08].

Let us fix $\mathcal{L}_1, \mathcal{L}_2 \in \mathcal{P}$ distinct primes such that the Galois representation $\rho_{\mathcal{L}_1\mathcal{L}_2,\phi}$ is surjective and the extension $F_{\mathcal{L}_1\mathcal{L}_2,\phi}/F$ is geometric, i.e. $\mathcal{L}_1, \mathcal{L}_2$ satisfy Corollaries 13 and 16. We remark that, by choosing d sufficiently large, we can ensure that these conditions hold. Now we consider the sum

$$S_{\mathcal{L}_1,\mathcal{L}_2} := \sideset{}{'}\sum_{\substack{\mathfrak{p} \in A \\ \deg \mathfrak{p} = d}} \left(\frac{g(T)\{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}\}}{\mathcal{L}_1}\right)\left(\frac{g(T)\{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}\}}{\mathcal{L}_2}\right),$$

which we write as

$$S_{\mathcal{L}_1,\mathcal{L}_2} = \left(\frac{g(T)}{\mathcal{L}_1}\right)\left(\frac{g(T)}{\mathcal{L}_2}\right)(T_1 + T_2 - T_3 - T_4), \tag{19}$$

where

$$T_1 := \#\left\{\mathfrak{p} \in A : \mathfrak{p} \text{ ordinary}, \deg \mathfrak{p} = d, \left(\frac{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}}{\mathcal{L}_1}\right) = \left(\frac{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}}{\mathcal{L}_2}\right) = 1\right\},$$
$$T_2 := \#\left\{\mathfrak{p} \in A : \mathfrak{p} \text{ ordinary}, \deg \mathfrak{p} = d, \left(\frac{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}}{\mathcal{L}_1}\right) = \left(\frac{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}}{\mathcal{L}_2}\right) = -1\right\},$$
$$T_3 := \#\left\{\mathfrak{p} \in A : \mathfrak{p} \text{ ordinary}, \deg \mathfrak{p} = d, \left(\frac{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}}{\mathcal{L}_1}\right) = -\left(\frac{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}}{\mathcal{L}_2}\right) = 1\right\},$$
$$T_4 := \#\left\{\mathfrak{p} \in A : \mathfrak{p} \text{ ordinary}, \deg \mathfrak{p} = d, \left(\frac{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}}{\mathcal{L}_1}\right) = -\left(\frac{a_{\mathfrak{p}}(\phi)^2 - 4\mu_{\mathfrak{p}}\mathfrak{p}}{\mathcal{L}_2}\right) = -1\right\}.$$

We will estimate each of the terms T_1, T_2, T_3 and T_4. Using Remark 15, we write

$$T_i = \#\{\mathfrak{p} \in A : \mathfrak{p} \text{ ordinary}, \deg \mathfrak{p} = d, (\hat{\rho}_{\mathcal{L}_1,\phi}(\sigma_{\mathfrak{p}}), \hat{\rho}_{\mathcal{L}_2,\phi}(\sigma_{\mathfrak{p}})) \in C_i\},$$

where $\sigma_{\mathfrak{p}}$ is the Frobenius at $\mathfrak{p}$ in F^{sep}/F and $C_i, 1 \leqslant i \leqslant 4$, are the unions of conjugacy classes in

$$\mathrm{Gal}(E_{\mathcal{L}_1\mathcal{L}_2}/F) \simeq \mathrm{PGL}_2(A/\mathcal{L}_1\mathcal{L}_2A)$$

defined by:

$$C_1 := \left\{(\hat{g}_1, \hat{g}_2) \in \mathrm{PGL}_2(A/\mathcal{L}_1\mathcal{L}_2A) : \left(\frac{(\mathrm{tr}\, g_1)^2 - 4\det g_1}{\mathcal{L}_1}\right) = \left(\frac{(\mathrm{tr}\, g_2)^2 - 4\det g_2}{\mathcal{L}_2}\right) = 1\right\},$$
$$C_2 := \left\{(\hat{g}_1, \hat{g}_2) \in \mathrm{PGL}_2(A/\mathcal{L}_1\mathcal{L}_2A) : \left(\frac{(\mathrm{tr}\, g_1)^2 - 4\det g_1}{\mathcal{L}_1}\right) = \left(\frac{(\mathrm{tr}\, g_2)^2 - 4\det g_2}{\mathcal{L}_2}\right) = -1\right\},$$
$$C_3 := \left\{(\hat{g}_1, \hat{g}_2) \in \mathrm{PGL}_2(A/\mathcal{L}_1\mathcal{L}_2A) : \left(\frac{(\mathrm{tr}\, g_1)^2 - 4\det g_1}{\mathcal{L}_1}\right) = -\left(\frac{(\mathrm{tr}\, g_2)^2 - 4\det g_2}{\mathcal{L}_2}\right) = 1\right\},$$
$$C_4 := \left\{(\hat{g}_1, \hat{g}_2) \in \mathrm{PGL}_2(A/\mathcal{L}_1\mathcal{L}_2A) : \left(\frac{(\mathrm{tr}\, g_1)^2 - 4\det g_1}{\mathcal{L}_1}\right) = -\left(\frac{(\mathrm{tr}\, g_2)^2 - 4\det g_2}{\mathcal{L}_2}\right) = -1\right\}.$$

We recall that $\hat{g}$ denotes the projective image of a matrix g. The conditions defining the sets C_i are well defined in $\mathrm{PGL}_2(A/\mathcal{L}_1\mathcal{L}_2A) \simeq \mathrm{PGL}_2(A/\mathcal{L}_1A) \times \mathrm{PGL}_2(A/\mathcal{L}_2A)$. Since they are unions of conjugacy classes in $\mathrm{PGL}_2(A/\mathcal{L}_1A) \times \mathrm{PGL}_2(A/\mathcal{L}_2A)$ and since $\mathcal{L}_1, \mathcal{L}_2$ have been chosen such that $\hat{\rho}_{\mathcal{L}_1\mathcal{L}_2,\phi}$ is an isomorphism, we can use Theorem 24 to estimate $T_i, 1 \leqslant i \leqslant 4$. For this, we only need to estimate $|C_i|, 1 \leqslant i \leqslant 4$. We rely on the following lemma.

Lemma 31. *Let q, A be as in § 1. Let $\mathcal{L} \in A$ be a prime such that $|\mathcal{L}| = \ell$. Then:*

(1) $\#\left\{\hat{g} \in \mathrm{PGL}_2(A/\mathcal{L}A) : \left(\frac{(\mathrm{tr}\, g)^2 - 4\det g}{\mathcal{L}}\right) = 1\right\} = \frac{\ell^3}{2} + \mathrm{O}(\ell^2);$

(2) $\#\left\{\hat{g} \in \mathrm{PGL}_2(A/\mathcal{L}A) : \left(\frac{(\mathrm{tr}\, g)^2 - 4\det g}{\mathcal{L}}\right) = -1\right\} = \frac{\ell^3}{2} + \mathrm{O}(\ell^2).$

Proof. The proof consists of an easy counting argument relying on (15), and we leave it as an exercise for the reader. □

Using this lemma, we obtain

$$|C_i| = \left(\frac{\ell_1^3}{2} + \mathrm{O}\left(\ell_1^2\right)\right)\left(\frac{\ell_2^3}{2} + \mathrm{O}(\ell_2^2)\right) = \frac{\ell_1^3\ell_2^3}{4} + \mathrm{O}(\ell_1^2\ell_2^2(\ell_1 + \ell_2)),$$

for each $1 \leqslant i \leqslant 4$. Then, by Theorem 24, we obtain

$$T_i = \frac{\ell_1^2\ell_2^2}{4(\ell_1^2 - 1)(\ell_2^2 - 1)} \cdot \frac{q^d}{d} + \mathrm{O}\left(\frac{\ell_1 + \ell_2}{\ell_1\ell_2} \cdot \frac{q^d}{d}\right) + \mathrm{O}_\phi(\ell_1^{3/2}\ell_2^{3/2} \cdot q^{d/2}\log_q(\ell_1 + \ell_2)) + \mathrm{O}_\phi(q^{(3/4)d})$$

for each $1 \leqslant i \leqslant 4$, where the last error term comes from the estimate given in Theorem 9 for the number of supersingular primes for ϕ.

We are now ready to estimate $S_{\mathcal{L}_1,\mathcal{L}_2}$ and to conclude the proof of the theorem. Using the above estimates for T_1, T_2, T_3 and T_4 in (19), we deduce that

$$S_{\mathcal{L}_1,\mathcal{L}_2} \ll_\phi \frac{q^{d-\theta}}{d} + q^{d/2+3\theta}\theta + q^{(3/4)d}, \tag{20}$$

where we are also using that $|\mathcal{L}_1| = |\mathcal{L}_2| = q^\theta$ (recall the definition of the set $\mathcal{P}$). By putting together (16)–(20), we deduce further that

$$\Pi_\phi(K;d) \ll_\phi q^{d/2+3\theta}\theta + q^{d-\theta}\frac{\theta}{d}[d + \deg g(T)] + q^{d-2\theta}\frac{\theta^2}{d}[d+\deg g(T)]^2 + q^{(3/4)d}.$$

We choose

$$\theta := \frac{d}{8}$$

and conclude that

$$\Pi_\phi(K;d) \ll_\phi q^{(7/8)d}[d+\deg g(T)] + q^{(3/4)d}d[d+\deg g(T)]^2.$$

We emphasize that the implicit $\ll_\phi$-constant depends only on ϕ, and not on the field K.

To prove Corollary 6, we write

$$\#\{\mathfrak{p} \in A : \mathfrak{p} \text{ prime }, \deg \mathfrak{p} = d\} = \Pi_\phi(0;d) + \sum_{K \in \mathcal{D}_\phi(d)} \Pi_\phi(K;d),$$

where $\Pi_\phi(0;d)$ denotes the number of degree d supersingular primes for ϕ and $\mathcal{D}_\phi(d)$ denotes the set of distinct fields $F(\pi_\mathfrak{p}(\phi))$ obtained by running over ordinary primes $\mathfrak{p} \in A$ with $\deg \mathfrak{p} = d$. Using Theorems 5 and 9, we obtain

$$|\mathcal{D}_\phi(d)| \gg_\phi \frac{q^d}{d \max_{K\in\mathcal{D}_\phi(d)} \Pi_\phi(K;d)} \gg_\phi \frac{q^{d/8}}{d^2}.$$

This completes the proof of the corollary. □

Acknowledgements

The authors would like to thank Bas Edixhoven, Ernst Gekeler, Hershy Kisilevsky, Richard Pink and Michael Rosen for helpful discussions and suggestions related to the present paper.

References

CD08 A. C. Cojocaru and C. David, *Frobenius fields for elliptic curves*, Amer. J. Math., to appear.

CFM05 A. C. Cojocaru, E. Fouvry and R. Murty, *The square sieve and the Lang–Trotter conjecture*, Canad. J. Math. **57** (2005), 1155–1177.

Dav01 C. David, *Frobenius distributions of Drinfeld modules of any rank*, J. Number Theory **90** (2001), 329–340.

Elk87 N. D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. **89** (1987), 561–567.

Gar02a F. Gardeyn, *Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld*, Arch. Math. **79** (2002), 241–251.

Gar02b F. Gardeyn, *t-Motives and Galois representations*, PhD thesis, Universiteit Gent (2002).

Hay92 D. Hayes, *A brief introduction to Drinfeld modules*, in *The arithmetic of function fields*, eds D. Goss *et al.* (de Gruyter, Berlin, 1992), 171–188.

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press

Hea84 D. R. Heath-Brown, *The square sieve and consecutive squarefree numbers,* Math. Ann. **226** (1984), 251–259.

LT76 S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics, vol. 504 (Springer, Berlin, 1976).

MS94 V. K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C. R. Acad. Sci. Paris, Série I **319** (1994), 523–528.

Pin97 R. Pink, *The Mumford–Tate conjecture for Drinfeld modules*, Publ. Res. Inst. Math. Sci., Kyoto Univ. **33** (1997), 393–425.

Poo98 B. Poonen, *Drinfeld modules with no supersingular primes*, Int. Math. Res. Not. **199B** (1998), no. 3, 151–159.

Ros02 M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 201 (Springer, New York, 2002).

Yu95 J.-K. Yu, *Isogenies of Drinfeld modules,* J. Number Theory **54** (1995), 161–171.

Alina Carmen Cojocaru cojocaru@math.uic.edu
University of Illinois at Chicago, Department of Mathematics, Statistics and Computer Science, 322 SEO, 851 S. Morgan Street, Chicago, IL 60607, USA
and the Institute of the Romanian Academy, Calea Grivitei 21, 010702, Bucharest, Romania

Chantal David cdavid@mathstat.concordia.ca
Concordia University, Department of Mathematics and Statistics, 1455 de Maisonneuve West, Montréal, Québec, H3G 1M8, Canada

https://doi.org/10.1112/S0010437X07003387 Published online by Cambridge University Press