A. C. Cojocaru and M. Papikian (2015) “Drinfeld Modules, Frobenius Endomorphisms, and CM-Liftings,”
International Mathematics Research Notices, Vol. 2015, No. 17, pp. 7787–7825
Advance Access Publication October 15, 2014
doi:10.1093/imrn/rnu178

# Drinfeld Modules, Frobenius Endomorphisms, and CM-Liftings

**Alina Carmen Cojocaru[1,2] and Mihran Papikian[3]**

[1]Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan Street, 322 SEO, Chicago, IL 60607, USA, [2]Institute of Mathematics “Simion Stoilow” of the Romanian Academy, 21 Calea Grivitei Street, Sector 1, Bucharest 010702, Romania, and [3]Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

*Correspondence to be sent to: cojocaru@uic.edu*

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

We give a global description of the Frobenius elements in the division fields of Drinfeld modules of rank 2. We apply this description to derive a criterion for the splitting modulo primes of a class of nonsolvable polynomials, and to study the frequency with which the reductions of Drinfeld modules have small endomorphism rings. We also generalize some of these results to higher rank Drinfeld modules and prove CM-lifting theorems for Drinfeld modules.

## 1 Introduction

Given a finite Galois extension $L/K$ of global fields and a conjugacy class $C \subseteq \mathrm{Gal}(L/K)$, a fundamental problem is that of describing the (unramified) primes $\mathfrak{p}$ of $K$ for which the conjugacy class of the Frobenius at $\mathfrak{p}$ is $C$. The Chebotarev Density Theorem provides the density $\#C/[L:K]$ of these primes, while, in general, the characterization of the primes themselves is a finer and deeper question.

One instance of a complete answer to this question is that of the cyclotomics. For example, for $a$ an odd positive integer, $\mathrm{Gal}(\mathbb{Q}(\zeta_a)) \simeq (\mathbb{Z}/a\mathbb{Z})^\times$, and so for any rational

Received January 28, 2014; Revised July 11, 2014; Accepted August 13, 2014

© The Author(s) 2014. Published by Oxford University Press. All rights reserved. For permissions, please e-mail: journals.permissions@oup.com.

prime $p \nmid a$, the Frobenius at $p$ is uniquely determined by the residue class of $p$ modulo $a$; in particular, $p$ splits completely in $\mathbb{Q}(\zeta_a)$ if and only if $p \equiv 1 \pmod a$. A similar result was proved by Hayes [19] for the cyclotomic function fields introduced by Carlitz.

Natural extensions of the cyclotomics occur in the context of abelian varieties and Drinfeld modules through the division fields associated to these objects. For an abelian variety of dimension 1 (an elliptic curve), defined over a global field, an explicit global characterization of the Frobenius in the division fields of the variety has been obtained using central results from the theory of complex multiplication, and similarly to the case of the cyclotomics, there are numerous applications of this characterization (cf. [12, 35]). For a higher dimensional abelian variety, the question of describing explicitly the Frobenius in the division fields of the variety is open. The focus of our paper is an investigation of this question in *the context of Drinfeld modules*, as described below.

Let $F$ be the function field of a smooth, projective, geometrically irreducible curve over the finite field $\mathbb{F}_q$ with $q$ elements. We distinguish a place $\infty$ of $F$, called the *place at infinity*, and we let $A$ denote the ring of functions in $F$ which have no poles away from $\infty$. Let $K$ be a field equipped with a homomorphism $\gamma : A \to K$. If $\gamma$ is injective, we say that $K$ has *A-characteristic* 0; if $\ker(\gamma) = \mathfrak{p} \lhd A$ is a nonzero (prime) ideal, then we say that $K$ has *A-characteristic* $\mathfrak{p}$. Note that $K$ contains $\mathbb{F}_q$ as a subfield. Let $\tau$ be the Frobenius endomorphism of $K$ relative to $\mathbb{F}_q$, that is, the map $x \mapsto x^q$, and let $K\{\tau\}$ be the noncommutative ring of polynomials in the indeterminate $\tau$ with coefficients in $K$ and the commutation rule $\tau c = c^q \tau$ for any $c \in K$. A *Drinfeld A-module over K* is a ring homomorphism

$$\psi : A \to K\{\tau\}$$

$$a \mapsto \psi_a = \gamma(a) + \sum_{1 \le i \le n_a} \alpha_i \tau^i, \quad \alpha_{n_a} \neq 0,$$

whose image is not contained in $K$. One shows that there is an integer $r \ge 1$, called the *rank of* $\psi$, such that $n_a = r \log_q |a|_\infty$ for all $a \in A$, where $|\cdot|_\infty$ is the normalized valuation of $F$ defined by $\infty$; see [11]. Two Drinfeld modules, $\psi, \phi$, are *isomorphic* over $K$ if there exists $c \in K^\times$ such that $\psi_a = c^{-1} \phi_a c$ for all $a \in A$.

Let $\psi$ be a Drinfeld module of rank $r$ over $F$, with $\gamma$ being the canonical embedding of $A$ into its fraction field $F$ (this shall be our setting throughout). We say $\psi$ has *good reduction* at the prime $\mathfrak{p}$ of $A$ if we can find $\phi$ over $F$ with the following properties:

(i) $\phi$ is isomorphic to $\psi$ over $F$;

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

(ii) for all $a \in A$, the coefficients of $\phi_a$ are integral at $\mathfrak{p}$;

(iii) the map

$$\begin{aligned} \phi \otimes \mathbb{F}_{\mathfrak{p}} : A &\to \mathbb{F}_{\mathfrak{p}}\{\tau\} \\ a &\mapsto \phi_a \bmod \mathfrak{p} \end{aligned}$$

is a Drinfeld $A$-module of rank $r$ over $\mathbb{F}_{\mathfrak{p}} := A/\mathfrak{p}$.

Let $\mathcal{P}_\psi$ denote the set of primes of good reduction of $\psi$. We will often implicitly assume that $\psi$ itself satisfies (ii) and (iii) at a given prime of good reduction.

The *ring of $K$-endomorphisms* of $\psi$, $\mathrm{End}_K(\psi)$, is the centralizer in $K\{\tau\}$ of the image of $A$ under $\psi$. Denote by $F_\infty$ the completion of $F$ at $\infty$. The ring $\mathrm{End}_K(\psi)$ is a projective $A$-module of rank $\leq r^2$ with the property that $D := \mathrm{End}_K(\psi) \otimes_A F$ is a division algebra over $F$ such that $D \otimes_F F_\infty$ is also a division algebra (over $F_\infty$). Moreover, if $K$ has $A$-characteristic 0, then $D$ is a field extension of $F$ of degree $\leq r$; see [11]. In this last case, the place $\infty$ does not split in the extension $D/F$. We call a finite field extension $F'$ of $F$ *imaginary* if $\infty$ does not split in $F'$.

The Drinfeld module $\psi$ endows the algebraic closure $\bar{K}$ of $K$ with an $A$-module structure, where $a \in A$ acts by $\psi_a$. We shall write ${}^{\psi}\bar{K}$ if we wish to emphasize this action. The *$a$-torsion* $\psi[a] \subset \bar{K}$ of $\psi$ is the kernel of $\psi_a$, that is, the set of zeros of the polynomial $\psi_a(x) := \gamma(a)x + \sum_{1 \leq i \leq n_a} \alpha_i x^{q^i} \in K[x]$. The field $K(\psi[a])$, obtained by adjoining the elements of $\psi[a]$ to $K$, is called the *$a$-division field* of $\psi$.

It is clear that $\psi[a]$ has a natural structure of an $A$-module. Assume $a$ is coprime to $\ker(\gamma)$, if the $A$-characteristic of $K$ is nonzero. Then, $\psi[a] \simeq_A (A/aA)^{\oplus r}$ and $\psi[a] \subset K^{\mathrm{sep}}$ (since $\psi_a'(x) = \gamma(a) \neq 0$). The action of $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ on $\psi[a]$ gives rise to a Galois representation

$$\bar{\rho}_{\psi,a} : G_K \to \mathrm{GL}_r(A/aA). \tag{1}$$

In the theory of Drinfeld modules, the study of the division fields and the Galois representations associated to $\psi$ plays a central role. For example, when $r = 1$, this study leads to explicit class field theory of $F$ (see [11, 19]).

In this paper, we mostly deal with Drinfeld modules for $A = \mathbb{F}_q[T]$, which, in some respects, is similar to that of elliptic curves over $\mathbb{Q}$. Our first goal is *to provide an explicit global characterization of the Frobenius at a prime $\mathfrak{p}$ of $F$ in the division fields of $\psi$* when $r = 2$. We also give a less explicit version of this result which is valid for any $r \geq 2$. These results have several interesting applications, including a criterion for the splitting

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

modulo primes of a class of nonsolvable polynomials studied by Abhyankar. The second goal of the paper is *to study the frequency with which the reductions of $\psi$ modulo $\mathfrak{p}$ have a small endomorphism ring*. This result opens up further important questions about the behaviour of the reductions of $\psi$ modulo primes and broadens a major theme of research related to the Sato–Tate conjecture and the Lang–Trotter conjectures. Finally, the third goal of the paper is *to prove CM-lifting theorems for general Drinfeld modules*, providing a function field counterpart of Deuring's Lifting Theorem.

Now we give the precise statements of our main results.

**Theorem 1.** Let $q$ be an odd prime power, $A = \mathbb{F}_q[T]$ and $F = \mathbb{F}_q(T)$. Let $\psi : A \to F\{\tau\}$ be a Drinfeld $A$-module over $F$, of rank 2. Let $\mathfrak{p} = pA \in \mathcal{P}_\psi$ be a prime of good reduction of $\psi$, where $p \in A$ is monic and irreducible. Let $a_\mathfrak{p}(\psi), b_\mathfrak{p}(\psi), \delta_\mathfrak{p}(\psi)$ be the following uniquely determined elements of $A$:

(a) $a_\mathfrak{p}(\psi)$ is the coefficient of $x$ in the $\mathfrak{p}$-Weil polynomial of $\psi$,

$$P_{\psi,\mathfrak{p}}(x) = x^2 + a_\mathfrak{p}(\psi)x + u_\mathfrak{p}(\psi)p \in A[x],$$

where $u_\mathfrak{p}(\psi) \in \mathbb{F}_q^\times$;

(b) $b_\mathfrak{p}(\psi)$ is the unique monic polynomial such that, for any root $\pi_\mathfrak{p}(\psi)$ of $P_{\psi,\mathfrak{p}}$,

$$\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p})/A[\pi_\mathfrak{p}(\psi)] \cong_A A/b_\mathfrak{p}(\psi)A;$$

(c) $\delta_\mathfrak{p}(\psi)$ is the unique generator of the discriminant ideal of $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p})$ satisfying

$$a_\mathfrak{p}(\psi)^2 - 4u_\mathfrak{p}(\psi)p = b_\mathfrak{p}(\psi)^2\delta_\mathfrak{p}(\psi).$$

Then, for any $a \in A$ coprime to $p$, the reduction modulo $a$ of the matrix

$$\begin{pmatrix} -\dfrac{a_\mathfrak{p}(\psi)}{2} & \dfrac{\delta_\mathfrak{p}(\psi)b_\mathfrak{p}(\psi)}{2} \\ \dfrac{b_\mathfrak{p}(\psi)}{2} & -\dfrac{a_\mathfrak{p}(\psi)}{2} \end{pmatrix} \in M_2(A)$$

represents the conjugacy class in $\mathrm{GL}_2(A/aA)$ of the image under $\bar{\rho}_{\psi,a}$ of the Frobenius at $\mathfrak{p}$ in the $a$-division field $F(\psi[a])$ of $\psi$. □

An immediate consequence to this result is a criterion for the splitting completely of a prime in $F(\psi[a])$, reminiscent of that for cyclotomic fields.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

**Corollary 2.** In the setting of Theorem 1, the prime $\mathfrak{p}$ splits completely in $F(\psi[a])/F$ if and only if

$$a_{\mathfrak{p}}(\psi) \equiv -2 \pmod{a}$$

and

$$b_{\mathfrak{p}}(\psi) \equiv 0 \pmod{a}. \qquad \square$$

Moreover, we deduce the $A$-module structure of $\mathbb{F}_{\mathfrak{p}}$ defined by the reduction $\psi \otimes \mathbb{F}_{\mathfrak{p}}$.

**Corollary 3.** In the setting of Theorem 1, the $A$-module structure ${}^{\psi}\mathbb{F}_{\mathfrak{p}}$ is given explicitly by

$$^{\psi}\mathbb{F}_{\mathfrak{p}} \simeq_A A/d_{1,\mathfrak{p}}(\psi)A \times A/d_{2,\mathfrak{p}}(\psi)A,$$

where

$$d_{1,\mathfrak{p}}(\psi) = \gcd\left(\frac{b_{\mathfrak{p}}(\psi)}{2}, \frac{a_{\mathfrak{p}}(\psi)}{2} + 1\right) \in A,$$

$$d_{2,\mathfrak{p}}(\psi) = \frac{1 + a_{\mathfrak{p}}(\psi) + u_{\mathfrak{p}}(\psi)p}{d_{1,\mathfrak{p}}(\psi)} \in A,$$

and $d_{1,\mathfrak{p}}(\psi)$ divides $d_{2,\mathfrak{p}}(\psi)$ (hence are uniquely determined up to a constant factor). In particular, if $b_{\mathfrak{p}}(\psi) = 1$, then ${}^{\psi}\mathbb{F}_{\mathfrak{p}}$ is $A$-cyclic. $\square$

For higher rank Drinfeld modules, we prove the following generalizations of Theorem 1.

**Theorem 4.** Let $A = \mathbb{F}_q[T]$ and $F = \mathbb{F}_q(T)$. Let $\psi : A \to F\{\tau\}$ be a Drinfeld $A$-module over $F$, of rank $r \geq 2$. Let $\mathfrak{p} = pA$ be a prime of good reduction of $\psi$, and $\pi_{\mathfrak{p}}(\psi)$ be any root of the $\mathfrak{p}$-Weil polynomial $P_{\psi,\mathfrak{p}}$ of $\psi$.

(a) There are uniquely determined nonzero monic polynomials $b_{\mathfrak{p},1}(\psi), \dots, b_{\mathfrak{p},r-1}(\psi) \in A$ such that

$$\mathrm{End}_{\mathbb{F}_{\mathfrak{p}}}(\psi \otimes \mathbb{F}_{\mathfrak{p}})/A[\pi_{\mathfrak{p}}(\psi)] \cong_A A/b_{\mathfrak{p},1}(\psi)A \oplus \cdots \oplus A/b_{\mathfrak{p},r-1}(\psi)A,$$

and

$$b_{\mathfrak{p},i}(\psi) \text{ divides } b_{\mathfrak{p},i+1}(\psi) \quad \text{for } i = 1, \dots, r-2.$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

(b) If $r$ is coprime to $q$, then

$$\mathrm{disc}(P_{\psi,\mathfrak{p}})A=\mathrm{disc}(\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi\otimes\mathbb{F}_\mathfrak{p}))(b_{\mathfrak{p},1}(\psi)\cdots b_{\mathfrak{p},r-1}(\psi))^2,$$

where $\mathrm{disc}(P_{\psi,\mathfrak{p}})$ is the discriminant of the polynomial of $P_{\psi,\mathfrak{p}}$, and $\mathrm{disc}(\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi\otimes\mathbb{F}_\mathfrak{p}))$ is the discriminant ideal of $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi\otimes\mathbb{F}_\mathfrak{p})$.

(c) Assume $0\neq a\in A$ is coprime to $p$. Let $J_a$ be the subfield of $F(\psi[a])$ fixed by $\bar{\rho}_{\psi,a}(G_F)\cap Z(A/aA)$, where $Z(A/aA)$ denotes the center of $\mathrm{GL}_r(A/aA)$. Then $\mathfrak{p}$ splits completely in $J_a$ if and only if $a$ divides $b_{\mathfrak{p},1}(\psi)$. □

Comparing (a) and (b) of Theorem 4 with (b) and (c) of Theorem 1, we see that the $r-1$ invariants $b_{\mathfrak{p},1}(\psi),\dots,b_{\mathfrak{p},r-1}(\psi)$ generalize $b_\mathfrak{p}(\psi)$ to the rank-$r$ case. Although Theorem 4 does not provide an explicit matrix for the Frobenius at $\mathfrak{p}$, Part (c) of the theorem can be interpreted as a generalization of Corollary 2. In the rank-2 case, $b_\mathfrak{p}(\psi)$ controls both $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi\otimes\mathbb{F}_\mathfrak{p})/A[\pi_\mathfrak{p}(\psi)]$ and the splitting behavior of $\mathfrak{p}$ in division fields. In higher ranks, $b_{\mathfrak{p},r-1}(\psi)$ controls the difference between the endomorphism rings, whereas $b_{\mathfrak{p},1}(\psi)$ controls the splitting of $\mathfrak{p}$. (Indeed, since all $b_{\mathfrak{p},i}(\psi)$ divide $b_{\mathfrak{p},r-1}(\psi)$, we have $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi\otimes\mathbb{F}_\mathfrak{p})\cong A[\pi_\mathfrak{p}(\psi)]$ if and only if $b_{\mathfrak{p},r-1}(\psi)=1$.)

An interesting arithmetic application of Theorems 1 and 4 is a "reciprocity law" for splitting of certain nonsolvable polynomials in the style of Klein's approach to nonsolvable quintics using elliptic curves (which itself is a generalization of a theorem of Gauss that the polynomial $x^3-2\in\mathbb{Z}[x]$ splits completely modulo a rational prime $p\geq 5$ if and only if $p=\alpha^2+27\beta^2$ for some integers $\alpha,\beta$). To introduce this class of polynomials, assume $A=\mathbb{F}_q[T]$ and let $\psi:A\to F\{\tau\}$ be a Drinfeld $A$-module of rank $r$ defined by

$$\psi_T=T+g_1\tau+g_2\tau^2+\cdots+g_r\tau^r. \tag{2}$$

Consider the polynomial

$$f_\psi(x):=T+g_1x+\cdots+g_rx^{(q^r-1)/(q-1)}\in F[x] \tag{3}$$

obtained from $\psi_T(x)$ via the relation

$$\psi_T(x)=xf_\psi(x^{q-1}).$$

**Theorem 5.** Assume $r\geq 2$ is coprime to $q$.

(a) $f_\psi$ splits completely modulo $\mathfrak{p}\in\mathcal{P}_\psi$ only if $T^2$ divides the discriminant of $P_{\psi,\mathfrak{p}}$. When $r=2$, this can be explicitly stated as $f_\psi$ splits completely modulo

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

$\mathfrak{p}$ only if $p = u\alpha^2 + aT^2$ for some $\alpha, a \in A$ and $u \in \mathbb{F}_q^\times$, where $p$ is the monic generator of $\mathfrak{p}$.

(b) Suppose $q \geq 5$, $r = 2$, and $f_\psi(x) = T + x + gx^{q+1}$. If $g \in \mathbb{F}_q^\times$ or $g = h^{q-1}$ for some nonconstant $h \in A$ not divisible by any prime of degree 1 except possibly $T$, then the Galois group of $f_\psi$ over $F$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$, and, in particular, is nonsolvable.

(c) If $f_\psi(x) = T + uTx + x^{(q^r-1)/(q-1)}$, where $u \in \mathbb{F}_q^\times$, then the Galois group of $f_\psi$ over $F$ is isomorphic to $\mathrm{PGL}_r(\mathbb{F}_q)$.

Under the assumptions in (b) or (c), the set of primes $\{\mathfrak{p} : b_{\mathfrak{p},1}(\psi) \equiv 0 \pmod{T}\}$ has Dirichlet density $1/\#\,\mathrm{PGL}_r(\mathbb{F}_q)$. □

Polynomials similar to $f_\psi(x)$ in (b) and (c) were extensively studied by Abhyankar in connection with the problem of resolution of singularities in positive characteristic (cf. [1, 2]); for that reason, we call them *Abhyankar trinomials*. In fact, the claim in Part (c) of Theorem 5 is a special case of [1, Theorem 1.1]. The argument in [1] is somewhat hard to follow, mostly due to the generality Abhyankar aims for, but also because of frequent references to his other papers. For that reason, we give a proof of (b) by adapting Serre's methods for elliptic curves [34] to Drinfeld modules.

In the above results, the invariants $a_\mathfrak{p}(\psi), b_\mathfrak{p}(\psi), \delta_\mathfrak{p}(\psi)$ associated to $\psi$ play an essential role. The first one, "the Frobenius trace", has been the subject of several studies in relation to the Sato–Tate and Lang–Trotter Conjectures for Drinfeld modules (cf. [3, 6, 9, 10, 15, 21, 31, 39, 41]). In this paper, we study the second invariant, $b_\mathfrak{p}(\psi)$, and prove the following theorem.

**Theorem 6.** Let the setting and notation be as in Theorem 1.

(a) If $\mathrm{End}_{\bar{F}}(\psi) = A$, then, for $x \in \mathbb{N}$ going to infinity, we have the asymptotic formula

$$\#\{\mathfrak{p} \in \mathcal{P}_\psi : \deg \mathfrak{p} = x, \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p}) = A[\pi_\mathfrak{p}(\psi)]\} \sim \sum_{\substack{m \in A \\ m \text{ monic}}} \frac{\mu_A(m) c_{J_m}(x)}{[J_m : F]} \cdot \frac{q^x}{x}, \tag{4}$$

where $\mu_A(\cdot)$ denotes the Möbius function on $A$, $J_m$ is the subfield of $F(\psi[m])$ fixed by the scalars, $c_{J_m} := [J_m \cap \bar{\mathbb{F}}_q : \mathbb{F}_q]$, and

$$c_{J_m}(x) := \begin{cases} c_{J_m} & \text{if } c_{J_m} | x, \\ 0 & \text{otherwise.} \end{cases}$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

Moreover, the Dirichlet density of the set $\{\mathfrak{p}\in\mathcal{P}_\psi : \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi\otimes\mathbb{F}_\mathfrak{p}) = A[\pi_\mathfrak{p}(\psi)]\}$ exists and equals $\sum_{\substack{m\in A\\ m\ \text{monic}}} \frac{\mu_A(m)}{[J_m:F]}$.

(b) If $\mathrm{End}_{\bar{F}}(\psi)$ is the integral closure of $A$ in a quadratic imaginary extension $K$ of $F$, then, for $x\in\mathbb{N}$ going to infinity, we have the asymptotic formula

$$\#\{\mathfrak{p}\in\mathcal{P}_\psi : \deg\mathfrak{p} = x, \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi\otimes\mathbb{F}_\mathfrak{p}) = A[\pi_\mathfrak{p}(\psi)]\} \sim \frac{c_K(x)}{2}\cdot\frac{q^x}{x}, \tag{5}$$

where $c_K := [K\cap\bar{\mathbb{F}}_q : \mathbb{F}_q]$ and

$$c_K(x) := \begin{cases} c_K & \text{if } c_K | x, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, the Dirichlet density of the set $\{\mathfrak{p}\in\mathcal{P}_\psi : \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi\otimes\mathbb{F}_\mathfrak{p}) = A[\pi_\mathfrak{p}(\psi)]\}$ exists and equals $\frac{1}{2}$. □

Theorem 1 is the function field analog of [12, Theorem 2.1]. To prove this theorem, Duke and Tóth use Deuring's Lifting Theorem. We avoid using such CM-liftings in the proof of Theorem 1 by exploiting the fact that a Drinfeld $A$-module of rank $r$ with endomorphism ring $A'$ can be considered as a Drinfeld $A'$-module of smaller rank. Nevertheless, the question of the existence of CM-liftings for Drinfeld modules is interesting. In this paper, we prove the following analogue of Deuring's Lifting Theorem.

**Theorem 7.** Let $A$ be arbitrary, as at the beginning of this section. Let $k$ be a finite field with $A$-characteristic $\mathfrak{p}$. Let $\phi$ be a Drinfeld $A$-module of rank 2 defined over $k$. Let $g\in\mathrm{End}_k(\phi)\setminus A$. Then, there exist a discrete valuation field $K$ with $A$-characteristic 0 and residue field $k$, a Drinfeld $A$-module $\psi$ of rank 2 defined over $K$, and $f\in\mathrm{End}_K(\psi)$, such that $\phi$ with endomorphism $g$ is the reduction of $\psi$ with endomorphism $f$. □

In Section 5, we prove a general result about CM-liftings of Drinfeld modules of arbitrary rank from which Theorem 7 follows. The proofs of our main results are based on both algebraic and analytic techniques.

## 2 Global Description of the Frobenius: Proof of Theorems 1 and 4

### 2.1 Preliminaries

Throughout this section, we assume that $A = \mathbb{F}_q[T]$. In addition to the notation in the introduction, we use the following:

- $A^{(1)}$ denotes the set of monic polynomials in $A$.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

- For $0 \neq a \in A$, $\deg(a)$ denotes the degree of $a$ as a polynomial in $T$ and $\deg(0) := -\infty$.
- For $f = \frac{a}{b} \in F = \mathbb{F}_q(T)$, $\deg(f) := \deg(a) - \deg(b)$. This defines a valuation on $F$ with normalized norm $|f|_\infty := q^{\deg(f)}$; the corresponding place of $F$ is $\infty$.
- For a prime ideal $0 \neq \mathfrak{p} \lhd A$, $F_\mathfrak{p}$ denotes the completion of $F$ at $\mathfrak{p}$, $\mathbb{F}_\mathfrak{p} := A/\mathfrak{p}$, and $\deg(\mathfrak{p}) := [\mathbb{F}_\mathfrak{p} : \mathbb{F}_q]$.

Let $\psi : A \to F\{\tau\}$ be a Drinfeld $A$-module of rank $r$. Let $\mathfrak{l} = \ell A \lhd A$ be a prime ideal with generator $\ell \in A$. For an integer $n \geq 1$, we define $\psi[\mathfrak{l}^n] := \psi[\ell^n]$. (It is easy to see that this does not depend on the choice of $\ell$.) For $n' \geq n$, we have the inclusion $\psi[\mathfrak{l}^n] \subseteq \psi[\mathfrak{l}^{n'}]$, which is compatible with the $A$-module structure and the action of $G_F$. Hence

$$\psi[\mathfrak{l}^\infty] := \varinjlim_n \psi[\mathfrak{l}^n] \cong (F_\mathfrak{l}/A_\mathfrak{l})^{\oplus r},$$

where $F_\mathfrak{l}$ and $A_\mathfrak{l}$ are the completions of $F$ and $A$ at $\mathfrak{l}$, respectively. The $\mathfrak{l}$*-adic Tate module of* $\psi$, defined as

$$T_\mathfrak{l}(\psi) := \mathrm{Hom}_{A_\mathfrak{l}}(F_\mathfrak{l}/A_\mathfrak{l}, \psi[\mathfrak{l}^\infty]) \cong A_\mathfrak{l}^{\oplus r},$$

is endowed with a continuous action of $G_F$, giving rise to a representation

$$\rho_{\psi,\mathfrak{l}} : G_F \to \mathrm{GL}_r(A_\mathfrak{l})$$

whose reduction modulo $\mathfrak{l}$ is $\bar{\rho}_{\psi,\ell}$ of (1).

Assume now that $\mathfrak{p} \neq \mathfrak{l}$ is a prime of good reduction of $\psi$. More precisely, if $\psi$ is given by (2), assume $\mathrm{ord}_\mathfrak{p}(g_i) \geq 0$ for all $1 \leq i \leq r-1$ and $\mathrm{ord}_\mathfrak{p}(g_r) = 0$. Then, according to [36, Theorem 1], the representation $\rho_{\psi,\mathfrak{l}}$ is unramified at $\mathfrak{p}$, and so, up to conjugation, there is a well-defined matrix

$$\rho_{\psi,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{p}) \in \mathrm{GL}_r(A_\mathfrak{l})$$

whose characteristic polynomial we denote by $P_{\psi,\mathfrak{p}}(x)$. The polynomial $P_{\psi,\mathfrak{p}}(x)$ has coefficients in $A$, does not depend on the choice of $\mathfrak{l}$, and is equal to the characteristic polynomial of the Frobenius endomorphism of the reduction $\psi \otimes \mathbb{F}_\mathfrak{p}$ acting on $T_\mathfrak{l}(\psi \otimes \mathbb{F}_\mathfrak{p})$; see [36, pp. 478–479]. In particular, the roots of $P_{\psi,\mathfrak{p}}(x)$ are integral over $A$. Let $\pi_\mathfrak{p}(\psi)$ denote one of those roots.

**Proposition 8.** The field extension $F(\pi_\mathfrak{p}(\psi))/F$ is imaginary of degree $r$. □

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

**Proof.** By the reduction properties of Drinfeld modules, $\pi := \pi_{\mathfrak{p}}(\psi)$ is a Weil number of rank $r$ over $\mathbb{F}_{\mathfrak{p}}$; cf. [36, p. 479; 38, p. 165]. Next, by the properties of Weil numbers, the extension $F(\pi)/F$ is imaginary of degree dividing $r$; see [38, pp. 165–166]. On the other hand, the norm $\mathrm{N}_{F(\pi)/F}(\pi) \in A$ generates the ideal $\mathfrak{p}^{[F(\pi):F]/r}$; cf. [38, p. 167]. Since $\mathfrak{p}$ is prime, we must have $[F(\pi):F] = r$. ■

Let

$$E_{\psi,\mathfrak{p}} := \mathrm{End}_{\mathbb{F}_{\mathfrak{p}}}(\psi \otimes \mathbb{F}_{\mathfrak{p}}), \quad \bar{E}_{\psi,\mathfrak{p}} := \mathrm{End}_{\bar{\mathbb{F}}_{\mathfrak{p}}}(\psi \otimes \mathbb{F}_{\mathfrak{p}}),$$

$$\mathcal{O}_{\psi,\mathfrak{p}} := \text{integral closure of } A \text{ in } F(\pi_{\mathfrak{p}}(\psi)).$$

As a consequence of [38, Theorem 1] and Proposition 8, we have $E_{\psi,\mathfrak{p}} \otimes_A F = F(\pi_{\mathfrak{p}}(\psi))$. Hence $A[\pi_{\mathfrak{p}}(\psi)]$ and $E_{\psi,\mathfrak{p}}$ are $A$-orders in $F(\pi_{\mathfrak{p}}(\psi))$, and we have the inclusions

$$A \subsetneq A[\pi_{\mathfrak{p}}(\psi)] \subseteq E_{\psi,\mathfrak{p}} \subseteq \mathcal{O}_{\psi,\mathfrak{p}}. \tag{6}$$

It is known that $\bar{E}_{\psi,\mathfrak{p}}$ is a division algebra over $F$, and at the level of division algebras, we have the inclusions

$$F \subsetneq F(\pi_{\mathfrak{p}}(\psi)) = E_{\psi,\mathfrak{p}} \otimes_A F = \mathcal{O}_{\psi,\mathfrak{p}} \otimes_A F \subseteq \bar{E}_{\psi,\mathfrak{p}} \otimes_A F. \tag{7}$$

We say that $\mathfrak{p}$ is a *supersingular* prime for $\psi$ if $\dim_F(\bar{E}_{\psi,\mathfrak{p}} \otimes_A F) = r^2$. We say that $\mathfrak{p}$ is an *ordinary* prime for $\psi$ if $\dim_F(\bar{E}_{\psi,\mathfrak{p}} \otimes_A F) = r$. If $r=2$, then any prime $\mathfrak{p} \in \mathcal{P}_\psi$ is either ordinary or supersingular.

When $r=2$, the coefficients of

$$P_{\psi,\mathfrak{p}}(x) = x^2 + a_{\mathfrak{p}}(\psi)x + a'_{\mathfrak{p}}(\psi)$$

can be explicitly determined as follows. Let $\mathrm{N}_{\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_q}$ be the norm map from $\mathbb{F}_{\mathfrak{p}}$ to $\mathbb{F}_q$. Let

$$u_{\mathfrak{p}}(\psi) := (-1)^{\deg(\mathfrak{p})} \mathrm{N}_{\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_q}(g_2)^{-1},$$

where, by abuse of notation, $g_2$ in the norm denotes the reduction of $g_2$ modulo $\mathfrak{p}$. For an integer $k \geq 1$, put $[k] := T^{q^k} - T$, and define $s_0 := 1$, $s_1 := g_1$,

$$s_k := -[k-1]s_{k-2}g_2^{q^{k-2}} + s_{k-1}g_1^{q^{k-1}} \quad (k \geq 2).$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

**Proposition 9.**

(i) The coefficient $a_{\mathfrak{p}}(\psi) \in A$ is uniquely determined by

$$a_{\mathfrak{p}}(\psi) \equiv -u_{\mathfrak{p}}(\psi) s_{\deg(\mathfrak{p})} (\bmod\, \mathfrak{p})$$

and

$$\deg a_{\mathfrak{p}}(\psi) \leq \frac{\deg(\mathfrak{p})}{2}. \tag{8}$$

(ii) The coefficient $a'_{\mathfrak{p}}(\psi) \in A$ is equal to $u_{\mathfrak{p}}(\psi) p$, where $p \in A^{(1)}$ is the monic generator of $\mathfrak{p}$. □

**Proof.** This follows from [15, Theorem 2.11, Proposition 3.7]. ■

### 2.2 Proof of Theorem 1 and its corollaries

We keep the notation of Section 2.1, but assume that $r = 2$ and $q$ is odd. Note that even though the characteristic polynomial of $\bar{\rho}_{\psi,a}(\mathrm{Frob}_{\mathfrak{p}})$ can be computed in terms of $g_1$, $g_2$, and $\mathfrak{p}$, this is not sufficient for determining the conjugacy class of $\bar{\rho}_{\psi,a}(\mathrm{Frob}_{\mathfrak{p}})$, as this matrix is not necessarily semi-simple. For this, we need an extra invariant $b_{\mathfrak{p}}(\psi)$ related to the reduction of $\psi$ at $\mathfrak{p}$. Both $A[\pi_{\mathfrak{p}}(\psi)]$ and $E_{\psi,\mathfrak{p}}$ are $A$-orders in $\mathcal{O}_{\psi,\mathfrak{p}}$, hence of the form

$$A[\pi_{\mathfrak{p}}(\psi)] = A + \mathfrak{c}_{\mathfrak{p}}(\psi)\mathcal{O}_{\psi,\mathfrak{p}}, \tag{9}$$

$$E_{\psi,\mathfrak{p}} = A + \mathfrak{c}'_{\mathfrak{p}}(\psi)\mathcal{O}_{\psi,\mathfrak{p}} \tag{10}$$

for some ideals $\mathfrak{c}_{\mathfrak{p}}(\psi)$, $\mathfrak{c}'_{\mathfrak{p}}(\psi)$ of $A$, satisfying

$$\mathfrak{c}'_{\mathfrak{p}}(\psi) \mid \mathfrak{c}_{\mathfrak{p}}(\psi). \tag{11}$$

We define

$$\mathfrak{b}_{\mathfrak{p}}(\psi) = b_{\mathfrak{p}}(\psi) A := \frac{\mathfrak{c}_{\mathfrak{p}}(\psi)}{\mathfrak{c}'_{\mathfrak{p}}(\psi)}, \tag{12}$$

where $b_{\mathfrak{p}}(\psi) \in A^{(1)}$. This is an ideal of $A$ such that

$$E_{\psi,\mathfrak{p}}/A[\pi_{\mathfrak{p}}(\psi)] \simeq A/\mathfrak{b}_{\mathfrak{p}}(\psi). \tag{13}$$

In other words, the ideal $\mathfrak{b}_{\mathfrak{p}}(\psi)$ measures how much larger the endomorphism ring $E_{\psi,\mathfrak{p}}$ is than $A[\pi_{\mathfrak{p}}(\psi)]$.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

**Proposition 10.** Let $\Delta(E_{\psi,\mathfrak{p}})$ denote the discriminant ideal of $E_{\psi,\mathfrak{p}}$. Then, with prior notation,

$$\left(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p\right)A = \mathfrak{b}_{\mathfrak{p}}(\psi)^2\Delta(E_{\psi,\mathfrak{p}}). \tag{14}$$

Consequently, there exists $\delta_{\mathfrak{p}}(\psi) \in A$ such that

$$\Delta(E_{\psi,\mathfrak{p}}) = \delta_{\mathfrak{p}}(\psi)A$$

and

$$a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p = b_{\mathfrak{p}}(\psi)^2\delta_{\mathfrak{p}}(\psi). \tag{15}$$

□

**Proof.** Let $\Delta(\mathcal{O}_{\psi,\mathfrak{p}})$ be the discriminant ideal of $\mathcal{O}_{\psi,\mathfrak{p}}$, and let

$$d_{\mathfrak{p}}(\psi) := a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p \in A$$

be the discriminant of the characteristic polynomial $P_{\psi,\mathfrak{p}}$. On one hand, by (10),

$$\Delta(E_{\psi,\mathfrak{p}}) = \mathfrak{c}'_{\mathfrak{p}}(\psi)^2\Delta(\mathcal{O}_{\psi,\mathfrak{p}});$$

hence, upon multiplying by $\mathfrak{c}_{\mathfrak{p}}(\psi)^2$ and using (12),

$$\mathfrak{b}_{\mathfrak{p}}(\psi)^2\Delta(E_{\psi,\mathfrak{p}}) = \mathfrak{c}_{\mathfrak{p}}(\psi)^2\Delta(\mathcal{O}_{\psi,\mathfrak{p}}). \tag{16}$$

On the other hand, by (9),

$$d_{\mathfrak{p}}(\psi)A = \mathfrak{c}_{\mathfrak{p}}(\psi)^2\Delta(\mathcal{O}_{\psi,\mathfrak{p}}). \tag{17}$$

By putting (16) and (17) together, we complete the proof. ■

**Proof of Theorem 1.** By definition, $E_{\psi,\mathfrak{p}}$ is the centralizer of the image of $A$ under $\psi$ in $\mathbb{F}_{\mathfrak{p}}\{\tau\}$. Thus there exists a natural embedding

$$\phi : E_{\psi,\mathfrak{p}} \hookrightarrow \mathbb{F}_{\mathfrak{p}}\{\tau\}$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

such that the diagram:

$$\begin{tikzcd} A \arrow[r] \arrow[dr, "\psi\otimes\mathbb{F}_\mathfrak{p}"'] & E_{\psi,\mathfrak{p}} \arrow[d, "\phi"] \\ & \mathbb{F}_\mathfrak{p}\{\tau\} \end{tikzcd}$$

is commutative.

Recalling that $A \subsetneq E_{\psi,\mathfrak{p}}$ and using that $E_{\psi,\mathfrak{p}}$ is an $A$-module of rank 2, while $\psi$ is a Drinfeld $A$-module of rank 2, we see that $\phi$ defines an elliptic $E_{\psi,\mathfrak{p}}$-module over $\mathbb{F}_\mathfrak{p}$ of rank 1 in the sense of [19, Definition 2.1]. We will use $\phi$ to determine the action of the Frobenius of $\text{Gal}(\bar{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$ on $\psi[a]$.

On one hand, since $(a, p) = 1$, we have an isomorphism of $E_{\psi,\mathfrak{p}}$-modules $\phi[a] \simeq_{E_{\psi,\mathfrak{p}}} E_{\psi,\mathfrak{p}}/aE_{\psi,\mathfrak{p}}$. On the other hand, from the commutative diagram, we have $\psi[a] \simeq_{E_{\psi,\mathfrak{p}}} \phi[a]$. Thus

$$\psi[a] \simeq_{E_{\psi,\mathfrak{p}}} E_{\psi,\mathfrak{p}}/aE_{\psi,\mathfrak{p}}.$$

Under this isomorphism, the action of the Frobenius of $\text{Gal}(\bar{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$ on $\psi[a]$ corresponds to multiplication by $\pi_\mathfrak{p}(\psi)$ on $E_\mathfrak{p}(\psi)/aE_{\psi,\mathfrak{p}}$.

We now explore how this action extends to the $A$-module structure of $\psi[a]$. We fix a square root $\sqrt{\delta_\mathfrak{p}(\psi)}$ of $\delta_\mathfrak{p}(\psi)$ in $F^{\text{sep}}$ and write

$$E_{\psi,\mathfrak{p}} = A + \sqrt{\delta_\mathfrak{p}(\psi)}A.$$

By (15),

$$\pi_\mathfrak{p}(\psi) = -\frac{a_\mathfrak{p}(\psi)}{2} + \sqrt{\delta_\mathfrak{p}(\psi)}\frac{b_\mathfrak{p}(\psi)}{2} \in E_{\psi,\mathfrak{p}}, \tag{18}$$

and so the action of $\pi_\mathfrak{p}(\psi)$ on the $A$-module $E_{\psi,\mathfrak{p}}$ is given by (18) and

$$\pi_\mathfrak{p}(\psi)\sqrt{\delta_\mathfrak{p}(\psi)} = \frac{\delta_\mathfrak{p}(\psi)b_\mathfrak{p}(\psi)}{2} + \sqrt{\delta_\mathfrak{p}(\psi)}\left(-\frac{a_\mathfrak{p}(\psi)}{2}\right).$$

This completes the proof of Theorem 1. ■

Corollary 2 is an immediate consequence to Theorem 1. The description of $d_{1,\mathfrak{p}}(\psi)$ in Corollary 3 is a consequence to Corollary 2 and the property that, for $a \in A$ with $(a, p) = 1$, $\mathfrak{p}$ splits completely in $F(\psi[a])/F$ if and only if $A/aA \times A/aA$ is isomorphic to

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

an $A$-submodule of ${}^{\psi}\mathbb{F}_{\mathfrak{p}}$; see [8, Proposition 23]. The description of $d_{2,\mathfrak{p}}(\psi)$ in Corollary 3 is a consequence to

$$P_{\psi,\mathfrak{p}}(1)A = \chi({}^{\psi}\mathbb{F}_{\mathfrak{p}}) = d_{1,\mathfrak{p}}(\psi)d_{2,\mathfrak{p}}(\psi)A,$$

where $\chi({}^{\psi}\mathbb{F}_{\mathfrak{p}})$ denotes the Euler–Poincaré characteristic of ${}^{\psi}\mathbb{F}_{\mathfrak{p}}$ (see [14]).

### 2.3 Proof of Theorem 4

To simplify the notation, let $\pi := \pi_{\mathfrak{p}}(\psi)$ and $E := E_{\psi,\mathfrak{p}}$. From Proposition 8 and (6) we get that $A[\pi] \subseteq E$ are $A$-orders in $F(\pi)$. Since $A$ is a principal ideal domain and $[F(\pi):F] = r$, the $A$-modules $A[\pi]$ and $E$ are free of rank $r$. Now by the elementary divisors theorem [24, Theorem III.7.8], there is an exact sequence of $A$-modules

$$0 \longrightarrow A[\pi] \longrightarrow E \longrightarrow A/b_0A \oplus A/b_1A \oplus \cdots \oplus A/b_{r-1}A \longrightarrow 0, \tag{19}$$

where $b_0, \ldots, b_{r-1} \in A$ are uniquely determined monic polynomials such that

$$b_0 \mid b_1 \mid \cdots \mid b_{r-1}. \tag{20}$$

(Of course, $b_0, \ldots, b_{r-1}$ depend on $\psi$ and $\mathfrak{p}$, which we omit from notation.) Note that every element of $A[\pi]$, considered as an element of $E$, is a multiple of $b_0$. But $1 \in A[\pi]$, so $b_0 = 1$. In other terms, $A/b_0A$ is trivial, and can be ignored. This proves Part (a) of the theorem.

If we assume that $r$ is coprime to $q$, then the extension $F(\pi)/F$ is separable. The elementary properties of discriminants then imply (cf. [24, Exercise VI.32])

$$\mathrm{disc}(P_{\psi,\mathfrak{p}})A = \mathrm{disc}(A[\pi]) = \mathrm{disc}(E)(b_{\mathfrak{p},1}(\psi)\cdots b_{\mathfrak{p},r-1}(\psi))^2,$$

which is (b).

As in the rank-2 case, we have an isomorphism $\psi[a] \simeq_E E/aE$ with the action of $\bar{\rho}_{\psi,a}(\mathrm{Frob}_{\mathfrak{p}})$ on the left-hand side corresponding to multiplication by $\pi$ on the right-hand side. Consider the $A$-linear transformation of the free rank-$r$ $A$-module $E$ induced by multiplication by $\pi$. This transformation is congruent to an element of the center $Z(A) \cong A$ of $M_r(A)$ modulo $a$ if and only if $A[\pi] \subseteq A + aE$. On the other hand, $A[\pi] \subseteq A + aE$ if and only if $(E/aE)/(A[\pi]/(A[\pi] \cap aE)) \simeq_A (A/aA)^{\oplus r-1}$. Tensoring (19) with $A/aA$, we see that this last condition is equivalent to

$$(A/b_1A \otimes_A A/aA) \oplus \cdots \oplus (A/b_{r-1}A \otimes_A A/aA) \simeq_A (A/aA)^{\oplus r-1}.$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

As is easy to check,

$$A/b_i A \otimes_A A/aA \simeq_A A/\gcd(b_i, a)A.$$

Thus, $\mathrm{Frob}_{\mathfrak{p}}$ acts trivially on $J_a$ (equivalently, $\mathfrak{p}$ splits completely in $J_a$) if and only if $a$ divides all $b_i$. Since $b_1$ divides all $b_i$, this last condition is equivalent to $a|b_1$. This concludes the proof of the theorem.

## 3 Abhyankar trimonials: proof of Theorem 5

Let $\psi$ and $f_\psi$ be as in (2) and (3), respectively. Let $\mathrm{Gal}(f_\psi)$ denote the Galois group of the splitting field of $f_\psi$ over $F$. We consider the composition of $\bar{\rho}_{\psi,T}$ with the natural projection onto $\mathrm{PGL}_r(A/TA)$, and, after identifying $A/TA \simeq \mathbb{F}_q$, we write it as

$$\hat{\rho}_{\psi,T} : G_F \longrightarrow \mathrm{PGL}_r(\mathbb{F}_q).$$

If $0 \neq s \in \psi[T]$, then $s^{q-1}$ is a zero of $f_\psi(x)$. The center $Z(\mathbb{F}_q) \simeq \mathbb{F}_q^\times$ of $\mathrm{GL}_2(\mathbb{F}_q)$ acts on $\psi[T]$ by the usual multiplication, that is, $\gamma \in \mathbb{F}_q^\times$ maps $s$ to $\gamma s \in F^{\mathrm{sep}}$. Hence $\gamma$ maps $s^{q-1}$ to $\gamma^{q-1}s^{q-1} = s^{q-1}$, and so the action of $\mathrm{GL}_r(\mathbb{F}_q)$ on the set of zeros of $f_\psi$, induced from the action on $\psi[T]$, factors through $\mathrm{PGL}_r(\mathbb{F}_q)$. This implies that the action of $G_F$ on the set of zeros of $f_\psi$ factors through $\hat{\rho}_{\psi,T}$, and

$$\mathrm{Gal}(f_\psi) \simeq \hat{\rho}_{\psi,T}(G_F). \tag{21}$$

Now let $\mathfrak{p} \in \mathcal{P}_\psi$, $\mathfrak{p} \neq T$. It follows from (21) and Theorem 4(c) that $f_\psi$ splits completely modulo $\mathfrak{p}$ if and only if $b_{\mathfrak{p},1}(\psi) \equiv 0 \pmod{T}$. Therefore, Part (a) of Theorem 5 follows from Theorem 4(b) and (15).

Now we focus on Part (b) of Theorem 5. Let $\psi$ be the rank-2 Drinfeld module defined by $\psi_T = T + \tau + g\tau^2$. Our goal is to prove that, provided either $g \in \mathbb{F}_q^\times$ or $g = h^{q-1}$ for some nonconstant $h \in A$ not divisible by any prime of degree 1 except possibly $T$,

$$\hat{\rho}_{\psi,T}(G_F) \simeq \mathrm{PGL}_2(\mathbb{F}_q). \tag{22}$$

For this, we will follow the general strategy of [34, Section 2.8].

Let us consider the case $g \in \mathbb{F}_q^\times$. Then $\psi$ has good reduction at every prime of $A$, and so the extension $F(\psi[T])/F$ is unramified away from $T$ and $\infty$. In particular, it is unramified at every prime $\mathfrak{p} = pA$ defined by $p = T - c$ for some $c \in \mathbb{F}_q^\times$. For such $\mathfrak{p}$ let us outline a few properties of $\bar{\rho}_{\psi,T}(\mathrm{Frob}_{\mathfrak{p}})$, which will eventually restrict the possible group

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

structures of $\hat{\rho}_{\psi,T}(G_F)$. By Proposition 9,

$$\det \bar{\rho}_{\psi,T}(\mathrm{Frob}_{\mathfrak{p}}) = u_{\mathfrak{p}}(\psi)\, p \bmod T = \frac{c}{g}.$$

Therefore

$$\det \bar{\rho}_{\psi,T} : G_F \longrightarrow \mathbb{F}_q^{\times} \quad \text{is surjective.} \tag{23}$$

Again, by Proposition 9,

$$\mathrm{tr}\, \bar{\rho}_{\psi,T}(\mathrm{Frob}_{\mathfrak{p}}) = -a_{\mathfrak{p}}(\psi) = -\frac{1}{g} \in \mathbb{F}_q^{\times}. \tag{24}$$

Hence

$$d_{\mathfrak{p}}(\psi) = a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\, p = \frac{1}{g^2} - \frac{4c}{g}, \tag{25}$$

$$t_{\mathfrak{p}}(\psi) := \frac{\mathrm{tr}\, \bar{\rho}_{\psi,T}(\mathrm{Frob}_{\mathfrak{p}})^2}{\det \bar{\rho}_{\psi,T}(\mathrm{Frob}_{\mathfrak{p}})} = \frac{a_{\mathfrak{p}}(\psi)^2}{u_{\mathfrak{p}}(\psi)\, p} = \frac{1}{cg}. \tag{26}$$

Since $q$ is odd, (25) implies that $d_{\mathfrak{p}}(\psi)$ assumes all values of $\mathbb{F}_q \backslash \{\frac{1}{g^2}\}$. In particular, since $q \geq 5$,

$$\text{there are } \mathfrak{p} \text{ for which } d_{\mathfrak{p}}(\psi) \text{ is a nonzero square} \tag{27}$$

and

$$\text{there are } \mathfrak{p} \text{ for which } d_{\mathfrak{p}}(\psi) \text{ is not a square.} \tag{28}$$

Moreover, (26) implies that there are $\mathfrak{p}$ for which

$$t_{\mathfrak{p}}(\psi) \notin \{0, 1, 2, 4\} \tag{29}$$

and

$$t_{\mathfrak{p}}(\psi) \text{ does not satisfy } u^2 - 3u + 1 = 0 \tag{30}$$

(e.g., if the characteristic is not 3, then $c := (3g)^{-1}$ gives the value 3, which satisfies these restrictions).

We will use the following classical theorem.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

**Theorem 11** (Dickson)**.** Any proper subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ is contained in one of the groups:

(i) a Borel subgroup;

(ii) $\mathrm{PSL}_2(\mathbb{F}_q)$;

(iii) a conjugate of the subgroup $\mathrm{PGL}_2(\mathbb{F})$ for some subfield $\mathbb{F} \subsetneq \mathbb{F}_q$;

(iv) a dihedral group $D_{2n}$ of order $2n$, where $n$ is not divisible by the characteristic of $\mathbb{F}_q$;

(v) a subgroup isomorphic to one of the permutation groups $A_4$, $A_5$, $S_4$. □

**Proof.** See [22, Theorem 8.27]. ■

The properties of $H := \hat{\rho}_{\psi,T}(G_F)$ derived from the above observations will exclude all cases in Dickson's theorem, leaving $H = \mathrm{PGL}_2(\mathbb{F}_q)$ as the only possibility. Indeed, (i) is not possible by (28), and (ii) is not possible by (23). If $H$ is conjugate to a subgroup of $\mathrm{PGL}_2(\mathbb{F})$, then $t_\mathfrak{p}(\psi) \in \mathbb{F}$ for all $p = T - c$. This contradicts the fact that $t_\mathfrak{p}(\psi) = (cg)^{-1}$ assumes all values in $\mathbb{F}_q^\times$ as $c$ varies. Hence (iii) is not possible. If $H$ is isomorphic to $A_4$, $A_5$, or $S_4$, then for each $h \in H$, the element $u = \mathrm{tr}(h)^2/\det(h)$ is equal to $0, 1, 2, 4$, or satisfies $u^2 - 3u + 1 = 0$; this follows from [34, Section 2.6], although in [34] this is stated for prime fields. Hence (v) is not possible by (29) and (30). Finally, to exclude (iv) we argue as in [34, p. 284]. If $H$ is cyclic or dihedral, then $\bar{\rho}_{\psi,T}(G_F)$ is contained in a normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. But the trace of $\bar{\rho}_{\psi,T}(\mathrm{Frob}_\mathfrak{p})$ is nonzero by (24), and by (28) there is $\mathfrak{p}$ for which $d_\mathfrak{p}(\psi)$ is not a square; this leads to a contradiction as in [34].

To prove that $\hat{\rho}_{\psi,T}(G_F) = \mathrm{PGL}_2(\mathbb{F}_q)$ when $g = h^{q-1}$ for some nonconstant $h \in A$ not divisible by any prime of degree 1, except possibly $T$, one can use the same arguments as above, based on the calculations (below, $\mathfrak{p} = T - c$ with $c \in \mathbb{F}_q^\times$)

$$\det(\bar{\rho}_{\psi,T}(\mathrm{Frob}_\mathfrak{p})) = (-1)h(c)^{-(q-1)}(T - c) = c \in \mathbb{F}_q^\times,$$

$$\mathrm{tr}(\bar{\rho}_{\psi,T}(\mathrm{Frob}_\mathfrak{p})) = -\frac{1}{h(c)^{q-1}} = -1 \in \mathbb{F}_q^\times.$$

As we mentioned in Section 1, Part (c) of Theorem 5 follows from the main result in [1]. Finally, for a Drinfeld module $\psi$ producing $f_\psi$ in Part (b) or (c), the Chebotarev Density Theorem implies that the Dirichlet density of

$$\{\mathfrak{p} \in \mathcal{P}_\psi : b_{\mathfrak{p},1}(\psi) \equiv 0 \pmod{T}\} = \{\mathfrak{p} \in \mathcal{P}_\psi : f_\psi \text{ splits completely modulo } \mathfrak{p}\}$$

exists and equals $\frac{1}{\#\,\mathrm{PGL}_r(\mathbb{F}_q)}$.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

## 4 Reductions of Drinfeld Modules: Proof of Theorem 6

### 4.1 Preliminaries

The proofs of the following two lemmas are elementary and are left to the reader.

**Lemma 12.** Let $y \geq 1$ be an integer. Then:

(i) $\sum_{\substack{m\in A^{(1)}\\ 0\leq \deg m\leq y}} 1 = \frac{q^{y+1}-1}{q-1}$;

(ii) $\sum_{\substack{m\in A^{(1)}\\ 0\leq \deg m\leq y}} \deg m \leq y\frac{q^{y+1}-1}{q-1}$. □

**Lemma 13.** Let $y \geq 3$ be an integer and let $\alpha > 1$. Then:

(i) $\sum_{\substack{a\in A\\ \deg a>y}} \frac{1}{q^{\alpha \deg a}} = \frac{q}{(1-\frac{1}{q^{\alpha-1}})q^{(\alpha-1)(y+1)}}$;

(ii) $\sum_{\substack{a\in A\\ \deg a>y}} \frac{\log \deg a}{q^{\alpha \deg a}} \leq \frac{\log y}{(\alpha-1)q^{(\alpha-1)y}\log q} + \frac{1}{y(\alpha-1)^2 q^{(\alpha-1)y}(\log q)^2}$, provided that

$$(\alpha-1)y\log q \log y > 1.$$ □

**Lemma 14.** Let $h \in A\backslash\mathbb{F}_q$ and $\tau_A(h) := \sum_{\substack{d\in A^{(1)}\\ d|h}} 1$ its divisor function. Then, for any $\varepsilon > 0$,

$$\tau_A(h) \ll_\varepsilon |h|_\infty^\varepsilon.$$ □

**Proof.** Over $\mathbb{Z}$, this is a well-known result (see, e.g., the proof in [17, p. 344]). Over $A$, one can prove the result essentially in the same way. We include the details for completeness.

Consider the prime factorization $h = u\prod_{\ell|h}\ell^\alpha$ of $h$. Then

$$\frac{\tau_A(h)}{|h|_\infty^\varepsilon} = \prod_{\ell|h}\frac{\alpha+1}{|\ell|_\infty^{\alpha\varepsilon}} = \prod_{\substack{\ell|h\\ |\ell|_\infty<2^{\frac{1}{\varepsilon}}}}\frac{\alpha+1}{|\ell|_\infty^{\alpha\varepsilon}}\cdot\prod_{\substack{\ell|h\\ |\ell|_\infty\geq 2^{\frac{1}{\varepsilon}}}}\frac{\alpha+1}{|\ell|_\infty^{\alpha\varepsilon}} \leq \prod_{\substack{\ell|h\\ |\ell|_\infty<2^{\frac{1}{\varepsilon}}}}\frac{\alpha+1}{|\ell|_\infty^{\alpha\varepsilon}}\cdot\prod_{\substack{\ell|h\\ |\ell|_\infty\geq 2^{\frac{1}{\varepsilon}}}}\frac{\alpha+1}{2^\alpha} \leq \prod_{\substack{\ell|h\\ |\ell|_\infty<2^{\frac{1}{\varepsilon}}}}\frac{\alpha+1}{|\ell|_\infty^{\alpha\varepsilon}}.$$

Observe that

$$\alpha\varepsilon\log 2 \leq \exp(\alpha\varepsilon\log 2) = 2^{\alpha\varepsilon} \leq |\ell|_\infty^{\alpha\varepsilon},$$

therefore

$$\frac{\alpha}{|\ell|_\infty^{\alpha\varepsilon}} \leq \frac{1}{\varepsilon\log 2}.$$

We thus obtain

$$\frac{\alpha+1}{|\ell|_\infty^{\alpha\varepsilon}} \leq \frac{2}{\varepsilon\log 2} \leq \exp\left(\frac{2}{\varepsilon\log 2}\right).$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

This gives

$$\prod_{\substack{\ell | h \\ |\ell|_\infty < 2^{\frac{1}{\varepsilon}}}} \frac{\alpha+1}{|\ell|_\infty^{\alpha\varepsilon}} \leq \exp\left(\frac{2}{\varepsilon \log 2} \cdot \#\{\ell | h : |\ell|_\infty < 2^{\frac{1}{\varepsilon}}\}\right) \leq \exp\left(\frac{2}{\varepsilon \log 2} \cdot \frac{q 2^{\frac{1}{\varepsilon}}}{q-1}\right),$$

a constant in $q$ and $\varepsilon$. ■

Now let us fix $a \in A \backslash \mathbb{F}_q$ and, as before, consider $F_a := F(\psi[a])$ and $J_a \subseteq F_a$ introduced in Part (c) of Theorem 4. This field may also be understood by considering the composition of $\bar{\rho}_{\psi,a}$ with the projection on to $\mathrm{PGL}_2(A/aA)$. Indeed, this composition leads to a Galois representation

$$\hat{\rho}_{\psi,a} : G_F \longrightarrow \mathrm{PGL}_2(A/aA)$$

satisfying

$$J_a = (F^{\mathrm{sep}})^{\mathrm{Ker}\, \hat{\rho}_{\psi,a}}.$$

(Note that we have already considered the special case $\hat{\rho}_{\psi,T}$ in the proof of Theorem 5.)

In what follows, we recall some more properties of the extensions $F_a/F$ and $J_a/F$.

**Theorem 15.**

(i) The degrees of the fields of constants of $F_a$ and $J_a$, that is,

$$\begin{aligned} c_{F_a} &:= [F_a \cap \bar{\mathbb{F}}_q : \mathbb{F}_q], \\ c_{J_a} &:= [J_a \cap \bar{\mathbb{F}}_q : \mathbb{F}_q], \end{aligned} \tag{31}$$

are uniformly bounded from above in terms of $\psi$. That is,

$$c_{J_a} \leq c_{F_a} \leq C(\psi)$$

for some constant $C(\psi) \in \mathbb{N} \backslash \{0\}$.

(ii) The genera $g_{F_a}$, $g_{J_a}$ of $F_a$, $J_a$ are bounded from above by

$$g_{J_a} \leq g_{F_a} \leq G(\psi) \# \mathrm{GL}_2(A/aA) \deg a$$

for some constant $G(\psi) \in \mathbb{N} \backslash \{0\}$.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

(iii) The degrees of $F_a/F$, $J_a/F$ are bounded from above by

$$[F_a : F] \le \# \operatorname{GL}_2(A/aA),$$
$$[J_a : F] \le \# \operatorname{PGL}_2(A/aA).$$

(iv) Assume that $\operatorname{End}_{\bar{F}}(\psi) = A$. There exists $M(\psi) \in A^{(1)}$ such that, if $(a, M(\psi)) = 1$, then

$$\operatorname{Gal}(F_a/F) \simeq \operatorname{GL}_2(A/aA),$$
$$\operatorname{Gal}(J_a/F) \simeq \operatorname{PGL}_2(A/aA)$$

and

$$c_{F_a} = c_{J_a} = 1;$$

if $a$ arbitrary, then

$$\frac{|a|_\infty^4}{\log \deg a + \log\log q} \ll_\psi [F_a : F] \le |a|_\infty^4,$$
$$\frac{|a|_\infty^3}{\log \deg a + \log\log q} \ll_\psi [J_a : F] \le |a|_\infty^3.$$

(v) Assume that $\operatorname{End}_{\bar{F}}(\psi) \ne A$. Then

$$\frac{|a|_\infty^2}{\log \deg a + \log\log q} \ll_\psi [F_a : F] \ll_\psi |a|_\infty^2,$$
$$\frac{|a|_\infty}{\log \deg a + \log\log q} \ll_\psi [J_a : F] \ll_\psi |a|_\infty.$$

(vi) For $x \in \mathbb{N}$, let

$$\Pi_1(x, F_a/F) := \#\{\mathfrak{p} \in \mathcal{P}_\psi : p \nmid a, \deg \mathfrak{p} = x, \mathfrak{p} \text{ splits completely in } F_a\},$$
$$\Pi_1(x, J_a/F) := \#\{\mathfrak{p} \in \mathcal{P}_\psi : p \nmid a, \deg \mathfrak{p} = x, \mathfrak{p} \text{ splits completely in } J_a\}.$$

Then

$$\Pi_1(x, F_a/F) = \frac{c_{F_a}(x)}{[F_a : F]} \cdot \frac{q^x}{x} + \mathrm{O}_\psi\left(\frac{q^{\frac{x}{2}}}{x} \deg a\right),$$
$$\Pi_1(x, J_a/F) = \frac{c_{J_a}(x)}{[J_a : F]} \cdot \frac{q^x}{x} + \mathrm{O}_\psi\left(\frac{q^{\frac{x}{2}}}{x} \deg a\right),$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

where

$$c_{F_a}(x) := \begin{cases} c_{F_a} & \text{if } c_{F_a} | x, \\ 0 & \text{else,} \end{cases}$$

$$c_{J_a}(x) := \begin{cases} c_{J_a} & \text{if } c_{J_a} | x, \\ 0 & \text{else.} \end{cases}$$

(vii) Let $\bar{C}$, $\hat{C}$ be conjugacy classes in $\mathrm{Gal}(F_a/F)$, respectively, in $\mathrm{Gal}(J_a/F)$. Denote by $a_{\bar{C}}$, $a_{\hat{C}}$, respectively, a positive integer such that, for any $\sigma \in \mathrm{Gal}(F_a/F)$, $\mathrm{Gal}(J_a/F)$, respectively, the restriction of $\sigma$ to $F_a \cap \bar{\mathbb{F}}_q$, $J_a \cap \bar{\mathbb{F}}_q$, respectively, equals the corresponding restriction of $\tau^{a_{\bar{C}}}$, $\tau^{a_{\hat{C}}}$, respectively. For $x \in \mathbb{N}$, let

$$\Pi_{\bar{C}}(x, F_a/F) := \#\{\mathfrak{p} \in \mathcal{P}_\psi : p \nmid a, \deg \mathfrak{p} = x, \sigma_{\mathfrak{p}} \subseteq \bar{C}\},$$

$$\Pi_{\hat{C}}(x, J_a/F) := \#\{\mathfrak{p} \in \mathcal{P}_\psi : p \nmid a, \deg \mathfrak{p} = x, \sigma_{\mathfrak{p}} \subseteq \hat{C}\}.$$

Then

$$\Pi_{\bar{C}}(x, F_a/F) = \frac{c_{F_a}(x) \cdot \#\bar{C}}{[F_a : F]} \cdot \frac{q^x}{x} + \mathrm{O}_\psi((\#\bar{C})^{\frac{1}{2}} q^{\frac{x}{2}} \deg a),$$

$$\Pi_{\hat{C}}(x, J_a/F) = \frac{c_{J_a}(x) \cdot \#\hat{C}}{[J_a : F]} \cdot \frac{q^x}{x} + \mathrm{O}_\psi((\#\hat{C})^{\frac{1}{2}} q^{\frac{x}{2}} \deg a),$$

where

$$c_{F_a}(x) := \begin{cases} c_{F_a} & \text{if } c_{F_a} | x - a_{\bar{C}}, \\ 0 & \text{else,} \end{cases} \tag{32}$$

$$c_{J_a}(x) := \begin{cases} c_{J_a} & \text{if } c_{J_a} | x - a_{\hat{C}}, \\ 0 & \text{else.} \end{cases} \tag{33}$$

Note that this notation generalizes the one in Part (vi). Moreover, note that, Part (vii) holds also for unions of conjugacy classes. □

**Proof.** For Part (i), see [16, Remark 7.1.9]. For Part (ii), see [13, Corollary 7]. Part (iii) follows from the injectivity of the residual representations $\mathrm{Gal}(F_a/F) \longrightarrow \mathrm{GL}_2(A/aA)$ and $\mathrm{Gal}(J_a/F) \longrightarrow \mathrm{PGL}_2(A/aA)$. The claims about $\mathrm{Gal}(F_a/F)$, $\mathrm{Gal}(J_a/F)$, $[F_a : F]$, and $[J_a : F]$ in Parts (iv) and (v) can be derived from the main results of [32], as explained in

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

[8, Section 3.6]. The fact that $c_{F_a} = c_{J_a} = 1$ then follows from Proposition 16 below. Parts (vi) and (vii) are applications of the effective Chebotarev Density Theorem of [29], as well as of the prior parts of Theorem 15; see [6, Section 4, 8, Section 4] for more details. That Part (vii) holds also for unions of conjugacy classes can be seen by modifying the proof in [29] by using the techniques of [28, Section 3]. ■

**Proposition 16.** Let $A = \mathbb{F}_q[T]$ and $F = \mathbb{F}_q(T)$. Let $\psi : A \to F\{\tau\}$ be a Drinfeld module of rank $r$ defined over $F$. Assume $\psi$ has good reduction at the primes dividing $a \in A$ and $\mathrm{Gal}(F_a/F) \cong \mathrm{GL}_r(A/aA)$. In addition, if $r = 2$, assume $q$ is odd. Under these assumptions, the extension $F_a$ of $F$ is geometric, that is, $\mathbb{F}_q$ is algebraically closed in $F_a$. □

**Proof.** Let $aA = \prod_i \mathfrak{p}_i^{s_i}$ be the prime decomposition of the ideal $aA$. Since there is an isomorphism of groups

$$\mathrm{GL}_r(A/aA) \cong \prod_i \mathrm{GL}_r(A/\mathfrak{p}_i^{s_i}),$$

the commutator of $\mathrm{GL}_r(A/aA)$ is the direct product of the commutators of $\mathrm{GL}_r(A/\mathfrak{p}_i^{s_i})$. On the other hand, since the set of nonunits in $A/\mathfrak{p}_i^{s_i}$ forms an ideal, according to [27] we have

$$[\mathrm{GL}_r(A/\mathfrak{p}_i^{s_i}), \mathrm{GL}_r(A/\mathfrak{p}_i^{s_i})] = \mathrm{SL}_r(A/\mathfrak{p}_i^{s_i}).$$

(Here we implicitly use the assumption that if $r = 2$, then $q$ is odd.) This implies that

$$[\mathrm{GL}_r(A/aA), \mathrm{GL}_r(A/aA)] = \mathrm{SL}_r(A/aA). \tag{34}$$

We also have the exact sequence

$$0 \to \mathrm{SL}_r(A/aA) \to \mathrm{GL}_r(A/aA) \xrightarrow{\det} (A/aA)^\times \to 0. \tag{35}$$

By assumption, $\mathrm{Gal}(F_a/F) \cong \mathrm{GL}_r(A/aA)$. Let $K$ be the subfield of $F_a$ fixed by $\mathrm{SL}_r(A/aA)$. Let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_q$ in $F_a$, and let $F' = \mathbb{F}F$. The extension $F'/F$ is Galois with Galois group isomorphic to $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$; in particular, it is cyclic. Due to (34), the field $F'$ must be a subfield of $K$, as $\mathrm{Gal}(F'/F)$ is a quotient group of $\mathrm{Gal}(F_a/F)$ which is abelian. Thus, it is enough to show that $K/F$ is geometric.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

There exists a Drinfeld $A$-module $\phi$ of rank-1 defined over $F$ such that there is an isomorphism of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$-modules (cf. [37])

$$\phi[a] \cong \bigwedge^{r} \psi[a].$$

Thus, $F(\phi[a])$ is the subfield of $F_a$ fixed by the kernel of the determinant on $\mathrm{GL}_r(A/aA)$. Therefore, due to (35), $K = F(\phi[a])$ and $\mathrm{Gal}(F(\phi[a])/F) \cong (A/aA)^\times$. Since $\psi$ has good reduction at the primes dividing $a$, the same is true for $\phi$. Finally, by [18, Proposition 5.2], $F(\phi[a])/F$ is geometric. ■

**Remark 17.** In general, a composition of geometric extensions need not be geometric, so in the previous proof we cannot immediately reduce to the case when $aA = \mathfrak{p}^s$. □

### 4.2 Proof of Part (a) of Theorem 6

Let

$$\mathcal{B}(\psi, x) := \#\{\mathfrak{p} \in \mathcal{P}_\psi : \deg \mathfrak{p} = x,\ E_{\psi,\mathfrak{p}} = A[\pi_\mathfrak{p}(\psi)]\}. \tag{36}$$

Our goal is to derive an explicit asymptotic formula for $\mathcal{B}(\psi, x)$, when $q$ is fixed and $x \to \infty$. We start with the simple remarks that

$$\begin{aligned}\mathcal{B}(\psi, x) &= \#\{\mathfrak{p} \in \mathcal{P}_\psi : \deg \mathfrak{p} = x,\ b_\mathfrak{p}(\psi) = 1\}\\ &= \#\{\mathfrak{p} \in \mathcal{P}_\psi : \deg \mathfrak{p} = x,\ \ell \nmid b_\mathfrak{p}(\psi)\ \forall \ell \in A^{(1)}\}\\ &= \sum_{m \in A^{(1)}} \mu_A(m) \#\{\mathfrak{p} \in \mathcal{P}_\psi : \deg \mathfrak{p} = x,\ m \mid b_\mathfrak{p}(\psi)\},\end{aligned}$$

where in the first line we used (13).

An essential aspect in the asymptotic study of such sums is that of determining the range of the polynomial $m \in A^{(1)}$ under summation as a function of $x$. By combining the property $m \mid b_\mathfrak{p}(\psi)$ with (15), we obtain

$$m^2 \mid (a_\mathfrak{p}(\psi)^2 - 4u_\mathfrak{p}(\psi)p).$$

Upon recalling (8) and using that $\deg \mathfrak{p} = x$, we deduce that $\deg m \le \frac{x}{2}$. Thus

$$\mathcal{B}(\psi, x) = \sum_{\substack{m \in A^{(1)}\\ \deg m \le \frac{x}{2}}} \mu_A(m) \#\{\mathfrak{p} \in \mathcal{P}_\psi : \deg \mathfrak{p} = x,\ m \mid b_\mathfrak{p}(\psi)\}.$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

By Theorem 1, the extension $J_m/F$ has the property that, for any $\mathfrak{p} = pA \in \mathcal{P}_\psi$ with $(p, m) = 1$,

$$m \mid b_{\mathfrak{p}}(\psi) \text{ if and only if } \mathfrak{p} \text{ splits completely in } J_m. \tag{37}$$

(Note that, if $\deg \mathfrak{p} = x$ and $\deg m \le \frac{x}{2}$, then the generator $p$ of $\mathfrak{p}$ is coprime with $m$; hence $\mathfrak{p}$ is unramified in $J_m$.) Consequently, we can write

$$\mathcal{B}(\psi, x) = \sum_{\substack{m \in A^{(1)} \\ \deg m \le y}} \mu_A(m) \Pi_1(x, J_m/F) + \sum_{\substack{m \in A^{(1)} \\ y < \deg m \le \frac{x}{2}}} \mu_A(m) \#\{\mathfrak{p} \in \mathcal{P}_\psi : \deg \mathfrak{p} = x, m \mid b_{\mathfrak{p}}(\psi)\}, \tag{38}$$

where $y = y(x)$ is a parameter to be chosen optimally later as a function of $q$ and $x$, and

$$\Pi_1(x, J_m/F) := \#\{\mathfrak{p} \in \mathcal{P}_\psi : (p, m) = 1, \deg \mathfrak{p} = x, \mathfrak{p} \text{ splits completely in } J_m/F\}.$$

The splitting of $\mathcal{B}(\psi, x)$ in two sums is guided by the natural strategy of using an effective version of the Chebotarev Density Theorem, and by the limitation of this tool for our problem. In particular, the Chebotarev Density Theorem can be used only for estimating the first sum on the right-hand side of $\mathcal{B}(\psi, x)$ above, while other methods must be developed to estimate the remaining sum. These latter methods constitute the heart of the proof.

### 4.2.1 *The main term of $\mathcal{B}(\psi, x)$*

For $y = y(x) \le \frac{x}{2}$ a parameter, we focus on

$$\mathcal{B}_1(\psi, x, y) := \sum_{\substack{m \in A^{(1)} \\ \deg m \le y}} \mu_A(m) \Pi_1(x, J_m/F).$$

By Part (vi) of Theorem 15, this becomes

$$\begin{aligned}\mathcal{B}_1(\psi, x, y) &= \sum_{\substack{m \in A^{(1)} \\ \deg m \le y}} \frac{\mu_A(m) c_{J_m}(x)}{[J_m : F]} \cdot \frac{q^x}{x} + \mathrm{O}_\psi\left( \sum_{\substack{m \in A^{(1)} \text{ squarefree} \\ \deg m \le y}} \frac{q^{\frac{x}{2}}}{x} \deg m \right) \\ &= \sum_{m \in A^{(1)}} \frac{\mu_A(m) c_{J_m}(x)}{[J_m : F]} \cdot \frac{q^x}{x} - \sum_{\substack{m \in A^{(1)} \\ \deg m > y}} \frac{\mu_A(m) c_{J_m}(x)}{[J_m : F]} \cdot \frac{q^x}{x} + \mathrm{O}_\psi(q^{\frac{x}{2} + y}),\end{aligned}$$

where, in the last line we used Part (ii) of Lemma 12.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

To estimate the middle term, we use Parts (i) and (iv) of Theorem 15, as well as Lemma 13, and obtain

$$\sum_{\substack{m\in A^{(1)}\\ \deg m>y}} \frac{\mu_A(m)c_{J_m}(x)}{[J_m:F]} \ll_\psi \sum_{\substack{m\in A^{(1)}\ \text{squarefree}\\ \deg m>y}} \frac{\log\deg m+\log\log q}{q^{3\deg m}} \ll \frac{\log y}{q^{2y}\log q}.$$

In summary,

$$\mathcal{B}_1(\psi,x,y)=\sum_{m\in A^{(1)}}\frac{\mu_A(m)c_{J_m}(x)}{[J_m:F]}\cdot\frac{q^x}{x}+\mathrm{O}_\psi(q^{\frac{x}{2}+y})+\mathrm{O}_\psi(q^{x-2y}). \tag{39}$$

### 4.2.2 *The error term of* $\mathcal{B}(\psi,x)$

For $y=y(x)\le\frac{x}{2}$, we focus on obtaining an upper bound for

$$\mathcal{B}_2(\psi,x,y):=\sum_{\substack{m\in A^{(1)}\\ y<\deg m\le\frac{x}{2}}}\mu_A(m)\#\{\mathfrak{p}\in\mathcal{P}_\psi:\deg\mathfrak{p}=x,\, m\mid b_{\mathfrak{p}}(\psi)\}.$$

By (15),

$$m\mid b_{\mathfrak{p}}(\psi)\ \Rightarrow\ m^2\mid(a_{\mathfrak{p}}(\psi)^2-4u_{\mathfrak{p}}(\psi)p).$$

Thus there exist $f,g\in A$ with $g$ squarefree such that

$$a_{\mathfrak{p}}(\psi)^2-4u_{\mathfrak{p}}(\psi)p=m^2f^2g.$$

Upon relabeling $h:=mf$, we obtain that

$$\mathcal{B}_2(\psi,x,y)\le q\sum_{\substack{h\in A\\ y<\deg h\le\frac{x}{2}}}\tau_A(h)\#\{\mathfrak{p}\in\mathcal{P}_\psi:\deg\mathfrak{p}=x,\ \exists g\in A\ \text{squarefree such that}$$
$$a_{\mathfrak{p}}(\psi)^2-4u_{\mathfrak{p}}(\psi)p=h^2g\}.$$

The above range for $\deg h$ is determined simply from

$$\deg h=\deg m+\deg f,$$

hence from

$$\deg h\ge\deg m>y,$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

and also from

$$h^2 \mid (a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\, p),$$

hence from

$$2 \deg h \le \deg p = x,$$

after recalling (8).

Using Lemma 14, we deduce that

$$\mathcal{B}_2(\psi, x, y) \ll_\varepsilon q^{\varepsilon x} \sum_{\substack{h \in A \\ y < \deg h \le \frac{x}{2}}} \#\{\mathfrak{p} \in \mathcal{P}_\psi : \deg \mathfrak{p} = x,\ \exists g \in A \text{ squarefree such that}$$

$$a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\, p = h^2 g\}.$$

Note that the factorization $a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\, p = h^2 g$ is unique up to the multiplication of $g$ by a square in $\mathbb{F}_q^\times$. As such,

$$\mathcal{B}_2(\psi, x, y) \ll_\varepsilon q^{x\varepsilon} \sum_{\substack{g \in A \text{ squarefree} \\ \deg g < x - 2y}} \#\{\mathfrak{p} \in \mathcal{P}_\psi : \deg \mathfrak{p} = x, g(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\, p) \text{ is a square in } A\}$$

$$=: q^{x\varepsilon} \sum_{\substack{g \in A \text{ squarefree} \\ \deg g < x - 2y}} S_g(\psi).$$

The range of $\deg g$ above is obtained once again using (8):

$$2 \deg h + \deg g \le x \ \Rightarrow\ \deg g \le x - 2 \deg h < x - 2y.$$

To estimate $S_g(\psi)$ we rely on the function field analog of the Square Sieve proved in [6, Section 7] and in Part (vii) of Theorem 15. Specifically, we use the resulting bound

$$S_g(\psi) \ll q^{\frac{7x}{8}} (x + \deg g) + q^{\frac{3x}{4}} x(x + \deg g)^2 \tag{40}$$

(which we will prove shortly) and deduce that

$$\mathcal{B}_2(\psi, x, y) \ll_{\psi,\varepsilon} q^{\frac{15x}{8} - 2y + x\varepsilon} x^3. \tag{41}$$

Now let us prove (40); our arguments use tools from [6, Sections 7, 8] and are included in detail for completeness. We recall the Square Sieve for $A$.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

**Theorem 18.** Let $\mathcal{A}$ be a finite multiset of nonzero elements of $A$. Let $\mathcal{P}$ be a finite set of primes of $A$. Let

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

and for any $a \in A$ define

$$\nu_{\mathcal{P}}(a) := \#\{\ell \in \mathcal{P} : \ell \mid a\}.$$

Then

$$\#S(\mathcal{A}) \leq \frac{\#\mathcal{A}}{\#\mathcal{P}} + \max_{\substack{\ell_1, \ell_2 \in \mathcal{P} \\ \ell_1 \neq \ell_2}} \left| \sum_{a \in \mathcal{A}} \left(\frac{a}{\ell_1}\right)\left(\frac{a}{\ell_2}\right) \right| + \frac{2}{\#\mathcal{P}} \sum_{a \in \mathcal{A}} \nu_{\mathcal{P}}(a) + \frac{1}{(\#\mathcal{P})^2} \sum_{a \in \mathcal{A}} \nu_{\mathcal{P}}(a)^2. \qquad \square$$

We apply Theorem 18 in the setting

$$\mathcal{A} := \{g(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p) : \mathfrak{p} \in \mathcal{P}_{\psi}, \deg \mathfrak{p} = x\}$$

and

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

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

We obtain

$$\begin{aligned} S_g(\psi) \leq \frac{\#\mathcal{A}}{\#\mathcal{P}} &+ \max_{\substack{\ell_1, \ell_2 \in \mathcal{P} \\ \ell_1 \neq \ell_2}} \left| \sum_{\substack{\mathfrak{p} \in \mathcal{P}_{\psi} \\ \deg \mathfrak{p} = x}} \left(\frac{g\left(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p\right)}{\ell_1}\right)\left(\frac{g\left(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p\right)}{\ell_2}\right) \right| \\ &+ \frac{2}{\#\mathcal{P}} \sum_{\substack{\mathfrak{p} \in \mathcal{P}_{\psi} \\ \deg \mathfrak{p} = x}} \nu_{\mathcal{P}}(g(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p)) + \frac{1}{(\#\mathcal{P})^2} \sum_{\substack{\mathfrak{p} \in \mathcal{P}_{\psi} \\ \deg \mathfrak{p} = x}} \nu_{\mathcal{P}}(g(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p))^2. \end{aligned} \tag{42}$$

On one hand, by the Prime Number Theorem for $A$,

$$\frac{\#\mathcal{A}}{\#\mathcal{P}} \asymp q^{x-\theta} \frac{\theta}{x}. \tag{43}$$

On the other hand, by noting that, for any $a \in A$, $\nu_{\mathcal{P}}(a) \leq \deg a$, and by using (8), we deduce that, for primes $\mathfrak{p}$ of degree $x$,

$$\nu_{\mathcal{P}}\left(g\left(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p\right)\right) \leq x + \deg g.$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

We infer the estimates

$$\frac{2}{\#\mathcal{P}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_{\psi}\\ \deg\mathfrak{p}=x}} \nu_{\mathcal{P}}\left(g\left(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\,p\right)\right) \ll q^{x-\theta}\frac{\theta}{x}(x+\deg g), \tag{44}$$

$$\frac{1}{(\#\mathcal{P})} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_{\psi}\\ \deg\mathfrak{p}=x}} \nu_{\mathcal{P}}(g(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\,p))^2 \ll q^{x-2\theta}\frac{\theta^2}{x}(x+\deg g)^2. \tag{45}$$

Now let $\ell_1, \ell_2 \in \mathcal{P}$ be distinct primes such that $(\ell_1\ell_2, M(\psi)) = 1$, where $M(\psi) \in A^{(1)}$ was introduced in Part (iv) of Theorem 15. (Note that, by choosing $x$ sufficiently large, hence, as we shall see, by choosing $\theta(x)$ sufficiently large, we can ensure that this condition holds.) We define

$$T_1 = T_1(\ell_1,\ell_2) := \#\left\{\mathfrak{p}\in\mathcal{P}_{\psi} : \deg\mathfrak{p} = x, \left(\frac{a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\,p}{\ell_1}\right) = \left(\frac{a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\,p}{\ell_2}\right) = 1\right\},$$

$$T_2 = T_2(\ell_1,\ell_2) := \#\left\{\mathfrak{p}\in\mathcal{P}_{\psi} : \deg\mathfrak{p} = x, \left(\frac{a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\,p}{\ell_1}\right) = \left(\frac{a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\,p}{\ell_2}\right) = -1\right\},$$

$$T_3 = T_3(\ell_1,\ell_2) := \#\left\{\mathfrak{p}\in\mathcal{P}_{\psi} : \deg\mathfrak{p} = x, \left(\frac{a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\,p}{\ell_1}\right) = -\left(\frac{a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\,p}{\ell_2}\right) = 1\right\},$$

$$T_4 = T_4(\ell_1,\ell_2) := \#\left\{\mathfrak{p}\in\mathcal{P}_{\psi} : \deg\mathfrak{p} = x, \left(\frac{a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\,p}{\ell_1}\right) = -\left(\frac{a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)\,p}{\ell_2}\right) = -1\right\},$$

and

$$\hat{C}_1 = \hat{C}_1(\ell_1,\ell_2) := \left\{(\hat{g}_1,\hat{g}_2)\in\mathrm{PGL}_2(A/\ell_1\ell_2A) : \left(\frac{(\operatorname{tr} g_1)^2 - 4\det g_1}{\ell_1}\right) = \left(\frac{(\operatorname{tr} g_2)^2 - 4\det g_2}{\ell_2}\right) = 1\right\},$$

$$\hat{C}_2 = \hat{C}_2(\ell_1,\ell_2) := \left\{(\hat{g}_1,\hat{g}_2)\in\mathrm{PGL}_2(A/\ell_1\ell_2A) : \left(\frac{(\operatorname{tr} g_1)^2 - 4\det g_1}{\ell_1}\right) = \left(\frac{(\operatorname{tr} g_2)^2 - 4\det g_2}{\ell_2}\right) = -1\right\},$$

$$\hat{C}_3 = \hat{C}_3(\ell_1,\ell_2) := \left\{\hat{g}_1,\hat{g}_2)\in\mathrm{PGL}_2(A/\ell_1\ell_2A) : \left(\frac{(\operatorname{tr} g_1)^2 - 4\det g_1}{\ell_1}\right) = -\left(\frac{(\operatorname{tr} g_2)^2 - 4\det g_2}{\ell_2}\right) = 1\right\},$$

$$\hat{C}_4 = \hat{C}_4(\ell_1,\ell_2) := \left\{(\hat{g}_1,\hat{g}_2)\in\mathrm{PGL}_2(A/\ell_1\ell_2A) : \left(\frac{(\operatorname{tr} g_1)^2 - 4\det g_1}{\ell_1}\right) = -\left(\frac{(\operatorname{tr} g_2)^2 - 4\det g_2}{\ell_2}\right) = -1\right\},$$

where $\hat{g}$ denotes the projective image of a matrix $g\in\mathrm{GL}_2(A/\ell_1\ell_2A)$.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

On one hand, we have

$$\begin{aligned} S_{\ell_1,\ell_2} &:= \sum_{\substack{\mathfrak{p}\in\mathcal{P}_\psi \\ \deg \mathfrak{p}=x}} \left(\frac{g\left(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p\right)}{\ell_1}\right)\left(\frac{g\left(a_{\mathfrak{p}}(\psi)^2 - 4u_{\mathfrak{p}}(\psi)p\right)}{\ell_2}\right) \\ &= \left(\frac{g}{\ell_1}\right)\left(\frac{g}{\ell_2}\right)(T_1 + T_2 - T_3 - T_4)\,. \end{aligned} \tag{46}$$

On the other hand, by Parts (v) and (vii) of Theorem 15, for each $1 \le i \le 4$ we have

$$T_i = \Pi_{\hat{C}_i}(x, J_{\ell_1\ell_2}/F) = \frac{\#\hat{C}_i}{\#\,\mathrm{PGL}_2(A/\ell_1\ell_2 A)}\cdot\frac{q^x}{x} + \mathrm{O}_\psi((\#\hat{C}_i)^{\frac{1}{2}} q^{\frac{x}{2}} \deg(\ell_1\ell_2)). \tag{47}$$

Easy counting arguments imply that, for any prime $\ell \in A$,

$$\begin{aligned} &\#\,\mathrm{PGL}_2(A/\ell A) = |\ell|_\infty(|\ell|_\infty^2 - 1), \\ &\#\left\{\hat{g}\in \mathrm{PGL}_2(A/\ell A) : \left(\frac{(\mathrm{tr}\, g)^2 - 4\det g}{\ell}\right) = 1\right\} = \frac{|\ell|_\infty^3}{2} + \mathrm{O}(|\ell|_\infty^2), \\ &\#\left\{\hat{g}\in \mathrm{PGL}_2(A/\ell A) : \left(\frac{(\mathrm{tr}\, g)^2 - 4\det g}{\ell}\right) = -1\right\} = \frac{|\ell|_\infty^3}{2} + \mathrm{O}(|\ell|_\infty^2). \end{aligned}$$

Therefore, for each $1 \le i \le 4$,

$$\#\hat{C}_i = \left(\frac{|\ell_1|_\infty^3}{2} + \mathrm{O}(|\ell_1|_\infty^2)\right)\left(\frac{|\ell_2|_\infty^3}{2} + \mathrm{O}(|\ell_2|_\infty^2)\right) = \frac{|\ell_1|_\infty^3|\ell_2|_\infty^3}{4} + \mathrm{O}(|\ell_1|_\infty^2|\ell_2|_\infty^2(|\ell_1|_\infty + |\ell_2|_\infty)),$$

where the O-constants are absolute. Consequently, by (47), for each $1 \le i \le 4$ we have

$$\begin{aligned} T_i = &\frac{|\ell_1|_\infty^2|\ell_2|_\infty^2}{4(|\ell_1|_\infty^2 - 1)(|\ell_2|_\infty^2 - 1)}\cdot\frac{q^x}{x} + \mathrm{O}\left(\frac{|\ell_1|_\infty + |\ell_2|_\infty}{|\ell_1|_\infty|\ell_2|_\infty}\cdot\frac{q^x}{x}\right) \\ &+ \mathrm{O}_\psi\left(|\ell_1|_\infty^{\frac{3}{2}}|\ell_2|_\infty^{\frac{3}{2}}\cdot q^{\frac{x}{2}}\log_q(|\ell_1|_\infty + |\ell_2|_\infty)\right). \end{aligned}$$

By plugging these estimates into (46) and recalling that $|\ell_1|_\infty = |\ell_2|_\infty = q^\theta$, we obtain

$$S_{\ell_1,\ell_2} \ll_\psi \frac{q^{x-\theta}}{x} + q^{\frac{x}{2}+3\theta}\theta. \tag{48}$$

Then, by combining (42) with (43)–(45) and (48), we obtain

$$S_g(\psi) \ll_\psi q^{x-\theta}\frac{\theta}{x}(x + \deg g) + q^{\frac{x}{2}+3\theta}\theta + q^{x-2\theta}\frac{\theta^2}{x}(x + \deg g)^2.$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

We now choose

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

and conclude that

$$S_g(\psi) \ll_\psi q^{\frac{7x}{8}}(x + \deg g) + q^{\frac{3x}{4}} x(x + \deg g)^2,$$

justifying (40).

### 4.2.3 *Conclusion*

By putting together (38), (39), (41), and by choosing

$$y(x) := \frac{11x}{24}$$

for any arbitrary $\varepsilon > 0$, we obtain that

$$\mathcal{B}(\psi, x) = \sum_{m \in A^{(1)}} \frac{\mu_A(m) c_{J_m}(x)}{[J_m : F]} \cdot \frac{q^x}{x} + \mathrm{O}_{\psi,F,\varepsilon}\left(q^{\frac{23x}{24} + x\varepsilon} x^3\right). \tag{49}$$

### 4.2.4 *Dirichlet density*

To determine the Dirichlet density of the set $\{\mathfrak{p} \in \mathcal{P}_\psi : b_\mathfrak{p}(\psi) = 1\}$, we make use of the asymptotic formula (49). In particular, for $s > 1$ (with $s \to 1$), we have

$$\begin{aligned}
\sum_{\substack{\mathfrak{p} \in \mathcal{P}_\psi \\ b_\mathfrak{p}(\psi) = 1}} q^{-s \deg \mathfrak{p}} &= \sum_{x \geq 1} q^{-sx} \mathcal{B}(\psi, x) \\
&= \sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[J_m : F]} \sum_{\substack{x \geq 1 \\ c_{J_m} | x}} \frac{q^{(1-s)x} c_{J_m}}{x} + \mathrm{O}_{\psi,F,\varepsilon}\left(\sum_{x \geq 1} q^{(\frac{23}{24} + \varepsilon - s)x}\right) \\
&= \sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[J_m : F]} \sum_{j \geq 1} \frac{q^{(1-s)jc_{J_m}}}{j} + \mathrm{O}_{\psi,F,\varepsilon}\left(\frac{q^{\frac{23}{24} + \varepsilon - s}}{1 - q^{\frac{23}{24} + \varepsilon - s}}\right) \\
&= -\sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[J_m : F]} \log(1 - q^{(1-s)c_{J_m}}) + \mathrm{O}_{\psi,F,\varepsilon}\left(\frac{q^{\frac{23}{24} + \varepsilon - s}}{1 - q^{\frac{23}{24} + \varepsilon - s}}\right).
\end{aligned}$$

Upon taking the quotient with $-\log(1 - q^{1-s})$ and the limit $s \to 1+$, we obtain $\sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[J_m : F]}$. We include some details for the limit of the first quotient: with $c := c_{J_m}$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

and upon applying l'Hospital, we obtain

$$\lim_{s\to 1+} \frac{\log(1-q^{(1-s)c})}{\log(1-q^{1-s})} = c \lim_{s\to 1+} \frac{q^{(1-s)c}(1-q^{1-s})}{q^{1-s}(1-q^{(1-s)c})}$$

$$= c \lim_{s\to 1+} \frac{q^{(c-1)(1-s)}}{1+q^{2(1-s)}+q^{3(1-s)}+\cdots+q^{(c-1)(1-s)}} = \frac{c}{c} = 1.$$

The limit of the second quotient is 0.

### 4.3 Proof of Part (b) of Theorem 6

With notation (36), we write

$$\begin{aligned}\mathcal{B}(\psi,x) = {}&\#\{\mathfrak{p}\in\mathcal{P}_\psi : \deg\mathfrak{p}=x, \mathfrak{p} \text{ ordinary}, E_{\psi,\mathfrak{p}} = A[\pi_\mathfrak{p}(\psi)]\}\\ &+\#\{\mathfrak{p}\in\mathcal{P}_\psi : \deg\mathfrak{p}=x, \mathfrak{p} \text{ supersingular}, E_{\psi,\mathfrak{p}} = A[\pi_\mathfrak{p}(\psi)]\}\\ =:{}& \mathcal{B}^o(\psi,x)+\mathcal{B}^{ss}(\psi,x).\end{aligned} \tag{50}$$

We will estimate each of the two terms above separately.

#### 4.3.1 *Ordinary primes*

Let $\mathfrak{p}\in\mathcal{P}_\psi$ be an ordinary prime for $\psi$. First of all,

$$\mathrm{End}_{\bar{F}}(\psi)\otimes_A F \subseteq \bar{E}_{\psi,\mathfrak{p}}\otimes_A F,$$

so using, the assumptions that $\mathfrak{p}$ is ordinary and that $\mathrm{End}_{\bar{F}}(\psi)$ is a maximal order in $K$, we deduce that

$$E_{\psi,\mathfrak{p}} \simeq \mathcal{O}_{\psi,\mathfrak{p}} \simeq \bar{E}_{\psi,\mathfrak{p}} \simeq \mathrm{End}_{\bar{F}}(\psi). \tag{51}$$

In particular, the discriminant $\Delta$ of $\mathrm{End}_{\bar{F}}(\psi)$ equals $\Delta(E_{\psi,\mathfrak{p}})$ and so, by (15), there exists $\delta\in A$, independent of $\mathfrak{p}$, such that

$$\Delta = \delta A$$

and

$$a_\mathfrak{p}(\psi)^2 - 4u_\mathfrak{p}(\psi)p = b_\mathfrak{p}(\psi)^2\delta.$$

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

Consequently,

$$b_{\mathfrak{p}}(\psi)=1 \;\Leftrightarrow\; u_{\mathfrak{p}}(\psi)p=\left(\frac{a_{\mathfrak{p}}(\psi)}{2}\right)^2-\frac{\delta}{4}. \tag{52}$$

Recalling (8) and using Part (i) of Lemma 12, we deduce that there are at most $\mathrm{O}(q^{\frac{x}{2}})$ possible $a_{\mathfrak{p}}(\psi)\in A$. Also, there are at most $q-1$ possible choices of $\delta$. Thus, by (52),

$$\mathcal{B}^{o}(\psi,x)\ll q^{\frac{x}{2}}. \tag{53}$$

### 4.3.2 *Supersingular primes*

Let $\mathfrak{p}\in\mathcal{P}_{\psi}$ be a supersingular prime for $\psi$. In other words,

$$a_{\mathfrak{p}}(\psi)=0 \tag{54}$$

(cf. [38, Proposition 4]). By using this in (15), we deduce that $-4u_{\mathfrak{p}}(\psi)p=b_{\mathfrak{p}}(\psi)^2\delta_{\mathfrak{p}}(\psi)$, which implies $b_{\mathfrak{p}}(\psi)=1$.

Under the assumption $\mathrm{End}_{\bar{F}}(\psi)\otimes_A F\simeq K$, we also have that any supersingular prime $\mathfrak{p}$ for $\psi$ is either ramified or inert in $K$. Indeed, $K\otimes_F F_{\mathfrak{p}}$ is a subalgebra of $\bar{E}_{\psi,\mathfrak{p}}\otimes_A F_{\mathfrak{p}}$. But if $\mathfrak{p}$ is a prime of supersingular reduction, then $\bar{E}_{\psi,\mathfrak{p}}\otimes_A F_{\mathfrak{p}}$ is the division quaternion algebra over $F_{\mathfrak{p}}$. This implies that $K\otimes_F F_{\mathfrak{p}}$ is a field, which itself implies that $\mathfrak{p}$ does not split in $K$. Combining this with the Chebotarev Density Theorem for $K$, we deduce that

$$\mathcal{B}^{ss}(\psi,x)=\frac{c_K(x)}{2}\cdot\frac{q^x}{x}+\mathrm{O}_K(q^{\frac{x}{2}}). \tag{55}$$

By putting together (50), (53) and (55), and by a similar calculation as in Section 4.2.4, we complete the proof of Part (b) of Theorem 6.

## 4.4 **Remarks**

(i) A natural question to ask is whether the Dirichlet density in Part (a) of Theorem 6 is positive. This question is related to a good understanding of the constant $M(\psi)$ introduced in Part (iv) of Theorem 15, and, in particular, to an understanding of effective versions of the Open Image Theorems for Drinfeld modules proved by Pink and Rütsche [32]. We point out that, unlike the situation for elliptic curves (cf. [5], where any elliptic

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

curve over $\mathbb{Q}$ with rational 2-torsion gives rise to a zero density of reductions with small endomorphism rings), there is no immediate obstruction for a Drinfeld module $\psi$ to have a positive Dirichlet density for $\{\mathfrak{p} \in \mathcal{P}_\psi : \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p}) = A[\pi_\mathfrak{p}(\psi)]\}$. In [40], Zywina gives an example of a rank-2 Drinfeld $\mathbb{F}_q[T]$-module $\psi$ over $\mathbb{F}_q(T)$ for which the residual representations $\bar{\rho}_{\psi,a}$ are surjective for all $a \in A$ and for which $\bar{\mathbb{F}}_q \cap F(\psi[a]) = \mathbb{F}_q$ for all $a \in A$. It is easy to see that for this particular $\psi$ the Dirichlet density in question is indeed nonzero.

(ii) As already emphasized in Corollary 3, the condition $b_\mathfrak{p}(\psi) = 1$ implies that ${}^{\psi}\mathbb{F}_\mathfrak{p}$ is $A$-cyclic. The reductions of $\psi$ giving rise to a cyclic $A$-module have been studied in several works, for example, [8, 20, 21, 23]. An outcome of Part (b) of Theorem 6 is that, for any rank 2 Drinfeld module $\psi$ whose endomorphism ring is the integral closure of $A$ in a quadratic imaginary extension of $F$, there is a density $\geq 0.5$ of primes which give rise to reductions of $\psi$ with $A$-cyclic structures. This is to be contrasted with the situation for elliptic curves (see [7]), where such a result is not true: there exist CM elliptic curves over $\mathbb{Q}$ (in fact, any CM curve with a rational 2-torsion) which have no reductions with cyclic structures; moreover, for CM elliptic curves over $\mathbb{Q}$ with no rational 2-torsion one cannot always ensure a density of $\geq 0.5$ of cyclic reductions.

## 5 CM-Liftings of Drinfeld Modules

### 5.1 CM-liftings of abelian varieties

To motivate the discussion and definitions in the setting of Drinfeld modules in Section 5.2, we first recall what is known about CM-liftings of abelian varieties.

Let $B$ be an abelian variety of dimension $g$ defined over a field $K$. Following [30, Definition 1.7], we say that $B$ has *sufficiently many complex multiplications* (or is *CM*, for short) if $\mathrm{End}^0_K(B) := \mathrm{End}_K(B) \otimes_\mathbb{Z} \mathbb{Q}$ contains a commutative semi-simple algebra $L$ of dimension $2g$ over $\mathbb{Q}$. If $B$ is simple, then $L$ is necessarily a CM field, that is, a totally imaginary quadratic extension of a totally real field.

Let $B_0$ be an abelian variety over a field $k$ of characteristic $p$. We say that $B$ is a *CM-lifting* of $B_0$ if there exists a normal domain $R$ with fraction field $K$ of characteristic zero, a ring homomorphism $R \to k$, and an abelian scheme $\mathcal{B}$ over $R$ such that $\mathcal{B} \otimes_R k \cong B_0$ and $B = \mathcal{B} \otimes_R K$ is CM.

The earliest result about CM-liftings is a well-known theorem of Deuring.

**Theorem 19.** Let $E_0$ be an elliptic curve over a finite field $k$. For any $f_0 \in \mathrm{End}_k(E_0)$ generating an imaginary quadratic field $L \subset \mathrm{End}^0_k(E_0)$, there is an elliptic curve $E$ over the ring

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

of integers $R$ of a finite extension of $\mathbb{Q}_p$ equipped with an endomorphism $f \in \mathrm{End}_K(E)$ such that $(E, f)$ has special fibre isomorphic to $(E_0, f_0)$. □

**Proof.** See Theorem 1.7.4.6 in [4]. ■

Next, as part of his proof that Tate's map from the isogeny classes of abelian varieties over a finite field to the Galois conjugacy classes of Weil numbers is surjective, Honda proved the following theorem.

**Theorem 20.** Given an abelian variety $B_0$ over a finite field $k$, there exists a finite extension $k \subset k'$ and an isogeny $B_0 \otimes_k k' \to C_0$ defined over $k'$ such that $C_0$ has CM-lifting. □

Finally, in the recent monograph [4] the authors show that both the isogeny and the field extension in the previous theorem are necessary for the existence of CM-liftings.

**Theorem 21.**

(a) For any $g \geq 3$, there exists an abelian variety over $\bar{\mathbb{F}}_p$ of dimension $g$ which does not admit CM-liftings. Hence the isogeny in Honda's theorem is necessary.

(b) There exists an abelian variety $B_0$ over a finite field $k$ such that any $C_0$ isogenous to $B_0$ over $k$ does not admit a CM-lifting. Hence the field extension $k'/k$ in Honda's theorem is necessary. □

### 5.2 CM-liftings of Drinfeld modules

As at the beginning of Section 1, let $F$ be the function field of a smooth, projective, geometrically irreducible curve over $\mathbb{F}_q$. Fix a place $\infty$ of $F$, and let $A$ be the subring of $F$ consisting of functions which are regular away from $\infty$.

Let $R$ be a discrete valuation ring with maximal ideal $\mathfrak{m}$ and field of fractions $K$. Assume $K$ is equipped with an injective homomorphism $\gamma : A \to K$, so the $A$-characteristic of $K$ is 0. A *Drinfeld $A$-module over $R$* of rank $r$ is an embedding $\psi : A \to R\{\tau\}$ which is a Drinfeld module over $K$ of rank $r$, as defined in Section 1, and such that the composite homomorphism $\overline{\psi} : A \to R\{\tau\} \to (R/\mathfrak{m})\{\tau\}$ is a Drinfeld module over $R/\mathfrak{m}$, again of rank $r$; cf. [19, Definition 7.1]. We say that $\psi$ has *CM* if $\mathrm{End}_K(\psi) \otimes_A F$ is a field extension $L$ of $F$ of degree $r$. (Note that $L$ is imaginary.)

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

Let $k$ be a finite field with $A$-characteristic $\mathfrak{p}$. Let $\psi_0$ be a Drinfeld $A$-module over $k$. We say that $\psi_0$ has a *CM-lifting* if there exists a discrete valuation ring $R$ with residue field $k$, and a CM Drinfeld module $\psi$ over $R$ such that $\bar{\psi}$ is isomorphic to $\psi_0$ over $k$.

Let $q^n$ be the cardinality of $k$. Let $\psi_0$ be a rank-$r$ Drinfeld $A$-module over $k$. Denote $E=\mathrm{End}_k(\psi_0)$ and $D=E\otimes_A F$. It is clear that $\pi:=\tau^n\in E$. Let $\tilde{F}:=F(\pi)\subseteq D$. The following is known about $D$ and $\tilde{F}$ (see [38, Theorem 1]):

- The degree of $\tilde{F}$ over $F$ divides $r$. Let $t:=r/[\tilde{F}:F]$.
- There is a unique place $\mathfrak{P}$ of $\tilde{F}$ which is a zero of $\pi$ and there is a unique place $\infty_{\tilde{F}}$ of $\tilde{F}$ which is a pole of $\pi$. Furthermore, $\mathfrak{P}$ lies over $\mathfrak{p}$, and $\infty_{\tilde{F}}$ is the unique place lying over $\infty$.
- $D$ is a central division algebra over $\tilde{F}$ of dimension $t^2$ with invariants

$$\mathrm{inv}_v(D)=\begin{cases}1/t & \text{if } v=\mathfrak{P},\\ -1/t & \text{if } v=\infty_{\tilde{F}},\\ 0 & \text{otherwise.}\end{cases}$$

By [33, Theorem 7.15], the maximal subfields of $D$ are those which have degree $r$ over $F$, and any such field contains $\tilde{F}$. Let $L$ be a maximal subfield of $D$. Denote by $A_L$ be the integral closure of $A$ in $L$ and put $\mathcal{A}=E\cap L$. We say that $L$ is *good* for $\psi_0$ if the conductor $\mathfrak{c}$ of $\mathcal{A}$ as an $A$-order in $A_L$ is coprime to $\mathfrak{p}$.

**Theorem 22.** If $L$ is good for $\psi_0$, then the Drinfeld module $\psi_0$ has a CM-lifting $\psi$ such that $\mathrm{End}_K(\psi)\otimes_A F=L$. □

**Proof.** We can consider $\psi_0$ as an elliptic $\mathcal{A}$-module of rank 1 defined over $k$:

$$\psi_0':\mathcal{A}\to k\{\tau\}.$$

The restriction of $\psi_0'$ to $A$ is the original module $\psi_0$. By [16, Proposition 4.7.19] or [19, Proposition 3.2], there is a Drinfeld $A_L$-module $\phi_0'$ of rank 1 over $k$, whose restriction to $\mathcal{A}$ is isogenous to $\psi_0'$ over $k$. Restricting $\phi_0'$ to $A$ we get a Drinfeld $A$-module $\phi_0$ of rank $r$. The fact that $\phi_0'$ and $\psi_0'$ are isogenous implies that there is an isogeny $i:\phi_0\to\psi_0$ over $k$. Moreover, since by assumption $\mathfrak{c}$ is coprime to $\mathfrak{p}$, we can choose $i$ so that the group-scheme $\ker(i)$ has trivial intersection with $\phi_0[\mathfrak{p}]$; cf. the proof of Proposition 4.7.19 in [16]. Now the deformation theory of Drinfeld modules implies that $\phi_0'$ lifts to a rank-1 Drinfeld $A_L$-module $\phi'$ over a discrete valuation ring $R$ whose field of fractions has zero $A$-characteristic; see [26, Section 3.1]. Restricting $\phi'$ to $A$ we get a rank-$r$ Drinfeld $A$-module

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

$\phi$ over $K$ with CM by $L$, whose reduction is $\phi_0$. Since $\ker(i)$ is étale, [26, Corollary 2.3 on p. 42] implies that the kernel of $i$ lifts to an $\mathcal{A}$-invariant submodule $H \subset {}^{\phi}K^{\mathrm{sep}}$ which is also invariant under $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. (Note that $H$ is not necessarily $A_L$-invariant.) By [16, Proposition 4.7.11], there is an isogeny $\phi \to \psi$ defined over $K$ whose kernel is $H$. It is easy to see that $\mathcal{A} \subset \mathrm{End}_K(\psi)$, and the reduction of $\psi$ is $\psi_0$, so $\psi$ is the desired CM-lifting of $\psi_0$. ■

**Corollary 23.** Any Drinfeld module $\psi_0$ is isogenous over $k$ to some Drinfeld module $\phi_0$ having a CM-lifting. □

**Proof.** This is clear from the proof of Theorem 22. ■

**Proposition 24.** In the following cases any maximal subfield $L$ is good:

(1) $\psi_0$ is supersingular.

(2) $r = 2$. □

**Proof.** Note that $\mathfrak{P}$ does not split in the extension $L/\tilde{F}$. By Corollary to Theorem 1 in [38], $\mathcal{A}_{\mathfrak{P}}$ is a maximal $A_{\mathfrak{p}}$ order, so the conductor $\mathfrak{c}$ is coprime to $\mathfrak{P}$. The Drinfeld module $\psi_0$ is supersingular if and only if $\mathfrak{P}$ is the only place of $\tilde{F}$ over $\mathfrak{p}$; see [25, (2.5.8)]. These two facts imply the first claim. Now assume $r = 2$. Then either $\psi_0$ is supersingular or $\tilde{F}$ is a separable quadratic extension of $F$ and $\mathfrak{p} = \mathfrak{P}\bar{\mathfrak{P}}$ splits in $\tilde{F}$. In the second case $L = \tilde{F}$, and if $f(x) = x^2 - ax + b = 0$ is the minimal polynomial of $\pi$ over $F$, then $a \notin \mathfrak{p}$. Note that $f'(\pi) = 2\pi - a = \pi - \bar{\pi}$ is divisible neither by $\mathfrak{P}$ nor $\bar{\mathfrak{P}}$, so $A[\pi]$ is maximal at $\mathfrak{p}$; the same then is true for $E = \mathcal{A}$. ■

By the previous proposition, if $r = 2$, then any $L$ is good. Since any $f_0 \in E$, which is not in $A$, generates a maximal subfield, we conclude that $(\psi_0, f_0)$ has a CM-lifting, in direct analogy with Deuring's Theorem 19. This proves Theorem 7 in Section 1.

## Funding

A.C.C.'s work on this material was partially supported by the National Science Foundation under agreements No. DMS-0747724 and No. DMS-0635607, and by the European Research Council under Starting Grant 258713. M.P. was supported in part by the Simons Foundation.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

**Acknowledgements**

The authors thank the Institute of Mathematics at the University of Göttingen for hosting them in the summer of 2012, while some of this research was carried out. They also thank their funding agencies (European Research Council, National Science Foundation, and Simons Foundation) and the University of Illinois at Chicago for providing them with research funds that enabled their collaboration. They thank Florian Breuer, Chris Hall and Lenny Taelman for useful conversations on material related to Theorem 5. Finally, they thank the anonymous referees for carefully reading the paper and providing them with numerous useful comments.

## References

[1] Abhyankar, S. "Nice equations for nice groups." *Israel Journal of Mathematics* 88, no. 1–3 (1994): 1–23.

[2] Abhyankar, S. "Resolution of singularities and modular Galois theory." *Bulletin of the American Mathematical Society (N.S.)* 38, no. 2 (2001): 131–69.

[3] Brown, M. "Singular moduli and supersingular moduli of Drinfeld modules." *Inventiones Mathematicae* 110, no. 2 (1992): 419–39.

[4] Chai, C.-L., B. Conrad, and F. Oort. *Complex Multiplication and Lifting Problems*. Mathematical Surveys and Monographs 195. Providence, RI: American Mathematical Society, 2014.

[5] Cojocaru, A. C. and W. Duke. "Reductions of an elliptic curve and their Tate–Shafarevich groups." *Mathematische Annalen* 329, no. 3 (2004): 513–34.

[6] Cojocaru, A. C. and C. David. "Frobenius fields for Drinfeld modules of rank 2." *Compositio Mathematica* 144, no. 4 (2008): 827–48.

[7] Cojocaru, A. C. and R. Murty. "Cyclicity of elliptic curves modulo $p$ and elliptic curve analogues of Linnik's problem." *Mathematische Annalen* 330, no. 3 (2004): 601–25.

[8] Cojocaru, A. C. and A. Shulman. "Elementary divisors of Drinfeld modules of arbitrary rank." (2013): preprint. arXiv:1304.2100.

[9] David, C. "Supersingular reduction of Drinfeld modules." *Duke Mathematical Journal* 78, no. 2 (1995): 399–412.

[10] David, C. "Frobenius distributions of Drinfeld modules of any rank." *J. Number Theory* 90, no. 2 (2001): 329–40.

[11] Drinfeld, V. "Elliptic modules." *Matematicheskii Sbornik (N.S.)* 94, no. 4 (1974): 594–627.

[12] Duke, W. and Á. Tóth. "The splitting of primes in division fields of elliptic curves." *Experimental Mathematics* 11, no. 4 (2002): 555–65.

[13] Gardeyn, F. "Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld." *Archiv der Mathematik (Basel)* 79, no. 4 (2002): 241–51.

[14] Gekeler, E.-U. "On finite Drinfeld modules." *Journal of Algebra* 141, no. 1 (1991): 187–203.

[15] Gekeler, E.-U. "Frobenius distributions of Drinfeld modules over finite fields." *Transactions of the American Mathematical Society* 360, no. 4 (2008): 1695–721.

[16] Goss, D. *Basic Structures of Function Field Arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 35. Berlin: Springer, 1996.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

[17] Hardy, G. H. and E. M. Wright. *An Introduction to the Theory of Numbers*, 6th ed. Oxford: Oxford University Press, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[18] Hayes, D. "Explicit class field theory for rational function fields." *Transactions of the American Mathematical Society* 189 (1974): 77–91.

[19] Hayes, D. *Explicit Class Field Theory in Global Function Fields*, 173–217. Studies in algebra and number theory, Adv. in Math. Suppl. Stud. 6. New York: Academic Press, 1979.

[20] Hsu, C.-N. "On Artin's conjecture for the Carlitz module." *Compositio Mathematica* 106, no. 3 (1997): 247–66.

[21] Hsia, L.-C. and J. Yu. "On characteristic polynomials of geometric Frobenius associated to Drinfeld modules." *Compositio Mathematica* 122, no. 3 (2000): 261–80.

[22] Huppert, B. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Berlin, New York: Springer, 1967.

[23] Kuo, W. and Y.-R. Liu. "Cyclicity of finite Drinfeld modules." *Journal of the London Mathematical Society* (2) 80, no. 3 (2009): 567–84.

[24] Lang, S. *Algebra*, 3rd ed., Advanced Book Program. Reading, MA: Addison-Wesley Publishing Company, 1993.

[25] Laumon, G. *Cohomology of Drinfeld Modular Varieties. Part I.* Cambridge Studies in Advanced Mathematics 41. Cambridge: Cambridge University Press, 1996, Geometry, counting of points and local harmonic analysis.

[26] Lehmkuhl, T. "Compactification of the Drinfeld modular surfaces." *Memoirs of the American Mathematical Society* 197, no. 921 (2009): xii+94.

[27] Litoff, O. "On the commutator subgroup of the general linear group." *Proceedings of the American Mathematical Society* 6, no. 3 (1955): 465–70.

[28] Murty, R., K. Murty, and N. Saradha. "Modular forms and the Chebotarev density theorem." *American Journal of Mathematics* 110, no. 2 (1988): 253–81.

[29] Murty, K. and J. Scherk. "Effective versions of the Chebotarev density theorem for function fields." *Comptes Rendus de l'Académie des Sciences - Series I - Mathematics* 319, no. 6 (1994): 523–8.

[30] Oort, F. "CM-liftings of abelian varieties." *Journal of Algebraic Geometry* 1, no. 1 (1992): 131–46.

[31] Poonen, B. "Drinfeld modules with no supersingular primes." *International Mathematics Research Notices* 1998, no. 3 (1998): 151–9.

[32] Pink, R. and E. Rütsche. "Adelic openness for Drinfeld modules in generic characteristic." *Journal of Number Theory* 129, no. 4 (2009): 882–907.

[33] Reiner, I. *Maximal Orders*. London Mathematical Society Monographs. New Series 28. Oxford: The Clarendon Press Oxford University Press, 2003, Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[34] Serre, J.-P. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." *Inventiones Mathematicae* 15, no. 4 (1972): 259–331.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016

[35] Shimura, G. “A reciprocity law in non-solvable extensions.” *Journal fr̈ die Reine und Angewandte Mathematik* 221 (1966): 209–20.

[36] Takahashi, T. “Good reduction of elliptic modules.” *Journal of the Mathematical Society of Japan* 34, no. 3 (1982): 475–87.

[37] van der Heiden, G.-J. “Weil pairing for Drinfeld modules.” *Monatshefte fr Mathematik* 143, no. 2 (2004): 115–43.

[38] Yu, J.-K. “Isogenies of Drinfeld modules over finite fields.” *Journal of Number Theory* 54, no. 1 (1995): 161–71.

[39] Yu, J.-K. “A Sato–Tate law for Drinfeld modules.” *Compositio Mathematica* 138, no. 2 (2003): 189–97.

[40] Zywina, D. “Drinfeld modules with maximal Galois action on their torsion points.” (2011): preprint. arXiv:1110.4365.

[41] Zywina, D. “The Sato-Tate law for Drinfeld modules.” (2011): preprint. arXiv:1110.4098.

Downloaded from http://imrn.oxfordjournals.org/ at Pennsylvania State University on February 7, 2016