DRINFEld MODULES, FROBENIUS ENDOMORPHISMS, AND CM-LIFTINGS

ALINA CARMEN COJOCARU and MIHRAN PAPIKIAN

Abstract. 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 non-solvable polynomials, and to study the frequency with which the reductions of Drinfeld modules have small endomorphism rings. We also prove CM-lifting theorems for Drinfeld modules.

1. Introduction

Given a finite Galois extension $L/K$ of global fields and a conjugacy class $C \subseteq \text{Gal}(L/K)$, a fundamental problem is that of describing the (unramified) primes $p$ of $K$ for which the conjugacy class of the Frobenius at $p$ 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, $\text{Gal}(\mathbb{Q}(\zeta_a)) \simeq (\mathbb{Z}/a\mathbb{Z})^\times$, and so for any rational 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 $p \equiv 1(\text{mod } a)$. A similar result was proven by Hayes [Hay79] 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. [Shi66] and [DT02]). 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 elements of $F$ which have only $\infty$ as a pole. Let $K$ be a field equipped with a homomorphism $\gamma : A \rightarrow K$. If $\gamma$ is injective, we say that $K$ has $A$-characteristic 0; if $\ker(\gamma) = p \triangleleft A$ is a non-zero (prime) ideal, then

A.C. Cojocaru’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. Papikian was supported in part by the Simons Foundation.
we say that \( K \) has \textbf{\( A \)-characteristic} \( p \). Note that \( K \) contains \( \mathbb{F}_q \) as a subfield. Let \( \tau \) be the Frobenius endomorphism of \( K \) relative to \( \mathbb{F}_q \), i.e., the map \( x \mapsto x^q \), and let \( K\{\tau\} \) be the non-commutative ring of polynomials in the indeterminate \( \tau \) with coefficients in \( K \) and the commutation rule \( \tau c = c^q \tau \) for any \( c \in K \).

\textbf{A Drinfeld \( A \)-module over} \( K \) is a ring homomorphism
\[
\psi : A \to K\{\tau\}
\]
whose image is not contained in \( K \). One shows that there is an integer \( r \geq 1 \), called the \textbf{rank of} \( \psi \), such that \( n_a = -r \deg(\infty) \ord_\infty(a) \) for all \( a \in A \); see [Dri74].

The \textbf{ring of \( K \)-endomorphisms} of \( \psi \), \( \text{End}_K(\psi) \), 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 \( \text{End}_K(\psi) \) is a projective \( A \)-module of rank \( \leq r^2 \) with the property that \( D := \text{End}_K(\psi) \otimes_A F \) is a division algebra over \( F \) such that \( D \otimes_F F_\infty \) is also a division algebra. Moreover, if \( K \) has \( A \)-characteristic 0, then \( D \) is a field extension of \( F \) of degree \( \leq r \); see [Dri74].

In this last case, the place \( \infty \) does not split in the extension \( D/F \). We call a finite field extension \( F' \) of \( F \) \textbf{imaginary} if \( \infty \) does not split in \( F' \).

The Drinfeld module \( \psi \) endows the algebraic closure \( \overline{K} \) of \( K \) with an \( A \)-module structure, where \( a \in A \) acts by \( \psi_a \). We shall write \( \overline{\psi} \overline{K} \) if we wish to emphasize this action. The \textbf{\( a \)-torsion} \( \psi[a] \subset \overline{K} \) of \( \psi \) is the kernel of \( \psi_a \), i.e., the set of zeros of the polynomial \( \psi_a(x) := \gamma(a)x + \sum_{i=1}^{n_a} \alpha_i x^q^i \in K[x] \). The field \( K(\psi[a]) \), obtained by adjoining the elements of \( \psi[a] \) to \( K \), is called the \textbf{\( a \)-th 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 non-zero. Then \( \psi[a] \simeq_A (A/aA)^{\oplus r} \) and the action of \( G_K := \text{Gal}(K^{\text{sep}}/K) \) on \( \psi[a] \) gives rise to a Galois representation
\[
\rho_{\psi,a} : G_K \to \text{GL}_r(A/aA).
\]

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 [Dri74], [Hay79]).

In this paper we primarily deal with the case \( r = 2 \), \( A = \mathbb{F}_q[T] \), which, in many 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 \( \psi \). This result has several interesting applications, including a criterion for the splitting modulo primes of a class of non-solvable 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 \textbf{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 conjecture. Finally, the third goal of the paper is to prove \textbf{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 \( \mathfrak{p} = pA \) be a prime of good reduction for \( \psi \) (in the sense of [Tak82]), where \( p \in A \) is monic and irreducible. Then there exist uniquely determined polynomials \( a_p(\psi), b_p(\psi), \delta_p(\psi) \in A \) such that, for any \( a \in A \) coprime to \( p \), the reduction modulo \( a \) of the matrix

\[
\begin{pmatrix}
-\frac{a_p(\psi)}{2} & \frac{\delta_p(\psi)b_p(\psi)}{2} \\
\frac{b_p(\psi)}{2} & -\frac{a_p(\psi)}{2}
\end{pmatrix} \in M_2(A)
\]

represents the class of the image under \( \bar{\rho}_{\psi,a} \) of the Frobenius at \( \mathfrak{p} \) in the \( a \)-division field \( F(\psi[a]) \) of \( \psi \). Here, \( a_p(\psi), b_p(\psi), \delta_p(\psi) \) are as follows:

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

\[
P_{\psi,p}(x) = x^2 + a_p(\psi)x + u_p(\psi)p \in A[x],
\]

where \( u_p(\psi) \in \mathbb{F}_q^\times \);

(b) \( b_p(\psi) \) is the unique monic polynomial such that, for any root \( \pi_p(\psi) \) of \( P_{\psi,p} \),

\[
\mathrm{End}_{\mathfrak{p}_p}(\psi \otimes \mathbb{F}_p)/A[\pi_p(\psi)] \simeq_A A/b_p(\psi)A,
\]

where \( \mathbb{F}_p \) is the residue field of \( \mathfrak{p} \) and \( \psi \otimes \mathbb{F}_p : A \to \mathbb{F}_p\{\tau\} \) is the reduction of \( \psi \) modulo \( \mathfrak{p} \);

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

\[
a_p(\psi)^2 - 4u_p(\psi)p = b_p(\psi)^2\delta_p(\psi).
\]

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:

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

\[
a_p(\psi) \equiv -2 \pmod{a}
\]

and

\[
b_p(\psi) \equiv 0 \pmod{a}.
\]

Moreover, we deduce the \( A \)-module structure of \( \mathbb{F}_p \) defined by the reduction \( \psi \otimes \mathbb{F}_p \):

**Corollary 3.** In the setting of Theorem 1, the \( A \)-module structure \( \psi \mathbb{F}_p \) is given explicitly by

\[
\psi \mathbb{F}_p \simeq_A A/d_{1,p}(\psi)A \times A/d_{2,p}(\psi)A,
\]

where

\[
d_{1,p}(\psi) = \gcd\left(\frac{b_p(\psi)}{2}, \frac{a_p(\psi)}{2} - 1\right) \in A,
\]

\[
d_{2,p}(\psi) = \frac{1 + a_p(\psi) + u_p(\psi)p}{d_{1,p}(\psi)} \in A.
\]
In particular, if \( b_p(\psi) \in \mathbb{F}_q^\times \), then \( \psi \mathbb{F}_p \) is \( A \)-cyclic.

Another application of Theorem 1 is a “reciprocity law” for splitting of certain non-solvable polynomials in the style of Klein’s approach to non-solvable 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 \( \alpha, \beta \)). Polynomials similar to \( f_\psi(x) \) below were extensively studied by Abhyankar in connection with the problem of resolution of singularities in positive characteristic; cf. [Abh94], [Abh01]; for that reason we call them Abhyankar trinomials.

**Theorem 4.** In the setting of Theorem 1, let \( \psi : A \rightarrow F\{\tau\} \) be a Drinfeld \( A \)-module over \( F \), of rank 2, defined by \( \psi_T = T + g_1 \tau + g_2 \tau^2 \). Consider the polynomial

\[
\psi(x) := T + g_1 x + g_2 x^{q+1} \in F[x].
\]

Then:

(a) for any prime \( p = pA \neq T \) of good reduction for \( \psi \), with \( p \) monic, \( \psi \) splits completely modulo \( p \) only if \( p = u\alpha^2 + T^2 \beta \) for some \( \alpha, \beta \in A \) and \( u \in \mathbb{F}_q^\times \);

(b) if \( q \geq 5 \), \( g_1 = 1 \) and either \( g_2 \in \mathbb{F}_q^\times \) or \( g_2 = h\tau^{-1} \) for some non-constant \( h \in A \) not divisible by any prime of degree 1 except possibly \( T \), then the Galois group of \( \psi \) over \( F \) is isomorphic to \( \text{PGL}_2(\mathbb{F}_q) \), and, in particular, is non-solvable. Moreover, the set of primes \( \{p : b_p(\psi) \equiv 0 \pmod{T}\} \) has positive Dirichlet density \( \frac{1}{\varphi(q^2-1)} \).

In the above results, the invariants \( a_p(\psi), b_p(\psi), \delta_p(\psi) \) 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. [Bro92], [CD08], [Dav95], [Dav01], [Gek08], [HY00], [Poo98], [Yu03], [Zyw11b]). In this paper we study the second invariant, \( b_p(\psi) \), and prove:

**Theorem 5.** Let the setting and notation be as in Theorem 1.

(a) If \( \text{End}_F(\psi) = A \), then, for \( x \in \mathbb{N} \) going to infinity, we have the asymptotic formula

\[
\# \left\{ p \in \mathcal{P}_\psi : \text{deg} \, p = x, \text{End}_F(\psi \otimes \mathbb{F}_p) = A[\pi_p(\psi)] \right\} \sim \sum_{\substack{m \in A \\ \text{monic}}} \frac{\mu_A(m) c_{J_m}(x)}{[J_m : F]} \frac{q^x}{x},
\]

where \( \mathcal{P}_\psi \) is the set of primes of good reduction of \( \psi \), \( \mu_A(\cdot) \) denotes the Möbius function on \( A \), \( J_m \) is the subfield of \( F(\psi[m]) \) fixed by the scalars, \( c_{J_m} := [J_m \cap \mathbb{F}_q : \mathbb{F}_q] \), and

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

Moreover, the Dirichlet density of the set \( \{ p \in \mathcal{P}_\psi : \text{End}_F(\psi \otimes \mathbb{F}_p) = A[\pi_p(\psi)] \} \) exists and equals

\[
\sum_{\substack{m \in A \\ \text{monic}}} \frac{\mu_A(m)}{[J_m : F]}.
\]
If $\text{End}_{\mathbb{F}_q}(\psi)$ 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

$$\# \{ p \in \mathcal{P}_\psi : \deg p = x, \text{End}_{\mathbb{F}_q}(\psi \otimes \mathbb{F}_p) = A[\pi_p(\psi)] \} \sim \frac{c_K(x)}{2} \cdot \frac{q^x}{x},$$

(3)

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

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

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

Theorem 1 is the function field analogue of Theorem 2.1 in [DT02]. 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 6.** Let $A$ be arbitrary and $k$ a finite field with $A$-characteristic $p$. Let $\phi$ be a Drinfeld $A$-module of rank 2 defined over $k$. Let $g \in \text{End}_k(\phi) \backslash A$. There exists 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 $f \in \text{End}_K(\psi)$, 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 6 follows. The proofs of our main results are based on both algebraic and analytic techniques. In particular, the proof of Theorem 5 is based on sieve methods such as the less standard Square Sieve, and, implicitly, also on effective versions of the Chebotarev Density Theorem.

2. **Global description of the Frobenius: Proof of Theorem 1**

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

- $A^{(1)}$ denotes the set of monic polynomials in $A$.
- For $0 \neq a \in A$, let $\deg(a)$ be the degree of $a$ as a polynomial in $T$ and put $\deg(0) := -\infty$.
- For $f = \frac{a}{b} \in F = \mathbb{F}_q(T)$, let $\deg(f) := \deg(a) - \deg(b)$. This defines a valuation on $F$ with normalized norm $|f|_\infty := q^{\deg(f)}$; the corresponding place of $F$ is $\infty$.
- For a non-zero prime ideal $p \subset A$, $\mathbb{F}_p := A/p$, $\deg(p) := \left[ \mathbb{F}_p : \mathbb{F}_q \right]$ and $|p|_\infty := q^{\deg p}$.

Let $\psi : A \to F\{\tau\}$ be a fixed Drinfeld $A$-module of rank 2 defined by

$$\psi_T = T + g_1 \tau + g_2 \tau^2.$$
Let \( I = \ell A \subset A \) be a prime ideal with generator \( \ell \in A \). For an integer \( n \geq 1 \), we define \( \psi[I^n] := \psi[\ell^n] \). (It is easy to see that this does not depend on the choice of \( \ell \).) For \( n' \geq n \) we have the inclusion \( \psi[I^n] \subseteq \psi[I^{n'}] \), which is compatible with the \( A \)-module structure and the action of \( GF \). Hence
\[
\psi[I^n] := \lim_{n \to \infty} \psi[I^n] \cong (F_1/A_1)^{\oplus 2},
\]
where \( F_1 \) and \( A_1 \) are the completions of \( F \) and \( A \) at \( I \), respectively. The \( l \)-adic Tate module of \( \psi \), defined as
\[
\mathcal{T}_I(\psi) := \text{Hom}_{A_1}(F_1/A_1, \psi[I^\infty]) \cong A_1^{\oplus 2},
\]
is endowed with a continuous action of \( GF \), giving rise to a representation
\[
\rho_{\psi, I}: GF \to GL_2(A_1)
\]
whose reduction modulo \( I \) is \( \overline{\rho}_{\psi, \ell} \) of (1).

Assume now that \( p \in P_\psi \) is not equal to \( I \). Then the representation \( \rho_{\psi, I} \) is unramified at \( p \) (see [Tak82, Thm. 1]), and so, up to conjugation, there is a well-defined matrix
\[
\rho_{\psi, I}(\text{Frob}_p) \in GL_2(A_1)
\]
whose characteristic polynomial we write as
\[
P_{\psi, p}(x) = x^2 + a_p(\psi)x + a'_p(\psi).
\]

This polynomial has remarkable properties:

**Proposition 7.**

(i) \( P_{\psi, p} \) has coefficients in \( A \) and does not depend on the choice of \( I \).

(ii) For any root \( \pi_p(\psi) \) of \( P_{\psi, p} \), we have that \( |\pi_p(\psi)|_\infty = |p|^{1/2} \) and the extension \( F \subseteq F(\pi_p(\psi)) \) is imaginary quadratic.

**Proof.** See [Tak82 Prop. 3].

The coefficients of \( P_{\psi, p} \) can be explicitly determined as follows. Let \( N_{F_p/F_q} \) be the norm map from \( F_p \) to \( F_q \). Let
\[
u_p(\psi) := (-1)^{\deg(p)}N_{F_p/F_q}(g_2)^{-1},
\]
where, by abuse of notation, \( g_2 \) in the norm denotes the reduction of \( g_2 \) modulo \( p \). For an integer \( k \geq 1 \), put
\[
[k] := T^{q^k} - T, \quad \text{and define } s_0 := 1, s_1 := g_1,
\]
\[
s_k := -[k-1]s_{k-2}g_2^{q^k-2} + s_{k-1}g_1^{q^k-1} \quad (k \geq 2).
\]

**Proposition 8.**
(i) The coefficient $a_p(\psi) \in A$ is uniquely determined by
\[
a_p(\psi) \equiv -u_p(\psi) s_{\deg(p)}(\mod p)
\]
and
\[
\deg a_p(\psi) \leq \frac{\deg(p)}{2}.
\] (5)

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

Proof. This follows from Theorem 2.11 and Proposition 3.7 in [Gek08], combined with the reduction properties of Drinfeld modules discussed on page 479 in [Tak82]. □

Note that even though the characteristic polynomial of $\bar{\rho}_{\psi,a}(\text{Frob}_p)$ can be computed in terms of $g_1, g_2$ and $p$, this is not sufficient for determining the conjugacy class of $\bar{\rho}_{\psi,a}(\text{Frob}_p)$, as this matrix is not necessarily semi-simple. For this we need an extra invariant $b_p(\psi)$ related to the reduction of $\psi$ at $p$. Let
\[
E_{\psi,p} := \text{End}_{F_p}(\psi \otimes F_p), \quad \overline{E}_{\psi,p} := \text{End}_{F_p}(\psi \otimes F_p),
\]
and denote by $O_{\psi,p}$ the integral closure of $A$ in $F(\pi_p(\psi))$. At the level of rings, we have the inclusions
\[
A \subseteq A[\pi_p(\psi)] \subseteq E_{\psi,p} \subseteq O_{\psi,p},
\] (6)
and, at the level of division algebras, we have the inclusions
\[
F \subseteq F(\pi_p(\psi)) = E_{\psi,p} \otimes_A F = O_{\psi,p} \otimes_A F \subseteq \overline{E}_{\psi,p} \otimes_A F.
\] (7)
The last inclusion in (7) is equality if $p$ is an ordinary prime for $\psi$, and is strict, of index 2, if $p$ is a supersingular prime for $\psi$.

Both $A[\pi_p(\psi)]$ and $E_{\psi,p} := \text{End}_{F_p}(\psi \otimes F_p)$ are $A$-orders in $O_{\psi,p}$, hence of the form
\[
A[\pi_p(\psi)] = A + \mathfrak{c}_p(\psi)O_{\psi,p}, \quad E_{\psi,p} = A + \mathfrak{c}'_p(\psi)O_{\psi,p}
\] (8)
(9)
for some ideals $\mathfrak{c}_p(\psi), \mathfrak{c}'_p(\psi)$ of $A$, satisfying
\[
\mathfrak{c}'_p(\psi) | \mathfrak{c}_p(\psi).
\] (10)
We define
\[
b_p(\psi) = b_p(\psi)A := \frac{\mathfrak{c}_p(\psi)}{\mathfrak{c}'_p(\psi)},
\] (11)
where $b_p(\psi) \in A^{(1)}$. This is an ideal of $A$ such that
\[
E_{\psi,p}/A[\pi_p(\psi)] \simeq A/b_p(\psi).
\] (12)
In other words, the ideal $b_p(\psi)$ measures how much larger the endomorphism ring $E_{\psi,p}$ is than $A[\pi_p(\psi)]$. 7
Proposition 9. Let $\Delta(E_{\psi,p})$ denote the discriminant ideal of $E_{\psi,p}$. Then, with prior notation,

$$(a_p(\psi)^2 - 4u_p(\psi)p) A = b_p(\psi)^2 \Delta(E_{\psi,p}). \tag{13}$$

Consequently, there exists $\delta_p(\psi) \in A$ such that

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

and

$$a_p(\psi)^2 - 4u_p(\psi)p = b_p(\psi)^2 \delta_p(\psi). \tag{14}$$

Proof. Let $\Delta(O_{\psi,p})$ be the discriminant ideal of $O_{\psi,p}$, and let

$$d(P_{\psi,p}) := a_p(\psi)^2 - 4u_p(\psi)p \in A$$

be the discriminant of the characteristic polynomial $P_{\psi,p}$. On one hand, by (9),

$$\Delta(E_{\psi,p}) = c'_p(\psi)^2 \Delta(O_{\psi,p});$$

hence, upon multiplying by $c_p(\psi)^2$ and using (11),

$$b_p(\psi)^2 \Delta(E_{\psi,p}) = c_p(\psi)^2 \Delta(O_{\psi,p}). \tag{15}$$

On the other hand, by (8),

$$d_p(\psi) A = c_p(\psi)^2 \Delta(O_{\psi,p}). \tag{16}$$

By putting (15) and (16) together, we complete the proof. \qed

2.2. Proof of Theorem 1 and its corollaries. By definition, $E_{\psi,p}$ is the centralizer of the image of $A$ under $\psi$ in $F_p\{\tau\}$. Thus there exists a natural embedding

$$\phi : E_{\psi,p} \hookrightarrow F_p\{\tau\}$$

such that the diagram

$$
\begin{array}{ccc}
A & \longrightarrow & E_{\psi,p} \\
\psi \otimes p & \downarrow \phi & \downarrow \phi \\
F_p\{\tau\}
\end{array}
$$

is commutative.

Recalling that $A \subseteq E_{\psi,p}$ and using that $E_{\psi,p}$ is an $A$-module of rank 2, while $\psi$ is a Drinfeld $A$-module of rank 2, we see that $\phi$ defines an elliptic $E_{\psi,p}$-module over $F_p$ of rank 1 in the sense of Definition 2.1 in [Hay79]. We will use $\phi$ to determine the action of the Frobenius of $\text{Gal}(\overline{F}_p/F_p)$ on $\psi[a]$.

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

$$\psi[a] \simeq_{E_{\psi,p}} E_{\psi,p}/aE_{\psi,p}.$$
Under this isomorphism, the action of the Frobenius of Gal($\mathbb{F}_p/F_p$) on $\psi[a]$ corresponds to multiplication by $\pi_p(\psi)$ on $E_p(\psi)/aE_p.\psi$. We now explore how this action extends to the $A$-module structure of $\psi[a]$. We fix a square root $\sqrt{\delta_p(\psi)}$ of $\delta_p(\psi)$ in $F_{\text{sep}}$ and write $E_{\psi,p} = A + \sqrt{\delta_p(\psi)}A$.

By (14),

$$\pi_p(\psi) = -a_p(\psi) + \sqrt{\delta_p(\psi)b_p(\psi)} \in E_{\psi,p},$$

and so the action of $\pi_p(\psi)$ on the $A$-module $E_{\psi,p}$ is given by (17) and

$$\pi_p(\psi)\sqrt{b_p(\psi)} = \delta_p(\psi)b_p(\psi) + \sqrt{\delta_p(\psi)}(\frac{a_p(\psi)}{2}).$$

This completes the proof of Theorem 1.

Corollary 2 is an immediate consequence to Theorem 1. The description of $d_{1,p}(\psi)$ in Corollary 3 is a consequence to Corollary 2 and the property that, for $a \in A$ with $(a,p) = 1$, $p$ splits completely in $F(\psi[a])/F$ if and only if $A/aA \times A/aA$ is isomorphic to an $A$-submodule of $\psi\mathbb{F}_p$; see [CS13, Prop. 23]. The description of $d_{2,p}(\psi)$ in Corollary 4 is a consequence to that of $d_{1,p}(\psi)$ and the property that

$$P_{\psi,p}(1)A = \chi(\psi\mathbb{F}_p),$$

where $\chi(\psi\mathbb{F}_p)$ denotes the Euler-Poincaré characteristic of $\psi\mathbb{F}_p$ (see [Gek91]).

3. Abhyankar trimonials: Proof of Theorem 4

We keep the setting and notation of Section 2. Let $\psi : A \to F\{\tau\}$ be the rank-2 Drinfeld module defined by (4). Consider the polynomial

$$f_\psi(x) := T + g_1x + g_2x^{q+1} \in F[x]$$

obtained from $\psi$ via the relation

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

First, we determine the structure of $\text{Gal}(f_\psi)$, the Galois group of the splitting field of $f_\psi$ over $F$. For this, we consider the composition of $\hat{\rho}_{\psi,T}$ with the natural projection onto $\text{PGL}_2(A/aA)$, and, after identifying $A/T A \simeq \mathbb{F}_q$, we write it as

$$\hat{\rho}_{\psi,T} : G_F \to \text{PGL}_2(\mathbb{F}_q).$$

By noting that the center $Z(\mathbb{F}_q) \simeq \mathbb{F}_q^*$ of $\text{GL}_2(\mathbb{F}_q)$ acts on $\psi[T]$ by usual multiplication, we deduce that

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

(18)

Now let $p \in P_{\psi}$, $p \neq T$. It follows from (18) and Theorem 1 that $f_\psi$ splits completely modulo $p$ if and only if $b_p(\psi) \equiv 0 \pmod{T}$. Therefore, Part (a) of Theorem 4 follows from (14).
To prove Part (b) of Theorem 4, we rename $g := g_2$ and focus on the 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 non-constant $h \in A$ not divisible by any prime of degree 1 except possibly $T$,

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

(19)

For this, we will follow the general strategy of [Ser72, Proposition 19].

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 $p = pA$ defined by $p = T - c$ for some $c \in \mathbb{F}_q^\times$. For such $p$ let us outline a few properties of $\hat{\rho}_{\psi,T}(\text{Frob}_p)$, which will eventually restrict the possible group structures of $\hat{\rho}_{\psi,T}(G_F)$. By Proposition 8,

$$\det \hat{\rho}_{\psi,T}(\text{Frob}_p) = u_p(\psi)p = \frac{c}{g} \in \mathbb{F}_q^\times,$$

and so the representation

$$\det \circ \hat{\rho}_{\psi,T} : G_F \rightarrow \mathbb{F}_q^\times$$

is surjective. Again, by Proposition 8,

$$\text{tr} \hat{\rho}_{\psi,T}(\text{Frob}_p) = a_p(\psi) \equiv \frac{1}{g} \pmod{p},$$

and upon recalling (5), we get

$$a_p(\psi) = \frac{1}{g} \in \mathbb{F}_q^\times.$$

Hence

$$d(P_{\psi,p}) := a_p(\psi)^2 - 4u_p(\psi)p = \frac{1}{g^2} - \frac{4c}{g},$$

(20)

$$f(P_{\psi,p}) := \frac{a_p(\psi)^2}{u_p(\psi)p} = \frac{1}{cg}.$$

(21)

Since $q$ is odd, (20) implies that $d(P_{\psi,p})$ assumes all values of $\mathbb{F}_q^\times \setminus \left\{\frac{1}{g}\right\}$. In particular, since $q \geq 5$,

$$d_{P_{\psi,p}}$$

assumes a non-zero square value

(22)

and

$d_{P_{\psi,p}}$ assumes a non-square value.

(23)

Moreover, (21) implies that $f(P_{\psi,p})$ assumes values such that

$$f(P_{\psi,p}) \notin \{0, 1, 2, 4\}$$

(24)

and

$$f(P_{\psi,p})$$

does not satisfy $u^2 - 3u + 1 = 0$

(25)

(for example, if the characteristic is not 3, then $c := (3g)^{-1}$ gives the value 3, which satisfies these restrictions).
Finally, let us focus on the structure of \( H := \hat{\rho}_\psi,T(G_F) \leq \PGL_2(F_q) \). By a classical theorem of Dickson, one of the following holds:

(i) \( H \) is conjugate to a subgroup of the upper-triangular matrices;
(ii) \( H \) is conjugate to \( \PSL_2(F) \) or \( \PGL_2(F) \) for some subfield \( F \subseteq F_q \);
(iii) \( H \) is isomorphic to the dihedral group \( D_{2n} \) of order \( 2n \) for some \( n \in \mathbb{N} \setminus \{0,1\} \) not divisible by the characteristic of \( F_q \);
(iv) \( H \) is isomorphic to the permutation groups \( A_4, S_4 \) or \( A_5 \).

The properties of \( H \) derived from the above observations will exclude all but one of these cases.

Indeed, (i) is not possible by (23), (iii) is not possible by (22), while (iv) is also not possible by (24) and (25); cf. [Ser72, p. 284]. Since \( \det \circ \bar{\rho}_\psi,T \) is surjective, \( H \) cannot be conjugate to \( \PSL_2(F_q) \). Furthermore, let \( I_T \) denote the inertia group at \( T \) and recall that, by Proposition 2.7 in [PR09], \( \hat{\rho}_\psi,T(I_T) \) contains a Cartan subgroup of \( \PGL_2(F_q) \). Thus \( H \) cannot be conjugate to \( \PGL_2(F_q) \) for a proper subfield \( F \subset F_q \). We are thus left with only one possibility: \( H = \PGL_2(F_q) \).

Now let us consider the case \( g = h^{q-1} \) for some non-constant \( h \in A \) not divisible by any prime of degree 1, except possibly \( T \). We use the same arguments as above, based on the calculations

\[
\det(\bar{\rho}_\psi,T(\Frob_p)) = (-1)h(c)^{-1}(T-c) = \epsilon \in F_q^*,
\]
\[
\text{tr}(\bar{\rho}_\psi,T(\Frob_p)) = -\frac{1}{h(c)^q-1} = -1 \in F_q^*.
\]

Using part (a), the above, and the Chebotarev Density Theorem, we deduce that the Dirichlet density of

\[
\{ p \in \mathcal{P}_\psi : f_\psi \text{splits completely modulo } p \} = \{ p \in \mathcal{P}_\psi : b_p(\psi) \equiv 0 \pmod{T} \}
\]

exists and equals \( \frac{1}{\# \PGL_2(F_q)} = \frac{1}{q(q^2-1)}. \) This completes the proof of Theorem 4.

4. REDUCTIONS OF DRINFELD MODULES: PROOF OF THEOREM 5

4.1. Preliminaries. The proofs of the following lemmas are elementary and are left to the reader:

**Lemma 10.** Let \( y \geq 1 \) be an integer. Then:

\[
(i) \sum_{m \in A(1) \atop 0 \leq \deg m \leq y} 1 = \frac{q^{y+1} - 1}{q - 1};
\]
\[
(ii) \sum_{m \in A(1) \atop 0 \leq \deg m \leq y} \deg m \leq y \frac{q^{y+1} - 1}{q - 1}.
\]

**Lemma 11.** Let \( y \geq 3 \) be an integer and let \( \alpha > 1 \). Then:

\[
(i) \sum_{a \in A \atop \deg a > y} \frac{1}{q^{\alpha \deg a}} = \frac{q}{(1 - \frac{1}{q^\alpha}) q^{(\alpha-1)(y+1)}},
\]
\[
(ii) \sum_{a \in A \atop \deg a > y} \log \deg a \leq \frac{\log q}{(\alpha-1)q^{(\alpha-1)y} \log q} + \frac{1}{y(\alpha-1)^2 q^{(\alpha-1)y}(\log q)^2}, \text{ provided that } (\alpha-1)y \log q \log y > 1.
\]
Now let us fix $a \in A \setminus F_q$ and, as before, consider $F_a := F(\psi[a]).$ An important subfield of $F_a$ is
\[ J_a := \{ z \in F_a : \sigma(z) = z \, \forall \sigma \in \text{Gal}(F_a/F) \text{ a scalar element} \}. \quad (26) \]
This field may be better understood by considering the composition of $\tilde{\rho}_{\psi,a}$ with the projection onto $\text{PGL}_2(A/aA).$ Indeed, this composition leads to a Galois representation
\[ \hat{\rho}_{\psi,a} : G_F \rightarrow \text{PGL}_2(A/aA) \]

satisfying
\[ J_a = (F^\text{sep})^{\ker \hat{\rho}_{\psi,a}}. \]
(Note that we have already considered the special case $\hat{\rho}_{\psi,T}$ in the proof of Theorem 4.)

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

**Theorem 12.**

(i) The degrees of the fields of constants of $F_a$ and $J_a$, that is,
\[
c_{F_a} := [F_a \cap F_q : F_q], \quad c_{J_a} := [J_a \cap F_q : F_q],
\]
are uniformly bounded from above in terms of $\psi$. That is,
\[
c_{J_a} \leq c_{F_a} \leq C(\psi)
\]
for some constant $C(\psi) \in \mathbb{N} \setminus \{0\}$.

(ii) The genera $g_{F_a}, g_{J_a}$ of $F_a, J_a$ are bounded from above by
\[
g_{J_a} \leq g_{F_a} \leq G(\psi)[F_a : F] \deg a
\]
for some constant $G(\psi) \in \mathbb{N} \setminus \{0\}$.

(iii) The degrees of $F_a/F, J_a/F$ are bounded from above by
\[
[F_a : F] \leq \# \text{GL}_2(A/aA), \quad [J_a : F] \leq \# \text{PGL}_2(A/aA).
\]

(iv) Assume that $\text{End}_F(\psi) = A.$ There exists $M(\psi) \in A^{(1)}$ such that, if $(a, M(\psi)) = 1$, then
\[
\text{Gal}(F_a/F) \simeq \text{GL}_2(A/aA).
\]

Consequently, if $(a, M(\psi)) = 1$, then
\[
[F_a : F] = \# \text{GL}_2(A/aA), \quad [J_a : F] = \# \text{PGL}_2(A/aA),
\]
and
\[
c_{F_a} = c_{J_a} = 1;
\]
if $a$ arbitrary, then
\[
\frac{|a|^4}{\log \deg a + \log \log q} \ll_{\psi} |F_a : F| \leq |a|_{\infty}^4,
\]
\[
\frac{|a|^3}{\log \deg a + \log \log q} \ll_{\psi} |J_a : F| \leq |a|_{\infty}^3.
\]

(v) Assume that $\text{End}_F(\psi) \neq A$. Then
\[
\frac{|a|^2}{\log \deg a + \log \log q} \ll_{\psi} |F_a : F| \ll_{\psi} |a|_{\infty}^2,
\]
\[
\frac{|a|}{\log \deg a + \log \log q} \ll_{\psi} |J_a : F| \ll_{\psi} |a|_{\infty}.
\]

(vi) Let $\bar{C}, \hat{C}$ be conjugacy classes in $\text{Gal}(F_a/F)$, respectively in $\text{Gal}(J_a/F)$. Denote by $a_{\bar{C}}, a_{\hat{C}}$ respectively, a positive integer such that, for any $\sigma \in \text{Gal}(F_a/F), \text{Gal}(J_a/F)$ respectively, the restriction of $\sigma$ to $F_a \cap \mathbb{F}_q, J_a \cap \mathbb{F}_q$ respectively, equals the corresponding restriction of $\tau^{a_{\bar{C}}}, \tau^{a_{\hat{C}}}$ respectively.
For $x \in \mathbb{N}$, let
\[
\Pi_{\bar{C}}(x, F_a/F) := \# \{ p \in \mathcal{P}_\psi : \deg p = x, \sigma_p \subseteq \bar{C} \},
\]
\[
\Pi_{\hat{C}}(x, J_a/F) := \# \{ p \in \mathcal{P}_\psi : \deg p = x, \sigma_p \subseteq \hat{C} \}.
\]
Then
\[
\Pi_{\bar{C}}(x, F_a/F) = \frac{c_{F_a}(x) \cdot \# \bar{C}}{|F_a : F|} \cdot \frac{q^x}{x} + O_\psi \left( \left( \# \bar{C} \right)^{\pm} q^{x/2} \deg a \right),
\]
\[
\Pi_{\hat{C}}(x, J_a/F) = \frac{c_{J_a}(x) \cdot \# \hat{C}}{|J_a : F|} \cdot \frac{q^x}{x} + O_\psi \left( \left( \# \hat{C} \right)^{\pm} q^{x/2} \deg a \right),
\]
where
\[
c_{F_a}(x) := \begin{cases} 
  c_{F_a} & \text{if } c_{F_a} | x - a_{\bar{C}}, \\
  0 & \text{else},
\end{cases}
\]
\[
c_{J_a}(x) := \begin{cases} 
  c_{J_a} & \text{if } c_{J_a} | x - a_{\hat{C}}, \\
  0 & \text{else}.
\end{cases}
\]

Proof. For part (i), see [Gos96, Remark 7.1.9]. For part (ii), see [Gar02, Cor. 7]. Parts (iv) and (v) can be derived from the main results of [PR09], as explained in [CS13, Section 3.6]. Part (vi) is an application of the second part of the effective Chebotarev Density Theorem of [KMS93], as well as the prior parts of Theorem 12.
4.2. Proof of Part (a) of Theorem \[5\] Let

\[
B(\psi, x) := \# \{ p \in \mathcal{P}_\psi : \deg p = x, E_{\psi, p} = A[\pi_p(\psi)] \}. \tag{30}
\]

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

\[
B(\psi, x) = \# \{ p \in \mathcal{P}_\psi : \deg p = x, b_p(\psi) = 1 \}
= \# \{ p \in \mathcal{P}_\psi : \deg p = x, \ell \mid b_p(\psi) \forall \ell \in A^{(1)} \}
= \sum_{m \in A^{(1)}} \mu_A(m) \# \{ p \in \mathcal{P}_\psi : \deg p = x, m \mid b_p(\psi) \},
\]

where in the first line we used (12).

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 \(m \mid b_p(\psi)\) with (14), we obtain

\[
m^2 \mid a_p(\psi)^2 - 4u_p(\psi)p.
\]

Upon recalling (5) and using that \(\deg p = x\), we deduce that \(\deg m \leq \frac{x}{2}\). Thus

\[
B(\psi, x) = \sum_{m \in A^{(1)} : \deg m \leq \frac{x}{2}} \mu_A(m) \# \{ p \in \mathcal{P}_\psi : \deg p = x, m \mid b_p(\psi) \}. \tag{31}
\]

By Theorem \[11\] the extension \(J_m/F\) has the property that, for any \(p = pA \in \mathcal{P}_\psi\) with \((p, m) = 1\),

\[
m \mid b_p(\psi) \text{ if and only if } p \text{ splits completely in } J_m.
\]

Consequently, we can write

\[
B(\psi, x) = \sum_{m \in A^{(1)} : \deg m \leq y} \mu_A(m) \Pi_1(x, J_m/F) + \sum_{m \in A^{(1)} : y < \deg m \leq \frac{y}{2}} \mu_A(m) \# \{ p \in \mathcal{P}_\psi : \deg p = x, m \mid b_p(\psi) \}, \tag{31}
\]

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

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

The splitting of \(B(\psi, x)\) 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 \(B(\psi, x)\) 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 $B(\psi, x)$. For $y = y(x) \leq \frac{x}{2}$ a parameter, we focus on

$$B_1(\psi, x, y) := \sum_{m \in A(1)} \mu_A(m) \Pi_1(x, J_m/F).$$

By part (vi) of Theorem 12 this becomes

$$B_1(\psi, x, y) = \sum_{m \in A(1)} \mu_A(m) c_{J_m}(x) \frac{q^x}{x} + O_{\phi}(x \phi(x/y^2)).$$

By (14), $m | b_p(\psi) \Rightarrow m^2 | (a_p(\psi)^2 - 4u_p(\psi)p)$.

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

$$a_p(\psi)^2 - 4u_p(\psi)p = m^2 f^2 g.$$ 

By (14),

$$m | b_p(\psi) \Rightarrow m^2 | (a_p(\psi)^2 - 4u_p(\psi)p).$$ 

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

$$B_2(\psi, x, y) \leq \sum_{h \in A \atop y < \deg h \leq \frac{x}{2}} \tau_A(h) \# \{p \in \mathcal{P}_\psi : \deg p = x, \exists g \in A \text{ squarefree such that } a_p(\psi)^2 - 4u_p(\psi)p = h^2 g\},$$

where

$$\tau_A(h) := \sum_{d | h} 1$$

is the divisor function of $h$.

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

$$\deg h = \deg m + \deg f,$$
hence from \( \deg h \geq \deg m > y \),

and also from

\[
h^2 \mid (a_p(\psi)^2 - 4u_p(\psi)p),
\]

hence from

\[
2 \deg h \leq \deg p = x,
\]

after recalling (5).

Using the bound

\[
\tau_A(h) \ll |h|_\infty \quad \forall \varepsilon > 0,
\]

we deduce that

\[
B_2(\psi,x,y) \ll \varepsilon q^{x\varepsilon} \sum_{\substack{h \in A \\
y < \deg h \leq x}} \# \{ p \in \mathcal{P}_\psi : \deg p = x, \exists g \in A \text{ squarefree such that } a_p(\psi)^2 - 4u_p(\psi)p = h^2 g \}.
\]

Note that the factorization \( a_p(\psi)^2 - 4u_p(\psi)p = h^2 g \) is unique. As such,

\[
B_2(\psi,x,y) \ll \varepsilon q^{x\varepsilon} \sum_{g \in A \text{ squarefree} \atop \deg g < x - 2y} \# \{ p \in \mathcal{P}_\psi : \deg p = x, g (a_p(\psi)^2 - 4u_p(\psi)p) \text{ is a square in } A \}
\]

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

The range of \( \deg g \) above is obtained once again using (5):

\[
2 \deg h + \deg g \leq x \implies \deg g \leq x - 2 \deg h < x - 2y.
\]

To estimate \( S_g(\psi) \) we rely on the function field analogue of the Square Sieve proven in [CD08, Section 7] and on part (vi) of Theorem 12. Specifically, we use the resulting bound

\[
S_g(\psi) \ll q^{\frac{2x}{3}}(x + \deg g) + q^{\frac{2x}{3}} x(x + \deg g)^2
\]

(which we will prove shortly) and deduce that

\[
B_2(\psi,x,y) \ll_{\psi,\varepsilon} q^{\frac{2x}{3} - 2y + x\varepsilon} x^3.
\]

Now let us prove (34); our arguments use tools from [CD08, Section 8] and are included in detail for completeness. We recall the Square Sieve for \( A \):

**Theorem 13.** Let \( A \) be a finite multiset of non-zero elements of \( A \). Let \( \mathcal{P} \) be a finite set of primes of \( A \). Let

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

and for any \( a \in A \) define

\[
\nu_{\mathcal{P}}(a) := \# \{ \ell \in \mathcal{P} : \ell \mid a \}.
\]
Then
\[
\#S(A) \leq \frac{\#A}{\#\mathcal{P}} + \max_{\ell_1, \ell_2 \in \mathcal{P}} \left| \sum_{p \in \mathcal{P}_\psi, \text{deg } p = x} \left( \frac{g(a_p(\psi)^2 - 4u_p(\psi)p)}{\ell_1} \right) \left( \frac{g(a_p(\psi)^2 - 4u_p(\psi)p)}{\ell_2} \right) \right|
\]
\[
+ \frac{2}{\#\mathcal{P}} \sum_{p \in \mathcal{P}_\psi, \text{deg } p = x} \nu_p \left( g(a_p(\psi)^2 - 4u_p(\psi)p) \right) + \frac{1}{(\#\mathcal{P})^2} \sum_{p \in \mathcal{P}_\psi, \text{deg } p = x} \nu_p^2 \left( g(a_p(\psi)^2 - 4u_p(\psi)p) \right).
\]

We apply Theorem 13 in the setting
\[
A := \{ g(a_p(\psi)^2 - 4u_p(\psi)p) : p \in \mathcal{P}_\psi, \text{deg } p = x \}
\]
and
\[
\mathcal{P} := \{ \ell \in A : \ell \text{ prime, deg } \ell = \theta \}
\]
for some parameter $\theta = \theta(x) \neq x$, to be chosen optimally later.

We obtain
\[
S_g(\psi) \leq \frac{\#A}{\#\mathcal{P}} + \max_{\ell_1, \ell_2 \in \mathcal{P}} \left| \sum_{p \in \mathcal{P}_\psi, \text{deg } p = x} \left( \frac{g(a_p(\psi)^2 - 4u_p(\psi)p)}{\ell_1} \right) \left( \frac{g(a_p(\psi)^2 - 4u_p(\psi)p)}{\ell_2} \right) \right|
\]
\[
+ \frac{2}{\#\mathcal{P}} \sum_{p \in \mathcal{P}_\psi, \text{deg } p = x} \nu_p \left( g(a_p(\psi)^2 - 4u_p(\psi)p) \right) + \frac{1}{(\#\mathcal{P})^2} \sum_{p \in \mathcal{P}_\psi, \text{deg } p = x} \nu_p^2 \left( g(a_p(\psi)^2 - 4u_p(\psi)p) \right). \tag{36}
\]

On one hand, by the Prime Number Theorem for $A$,
\[
\frac{\#A}{\#\mathcal{P}} \asymp q^{-\theta} \frac{\theta}{d}. \tag{37}
\]

On the other hand, by noting that, for any $a \in A$, $\nu_p(a) \leq \deg a$, and by using (3), we deduce that, for primes $p$ of degree $x$,
\[
\nu_p \left( g(a_p(\psi)^2 - 4u_p(\psi)p) \right) \leq x + \deg g.
\]

We infer the estimates
\[
\frac{2}{\#\mathcal{P}} \sum_{p \in \mathcal{P}_\psi, \text{deg } p = x} \nu_p \left( g(a_p(\psi)^2 - 4u_p(\psi)p) \right) \ll q^{-\theta} \frac{\theta}{x} (x + \deg g), \tag{38}
\]
\[
\frac{1}{(\#\mathcal{P})^2} \sum_{p \in \mathcal{P}_\psi, \text{deg } p = x} \nu_p^2 \left( g(a_p(\psi)^2 - 4u_p(\psi)p) \right) \ll q^{-2\theta} \frac{\theta^2}{x} (x + \deg g)^2. \tag{39}
\]

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 12. (Note that, by choosing $x$ sufficiently large, we can ensure that this condition holds.) We define
\[
T_1 = T_1(\ell_1, \ell_2) := \# \left\{ p \in \mathcal{P}_\psi : \text{deg } p = x, \left( \frac{a_p(\psi)^2 - 4u_p(\psi)p}{\ell_1} \right) = \left( \frac{a_p(\psi)^2 - 4u_p(\psi)p}{\ell_2} \right) = 1 \right\},
\]
\[
T_2 = T_2(\ell_1, \ell_2) := \# \left\{ p \in \mathcal{P}_\psi : \text{deg } p = x, \left( \frac{a_p(\psi)^2 - 4u_p(\psi)p}{\ell_1} \right) = \left( \frac{a_p(\psi)^2 - 4u_p(\psi)p}{\ell_2} \right) = -1 \right\},
\]
\[
T_3 = T_3(\ell_1, \ell_2) := \# \left\{ p \in \mathcal{P}_\psi : \text{deg } p = x, \left( \frac{a_p(\psi)^2 - 4u_p(\psi)p}{\ell_1} \right) = - \left( \frac{a_p(\psi)^2 - 4u_p(\psi)p}{\ell_2} \right) = 1 \right\},
\]
\[ T_4 = T_4(\ell_1, \ell_2) := \# \left\{ p \in P_\psi : \deg p = x, \frac{(a_p(\psi)^2 - 4u_p(\psi)p)}{\ell_1} = -1 \right\}, \]

and

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

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

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

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

where \( \hat{g} \) denotes the projective image of a matrix \( g \in \text{GL}_2(A/\ell_1 \ell_2 A) \).

On one hand, we have

\[ S_{\ell_1, \ell_2} := \left( g \frac{(a_p(\psi)^2 - 4u_p(\psi)p)}{\ell_1} \right) \left( g \frac{(a_p(\psi)^2 - 4u_p(\psi)p)}{\ell_2} \right) = \left( \frac{g}{\ell_1} \right) \left( \frac{g}{\ell_2} \right) (T_1 + T_2 - T_3 - T_4). \] (40)

On the other hand, by parts (v) and (vii) of Theorem 12 for each \( 1 \leq i \leq 4 \) we have

\[ T_i = \Pi_{\hat{C}_i}(x, J_{\ell_1, \ell_2}/F) = \frac{\# \hat{C}_i}{\# \text{PGL}_2(A/\ell_1 \ell_2 A)} \cdot \frac{q^x}{x} + O_{\psi} \left( (\# \hat{C}_i) \frac{q^x}{x} \deg(\ell_1 \ell_2) \right). \] (41)

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

\[ \# \text{PGL}_2(A/\ell A) = |\ell|_{\infty}(|\ell|_{\infty}^2 - 1), \]

\[ \# \left\{ \hat{g} \in \text{PGL}_2(A/\ell A) : \frac{(\text{tr} g)^2 - 4 \det g}{\ell} = 1 \right\} = \frac{|\ell|_{\infty}^3}{2} + O \left( |\ell|_{\infty}^2 \right), \]

\[ \# \left\{ \hat{g} \in \text{PGL}_2(A/\ell A) : \frac{(\text{tr} g)^2 - 4 \det g}{\ell} = -1 \right\} = \frac{|\ell|_{\infty}^3}{2} + O \left( |\ell|_{\infty}^2 \right). \]

Therefore, for each \( 1 \leq i \leq 4 \),

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

where the O-constants are absolute. Consequently, by (41), for each \( 1 \leq i \leq 4 \) we have

\[ T_i = \frac{|\ell_1|_{\infty}^3 |\ell_2|_{\infty}^3}{4 (|\ell_1|_{\infty}^2 - 1) (|\ell_2|_{\infty}^2 - 1)} \cdot \frac{q^x}{x} + O \left( \frac{|\ell_1|_{\infty} |\ell_2|_{\infty}}{|\ell_1|_{\infty} + |\ell_2|_{\infty}} \cdot \frac{q^x}{x} \right) + O_{\psi} \left( |\ell_1|_{\infty} |\ell_2|_{\infty}^2 \cdot q^x \log_q(|\ell_1|_{\infty} + |\ell_2|_{\infty}) \right). \]

By plugging these estimates into (40) and recalling that \( |\ell_1|_{\infty} = |\ell_2|_{\infty} = q^\theta \), we obtain

\[ S_{\ell_1, \ell_2} \ll_{\psi} \frac{q^{x-\theta}}{x} + q^{\frac{3}{2} \theta} \theta. \] (42)

Then, by combining (36) with (37), (38), (39), and (42), we obtain

\[ S_g(\psi) \ll_{\psi} q^{x-\theta} \theta (x + \deg g) + q^{\frac{3}{2} \theta} \theta + q^{x-2\theta} \theta^2 \frac{(x + \deg g)^2}{x}. \]
We now choose

\[ \theta := \frac{x}{8} \]

and conclude that

\[ S_g(\psi) \ll \psi^{x} q^{x} (x + \deg g) + q^{x} x (x + \deg g)^2, \]

justifying (34).

4.2.3. **Conclusion.** By putting together (31), (32), (35), and by choosing

\[ y(x) := \frac{11x}{24} + \varepsilon \]

for any arbitrary \( \varepsilon > 0 \), we obtain that

\[ B(\psi, x) = \sum_{m \in A(1)} \mu_A(m) [J_m : F] q^{x} \sum_{x \geq 1} c^{J_m} \left( \frac{q^{x}}{x} + O_{\psi, F, \varepsilon} \left( q^{\frac{23}{24} + x \varepsilon} x^3 \right) \right). \] (43)

4.2.4. **Dirichlet density.** To determine the Dirichlet density of the set \( \{ p \in \mathcal{P}_\psi : b_p(\psi) = 1 \} \), we make use of the asymptotic formula (43). In particular, for \( s > 1 \) (with \( s \to 1^+ \)), we have:

\[ \sum_{p \in \mathcal{P}_\psi \ b_p(\psi) = 1} q^{-s \deg p} = \sum_{x \geq 1} q^{-sx} B(\psi, x) \]

\[ = \sum_{m \in A(1)} \mu_A(m) [J_m : F] \sum_{x \geq 1} q^{(1-s)x} c^{J_m} \left( \frac{q^{x}}{x} + O_{\psi, F, \varepsilon} \left( q^{\frac{23}{24} + x \varepsilon - s} x \right) \right) \]

\[ = \sum_{m \in A(1)} \mu_A(m) [J_m : F] \sum_{j \geq 1} q^{(1-s)j c^{J_m}} \left( \frac{q^{x}}{1 - q^{\frac{23}{24} + x \varepsilon - s}} \right) \]

\[ = - \sum_{m \in A(1)} \mu_A(m) [J_m : F] \log \left( 1 - q^{1-s} c^{J_m} \right) + O_{\psi, F, \varepsilon} \left( q^{\frac{23}{24} + x \varepsilon - s} \right). \]

Upon taking the quotient with \( - \log (1 - q^{1-s}) \) and the limit \( s \to 1^+ \), we obtain

\[ \sum_{m \in A(1)} \frac{\mu_A(m)}{[J_m : F]}. \]

4.3. **Proof of Part (b) of Theorem 5.** With notation (30), we write

\[ B(\psi, x) = \# \{ p \in \mathcal{P}_\psi : \deg p = x, p \text{ ordinary}, E_{\psi, p} = A[\pi_p(\psi)] \} + \# \{ p \in \mathcal{P}_\psi : \deg p = x, p \text{ supersingular}, E_{\psi, p} = A[\pi_p(\psi)] \} \]

\[ = B^o(\psi, x) + B^{ss}(\psi, x). \] (44)

We will estimate each of the two terms above separately.
4.3.1. Ordinary primes. Let $p \in \mathcal{P}_\psi$ be an ordinary prime for $\psi$. First of all,

$$\text{End}_{\mathbf{F}_p}(\psi) \otimes_A F \subseteq \mathcal{E}_{\psi,p} \otimes_A F,$$

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

$$E_{\psi,p} \simeq \mathcal{O}_{\psi,p} \simeq \mathcal{E}_{\psi,p} \simeq \text{End}_{\mathbf{F}_p}(\psi). \quad (45)$$

In particular, the discriminant $\Delta$ of $\text{End}_{\mathbf{F}_p}(\psi)$ equals $\Delta(E_{\psi,p})$ and so, by (14), there exists $\delta \in A$, independent of $p$, such that

$$\Delta = \delta A$$

and

$$a_p(\psi)^2 - 4u_p(\psi)p = b_p(\psi)^2\delta.$$ 

Consequently,

$$b_p(\psi) = 1 \iff u_p(\psi) = \left(\frac{a_p(\psi)}{2}\right)^2 - \frac{\delta}{4}. \quad (46)$$

Recalling (5) and using part (i) of Lemma 10, we deduce that there are at most $O(\mathbf{q}^2)$ possible $a_p(\psi) \in A$. Thus, by (46),

$$B^0(\psi, x) \ll \mathbf{q}^2. \quad (47)$$

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

$$a_p(\psi) = 0 \quad (48)$$

(cf. [Yu95, Prop. 4]). By using this in (14), we deduce that $-4u_p(\psi)p = b_p(\psi)^2\delta_p(\psi)$, which implies $b_p(\psi) = 1$.

Under the assumption $\text{End}_{\mathbf{F}_p}(\psi) \otimes_A F \simeq K$, we also have that any supersingular prime for $\psi$ is either ramified or inert in $K$ (cf. [Yu95]). Combining this with the above and invoking the Chebotarev Density Theorem for $K$, we deduce that

$$B^{ss}(\psi, x) = \frac{c_K(x)}{2} \cdot \frac{\mathbf{q}^2}{x} + O_K(\mathbf{q}^2). \quad (49)$$

By putting together (44), (47) and (49), and by a similar calculation as in Section 4.2.4, we complete the proof of part (b) of Theorem 5.
4.4. Remarks. (i) A natural question to ask is whether the Dirichlet density in part (a) of Theorem 5 is positive. This question is related to a good understanding of the constant $M(\psi)$ introduced in part (iv) of Theorem 12 and, in particular, to an understanding of effective versions of the Open Image Theorems for Drinfeld modules proven by R. Pink and E. Rütsche [PR09]. We point out that, unlike the situation for elliptic curves (cf. [CD04], where any elliptic 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 $\{p \in \mathcal{P}_\psi : \text{End}_{\mathbb{F}_p}(\psi \otimes \mathbb{F}_p) = A[\pi_p(\psi)]\}$. In [Zyw11a], 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 $\mathbb{F}_q \cap F(\psi[a]) = \mathbb{F}_q$ for all $a \in A$. It is easy to see that for this particular $\psi$ the Dirichlet density in question is indeed non-zero.

(ii) As already emphasized in Corollary 3 the condition $b_p(\psi) = 1$ implies that $\psi|_{\mathbb{F}_p}$ is $A$-cyclic. The reductions of $\psi$ giving rise to a cyclic $A$-module have been studied in several works, for example, [CS13], [Hsu97], [HY00], and [KL09]. An outcome of part (b) of Theorem 5 is then 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 [CM04]), where such a result is not true: there exist CM elliptic curves over $\mathbb{Q}$ (in fact, any such curve with a rational 2-torsion) which have no reductions with cyclic structures; moreover, for such CM elliptic curves with no rational 2-torsion one cannot always ensure a density of $\geq 0.5$ of cyclic reductions.

(iii) For comparison, we recall that the Lang-Trotter Conjecture for Drinfeld modules predicts that, for any rank-2 Drinfeld module $\psi : A \to F\{\tau\}$ and any $a \in A$ (non-zero, if $\psi$ has CM),

$$A(\psi, a, x) := \#\{p \in \mathcal{P}_\psi : \text{deg } p = x, a_p(\psi) = a\} \sim C(\psi, a)q^{x^2}/x$$

for some constant $C(\psi, a) \geq 0$. Less is known about this asymptotic formula compared to what we have just proved about $b_p(\psi)$. Specifically, apart from lower bounds for the case $a = 0$ (see [Bro92] and [Dav95]), only upper bounds for $A(\psi, x, a)$ are currently known (see [CD08], [Dav01], and [Zyw11b]). Moreover, the particular case $a = 0$, which is equivalent to the study of supersingular primes, has led to intriguing results. Indeed, unlike for elliptic curves over $\mathbb{Q}$ where there are always infinitely many supersingular primes, there exist Drinfeld modules $\psi$ with no supersingular prime (see [Poo98] and the references therein).

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 4.2 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 [Oor92 Def. 1.7], we say that $B$ has sufficiently many complex multiplications (or is CM, for short) if $\text{End}_K^0(B) := \text{End}_K(B) \otimes \mathbb{Q}$
contains a commutative semi-simple algebra $L$ of dimension $2g$ over $\mathbb{Q}$. If $B$ is simple, then $L$ is necessarily a CM field, i.e., 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 an integral domain $R$ with fraction field $K$ of characteristic zero, a ring homomorphism $R \rightarrow k$, and an abelian scheme $\mathcal{B}$ over $R$ such that $\mathcal{B} \otimes_R k \cong B_0$ and $\mathcal{B} = \mathcal{B} \otimes_R K$ is CM.

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

**Theorem 14.** Let $E_0$ be an elliptic curve over a finite field $k$. For any $f_0 \in \text{End}_k(E_0)$ generating an imaginary quadratic field $L \subset \text{End}_k^0(E_0)$, there is an elliptic curve $E$ over the ring of integers $R$ of a finite extension of $\mathbb{Q}_p$ equipped with an endomorphism $f \in \text{End}_K(E)$ such that $(E, f)$ has special fibre isomorphic to $(E_0, f_0)$.

*Proof.* See Theorem 1.7.4.5 in [CCO13].

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

Finally, in the recent monograph [CCO13] the authors show that both the isogeny and the field extension in the previous theorem are necessary for the existence of CM-liftings:

**Theorem 16.**

(a) For any $g \geq 3$, there exists an abelian variety over $\mathbb{F}_p$ 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.** Let $F$ be an arbitrary function field with field of constants $\mathbb{F}_q$, and $\infty$ be a fixed place of $F$. As in the introduction, let $A$ denote the ring of elements of $F$ which have only $\infty$ as a pole.

Let $R$ be a discrete valuation ring with maximal ideal $m$ and field of fractions $K$. Assume $K$ is equipped with an injective homomorphism $\gamma : A \rightarrow K$, so the $A$-characteristic of $K$ is 0. A Drinfeld $A$-module over $R$ of rank $r$ is an embedding $\psi : A \rightarrow R\{\tau\}$ which is a Drinfeld module over $K$ of rank $r$, as defined in the introduction, and such that the composite homomorphism $\bar{\psi} : A \rightarrow R\{\tau\} \rightarrow \bar{R}/\bar{m}\{\tau\}$ is a Drinfeld module over $\bar{R}/\bar{m}$, again of rank $r$; cf. Definition 7.1 in [Hay79]. We say that $\psi$ has **CM** if $\text{End}_K(\psi) \otimes_A F$ is a field extension $L$ of $F$ of degree $r$. (Note that since $\infty$ does not split in $L$, it is imaginary.)
Let $k$ be a finite field with $A$-characteristic $p$. Let $\psi_0$ be a Drinfeld $A$-module over $k$. We say that $\psi_0$ has a \textbf{CM-lifting} if there exists a discrete valuation ring $R$ with residue field $k$, and a CM Drinfeld module $\psi$ over $R$ such that $\overline{\psi}$ 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 $E = \text{End}_k(\psi_0)$ and $D = E \otimes_A F$. It is clear that $\pi := \tau^n \in E$. Let $\widetilde{F} := F(\pi) \subseteq D$. The following is known about $D$ and $\widetilde{F}$ (see Theorem 1 in [Yui95]):

- The degree of $\widetilde{F}$ over $F$ divides $r$. Let $t := r/|\widetilde{F} : F|$.
- There is a unique place $\mathfrak{P}$ of $\widetilde{F}$ which is a zero of $\pi$ and there is a unique place $\infty_{\widetilde{F}}$ of $\widetilde{F}$ which is a pole of $\pi$. Furthermore, $\mathfrak{P}$ lies over $\mathfrak{p}$, and $\infty_{\widetilde{F}}$ is the unique place lying over $\infty$.
- $D$ is a central division algebra over $\widetilde{F}$ of dimension $t^2$ with invariants
  \[
  \text{inv}_v(D) = \begin{cases} 
  1/t & \text{if } v = \mathfrak{P} \\
  -1/t & \text{if } v = \infty_{\widetilde{F}} \\
  0 & \text{otherwise.}
  \end{cases}
  \]

By Theorem 7.15 in [Rei03], the maximal subfields of $D$ are those which have degree $r$ over $F$, and any such field contains $\widetilde{F}$. Let $L$ be a maximal subfield of $D$. Denote by $A_L$ be the integral closure of $A$ in $L$ and put $A = E \cap L$. We say that $L$ is \textbf{good} for $\psi_0$ if the conductor $c$ of $A$ as an $A$-order in $A_L$ is coprime to $\mathfrak{p}$.

**Theorem 17.** If $L$ is good for $\psi_0$, then the Drinfeld module $\psi_0$ has a CM-lifting $\psi$ such that $\text{End}_K(\psi) \otimes_A F = L$.

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

\[
\psi_0 : A \to k \{\tau\}.
\]

The restriction of $\psi'_0$ to $A$ is the original module $\psi_0$. By Proposition 3.2 in [Hay79], there is a Drinfeld $A_L$-module $\phi'_0$ of rank 1 over $k$, whose restriction to $A$ 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 $c$ 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. Proposition 4.7.19 in [Gos96]. 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 [Leh09] §3.1. Restricting $\phi'$ to $A$ we get a rank-$r$ Drinfeld $A$-module $\phi$ over $K$ with CM by $L$, whose reduction is $\phi_0$. Since $\ker(i)$ is étale, Corollary 2.3 on page 22 in [Leh09] implies that the kernel of $i$ also lifts to an $A$-invariant submodule $H \subset \phi K^{\text{sep}}$ which is also invariant under $\text{Gal}(K^{\text{sep}}/K)$. (Note that $H$ is not necessarily $A_L$-invariant.) By Proposition 4.7.11 in [Gos96], there is an isogeny $\phi \to \psi$ defined over $K$ whose kernel is $H$. It is easy to see that $A \subset \text{End}_K(\psi)$, and the reduction of $\psi$ is $\psi_0$, so $\psi$ is the desired CM-lifting of $\psi_0$. 

\[\Box\]
Corollary 18. 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 17.

Proposition 19. 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 $L/F$. By Corollary to Theorem 1 in [Yu95], $A_{\mathfrak{p}}$ is a maximal $A_p$ order, so the conductor $c$ is coprime to $\mathfrak{p}$. The Drinfeld module $\psi_0$ is supersingular if and only if $\mathfrak{p}$ is the only place of $\overline{F}$ over $\mathfrak{p}$; see [Lau96] (2.5.8)]. These two facts imply the first claim. Now assume $r = 2$. Then either $\psi_0$ is supersingular, or $\overline{F}$ is a separable quadratic extension of $F$ and $\mathfrak{p} = \mathfrak{p}\mathfrak{p}'$ splits in $\overline{F}$. In the second case $L = \overline{F}$, and if $f(x) = x^2 - ax + b = 0$ is the minimal polynomial of $\pi$ over $F$, then $a \notin \mathfrak{p}$. Note that $f'(\pi) = 2\pi - a = \pi - \pi$ is divisible neither by $\mathfrak{p}$ nor $\mathfrak{p}'$, so $A[\pi]$ is maximal at $\mathfrak{p}$; the same then is true for $E = A$.

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 14. This proves Theorem 6 in the introduction.

Acknowledgments. 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. Moreover, they thank Florian Breuer, Chris Hall and Lenny Taelman for useful conversations on material related to Theorem 4.

References

[Abh94] Shreeram S. Abhyankar, Nice equations for nice groups, Israel J. Math. 88 (1994), no. 1-3, 1–23.

[Abh01] Shreeram S. Abhyankar, Resolution of singularities and modular Galois theory, Bull. Amer. Math. Soc. (N.S.) 38 (2001), no. 2, 131–169.

[Bro92] Martin Brown, Singular moduli and supersingular moduli of Drinfeld modules, Invent. Math. 110 (1992), no. 2, 419–439.

[CCO13] Ching-Li Chai, Brian Conrad, and Frans Oort, CM-liftings, available at http://math.stanford.edu/~conrad/, 2013.

[CD04] Alina Carmen Cojocaru and William Duke, Reductions of an elliptic curve and their Tate-Shafarevich groups, Math. Ann. 329 (2004), no. 3, 513–534.

[CD08] Alina Carmen Cojocaru and Chantal David, Frobenius fields for Drinfeld modules of rank 2, Compositio Math. 144 (2008), no. 4, 827–848.

[CM04] Alina Carmen Cojocaru and M. Ram Murty, Cyclicity of elliptic curves modulo $p$ and elliptic curve analogues of Linnik’s problem, Math. Ann. 330 (2004), no. 3, 601–625.
[CS13] Alina Carmen Cojocaru and Andrew Michael Shulman, *Elementary divisors of Drinfeld modules of arbitrary rank*, arXiv:1304.2100, 2013.

[Dav95] Chantal David, *Supersingular reduction of Drinfeld modules*, Duke Math. J. **78** (1995), no. 2, 399–412.

[Dav01] Chantal David, *Frobenius distributions of Drinfeld modules of any rank*, J. Number Theory **90** (2001), no. 2, 329–340.

[Dri74] Vladimir Drinfeld, *Elliptic modules*, Mat. Sb. (N.S.) **94** (1974), 594–627.

[DT02] William Duke and Árpád Tóth, *The splitting of primes in division fields of elliptic curves*, Experiment. Math. **11** (2002), no. 4, 555–565.

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

[Gek91] Ernst-Ulrich Gekeler, *On finite Drinfeld modules*, J. Algebra **141** (1991), no. 1, 187–203.

[Gek08] Ernst-Ulrich Gekeler, *Frobenius distributions of Drinfeld modules over finite fields*, Trans. Amer. Math. Soc. **360** (2008), no. 4, 1695–1721.

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

[Hay79] David R. Hayes, *Explicit class field theory in global function fields*, Studies in algebra and number theory, Adv. in Math. Suppl. Stud., vol. 6, Academic Press, New York, 1979, pp. 173–217.

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

[HY00] Liang-Chung Hsia and Jing Yu, *On characteristic polynomials of geometric Frobenius associated to Drinfeld modules*, Compositio Math. **122** (2000), no. 3, 261–280.

[KL09] Wentang Kuo and Yu-Ru Liu, *Cyclicity of finite Drinfeld modules*, J. Lond. Math. Soc. (2) **80** (2009), no. 3, 567–584.

[KMS94] Vijaya Kumar Murty and John Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 6, 523–528.

[Lau96] Gérard Laumon, *Cohomology of Drinfeld modular varieties. Part I*, Cambridge Studies in Advanced Mathematics, vol. 41, Cambridge University Press, Cambridge, 1996, Geometry, counting of points and local harmonic analysis.

[Leh09] Thomas Lehmkühl, *Compactification of the Drinfeld modular surfaces*, Mem. Amer. Math. Soc. **197** (2009), no. 921, xii+94.

[Oor92] Frans Oort, *CM-liftings of abelian varieties*, J. Algebraic Geom. **1** (1992), no. 1, 131–146.

[Poo98] Bjorn Poonen, *Drinfeld modules with no supersingular primes*, Internat. Math. Res. Notices (1998), no. 3, 151–159.

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

[Rei03] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press Oxford University Press, Oxford, 2003, Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[Shi66] Goro Shimura, *A reciprocity law in non-solvable extensions*, J. Reine Angew. Math. **221** (1966), 209–220.

[Tak82] Toyofumi Takahashi, *Good reduction of elliptic modules*, J. Math. Soc. Japan **34** (1982), no. 3, 475–487.

[Yu95] Jin-Kang Yu, *Isogenies of Drinfeld modules over finite fields*, J. Number Theory **54** (1995), no. 1, 161–171.

[Yu03] Jin-Kang Yu, *A Sato-Tate law for Drinfeld modules*, Compositio Math. **138** (2003), no. 2, 189–197.

[Zyw11a] David Zywina, *Drinfeld modules with maximal Galois action on their torsion points*, arXiv:1110.4365, 2011.

[Zyw11b] David Zywina, *The Sato-Tate law for Drinfeld modules*, arXiv:1110.4098, 2011.

(Alina Carmen Cojocaru)
- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA;
- Institute of Mathematics “Simion Stoilow” of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania

E-mail address, Alina Carmen Cojocaru: cojocaru@uic.edu

(Mihran Papikian)

- Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

E-mail address, Mihran Papikian: papikian@math.psu.edu