*Composito Mathematica* **122:** 261–280, 2000.



# On Characteristic Polynomials of Geometric Frobenius Associated to Drinfeld Modules

LIANG-CHUNG HSIA[1] AND JING YU[2]
[1]*Department of Mathematics, National Central University, Chung-Li, Taiwan, Republic of China. e-mail: hsia@math.ncu.edu.tw*
[2]*Institute of Mathematics, Academia Sinica and NSC Center for Theoretical Sciences, Taipei, Taiwan, Republic of China. e-mail: yu@math.sinica.edu.tw*

(Received: 16 June 1998; accepted in final form: 19 March 1999)

**Abstract.** Let $K$ be a function field over finite field $\mathbb{F}_q$ and let $\mathbb{A}$ be a ring consisting of elements of $K$ regular away from a fixed place $\infty$ of $K$. Let $\phi$ be a Drinfeld $\mathbb{A}$-module defined over an $\mathbb{A}$-field $L$. In the case where $L$ is a finite $\mathbb{A}$-field, we study the characteristic polynomial $P_\phi(X)$ of the geometric Frobenius. A formula for the sign of the constant term of $P_\phi(X)$ in terms of 'leading coefficient' of $\phi$ is given. General formula to determine signs of other coefficients of $P_\phi(X)$ is also derived. In the case where $L$ is a global $\mathbb{A}$-field of generic characteristic, we apply these formulae to compute the Dirichlet density of places where the Frobenius traces have the maximal possible degree permitted by the 'Riemann hypothesis'..

**Mathematics Subject Classifications (2000):** 11Gxx, 11Rxx, 11Txx.

**Key words:** Drinfeld module, geometric Frobenius, sign function, characteristic polynomial, power residue symbol, Tate module, endomorphism ring, Dirichlet density.

## 1. Introduction

Let $\mathcal{C}$ be a smooth, projective, geometrically connected curve over a fixed finite field $\mathbb{F}_q$. Fix a closed point $\infty \in \mathcal{C}$ whose residue field is denoted by $\mathbb{F}_{q_\infty}$ and let $\mathbb{A}$ be the ring of functions on $\mathcal{C}$ regular away from $\infty$. In the fundamental paper [2], Drinfeld introduces the objects now called *Drinfeld $\mathbb{A}$-modules*. In many ways, these objects play the role of elliptic curves. In particular, Drinfeld $\mathbb{F}_q[T]$-modules over $\mathbb{F}_q(T)$ are the analogues of elliptic curves over $\mathbb{Q}$ and Drinfeld $\mathbb{F}_q[T]$-modules over $\mathbb{F}_q[T]/(\mathcal{P})$, where $\mathcal{P}$ is a monic irreducible polynomial in $\mathbb{F}_q[T]$, are the analogues of elliptic curves over finite prime fields.

Given Drinfeld $\mathbb{A}$-module $\phi$ over a finite $\mathbb{A}$-field, its most important invariant is the characteristic polynomial $P_\phi(X)$ of the geometric Frobenius acting on Tate modules. This polynomial is in $\mathbb{A}[X]$, and is an isogeny class invariant. However, unlike the case of elliptic curves, the sign of $P_\phi(0)$ can vary. More precisely, by fixing a sign function, the norm of the Frobenius has a sign depending on $\phi$. We first show in Section 3 that this sign depends only on the 'leading coefficients' of $\phi$. Moreover, there is a simple formula for this sign (Theorem 3.2) in terms of a power residue symbol. In the case of rank 2 Drinfeld $\mathbb{F}_q[T]$-modules, with this formula at hand, the computation of $P_\phi(X)$ is almost as fast as computing the zeta function of an elliptic curve over a finite field.

There is the natural degree function $\deg\colon \mathbb{A}\setminus\{0\}\to\mathbb{Z}$ which is given by $\deg(a) =_{\mathrm{def}} \dim_{\mathbb{F}_q}\mathbb{A}/(a)$ for any nonzero element $a$. According to the 'Riemann hypothesis' for Drinfeld $\mathbb{A}$-modules over finite $\mathbb{A}$-field $L$, the degree of the trace of Frobenius is always less than or equal to $[L:\mathbb{F}_q]/\operatorname{rank}\phi$. This trace of Frobenius is certainly the most interesting coefficient of $P_\phi(X)$. We want to know when this coefficient has degree exactly $[L:\mathbb{F}_q]/\operatorname{rank}\phi$. This is answered in Section 4 and the answer also depends only on the 'leading coefficients' of $\phi$. Moreover, in the case where the trace of Frobenius has its degree equal to $[L:\mathbb{F}_q]/\operatorname{rank}\phi$, the sign of this trace can be computed from the 'leading coefficients' of $\phi$. For the other coefficients of $P_\phi(X)$, similar results can be derived just as well. An explanation for this phenomenon is as follows. In the case where $r=\operatorname{rank}\phi$ divides $n=[L:\mathbb{F}_{q_\infty}]$, the 'leading coefficients' of $\phi$ give rise to yet another action of the Frobenius. This Frobenius action on $\mathbb{F}_{q_\infty^r}$ is identified as a scalar multiplication by $\delta^{-1}\in\mathbb{F}_{q_\infty^r}^*$, with $\delta$ explicitly given in terms of the 'leading coefficients' of $\phi$. It turns out that the characteristic polynomial of $\delta^{-1}$ is essentially the sign of the characteristic polynomial $P_\phi(X)$ (Theorem 4.6).

Let $\phi$ be a Drinfeld $\mathbb{A}$-module over a global $\mathbb{A}$-field $L$ of generic characteristic. For almost all finite places $v$ of $L$, one has Drinfeld $\mathbb{A}$-module $\phi_v$ defined over the finite residue field $L(v)$, hence the characteristic polynomial $P_{\phi,v}(X)\in\mathbb{A}[X]$. We are interested in the set of places $v$ for which the polynomials $P_{\phi,v}(X)$ enjoy certain property. In Section 5 we begin by deducing that the 'leading coefficients' of $\phi$ determine what are the possible signs of $P_{\phi,v}(0)$. All the possible signs of $P_{\phi,v}(0)$ are equally distributed as the finite place $v$ varies. In Section 6 we study the set $\mathcal{T}_\phi$ of places $v$ for which the trace of the Frobenius at $v$ has degree exactly $[L(v):\mathbb{F}_q]/\operatorname{rank}\phi$ and more generally, we also study the set $\mathcal{D}_\phi$ of places $v$ for which all the coefficients of $P_{\phi,v}(X)$ attain their maximal degrees allowed by the 'Riemann Hypothesis' for Drinfeld $\mathbb{A}$-modules. We show in particular that $\mathcal{T}_\phi$ always has a positive density provided that the characteristic of $\mathbb{F}_q$ does not divide $\operatorname{rank}\phi$. On the other hand, in the case where the characteristic of $\mathbb{F}_q$ does indeed divide $\operatorname{rank}\phi$, it may happen that for a given $\phi$ the degree of the trace of Frobenius never equals $[L(v):\mathbb{F}_q]/\operatorname{rank}\phi$ (Theorem 6.1). Finally, in Theorem 6.2, we show that $\mathcal{D}_\phi$ has positive density provided the characteristic of $\mathbb{F}_q$ is greater than $\operatorname{rank}\phi$.

## 2. Preliminaries and Notations

We first fix some notations that will be used throughout this paper. Let $\mathcal{C}$ be a smooth, projective, geometrically connected curve over a fixed finite field $\mathbb{F}_q$. Let $K$ be its function field over $\mathbb{F}_q$. Fix a closed point $\infty\in\mathcal{C}$ and let $\mathbb{A}$ be the ring of elements of $K$ regular outside $\infty$. In the sequel, we'll denote the degree of $\infty$ by $d_\infty$ and the normalized valuation on $K_\infty^*$ by $v_\infty$ so that we have

$v_\infty(x) = -\deg(x)/d_\infty$ for all $x \in K_\infty^*$. The natural degree function on $\mathbb{A}$ is extended to any nonzero ideal $\mathfrak{a}$ of $\mathbb{A}$ by setting $\deg(\mathfrak{a}) = \dim_{\mathbb{F}_q} \mathbb{A}/\mathfrak{a}$. We shall use notation $|\mathfrak{a}| \stackrel{\text{def}}{=} q^{\deg(\mathfrak{a})}$ to denote the absolute norm of $\mathfrak{a}$. Set

$$\tau \stackrel{\text{def}}{=} (x \mapsto x^q) \in \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_a)$$

the Frobenius endomorphism of $\mathbb{G}_a$ over $\mathbb{F}_q$.

Let $E$ be any global function field over finite fields together with a distinguished closed point $\infty_E$. Let $E_\infty$ denote the completion of $E$ at the place corresponding to $\infty_E$ and $E(\infty)$ the residue field of $E_\infty$. Recall the definition of sign function [9, Section 4] for the pair $(E, \infty_E)$

DEFINITION 1. A sign function on $E_\infty$ is a homomorphism $\mathrm{sgn} : E_\infty^* \to E(\infty)^*$ which is the identity on $E(\infty)^*$. In addition, sgn is extended to $E_\infty$ by setting $\mathrm{sgn}(0) = 0$. Let $\sigma$ be an $\mathbb{F}_q$-automorphism of $E(\infty)$. The composite map $\sigma \circ \mathrm{sgn}$ is called a twisted sign function of sgn by $\sigma$.

We shall fix a sign function $\mathrm{sgn} : K_\infty \to K(\infty)$ throughout this paper. Then sgn is defined on $K$ via the canonical embedding $K \hookrightarrow K_\infty$. An element $a \in K_\infty$ is said to be *monic* if $\mathrm{sgn}(a) = 1$. For any prime ideal $\mathfrak{p}$ of $\mathbb{A}$ and any element $a \in \mathbb{A} \setminus \mathfrak{p}$ we define the $(q-1)$th power residue symbol to be the unique element $\{a/\mathfrak{p}\} \in \mathbb{F}_q^*$ such that

$$\left\{\frac{a}{\mathfrak{p}}\right\} \equiv a^{\frac{|\mathfrak{p}|-1}{q-1}} \pmod{\mathfrak{p}}.$$

The definition of the power residue symbol is extended in the usual way to $\{b/\mathfrak{a}\}$ for any ideal $\mathfrak{a}$ of $\mathbb{A}$ and any $b \in \mathbb{A}$ which is relatively prime to $\mathfrak{a}$. If $\mathfrak{a} = (a)$ is principal we simply write $\{b/a\}$ instead of $\{b/\mathfrak{a}\}$. We recall the following reciprocity law for $(q-1)$th power residues.

THEOREM 2.1 ([12, Chap. IV, Theorem 9.3 and Chap. III, Theorem 5.4]). *Suppose $a, b \in \mathbb{A}$ are nonzero relatively prime elements. Put $\alpha = v_\infty(a)$ and $\beta = v_\infty(b)$, then we have*

$$\left\{\frac{a}{b}\right\}\left\{\frac{b}{a}\right\}^{-1} = \mathrm{sgn}\left[(-1)^{\alpha\beta}\frac{b^\alpha}{a^\beta}\right]^{(q_\infty-1)/(q-1)}$$

*where $q_\infty = q^{d_\infty}$ denotes the cardinality of $K(\infty)$.*

Let $L$ be an $\mathbb{A}$-field, that is, $L$ together with a ring homomorphism $\iota : \mathbb{A} \to L$. Then the kernel $\ker(\iota)$, called the *characteristic* of $L$, is either the zero ideal or a nontrivial prime ideal $\mathfrak{p}$ of $\mathbb{A}$. In the former case, $L$ is said to be of *generic characteristic* and the latter case, $L$ is of *characteristic* $\mathfrak{p}$. Denote by $L\{\tau\}$ the twisted polynomial ring which is generated by $L$ and $\tau$ as a subalgebra of all $L$-endomorphism of the additive group scheme $\mathbb{G}_a/L$. A Drinfeld $\mathbb{A}$-module over $L$ of rank $r \geqslant 1$ is a ring homomorphism

$$\phi : \mathbb{A} \to L\{\tau\} \subset \mathrm{End}_L(\mathbb{G}_a),$$

$$a \mapsto \phi_a$$

such that $\phi \neq \iota$ together with the following two conditions:

(i) $\deg_\tau \phi_a = r \cdot \deg(a)$,
(ii) the coefficient of $\tau^0$ in $\phi_a$ is $\iota(a)$.

To ease the notations, we'll simply write $a$ instead of $\iota(a)$ to denote the image in $L$ if there is no danger of confusion.

In the sequel we assume that there exist rank $r$ Drinfeld $\mathbb{A}$-modules defined over $L$ and fix such a rank $r$ Drinfeld $\mathbb{A}$-module $\phi$. Then, $L$ contains a subfield $\mathbb{F}_{q_\infty}$ which is isomorphic to $K(\infty)$ (see for example, [8, pp. 199, Remark 7.2.13]). For $a \in \mathbb{A}$, $\phi_a$ has the following form

$$\phi_a = a\tau^0 + g_{a,1}\tau + \cdots + g_{a,l-1}\tau^{l-1} + \Delta_a\tau^l, \tag{1}$$

where $g_{a,i} \in L$, $\Delta_a \in L^*$ and $l = r \cdot \deg(a)$. Let $\overline{L}$ denotes an algebraic closure of $L$. For any $x \in \mathbb{G}_a(\overline{L})$ we let $\phi_a(x)$ denote the image of $x$ under the morphism $\phi_a$. The $a$-torsion, denoted by $\phi[a]$, is the set of $x \in \mathbb{G}_a(\overline{L})$ such that $\phi_a(x) = 0$. By definition, $\phi[a]$ is the set of roots of the polynomial

$$\phi_a(X) = \Delta_a X^{q^l} + g_{a,l-1}X^{q^{l-1}} + \cdots + g_{a,1}X^q + aX.$$

Note that the $a$-torsion forms an $\mathbb{F}_q$-vector space of dimension $r \cdot \deg(a)$. Put $\phi[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \phi[a]$ for any ideal $\mathfrak{a}$ of $\mathbb{A}$ which is prime to the characteristic $\mathfrak{p}$. For any prime ideal $\mathfrak{q}$ which is different from $\mathfrak{p}$, the Tate module is defined by

$$T_{\mathfrak{q}}(\phi) = \varprojlim_{\ell} \phi[\mathfrak{q}^\ell].$$

The Tate module $T_{\mathfrak{q}}(\phi)$ gives rise to a $\mathfrak{q}$-adic representation of the ring $\mathrm{End}(\phi)$ consisting of endomorphisms of $\phi$. In the case that $L$ is a finite $\mathbb{A}$-field, we'll denote the degree of $L$ over $\mathbb{F}_{q_\infty}$ by $n$ and put $n_\infty = d_\infty n$. Moreover, $L$ must be of characteristic $\mathfrak{p}$ for some nonzero prime ideal $\mathfrak{p}$. Assume $\mathfrak{p}$ is of degree $d$ and $L$ is a finite extension of degree $m$ of $\mathbb{F}_{\mathfrak{p}} \overset{\mathrm{def}}{=} \mathbb{A}/\mathfrak{p}$. Denote by $\mathrm{Frob}_L := \tau^{n_\infty}$ the geometric Frobenius of $\mathbb{G}_a$ over $L$ which is certainly in $\mathrm{End}(\phi)$. Let $P_\phi(X)$ be the characteristic polynomial associated to $\mathrm{Frob}_L$ via the $\mathfrak{q}$-adic representation. Then $P_\phi(X)$ is a monic polynomial of degree $r$ with coefficients in $\mathbb{A}$ which is independent of $\mathfrak{q}$. Writing the characteristic polynomial as

$$P_\phi(X) = X^r - a_1X^{r-1} + \cdots + (-1)^r a_r, \quad a_i \in \mathbb{A}, \tag{2}$$

$P_\phi(X)$ is an isogeny class invariant and the constant term $P_\phi(0)$ has the property that

$\big(P_\phi(0)\big) = \mathfrak{p}^m$. That is, $\mathfrak{p}^m$ is principal and $P_\phi(0)$ is a generator of $\mathfrak{p}^m$ (see [4, Section 3, Section 5] for details). The goal in the next section is to determine the sign $\mathrm{sgn}(a_r)$ of the constant of $P_\phi(X)$.

## 3. Determining the Sign $\mathrm{sgn}(a_r)$

In this section, we consider the case that $L = \mathbb{F}_{q_\infty^n}$, a finite $\mathbb{A}$-field of characteristic $\mathfrak{p}$. We would like to compute the sign of the constant term of the characteristic polynomial $P_\phi(X)$. First we have the following formula connecting $\mathrm{sgn}(a_r)$ to non-constant element $b \in \mathbb{A}$.

THEOREM 3.1. *Let $L$ be an $\mathbb{A}$-field of characteristic $\mathfrak{p}$ and of degree $n$ over $\mathbb{F}_{q_\infty}$. Let $\phi$ be a rank $r$ Drinfeld $\mathbb{A}$-module over $L$. Suppose $b \in \mathbb{A}$ is a non-constant element which is relatively prime to $\mathfrak{p}$ then*

$$\mathbf{N}_{\mathbb{F}_q}^{K(\infty)}(\mathrm{sgn}(a_r))^{-v_\infty(b)} = \mathbf{N}_{\mathbb{F}_q}^{L}\left((-1)^{(r+1)\deg(b)}\frac{\mathrm{sgn}(b)}{\Delta_b}\right)$$

*where $\mathbf{N}_{\mathbb{F}_q}^{L}$ ($\mathbf{N}_{\mathbb{F}_q}^{K(\infty)}$) is the norm map from $L$ ($K(\infty)$, respectively) to $\mathbb{F}_q$.*

*Proof.* Since $b$ is relatively prime to $\mathfrak{p}$ and the Drinfeld $\mathbb{A}$-module $\phi$ is of rank $r$, it follows that the $b$-torsion is a free $\mathbb{A}/(b)$-module of rank $r$. Moreover, $\phi$ is defined over $L$, the action of $\mathrm{Frob}_L$ commutes with the $\mathbb{A}$-action. Therefore $\mathrm{Frob}_L$ gives rise to a $\mathbb{A}/(b)$-linear automorphism of $\phi[b]$. The characteristic polynomial is just $P_\phi(X) \bmod (b)$. Thus the determinant of $\mathrm{Frob}_L$, as an $\mathbb{A}/(b)$-linear automorphism on $\phi[b]$, is $a_r \bmod (b)$.

On the other hand, $\phi[b]$ is a $\mathbb{F}_q$-vector space of dimension $r\deg(b)$ and $\mathrm{Frob}_L$ is also a $\mathbb{F}_q$-linear automorphism of the $\mathbb{F}_q$-vector space $\phi[b]$. Note that the action of $\mathrm{Frob}_L$ as a $\mathbb{F}_q$-linear automorphism is compatible with that of $\mathbb{A}/(b)$-linear action since the $\mathbb{F}_q$-linear action arises from the canonical embedding $\mathbb{F}_q \hookrightarrow \mathbb{A}/(b)$. The determinant of $\mathrm{Frob}_L$, as $\mathbb{F}_q$-linear automorphism, is therefore $\mathbf{N}[a_r \bmod (b)]$ where $\mathbf{N}(\cdot)$ is the norm from the $\mathbb{F}_q$-algebra $\mathbb{A}/(b)$ down to $\mathbb{F}_q$. We have

$$\mathbf{N}[a_r \bmod (b)] = \left\{\frac{a_r}{b}\right\}. \tag{3}$$

To see this, observe that both sides are multiplicative in $b$ by Chinese Remainder Theorem and the definition of the power residue symbol. One simply needs to check the case that the algebra is $\mathbb{A}/\mathfrak{q}^e$ with prime ideal $\mathfrak{q} \neq \mathfrak{p}$. Put $V_i = \mathfrak{q}^i/\mathfrak{q}^e$, $0 \leqslant i \leqslant e-1$ which are $\mathbb{F}_q$-vector subspaces of $V_0 = \mathbb{A}/\mathfrak{q}^e$. Observe that the multiplication by $a_r$ on $V_i$ gives rise to an $\mathbb{F}_q$-automorphism of $V_i$. The $\mathbb{F}_q$-vector space $\mathbb{A}/\mathfrak{q}^e$ has the following filtration of subspaces.

$$\mathbb{A}/\mathfrak{q}^e = V_0 \supset V_1 \supset \cdots \supset V_{e-1}.$$

Note that (3) is true for the case $e = 1$ and $V_i/V_{i+1}$ is of rank one as an $\mathbb{A}/\mathfrak{q}$-module for $0 \leqslant i \leqslant e-1$. Now (3) follows by induction on $e$.

https://doi.org/10.1023/A:1002015330987 Published online by Cambridge University Press

To obtain the result, we compute det(Frob$_L$) in another way. First, as $\phi_b \in L\{\tau\}$ is given by (1), we may write

$$\phi_b = \Delta_b \left\{ \tau^l + \frac{g_{b,l-1}}{\Delta_b}\tau^{l-1} + \cdots + \frac{g_{b,1}}{\Delta_b}\tau + \frac{b}{\Delta_b}\tau^0 \right\}, \qquad l = r \cdot \deg(b).$$

By [8, Proposition 1.3.5], the polynomial $\Delta_b^{-1}\phi_b$ has a decomposition into product of linear factors in $\overline{L}\{\tau\}$. That is, there exist $u_l, u_{l-1}, \cdots, u_1 \in \overline{L}$ such that

$$\phi_b = \Delta_b(\tau - u_l\,\tau^0)\cdots(\tau - u_1\,\tau^0)$$

with $u_l\,u_{l-1}\cdots u_1 = (-1)^l b/\Delta_b$. The $\mathbb{F}_q$-vector space $\phi[b]$ is, by definition, $\ker(\Delta_b^{-1}\phi_b)$. We choose a basis $\{w_1, w_2, \cdots, w_l\}$ to be solutions of the following system of equations:

$$\begin{aligned} &(\tau - u_i\,\tau^0)\,w_i = w_{i+1} \quad \text{if } 1 \leqslant i \leqslant l-1, \\ &(\tau - u_l\,\tau^0)\,w_l = 0. \end{aligned} \tag{4}$$

Set $A$ to be the column vector $[w_1, w_2, \cdots, w_l]^t$. Then the above equation can be expressed as $\tau A = MA$ where $M$ is a $l \times l$ matrix with entries in $\overline{L}$. In fact,

$$M = \begin{pmatrix} u_1 & 1 & 0 & & 0 \\ 0 & u_2 & 1 & & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & u_{l-1} & 1 \\ 0 & 0 & \ldots & \ldots & u_l \end{pmatrix}.$$

Since Frob$_L = \tau^n$, by iterating the relations, we have

$$\text{Frob}_L A = M^{(n-1)}\,M^{(n-2)}\cdots M^{(1)}\,MA$$

where $M^{(i)}$ means to raise the entries of $M$ to the $q^i$th power. Thus, as a $\mathbb{F}_q$-linear transformation, Frob$_L$ is given by the matrix $M^{(n-1)}\,M^{(n-2)}\cdots M^{(1)}\,M$. Now,

$$\det(M) = u_l\,u_{l-1}\cdots u_1 = (-1)^l\,\frac{b}{\Delta_b}.$$

As a result

$$\det(\text{Frob}_L) = \left((-1)^l\,\frac{b}{\Delta_b}\right)^{q^{(n-1)}+\cdots+q+1} = \mathbf{N}^L_{\mathbb{F}_q}\left((-1)^l\,\frac{b}{\Delta_b}\right).$$

Since $b \in \mathbb{F}_{\mathfrak{p}}$ and $L$ is of degree $m$ over $\mathbb{F}_{\mathfrak{p}}$, we have that $\mathbf{N}^L_{\mathbb{F}_q}(b) = \{b/\mathfrak{p}\}^m$. Also, $\mathfrak{p}^m = (a_r)$ by [4, Thm. 5.1 (ii)] and by the definition of power residue symbol, $\{b/\mathfrak{p}\}^m = \{b/a_r\}$. Consequently,

$$\det(\text{Frob}_L) = \left\{\frac{b}{a_r}\right\}\mathbf{N}^L_{\mathbb{F}_q}((-1)^l\Delta_b)^{-1}.$$

Combining with identity (3), we obtain the following

$$\left\{\frac{a_r}{b}\right\} = \left\{\frac{b}{a_r}\right\} \mathbf{N}^L_{\mathbb{F}_q}((-1)^l \Delta_b)^{-1}. \tag{5}$$

It follows by the reciprocity law of power residue–Theorem 2.1 that,

$$\begin{aligned}\mathbf{N}^L_{\mathbb{F}_q}((-1)^l \Delta_b)^{-1} &= \left\{\frac{a_r}{b}\right\}\left\{\frac{b}{a_r}\right\}^{-1} \\ &= \operatorname{sgn}\left[(-1)^{v_\infty(a_r)v_\infty(b)} \frac{b^{v_\infty(a_r)}}{a_r^{v_\infty(b)}}\right]^{(q_\infty-1)/(q-1)} \\ &= (-1)^{\deg(a_r)\deg(b)} \mathbf{N}^{K(\infty)}_{\mathbb{F}_q}(\operatorname{sgn}(a_r))^{-v_\infty(b)} \mathbf{N}^{K(\infty)}_{\mathbb{F}_q}(\operatorname{sgn}(b))^{v_\infty(a_r)}.\end{aligned}$$

Note that $l = r \cdot \deg(b)$ and $-v_\infty(a_r) = n = [L : K(\infty)]$. Simplifying the formulae above, we obtain

$$\mathbf{N}^{K(\infty)}_{\mathbb{F}_q}(\operatorname{sgn}(a_r))^{-v_\infty(b)} = \mathbf{N}^L_{\mathbb{F}_q}\left((-1)^{(r+1)\deg(b)} \frac{\operatorname{sgn}(b)}{\Delta_b}\right).$$

This completes the proof. □

*Remark 1.* Note that by Riemann–Roch Theorem, for sufficiently large integer $N$, there exist elements $b$, $b' \in \mathbb{A}$ which are prime to $\mathfrak{p}$ such that $v_\infty(b) = -N$ and $v_\infty(b') = -N - 1$. We choose $b, b'$ so that $b/b' = \pi_\infty$ is a uniformizer of $K_\infty$ such that $\operatorname{sgn}(\pi_\infty) = 1$. Set $\Delta^* = \Delta_b^{-1} \cdot \Delta_{b'}$, then

$$\mathbf{N}^{K(\infty)}_{\mathbb{F}_q}(\operatorname{sgn}(a_r)) = \mathbf{N}^L_{\mathbb{F}_q}((-1)^{(r+1)d_\infty} \Delta^*)^{-1}. \tag{6}$$

In most applications, the closed point $\infty$ is rational over $\mathbb{F}_q$. In this case, we have $d_\infty = 1$, then Theorem 3.1 and (6) have simpler forms.

THEOREM 3.2. *Assume that $\infty$ is a rational closed point of $\mathcal{C}$.*

(1) *We have* $\operatorname{sgn}(a_r)^{\deg(b)} = \mathbf{N}^L_{\mathbb{F}_q}\left((-1)^{(r+1)\deg(b)} \Delta_b\right)^{-1}$ *for every nonconstant monic element $b \in \mathbb{A}$.*
(2) *Let $b, b' \in \mathbb{A}$ be monic elements such that are prime to $\mathfrak{p}$ and* $(\deg(b), \deg(b') = 1$. *Let $i, i' \in \mathbb{Z}$ be integers such that* $i \deg(b) + i' \deg(b') = 1$. *Put* $\Delta^* = \Delta_b^i \cdot \Delta_{b'}^{i'}$ *then* $\operatorname{sgn}(a_r) = \mathbf{N}^L_{\mathbb{F}_q}((-1)^{r+1} \Delta^*)^{-1}$.

*Remark 2.* In Theorem 3.2, since $(\deg(b), \deg(b')) = 1$, we have $(|b|^r - 1, |b'|^r - 1) = q^r - 1$. Let $j, j'$ be integers such that $j(|b|^r - 1) + j'(|b'|^r - 1) = q^r - 1$. Put

https://doi.org/10.1023/A:1002015330987 Published online by Cambridge University Press

$\Delta = \Delta_b^j \Delta_{b'}^{j'}$ then the following formula holds also.

$$\mathrm{sgn}(a_r) = \mathbf{N}_{\mathbb{F}_q}^{L}((-1)^{r+1}\,\Delta)^{-1} \tag{7}$$

EXAMPLE 1. We apply Theorem 3.2 to the case that $\mathbb{A} = \mathbb{F}_q[T]$ and $L = \mathbb{F}_{\mathcal{P}} = \mathbb{F}_q[T]/(\mathcal{P})$ where $\mathcal{P}$ is a degree $d$ monic irreducible polynomial in $\mathbb{F}_q[T]$. Assume that the Drinfeld $\mathbb{A}$-module $\phi$ is defined over $K$ which is given by

$$\phi_T = T\tau^0 + g_1\tau + \cdots + g_{r-1}\tau^{r-1} + \Delta\tau^r$$

with $T, g_1, \cdots, \Delta \in \mathbb{A}$ and suppose that $\Delta \in \mathbb{A} \setminus (\mathcal{P})$. Let $\overline{\phi}$ denote the reduction of $\phi$ modulo $\mathcal{P}$ so that

$$\overline{\phi}_T = \overline{T}\tau^0 + \overline{g}_1\tau + \cdots + \overline{g}_{r-1}\tau^{r-1} + \overline{\Delta}\tau^r$$

where the bar denotes the reduction modulo $\mathcal{P}$. Consider the characteristic polynomial of the geometric Frobenius associated to $\overline{\phi}$ as a Drinfeld $\mathbb{A}$-module over $L$. We may assume that $\mathcal{P} \neq T$. In this case, letting $a = T$ and $a' = 1$ in Theorem 3.2 we have the following very simple formula

$$\mathrm{sgn}(a_{r,\phi}) = (-1)^{d(r+1)} \left\{\frac{\Delta}{\mathcal{P}}\right\}^{-1}. \tag{8}$$

*Remark 3.* Suppose $\phi$ is a rank 2 Drinfeld $\mathbb{F}_q[T]$-module defined over the prime $\mathbb{A}$-field $\mathbb{F}_{\mathcal{P}}$ as in the above example (see [4, Section 5]). Then the characteristic polynomial of $\phi$ can be shown easily to be

$$P_\phi(X) = X^2 - (-1)^{\deg\mathcal{P}} \left\{\frac{\Delta}{\mathcal{P}}\right\}^{-1} H(\phi)\ X + (-1)^{\deg\mathcal{P}} \left\{\frac{\Delta}{\mathcal{P}}\right\}^{-1} \mathcal{P},$$

where $H(\phi)$ is the Hasse invariant of the Drinfeld module $\phi$, identified as a polynomial in $\mathbb{F}_q[\mathbb{T}]$ with degree less than $\deg\mathcal{P}$. Recall that $H(\phi)$ is actually the coefficient of $\tau^{\deg\mathcal{P}}$ in $\phi_{\mathcal{P}}$. It follows that the invariants $P_\phi(X)$ (hence also the Euler–Poincaré characteristic of the finite $\mathbb{F}_q[T]$-module $\phi(\mathbb{F}_{\mathcal{P}})$) can be efficiently computed.

## 4. Sign of the Trace

We retain assumptions and notations from Section 3. Let $L(\tau)$ be the division ring of fractions of $L\{\tau\}$. The Drinfeld $\mathbb{A}$-module $\phi : \mathbb{A} \to L\{\tau\}$ is regarded as an embedding so that $\phi$ extends to an embedding of $K$ into $L(\tau)$. We identify $K$ with its image as a subfield contained in $L(\tau)$. In the following, the notation $\deg_\tau(a)$ denotes the degree in $\tau$ for $a \in \mathbb{A}$. The identity $\deg_\tau(a) = r \cdot \deg(a)$ holds. Let $K(F)$ be the extension of $K$ generated by $F := \mathrm{Frob}_L$. Note that $\mathrm{Frob}_L$ commutes with $\mathbb{A}$-action. It follows that $K(F)/K$ is a field extension. Recall the following basic facts about $K(F)$ and $\mathrm{End}_L(\phi)$ from [3, 4, 13]:

https://doi.org/10.1023/A:1002015330987 Published online by Cambridge University Press

THEOREM 4.1. (1) $\mathrm{End}_L(\phi)\otimes_{\mathbb{A}} K$ *is a central division algebra over* $K(F)$ *and* $\dim_{K(F)}\mathrm{End}_L(\phi)\otimes_{\mathbb{A}} K=(r')^2$ *where* $r'=r/[K(F):K]$ *is an integer.*

(2) *There is only one place* $\infty'$ *of* $K(F)$ *that is above* $\infty$ *corresponding to the pole of* $F$. *Let* $K(F)_\infty$ *denote the completion of* $K(F)$ *at the place* $\infty'$. *Then* $K(F)_\infty=K(F)\otimes K_\infty$ *and* $[K(F):K]=[K(F)_\infty:K_\infty]=ef$ *where* $e,f$ *are the ramification index and residue degree of* $K(F)_\infty/K_\infty$ *respectively.*

(3) *Let* $M_\phi(X)$ *be the minimal polynomial of* $F$ *over* $K$ *then the characteristic polynomial* $P_\phi$ *of* $F$ *acting on Tate modules is related to* $M_\phi(X)$ *by the identity* $P_\phi(X)=M_\phi(X)^{r'}$.

(4) *The valuation* $v_\infty$ *at the infinite place has an extension which we still use the same notation* $v_\infty:K(F)^*\to\mathbb{Q}$ *so that* $v_\infty(F)=-n/r$. *Moreover, all roots of* $P_\phi(X)$ *have the same valuation* $-n/r$.

Write

$$P_\phi(X)=X^r-a_1X^{r-1}+\cdots+(-1)^r a_r,\quad a_i\in\mathbb{A}.$$

It follows from Theorem 4.1 (4) that the coefficients $a_i$ of $P_\phi(X)$ have valuation $v_\infty(a_i)\geqslant -in/r$. Define the function

$$\omega(a_i)=\begin{cases}\mathrm{sgn}(a_i) & \text{if } v_\infty(a_i)=-i\,n/r,\\ 0 & \text{otherwise.}\end{cases}\tag{9}$$

Note $\omega(a_i)$ is necessarily 0 if $i\cdot n$ is not divisible by $r$.

Let $E$ be a maximal commutative field in $\mathrm{End}_L(\phi)\otimes_{\mathbb{A}}K$ containing $K(F)$. Then, $E$ is of degree $r'[K(F):K]=r$ over $K$. It follows from the proof of [13, Theorem 1] that assertions (2), (3) and (4) of Theorem 4.1 remain valid with $K(F)$ replaced by $E$. We'll denote by $\infty_E$ the unique place of $E$ that lies above $\infty$ and $E_\infty$ the completion of $E$ at the place $\infty_E$. We fix an extension of $v_\infty$ to $E^*$ and denote this extension by $v_\infty$ again so that $v_\infty(F)=-n/r$. Note that in this case, we have $ef=r$. In the remainder of this section, $e,f$ are reserved to denote the ramification index and the residue degree of $E_\infty$ over $K_\infty$. Therefore, the residue field $E(\infty)\simeq\mathbb{F}_{q_\infty^f}$. We use the notation $|B|=q_\infty^{-v_\infty(B)}$ to denote the absolute value of $B\in E_\infty$. Put $\mathbb{A}_E=E\cap\mathrm{End}_L(\phi)$. Since $E\subset\mathrm{End}_L(\phi)\otimes_{\mathbb{A}}K$, for any $B\in E$ there exists an $a\in\mathbb{A}$ such that $aB\in\mathrm{End}_L(\phi)$. It follows that $E$ is the quotient field of $\mathbb{A}_E$.

Let $E_\infty^*$ act on $\bar{L}^*$ in the following way

$$x\cdot\xi=\xi^{|x|^r},\quad \text{for } \xi\in\overline{L}^* \text{ and } x\in E_\infty^*.$$

If $|x|^r<1$, then $\xi^{|x|^r}$ means the unique element $\lambda\in\bar{L}^*$ such that $\lambda^{1/|x|^r}=\xi$. For any nonzero element $x\in\mathbb{A}_E\subset L\{\tau\}$, let $\Delta_x\in L^*$ be the leading coefficient of $x$ in $\tau$. The leading coefficient map $\mu_\phi:\mathbb{A}_E\setminus\{0\}\to L^*$ defined by $\mu_\phi(x)=\Delta_x$, satisfies the following relation

$$\mu_\phi(xy)=\mu_\phi(x)\mu_\phi(y)^{|x|^r}=(x\cdot\mu_\phi(y))\mu_\phi(x).$$

https://doi.org/10.1023/A:1002015330987 Published online by Cambridge University Press

It is clear that $\mu_\phi$ is a cocycle on the monoid $\mathbb{A}_E \setminus \{0\}$. Let $z = y/x \in E^*$ be any non-zero element with $x, y \in \mathbb{A}_E$. We extend the leading coefficient map $\mu_\phi$ to $E^*$ by setting

$$\mu_\phi(z) \overset{\text{def}}{=} \mu_\phi(zx)\mu_\phi(x)^{-|z|^r} = \mu_\phi(y)\mu_\phi(x)^{-|z|^r}.$$

Note that for any nonzero $x' \in \mathbb{A}_E$,

$$\mu_\phi(zxx')\mu_\phi(xx')^{-|z|^r} = \mu_\phi(zx)\mu_\phi(x')^{|zx|^r}\mu_\phi(x)^{-|z|^r}\mu_\phi(x')^{-|zx|^r}$$

$$= \mu_\phi(zx)\mu_\phi(x)^{-|z|^r}.$$

Let $z = y'/x'$ be another representative of $z$. We have

$$\mu_\phi(zx)\mu_\phi(x)^{-|z|^r} = \mu_\phi(zxx')\mu_\phi(xx')^{-|z|^r} = \mu_\phi(zx')\mu_\phi(x')^{-|z|^r}$$

since $x, x'$ commute. Thus the definition is independent of representatives of $z$. Note that $\mu_\phi$ also extends to a cocycle on $E^*$. Denote by $U_1$ the principal unit group in $E^*_\infty$.

LEMMA 4.2. *For any $u \in E^* \cap U_1$, we have $\mu_\phi(u) = 1$.*

*Proof.* Let $u = y/x \in E^*$ be any 1-unit. By definition, we have

$$\mu_\phi(u) = \mu_\phi(y)\,\mu_\phi(x)^{-1}.$$

As $u$ is a 1-unit, $v_\infty((y-x)/x) = v_\infty(u-1) > 0$. Consequently, $\mu_\phi(x) = \mu_\phi(y)$ and hence $\mu_\phi(u) = 1$. □

As shown by Lemma 4.2, $\mu_\phi$ is continuous with respect to $\infty_E$-adic topology on $E^*$. It has a unique extension to $E^*_\infty$ which we still denote by $\mu_\phi$. Put $\mu_\phi(0) = 0$.

LEMMA 4.3. *The restriction of $\mu_\phi$ on $E(\infty)$ gives an $\mathbb{F}_q$-embedding of fields $E(\infty) \to \bar{L}$.*

*Proof.* (Following [9, Prop. 4.5].)
It suffices to show $\mu_\phi(1-\alpha) = 1 - \mu_\phi(\alpha)$ for all $\alpha \in E(\infty)$. Clearly, we only need to check the identity for $\alpha \neq 0, 1$. By continuity, we may choose unit $z = y/x \in E$ with $x, y \in \mathbb{A}_E$ so that $\mu_\phi(z) = \mu_\phi(\alpha)$ and $\mu_\phi(1-z) = \mu_\phi(1-\alpha)$. Note that $z \notin U_1$, therefore $v_\infty(x-y) = v_\infty(x) = v_\infty(y)$ which implies $\mu_\phi(x-y) = \mu_\phi(x) - \mu_\phi(y)$. Thus, $\mu_\phi(1-z) = 1 - \mu_\phi(z)$. □

We summarize the two properties proved in Lemma 4.2 and 4.3 as follows:

(i) $\mu_\phi$ is a continuous cocycle on $E^*_\infty$, i.e. $\mu_\phi(xy) = \mu_\phi(x)\,\mu_\phi(y)^{|x|^r}$ for all $x, y \in E^*_\infty$ ([8, Prop. 7.2.12.2]),
(ii) the restriction of $\mu_\phi$ to $E(\infty)^*$ is a restriction of an $\mathbb{F}_q$-embedding of fields $E(\infty) \to \bar{L}$, [8, Remark 7.2.13].

https://doi.org/10.1023/A:1002015330987 Published online by Cambridge University Press

By definition, a coboundry $\delta(\xi)$ is determined by element $\xi \in \bar{L}^*$ such that

$$\delta(\xi)_x = (x \cdot \xi)\xi^{-1} = \xi^{|x|^r - 1}$$

for all $x \in E^*_\infty$. It follows directly from the definition that cocycles which are cohomologous to $\mu_\phi$ enjoy the same properties as $\mu_\phi$ does.

Let $\pi_\infty$ be a uniformizer of $K_\infty$ such that $\mathrm{sgn}(\pi_\infty) = 1$. Put $\Delta = \mu_\phi(\pi_\infty^{-1})$ and let us fix any $(q^r_\infty - 1)$-root of $\Delta$, denoted by $\xi_\Delta$. Set $c_\Delta = \mu_\phi/\delta(\xi_\Delta)$. Then $c_\Delta$ is a cocycle on $E^*_\infty$ which is cohomologous to $\mu_\phi$; furthermore, $c_\Delta$ satisfies properties (i) and (ii) above.

PROPOSITION 4.4. *$c_\Delta$ takes values in* $\mathbb{F}^*_{q^r_\infty}$.

*Proof.* Fix a uniformizer $\pi_E$ of $E_\infty$. For any $x \in E^*_\infty$, there exist a $\epsilon_x \in E(\infty)$ and a $w_x \in U_1$ such that $x = \epsilon_x w_x \pi_E^{e\, v_\infty(x)}$. By the cocycle relation,

$$\begin{aligned} c_\Delta(x) &= c_\Delta(\epsilon_x)\, c_\Delta(\pi_E^{e\, v_\infty(x)}) \\ &= c_\Delta(\epsilon_x) c_\Delta(\pi_E)^{(|x|^r - 1)/(|\pi_E|^r - 1)} \end{aligned}$$

Since $c_\Delta$ is an embedding of $E(\infty)$ it follows that $c_\Delta(\epsilon_x) \in E(\infty) \simeq \mathbb{F}_{q^f_\infty}$. Also, note that $|\pi_E|^r - 1$ divides $|x|^r - 1$. It suffices to prove the proposition for $x = \pi_E^{-1}$. We have $\pi_E^{-e} = \epsilon w \pi_\infty^{-1}$ for some $\epsilon \in E(\infty)$ and $w \in U_1$. Then,

$$\begin{aligned} \left(c_\Delta(\pi_E^{-1})\right)^{(|\pi_E^{-1}|^{er} - 1)/(|\pi_E^{-1}|^r - 1)} &= c_\Delta(\pi_E^{-e}) \\ &= c_\Delta(\epsilon) c_\Delta(\pi_\infty^{-1}) \\ &= c_\Delta(\epsilon). \end{aligned}$$

Note that $ef = r$ and $|\pi_E^{-1}|^e = q_\infty$, we have the identity

$$\left(c_\Delta(\pi_E^{-1})\right)^{(q^r_\infty - 1)/(q^f_\infty - 1)} = c_\Delta(\epsilon).$$

Since $c_\Delta(\epsilon) \in E(\infty) \simeq \mathbb{F}_{q^f_\infty}$,

$$\left(c_\Delta(\pi_E^{-1})\right)^{q^r_\infty - 1} = 1.$$

The proposition now follows. □

COROLLARY 4.5. *The restriction $c_\Delta|_{K^*_\infty}$ of the cocycle $c_\Delta$ to $K^*_\infty$ is equal to a twisted sign function of* sgn.

*Proof.* It follows from the fact that $c_\Delta(x)$ is an integer for all $x \in K^*_\infty$ and the cocycle relation, we have $c_\Delta(xy) = c_\Delta(x)\, c_\Delta(y)$ for all $x, y \in K^*_\infty$. Moreover, $c_\Delta$ gives rise to an $\mathbb{F}_q$-automorphism of $K(\infty)$. As a consequence, $c_\Delta$ and $\gamma \circ \mathrm{sgn}$ are identical on the unit group of $K^*_\infty$ for some $\gamma \in \mathrm{Gal}(K(\infty)/\mathbb{F}_q)$. Therefore, $c_\Delta/\gamma \circ \mathrm{sgn}$ factors through $v_\infty : K^*_\infty \to \mathbb{Z}$. There exists a $\lambda \in \mathbb{F}^*_{q^r_\infty}$ such that $c_\Delta(x) = \gamma \circ \mathrm{sgn}(x)\lambda^{v_\infty(x)}$

https://doi.org/10.1023/A:1002015330987 Published online by Cambridge University Press

for all $x \in K_\infty^*$. Let $x = \pi_\infty^{-1}$, then $\lambda^{-1} = c_\Delta(\pi_\infty^{-1}) = 1$. Hence, $c_\Delta$ and $\gamma \circ \mathrm{sgn}$ agree on $K_\infty^*$ and this proves the Corollary. □

We shall fix any such cocycle and we denote it by $\widetilde{\mathrm{sgn}}$. By Theorem 4.5, $\widetilde{\mathrm{sgn}}|_{K_\infty} = \gamma \circ \mathrm{sgn}$ for some $\gamma \in \mathrm{Gal}(K(\infty)/\mathbb{F}_q)$. We now prove the main result of this section.

THEOREM 4.6. *Assume $r \mid n$ and put $\delta = \Delta^{(q_\infty^n - 1)/(q_\infty^r - 1)} \in \mathbb{F}_{q_\infty^r}^*$. Let $\tilde{\omega} = \gamma \circ \omega$. Then, the characteristic polynomial of the scalar multiplication by $\widetilde{\mathrm{sgn}}(F) = \delta^{-1}$ on $\mathbb{F}_{q_\infty^r}$ over $\mathbb{F}_{q_\infty}$ is*

$$\tilde{\omega}(P_\phi(X)) := X^r - \tilde{\omega}(a_1)\, X^{r-1} + \cdots + (-1)^{r-1}\tilde{\omega}(a_{r-1})\, X + (-1)^r \tilde{\omega}(a_r).$$

*In particular, we have*

$$\tilde{\omega}(a_1) = \mathbf{Tr}(\delta^{-1}), \qquad \tilde{\omega}(a_r) = \gamma \circ \mathrm{sgn}(a_r) = \mathbf{N}(\delta^{-1})$$

*where $\mathbf{Tr} : \mathbb{F}_{q_\infty^r} \to \mathbb{F}_{q_\infty}$ and $\mathbf{N} : \mathbb{F}_{q_\infty^r}^* \to \mathbb{F}_{q_\infty}^*$ are the trace and norm respectively.*

*Proof.* Let $K'_\infty$ denote the maximal unramified subfield of $E_\infty$ over $K_\infty$. It follows that $E_\infty$ over $K'_\infty$ is a totally ramified extension of degree $e$. As the extension $K'_\infty/K_\infty$ is unramified, it is Galois and is the constant field extension. The Galois group $\mathrm{Gal}(K'_\infty/K_\infty)$ is thus generated by $\sigma$ which restricts to the Frobenius automorphism of $\mathbb{F}_{q_\infty^f}$ over $\mathbb{F}_{q_\infty}$. Choose an automorphism of $\overline{K}_\infty$ lifting $\sigma$ and denoted this lifting by $\sigma$ again. Let $\tau_j : E_\infty \to \overline{K}_\infty$ be $K'_\infty$-embeddings of $E_\infty$ with $1 \leqslant j \leqslant e$. Here, each embedding $\tau_j$ is occurred with multiplicity equal to the inseparable degree of $E_\infty$ over $K'_\infty$. Over $\overline{K}_\infty$, we then have

$$P_\phi(X) = \prod_{i=0}^{f-1}\prod_{j=1}^{e}(X - \sigma^i \tau_j F).$$

Since $r \mid n$, we may express the Frobenius element $F$ as follows

$$F = \rho\, w\, \pi_\infty^{-n/r}$$

where $\rho \in \mathbb{F}_{q_\infty^f}$ and $w \in U_1$ is a 1-unit. Applying $\widetilde{\mathrm{sgn}}$ on both sides, it follows $\widetilde{\mathrm{sgn}}(\rho) = \widetilde{\mathrm{sgn}}(F) = 1/\delta$. Note that $\widetilde{\mathrm{sgn}}$ is an $\mathbb{F}_q$-embedding of $E(\infty)$ into $\bar{\mathbb{F}}_q$ and its restriction on $\mathbb{F}_{q_\infty}$ is equal to $\gamma$, $\widetilde{\mathrm{sgn}}|_{E(\infty)}$ is actually an extension of $\gamma$.

Let's rewrite $P_\phi(X)$ as follows

$$P_\phi(X) = \prod_{i=0}^{f-1}\prod_{j=1}^{e}(X - (\sigma^i \rho) w_i^{(j)} \pi_\infty^{-n/r}) \quad \text{where } w_i^{(j)} = \sigma^i \tau_j\, w,$$

$$= \pi_\infty^{-n} \prod_{j=1}^{e}\prod_{i=0}^{f-1}(\pi_\infty^{n/r}\, X - (\sigma^i\, \rho) w_i^{(j)})$$

https://doi.org/10.1023/A:1002015330987 Published online by Cambridge University Press

Consider the polynomial

$$h(X) = \pi_\infty^n P_\phi(\pi_\infty^{-n/r} X) = \prod_{j=1}^{e} \prod_{i=0}^{f-1} (X - (\sigma^i \rho)\, w_i^{(j)}) \tag{10}$$

$$= X^r - a'_1 X^{r-1} + \cdots + (-1)^r a'_r \tag{11}$$

Note that $a'_i = \pi_\infty^{in/r} a_i$ and $v_\infty(a'_i) \geqslant 0$. By reducing $h(X)$ modulo $\pi_\infty$, we put

$$\bar{h}(X) := X^r - \bar{a}'_1 X^{r-1} + \cdots + (-1)^r \bar{a}'_r$$

where $\bar{a}'_i$ denote the unique element in $K(\infty)$ which is congruent to the reduction $a'_i \,(\mathrm{mod}\, \pi_\infty)$. Observe that, by definition, $\bar{a}'_i = \omega(a_i)$. On the other hand, note that $w_i^{(j)}$ are all 1-unit. We also have

$$\bar{h}(X) = \prod_{j=1}^{e} \prod_{i=0}^{f-1} (X - \sigma^i \rho) = \left\{ \prod_{i=0}^{f-1} (X - \sigma^i \rho) \right\}^e \tag{12}$$

by (10). As $\rho = \widetilde{\mathrm{sgn}}^{-1}(1/\delta)$ over $\mathbb{F}_q$ and $\mathrm{Gal}(E(\infty)/\mathbb{F}_q)$ is abelian, (12) implies that $\widetilde{\mathrm{sgn}}(\bar{h}(X))$ is the characteristic polynomial of $1/\delta$ over $\mathbb{F}_{q_\infty}$ as the scalar multiplication on $\mathbb{F}_{q_\infty^r}$. The theorem now follows by observing that $\widetilde{\mathrm{sgn}}(\bar{h}(X)) = \tilde{\omega}(P_\phi(X))$. □

*Remark 4.* (1) In fact, using the same arguments as in Corollary 4.5, the restriction of the cocycle sgn to $K'_\infty$ can be shown to be a twisted sign function on $K'_\infty$.

(2) Taking norm down to $\mathbb{F}_q$, we have that

$$\mathbf{N}_{\mathbb{F}_q}^{K(\infty)}(\mathrm{sgn}(a_r)) = \mathbf{N}_{\mathbb{F}_q}^{K(\infty)}(\widetilde{\mathrm{sgn}}(a_r)) = \mathbf{N}_{\mathbb{F}_q}^{L}\left(\frac{1}{\Delta}\right).$$

(3) With a little more effort, we can show that $\widetilde{\mathrm{sgn}}(a_r) = (-1)^{n(e+1)} \mathbf{N}_{\mathbb{F}_{q_\infty}}^{L}(\Delta)^{-1}$ without assuming $r \mid n$. By the congruence $n\,e \equiv n\,r \,(\mathrm{mod}\, 2)$, this leads to another proof of Theorem 3.2 (see also Remark 1).

## 5. Distribution of the Signs

Although our arguments can be extended to general cases, for the sake of simplicity and practical purpose, we'll assume the closed point $\infty$ of $\mathcal{C}$ is rational over $\mathbb{F}_q$ in the remaining of this paper. We restate Theorem 4.6 in this case as follows.

THEOREM 5.1. *Assume $r \mid n$ and put $\delta = \Delta^{(q^n-1)/(q^r-1)} \in \mathbb{F}_{q^r}^*$. Then, the characteristic polynomial of the scalar multiplication by* $\mathrm{sgn}(F) = \delta^{-1}$ *on $\mathbb{F}_{q^r}$ is*

$$\omega(P_\phi(X)) := X^r - \omega(a_1) X^{r-1} + \cdots + (-1)^{r-1} \omega(a_{r-1}) X + (-1)^r \omega(a_r).$$

https://doi.org/10.1023/A:1002015330987 Published online by Cambridge University Press

*In particular, we have*

$$\omega(a_1) = \mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\delta^{-1}),$$

$$\omega(a_r) = \mathrm{sgn}(a_r) = \mathbf{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\delta^{-1})$$

*where* $\mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ *and* $\mathbf{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}} : \mathbb{F}_{q^r}^* \to \mathbb{F}_q^*$ *are the trace and norm respectively.*

Let $L$ be a global function field over finite field and we assume that $L$ is an $\mathbb{A}$-field of generic characteristic. Fix $\phi$ to be a fixed rank $r$ Drinfeld $\mathbb{A}$-module over $L$. Then there is a finite set of places, denoted by $S$, of $L$ so that $\phi$ has good reduction outside $S$ [2]. Let $\mathcal{O}_L$ be the integral closure of $\mathbb{A}$ in $L$. Extending $S$, if necessary, we may assume that $S$ contains places of $L$ which are above $\infty$ and that $\phi$ is defined over $S$-integers of $L$.

NOTATIONS.

$p$ : the characteristic of $\mathbb{A}$ = the characteristic of $\mathbb{F}_q$,
$M_L$ : the set of places of $L$,
$L(v)$ : the residue field at the place $v \in M_L$,
$n_v$ : the degree of $L(v)$ over $\mathbb{F}_q$,
$\mathrm{Frob}_v := \tau^{n_v}$ the geometric Frobenius endomorphism of $\mathbb{G}_a$ over $L(v)$.

Consider any place $v \notin S$ and by choice, $\phi$ has good reduction at $v$. We thus have a well defined characteristic polynomial $P_{\phi,v}(X)$ associated with $\mathrm{Frob}_v$ at $v$. The polynomial $P_{\phi,v}(X) \in \mathbb{A}[X]$ has the form as given in (2). To indicate the dependence on $v$, we change the notation as follows:

$$P_{\phi,v}(X) = X^r - a_{1,v}X^{r-1} + \cdots + (-1)^r a_{r,v}. \tag{13}$$

Set $\mathcal{P}_v$ to be the monic element of $\mathbb{A}$ such that $a_{r,v} = \epsilon_v \mathcal{P}_v$. In this section, we will be interested in the distribution of the signs $\epsilon_v$ as $v$ varies.

Given

$$\phi_a = a\tau^0 + g_1\tau + \cdots + \Delta_a \tau^{r\deg(a)}$$

with $g_i \in L$, $\Delta_a \in L^*$, for $a \in \mathbb{A} \setminus \mathbb{F}_q$. If $a$ does not vanish at place $v$, then we have

$$\epsilon_v^{\deg(a)} = \mathbf{N}_{\mathbb{F}_q}^{L(v)}((-1)^{(r+1)\deg(a)}\Delta_a)^{-1}$$

by Theorem 3.1. For any $b \in \mathcal{O}_L$ nonvanishing at $v$, the $(q-1)$th power residue symbol for $b$ at $v$ is by definition, the unique element $\left\{\frac{b}{v}\right\}$ in $\mathbb{F}_q^*$ such that $\left\{\frac{b}{v}\right\} \equiv b^{(|v|-1)/(q-1)} (\mathrm{mod}\, v)$. Here $|v|$ denotes the cardinality of the finite field $L(v)$.

https://doi.org/10.1023/A:1002015330987 Published online by Cambridge University Press

We may rewrite Theorem 3.1 in terms of $(q-1)$-th power residue symbol

$$\epsilon_v^{\deg a} = \left\{ \frac{(-1)^{(r+1)\deg a}\Delta_a}{v} \right\}^{-1}. \tag{14}$$

Let $a, a' \in \mathbb{A}$ be two monic elements such that $(\deg(a), \deg(a')) = 1$. Enlarge $S$ if necessary, we assume that $S$ contains places where $a, a'$ vanish. Let $j, j'$ be two integers such that $j(|a|^r - 1) + j'(|a'|^r - 1) = q^r - 1$. Put $\Delta = \Delta_a^j \Delta_{a'}^{j'}$ then, as in Remark 2, we have

$$\epsilon_v = \left\{ \frac{(-1)^{r+1}\Delta}{v} \right\}^{-1}. \tag{15}$$

Define the subset $N_\eta$ of $M_L^0$ as follows :

$$N_\eta = \{v \in M_L \setminus S : \epsilon_v = \eta\}, \quad \text{for } \eta \in \mathbb{F}_q.$$

We are interested in determining the Dirichlet density of $N_\eta$.

THEOREM 5.2. *Let $\ell$ be the smallest non-negative integer such that $((-1)^{r+1}\Delta)^\ell$ is in $(L^*)^{q-1}$. Then*

(1) $\epsilon_v \in (\mathbb{F}_q^*)^{(q-1)/\ell}$ *for all* $v \notin S$,
(2) *given any* $\eta \in (\mathbb{F}_q^*)^{(q-1)/\ell}$ *the Dirichlet density for* $N_\eta$ *is equal to* $1/\ell$.

*Proof.* The assertion (1) follows from the definition of $\ell$ and the multiplicativity of power residue symbol. We proceed to prove (2). Let $L' = L\left(\sqrt[q-1]{(-1)^{r+1}\Delta}\right)$ be the extension by adjoining any $(q-1)$th root of $(-1)^{r+1}\Delta$. As $L$ contains $(q-1)$th roots of unity and $((-1)^{r+1}\Delta)^\ell \in (L^*)^{q-1}$ the extension $L'/L$ is a Kummer extension and is cyclic of degree $\ell$. It follows [12, III. 5.1],

$$(v, L'/L)\left(\sqrt[q-1]{(-1)^{r+1}\Delta}\right) = \left\{ \frac{(-1)^{r+1}\Delta}{v} \right\} \sqrt[q-1]{(-1)^{r+1}\Delta} = \epsilon_v^{-1} \sqrt[q-1]{(-1)^{r+1}\Delta},$$

where $(v, L'/L)$ is the Artin symbol. Now assertion (2) follows from Čebotarev density theorem. □

*Remark 5.* The integer $\ell$ appeared in Theorem 5.2 is an invariant which is independent of the choice of $a, a'$ with $(\deg(a), \deg(a')) = 1$.

EXAMPLE 2. We consider the special case that $\mathbb{A} = \mathbb{F}_q[T]$ and $L = K = \mathbb{F}_q(T)$ which is the most interesting case in practice. Let $\phi$ be a $\mathbb{F}_q[T]$-modules over $L$

of rank $r$. Then $\phi$ is given by

$$\phi_T = T\tau^0 + g_1\tau + \cdots + g_{r-1}\tau^{r-1} + \Delta\tau^r,$$

where $g_1, \cdots, g_{r-1} \in L$ and $\Delta \in L^*$. Let $S$ be the set of prime ideals of $\mathbb{A}$ such that $g_1, \cdots, \Delta$ are $S$-integers. Let $\mathfrak{p} \notin S$ be a prime ideal and $\mathcal{P}$ be its monic generator. By taking $\mathfrak{a} = (T)$ in Theorem 3.1 and applying Theorem 5.2, we conclude that:

(1) $\epsilon_{\mathfrak{p}} = \left\{\frac{(-1)^{(r+1)}\Delta}{\mathcal{P}}\right\}^{-1}$ and

(2) the Dirichlet density for $N_\eta$ is equal to $1/\ell$ for any given $\eta \in (\mathbb{F}_q^*)^{(q-1)/\ell}$ where $\ell$ is as defined in Theorem 5.2.

EXAMPLE 3. Consider the rank 2 Drinfeld $\mathbb{F}_5[T]$-module $\phi_T = T\tau^0 + \tau + T\tau^2$ defined over $\mathbb{F}_5(T)$. Then $\ell = 4$ for this particular module. Computation gives

| deg $v$ | # of $\epsilon_v = 1$ | # of $\epsilon_v = 2$ | # of $\epsilon_v = 3$ | # of $\epsilon_v = 4$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 3 | 3 | 2 |
| 3 | 10 | 10 | 10 | 10 |
| 4 | 36 | 39 | 39 | 36 |

## 6. Distribution of the Degrees of Traces

Let assumptions be the same as those in Section 5. The coefficient $a_{1,v}$ of the characteristic polynomial $P_{\phi,v}(X)$ has degree at most $n_v/r$. It is natural to ask how often the Frobenius trace has degree equal to $n_v/r$ as $v$ varies. We are interested in the following set of places

$$\mathcal{T}_\phi = \left\{v \in M_L \setminus S \ : \ \deg(a_{1,v}) = \frac{n_v}{r}\right\}.$$

Let $\mathbb{F}_L$ denote the constant field of $L$. Moreover let $s$ be the smallest positive integer such that $\Delta^s \in (L^*)^{q^r-1}$. Our main theorem in this section is the following.

THEOREM 6.1. (1) *Let* $H_s = (\mathbb{F}_{q^r}^*)^{(q^r-1)/s}$, *and let* $u$ *be the cardinality of the set* $H_s \cap \ker(\mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}})$. *Then the Dirichlet density of* $\mathcal{T}_\phi$ *is equal to* $(s-u)/(s[\mathbb{F}_{q^r} : \mathbb{F}_L])$.
(2) *Assume that* $r$ *is relatively prime to* $p$. *Let* $\{p_1, \cdots, p_t\}$ *be the set of prime factors of* $s$. *Set* $t = 0$ *if* $s = 1$. *Then the Dirichlet density of the set* $\mathcal{T}_\phi$ *is greater than* $(2t+1)/(s[\mathbb{F}_{q^r} : \mathbb{F}_L])$ *if* $s$ *is odd and greater than* $2t/(s[\mathbb{F}_{q^r} : \mathbb{F}_L])$ *if* $s$ *is even. In particular, the Dirichlet density for* $\mathcal{T}_\phi$ *is always positive.*
(3) *Assume that* $r$ *is divisible by* $p$ *then the following statements are equivalent.*

(i) $\mathcal{T}_\phi$ *is empty,*
(ii) *the Dirichlet density for* $\mathcal{T}_\phi$ *is zero,*

https://doi.org/10.1023/A:1002015330987 Published online by Cambridge University Press

(iii) $[\mathbb{F}_{q^r} : \mathbb{F}_q(H_s)]$ *is divisible by* $p$.

*Proof.* Let $L_r$ be the extension of $L$ by adjoining $(q^r - 1)$-th roots of unity and let $L_\Delta = L_r(\sqrt[q^r-1]{\Delta})$. We have $\mathrm{Gal}(L_r/L) \simeq \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_L)$ and $\mathrm{Gal}(L_\Delta/L_r) \simeq H_s$. Let $G$ denote the Galois group of $L_\Delta/L$. Then the Galois group $G$ is an extension of the group $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_L)$ by $H_s$ and the cardinality of $G$ is equal to $s[\mathbb{F}_{q^r} : \mathbb{F}_L]$. Note that by fixing a $(q^r - 1)$-th root $\sqrt[q^r-1]{\Delta}$ of $\Delta$, the isomorphism $\mathrm{Gal}(L_\Delta/L_r) \simeq H_s$ is given by $\gamma \mapsto \zeta_\gamma$ such that $\gamma(\sqrt[q^r-1]{\Delta}) = \zeta_\gamma \sqrt[q^r-1]{\Delta}$ for some $\zeta_\gamma \in H_s$. Moreover $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_L)$ acts on $\mathrm{Gal}(L_\Delta/L_r)$ and the action is given by

$$(\sigma * \gamma)(\sqrt[q^r-1]{\Delta}) = \sigma(\zeta_\gamma) \sqrt[q^r-1]{\Delta} \tag{16}$$

for $\gamma \in \mathrm{Gal}(L_\Delta/L_r)$ and $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_L)$. This action corresponds to conjugation in $G$. Namely, for any lifting $\tilde{\sigma} \in G$ of $\sigma$ we have $\tilde{\sigma}\gamma\tilde{\sigma}^{-1} = \sigma * \gamma$. For places $v \in M_L^0 \setminus S$, we note that $\omega(a_{1,v}) = 0$ unless $n_v$ is divisible by $r$. Thus we only need to consider places $v$ such that the degrees $n_v$ are multiples of $r$. Let $w$ denote any place of $L_\Delta$ which lies above $v$ and let $[w, L_\Delta/L]$ denote the Frobenius automorphism attached to $w$. Then the conjugacy class of $[w, L_\Delta/L]$ is the Artin symbol $(v, L_\Delta/L)$. Since the degree of $v$ is a multiple of $r$, the place $v$ splits completely in $L_r$ and the restriction of $[w, L_\Delta/L]$ to $L_r$ is the identity automorphism of $L_r$. Hence $[w, L_\Delta/L]$ lies in $\mathrm{Gal}(L_\Delta/L_r)$, denoted by $\gamma_w$. Let $\zeta_{\gamma_w} \in H_s$ denote the image of $\gamma_w$ under the isomorphism $\mathrm{Gal}(L_\Delta/L_r) \simeq H_s$. By (16), the conjugacy class $(v, L_\Delta/L)$ is the set of Galois conjugates of $\zeta_{\gamma_w}$ regarded as elements over $\mathbb{F}_q$. We have

$$\zeta_{\gamma_w} \equiv \Delta^{(q^{n_v}-1)/(q^r-1)} \pmod{\mathfrak{p}_v} \tag{17}$$

for some $\gamma_w \in (v, L_\Delta/L)$. Therefore, by Theorem 5.1, we see that $\omega(a_{1,v})$ is equal to the trace of $\zeta_{\gamma_w}^{-1}$ from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$. By assumption, there are $u$ elements of $H_s$ which are of zero trace and note that $H_s$ has cardinality $s$. As the set $\mathcal{T}_\phi$ corresponds to $\omega(a_{1,v}) \neq 0$, (1) follows from Čebotarev density theorem [11, Chap. 5].

For (2), we observe that $H_s$ is the group of $s$-th roots of unity. It contains $p_i$-th roots of unity for any prime $p_i$ that divides $s$. Let $\zeta_{p_i}$ denote any primitive $p_i$-th root of unity. We have either $\zeta_{p_i} \in \mathbb{F}_q^*$ or all $\zeta_{p_i}^j$, $1 \leqslant j \leqslant p_i - 1$, are not in $\mathbb{F}_q$.

If $\zeta_{p_i} \in \mathbb{F}_q^*$ then $\mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\zeta_{p_i}) = r\zeta_{p_i}$ which is not zero since $r$ is prime to $p$. The cardinality of such $\zeta_{p_i}$ is at least 2 unless $p_i = 2$ in which case the cardinality is 1. On the other hand, if $\zeta_{p_i} \notin \mathbb{F}_q$ then the set $\{\zeta_{p_i}, \zeta_{p_i}^2, \cdots, \zeta_{p_i}^{p_i-1}\}$ is decomposed into disjoint union of Galois orbits over $\mathbb{F}_q$. We note that $\sum_{j=1}^{p_i-1} \zeta_{p_i}^j = -1$. As the total sum is nonzero there must exist one Galois orbit over $\mathbb{F}_q$ whose sum is not zero. Since $\zeta_{p_i} \notin \mathbb{F}_q$ this orbit contains at least two elements. Let $\xi_i$ be a representative of this orbit. Then $\mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\xi_i) = w_i \mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_q(\xi_i)}(\xi_i) \neq 0$ for some $w_i \mid r$. Take the unity 1 of $H_s$ into account. Thus, the number of elements in $H_s$ whose trace over $\mathbb{F}_q$ is nonzero is at least $(2t + 1)$ for $s$ odd and at least $2t$ for $s$ even. Therefore we have (2).

We begin to prove (3). As (i) implying (ii) is clear we show that (iii) follows from (ii). Assume that $d_s = [\mathbb{F}_{q^r} : \mathbb{F}_q(H_s)]$ is prime to $p$. Since $r$ is a multiple of $p$, the extension $\mathbb{F}_q(H_s)/\mathbb{F}_q$ must be nontrivial. On the other hand, $H_s$ is generated by any primitive $s$-th roots of unity. It follows that $\mathbb{F}_q(\zeta_s) = \mathbb{F}_q(H_s)$ where $\zeta_s \in H_s$ is any primitive $s$-th roots of unity. Then the extension $\mathbb{F}_q(\zeta_s)/\mathbb{F}_q$ has $\{1, \zeta_s, \cdots, \zeta_s^{(r/d_s)-1}\}$ as a basis. As $\mathbb{F}_q(\zeta_s)/\mathbb{F}_q$ is separable, $\{\zeta_s^i : 0 \leqslant i \leqslant (r/d_s) - 1\}$ cannot be all of zero trace from $\mathbb{F}_q(\zeta_s)$ to $\mathbb{F}_q$. Let $\zeta$ be an element of nonzero trace from $\mathbb{F}_q(\zeta_s)$ to $\mathbb{F}_q$ among $\{\zeta_s^i : 0 \leqslant i \leqslant (r/d_s) - 1\}$. Since $\mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\zeta) = d_s \mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_q(\zeta_s)}(\zeta)$ and $d_s$ is prime to $p$, it follows $\mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\zeta)$ is nonzero. We have exhibited an element in $H_s$ which has nonzero trace from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$. By (1), the Dirichlet density of $\mathcal{T}_\phi$ is positive and therefore (ii) implies (iii).

Assume that $d_s$ is divisible by $p$. Because $\mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\xi) = d_s \mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_q(\xi)}(\xi)$ for any $\xi \in \mathbb{F}_q(H_s)$ and $d_s$ is a multiple of $p$ we see that $\mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\xi) = 0$ for all $\xi \in \mathbb{F}_q(H_s)$. In particular, all elements of $H_s$ are of zero trace from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$. Now, by Theorem 5.1, for places $v \in M_L^0 \setminus S$ such that $r \mid n_v$ $\omega(a_{1,v}) = \mathbf{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\zeta_{\gamma_w}^{-1})$ where $\gamma_w \in (\mathfrak{p}_v, L_\Delta/L)$ and $\zeta_{\gamma_w} \in H_s$ is given by the $(q^r - 1)$-th power residue symbol of $\Delta$ at the prime $\mathfrak{p}_v$. Thus $\mathcal{T}_\phi$ does not contain any place $v \in M_L^0 \setminus S$ with $r \mid n_v$. As for places such that $r \nmid n_v$, $\deg(a_{1,v})$ is less than $n_v/r$ already. Therefore, $\mathcal{T}_\phi$ is empty and the proof of (3) is completed. □

EXAMPLE 4. We consider the case that $\mathbb{A} = \mathbb{F}_q[T]$ and that $L = \mathbb{F}_q(T)$. Let $\phi$ be a rank $r$ Drinfeld $\mathbb{A}$-module over $L$ given by

$$\phi_T = T\tau^0 + g_1\tau + \cdots + g_{r-1}\tau^{r-1} + \Delta\tau^r.$$

Assume that $s = q^r - 1$ for $\Delta$, that is, $\Delta$ is of order $q^r - 1$ in $L^*/(L^*)^{q^r-1}$. In this case, $H_s$ is the full group $\mathbb{F}_{q^r}^*$. There are exactly $q^{r-1} - 1$ elements of trace zero over $\mathbb{F}_q$ in $\mathbb{F}_{q^r}^*$. Hence the number of elements with nonzero trace over $\mathbb{F}_q$ is $q^r - q^{r-1}$. Also, $\mathbb{F}_L = \mathbb{F}_q$, by Theorem 6.1 (1), the Dirichlet density for $\mathcal{T}_\phi$ is $q^{r-1}(q-1)/(r(q^r-1))$. In particular if $\phi_T = T\tau^0 + \tau + T\tau^2$ and $q = 3$, the density of $\mathcal{T}_\phi$ for this particular Drinfeld module is 3/8. The proportion of places $v$ of fixed even degree $d$ in $\mathcal{T}_\phi$ should go to 3/4 as $d$ goes to infinity. One checks that among those places of degree 2, the proportion in $\mathcal{T}_\phi$ is 2/3, those of degree 4, the proportion is 7/9, and those of degree 6, the proportion is 3/4.

EXAMPLE 5. Let $\mathbb{A}$, $\phi$, $L$ be as given in Example 4. Assume that $s = 1$, that is $\Delta$ is of $(q^r - 1)$-th power in $L^*$. By passing to isomorphism class over $L$ we may assume that $\Delta = 1$. If $r$ is prime to $p$ then 1 is of nonzero trace; if $r$ is a multiple of $p$ then the trace from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ of 1 is zero. It follows that the Dirichlet density of $\mathcal{T}_\phi$ is $1/[\mathbb{F}_{q^r} : \mathbb{F}_L]$ if $r$ is prime to $p$ and the Dirichlet density is zero if $r$ is divisible by $p$.

As a last application of Theorem 5.1, we study the more general question that how often all the coefficients of the characteristic polynomial attain their maximal degrees (i.e. $\deg a_i = (i\,n_v)/r$). We define the following set

$$\mathcal{D}_\phi = \{v \in M_L \setminus S \ :\ \deg(a_{i,v}) = \frac{i\,n_v}{r},\ 1 \leqslant i \leqslant r\}.$$

It's clear that if $r \nmid n_v$ then $v \notin \mathcal{D}_\phi$. Following the method used in the proof of Theorem 6.1, we have the following

THEOREM 6.2. *Assume that p is greater than r then the Dirichlet Density for* $\mathcal{D}_\phi$ *is always positive.*

*Proof.* Following the notations of the proof of Theorem 6.1, we let $L_r$ be the extension of $L$ by adjoining $(q^r-1)$-th roots of unity and $L_\Delta = L_r(\sqrt[q^r-1]{\Delta})$. Let $G$ and $H_s$ be defined as in the proof of Theorem 6.1. As remarked above, we only need to consider places $v$ such that $v \notin S$ and $r \mid n_v$. In this case, let $w$ be any place lying above $v$. It follows the Frobenius automorphism $[w, L_\Delta/L]$ attached to $w$ lies in $\mathrm{Gal}(L_\Delta/L_r)$, denoted by $\gamma_w$. Let $\zeta_{\gamma_w}$ be the image of the isomorphism $\mathrm{Gal}(L_\Delta/L_r) \simeq H_s$ (see the first part of the proof of Theorem 6.1). We have the congruence relation (17),

$$\zeta_{\gamma_w} \equiv \Delta^{(q^{n_v}-1)/(q^r-1)} \pmod{\mathfrak{p}_v}$$

for an appropriate $(q^r-1)$-th root of $\Delta^{(q^{n_v}-1)}$. By Theorem 5.1, the characteristic polynomial of $\zeta_{\gamma_w}^{-1}$ viewed as scalar multiplication on $\mathbb{F}_{q^r}$ is

$$\omega(P_{\phi,v}(X)) := X^r - \omega(a_{1,v})X^{r-1} + \cdots + (-1)^r\omega(a_{r,v})$$

and $\deg a_i = (i\,n_v)/r$ if and only if $\omega(a_i) \neq 0$. We consider the places $v$ such that $\zeta_{\gamma_v} = 1 \in H_s$. The characteristic polynomial of 1 as scalar multiplication on $\mathbb{F}_{q^r}$ is just

$$\omega(P_{\phi,v}(X)) = (X-1)^r.$$

Since $p > r$ all the coefficients of $\omega(P_{\phi,v}(X))$ are non-zero and since $H_s$ always contains 1, it follows $\mathcal{D}_\phi$ has Dirichlet density greater than or equal to $1/(s[\mathbb{F}_{q^r} : \mathbb{F}_L])$. Now the conclusion follows. □

## Acknowledgement

We would like to thank Jiu-Kang Yu for his valuable comments and suggestions. Especially, his comments on Section 4 make the results more general and improve the presentation there.

## References

1. Carlitz, L.: The arithmetic of polynomials in a Galois field, *Amer. J. Math.* **54** (1932), 39–50.
2. Drinfeld, V. G.: Elliptic modules, *Math. USSR-Sb.* **23** (1976), 561–592.

3. Drinfeld, V. G.: Elliptic modules II, *Math. USSR-Sb.* **31** (1977), 159–170.
4. Gekeler, E.-U.: On finite Drinfeld modules, *J. Algebra* **141** (1991), 187–203.
5. Gekeler, E.-U.: Zur Arithmetik von Drinfeld-Moduln, *Math. Ann.* **262** (1983), 167–182.
6. Gekeler, E.-U.: *Drinfeld Modular Curves,* Lecture Notes in Math. 1231, Springer, New York, 1986.
7. Goss, D.: *L*-series of *t*-motives and Drinfeld modules, In: D. Goss, D. Hayes and M. Rosen (eds), *The Arithmetic of Function fields*, de Gruyter, Berlin, 1992, pp. 313–402.
8. Goss, D.: *Basic Structure of Function Field Arithmetic,* Springer, Berlin, 1996.
9. Hayes, D.: Stickelberger elements in function fields, *Compositio Math.* **55** (1985), 209–239.
10. Hayes, D.: A brief introduction to Drinfeld modules, In: D. Goss, D. Hayes and M. Rosen (eds), *The Arithmetic of Function Fields*, de Gruyter, Berlin, 1992, pp. 1–32.
11. Fried, M. and Jarden, M.: *Field Arithmetic*, Springer, Berlin, 1986.
12. Neukirch, J.: *Class Field Theory,* Springer, Berlin, 1986.
13. Yu, Jiu-Kang: Isogenies of Drinfeld modules over finite fields, *J. Number Theory* **54**(1) (1995), 161–171.