ACTA ARITHMETICA
Online First version

Masser–Wüstholz bound for reducibility of Galois representations for Drinfeld modules of arbitrary rank

by

Chien-Hua Chen (Taipei)

Abstract. We give an explicit bound on the irreducibility of the mod-$\mathfrak{l}$ Galois representation for Drinfeld modules of arbitrary rank without complex multiplication. This is a function field analogue of the Masser–Wüstholz bound on irreducibility of the mod-ℓ Galois representation for elliptic curves over a number field.

1. Introduction. In 1993, Masser and Wüstholz [MW93b] proved a famous result on existence of isogeny, with degree bounded by an explicit formula, between two isogenous elliptic curves. Building upon this, they established an explicit bound on the irreducibility of the mod-ℓ Galois representation associated to elliptic curves over number fields without complex multiplication (CM). This bound was then used to deduce a bound on the surjectivity of the mod-ℓ Galois representation for elliptic curves over number fields without CM.

Analogous to the elliptic curve theory, David and Denis [DD99] introduced an isogeny estimation applicable to Anderson t-modules. In particular, they deduced an isogeny estimation for Drinfeld $\mathbb{F}_q[T]$-modules over a global function field; see Theorem 2.12 for more details. This naturally prompts the query of whether the strategy employed by Masser–Wüstholz can be adapted to deduce an irreducibility limit for the mod-$\mathfrak{l}$ Galois representations concerning rank-r Drinfeld modules without CM. However, the Masser–Wüstholz strategy cannot be applied directly to the context of Drinfeld modules. The main reason is that when one computes the degree of an isogeny between Drinfeld modules, the degree is always a power of q, which is not a prime number. Thus the computational trick in [MW93a, Lemma 3.1] does not work for Drinfeld modules.

2020 *Mathematics Subject Classification*: Primary 11G09; Secondary 11G50.
Key words and phrases: Drinfeld modules, Galois representations, heights.
Received 28 June 2023; revised 26 October 2023.
Published online 6 May 2024.

DOI: 10.4064/aa230628-20-11

Nevertheless, the fundamental concept underlying the Masser–Wüstholz approach has inspired us to produce a similar method. By combining this concept with the height estimate on isogenous Drinfeld modules, as established by Breuer, Pazuki, and Razafinjatovo (as detailed in Theorem 2.13), we are able to deduce our main result: an explicit bound on the irreducibility of the mod-$\mathfrak{l}$ Galois representation for Drinfeld modules of any rank, without CM.

THEOREM 1.1. *Let $q = p^e$ be a prime power, $A := \mathbb{F}_q[T]$, and K a finite extension of $F := \mathbb{F}_q(T)$ of degree d. Let ϕ be a rank-r Drinfeld A-module over K of generic characteristic and assume that* $\mathrm{End}_{\bar{K}}(\phi) = A$. *Let $\mathfrak{l} = (\ell)$ be a prime ideal of A, and consider the mod-$\mathfrak{l}$ Galois representation*

$$\bar{\rho}_{\phi,\mathfrak{l}} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(\phi[\mathfrak{l}]) \cong \mathrm{GL}_r(A/\mathfrak{l}).$$

If $\bar{\rho}_{\phi,\mathfrak{l}}$ is reducible, then either

$$\deg_T \ell - N_d \log \deg_T \ell \leqslant \log C + N_d\{\log d + r + \log[h_G(\phi) + 2]\}, \tag{1}$$

or

$$\deg_T \ell \leqslant \log C + N_d[\log d \cdot h(\phi)]. \tag{2}$$

Here C is a computable constant depending on q and r, and $N_d = 10(d+1)^7$. Furthermore, $h(\phi)$ denotes the naive height of the Drinfeld module, while $h_G(\phi)$ is its graded height (*see Definition* 2.5).

As a corollary, we deduce a sufficient condition on $\deg_T \ell$ for the mod-$\mathfrak{l}$ Galois representation $\bar{\rho}_{\phi,\mathfrak{l}}$ to be irreducible. See Corollary 4.2 for details.

Regarding the specialized scenario of "rank-2 Drinfeld modules over $\mathbb{F}_q(T)$", a more nuanced estimation concerning the irreducibility of the mod-$\mathfrak{l}$ Galois representation has been advanced by Chen and Lee [CL19]. However, their strategy uses the fact that a power of a 1-dimensional group representation is again a group representation (see [CL19, proof of Proposition 7.1]). In rank-2 scenarios, the reducibility of the mod-$\mathfrak{l}$ Galois representation always contributes a 1-dimensional subrepresentation. But this is not true for higher rank Drinfeld modules.

On the other hand, Chen and Lee [CL19] gave an explicit bound on surjectivity of mod-$\mathfrak{l}$ Galois representations for rank-2 Drinfeld modules over $\mathbb{F}_q(T)$ without CM. Such an explicit bound is still unknown for higher rank Drinfeld modules. The main difficulty is the classification of maximal subgroups (up to conjugacy classes) in GL_r over a finite field, which is much more complicated than in the GL_2 case, where one only needs to take care of the Borel and Cartan cases.

2. Preliminaries. Let $A = \mathbb{F}_q[T]$ be the polynomial ring over a finite field with $q = p^e$ an odd prime power, $F = \mathbb{F}_q(T)$ be the fractional field of A, and K be a finite extension of F. Throughout this paper, "log" refers to the logarithm to base q.

2.1. Drinfeld modules

DEFINITION 2.1. Let $K\langle x\rangle := \{\sum_{i=0}^{n} c_i x^{q^i} \mid c_i \in K\}$. Define $(K\langle x\rangle, +, \circ)$ to be the ring of twisted q-polynomials with the usual addition, and with multiplication defined to be the composition of q-polynomials.

DEFINITION 2.2. A *Drinfeld A-module* of rank r over K of generic characteristic is a ring homomorphism

$$\phi : A \to K\langle x\rangle, \quad a \mapsto \phi_a(x),$$

determined by

$$\phi_T(x) = Tx + g_1 x^q + \cdots + g_r x^{q^r}.$$

For an ideal $\mathfrak{a} = \langle a\rangle$ of A, we may define the $\mathfrak{a}$-torsion of the Drinfeld module ϕ over K.

DEFINITION 2.3. The $\mathfrak{a}$-*torsion* of a Drinfeld module ϕ over K is defined to be

$$\phi[\mathfrak{a}] := \{\text{zeros of } \phi_a(x) \text{ in } \bar{K}\} \subset \bar{K}.$$

Now we define the A-module structure on $\bar{K}$. For any $b \in A$ and $\alpha \in \bar{K}$, we define the A-action of b on α via

$$b \cdot \alpha := \phi_b(\alpha).$$

This gives $\bar{K}$ an A-module structure, which is inherited by $\phi[\mathfrak{a}]$. As our Drinfeld module ϕ over K has generic characteristic, we have the following proposition.

PROPOSITION 2.4. *$\phi[\mathfrak{a}]$ is a free $A/\mathfrak{a}$-module of rank r.*

Proof. See [Gos96, Proposition 4.5.3]. ■

Let $\mathfrak{l}$ be a prime ideal of A. Then the $\mathfrak{l}$-torsion $\phi[\mathfrak{l}]$ of the Drinfeld module ϕ is an r-dimensional $A/\mathfrak{l}$-vector space. Applying the action of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ on $\phi[\mathfrak{l}]$, we obtain the so-called *mod-$\mathfrak{l}$ Galois representation*

$$\bar{\rho}_{\phi,\mathfrak{l}} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(\phi[\mathfrak{l}]) \cong \mathrm{GL}_r(A/\mathfrak{l})$$

for the Drinfeld module ϕ over K.

Now we proceed to define various heights associated to Drinfeld modules. Let M_K be the set of all places of K including places above ∞. For each place $\nu \in M_K$, we define $n_\nu := [K_\nu : F_\nu]$, the degree of the local field extension K_ν/F_ν. Furthermore, we set $|\cdot|_\nu$ to be a normalized valuation of K_ν.

DEFINITION 2.5. Let ϕ be a rank-r Drinfeld module over K determined by $\phi_T(x) = Tx + g_1x^q + \cdots + g_{r-1}x^{q^{r-1}} + g_rx^{q^r}$, where $g_i \in K$ and $g_r \in K^*$.

(1) The *naive height* of ϕ is defined to be

$$h(\phi) := \max\{h(g_1), \ldots, h(g_r)\}, \quad \text{where} \quad h(g_i) := \frac{1}{[K:F]} \sum_{\nu \in M_K} n_\nu \cdot \log |g_i|_\nu.$$

(2) The *graded height* of ϕ is defined to be

$$h_G(\phi) := \frac{1}{[K:F]} \sum_{\nu \in M_K} n_\nu \cdot \log \max\{|g_i|_\nu^{1/(q^i-1)} \mid 1 \leqslant i \leqslant r\}.$$

From the definition we obtain

COROLLARY 2.6.

$$h(\phi) \leqslant (q^r - 1) \cdot h_G(\phi).$$

2.2. Isogenies

DEFINITION 2.7. Let ϕ and ψ be two rank-r Drinfeld A-modules over K. A *morphism* $u : \phi \to \psi$ over K is a twisted q-polynomial $u \in K\langle x\rangle$ such that

$$u\phi_a = \psi_a u \quad \text{for all } a \in A.$$

A non-zero morphism $u : \phi \to \psi$ is called an *isogeny.* A morphism $u : \phi \to \psi$ is called an *isomorphism* if its inverse exists.

Set $\mathrm{Hom}_K(\phi, \psi)$ to be the group of all morphisms $u : \phi \to \psi$ over K. We denote $\mathrm{End}_K(\phi) = \mathrm{Hom}_K(\phi, \phi)$. For any field extension L/K, we define

$$\mathrm{Hom}_L(\phi, \psi) = \{u \in L\langle x\rangle \mid u\phi_a = \psi_a u \text{ for all } a \in A\}.$$

For $L = \bar{K}$, we omit subscripts and write

$$\mathrm{Hom}(\phi, \psi) := \mathrm{Hom}_{\bar{K}}(\phi, \psi) \quad \text{and} \quad \mathrm{End}(\phi) := \mathrm{End}_{\bar{K}}(\phi).$$

DEFINITION 2.8. The composition of morphisms makes $\mathrm{End}_L(\phi)$ a subring of $L\langle x\rangle$, called the *endomorphism ring* of ϕ over L. For any rank-r Drinfeld module ϕ over K with $\mathrm{End}(\phi) = A$, we say that ϕ *does not have complex multiplication.*

DEFINITION 2.9. Let $f : \phi \to \psi$ be an isogeny of Drinfeld modules over K of rank r. We define the *degree* of f to be

$$\deg f := \#\ker(f).$$

PROPOSITION 2.10. *Let $f : \phi \to \psi$ be an isogeny of Drinfeld modules over K of rank r. There exists a dual isogeny $\hat{f} : \psi \to \phi$ such that*

$$f \circ \hat{f} = \psi_a \quad \textit{and} \quad \hat{f} \circ f = \phi_a.$$

Here $0 \neq a \in A$ is an element of minimal T-degree such that $\ker(f) \subset \phi[a]$.

Proof. See [Gos96, Proposition 4.7.13 and Corollary 4.7.14]. ∎

The following corollary is immediate by counting cardinalities.

COROLLARY 2.11. *In the setting of Proposition* 2.10, *we have*

$$q^{r\cdot\deg_T(a)} = (\deg f)\cdot(\deg \hat{f}).$$

Now we can state the key tools to derive our main result:

THEOREM 2.12 ([DD99, Theorem 1.3]). *Let K be a finite extension of F with $[K:F] := d$. Suppose that there are two $\bar{K}$-isogenous Drinfeld modules ϕ and ψ defined over K. Then there is an isogeny $f:\phi\to\psi$ such that*

$$\deg f \leqslant c_2\cdot(dh(\phi))^{10(r+1)^7}.$$

Here $c_2 = c_2(r,q)$ is an effectively computable constant that depends only on r and q.

THEOREM 2.13 ([BPR21, Theorem 3.1]). *Let $f:\phi\to\psi$ be an isogeny of rank-r Drinfeld modules over $\bar{K}$ and suppose that* $\ker(f)\subset\phi[N]$ *for some $0\neq N\in A$. Then*

$$|h_G(\psi)-h_G(\phi)| \leqslant \deg_T(N) + \left(\frac{q}{q-1}-\frac{q^r}{q^r-1}\right).$$

3. Proof of Theorem 1.1. We are given a rank-r Drinfeld module ϕ defined over K with $\mathrm{End}(\phi)=A$. Suppose the image of the mod-$\mathfrak{l}$ Galois representation $\mathrm{Im}\,\bar{\rho}_{\phi,\mathfrak{l}}$ acting on $\phi[\mathfrak{l}]$ has an invariant $A/\mathfrak{l}$-subspace H of dimension $1\leqslant k\leqslant r-1$.

By [Gos96, Proposition 4.7.11 and Remark 4.7.12], there is an isogeny

$$f:\phi\to\phi/H$$

with $\ker(f)=H$. Since ϕ and f both are defined over K, one can see that ϕ/H is a rank-r Drinfeld module defined over K as well. In addition, we have

$$\deg f = \#H = q^{k\cdot\deg_T\mathfrak{l}}.$$

Take a dual isogeny $\hat{f}:\phi/H\to\phi$ of f. The degree of $\hat{f}$ can be computed using Corollary 2.11. We get

$$\deg\hat{f} = q^{(r-k)\cdot\deg_T\mathfrak{l}}.$$

Moreover, from Theorem 2.12, we can find two isogenies defined over $\bar{K}$ between ϕ and ϕ/H with bounded degree:

- $u:\phi\to\phi/H$ with $\deg u\leqslant c_2\cdot(dh(\phi))^{10(d+1)^7}$,
- $u':\phi/H\to\phi$ with $\deg u'\leqslant c_2\cdot(dh(\phi/H))^{10(d+1)^7}$.

Since $\mathrm{End}(\phi)=A$, we have $u'\circ u=\phi_b$ for some $b\in A$.

Now we consider the composition of isogenies

$$u'\circ f\circ\hat{f}\circ u:\phi\to\phi/H\to\phi\to\phi/H\to\phi.$$

Since $\mathrm{End}(\phi) = A$, we can find N_1 and N_2 in A such that

$$u' \circ f = \phi_{N_1}, \qquad \hat{f} \circ u = \phi_{N_2}.$$

Thus

$$u' \circ f \circ \hat{f} \circ u = (u' \circ f) \circ (\hat{f} \circ u) = \phi_{N_1 N_2}.$$

On the other hand, we compute in different order and get

$$u' \circ f \circ \hat{f} \circ u = u' \circ (f \circ \hat{f}) \circ u = u' \circ (\phi/H)_\ell \circ u = \phi_\ell \circ (u' \circ u) = \phi_{\ell b}.$$

Thus we get $\ell b = N_1 N_2$. As ℓ is prime, we have either $\ell \mid N_1$ or $\ell \mid N_2$.

Case 1: $\ell \mid N_1$. Then $N_1 = \ell\beta$ for some $0 \neq \beta \in A$. From the equality $u' \circ f = \phi_{N_1}$, we have

$$\log \deg u' + k \cdot \deg_T \ell = r(\deg_T \ell + \deg_T \beta).$$

Hence

$$\log \deg u' = (r-k) \deg_T \ell + r \deg_T \beta.$$

Combining this with the bound $\deg u' \leqslant c_2 \cdot (dh(\phi/H))^{10(d+1)^7}$, we obtain

$$\begin{aligned}(r-k)\deg_T \ell &\leqslant \log c_2 + 10(d+1)^7 \log[dh(\phi/H)] - r \deg_T \beta \\ &\leqslant \log c_2 + 10(d+1)^7 \log[dh(\phi/H)].\end{aligned}$$

Thus

$$(\star) \qquad \begin{aligned}\deg_T \ell &\leqslant \frac{1}{r-k} \cdot \big(\log c_2 + 10(d+1)^7 \log[dh(\phi/H)]\big) \\ &\leqslant \log c_2 + 10(d+1)^7 \log[dh(\phi/H)].\end{aligned}$$

Now from Corollary 2.6 and Theorem 2.13, we have

$$h(\phi/H) \leqslant (q^r - 1) h_G(\phi/H) \leqslant (q^r - 1) \cdot \left[h_G(\phi) + \deg_T \ell + \left(\frac{q}{q-1} - \frac{q^r}{q^r-1}\right)\right].$$

Consequently,

$$\begin{aligned}\log h(\phi/H) &\leqslant \log(q^r - 1) + \log\left(h_G(\phi) + \deg_T \ell + \left(\frac{q}{q-1} - \frac{q^r}{q^r-1}\right)\right) \\ &\leqslant r + \log \deg_T \ell + \log\left(h_G(\phi) + 1 + \left(\frac{q}{q-1} - \frac{q^r}{q^r-1}\right)\right).\end{aligned}$$

Combining this with the inequality $(\star)$ and the fact that

$$\frac{q}{q-1} - \frac{q^r}{q^r-1} < 1,$$

we obtain

$$\begin{aligned}&\deg_T \ell - 10(d+1)^7 \log \deg_T \ell \\ &\qquad\qquad \leqslant \log c_2 + 10(d+1)^7 \{\log d + r + \log[h_G(\phi) + 2]\}.\end{aligned}$$

After renaming $C := c_2$ and $N_d := 10(d+1)^7$, we get the desired inequality (1).

Case 2: $\ell \mid N_2$. Then $N_2 = \ell\beta$ for some $0 \neq \beta \in A$. From the equality $\hat{f} \circ u = \phi_{N_2}$, we have

$$(r-k)\deg_T \ell + \log \deg u = r(\deg_T \ell + \deg_T \beta).$$

Thus we get $\log \deg u = k \deg_T \ell + r \deg_T \beta$. Together with the bound $\deg u \leqslant c_2 \cdot (dh(\phi))^{10(d+1)^7}$, we achieve

$$k \deg_T \ell \leqslant \log c_2 + 10(d+1)^7 \log[dh(\phi)] - r \deg_T \beta \leqslant c_2 \cdot (dh(\phi))^{10(d+1)^7}.$$

Hence

$$\begin{aligned} \deg_T \ell &\leqslant \frac{1}{k} \cdot (\log c_2 + 10(d+1)^7 [\log d \cdot h(\phi)]) \\ &\leqslant \log c_2 + 10(d+1)^7 [\log d \cdot h(\phi)]. \end{aligned}$$

Again, relabelling $C := c_2$ and $N_d := 10(d+1)^7$ gives us inequality (2).

This completes the proof of Theorem 1.1.

4. Lower bound on irreducibility of $\bar{\rho}_{\phi,\mathfrak{l}}$. In the setting of Theorem 1.1, one may further solve inequality (1) for $\deg_T \ell$. By setting

$$\Omega_\phi := \max\{\log C + N_d(\log d + r + \log[h_G(\phi)+2]), \log C + N_d[\log d \cdot h(\phi)]\},$$

Theorem 1.1 implies that the mod-$\mathfrak{l}$ Galois representation is irreducible when

$$\frac{q^{\deg_T \ell}}{\deg_T \ell^{N_d}} > q^{\Omega_\phi} \quad \text{and} \quad \deg_T \ell > \Omega_\phi.$$

When we fix a finite extension K/F and a Drinfeld module ϕ, the numbers N_d and Ω_ϕ are fixed. Elementary calculus can tell us that the fraction $\frac{q^{\deg_T \ell}}{\deg_T \ell^{N_d}}$ tends to infinity as $\deg_T \ell \to \infty$. Thus we can always find a real number $C_{\phi,d}$ such that $\deg_T \ell > C_{\phi,d}$ implies $\frac{q^{\deg_T \ell}}{\deg_T \ell^{N_d}} > q^{\Omega_\phi}$. Now we try to compute $C_{\phi,d}$ explicitly:

Lemma 4.1. *Let a, b, and c be positive real numbers such that $c^{1/b} \cdot \frac{b}{\ln a} \geqslant e$, where e is the Euler number and $\ln := \log_e$. Then*

$$x > \frac{-b \cdot W_{-1}\left(\frac{-\ln a}{c^{1/b} \cdot b}\right)}{\ln a}$$

is a solution to the inequality

$$\frac{a^x}{x^b} > c.$$

Here W_{-1} is the negative brach of the real-valued Lambert W-function, i.e. the inverse function of the complex-valued function $f(y) = ye^y$.

Proof. The proof is by direct computation, hence we leave it to the reader as an exercise. ■

Now we take $x = \deg_T \ell$, $a = q$, $b = N_d$, and $c = q^{\Omega_\phi}$. One can check that

$$c^{1/b} \cdot \frac{b}{\ln a} \geqslant e.$$

Therefore, Lemma 4.1 shows that

$$C_{\phi,d} = \frac{-b \cdot W_{-1}\left(\frac{-\ln a}{c^{1/b} \cdot b}\right)}{\ln a}.$$

And we can conclude the following corollary:

COROLLARY 4.2. *Let $q = p^e$ be a prime power, $A := \mathbb{F}_q[T]$, and K a finite extension of $F := \mathbb{F}_q(T)$ of degree d. Let ϕ be a rank-r Drinfeld A-module over K of generic characteristic and assume that $\mathrm{End}_{\bar{K}}(\phi) = A$. Let $\mathfrak{l} = (\ell)$ be a prime ideal of A, and consider the mod-$\mathfrak{l}$ Galois representation*

$$\bar{\rho}_{\phi,\mathfrak{l}} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(\phi[\mathfrak{l}]) \cong \mathrm{GL}_r(A/\mathfrak{l}).$$

If $\deg_T \ell > \max\{C_{\phi,d}, \Omega_\phi\}$, then $\bar{\rho}_{\phi,\mathfrak{l}}$ is irreducible. Here

$$\Omega_\phi := \max\{\log C + N_d(\log d + r + \log[h_G(\phi) + 2]), \log C + N_d[\log d \cdot h(\phi)]\},$$

$$C_{\phi,d} = \frac{-N_d \cdot W_{-1}\left(\frac{-\ln q}{q^{\Omega_\phi/N_d} \cdot N_d}\right)}{\ln q},$$

and $C = c_2(r, q)$ is the effectively computable constant of Theorem 2.12.

Acknowledgements. The author would like to thank Sophie Marques for inspiring discussions, Wei-Hung Su for showing him the computation for Lemma 4.1, and the referee for helpful suggestions.

References

[BPR21] F. Breuer, F. Pazuki, and M. H. Razafinjatovo, *Heights and isogenies of Drinfeld modules*, Acta Arith. 197 (2021), 111–128.

[CL19] I. Chen and Y. Lee, *Explicit surjectivity results for Drinfeld modules of rank 2*, Nagoya Math. J. 234 (2019), 17–45.

[DD99] S. David et L. Denis, *Isogénie minimale entre modules de Drinfel'd*, Math. Ann. 315 (1999), 97–140.

[Gos96] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergeb. Math. Grenzgeb. (3) 35, Springer, Berlin, 1996.

[MW93a] D. W. Masser and G. Wüstholz, *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc. 25 (1993), 247–254.

[MW93b] D. Masser and G. Wüstholz, *Isogeny estimates for abelian varieties, and finiteness theorems*, Ann. of Math. (2) 137 (1993), 459–472.

Chien-Hua Chen
Mathematics Division
National Center for Theoretical Sciences
Taipei, Taiwan
ORCID: 0000-0003-3267-5603
E-mail: danny30814@ncts.ntu.edu.tw