ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

ALGEBRAIC INDEPENDENCE AND PRODUCTS OF DRINFELD MODULES

ROBERT TUBBS

Dedicated to Wolfgang Schmidt on the occasion of his 60th birthday

1. Introduction. The purpose of this paper is to study the transcendence degrees of fields of definition of certain points on one-dimensional analytic subgroups of products of nonisogenous Drinfeld modules. Such a product is endowed with an analytic structure through its canonically associated exponential function. A one-dimensional analytic subgroup is the image under the exponential mapping of a one-dimensional vector subspace of the tangent space. We will expand on this below.

We begin with notation which we retain throughout this paper: $\mathbf{F}_q$ is a finite field with $q = p^s$ elements, C is a smooth projective geometrically irreducible curve over $\mathbf{F}_q$, ∞ is a fixed closed point of C of degree denoted by $\deg(\infty)$, k is the function field of C over $\mathbf{F}_q$ and A is the ring of functions in k which are regular on $C\backslash\{\infty\}$.

In the above circumstances a valuation may be defined on the elements of k by $v(a) = -d_\infty(a)$ where $d_\infty : k \to \mathbf{Z}$ is defined by

$$d_\infty(a) = (\text{order of pole of } a \text{ at } \infty) \cdot \deg(\infty).$$

We then make the following choices of notation: $\bar{k}$ is the algebraic closure of k, k_∞ is the completion of k with respect to the valuation v above, and $\bar{k}_\infty$ is the algebraic closure of k_∞.

A Drinfeld elliptic A-module of rank d may then be defined by taking an A-module Λ of $\bar{k}_\infty$ which is discrete with respect to the valuation v and which has $\operatorname{rank}_A \Lambda = d < \infty$ (i.e., Λ is a lattice). There is then a

Received by the editors on July 17, 1995, and in revised form on December 18, 1995.

corresponding exponential function

$$e(z) = z \prod_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \left(1 - \frac{z}{\lambda}\right)$$

which is entire with lattice of periods Λ. The A-action is then given by a homomorphism

$$\varphi : A \to \bar{k}_\infty\{F\},$$

where $\bar{k}_\infty\{F\}$ denotes the twisted polynomial ring in the Frobenius $F : X \mapsto X^q$, which satisfies

$$e(az) = \varphi(a) \circ e(z) \tag{1}$$

for all $a \in A$. (For details see, e.g., [**2**]).

In this setting φ must satisfy

$$\varphi(a) = a + \varphi^{(1)}(a)F + \cdots + \varphi^{(k)}(a)F^k$$

where $\varphi^{(k)}(a) \neq 0$ and $k = d \cdot d_\infty(a)$. We say that φ is defined over a subfield L of $\bar{k}_\infty$ if $\varphi(a) \in L\{F\}$ for all $a \in A$. Moreover, given a discrete A-module Λ and an associated homomorphism $\varphi : A \to L\{F\}$, which satisfies (1) when $e(z)$ is the exponential mapping associated with Λ, we say that the Drinfeld module $(\mathbf{G}_a(\bar{k}_\infty), \varphi)$ has rank d and is defined over L. If we take φ to be the identity mapping, then we obtain the "trivial Drinfeld module" whose exponential mapping is given by $e(z) = z$. We denote this by $\mathbf{G}_L$.

Let $G_1 = (\mathbf{G}_a, \varphi_1), \ldots, G_b = (\mathbf{G}_a, \varphi_b)$ be Drinfeld modules with period lattices $\Lambda_1, \ldots, \Lambda_b$ all of A-rank at most d. Let $e_1(z), \ldots, e_b(z)$ be the associated Drinfeld exponential functions. Then the product $G = \mathbf{G}_L \times G_1 \times \cdots \times G_b$ can be endowed with the structure of a t-module (see [**1**]) which has as its exponential mapping the mapping:

$$\exp_G(z_0, \ldots, z_b) = (z_0, e_1(z_1), \ldots, e_b(z_b)).$$

In this setting the A-action is the diagonal one, which we denote by $\phi(a)$.

A one-dimensional analytic subgroup of G, defined over a subfield K of $\bar{k}_\infty$, is an entire $\mathbf{F}_q$-linear mapping

$$\Phi : \bar{k}_\infty \longrightarrow G(\bar{k}_\infty)$$

which satisfies:

(i) $\Phi(az) = \phi(a) \circ \Phi(z)$ for all $z \in \bar{k}_\infty$

(ii) $\Phi(z) = \sum_{h=0}^{\infty} \beta_h z^{q^h}$ with $\beta_h \in K$.

It is not hard to see, indeed it is implicit in [**1**], that in this situation there is a linear mapping

$$\Phi_* : \bar{k}_\infty \longrightarrow \bar{k}_\infty^b$$

so that

$$\Phi(z) = \exp_G(\Phi_*(z)). \tag{2}$$

A morphism between two Drinfeld modules G_1 and G_2 is a morphism of the additive group schemes which respects the two A-actions. In particular, a morphism defined over a field K is an element f in $K\{F\}$ which satisfies

$$f \circ \varphi_1(a) = \varphi_2(a) \circ f$$

for all a in A. An isogeny is a nonzero morphism.

We say that two Drinfeld modules G_1 and G_2 are nonisogenous if there does not exist an isogeny from G_1 to G_2 defined over $\bar{k}_\infty$. There is a straightforward criterion for two Drinfeld modules to be isogenous.

Proposition 1. *There exists an isogeny $f : G_1 \to G_2$ between two Drinfeld modules of the same rank if and only if there exists a nonzero element u in $\bar{k}_\infty$ such that $u\Lambda_1 \subseteq \Lambda_2$.*

Proof. See, e.g., [**3**]. □

Indeed, if G_1 and G_2 are isogenous, then they have the same rank and there exists u such that $u\Lambda_1 \subseteq \Lambda_2$. As a consequence, if $e_1(z)$ and $e_2(z)$ are nonisogenous Drinfeld modules of rank at most d, then

$$\operatorname{rank}_A(\Lambda_1 \cap \Lambda_2) \le d - 1.$$

Suppose that $G_1, \dots, G_b$ are nonisogenous Drinfeld modules all defined over $\bar{k}$, and let $G = \mathbf{G}_L \times G_1 \times \cdots \times G_b$. Suppose further that $\Phi : \bar{k}_\infty \to G(\bar{k}_\infty)$ is a one-dimensional analytic homomorphism, defined over a subfield K of $\bar{k}_\infty$. By (2) we have a representation

$$\Phi(z) = (\alpha_0 z, e_1(\alpha_1 z), \dots, e_b(\alpha_b z)) \tag{3}$$

with $\alpha_i \in K$.

We want the image $\Phi(\bar{k}_\infty)$ to be Zariski-dense in $G(\bar{k}_\infty)$ and, therefore, the coordinate functions to be algebraically independent. Since $\mathbf{G}_L, G_1, \dots, G_b$ are nonisogenous Theorem 5.1 of [**3**] tells us that this holds if all of $\alpha_0, \dots, \alpha_b$ are nonzero. From this we see that any result concerning the values of the coordinate functions of $\Phi(z)$ can be formulated in terms of the values of Drinfeld exponential functions. We take this point of view in stating our results.

Theorem 2. *Let $u_1, \dots, u_l$ be A-linearly independent elements of $\bar{k}_\infty$, and let $G_1 = (\mathbf{G}_a, \varphi_1), \dots, G_b = (\mathbf{G}_a, \varphi_b)$, with $b \geq 2$, be nontrivial, nonisogenous Drinfeld modules of rank at most d, all of which are defined over $\bar{k}$. Let $e_1(z), \dots, e_b(z)$ denote the associated exponential functions and assume that $v_1, \dots, v_b$ are all nonzero.*

If

$$l > \frac{b}{b-1} d$$

then at least two of the values

$$u_j, v_i, e_i(v_i u_j), \quad 1 \leq i \leq b,\ 1 \leq j \leq l$$

are algebraically independent over $\bar{k}$.

As a companion to Theorem 2, we have:

Theorem 3. *Under the hypotheses of Theorem 3, if*

$$l \geq \frac{2b}{b-1} d$$

then at least two of the values

$$u_j, e_i(v_i u_j), \quad 1 \leq i \leq b,\ 1 \leq j \leq l$$

are algebraically independent over $\bar{k}$.

We remark that the proofs of Theorem 2 and Theorem 3 involve the use of Gelfond's method and Schneider's method, respectively. The difference between these two, which is manifested in whether or not the set which is shown to contain algebraically independent elements contains the values v_i, for $1 \leq i \leq b$, is that the former involves differentiation of the component functions of $\Phi(z)$ while the latter does not.

If we consider a one-parameter subgroup of $G_1 \times \cdots \times G_b$, where G has no $\mathbf{G}_L$ factor, we obtain the result:

Theorem 4. *Let* $u_1, \ldots, u_l$ *be* A*-linearly independent elements of* $\bar{k}_\infty$, *and let* $G_1, \ldots, G_b$, *with* $b \geq 3$, *be nontrivial, nonisogenous, Drinfeld modules all of rank at most* d. *Assume that* $v_1, \ldots, v_b$ *are nonzero elements of* $\bar{k}_\infty$ *with*

$$\frac{1}{v_i}\Lambda_i \bigcap \frac{1}{v_j}\Lambda_j = \{0\} \tag{4}$$

for $i \neq j$. *If*

$$l \geq \frac{b}{b-2}d,$$

then at least two of the values

$$v_i, e_i(v_i u_j), \quad 1 \leq i \leq b,\ 1 \leq j \leq l$$

are algebraically independent over $\bar{k}$.

Just as Theorem 2 above has a companion wherein the algebraically independent set does not involve the values v_i, so does Theorem 4.

Theorem 5. *Under the hypotheses of Theorem* 4, *if*

$$l \geq \frac{2b}{b-2}d$$

then at least two of the values

$$e_i(v_i u_j), \quad 1 \leq i \leq b,\ 1 \leq j \leq l$$

are algebraically independent over $\bar{k}$.

One expects in both Theorem 4 and Theorem 5 the condition (4) is either not necessary or can be relaxed. However, it does not seem possible to do so using the techniques of this paper.

2. Arithmetic estimates. For a fixed lattice Λ_i, of A-rank d, the exponential function, $e_i(z)$, associated with Λ_i is an E_q-function. What this means is that when $e_i(z)$ is written as a power series

$$e_i(z) = \sum_{k=0}^{\infty} b_k^{(i)} z^{q^k},$$

which must be of this form by Artin's theorem, one has a good bit of arithmetic information concerning the coefficients $b_k^{(i)}$. If the field of definition of $\varphi(a)$ is $L \subseteq \bar{k}$, then each $b_k^{(i)} \in L$ and there exists a constant $C_1^{(i)} = C_1(e_i(z))$ such that for all k

$$\max\{d_\infty(b_k^{(i)^\sigma}) : b_k^{(i)^\sigma} \text{ a conjugate of } b_k^{(i)}\} \leq C_1^{(i)}.$$

What is also important is that the denominators of the sequence $\{b_k^{(i)}\}$ are well-behaved. More precisely, there exists a sequence $\{a_k^{(i)}\} \subseteq A$ and a positive constant $C_2^{(i)} = C_2(e_i(z))$ with

(1) $d_\infty(a_k^{(i)}) \leq C_2^{(i)} k q^k$ for all k

(2) for all $h \leq k$, $a_k^{(i)} b_h^{(i)}$ is integral over A

(3) if $q^{k_1} + \cdots + q^{k_s} < q^N$, then $a_{k_1}^{(i)} \cdots a_{k_s}^{(i)} \mid a_N^{(i)}$.

We will use this information to study the arithmetic properties of the functions $z, e_1(v_1 z), \dots, e_b(v_b z)$ at points from the set:

$$\mathcal{U}(s) = \{a_1 u_1 + \cdots + a_l u_l : a_j \in A, d_\infty(a_j) \leq S\}.$$

Let L denote an algebraic field of definition of the Drinfeld modules $\varphi_1, \dots, \varphi_b$. Let K be an extension of L which contains all of the values $v_1, \dots, v_b$.

Let $\theta_1, \dots, \theta_s$ denote a transcendence basis of K over L, and let $\nu_1, \dots, \nu_n$ (with $\nu_1 = 1$) be a vector space basis for K over $L(\theta_1, \dots, \theta_s)$. For any $x \in K$ we then have a representation:

$$x = \left(\sum_{\sigma=1}^{n} P_{\sigma,x}(\theta_1, \dots, \theta_s)\nu_\sigma \right) \Big/ P_{0,x}(\theta_1, \dots, \theta_s), \tag{5}$$

where we take the polynomials $P_{0,x}, P_{1,x}, \dots, P_{n,x}$ with coefficients in A_φ, the integral closure of A in L, without a common factor. We let $D(x) = \max\{\deg P_{0,x}, \dots, \deg P_{n,x}\}$, and let $h_\infty(x)$ denote the maximum d_∞ of the coefficients of $P_{0,x}, \dots, P_{n,x}$.

Hence, for

$$e_i(v_i z) = \sum_{k=0}^{\infty} b_k^{(i)} v_i^{q^k} z^{q^k},$$

the Taylor coefficients now lie in K. Indeed, by the properties of the E_q-functions above, it follows that $b_k^{(i)} v_i^{q^k}$ has a denominator $\delta_{i,k}$ in $A_\varphi[\theta_1, \dots, \theta_s]$ which satisfies the estimates:

(1) $D(\delta_{i,k}) \le q^k C_3(v_i)$

(2) $h_\infty(\delta_{i,k}) \le C_2^{(i)} k q^k + h_\infty(v_i) q^k$

(3) if $q^{k_1} + \dots + q^{k_s} < q^N$ then $\delta_{i,k_1} \cdots \delta_{i,k_s} | \delta_{i,N}$.

For a fixed $u(\mathbf{a}) = a_1 u_1 + \dots + a_l u_l \in \mathcal{U}(S)$, and for each i,

$$e_i(v_i z) = e_i(v_i u(\mathbf{a})) + \sum_{k=0}^{\infty} b_k^{(i)} v_i^{q^k} (z - u(\mathbf{a}))^{q^k}. \tag{6}$$

However, using the A-module action given by φ, we have

$$e_i(v_i u(\mathbf{a})) = \sum_{j=1}^{l} \varphi(a_j) \circ e_i(v_i u_j), \tag{7}$$

where $\varphi(a_j) \in L\{F\}$, $a_j \in A$.

It is well known that k is a finite separable extension of $\mathbf{F}_q[\tau]$ for any τ with $d_\infty(\tau) = 1$. Moreover, A is a subring of the integral closure of $\mathbf{F}_q[\tau]$ in k. Fix such a τ and suppose that $\eta_1 = 1, \eta_2, \dots, \eta_f$ is a vector space basis for A over $\mathbf{F}_q[\tau]$. Then for $a \in A$

$$a = \alpha_1 \eta_1 + \dots + \alpha_f \eta_f \tag{8}$$

with $a_t \in \mathbf{F}_q[\tau]$. Therefore

$$\varphi(a) = \sum_{t=1}^{f} \varphi(\alpha_t)\varphi(\eta_t). \tag{9}$$

Proposition 9. *Let $a \in A$ with $d_\infty(a) = \delta$. Fix τ with $d_\infty(\tau) = 1$ and a basis $\eta_1 = 1, \eta_2, \dots, \eta_f$ of A over $\mathbf{F}_q[\tau]$. Suppose that a is represented as in (8). Then, if $\varphi(a) = a + \varphi^{(1)}(a)F + \dots + \varphi^{(k)}(a)F^k$, and $\varphi^{(0)}(a) = a$, we have*

$$\begin{aligned}\max_{0\le t\le k} d_\infty(\varphi^{(t)}(a)) \le \max_{1\le t\le f}&\{d_\infty(\alpha_t), d_\infty(\varphi^{(1)}(\alpha_t)), \dots, d_\infty(\varphi^{(dd_\infty(\alpha_t))}(\alpha_t))\} \\ &+ \max_{1\le j\le d} d_\infty(\varphi^{(j)}(\tau)) \\ &\times \frac{q^{d\max_{1\le t\le f}\{d_\infty(\eta_t)\}} - 1}{q^d - 1}\, q^{d(\max_{1\le t\le f}\{d_\infty(\alpha_t)\}-1)}.\end{aligned}$$

Proof. For $a = \alpha_1\eta_1 + \dots + \alpha_f\eta_f$ with $\alpha_t \in \mathbf{F}_q[\tau]$ we are reduced to computing $d_\infty(\varphi(\alpha_t\eta_t))$ for each t. Yet

$$\begin{aligned}\varphi(\alpha_t\eta_t) &= \varphi(\alpha_t)\varphi(\eta_t) \\ &= \sum_{i=0}^{d\cdot d_\infty(\alpha_t)} \sum_{j=0}^{k_t} (\varphi^{(i)}(\alpha_t)F^i)(\varphi^{(j)}(\eta_t)F^j) \\ &= \sum_{i=0}^{d\cdot d_\infty(\alpha_t)} \sum_{j=0}^{k_t} \varphi^{(i)}(\alpha_t)\varphi^{(j)^{q^i}}(\eta_t)F^{i+j}.\end{aligned}$$

We then apply the estimate for $d_\infty(\varphi^{(j)}(\eta_t))$ given by Lemma 2.1 of [**2**] to obtain our result. □

Let $u(\mathbf{a}) = a_1u_1 + \dots + a_lu_l$ with $a_j = \alpha_{j1}\eta_1 + \dots + \alpha_{jf}\eta_f$. From the expression (7) for $e_i(v_iu(\mathbf{a}))$, we see that we can write

$$e_i(v_iu(\mathbf{a})) = \sum_{k=1}^{l} P^{(i)}_{k,e_i(u(\mathbf{a}))}(e_i(v_iu_k))$$

where each $P^{(i)}_{k,e_i(u(\mathbf{a}))} \in A_\varphi[X]$ is an $\mathbf{F}_q$-linear polynomial with

$$\deg_X P^{(i)}_{k,e_i(u(\mathbf{a}))} \leq q^{d \max_{1\leq t\leq f, 1\leq j\leq l}\{d_\infty(\alpha_{jt})+d_\infty(\eta_t)\}}.$$

(This estimate comes from the observation that the degree in F of $\varphi(a)$, when a is represented as in (8), is at most

$$\max_{\substack{1\leq t\leq f\\ 1\leq j\leq l}}\{d\cdot d_\infty(\alpha_{jt}) + d\cdot d_\infty(\eta_t)\}.)$$

Additionally, it follows from Proposition 6 above that the coefficients of each $P^{(i)}_{k,e_i(u(\mathbf{a}))}$ have d_∞ at most

$$C_4 q^{d \max_{1\leq t\leq f, 1\leq j\leq l}\{d_\infty(\alpha_{jt})+d_\infty(\eta_t)\}}$$

where $C_4 = \max_{j,k}\{d_\infty \varphi^{(k)}(a_j)\}$.

When we have a_j represented as above, we also note that if $\deg_\infty(a) > C_5 = C_5(\eta_1, \dots, \eta_f)$, it is possible to assume that for each t:

$$d_\infty(a_j) = d_\infty(\alpha_{jt}) + d_\infty(\eta_t);$$

therefore, we can rewrite the above estimates for $\deg_X P^{(i)}_{k,e_i(u(\mathbf{a}))}$ and d_∞ of the coefficients of $P^{(i)}_{k,e_i(u(\mathbf{a}))}$ in terms of $d_\infty(a)$ instead of $\max_{1\leq t\leq f, 1\leq j\leq l}\{d_\infty(\alpha_{jt})\}$. In particular, we obtain

$$\deg_X P^{(i)}_{k,e_i(u(\mathbf{a}))} \leq q^{d(C_5+d_\infty(a))}$$
$$h_\infty(P^{(i)}_{k,e_i(u(\mathbf{a}))}) \leq q^{d(C_5+d_\infty(a))}.$$

3. Multiplicity estimate. We temporarily let G be a product of n nonisogenous Drinfeld modules where one of the factors is, possibly, $\mathbf{G}_L$. For a polynomial $P(X_1, \dots, X_n)$ we define the order of vanishing of P at a point u, along an analytic subgroup $\Phi : \bar{k}_\infty \to G(\bar{k}_\infty)$ as in [**2**]. For completeness, we recall this here: We first define the hyperderivatives of P with respect to Φ to be the coefficients in the Taylor expansion:

$$P(\mathbf{X} + \Phi(z)) = \sum_{j=0}^{\infty} \Delta_j^\Phi P(\mathbf{X}) z^j.$$

For any $u \in \bar{k}_\infty$ we can write

$$P(\Phi(z)) = \sum_{j=0}^{\infty} \Delta_j^{\Phi} P(\Phi(u))(z-u)^j$$

(see [**2**]).

We say that P vanishes to order T at $\Phi(u)$, along Φ, if

$$\Delta_j^{\Phi} P(\Phi(u)) = 0, \quad 0 \le j < T.$$

In this context we have the following result, which is due to Yu [**7**]:

Proposition 7. *Let $P(X_1, \dots, X_n)$ be a polynomial with $\deg_{X_i} P = D_i$, and let $\Phi(z) = (e_1(\alpha_1 z), \dots, e_n(\alpha_n z))$. Let $u_1, \dots, u_b$ be A-linearly independent points in $\bar{k}_\infty$, and for $S > 0$ recall that*

$$\mathcal{U}(S) = \{a_1 u_1 + \cdots + a_l u_l : a_i \in A, d_\infty(a_i) \le S\}.$$

Suppose that P vanishes at each point $\gamma \in \Gamma(S) = \Phi(\mathcal{U}(S))$, along Φ, to order at least T. Then there exists an algebraic subgroup H of G, with $H = H_1 \times \cdots \times H_n$, which is invariant under the A-action on G, so that:

$$T \operatorname{card}\left(\frac{\Gamma(S)+H}{H}\right) \deg H \le C(G) \prod_{i=1}^{n} D_i^{\dim G_i/H_i}.$$

Proof. This is nothing more than Theorem 2.1 of [**2**] together with the description of A-invariant connected algebraic subgroups of G, Theorem A of [**3**]. □

Proof of Theorem 2. Let $G = \mathbf{G}_L \times G_1 \times \cdots \times G_b$. We view the integer S used in the definition of $\mathcal{U}(S)$ above as free and let L_0, L_1 and T be integers (depending on S) which we choose below. The constants $c_1, c_2, \dots$ which appear below do not depend on any of these integers. Put

$$\mathcal{L} = \{(l_0, \dots, l_b) \in \mathbf{N}^{b+1} : 0 \le l_0 \le L_0, \quad 0 \le l_j \le L_1 \text{ for } j = 1, \dots, b\}.$$

Assume that all of the values $u_j, v_i, e_i(v_i u_j)$, $1 \leq i \leq b$, $1 \leq j \leq l$, lie in a field K of transcendence degree one over L. Let θ denote a transcendental generator of K over L. We then let $(\gamma_{\mathbf{l}})_{\mathbf{l}\in\mathcal{L}}$ denote an element of $(A_\varphi[\theta])^{(L_0+1)(L_1+1)^b}$. Associated with each such vector there is a function

$$F_\gamma(z) = \sum_{\mathbf{l}\in\mathcal{L}} \gamma_{\mathbf{l}} z^{l_0} e_1^{l_1}(v_1 z)\cdots e_b^{l_b}(v_b z). \tag{10}$$

Our immediate aim is to find a nonzero vector $\gamma = (\gamma_{\mathbf{l}})_{\mathbf{l}\in\mathcal{L}}$ so that the associated function F_γ vanishes at all points $u(\mathbf{a}) \in \mathcal{U}(\mathbf{S})$, with multiplicity q^T. Moreover, we want to maintain control of the arithmetic (D and h_∞) of the coordinates of the vector γ.

We choose the integers L_0, L_1 and T maximal so that

$$q^T \leq q^{((l+db)/b)S}, \qquad q^{L_1} \leq q^{(l/b)S}$$

and $L_0 = T + \log_q 5$.

For each $u(\mathbf{a}) \in \mathcal{U}(\mathbf{S})$, we substitute the representations (6) for $e_i(v_i z)$ directly into (10) above and obtain:

$$\begin{aligned} F_\gamma(z) = &\sum_{l\in\mathcal{L}} \gamma_l \{u(\mathbf{a}) + (z-u(\mathbf{a}))\}^{l_0} \\ &\times \prod_{i=1}^{b} \left\{ e_i(v_i u(\mathbf{a})) + \sum_{k=0}^{\infty} b_k^{(i)} v_i^{q^k} (z-u(\mathbf{a}))^{q^k} \right\}^{l_i}. \end{aligned}$$

When we compare this with the Taylor expansion of $F_\gamma(z)$ at $u(\mathbf{a})$,

$$F_\gamma(z) = \prod_{r=0}^{\infty} f_r(u(\mathbf{a}))(z-u(\mathbf{a}))^r,$$

we see that:

$$\begin{aligned} f_r(u(\mathbf{a})) = \sum_{l\in\mathcal{L}} \gamma_l \Bigg\{ &\sum_{\substack{t_0+\cdots+t_b=r \\ t_0\leq l_0}} \Bigg(\frac{t_o!}{l_o!(l_0-t_0)!} u(\mathbf{a})^{l_0-t_0} \\ &\times \prod_{i=1}^{b} \sum_{\substack{q^{k_1}+\cdots+q^{k_{s_i}}=t_i \\ s_i\leq l_i}} e_i(v_i u(\mathbf{a}))^{l_i-s} v_i^{t_i} b_{k_1}^{(i)} \cdots b_{k_{s_i}}^{(i)} \Bigg) \Bigg\}. \end{aligned}$$

If we substitute the representation of $e_i(v_i u(\mathbf{a}))$ given by (5) and (7) into the above expressions, and clear denominators, we obtain

$$\left(\prod_{i=1}^{b} P^{L_2}_{0,e_i(u(\mathbf{a}))}(\theta)\right) a_p^{(i)} f_r(u(\mathbf{a})) = \sum_{l\in\mathcal{L}} \gamma_l \sum_{\sigma=1}^{n} P^{(r)}_{\sigma,l,e_i(u(\mathbf{a}))}(\theta)\nu_\sigma$$

where $p = \max\{0, [1+\log_q r]\}$.

Moreover, we have the easy, but not immediate, estimates:

$$\begin{aligned} \max_{\substack{l\in\mathcal{L}\\ 0\le\sigma\le n}} \deg (P^{(r)}_{\sigma,l,e_i(u(\mathbf{a}))})) &\le c_1 q^{L_0} + c_2 b q^{L_1+d(S+c_3)} + c_4 r \\ &\le c_5\{q^{L_0} + q^{L_1+dS} + r\} \\ \max_{\substack{l\in\mathcal{L}\\ 0\le\sigma\le n}} h_\infty(P^{(r)}_{\sigma,l,e_i(u(\mathbf{a}))}) &\le c_6\{q^{L_0} + q^{L_1+dS} + r\log r\}. \end{aligned}$$

Then, if we assume that all of our values:

$$u_j, v_1, e_i(v_i u_j), \quad 1\le i\le b,\ 1\le j\le l$$

lie in $\mathbf{F}_q[\tau,\theta]$, we can apply Lemma 4.3 (the Thue-Siegel lemma) of [**3**] to obtain $(\gamma_{\mathrm{l}})_{\mathrm{l}\in\mathcal{L}} \ne 0$ with

$$\begin{aligned} \max_{\mathrm{l}\in\mathcal{L}} D(\gamma_{\mathrm{l}}) &\le c_7\{q^{L_0} + q^{L_1+dS} + q^T\} \\ \max_{\mathrm{l}\in\mathcal{L}} h_\infty(\gamma_{\mathrm{l}}) &\le c_8\{Tq^T + q^{L_1+dS}\} \end{aligned}$$

so that the associated function $F(z)$ has the desired zeros, each with multiplicity q^T.

This means that when $F(z)$ is expanded as a Taylor series about a fixed point $u(\mathbf{a}) \in \mathcal{U}(S)$, one has

$$F(z) = \sum_{j=0}^{\infty} f_j(u(\mathbf{a}))(z-u(\mathbf{a}))^j$$

where $f_j(u(\mathbf{a})) = 0$ for $0\le j< q^T$.

We now apply the multiplicity estimate above, Proposition 7. Suppose that for some $c_9 > 0$, P vanishes at all of the points $\Gamma(S+c_9)$, along Φ, to order at least q^T. By the multiplicity estimate there exists an A-invariant algebraic subgroup $H = H_0 \times \cdots \times H_b$ so that:

$$q^T \operatorname{card}\left(\frac{\Gamma(S+c_9)+H}{H}\right)\deg H \le C(G) q^{L_0 \dim \mathbf{G}_L/H_0 + L_1 \dim \mathbf{G}_1/H_1 + \cdots + L_1 \dim \mathbf{G}_b/H_b}. \tag{11}$$

We consider the cases: We first note that for c_9 sufficiently large (11) cannot hold for $H = \{0\}$.

If $H_0 = \{0\}$, then (11) takes the form:

$$q^T \operatorname{card}\left(\frac{\Gamma(S+c_9)+H}{H}\right)\deg H \le C(G) q^{L_0 + L_1(\operatorname{codim} H - 1)}.$$

As $\operatorname{codim} H \le b$ we deduce from our choice of L_0, L_1 and T that

$$\operatorname{card}\left(\frac{\Gamma(S+c_9)+H}{H}\right)\deg H \le C(G) q^{((b-1)/b)lS} < q^{lS},$$

provided that S is sufficiently large. In particular, there exists a nonzero element $u \in \mathcal{U}(S)$ so that $\Phi(u) \in H$. But $H_0 = \{0\}$ so $u = 0$, a contradiction.

Therefore, the subgroup H given by Proposition 7 must have $H_0 = \mathbf{G}_L$. In this case, if $\operatorname{codim} H = 1$, then (11) becomes:

$$q^T \operatorname{card}\left(\frac{T(S+c_9)+H}{H}\right)\deg H \le C(G) q^{L_0}.$$

By our choice of parameters we then obtain:

$$\operatorname{card}\left(\frac{\Gamma(S+c_9)+H}{H}\right)\deg H \le C(G).$$

In particular, since $H_j = \{0\}$ for some j, $1 \le j \le b$, we find that $e_j(v_j z)$ has l A-linearly independent periods. Since $l > d$ this is a contradiction.

Hence, we must have $H_0 = \mathbf{G}_L$ and $\operatorname{codim} H \ge 2$. In particular, $H_i = H_j = \{0\}$ for some $i \ne j$. Since G_i and G_j are nonisogenous, of rank at most d, the functions $e_i(v_i z)$ and $e_j(v_j z)$ have at most $d-1$

A-linearly independent periods in common. From the A-analogue of Lemma 3 of [**4**], whose proof is exactly the same with A replacing $\mathbf{Z}$ throughout, it follows that

$$\operatorname{card}\left(\frac{\Gamma(S+c_9)+H}{H}\right)\deg H > q^{(l-d)S}.$$

Using this estimate in (11) we find that $\operatorname{codim} H \geq b+1$; that is, H is trivial (which is contrary to $H_0 = \mathbf{G}_L$).

Therefore, for c_9 sufficiently large, we have that there exists $u(\mathbf{a}') \in \mathcal{U}(S+c_9)$ and j with $j < q^T$ so that $f_j(u(\mathbf{a}')) \neq 0$. Applying the techniques of [**2**], Section D with $R = ((d+l)/d)S$, we deduce that

$$d_\infty(f_j(u(\mathbf{a}'))) \leq -c_{10}q^{T+lS}.$$

This leads to a polynomial $P_S(X) \in A[X]$ with

$$\begin{aligned} \deg(P_S) &\leq c_{11}q^{L_1+dS} \\ h_\infty(P_S) &\leq c_{12}\{Tq^T + q^{L_1+dS}\} \end{aligned}$$

so that

$$d_\infty(P_S(\theta)) \leq -c_{13}q^{T+lS}.$$

Under our hypothesis that $l > (b/(b-1))d$ it follows from the A-analog of Gelfond's criterion (Proposition 3 of [**5**]) that θ is algebraic over $\mathbf{F}_q[\tau]$. However, this contradicts Theorem 4.1 of [**6**], which states that at least one of the values under consideration must be transcendental. □

We only include the highlights of the proof of Theorem 3, as it is virtually identical to the above proof. To establish this result, one assumes that all of the indicated values lie in $k(\theta)$ and constructs an auxiliary function as in displayed line (10). Here we use parameters L_0 and L_1 which are chosen maximally with:

$$q^{L_0} \leq q^{((l+db)/(b+1))}S, \qquad q^{L_1} \leq 5q^{((l-d)/(b+1))S}.$$

By Siegel's lemma it is possible to find $(\gamma_l)_{l\in\mathcal{L}}$ with

$$\begin{aligned} D(\gamma_l) &\leq c_{14}\{q^{L_0} + q^{L_1+dS}\} \\ ht\gamma_l &\leq c_{15}\{q^{L_0} + q^{L_1+dS}\} \end{aligned}$$

so that for $u \in \mathcal{U}(S)$
$$F(u) = 0.$$

As in the proof of Theorem 2, this leads to a polynomial $P_S(X) \in A[X]$ with:
$$\deg P_S \leq c_{16} q^{L_1 + dS}$$
$$h_\infty P_S \leq c_{17} q^{L_1 + dS},$$
and $P_S(\theta)$ is nonzero with
$$d_\infty(P_S(\theta)) < -c_{18} S q^{lS}.$$

It follows from "Gelfond's criterion" that θ is algebraic, contrary to Theorem 4.1 of [**6**].

Proof of Theorem 4. The proof of Theorem 4 is similar, where we construct our function $F(z)$ as above with the choice of parameters made so that $L = L_0 = L_1$ and
$$q^S \leq T^{b/(l+bd)} q^{((b-1)/(l+bd))T}$$
$$q^L \leq 5 T^{l/(l+bd)} q^{((l+d)/(l+bd))T}.$$

With the set $\mathcal{U}(S)$ defined as above and with the indexing set $\mathcal{L} = \{(l_1, \ldots, l_b) : 0 \leq l_j \leq q^L, 1 \leq j \leq b\}$, we construct an auxiliary function
$$F(z) = \sum_{\mathbf{l} \in \mathcal{L}} \gamma_{\mathbf{l}} e_1^{l_1}(v_1 z) \cdots e_b^{l_b}(v_b z). \tag{12}$$

If we assume that all of our values lie in a field $K = L(\theta)$, our choice of integers L, T and S allows us to conclude from the Thue-Siegel lemma (Lemma 4.3 of [**2**]) that there exists a nonzero vector
$$(\gamma_{\mathbf{l}})_{\mathbf{l} \in \mathcal{L}} \in A_\varphi[\theta]^{(L+1)^b}$$
with
$$\max_{\mathbf{l} \in \mathcal{L}} D(\gamma_{\mathbf{l}}) \leq c_{19} \{q^{L+dS} + q^T\}$$
$$\max_{\mathbf{l} \in \mathcal{L}} h_\infty(\gamma_{\mathbf{l}}) \leq c_{20} \{q^{L+dS} + T q^T\}$$

so that $F(z)$ vanishes at each point in $\mathcal{U}(S)$ with multiplicity q^T.

If we view $F(z)$ in the explicit form

$$F(z) = P(e_1(v_1 z), \dots, e_b(v_b z))$$

where $P(X_1, \dots, X_b) \in A_\varphi[\theta][X_1, \dots, X_b]$, we may apply the above multiplicity estimate. Let $c_{21} > 0$ and suppose that $F(z)$ vanishes at all points in $\mathcal{U}(S + c_{21})$ with multiplicity q^T. Then there exists a connected A-invariant algebraic subgroup $H = H_1 \times \cdots \times H_b$ of G so that

$$q^T \operatorname{card}\left(\frac{\Gamma(S + c_{21}) + H}{H}\right) \deg H \leq c(G) q^{L \operatorname{codim}_G H}. \tag{13}$$

If H is trivial, then (13) cannot hold for c_{21} sufficiently large. Hence, we assume that H is nontrivial. If $\operatorname{codim} H = 1$, then since each $e_i(v_i z)$ has rank at most d,

$$\operatorname{card}\left(\frac{\Gamma(S + c_{21}) + H}{H}\right) > q^{(l-d+1)S}$$

and (13), together with the choice of parameters, yields a contradiction.

Therefore, $\operatorname{codim} H \geq 2$ and, as $e_i(v_i z)$ and $e_j(v_j z)$ cannot have a common period, for $i \neq j$, by our hypothesis (4), we obtain

$$\operatorname{card}\left(\frac{\Gamma(S + c_{21}) + H}{H}\right) = q^{lS}.$$

Hence, $\operatorname{codim} H \geq b$, and H is trivial.

Then, as above and as in Section D of [**2**], we obtain a nonzero polynomial $P_S(X) \in A[X]$ with

$$\begin{aligned} \deg(P_S) &\leq c_{22} q^{L+dS} \\ h_\infty(P_S) &\leq c_{23}\{q^{L+dS} + Tq^T\} \end{aligned}$$

and

$$d_\infty(P_S(\theta)) < -c_{24} S q^{T+lS}.$$

Hence, $\theta \in \bar{k}$, contradicting Theorem 4.1 of [**6**]. □

We do not include the similar proof of Theorem 5. We only indicate that one finds an auxiliary function of the form (12) where L is chosen maximal with:

$$q^L \leq 5q^{(l/b)S},$$

so that $F(u) = 0$ for all $u \in \mathcal{U}(S)$. The proof is then as above.

REFERENCES

1. G. Anderson, *t-motives*, Duke Math. J. **53** (1986), 457–502.

2. P.G. Becker, W.D. Brownawell and R. Tubbs, *Gelfond's theorem for Drinfeld modules*, Michigan Math. J. **41** (1994), 219–233.

3. W.D. Brownawell, *Algebraic independence of Drinfeld exponential and quasi-periodic functions*, in *Advances in number theory* (F. Gouvea and N. Yui, eds.), Clarendon Press, Oxford, 1993.

4. D.W. Masser, *On polynomials and exponential polynomials in several complex variables*, Invent. Math. **63** (1981), 81–95.

5. A. Thiery, *Indépendance algébriques des périodes et quasi-périodes d'un module de Drinfeld*, in *The Arithmetic of function fields* (D. Goss, D.R. Hayes and M.I. Rosen, eds.), Ohio State Univ. Math. Research Institute Publications **2** (1992).

6. J. Yu, *Transcendence and Drinfeld modules*, Invent. Math. **83** (1986), 507–517.

7. J. Yu, *Transcendence in finite characteristic*, in *The arithmetic of function fields* (D. Goss, D.R. Hayes and M.I. Rosen, eds.), Ohio State Univ. Math. Research Institute Publications **2** (1992).

Department of Mathematics, University of Colorado, Boulder, CO 80309
E-mail address: tubbs@boulder.colorado.edu