Gelfond's Theorem for Drinfeld Modules

PAUL-GEORG BECKER, W. DALE BROWNAWELL, & ROBERT TUBBS

I. Introduction and Statement of Results

In 1949 Gelfond [Ge] proved that when α and β are algebraic numbers with $\alpha \neq 0$, $\log \alpha \neq 0$, and β cubic over $\mathbb{Q}$, the numbers α^{β} and α^{β^2} are algebraically independent. Our goal is to establish an analogue of this result where the ordinary exponential function is replaced by the exponential function associated with a Drinfeld module with "algebraic" coefficients. Before stating our result we begin with some background material.

CURVE NOTATION.

$\mathbb{F}_q$	finite field of $q = p^s$ elements
$\mathcal{C}$	a smooth projective geometrically irreducible curve over $\mathbb{F}_q$
∞	a fixed closed point of $\mathcal{C}$ of degree denoted by $\deg(\infty)$
k	the function field of $\mathcal{C}$ over $\mathbb{F}_q$
A	the ring of functions in k regular on $\mathcal{C}\setminus\{\infty\}$
d_∞	defined by $d_\infty(a) = (\text{order of pole of } a \text{ at } \infty) \cdot \deg(\infty)$
$\bar{k}$	algebraic closure of k
k_∞	completion of k with respect to the valuation $-d_\infty$
$\bar{k}_\infty$	algebraic closure of k_∞
$d_\infty : \bar{k}_\infty \to \mathbb{Q}$	the extension of d_∞ to $\bar{k}_\infty$

A. Drinfeld Background

To describe a Drinfeld A-module, we may begin with a lattice $\Lambda \subseteq \bar{k}_\infty$, that is, an A-module which is discrete with respect to the additive valuation $-d_\infty$ and for which $d := \dim_{k_\infty} k_\infty \otimes \Lambda < \infty$. The corresponding exponential function is defined by $e(z) = z \prod (1 - z/\lambda)$, where the product runs over all nonzero λ in Λ.

Let $\bar{k}_\infty\{F\}$ denote the ring of "twisted polynomial" operators $\sum_{i=0}^{I} a_i F^i$, where F is the qth power Frobenius mapping $F: X \mapsto X^q$. (Multiplication in $\bar{k}_\infty\{F\}$ is given on monomials by $a_i F^i (a_j F^j) = a_i a_j^{q^i} F^{i+j}$ and extended

Received March 4, 1992. Revision received November 8, 1993.
The first author held a Feodor Lynen Fellowship at Penn State; the first two authors were partially supported by an NSF grant.
Michigan Math. J. 41 (1994).

linearly to all of $\bar{k}_\infty\{F\}$.) Then, for each $a\in A$, one can show (see e.g. step 2 in Lemma 2.2) that there is a $\varphi(a)\in\bar{k}_\infty\{F\}$ such that $\varphi(a)e(z)=e(az)$. In fact, $\varphi\colon a\mapsto\varphi(a)$ gives a homomorphism $A\to\bar{k}_\infty\{F\}$ for which

$$\varphi(a)=a+\varphi_1(a)F+\cdots+\varphi_i(a)F^i \tag{1}$$

with $\varphi_i(a)\neq 0$ for $i=d\cdot d_\infty(a)$.

It is a fundamental theorem of Drinfeld [Dr] that any $\varphi\in\operatorname{Hom}_{\mathbb{F}_q}(A,\bar{k}_\infty)$ having images of the form (1) with some $\varphi_i(a)\neq 0$ $(i>0)$ arises, as above, from a uniquely determined lattice Λ in $\bar{k}_\infty$. We say that φ is *defined over* a field $l\subset\bar{k}_\infty$ if $\varphi(a)\in l\{F\}$ for all $a\in A$. The *field of definition* of φ is the least such l. Let us now summarize the Drinfeld module notation used to state our results.

DRINFELD MODULE NOTATION.

- φ a Drinfeld module defined over a finite extension l of k, i.e., $\varphi\colon A\to l\{F\}\subset\bar{k}_\infty\{F\}$
- $e(z)$ the exponential function corresponding to φ
- Λ the A-lattice of periods of $e(z)$
- d the A-rank of Λ
- R_φ the multiplication ring of φ (or Λ) $=\{c\in\bar{k}_\infty : c\Lambda\subset\Lambda\}$
- r the A-rank of R_φ
- K_φ the field of quotients of R_φ

B. Statement of Results

THEOREM. *Suppose that $\beta_1,\dots,\beta_b,u_1,\dots,u_\kappa$ are elements of $\bar{k}_\infty$ such that*

(1) *each β_i is algebraic over k,*
(2) *$\{\beta_1,\dots,\beta_b\}$ and $\{u_1,\dots,u_\kappa\}$ are K_φ-linearly independent sets, and*
(3) *no product of two nontrivial R_φ-linear forms, one in $\beta_1,\dots,\beta_b$, and one in $u_1,\dots,u_\kappa$, respectively, lies in Λ.*

If $\kappa\geq(d/r)(b/(b-2))$, then

$$\operatorname{tr\,deg}_k k(e(\beta_1u_1),\dots,e(\beta_bu_\kappa))\geq 2.$$

When β is algebraic over K_φ of degree b and $u\in\bar{k}_\infty$ is nonzero, we can take $b=\kappa$, $\beta_i=\beta^{i-1}$, and $u_i=\beta^{i-1}u$ $(i=1,\dots,b)$ to obtain the following result.

COROLLARY 1. *If $\beta\in\bar{k}$ is of degree $b\geq d/r+2$ over K_φ and $u\in\bar{k}_\infty\backslash\{0\}$ with $K_\varphi(\beta)\cap(1/u)\Lambda=\{0\}$, then*

$$\operatorname{tr\,deg}_k k(e(u),e(u\beta),\dots,e(u\beta^{b-1}))\geq 2.$$

It is known that $r\leq d$ (see [Y2, Thm. 3.1]). When $b=3$ and $r=d$, we obtain the analogue of Gelfond's theorem.

COROLLARY 2. *Assume that $b=3$ and $r=d$. If $u\in\bar{k}_\infty$ with $e(u)\in\bar{k}$, but $u\notin K_\varphi\Lambda$ and β is cubic over K_φ, then $e(u\beta)$ and $e(u\beta^2)$ are algebraically independent over k.*

Proof. Since $u \notin K_\varphi \Lambda$, we know that, for any nonzero $\lambda \in \Lambda$, u and λ are K_φ-linearly independent. Yet $e(u) \in \bar{k}$ implies that both u and λ are "logarithms" of numbers in $\bar{k}$. J. Yu's version of the Gelfond–Schneider theorem ([Y1, Thm. 5.1] or [Y3, Thm. 5.5]) then implies that u and λ are $\bar{k}$-linearly independent. Hence u satisfies the hypotheses of Corollary 1, and Corollary 2 follows. □

We thank J. Yu for sharing his work [Y5] before publication and W. C. Waterhouse and the referee for helpful comments.

II. Preliminaries

A. Reduction to Case $A = \mathbb{F}_q[t]$

Equation (1) tells us how the F-degree of $\varphi(a)$ grows with respect to $d_\infty(a)$. We also need to know about d_∞ of the coefficients of $\varphi(a)$.

LEMMA 2.1. *For $a \in \mathbb{F}_q[t] \subset A$ of degree δ in t,*

$$\max d_\infty(\textit{coefficients of } \varphi(a)) \leq \max d_\infty(\textit{coefficients of } \varphi(t)) \frac{g^\delta - 1}{g - 1},$$

where $g = q^{d \cdot d_\infty(t)}$.

Proof. Prove by induction on δ for $a = t^\delta$ and then use linearity. □

For technical reasons, in Sections III and IV it will be convenient to reduce to the case $A = \mathbb{F}_q[t]$. It is standard (see e.g. [Si, Prop. 1.4, p. 22]) that, for any uniformizer $t \in A$ at ∞, k is a finite separable extension of $\mathbb{F}_q(t)$ and A a subring of the integral closure of $\mathbb{F}_q[t]$ in k. However, more generally, the proof remains valid for *any* $t \in A$ with $d_\infty(t)$ not divisible by p. By the Riemann part of the Riemann–Roch theorem [Si, p. 39], there exist t_1, t_2 in A with $d_\infty(t_1) = 2g$ and $d_\infty(t_2) = 2g + 1$, where g is now the genus of $\mathcal{C}$. At least one of these values $d_\infty(t_i)$ is not divisible by p, and we choose t to be the corresponding t_i.

Thus in particular, $\operatorname{rank}_{\mathbb{F}_q[t]} A = \alpha < \infty$, Λ is a $\mathbb{F}_q[t]$-module of $\mathbb{F}_q[t]$-rank $d\alpha$, and R_φ is a $\mathbb{F}_q[t]$-module of $\mathbb{F}_q[t]$-rank equal to $r\alpha$. Moreover, $\varphi|_{\mathbb{F}_q[t]}$: $\mathbb{F}_q[t] \to l\{F\}$ and l is a finite extension of $\mathbb{F}_q(t)$.

Since $e(az) = \varphi(a) e(z)$ for any $a \in \mathbb{F}_q[t]$, we see by the Drinfeld correspondence relating $\mathbb{F}_q[t]$-lattices and $\mathbb{F}_q[t]$-Drinfeld modules that $\varphi|_{\mathbb{F}_q[t]}$ *is* the $\mathbb{F}_q[t]$-Drinfeld module corresponding to the $\mathbb{F}_q[t]$-lattice Λ.

Finally, we remark that $\bar{k}, \bar{k}_\infty, R_\varphi, K_\varphi$ remain the same for $\varphi|_{\mathbb{F}_q[t]}$, while d_∞ is scaled by the reciprocal of the nonzero constant $d_\infty(t)$. Therefore we have established the following reduction principle.

REDUCTION PRINCIPLE. *We may assume that $A = \mathbb{F}_q[t]$ without affecting $\bar{k}$, $\bar{k}_\infty$, Λ, R_φ, K_φ, or $e(z)$ (thus* a fortiori *the values $e(\beta_i u_\nu)$), and without* *extending the field of definition of φ; however, $d_\infty|_{\mathbb{F}_q[t]}$ is changed by a nonzero constant factor (namely $d_\infty(t)^{-1}$).*

B. Extension of φ

Although φ is given as defined on A, we show that it extends uniquely to R_φ (cf. [Y4, p. 565]).

LEMMA 2.2. *There is a finite separable extension L_φ of lK_φ such that the map φ extends uniquely to a homomorphism $\varphi\colon R_\varphi \to L_\varphi\{F\}$, satisfying*

$$\varphi(\rho)e(z) = e(\rho z) \tag{2}$$

for all $\rho \in R_\varphi$.

Proof. We carry out the proof in several steps.

Step 1: R_φ is contained in the integral closure of A in K_φ. Multiplication by any element $\rho \in R_\varphi$ carries the finitely generated A-module Λ into itself. Thus ρ is integral over A of degree at most d.

Step 2: For any nonzero $\rho \in R_\varphi$, let $\lambda_1, \dots, \lambda_I$, where $\lambda_1 = 0$ and $I = I(\rho)$, be a complete set of coset representatives for Λ in $(1/\rho)\Lambda$. Then $e(\rho z) = \varphi(\rho)(e(z))$, for a unique twisted polynomial $\varphi(\rho) \in K_\varphi(e(\lambda_2), \dots, e(\lambda_I))\{F\}$. By comparing zeros and coefficients of z, we see that

$$e(\rho z) = \rho e(\lambda_2)^{-1} \cdots e(\lambda_I)^{-1} \prod_{i=1}^{I} e(z - \lambda_i).$$

Since the values $e(\lambda_i)$ form a finite $\mathbb{F}_q$-vector space, the polynomial

$$P_\rho(X) = \rho e(\lambda_2)^{-1} \cdots e(\lambda_I)^{-1} \prod_{i=1}^{I} (X - e(\lambda_i))$$

has the form

$$P_\rho(X) = \sum_{j=0}^{J} c_j X^{q^j}$$

with $c_j \in K_\varphi(e(\lambda_2), \dots, e(\lambda_I))$. Thus we have the existence of

$$\varphi(\rho) = \sum_{j=0}^{J} c_j F^j \in K_\varphi(e(\lambda_2), \dots, e(\lambda_I))\{F\},$$

satisfying (2). Since the λ_i are uniquely determined modulo Λ and $e(\lambda_i + \lambda) = e(\lambda_i)$ for all $\lambda \in \Lambda$, the polynomial $P_\rho(X)$ and thus $\varphi(\rho)$ are uniquely determined.

Step 3: If $\rho \in R_\varphi \setminus \{0\}$ and $\lambda \in (1/\rho)\Lambda$, then $e(\lambda)$ is separable algebraic over l. As $(1/\rho)\Lambda/\Lambda$ is a finite A-module, there is a nonzero $a \in A$ such that $a \cdot (1/\rho)\Lambda \subset \Lambda$. Thus for $\lambda \in (1/\rho)\Lambda$, $0 = e(a\lambda) = \varphi(a)e(\lambda)$. Therefore $e(\lambda)$ is a root of the polynomial

$$P_a(X) = \varphi(a)X = aX + \varphi_1(a)X^q + \cdots + \varphi_i(a)X^{q^i}.$$

Since $P_a'(X) = a \neq 0$, $P_a(X)$ has no repeated roots and $e(\lambda)$ is separable algebraic over l.

Step 4: There is a finite separable extension L_φ of lK_φ such that $\varphi(R_\varphi) \subset L_\varphi\{F\}$. Let $\rho_1, \ldots, \rho_r$ be a maximal A-linearly independent subset of R_φ. Let L_φ' denote the field extension of lK_φ generated by the finitely many values occurring in the sets $e((1/\rho_1)\Lambda), \ldots, e((1/\rho_r)\Lambda)$. Since the preceding step shows that each value is separable over l, L_φ' is a finite separable extension of lK_φ.

For each nonzero $\rho \in R_\varphi$, there are $a_0, a_1, \ldots, a_r \in A$ such that

$$a_0\rho = a_1\rho_1 + \cdots + a_r\rho_r, \quad a_0 \neq 0.$$

Since φ is a ring homomorphism,

$$\varphi(a_0)\varphi(\rho) = \varphi(a_1)\varphi(\rho_1) + \cdots + \varphi(a_r)\varphi(\rho_r),$$

with each $\varphi(a_i) \in l\{F\}$. It is not hard to check by solving recursively for coefficients that the ring $l\{\{F\}\}$ of twisted power series contains $\varphi(a_0)^{-1}$. Thus

$$\varphi(\rho) = \varphi(a_0)^{-1}\varphi(a_1)\varphi(\rho_1) + \cdots + \varphi(a_0)^{-1}\varphi(a_r)\varphi(\rho_r)$$

lies in $\bar{k}_\infty\{F\} \cap L_\varphi'\{\{F\}\} = L_\varphi'\{F\}$.

Now let $L_\varphi = \bigcap L_\varphi'$, where the intersection runs over all choices of $\rho_1, \ldots, \rho_r$. ❑

C. A Further Reduction

REMARK 2.3. We may assume without loss of generality that

$$\varphi(A\rho_1 + \cdots + A\rho_r) \subset A_\varphi\{F\},$$

where A_φ denotes the integral closure of A in L_φ.

Proof. Recall that $A = \mathbb{F}_q[t]$. Let $a_* \in A$ be a common denominator for the coefficients of $\varphi(t), \varphi(\rho_1), \ldots, \varphi(\rho_r)$. Then if we replace Λ by the lattice $\Lambda^* = a_*^{-1}\Lambda$, the associated Drinfeld module $\varphi^* = \varphi_{a_*^{-1}\Lambda}$ satisfies

$$e(z) = e_\varphi(z) = a_* e_{\varphi^*}(a_*^{-1}z),$$

and if $\varphi(\rho) = \rho + \varphi_1(\rho)F + \cdots + \varphi_i(\rho)F^i$ then

$$\varphi^*(\rho) = \rho + a_*^{q-1}\varphi_1(\rho)F + \cdots + a_*^{q^i-1}\varphi_i(\rho)F^i \in A_\varphi\{F\}.$$

Since this holds for $\rho = t$, we see also that $\varphi^*(t^j) = \varphi^*(t)^j \in A_\varphi\{F\}$ for all $j \in \mathbb{N}$, and by linearity $\varphi^*(\mathbb{F}_q[t]) \subseteq A_\varphi\{F\}$. Moreover, $d^* = \operatorname{rank}_A \Lambda^* = d$ and $R_{\varphi^*} = R_\varphi$, so that $r^* = r$ and φ^* is defined over l.

Now if the hypotheses of the theorem are fulfilled, they are also fulfilled for the sets $\{\beta_i\}$ and $\{u_\nu^*\}$, where $u_\nu^* = a_*^{-1}u_\nu$ $(\nu = 1, \ldots, \kappa)$. If we can establish the Theorem for $e_{\varphi^*}(z)$ then, since each $e(\beta_i u_\nu) = a_* e_{\varphi^*}(\beta_i u_\nu^*)$ and $a_* \in A$, we will have the conclusion of the theorem for $e(z)$. ❑

III. Proof of Theorem

A. Notation and Preliminary Estimates

In the course of our proof, we will use $c_1, c_2, \dots$ to designate sufficiently large positive constants depending on $\varphi, \beta_1, \dots, \beta_b, u_1, \dots, u_\kappa$, and any c_i with lower index i, but not upon the parameters L, R, S, T, which are specified below. To establish our theorem we will consider the functions $e(\beta_1 z), \dots, e(\beta_b z)$ at points giving values in a finitely generated extension of k. To describe those points we recall our maximal A-linearly independent subset $\rho_1, \dots, \rho_r$ of R_φ. For $S > 0$, let $\mathfrak{M}_{r,\kappa}(S)$ be the set of all $r \times \kappa$ matrices $(a_{\mu\nu})$ with entries in A having $d_\infty(a_{\mu\nu}) < S$.

We then consider the set

$$\mathfrak{U}(S) = \{u_{\mathbf{a}} = (\rho_1, \dots, \rho_r)\mathbf{a}(u_1, \dots, u_\kappa)^{\mathrm{tr}} : \mathbf{a} \in \mathfrak{M}_{r,\kappa}(S)\},$$

where "tr" denotes the transpose of the vector.

We recall that

$$e(z) = \sum_{h=0}^{\infty} b_h z^{q^h}$$

is a so-called E_q-function with respect to l, the field of definition of φ. This means that we have control of the arithmetic growth of the coefficients b_h in the following sense: To begin with, each $b_h \in l$; if we let $\|b_h\| = \max\{d_\infty(b_h') : b_h'$ is a conjugate of b_h over $k\}$ then there exists a constant C_e such that $\|b_h\| \le C_e$ for all $h \in \mathbb{N}$. Moreover, according to Lemma 3.1 of [Y3], there is a nonzero sequence $\{a_h\} \subseteq A$ and a positive constant c with:

(i) $d_\infty(a_h) \le chq^h$;
(ii) for all $j \le h$, $a_h b_j \in l$ is integral over A;
(iii) if $q^{h_1} + \dots + q^{h_s} < q^N$, then $a_{h_1} \cdots a_{h_s} \mid a_N$.

This information will help us to understand the arithmetic of the values $e(\beta_i u_{\mathbf{a}})$ with $u_{\mathbf{a}} \in \mathfrak{U}(S)$. We first note that for $u_{\mathbf{a}}$ fixed we can write

$$e(\beta_i z) = e(\beta_i u_{\mathbf{a}}) + \sum_{h=0}^{\infty} b_h (\beta_i z - \beta_i u_{\mathbf{a}})^{q^h}. \tag{3}$$

Our first aim is to express each $e(\beta_i u_{\mathbf{a}})$ in terms of $e(\beta_i u_1), \dots, e(\beta_i u_\kappa)$. From the definition of $u_{\mathbf{a}}$ we have that

$$\begin{aligned} e(\beta_i u_{\mathbf{a}}) &= e(\beta_i \cdot (\rho_1, \dots, \rho_r)\mathbf{a}(u_1, \dots, u_\kappa)^{\mathrm{tr}}) \\ &= e\left(\sum_{\mu=1}^{r} \sum_{\nu=1}^{\kappa} \rho_\mu a_{\mu\nu} \beta_i u_\nu\right). \end{aligned}$$

We recall that the Drinfeld action φ has been extended to R_φ; hence

$$e(\beta_i u_{\mathbf{a}}) = \sum_{\mu=1}^{r} \sum_{\nu=1}^{\kappa} \varphi(\rho_\mu a_{\mu\nu}) e(\beta_i u_\nu).$$

Thus we express $e(\beta_i u_{\mathbf{a}})$ as

$$e(\beta_i u_{\mathbf{a}}) = \sum_{\nu=1}^{\kappa} P_{i,\nu,\mathbf{a}}(e(\beta_i u_\nu)),$$

with $\mathbb{F}_q$-linear polynomials $P_{i,\nu,\mathbf{a}} \in L_\varphi[X]$ satisfying

$$\deg_X P_{i,\nu,\mathbf{a}} \leq q^{c_1 + d \max d_\infty(a_{\mu\nu})}$$

and, by Lemma 2.1,

$$d_\infty(\text{coefficients of } P_{i,\nu,\mathbf{a}}) \leq q^{c_2 + d \max d_\infty(a_{\mu\nu})}.$$

In order to specify our function depending on the parameter T, we now adopt the working hypothesis that the claim of the theorem is false. This allows us to utilize the notation of the appendix, where we take $L = L_\varphi(\beta_1, \ldots, \beta_d)$, $K = L(e(\beta_i u_\nu))_{1 \leq i \leq b, 1 \leq \nu \leq \kappa}$, $s=1$, $\theta_1 = \theta$ to be a fixed transcendental value $e(\beta_{i'} u_{\nu'})$, and $n = [K : L(\theta)]$. (By Yu's Drinfeld version of the Gelfond–Schneider theorem, we know that not both $e(\beta_1 u_1)$ and $e(\beta_2 u_1)$ can be algebraic over L.)

We can now rather explicitly describe the auxiliary function we need. Let T be a positive real number and let L and S be integers chosen to be maximal satisfying the inequalities

$$q^L < 5nqT^{r\kappa/(r\kappa+bd)} q^{T(r\kappa+d)/(r\kappa+bd)} \quad \text{and} \quad q^S < T^{b/(r\kappa+bd)} q^{T(b-1)/(r\kappa+bd)}. \tag{4}$$

Let $\mathfrak{L} = \{l = (l_1, \ldots, l_b) : 0 \leq l_i < q^L, 1 \leq i \leq b\}$. For $l \in \mathfrak{L}$, let

$$\mathbf{e}(z)^l = e(\beta_1 z)^{l_1} e(\beta_2 z)^{l_2} \cdots e(\beta_b z)^{l_b}.$$

We consider a function of the form

$$F_T(z) = \sum_{l \in \mathfrak{L}} \gamma_l \mathbf{e}(z)^l, \tag{5}$$

where the coordinates γ_l are treated as unknowns.

Our goal is to find $\gamma_l \in A_\varphi[\theta]$ (not all zero) so that $F_T(z)$ has a zero of order at least q^T at each point $u_{\mathbf{a}} \in \mathfrak{U}(S)$. This means that when $F_T(z)$ is expanded as a Taylor series about a fixed $u_{\mathbf{a}}$,

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

we have

$$f_j(\mathbf{a}) = 0, \quad j = 0, \ldots, q^T - 1.$$

To obtain this Taylor series at $u_{\mathbf{a}}$ we take the representation (5) of $F_T(z)$ and replace each function $e(\beta_i z)$ by its Taylor expansion (3).

Thus at $u_{\mathbf{a}}$ we can write

$$F_T(z) = \sum_{l \in \mathfrak{L}} \gamma_l \prod_{i=1}^{b} \left\{ \sum_{\nu=1}^{\kappa} P_{i,\nu,\mathbf{a}}(e(\beta_i u_\nu)) + \sum_{h=0}^{\infty} b_h \beta_i^{q^h} (z - u_{\mathbf{a}})^{q^h} \right\}^{l_i}.$$

For $j \geq 0$, let $h = h(j) = \max\{0, 1 + [\log_q j]\}$. Then, by Lemma 4.1 of the Appendix, we see that, for each fixed $u_{\mathbf{a}} \in \mathfrak{U}(S)$, there are polynomials $P_0^{j\mathbf{a}}(\theta), P_{\sigma l}^{j\mathbf{a}}(\theta) \in A_\varphi[\theta]$, $P_0^{j\mathbf{a}}(\theta) \neq 0$, such that

$$P_0^{j\mathbf{a}}(\theta)a_h f_j(\mathbf{a}) = \sum_{l\in\mathcal{L}} \gamma_l \sum_{\sigma=1}^{n} P_{\sigma l}^{j\mathbf{a}}(\theta)\eta_\sigma, \tag{6}$$

and

$$\begin{aligned} D(P_0^{j\mathbf{a}}(\theta)), D(P_{\sigma l}^{j\mathbf{a}}(\theta)) &\le bq^L \cdot q^{c_3+d\max d_\infty(a_{\mu\nu})} \le c_4 q^{L+dS}; \\ h(P_0^{j\mathbf{a}}(\theta)), h(P_{\sigma l}^{j\mathbf{a}}(\theta)) &\le bq^L \cdot q^{c_5+d\max d_\infty(a_{\mu\nu})} + c_6 j\log j \\ &\le c_7(q^{L+dS}+Tq^T). \end{aligned} \tag{7}$$

REMARK 3.1. We note for later use that the representation (6) with the bounds (7) holds for arbitrary $L, S, T \ge 1$, not only for $S = S(T)$ and $L = L(T)$.

B. *Choice of Auxiliary Function*

We force our auxiliary function $F_T(z)$ to vanish at the points of $\mathfrak{U}(S)$ to order q^T by setting equal to zero the coefficients of each η_σ appearing in (6). Thus we obtain $M = nq^{T+r\kappa S}$ equations in $N = q^{bL}$ unknowns. Since

$$bL \ge 1 + \log_q 4n + T + r\kappa S,$$

we can apply the Thue–Siegel lemma of the Appendix to choose nontrivial $\gamma_l \in A_\varphi[\theta]$ so that

(i) $F_T(z)$ has zeros of order at least q^T at the points $u_\mathbf{a} \in \mathfrak{U}(S)$, and moreover

(ii) $D(\gamma_l) \le c_9(q^{L+dS})$ and $h(\gamma_l) \le c_{10}(q^{L+dS}+Tq^T)$.

REMARK 3.2. We note for later use that, according to Lemma 4.1 of the Appendix, for this choice of $F_T(z)$, when $j \le q^T$ and $u_\mathbf{a} \in \mathfrak{U}(S')$ with $S' \ge S$, there are polynomials $Q_0^{j\mathbf{a}}(\theta), Q_{\sigma l}^{j\mathbf{a}}(\theta) \in A_\varphi[\theta]$ with

$$\max\{D(Q_0^{j\mathbf{a}}(\theta)), D(Q_{\sigma l}^{j\mathbf{a}}(\theta))\} \le c_{11}(q^{L+dS'})$$

and

$$\max\{h(Q_0^{j\mathbf{a}}(\theta), h(Q_{\sigma l}^{j\mathbf{a}}(\theta))\} \le c_{12}(q^{L+dS'}+Tq^T)$$

such that

$$f_j(\mathbf{a}) = \sum_{\sigma=1}^{n} \frac{Q_{\sigma l}^{j\mathbf{a}}(\theta)\eta_\sigma}{Q_0^{j\mathbf{a}}(\theta)}.$$

That is,

$$\begin{aligned} D(f_j(\mathbf{a})) &\le c_{13}q^{L+dS'}; \\ h(f_j(\mathbf{a})) &\le c_{14}(q^{L+dS'}+Tq^T). \end{aligned}$$

C. *Zero Estimates*

CLAIM 3.3. *There is a constant c_{15} such that, for some $0 \le j < q^T$ and $\mathbf{a}' \in \mathfrak{M}_{r,\kappa}(c_{15}+S)$,*

$$f_j(\mathbf{a}') \ne 0.$$

Proof. Let $G=(\mathbb{G}_a(\bar{k}_\infty),\varphi)$ be the "Drinfeld module" with associated exponential function $e(z)$, and consider the t-module $G^b=G\times\cdots\times G$ and the analytic homomorphism $\Phi:\bar{k}_\infty\to G^b(\bar{k}_\infty)$ defined by

$$\Phi(z)=(e(\beta_1 z),\ldots,e(\beta_b z)).$$

For every positive real number S', let

$$\Gamma(S')=\{\Phi(u_{\mathrm{a}}): u_{\mathrm{a}}\in\mathcal{U}(S')\}.$$

We have constructed a polynomial $P(X_1,\ldots,X_b)$ with $\deg_{X_i}P\le q^L$ and such that $P(X_1,\ldots,X_b)$ vanishes along Φ to order at least q^T at all points $\gamma_{\mathrm{a}}\in\Gamma(S)$.

If our constructed polynomial $P(X_1,\ldots,X_b)$ vanishes along Φ to order at least q^T at all points $\gamma_{\mathrm{a}}\in\Gamma(S')$, then Theorem 2.1 of [Y5] tells us that there exists a proper algebraic $\mathbb{F}_q[t]$-submodule $H\subset G^b$ such that

$$(q^T-1)\operatorname{card}\left(\frac{\Gamma(S'-b+1)+H}{H}\right)\le c(G)(q^L)^{\operatorname{cod}_G H}. \tag{8}$$

Our immediate goal is to show that for some constant c_{16}, inequality (8) cannot hold for any proper algebraic $\mathbb{F}_q[t]$-submodule $H\subset G^b$ with $S'=c_{16}+S$. By our choice of parameters (4), it is easy to see that there exists a constant c_{17} such that, when $S'=c_{17}+S$, inequality (8) cannot hold for $H=0$.

Hence, by our choice of parameters (4), for $H\ne\{0\}$ we obtain from (8) that

$$\operatorname{card}\left(\frac{\Gamma(S'-b+1)+H}{H}\right)<\operatorname{card}(\Gamma(S'-b+1)),$$

and consequently there exists $u_{\mathrm{a}}\in\mathcal{U}(S'-b+1)$ with $\Phi(u_{\mathrm{a}})\in H$.

Now let $\pi_i: G^b\to G$ denote projection onto the ith factor of G^b. By Theorem 1.3 of [Y5], there then exist endomorphisms $f_1,\ldots,f_b$ of G (not all trivial) such that for every $h\in H$,

$$f_1\circ\pi_1(h)+\cdots+f_b\circ\pi_b(h)=0.$$

In particular, for $h=\Phi(u_{\mathrm{a}})$ we obtain

$$f_1\circ e(\beta_1 u_{\mathrm{a}})+\cdots+f_b\circ e(\beta_b u_{\mathrm{a}})=0.$$

As we have identified the endomorphism ring of G with R_φ, we have

$$e\left(\sum_{i=1}^b f_i\beta_i u_{\mathrm{a}}\right)=0.$$

Since $u_{\mathrm{a}}\ne 0$ and the β_i are K_φ-linearly independent with some $f_i\in R_\varphi$ nonzero,

$$\left(\sum_{i=1}^b f_i\beta_i\right)u_{\mathrm{a}}=\lambda\in\Lambda$$

with $\lambda\ne 0$. This is contradicted by hypothesis (3) of our theorem. Hence our claim is established. □

D. Smallness of Nonzero Hyperderivative

Select a pair $(\mathbf{a}', j)$ satisfying Claim 3.2 in which, first of all, $\max d_\infty(a'_{\mu\nu})$ is minimal and then j is minimal. Then $\mathbf{a}' \in \mathfrak{M}_{r,\kappa}(S') \setminus \mathfrak{M}_{r,\kappa}(S)$. So, since the order of zero of $F_T(z)$ at $u_{\mathbf{a}'} \notin \mathfrak{U}(S)$ is j, the entire function

$$G_T(z) := \frac{F_T(z)}{(z-u_{\mathbf{a}'})^j \prod (z-u_{\mathbf{a}})^{q^T}},$$

where the product here (and in the next displayed line) runs over all elements of $\mathfrak{M}_{r,\kappa}(S)$, satisfies

$$G_T(u_{\mathbf{a}'}) = \frac{f_j(\mathbf{a}')}{\prod (u_{\mathbf{a}'}-u_{\mathbf{a}})^{q^T}}.$$

Recall that for an entire function

$$F(z) = \sum_{h=0}^{\infty} f_h z^h$$

on $\bar{k}_\infty$, the maximum modulus principle states that the maximum modulus is given in any one of several equivalent ways:

$$\begin{aligned} M_r(F) = \max_h \{d_\infty(f_h) + rh\} &= \sup_{d_\infty(z) \le r} d_\infty(F(z)) \\ &= \sup_{d_\infty(z) = r} d_\infty(F(z)). \end{aligned}$$

To apply this result to our function, we need the following lemma.

LEMMA 3.4. *There is a constant c_e such that for all $R > 0$, $M_R(e(z)) \le c_e \cdot q^{dR}$.*

Proof. We proceed along the lines of the proof of Lemma 2.4 of [Y1]. We remove an ϵ which appears in that result by appealing to Lemma 5.8 of [Ha], which gives that

$$d_\infty(b_h) \le (c''_e - h/d) q^h,$$

for some c''_e. The maximum over all of the right-hand terms in the inequality

$$d_\infty(b_h) + q^h R \le -(h/d) q^h + q^h (R + c''_e)$$

occurs when h is within distance 1 of

$$-\frac{1}{\log q} + d(R + c''_e).$$

Hence

$$M_R(e(z)) \le \frac{q}{d}\left(1 + \frac{1}{\log q}\right) q^{d(R+c''_e)} \le c_e q^{dR}. \qquad \square$$

Applying this bound and the maximum modulus principle to $G_T(z)$ in the usual way shows that for all $R > c_{18} + S$,

$$d_\infty(f_j(\mathbf{a}')) \leq -q^{T+r\kappa S}(R-S-c_{18})+c_{19}(q^{L+dS}+Tq^T+q^{L+dR}).$$

Keeping in mind that $b \geq 2$, we can apply this inequality with

$$R=\left(\frac{r\kappa+d}{d}\right)S$$

to obtain the following.

LEMMA 3.5. *For $S > c_{20}$,*

$$d_\infty(f_j(\mathbf{a}')) \leq -\frac{1}{c_{21}}T^{((b+1)r\kappa+bd)/(r\kappa+bd)}q^{b(r\kappa+d)T/(r\kappa+bd)}.$$

E. Application of Gelfond's Criterion

Now if

$$d_\infty(Q_0^{j\mathbf{a}'}(\theta)) \leq -\frac{1}{c_{22}}T^{((b+1)r\kappa+bd)/(r\kappa+bd)}q^{b(r\kappa+d)T/(r\kappa+bd)}, \tag{9}$$

we set

$$P_T(X)=Q_0^{j\mathbf{a}'}(X).$$

Otherwise, by Remark 3.2, we see that when we take the "norm" (i.e., the product over all conjugate expressions raised to the degree of inseparability) of $f_j(\mathbf{a})$ from K to K_θ, we obtain a nonzero rational function

$$R_T(\theta)=\frac{P_T(\theta)}{Q_T(\theta)}$$

with

(1) $P_T(\theta), Q_T(\theta)$ $(=Q_0^{j\mathbf{a}'}(\theta)^{[K:K_\theta]}) \in K_\theta$;
(2) $\max\{D(P_T(\theta)), D(Q_T(\theta))\} \leq c_{23}q^{L+dS} \leq c_{24}Tq^T$; and
(3) $\max\{h(P_T(\theta)), h(Q_T(\theta))\} \leq c_{25}Tq^T$.

By our lower bound on $d_\infty(Q_0^{j\mathbf{a}'}(\theta))$, we see that d_∞ of the "conjugates" of $f_j(\mathbf{a})$ are at most $\leq c_{26}Tq^T$. Thus

$$d_\infty(R_T(\theta)) \leq -\frac{1}{c_{27}}T^{((b+1)r\kappa+bd)/(r\kappa+bd)}q^{b(r\kappa+d)T/(r\kappa+bd)}.$$

Finally, by our negation of (9), we see that

$$d_\infty(P_T(\theta)) \leq -\frac{1}{c_{28}}T^{((b+1)r\kappa+bd)/(r\kappa+bd)}q^{b(r\kappa+d)T/(r\kappa+bd)}.$$

Now we apply Gelfond's criterion (see Appendix) to the sequence $\{P_T(X)\}$ to conclude that

$$\kappa < \frac{d}{r}\frac{b}{b-2},$$

contrary to our hypothesis. This establishes the theorem. □

IV. Appendix

In this section we collect a few of the results needed in our proof of the main theorem above. We retain the previous Drinfeld module notation.

To begin we let K be a finitely generated extension of a finite extension L of k. Our goal is to define a degree and a height for nonzero elements of K. To this end, fix a transcendence basis $\theta_1, \ldots, \theta_s$ for K over L; set $K_\theta = L(\theta_1, \ldots, \theta_s)$; and fix a vector space basis $\eta_1, \ldots, \eta_n$ for K over K_θ (with $\eta_1 = 1$). Additionally, let $\alpha_1, \ldots, \alpha_f$ denote a k-basis of L with each α_i integral (and $\alpha_1 = 1$). Let A_φ denote the A-span of $\{\alpha_1, \ldots, \alpha_f\}$.

An arbitrary nonzero element $x \in K$ can be written uniquely as

$$x = \left(\sum_{\sigma=1}^{n} P_\sigma(\theta_1, \ldots, \theta_s)\eta_\sigma \right) \Big/ P_0(\theta_1, \ldots, \theta_s), \tag{10}$$

where $P_0, P_1, \ldots, P_n$ are elements of $A_\varphi[X_0, \ldots, X_s]$ which are coprime in the sense that, when each P_i is written as

$$P_i(X_1, \ldots, X_s) = \sum_{\mathbf{d} = (d_1, \ldots, d_s)} \left(\sum_{j=1}^{f} a_{i,\mathbf{d},j}\alpha_j \right) X_1^{d_1} \cdots X_s^{d_s},$$

the collection of coefficients $a_{i,\mathbf{d},j}$ does not have any common factors from $A \setminus \mathbb{F}_q$. Let $\deg_X P$ denote the total degree of P as a polynomial in $X_1, \ldots, X_s$.

Given the representation of x as in (10) we define the degree of x, $D(x)$, and the height of x, $h(x)$, by

$$D(x) = \max\{\deg_X P_0, \ldots, \deg_X P_n\};$$

$$h(x) = \max\{d_\infty(a_{i,\mathbf{d},j})\}.$$

When $x = 0$, put $D(x) = -\infty$.

We call any nonzero multiple of $P_0(\theta_1, \ldots, \theta_s)$ which lies in $A_\varphi[\theta_1, \ldots, \theta_s]$ a *denominator* for x.

LEMMA 4.1. *Let* $R_\eta = A_\varphi[\theta_1, \ldots, \theta_s]\eta_1 + \cdots + A_\varphi[\theta_1, \ldots, \theta_s]\eta_n$.

(1) *For* $x, y \in R_\eta$,

$$D(x+y) \le \max\{D(x), D(y)\} \text{ and } h(x+y) \le \max\{h(x), h(y)\}.$$

(2) *There are positive real constants* C_D *and* C_h *such that for any elements* $x_1, \ldots, x_l$ *in* K,

$$D(x_1 \cdots x_l) \le D(x_1) + \cdots + D(x_l) + C_D(l-1);$$

$$h(x_1 \cdots x_l) \le h(x_1) + \cdots + h(x_l) + C_h(l-1).$$

(3) *For* $x \in K_\theta$ *and* $y \in R_\eta$, $D(xy) = D(x) + D(y)$ *and* $h(xy) = h(x) + h(y)$.

Proof. Standard. (Compare, for example, [Th, §IV] or, for great generality, a forthcoming paper of P. Philippon.) □

Thiery [Th] has proved a version of Gelfond's criterion in this setting for an element $\pi \in \bar{k}_\infty$ to be algebraic over k.

LEMMA 4.2 (Gelfond's criterion). *Suppose that $\pi \in \bar{k}_\infty$ and that $(P_n)_n$ is an infinite sequence of polynomials in $A[X]$. Let*

$$\delta_n = D(P_n), \quad h_n = h(P_n), \quad \textit{and} \quad s_n = -d_\infty(P_n(\pi)).$$

If for all $n \geq N_0$ one has

$$s_n > \max\{h_n\delta_n + h_n\delta_{n+1} + h_{n+1}\delta_n,\ h_n\delta_n + h_n\delta_{n-1} + h_{n-1}\delta_n\}$$

and

$$\lim_{n\to\infty}\left(\frac{s_n}{\delta_n} - h_n\right) = +\infty,$$

then $P_n(\pi) = 0$ for all $n \geq N_0$.

Proof. See [Th, Prop. 3]. □

This version of Gelfond's criterion applies in the analogue of Gelfond's setting [Ge], namely when the values under consideration are assumed to generate a field of transcendence degree 1 over K_φ. The usual transcendence techniques providing a sequence of polynomials satisfying this criterion rest, as in the classical case, on a construction of auxiliary functions. This construction ultimately is based upon Dirichlet's box principle, codified in the following lemma.

LEMMA 4.3 (Thue–Siegel lemma). *Let K and L be fields as above. When $N \geq 2^{s+1}M$ and $a_{ij} \in A_\varphi[\theta_1, \ldots, \theta_s]$ $(1 \leq i \leq N,\ 1 \leq j \leq M)$, the system of M equations*

$$\sum_{i=1}^{N} a_{ij}x_i = 0, \quad 1 \leq j \leq M,$$

has a nontrivial solution $x_1, \ldots, x_N$ in $A_\varphi[\theta_1, \ldots, \theta_s]$ with

$$\max D(x_i) \leq \max D(a_{ij})$$

and

$$\max h(x_i) \leq \max h(a_{ij}) + C_h + 2d_\infty(t),$$

where C_h is the constant from Lemma 4.1.

Proof. For positive integers D and H, let

$$\Omega_{H,D} = \{(\omega_i)_{1\leq i\leq N} \in A_\varphi[\theta_1, \ldots, \theta_s]^N : \max D(\omega_i) \leq D,\ \max h(\omega_i) < H\}.$$

Then

$$q^{[H/d_\infty(t)]N\binom{D+s}{s}f} \leq \operatorname{card}(\Omega_{H,D}) \leq q^{(H/d_\infty(t))N\binom{D+s}{s}f}.$$

For $\omega=(\omega_1,\dots,\omega_N)\in\Omega_{H,D}$,

$$D\left(\sum_{i=1}^{N} a_{ij}\omega_i\right)\le D+\max D(a_{ij})$$

and

$$h\left(\sum_{i=1}^{N} a_{ij}\omega_i\right)\le H+\max h(a_{ij})+C_h$$

for $j=1,\dots,M$. But the number of distinct M-tuples from $A_\varphi[\theta_1,\dots,\theta_s]$ satisfying these bounds is at most

$$q^{\left[f\cdot M\cdot\frac{(H+\max h(a_{ij})+C_h)}{d_\infty(t)}\binom{D+\max D(a_{ij})+s}{s}\right]}.$$

Then we have a nontrivial solution of our system of equations as soon as

$$M\frac{(H+\max h(a_{ij})+C_h)}{d_\infty(t)}\binom{D+\max D(a_{ij})+s}{s}<N\binom{D+s}{s}\left[\frac{H}{d_\infty(t)}\right]$$

or

$$\frac{N}{M}\ge\frac{H+\max h(a_{ij})+C_h}{H-d_\infty(t)}\left(\binom{D+\max D(a_{ij})+s}{s}\Big/\binom{D+s}{s}\right).$$

Since

$$\left(\binom{D+\max D(a_{ij})+s}{s}\Big/\binom{D+s}{s}\right)\le\left(\frac{D+\max D(a_{ij})}{D}\right)^s,$$

it is sufficient to choose D and H so large that

$$\frac{N}{M}\ge\frac{H+\max h(a_{ij})+C_h}{H-d_\infty(t)}\left(\frac{D+\max D(a_{ij})}{D}\right)^s.$$

Now choose $H\ge 2d_\infty(t)+\max h(a_{ij})+C_h$ and $D\ge\max D(a_{ij})$. □

HYPERDERIVATIVES. Our nonzero auxiliary functions will be constructed with a certain vanishing of the initial coefficients in their Taylor series (at various prescribed points). It is convenient to be able to describe these coefficients via a notion of derivation in positive characteristic.

For a fixed analytic homomorphism $\Phi:\bar{k}_\infty^n\to G_a^m(\bar{k}_\infty)$ and a given polynomial $Q(\mathbf{X})=(X_1,\dots,X_m)$ over $\bar{k}_\infty$, Yu [Y5] defines the *hyperderivatives of Q with respect to Φ* as the coefficients in the Taylor series

$$Q(\mathbf{X}+\Phi(\mathbf{z}))=\sum_j\{\Delta_{\mathbf{j}}^{\Phi}Q(\mathbf{X})\}\mathbf{z}^{\mathbf{j}},$$

where $\mathbf{j}=(j_1,\dots,j_m)$ and $\mathbf{z}^{\mathbf{j}}=z_1^{j_1}\cdots z_m^{j_m}$.

In particular,

$$Q(\mathbf{X}+\Phi(\mathbf{z}-\omega))=\sum_j\{\Delta_{\mathbf{j}}^{\Phi}Q(\mathbf{X})\}(\mathbf{z}-\omega)^{\mathbf{j}}$$

and

$$Q(\Phi(\omega)+\Phi(\mathbf{z}-\omega))=\sum_j\{\Delta_{\mathbf{j}}^{\Phi}Q(\Phi(\omega))\}(\mathbf{z}-\omega)^{\mathbf{j}}.$$

Since Φ is additive, we see that

$$Q(\Phi(\mathbf{z})) = \sum_{j} \{\Delta_{\mathbf{j}}^{\Phi} Q(\Phi(\omega))\}(\mathbf{z}-\omega)^{\mathbf{j}}.$$

In other words, the hyperderivatives $\Delta_{\mathbf{j}}^{\Phi} Q(\Phi(\omega))$ are the coefficients of the power series expansions of the composite $Q \circ \Phi$ at points ω.

If, for some $\omega \in \bar{k}_{\infty}^{n}$, the hyperderivatives vanish for all $\mathbf{j}$ with $0 \leq j_i < T$, we say that $Q(\mathbf{X})$ *vanishes to order* T *at* $\Phi(\omega)$ *along* Φ.

References

[Dr] V. G. Drinfeld, *Elliptic modules,* Mat. Sb. (N.S.) 94 (1974), 594–627; translation in Math. USSR-Sb. 23 (1974), 561–592.

[Ge] A. O. Gelfond, *On the algebraic independence of transcendental numbers of certain classes,* Uspekhi Mat. Nauk 4 (1949), 14–48; translation in Amer. Math. Soc. Transl. 66 (1952).

[Ha] D. R. Hayes, *Explicit class field theory in global function fields,* Studies in algebra and number theory (G.-C. Rota, ed.), pp. 173–217, Academic Press, New York, 1979.

[Si] J. H. Silverman, *The arithmetic of elliptic curves,* Springer, New York, 1986.

[Y1] J. Yu, *Transcendence theory over function fields,* Duke Math. J. 52 (1985), 517–527.

[Y2] ———, *A six exponentials theorem in finite characteristic,* Math. Ann. 272 (1985), 91–98.

[Y3] ———, *Transcendence and Drinfeld modules,* Invent. Math. 83 (1986), 507–517.

[Y4] ———, *Transcendence and Drinfeld modules: several variables,* Duke Math. J. 58 (1989), 559–575.

[Y5] ———, *Analytic homomorphisms into Drinfeld modules* (to appear).

[Th] A. Thiery, *Indépendance algébrique des périodes et quasi-périodes d'un module de Drinfeld,* The arithmetic of function fields, (D. Goss, D. R. Hayes, M. I. Rosen, eds.), pp. 265–284, W. DeGruyter, Berlin, 1992.

P.-G. Becker
Mathematisches Institut der
Universität zu Köln
Weyertal 86-90
D-50931 Köln
Germany

W. D. Brownawell
Mathematics Department
Penn State University
University Park, PA 16802

R. Tubbs
Mathematics Department
University of Colorado
Boulder, CO 80309