

EXPLICIT FORMULAS FOR DRINFELD MODULES AND THEIR PERIODS

AHMAD EL-GUINDY AND MATTHEW A. PAPANIKOLAS

ABSTRACT. We provide explicit series expansions for the exponential and logarithm functions attached to a rank r Drinfeld module that generalize well known formulas for the Carlitz exponential and logarithm. Using these results we obtain a procedure and an analytic expression for computing the periods of rank 2 Drinfeld modules and also a criterion for supersingularity.

1. INTRODUCTION

The goal of this paper is to determine explicit formulas for exponential functions, logarithms, and periods of Drinfeld modules. Originally Carlitz [1] and Wade [16] worked out a complete picture for the Carlitz module by deducing closed formulas for both the power series expansions of its associated exponential and logarithm functions and the Carlitz period. Building on work of Hayes [9] on sgn-normalized Drinfeld modules of rank 1, Gekeler [5] determined formulas for periods of rank 1. Later Thakur [13], [14], building on Hayes' work, found explicit formulas for exponentials and logarithms of rank 1 modules using special values of shtuka functions. (See also [8, Ch. 3, 4, 7] and [15, Ch. 2, 8] for more information.) In the current paper we have attempted to continue these investigations in a similar spirit for Drinfeld modules of arbitrary rank by developing a combinatorial framework of “shadowed partitions” to keep track of coefficient data. As a result we obtain explicit formulas for the exponential and logarithm functions and for periods, and we further obtain a precise criterion for supersingularity that complements previous work of Cornelissen [3], [4] and Gekeler [6].

Let q be a power of a prime p , and let \mathbb{F}_q denote the field with q elements. Consider the polynomial ring $\mathbb{A} = \mathbb{F}_q[T]$, and let \mathbb{K} denote the fraction field of \mathbb{A} . Consider the unique valuation on \mathbb{K} defined by

$$v(T) = -1,$$

which is the valuation at the “infinite prime” of the ring \mathbb{A} . Let \mathbb{K}_∞ denote the completion of \mathbb{K} with respect to v , and let \mathbb{C}_∞ denote the completion of an algebraic closure of \mathbb{K}_∞ . It is well known that v has a unique extension to \mathbb{C}_∞ that we still denote by v , and that \mathbb{C}_∞ is a complete algebraically closed field. For any integer $n \in \mathbb{N} = \{0, 1, \dots\}$ we write

$$\begin{aligned} [n] &:= T^{q^n} - T, \\ (1) \quad D_n &:= [n][n-1]^q[n-2]^{q^2} \cdots [1]^{q^{n-1}}, \quad D_0 := 1, \\ L_n &:= (-1)^n [n][n-1] \cdots [2][1], \quad L_0 := 1. \end{aligned}$$

Date: December 22, 2011.

2010 Mathematics Subject Classification. 11G09, 11F52, 11R58.

Key words and phrases. Drinfeld modules, exponentials, logarithms, periods, supersingularity.

Research of the second author was partially supported by NSF Grant DMS-0903838.

A field L is called an \mathbb{A} -*field* if there is a nonzero homomorphism $\iota : \mathbb{A} \rightarrow L$. Examples of such fields are extensions of either \mathbb{K} or \mathbb{A}/\mathfrak{p} , where \mathfrak{p} is a nonzero prime ideal of \mathbb{A} . For simplicity we will write a in place of $\iota(a)$ when the context is clear. Such a field has a *Frobenius homomorphism*

$$\begin{aligned} \tau : L &\rightarrow L \\ z &\mapsto z^q, \end{aligned}$$

and we can consider the ring $L\{\tau\}$ of polynomials in τ under addition and composition. Thus $\tau\ell = \ell^q\tau$ for any $\ell \in L$. A *Drinfeld module of rank r over L* is an \mathbb{F}_q -linear ring homomorphism $\phi : \mathbb{A}[T] \rightarrow L\{\tau\}$ such that

$$(2) \quad \phi_T = T + \sum_{i=1}^r A_i \tau^i, \quad A_i \in L, \quad A_r \neq 0.$$

It then follows that the constant term of ϕ_a is a for all $a \in \mathbb{A}$ and that the degree of ϕ_a in τ is $r \deg_T(a)$.

The simplest example of a Drinfeld module is the *Carlitz module \mathcal{C}* given by

$$\mathcal{C}_T = T + \tau,$$

which has rank 1. Associated to the Carlitz module is the *Carlitz exponential*

$$(3) \quad e_{\mathcal{C}}(z) := \sum_{n=0}^{\infty} \frac{z^{q^n}}{D_n}.$$

The series for $e_{\mathcal{C}}$ converges for all $z \in \mathbb{C}_{\infty}$ and defines an entire, \mathbb{F}_q -linear, and surjective function. The key property connecting the Carlitz exponential to the Carlitz module is

$$(4) \quad e_{\mathcal{C}}(Tz) = \mathcal{C}_T(e_{\mathcal{C}}(z)),$$

from which it follows that for all $a \in \mathbb{A}$,

$$e_{\mathcal{C}}(az) = \mathcal{C}_a(e_{\mathcal{C}}(z)).$$

The zeros of $e_{\mathcal{C}}(z)$ form an \mathbb{A} -lattice of rank one in \mathbb{C}_{∞} with a certain generator $\pi_{\mathcal{C}} \in \mathbb{C}_{\infty}$ called the *Carlitz period*, and we have an alternate expression for the Carlitz exponential as

$$(5) \quad e_{\mathcal{C}}(z) = z \prod_{0 \neq \lambda \in \pi_{\mathcal{C}}\mathbb{A}} \left(1 - \frac{z}{\lambda}\right).$$

It is useful to also consider the (local) composition inverse of $e_{\mathcal{C}}$, called the *Carlitz logarithm*, defined by

$$(6) \quad \log_{\mathcal{C}}(z) := \sum_{n=0}^{\infty} \frac{z^{q^n}}{L_n}, \quad v(z) > \frac{-q}{q-1}.$$

These results go back to Carlitz [1] and Wade [16], who were investigating explicit class field theory over $\mathbb{F}_q(T)$. See [8, Ch. 3], [15, Ch. 2] for more details on the above constructions.

Analogues of (4), (5), and (6) hold for any Drinfeld module over \mathbb{C}_{∞} (see [8, Ch. 4], [15, Ch. 2] for more details). Indeed in [2], Carlitz himself had begun to study lattice functions for higher rank lattices long before Drinfeld developed the complete story. In particular, if $\Lambda \subset \mathbb{C}_{\infty}$ is an \mathbb{A} -lattice of rank r then the *lattice exponential function* defined by

$$(7) \quad e_{\Lambda}(z) := z \prod_{0 \neq \lambda \in \Lambda} \left(1 - \frac{z}{\lambda}\right)$$

is an entire, surjective, \mathbb{F}_q -linear function from \mathbb{C}_∞ to \mathbb{C}_∞ with kernel Λ , and there exists a unique rank r Drinfeld module $\phi = \phi(\Lambda)$ such that

$$(8) \quad e_\Lambda(Tz) = \phi_T(e_\Lambda(z)).$$

Furthermore, e_Λ has a series expansion of the form

$$(9) \quad e_\Lambda(z) = \sum_{n=0}^{\infty} \alpha_n z^{q^n}.$$

It also has a local composition inverse \log_Λ with a series expansion

$$(10) \quad \log_\Lambda(z) = \sum_{n=0}^{\infty} \beta_n z^{q^n}.$$

Note that the coefficients $\alpha_n \in \mathbb{C}_\infty$ (and consequently β_n) could be expressed in terms of Λ by expanding (7): for instance

$$(11) \quad \begin{aligned} \alpha_1 &= \sum_{\{\lambda_1, \dots, \lambda_{q-1}\} \subset \Lambda} \prod_{i=1}^{q-1} \frac{1}{\lambda_i}, \\ &\quad \lambda_i \neq \lambda_j \text{ for } i \neq j \\ \beta_1 &= -\alpha_1, \end{aligned}$$

which is explicit, but rather complicated and impractical as it involves infinitely many terms. We can also describe the Drinfeld module $\phi(\Lambda)$ in terms of Λ as follows. Start by noticing that $\Lambda/T\Lambda$ is a vector space of dimension r over \mathbb{F}_q . Write

$$(12) \quad f(x) := \prod_{\lambda \in \Lambda/T\Lambda} \left(x - e_\Lambda \left(\frac{\lambda}{T} \right) \right).$$

It is well-known (see [8, §4.3]) that $f(x)$ is \mathbb{F}_q -linear of degree q^r , hence of the form $f(x) = \sum_{n=0}^r A_n(\Lambda)x^{q^n}$ for some $A_n(\Lambda) \in \mathbb{C}_\infty$. Furthermore we have

$$(13) \quad \phi_T(\Lambda) = \sum_{n=0}^r A_n(\Lambda)\tau^n.$$

The general theme of the paper is in some sense to reverse the point of view of the previous paragraphs, and provide explicit identities for the lattice Λ , as well as the functions e_Λ and \log_Λ , starting only from the knowledge of the Drinfeld module ϕ . This is achieved by using relatively simple combinatorial objects that we name “shadowed partitions” which we introduce and study in §2. Using them, in §3 we obtain concrete formulas for e_Λ and \log_Λ (Theorem 3.1 and Theorem 3.3) that are as similar as could be hoped for to (3) and (6). In §4 we restrict our attention to rank 2 modules, and we proceed to study the convergence properties of \log_Λ making use of the detailed description we have for its coefficients (Corollary 4.2 and Corollary 4.3). In §5 we examine the properties of T -torsion points of rank two Drinfeld modules, and show how, combined with the properties of \log_Λ , we can recover at least one, and sometimes both generators of the lattice Λ in certain naturally defined “families” (Theorem 5.3), thus in some sense obtaining a converse of (13). In §6 we introduce additional conditions that enable us to obtain a completely analytic description for the period with maximal valuation (Theorem 6.3). In §7 we compare our results to an

example of Thakur [13] arising from Drinfeld modules with complex multiplication. Finally in §8 we study yet another application of shadowed partitions, where we introduce a “multinomial” theorem for any rank r Drinfeld module (Theorem 8.1) and obtain as a consequence a concrete condition for supersingularity of a rank 2 Drinfeld module at a prime $\mathfrak{p} \in \mathbb{A}$ of any degree (Corollary 8.2).

A note on notation. In order to emphasize that our starting point is the Drinfeld module rather than the lattice, from now on we shall write e_ϕ , \log_ϕ , and $A_n(\phi)$ instead of e_Λ , \log_Λ , and $A_n(\Lambda)$, respectively.

2. SHADOWED PARTITIONS

Recall that a *partition* of a set S is a collection of subsets of S that are pairwise disjoint, and whose union is equal to S itself. Also, if $S \subset \mathbb{Z}$, $j \in \mathbb{Z}$, then $S + j := \{i + j : i \in S\}$. For $r \in \mathbb{N}$ and $n \in \mathbb{Z}^+$, we set

$$(14) \quad P_r(n) := \{(S_1, S_2, \dots, S_r) : S_i \subset \{0, 1, \dots, n-1\}, \\ \text{and } \{S_i + j : 1 \leq i \leq r, 0 \leq j \leq i-1\} \text{ form a partition of } \{0, 1, \dots, n-1\}\}.$$

We also set $P_r(0) := \{\emptyset\}$ and $P_r(-n) := \emptyset$. We propose to name elements of $P_r(n)$ as *order r index-shadowed partitions of n* , or *shadowed partitions* for short, as each S_i relies on its i “shadows” $S_i + j$ (including itself) so that all together they partition n elements. Furthermore, for $1 \leq i \leq r$ we set

$$(15) \quad P_r^i(n) := \{(S_1, S_2, \dots, S_r) \in P_r(n) : 0 \in S_i\}.$$

We collect some simple, yet important facts about these objects in the following lemma. Recall that the sequence of *r -step Fibonacci numbers* $\{F_n^{(r)}\}$ is defined as follows ($n \in \mathbb{Z}^+$)

$$(16) \quad F_{-n}^{(r)} = 0, \quad F_0^{(r)} = 1, \quad F_n^{(r)} = \sum_{i=n-r}^{n-1} F_i^{(r)}.$$

Lemma 2.1. (i) $\{P_r^i(n) : 1 \leq i \leq r\}$ is a partition of $P_r(n)$.

(ii) For $1 \leq i \leq r$, $P_r(n-i)$ could be identified with $P_r^i(n)$ via the well-defined bijection

$$(17) \quad (S_1, S_2, \dots, S_r) \mapsto (S_1 + i, S_2 + i, \dots, \{0\} \cup (S_i + i), \dots, S_r + i).$$

(iii) For all $r > 0$ and all $n \in \mathbb{Z}$ we have $|P_r(n)| = F_n^{(r)}$.

Proof. The proofs of (i) and (ii) consist of simple verifications that we leave to the reader, and statement (iii) follows from combining (i) and (ii). \square

Let $S \subset \mathbb{N}$ be finite, and define the integer $w(S)$ by

$$(18) \quad w(S) := \sum_{i \in S} q^i.$$

Note that $w(\emptyset) = 0$. To help simplify our formulas, we shall usually denote $(S_1, \dots, S_r) \in P_r(n)$ by \mathbf{S} . We fix the following notation for the rest of the paper

$$|\mathbf{S}| := \sum_{i=1}^r |S_i|, \quad \bigcup \mathbf{S} := \bigcup_{i=1}^r S_i,$$

and

$$\mathbf{S} + i := (S_1 + i, \dots, S_r + i) \in P_r(n+i), \text{ for } i \in \mathbb{N}.$$

We collect some more facts that are relevant to our results.

Lemma 2.2. (i) For $\mathbf{S} \in P_r(n)$, $\cup \mathbf{S}$ uniquely defines \mathbf{S} . Hence

$$(19) \quad F_n^{(r)} = |P_r(n)| \leq 2^n.$$

(ii) The r -tuple of sets (S_1, \dots, S_r) is in $P_r(n)$ if and only if

$$(20) \quad \sum_{i=1}^r (q^i - 1)w(S_i) = q^n - 1.$$

Proof. To prove (i), write

$$\cup \mathbf{S} = \{s_1, s_2, \dots, s_m\},$$

with $s_i < s_{i+1}$. Note that the conditions in (14) on $P_r(n)$ imply that $1 \leq s_{i+1} - s_i \leq r$ and also $1 \leq n - s_m \leq r$. It follows that we must have

$$s_m \in S_{n-s_m},$$

and, for $1 \leq i \leq m - 1$

$$s_i \in S_{s_{i+1}-s_i}.$$

Thus the sets S_i are completely defined once we know $\cup \mathbf{S}$. It follows that the map

$$\cup : P_r(n) \rightarrow \text{Subsets of } \{0, \dots, n-1\}$$

is an injection, and (19) follows. To prove (20) divide both sides by $q - 1$ to get

$$\begin{aligned} w(S_1) + (q+1)w(S_2) + \dots + (q^{r-1} + q^{r-2} + \dots + q + 1)w(S_r) \\ = q^{n-1} + q^{n-2} + \dots + q + 1, \end{aligned}$$

and the statement of (ii) follows. \square

3. EXPLICIT FORMULAS FOR LATTICE FUNCTIONS

Let ϕ be a Drinfeld module of rank r over \mathbb{C}_∞ . The corresponding exponential function e_ϕ on \mathbb{C}_∞ satisfies

$$(21) \quad e_\phi(Tz) = \phi_T(e_\phi(z)).$$

It has the series expansion

$$e_\phi(z) = \sum_{n=0}^{\infty} \alpha_n z^{q^n},$$

with $\alpha_n = \alpha_n(\phi) \in \mathbb{C}_\infty$ and $\alpha_0 = 1$. In the next theorem we give an explicit formula for α_n in terms of the coefficients of ϕ , and thus we give a proof of the existence of e_ϕ different from (7). For notational convenience, for $(A_1, \dots, A_r) \in \mathbb{C}_\infty^r$ and $\mathbf{S} \in P_r(n)$ we write

$$(22) \quad \mathbf{A}^{\mathbf{S}} := \prod_{i=1}^r A_i^{w(S_i)}.$$

Note that $\mathbf{A}^\emptyset = 1$.

Theorem 3.1. *Let ϕ be a rank r Drinfeld module given by*

$$\phi_T = \sum_{i=0}^r A_i \tau^i, \quad A_i \in \mathbb{C}_\infty.$$

For $n \geq 0$ and for any $S \subset \{0, 1, \dots, n-1\}$ set

$$(23) \quad D_n(S) := \prod_{i \in S} [n-i]^{q^i}.$$

If we set

$$(24) \quad \alpha_n = \sum_{\mathbf{S} \in P_r(n)} \frac{\mathbf{A}^{\mathbf{S}}}{D_n(\cup \mathbf{S})},$$

then the series $\sum_{n=0}^{\infty} \alpha_n z^{q^n}$ converges on \mathbb{C}_∞ and is the unique solution to (21) with $\alpha_0 = 1$ and thus $\exp_\phi(z) = \sum_{n=0}^{\infty} \alpha_n z^{q^n}$.

Proof. The functional equation

$$e_\phi(Tz) = T e_\phi(z) + \sum_{i=1}^r A_i e_\phi(z)^{q^i}$$

is equivalent to the recursion

$$(25) \quad \alpha_n T^{q^n} = \sum_{i=0}^r A_i \alpha_{n-i}^{q^i}.$$

For convenience, we can set $\alpha_n = 0$ for $n < 0$ so that (25) holds for all $n \geq 0$. We proceed by induction on n to show that (24) is the unique solution to (25) with $\alpha_0 = 1$. Since $D_n(\emptyset) = 1$, formula (24) indeed gives $\alpha_0 = 1$. Substituting $A_0 = T$, the induction hypothesis gives

$$\begin{aligned} \alpha_n &= \frac{1}{[n]} \sum_{i=1}^r A_i \sum_{\mathbf{S} \in P_r(n-i)} \left(\frac{\mathbf{A}^{\mathbf{S}}}{D_{n-i}(\cup \mathbf{S})} \right)^{q^i} \\ &= \frac{1}{[n]} \sum_{i=1}^r A_i \sum_{\mathbf{S} \in P_r(n-i)} \frac{\mathbf{A}^{\mathbf{S}+i}}{D_n(\cup \mathbf{S} + i)} \\ &= \sum_{i=1}^r \sum_{\mathbf{S} \in P_r^i(n)} \frac{\mathbf{A}^{\mathbf{S}}}{D_n(\cup \mathbf{S})}, \end{aligned}$$

where the last equality follows from Lemma 2.1(ii) and the fact that

$$D_{n-i}(S)^{q^i} = D_n(S+i).$$

Thus (24) is proved.

We could deduce the convergence of $\sum \alpha_n z^{q^n}$ on all of \mathbb{C}_∞ by relying on the corresponding property of the lattice exponential function given by (7). However, to emphasize that our approach suffices to develop important aspects of the theory, we use (24) to give a direct proof from first principles. Note that $v([n-i]^{q^i}) = -q^n$, and thus $v(D_n(S)) = -q^n |S|$. It follows that for $\mathbf{S} \in P_r(n)$ we have

$$(26) \quad v(D_n(\cup \mathbf{S})) \leq -\frac{nq^n}{r}.$$

Next, set $v_0 = \min_{1 \leq i \leq r} v(A_i)$. It is easy to see that for $\mathbf{S} \in P_r(n)$ we have

$$(27) \quad v(\mathbf{A}^{\mathbf{S}}) \geq w(\cup \mathbf{S})v_0.$$

For $\mathbf{S} \in P_r(n)$ we have

$$\frac{q^n - 1}{q^r - 1} \leq w(\cup \mathbf{S}) \leq \frac{q^n - 1}{q - 1}.$$

Together with (26) and (27) we get

$$(28) \quad v(\alpha_n z^{q^n}) \geq \begin{cases} q^n \left(\frac{n}{r} + \frac{v_0}{q-1} + v(z) \right), & \text{if } v_0 < 0, \\ q^n \left(\frac{n}{r} + v(z) \right), & \text{if } v_0 \geq 0, \end{cases}$$

and it follows that

$$\lim_{n \rightarrow +\infty} v(\alpha_n z^{q^n}) = +\infty.$$

Hence the series converges for all $z \in \mathbb{C}_\infty$. \square

Example 3.2. We write a few concrete cases to clarify (24). Let the superscript on α indicate the rank r of the corresponding module. Then for $r = 2$ we get, for instance

$$\begin{aligned} \alpha_3^{(2)} &= \frac{A_1^{q^2+q+1}}{[1]^{q^2}[2]^q[3]} + \frac{A_2^q A_1}{[2]^q[3]} + \frac{A_1^{q^2} A_2}{[1]^{q^2}[3]}, \\ \alpha_4^{(2)} &= \frac{A_1^{q^3+q^2+q+1}}{[1]^{q^3}[2]^{q^2}[3]^q[4]} + \frac{A_2^q A_1^{q^3+1}}{[2]^{q^2}[3]^q[4]} + \frac{A_1^{q^3+q^2} A_2}{[1]^{q^3}[3]^q[4]} + \frac{A_2^{q^2} A_1^{q+1}}{[2]^{q^2}[3]^q[4]} + \frac{A_2^{q^2+1}}{[2]^{q^2}[4]}, \end{aligned}$$

whereas for $r = 3$ we get

$$\begin{aligned} \alpha_3^{(3)} &= \frac{A_1^{q^2+q+1}}{[1]^{q^2}[2]^q[3]} + \frac{A_2^q A_1}{[2]^q[3]} + \frac{A_1^{q^2} A_2}{[1]^{q^2}[3]} + \frac{A_3}{[3]}, \\ \alpha_4^{(3)} &= \frac{A_1^{q^3+q^2+q+1}}{[1]^{q^3}[2]^{q^2}[3]^q[4]} + \frac{A_2^q A_1^{q^3+1}}{[2]^{q^2}[3]^q[4]} + \frac{A_1^{q^3+q^2} A_2}{[1]^{q^3}[3]^q[4]} + \frac{A_2^{q^2} A_1^{q+1}}{[2]^{q^2}[3]^q[4]} \\ &\quad + \frac{A_2^{q^2+1}}{[2]^{q^2}[4]} + \frac{A_3 A_1^{q^3}}{[1]^{q^3}[4]} + \frac{A_3^q A_1}{[3]^q[4]}. \end{aligned}$$

Next we study the function \log_ϕ . From (21) we obtain the functional equation

$$(29) \quad T \log_\phi(z) = \log_\phi(\phi_T(z)).$$

The following proposition provides a concrete description of the coefficients of \log_ϕ .

Theorem 3.3. *Given a Drinfeld module ϕ of rank r , write*

$$\log_\phi(z) = \sum_{n=0}^{\infty} \beta_n z^{q^n}.$$

For $\mathbf{S} \in P_r(n)$ set

$$(30) \quad L(\mathbf{S}) := \prod_{j=1}^r \prod_{i \in S_j} (-[i+j]).$$

Then

$$(31) \quad \beta_n = \sum_{\mathbf{S} \in P_r(n)} \frac{\mathbf{A}^{\mathbf{S}}}{L(\mathbf{S})}.$$

Proof. Since $L(\emptyset) = 1$, we see that $\beta_0 = 1$, as expected. Now the functional equation (29) gives the recursion

$$(32) \quad T\beta_n = \sum_{i=0}^r \beta_{n-i} A_i^{q^{n-i}},$$

where again we set $\beta_n = 0$ for $n < 0$. Applying $A_0 = T$ and the induction hypothesis gives

$$(33) \quad -[n]\beta_n = \sum_{i=1}^r A_i^{q^{n-i}} \sum_{\mathbf{S} \in P_r(n-i)} \frac{\mathbf{A}^{\mathbf{S}}}{L(\mathbf{S})}.$$

Note that for $1 \leq i \leq r$, the map $\Psi_i : P_r(n-i) \rightarrow P_r(n)$ given by

$$\Psi_i(S_1, S_2, \dots, S_i, \dots, S_r) = (S_1, S_2, \dots, S_i \cup \{n-i\}, \dots, S_r),$$

is a well-defined injection, and furthermore the collection $\{\Psi_i(P_r(n-i)) : 1 \leq i \leq r\}$ is a partition of $P_r(n)$. Also, note that for all $1 \leq i \leq r$,

$$L(\Psi_i \mathbf{S}) = -[n] \cdot L(\mathbf{S}).$$

Thus from (33) we get

$$\beta_n = \sum_{i=1}^r \sum_{\mathbf{S} \in \Psi_i(P_r(n-i))} \frac{\mathbf{A}^{\mathbf{S}}}{L(\mathbf{S})},$$

and the result follows. \square

Remark 3.4. When ϕ is the Carlitz module \mathcal{C} , we recover (3) and (6) from (24) and (31), respectively.

Remark 3.5. If we assign to each A_n a “weight” of $q^n - 1$, and extend it to products in the usual way ($\text{wt}(AB) = \text{wt}(A) + \text{wt}(B)$), then by (20) the total weight of any $\mathbf{A}^{\mathbf{S}}$ appearing as a summand in the coefficient of z^{q^n} in either e_ϕ or \log_ϕ is always $q^n - 1$.

4. CONVERGENCE AND RANGE OF \log_ϕ IN RANK TWO

Let ϕ be a rank 2 Drinfeld module given by

$$(34) \quad \phi_T = T + A\tau + B\tau^2.$$

The j -invariant of ϕ is defined by

$$(35) \quad j(\phi) := \frac{A^{q+1}}{B}.$$

In this section we study the convergence properties of the series defining \log_ϕ . We start with determining the valuation of its coefficients.

Lemma 4.1. *Let ϕ be as in (34) and write*

$$\log_\phi(z) = \sum_{n=0}^{\infty} \beta_n z^{q^n}.$$

Then for $n \in \mathbb{N}$, $v(\beta_n)$ is given by the following formula.

$$(36) \quad v(\beta_n) = \begin{cases} \frac{q^n - 1}{q - 1}(v(A) + q), & \text{if } v(j) < -q, \\ \frac{q^n - 1}{q^2 - 1}(v(B) + q^2), & \text{if } v(j) > -q \text{ and } n \text{ is even,} \\ \frac{q^n - 1}{q^2 - 1}(v(B) + q^2) + \frac{v(j) + q}{q + 1}, & \text{if } v(j) > -q \text{ and } n \text{ is odd.} \end{cases}$$

In the case where $v(j) = -q$ we have

$$(37) \quad v(\beta_n) \geq \frac{q^n - 1}{q - 1}(v(A) + q) = \frac{q^n - 1}{q^2 - 1}(v(B) + q^2),$$

with equality holding infinitely often.

Proof. From (31) we have

$$\beta_n = \sum_{(S_1, S_2) \in P_2(n)} \frac{A^{w(S_1)} B^{w(S_2)}}{L(S_1, S_2)},$$

where

$$L(S_1, S_2) = \prod_{i \in S_1} (-[i + 1]) \prod_{i \in S_2} (-[i + 2]).$$

It is easy to see that

$$v\left(\frac{A^{w(S_1)} B^{w(S_2)}}{L(S_1, S_2)}\right) = w(S_1)v(A) + w(S_2)v(B) + qw(S_1) + q^2w(S_2).$$

In addition, by (20) we have $(q - 1)w(S_1) + (q^2 - 1)w(S_2) = q^n - 1$, hence

$$w(S_1) = \frac{q^n - 1}{q - 1} - (q + 1)w(S_2),$$

and consequently

$$(38) \quad v\left(\frac{A^{w(S_1)} B^{w(S_2)}}{L(S_1, S_2)}\right) = \frac{q^n - 1}{q - 1}(v(A) + q) - w(S_2)(v(j) + q).$$

Thus our analysis naturally breaks into the following three cases.

Case 1: $v(j) > -q$. In this case, we see that $v\left(\frac{A^{w(S_1)} B^{w(S_2)}}{L(S_1, S_2)}\right)$ is a strictly decreasing function of $w(S_2)$, and hence attains its minimal value when $w(S_2)$ is maximal. It is easy to see that

$$(39) \quad \max_{(S_1, S_2) \in P_r(n)} (w(S_2)) = \begin{cases} \frac{q^n - 1}{q^2 - 1}, & \text{if } n \text{ is even,} \\ \frac{q^n - q}{q^2 - 1}, & \text{if } n \text{ is odd.} \end{cases}$$

(Corresponding to $S_1 = \emptyset$ for n even and $S_1 = \{0\}$ for odd n). The ultrametric property implies

$$(40) \quad v(\beta_n) = \begin{cases} \frac{q^n - 1}{q - 1}(v(A) + q) - \frac{q^n - 1}{q^2 - 1}(v(j) + q), & \text{if } n \text{ is even,} \\ \frac{q^n - 1}{q - 1}(v(A) + q) - \frac{q^n - q}{q^2 - 1}(v(j) + q), & \text{if } n \text{ is odd,} \end{cases}$$

and the corresponding part of (36) follows.

Case 2: $v(j) < -q$. From (38) we see that $v\left(\frac{A^{w(S_1)}B^{w(S_2)}}{L(S_1, S_2)}\right)$ is strictly increasing in $w(S_2)$. Thus the minimal valuation is attained when $S_2 = \emptyset$, which implies the first line of (36).

Case 3: $v(j) = -q$. In this case we see that $v\left(\frac{A^{w(S_1)}B^{w(S_2)}}{L(S_1, S_2)}\right)$ is always equal to

$$\frac{q^n - 1}{q - 1}(v(A) + q) = \frac{q^n - 1}{q^2 - 1}(v(B) + q^2),$$

and hence $v(\beta_n) \geq \frac{q^n - 1}{q - 1}(v(A) + q)$. It is easy to see by direct calculation that we have equality for $n = 0, 1$. The recurrence formula

$$-[n]\beta_n = A^{q^{n-1}}\beta_{n-1} + B^{q^{n-2}}\beta_{n-2}$$

implies that

$$v(\beta_n) - q^n \geq \inf\left(q^{n-1}v(A) + v(\beta_{n-1}), q^{n-2}v(B) + v(\beta_{n-2})\right).$$

Since $v(j) = -q$, an easy computation shows that

$$\begin{aligned} q^{n-1}v(A) + \frac{q^{n-1} - 1}{q - 1}(v(A) + q) \\ = q^{n-2}v(B) + \frac{q^{n-2} - 1}{q - 1}(v(A) + q) = \frac{q^n - 1}{q - 1}(v(A) + q) - q^n. \end{aligned}$$

Thus if $v(\beta_n) > \frac{q^n - 1}{q - 1}(v(A) + q)$, while $v(\beta_{n-1}) = \frac{q^{n-1} - 1}{q - 1}(v(A) + q)$, then we must have $v(\beta_{n+1}) = \frac{q^{n+1} - 1}{q - 1}(v(A) + q)$ and also $v(\beta_{n+2}) = \frac{q^{n+2} - 1}{q - 1}(v(A) + q)$. Thus equality in (37) actually occurs at least two thirds of the time, and the result follows. \square

Corollary 4.2. *Set*

$$(41) \quad \begin{aligned} \rho_B &:= -\frac{q^2 + v(B)}{q^2 - 1}, \\ \rho_A &:= -\frac{q + v(A)}{q - 1}. \end{aligned}$$

If $v(j) \geq -q$ then the series $\sum \beta_i z^{q^i}$ converges exactly for $z \in \mathbb{C}_\infty$ with $v(z) > \rho_B$, and if $v(j) \leq -q$ then it converges exactly for $v(z) > \rho_A$.

Proof. We know that the series converges if and only if $\lim_{n \rightarrow +\infty} v(\beta_n z^{q^n}) = +\infty$. From Lemma 4.1 we have

$$(42) \quad v(\beta_n z^{q^n}) = \begin{cases} (q^n - 1) \left(\frac{v(A)+q}{q-1} + v(z) \right) + v(z), & \text{if } v(j) < -q, \\ (q^n - 1) \left(\frac{v(B)+q^2}{q^2-1} + v(z) \right) + v(z), & \text{if } v(j) > -q \\ & \text{and } n \text{ is even,} \\ (q^n - 1) \left(\frac{v(B)+q^2}{q^2-1} + v(z) \right) + v(z) + \frac{v(j)+q}{q+1}, & \text{if } v(j) > -q \\ & \text{and } n \text{ is odd.} \end{cases}$$

When $v(j) = -q$ then we have

$$(43) \quad v(\beta_n z^{q^n}) \geq (q^n - 1) \left(\frac{v(B) + q^2}{q^2 - 1} + v(z) \right) + v(z),$$

with equality holding for infinitely many values of n . The result follows at once. \square

Corollary 4.3. *If the series for \log_ϕ converges for $z \in \mathbb{C}_\infty$ then we must have*

$$(44) \quad v(\log_\phi(z)) = v(z).$$

Proof. From (42) and (43), it is easy to see that in the case of convergence we must have

$$v(z) < v(\beta_n z^{q^n}) \text{ for all } n \geq 1,$$

and the result follows by the ultrametric property of v . □

Remark 4.4. Note that $\rho_B - \rho_A = \frac{v(j)+q}{q^2-1}$. If we set

$$\rho_\phi := \max(\rho_A, \rho_B),$$

then we can rephrase Corollary 4.2 by saying that the series of \log_ϕ converges at $z \in \mathbb{C}_\infty$ if and only if $v(z) > \rho_\phi$.

5. COMPUTING THE PERIODS OF RANK TWO DRINFELD MODULES

Let ϕ be a Drinfeld module given by

$$\phi_T = T + A\tau + B\tau^2,$$

and let Λ_ϕ be the corresponding lattice. We can describe Λ_ϕ as the unique lattice for which

$$(45) \quad e_{\Lambda_\phi} = e_\phi.$$

In other words, Λ_ϕ is the set of zeros of e_ϕ . Our goal in this section is to outline a procedure for obtaining *periods* of ϕ , (i.e. elements of the lattice Λ_ϕ) in terms of the coefficients A and B . We start with an easy lemma on the values of e_ϕ at the T -division points of ϕ .

Lemma 5.1. *For every $\lambda \in \Lambda_\phi$, $\delta_\lambda := e_\phi\left(\frac{\lambda}{T}\right)$ is a root of the polynomial*

$$Bx^{q^2} + Ax^q + Tx = 0.$$

Proof. The function e_ϕ satisfies the functional equation $e_\phi(Tz) = \phi_T(e_\phi(z))$. Hence

$$0 = e_\phi\left(T \cdot \frac{\lambda}{T}\right) = T\delta_\lambda + A\delta_\lambda^q + B\delta_\lambda^{q^2},$$

and the result follows. □

For the remainder of the paper, we let

$$(46) \quad f_\phi(x) = Bx^{q^2} + Ax^q + Tx.$$

Also set

$$\begin{aligned} V_\phi &:= \{\delta \in \mathbb{C}_\infty : f_\phi(\delta) = 0\}, \\ V_\phi^* &:= \{\delta \in \mathbb{C}_\infty : B\delta^{q^2-1} + A\delta^{q-1} + T = 0\}. \end{aligned}$$

As V_ϕ is the T -torsion submodule on ϕ it follows that V_ϕ is a 2-dimensional vector space over \mathbb{F}_q , and V_ϕ^* is its set of nonzero elements. The following lemma gives a complete description of the possible valuations on V_ϕ^* .

Lemma 5.2. *Let ϕ be a rank 2 Drinfeld module given by (34), and let j be its j -invariant as in (35). Exactly one of the following cases hold.*

(i) All the elements of V_ϕ^* have the same valuation given by

$$(47) \quad v(\delta) = \frac{-(1+v(B))}{q^2-1} \text{ for all } \delta \in V_\phi^*.$$

This case happens if and only if $v(j) \geq -q$.

(ii) There is an element $\eta \in V_\phi^*$ such that all elements of $\mathbb{F}_q^* \eta$ have strictly larger valuation than the rest of V_ϕ^* if and only if $v(j) < -q$. In this case we have

$$(48) \quad v(\eta) = \frac{-(1+v(A))}{q-1} \text{ and } v(\delta) = \frac{v(A)-v(B)}{q^2-q} \text{ for all } \delta \in V_\phi \setminus \mathbb{F}_q \eta.$$

Proof. The lemma follows from an analysis of the Newton polygon of the defining polynomial $f_\phi(x)/x = Bx^{q^2-1} + Ax^{q-1} + T = 0$ of V_ϕ^* [8, Ch. 2], [10, §I.2]. Indeed the line segment connecting $(0, -1)$ and $(q^2-1, v(B))$ has slope $\frac{v(B)+1}{q^2-1}$, and one checks that $(q-1, v(A))$ lies on or above this line segment if and only if $v(j) = (q+1)v(A) - v(B) \geq -q$. Thus $v(j) \geq -q$ if and only if all zeroes of $f_\phi(x)/x$ have valuation $-\frac{v(B)+1}{q^2-1}$. Otherwise, when $v(j) < -q$, the Newton polygon breaks into two segments: one of width $q-1$ from $(0, -1)$ to $(q-1, v(A))$ of slope $\frac{v(A)+1}{q-1}$, and another of width q^2-q from $(q-1, v(A))$ to $(q^2-1, v(B))$ of slope $\frac{v(B)-v(A)}{q^2-q}$. The result then follows. \square

Guided by the results above, we consider certain families of rank two Drinfeld modules as follows. Fix $0 \neq \delta \in \mathbb{C}_\infty$, and set

$$(49) \quad \mathcal{F}_\delta := \{\text{All rank 2 Drinfeld modules } \phi \text{ such that } \mathbb{F}_q \delta \subset V_\phi\}.$$

The following theorem gives a complete description of the cases where the lattice Λ_ϕ could be recovered by applying \log_ϕ to V_ϕ .

Theorem 5.3. *Let $\phi \in \mathcal{F}_\delta$ be given by $\phi_T = T + A\tau + B\tau^2$. Fix a choice of a $(q-1)$ -st root of $\frac{T}{B}$ and set*

$$(50) \quad c := \delta^{-1} \left(\frac{T}{B} \right)^{\frac{1}{q-1}}.$$

Let ζ be a root of

$$(51) \quad x^q - \delta^{q-1}x = c.$$

We have the following cases.

(i) If $v(j) \geq -q$, then $v(\delta) = v(\zeta) = \frac{-(1+v(B))}{q^2-1}$. Hence \log_ϕ converges at δ and ζ , and the period lattice Λ_ϕ is generated by $\{T \log_\phi(\delta), T \log_\phi(\zeta)\}$.

(ii) If $v(j) < -q$ and $v(\delta) = \frac{-(1+v(A))}{q-1}$, then \log_ϕ converges at δ , and $T \log_\phi(\delta)$ is a period in Λ_ϕ . Furthermore $v(\zeta) = \frac{v(A)-v(B)}{q^2-q}$, and \log_ϕ converges on all of V_ϕ if and only if

$$(52) \quad v(j) > -q^2.$$

If (52) is satisfied then the period lattice Λ_ϕ is generated by $\{T \log_\phi(\delta), T \log_\phi(\zeta)\}$.

(iii) If $v(j) < -q$ and $v(\delta) = \frac{v(A)-v(B)}{q^2-q}$, then $v(\zeta) = \frac{-(1+v(A))}{q-1}$ and \log_ϕ converges at ζ , hence $T \log_\phi(\zeta)$ is a period in Λ_ϕ . Again \log_ϕ converges on all of V_ϕ if and only if (52) is satisfied, in which case the period lattice Λ_ϕ is generated by $\{T \log_\phi(\delta), T \log_\phi(\zeta)\}$.

Proof. The condition $\phi \in \mathcal{F}_\delta$ is equivalent to

$$(53) \quad B\delta^{q^2} + A\delta^q + T\delta = 0.$$

Substituting (53) in $f_\phi(x)$ we get

$$\begin{aligned} f_\phi(x) &= Bx^{q^2} - (T\delta^{1-q} + B\delta^{q^2-q})x^q + Tx \\ &= B(x^q - \delta^{q-1}x)^q - T\delta^{1-q}(x^q - \delta^{q-1}x). \end{aligned}$$

It follows that any $\zeta \in V_\phi \setminus \mathbb{F}_q\delta$ must satisfy

$$(54) \quad \zeta^q - \delta^{q-1}\zeta = \delta^{-1} \left(\frac{T}{B} \right)^{\frac{1}{q-1}}.$$

Obviously $\frac{-(1+v(B))}{q^2-1} > \rho_B$, and it follows that when $v(j) \geq -q$, \log_ϕ converges on all of V_ϕ .

When $v(j) < -q$, we also have $\frac{-(1+v(A))}{q-1} > \rho_A$; however we have

$$\frac{v(A) - v(B)}{q^2 - q} > \rho_A = -\frac{q + v(A)}{q - 1} \text{ if and only if } v(j) > -q^2.$$

Finally assume that δ and ζ are linearly independent over \mathbb{F}_q , and that \log_ϕ converges at both of them. We need to show that $\log_\phi(\delta)$ and $\log_\phi(\zeta)$ are linearly independent over \mathbb{A} . From Lemma 5.1 we see that $e_\phi(T^n \log_\phi \eta) = 0$ for all $n \geq 1$ and all $\eta \in V_\phi$. Thus if $a, b \in \mathbb{A}$ are polynomials with constant terms a_0 and b_0 respectively, then

$$e_\phi(a \log_\phi(\delta) + b \log_\phi(\zeta)) = a_0\delta + b_0\zeta,$$

and it follows that indeed $\{\log_\phi(\delta), \log_\phi(\zeta)\}$ are linearly independent over \mathbb{A} . \square

Remark 5.4. We note that (51) could be written as

$$(55) \quad X^q - X = \frac{c}{\delta^q},$$

where $X := \frac{x}{\delta}$. Thus computing ζ is reduced to the extraction of an Artin-Schreier root.

6. AN ANALYTIC EXPRESSION FOR PERIODS

In the previous section we obtained a procedure for computing periods which involved the extraction of certain roots. In this section we show that under additional conditions (cf. (60)) we can obtain a completely analytic expression for the periods. We start with a lemma on expressing the roots of a certain algebraic equation in terms of series.

Lemma 6.1. *Let $C, \delta \in \mathbb{C}_\infty \setminus \{0\}$. If*

$$(56) \quad v(C) > qv(\delta)$$

then the set of solutions of the equation

$$(57) \quad x^q - \delta^{q-1}x = C$$

is given by

$$(58) \quad \mathbb{F}_q\delta - \delta \sum_{i=0}^{\infty} \left(\frac{C}{\delta^q} \right)^{q^i}.$$

Proof. Condition (56) guarantees the convergence of the infinite series. It can easily be seen that it satisfies (57). Finally, notice that a polynomial of degree q can have at most q distinct solutions. \square

Corollary 6.2. *Let $\phi_T = T + A\tau + B\tau^2$ be a Drinfeld module with $v(j) < -q$, and assume that $\delta \in V_\phi$ with $v(\delta) = \frac{v(A)-v(B)}{q^2-q}$. Fix a choice of a $(q-1)$ -root of $\frac{T}{B}$. Then the unique subspace of V_ϕ where the valuation of the nonzero elements is $\frac{-(1+v(A))}{q-1}$ is generated by*

$$(59) \quad \eta = -\delta \sum_{n=0}^{\infty} \left(\frac{T}{\delta^{q^2-1}B} \right)^{\frac{q^n}{q-1}}.$$

Proof. With c as in (50), we see that

$$v\left(\frac{c}{\delta^q}\right) = -(q+1)\frac{v(A)-v(B)}{q^2-q} - \frac{1+v(B)}{q-1} = \frac{-(v(j)+q)}{q^2-q} > 0,$$

and thus the series converges, and the valuation of the sum is equal to that of the first term by the ultrametric property. So indeed

$$v(\eta) = v(\delta^{1-q}c) = \frac{-q(v(A)-v(B))}{q^2-q} - \frac{(1+v(B))}{q-1} = \frac{-(1+v(A))}{q-1},$$

and the result follows from Lemma 6.1 and Lemma 5.2. \square

For $0 \neq \delta \in \mathbb{C}_\infty$ we consider the subfamily \mathcal{F}_δ^* of \mathcal{F}_δ defined by

$$(60) \quad \mathcal{F}_\delta^* := \left\{ \phi \in \mathcal{F}_\delta : v(j) < -q \text{ and } v(\delta) = \frac{v(A)-v(B)}{q^2-q} \right\}.$$

We have the following analytic expression for periods in \mathcal{F}_δ^* .

Theorem 6.3. *Let $\phi \in \mathcal{F}_\delta^*$ be given, and set c as in (50). Let β_j be the coefficients of \log_ϕ . Set*

$$(61) \quad \begin{aligned} \mathbf{a}_\delta(n) &:= T \sum_{j=0}^n \beta_j \delta^{q^j}, \text{ and} \\ \mathbf{f}(z) &:= \sum_{n=0}^{\infty} \mathbf{a}_\delta(n) z^{q^n}. \end{aligned}$$

Then the series \mathbf{f} converges for $z = \delta^{-q}c$, and $\mathbf{f}(\delta^{-q}c)$ is a period of Λ_ϕ with maximal valuation.

Proof. Let η be as in (59). From Theorem 5.3 and Corollary 6.2, we see that a period $\lambda \in \Lambda_\phi$ is given by

$$\begin{aligned} \lambda := T \log_\phi(\eta) &= T \log_\phi \left(\sum_{i=0}^{\infty} \delta^{1-q^{i+1}} c^{q^i} \right) = T \sum_{j=0}^{\infty} \beta_j \sum_{i=0}^{\infty} \delta^{q^j - q^{i+j+1}} c^{q^{i+j}} \\ &= \sum_{n=0}^{\infty} T \left(\sum_{j=0}^n \beta_j \delta^{q^j} \right) \left(\frac{c}{\delta^q} \right)^{q^n} = \mathbf{f}(\delta^{-q}c). \end{aligned}$$

By Corollary 4.3 we see that

$$v(\lambda) = -1 - \frac{1+v(A)}{q-1} = \frac{-(q+v(A))}{q-1}.$$

If $\lambda' \in \Lambda_\phi$ has larger valuation, then $e_\phi(T^{-1}\lambda')$ is an element of V_ϕ with valuation larger than $\frac{-(1+v(A))}{q-1}$, which contradicts Lemma 5.2, and the theorem follows. \square

We end this section with a more detailed analysis of the function \mathfrak{f} .

Proposition 6.4. *Let $\phi \in \mathcal{F}_\delta^*$ be given, and let \mathfrak{a}_δ and \mathfrak{f} be as in (61). If $-q > v(j) > -q^2$ then \mathfrak{f} converges if and only if $v(z) > 0$, and if $v(j) < -q^2$ then \mathfrak{f} converges if and only if*

$$(62) \quad v(z) > \frac{-(v(j) + q^2)}{q^2 - q} > 0.$$

If $v(j) = -q^2$, then \mathfrak{f} converges at least for $v(z) > 0$. Furthermore for $n \geq 0$ we have

$$(63) \quad \mathfrak{a}_\delta(n) = (T\delta)^{q^n} \beta_n - (B\delta^{q^2})^{q^{n-1}} \beta_{n-1},$$

and in the range $v(z) > \frac{-(q+v(j))}{q^2-q}$, \mathfrak{f} has the representation

$$(64) \quad \mathfrak{f}(z) = \log_\phi(T\delta z) - \log_\phi(B\delta^{q^2} z^q).$$

Proof. From (42), we see that

$$\begin{aligned} v(\beta_n \delta^{q^n}) &= (q^n - 1) \left(\frac{q + v(A)}{q - 1} + \frac{v(A) - v(B)}{q^2 - q} \right) + v(\delta) \\ &= (q^n - 1) \left(\frac{v(j) + q^2}{q^2 - q} \right) + v(\delta). \end{aligned}$$

Thus our analysis naturally breaks into three cases.

Case 1: $v(j) > -q^2$. In this case $v(T\beta_n \delta^{q^n})$ is strictly increasing in n , and thus

$$v(\mathfrak{a}_\delta(n)) = v(\delta) - 1 \text{ for all } n \geq 0.$$

It follows that the series for \mathfrak{f} converges if and only if $v(z) > 0$.

Case 2: $v(j) < -q^2$. In this case $v(T\beta_n \delta^{q^n})$ is strictly decreasing in n , and thus

$$v(\mathfrak{a}_\delta(n)) = v(T\beta_n \delta^{q^n}).$$

Hence

$$v(\mathfrak{a}_\delta(n) z^{q^n}) = v(z) + v(\delta) - 1 + (q^n - 1) \left(v(z) + \frac{v(j) + q^2}{q^2 - q} \right),$$

and \mathfrak{f} converges if and only if $v(z) > \frac{-(v(j)+q^2)}{q^2-q}$.

Case 3: $v(j) = -q^2$. In this case $v(T\beta_n \delta^{q^n}) = v(\delta) - 1$ for all n , and thus

$$v(\mathfrak{a}_\delta(n)) \geq v(\delta) - 1 \text{ for all } n \geq 0.$$

It follows that the series for \mathfrak{f} converges at least for all $v(z) > 0$.

The first part of the proposition follows from the analysis above. To prove the second part, note that (32) and (53) give

$$\begin{aligned} T\beta_i \delta^{q^i} &= (T\delta)^{q^i} \beta_i + (A\delta^q)^{q^{i-1}} \beta_{i-1} + (B\delta^{q^2})^{q^{i-2}} \beta_{i-2} \\ &= (T\delta)^{q^i} \beta_i - (T\delta)^{q^{i-1}} \beta_{i-1} - (B\delta^{q^2})^{q^{i-1}} \beta_{i-1} + (B\delta^{q^2})^{q^{j-2}} \beta_{i-2}. \end{aligned}$$

Hence

$$\mathfrak{a}_\delta(n) = (T\delta)^{q^n} \beta_n - (B\delta^{q^2})^{q^{n-1}} \beta_{n-1}.$$

Consequently we (formally) get

$$\mathfrak{f}(z) = \log_\phi(T\delta z) - \log_\phi(B\delta^{q^2} z^q).$$

The expression on the right hand side converges for $v(T\delta z) > \rho_A$ and $v(B\delta^{q^2} z^q) > \rho_A$. Either statement is equivalent to

$$v(z) > \frac{-(v(j) + q)}{q^2 - q},$$

and the result follows. \square

Remark 6.5. Note that since $v(\delta^{-q}c) = \frac{-(v(j)+q)}{q^2-q}$, we can not use (64) to evaluate $\lambda = \mathfrak{f}(\delta^{-q}c)$. Instead we can only use (61) for that evaluation, and indeed the argument above gives another proof that \mathfrak{f} does converge at that point.

7. AN EXAMPLE FROM COMPLEX MULTIPLICATION

In [13], Thakur determined the power series expansions of the exponential and logarithm functions of sgn-normalized rank 1 Drinfeld modules, and he showed how his constructions fit into the more general framework of shtuka functions in [14], which is particular to the rank 1 theory. Thakur's Drinfeld modules, originally studied by Hayes [9] in the context of explicit class field theory, are rank 1 over extensions of \mathbb{A} but can be thought of as higher rank Drinfeld \mathbb{A} -modules with complex multiplication. Here we consider one of Thakur's examples [13, Ex. A] and compare it to the constructions of the previous sections.

Let $q = 3$, and let $y \in \mathbb{C}_\infty$ satisfy $y^2 = T^3 - T - 1$. Then define a rank 2 Drinfeld module ϕ by setting

$$(65) \quad \phi_T := T + y(T^3 - T)\tau + \tau^2.$$

The module ϕ is special in that it has complex multiplication by the ring $\mathbb{F}_3[T, y]$, which itself has class number one, and so ϕ is a rank 1 Drinfeld $\mathbb{F}_3[T, y]$ -module but a rank 2 Drinfeld \mathbb{A} -module. For $n \geq 1$, Thakur lets $[n]_y := y^{3^n} - y$ and sets

$$f_n = \frac{[n]_y - y[n]}{[n] - 1}, \quad g_n = \frac{[n]_y - y^{3^n}[n]}{[n + 1] + 1}.$$

He then establishes that if $e_\phi(z) = \sum \alpha_n z^{3^n}$ and $\log_\phi(z) = \sum \beta_n z^{3^n}$, then for $n \geq 1$,

$$\alpha_n = \frac{\alpha_{n-1}^3}{f_n}, \quad \beta_n = \frac{\beta_{n-1}}{g_n}.$$

Therefore,

$$\alpha_n = \frac{1}{f_n f_{n-1}^3 \cdots f_1^{3^{n-1}}}, \quad \beta_n = \frac{1}{g_n g_{n-1} \cdots g_1}.$$

After some calculations (and using that $v(y) = -\frac{3}{2}$), it follows that for $n \geq 1$,

$$(66) \quad v(\alpha_n) = \frac{1}{2}(n - 2)3^n,$$

$$(67) \quad v(\beta_n) = -\frac{3}{4}(3^n - 1).$$

See also Lutes [11, §IV.C]. (In both Lutes and Thakur the formulas differ from the ones above by a factor of $\frac{1}{2}$, as they set $v(T) = -2$ instead of -1 .)

Certainly the valuation of α_n in (66) is consistent with (28), since $v_0 = -\frac{9}{2}$ in this case. Now $j(\phi) = y^4(T^3 - T)^4$, and so $v(j(\phi)) = -18$. Therefore (67) matches with Lemma 4.1,

and $\log_\phi(z)$ converges for $v(z) > \frac{3}{4}$, which coincides with Corollary 4.2. Now the set V_ϕ is generated over \mathbb{F}_3 by $e_\phi(1/T)$ and $e_\phi(y/T)$, which have valuations $\frac{7}{4}$ and $-\frac{3}{4}$ respectively (see [12, Ex. 4.15]), and thus ϕ fits into the situation of Theorem 5.3 with $v(j) < -q^2$ (so \log_ϕ does not converge on all of V_ϕ). However, one can also calculate the period by other means (see [5, §III], [8, §7.10], [12, Ex. 4.15]), and one finds that a period π with maximal valuation has $v(\pi) = \frac{3}{4}$, agreeing with Theorem 6.3.

8. A MULTINOMIAL FORMULA AND SUPERSINGULAR MODULES

Let $\mathfrak{p} \in \mathbb{A}$ be monic and irreducible of degree d , and let $L_{\mathfrak{p}}$ be a field extension of \mathbb{A}/\mathfrak{p} . A Drinfeld module ϕ of rank r over $L_{\mathfrak{p}}$ is said to be *supersingular* if $\phi_{\mathfrak{p}}$ is purely inseparable. If ϕ has rank 2 then its supersingularity is equivalent to the vanishing of the coefficient of τ^d in $\phi_{\mathfrak{p}}$ modulo \mathfrak{p} . (See Gekeler [6], [7] for further discussion and characterizations of supersingularity).

It is thus natural to seek a characterization of ϕ_{T^m} for all $m \in \mathbb{N}$ in terms of the coefficients of ϕ_T . It turns out that the shadowed partitions of §2 above will be crucial here as well. However, we need to introduce just a little more notation before we can state our result. Let $n \in \mathbb{Z}$ and let S be a finite subset of \mathbb{N} . Set

$$(68) \quad I_n(S) := \{(k_i)_{i \in S} : k_i \in \mathbb{N} \text{ and } \sum_{i \in S} k_i = n\},$$

and define

$$(69) \quad h_n^S := \sum_{(k_i) \in I_n(S)} T^{\sum_{i \in S} k_i q^i} \in \mathbb{A}.$$

Note that if $n < 0$, then $I_n(S) = \emptyset$ and hence $h_n^S = 0$. Also $h_0^S = 1$. (These properties hold even if $S = \emptyset$ since $I_n(\emptyset) = \emptyset$ for all $n \neq 0$ and $I_0(\emptyset) = \{\emptyset\}$). We are now ready to state a Drinfeld multinomial Theorem.

Theorem 8.1 (Multinomial Formula). *Let ϕ be a rank r Drinfeld module over any \mathbb{A} -field L given by*

$$(70) \quad \phi_T = T + \sum_{i=1}^r A_i \tau^i.$$

For $m \in \mathbb{N}$ and $n \in \mathbb{Z}$ define the coefficients $c(n; m) := c(n; m; \phi)$ by

$$(71) \quad \phi_{T^m} = \sum_{n=0}^{rm} c(n; m) \tau^n,$$

and $c(n; m) = 0$ for $n < 0$ or $n > rm$. Then for all $m, n \geq 0$ we have

$$(72) \quad c(n; m) = \sum_{\mathbf{S} \in P_r(n)} \mathbf{A}^{\mathbf{S}} \cdot h_{m-|\mathbf{S}|}^{(\cup \mathbf{S}\{n\})}.$$

Proof. We proceed by induction on m . It is easy to verify that formula (72) gives $c(0; 0) = 1$ since $P_r(0) = \{\emptyset\}$. For $n > 0$ and $\mathbf{S} \in P_r(n)$ we must have $|\mathbf{S}| > 0$, hence $m - |\mathbf{S}| < m$, and thus formula (72) gives $c(n; 0) = 0$ for all $n > 0$. So the statement is valid for $m = 0$

since $\phi_1 = 1$. Next we note that, because of the identity $\phi_{T^{m+1}} = \phi_T(\phi_{T^m})$, the coefficients $c(n; m)$ satisfy the recursion formula

$$(73) \quad c(n; m+1) = Tc(n; m) + \sum_{i=1}^r A_i \cdot c(n-i; m)^{q^i}.$$

Thus, by the induction hypothesis we have

$$(74) \quad c(n; m+1) = T \sum_{\mathbf{S} \in P_r(n)} \mathbf{A}^{\mathbf{S}} \cdot h_{m-|\mathbf{S}|}^{(\cup \mathbf{S} \cup \{n\})} + \sum_{i=1}^r A_i \sum_{\mathbf{S}^{(i)} \in P_r(n-i)} \left(\mathbf{A}^{\mathbf{S}^{(i)}} \right)^{q^i} \left(h_{m-|\mathbf{S}^{(i)}|}^{(\cup \mathbf{S}^{(i)} \cup \{n-i\})} \right)^{q^i}$$

Note that $A_j^{q^i \cdot w(S_j^{(i)})} = A_j^{w(S_j^{(i)}+i)}$, $A_i \cdot A_i^{q^i \cdot w(S_i^{(i)})} = A_i^{w(\{0\} \cup (S_i^{(i)}+i))}$, and that

$$\left(h_{m-|\mathbf{S}^{(i)}|}^{(\cup \mathbf{S}^{(i)} \cup \{n-i\})} \right)^{q^i} = h_{m-|\mathbf{S}^{(i)}|}^{(\cup (\mathbf{S}^{(i)}+i) \cup \{n\})}.$$

Using the identification (17) of $P_r(n-i)$ and $P_r^i(n)$ we see that (74) becomes

$$(75) \quad \begin{aligned} c(n; m+1) &= \sum_{i=1}^r \sum_{\mathbf{S} \in P_r^i(n)} \mathbf{A}^{\mathbf{S}} \cdot \left[T h_{m-|\mathbf{S}|}^{(\cup \mathbf{S} \cup \{n\})} + h_{m-[(|\mathbf{S}|-1)+\sum_{j \neq i} |S_j|]}^{(\cup_{j=1}^r (S_j \setminus \{0\}) \cup \{n\})} \right] \\ &= \sum_{i=1}^r \sum_{\mathbf{S} \in P_r^i(n)} \mathbf{A}^{\mathbf{S}} \cdot h_{m+1-|\mathbf{S}|}^{(\cup \mathbf{S} \cup \{n\})}, \end{aligned}$$

which proves the result, since the summands are uniform in i and the sets $P_r^i(n)$ partition $P_r(n)$. \square

Corollary 8.2. *Let $\mathfrak{p} \in \mathbb{A}$ be a monic prime of the form*

$$(76) \quad \mathfrak{p} = \sum_{i=0}^d \mu_i T^i,$$

and let $L_{\mathfrak{p}}$ be a field extension of \mathbb{A}/\mathfrak{p} . Let ϕ be a rank 2 Drinfeld module over $L_{\mathfrak{p}}$ given by

$$\phi_T = T + A\tau + B\tau^2,$$

and let $c(n; m)$ be as in (72), then ϕ is supersingular at \mathfrak{p} if and only if

$$(77) \quad \sum_{i=\lceil \frac{d}{2} \rceil}^d \mu_i c(d; i) \equiv 0 \pmod{\mathfrak{p}}.$$

Proof. We have

$$\phi_{\mu_0 + \dots + \mu_d T^d} = \sum_{i=0}^d \mu_i \sum_{n=0}^{2i} c(n; i) \tau^n = \sum_{n=0}^{2d} \left(\sum_{i=\lceil \frac{n}{2} \rceil}^d \mu_i c(n; i) \right) \tau^n,$$

and the result follows by recognizing the coefficient of τ^d . \square

Example 8.3. To illustrate the results above, we identify the condition for a rank 2 Drinfeld module to be supersingular at a degree 4 monic prime \mathfrak{p} . By (77) this is equivalent to the vanishing modulo \mathfrak{p} of

$$(78) \quad \begin{aligned} & \mu_2 c(4; 2) + \mu_3 c(4; 3) + c(4; 4) \\ &= \mu_2 B^{1+q^2} + \mu_3 [B^{1+q^2} (T + T^{q^2} + T^{q^4}) + A^{1+q} B^{q^2} + A^{1+q^3} B^q + A^{q^2+q^3} B] \\ & \quad + B^{1+q^2} (T^2 + T^{2q^2} + T^{2q^4} + T^{1+q^2} + T^{1+q^4} + T^{q^2+q^4}) \\ & \quad + A^{1+q} B^{q^2} (T + T^q + T^{q^2} + T^{q^4}) + A^{1+q^3} B^q (T + T^q + T^{q^3} + T^{q^4}) \\ & \quad + A^{q^2+q^3} B (T + T^{q^2} + T^{q^3} + T^{q^4}) + A^{1+q+q^2+q^3}. \end{aligned}$$

Note that $\{T^{q^i} \pmod{\mathfrak{p}}, 0 \leq i \leq 3\}$ are the 4 distinct roots of \mathfrak{p} in $L_{\mathfrak{p}}$. Thus we have the following congruences

$$(79) \quad \begin{aligned} \mu_2 &\equiv T^{1+q} + T^{1+q^2} + T^{1+q^3} + T^{q+q^2} + T^{q+q^3} + T^{q^2+q^3} \pmod{\mathfrak{p}}, \\ \mu_3 &\equiv -(T + T^q + T^{q^2} + T^{q^4}) \pmod{\mathfrak{p}}, \\ T^{q^4} &\equiv T \pmod{\mathfrak{p}}. \end{aligned}$$

Substituting (79) into (78), a simple computation yields

$$\begin{aligned} & \mu_2 c(4; 2) + \mu_3 c(4; 3) + c(4; 4) \\ &= A^{1+q+q^2+q^3} - [1]A^{q^2+q^3}B - [2]A^{1+q^3}B^q - [3]A^{1+q}B^{q^2} + [2][3]B^{1+q^2}. \end{aligned}$$

Finally, dividing the above expression by B^{1+q^2} we see that ϕ is supersingular at \mathfrak{p} if and only if $j(\phi)$ is a root of

$$(80) \quad j^{q^2+1} - [1]j^{q^2} - [2]j^{q^2-q+1} - [3]j + [1][3] \equiv 0 \pmod{\mathfrak{p}}.$$

Using methods from Drinfeld modular forms, Cornelissen [3], [4] has also developed recursive formulas for polynomials defining supersingular j -invariants, and one can successfully compare (80) with $P_4(j)$ in [4, (2.2)].

REFERENCES

- [1] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1** (1935), 137–168.
- [2] L. Carlitz, *Chapter 19 of “The arithmetic of polynomials”*, Finite Fields Appl. **1** (1995), 157–164.
- [3] G. Cornelissen, *Deligne’s congruence and supersingular reduction of Drinfeld modules*, Arch. Math. (Basel) **72** (1999), 346–353.
- [4] G. Cornelissen, *Zeros of Eisenstein series, quadratic class numbers and supersingularity for rational function fields*, Math. Ann. **314** (1999), 175–196.
- [5] E.-U. Gekeler, *Drinfeld modular curves*, Lecture Notes in Mathematics, vol. 1231, Springer-Verlag, Berlin, 1986.
- [6] E.-U. Gekeler, *On the coefficients of Drinfeld modular forms*, Invent. Math. **93** (1988), 667–700.
- [7] E.-U. Gekeler, *On finite Drinfeld modules*, J. Algebra **141** (1991), 187–203.
- [8] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer, Berlin, 1996.
- [9] D. R. Hayes, *Explicit class field theory in global function fields*, in: Studies in algebra and number theory, Adv. in Math. Suppl. Stud. **6**, Academic Press, New York, 1979, pp. 173–217.
- [10] K. S. Kedlaya, *p -adic Differential Equations*, Cambridge Univ. Press, Cambridge, 2010.
- [11] B. A. Lutes, *Special values of the Goss L -function and special polynomials*, Ph.D. thesis, Texas A&M University, 2010. (Available at <http://www.math.tamu.edu/~map/>.)

- [12] B. A. Lutes and M. A. Papanikolas, *Algebraic independence of values of Goss L -functions at $s = 1$* , arXiv:1105.6341, 2011.
- [13] D. S. Thakur, *Drinfeld modules and arithmetic in the function fields*, Internat. Math. Res. Notices **1992** (1992), no. 9, 185–197.
- [14] D. S. Thakur, *Shtukas and Jacobi sums*, Invent. Math. **111** (1993), 557–570.
- [15] D. S. Thakur, *Function Field Arithmetic*, World Scientific Publishing, River Edge, NJ, 2004.
- [16] L. I. Wade, *Remarks on the Carlitz ψ -functions*, Duke Math. J. **13** (1946), 71–78.

CURRENT ADDRESS: SCIENCE PROGRAM, TEXAS A&M UNIVERSITY IN QATAR, DOHA, QATAR

PERMANENT ADDRESS: DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, CAIRO UNIVERSITY, GIZA, EGYPT 12613

E-mail address: `a.elguindy@gmail.com`

DEPARTMENT OF MATHEMATICS, TEXAS A&M UNIVERSITY, COLLEGE STATION, TX 77843, U.S.A.

E-mail address: `map@math.tamu.edu`