Factorization of Coefficients for Characteristic p Exponentials and Logarithms in Function Fields

by

Kwun Chung

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2021

Doctoral Committee:

Professor Kartik Prasanna, Chair
Professor Kenneth Cadigan
Professor Jeffrey Lagarias
Professor Andrew Snowden
Professor Michael Zieve

Kwun Chung
angusck@umich.edu
ORCID iD: 0000-0002-6772-1107

To my parents

ACKNOWLEDGEMENTS

I would first take this opportunity to express my huge gratitude towards my advisor, Kartik Prasanna. Kartik has given me enormous guidance and encouragement throughout my years in Michigan. He has inspired me so much on how to approach mathematics and research. Kartik has not only guided me intellectually, but also given me emotional support during some of my difficult times. In 2019, I felt stressed and hopeless towards the decline of freedom and police brutality in my hometown Hong Kong. When I told Kartik about this, he expressed sincere sympathy and suggested ways for me to feel better. Without him, I would suffer a lot more during the time. I cannot express enough how grateful I am to have him as my advisor. Thank you for everything.

I am indebted to Dinesh Thakur, Nathan Green, Federico Pellarin, Tuan Ngo Dac, and Chieh-Yu Chang for their very helpful discussion on my thesis work. The research community of function field arithmetic is a very knowledgeable, and at the same time, welcoming one. I am very grateful to be part of the community and have learned a lot from all people previously mentioned, as well as Mihran Papikian, Matthew Papanikolas, Ernst-Ulrich Gekeler, Jing Yu, Cristian Popescu, Yoshinori Mishiba, and many others.

I would like to thank Andrew Snowden, Jeffrey Lagarias, Michael Zieve, and Kenneth Cadigan for serving on the defense committee. I also want to thank Wei Ho, Kartik Prasanna, Tasho Kaletha, Stephen DeBacker, Bhargav Bhatt, Andrew Snowden, Jeffrey Lagarias, Michael Zieve, for organizing seminars and conferences for the number theory, representation theory and arithmetic geometry group in Michigan. They have put a lot of effort to create a friendly environment to everyone in the community, which is key to my accomplishment.

As a graduate student in Michigan, I have taught Calculus for a lot of semesters. I want to express my sincere gratitude to the teaching faculties in the department: Hanna Bennett, Paul Kessenich, Angela Kubena, Fernando Carreon, Irina Arakelian, and Beth Wolf. I have learned a lot on how to be a good instructor and have got valuable feedback from them. In particular, they have worked very hard to make remote teaching during the pandemic easier for both us instructors and the students. Apart from classroom teaching, I have also served in various outreach activities. I want to thank Sarah Koch and Stephen DeBacker for

organizing and managing all these outreach programs.

A huge thank to Teresa Stokes, the graduate program coordinator of the UM math department. Her great effort and care with enthusiasm has helped me to focus on math and live a better life in Ann Arbor. Also thank you to all past and current staff in the UM math department, including Stephanie Carroll, Molly Long, Anne Speigle, Doreen Fussman, and a lot others. Without them, the department would not be able to function at all.

There are many friends I get to know in Ann Arbor with whom I shared a lot of unforgettable memories. First I thank Eamon Quinlan and Andy Odesky for living with me and having a lot of fun time together. Thanks Eamon Quinlan, Robert Cochane, Nawaz Sultani, Andy Odesky, Suki, Zhan Jiang, Yifeng Huang, Feng Zhu, Joel Tan for all the board game days and nights. I also enjoy playing bridge, and am lucky to have played with Yifeng Huang, Mel Hochster as well as others. I am very happy to have shared an office with Yiwang Chen and Jacob Haley for my entire time in Michigan. Thanks Ruian Chen, Zhan Jiang, Gilyoung Cheong, Edgar Chung, Ningyuan Wang, Yuchen Liao, Sanal Shivaprasad, Nancy Wang, Harry Richman, Lara Du, Farrah Yhee, Mark Greenfield, Meg Daupan, Alex Cheung, Leo Tse, Jimmy Chen, Natalie Ngai, John Lee for being my regular hang-out buddies. I sincerely thank Wai Wong for his support and encouragement. Let me try to thank all other people I spent time with in Ann Arbor that I have not yet mentioned: Aleksander Horawa, Emmanual Reinecke, Takumi Murayama, Monica Lewis, Corey Everlove, Charlotte Chan, Karthik Ganapathy, Valia Gazaki, Karol Koziol, Shizhang Li, Jakub Witaszek, Kannappan Sampath, Brandon Carter, Kyu-Jun Hyung, Francesca Gandini, Patricia Klein, Joe Kraisler, Ari Shnidman, Patrick Kelley, Jazzi Kelley, Suchandan Pal, Matthew Chan, Tommy Wong, Justin Hong, Kristina Kan, Jeffrey Wong, Queenie Leung, Yan-Ling Choi, Charlotte Chan, Rex Fung, Moses Chan, Kenneth Ho, Elpis Wong.

I want to thanks to my friends since middle school: Benjamin Man-Hin Lui, Raymond Chun-Tung Lo, Francis Wong, Dick Wong, Debby Lui, Steven Yuen, Franklin Chan, Ronald Chiang, Kelvin Cheng, Joshua Lam, Anthony Yu, Sunny Yu, Ken Ho, Kenneth Lee, Felip Lai, Tony Lo, Leo Fang, Jeffrey Ng, Aaron Lui, Leo Lo. People say that friends met in teenage are one's life-long friends. My experience with these friends has shaped who I am. I really treasure the friendship with all of you. Thanks Albert Li, Dalton Fung and Pak-Hin Lee, whom I knew since high school and have also been in a math PhD program in US, for sharing each other's experiences and struggles.

Finally, this thesis is dedicated to my parents, for their love and support at all time.

TABLE OF CONTENTS

ABSTRACT

Let X be an elliptic curve or a ramifying hyperelliptic curve over $\mathbb{F}_q$. We will discuss how to factorize the coefficients of exponential and logarithm series for a Hayes module over such a curve. This allows us to obtain v-adic convergence results for such exponential and logarithm series, for v a "finite" prime. As an application, we can show that the v-adic Goss L-value $L_v(1, \Psi)$ is log-algebraic for suitable characters Ψ.

CHAPTER I
Introduction

In the number field case, it is known that the exponential series

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

converges for all $z \in \mathbb{C}_p$ with $|z|_p < p^{-\frac{1}{p-1}}$, and the logarithm series

$$\log(1+z) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{z^n}{n}$$

converges for all $z \in \mathbb{C}_p$ with $|z|_p < 1$. See [Kob84, §IV.2] for example.

In the function field case, characteristic p exponential and logarithm functions arising from Drinfeld modules were first studied by Carlitz [Car35] and Drinfeld [Dri74]. Let X be a smooth, projective, geometrically connected curve over $\mathbb{F}_q$. We pick a closed point ∞ on X, and let $\mathbb{A} := \Gamma(X - \infty, \mathcal{O}_X)$, $\mathbb{K} = \mathrm{Frac}(\mathbb{A})$. The idea of a Drinfeld module is to define another $\mathbb{A}$-action (other than scalar multiplication) on the function fields and their field extensions. To distinguish the action and the space being act on, we set A, K to be an isomorphic copy of $\mathbb{A}, \mathbb{K}$ respectively, and use non-bold characters to represent spaces being act on.

We are particularly interested in a special class of Drinfeld modules, called sgn-normalized Drinfeld modules, or Hayes modules. They were first investigated by Hayes [Hay74], [Hay79], who utilized them to work out the class field theory of function fields. The simplest case of a Hayes module is when $X = \mathbb{P}^1$, $\mathbb{A} = \mathbb{F}_q[t]$, $A = \mathbb{F}_q[\theta]$. What we get is the usual Carlitz module [Car35]. In this case,

$$e_\rho(z) = \sum_{n=0}^{\infty} \frac{1}{(\theta^{q^n} - \theta)(\theta^{q^{n-1}} - \theta)^q \cdots (\theta^q - \theta)^{q^{n-1}}} z^{q^n},$$

$$\log_\rho(z) = \sum_{n=0}^{\infty} \frac{1}{(\theta - \theta^q) \cdots (\theta - \theta^{q^n})} z^{q^n}.$$

Similar to the number field case, there is a v-adic convergence result for these series, where v is a place of $K = \mathbb{F}_q(\theta)$ corresponding to a prime ideal $\mathfrak{p}$ in A. This can be found, for instance, in [AT90] (where we take the special case of dimension 1 from the paper).

- $e_\rho(z)$ converges in $\mathbb{C}_v$ for all $z \in \mathbb{C}_v$ with $v(z) > \frac{1}{q^{\deg \mathfrak{p}}-1}$;
- $\log_\rho(z)$ converges in $\mathbb{C}_v$ for all $z \in \mathbb{C}_v$ with $v(z) > 0$.

We call the functions on $\mathbb{C}_v$ defined by these series $e_{v,\rho}(z)$ and $\log_{v,\rho}(z)$ respectively.

Anderson [And96] gave an application for the v-adic convergence, showing that the value of v-adic L-function $L_v(1,\chi)$ for a character $\chi : A \to A/\mathfrak{p} \to \mathbb{C}_\infty$ is "log-algebraic". Namely, it is of the form

$$\sum_{i=1}^{s} \alpha_i \log_{v,\rho} S_i$$

for $\alpha_i, S_i \in \overline{K}$. A similar application is given by Anderson and Thakur [AT90], which uses a higher-dimensional version of the v-adic convergence to compute certain v-adic zeta values.

I.1: Main results

In this thesis, we will generalize the v-adic convergence result to more general Hayes modules. Specifically, we study the case of an elliptic curve or a *ramifying hyperelliptic curve*, i.e. a curve with an affine model

$$\Gamma(X - \infty, \mathcal{O}_X) = \mathbb{F}_q[t,y]/(y^2 + F_2(t)y - F_1(t))$$

for some rational point ∞ on X, see Chapter III. Fix a Hayes module ρ for the pair (X,∞) and a place v other than ∞ on such a curve. The exponential and logarithm series $e_\rho(z)$ and $\log_\rho(z)$ for ρ have coefficients in a finite Galois extension of K, see §II.3.4. Fix an embedding $\overline{K} \to \mathbb{C}_v$. Our main result is that:

Theorem V.3. *The power series $e_\rho(z)$ converges in $\mathbb{C}_v$ for $z \in \mathbb{C}_v$ with*

$$v(z) > C_1 + C_2 \frac{1}{q^{C_3} - 1},$$

where C_1, C_2, C_3 are explicit constants, to be given in V.3. In particular, C_1 is related to the Drinfeld divisor V (to be defined in Chapter II), C_2 to some ramification indices, and C_3 to the degree of v and some inertial degrees.

Moreover,

Theorem V.2. *The power series* $\log_\rho(z)$ *converges in* $\mathbb{C}_v$ *for* $z \in \mathbb{C}_v$ *with* $v(z) > 0$.

Similar to the Carlitz case, we call the functions on $\mathbb{C}_v$ defined by these series $e_{v,\rho}(z)$ and $\log_{v,\rho}(z)$ respectively.

As an application, we will prove a similar log-algebraicity theorem for v-adic L-values over these curves.

Theorem VI.10. *Let* Ψ *be a multiplicative character of conductor* v *on the group of* $\mathbb{A}$*-fractional ideals prime to* v*. Then* $L_v(1,\chi)$ *is log-algebraic, i.e. there exists*

$$\alpha_1, \cdots, \alpha_s, S_1, \cdots, S_s \in \overline{K},$$

with $v(S_i) > 0$*, such that*

$$L_v(1,\chi) = \sum_i \alpha_i \log_{v,\rho} S_i.$$

To prove Theorems V.3 and V.2, we recall an expression of $e_\rho(z)$ and $\log_\rho(z)$ given by Thakur, Anderson [Tha93, 0.3.6, 0.3.8], Green and Papanikolas [GP18, Corollary 3.5]. These expressions are given in terms of a special function f, called the shtuka function, which was first studied by Thakur [Tha93] and realizes the correspondence that Drinfeld showed in [Dri77]. The expressions are:

$$e_\rho(z) = \sum_{n=0}^{\infty} \frac{1}{f f^{(1)} \cdots f^{(n-1)}}\bigg|_{\Xi^{(n)}} z^{q^n},$$

$$\log_\rho(z) = \sum_{n=0}^{\infty} \frac{\delta^{(n+1)}}{\delta^{(1)} f^{(1)} \cdots f^{(n)}}\bigg|_{\Xi} z^{q^n},$$

where Ξ is the point corresponding to $\mathbb{A} \to A \to \mathbb{C}_\infty$, δ is a function derived from the shtuka function f, and (n) is the Frobenius twist. See Chapter II.

We then proceed to study the coefficients by a factorization. The factorization will be done via Proposition IV.1. Essentially, it tells us that the ideal generated by a sufficiently integral function can be factorized into a product of ideals given by the zeros of the function. Applying this to our coefficients, we will be able to obtain the factorization of the exp and log coefficients from the divisors of the shtuka function and its twists. We then use some basic theory of extension of valuations to study the valuations of each of the factors in Chapter V, thus proving Theorems V.3 and V.2.

I.2: Outline of Thesis

We will first recall some theory on Drinfeld modules, Hayes modules, and shtuka functions in Chapter II. In Chapter III, we will derive a simplified expression for the logarithm series for our curves, following Green and Papanikolas [GP18, Corollary 3.5]. Chapter IV is where we prove the proposition IV.1 mentioned above that allows us to factorize functions according to its divisors. We will then prove Theorems V.3 and V.2 in Chapter V. In Chapter VI, we will discuss the background of Goss L-functions on function fields, and show the log-algebraicity theorem VI.10 for v-adic Goss L-value $L_v(1, \Psi)$ as an application of our results. Then we will give some examples as well as discussing possibilities of generalizations in Chapter VII.

CHAPTER II
Drinfeld Modules

II.1: Notation and Definition

For expository purpose, we will give the basics of Drinfeld modules in a more general setting, rather than just restricting to elliptic curves and ramifying hyperelliptic curves.

Let $\mathbb{F}_q$ be a finite field of q elements, X be a smooth projective geometrically connected curve of genus g over $\mathbb{F}_q$, and $\mathbb{K}$ the function field of X. Let $\infty \in X(\mathbb{F}_q)$ be a closed point of degree d_∞ with residue field $\mathbb{F}_\infty := \mathcal{O}_{K_\infty}/(\infty)$, and $\mathbb{A} := \Gamma(X - \infty, \mathcal{O}_X)$ be the ring of functions regular away from ∞. Since X is finite over $\mathbb{P}^1$, $\mathbb{A}$ is a finite module over $\mathbb{F}_q[t]$ of positive rank. We suppose $\mathbb{F}_q[t]$ is the affine coordinate ring of $\mathbb{P}^1 - \infty$ (the image of ∞ in the cover $X \to \mathbb{P}^1$). Thus $\infty \in X(\mathbb{F}_q)$ lies above the valuation $v_\infty(f) := -\deg_t f$ for $f \in \mathbb{F}_q[t]$.

Let K' be a field extension of $\mathbb{K}$. Then $\mathbb{A}$ acts on $\mathbb{K}'$ via the usual scalar multiplication. The idea of a Drinfeld module is to have another $\mathbb{F}_q$-linear action of $\mathbb{A}$ on K'. To distinguish these two actions, we set A to be a ring isomorphic to $\mathbb{A}$ with an $\mathbb{F}_q$-algebra isomorphism $\iota : \mathbb{A} \to A$, and that $\mathbb{F}_q[t]$ is mapped to $\mathbb{F}_q[\theta]$ via ι. An easy way to think about A is that it has different names for the variables than $\mathbb{A}$. For instance, we have $\mathbb{F}_q[\theta]$ instead of $\mathbb{F}_q[t]$. We define $K := \mathrm{Frac}(A)$ to be the counterpart of $\mathbb{K}$, K_∞ to be the completion of K at the place corresponding to ∞ in $\mathbb{K}$, and $\mathbb{C}_\infty := (\overline{K_\infty})^\wedge$ to be the field by taking an algebraic closure of K_∞ and then completing it. From now on, the field K' is a field extension of K, not $\mathbb{K}$. For us, K' is usually $\mathbb{C}_\infty$.

A table for comparison with number fields is given below.

$\mathbb{Z}$	$\mathbb{F}_q[\theta]$
$\mathbb{Q}$	$\mathbb{F}_q(\theta)$
$K/\mathbb{Q}$ finite	$K/\mathbb{F}_q(\theta)$ finite
$\mathbb{R}$	$K_\infty := \mathbb{F}_q((\frac{1}{\theta}))$
$\mathbb{C}$	$\mathbb{C}_\infty := (\overline{K_\infty})^\wedge$
$\mathbb{C}_p$	$\mathbb{C}_v$ (where v is some finite place of K)

For any field extension K' of K, we denote the integral closure of A in K' to be $\mathcal{O}_{K'}$. We use the same notation to denote the ring of integers if K' is any local field.

As we mentioned, a Drinfeld module is a second $\mathbb{A}$-action (non-scalar multiplication) on K' that are $\mathbb{F}_q$-linear endomorphisms, i.e. elements of $\mathrm{End}_{\mathbb{F}_q}(K')$. Let τ be the Frobenius map on K', $\tau(f) = f^q$. Then the set of polynomials $K'[\tau]$ is a subset of $\mathrm{End}_{\mathbb{F}_q}(K')$. In fact, it is a non-commutative subring, where the multiplication is composition of endomorphisms rather than the usual multiplication of polynomials. To emphasize the distinction, we set $K'\{\tau\}$ to be the *ring of twisted polynomials*, i.e. the non-commutative subring of $\mathrm{End}_{\mathbb{F}_q}(K')$ where the underlying set is $K'[\tau]$. Explicitly, the multiplication is defined by

$$\tau a = a^q \tau \qquad \text{for } a \in K'.$$

We are ready to define Drinfeld modules.

Definition II.1. A *Drinfeld module* over K' is an $\mathbb{F}_q$-algebra homomorphism

$$\rho : \mathbb{A} \to K'\{\tau\}$$

$$a \mapsto \rho_a$$

such that

1. the "constant term" of ρ_a, i.e. coefficient of τ^0 of ρ_a, is $\iota(a)$;
2. (non-triviality) there exists $a \in \mathbb{A}$ such that $\rho_a \neq \iota(a)\tau^0$.

Example II.2. The most basic example of a Drinfeld module is the Carlitz module. Let $\mathbb{A} = \mathbb{F}_q[t]$, and $K' = K = \mathbb{F}_q(\theta)$ with $\iota : \mathbb{A} \to K$ given by $t \mapsto \theta$.

Definition II.3. The *Carlitz module* is the $\mathbb{F}_q$-algebra map $\phi_C : \mathbb{A} \to K\{\tau\}$ defined by

$$\phi_{C,t} = \theta + \tau.$$

For instance, for $z \in K$,

$$\phi_{C,t}(z) = \theta z + z^q.$$

Example II.4. Our second example is over $\mathbb{A} = \mathbb{F}_3[t, y]/(y^2 - (t^3 - t - 1))$. Let $A = \mathbb{F}_3[\theta, \eta]/(\eta^2 - (\theta^3 - \theta - 1))$, and fix the isomorphism $\mathbb{A} \xrightarrow{\sim} A$ with $t \mapsto \theta$ and $y \mapsto \eta$. Let $K' = K = \mathrm{Frac}(A)$. We define $\rho : \mathbb{A} \to K\{\tau\}$ by

$$\rho_t = \theta + \eta(\theta^3 - \theta)\tau + \tau^2, \ \rho_y = \eta + \eta(\eta^3 - \eta)\tau + (\eta^9 + \eta^3 + \eta)\tau^2 + \tau^3.$$

One can check that this is well-defined, i.e. $\rho_t\rho_y = \rho_{ty} = \rho_y\rho_t$.

In general, a Drinfeld module does not need to be defined over a field extension of K. However, we will not go into this more general definition. Interested readers can check the standard references [Gos98, Tha04].

II.2: Properties of Drinfeld modules

In this section, we will outline some basic properties of Drinfeld modules.

II.2.1: Rank

The closed point $\infty \in X(\mathbb{F}_q)$ defines a valuation v_∞ on K or $\mathbb{K}$, via the order of vanishing at ∞. Since $K/\mathbb{F}_q(\theta)$ is finite, the value group $v_\infty(K^\times)$ is discrete. Upon normalization, we set v_∞ such that the value group $v_\infty(K^\times)$ is $\mathbb{Z}$. For $a \in \mathbb{A}$, we define the *degree* of a to be $\deg a := -d_\infty v_\infty(a)$. By abuse of notation, we sometimes talk about the degree of an element in A, via the isomorphism $A \to \mathbb{A}$.

From the examples of Drinfeld modules given, one can observe that the degree of ρ_a, as a polynomial in τ, is related to the degree of a, equivalently $v_\infty(a)$.

Proposition II.1. *([Gos98] 4.5.1, 4.5.3) Let $\rho : \mathbb{A} \to K'\{\tau\}$ be a Drinfeld module. There is a positive integer d, which we will call the* **rank** *of ρ, such that*

$$\deg_\tau \rho_a = d \deg a.$$

Example II.2. One can check from the definition that Carlitz module II.3 is of rank 1. As for example II.4, we have $\deg(t) = 2$ and $\deg(y) = 3$, so the example is also of rank 1.

Example II.3. Let $2 \nmid q$, $\mathbb{A} = \mathbb{F}_q[t]$, $L = \mathbb{F}_q(\sqrt{\theta})$. Define $\rho : \mathbb{A} \to L\{\tau\}$ by $\rho_t = \theta + (\sqrt{\theta} + \sqrt{\theta}^q)\tau + \tau^2$. Then ρ is a rank 2 Drinfeld module.

II.2.2: Over $\mathbb{C}_\infty$: Exponential Function and Uniformization

Historically, Drinfeld modules over $\mathbb{C}_\infty$ were constructed as a characteristic p analogue of elliptic curves over $\mathbb{C}$, possessing a uniformization property and reduction theory. The usual uniformization theory of elliptic curves states that all elliptic curves over $\mathbb{C}$ are isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$, i.e. a discrete finitely-generated $\mathbb{Z}$-module. Due to the topology of $\mathbb{C}$, a lattice has to be of rank 1 or 2. However this is not the case in function field. We define an *A-lattice* in $\mathbb{C}_\infty$ to be a discrete and finitely-generated A-module in $\mathbb{C}_\infty$. A lattice

in $\mathbb{C}_\infty$ can be of arbitrary rank, since $[\mathbb{C}_\infty : K_\infty]$ is infinite, in contrast to $[\mathbb{C} : \mathbb{R}] = 2$. Notice that we do not require that a lattice to be cocompact in $\mathbb{C}_\infty$, and in fact it is never going to be the case.

We call the *rank* of a lattice to be its A-rank. Two lattices $\Lambda, \Lambda' \subset \mathbb{C}_\infty$ are *homothetic* or *isomorphic* if there is $c \in \mathbb{C}_\infty^\times$ such that $\Lambda = c\Lambda'$. Given a non-zero lattice $\Lambda \subset \mathbb{C}_\infty$, its corresponding *exponential function* is defined as

$$\exp_\Lambda(z) = z \prod_{\lambda \in \Lambda}{}' \left(1 - \frac{z}{\lambda}\right),$$

where the product is taken in the order of increasing $|\lambda|$. This gives a power series over $\mathbb{C}_\infty$, which converges for all $z \in \mathbb{C}_\infty$. Since Λ is in particular an $\mathbb{F}_q$-module, the exponential function is $\mathbb{F}_q$-linear, and hence the power series is a power series in z^{q^n}. As an endomorphism of $\mathbb{C}_\infty$, the exponential function $\exp_\Lambda$ has kernel Λ and is surjective. This defines an $\mathbb{A}$-action on the image $\mathbb{C}_\infty$ via multiplication by $\iota(a) \in A$ in the domain.

$$\begin{array}{ccc} \mathbb{C}_\infty & \xrightarrow{\cdot\iota(a)} & \mathbb{C}_\infty \\ \downarrow{\scriptstyle \exp_\Lambda} & & \downarrow{\scriptstyle \exp_\Lambda} \\ \mathbb{C}_\infty & \xrightarrow{\rho_a} & \mathbb{C}_\infty \end{array}$$

That is, $\rho_a(\exp_\Lambda(z)) = \exp_\Lambda(\iota(a)z)$. As the notation suggests, this $\mathbb{A}$-action gives a Drinfeld module $\rho : \mathbb{A} \to \mathbb{C}_\infty\{\tau\}$. The rank of ρ as a Drinfeld module is the same as the rank of Λ as a lattice.

The uniformization theorem states that given a Drinfeld module over $\mathbb{C}_\infty$, there is an associated exponential function and a lattice $\Lambda \subset \mathbb{C}_\infty$, which is the kernel of the exponential function.

Theorem II.4. *([Gos98] 4.6.7, 4.6.9) For each Drinfeld module $\rho : \mathbb{A} \to \mathbb{C}_\infty\{\tau\}$ of rank d, there is a power series $\exp_\rho(z) \in \mathbb{C}_\infty[[z]]$ such that*

- $\exp_\rho(z) = z + O(z^q)$;
- *for all $a \in \mathbb{A}$,*

$$\exp_\rho(\iota(a)z) = \rho_a(\exp_\rho(z)).$$

Moreover, the kernel of $\exp_\rho$ is an A-lattice of rank d in $\mathbb{C}_\infty$.

II.3: Hayes modules

One application of elliptic curves is to construct abelian extensions of imaginary quadratic number fields. Specifically, we use the torsion points of elliptic curves to construct such

extensions, just as we use the torsion points of the algebraic group $\mathbb{G}_m$ to construct abelian extensions of $\mathbb{Q}$. In a similar manner, we can construct abelian extensions of all global function fields. This was developed by Hayes in [Hay74] and [Hay79]. What he did is to consider a specific type of rank 1 Drinfeld modules, which are later called *Hayes modules*. There are lots of good expositions on this subject, for instance [Gos98, Ch. 7], [Tha04, Ch. 3], which we will closely follow in this section.

II.3.1: sign functions

To define Hayes modules, we need a way to normalize elements in $\mathbb{A}$. Thus we need to have a notion similar to the leading coefficient of a polynomial. We set $\mathbb{K}_\infty$ to be the field isomorphic to K_∞ and containing $\mathbb{A}$, extending from the isomorphism $\iota : \mathbb{A} \to A$.

Definition II.1. A *sign function* is a group homomorphism $\mathrm{sgn} : \mathbb{K}_\infty^\times \to \mathbb{F}_\infty^\times$ such that when restricted to $\mathcal{O}_{K_\infty}^\times$, it is the same as

$$\mathcal{O}_{K_\infty}^\times \xrightarrow{\text{mod } \infty} (\mathcal{O}_{K_\infty}/(\infty))^\times = \mathbb{F}_\infty^\times.$$

We also set $\mathrm{sgn}(0) = 0$.

From the definition, we make 2 observations:

- on the group of 1-units $U_1 \subset \mathcal{O}_{K_\infty}^\times$, sgn is trivial;
- the composition of sgn with the Hensel's lift is the identity map:

$$\mathbb{F}_\infty^\times \xrightarrow[\text{lift}]{\text{Hensel's}} \mathcal{O}_{K_\infty}^\times \xrightarrow{\text{sgn}} \mathbb{F}_\infty^\times.$$

Example II.2. Let $c \in \mathbb{F}_q^\times$. A list of examples for sign functions on $\mathbb{F}_q((\frac{1}{t}))$ is

$$\mathrm{sgn}(t) = c.$$

This completely determined a sign function since $\mathbb{F}_q((\frac{1}{t}))^\times \simeq t^{\mathbb{Z}} \times U_1 \times \mathbb{F}_q^\times$.

When $c = 1$, this sign function is a generalization of the "leading coefficient of a polynomial". To illustrate, observe that

$$a_n t^n + \cdots + a_0 = (t^{-1})^{-n} a_n (1 + O(t^{-1})),$$

and hence $\mathrm{sgn}(a_n t^n + \cdots + a_0) = a_n$.

From the previous example, we can see that to give a sign function, it is equivalent to specify a uniformizer $\pi \in \mathbb{K}_\infty$ and give the value $\mathrm{sgn}(\pi)$.

II.3.2: Definition of Hayes modules

Below we will fix a sign function sgn. Let ρ be a rank 1 Drinfeld module over $\mathbb{C}_\infty$. For $a \in \mathbb{A}$, define $\mu(a)$ to be the leading coefficient of $\rho_a(\tau)$. For our purpose later, we require by repicking ρ from its isomorphism class that $\mu(a) = 1$ for some non-constant a. By the equality

$$\mu(ab) = \mu(a)\mu(b)^{q^{\deg a}} = \mu(a)^{q^{\deg b}}\mu(b),$$

$\mu(b)$ is in $\mathbb{F}_{q^{\deg a}}$ for all $b \in \mathbb{A}$.

By Riemann-Roch, there exists $a \in \mathbb{A}$ with $v_\infty(a) = -n$ for all $n \gg 0$. We can extend μ to $\mathbb{K}_\infty$ by setting $\mu(U_1) = 1$ for the 1-units $U_1 \subset \mathbb{K}_\infty^\times$, and determine $\mu(a')$ for $a' \in \mathbb{K}_\infty^\times$ by having $b, b' \in \mathbb{A}$ such that $a'b = b'$ modulo U_1. The equality uniquely determines $\mu(a')$ as $\mu(b), \mu(b')$ are in a finite field over $\mathbb{F}_q$, in which raising by powers of q is a bijection. By composing μ with the Hensel's lift $\mathbb{F}_\infty^\times \to \mathbb{K}_\infty^\times$, one can see easily that the composition

$$\mathbb{F}_\infty^\times \xrightarrow{\text{Hensel's lift}} \mathbb{K}_\infty^\times \xrightarrow{\text{sgn}} \mathbb{F}_\infty^\times$$

is a map in $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}_q)$.

Definition II.3. A *(Drinfeld-)Hayes module* or a sgn-*normalized Drinfeld module* is a rank 1 Drinfeld module $\rho : \mathbb{A} \to \mathbb{C}_\infty\{\tau\}$ such that

$$\mu(a) = \sigma(\mathrm{sgn}(a))$$

for some $\sigma \in \mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}_q)$.

Example II.4. The Carlitz module is a Hayes module with respect to $\mathrm{sgn}(t) = 1$.

Example II.5. Example II.4 gives a Hayes module with respect to $\mathrm{sgn}(t) = \mathrm{sgn}(y) = 1$.

Fix sgn. Hayes modules should be thought of as a good representative in isomorphism classes of rank 1 Drinfeld modules over $\mathbb{C}_\infty$. This will be illustrated with class field theory later. In particular, we can count the number of Hayes module from the number of isomorphism classes of rank 1 Drinfeld modules. We cite the following result from [Gos98, 7.2.15] and [Tha04, 3.2.2].

Proposition II.6. *Fix a* sgn. *Every rank 1 Drinfeld module over* $\mathbb{C}_\infty$ *is isomorphic to some Hayes module for* sgn.

The proof is quite easy: just fix an isomorphism $\rho = c\rho' c^{-1}$ and examine $\mu(\pi)$ for ρ and ρ' for some uniformizer π.

By the uniformization theorem, any rank 1 Drinfeld modules over $\mathbb{C}_\infty$ corresponds to an A-lattice in $\mathbb{C}_\infty$. Since A is a Dedekind domain, any finitely-generated torsion-free A-module is isomorphic to

$$A^{d-1} \oplus I$$

for some non-zero ideal $I \subset A$, and d is the A-rank of the module. For the rank 1 case, every rank 1 A-lattice in $\mathbb{C}_\infty$ is isomorphic to an A-ideal, so there are $h(A)$ many isomorphism classes for rank 1 Drinfeld module over $\mathbb{C}_\infty$, where $h(A)$ is the class number of A.

It is possible that two Hayes modules lie in the same isomorphism class. If ρ is a Hayes module for sgn and $c \in \mathbb{C}_\infty^\times$, then $\rho' := c^{-1}\rho c$ is a Hayes module if and only if

$$c^{q^{d_\infty}-1} = 1$$

([Gos98, 7.2.18], [Tha04, 3.2.4]), i.e. $c \in \mathbb{F}_\infty^\times$. However, not all such c gives a different Hayes module. A simple calculation shows that $\rho = \rho'$ if and only if $c^{q-1} = 1$, i.e. $c \in \mathbb{F}_q^\times$. Therefore, we have the following count for Hayes module.

Proposition II.7. *There are* $h(A) \cdot \dfrac{\#\mathbb{F}_\infty^\times}{\#\mathbb{F}_q^\times}$ *many Hayes modules for* sgn.

II.3.3: Action of ideals on Hayes modules

Let $\mathfrak{X}$ be the set of Hayes modules with respect to $(K, \infty, \mathrm{sgn})$. In this subsection we will define an action on $\mathfrak{X}$ by ideals of A. This action by ideals will be used to relate Hayes modules with class field theory.

Definition II.8. Let ρ be a Hayes module and $I \subset A$ a nonzero ideal. We define $\rho_I(\tau) \in \mathbb{C}_\infty\{\tau\}$ to be the monic (as a polynomial in τ) element generating the (principal, see [Gos98, Cor 1.6.3]) left ideal in $\mathbb{C}_\infty\{\tau\}$:

$$\mathbb{C}_\infty\{\tau\}\{\rho_i \mid i \in I\}$$

(here we abuse the notation of $i \in I \subset A$ and $i \in \mathbb{A}$ for ρ_i). We define $D(\rho_I)$ to be the constant term of $\rho_I(\tau)$.

Proposition II.9. *For any Drinfeld module ρ of any rank over any field L, there is a Drinfeld module $I * \rho$, of the same rank over the same field, such that for all $a \in \mathbb{A}$,*

$$(I * \rho)_a \rho_I = \rho_I \rho_a.$$

If ρ is a Hayes module, so is $I * \rho$.

(See [Gos98, §4.9], [Tha04, 2.4.3(4)].) Let $\mathcal{I}$ be the group of fractional A-ideals in K. Then $\rho \mapsto I * \rho$ gives an action of $\mathcal{I}$ on $\mathfrak{X}$. It is easy to see that the action factors through $\mathcal{P}^+$, the subgroup of principal ideals generated by sgn 1 elements. This is because if $I = (i)$ for some $\operatorname{sgn} i = 1$, then $\rho_I = \rho_i$. What's more interesting is that the action of $\mathcal{I}/\mathcal{P}^+$ on $\mathfrak{X}$ is transitive and free, which can be seen by the uniformization theorem. See [Gos98, 4.9.5].

Proposition II.10. *The set $\mathfrak{X}$ is a principal homogeneous space for the group action $\mathcal{I}/\mathcal{P}^+$.*

II.3.4: Field of Definition and Hilbert class field

For a Hayes module ρ and a non-constant element $a \in \mathbb{A}$, let H^+ be the field generated by K and coefficients of ρ_a in $\mathbb{C}_\infty$. It turns out that H^+ is independent of the choice of a ([Gos98, Prop7.4.2], because of $\rho_a\rho_b = \rho_b\rho_a$) or ρ (because of the ideal action as illustrated in the previous subsection), but just on the choice of ∞ and sgn. From the equations

$$e_\rho(\iota(a)z) = \rho_a(z), \qquad \log_\rho(\rho_a(z)) = \iota(a)\log_\rho(z)$$

and that the coefficients of z are 1 for both series, the coefficients of $e_\rho(z)$ and $\log_\rho(z)$ are in H^+.

Let $\mathrm{Cl}^+(A)$ be the narrow class group of A, i.e.

$$\mathrm{Cl}^+(A) := \mathcal{I}/\mathcal{P}^+.$$

It is not hard to see that the extension H^+/K is finite Galois [Gos98, Prop 7.4.3]. Once we have taken the action of $\mathrm{Cl}^+(A)$ on $\mathfrak{X}$ into account, we can see that H^+/K is abelian [Gos98, Prop 7.4.4]. In fact, we have the following result.

Proposition II.11. *The field extension H^+/K is finite abelian with Galois group naturally isomorphic to $\mathrm{Cl}^+(A)$. The isomorphism between the Galois group and the class group coincides with the Artin map. That is, if I is a nonzero ideal and $\sigma_I \in \mathrm{Gal}(H^+/K)$ is the Artin map associated to I, then*

$$\sigma_I \rho = I * \rho$$

for any Hayes module ρ.

The proof is done in detail in [Tha04, §3.3] and [Gos98, §7.4]. The key step is to analyze the Artin map $\sigma_\mathfrak{p}$ of a prime $\mathfrak{p}$, and reduce modulo $\mathfrak{p}$. By definition of Artin map, the map mod $\mathfrak{p}$ is given by Frobenius. Then some reduction theory of rank 1 Drinfeld module ([Tha04, 3.3.2], [Gos98, 7.4.6]) allows us to lift the equality to the ring before modulo $\mathfrak{p}$.

By the same idea of reducing mod $\mathfrak{p}$ and lifting up, we have the following result.

Proposition II.12. *The extension H^+/K is unramified at all finite places of K. The decomposition group and the inertia group at ∞ are both isomorphic to $\mathbb{F}_\infty^\times/\mathbb{F}_q^\times$. The fixed field of the decomposition group at ∞, which we denote by H, has that H/K is totally split at ∞.*

This H is the *Hilbert class field* of K (with respect to ∞).

As a remark, initially Drinfeld developed the class field theory of function fields using the moduli schemes of Drinfeld modules (of rank d, with level I-structure). This can be bypassed with more elementary tools, as illustrated by Thakur in [Tha04, Ch. 3]. Since we will not be using the idea of moduli scheme, we have been following Thakur's approach on this subject.

II.3.5: Division fields and narrow ray class field

For a Drinfeld module ρ over $\mathbb{C}_\infty$ and an ideal $I \subset A$, we define the *I-torsion points of ρ* to be

$$\rho[I] := \{z \in \mathbb{C}_\infty \mid \rho_i(z) = 0 \text{ for all } i \in I\}$$

The set $\rho[I]$ naturally comes with an A/I-module structure given by ρ, and is isomorphic to $(A/I)^{\mathrm{rank}\rho}$ as an A/I-module. For ρ a Hayes module, define $K(\rho[I])$ to be the extension of H^+ generated by $\rho[I]$. By a similar argument of H^+/K is Galois from the group action of $\mathcal{I}/\mathcal{P}^+$ on $\mathfrak{X}$, the extension $K(\rho[I])/K$ is Galois and abelian, and that $\mathrm{Gal}(K(\rho[I])/K)$ is a subgroup of the narrow ray class group

$$\mathrm{Cl}^+(I) := \mathcal{I}(I)/\mathcal{P}_I^+,$$

where $\mathcal{I}(I)$ is the group of fractional ideals prime to I, and $\mathcal{P}_I^+$ is the group of principal ideals generated by elements of sgn 1 and congruent to 1 modulo I.

Proposition II.13. *([Tha04, §3.6], [Gos98, §7.5]) The Galois group $\mathrm{Gal}(K(\rho[I])/K)$ is isomorphic to $\mathrm{Cl}^+(I)$ with the isomorphism given by the ideal action as above. In particular, the Galois group $\mathrm{Gal}(K(\rho[I])/H^+)$ is isomorphic to $(A/I)^\times$. The extension $K(\rho[I])/K$ is unramified at places away from I, ∞. The decomposition and inertia groups at ∞ for $K(\rho[I])/K$ is isomorphic to $\mathbb{F}_\infty^\times$.*

We say λ is a *primitive I-torsion point of ρ* if $\lambda \in \rho[I]$ and $\lambda \notin \rho[J]$ for any $J \supsetneq I$. Over $\mathbb{Q}$, the narrow ray class field modulo $n\infty$ is the cyclotomic field $\mathbb{Q}(\zeta_n)$, generated by one (and any) primitive n-torsion point of $\mathbb{G}_m$. This is the same over function fields.

Proposition II.14. *([Tha04, 3.6.2], [Gos98, 7.5.15]) Fix a primitive I-torsion point λ. Then*

$$K(\rho[I]) = K(\lambda).$$

II.4: Shtuka and shtuka function

Shtuka is a generalization of Drinfeld module that Drinfeld constructed to prove the Langlands correspondence for GL_2 in function field. Roughly speaking, a shtuka is a set of quasi-coherent modules together with some linking maps such that the cokernels satisfy certain properties. At first glance, this geometric object has nothing to do with Drinfeld modules at all. Drinfeld made a clever observation that gives an equivalence between such sets of sheaves and (classes of) functions into ring of twisted polynomials, of which Drinfeld module is a particular instance. See [Dri77], [Dri87], [Mum77], [Gos98, §6.2], [Tha04, §7.8].

Since we are primarily interested in Hayes module, which is in particular of rank 1, for our purpose we do not need the full generality of shtuka. In the rank 1 case, Thakur [Tha93] observed that a shtuka boils down to a point $\overline{\infty} \in X(\mathbb{C}_\infty)$ and a divisor V, called a *Drinfeld divisor*, which is a solution to an equation involving Frobenius. From a Drinfeld divisor and a fixed choice of sign function, one can fix a meromorphic function called a *shtuka function*. It turns out that the set of shtuka functions and the set of Hayes modules are in bijective correspondence.

In this section, we will show how to construct a Drinfeld divisor from a curve and then a shtuka function upon fixing a sign function. We will also see the correspondence between shtuka functions and Hayes modules. As an application, we will see how we can express the exponential and logarithm series of a Hayes module in terms of the corresponding shtuka function.

II.4.1: Drinfeld vanishing lemma

The correspondence that Drinfeld showed in [Dri77, Prop 2] or [Mum77] relies heavily on a vanishing lemma, see [Dri77, Remark after Prop 3], [Gos98, 6.2.3]. In the rank 1 case, Thakur [Tha93, 0.3.1] restated this lemma can be stated in simpler terms, which we will go through in this subsection.

We begin by fixing some notations. We continue to use X, A, $\mathbb{A}$, etc in the same way as before. Recall that g is the genus of X. Let L be an algebraically closed field containing and transcendental over $\mathbb{F}_q$, $\overline{X} = X_L := X \times_{\mathbb{F}_q} \operatorname{Spec} L$, $\overline{X}(L)$ the L-closed points of $\overline{X}$, and $\overline{\infty} \in X(L)$ a point (out of the d_∞ many choices) above $\infty \in X(\overline{\mathbb{F}_q})$. One can think of $L = \mathbb{C}_\infty$ for simplicity.

For a point P or a divisor V on X or $\overline{X}$, we define $P^{(1)}$, $V^{(1)}$ to be the Frobenius twist of the point and the divisor. If we have an affine open model of the curve, the Frobenius twist is the same as raising q-th power to each coordinate.

Lemma II.1 (Drinfeld vanishing lemma, rank 1)**.** *[Tha93, 0.3.1] Let $\xi, \eta \in X(L)$. Suppose V is a divisor of $\overline{X}$ of degree g and f is a meromorphic function on $\overline{X}$ such that*

$$\operatorname{div}(f) = V^{(1)} - V + (\xi) - (\eta).$$

If $\xi \neq \eta^{(s-1)}$ for all $|s| < g$, then

$$H^0(\overline{X}, \mathcal{O}_{\overline{X}}(V - \eta^{(-1)})) = H^1(\overline{X}, \mathcal{O}_{\overline{X}}(V - \eta^{(-1)})) = 0.$$

Proof. If $g = 0$, then both $\mathcal{O}_{\overline{X}}(V - (\eta^{(-1)}))$ and $\omega_{\overline{X}} \otimes \mathcal{O}_{\overline{X}}(-V + (\eta^{(-1)}))$ have degree $-1 < 0$, so both of these cohomology groups vanish.

Now suppose $g > 0$. For each $i \in \mathbb{Z}$, define V_i inductively by

$$V_0 := V - (\eta^{(-1)}), \qquad V_{i+1} := V_i + (\eta^{(i-1)}).$$

In particular, $\deg V_i = g - 1 + i$. Set $\mathcal{L}_i := \mathcal{O}_{\overline{X}}(V_i)$.

We would like to show that $h^0(\overline{X}, \mathcal{L}_0) = h^1(\overline{X}, \mathcal{L}_0) = 0$. By Riemann-Roch, the Euler characteristic $\chi(\overline{X}, \mathcal{L}_0) = g - 1 + 1 - g = 0$, so it suffices to show that $h^0(\overline{X}, \mathcal{L}_0) = 0$.

Consider the following set

$$S := \{1 - g \leq s \leq g \mid h^0(\overline{X}, \mathcal{L}_s) = h^0(\overline{X}, \mathcal{L}_{s-1}) + 1\}.$$

Since $\deg \mathcal{L}_{-g} = -1 < 0$, we have $h^0(\overline{X}, \mathcal{L}_{-g}) = 0$. Also since $\deg \mathcal{L}_g = 2g - 1$, we have $\deg(\omega_{\overline{X}} \otimes \mathcal{L}_g^{-1}) = (2g - 2) - (2g - 1) = -1$. Thus by Serre duality, $h^1(\overline{X}, \mathcal{L}_g) = h^0(\overline{X}, \omega_{\overline{X}} \otimes \mathcal{L}_g^{-1}) = 0$. Hence $h^0(\overline{X}, \mathcal{L}_g) = \chi(\overline{X}, \mathcal{L}_g) = g$. Since it is always true that $h^0(\overline{X}, \mathcal{L}_s) \leq h^0(\overline{X}, \mathcal{L}_{s-1}) + 1$, the cardinality of S is g. We will show that $S = \{1, 2, \ldots, g\}$, and thus $h^0(\overline{X}, \mathcal{L}_0) = h^0(\overline{X}, \mathcal{L}_g) - g = 0$.

Suppose we have an integer $s \in S$ and $s < g$. We will show that $s + 1 \in S$. By definition of S, we can find a global section $e \in H^0(\overline{X}, \mathcal{L}_s)$ that does not come from $H^0(\overline{X}, \mathcal{L}_{s-1})$. In terms of poles and zeros, $e \in H^0(\overline{X}, \mathcal{L}_s)$ means e has zeros and potential poles described by

V, and adjusted by

$$\begin{cases} \text{at most another pole / one less zero at } \eta^{(i)} \text{ for } i = 0, 1, \ldots, s-2, & \text{if } s > 1 \\ \text{at least another zero / one less pole at } \eta^{(i)} \text{ for } i = -1, -2, \ldots, -(1-s), & \text{if } s < 1 \\ \text{(no adjustment)} & \text{if } s = 1. \end{cases}$$

And $e \notin H^0(\overline{X}, \mathcal{L}_{s-1})$ means that e does have another pole / one less zero at $\eta^{(s-2)}$, compared to the description from V.

Now consider the zeros and pole of $fe^{(1)}$. By multiplying by f, the potential poles of $e^{(1)}$ at $V^{(1)}$ got canceled, while the potential poles at V are given back. It also adds a pole at $\eta^{(0)}$ and a zero at ξ. By assumption, $\xi \neq \eta^{(s)}$ for $|s| < g$, so the new zero does not cancel with the poles at $\eta^{(i)}$ which we have been keeping track of. Together, $fe^{(1)}$ has zeros and potential poles described by V, and adjusted by

$$\begin{cases} \text{at most another pole / one less zero at } \eta^{(i)} \text{ for } i = 0, 1, \ldots, s-1, & \text{if } s > 1 \\ \text{at least another zero / one less pole at } \eta^{(i)} \text{ for } i = -1, -2, \ldots, s, & \text{if } s < 1 \\ \text{(no adjustment)} & \text{if } s = 1. \end{cases}$$

This shows that $fe^{(1)} \in H^0(\overline{X}, \mathcal{L}_{s+1})$. Also $fe^{(1)}$ does have another pole / one less zero at $\eta^{(s-1)}$, so $fe^{(1)} \notin H^0(\overline{X}, \mathcal{L}_s)$. Thus $s+1 \in S$ for all $s \in S$ with $s < g$. Since $\#S = g$, we can conclude by induction that $S = \{1, 2, \ldots, g\}$, and hence we have the desired result.

□

Corollary II.2. *[Tha93, 0.3.3] Let $\xi, \eta \in \overline{X}(L)$.*

1. *Suppose that for all $|s| < g$, we have $\xi \neq \eta^{(s-1)}$. Then for all effective divisor V of degree g on $\overline{X}$ such that $V^{(1)} - V + (\xi) - (\eta)$ is principal, the points $\eta^{(-1)}$ and ξ are not in the support of V.*

2. *Suppose that for all $|s| < g$, we have $\xi \neq \eta^{(s)}$. Then for all effective divisor V of degree g on $\overline{X}$ such that $V^{(1)} - V + (\xi) - (\eta)$ is principal, the support of V does not contain any $\mathbb{F}_q$-rational point.*

3. *Let $d < g$ be a non-negative integer. Suppose that for all $|s| < g$, we have $\xi \neq \eta^{(g-d+s-1)}$. Then for all effecitve divisor W of degree d on $\overline{X}$, $W^{(1)} - W + (\xi) - (\eta)$ cannot be principal.*

Proof. 1. Let V be such a divisor. By Drinfeld vanishing lemma II.1, the global section $H^0(\overline{X}, \mathcal{O}_{\overline{X}}(V - (\eta^{(-1)}))) = 0$. Since scalars are global sections to all effective divisors,

this shows that $V - (\eta^{(-1)})$ is not effective. To see that ξ is not in the support of V, suppose the contrary, and let $V' = V - (\xi) + (\eta)$. Then V' is effective of degree g, and

$$V'^{(1)} - V' + (\xi^{(1)}) - (\eta^{(1)}) = V^{(1)} - V + (\xi) - (\eta)$$

is principal. Since $\xi^{(1)} \neq (\eta^{(1)})^{(s-1)}$ for all $|s| < g$, this gives a contradiction to the fact that $\eta^{(1-1)}$ should not be in the support of V'.

2. Let V be such a divisor, and suppose for contradiction that μ is a rational point in the support of V. Let $V' = V - (\mu) + (\eta)$. Then V' is effective of degree g, and

$$V'^{(1)} - V' + (\xi) - (\eta^{(1)}) = V^{(1)} - V + (\xi) - (\eta)$$

is principal. Since $\xi \neq (\eta^{(1)})^{(s-1)}$ for all $|s| < g$ and $\eta^{(1-1)}$ is in the support of V', this contradicts with (a).

3. For sake of contradiction, let $d < g$ and W be an effective divisor of degree d with $W^{(1)} - W + (\xi) - (\eta)$ principal. Let

$$V = \begin{cases} W + (\eta) + (\eta^{(1)}) + \cdots + (\eta^{(g-d-2)}) + (\xi^{(-1)}) & \text{if } d < g-1; \\ W + (\eta) & \text{if } d = g-1. \end{cases}$$

Then V is an effective divisor of degree g and

$$\begin{aligned} V^{(1)} - V + (\xi^{(-1)}) - (\eta^{(g-d-1)}) \text{ for } d < g-1 \\ V^{(1)} - V + (\xi) - (\eta^{(1)}) \text{ for } d = g-1 \end{aligned}$$

is principal and has $\eta^{(g-d-2)}$ or η in its support, contradicting (a).

□

For any point $\xi \in \overline{X}(L)$ transcendental over $\mathbb{F}_q$, one can show, by using the isomorphism of the degree-zero Picard group and the Jacobian variety of X, of the following.

Proposition II.3. *There exists an effective divisor V of degree g on $\overline{X}$ such that*

$$V^{(1)} - V + (\xi) - (\overline{\infty}^{(1)})$$

is principal.

Proof. We will first ignore the degree and effective requirement and construct a divisor satisfying the equation. Then we adjust V to have degree g, and finally make it effective.

Via the isomorphism $\mathrm{Jac}(\overline{X}) \simeq \mathrm{Pic}^0(\overline{X})$, we transfer the problem to solving an equation on the abelian variety $\mathrm{Jac}(\overline{X})$. The endomorphism $\mathrm{Id} - \mathrm{Frob}$ on the abelian variety $\mathrm{Jac}(\overline{X})$ has finite kernel, namely $\mathrm{Pic}^0(\overline{X})(\mathbb{F}_q)$, the $\mathbb{F}_q$-points of the abelian variety. Hence $\mathrm{Id} - \mathrm{Frob}$ is an isogeny, and thus surjective. As a result, there is a degree 0 divisor V such that $V - V^{(1)}$ is linearly equivalent to $(\Xi) - (\overline{\infty}^{(1)})$, as desired.

We then proceed to increase the degree of V. By [Har13, Exercise V.1.10],

$$\#X(\mathbb{F}_{q^m}) = 1 - a + q^m, \qquad \text{where } |a| \leq 2g\sqrt{q^m}.$$

In particular, $\#X(\mathbb{F}_{q^m}) \geq 1$ for all $m \gg 0$. Fix such an m and let $\zeta_1 \in X(\mathbb{F}_{q^m})$ and $\zeta_2 \in X(\mathbb{F}_{q^{m+1}})$, and define

$$D := (\zeta_2) + (\zeta_2^{(1)}) + \cdots + (\zeta_2^{(m)}) - (\zeta_1) - (\zeta_1^{(1)}) - \cdots - (\zeta_1^{(m-1)}).$$

By definition, $\deg D = 1$, and $D^{(1)} - D = 0$. By adding g copies of D to the divisor we got previously, we get a degree g divisor V with $V^{(1)} - V + (\xi) - (\overline{\infty}^{(1)})$ principal.

Finally, we attempt to make V effective by removing its poles. By Riemann-Roch, the Euler characteristic $\chi(\overline{X}, \mathcal{O}_{\overline{X}}(V)) = 1$. In particular, $h^0(\overline{X}, \mathcal{O}_{\overline{X}}(V)) \geq 1$. Let h be a nonzero global section of $\mathcal{O}_{\overline{X}}(V)$. By definition,

$$V + \mathrm{div}(h) \geq 0.$$

By construction,

$$[V + \mathrm{div}(h)]^{(1)} - [V + \mathrm{div}(h)] + (\xi) - (\overline{\infty}^{(1)}) = \mathrm{div}\left(\frac{fh^{(1)}}{h}\right),$$

where

$$\mathrm{div}(f) = V^{(1)} - V + (\xi) - (\overline{\infty}^{(1)}).$$

So $V + \mathrm{div}(h)$ is an effective divisor of degree g satisfying the desired assumption.

□

Let $L = \mathbb{C}_\infty$ and Ξ be the point in $X(\mathbb{C}_\infty)$ corresponding to the map

$$\mathbb{A} \xrightarrow{\sim} A \hookrightarrow \mathbb{C}_\infty.$$

In terms of coordinates, we are corresponding the variables of $\mathbb{A}$ to A.

Example II.4. For $X = \mathbb{P}^1$ and $\mathbb{A} = \mathbb{F}_q[t]$, the point Ξ is the point having the coordinate

$t = \theta$ in $X(\mathbb{C}_\infty)$.

We can now define a Drinfeld divisor.

Definition II.5. We define a *Drinfeld divisor* (with respect to $\overline{\infty}$) to be an effective divisor V of degree g such that

$$V^{(1)} - V + (\Xi) - (\overline{\infty}^{(1)})$$

is principal.

By the proposition above, a Drinfeld divisor exists. One then naturally asks whether it is unique, or if not, is there a classification for such divisors. This question is answered with the help of Drinfeld vanishing lemma II.1.

Proposition II.6. *(a) Drinfeld divisor is unique in its divisor class. That is, if V_1, V_2 are Drinfeld divisors such that $V_1 - V_2 = \mathrm{div}(h)$ for some meromorphic function h on $\overline{X}$, then $V_1 = V_2$.*

(b) Upon fixing $\overline{\infty}$, there are $\#\operatorname{Pic}(\overline{X})(\mathbb{F}_q)$ many Drinfeld divisors on X.

Proof. (a) Since Ξ is transcendental and $\overline{\infty}^{(1)}$ is algebraic over $\mathbb{F}_q$, we have $\Xi \neq \overline{\infty}^{(1+s)}$ for any s. By Drinfeld vanishing lemma II.1,

$$h^0(\overline{X}, \mathcal{O}_{\overline{X}}(V_i)) = 1$$

for $i = 1, 2$. Since V_i are effective, all scalars are in $H^0(\overline{X}, \mathcal{O}_{\overline{X}}(V_i))$, so in fact the global sections are just $\mathbb{C}_\infty$ from the dimension. Finally, multiplication by h defines an isomorphism

$$H^0(\overline{X}, \mathcal{O}_{\overline{X}}(V_1)) \to H^0(\overline{X}, \mathcal{O}_{\overline{X}}(V_2)),$$

so h must be in $\mathbb{C}_\infty^\times$. This shows that $V_1 = V_2$.

(b) If V_1, V_2 are two Drinfeld divisors, then $V_1^{(1)} - V_2^{(1)}$ is linearly equivalent to $V_1 - V_2$. Hence $V_1 - V_2$ is in $\operatorname{Pic}^0(\overline{X})(\mathbb{F}_q)$. Since each divisor class can have at most one Drinfeld divisor, we have at most $\operatorname{Pic}^0(\overline{X})(\mathbb{F}_q)$ many Drinfeld divisors.

The existence of a Drinfeld divisor in each divisor class comes from the construction of Drinfeld divisor in Proposition II.3: in the construction we first pick a divisor V such that $V - V^{(1)}$ is linearly equivalent to $(\Xi) - (\overline{\infty}^{(1)})$. Recall from the proof that such a V exists because the map $\mathrm{Id} - \mathrm{Frob}$ on $\operatorname{Pic}^0(\overline{X})$ is an isogeny. This isogeny has kernel $\operatorname{Pic}^0(\overline{X})(\mathbb{F}_q)$. If $D \in \operatorname{Pic}^0(\overline{X})(\mathbb{F}_q)$ and we replace V by $V' := V + D$ and proceed with the construction, one can see by examining the proof that:

- at the second step (making the divisor of degree g), we can change our divisor from step 1 by a fixed divisor; hence the divisor class of the resulting degree g divisor we obtain from V' will be of a different divisor class compared to that we obtain from V;
- at the third step (making the divisor effective), we are adding div of a meromorphic function, thus not changing the divisor class.

Therefore, the Drinfeld divisors we get by using V' is of a different divisor class from the Drinfeld divisor we get by using V. This shows that we have at least $\mathrm{Pic}^0(\overline{X})(\mathbb{F}_q)$ many Drinfeld divisors.

□

The above calculation shows some evidence of the relation between Drinfeld divisors and Hayes modules. Recall that there are $h(\mathbb{A}) \cdot \frac{\#\mathbb{F}_\infty^\times}{\#\mathbb{F}_q^\times} = \#\,\mathrm{Pic}^0(\overline{X})(\mathbb{F}_q) \cdot d_\infty \cdot \frac{\#\mathbb{F}_\infty^\times}{\#\mathbb{F}_q^\times}$ many Hayes modules with respect to a fixed sgn for $\overline{\infty}$. Among them, every $\frac{\#\mathbb{F}_\infty^\times}{\#\mathbb{F}_q^\times}$ of them lie in the same isomorphism class, so there are actually $\#\,\mathrm{Pic}^0(\overline{X})(\mathbb{F}_q) \cdot d_\infty$ many isomorphism classes of Hayes module with respect to a fixed sgn. On the Drinfeld divisors's end, there are $\#\,\mathrm{Pic}^0(\overline{X})(\mathbb{F}_q)$ many Drinfeld divisors for each choice of $\overline{\infty}$, and there are d_∞ many such choices. This is the rank 1 instance of Drinfeld's shtuka correspondence. We will make this precise soon by constructing Hayes modules from Drinfeld divisors.

II.4.2: $\widetilde{\mathrm{sgn}}$

Fix $\overline{\infty} \in \overline{X}(\mathbb{C}_\infty)$ and a Drinfeld divisor V. Out of the principal divisor class $V^{(1)} - V + (\Xi) - (\overline{\infty}^{(1)})$, we want to pick a good choice of meromorphic function representing the class. For meromorphic functions over X, we have the notion of a sign function to help us pick a choice of a function, coming from the idea of picking a monic polynomial out of a principal ideal. We will extend this idea to $\overline{X}$. This motivates us to extend the notion of a sign function sgn to $\overline{X}$. We will do this generally for X_L, where L is any field containing $\mathbb{F}_q$.

Recall that fixing a sign function sgn is equivalent to assigning the value $\mathrm{sgn}\,\pi \in \mathbb{F}_\infty^\times$ for a uniformizer π at ∞. Fix such a uniformizer $\pi \in K_\infty$. To extend sgn to $\mathrm{Frac}(L \otimes \mathbb{A})$, the function field of X_L, first fix a closed point $\overline{\infty} \in \overline{X}(L)$ above ∞. We have that $\pi \in K \hookrightarrow \mathrm{Frac}(L \otimes \mathbb{A})$ is a uniformizer at $\overline{\infty}$. In the completion $(\mathrm{Frac}(L \otimes \mathbb{A}))_{\overline{\infty}} \simeq L((\pi))$, a function $G \in \mathrm{Frac}(L \otimes \mathbb{A})$ has an expansion

$$G = \sum_{n=-m}^{\infty} a_n \pi^n,$$

with $a_n \in L$ and $a_{-m} \neq 0$. We define

$$\widetilde{\mathrm{sgn}} : \mathrm{Frac}(L \otimes_{\mathbb{F}_q} \mathbb{A}) \to L$$

by $\widetilde{\mathrm{sgn}}(G) := a_{-m}(\mathrm{sgn}\,\pi)^{-m}$. The multiplication is defined since L, being algebraically closed, contains $\mathbb{F}_\infty$.

Example II.7. Suppose $\mathbb{A} = \mathbb{F}_q[t]$, sgn defined by $\mathrm{sgn}(1/t) = 1$, $L = \mathbb{C}_\infty$. Then $\widetilde{\mathrm{sgn}}(\theta t+1) = \theta$. In this example, $\widetilde{\mathrm{sgn}}$ is extending sgn to broader coefficients.

Example II.8. If $v_{\overline{\infty}}(F) = 0$ for a function F in the function field of $\overline{X}$, then $\widetilde{\mathrm{sgn}}F = F \pmod{\overline{\infty}} = F|_{\overline{\infty}}$, just by unwinding the definition of $\widetilde{\mathrm{sgn}}$.

II.4.3: Shtuka function

In this subsection, we will construct the meromorphic functions we have been preparing for, called the *shtuka function*. Fix an $\overline{\infty}$, a Drinfeld divisor V, and a sign function sgn.

Definition II.9. A *shtuka function* corresponding to the datum $(\overline{\infty}, V, \mathrm{sgn})$ is a meromorphic function f on $X(\mathbb{C}_\infty)$ such that

$$\mathrm{div}(f) = V^{(1)} - V + (\Xi) - (\overline{\infty}^{(1)}),$$

and

$$\widetilde{\mathrm{sgn}}(f f^{(1)} \cdots f^{(d_\infty - 1)}) = 1.$$

From the definition, we can see that a datum $(\overline{\infty}, V, \mathrm{sgn})$ defines a shtuka function f up to a $\dfrac{q^{d_\infty} - 1}{q - 1}$-th root of unity.

Remark II.10. This definition / normalization of shtuka function is different from the original one of Thakur [Tha93]. This observation can be found in [ANDTR17, Remark 2.3]. With the initial normalization, we cannot obtain a Hayes module from Thakur's construction in [Tha93, 0.3.5]. See Remark II.15.

We first assert that if we pick a different datum, we will get a different shtuka function. By "different", we mean that they do not simply differ by a $\dfrac{q^{d_\infty} - 1}{q - 1}$-th root of unity. In fact, the divisors of the two shtuka functions obtained would need to be different.

Proposition II.11. *If $(V_1, \overline{\infty}_1)$ and $(V_2, \overline{\infty}_2)$ are two different Drinfeld divisors, then in* $\mathrm{Div}(\overline{X})$,

$$V_1^{(1)} - V_1 + (\Xi) - (\overline{\infty}_1^{(1)}) \neq V_2^{(1)} - V_2 + (\Xi) - (\overline{\infty}_2^{(1)}).$$

In particular, two different data $(V_1, \overline{\infty}_1, \mathrm{sgn}_1)$, $(V_2, \overline{\infty}_2, \mathrm{sgn}_2)$ *cannot share the same shtuka function.*

Proof. Suppose $(V_1, \overline{\infty}_1)$, $(V_2, \overline{\infty}_2)$ are two Drinfeld divisors with

$$V_1^{(1)} - V_1 + (\Xi) - (\overline{\infty}_1^{(1)}) = V_2^{(1)} - V_2 + (\Xi) - (\overline{\infty}_2^{(1)}).$$

Since V_1, V_2 are effective, the zeros of the divisor above are given by

$$V_1^{(1)} + (\Xi) = V_2^{(1)} + (\Xi).$$

Hence $V_1 = V_2$. Looking at the poles, we have that $\overline{\infty}_1 = \overline{\infty}_2$.

□

Now if $(V_1, \overline{\infty}_1, \mathrm{sgn}_1)$ and $(V_2, \overline{\infty}_2, \mathrm{sgn}_2)$ gives the same shtuka function f (up to a $\dfrac{q^{d_\infty}-1}{q-1}$-th root of unity), then $V_1 = V_2$ and $\overline{\infty}_1 = \overline{\infty}_2$. The shtuka function is then determined up to a scalar. Since different choices of a $\dfrac{q^{d_\infty}-1}{q-1}$-th roots of unity gives the same product $ff^{(1)}\cdots f^{(d_\infty-1)}$, this forces $\mathrm{sgn}_1 = \mathrm{sgn}_2$.

We can then obtain a count of shtuka function upon fixing X, ∞ and sgn. As we can see, this is exactly the same as the number of Hayes modules for $(X, \infty, \mathrm{sgn})$.

Proposition II.12. *Given* X, ∞ *and* sgn, *there are* $\#\operatorname{Pic}^0(\overline{X})(\mathbb{F}_q)\cdot d_\infty \cdot \dfrac{q^{d_\infty}-1}{q-1}$ *many shtuka functions.*

II.4.4: Shtuka function and Hayes module

Let f be a shtuka function associated to $(V, \overline{\infty}, \mathrm{sgn})$. We are going to construct a Hayes module from the shtuka function f. We first establish an $\mathbb{C}_\infty$-basis for $\Gamma(\overline{X} - \infty, \mathcal{O}_{\overline{X}}(V))$.

Proposition II.13. *The set*

$$1, f, ff^{(1)}, ff^{(1)}f^{(2)}, \ldots$$

gives an $\mathbb{C}_\infty$*-basis for the vector space* $\Gamma(\overline{X} - \infty, \mathcal{O}_{\overline{X}}(V))$.

Proof. We reuse the notation $\mathcal{L}_i := \mathcal{O}_{\overline{X}}(V_i)$ from the proof of Drinfeld vanishing lemma II.1. By the same lemma, $h^1(\overline{X}, \mathcal{O}_{\overline{X}}(V - \overline{\infty})) = 0$. Hence $h^1(\overline{X}, \mathcal{L}_n) \le h^1(\overline{X}, \mathcal{L}_0) = 0$ for all $n \ge 0$, and thus $h^0(\overline{X}, \mathcal{L}_n) = \chi(\overline{X}, \mathcal{L}_n) = n$ for all $n \ge 0$.

Points in $\overline{X}(\mathbb{C}_\infty)$ above ∞ are precisely $\{\overline{\infty}^{(j)}\}_{0\le j\le d_\infty-1}$. Hence every function in $\Gamma(\overline{X} - \infty, \mathcal{O}_{\overline{X}}(V))$ lies in $H^0(\overline{X}, \mathcal{L}_n)$ for some $n \gg 0$. By the proof of Drinfeld vanishing lemma,

we have that

$$\mathcal{L}_n = \mathcal{L}_{n-1} + f\mathcal{L}_{n-1}^{(1)} \qquad \text{for } n \geq 1,$$

and $\mathcal{L}_n/\mathcal{L}_{n-1}$ is of rank 1 with $fe^{(1)}$ being a basis for some $e \in \mathcal{L}_{n-1} - \mathcal{L}_{n-2}$. By induction,

$$1, f, ff^{(1)}, \ldots, ff^{(1)} \cdots f^{(n-1)}$$

is a $\mathbb{C}_\infty$-basis for $H^0(\overline{X}, \mathcal{L}_{n+1})$ for all $n \geq 0$. Take $n \to \infty$, we have

$$1, f, ff^{(1)}, ff^{(1)}f^{(2)}, \ldots$$

being a $\mathbb{C}_\infty$-basis for $\Gamma(\overline{X} - \infty, \mathcal{O}_{\overline{X}}(V))$.

□

For each $a \in \mathbb{A}$, we have $a \in \Gamma(X - \infty, \mathcal{O}_X) \subset \Gamma(\overline{X} - \infty, \mathcal{O}_{\overline{X}}(V))$. Define $\rho_{a,j} \in \mathbb{C}_\infty$ by

$$a = \sum_j \rho_{a,j} ff^{(1)} \cdots f^{(j-1)}.$$

By considering poles of a at each $\overline{\infty}^{(i)}$, we can see that the largest j such that $\rho_{a,j} \neq 0$ is $j = \deg a$. We define $\rho : \mathbb{A} \to \mathbb{C}_\infty\{\tau\}$ by

$$\rho_a := \sum_{j=0}^{\deg a} \rho_{a,j} \tau^j$$

is the Hayes module for sgn associated to $(V, \overline{\infty})$. To see that this is a Hayes module, it is clear that it is $\mathbb{F}_q$-linear, nontrivial (i.e. $\rho_a \neq a(\Xi)$ for some (hence all) non-constant a), has the correct degree as a polynomial of τ, and also has the correct top coefficient, see Remark II.15 below. To see that this is multiplicative, one needs to look at the action of $\mathbb{A}$ on the vector space $\Gamma(\overline{X} - \infty, \mathcal{O}_{\overline{X}}(V))$ more carefully.

With this, we can then state the shtuka correspondence for rank 1.

Proposition II.14 (Shtuka correspondence, rank 1 version)**.** *Fix $(X, \infty, \mathrm{sgn})$. The set of $(V, \overline{\infty})$ is in bijective correspondence to the set of isomorphism classes of Hayes modules. Moreover, the set of shtuka functions for $(X, \infty, \mathrm{sgn})$ (resp., $(\overline{\infty}, V, \mathrm{sgn})$) is in bijective correspondence to the set of Hayes module for the same respective datum, with the Hayes module for f as constructed above.*

Remark II.15. We need

$$\widetilde{\mathrm{sgn}}(ff^{(1)} \cdots f^{(d_\infty - 1)}) = 1$$

instead of

$$\widetilde{\operatorname{sgn}}(f) = 1$$

to ensure that we get the correct leading coefficient in $\rho_a(\tau)$. First of all, having $\widetilde{\operatorname{sgn}}(f) = 1$ does **not** guarantee $\widetilde{\operatorname{sgn}}(ff^{(1)} \cdots f^{(d_\infty - 1)}) = 1$. There is basically no way to calculate $\widetilde{\operatorname{sgn}}(f^{(1)})$ from $\widetilde{\operatorname{sgn}}(f)$. This is because the Frobenius twist does not interact well with an infinite series at $\overline{\infty}$, i.e. we cannot obtain a local expansion at $\overline{\infty}$ from Frobenius twisting an existing one. In fact, $\widetilde{\operatorname{sgn}}(f^{(1)})$ can be transcendental over $\mathbb{F}_q$ while $\widetilde{\operatorname{sgn}}(f) = 1$! See Example VII.1.4 for such an example.

However, we do have that

$$\widetilde{\operatorname{sgn}}(h^{(d_\infty)}) = (\widetilde{\operatorname{sgn}}(h))^{(d_\infty)}$$

for any function h on $\overline{X}$, since Frobenius twisting an expansion at $\overline{\infty}$ by d_∞ times does give an appropriate expansion at $\overline{\infty}$. In particular, if

$$\widetilde{\operatorname{sgn}}(ff^{(1)} \cdots f^{(d_\infty - 1)}) = 1,$$

then

$$\widetilde{\operatorname{sgn}}(ff^{(1)} \cdots f^{(md_\infty - 1)}) = 1$$

for all positive integers m.

To ensure that we obtain a Hayes module in the above construction, we need the top coefficient $\rho_{a,\deg a}$ to be $\operatorname{sgn} a$. We can see that this is satisfied by considering the poles at $\overline{\infty}^{(1)}$ and taking $\widetilde{\operatorname{sgn}}$ for the equation

$$a = \sum_{j=0}^{\deg a} \rho_{a,j} f f^{(1)} \cdots f^{(j-1)}.$$

Since $\deg a$ is divisible by d_∞, by the above discussion we have that

$$\widetilde{\operatorname{sgn}}(ff^{(1)} \cdots f^{(\deg a - 1)}) = 1.$$

So via taking $\widetilde{\operatorname{sgn}}$, we have $\operatorname{sgn} a = \rho_{a,\deg a}$.

II.4.5: Exponential and Logarithm of Hayes modules in terms of shtuka function

An application of shtuka function, found by Thakur and Anderson [Tha93], is that we are able to write the exponential and logarithm series associated to a Hayes module ρ in terms

of shtuka function.

Theorem II.16. *[Tha93, 0.3.6]*

$$e_\rho(z) = \sum_{n=0}^{\infty} \frac{1}{f \cdots f^{(n-1)}}\bigg|_{\Xi^{(n)}} z^{q^n}.$$

In particular, the coefficients in the series are finite.

Proof. From

$$\operatorname{div}(f) = V^{(1)} - V + (\Xi) - (\overline{\infty}^{(1)}),$$

we have

$$\operatorname{div}(f f^{(1)} \cdots f^{(n-1)}) = V^{(n)} - V + \sum_{i=0}^{n-1} (\Xi^{(i)}) - \sum_{i=0}^{n-1} (\overline{\infty}^{(i+1)}).$$

By Corollary II.2, Ξ is not in the support of V. Hence $\Xi^{(n)}$ is not in the support of $V^{(n)}$. This shows that $f f^{(1)} \cdots f^{(n-1)}$ does not vanish at $\Xi^{(n)}$, hence the coefficients of the series are defined.

To see that the series is indeed the exponential series for ρ, we need to check that it satisfies the two defining properties of exponential function:

- coefficient of z is 1;
- functional equation: $e_\rho(a|_\Xi \cdot z) = \rho_a(e_\rho(z))$; note that $a|_\Xi$ is the same as $\iota(a)$ by definition of Ξ.

The first condition is clear as we have an empty product on the right when $n = 0$. The proof of the second condition uses the equality

$$a = \sum_{j=0}^{\deg a} \rho_{a,j} f f^{(1)} \cdots f^{(j-1)}.$$

By dividing this by $f f^{(1)} \cdots f^{(n-1)}$ and evaluating at $\Xi^{(n)}$, we have

$$\frac{a}{f f^{(1)} \cdots f^{(n-1)}}\bigg|_{\Xi^{(n)}} = \sum_{j=0}^{\min(\deg a, n)} \rho_{a,j} \frac{1}{f^{(j)} \cdots f^{(n-1)}}\bigg|_{\Xi^{(n)}}.$$

Hence

$$\begin{aligned}
e_\rho(a|_\Xi z) &= \sum_{n=0}^{\infty} \frac{1}{f \cdots f^{(n-1)}}\bigg|_{\Xi^{(n)}} (a|_\Xi z)^{q^n} \\
&= \sum_{n=0}^{\infty} \frac{a}{f \cdots f^{(n-1)}}\bigg|_{\Xi^{(n)}} z^{q^n} \\
&= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{\min(\deg a, n)} \rho_{a,j} \frac{1}{f^{(j)} \cdots f^{(n-1)}}\bigg|_{\Xi^{(n)}} \right) z^{q^n} \\
&= \sum_{n=0}^{\infty} \sum_{j=0}^{\min(\deg a, n)} \rho_{a,j} \left(\frac{1}{f \cdots f^{(n-j-1)}}\bigg|_{\Xi^{(n-j)}} z^{q^{n-j}} \right)^{q^j} \\
&= \sum_{j=0}^{\deg a} \rho_{a,j} \left(\sum_{m=0}^{\infty} \frac{1}{f \cdots f^{(m-1)}}\bigg|_{\Xi^{(m)}} z^{q^m} \right)^{q^j} \\
&= \rho_a(e_\rho(z)).
\end{aligned}$$

□

As for the logarithm series, Anderson described the coefficients in terms of the residue of a differential form. We will first get our hand on such a differential form.

Proposition II.17.

$$h^0(\overline{X}, \Omega^1_{\overline{X}}(-V + (\overline{\infty}) + (\overline{\infty}^{(-1)}))) = 1$$

Proof. We will first show that the first cohomology of $\Omega^1_{\overline{X}}(-V + (\overline{\infty}) + (\overline{\infty}^{(-1)}))$ vanishes. Since $\overline{X}$ is a curve, the canonical bundle $\omega_{\overline{X}}$ is by definition the sheaf of differential $\Omega^1_{\overline{X}}$. By Serre duality,

$$H^1(\overline{X}, \omega_{\overline{X}}(-V + (\overline{\infty}) + (\overline{\infty}^{(-1)}))) \simeq H^0(\overline{X}, \mathcal{O}_{\overline{X}}(V - (\overline{\infty}) - (\overline{\infty}^{(-1)}))).$$

The latter embeds into $H^0(\overline{X}, \mathcal{O}_{\overline{X}}(V - (\overline{\infty})))$, which is 0 by Drinfeld vanishing lemma II.1.

We can then compute the h^0 by Riemann-Roch. We have that $\deg \omega_{\overline{X}}(-V + (\overline{\infty}) + (\overline{\infty}^{(-1)}) = 2g - 2 - g + 2 = g$. Therefore,

$$h^0(\overline{X}, \omega_{\overline{X}}(-V + (\overline{\infty}) + (\overline{\infty}^{(-1)}))) = \chi(\overline{X}, \omega_{\overline{X}}(-V + (\overline{\infty}) + (\overline{\infty}^{(-1)}))) = g + 1 - g = 1.$$

□

Lemma II.18. *Let $\omega' \in H^0(\overline{X}, \Omega^1_{\overline{X}}(-V + (\overline{\infty}) + (\overline{\infty}^{(-1)})))$ be nonzero. Then $\dfrac{\omega'^{(1)}}{f}$ has a simple pole at Ξ and $\overline{\infty}$, with no other pole.*

Proof. By definition of ω' and f, we have that

$$\frac{\omega'^{(1)}}{f} \in H^0(\overline{X}, \Omega^1_{\overline{X}}(-V + (\Xi) + (\overline{\infty}))),$$

so $\omega'^{(1)}/f$ has at worst simple poles at Ξ and $\overline{\infty}$. We will first show that ω'/f has a simple pole at $\overline{\infty}$.

Let $k = \operatorname{ord}_{\overline{\infty}^{(-1)}} V$. Since $\omega' \in H^0(\overline{X}, \Omega^1_{\overline{X}}(-V + (\overline{\infty}) + (\overline{\infty}^{(-1)})))$, we know that $\operatorname{ord}_{\overline{\infty}^{(-1)}} \omega' \geq k-1$ when $d_\infty > 1$. By Serre duality, $H^0(\overline{X}, \Omega^1_{\overline{X}}(-V+(\overline{\infty}))) \simeq H^1(\overline{X}, \mathcal{O}^1_{\overline{X}}(V - (\overline{\infty})))$, which is 0 by Drinfeld vanishing lemma II.1. This shows that

$$\operatorname{ord}_{\overline{\infty}^{(-1)}} \omega' = \operatorname{ord}_{\overline{\infty}^{(-1)}} \left(V - (\overline{\infty}) - (\overline{\infty}^{(-1)})\right)$$

Hence,

$$\operatorname{ord}_{\overline{\infty}^{(-1)}} \omega' = \begin{cases} k-1 & \text{if } d_\infty > 1 \\ -2 & \text{if } d_\infty = 1. \end{cases}$$

To see the calculation for $d_\infty = 1$, notice that $\overline{\infty} = \overline{\infty}^{(-1)}$, and recall that $\overline{\infty}$ is not in the support of V by corollary II.2.

Now we look at $\operatorname{ord}_{\overline{\infty}} f$. Once again, $\overline{\infty}$ is not in the support of V. By studying the equation

$$\operatorname{div}(f) = V^{(1)} - V + (\Xi) - (\overline{\infty}^{(1)}),$$

we have

$$\operatorname{ord}_{\overline{\infty}} f = \begin{cases} \operatorname{ord}_{\overline{\infty}} V^{(1)} = k & \text{if } d_\infty > 1; \\ -1 & \text{if } d_\infty = 1. \end{cases}$$

For $d_\infty = 1$, the pole comes from $\overline{\infty}^{(1)} = \overline{\infty}$. Combining these, we obtain that

$$\operatorname{ord}_{\overline{\infty}} \frac{\omega'^{(1)}}{f} = -1.$$

Since a differential cannot have only a simple pole and be holomorphic elsewhere, $\omega'^{(1)}/f$ must also have a simple pole at Ξ. □

Definition II.19. Define $\omega = \omega(V)$ to be the element in $H^0(\overline{X}, \Omega^1_{\overline{X}}(-V + (\overline{\infty}) + (\overline{\infty}^{(-1)})))$ such that

$$\operatorname{Res}_\Xi \frac{\omega^{(1)}}{f} = 1.$$

By Residue theorem, we have the following equivalent definition: $\omega = \omega(V)$ is the unique

element in $H^0(\overline{X}, \Omega^1_{\overline{X}}(-V + (\overline{\infty}) + (\overline{\infty}^{(-1)})))$ such that

$$\mathrm{Res}_{\overline{\infty}} \frac{\omega^{(1)}}{f} = -1.$$

With ω, we can now derive a concrete series expansion of $\log_\rho(z)$ in terms of some residues.

Theorem II.20. *[Tha93, 0.3.8] (see also [Tha20]) We have that*

$$\log_\rho(z) = \sum_{n=0}^{\infty} \mathrm{Res}_\Xi \frac{\omega^{(n+1)}}{f f^{(1)} \cdots f^{(n)}} z^{q^n}.$$

Proof. We will show that $e_\rho(\text{above series}) = z$. Expand the left side with the series expansion of e_ρ in Theorem II.16.

$$\begin{aligned}
& e_\rho \left(\sum_{n \geq 0} \left(\mathrm{Res}_\Xi \frac{\omega^{(n+1)}}{f \cdots f^{(n)}} z^{q^n} \right) \right) \\
&= \sum_{m \geq 0} \left(\frac{1}{f f^{(1)} \cdots f^{(m-1)}} \bigg|_{\Xi^{(m)}} \right) \sum_{n \geq 0} \left(\mathrm{Res}_\Xi \frac{\omega^{(n+1)}}{f \cdots f^{(n)}} z^{q^n} \right)^{q^m} \\
&= \sum_{m \geq 0} \sum_{n \geq 0} \left(\frac{1}{f f^{(1)} \cdots f^{(m-1)}} \bigg|_{\Xi^{(m)}} \right) \left(\mathrm{Res}_{\Xi^{(m)}} \frac{\omega^{(m+n+1)}}{f^{(m)} \cdots f^{(m+n)}} \right) z^{q^{m+n}} \\
&= \sum_{m \geq 0} \sum_{n \geq 0} \left(\mathrm{Res}_{\Xi^{(m)}} \frac{\omega^{(m+n+1)}}{f f^{(1)} \cdots f^{(m-1)} f^{(m)} \cdots f^{(m+n)}} \right) z^{q^{m+n}} \\
&= \sum_{k=0}^{\infty} \left(\sum_{m=0}^{k} \left(\mathrm{Res}_{\Xi^{(m)}} \frac{\omega^{(k+1)}}{f \cdots f^{(k)}} \right) \right) z^{q^k}
\end{aligned}$$

By definition of ω, we have that

$$\mathrm{div} \frac{\omega^{(k+1)}}{f f^{(1)} \cdots f^{(k)}} \geq -(\overline{\infty}^{(k+1)}) - (\overline{\infty}^{(k)}) + V + \sum_{n=0}^{k} \left((\overline{\infty}^{(n+1)}) - (\Xi^{(n)}) \right).$$

In particular, for $k \geq 1$, the differential $\dfrac{\omega^{(k+1)}}{f f^{(1)} \cdots f^{(k)}}$ only has poles at $\Xi, \ldots, \Xi^{(k)}$. Therefore, the above coefficients of z^{q^k} are 0 for $k \geq 1$. At $k = 0$, the coefficient is 1 by definition of ω, completing the proof.

□

Remark II.21. The definition of ω stated in [Tha93, 0.3.7] and [Gos98, §7.11] specifies that

ω has a double pole at $\overline{\infty}$. When $d_\infty > 1$, the author finds that differential

$$\frac{\omega^{(k+1)}}{f f^{(1)} \cdots f^{(k)}}$$

has a simple pole at $\overline{\infty}^{(k+1)}$ for $1 \leq k < d_\infty$, which is undesired. To fix this, Thakur has found that we should have the poles of ω at $\overline{\infty}$ and $\overline{\infty}^{(-1)}$ instead. See [Tha20, (14)].

CHAPTER III
Ramifying Hyperelliptic Curves

For elliptic curves, Thakur [Tha92, Theorem V] gave an integral expression for the shtuka function f, and Green and Papanikolas [GP18, Corollary 3.5] gave a simplified expression for logarithm series. We will show that such expressions also exist for a certain class of curves, *ramifying hyperelliptic curves*. We will first define such curves, and then write down the shtuka function f and the differential ω for these curves explicitly. This will allow us to express the logarithm series for such curves in a similar fashion as the elliptic curves.

III.1: Definition for Ramifying Hyperelliptic Cruves

Definition III.1. A *ramifying hyperelliptic curve* over $\mathbb{F}_q$ is a hyperelliptic curve X of genus g over $\mathbb{F}_q$, together with a rational point $\infty \in X(\mathbb{F}_q)$, such that the affine open $\mathbb{A} := \Gamma(X - \infty, \mathcal{O}_X)$ has a model

$$\mathbb{A} = \mathbb{F}_q[t, y]/(y^2 + F_2(t)y - F_1(t)),$$

with $F_1, F_2 \in \mathbb{F}_q[t]$, F_1 monic of degree $2g + 1$, F_2 of degree at most g.

Since X is a hyperelliptic curve, the genus g is at least 2. Note that if we allow $g = 1$, then the above model is the usual Weierstrass model of an elliptic curve.

The word "ramifying" signifies that the place ∞ ramifies in the extension $\mathbb{K}/\mathbb{F}_q(t)$, where $\mathbb{K}$ is, as in the previous chapter, the function field of X. We denote by $F(t, y)$ the polynomial $y^2 + F_2(t)y - F_1(t)$.

We set $A := \mathbb{F}_q[\theta, \eta]/F(\theta, \eta)$, and the isomorphism $\iota : \mathbb{A} \to A$ by $\iota(t) = \theta$, $\iota(y) = \eta$.

Example III.2. Let $\mathbb{A} = \mathbb{F}_2[t, y]/(y^2 + y - (t^5 + t^3 + 1))$. Then $\mathbb{A}$ is the affine open of a ramifying hyperelliptic curve of genus 2.

III.2: Degree and Sign on Ramifying Hyperelliptic Curves

Since we have a good model of $\mathbb{A}$, we can describe the degree and sign functions from the last chapter more explicitly. The degree function is defined by $\deg a = -d_\infty v_\infty(a)$. Since ∞ is a rational point, $d_\infty = 1$. From the equation $y^2 + F_2(t)y - F_1(t)$, we can calculate that $\deg t = 2$, $\deg y = g$, and that t^g/y is a uniformizer at ∞.

As for a sign function, we want to extend from the notion of "leading coefficient". Because of the equation $y^2 + F_2(t)y - F_1(t)$, the set $\{t^i, yt^i\}_{i\geq 0}$ is an $\mathbb{F}_q$-basis for $\mathbb{A}$. Using the above explicit description of degree, we can see that every term in this basis has a unique degree. As a result, we can call the "leading coefficient" of any nonzero $a \in \mathbb{A}$ to be the coefficient of the highest degree term with respect to this basis. We fix a sign function

$$\operatorname{sgn} : \mathbb{K}_\infty \to \mathbb{F}_q$$

by defining $\operatorname{sgn} a$ to be the leading coefficient of a in the above sense if $a \neq 0$, and $\operatorname{sgn} 0 = 0$, and extend to $\mathbb{K}_\infty$. In particular, we have that $\operatorname{sgn} t = \operatorname{sgn} y = 1$.

Since $d_\infty = 1$, other sign functions are obtained by fixing $\operatorname{sgn}(t^g/y)$ as another element in $\mathbb{F}_q^\times$, or more explicitly $\operatorname{sgn} t = c^2$, $\operatorname{sgn} y = c^g$ for some $c \in \mathbb{F}_q^\times$. For the rest of this thesis, we will stick with our "leading coefficient" sign function for simplicity, but everything in the thesis works for any other sign function.

The ring $\mathbb{C}_\infty \otimes_{\mathbb{F}_q} \mathbb{A}$ also has $\{t^i, yt^i\}_{i\geq 0}$ as a $\mathbb{C}_\infty$-vector space. We can extend sgn to

$$\widetilde{\operatorname{sgn}} : \mathbb{C}_\infty \otimes_{\mathbb{F}_q} \mathbb{A} \to \mathbb{C}_\infty$$

also by taking the leading coefficient with respect to the basis.

III.3: Shtuka function for Ramifying Hyperelliptic Curves

The expression of shtuka function f for elliptic curves given by [Tha92, Theorem V] is very integral, in the sense that it has a "monic" numerator and denominator, and that all zeros of the numerator and denominator are integral. We will make this precise and generalize this to ramifying hyperelliptic curves.

Proposition III.1. *There exist polynomials $\delta, Q \in \mathcal{O}_H[t]$ in t such that:*

1. *δ is monic of degree g, and Q is of degree at most g;*
2. *setting*

$$\nu = y - \eta - Q(t),$$

the shtuka function f has a presentation

$$f = \frac{\nu}{\delta};$$

3. $\widetilde{\mathrm{sgn}}(\nu) = \widetilde{\mathrm{sgn}}(\delta) = 1$;

4. *in the affine model $\overline{X} - \overline{\infty}$ with coordinate ring $\mathbb{C}_\infty \otimes_{\mathbb{F}_q} \mathbb{A}$, the coordinates of the zeros of ν and δ are integral over $\mathcal{O}_H$.*

The proof is by long division, as in the proof of [Tha92, Theorem V].

Proof. The shtuka correspondence of Hayes modules from chapter II tells us that

$$\begin{aligned} t &= \theta + \rho_{t,1} f + f f^{(1)}, \\ y &= \eta + \rho_{y,1} f + \rho_{y,2} f f^{(1)} + \cdots + f f^{(1)} \cdots f^{(2g)}. \end{aligned}$$

Rearranging, we get

$$(\theta - t) + \rho_{t,1} f + f f^{(1)} = 0, \tag{1}$$

$$(\eta - y) + \rho_{y,1} f + \rho_{y,2} f f^{(1)} + \cdots + f f^{(1)} \cdots f^{(2g)} = 0. \tag{2}$$

The long division starts as follows:

(1) apply Frobenius twist to the equation (1) by $2g-1$ times,

(2) multiply by $-f f^{(1)} \cdots f^{(2g-2)}$,

(3) add equation (2).

That is, we have (2) $- f f^{(1)} \cdots f^{(2g-2)} \cdot ((1)^{(2g-1)})$:

$$\begin{aligned} (\eta - y) + \cdots + \rho_{y,2g-2} f f^{(1)} \cdots f^{(2g-3)} \\ + (\rho_{y,2g-1} - (\theta^{(2g-1)} - t)) f f^{(1)} \cdots f^{(2g-2)} + (\rho_{y,2g} - \rho_{t,1}^{(2g-1)}) f f^{(1)} \cdots f^{(2g-1)} = 0. \end{aligned} \tag{3}$$

Continue with process of long division to get equation (4) out of equations (1), (3), to get equation (5) out of equations (1), (4), etc.

Claim: For $3 \leq n \leq 2g+1$, after $n-2$ steps in the long division, equation (n) is of the form

$$\begin{aligned} (\eta - y) + \cdots + \rho_{y,2g-n+1} f f^{(1)} \cdots f^{(2g-n)} \\ + P_n(t) f f^{(1)} \cdots f^{(2g-n+1)} + Q_n(t) f f^{(1)} \cdots f^{(2g-n+2)} = 0, \end{aligned} \tag{n}$$

where $P_n(t), Q_n(t)$ are polynomials in $\mathcal{O}_H[t]$ of degree (in t).

Moreover, when n is odd we have that P_n is monic with $\deg_t P_n(t) = \dfrac{n-1}{2}$, and $\deg_t Q_n(t) < \deg_t P_n(t)$. When n is even we have that Q_n is monic with $\deg_t Q_n(t) = \dfrac{n-2}{2}$, and $\deg_t P_n(t) \leq \deg_t Q_n(t)$.

Proof of Claim: This claim can be seen by induction. For the base case $n = 3$, we have that $P_3(t) = \rho_{y,2g-1} - (\theta^{(2g-1)} - t)$, and $Q_3(t) = \rho_{y,2g} - \rho_{t,1}^{(2g-1)}$. In particular, P_3 is monic of degree 1, and Q_3 is of degree 0 (or $-\infty$ if $Q_3 = 0$).

For the inductive step, we obtain equation (n) via dividing equation $(n-1)$ by equation (1), and have that

$$P_n(t) = \rho_{y,2g-n+2} - (\theta^{(2g-n+2)} - t)Q_{n-1}(t), \qquad Q_n(t) = P_{n-1}(t) - \rho_{t,1}^{(2g-n+2)}Q_{n-1}(t).$$

If n is odd, then $Q_{n-1}(t)$ is monic and $\deg_t Q_{n-1}(t) = \dfrac{(n-1)-2}{2} = \dfrac{n-1}{2} - 1$. Hence $P_n(t)$ is monic of degree $\dfrac{n-1}{2}$. At the same time,

$$\deg_t Q_n(t) \leq \max\{\deg_t P_{n-1}(t), \deg_t Q_{n-1}(t)\} = \deg_t Q_{n-1}(t) = \frac{n-1}{2} - 1 < \deg_t P_n(t).$$

If n is even, then $P_{n-1}(t)$ is monic of degree $\dfrac{(n-1)-1}{2} = \dfrac{n-2}{2}$, and $\deg_t Q_{n-1}(t) < \deg_t P_{n-1}(t)$. Thus $Q_n(t)$ is monic and $\deg_t Q_n(t) = \deg_t P_{n-1}(t) = \dfrac{n-2}{2}$, and

$$\deg_t P_n(t) = \deg_t Q_{n-1}(t) + 1 \leq \deg_t P_{n-1}(t) = \deg_t Q_n(t).$$

This completes the proof of the claim. Back to the proof of the Proposition. Take equation $(2g+1)$ and divide it by equation (1) to obtain

$$(\eta - y - (\theta - t)Q_{2g+1}(t)) + (P_{2g+1}(t) - \rho_{t,1}Q_{2g+1}(t))f = 0.$$

Define

$$\delta := P_{2g+1}(t) - \rho_{t,1}Q_{2g+1}(t), \quad Q := (t-\theta)Q_{2g+1}(t).$$

From the claim, $\deg_t P_{2g+1}(t) = g$, $\deg_t Q_{2g+1}(t) \leq g-1$, and P_{2g+1} is monic. Thus,

1. δ and Q are in $\mathcal{O}_H[t]$;
2. $\deg_t \delta = g$, and $\deg_t Q \leq g$;

3. δ is monic;

4. by setting $\nu := y - \eta - Q(t)$, we have $f = \dfrac{\nu}{\delta}$;

5. $\widetilde{\mathrm{sgn}}(\delta) = 1$ comes directly from δ being a monic polynomial in t;

6. since the degrees of y and $Q(t)$ in $\mathbb{A}$ are $2g+1$ and at most $2g$ respectively, $\widetilde{\mathrm{sgn}}(\nu) = 1$.

What remains to be checked is the integrality of the zeros in the affine model. Since

$$\mathrm{div}(f) = V^{(1)} - V + (\Xi) - (\overline{\infty}),$$

we must have $\mathrm{div}(\delta) \geq V$. Set $V' = \mathrm{div}\delta - V + 2g(\overline{\infty})$, that is,

$$\mathrm{div}(\delta) = V + V' - 2g(\overline{\infty}).$$

Since δ is a monic polynomial in t with degree g in t, V' is the effective divisor of degree g. Then

$$\mathrm{div}(\nu) = V^{(1)} + V' + (\Xi) - (2g+1)(\overline{\infty}).$$

Thus the zeros of δ and ν are given by $V^{(1)}$, V, V', and Ξ. By definition Ξ has coordinates (θ, η), both are in $\mathcal{O}_H$. The coordinates for $V^{(1)}$ are q-th power of the coordinates for V. It remains to show that all points in the support of V and V' have coordinates integral over $\mathcal{O}_H$.

The t-coordinates of all points in the support of V and V' are precisely the the roots of the polynomial δ, when viewed as a polynomial in t. Since δ is monic and has coefficients in $\mathcal{O}_H$, the t-coordinates are integral.

Plug in the t-coordinates for V and V', all of which integral over $\mathcal{O}_H$, into $F(t, y) = y^2 + F_2(t)y - F_1(t)$. We can see each of the y-coordinates for V and V' as a root of a monic quadratic polynomial over some integral extension of $\mathcal{O}_H$. Therefore the y-coordinates for V and V' are also integral.

□

III.4: Log series for Ramifying Hyperelliptic Curves

With this presentation of the shtuka function, we can write down the differential $\omega \in H^0(\overline{X}, \Omega^1_{\overline{X}}(-V + 2(\overline{\infty})))$ from the previous chapter explicitly. This expression of the differential and the expression of the logarithm series derived from it (proposition III.2) below is generalizes a result of Green and Papanikolas [GP18, Corollary 3.5] to our setting.

Proposition III.1. *Set*

$$\omega := \frac{\delta}{2y + F_2(t)} dt.$$

Then $\omega \in H^0(\overline{X}, \Omega^1_{\overline{X}}(-V + 2(\overline{\infty})))$, *and*

$$\mathrm{Res}_{\overline{\infty}} \frac{\omega^{(1)}}{f} = -1.$$

Proof. We first analyze the divisor of the differential $\dfrac{dt}{2y + F_2(t)}$. The function t is holomorphic everywhere except at $\overline{\infty}$. Thus dt cannot have pole except at $\overline{\infty}$. Recall that $v_\infty(t) = -2$ and $v_\infty(y) = -(2g+1)$, so we can pick $u := \dfrac{t^g}{y}$ to be a uniformizer at $\overline{\infty}$. First, we differentiate $F(t, y) = 0$ and see that

$$(2y + F_2(t))dy = (F_1'(t) - F_2'(t)y)dt.$$

Next, we analyze du:

$$\begin{aligned}
du &= \frac{gt^{g-1}}{y} dt - \frac{t^g}{y^2} dy \\
&= \frac{gt^{g-1}}{y} dt - \frac{t^g}{y^2} \frac{F_1'(t) - F_2'(t)y}{2y + F_2(t)} dt \\
&= \frac{t^{g-1}}{y^2(2y + F_2(t))} \left(g(2y^2 + F_2(t)y) - t(F_1'(t) - F_2'(t)y) \right) dt \\
&= \frac{t^{g-1}}{y^2(2y + F_2(t))} \left(g(2F_1(t) - F_2(t)y) - t(F_1'(t) - F_2'(t)y) \right) dt \\
&= \frac{t^{g-1}}{y^2(2y + F_2(t))} \left((2gF_1(t) - tF_1'(t)) + (-gF_2(t)y + F_2'(t)ty) \right) dt.
\end{aligned}$$

Since $F_1(t)$ is monic of degree $2g+1$ in t, the polynomial $2gF_1(t) - tF_1'(t)$ is also of degree $2g+1$ in t, with leading coefficient -1. The term $-gF_2(t)y + F_2'(t)ty$ has fewer poles at $\overline{\infty}$ than t^{2g+1} does. This shows that

$$\frac{dt}{2y + F_2(t)} = (-u^{2g-2} + O(u^{2g-1}))du.$$

Since X is smooth, dt and dy cannot share any zero. By revisiting the equation

$$(2y + F_2(t))dy = (F_1'(t) - F_2'(t)y)dt,$$

all zeros of dt must also be zeros of $2y + F_2(t)$ (counting multiplicities). That is, the differential

$\dfrac{dt}{2y+F_2(t)}$ has no zeros except potentially at the poles of $2y+F_2(t)$, i.e. at $\overline{\infty}$. Since all differentials on X have degree $2g-2$ and $\dfrac{dt}{2y+F_2(t)}$ has degree $2g-2$ at $\overline{\infty}$, the differential $\dfrac{dt}{2y+F_2(t)}$ has no zero nor pole away from $\overline{\infty}$. Therefore,

$$\omega = \frac{\delta}{2y+F_2(t)}dt$$

has zeros at V, V', a double pole at $\overline{\infty}$, and no other zeros or poles. In particular, $\omega \in H^0(\overline{X}, \Omega^1_{\overline{X}}(-V+2(\overline{\infty})))$.

To prove the second statement about the residue, let us expand the differential

$$\frac{\omega^{(1)}}{f} = \frac{1}{f}\frac{\delta^{(1)}}{2y+F_2(t)}dt$$

with respect to the uniformizer $u = \dfrac{t^g}{y}$. By definition of f we have $\widetilde{\operatorname{sgn}}(f) = 1$. Since $\operatorname{sgn} t = \operatorname{sgn} y = 1$, we have $\widetilde{\operatorname{sgn}}(u) = 1$. This shows that

$$f = u^{-1} + O(1).$$

Since $\delta^{(1)}$ is a monic polynomial of degree g in t, we have that

$$\delta^{(1)} = u^{-2g} + O(u^{-2g+1}).$$

Therefore,

$$\frac{\omega^{(1)}}{f} = -u^{-1} + O(1),$$

showing that

$$\operatorname{Res}_{\overline{\infty}}\frac{\omega^{(1)}}{f} = -1.$$

□

With the explicit description of ω, we can then write down formulae for the residues

appearing in Theorem II.20. Note that $t-\theta$ is a uniformizer at Ξ, with $d(t-\theta)=dt$. Thus,

$$\begin{aligned}\mathrm{Res}_\Xi \frac{\omega^{(n+1)}}{f f^{(1)}\cdots f^{(n)}} &= \mathrm{Res}_\Xi \frac{\delta^{(n+1)}}{f f^{(1)}\cdots f^{(n)}}\frac{dt}{2y+F_2(t)}\\ &= \left.\frac{\delta^{(n+1)}}{\delta^{(1)} f^{(1)}\cdots f^{(n)}}\right|_\Xi \mathrm{Res}_\Xi \frac{\delta^{(1)}dt}{(2y+F_2(t))f}\\ &= \left.\frac{\delta^{(n+1)}}{\delta^{(1)} f^{(1)}\cdots f^{(n)}}\right|_\Xi \mathrm{Res}_\Xi \frac{\omega^{(1)}}{f}\\ &= \left.\frac{\delta^{(n+1)}}{\delta^{(1)} f^{(1)}\cdots f^{(n)}}\right|_\Xi .\end{aligned}$$

Proposition III.2. *(cf. [GP18, Cor 3.5])*

$$\log_\rho(z) = \sum_{n=0}^{\infty} \left.\frac{\delta^{(n+1)}}{\delta^{(1)} f^{(1)}\cdots f^{(n)}}\right|_\Xi z^{q^n}.$$

CHAPTER IV
Ideal Factorization of Integral Functions by Divisors

In this chapter, we will state and prove a proposition that factorizes a "nice enough" function G according to divisors. We will do this more generally, so one can hope to apply this proposition in other circumstances.

Let $X/\mathbb{F}_q$ be a smooth projective geometrically connected curve over $\mathbb{F}_q$, ∞ a closed point (not necessarily rational), $\mathbb{A} := \Gamma(X - \infty, \mathcal{O}_X)$, and $\mathbb{K}$, A, $\mathbb{F}_\infty$, etc. as before. Let R be a finitely-generated integral domain over $\mathbb{F}_q$, $F = \mathrm{Frac}(R)$ and $L = \overline{F}$. All tensor products will be over $\mathbb{F}_q$ unless otherwise specified.

Since $\mathbb{F}_q$ is perfect, X is geometrically normal. Thus $F \otimes \mathbb{A}$ is a domain, integrally closed in its field of fractions. In particular, $R \otimes \mathbb{A}$ is an integral domain. It is easy to check that

$$\mathrm{Frac}(R \otimes \mathbb{A}) = \mathrm{Frac}(F \otimes \mathbb{A}),$$

with the "=" sign indicating a canonical isomorphism. Note that the latter field is the function field of $X_F := X \times_{\mathbb{F}_q} \mathrm{Spec}\, F$.

Our goal is to analyze $R \otimes \mathbb{A}$-ideals, using the information we can obtain when we view elements in $R \otimes \mathbb{A}$ as functions on X_F or $X_L := X \times_{\mathbb{F}_q} \mathrm{Spec}\, L$.

IV.1: Functions in the subring $R \otimes \mathbb{A}$

Suppose we have an element $G \in R \otimes \mathbb{A}$. We can view G as a meromorphic function on the curve X_F or X_L. In the latter case, since L is algebraically closed, we can write

$$\mathrm{div}(G) = \sum_i Z_i - \sum_j P_j,$$

where $Z_i, P_j \in X(L)$ are the zeros and poles of G respectively. Since $G \in F \otimes \mathbb{A} = \Gamma(X_F - \infty, \mathcal{O}_X)$, it is regular away from ∞. That is, all poles of G must lie above ∞.

We now fix a model for $\mathbb{A}$. Suppose

$$\mathbb{A} = \mathbb{F}_q[t_1, t_2, \cdots, t_n]/(F_1, F_2, \cdots, F_m).$$

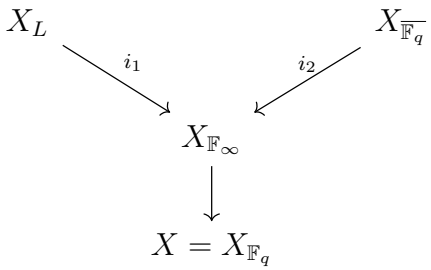
With the model, we can talk about the zeros of G in terms of coordinates. Say Z_i is given by $t_1 = a_{i,1}, t_2 = a_{i,2}, \ldots, t_n = a_{i,n}$, where $a_{i,k} \in L$.

Definition IV.1. Suppose $G \in R \otimes \mathbb{A}$. If there exists a model for $\mathbb{A}$ such that for all i, k, we have $a_{i,k} \in R$ with $a_{i,k}$ the coordinates of the zeros of G, then we say that **all zeros of G are in R.**

If all zeros of G are in R, we can reduce the zeros modulo primes from R. This is what we will use for the proof of the proposition of the next subsection. As a remark, if all zeros of G are in R for one model of $\mathbb{A}$, then it is true for all models of $\mathbb{A}$. This is because the coordinates in a model are $\mathbb{F}_q$-polynomials in terms of the coordinates in a second model, given by the $\mathbb{F}_q$-algebra isomorphism between the models.

IV.2: Infinities and sgn

Consider the points lying above $\infty \in X_{\mathbb{F}_q}$ in the tower:



The point ∞, as a closed point in X, can only split or be inert in this tower, and it splits completely as long as the field of constants contains $\mathbb{F}_\infty$. Hence, the fibers of ∞ in X_L and in $X_{\overline{\mathbb{F}_q}}$ are in natural bijection (upon fixing embeddings $\mathbb{F}_\infty \to L$ and $\mathbb{F}_\infty \to \overline{\mathbb{F}_q}$), given by

$$\begin{aligned} \{\infty\} \times_X X_L &\xrightarrow{=} \{\infty\} \times_X X_{\overline{\mathbb{F}_q}} \\ \overline{\infty} &\mapsto i_2^*(i_{1,*}(\overline{\infty})). \end{aligned}$$

By abuse of notation, we use "$\overline{\infty}$" to denote both a point in X_L above ∞, and the corresponding point in $X_{\overline{\mathbb{F}_q}}$.

For a sign function sgn on $\mathbb{K}_\infty$, as in §II.4.2 it can be extended to a function

$$\widetilde{\mathrm{sgn}}_{\overline{\infty}} : \mathrm{Frac}(L \otimes \mathbb{A}) \to L.$$

This extension depends on a choice of $\overline{\infty} \in X(L)$ above ∞, and is unique upon such a choice. In the same manner, we can also extend sgn to a function

$$\widetilde{\mathrm{sgn}}_{\overline{\infty}} : \mathrm{Frac}(\overline{\mathbb{F}_q} \otimes \mathbb{A}) \to \overline{\mathbb{F}_q}.$$

By abuse of notation, we denote by $\widetilde{\mathrm{sgn}}_{\overline{\infty}}$ both extensions with respect to $\overline{\infty}$.

IV.3: Relating the ideal by zeros of the function

We are now ready to state our proposition that factorizes "sufficiently integral" functions in terms of their divisor. Let $R[\mathbb{F}_\infty]$ to be the smallest subring of L containing R and $\mathbb{F}_\infty$.

Proposition IV.1. *Suppose we have $G \in R \otimes \mathbb{A}$ such that $\widetilde{\mathrm{sgn}}_{\overline{\infty}}(G) \in (R[\mathbb{F}_\infty])^\times$ for all choices of $\overline{\infty}$, and that all its zeros are in R. Fix a model for $\mathbb{A}$ and let $\{(a_{i,k})_k\}_i$ be the zeros of G. Then we have an equality of $R \otimes \mathbb{A}$-ideals*

$$(G) = \prod_i (t_1 - a_{i,1}, \cdots, t_n - a_{i,n}).$$

This is proved by reducing mod $\mathfrak{m}$ for maximal ideals $\mathfrak{m}$ in R. Let $\widetilde{G} := G \mod \mathfrak{m}$. We first prove a lemma that computes the degree of $\widetilde{G}$.

Lemma IV.2. *Fix $\mathfrak{m} \subset R$ a maximal ideal. Since R is finitely generated over $\mathbb{F}_q$, $R/\mathfrak{m}$ is a finite extension of $\mathbb{F}_q$ and can be considered as a subfield of $\overline{\mathbb{F}_q}$. Fix a closed point $\overline{\infty}$ in X_L above ∞, and we also denote by $\overline{\infty}$ the corresponding point on $X_{\overline{\mathbb{F}_q}}$. Then*

$$\mathrm{ord}_{\overline{\infty}}(G) \text{ in } X_L = \mathrm{ord}_{\overline{\infty}}(\widetilde{G}) \text{ in } X_{\overline{\mathbb{F}_q}}.$$

Proof. Fix a uniformizer π in $\mathbb{K}_\infty$ of ∞. Then

$$G = f_{-m}\pi^{-m} + O(\pi^{-m+1}),$$

where $f_{-m} \in F$. By assumption in Proposition IV.1, $\widetilde{\mathrm{sgn}}_{\overline{\infty}}(G) = f_{-m}(\mathrm{sgn}\,\pi)^{-m}$ is a unit in $R[\mathbb{F}_\infty]$, so f_{-m} is a unit in $R[\mathbb{F}_\infty]$. In particular, f_{-m} is in $F \cap R[\mathbb{F}_\infty] = R$, and hence $f_{-m} \in R^\times$ by going-up theorem. By reducing modulo $\mathfrak{m}$, viewing the coefficients of the expansion of G as in $F_\mathfrak{m}$, we get

$$\widetilde{G} = \widetilde{f_{-m}}\pi^{-m} + O(\pi^{-m+1}),$$

showing that G and $\widetilde{G}$ has the same order of poles at $\overline{\infty}$.

□

Proof of Proposition IV.1. Let M_1, M_2 be the $R \otimes \mathbb{A}$-modules on the left and right side respectively. We will show that for all maximal ideals $\mathfrak{m}$ of R, the $(R/\mathfrak{m}) \otimes \mathbb{A}$-modules $\widetilde{M_i} := M_i/(\mathfrak{m} \otimes \mathbb{A})M_i$ are equal for $i = 1, 2$. Then we will use Nakayama's lemma to conclude that $M_1 = M_2$.

Since G and $\widetilde{G}$ have the same number of poles at each (respective) $\overline{\infty}$ and they cannot have any pole elsewhere, they have the same number of zeros. Thus in $X_{\overline{\mathbb{F}_q}}$, we can write

$$\operatorname{div}(\widetilde{G}) = \sum_i (t_1 - \widetilde{a_{i,1}}, \cdots, t_n - \widetilde{a_{i,n}}) - \sum \text{poles above } \infty.$$

Since X is a smooth curve over $\mathbb{F}_q$, the ring $\overline{\mathbb{F}_q} \otimes \mathbb{A}$ is noetherian (from X being locally of finite type over $\mathbb{F}_q$), integrally closed (since X is smooth, hence normal, hence geometrically normal as $\mathbb{F}_q$ is perfect), and has Krull dimension 1. That is, it is Dedekind. As a result, all non-zero ideals of $\overline{\mathbb{F}_q} \otimes \mathbb{A}$ can be factored into a product of maximal ideals. By the Nullstellensatz, maximal ideals of

$$\overline{\mathbb{F}_q}[t_1, \cdots, t_n]$$

are of the form

$$(t_1 - \alpha_1, \cdots, t_n - \alpha_n).$$

Since ideals of $\overline{\mathbb{F}_q} \otimes \mathbb{A}$ are in natural bijection with ideals of $\overline{\mathbb{F}_q}[t_1, \cdots, t_n]$ which contain $F_1, \cdots, F_m$, we have as ideals in $\overline{\mathbb{F}_q} \otimes \mathbb{A}$,

$$(\widetilde{G}) = \prod_i (t_1 - \widetilde{a_{i,1}}, \cdots, t_n - \widetilde{a_{i,n}}).$$

Let $k' := R/\mathfrak{m}$. Intersecting the ideals with $k' \otimes \mathbb{A}$ (or equivalently, taking $\operatorname{Gal}(\overline{k'}/k')$-invariant), we have that $\widetilde{M_1} = \widetilde{M_2}$.

We now proceed to show that $M_1 = M_2$. Let $M_3 = M_1 \cap M_2$ in $R \otimes \mathbb{A}$. From above, we know that

$$(\mathfrak{m} \otimes \mathbb{A})(M_i/M_3) = M_i/M_3$$

for $i = 1, 2$ and for all $\mathfrak{m} \subset R$ maximal. Now for any maximal ideal $\mathfrak{M}$ of $R \otimes \mathbb{A}$, the pullback of $\mathfrak{M}$ to R along $R \to R \otimes \mathbb{A}$ is maximal, because R is of finite type over $\mathbb{F}_q$. Thus $\mathfrak{M}$ contains $\mathfrak{m} \otimes 1$ for some $\mathfrak{m} \subset R$ maximal. As a result,

$$\mathfrak{M}(M_i/M_3) = M_i/M_3$$

for all maximal ideals $\mathfrak{M} \subset R \otimes \mathbb{A}$. Since M_i/M_3 are finitely generated as $R \otimes \mathbb{A}$-modules, by Nakayama's lemma $M_i/M_3 = 0$. Therefore $M_1 = M_3 = M_2$.

□

The main way we apply this proposition is to evaluate at a certain closed point in $\overline{X}$ not above ∞.

Corollary IV.3. *Let ξ be a closed point of $\overline{X}$ not above ∞, with coordinates in the model $\mathbb{A}$ given by $(\theta_1, \cdots, \theta_n)$ such that $\theta_k \in R$ for all k. Then as R-ideals,*

$$(G|_\xi) = \prod_i (\theta_1 - a_{i,1}, \cdots, \theta_n - a_{i,n}).$$

□

IV.4: Applying the proposition to exp and log coefficients

We analyze the log coefficients for elliptic curves and ramifying hyperelliptic curves in this subsection. Recall from chapter II that the shtuka function has a presentation

$$f = \frac{\nu}{\delta},$$

where $\nu, \delta \in \mathcal{O}_H$, $\widetilde{\mathrm{sgn}}(\nu) = \widetilde{\mathrm{sgn}}(\delta) = 1$, and all coordinates of their zeros are also integral over $\mathcal{O}_H$. Recall also that

$$\mathrm{div}(\nu) = V^{(1)} + V' + (\Xi) - (2g+1)(\overline{\infty}), \qquad \mathrm{div}(\delta) = V + V' - 2g(\overline{\infty}),$$

where V' is an effective divisor of degree g. Let $\{(t = \alpha_i, y = \beta_i)\}_{i=1}^g$ be the coordinates for V, and $\{(t = \alpha_i', y = \beta_i')\}_{i=1}^g$ be the coordinates for V'. Define K_V to be the smallest field extension of H in $\mathbb{C}_\infty$ containing all these coordinates, and R the integral closure of A in K_V. By applying proposition IV.1 to $\nu^{(k)}$, $\delta^{(k)}$ and the R we just defined, we can see that as ideals of $R \otimes \mathbb{A}$,

$$(\nu^{(k)}) = (t - \theta^{q^k}, y - \eta^{q^k}) \prod_i \left[(t - \alpha_i^{q^{k+1}}, y - \beta_i^{q^{k+1}})(t - \alpha_i'^{q^k}, y - \beta_i'^{q^k}) \right],$$
$$(\delta^{(k)}) = \prod_i \left[(t - \alpha_i^{q^k}, y - \beta_i^{q^k})(t - \alpha_i'^{q^k}, y - \beta_i'^{q^k}) \right].$$

Apply corollary IV.3 to the same set of data, with $\xi = \Xi$, we obtain that as R-ideals,

$$(\nu^{(k)}|_\Xi) = (\theta - \theta^{q^k}, \eta - \eta^{q^k}) \prod_i \left[(\theta - \alpha_i^{q^{k+1}}, \eta - \beta_i^{q^{k+1}})(\theta - \alpha_i'^{q^k}, \eta - \beta_i'^{q^k}) \right],$$
$$(\delta^{(k)}|_\Xi) = \prod_i \left[(\theta - \alpha_i^{q^k}, \eta - \beta_i^{q^k})(\theta - \alpha_i'^{q^k}, \eta - \beta_i'^{q^k}) \right].$$

Therefore, we have the following factorization of coefficients for e_ρ and $\log_\rho$:

Proposition IV.1. *As fractional R-ideals,*

$$\begin{aligned}\left(\frac{1}{f f^{(1)} \cdots f^{(n-1)}} \Big|_{\Xi^{(n)}} \right) &= \left(\frac{\delta \cdots \delta^{(n-1)}}{\nu \cdots \nu^{(n-1)}} \Big|_{\Xi^{(n)}} \right) \\ &= \left(\prod_{k=0}^{n-1} (\theta^{q^n} - \theta^{q^k}, \eta^{q^n} - \eta^{q^k})^{-1} \right) \\ &\quad \cdot \left(\prod_i (\theta^{q^n} - \alpha_i, \eta^{q^n} - \beta_i)(\theta^{q^n} - \alpha_i^{q^n}, \eta^{q^n} - \beta_i^{q^n})^{-1} \right),\end{aligned}$$

and

$$\begin{aligned}\left(\frac{\delta^{(n+1)}}{\delta^{(1)} f^{(1)} \cdots f^{(n)}} \Big|_{\Xi} \right) &= \left(\frac{\delta^{(2)} \cdots \delta^{(n+1)}}{\nu^{(1)} \cdots \nu^{(n)}} \Big|_{\Xi} \right) \\ &= \left(\prod_{k=1}^{n} (\theta - \theta^{q^k}, \eta - \eta^{q^k})^{-1} \right) \\ &\quad \cdot \left(\prod_i (\theta - \alpha_i'^{q^{n+1}}, \eta - \beta_i'^{q^{n+1}})(\theta - \alpha_i'^{q}, \eta - \beta_i'^{q})^{-1} \right).\end{aligned}$$

□

CHAPTER V
Coefficients of Exponential and Logarithm for Hayes Modules

In this chapter, we will study the v-adic valuation of the coefficients of exponential and logarithm series for elliptic curves and ramifying hyperelliptic curves. This will allow us to show that $e_\rho(z)$ and $\log_\rho(z)$, when viewed as power series over $\mathbb{C}_v$, converges when z is within disc of certain radii. For ease of notation, let e_n and l_n be defined by

$$e_\rho(z) = \sum_{n\geq 0} e_n z^{q^n},$$

$$\log_\rho(z) = \sum_{n\geq 0} l_n z^{q^n}.$$

As a remark, none of l_n is 0 by [Tha04, Theorem 8.3.13].

V.1: Notations from Elementary Number Theory

Let us first fix some notation for this section. Recall that $\mathfrak{p} \subset A$ is the prime corresponding to v. Suppose $\mathfrak{p}$ has degree $d_\mathfrak{p}$, i.e. $d_\mathfrak{p} = -d_\infty v_\infty(\mathfrak{p}) = -v_\infty(\mathfrak{p})$. Let $\mathfrak{p}_\theta \in \mathbb{F}_q[\theta]$, $\mathfrak{p}_\eta \in \mathbb{F}_q[\eta]$ be the monic generator of the ideals $\mathfrak{p} \cap \mathbb{F}_q[\theta]$ and $\mathfrak{p} \cap \mathbb{F}_q[\eta]$ respectively. By abuse of notation, we also use $\mathfrak{p}_\theta$, $\mathfrak{p}_\eta$ to denote the maximal ideal they generate in $\mathbb{F}_q[\theta]$ and $\mathbb{F}_q[\eta]$ respectively. By elementary number theory, we have that

$$\deg \mathfrak{p} = \deg_\theta \mathfrak{p}_\theta \cdot f_\theta = \deg_\eta \mathfrak{p}_\eta \cdot f_\eta,$$

where f_θ, f_η are the inertial degree of $\mathfrak{p}$ over $\mathfrak{p}_\theta$, $\mathfrak{p}_\eta$ respectively. Note that $\deg \mathfrak{p}$ is divisible by both f_θ and f_η, hence also by $\gcd(f_\theta, f_\eta)$. We also set $v_{\mathfrak{p}_\theta}$ and $v_{\mathfrak{p}_\eta}$ to be the valuation on $\mathbb{F}_q(\theta)$ and $\mathbb{F}_q(\eta)$ corresponding to $\mathfrak{p}_\theta$ and $\mathfrak{p}_\eta$ respectively, such that $v_{\mathfrak{p}_\theta}(\mathfrak{p}_\theta) = 1$ and $v_{\mathfrak{p}_\eta}(\mathfrak{p}_\eta) = 1$. Because we normalize v so that the value group is $\mathbb{Z}$, for $b_1 \in \mathbb{F}_q(\theta)$ and $b_2 \in \mathbb{F}_q(\eta)$, by

viewing b_1, b_2 as functions in K, we have

$$v(b_1) = v_{\mathfrak{p}_\theta}(b_1) \cdot e_\theta, \quad v(b_2) = v_{\mathfrak{p}_\eta}(b_2) \cdot e_\eta,$$

where e_θ is the ramification index of $\mathfrak{p}$ over $\mathfrak{p}_\theta$, and similarly for e_η.

We define K_V as in the previous chapter: recall that K_V is the smallest extension of H^+ ($= H$ since $d_\infty = 1$ for our case) containing all coordinates of all zeros of ν and δ, and R the integral closure of A in K_V. Fix an embedding $\overline{K} \hookrightarrow \overline{K_v}$. This gives a valuation w on K_V. We normalize w so that the value group is $\mathbb{Z}$. Then once again, for a function $b_3 \in K$, by viewing $b_3 \in K_V$, we have

$$w(b_3) = v(b_3) \cdot e_w,$$

where e_w is the ramification index of w over v.

Finally, we let I_k to be the A-ideal $(\theta - \theta^{q^k}, \eta - \eta^{q^k})$, $J_{k,i}$ to be the R-ideal $(\theta^{q^k} - \alpha_i, \eta^{q^k} - \beta_i)$, $J'_{k,i}$ to be the R-ideal $(\theta - \alpha_i'^{q^k}, \eta - \beta_i'^{q^k})$, J_k the R-ideal $\prod_i J_{k,i}$, and J'_k be the R-ideal $\prod_i J'_{k,i}$. Hence as fractional R-ideals,

$$(e_n) = \left(\prod_{k=0}^{n-1} I_{n-k}^{(k)} R\right)^{-1} J_n (J_0^{(n)})^{-1},$$

$$(l_n) = \left(\prod_{k=1}^{n} I_k R\right)^{-1} J'_{n+1} J_1'^{-1}.$$

Thus,

Proposition V.1.

$$w(e_n) = w(J_n) - w(J_0^{(n)}) - e_w \sum_{k=0}^{n-1} v(I_{n-k}^{(k)}),$$

$$w(l_n) = w(J'_{n+1}) - w(J'_1) - e_w \sum_{k=1}^{n} v(I_k).$$

□

V.2: Main term for logarithm, and one term from exponential: I_k

The main contribution of $w(l_n)$ will come from $v(I_k)$, which we shall first compute. We will also compute $v(I_{n-k}^{(k)})$ for the exponential series.

Lemma V.1.

$$v_{\mathfrak{p}_\theta}(\theta - \theta^{q^k}) = \begin{cases} 1 & \text{if } \deg_\theta \mathfrak{p}_\theta \mid k, \\ 0 & \text{else.} \end{cases}$$

The same is true for η.

Proof. All elements in $\mathbb{F}_{q^k}$ are roots of the equation $X^{q^k} - X = 0$, so $X^{q^k} - X = \prod_{c \in \mathbb{F}_{q^k}} (X - c)$. By grouping $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$-conjugates of the right hand side, we have that

$$X^{q^k} - X = \prod_{\substack{a \in \mathbb{F}_q[X] \\ a \text{ monic irreducible} \\ \deg a \mid k}} a.$$

□

Proposition V.2.

$$v(I_k) = \begin{cases} \min\{e_\theta, e_\eta\} & \text{if } \deg \mathfrak{p} \mid k \gcd(f_\theta, f_\eta), \\ 0 & \text{else.} \end{cases}$$

Proof. To have $v(I_k) > 0$, we must have $\mathfrak{p}$ dividing both $\theta - \theta^{q^k}$ and $\eta - \eta^{q^k}$. By the previous lemma, the first requirement is satisfied when $\deg_\theta \mathfrak{p}_\theta \mid k$, and the second is satisfied when $\deg_\eta \mathfrak{p}_\eta \mid k$. Expressing both of these with $\deg \mathfrak{p}$, we have that $\deg \mathfrak{p}$ divides both $k f_\theta$ and $k f_\eta$, which is equivalent to $\deg \mathfrak{p}$ dividing $k \gcd(f_\theta, f_\eta)$.

Now suppose $v(I_k) > 0$ and we would like to compute $v(I_k)$. Recall that

$$v(\theta - \theta^{q^k}) = v_\theta(\theta - \theta^{q^k}) \cdot e_\theta,$$

which is e_θ by the previous lemma and our assumption that $v(I_k) > 0$. Similarly, $v(\eta - \eta^{q^k}) = e_\eta$. As a result,

$$v(I_k) = v((\theta - \theta^{q^k}, \eta - \eta^{q^k})) = \min\{e_\theta, e_\eta\}.$$

□

By adding these up for $k = 1, \cdots, n$, we can see that

Corollary V.3.

$$\sum_{k=1}^{n} v(I_k) = \min\{e_\theta, e_\eta\} \left\lfloor \frac{n \gcd(f_\theta, f_\eta)}{\deg \mathfrak{p}} \right\rfloor.$$

□

We observe in particular that this has the order of magnitude $O(n)$.

We now proceed to compute $v(I_{n-k}^{(k)})$.

Proposition V.4. *For* $0 \leq k \leq n-1$,

$$v(I_{n-k}^{(k)}) = \begin{cases} \min\{e_\theta, e_\eta\} q^k & \text{if } \deg \mathfrak{p} \mid (n-k)\gcd(f_\theta, f_\eta) \\ 0 & \text{else.} \end{cases}$$

Proof. By lemma V.1,

$$v_{\mathfrak{p}_\theta}(\theta^{q^n} - \theta^{q^k}) = v_{\mathfrak{p}_\theta}((\theta^{q^{n-k}} - \theta)^{q^k}) = \begin{cases} q^k & \text{if } \deg_\theta \mathfrak{p}_\theta \mid k \\ 0 & \text{else.} \end{cases}$$

The same is true for η. The result now follows by a similar argument as Proposition V.2.

□

For our purpose, we will only give an upper bound for the sum of $v(I_{n-k}^{(n-k)})$.

Corollary V.5. *Let* $C = \dfrac{\deg \mathfrak{p}}{\gcd(f_\theta, f_\eta)}$. *Then*

$$\sum_{k=0}^{n-1} v(I_{n-k}^{(k)}) < q^n \min\{e_\theta, e_\eta\} \frac{1}{q^C - 1}.$$

Proof.

$$\begin{aligned} \sum_{k=0}^{n-1} v(I_{n-k}^{(k)}) &= \sum_{k=1}^{n} v(I_k^{(n-k)}) \\ &= \min\{e_\theta, e_\eta\} \left(q^{n-C} + q^{n-2C} + \cdots + q^{n - \lfloor \frac{n}{C\gcd(f_\theta, f_\eta)} \rfloor C} \right) \\ &= \min\{e_\theta, e_\eta\} q^n \frac{1 - q^{-C\lfloor \frac{n}{C\gcd(f_\theta, f_\eta)} \rfloor}}{q^C - 1} \\ &< q^n \min\{e_\theta, e_\eta\} \frac{1}{q^C - 1}. \end{aligned}$$

□

Even though we give this as an upper bound, we can see from the proof that sum of $v(I_{n-k}^{(k)})$ has order $O(q^n)$.

V.3: Other terms for logarithm

We then proceed to show that the term $w(J'_n)$ does not matter when compared to the sum of $v(I_k)$'s.

Proposition V.1. *Fix an i. $w(J'_{n,i})$ is bounded by some constant independent on n.*

Proof. If $w(J'_{n,i}) > 0$ for only finitely one n, we are done. Suppose not. Let $N_1 > N_2 > 0$ be two integers where $w(J'_{N_1,i})$ and $w(J'_{N_2,i})$ are positive. Then

$$w\left((\theta - \alpha_i'^{q^{N_1}}, \eta - \beta_i'^{q^{N_1}}, \theta - \alpha_i'^{q^{N_2}}, \eta - \beta_i'^{q^{N_2}})\right) = w(J'_{N_1,i} + J'_{N_2,i}) > 0.$$

We can rewrite this R-ideals as

$$(\theta - \alpha_i'^{q^{N_2}}, \theta - \theta^{q^{N_1-N_2}}, \eta - \beta_i'^{q^{N_2}}, \eta - \eta^{q^{N_1-N_2}}),$$

by considering $\theta - \alpha_i'^{q^{N_1}}$ modulo $\theta - \alpha_i'^{q^{N_2}}$, and similarly for η, β'_i. In particular, we can see that

$$J'_{N_1,i} + J'_{N_2,i} \supset I_{N_1-N_2}R.$$

Thus

$$\min\{w(J'_{N_1,i}), w(J'_{N_2,i})\} = w(J'_{N_1,i} + J'_{N_2,i}) \leq w(I_{N_1-N_2}),$$

By Proposition V.2, the last term is bounded by $e_w \cdot \max\{e_\theta, e_\eta\}$. What we have shown is that if we pick any two N_1, N_2 with $w(J'_{N_1,i}), w(J'_{N_2,i})$ both positive, then at least one of them is bounded by $e_w \cdot \max\{e_\theta, e_\eta\}$. Thus we can have at most one N such that $w(J'_{n,i})$ is bigger than the $e_w \cdot \max\{e_\theta, e_\eta\}$. Therefore, $w(J'_{n,i})$ is bounded by a constant independent on n.

□

Corollary V.2. *$w(J'_n)$ is bounded by some constant independent on n.*

Proof. This comes from $w(J'_n) = \sum_{i=1}^{g} w(J'_{n,i})$. □

V.4: Other terms for the exponential

As for the exponential, the term $w(J_0^{(n)})$ will actually contribute potentially.

Lemma V.1.

$$w(J_{0,i}^{(n)}) = q^n w(J_{0,i}),$$

and hence

$$w(J_0^{(n)}) = q^n w(J_0).$$

Proof.

$$\begin{aligned} w(J_{0,i}^{(n)}) &= \min\{w((\theta-\alpha_i)^{(n)}), w((\eta-\beta_i)^{(n)})\} \\ &= q^n \min\{w(\theta-\alpha_i), w(\eta-\beta_i)\} \\ &= q^n w(J_{0,i}). \end{aligned}$$

□

This means that in the formula for $w(l_n)$ in Proposition V.1, $w(J_{0,i}^{(n)})$ either does not contribute at all, or it has order $O(q^n)$, which is the same as the sum of $v(I_k^{(n-k)})$'s.

The term $w(J_n)$ can be ignored when computing the w-adic convergence of exponential: since it is positive, it only make the convergence easier.

V.5: Conclusion for w-adic convergence of exponential and logarithm

Recall from Proposition V.1 that

$$w(l_n) = w(J'_{n+1}) - w(J'_1) - e_w \sum_{k=1}^{n} v(I_k),$$

By using Corollary V.5 and Corollary V.2, we now have the following result.

Theorem V.1. *For $n \gg 0$, $w(l_n)$ is negative, and $|w(l_n)|$ has order of magnitude $O(n)$.*

This allows us to show the v (or equivalently w)-adic convergence of Hayes logarithm in $\mathbb{C}_v$.

Theorem V.2. *The logarithm series for Hayes module, in the cases of an elliptic curve or a ramifying hyperelliptic curve with ∞ the rational point at infinity, converges w-adically for all $z \in \mathbb{C}_v$ with $w(z) > 0$.*

Proof. Suppose $z \in \mathbb{C}_v$ with $w(z) > 0$. Then

$$w(l_n z^{q^n}) = w(l_n) + q^n w(z).$$

Since $w(z) > 0$ and $w(l_n)$ is in the order of magnitude $O(n)$, $w(l_n z^{q^n})$ goes to infinity as n does, showing that the series

$$\log_\rho(z) = \sum_{n=0}^{\infty} l_n z^{q^n}$$

converges in $\mathbb{C}_v$. □

As for exponential, we can conclude the following.

Theorem V.3. *The exponential series for Hayes module, in the case of an elliptic curve or a ramifying hyperelliptic curve with ∞ as the rational point at infinity, converges w-adically for all $z \in \mathbb{C}_v$ with*

$$w(z) > w(J_0) + e_w \min\{e_\theta, e_\eta\} \frac{1}{q^C - 1}.$$

where $C = \dfrac{\deg \mathfrak{p}}{\gcd(f_\theta, f_\eta)}$.

Proof. By combining Corollary V.5 and Lemma V.1, we can see that

$$\begin{aligned} w(e_n) &= w(J_n) - w(J_0^{(n)}) - e_w \sum_{k=0}^{n-1} v(I_{n-k}^{(k)}) \\ &\geq -\left(w(J_0) + e_w \min\{e_\theta, e_\eta\} \frac{1}{q^C - 1} \right) q^n. \end{aligned}$$

Hence if $w(z)$ is bigger than the number in the parentheses, we have that

$$w(e_n z^{q^n}) \geq \varepsilon q^n,$$

for some $\varepsilon > 0$. This valuation goes to infinity as $n \to \infty$. This shows that the series

$$e_\rho(z) = \sum_{n=0}^{\infty} e_n z^{q^n}$$

converges in $\mathbb{C}_v$. □

Definition V.4. We denote by $e_{v,\rho}(z)$ and $\log_{v,\rho}(z)$ the functions defined by the respective series on $\mathbb{C}_v$, whenever the series converges.

CHAPTER VI
L-functions on Drinfeld Modules

As an application of the v-adic convergence of $\log_{v,\rho}$, we will prove a log-algebraicity formula for a certain analogue of p-adic L-function in characteristic p. In this chapter, we will first provide the preliminaries for L-functions over function fields, and then prove the log-algebracity result.

The theory of zeta functions, L-functions and p-adic L-functions is important in number theory. In the number field case, it provides useful tools for studying a lot of interesting topics, such as prime distributions, representations, elliptic curves, etc. Given how well the analogy between number fields and function fields is, we naturally hope that we can develop a similar theory in the function field case.

There have been L-functions defined on algebraic curves (or more generally, varieties) in algebraic geometry. To quickly recall, given a smooth projective curve X over $\mathbb{F}_q$, the arithmetic zeta function is defined to be

$$\zeta(X, s) := \exp\left(\sum_{m\geq 1} \frac{N_m}{m} q^{-ms}\right),$$

where $N_m := \#X(\mathbb{F}_{q^m})$ is the number of $\mathbb{F}_{q^m}$-points of X. It is well-known (e.g. [Har13, Appendix C]) that this zeta function is a rational function (of q^{-s}), satisfies a functional equation and a version of Riemann hypothesis.

However, this zeta function does not match all aspects of the Riemann zeta function. For example:

- it does not give good information about closed points of X: this zeta function counts the number of closed points of each degree, but does not distinguish them;
- it does not have an Euler product with respect to closed points of X;
- there is no analogy of trivial zeros;
- it is rational;

- it is a function on $\mathbb{C}$, while the curve is over characteristic p.

The first characteristic p zeta function was studied by Carlitz in 1935 [Car35]. His approach was to directly imitate the Riemann zeta function: summing up the reciprocal of a nicely-chosen representative from each nonzero ideal of $\mathbb{F}_q[\theta]$.

$$\zeta_C(n) := \sum_{\substack{a \in \mathbb{F}_q[\theta] \\ a \text{ monic}}} \frac{1}{a^n}$$

The first analogue of this zeta function and the Riemann zeta function was discovered in the same paper: the special values of this zeta function at positive "even" integers are given by power of transcendental period and Bernoulli numbers.

Perhaps due to Carlitz's massive amount of writings, this new zeta function was forgotten for a while. At the 70s, Goss [Gos78], [Gos79], [Gos80] revisited the idea and generalize this to L-functions on all curves $X/\mathbb{F}_q$. We will see how these L-functions are defined and show where they converges in the next section. We will also describe how we can extend the domain from $\mathbb{Z}$ to a characteristic p analytic space in section VI.3.

With the convergence results, Goss also defined, for each closed point v of X, a v-adic L-function on characteristic p. These v-adic L-functions satisfies an interpolation formula, just as the p-adic L-function over $\mathbb{Q}$ does. We will give the definition in section VI.2. As a remark, the theory of such v-adic L-function is still in development. For instance, its relationship with towers of v-cyclotomic extensions and Iwasawa theory are still not clear.

In the number field case, we have a formula for the special L-values $L(1,\chi)$ and $L_p(1,\chi)$ for Dirichlet characters χ. Under certain conditions for χ, these values are $\overline{\mathbb{Q}}$-linear combinations of logarithm of elements in $\overline{\mathbb{Q}}$ (cf. [Was97, 4.9,5.18]). We will call this a *log-algebraic formula*. In 1996, Anderson [And96] discovered a log-algebraic formula for the Goss L-values and v-adic L-values $L(1,\chi)$ and $L_v(1,\chi)$ for $\mathbb{F}_q[\theta]$, where χ is a Dirichlet character of conductor v on $\mathbb{F}_q[\theta]$. Then in 2010, Lutes [Lut10] generalized Anderson's result for Goss L-values to any curve and any $\mathbb{A}$ in his thesis. In this thesis, we will show a log-algebraic formula for the Goss v-adic L-values for elliptic curves and ramifying hyperelliptic curves in section VI.4.

VI.1: Goss zeta function

VI.1.1: Simple case: PID

To make things simple, let us first talk about zeta function instead of an L-function. We begin with the assumption that A is a PID, so we can make direct analogies from the Riemann zeta function. It should be noted that this does not occur a lot: since $h(A)$, the class number

of the Dedekind domain A, is the same as $h_X \cdot d_\infty$, where h_X is the class number of the curve X, we need both $h_X = 1$ and the existence of a rational point in X. There are only 5 (up to isomorphism) cases where A is a PID (cf. [LMQ75], [Mac71], [Sti14]):

1. $\mathbb{F}_q[\theta]$, $g = 0$;
2. $\mathbb{F}_3[\theta, \eta]/(\eta^2 - (\theta^3 - \theta - 1))$, $g = 1$;
3. $\mathbb{F}_2[\theta, \eta]/(\eta^2 + \eta + (\theta^3 + \theta + 1))$, $g = 1$;
4. $\mathbb{F}_4[\theta, \eta]/(\eta^2 + \eta + (\theta^3 + c))$ where c generates $\mathbb{F}_4^\times$, $g = 1$;
5. $\mathbb{F}_2[\theta, \eta]/(\eta^2 + \eta + (\theta^5 + \theta^3 + 1))$, $g = 2$.

Following Carlitz's definition of the zeta function on $\mathbb{F}_q[\theta]$, we need to pick a "good" representative from each nonzero ideal of A. For $\mathbb{F}_q[\theta]$, Carlitz picked the monic generator from each ideal. For general A, we have generalized the notion of "monic" element, by fixing a sign function. Upon fixing sgn, we define A^+ to be the subset of A of *monic* (i.e. sgn 1) elements, and $A^+(d)$ to be the subset of monic degree d elements for each $d \in \mathbb{Z}$.

Definition VI.1. For $n \in \mathbb{Z}_{\geq 0}$ and A a PID, we define the *Goss zeta function* to be the series

$$\zeta(n) = \sum_{a \in A^+} \frac{1}{a^n} := \sum_{d \geq 0} \sum_{a \in A^+(d)} \frac{1}{a^n}.$$

The series is summed in the order of increasing degree. This matches how the Riemann zeta series is summed up: the latter terms in the series should have smaller (infinity-adic) absolute values. For $a \in A$, recall that $|a|_\infty = q^{\deg a}$, so the above sum is indeed in the order of decreasing ∞-adic absolute value.

Since the absolute value $|\cdot|_\infty$ is non-archimedean and the terms in the series go to 0, the series converges for all $n \in \mathbb{Z}_{>0}$. For $n = 0$, we have $\zeta(0) = 1$ since the partial sum for each degree $d \geq 1$ is 0. Hence $\zeta(n)$ is an element in $\mathbb{C}_\infty$ for all $n \in \mathbb{Z}_{\geq 0}$.

VI.1.2: Goss's Lemma

The usual Riemann zeta series converges for $\mathrm{Re} z > 1$, and can be extended to a meromorphic function on $\mathbb{C}$. Interestingly, the Goss zeta series actually converges at the negative integers as well, which we will see in section VI.1.3. This is because the degree d partial sum vanishes for $d \gg 0$. This observation is due to Goss [Gos79], using the following lemma. Using this lemma, Goss extended the L-functions and v-adic L-functions to certain characteristic p analytic spaces, which we will see in section VI.3. The following version of the lemma is

from Goss's book [Gos98]. The details of the induction in the second part is found in [Gos92, 3.6.7].

Lemma VI.2 (Goss's Lemma). *1. Let J, J_1 be two fields over $\mathbb{F}_q$, $W \subset J$ be a finite-dimensional vector space over $\mathbb{F}_q$ of dimension α, and let $\{\mathcal{L}_1, \ldots, \mathcal{L}_t\}$ be $\mathbb{F}_q$-linear maps of J into J_1. Let $x \in J$ and $\{i_1, \ldots, i_t\}$ be a set of non-negative integers such that*

$$\sum_{h=1}^{t} i_h < (q-1)\alpha.$$

Then

$$\sum_{w \in W} \left(\prod_{h=1}^{t} \mathcal{L}_h(x+w)^{i_h} \right) = 0.$$

2. Suppose now that J_1 has an additive valuation v with $v(\mathcal{L}_h(w)) > 0$ for all h and for all $w \in W$. Let $\{i_h\}$ be an arbitray collection of non-negative integers. For $j > 0$, define

$$W_j = \{w \in W \mid v(\mathcal{L}_h(w)) \geq j \text{ for all } h\}.$$

Then

$$v\left(\sum_{w \in W} \prod_{h=1}^{t} \mathcal{L}_h(w)^{i_h} \right) \geq (q-1) \sum_{j=1}^{\infty} d_j,$$

where

$$d_j = \dim_{\mathbb{F}_q}(W_j).$$

Note that this is independent on i_h.

Proof. The proof of the first part is a straightforward application of the multinomial theorem. Let $\{e_1, \ldots, e_\alpha\}$ be a basis for W over $\mathbb{F}_q$. Then the sum in the lemma becomes

$$\sum_{c_1, \ldots, c_\alpha \in \mathbb{F}_q} \prod_{h=1}^{t} \left(\mathcal{L}_h(x) + c_1 \mathcal{L}_h(e_1) + \cdots + c_\alpha \mathcal{L}_h(e_\alpha) \right)^{i_h}.$$

Expand $\left(\mathcal{L}_h(x) + c_1 \mathcal{L}_h(e_1) + \cdots + c_\alpha \mathcal{L}_h(e_\alpha) \right)^{i_h}$ via multinomial theorem.

$$\sum_{j_1^h, \ldots, j_\alpha^h} \binom{i_h}{(i_h - j_1^h - \cdots - j_\alpha^h), j_1^h, \ldots, j_\alpha^h} \mathcal{L}_h(x)^{i_h - j_1^h - \cdots - j_\alpha^h} \cdot \mathcal{L}_h(e_1)^{j_1^h} \cdots \mathcal{L}_h(e_\alpha)^{j_\alpha^h} c_1^{j_1^h} \ldots c_\alpha^{j_\alpha^h}.$$

Here the superscript h on j's is an index, not a power. Take the product over h. Each

term in the sum (over $c_1, \ldots, c_\alpha \in \mathbb{F}_q$ and over j_i^h) now looks like

$$(\text{junk}) c_1^{j_1^1 + \cdots + j_1^t} \ldots c_\alpha^{j_\alpha^1 + \cdots + j_\alpha^t},$$

where (junk) is in J_1 and depends only on x and j's, but not c's.

The sum of the exponents

$$j_1^1 + j_1^2 + \cdots + j_\alpha^t = (j_1^1 + j_2^1 + \cdots + j_\alpha^1) + \cdots + (j_1^t + \cdots + j_\alpha^t) \leq i_1 + \cdots + i_t,$$

which is by assumption less than $(q-1)\alpha$. Hence, for each term in the sum, at least one of the exponent of c's is less than $(q-1)$. For that particular combination of j_i^h with $\sum_h j_i^h < q-1$, we consider the sum over $c_i \in \mathbb{F}_q$:

$$\sum_{c_i \in \mathbb{F}_q} (\text{junk}) c_1^{j_1^1 + \cdots + j_1^t} \ldots c_\alpha^{j_\alpha^1 + \cdots + j_\alpha^t} = \left((\text{junk}) \cdot \prod_{\substack{1 \leq i' \leq \alpha \\ i' \neq i}} c_{i'}^{j_{i'}^1 + \cdots + j_{i'}^t} \right) \sum_{c_i \in \mathbb{F}_q} c_i^{j_i^1 + \cdots + j_i^t}$$

The equality is true since everything in the product other than the term

$$c_i^{j_i^1 + \cdots + j_i^t}$$

stays constant in the sum. If $\sum_i j_i^h = 0$, i.e. $j_i^h = 0$ for all h, then the c_i term is 1 in the multinomial expansion (even for $c_i = 0$) as no power of c_i is picked up in the expansion. The sum over c_i is then

$$\sum_{c_i \in \mathbb{F}_q} 1 = 0$$

For other exponent $1 \leq C < q-1$,

$$\sum_{c_i \in \mathbb{F}_q} c_i^C = 0$$

for $1 \leq C < q-1$. Hence the sum

$$\sum_{c_i \in \mathbb{F}_q} (\text{junk}) c_1^{j_1^1 + \cdots + j_1^t} \ldots c_\alpha^{j_\alpha^1 + \cdots + j_\alpha^t}$$

is 0. Repeat this process for every tuple $(j_i^h)_{i,h}$, we can see that the entire sum

$$\sum_{c_1, \ldots, c_\alpha \in \mathbb{F}_q} \prod_{h=1}^{t} (\mathcal{L}_h(x) + c_1 \mathcal{L}_h(e_1) + \cdots + c_\alpha \mathcal{L}_h(e_\alpha))^{i_h} = 0,$$

completing the proof of the first part.

As for the second part, first observe that since W is finite-dimensional over $\mathbb{F}_q$, the set $\{v(\mathcal{L}_h(w))|h, w\}$ is bounded. Hence there is an integer $j_0 > 0$ such that $W_{j_0+1} = 0$ but $W_{j_0} \neq 0$. This also shows that the sum on the right hand side of the inequality is finite.

We claim the following.

Claim: For any integer j with $1 \leq j \leq j_0$, and for any choice of exponents $\{i_1, \ldots, i_t\}$,

$$v\left(\sum_{w \in W_j} \prod_{h=1}^{t} \mathcal{L}_h(w)^{i_h}\right) \geq (q-1)d_j j + (q-1)\sum_{l>j} d_l.$$

The second part of Goss's lemma is the case when $j = 1$. We will prove the claim by induction in reverse order.

For $j = j_0$, we have two cases. If $\sum_h i_h < (q-1)d_{j_0}$, then the first part of the lemma with $x = 0$ implies that the sum is 0, and so the left hand side is ∞. Now we suppose $\sum_h i_h \geq (q-1)d_{j_0}$. By definition of W_{j_0}, $v(\mathcal{L}_h(w)) \geq j_0$ for all w and all h. Thus

$$v\left(\prod_{h=1}^{t} \mathcal{L}_h(w)^{i_h}\right) = \sum_{h=1}^{t} i_h v(\mathcal{L}_h(w)) \geq \sum_{h=1}^{t} i_h j_0 \geq (q-1)d_{j_0} j_0.$$

Now suppose the claim holds for some $j+1$ with $2 \leq j+1 \leq j_0$. If $d_j = d_{j+1}$, then both sides of the inequality do not change. Suppose $d_j > d_{j+1}$. Pick a basis $\{e_1, \ldots, e_{d_j}\}$ for W_j such that $\{e_1, \ldots, e_{d_{j+1}}\}$ is a basis for W_{j+1}. This gives us a decomposition

$$W_j = W_{j+1} \oplus \mathbb{F}_q[e_{d_{j+1}+1}, \ldots, e_{d_j}].$$

For every $w \in W_j$, let $w' \in \mathbb{F}_q[e_1, \ldots, e_{d_{j+1}}] = W_{j+1}$ and
$w'' \in \mathbb{F}_q[e_{d_{j+1}+1}, \ldots, e_{d_j}] =: W_j/W_{j+1}$ such that $w = w' + w''$. By binomial theorem,

$$\sum_{w \in W_j} \prod_{h=1}^{t} \mathcal{L}_h(w)^{i_h} = \sum_{w' \in W_{j+1}} \sum_{w'' \in W_j/W_{j+1}} \prod_{h=1}^{t} \sum_{k_h=0}^{i_h} \binom{i_h}{k_h} \mathcal{L}_h(w')^{i_h-k_h} \mathcal{L}_h(w'')^{k_h}.$$

Exchange the order of summation and factorize, the sum is equal to

$$\sum_{i_h, k_h} \binom{i_h}{k_h} \left(\sum_{w' \in W_{j+1}} \prod_{h=1}^{t} \mathcal{L}_h(w')^{i_h-k_h}\right) \left(\sum_{w'' \in W_j/W_{j+1}} \prod_{h=1}^{t} \mathcal{L}_h(w'')^{k_h}\right).$$

By induction hypothesis, the first part in the factorization has valuation $\geq (q-1)d_{j+1}(j+1) + (q-1)\sum_{l>j+1} d_l$. For the second part of the factorization, we use the first part of Goss's

lemma again. If $\sum_h i_h < (q-1)\dim_{\mathbb{F}_q} W_j/W_{j+1}$, the second part is 0 by the first part of the lemma. Else, a similar calculation as above shows that

$$v\left(\sum_{w''\in W_j/W_{j+1}}\prod_{h=1}^{t}\mathcal{L}_h(w'')^{k_h}\right) \geq (q-1)\dim_{\mathbb{F}_q}(W_j/W_{j+1})j$$
$$= (q-1)(d_j - d_{j+1})j.$$

Therefore, each term in our sum has valuation at least

$$\left((q-1)d_{j+1}(j+1) + (q-1)\sum_{l>j+1} d_l\right) + (q-1)(d_j - d_{j+1})j$$
$$= (q-1)d_j j + (q-1)\sum_{l>j} d_l.$$

□

VI.1.3: Convergence at negative integers

As a small application of the lemma, we will show that the Goss zeta function over a PID converges at negative integers n.

Proposition VI.3. *Suppose A is a PID. The Goss zeta function converges at negative integers $n < 0$.*

Proof. This can be seen directly with first part of lemma VI.2, with $\{J = J_1 = \mathbb{C}_\infty\}$, W the space of elements with degree at most $d-1$, $\{\mathcal{L}_h\}_h = \{\mathrm{id}\}$, x a nonzero element in $A^+(d)$, and $i_1 = -n > 0$. Then for $d \gg 0$, we have

$$-n < (q-1)\dim_{\mathbb{F}_q} A^+(d-1).$$

By the first part of lemma VI.2,

$$\sum_{a\in W}(x+a)^{-n} = 0.$$

For A a PID, all elements in $A^+(d)$ is in the form x plus an element in W, for a fixed nonzeros $x \in A^+(d)$. Therefore

$$\sum_{a\in A^+(d)} a^{-n} = 0.$$

□

As we can see in the proof, $\zeta(-n)$ is actually an element in A. This is an instance of the phenomenon called "essential algebraicity" of Goss L-function. See [Gos98, 8.4].

VI.2: Goss v-adic zeta function

The usual p-adic L-function in the $\mathbb{Q}$ and $\mathbb{Q}_p$ case is defined via interpolating values of L-function at negative integers, see [Was97]. In particular, the Riemann zeta series with the terms divisible by p taken away do not converge p-adically. However, this is very different in the function field case. Fix a finite place v. With the help of Goss's lemma from the last section, Goss [Gos79] showed that the series defining the Goss zeta function, with terms divisible by v taken away, does converge v-adically. We will illustrate the details in this section.

VI.2.1: Simple case: PID

Let v be a place of X away from ∞, and $\mathfrak{p} \subset A$ the corresponding maximal ideal. Let $A_v, \mathbb{A}_v, K_v, \mathbb{K}_v$ be the completion of the corresponding rings/fields with the place v, and $\mathbb{C}_v$ the completion of the algebraic closure of K_v (NOT $\mathbb{K}_v$). Let n be an integer, and consider the formal zeta series in $\mathbb{C}_v$.

$$\sum_{d\geq 0} \sum_{a\in A^+(d)} \frac{1}{a^n}.$$

There is no hope for convergence in $\mathbb{C}_v$, since there are more and more poles at v as d increases. A way to fix this is to remove those a divisible by $\mathfrak{p}$ from the sum.

$$\sum_{d\geq 0} \sum_{\substack{a\in A^+(d) \\ \mathfrak{p}\nmid a}} \frac{1}{a^n}.$$

We will see in the next section that this series converges in $\mathbb{C}_v$ for $n \in \mathbb{Z}$.

VI.2.2: Convergence

Proposition VI.1. *Fix a nonzero congruence class $\alpha \mod \mathfrak{p}$. The series*

$$\sum_{d\geq 0} \sum_{\substack{a\in A^+(d) \\ a\equiv\alpha \pmod{\mathfrak{p}}}} a^{-n}$$

converges in $\mathbb{C}_v$ for all integers n. Hence for all integers n, we can define

$$\zeta_v(n) := \sum_{d\geq 0} \sum_{\substack{a\in A^+(d)\\ \mathfrak{p}\nmid a}} a^{-n} := \sum_{\alpha\in(A/\mathfrak{p})^\times} \sum_{d\geq 0} \sum_{\substack{a\in A^+(d)\\ a\equiv\alpha \pmod{\mathfrak{p}}}} a^{-n}.$$

Proof. For $n \leq 0$, the proof is the same as Proposition VI.3, which shows $\zeta(n)$ converges for $n < 0$. Fix $d \gg 0$. Define W to be the space of elements of degree at most $d-1$ and divisible by $\mathfrak{p}$, and x an element of degree d such that $x - \alpha$ is divisible by $\mathfrak{p}$, which exists since $d \gg 0$. The degree d partial sum is then

$$\sum_{\substack{a\in A^+(d)\\ a\equiv\alpha \pmod{\mathfrak{p}}}} a^{-n} = \sum_{w\in W} (x+w)^{-n},$$

which is 0 by part 1 of Goss's lemma VI.2.

For $n > 0$, this requires part 2 of Goss's lemma VI.2. As with the proof of $n \leq 0$, fix $d \gg 0$, and define W, x in the same way. Then

$$\sum_{\substack{a\in A^+(d)\\ a\equiv\alpha \pmod{\mathfrak{p}}}} a^{-n} = \sum_{w\in W} (x+w)^{-n} = \sum_{w\in W} x^{-n}\left(1+\frac{w}{x}\right)^{-n}.$$

Since w/x has v-adic absolute value less than 1, we can expand $(1+w/x)^{-n}$ via binomial theorem in $\mathbb{C}_v$.

$$\sum_{w\in W} x^{-n}\left(1+\frac{w}{x}\right)^{-n} = \sum_{w\in W} x^{-n} \sum_{k=0}^{\infty} \binom{-n}{k} \left(\frac{w}{x}\right)^k = x^{-n} \sum_{k=0}^{\infty} \binom{-n}{k} \sum_{w\in W} \left(\frac{w}{x}\right)^k.$$

By part 2 of Goss's lemma VI.2, in particular with $w \mapsto \dfrac{w}{x}$ as the $\mathbb{F}_q$-linear map,

$$v\left(\sum_{w\in W} \left(\frac{w}{x}\right)^k\right) \geq (q-1)\sum_{j=1}^{\infty} d_j,$$

where d_j is defined as in the lemma

$$d_j = \dim_{\mathbb{F}_q} W_j = \dim_{\mathbb{F}_q}\{w \in W \mid v(w/x) \geq j\}.$$

Since A is a PID, we have that

$$\dim_{\mathbb{F}_q}\{w \in W \mid v(w/x) \geq j\} = \dim_{\mathbb{F}_q}\{a \in A \mid \deg a \leq (d-1), \mathfrak{p}^j \mid a\}$$

$$= \dim_{\mathbb{F}_q}\{a \in A \mid \deg a \leq (d-1) - \deg \mathfrak{p}^j\} = d - j \deg \mathfrak{p},$$

which is, upon fixing j, linear with respect to d. As a remark, we used that A is a PID to derive an explicit formula for the dimension, but the dimension will always be linear with respect to d even if A is not a PID, because of Riemann-Roch.

Putting this back to the inequality from Goss's lemma, we can see that

$$v\left(\sum_{w \in W} \left(\frac{w}{x}\right)^k\right) \geq (q-1)\sum_{j=1}^{\infty} d_j$$

grows quadratically with respect to d, and is independent on the exponent k. Therefore,

$$\sum_{d \geq 0} x^{-n} \sum_{k=0}^{\infty} \binom{-n}{k} \sum_{w \in W} \left(\frac{w}{x}\right)^k$$

converges in $\mathbb{C}_v$. □

In fact, the proof for $n > 0$ works for all integers, and even for $n \in \mathbb{Z}_p$, if we have a way to make sense of x^{-n}. This hints that the Goss zeta series converges on a larger domain. We shall investigate the extension of domain in the next section.

VI.3: Extension to a larger domain

In this section, we will extend the Goss zeta functions in two ways following Goss: analytic extension to a larger space, and to define the series when A is not a PID. We first describe how the extension to larger space is done, motivated by generalizing the power functions x^n to non-integer exponent. To go from PID to non-PID, for each integral ideal we need to assign an element to the series. Unlike Dedekind L-function in the number field case, where we take the norm of ideals to $\mathbb{Q}$ to get a principal ideal, in function field Goss achieved the goal by defining the exponentiation of an ideal as an element.

VI.3.1: S_∞

In number fields, the Dirichlet L-series are extended from $\mathbb{Z}$ to $\mathbb{C}$. Following the insight, the ideal candidate of a larger analytic space as the domain of L-function will be $\mathbb{C}_\infty$. To extend the L-function to an analytic space, we need to make sense of exponentiation with exponent somehow in $\mathbb{C}_\infty$. This needs to be done in a way that is compatible with the usual exponentiation with exponent in $\mathbb{Z}$. Since $\mathbb{C}_\infty$ has characteristic p, we need to embed $\mathbb{Z}$ into $\mathbb{C}_\infty^\times$ multiplicatively, instead of into $\mathbb{C}_\infty$ additively.

Definition VI.1. (cf. [Gos98, §8.1]) Set

$$S_\infty := \mathbb{C}_\infty^\times \times \mathbb{Z}_p.$$

Fix a uniformizer $\pi \in K_\infty$ with $\operatorname{sgn} \pi = 1$, and let π_* be a d_∞-th root of π in $\mathbb{C}_\infty$. Then $\mathbb{Z}$ embeds into S_∞ via

$$j \mapsto (\pi_*^{-j}, j).$$

For $\alpha \in K_\infty^\times$, we can write

$$\alpha = \operatorname{sgn} \alpha \cdot \pi^{v_\infty(\alpha)} \cdot \langle \alpha \rangle,$$

where $\langle \alpha \rangle$ is a 1-unit in $\mathbb{C}_\infty^\times$. In particular it makes sense to raise it by an exponent in $\mathbb{Z}_p$. For $s = (x, y) \in S_\infty$, we define

$$\alpha^s := x^{-d_\infty v_\infty(\alpha)} \langle \alpha \rangle^y.$$

This extends the usual exponentiation with integer exponent.

For $n \in \mathbb{Z}$, we denote $[n] \in S_\infty$ to be the corresponding element in S_∞. We can then define the extend the Goss zeta function (for A a PID at the moment) to a function $S_\infty \to \mathbb{C}_\infty$

$$\zeta(s) := \sum_{d \geq 0} \sum_{a \in A^+(d)} a^{-s}.$$

We will check the convergence later when we also generalize the function for A not a PID.

VI.3.2: Ideal Exponentiation

Recall our notation that $\mathcal{I}$ is the group of fractional A-ideals in K, and $\mathcal{P}^+$ is the subgroup of principal ideals generated by sgn 1 elements. Let $\widehat{U_1}$ be the group of 1-units in $\mathbb{C}_\infty^\times$. The exponential function

$$u_1^a$$

for $u_1 \in \widehat{U_1}$ can be extended uniquely from $a \in \mathbb{Z}_p$ to $a \in \mathbb{Q}_p$. Thus the group $\widehat{U_1}$ is uniquely-divisible. Since $\mathcal{I}/\mathcal{P}^+$ is finite, we can extend

$$\langle - \rangle : \mathcal{P}^+ \to \widehat{U_1}$$

uniquely to $\mathcal{I}$.

Now we can define exponentiation of an ideal by an element in S_∞:

Definition VI.2. (cf. [Gos98, §8.2]) Let $I \subset A$ be a nonzero ideal and $s = (x, y) \in S_\infty$. We

define

$$\deg I := -d_\infty v_\infty(I),$$

and

$$I^s := x^{\deg I}\langle I\rangle^y.$$

One can check that this is an extension of exponentiation of a positive element by an exponent in S_∞ ([Gos98, 8.2.6]).

This takes care of the ∞-adic extension, but we also want to extend the v-adic functions, which have image in $\mathbb{C}_v$. To do so, we study the field that contains all such $I^{[1]}$.

Definition VI.3. Let $V \subset \mathbb{C}_\infty$ be the smallest subfield generated by K and $\{I^{[1]} \mid I \in \mathcal{I}\}$.

Proposition VI.4. *[Gos98, 8.2.9, 8.2.10] V/K is finite, with*

$$I\mathcal{O}_V = (I^{[1]}).$$

It is however **not** true that $V = H^+$. In fact, V/K could be inseparable, which happens if $p \mid h(A)$.

VI.3.3: S_v and v-adic ideal exponentiation

Since V/K is finite, upon fixing an embedding $\overline{K} \hookrightarrow \overline{K_v}$ we can also define ideal exponentiation v-adically. Let w be the place of V above v given by the embedding $V \subset \overline{K} \hookrightarrow \overline{K_v}$.

The decomposition of a nonzero positive element is slightly more complicated in V_w than in K_∞: Since a positive element has sgn 1, we do not have to worry about roots of unity $\mathbb{F}_\infty^\times$ in the decomposition of $K_\infty^\times$. However, this cannot be omitted in $V_w^\times$, as a monic polynomial is not necessarily a 1-unit in $\mathbb{C}_v$.

Imitating what we did for the v-adic Goss zeta function when A is a PID, we do not consider those ideals divisible by $\mathfrak{p}$. This means that we only have to define exponentiation with base from the group of integral units $\mathcal{O}_{V,w}^\times$ instead of the entire $V_w^\times$.

For all $\alpha \in \mathcal{O}_{V,w}^\times$, we have a decomposition

$$\alpha = \omega_w(\alpha)\langle\alpha\rangle_w,$$

where $\omega_w(\alpha) \in \mathbb{F}_w^\times$ is given by the composition

$$\mathcal{O}_{V,w}^\times \to (\mathcal{O}_{V,w}/(w))^\times \xrightarrow{\text{Hansel's lift}} \mathcal{O}_{V,w}^\times,$$

and $\langle\alpha\rangle_w \in U_{1,w}$ is a 1-unit. Let $D_w := \#(\mathbb{F}_w^\times)$. This gives us the following requirements for defining the topological group of possible exponents for v-adic ideal exponentiation:

- the group of possible exponents should have a $\mathbb{Z}/D_w\mathbb{Z}\times\mathbb{Z}_p$ component, to accommodate for $\omega_w(\alpha)$ and $\langle\alpha\rangle_w$ respectively;
- the embedding from $\mathbb{Z}$ into the space of possible exponents needs to send n to (n, n) in $\mathbb{Z}/D_w\mathbb{Z} \times \mathbb{Z}_p$;
- as with the $\mathbb{C}_\infty$ case, there is a $\mathbb{C}_v^\times$ component; the image of $\mathbb{Z}$ to the $\mathbb{C}_v^\times$ component in the group of exponents is 1, so the exponentiation is compatible with the usual one with positive integer exponent.

This gives the following definition.

Definition VI.5. (cf. [Gos98, §8.3])

1. For $(s_1, s_2) \in S_v := \mathbb{Z}/D_w\mathbb{Z} \times \mathbb{Z}_p$ and $\alpha \in \mathcal{O}_{V,w}^\times$, we define
$$\alpha^{(s_1,s_2)} := \omega_w(\alpha)^{s_1}\langle\alpha\rangle_w^{s_2}$$
2. For $(x, s_1, s_2) \in \mathbb{C}_v^\times \times S_v = \mathbb{C}_v^\times \times \mathbb{Z}/D_w\mathbb{Z}\times\mathbb{Z}_p$, and $I \subset \mathcal{I}$ an ideal prime to $\mathfrak{p}$, we define
$$I^{(x,s_1,s_2)} := x^{\deg I}(I^{[1]})^{(s_1,s_2)}.$$
Here we view $I^{[1]}$ as an element in $\mathcal{O}_{V,w}^\times$ via the fixed embedding $\overline{K} \to \overline{K}_v$.

This coincides with the exponentiation of a positive element by a positive integer, via the embedding $\mathbb{Z} \to \mathbb{C}_v^\times \times S_v$ with $n \mapsto (1, n, n)$.

VI.3.4: Extension of Goss zeta and v-adic zeta functions

We are now ready to extend the Goss zeta function and v-adic zeta function to a non-PID A and to an analytic domain. Let $h^+ = \#\mathcal{I}/\mathcal{P}^+$ be the narrow class number, and $\mathfrak{a}_1, \cdots, \mathfrak{a}_{h^+} \subset A$ be A-ideals representing the classes of $\mathcal{I}/\mathcal{P}^+$. We borrow the notation from number fields and use $\mathfrak{a}_j^{-1}$ to stand for the inverse fractional A-ideal of $\mathfrak{a}_j$, and we denote the subset of sgn 1 elements in $\mathfrak{a}_j^{-1}$ by $\mathfrak{a}_j^{-1,+}$.

Definition VI.6. For $s \in S_\infty$ and a general A, we define
$$\zeta_A(s) = \sum_{0\neq I\subset A}\frac{1}{I^s} := \sum_{j=1}^{h^+}\frac{1}{\mathfrak{a}_j^s}\sum_{d=0}^{\infty}\sum_{\substack{i\in\mathfrak{a}_j^{-1,+}\\ \deg i+\deg\mathfrak{a}_j=d}}\frac{1}{i^s}.$$

And for $(x, s) \in \mathbb{C}_v^\times \times S_v$, we define

$$\zeta_{A,v}(x,s) := \sum_{d \geq 0} \sum_{\substack{0 \neq I \subset A \\ v(I)=0 \\ \deg I = d}} I^{-s},$$

with the sum split into different congruence classes of the narrow ray class group $\mathcal{I}(I)/\mathcal{P}_I^+$.

For a finite order character Ψ of conductor $\mathfrak{p}$ on $\mathcal{I}$, the Goss L-function $L(s, \Psi)$ and $L_v(1, \Psi)$ can be defined similarly.

As for convergence, the difficulty of the proof resembles the number field case. Namely, it is very easy to prove convergence when the absolute value is sufficiently large, similar to the convergence of zeta functions over number fields at the complex right half plane. On the other hand, the convergence when the absolute value is small is also true, but the proof is a lot more involved, invoking Goss's lemma VI.2 and requiring more technical details. We will illustrate the proof for the sufficiently large case, and refer readers to Goss's book [Gos98] for the general case.

Proposition VI.7. *The function $\zeta_A(s)$ converges for $|x| > 1$, where $s = (x, y)$, and $\zeta_{A,v}(x, s)$ converges for all $(x, s) \in \mathbb{C}_v^\times \times S_v$ with $|x|_v > 1$.*

Proof. We will only show the proof for $\zeta_A(s)$. The proof for $\zeta_{A,v}(x, s)$ is very similar. We unwind the exponential i^s from the $\mathfrak{a}_j$-component of the zeta series.

$$\begin{aligned}
&\sum_{d=0}^{\infty} \sum_{\substack{i \in \mathfrak{a}_j^{-1,+} \\ \deg i + \deg \mathfrak{a}_j = d}} i^{-s} \\
=& \sum_{d=0}^{\infty} \sum_{\substack{i \in \mathfrak{a}_j^{-1,+} \\ \deg i + \deg \mathfrak{a}_j = d}} x^{-\deg i} \langle i \rangle^{-y} \\
=& \sum_{d=0}^{\infty} x^{-(d - \deg \mathfrak{a}_j)} \sum_{\substack{i \in \mathfrak{a}_j^{-1,+} \\ \deg i + \deg \mathfrak{a}_j = d}} \langle i \rangle^{-y}
\end{aligned}$$

Since the sums of 1-units $\langle i \rangle^{-y}$ have absolute value at most 1, the infinite sum (over d) converges as $|x| > 1$. □

Proposition VI.8. *(cf. [Gos98, Theorem 8.9.2]) The function $\zeta_A(s)$ converges for all $s = (x, y)$, and the function $\zeta_{A,v}(x, s)$ converges for all $(x, s) \in \mathbb{C}_v^\times \times S_v$.*

In fact, Goss proved a statement for these L-functions better than just convergence: these functions are analytic in the $\mathbb{C}_\infty^\times$ (resp. $\mathbb{C}_v^\times$) variable, and varies continuously along the $\mathbb{Z}_p$ (resp. S_v) variable. See [Gos98, Ch 8] for the definition and discussion of analyticity on S_∞ and $\mathbb{C}_v^\times \times S_v$.

VI.4: Log-algebraicity

In his paper introducing log-algebraicity [And96], Anderson discovered a strong log-algebraicity statement, and used it to deduce a formula for $L(1,\chi)$, which follows the classical "Gauss sum $\cdot$ log(algebraic integers)" pattern as in the number field case. He then applied his formula as well as the fact that the Carlitz logarithm as v-adic radius of convergence 1 to show a similar formula for $L_v(1,\chi)$. Later, Lutes in his thesis [Lut10] used Anderson's technique to compute $L(1,\Psi)$ over any ring A, where Ψ is now a character on the group of fractional A-ideals with prime conductor. Our goal in this section is to use Anderson's idea to expand Lutes's computation to $L_v(1,\Psi)$.

It is also worth mentioning that Green and Papanikolas [GP18] use independent techniques to come up with another formula for $L(1,\Psi)$ in the genus 1 case, as a special case for a formula for Pellarin L-series. It would be an exciting idea to see if we can come up with similar v-adic results for Pellarin L-series [Pel12] or in the sense of Taelman [Tae12].

VI.4.1: Anderson's Log algebraicity

We shall first briefly go through Anderson's log-algebracity statement. Let $\rho_I(\tau)$ be the monic generator of the principal left ideal $\{\rho_i(\tau) \mid i \in I\} \subset H^+\{\tau\}$, $D(\rho_I)$ be its constant term, and $\rho_I(Y)$ be obtained by replacing τ^j with Y^{q^j} in $\rho_I(\tau)$. Here Y is a free variable, in particular transcendental over H^+.

Let ϖ_ρ to be a generator of zero lattice Λ_ρ for $e_\rho(z)$. To ease the notations, define $\mathbf{e}_A(z) := e_\rho(\varpi_\rho z)$, and $\mathbf{e}_I(z) := e_{I*\rho}(D(\rho_I)\varpi_\rho z)$.

Definition VI.1. 1. Let

$$b(Y) = \sum_{i=0}^{\deg b} b_i Y^i \in H^+[Y].$$

We define an action of nonzero A-ideals on $H^+[Y]$ by

$$(J * b)(Y) := \sum_{i=0}^{\deg b} b_i^{(J,H^+/K)} \rho_J(Y)^i,$$

where $(J, H^+/K) \in \mathrm{Gal}(H^+/K)$ is the Artin symbol.

2. For each $b \in H^+[Y]$, let $l(b;z)$ be a power series in z over $H^+[Y]$ defined by

$$l(b;z) := \sum_J \frac{J * b}{D(\rho_J)} z^{q^{\deg J}},$$

where the sum is over all nonzero ideals $J \subset A$. Similarly, upon fixing a nonzero ideal $I \subset A$, we define

$$l_I(b;z) := \frac{1}{D(\rho_I)} \sum_{\alpha \in I^{-1,+}} \frac{(\alpha I) * b}{\alpha} z^{q^{\deg I + \deg \alpha}}.$$

As a remark, it is clear that $l(b;z) = \sum_{i=1}^{h^+} l_{\mathfrak{a}_i}(b;z)$, where $\mathfrak{a}_i$ goes over all classes of $\mathcal{I}/\mathcal{P}^+$. Anderson's main result in [And96] asserts that given $b \in \mathcal{O}_{H^+}[Y]$, $l(b;z)$ can be viewed as a certain logarithm. To be precise, by applying the exponential power series associated to ρ, we can obtain a polynomial in Y, z over $\mathcal{O}_{H^+}$.

Theorem VI.2. *(Anderson, [And96, Theorem 3]) For $b \in \mathcal{O}_{H^+}[Y]$, the formal power series*

$$S(b;z) := e_\rho(l(b;z)),$$

a priori in the ring $(H^+[Y])[[z]]$, is in fact in $\mathcal{O}_{H^+}[Y,z]$.

This is an analogue of the fact that $\exp(\log(1-z))$, a priori a formal power series in $\mathbb{Q}[[z]]$, is in fact in $\mathbb{Z}[z]$. Readers can refer to [And96] for a more careful formulation of this theorem, via writing $l(b;z)$ in increasing power of z and defining $S(b;z)$ in terms of such coefficients. Readers can also refer to a beautiful survey article by Perkins [Per13].

By definition of $S(b;z)$, we have that $S(Y^m;z)$ is divisible by Y^m. We will use this observation very soon.

VI.4.2: $L(1,\Psi)$

Next, we pick appropriate $b \in \mathcal{O}_{H^+}[Y]$, and evaluate at particular values of Y and z.

Definition VI.3. For a nonzero ideal $I \subset A$, we define

$$l_{m,I}(x) = \frac{1}{D(\rho_I)} \sum_{\alpha \in (I^{-1})^+} \frac{\mathbf{e}_I(\alpha x)}{\alpha} = l_I(X^m;z)|_{Y=\mathbf{e}_A(x),z=1}.$$

Here x is another formal variable. Later we will substitute x by elements in $\mathfrak{p}^{-1}\Lambda_\rho/\Lambda_\rho$.

Fix an isomorphism

$$A/\mathfrak{p} \longrightarrow \mathfrak{p}^{-1}\Lambda_\rho/\Lambda_\rho$$

$$a \mapsto a\mu$$

Recall that $\mathfrak{a}_1, \ldots, \mathfrak{a}_{h^+} \subset A$ are integral ideals representing the classes of $\mathcal{I}/\mathcal{P}^+$. We then substitute $b = Y^m$, $Y = \mathbf{e}_I(a\mu)$, and $z = 1$ to Anderson's log-algebraicity and obtain that

$$e_\rho\left(\sum_{i=1}^{h^+} l_{m,\mathfrak{a}_i}(a\mu)\right) = S(Y^m; z)|_{Y=\mathbf{e}_A(a\mu),z=1}$$

is an algebraic integer in $\mathcal{O}_{H^+}[\rho[\mathfrak{p}]]$. Before we move on to values of $L(1, \Psi)$, we shall first mention an important lemma. This lemma is a key to prove the log-algebraicity for $L_v(1, \Psi)$.

Lemma VI.4. *For any $\beta \in \mathcal{O}_{K(\rho[\mathfrak{p}])}$, the element $S(\beta Y^m; z)|_{Y=\mathbf{e}_A(a\mu),z=1}$ is divisible by $\mathbf{e}_A(a\mu)^m$ in $\mathcal{O}_{K(\rho[\mathfrak{p}])}$.*

Proof. Recall from the discussion after Theorem VI.2 that $S(Y^m; z)$ is divisible by Y^m. The exact same argument shows that the same is true for $S(\beta Y^m; z)$. Now evaluate at $Y = \mathbf{e}_A(a\mu), z = 1$, we have that $S(\beta Y^m; z)|_{Y=\mathbf{e}_A(a\mu),z=1}$ is divisible by

$$\mathbf{e}_A(a\mu)^m = (\rho_a(\mathbf{e}_A(\mu)))^m,$$

which is divisible by $\mathbf{e}_A(\mu)^m$. □

We now return to the study of $L(1, \Psi)$. With the notation $l_{m,I}(x)$, Anderson and Lutes gave formula for $L(1, \Psi)$ in terms of $\mathbf{e}_I(a\mu)$'s and $l_{m,I}(b\mu)$, using Lagrange interpolation.

Theorem VI.5. *1. (Anderson, [And96, (38)]) Let $A = \mathbb{F}_q[\theta]$ and $\chi : A \to \mathbb{C}_\infty$ a character of conductor $\mathfrak{p}$. In this case $\mathcal{I}/\mathcal{P}^+ = 1$. Then*

$$L(1, \chi) = -\frac{1}{\mathfrak{p}^{[1]}} \sum_{m=1}^{q^{\deg \mathfrak{p}}-1} \left(\sum_{a\in\mathbb{F}_\mathfrak{p}^\times} \mathbf{e}_m^*(a)\right)\left(\sum_{b\in\mathbb{F}_\mathfrak{p}^\times} \chi^{-1}(b) l_{m,A}(b\mu)\right).$$

The $\mathbf{e}_m^*(a)$ are elements algebraic over $\mathbb{F}_q(\theta)$, obtained via Lagrange interpolation.

2. (Lutes, [Lut10, V.13]) For a general A, and Ψ a character of conductor $\mathfrak{p}$ on $\mathcal{I}(\mathfrak{p})$, the group of fractional A-ideals prime to $\mathfrak{p}$,

$$L(1, \Psi) = \sum_{j=1}^{h^+} \Bigg[-\frac{\chi(\mathfrak{a}_j)}{\mathfrak{a}_j^{[1]}} \sum_{m=1}^{q^{\deg \mathfrak{p}}-1} \sum_{a\in\mathbb{F}_\mathfrak{p}^\times} \left(\chi(a)\mathbf{e}_{m,\mathfrak{a}_j}^*(a/\nu_j)\right) \sum_{b\in\mathbb{F}_\mathfrak{p}^\times} \left(\chi^{-1}(b) l_{m,\mathfrak{a}_j}(b\mu)\right) \Bigg].$$

The ν_j's, $\mathbf{e}_{m,\mathfrak{a}_j}(a/\nu_j)$'s are defined similarly as μ and $\mathbf{e}^*_m(a)$. See [Lut10] for detailed definitions.

When $A = \mathbb{F}_q[\theta]$, we can rewrite the term $l_{m,A}(b\mu)$ as

$$l_{m,A}(b\mu) = l(Y^m; z)|_{Y=\mathbf{e}_A(b\mu),z=1} = \log_\rho S(Y^m; z)|_{Y=\mathbf{e}_A(b\mu),z=1},$$

in particular the Carlitz logarithm of an algebraic integer. This shows that $L(1,\chi)$ is log-algebraic.

However, in Lutes's scenario, the log-algebraicity is not as immediate. A direct difficulty we encounter is that we cannot directly conclude that $l_{m,\mathfrak{a}_j}(b\mu)$ is log-algebraic. To fix this, Lutes fixed a set of K-linearly independent elements $\{\beta_1, \cdots, \beta_{h^+}\}$ in $\mathcal{O}_{H^+}$. Then he applied Anderson's log-algebraicity theorem VI.2 to $b = \beta_j Y^m$ instead of Y^m. This shows that

$$S(\beta_j Y^m; z) = e_\rho(l(\beta_j Y^m; z))$$

is a polynomial in Y, z with coefficients in $\mathcal{O}_{H^+}$. Evaluate this at $Y = \mathbf{e}_A(b\mu), z = 1$, we have that

$$S(\beta_j Y^m; z)_{Y=\mathbf{e}_A(b\mu),z=1}$$

is an algebraic integer for all β_j. Now, unwinding the right side, we see that

$$\begin{aligned}
S(\beta_j Y^m; z)_{Y=\mathbf{e}_A(b\mu),z=1} &= e_\rho\left(l(\beta_j Y^m; z)\right)_{Y=\mathbf{e}_A(b\mu),z=1} \\
&= \sum_{i=1}^{h^+} e_\rho\left(l_{\mathfrak{a}_i}(\beta_j Y^m; z)\right)_{Y=\mathbf{e}_A(b\mu),z=1} \\
&= \sum_{i=1}^{h^+} e_\rho\left(\beta_j^{(\mathfrak{a}_i, H^+/K)} l_{\mathfrak{a}_i}(Y^m; z)\right)_{Y=\mathbf{e}_A(b\mu),z=1} \\
&= \sum_{i=1}^{h^+} e_\rho(\beta_j^{(\mathfrak{a}_i, H^+/K)} l_{m,\mathfrak{a}_i}(b\mu)).
\end{aligned}$$

As β_j varies in the set $\{\beta_1, \ldots, \beta_{h^+}\}$, these equations can be written in terms of a matrix equation. For ease of notation, set $\mathfrak{L}_j := \log_\rho\left(S(\beta_j Y^m; z)_{Y=\mathbf{e}_A(b\mu),z=1}\right)$.

$$\begin{pmatrix} \mathfrak{L}_1 \\ \mathfrak{L}_2 \\ \vdots \\ \mathfrak{L}_{h^+} \end{pmatrix} = \begin{pmatrix} \beta_1^{(\mathfrak{a}_1, H^+/K)} & \beta_1^{(\mathfrak{a}_2, H^+/K)} & \cdots & \beta_1^{(\mathfrak{a}_{h^+}, H^+/K)} \\ \beta_2^{(\mathfrak{a}_1, H^+/K)} & \beta_2^{(\mathfrak{a}_2, H^+/K)} & \cdots & \beta_2^{(\mathfrak{a}_{h^+}, H^+/K)} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{h^+}^{(\mathfrak{a}_1, H^+/K)} & \beta_{h^+}^{(\mathfrak{a}_2, H^+/K)} & \cdots & \beta_{h^+}^{(\mathfrak{a}_{h^+}, H^+/K)} \end{pmatrix} \begin{pmatrix} l_{m,\mathfrak{a}_1}(b\mu) \\ l_{m,\mathfrak{a}_2}(b\mu) \\ \vdots \\ l_{m,\mathfrak{a}_{h^+}}(b\mu) \end{pmatrix}.$$

By definition, $\{\beta_1, \cdots, \beta_{h^+}\}$ is K-linearly independent. Thus the matrix here has linearly-independent rows, equivalently nonzero determinant. This shows that $l_{m,\mathfrak{a}_i}(b\mu)$ is an H^+-linear combination of $\mathfrak{L}_j = \log_\rho \left(S(\beta_j Y^m; z)_{Y=\mathbf{e}_A(b\mu),z=1}\right)$. Combining this with theorem VI.5, we obtain the following.

Theorem VI.6. *[Lut10, V.14] The special value $L(1,\Psi)$ is log-algebraic, i.e. there exists $\alpha_1, \cdots, \alpha_s$, $S_1, \cdots, S_s \in \overline{K}$ such that*

$$L(1,\Psi) = \sum_i \alpha_i \log_\rho S_i.$$

In fact, we can pick $S_i \in K(\rho[\mathfrak{p}])$, $\alpha_i \in V(\rho[\mathfrak{p}])$, and $s \leq (q^{\deg \mathfrak{p}} - 1)^2 \cdot h^+$. □

If one wishes, the α_i's can be written very explicitly, by using Cramer's rule to solve the matrix equation. The expression will get too long, so we skip it here. Interested readers can refer to [Lut10].

VI.4.3: $L_v(1,\chi)$ over $\mathbb{F}_q[\theta]$

Anderson applied the log-algebraicity for $L(1,\chi)$ as well as the v-adic convergence for $\log_\rho$ to deduce the log-algebraicity for $L_v(1,\chi)$ on the Carlitz module. We will illustrate it here as a motivation to our generalization of this result. In this section, $A = \mathbb{F}_q[\theta]$ and we are using the Carlitz module $\rho_t = \theta + \tau$.

Proposition VI.7. *[And96, Prop 12] The series*

$$\sum_{d\geq 0} \left(\sum_{\substack{a\in A^+ \\ v(a)=0 \\ \deg a = d}} \frac{\mathbf{e}_A(ab/\mathfrak{p})^m}{a} \right)$$

converges v-adically to $\log_v(S(Y^m;z)|_{Y=\mathbf{e}_A(b\mu,z=1)})$.

The proof is easy: realize that $S(Y^m;z)|_{Y=\mathbf{e}_A(b\mu,z=1)}$ lies in the radius of convergence for $\log_v$, and the calculation follows from formal manipulation of series.

Using this, Anderson wrote down a formula for $L_v(1,\chi)$, which is similar to the Kubota-Leopoldt formula.

Proposition VI.8. *[And96, (43)]*

$$L_v(1,\chi) = -\sum_{m=1}^{q^d-1}\left(\frac{1}{\mathfrak{p}^{[1]}}\sum_{a\in\mathbb{F}_{\mathfrak{p}}^{\times}}\chi(a)\mathbf{e}_m^*(a)\right) \cdot\left(\sum_{b\in\mathbb{F}_{\mathfrak{p}}^{\times}}\chi^{-1}(b)\log_v(S(Y^m;z)|_{Y=\mathbf{e}_A(b\mu,z=1)})\right).$$

In particular the elements $\mathbf{e}_m^*(a)$ *is the same as in VI.5.*

VI.4.4: Log-algebraicity for $L_v(1,\Psi)$ on Elliptic curves and Ramifying Hyperelliptic curves

We now proceed to prove our application, which is the log-algebraicity for $L_v(1,\Psi)$ for our curves.

Proposition VI.9. *Fix* $\beta\in\mathcal{O}_{H^+}$. *The series*

$$\sum_{j=1}^{h^+}\beta^{(\mathfrak{a}_j,H^+/K)}l_{m,\mathfrak{a}_j}(b\mu) = \sum_{k=0}^{\infty}\left(\sum_{j=1}^{h^+}\frac{1}{D(\rho_{\mathfrak{a}_j})}\beta^{(\mathfrak{a}_j,H^+/K)}\left(\sum_{\substack{\alpha\in\mathfrak{a}_j^{-1,+}\\ \deg\mathfrak{a}_j+\deg\alpha=k}}\frac{\mathbf{e}_{\mathfrak{a}_j}(\alpha b\mu)^m}{\alpha}\right)\right),$$

summing in the order as indicated, converges v*-adically to*

$$\log_{v,\rho}\left(S(\beta Y^m;z)|_{Y=\mathbf{e}_A(b\mu),z=1}\right).$$

Proof. By definition of $e_I(z)$,

$$\mathbf{e}_{\mathfrak{a}_j}(\alpha b\mu) = e_{\mathfrak{a}_j*\rho}(D(\rho_{\mathfrak{a}_j})\varpi_\rho\alpha b\mu).$$

We shall investigate the right hand side. Since α is positive, by definition of ρ_I we have that

$$D(\rho_{\alpha\mathfrak{a}_j}) = \alpha D(\rho_{\mathfrak{a}_j}).$$

Since $\alpha\mathfrak{a}_j$ is in the same ideal class as $\mathfrak{a}_j$, the Hayes modules $(\alpha\mathfrak{a}_j)*\rho$ and $\mathfrak{a}_j*\rho$ are the

same. As a result

$$e_{(\alpha\mathfrak{a}_j)*\rho} = e_{\mathfrak{a}_j*\rho}.$$

Thus

$$\mathbf{e}_{\mathfrak{a}_j}(\alpha b\mu) = e_{(\alpha\mathfrak{a}_j)*\rho}(D(\rho_{\alpha\mathfrak{a}_j})\varpi_\rho b\mu) = \rho_{\alpha\mathfrak{a}_j}(\mathbf{e}_A(b\mu)),$$

where functional equation for ρ_I is used in the last equality. Putting everything together, the degree-k part of our series becomes

$$\sum_{j=1}^{h^+} \sum_{\substack{\alpha\in\mathfrak{a}_j^{-1,+} \\ \deg\mathfrak{a}_j+\deg\alpha=k}} \frac{\beta^{(\mathfrak{a}_j,H^+/K)}}{\alpha D(\rho_{\mathfrak{a}_j})}(\rho_{\alpha\mathfrak{a}_j}(\mathbf{e}_A(b\mu)))^m$$

$$= \sum_{j=1}^{h^+} \sum_{\substack{\alpha\in\mathfrak{a}_j^{-1,+} \\ \deg\mathfrak{a}_j+\deg\alpha=k}} \frac{1}{D(\rho_{\alpha\mathfrak{a}_j})}((\alpha\mathfrak{a}_j)*(\beta Y^m))\Big|_{Y=\mathbf{e}_A(b\mu)}.$$

The sum goes over all ideals $J\subset A$ with $\deg J = k$. Hence this equals

$$\sum_{\deg J=k} \frac{J*(\beta Y^m)}{D(\rho_J)}\Big|_{Y=\mathbf{e}_A(b\mu)}.$$

Therefore, our whole series is the same as

$$\sum_{k=0}^{\infty}\left(\sum_{\deg J=k}\frac{J*(\beta Y^m)}{D(\rho_J)}\right)\Big|_{Y=\mathbf{e}_A(b\mu)} = l(\beta Y^m;z)|_{Y=\mathbf{e}_A(b\mu),z=1}.$$

By Anderson's log-algebraicity theorem VI.2, the formal power series

$$e_\rho(l(\beta Y^m;z))$$

is actually a polynomial in Y,z over $\mathcal{O}_{H^+}$. Hence as formal series,

$$\begin{aligned} l(\beta Y^m;z)|_{Y=\mathbf{e}_A(b\mu),z=1} &= \log_{v,\rho} S(\beta Y^m;z)|_{Y=\mathbf{e}_A(b\mu),z=1} \\ &= \sum_{n\geq 0} L_n(S(\beta Y^m;z)|_{Y=\mathbf{e}_A(b\mu),z=1})^{q^n}, \end{aligned}$$

where L_n are the coefficients of logarithm. To makes sense of this series, we need the right hand side to converge v-adically. By Lemma VI.4, $S(\beta Y^m;z)|_{Y=\mathbf{e}_A(b\mu),z=1}$ is an algebraic integer divisible by $\mathbf{e}_A(\mu)^m$. Since $\mathbf{e}_A(\mu)$ has positive v-adic valuation, so is $S(\beta Y^m;z)|_{Y=\mathbf{e}_A(b\mu),z=1}$.

Therefore, by Theorem V.2 the series converges v-adically to $\log_{v,\rho}(S(\beta Y^m; z)|_{Y=\mathbf{e}_A(b\mu)z=1})$. □

Following the method of Anderson, we are now able to prove the log-algebraicity of $L(1, \Psi)$ for elliptic curves and ramifying hyperelliptic curves.

Theorem VI.10. *$L_v(1, \Psi)$ is log-algebraic, i.e. there exists*

$$\alpha_1, \cdots, \alpha_s, S_1, \cdots, S_s \in \overline{K},$$

with $v(S_i) > 0$, such that

$$L_v(1, \Psi) = \sum_i \alpha_i \log_{v,\rho} S_i.$$

The α_i, S_i, s are the same as in log-algebraic theorem VI.6 for $L(1, \Psi)$.

Proof. The expression

$$\sum_{j=1}^{h^+} \beta^{(\mathfrak{a}_j, H^+/K)} l_{m,\mathfrak{a}_j}(b\mu)$$

we considered in Proposition VI.9 is precisely $S(\beta Y^m; z)_{Y=\mathbf{e}_A(b\mu),z=1}$. As in the proof of Theorem VI.6, let $\{\beta_1, \cdots, \beta_{h^+}\}$ be a K-linearly independent subset of $\mathcal{O}_{K(\rho[\mathfrak{p}])}$. By going through the same argument as the proof of Theorem VI.6 again, but doing everything v-adically, we arrive at the desired equality. □

CHAPTER VII
Examples and Possible Generalizations

VII.1: Examples

VII.1.1: $\mathbb{A} = \mathbb{F}_3[t,y]/(y^2-(t^3-t-1)), g=1, h=1$

([Hay79, 11.5], [Tha93, 2.3c], [GP18, 9.1], [Lut10, VIII.4]) Our first example is an elliptic curve over $\mathbb{F}_3$ with $h(\mathbb{A})=1$. Let $\mathbb{A}=\mathbb{F}_3[t,y]/(y^2-(t^3-t-1))$. Then $V=(\theta+1,\eta)$, and

$$f=\frac{y-\eta-\eta(t-\theta)}{t-(\theta+1)}.$$

The Hayes module is given by

$$\rho_t=\theta+\eta(\theta^3-\theta)\tau+\tau^2,\ \rho_y=\eta+\eta(\eta^3-\eta)\tau+(\eta^9+\eta^3+\eta)\tau^2+\tau^3.$$

Let v be place on K corresponding to the prime ideal $\mathfrak{p}:=(\theta)$. Fix $\sqrt{-1}\in\mathbb{F}_9$. This gives a character of conductor $\mathfrak{p}$ by $\chi: A\to\mathbb{F}_9$, $a(\theta,\eta)\mapsto a(0,\sqrt{-1})$. Let $\lambda\in K(\rho[\mathfrak{p}])$ be a primitive t-torsion point of ρ, i.e. a generator of $\rho[\mathfrak{p}]$ as an $\mathbb{A}$-module, and let $\lambda'=\rho_y(\lambda)$. In [Lut10, VIII.4], a log-algebraic formula of $L(1,\chi)$ is given as

$$L(1,\chi)=\frac{\log_\rho(\lambda')+\sqrt{-1}\log_\rho(\lambda)}{\lambda'+\sqrt{-1}\lambda},$$
$$L(1,\chi^3)=\frac{\log_\rho(\lambda')-\sqrt{-1}\log_\rho(\lambda)}{\lambda'-\sqrt{-1}\lambda}.$$

By Theorem VI.10, we obtain a log-algebraic formula for $L_v(1,\chi)$ given by the same

numbers.

$$L_v(1,\chi) = \frac{\log_{v,\rho}(\lambda') + \sqrt{-1}\log_{v,\rho}(\lambda)}{\lambda' + \sqrt{-1}\lambda},$$
$$L_v(1,\chi^3) = \frac{\log_{v,\rho}(\lambda') - \sqrt{-1}\log_{v,\rho}(\lambda)}{\lambda' - \sqrt{-1}\lambda}.$$

VII.1.2: $\mathbb{A} = \mathbb{F}_2[t,y]/(y^2+y+(t^5+t^3+1), g=2, h=1$

([Hay79, 11.6], [Tha93, 2.3d]) This is the only genus at least 2 example with $h(\mathbb{A}) = 1$ (cf. [LMQ75, Sti14]). Let $\mathbb{A} = \mathbb{F}_2[t,y]/(y^2+y+(t^5+t^3+1))$. Then $V = (\theta, \eta+1)+(\theta^2+1, \eta^2+\theta^4)$, and

$$f = \frac{y+\eta+(t+\theta)(\theta^4+\theta^3+\theta^2(t+1))}{t^2+(\theta^2+\theta+1)t+(\theta^3+\theta)}.$$

The Hayes module is given by

$$\rho_t = \theta + (\theta^2+\theta)^2\tau + \tau^2, \qquad \rho_y = \eta + y_1\tau + y_2\tau^2 + y_3\tau^3 + y_4\tau^4 + \tau^5,$$

where

$$\begin{aligned}
y_1 &= (\theta^2+\theta)(\eta^2+\eta)\\
y_2 &= \theta^2(\theta+1)(\eta^2+\eta)(\eta+\theta^3)(\eta+\theta^3+1)\\
y_3 &= \eta(\eta+1)(\theta^5+\theta^3+\theta^2+\theta+1)[(\theta^3+\theta^2+1)\eta+\theta^7+\theta^4+\theta^2]\\
&\quad [(\theta^3+\theta^2+1)\eta+\theta^7+\theta^4+\theta^3+1]\\
y_4 &= [\theta(\eta^2+\eta)(\theta^5+\theta^2+1)(\eta+\theta)(\eta+\theta+1)]^2.
\end{aligned}$$

To illustrate our Corollary IV.3 and V.3, we have factorized the first few coefficients of $\log_\rho$ as A-ideals.

$$\begin{aligned}
(l_1) &= (\theta)(\theta+1),\\
(l_2) &= (\theta)^{-1}(\theta+1)^{-1}(\theta^8+\theta^6+\theta^5+\theta^4+\theta^3+\theta+1),\\
(l_3) &= (\theta^2+\theta+1)^2(\theta^{10}+\theta^9+\theta^8+\theta^3+\theta^2+\theta+1),\\
(l_4) &= (\theta^2+\theta+1)^{-1}(\theta)^{-2}(\theta+1)^{-2}(\eta+\theta^2)(\eta+\theta^2+1)(\eta+\theta)(\eta+\theta+1)\\
&\quad (\eta+\theta^2+\theta)(\eta+\theta^2+\theta+1)(\eta+1)(\eta)\\
&\quad (\theta^{12}+\theta^9+\theta^8+\theta^6+\theta^3+\theta^2+1)(\theta^4+\theta+1).
\end{aligned}$$

As an illustration of Proposition V.1 and Corollary V.3, the primes (θ) and $(\theta+1)$, both

of degree 2, divide l_2^{-1} once and l_4^{-1} twice. It is worth noticing that Corollary V.3 predicts that (θ) and $(\theta+1)$ should also divide l_3^{-1} once, but they did not show up in the above factorization. This is because both of them get canceled by the terms coming from $V'^{(4)}$, equivalently $w(J'_{n+1})$ as in Proposition V.1.

VII.1.3: $\mathbb{A} = \mathbb{F}_3[t,y]/(y^2-(t^3+t^2+t), g=1, h=2$

([Hay79, 11.7], [GP18, 9.2], [Lut10, VIII.5]) The third example is a class number 2 elliptic curve over $\mathbb{F}_3$. Let $\mathbb{A} = \mathbb{F}_3[t,y]/(y^2-(t^3-t^2-t))$. We have $h(\mathbb{A})=2$, $H = K(\sqrt{\theta})$ and $\mathcal{O}_H = \mathbb{F}_3[\sqrt{\theta}, \frac{\eta}{\sqrt{\theta}}]$. We have to fix a Hayes module with respect to sgn. Set

$$\rho_t = \theta + (\sqrt{\theta} - \theta^{\frac{9}{2}} - \eta - \eta^3)\tau + \tau^2,$$

and ρ_y is determined uniquely from ρ_t by $\rho_t\rho_y = \rho_y\rho_t$. For this Hayes module, we have $V = (-\theta - 1 - \frac{\eta}{\sqrt{\theta}}, -\eta - \theta^{\frac{3}{2}} - \sqrt{\theta})$, and

$$f = \frac{y - \eta - (-\eta - \theta^{\frac{3}{2}} + \sqrt{\theta})(t-\theta)}{t + \theta + 1 + \frac{\eta}{\sqrt{\theta}}}.$$

We have that

$$\begin{aligned}
(l_1^{-1}) =& (\sqrt{\theta})(\frac{\eta}{\sqrt{\theta}} - 1, \theta+1)^{-1},\\
(l_2^{-1}) =& (\sqrt{\theta})^2(\frac{\eta}{\sqrt{\theta}} + \sqrt{\theta})(\frac{\eta}{\sqrt{\theta}} - \sqrt{\theta})(\frac{\eta}{\sqrt{\theta}} + 1, \theta+1)(\frac{\eta}{\sqrt{\theta}} - 1, \theta+1)\\
& (\sqrt{\theta}+1)(\sqrt{\theta}-1)(\frac{\eta}{\sqrt{\theta}})\left(\theta^2(\theta-1)^3\frac{\eta}{\sqrt{\theta}} + (\theta^5+\theta^3+\theta^2+1)\right)^{-1}
\end{aligned}$$

This time, the ideal coming from $\Xi^{(1)}$ is

$$(\theta^2-\theta, \eta^2-\eta) = (\sqrt{\theta}),$$

instead of (1), since $(\sqrt{\theta}) \cap A = (\theta)$ in A is of degree 2, not 1. As we can see, $(\sqrt{\theta})$ divides (l_2^{-1}) twice, matching the prediction from proposition V.2.

Let v be the place on K corresponding to the prime ideal $\mathfrak{p} := (\theta, \eta)$. Then ([Hay79, 11.7])

$$\rho_{\mathfrak{p}} = \left(1 + \theta + \frac{\eta}{\sqrt{\theta}}\right)^{-1}\sqrt{\theta} + \tau.$$

We define a character $\chi : A \to \mathbb{F}_3$ of conductor $\mathfrak{p}$ by $a(\theta,\eta) \mapsto a(0,0)$. Extend χ to a

character Ψ on the group of fractional A-ideals in K. Fix λ to be a primitive $\mathfrak{p}$-torsion point. An log-algebraic expression for $L(1,\Psi)$ is given by ([Lut10, VIII.5])

$$L(1,\Psi) = \left(\frac{D(\rho_{\mathfrak{p}})}{\sqrt{\theta}} - \frac{1}{\lambda}\right)\log_\rho S(X;1)_{X=\lambda} + \left(-\frac{\sqrt{D(\rho_{\mathfrak{p}}}}{\theta} - \frac{1}{\lambda\sqrt{\theta}}\right)\log_\rho S(\sqrt{\theta}X;1)_{X=\lambda}.$$

Lutes also computed the special polynomial $S(Y;z)$:

$$S(Y;z) = Yz + \left((-\eta-\sqrt{\theta})(\theta-1)Y^3 + Y\right)z^3 + \left(Y^9 + (\eta+\sqrt{\theta}(\theta-1)Y^3\right)z^9 - Y^9 z^{27}.$$

Once again, the same formula holds v-adically.

VII.1.4: $\widetilde{\mathrm{sgn}}(F) = 1$, but $\widetilde{\mathrm{sgn}}(F^{(1)})$ transcendental

Back in Remark II.15, we have promised an example of a function F with $\widetilde{\mathrm{sgn}}(F) = 1$, but $\widetilde{\mathrm{sgn}}(F^{(1)})$ transcendental over $\mathbb{F}_q$. Here we provide such an example: suppose $X = \mathbb{P}^1$ with function field $\mathbb{F}_q(t)$, and set $\overline{\infty}$ to be corresponding to $t - c$ for some $c \in \overline{\mathbb{F}_q}$. Fix sgn such that sgn of the minimal polynomial of ∞ is 1. Then the function

$$F = \frac{c - c^q}{c-\theta}\frac{t-\theta}{t-c^q}$$

has $\widetilde{\mathrm{sgn}}(F) = 1$. For $d_\infty > 2$, we have that

$$\widetilde{\mathrm{sgn}}(F^{(1)}) = \left(\frac{c-c^q}{c-\theta}\right)^q \frac{c-\theta^q}{c-c^{q^2}} = \frac{c^q - c^{q^2}}{c-c^{q^2}}\frac{c-\theta^q}{c^q-\theta^q},$$

which is transcendental over $\mathbb{F}_q$. If $d_\infty = 2$, then from

$$\widetilde{\mathrm{sgn}}((t-c)(t-c^q)) = 1,$$

we have that

$$\widetilde{\mathrm{sgn}}(t-c) = \frac{1}{c-c^q}.$$

Thus

$$\widetilde{\mathrm{sgn}}(F^{(1)}) = \left(\frac{c-c^q}{c-\theta}\right)^q (c-\theta^q)(c-c^q) = (c-c^q)^{q+1}\frac{c-\theta^q}{c^q-\theta^q},$$

which is also transcendental over $\mathbb{F}_q$.

VII.1.5: $X = \mathbb{P}^1$, any d_∞

To end our list of examples, we will have a glimpse on how the v-adic convergence should work for a general curve, by studying Hayes modules coming from $\mathbb{P}^1$ other than the Carlitz module.

We continue using the settings from the previous example VII.1.4. Let $X = \mathbb{P}^1$ with function field $\mathbb{F}_q(t)$. Set $\overline{\infty}$ to be the point corresponding to the place $t - c$ for some $c \in \overline{\mathbb{F}_q}$. This will only exclude the case with ∞ corresponding to the usual degree at t, which gives the well-understood Carlitz module.

Once again, fix sgn such that sgn of the minimal polynomial of ∞ is 1. A shtuka function f has divisor

$$\operatorname{div}(f) = V^{(1)} - V + (\Xi) - (\overline{\infty}^{(1)}),$$

and is given by

$$f = C\frac{t-\theta}{t-c^q},$$

where $C \in \mathbb{C}_\infty$ is a constant. Since

$$\widetilde{\operatorname{sgn}}(ff^{(1)}\cdots f^{(d_\infty-1)}) = 1$$

(see Remark II.15), we can compute that

$$C^{\frac{q^{d_\infty}-1}{q-1}} = \left((c-\theta)(c-\theta^q)\cdots(c-\theta^{q^{d_\infty-1}})\right)^{-1}.$$

We can also rewrite the shtuka functions as

$$f = U\frac{1}{c-\theta}\frac{t-\theta}{t-c^q},$$

where

$$U^{\frac{q^{d_\infty}-1}{q-1}} = \frac{(c-\theta)^{\frac{q^{d_\infty}-q}{q-1}}}{(c-\theta^q)\cdots(c-\theta^{q^{d_\infty-1}})}.$$

The advantage of writing f in this way is that as an element in H, the $\dfrac{q^{d_\infty}-1}{q-1}$-th power of U only has nonzero valuation at places above ∞ (as in K, not $\mathbb{K}$). The notation U comes from the fact that the $\dfrac{q^{d_\infty}-1}{q-1}$-th power of U is a unit in $\mathcal{O}_H$. In particular, U has valuation zero at the place above "degree in θ", which is not true for C. This will help us to compute the v-adic convergence of e_ρ and $\log_\rho$ for v to be the place "degree in θ".

Now fix such a U (out of the choice of a $\frac{q^{d_\infty}-1}{q-1}$-th root of unity). The exponential series for the Hayes module corresponding to this choice is given by

$$\begin{aligned} e_\rho(z) &= z + U^{-1}(c-\theta)\frac{(\theta-c)^q}{\theta^q-\theta}z^q \\ &\quad + U^{-(q+1)}(c-\theta)^{1+q}\frac{(\theta^q-c)^q(\theta-c)^{q^2}}{(\theta^{q^2}-\theta)(\theta^q-\theta)^q}z^{q^2}+\cdots \\ &= z - \sum_{n=1}^{\infty} U^{-\frac{q^n-1}{q-1}}(c-\theta)^{\frac{q^{n+1}-1}{q-1}} \\ &\qquad \cdot \frac{(\theta^{q^{n-1}}-c)^q(\theta^{q^{n-2}}-c)^{q^2}\cdots(\theta^q-c)^{q^{n-1}}}{(\theta^{q^n}-\theta)(\theta^{q^{n-1}}-\theta)^q\cdots(\theta^q-\theta)^{q^{n-1}}}z^{q^n}. \end{aligned}$$

The differential $\omega \in H^0(\overline{X}, \Omega^1(V-(\overline{\infty})-(\overline{\infty}^{(-1)})))$ as in Definition II.19 and [Tha93, 0.3.7] (also see Remark II.21) is given by

$$\omega^{(1)} = -U\frac{dt}{(t-c^q)(t-c)},$$

and the logarithm series is given by

$$\begin{aligned} \log_\rho(z) &= z + U^{-1}(c-\theta)\frac{(\theta-c)^q}{(\theta-\theta^q)}z^q \\ &\quad + U^{-(q+1)}(c-\theta)^{1+q}\frac{(\theta-c)^{q^2}(\theta-c^q)}{(\theta-\theta^q)(\theta-\theta^{q^2})}z^{q^2}+\cdots \\ &= z - \sum_{n=1}^{\infty} U^{-\frac{q^n-1}{q-1}}(c-\theta)^{\frac{q^{n+1}-1}{q-1}} \\ &\qquad \cdot \frac{(\theta-c^q)(\theta-c^{q^2})\cdots(\theta-c^{q^{n-1}})}{(\theta-\theta^q)(\theta-\theta^{q^2})\cdots(\theta-\theta^{q^n})}z^{q^n}. \end{aligned}$$

From the calculation we have done in Chapter V, namely Corollary V.3, we can see that if v is a place of $\mathbb{P}^1$ away from ∞ and the one corresponding to deg on θ, then

- $e_\rho(z)$ converges in $\mathbb{C}_v$ for all $w(z) > e_w\frac{1}{q^{\deg \mathfrak{p}}-1}$, where w, e_w are as in section V;
- $\log_\rho(z)$ converges in $\mathbb{C}_v$ for all $v(z) > 0$.

For v corresponding to degree in θ, we can directly compute the valuation. Let w be a place in $H^+ := H(U)$ above v, and e_w the ramification index of w over v. Then

$$w(e_n) = -e_w\frac{q^n-1}{q-1} > -e_w q^n\frac{1}{q-1},$$

$$w(l_n) = -e_w n,$$

by looking at the degree in θ of the coefficients. This shows that the v-adic convergence behavior of $e_\rho(z)$ and $\log_\rho(z)$ is the same also when v is the "degree in θ". This gives evidence to the general v-adic convergence behavior of e_ρ and $\log_\rho$ in the case when $d_\infty > 1$.

VII.2: Possible directions for generalization

Before we end this thesis, we present a few possible directions for generalizing results in this paper.

VII.2.1: A conjecture for the general case

From the previous $\mathbb{P}^1$ example and Theorems V.2 and V.3, we formulate the following conjecture that predicts the general v-adic convergence for e_ρ and $\log_\rho$.

Conjecture VII.2.1. *Let ρ be a Hayes module on X, with no restriction on genus X or d_∞. Fix a place v of X the same as ∞. Let* Frac$R$ *be the field extension of H^+ containing all zeros of the Drinfeld divisor V corresponding to ρ. Let w be the place (normalized so the value group is $\mathbb{Z}$) in* Frac$R$ *over v upon a fixed embedding $\overline{K} \to \overline{K}_v$, and e_w the ramification index of w over v. Then:*

1. *the exponential series $e_\rho(z)$ converges in $\mathbb{C}_v$ when*

$$w(z) > w(J_0) + e_w \cdot e_\theta \cdot \frac{1}{q^{\frac{\deg \mathfrak{p}}{f_\theta}} - 1},$$

   where J_0 is some ideal coming from V evaluated at Ξ, e_θ is some number coming from ramification, and f_θ is some number coming from intertia;

2. *the logarithm series $\log_\rho(z)$ converges in $\mathbb{C}_v$ when $v(z) > 0$. Moreover, the coefficients of logarithm should have v-adic valuation in the order of $O(n)$.*

An immediate difficulty that we face when trying to prove this conjecture is that it is hard to explicitly write down

1. the shtuka function f with a nice integral model, with all zeros being integral;
2. the differential ω in terms of the shtuka function f.

In particular, the way we obtain the good presentation for the shtuka functions f for elliptic curves and ramifying hyperelliptic curves is via long division, which requires that

there is a degree 2 element in $\mathbb{A}$. Obviously this does not have to be true in general. For instance this will fail immediately when $d_\infty \geq 3$. In the general case, long division can still be done, but the result will no longer be in terms of integral functions, needless to say $\widetilde{\text{sgn}}$ 1 functions. It also becomes hard to keep track of the relations of the generators in a model for $\mathbb{A}$, when there are more than 2 generators and/or more than 1 relation.

VII.2.2: Higher dimension

It has been shown by Anderson and Thakur [AT90, 2.4.1] that for the n-th tensor of Carlitz module $C^{\otimes n}$, the logarithm series $\text{Log}_n(z)$ converges v-adically for all $z \in \mathbb{C}_v^n$ with $v(z) > 0$, and they used the convergence to calculate the values $\zeta_v(n)$. In [CM17, Theorem 3.3.3], Chang and Mishiba showed a generalization for some uniformizable t-modules. As for elliptic curves with ∞ as the rational point at infinity, Green has given an expression of coefficients of the logarithm series for the n-tensor power of a Hayes module in his thesis [Gre18, Theorem 4.2.4]. A work in progress of the author is to prove a similar v-adic convergence result on the tensor product, which can be used to calculate v-adic zeta values.

VII.2.3: Other L-series

It is also worth mentioning that Green and Papanikolas [GP18] studied the shtuka functions for elliptic curves and come up with another formula for $L(1, \chi)$, as a special case for a formula for Pellarin L-series [Pel12]. It would be an exciting idea to see if we can come up with similar v-adic results for Pellarin L-series [Pel12].

BIBLIOGRAPHY

[And96] Greg W. Anderson. Log-algebraicity of twisted a-harmonic series and special values of L-series in characteristic p. *Journal of Number Theory*, 60(1):165–209, 1 1996.

[ANDTR17] Bruno Anglès, Tuan Ngo Dac, and Floric Tavares Ribeiro. Special functions and twisted l-series. *Journal de Théorie des Nombres de Bordeaux*, 29(3):931–961, 2017.

[AT90] Greg W. Anderson and Dinesh S. Thakur. Tensor powers of the carlitz module and zeta values. *Annals of Mathematics*, 132(1):159–191, 1990.

[Car35] Leonard Carlitz. On certain functions connected with polynomials in a galois field. *Duke Math. J.*, 1(2):137–168, 06 1935.

[CM17] Chieh-Yu Chang and Yoshinori Mishiba. On Multiple Polylogarithms in Characteristic p: v-Adic Vanishing Versus ∞-Adic Eulerianness. *International Mathematics Research Notices*, 2019(3):923–947, 07 2017.

[Dri74] Vladimir G. Drinfel'd. Elliptic modules. *Mathematics of the USSR-Sbornik*, 23(4):561–592, apr 1974.

[Dri77] Vladimir G. Drinfel'd. Commutative subrings of certain noncommutative rings. *Functional Analysis and its applications*, 11:9–12, 1977.

[Dri87] Vladimir G. Drinfel'd. Varieties of modules of f-sheaves. *Functional Analysis and its applications*, 21:107–122, 1987.

[Gos78] David Goss. von staudt for $\mathbb{F}_q[T]$. *Duke Mathematical Journal*, 45(4):885–910, December 1978.

[Gos79] David Goss. v-adic zeta functions,L-series and measures for function fields. *Inventiones mathematicae*, 55(2):107–116, Jun 1979.

[Gos80] David Goss. π-adic eisenstein series for function fields. *Compositio Mathematica*, 41(1):3–38, 1980.

[Gos92] David Goss. L-series of t-motives and drinfel'd modules. In David Goss, David R. Hayes, and Michael I. Rosen, editors, *The Arithmetic of Function Fields : Proceedings of the Workshop at the Ohio State University, June 17-26 1991*, pages 313–402. De Gruyter, Berlin/Boston, 1992.

[Gos98] David Goss. *Basic structures of function field arithmetic*. Springer, 1998.

[GP18] Nathan Green and Matthew A. Papanikolas. Special L-values and shtuka functions for drinfeld modules on elliptic curves. *Research in the Mathematical Sciences*, 5(1):4, Jan 2018.

[Gre18] Nathan Green. *Tensor powers of Drinfeld modules and zeta values*. PhD thesis, Texas A&M University, 2018.

[Har13] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer New York, 2013.

[Hay74] David R. Hayes. Explicit class field theory for rational function fields. *Transactions of the American Mathematical Society*, 189:77–91, 1974.

[Hay79] David R. Hayes. Explicit class field theory in global function fields. *Studies in algebra and number theory*, pages 173–217, 1979.

[Kob84] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer-Verlag New York, 2 edition, 1984.

[LMQ75] James R.C. Leitzel, Manohar L. Madan, and Clifford S. Queen. Algebraic function fields with small class number. *Journal of Number Theory*, 7:11–27, 1975.

[Lut10] Brad Lutes. *Special values of the Goss L-function and special polynomials*. PhD thesis, Texas A&M University, 2010.

[Mac71] R.E MacRae. On unique factorization in certain rings of algebraic functions. *Journal of Algebra*, 17(2):243 – 261, 1971.

[Mum77] David Mumford. An algebro-geometric construction of commuting operators and of solutions to the toda lattice equation , korteweg devries equation and

related non-linear equations. *Proceedings of the International Symposium on Algebraic Geometry*, pages 115–153, 1977.

[Pel12] Federico Pellarin. Values of certain L-series in positive characteristic. *Annals of Mathematics*, 176(3):2055–2093, 2012.

[Per13] Rudolph B. Perkins. What is anderson's log-algebracity. https://math.osu.edu/sites/math.osu.edu/files/LogAlgebraicity.pdf, 2013.

[Sti14] Claudio Stirpe. A counterexample to 'algebraic function fields with small class number'. *Journal of Number Theory*, 143:402 – 404, 2014.

[Tae12] Lenny Taelman. Special L-values of drinfeld modules. *Annals of Mathematics*, 175(1):369–391, 2012.

[Tha92] Dinesh S. Thakur. Drinfel'd modules and arithmetic in the function fields. *International Mathematics Research Notices*, 1992(9):185–197, 05 1992.

[Tha93] Dinesh S. Thakur. Shtukas and jacobi sums. *Inventiones mathematicae*, 111:557–570, 1993.

[Tha04] Dinesh S. Thakur. *Function Field Arithmetic*. World Scientific Publishing, 2004.

[Tha20] Dinesh S. Thakur. updates. https://web.math.rochester.edu/people/faculty/dthakur2/updates.pdf, 2020. Accessed: 2020-10-1.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*. Springer, 2nd edition, 1997.