INAUGURAL-DISSERTATION

zur Erlangung der Doktorwürde der

Naturwissenschaftlich-Mathematischen Gesamtfakultät

der Ruprecht-Karls-Universität Heidelberg

vorgelegt von

M.Sc. Yujia Qiu

aus Quzhou, China

Tag der mündlichen Prüfung: ______________

Thema

On the zero Distribution of Special Values of Goss zeta Functions

Gutachter: Prof. Dr. Gebhard Böckle

Abstract

In this dissertation we deal with the distribution of zeros of special values of Goss zeta functions. Firstly, we prove an analogue of Riemann hypothesis for curves defined over prime field of arbitrary genus as well as for curves defined over $\mathbb{F}_q$ with $q \neq p$ whose genus is bounded by $(p+q)/2$. Secondly, we prove some results on partial zeta functions. Thirdly, we apply the cohomological method to a specified curve and prove an analogue of Riemann hypothesis for certain n. Finally, we set up a relation between the ∞-adic and v-adic zeta functions.

Zusammenfassung

In dieser Doktorarbeit wird die Verteilung der Nullstellen der speziellen Werte der Goss Zeta-Funktionen untersucht. Zuerst beweisen wir ein Analogon der Riemannschen Vermutung für Kurven von beliebigem Geschlecht, die über einem Primkörper definiert werden, sowie für Kurven definiert über $\mathbb{F}_q$ von Charasteristik p, deren Geschlecht nicht größer als $(p+q)/2$ ist. Zweitens beweisen wir einige Resultate für partielle Zeta-Funktionen. Drittens wenden wir die kohomologische Theorie der Kristalle auf eine gegebene Kurve an, um ein Analogon der Riemannschen Vermutung für n, die eine spezielle Form besitzen, zu beweisen. Schließlich geben wir einen Zusammenhang zwischen den ∞-adischen und den v-adischen Zeta-Funktionen an.

一生二
二生三
三生万物
-----老子《道德经》

真·善·美
天·地·人
宇宙·素数·ζ
-----加藤和也 Kazuya Kato

Acknowledgements

I am very grateful to my supervisor Professor Gebhard Böckle, for his constant support, who is indispensable for the completion of this dissertation.

I also want to thank Professor Dinesh Thakur, for being the second referee of my thesis and the helpful discussion held in London.

I also would like to thank the Heidelberg University and the Faculty of mathematics and computer science for offering me the chance to study in this beautiful city. I am also very grateful for the LGFG scholarship.

Last but not the least, my most heartfelt thanks go to my friends who have offered me so much help during my study and life here. I would like to thank my husband Heer Zhao for his support from all aspects and Jochem Berndsen for a careful proofreading of my thesis. I also owe thanks to my fellow students, Ann-Kristin Juschka, Yamidt Bermudez Tobon, Konrad Fischer, David-Alexandre Guiraud, Özge Ülkem and Peter Gräf. I would like to thank Dr. Andreas Maurischat for his help in latex, Magma as well as my life in Heidelberg.

Contents

1. Introduction

1.1 Motivation

The study of Riemann zeta function dates back to the first half of the nineteenth century when it was introduced and studied by Leonhard Euler even before the development of complex analysis. It was named after Bernhard Riemann due to his memoir "Über die Anzahl der Primzahlen unter einer gegebenen Größe" in 1859, in which he extended Euler's definition to a complex variable and proved its meromorphic continuation and functional equation, as well as established a relation between its zeros and the distribution of prime numbers. The Riemann zeta function, usually denoted by $\zeta(s)$ is defined to be a function of a complex variable s that analytically continues the infinite series

$$\sum_{n=1}^{\infty} n^{-s},$$

which converges when the real part of s is greater than 1. It has a simple pole at $s = 1$ and trivial zeros at negative even integers.

The famous Riemann hypothesis, proposed in the above memoir by Riemann, asserts that any non-trivial zero of the Riemann zeta function lies on the critical line, i.e., has real part equal to 1/2. It has huge impacts on the development of number theory, for example, as already been observed by Riemann, the distribution of its zeros has a close relation to that of the prime numbers. Lots of mathematicians, including Hardy, Littlewood and Selberg, made significant contributions to the very problem. Although the Riemann hypothesis remains unproved in the classical case, progress has been made in some analogues of it, for example, the Riemann hypothesis for varieties over finite fields was proved by Deligne in 1974. The Goss zeta functions, which are analogues of Riemann zeta function in function field case, were also shown to satisfy the analogous Riemann hypothesis by Wan in the case of projective lines over prime fields and Sheats in the case of general projective lines. In this thesis, we will try to extend the result to the function field of more general curves.

Algebraic function fields over finite fields represent a striking analogy with algebraic number fields, i.e., finite extensions of the field of rational numbers $\mathbb{Q}$. They often serve as an important model of the theory of algebraic number fields. So it is a natural question to ask whether there exists a nice analogue of Riemann hypothesis for function fields and, if so, whether we can get our hands on it. As a first step, in his book [Gos98], Goss defined function field analogues of classical L-functions and zeta functions, for instance the Carlitz zeta function, or the L-function attached to a Drinfeld module in analogy to that of an elliptic curve. More details can be found in [Gos98]. In their book [BP09], Böckle and Pink associated a global L-function to a flat crystal. In particular, for the crystals associated to Drinfeld modules, this gives a new way to study Goss L-functions.

As in the classical situation, the special values of a Goss zeta function may reveal lots of facts concerning function field arithmetic which we are interested in. Goss, Wan, Diaz-Vargas and various mathematicians working on this field developed an analogue of the Riemann hypothesis in the function field setting. A Goss L-function is a continuous map from $\mathbb{Z}_p$ to a ring of power series, and the Riemann hypothesis is an assertion on the distribution of the zeroes of these power series. The special values of Goss zeta functions at negative integers are polynomials, and the main subject we will study in this dissertation is the zero distribution of these polynomials.

The investigation into the distribution of the zeros of special values of Goss zeta functions, also known as the Riemann hypothesis of positive characteristic, dates back to 1990's when D. Wan in [Wan96], J. Diaz-Vargas in [DV96] and J. Sheats in [She98] completed the problem for all rational function fields over a finite field and a chosen rational point. In [Gos00], D. Goss gave an interpretation of the analogue of the classical Riemann hypothesis, focusing on the distribution of the zeros. Although predicted by Wan in [Wan96] that it should be possible to refine and generalize this method to general A with a rational ∞ point, there was no further success in this direction. However, as we will mention in Chapter 5, G. Böckle solved the problem for the curve defined by $y^2+y=x^3+x+1$ over $\mathbb{F}_2$ with an $\mathbb{F}_2$-rational infinite point with the help of cohomological method, see [Böc13]. In particular, this method provides us a polynomial time algorithm. More details will come up in Chapter 5.

1.2 Structure of the thesis

Let $\mathcal{C}$ be a smooth projective geometrically irreducible curve over a finite field $\mathbb{F}_q$. It is easy to show that the set of rational functions on $\mathcal{C}$ is a field of transcendental degree one over $\mathbb{F}_q$, i.e., a global function field, denoted by K. As an example, the function field of the projective line over $\mathbb{F}_q$ is isomorphic to $\mathbb{F}_q(t)$ with t transcendental over $\mathbb{F}_q$. This is the analogue of the field of rational numbers $\mathbb{Q}$. There is a one-to-one correspondence between global function fields over $\mathbb{F}_q$ and smooth projective geometrically irreducible curves over the same finite field. Let ∞ be a fixed place of the function field, and by A we denote the ring of elements in K which are regular away from ∞, i.e., $A := \Gamma(\mathcal{C} - \{\infty\}, \mathcal{O}_{\mathcal{C}})$. We define K_∞ to be the completion of K at ∞, and $\mathbb{C}_\infty$ to be the completion of an algebraic closure of K_∞. Note that K_∞ is the analogue of $\mathbb{R}$ and $\mathbb{C}_\infty$ is that of $\mathbb{C}$. It is necessary to point out here that this is quite different from the number field case where the algebraic closure of a number field completed at an infinity place is already complete. For instance, when taking $\mathcal{C}$ to be the projective line $\mathbb{P}^1$ over $\mathbb{F}_q$, the function field K is $\mathbb{F}_q(t)$, the field of rational functions in one variable. Furthermore if ∞ denotes the place defined by $1/t$, then A is $\mathbb{F}_q[t]$, the ring of polynomials, and K_∞ is $\mathbb{F}_q((1/t))$, the field of Laurent series over $\mathbb{F}_q$.

We can define the ∞-*adic Goss zeta function*, which, after renormalisation, can be interpolated as power series:

$$\zeta_A(-n, T) = \sum_{d \geq 0} T^d \cdot \left(\sum_{\substack{\mathfrak{a} \in \mathcal{I}^\infty, \mathfrak{a} \subset A \\ \deg_\infty(\mathfrak{a}) = d}} \mathfrak{a}_\infty^n \right),$$

where n is an integer, $\mathcal{I}^\infty$ is the group of all nonzero fractional ideals of A and the ∞-adic exponentiation $\mathfrak{a}_\infty^n$ of an ideal $\mathfrak{a}$ is as defined in Section 2.3.1.1. We define also the ∞-adic Goss-Thakur zeta function, where, instead of summing up the exponentiations of all ideals, we consider only the principal ideals, i.e.,

$$\zeta_A(-n, T) = \sum_{d \geq 0} T^d \cdot \left(\sum_{a \in A_{+,d}} a^n \right)$$

where $A_{+,d}$ denotes the subset of A consisting of the elements which are positive with respect to certain sign function and of degree d. If $A = \mathbb{F}_q[t]$, then the set $A_{+,d}$ contains all polynomials in A which are monic and of degree d. Clearly the Goss zeta function and Goss-Thakur zeta function coincide when A has strict class number 1. Although defined to be power series, thanks to Theorem 1 in [Tha95], the value of Goss zeta function at any negative integer is in fact a polynomial.

Furthermore, Thakur also gives an explicit upper bound of the degree of this polynomial. On the other hand, after fixing a place v of K which is different from ∞, we can define the *v-adic Goss zeta function* as

$$\zeta_A^{(v)}(-n,T) := \sum_{d\geq 0} T^d \cdot \left(\sum_{\substack{\mathfrak{a}\in\mathcal{I}^{\infty,\{v\}},\mathfrak{a}\subset A \\ \deg_\infty(\mathfrak{a})=d}} \mathfrak{a}_{\infty,v}^n \right),$$

where n is an integer, $\mathcal{I}^{\infty,\{v\}}$ consists of all nonzero fractional ideals in $\mathcal{I}^\infty$ which are prime to v and the v-adic exponentiation $\mathfrak{a}_{\infty,v}^n$ of an ideal $\mathfrak{a}$ is as defined in Section 2.3.1.2. Similarly, we also have v-adic Goss-Thakur zeta functions.

In his 1998 paper [She98], Sheats proved the following theorem for $A = \mathbb{F}_q[t]$:

Theorem 1.2.1. *Fix $n \in \mathbb{Z}_p$. As a function in T, the zeros of $\zeta_A(-n,T)$ are simple and lie in K_∞. In fact, they have pairwise distinct valuations and lie in the subfield $\mathbb{F}_p((t^{-1}))$.*

The main tool he used to study the zero distributions is via Newton Polygons associated to the power series, or in this case, polynomials, which is a piecewise linear function from $\mathbb{R}$ to $\mathbb{R}$ and provides us insights on the valuations of the zeroes of the power series. By associating a weight to any vector in $\mathbb{N}^s$, he turned the problem into the uniqueness of the optimal element in certain subset of $\mathbb{N}^s$. With the help of some combinatorical tools, he successfully proved the above theorem. In Chapter 3, we will apply this method to a wider generality. To be more precise, for any $i = 0, 1, \ldots$, let φ_i be the smallest integer n such that the dimension of the Riemann-Roch space $L(n\infty)$ is $i+1$, and $\tilde{\varphi}_j := \varphi_{j+1} - \varphi_j$. Let $U_m(n)$ consist of valid compositions of length m, as defined in Definition 3.2.7. We call an element in $U_m(n)$ greedy if it is in reverse order lexicographically largest, and an element optimal if it has the maximal weight, as in Definition 3.2.6. We prove the following theorem:

Theorem 1.2.2 (Theorem 3.3.2, Theorem 3.5.7)**.** *Suppose that either $p = q$ or $p \neq q$ and $g \leq \frac{p+q}{2}$. Let n be a fixed positive integer. The following holds:*

(a) The x-coordinates of the break points of the Newton polygon associated to $\zeta_A(-n,T)$ are φ_i for all $i = 0, 1, \ldots$.

(b) The slope of the i-th segment between φ_{i-1} and φ_i is G_i^i, where G_i^i appears as the last entry of the greedy element in $U_{i+1}(n)$. In particular, the sequence $\{G_1^1, G_2^2, G_3^3, \ldots\}$ is strictly increasing.

Let $m \leq g$ be the smallest positive integer such that $\tilde{\varphi}_i = 1$ for all $i > m$. Except for the φ_m zeros of lowest valuations, all other zeros of $\zeta_A(-n, T)$ are simple with pairwise distinct valuations.

As a part of this chapter, we also consider some examples, among which are hyperelliptic curves and curves of strict class number one. The examples suggest that it is possible to improve the upper bound of the genus to $O(q^2)$. They also suggest that we cannot expect to solve the problem completely by this method.

In Chapter 4, we will consider the special values of the partial Goss zeta functions. Suggested by numerical experiments, the zeros of special values of partial Goss zeta functions behave in a nice pattern. We only consider the case when $A = \mathbb{F}_q[t]$ and the degree of place v is either 1 or 2. Let Γ be a function from $\mathbb{N}$ to $\mathbb{N}^s$, sending any n to a vector $(t_0, t_1, \ldots, t_{s-1})$ such that $t_i = \sum_{j \equiv i \pmod{s}} n_j$ with $n = \sum_j n_j p^j$ the p-adic expansion of n. Let I_m be a set of vectors consisting of $\Gamma(n)$ where n has a valid composition of length m, as defined in Definition 3.4.8. When v is of degree 1, we prove the following theorem:

Theorem 1.2.3 (Theorem 4.2.7)**.** *Suppose that both ∞ and v are $\mathbb{F}_q$-rational places. Let n be any positive integer and $\bar{b}$ be a nonzero congruent class with respect to v.*

(a) All segments of the Newton polygon associated to $\zeta_{\mathbb{F}_q[t]}(-n, T, \bar{b})$ have width 1.

(b) The d-th slope is $\sum_{j=1}^{d-1} G_{m-j}$ where m is defined such that $\Gamma(n) \in I_m \backslash I_{m+1}$ and $G = (G_0, \ldots, G_{m-1}, 0)$ is the t-greedy element in $V_m(n)$.

In particular, all zeros of $\zeta_{\mathbb{F}_q[t]}(-n, T, \bar{b})$ have pairwise distinct valuations at v. Hence they are all simple.

When v is of degree 2, we present a recursive formula and apply it to the case when $q = 2$ in Section 4.3.1; and in Section 4.3.2, we investigate instead the valuation of $\tilde{S}(n) := 1 + \sum_{a \in \mathbb{F}_q} (t + a)^n$ which appears in the expansion of the coefficients of partial Goss zeta functions. Theorem 4.3.9 provides a close formula to the valuations as well as the leading terms of $\tilde{S}$'s.

In Chapter 5, we apply the cohomological method to the curve defined by $y^2 = x^3 - x - 1$ over $\mathbb{F}_3$, which is one of the only four non-trivial curves of class number 1 with a rational point, see [Hay79]. We prove the following theorem for this particular curve:

Theorem 1.2.4 (Corollary 5.4.4)**.** *Let $n = \sum_{i=1}^{l} 2 \cdot 3^{n_i}$ with $n_1 < n_2 < \ldots < n_l$. The slopes of the Newton polygon of $z_A(-n, T)$ are:*

$$2 \cdot 3^{n_1},\ 2 \cdot 3^{n_1},\ 2 \cdot 3^{n_1} + 2 \cdot 3^{n_2},\ 2 \cdot 3^{n_1} + 2 \cdot 3^{n_2} + 2 \cdot 3^{n_3},\ \ldots,$$

in increasing order. In particular, apart from the first slope, all slopes occur with multiplicity 1.

Note that although this particular case is treated in Example 3.6.5, even in more generality, we hope this method can provide a polynomial time algorithm.

In Chapter 6, we compare the ∞-adic with v-adic zeta functions. By setting up a joint uniformizer at both places ∞ and v, we can compare the ∞-adic with v-adic zeta functions twisted by a character. Denote by $\mathcal{J}^{\infty,\{v\}}$ (resp. $\mathcal{J}^{v,\{\infty\}}$) be the group of nonzero fractional ideals of A^∞ (resp. A^v) which are prime to v (resp. ∞). Then we can define $\zeta_{A^v}^{\{\infty\}}$ and $\zeta_{A^\infty}^{\{v\},(v)}$ and their renormalisations $z_{A^v}^{\{\infty\}}$ and $z_{A^\infty}^{\{v\},(v)}$ as in Section 6.4. We have the following result:

Theorem 1.2.5. *(a) There exists a natural isomorphism $\phi : \mathcal{J}^{\infty,\{v\}} \to \mathcal{J}^{v,\{\infty\}}$.*

(b) Let (χ, χ') be any pair of characters such that the diagram

$$\begin{tikzcd}
\mathcal{J}^{\infty,\{v\}} \arrow[r, "\chi"] \arrow[d, "\phi"'] & K^{\mathrm{alg}} \\
\mathcal{J}^{v,\{\infty\}} \arrow[ur, "\chi'"'] &
\end{tikzcd} \tag{1.1}$$

commutes. Let $\tilde{\omega} : \mathcal{J}^{\infty,\{v\}} \to \mathbb{F}_q^{\mathrm{alg}}$ be the character of finite order sending any $\mathfrak{a}$ to $\omega(\sigma(\mathfrak{a}_\infty^1))$ with ω as in the definition of v-adic exponentiation of an ideal. Then we have:

$$z_{A^v}^{\{\infty\}}(-n, T, \varphi(\mathfrak{a}) \pmod{\mathfrak{J}'}, \chi') = z_{A^\infty}^{\{v\},(v)}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi\tilde{\omega}^{-1})$$

for any $\mathfrak{a} \in \mathcal{J}^{\infty,\{v\}}$.

In Section 6.5, we have more general results where the sets $\{\infty\}$ and $\{v\}$ are substituted by some more general ones.

2. Drinfeld Modules and Goss Zeta Functions

In this chapter, we provide the readers some background on Drinfeld modules and Goss zeta functions.

2.1 Notation and Basic Definitions

Through out the dissertation, we fix the following notation.

- Denote by $\mathbb{N}$ the set of non-negative integers.
- Fix a prime number p. Given a positive integer n, let $n = \sum_{i=0}^{l} n_i p^i$ be the base p expansion of n, i.e., for $0 \leq i \leq l$, we have $0 \leq n_i \leq p-1$, and $n_l \neq 0$. Then we define the p-degree of n as $\deg_p(n) := l = \lfloor \log_p(n) \rfloor$, and the p-digit sum of n as $\operatorname{digsum}_p(n) := \sum_{i=0}^{l} n_i$. We sometimes drop the index p if it is clear from the context.
- We denote by $\mathcal{C}$ a smooth projective, geometrically irreducible curve over a finite field $k := \mathbb{F}_q$ of characteristic p, where $q = p^s$. The function field of $\mathcal{C}$ is denoted by K.
- We denote a fixed infinite place of $\mathcal{C}$ by ∞. Note that here we do not assume that ∞ is $\mathbb{F}_q$-rational, and the degree of ∞ is denoted by d_∞. Set $A := H^0(\mathcal{C} - \{\infty\}, \mathcal{O}_{\mathcal{C}})$. We denote by K_∞ the completion of K with respect to ∞, and its ring of integers is denoted by $\mathcal{O}_\infty$. Set $k_\infty := \mathcal{O}_\infty / \mathfrak{m}_\infty$ where $\mathfrak{m}_\infty$ is the maximal ideal of $\mathcal{O}_\infty$. The completion of the algebraic closure of K_∞ is again algebraically closed, denoted by $\mathbb{C}_\infty$. By [NX02, Proposition 1.2.5], the class number of A is hd_∞, where h is the class number of K. The tuple (K, ∞, A) plays a role as analogous to $(\mathbb{Q}, \infty, \mathbb{Z})$.

- For a nonzero ideal $\mathfrak{a}$ of A, we define the ∞-degree of $\mathfrak{a}$ to be $\deg_\infty(\mathfrak{a}) := \log_q(|A/\mathfrak{a}|)$. For an element $\alpha \neq 0$ in A, the ∞-degree of α is defined to be $\deg_\infty((\alpha))$. This definition extends to the fractional ideals of A by setting $\deg_\infty(a/b) = \deg_\infty(a) - \deg_\infty(b)$ and $\deg_\infty(0) = 0$. We sometimes drop ∞ if it is clear from the context.

- Fix a uniformizer π_∞ of the place ∞, and fix a d_∞-th root of it, denoted by $\pi_{\infty,*}$.

- A sign function sgn_∞ is an $\mathbb{F}_q$-homomorphism from K_∞^* to k_∞^*. We call an element f *positive at* ∞ or ∞*-positive* if and only if $\mathrm{sgn}_\infty(f) = 1$, and the set of such elements in $A\backslash\{0\}$ is denoted by A_{+_∞}, or A_+ if no confusion is caused. Denote by $A_{+_\infty,d}$ the set of ∞-positive elements of ∞-degree d. With respect to a chosen sign function, the strict class number is $hd_\infty(q^{d_\infty} - 1)/(q-1)$. Fixing a uniformizer π_∞ at ∞, we can define the corresponding sign function by sending $\pi_\infty^n \cdot u$ with u in $\mathcal{O}_\infty^*$ to $u \bmod \pi_\infty$.[1]

Example 2.1.1. If we choose the curve $\mathcal{C}$ to be the projective line over $\mathbb{F}_q$, then K is $\mathbb{F}_q(t)$, the field of rational functions in one variable over $\mathbb{F}_q$. Choose the infinite place ∞ to be the "usual" infinite place $(1/t)$, then A is the polynomial ring $\mathbb{F}_q[t]$, K_∞ is $\mathbb{F}_q((t^{-1}))$, the field of Laurent series in $1/t$ and $\mathcal{O}_\infty$ is just $\mathbb{F}_q[[t^{-1}]]$. The ∞-degree of any $\alpha \in A$ is just its degree as a polynomial in t. If we choose a uniformizer at ∞ to be $1/t$, then the canonical sign homomorphism sends any $\alpha \in A$ to its leading coefficient, which means that A_{+_∞} contains all the monic polynomials over $\mathbb{F}_q$.

2.2 Drinfeld A-Modules

Drinfeld modules, named after Vladmir Drinfeld, were first introduced under the name 'elliptic modules' in [Dri74] by Drinfeld. The name 'elliptic module' comes from the analogy with elliptic curve, which we will briefly introduce here. An elliptic curve over an algebraically closed field k can be defined as a variety of dimension 1 equipped with a $\mathbb{Z}$-module structure, such that for any invertible n, the kernel of multiplication by n consists of n^2 elements. By analogue: a Drinfeld module of rank d over a scheme X is a group scheme G over X, locally isomorphic to $\mathbb{G}_a$ and equipped with an A-module structure, such that the kernel of multiplication by any nonzero a is finite over X, of degree $|A/a|^d$ over X. The action of A on $\mathrm{Lie}(G)$ gives rise to a homomorphism $A \to \mathcal{O}_X$; this makes X

[1] This is the canonical sign function we are going to use once we fix the uniformizer.

a scheme over $\mathrm{Spec}(A)$. Note that here, the ring A can be defined for arbitrary choice of the place ∞. Elliptic curves over $\mathbb{C}$ can be interpreted as classes of certain lattices in $\mathbb{C}$. Analogously, we can describe Drinfeld modules over $\mathbb{C}_\infty$ in terms of A-lattices in $\mathbb{C}_\infty$ defined over A.

In this section, we first introduce the algebraic definition and some important properties of Drinfeld A-modules over an A-field; it is followed by the definition of Drinfeld A-modules over a scheme X. We mainly follow [BP09], [DH87] and [Gos98]. Then we will define τ-sheaves and A-motives, along with the τ-sheaf corresponding to a given Drinfeld A-module. At the end of this section, we will introduce two important examples of Drinfeld A-modules, namely the Carlitz module and Drinfeld-Hayes module.

Throughout this section, we fix a curve $\mathcal{C}$, a place ∞ and thus the affine coordinate ring A.

2.2.1 Definition of Drinfeld A-modules over an A-field

Before defining Drinfeld A-modules, we would like to recall some results on q-linear polynomials. For details, one may refer to [Gos98, Chapter 1] and [DH87]. Let L be a field containing k.

Definition 2.2.1. A polynomial $f(X) \in L[X]$ is called *additive* if $f(X+Y) = f(X) + f(Y)$ holds in $L[X,Y]$.

It is called *q-linear* if it is additive and $f(\alpha X) = \alpha f(X)$ for any $\alpha \in k$.

It follows from the definition that all q-linear polynomials form a ring under addition and composition.

Now define $L\{\tau\}$ to be a skew polynomial ring over L with commutating law $(\sum_{i\geq 0} a_i\tau^i)(\sum_{j\geq 0} b_j\tau^j) := \sum_{k\geq 0}(\sum_{i=0}^{k} a_i b_{k-i}^{q^i})\tau^k$. We embed $L\{\tau\}$ into $L[X]$ via $\sum_{i=0}^{n} a_i\tau^i \mapsto \sum_{i=0}^{n} a_i X^{q^i}$. Then $L\{\tau\}$ can be identified with the set of all q-linear polynomials in $L[X]$. One may think of $L\{\tau\}$ as a 'ring of operators' with τ being the Frobenius operator. Note that although $L\{\tau\}$ can be embedded into $L[X]$, these two rings possess completely different multiplications. Moreover, it is worthwhile to point out here that in $L\{\tau\}$, the constants are of the form $a\tau^0$ with $a \in L$, i.e., aX if considered as a q-linear polynomial. To avoid confusion, for a q-linear polynomial f, we denote by $\deg(f)$ the degree of f as a polynomial in X and by $\deg_\tau(f)$ the highest exponent of τ appearing in the expression of f as an element in $L\{\tau\}$, i.e., for $f(X) = a_0X + a_1X^p + \ldots + a_lX^{p^l}$ with $a_l \neq 0$, we have $\deg(f) = p^l$

and $\deg_\tau(f) = l$. For a q-linear polynomial $f(X) = a_0X + a_1X^p + \ldots + a_lX^{p^l}$, we define its *derivative* to be $\mathrm{d}(f(X)) := a_0$, which is the usual derivative of f as a polynomial in X.

Now we give the definition of A-fields and Drinfeld A-modules over an A-field.

Definition 2.2.2. An *A-field* F is a field F equipped with a fixed homomorphism $\iota : A \to F$. The homomorphism ι is called the *characteristic* of F. By abuse of notation, we also call the kernel of ι the characteristic of F.

From now on, let L be an A-field of characteristic ι.

Definition 2.2.3. *A Drinfeld A-module over* L is a k-algebra homomorphism

$$\begin{aligned} \rho : A &\longrightarrow L\{\tau\} \\ a &\longmapsto \rho_a := \sum_{i=0}^{r} u_i(a)\tau^i \end{aligned}$$

such that $\mathrm{d} \circ \rho = \iota$ and ρ does not factor through L, i.e., there exists at least one $a \in A$ such that $\rho_a \notin L$.

Given two Drinfeld A-modules ρ and ρ', a *homomorphism* $f : \rho \to \rho'$ *of Drinfeld A-modules over* L is given by some $f \in L\{\tau\}$ such that $f\rho_a = \rho'_a f$ holds for all $a \in A$.

Remark 2.2.4. The nomenclature of 'Drinfeld A-module' emphasizes that the notion gives any L-algebra S an A-module structure by $a.s := \rho_a(s)$.

Definition 2.2.5. The k-algebra homomorphism $\mathrm{ch} := \mathrm{d} \circ \rho : A \to L$ is called the *characteristic* or the characteristic homomorphism of the Drinfeld A-module ρ. Its kernel is a prime ideal of A, denoted by $\mathfrak{p}_0$. We say that ρ is

(1) of *generic characteristic* if $\mathfrak{p}_0 = 0$;

(2) of *special characteristic* otherwise.

By abuse of notation, the ideal $\mathfrak{p}_0$ is sometimes also called the characteristic of ρ.

Remark 2.2.6. The characteristic of a Drinfeld A-module over L is by definition the same as the characteristic of L as an A-field.

The following proposition defines the rank of a Drinfeld A-module:

Proposition-Definition 2.2.7 ([Gos98, Lemma 4.5.1, Proposition 4.5.3]). *For any Drinfeld A-module ρ over L, there exists a unique integer $r > 0$ such that for all nonzero $a \in A$, we have*

$$\deg_\tau(\rho_a) = r \deg(a).$$

We call this r the rank *of the Drinfeld A-module.*

Remark 2.2.8. From the definition of homomorphisms between Drinfeld A-modules, it is easy to see that there exist non-trivial homomorphisms between two Drinfeld A-modules only if they have the same rank.

In number field case, the elliptic curves over $\mathbb{C}$ are equivalent to the rank 2 $\mathbb{Z}$-lattices in $\mathbb{C}$, and this equivalence gives us some analytic insights into the theory of elliptic curves. Similarly, we can also associate an A-lattice in $\mathbb{C}_\infty$ to any Drinfeld A-module of generic characteristic over $\mathbb{C}_\infty$ and vice versa. To do this, we consider $\mathbb{C}_\infty$ as an infinite dimensional vector space over K_∞, equipped with sup-norm extending the absolute value on K_∞.

We first recall that for a normed vector space U, a subset S is called discrete in U if every point $u \in U$ has a neighborhood $W \subset U$ such that $W \cap S = \{u\}$.

Definition 2.2.9. *A finitely generated A-lattice* in $\mathbb{C}_\infty$ is a finitely generated, discrete sub-A-module of $\mathbb{C}_\infty$.

Proposition-Definition 2.2.10. *Given a Drinfeld A-module ρ of generic characteristic over $\mathbb{C}_\infty$, there exists a unique entire function* $\exp_\rho : \mathbb{C}_\infty \to \mathbb{C}_\infty$ *satisfying*

$$\exp_\rho(ax) = \rho_a \circ \exp_\rho(x),\ \forall x \in \mathbb{C}_\infty,\ a \in A.$$

This function is called the exponential map associated to ρ.

Remark 2.2.11. We have the following commutative diagram, where the rows are exact:

$$\begin{tikzcd}
 & 0 \arrow[r] & \mathbb{C}_\infty \arrow[r, "\cdot a"] \arrow[d, "\exp_\rho"'] & \mathbb{C}_\infty \arrow[r] \arrow[d, "\exp_\rho"] & 0 \\
0 \arrow[r] & \rho[a] \arrow[r] & \mathbb{C}_\infty \arrow[r, "\rho_a"] & \mathbb{C}_\infty \arrow[r] & 0.
\end{tikzcd}$$

In the above diagram $\rho[a] := \mathrm{Ker}(\rho_a) \subset \mathbb{C}_\infty$ is called the *torsion of a*. The above diagram remains true when we substitute $\mathbb{C}_\infty$ by K^{alg} or even K^{sep}.

We slightly reformulate [Gos98, Theorem 4.6.9] which describes the correspondence between Drinfeld A-modules and A-lattices.

Theorem 2.2.12. *Given a Drinfeld A-module ρ over $\mathbb{C}_\infty$ which is of generic characteristic, let $\exp_\rho$ be the associated exponential map. Let Λ be the kernel of $\exp_\rho$ in $\mathbb{C}_\infty$. Then this Λ is an A-lattice in $\mathbb{C}_\infty$.*

Conversely, given a finitely generated A-lattice Λ in $\mathbb{C}_\infty$, we define

$$\exp_\Lambda(x) := x \prod_{\alpha\in\Lambda,\alpha\neq 0} (1 - \frac{x}{\alpha}).$$

Then there exists a Drinfeld A-module ρ such that

$$\exp_\Lambda(ax) = \rho_a \circ \exp_\Lambda(x), \ \textit{for } x \in \mathbb{C}_\infty,\ a \in A.$$

In fact, for any $a \in A$, we have

$$\rho_a(x) = ax \prod_{\alpha\in\Lambda,\alpha\neq 0} (1 - \frac{x}{\exp_\Lambda(\alpha)}).$$

The above correspondence gives an equivalence between the category of Drinfeld A-modules of generic characteristic over $\mathbb{C}_\infty$ and the category of finitely generated A-lattices in $\mathbb{C}_\infty$.

Remark 2.2.13. Thanks to the above correspondence, we can complete the commutative diagram in Remark 2.2.11 (where all columns and rows are exact):

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & & \\
 & 0 \arrow[r] & \Lambda \arrow[r] \arrow[d] & \Lambda \arrow[r] \arrow[d] & \Lambda/a\Lambda \arrow[r] & 0 \\
 & 0 \arrow[r] & \mathbb{C}_\infty \arrow[r, "\cdot a"] \arrow[d, "\exp"'] & \mathbb{C}_\infty \arrow[r] \arrow[d, "\exp"] & 0 & \\
0 \arrow[r] & \rho[a] \arrow[r] & \mathbb{C}_\infty \arrow[r, "\rho_a"] \arrow[d] & \mathbb{C}_\infty \arrow[r] \arrow[d] & 0 & \\
 & & 0 & 0 & &
\end{tikzcd}$$

Remark 2.2.14. We can define the *rank* of an A-lattice Λ to be the dimension of $K \otimes_A \Lambda$ as an K-vector space. It can be shown that the rank of an A-lattice is the same as the rank of the corresponding Drinfeld A-module. Moreover, the homomorphisms of Drinfeld modules correspond to the morphisms of the corresponding lattices.

2.2.2 Drinfeld A-modules over a scheme X

Let X be a scheme.

Definition 2.2.15. A *Drinfeld A-module of rank $r > 0$ on X* consists of a line bundle L on X and a ring homomorphism $\rho : A \to \mathrm{End}_k(L)$, $a \mapsto \rho_a$, such that for all points $x \in X$ with residue field k_x the induced map

$$\begin{aligned}\rho_x : A &\longrightarrow \mathrm{End}_k(L|x) \cong k_x[\tau],\\ a &\longmapsto \sum_{i=0}^{\infty} u_i(a)\tau^i\end{aligned}$$

has coefficients $u_i(a) = 0$ for $i > r\deg(a)$ and $u_{r\deg a}(a) \in k_x^*$.

A *homomorphism* $(L, \rho) \to (L', \rho')$ *of Drinfeld A-modules over X* is a k-linear homomorphism of line bundles $L \to L'$ that is equivariant with respect to the actions ρ and ρ'.

The *characteristic of* (L, ρ) is the morphism of schemes $\mathrm{ch}_\rho : X \to \mathrm{Spec}\, A$ corresponding to the ring homomorphism $\mathrm{d}\rho : A \to \mathrm{End}_{\mathcal{O}_X}(\mathrm{Lie}(L)) \cong \Gamma(X, \mathcal{O}_X)$.

Remark 2.2.16. In the special case when $X = \mathrm{Spec}\, R$ with R an A-field and the line bundle L is free over X, the above definition is isomorphic to the algebraic definition given in 2.2.3.

2.2.3 τ-sheaves and A-motives

The notion of A-motives was first introduced by Anderson in [And86], or more precisely t-motives since he only considered the case when $A = \mathbb{F}_q[t]$. In some literature, the A-motives bear the name of abelian A-motives due to the similarity to abelian varieties. In this section, we will briefly define τ-sheaves and A-motives, then introduce the construction of the τ-sheaf corresponding to a given Drinfeld A-module. Those who are interested may refer to the original paper [And86] by Anderson or [BP09] for a more general theory.

Definition 2.2.17. A *τ-sheaf* $\underline{\mathscr{M}} = (\mathscr{M}, \tau_{\mathscr{M}})$ over A on a scheme X consists of a quasi-coherent sheaf $\mathscr{M}$ on $X \times \mathrm{Spec}\, A$ and an $\mathcal{O}_{X\times \mathrm{Spec}\, A}$-linear homomorphism $\tau_{\mathscr{M}} : (\sigma \times \mathrm{id})^*\mathscr{M} \to \mathscr{M}$ where σ denotes the absolute Frobenius on X over k.[1]

[1] We sometimes drop off the lower index of $\tau_{\mathscr{M}}$ when the sheaf is clear from the context.

A *homomorphism of τ-sheaves* $(\mathscr{M},\tau_{\mathscr{M}}) \to (\mathscr{N},\tau_{\mathscr{N}})$ is a homomorphism f of the underlying sheaves such that the following diagram commutes:

$$\begin{tikzcd}
(\sigma \times \mathrm{id})^*\mathscr{M} \arrow[r, "(\sigma\times\mathrm{id})^* f"] \arrow[d, "\tau_{\mathscr{M}}"'] & (\sigma \times \mathrm{id})^*\mathscr{N} \arrow[d, "\tau_{\mathscr{N}}"] \\
\mathscr{M} \arrow[r, "f"'] & \mathscr{N}
\end{tikzcd}$$

We denote by $QCoh_\tau(X, A)$ the category of τ-sheaves over A on X.

We call a τ-sheaf *coherent* if its underlying sheaf is coherent. The full subcategory of coherent τ-sheaves is denoted by $Coh_\tau(X, A)$.

For any τ-sheaf $\underline{\mathscr{M}}$ we define the iterates $\tau^n_{\mathscr{M}}$ of $\tau_{\mathscr{M}}$ by setting inductively $\tau^0_{\mathscr{M}} := \mathrm{id}$ and $\tau^{n+1}_{\mathscr{M}} := \tau_{\mathscr{M}} \circ (\sigma \times \mathrm{id})^*\tau^n_{\mathscr{M}}$ for any $n \in \mathbb{N}$. For any $n \in \mathbb{N}$, each $(\sigma^n \times \mathrm{id})^*\underline{\mathscr{M}} := ((\sigma^n \times \mathrm{id})^*\mathscr{M}, (\sigma^n \times \mathrm{id})^*\tau_{\mathscr{M}})$ is again a τ-sheaf, and $\tau^n_{\mathscr{M}}$ is a homomorphism of τ-sheaves from $(\sigma^n \times \mathrm{id})^*\underline{\mathscr{M}}$ to $\underline{\mathscr{M}}$.

Definition 2.2.18. A τ-sheaf $\underline{\mathscr{M}}$ is called

(a) *nilpotent* if $\tau^n_{\mathscr{M}}$ vanishes for some n;

(b) *locally nilpotent* if it is a union of nilpotent τ-subsheaves.

Definition 2.2.19. A homomorphism of τ-sheaves is called a *nil-isomorphism* if both its kernel and its cokernel are locally nilpotent.

Proposition 2.2.20 ([BP09, Proposition 3.3.9])**.** *A homomorphism of τ-sheaves $f : \underline{\mathscr{M}} \to \underline{\mathscr{N}}$ is a nil-isomorphism if there exist $n \geq 0$ and a homomorphism of τ-sheaves α making the following diagram commute:*

$$\begin{tikzcd}
(\sigma^n \times \mathrm{id})^*\underline{\mathscr{M}} \arrow[r, "(\sigma^n\times\mathrm{id})^* f"] \arrow[d, "\tau^n_{\mathscr{M}}"'] & (\sigma^n \times \mathrm{id})^*\underline{\mathscr{N}} \arrow[d, "\tau^n_{\mathscr{N}}"] \arrow[dl, "\alpha"] \\
\underline{\mathscr{M}} \arrow[r, "f"'] & \underline{\mathscr{N}}.
\end{tikzcd}$$

If $\underline{\mathscr{M}}$ and $\underline{\mathscr{N}}$ are coherent, then the converse is also true.

Due to Drinfeld, we can associate a coherent τ-sheaf to any Drinfeld A-module (L, ρ). We quote the construction from [BP09]. Note first that $U \mapsto \mathrm{Hom}_k(L|U, \mathbb{G}_a \times U)$ defines a quasi-coherent sheaf of $\mathcal{O}_X$-modules on X. By right composition with

ρ_a it becomes a sheaf of $\mathcal{O}_X \otimes A$-modules. We let $\mathscr{M}(\rho)$ be the corresponding quasi-coherent $\mathcal{O}_{X\times \operatorname{Spec} A}$-modules on $X \times \operatorname{Spec} A$, which is easily seen to be locally free of rank r. Let now $\sigma \in \operatorname{End}_k(\mathbb{G}_a \times X)$ denote the Frobenius endomorphism relative to X. Then left composition with σ defines an $\mathcal{O}_{X\times \operatorname{Spec} A}$-linear homomorphism $\mathscr{M}(\rho) \to (\sigma \times \mathrm{id})_* \mathscr{M}(\rho)$, and thus via adjunction an $\mathcal{O}_{X\times \operatorname{Spec} A}$-linear homomorphism $\tau : (\sigma \times \mathrm{id})^* \mathscr{M}(\rho) \to \mathscr{M}(\rho)$. We denote the resulting τ-sheaf by $\underline{\mathscr{M}}(\rho)$. Clearly this construction is functorial in (L, ρ). Also it is easy to see that $\operatorname{Coker}(\tau)$ is supported on the graph of ch_ρ and locally free of rank 1 over X.

We fix a homomorphism $\mathrm{ch} : X \to \operatorname{Spec} A$.

Definition 2.2.21. A *family of A-motives over X*, or in short an *A-motive on X*, *of rank r and of characteristic* ch is a coherent τ-sheaf $\underline{\mathscr{M}}$ on X such that

(a) the underlying sheaf $\mathscr{M}$ is locally free of rank r, and

(b) the set-theoretic support of $\operatorname{Coker}(\tau)$ is a subset of the graph of ch.

The category of Drinfeld A-modules does not permit the formation of direct sums or tensor products or related operations from linear algebra. The passage to Anderson's t-motives, and more generally A-motives, adds this missing flexibility.

2.2.4 An Example: the Carlitz module

The Carlitz module was first inspected by Carlitz in [Car35], even before the invention of Drinfeld modules. It is a special kind of Drinfeld A-module over K of rank 1 with A being $k[t]$ and K being $k(t)$.

Definition 2.2.22. The Carlitz module is defined to be

$$\begin{aligned} C : A &\longrightarrow K\{\tau\} \\ a &\longmapsto a + \tau. \end{aligned}$$

This is by definition a Drinfeld A-module of rank 1 of generic characteristic.

The next natural question is to write down the exponential map and the associated A-lattice.

Definition 2.2.23. We define the following q-linear polynomials.

(1) For $i \geq 1$, $[i] := t^{q^i} - t$.

(2) For $i \geq 1$, $L_i := \prod_{1 \leq j \leq i}[j]$; $L_0 := 1$.

(3) For $i \geq 1$, $D_i := \prod_{1 \leq j \leq i}[j]^{q^{i-j}}$; $D_0 := 1$.

Note that by [Gos98, Proposition 3.1.6] L_i is in fact the least common multiple of all polynomials of degree i, while D_i is the product of all monic polynomials of degree i in A.

We can write down the exponential map of Carlitz module explicitly:

$$\exp_C = \sum_{i \geq 0} \frac{1}{D_i} \tau^i.$$

By Remark 2.2.14 the associated A-lattice has rank 1. Let λ be a $(q-1)$-th root of $-[1]$ in K_∞^{alg} and $\xi_\infty := \prod_{i \geq 1}(1 - \frac{[i]}{[i+1]})$. Define $\varpi := \lambda \xi_\infty$. We can check that ϖA is the A-lattice associated to the Carlitz module. For more details one may refer to [Gos98, 3.2].

2.2.5 Another Example: Drinfeld-Hayes module

Another example of rank 1 Drinfeld A-modules is the Drinfeld-Hayes module, or rank 1 sign-normalized Drinfeld module. We call a continuous homomorphism $\mathrm{sgn} : K_\infty^* \to k_\infty^*$ a *twisted sign function* if there exists some $\sigma \in \mathrm{Gal}(k_\infty/k)$ such that $\mathrm{sgn} = \sigma$ when restricted to k_∞^*.

Definition 2.2.24. A *Drinfeld-Hayes module*, or rank 1 sign-normalized Drinfeld module (for sgn) is a rank 1 Drinfeld A-module ρ of generic characteristic over $\mathbb{C}_\infty$ such that for any $a \in A$, the leading coefficient of ρ_a agrees with the image of a under the restriction of a twisted sign function sgn to $A \subset K_\infty$, i.e., it is given by

$$\begin{aligned} \rho : A &\longrightarrow \mathbb{C}_\infty\{\tau\} \\ a &\longmapsto \rho_a := \sum_{i=0}^{r\deg(a)} u_i(a)\tau^i, \end{aligned}$$

where $u_{r\deg(a)}(a) = \mathrm{sgn}(a)$ for a twisted sign function sgn.

A result from Hayes states that any rank one Drinfeld module of generic characteristic over $\mathbb{C}_\infty$ is isomorphic to a Drinfeld-Hayes module. Therefore, we can count the number of Drinfeld-Hayes modules. Let h be the class number of A.

Proposition 2.2.25 ([Gos98, Proposition 7.2.17]). *There are exactly h isomorphism classes of rank one Drinfeld modules over $\mathbb{C}_\infty$.*

Proposition 2.2.26 ([Gos98, Corollary 7.2.19]). *There are exactly $h(q^{d_\infty}-1)/(q-1)$ Drinfeld-Hayes modules.*

In particular, if A has strict class number 1, then there exists a unique Drinfeld-Hayes module for a fixed sgn.

Remark 2.2.27. One big advantage of the introduction of Drinfeld-Hayes modules is that it allows us to formulate the explicit class field theory for function field. For details one may refer to [RS97].

2.3 Goss zeta functions and their variations

The study of Riemann zeta functions has a long and profound history, where engraved lots of great names. The Riemann hypothesis is among the most challenging and famous unsolved problems. As we have discussed in Chapter 1, we will work on the analogue of Riemann hypothesis for function fields, i.e., on the zero distribution of special values of the Goss zeta functions. In this section, we will introduce the definition of Goss zeta functions and some variations.

2.3.1 The Exponentiations of Ideals

In this section, we want to give some detailed description of the exponentiation of ideals, ∞-adically as well as v-adically, as the first step to define the Goss zeta function.

In principal, the exponentiation map $e : \mathbb{R}^* \times \mathbb{Z} \to \mathbb{R}^*$, $(x, y) \mapsto x^y$ is a bilinear map, i.e., it is multiplicative at the first coordinate and additive at the second one. Here we consider the domain of the first coordinate to be the group of fractional ideals, with or without extra requirements, and the domain of the second coordinates to be $\mathbb{Z}$ or more generally S_∞ or S_v, which will be defined later. In commutative algebra, the integral powers of ideals are defined to be ideals, while in his book [Gos98], Goss defined the ∞-adic and v-adic exponentiations of fractional ideals to be elements in $\mathbb{C}_\infty$, and this is the definition we will introduce here.

2.3.1.1 The ∞-adic Exponentiation

Recall that we fix a uniformizer π_∞ at ∞ and denote by sgn_∞ a fixed sign function on K_∞^*. Besides the ideal class group $Cl(A)$, we also have the strict ideal class group $Cl^+(A)$ with respect to sgn_∞. We can define the Hilbert class field H (resp. the strict Hilbert class field H^+) of K as the abelian extension of K which has Galois group isomorphic to $Cl(A)$ (resp. $Cl^+(A)$). Corresponding to the field extensions $H^+ \supset H \supset K$, we have under the reciprocity map:

$$\prod_{w\neq\infty} \mathcal{O}_w^* \times \ker(\mathrm{sgn}_\infty) \subset \prod_{w\neq\infty} \mathcal{O}_w^* \times K_\infty^* \subset \mathbb{A}_K^*.$$

Let $\mathfrak{m}_\infty$ be the maximal ideal of $\mathcal{O}_\infty$, then we have $\ker(\mathrm{sgn}_\infty) = \pi_\infty^{\mathbb{Z}} \times (1+\mathfrak{m}_\infty)$. By [Böc02, Proposition 10.4], there exists a unique homomorphism

$$\langle\cdot\rangle : \mathcal{I}^\infty \longrightarrow \mathcal{U}_1^{\mathrm{perf}}$$

where $\mathcal{I}^\infty$ is the group of nonzero fractional ideals of A, and $\mathcal{U}_1^{\mathrm{perf}}$ is the group of 1-units in the perfect closure of K_∞, such that for any ∞-positive element α in A, we have

$$\langle(\alpha)\rangle = \alpha \cdot \pi_\infty^{-v_\infty(\alpha)},$$

i.e., for any ideal $\mathfrak{a}$ of A, let a be an ∞-positive generator of $\mathfrak{a}^{h(q^{d_\infty}-1)}$, then $\langle\mathfrak{a}\rangle = (a\cdot\pi_\infty^{-v_\infty(a)})^{\frac{1}{h(q^{d_\infty}-1)}}$, where we take the 1-unit root.

Remark 2.3.1. Note that the map $\langle\cdot\rangle$ depends on the choice of π_∞. Suppose we have two different uniformizers, say ${}_1\pi_\infty$ and ${}_2\pi_\infty$. We denote by $\langle\cdot\rangle_1$ and $\langle\cdot\rangle_2$ the corresponding 1-unit parts. Let $u := {}_1\pi_\infty/{}_2\pi_\infty$, then u is a 1-unit in K_∞. It is stated in [Gos98, Proposition 8.2.15] that for any ideal $\mathfrak{a}$ of A, we have $\langle\mathfrak{a}\rangle_1 = u_*^{\deg\mathfrak{a}}\langle\mathfrak{a}\rangle_2$ with u_* the 1-unit d_∞-th root of u.

Lemma 2.3.2. *Given m and n in $\mathbb{Z}_p$ such that $m \equiv n \pmod{p^k}$, for any ideal $\mathfrak{a}$ we have*

$$\langle\mathfrak{a}\rangle^n \equiv \langle\mathfrak{a}\rangle^m \pmod{\pi_\infty^{p^k}}.$$

Then we can define the ∞-adic exponentiations of ideals.

Definition 2.3.3. For any $s=(x,y)\in S_\infty := \mathbb{C}_\infty^* \times \mathbb{Z}_p$ and $\mathfrak{a}$ a fractional ideal in $\mathcal{I}^\infty$, we define the ∞-*adic exponentiation* of $\mathfrak{a}$ as:

$$\mathfrak{a}_\infty^s := \langle\mathfrak{a}\rangle^y \cdot x^{\deg_\infty \mathfrak{a}}.$$

Let $\pi_{\infty,*} \in \mathbb{C}_\infty^*$ be a fixed d_∞-th root of π_∞.

Proposition 2.3.4 ([Gos98, Proposition 8.2.6, Corollary 8.2.7]). *Let $s = (x, y) \in S_\infty$ and $\mathfrak{a} = (\alpha) \in \mathcal{I}^\infty$ such that α is ∞-positive. Then*

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

In particular, for $n \in \mathbb{Z}$ we have

$$\mathfrak{a}_\infty^{(\pi_{\infty,*}^{-n},n)} = \alpha^n.$$

Definition 2.3.5. For an integer n and a fractional ideal $\mathfrak{a}$ of A^∞, we define $\mathfrak{a}_\infty^n := \mathfrak{a}_\infty^{(\pi_{\infty,*}^{-n},n)}$ for abbreviation.

Remark 2.3.6. In other words, we embed $\mathbb{Z}$ into S_∞ by sending an integer n to $(\pi_{\infty,*}^{-n}, n)$.

Important properties of the ∞-adic exponentiation defined above are that for any $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{I}^\infty$, any s and t in S_∞, we have

$$\mathfrak{a}_\infty^s \cdot \mathfrak{b}_\infty^s = (\mathfrak{a} \cdot \mathfrak{b})_\infty^s, \quad \mathfrak{a}_\infty^s \mathfrak{a}_\infty^t = \mathfrak{a}_\infty^{s+t},$$

which implies that our map is bilinear, thus a well-defined exponentiation map.

Remark 2.3.7. The integral ∞-adic exponentiation depends on the choice of $\pi_{\infty,*}$. For $i \in \{1, 2\}$, let ${}_i\pi_\infty$ be a uniformizer at ∞ and let ${}_i\pi_{\infty,*}$ be a fixed d_∞-th root of ${}_i\pi_\infty$, then we denote by ${}_i\mathfrak{a}_\infty$ the corresponding ∞-adic exponentiation of an ideal $\mathfrak{a}$. Then [Gos98, Proposition 8.2.16] states that there exists a d_∞-th root of unity ζ such that ${}_1\mathfrak{a}_\infty{}^1 = \zeta^{\deg\mathfrak{a}}{}_2\mathfrak{a}_\infty{}^1$ for any ideal $\mathfrak{a}$ of A. To be more precise, let $u := {}_1\pi_\infty/{}_2\pi_\infty$ and let u_* be the 1-unit d_∞-th root of u, then $\zeta = u_* \cdot {}_2\pi_{\infty,*}/{}_1\pi_{\infty,*}$.

Example 2.3.8. As in Example 2.1.1, take $A = \mathbb{F}_q[t]$. Then the integral ∞-adic exponentiation of any ideal $\mathfrak{a}$ of A can be given as $\mathfrak{a}_\infty^n = f_\mathfrak{a}^n$ with $f_\mathfrak{a}$ the monic polynomial generating $\mathfrak{a}$.

2.3.1.2 The v-adic Exponentiation

To define the v-adic exponentiation, we need a bit more work. Recall that we fix a place ∞ and let S be a nonempty set of places which does not contain ∞. Fix a place $v \in S$ and denote by d_v its degree. Let $\mathcal{I}^{\infty,S}$ contain all nonzero fractional ideals of A which are prime to all places in S.

Let K_v be the completion of K with respect to v, and σ a homomorphism from the value field $\mathbb{V} := K(\{\mathfrak{a}_\infty^1 : \mathfrak{a} \in \mathcal{I}^\infty\})$ to $\overline{K_v}$ over K. By [Gos98, Proposition 8.2.9], the field $\mathbb{V}$ is finite over K, thus $K_{\sigma,v} := K_v(\sigma(\mathbb{V}))$ is also finite over K_v.

We denote by f the residue degree. Denote by $\mathcal{O}_{\sigma,v}$ the ring of integers in $K_{\sigma,v}$. Then every element $\alpha \in \mathcal{O}_{\sigma,v}^*$ can be decomposed into

$$\alpha = \langle \alpha \rangle_v \cdot \omega(\alpha),$$

where $\omega(\alpha)$ is a $(q^{d_v f}-1)$-th root of unity in $\mathcal{O}_{\sigma,v}$ and $\langle \alpha \rangle_v$ is a 1-unit. There exists a unique homomorphism generalising $\langle \cdot \rangle_v$ to the fractional ideals of $K_{\sigma,v}$, which is denoted also by $\langle \cdot \rangle_v$. To be more precise, for any fractional ideal $\mathfrak{a}$ of $K_{\sigma,v}$, let a be a doubly-positive generator of $\mathfrak{a}^{h(q^{d_\infty}-1)(q^{d_v}-1)}$, then $\langle \mathfrak{a} \rangle_v = (a \cdot \omega(a)^{-1})^{\frac{1}{h(q^{d_\infty}-1)(q^{d_v}-1)}}$, where we take the 1-unit root.

For the map $\langle \cdot \rangle_v$, we also have the interpolation lemma similar to Lemma 2.3.2.

Lemma 2.3.9. *Given m and n in $\mathbb{Z}_p$ such that $m \equiv n \pmod{p^k(q^{d_v f}-1)}$, for any fractional ideal $\mathfrak{a} \in \mathcal{I}^{\infty,S}$ we have*

$$\langle \mathfrak{a} \rangle_v^n \equiv \langle \mathfrak{a} \rangle_v^m \pmod{\pi_v^{p^k}}.$$

The v-adic exponentiation map is defined as follows:

Definition 2.3.10. For any $s = (x, y_1, y_2) \in S_v := \mathbb{C}_v^* \times \mathbb{Z}_p \times \mathbb{Z}/(q^{d_v f}-1)$, we define the v-adic exponentiation for any $\mathfrak{a} \in \mathcal{I}^{\infty,S}$ as

$$\mathfrak{a}_{\infty,v}^s := \langle \sigma(\mathfrak{a}_\infty^1) \rangle_v^{y_1} \cdot \omega(\sigma(\mathfrak{a}_\infty^1))^{y_2} \cdot x^{\deg_\infty(\mathfrak{a})}.$$

In particular, for $\alpha \in A^\infty$ positive at both ∞ and v and prime to all places in S, we have that:

$$\begin{aligned}(\alpha)_{\infty,v}^{(1,n,n)} &= \langle \sigma((\alpha)_\infty^1) \rangle_v^n \cdot \omega(\sigma((\alpha)_\infty^1))^n \cdot 1^{\deg_\infty(\alpha)} \\ &= \langle \sigma(\alpha) \rangle_v^n \cdot \omega(\sigma(\alpha))^n = \alpha^n.\end{aligned}$$

Definition 2.3.11. For an integer n and a fractional ideal $\mathfrak{a}$ in $\mathcal{I}^{\infty,S}$, we denote by $\mathfrak{a}_{\infty,v}^n := \mathfrak{a}_{\infty,v}^{(1,n,n)}$ for abbreviation.

Remark 2.3.12. In other words, for v-adic exponentiation, we embed $\mathbb{Z}$ into S_v by sending n to $(1, n, n)$.

Similar as the ∞-adic exponentiation, we have the following nice properties:

$$\mathfrak{a}_{\infty,v}^s \cdot \mathfrak{b}_{\infty,v}^s = (\mathfrak{a} \cdot \mathfrak{b})_{\infty,v}^s, \quad \mathfrak{a}_{\infty,v}^s \mathfrak{a}_{\infty,v}^t = \mathfrak{a}_{\infty,v}^{s+t}$$

for any $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}^{\infty,S}$ and $s, t \in S_v$. Thus it is a well-defined exponentialtion map.

Remark 2.3.13. As we have seen in Remark 2.3.7, the integral ∞-adic exponentiation depends on the choice of the infinite place and $\pi_{\infty,*}$. For the integral v-adic exponentiation, it depends on the choices of both places v, ∞, the embedding σ, the character ω as well as $\pi_{\infty,*}$.

2.3.2 Definition of Goss zeta function

Thanks to the introduction of ∞-adic and v-adic exponentiations, now we can define the Goss ∞-adic and v-adic zeta functions. Recall that S is a nonempty set of places of K such that $\infty \notin S$ and $v \in S$.

Definition 2.3.14. Let $n \in \mathbb{Z}$. We define the ∞-adic Goss zeta function as

$$\zeta_A(-n, T) := \sum_{\mathfrak{a} \in \mathcal{I}^{\infty}, \mathfrak{a} \subset A} \mathfrak{a}_{\infty}^{n} T^{\deg_{\infty}(\mathfrak{a})},$$

and the v-adic Goss zeta function as

$$\zeta_A^{S,(v)}(-n, T) := \sum_{\mathfrak{a} \in \mathcal{I}^{\infty, S}, \mathfrak{a} \subset A} \mathfrak{a}_{\infty,v}^{n} T^{\deg_{\infty}(\mathfrak{a})}.$$

Thakur introduced a principal ideal version of Goss zeta function when the place ∞ is k-rational, which, by its name, only sums over the principal ideals. Let $\mathcal{P}^{\infty}$ (resp. $\mathcal{P}^{\infty,S}$) be the subgroup of $\mathcal{I}^{\infty}$ (resp. $\mathcal{I}^{\infty,S}$) containing the principal fractional ideals.

Definition 2.3.15. We define the ∞-adic Goss-Thakur zeta function as

$$\zeta_A(-n, T) := \sum_{\mathfrak{a} \in \mathcal{P}^{\infty}, \mathfrak{a} \subset A} \mathfrak{a}_{\infty}^{n} T^{\deg_{\infty}(\mathfrak{a})},$$

and the v-adic Goss-Thakur zeta fucntion as

$$\zeta_A^{S,(v)}(-n, T) := \sum_{\mathfrak{a} \in \mathcal{P}^{\infty, S}, \mathfrak{a} \subset A} \mathfrak{a}_{\infty,v}^{n} T^{\deg_{\infty}(\mathfrak{a})}.$$

2.3.3 Goss zeta function as the dual characteristic polynomial

In Chapter 5, we will use cohomological method to investigate the zeros of the special values of Goss zeta function. Therefore, we would like to introduce an alternative definition of the Goss zeta function here. To be more precise, in this section we will define the L-function attached to a given A-motive or a given τ-sheaf. One may refer to [BP09] and [Böc13] and the references stated there for more details.

We first introduce the global L-function of certain τ-sheaf following [Böc13]. Let X be a scheme of finite type over k and $\underline{\mathscr{M}}$ is an A-motive over X of characteristic ch. For any closed point $x \in |X|$, we denote by $\mathfrak{p}_x$ its image in $\operatorname{Spec} A$ under the characteristic homomorphism. It is easy to see that $d_{\mathfrak{p}_x} | d_x$. We denote by i_x the natural embedding of its residue field into X. Denote by $\underline{\mathscr{M}}_x := i_x^* \underline{\mathscr{M}}$.

Definition 2.3.16. The *global L-function of $\underline{\mathscr{M}}$ over x* is

$$L(x, \underline{\mathscr{M}}, T) := \det_A(\mathrm{id} - T\tau \mid \underline{\mathscr{M}}_x) \in 1 + T^{d_x} A[[T^{d_x}]].$$

Definition 2.3.17. We define the *global L-function of $\underline{\mathscr{M}}$* as:

$$L^{\mathrm{glob}}(X, \underline{\mathscr{M}}, s) := \prod_{x \in |X|} L(x, \underline{\mathscr{M}}, T)_{\,|\, T^{d_{\mathfrak{p}_x}} = \mathfrak{p}^{-s}} \in 1 + \mathbb{C}_\infty[[T]].$$

As we have seen in Section 2.2.5, for any ring A we can define a Drinfeld-Hayes module, and the number of Drinfeld-Hayes modules is the strict class number of A. Now we consider the case when A has strict class number 1. Then there exists a unique Drinfeld-Hayes module. Denote the structure morphism $\operatorname{Spec} \mathcal{O}^+ \to \operatorname{Spec} A$ by s and the A-motive associated to this Drinfeld-Hayes module by $\mathscr{H}_A$. Thus $\mathscr{H}_A$ is a locally free τ-sheaf on $\operatorname{Spec} \mathcal{O}^+$ over A of rank 1. We quote the following theorem from [Böc13].

Theorem 2.3.18 ([Böc13, Theorem 3.3])**.** *Let A have strict class number one. Let $n \in \mathbb{N}$. Let $\overline{\underline{\mathscr{H}}}_n$ be a locally free τ-sheaf on X over K whose restriction to* $\operatorname{Spec} A$ *is nil-isomorphic to the n-th tensor power of $\mathscr{H}_A$. Let*

$$L(\infty, \overline{\underline{\mathscr{H}}}_n, T)^{-1} \in 1 + TA[T]$$

be the characteristic polynomial of the restriction $\overline{\underline{\mathscr{H}}}_n$ to $\operatorname{Spec}(k_\infty \times K)$*. Then we have:*

(a) $\zeta_A(-n, T) = L(\operatorname{Spec} A, \overline{\underline{\mathscr{H}}}_n, T)$.

(b) $L(X, \overline{\underline{\mathscr{H}}}_n, T) L(\infty, \overline{\underline{\mathscr{H}}}_n, T)^{-1} = L(\operatorname{Spec} A, \overline{\underline{\mathscr{H}}}_n, T)$.

(c) $H^1(X \times \operatorname{Spec} K, \overline{\underline{\mathscr{H}}}_n)$ *is a free finitely generated K-vector space which carries an action $H^1(\tau)$ induced from the action of τ on $\overline{\underline{\mathscr{H}}}_n$ via the functoriality of cohomology.*

(d) $L(X, \overline{\underline{\mathscr{H}}}_n, T) = \det_K(1 - TH^1(\tau) \mid H^1(X \times \operatorname{Spec} K, \overline{\underline{\mathscr{H}}}_n)) \in 1 + A[T]$.

(e) Let $\kappa : (\sigma \times \mathrm{id})_* D(\overline{\underline{\mathscr{H}}}_n) \to D(\overline{\underline{\mathscr{H}}}_n)$ denote the Cartier dual action on $D(\overline{\underline{\mathscr{H}}}_n) =$ $\mathcal{H}om(\overline{\underline{\mathscr{H}}}_n, \Omega_{X \times \operatorname{Spec} K})$ *induced from τ. Then $\Gamma(X \times \operatorname{Spec} K, D(\overline{\underline{\mathscr{H}}}_n))$ is a free finitely generated K-vector space and for the action induced from κ on global sections, $\kappa : \Gamma(X \times \operatorname{Spec} K, D(\overline{\underline{\mathscr{H}}}_n)) \to \Gamma(X \times \operatorname{Spec} K, D(\overline{\underline{\mathscr{H}}}_n))$, one has*

$$L(X, \overline{\underline{\mathscr{H}}}_n, T) = \det_K(1 - T\kappa \mid \Gamma(X \times \operatorname{Spec} K, D(\overline{\underline{\mathscr{H}}}_n))).$$

3. On The Riemann Hypothesis of Positive Characteristic

3.1 Introduction

As we have discussed in Chapter 1, in this chapter, we would like to generalize the result of Sheats to general A's. Recall that for an arbitrary curve, we can define the principal ideal Goss zeta function, or Goss-Thakur zeta function, as

$$\zeta_A(-n, T) := \sum_{d \geq 0} T^d \sum_{a \in A_{+,d}} a^n,$$

where $A_{+,d}$ consists of all functions of degree d which are positive at ∞. For a positive integer n, the special value of $\zeta_A(-n, T)$ at $-n$ is in fact a polynomial. We would like to look at the zeros of this polynomial. A natural method to do so is by looking at the break points of the associated Newton polygon.

But a direct shortage of using the method of Newton polygon is that we cannot expect to show that all zeros are simple. When the genus of the curve is not 0, by the Riemann-Roch theorem there exists no function of degree d where d is a Weierstrass gap. Thus for these d's, the coefficient of T^d in the Goss-Thakur zeta function is simply zero. In particular, one cannot expect a break point with the x-coordinate being d. On the other hand, this situation can only happen for a limited number of d's, which, to be more precise, cannot exceed $2g$ and the number of these d's is exactly g. Hence we face an inevitable obstacle when dealing with the zeros of small valuations.

However, we successfully generalize Sheats' result to certain cases.

Theorem 3.1.1. *Suppose that either $p = q$ or $p \neq q$ and $g \leq \frac{p+q}{2}$. Let n be a fixed positive integer. The following holds:*

(a) The x-coordinates of the break points of the Newton polygon associated to $\zeta_A(-n,T)$ are φ_i for all $i = 0, 1, \ldots$.

(b) The slope of the i-th segment between φ_{i-1} and φ_i is G_i^i, where G_i^i appears as the last entry of the greedy element in $U_{i+1}(n)$. In particular, the sequence $\{G_1^1, G_2^2, G_3^3, \ldots\}$ is strictly increasing.

Let $m \leq g$ be the smallest positive integer such that $\tilde{\varphi}_i = 1$ for all $i > m$. Except for the φ_m zeros of lowest valuations, all other zeros of $\zeta_A(-n,T)$ are simple with pairwise distinct valuations.

Before going to an outline of this chapter, I would like to draw the reader's attention to a question on the splitting field of $\zeta_A(-n,T)$ posted by G. Böckle in [Böc13]. By the above theorem, there exists a trivial upper bound of the extension degree of the splitting field, namely $2g$. By the semigroup structure of the non-Weierstrass numbers, the maximal multiplicity of a zero is $\tilde{\varphi}_0$, i.e., the distance between 0 and the first positive non-Weierstrass number. Moreover, from the proof of the main theorem, we can gain some knowledge on the valuations of these zeros. Hence if the gap sequence of the given curve is known, we can expect to gain some more insight into the splitting field.

Let us have a quick look at the proof of the main theorem. The proof follows the method of Sheats in [She98], i.e., we first expand each coefficient of T-powers with respect to a chosen basis of the Riemann-Roch spaces, then investigate the valuation of each non-zero summand, which is called the *weight* of the corresponding vector. The key point of the proof is to show that there exists a unique *optimal* element in the set of *valid compositions*, and it happens to be the so-called *greedy* element. To show this, we use combinatorical method developed in Sections 3.2 and 3.4. We will then prove in Section 3.3 the case $p = q$ and in Section 3.5 the other case. To be more precise, in Section 3.5, we show that if there exists an optimal element which is not greedy, then we can always construct a vector whose weight exceeds that of the 'optimal' one, hence get a contradiction. After gaining knowledge on the valuations of each coefficient, the theorem follows directly.

In Section 3.6, we will see an application of the above theorem to some special curves, namely the curves whose A's have strict class number 1, when the Goss zeta functions are exactly the same as the Goss-Thakur zeta functions. Note that as given in [Hay79], despite the projective lines, there exists exactly four curves with the corresponding A of strict class number 1. In Section 3.7, we look at some counter examples, when there exists an optimal element different from the greedy one. This implies that we should not expect to generalize Sheats' method to full generality, while on the other hand, although we only proved the theorem for curves whose genera are bounded by $O(q)$, the examples suggest that we may expect to improve the upper bound to $O(q^2)$ instead. In the last section, we can see that for certain cases, namely for hyperelliptic curves or the curves with a specified gap sequence, we are indeed able to achieve $O(q^2)$.

3.2 Basic Definitions and Results

In this section, we will introduce some basic definitions, e.g., the weight of a vector, valid compositions, optimal and greedy elements, etc., as well as some results regarding the weight. A particularly important result of this section is that all greedy and optimal elements are τ-monotonic, which provides us some insights on the structure of these elements. This result will play an important role when we deal with the case $q \neq p$.

By convention, we equip any vector space $\mathbb{Q}^k$ with a partial ordering, namely for $x = (x_1, \ldots, x_k)$ and $y = (y_1, \ldots, y_k)$, we say $x \leq y$ if and only if $x_i \leq y_i$ for all i; we say $x < y$ if $x \leq y$ and there exists at least one i such that $x_i < y_i$.

Let $L(n \cdot \infty) := \{a \in K^* : \mathrm{div}_K(a) + n \cdot \infty \text{ is effective}\} \cup \{0\}$ be the Riemann-Roch space for $n \in \mathbb{N}$. They form a sequence of finite dimensional sub-$\mathbb{F}_q$-vector spaces of A:

$$L(0 \cdot \infty) \subseteq L(1 \cdot \infty) \subseteq \ldots \subseteq L((n-1) \cdot \infty) \subseteq L(n \cdot \infty) \subseteq \ldots \subset A$$

Let l_n be the dimension of $L(n\infty)$. One has $l_0 = 1$, and by the Riemann-Roch theorem, $l_{2g-1+k} = g + k$ for $k \geq 0$. Then we can choose a sequence of functions $f_0, f_1, \ldots, f_n, \ldots$ such that for any n, the first l_n functions form a basis of $L(n\infty)$. We define a map:

$$\begin{aligned} \varphi : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto \varphi_n := \deg(f_n). \end{aligned}$$

Note that this map is injective, and strictly increasing. By definition, for any $\varphi_{d-1} \leq n < \varphi_d$, we have $d = \dim_{\mathbb{F}_q} L(n\infty)$ and the positive integers which do not occur as images of φ are exactly the Weierstrass gaps. It is easy to see that $\varphi_0 = 0$, and $\varphi_i = i + g$ for any $i \geq g$. Moreover, we define $\tilde{\varphi}_j$ to be

$$\tilde{\varphi}_j := \varphi_{j+1} - \varphi_j$$

for $j \geq 0$.

We have some immediate properties of $\tilde{\varphi}_i$'s.

Lemma 3.2.1. *We have the following:*

(a) $\tilde{\varphi}_0 = \varphi_1$*;*

(b) $1 \leq \tilde{\varphi}_j \leq g+1$ *for any* $0 \leq j \leq g-1$*;*

(c) $\tilde{\varphi}_j = 1$ *for any* $j \geq g$*.*

Moreover, we have

$$\sum_{j=0}^{g-1} \tilde{\varphi}_j = 2g.$$

All φ_i's form a semigroup, which is called the *Weierstrass semigroup*. It has the following important property:

Lemma 3.2.2 ([Tor94, Lemma 2.1])**.** *The following hold:*

(a) The curve $\mathcal{C}$ *is hyperelliptic if and only if* $\varphi_i = 2i$ *for* $i = 1, 2, \ldots, g$*;*

(b) The curve $\mathcal{C}$ *is non-hyperelliptic if and only if* $\varphi_i \geq 2i+1$ *for* $i = 1, 2, \ldots, g-2$ *and* $\varphi_{g-1} \geq 2g-2$*.*

By Lemma 3.2.2, we infer the following properties of $\tilde{\varphi}$:

Corollary 3.2.3. *The following hold:*

(a) $\tilde{\varphi}_i \leq \tilde{\varphi}_0$ *for* $i = 1, 2, \ldots, g-1$*.*

(b) The curve $\mathcal{C}$ *is hyperelliptic if and only if* $\tilde{\varphi}_i = 2$ *for* $i = 0, 1, \ldots, g-1$*.*

(c) If the curve $\mathcal{C}$ *is non-hyperelliptic, then*

(i) $\tilde{\varphi}_0 \geq 3$, $\tilde{\varphi}_{g-1} \leq 2$*;*

(ii) $\tilde{\varphi}_i \leq g-i$ *for* $i = 0, 1, \ldots, g-2$*.*

We now define the weight of an m-tuple of rationals in terms of the φ_j's:

Definition 3.2.4. Let $X = (X_0, \ldots, X_{m-1}) \in \mathbb{Q}^m$. Its *weight* is defined as

$$wt(X) := wt(X_0, \ldots, X_{m-1}) := \varphi_0 X_0 + \varphi_1 X_1 + \ldots + \varphi_{m-1} X_{m-1}.$$

Remark 3.2.5. Denote by $\tilde{X}_j := X_j + X_{j-1} + \ldots + X_0$ the partial sums of the coordinates, then we can apply Abel's summation formula to rewrite the above as

$$\begin{aligned} wt(X) =& \varphi_{m-1}\tilde{X}_{m-1} - \tilde{\varphi}_{m-2}\tilde{X}_{m-2} - \ldots - \tilde{\varphi}_0\tilde{X}_0 \\ =& \varphi_{m-1}n - \tilde{\varphi}_{m-2}\tilde{X}_{m-2} - \ldots - \tilde{\varphi}_0\tilde{X}_0. \end{aligned} \tag{3.1}$$

Definition 3.2.6. For any subset S of $\mathbb{Q}^m$, we say that $X = (X_0, \ldots, X_{m-1}) \in S$ is

(1) an *optimal* element of S if it has maximal weight among the elements in S;

(2) the *greedy* element of S if the tuple $(X_{m-1}, \ldots, X_0)$ is lexicographically largest.

Note that for any given set S, the greedy element is unique by definition, whereas it is likely to have several optimal elements.

Definition 3.2.7. An important subset of $\mathbb{Q}^m$ for our purpose will be the following:

$$\begin{aligned} U_m(n) := \{X = (X_0, X_1, \ldots, X_{m-1}) \in \mathbb{N}^m : & X_0 + \ldots + X_{m-1} = n, \\ & p \nmid \binom{n}{X_0, X_1, \ldots, X_{m-1}}, \\ X_i \text{ is a positive multiple of } q-1, & \text{ for } i = 0, 1, \ldots, m-2\}. \end{aligned}$$

We call the elements in $U_m(n)$ *valid compositions*.

We would like to make some observations regarding the greedy and optimal elements in $U_m(n)$.

Let $\tau(n)$ be the multiset consisting of all p-powers occurring in the p-adic expansion of n. Thus for each p^i, its multiplicity in $\tau(n)$ is exactly its coefficient in the p-adic expansion of n. Let $n = n_0 + n_1 p + n_2 p^2 + \ldots + n_l p^l$ with $0 \le n_0, n_1, \ldots, n_{l-1} \le p-1$ and $1 \le n_l \le p-1$, then

$$\tau(n) = \{\underbrace{p^0, \ldots, p^0}_{n_0 \text{ times}}, \underbrace{p^1, \ldots, p^1}_{n_1 \text{ times}}, \ldots, \underbrace{p^l, \ldots, p^l}_{n_l \text{ times}}\}.$$

We align the elements in $\tau(n)$ in non-decreasing order, and denote by $\tau^i(n)$ the i-th element in $\tau(n)$. By convention, let $\tau^0(n)$ be 0. It is easy to see that $\deg_p(n) = \log_p(\max \tau(n))$.

If $q \neq p$, then let s be $\log_p(q)$. Then we define for $h = 0, 1, \dots, s-1$ a submultiset $\tau_h(n)$ of $\tau(n)$, which containes all p^k's such that $k \equiv h \pmod{s}$, i.e.,

$$\tau_h(n) := \{p^k : p^k \in \tau(n) \text{ s.t. } k \equiv h \pmod{s}\}.$$

Similarly, we can define $\tau_h^i(n)$ to be the i-th element in $\tau_h(n)$ and $\tau_h^0(n) := 0$.

Definition 3.2.8. We call an element $X = (X_0, X_1, \dots, X_{m-1})$ *τ-monotonic* if

$$\max \tau_h(X_i) \leq \min \tau_h(X_j)$$

holds for any $0 \leq h \leq s-1$ and $i < j$.

Definition 3.2.9. Define a map Γ as follows

$$\begin{aligned} \Gamma : \mathbb{N}\backslash\{0\} &\to \mathbb{N}^s\backslash\{\underline{0}\} \\ n &\mapsto (|\tau_0(n)|, \dots, |\tau_{s-1}(n)|)^t. \end{aligned}$$

By convention, set $\Gamma(0) := \underline{0}$.

Remark 3.2.10. Note that this map Γ is surjective, since for any s-tuple in $\mathbb{N}^s\backslash\{\underline{0}\}$, denoted by $(a_0, \dots, a_{s-1})$, there exists a natural candidate for the preimage, given as follows:

$$n := \sum_{i=0}^{s-1} \sum_{k=0}^{\lfloor a_i/(p-1) \rfloor} \min\{a_i - k(p-1), p-1\} p^{i+ks}.$$

An immediate consequence from the definition is that

$$(1, p, \dots, p^{s-1}) \cdot \Gamma(n) \equiv n \pmod{p^s - 1}.$$

We denote by $\underline{\psi}_0$ the row vector $(1, p, \dots, p^{s-1})$. Then we can rewrite the previous statement as $\underline{\psi}_0 \cdot \Gamma(n) \equiv n \pmod{p^s - 1}$.

We can extend the map Γ to $\mathbb{N}^m$ as:

$$\begin{aligned} \Gamma^m : \qquad \mathbb{N}^m &\longrightarrow Mat_{s \times m}(\mathbb{N}) \\ (X_0, \dots, X_{m-1}) &\longmapsto (\Gamma(X_0), \dots, \Gamma(X_{m-1})). \end{aligned}$$

This map is again surjective following Remark 3.2.10.

Using the above notation, we can rewrite the conditions in the definition of valid compositions. Recall that by Lukas' lemma, the binomial coefficient $\binom{n}{n'}$ equals to the product of corresponding binomial coefficients of the p-adic expansion of n and n' in $\mathbb{F}_p$, hence it is not divisible by p if and only if $\tau(n')$ is a subset of $\tau(n)$.

(1) For non-negative integers $X_0, X_1, \ldots, X_{m-1}$ summing up to n, $\binom{n}{X_0,X_1,\ldots,X_{m-1}}$ is not divisible by p if and only if $\{\tau(X_0), \tau(X_1), \ldots, \tau(X_{m-1})\}$ is a partition of $\tau(n)$, i.e., the disjoint union of all $\tau(X_i)$'s happens to be $\tau(n)$.

(2) For $i = 0, 1, \ldots, m-2$, X_i being a positive multiple of $p^s - 1$ is equivalent to that $\underline{\psi}_0 \cdot \Gamma(X_i) \equiv 0 \pmod{p^s - 1}$ and $\Gamma(X_i) > 0$.

In particular, if $q = p$, then the second condition is equivalent to each $\tau(X_i)$ being a positive multiple of $p - 1$.

Lemma 3.2.11. *The greedy and optimal elements of $U_m(n)$ must be τ-monotonic.*

Proof. The greedy element is τ-monotonic by definition.

To show that an optimal element is τ-monotonic, we first observe that for any non-τ-monotonic element $X = (X_0, X_1, \ldots, X_{m-1}) \in U_m(n)$, there exists a pair (i, j) with $0 \le i < j \le m-1$ and some $h \in \{0, 1, \ldots, s-1\}$, such that we can find some $p^l \in \tau_h(X_i)$ and some $p^k \in \tau_h(X_j)$ such that $l > k$, then we can construct another valid composition

$$X' := (X_0, \ldots, X_i - p^l + p^k, \ldots, X_j + p^l - p^k, \ldots, X_{m-1}),$$

and

$$\begin{aligned} wt(X') = &\varphi_0 X_0 + \ldots + \varphi_i(X_i - p^l + p^k) + \ldots + \varphi_j(X_j + p^l - p^k) \\ &+ \ldots + \varphi_{m-1} X_{m-1} \\ = &\varphi_0 X_0 + \ldots + \varphi_i X_i + \ldots + \varphi_j X_j + \ldots + \varphi_{m-1} X_{m-1} \\ &+ (p^l - p^k)(\varphi_j - \varphi_i) \\ = &wt(X) + (p^l - p^k)(\varphi_j - \varphi_i) > wt(X). \end{aligned}$$

The above argument shows that whenever we have a non-τ-monotonic element, we can always construct another element with greater weight, hence an optimal element must be τ-monotonic. □

Definition 3.2.12. Let $B = (\underline{b}_0, \underline{b}_1, \ldots, \underline{b}_{m-1})$ be an $s \times m$-matrix with integral entries. Define the set of valid compositions of n with respect to B as

$$U_m^B(n) := \{X \in U_m(n) : \Gamma^m(X) = B\}.$$

The following lemma follows directly from construction.

Lemma 3.2.13. *If $U_m^B(n)$ is nonempty, then it has a unique τ-monotonic element.*

3.3 The $q = p$ case

Theorem 3.3.1. *If $q = p$, then any optimal element in $U_m(n)$ must be greedy.*

Proof. As shown in Lemma 3.2.11, the greedy element as well as all optimal elements in $U_m(n)$ must be τ-monotonic. Denote by G the greedy element and by O any optimal element. It suffices to show that both G and O lie in the same $U_m^B(n)$, i.e., $\Gamma^m(G) = \Gamma^m(O) =: B$. In fact, we can write down B explicitly:

$$B = (p-1, p-1, \dots, p-1, \Gamma(n) - (m-1)(p-1)) \,.$$

If this is true, due to Lemma 3.2.13, for a fixed B, the set $U_m^B(n)$, if non empty, contains a unique τ-monotonic element, so the optimal element must be greedy.

That $\Gamma^m(G) = B$ is clear by the greediness of G.

Suppose that there exists some optimal element O such that $\Gamma^m(O) = B'$ for some $B' \neq B$. From the structure of valid compositions, we know that B' must of the shape $(b_0(p-1), b_1(p-1), \dots, b_{m-2}(p-1), *)$ where $* = \Gamma(n) - (b_0 + b_1 + \dots + b_{m-2})(p-1)$ and $b_i \in \mathbb{Z}_{>0}$ with at least one b_i larger than 1. Let j be such that $b_j > 1$. Then we have that $|\tau(O_j)| = b_j(p-1)$, so that we can split the multiset $\tau(O_j)$ into two multisets $\tau_{1,j}$ and $\tau_{2,j}$ such that $\tau(O_j) = \tau_{1,j} \sqcup \tau_{2,j}$ and $|\tau_{1,j}| = p-1$. Let Q be the sum of all elements in $\tau_{1,j}$. Then we construct a new $O' = (O'_0, O'_1, \dots, O'_{m-1})$ by

$$O'_i = \begin{cases} Q & \text{for } i = j; \\ O_{m-1} - O_j + Q & \text{for } i = m-1; \\ O_i & \text{for } i \neq j,\, m-1. \end{cases}$$

It is easy to see that O' is again a valid composition of n and it has weight

$$\begin{aligned} wt(O') - wt(O) &= \varphi_j(Q - O_i) + \varphi_{m-1}(O_{m-1} - O_j + Q - O_{m-1}) \\ &= (O_i - Q)(\varphi_{m-1} - \varphi_j) > 0 \end{aligned}$$

because both $\varphi_{m-1} - \varphi_i$ and $O_i - Q$ are positive. This contradicts the optimality of O. □

Hence we can conclude that the zeros of large valuations are simple.

Theorem 3.3.2. *Suppose that $p = q$. Let n be a fixed positive integer. The following holds:*

(a) The x-coordinates of the break points of the Newton polygon associated to $\zeta_A(-n,T)$ are φ_i for all $i = 0, 1, \ldots$.

(b) The slope of the i-th segment between φ_{i-1} and φ_i is G_i^i, where G_i^i appears as the last entry of the greedy element in $U_{i+1}(n)$. In particular, the sequence $\{G_1^1, G_2^2, G_3^3, \ldots\}$ is strictly increasing.

Let $m \leq g$ be the smallest positive integer such that $\tilde{\varphi}_i = 1$ for all $i > m$. Except for the φ_m zeros of lowest valuations, all other zeros of $\zeta_A(-n,T)$ are simple with pairwise distinct valuations.

Proof. Recall that we define the Goss-Thakur zeta function as:

$$\zeta_A(-n,T) := \sum_{d \geq 0} T^d S_d(n),$$

where $S_d(n) = \sum_{a \in A_{+,d}} a^n$. As we have seen, there exists no function of degree d for d a Weierstrass gap, i.e., $S_d(n) = 0$, hence it suffices to consider only the $S_{\varphi_m}(n)$'s. Expanding $S_{\varphi_m}(n)$ with respect to the basis of the Riemann-Roch spaces we fixed in Section 3.2, we have

$$\begin{aligned} S_{\varphi_m}(n) &= \sum_{a \in A_{+,\varphi_m}} a^n = \sum_{a_i \in \mathbb{F}_p} (a_0 f_0 + \ldots + a_{m-1} f_{m-1} + f_m)^n \\ &= \sum_{a_i \in \mathbb{F}_p} \sum_{X_0 + \ldots + X_m = n} \binom{n}{X_0, \ldots, X_m} a_0^{X_0} \ldots a_{m-1}^{X_{m-1}} f_0^{X_0} \ldots f_{m-1}^{X_{m-1}} f_m^{X_m} \\ &= \sum_{X \in \mathbb{N}^{m+1}} T_X, \end{aligned}$$

where

$$T_X := \begin{cases} \sum_{a_i \in \mathbb{F}_p} \binom{n}{X_0, \ldots, X_m} a_0^{X_0} \ldots a_{m-1}^{X_{m-1}} f_0^{X_0} \ldots f_{m-1}^{X_{m-1}} f_m^{X_m}, & \text{if } \sum_{i=0}^{m} X_i = n; \\ 0, & \text{otherwise.} \end{cases}$$

It is easy to see that T_X is nonzero if and only if $X \in U_{m+1}(n)$. Comparing the definition of the weight of $X \in U_{m+1}(n)$ and the valuation of T_X at ∞, we see that $v_\infty(T_X) = -wt(X)$. Moreover, by Theorem 3.3.1, if the set $U_{m+1}(n)$ is nonempty, then it contains a unique optimal element, which is just the greedy element. Let G^{m+1} be the greedy element in $U_{m+1}(n)$. Then $T_{G^{m+1}}$ is the summand with smallest valuation hence it determines the valuation of $S_{\varphi_m}(n)$.

Write $n = n_0 + n_1 + \ldots + n_l$ where

$$\begin{aligned}
&n_0 = \tau^1(n) + \ldots + \tau^{p-1}(n);\\
&n_1 = \tau^p(n) + \ldots + \tau^{2(p-1)};\\
&\ldots\\
&n_{l-1} = \tau^{(l-1)(p-1)+1}(n) + \ldots + \tau^{l(p-1)}(n);\\
&n_l = n - n_{l-1} - \ldots - n_1 - n_0,
\end{aligned}$$

where $l = \lfloor \frac{\mathrm{digsum}_p(n)}{p-1} \rfloor$. Hence l is the largest integer such that $U_{l+1}(n)$ is nonempty and the greedy element in $U_{m+1}(n)$ is just $(n_0, \ldots, n_{m-1}, n_m + \ldots + n_l)$ for any $m \leq l$. We can thus compute the weight of $T_{G^{m+1}}$ thus the valuation of $S_{\varphi_m}(n)$:

$$\begin{aligned}
v_\infty(S_{\varphi_m}(n)) =& v_\infty(T_{G^{m+1}}) = -wt(G^{m+1})\\
=& -(\varphi_0 n_0 + \ldots + \varphi_{m-1} n_{m-1} + \varphi_m(n_m + \ldots + n_l)).
\end{aligned}$$

Therefore, we can compute the m-th slope as

$$\frac{v_\infty(S_{\varphi_m}(n)) - v_\infty(S_{\varphi_{m-1}}(n))}{\varphi_m - \varphi_{m-1}} = -(n_m + \ldots + n_l).$$

We can conclude that all of these points appear as break points of the Newton polygon. In particular, when $m \geq g$, all the slopes have horizontal width one, which means that except for the zeros of the lowest g valuations, i.e., the $2g$ zeros of smallest valuations, all the other zeros are simple and have pairwise distinct valuations. □

3.4 Some facts for the case $q \neq p$

After dealing with the case $q = p$, we now move on to consider the case $q \neq p$. In this section, we will see some results which help to prepare for the proof of the main result for the case $q \neq p$. We start by investigating some properties of the structure of $\Gamma(n)$ when n is a positive multiple of $q - 1$. This is followed by a characterization of nonempty $U_m^B(n)$'s and how to construct an optimal or greedy element from existing ones for some other n or m. Next, we define some special subsets of $\mathbb{N}$ depending on the maximal length of valid compositions. We can then locate most of the entries of optimal and greedy elements with respect to these sets. At the end of this section, we will show Proposition 3.8.2, where an element of special properties is constructed. This will be of importance in our proof of the main theorem.

From now on, we always assume that $q \neq p$, i.e., $s \geq 2$.

Let $\underline{e}_0, \underline{e}_1, \ldots, \underline{e}_{s-1}$ be the standard basis of column vectors in $\mathbb{Q}^s$. We define the $s \times s$-matrix $E := (\underline{\epsilon}_0, \underline{\epsilon}_1, \ldots, \underline{\epsilon}_{s-1})$, where $\underline{\epsilon}_i = p\underline{e}_{i-1} - \underline{e}_i = (0, \ldots, 0, p, -1, 0, \ldots, 0)^t$ for $i = 1, 2, \ldots, s-1$, and $\underline{\epsilon}_0 = p\underline{e}_{s-1} - \underline{e}_0 = (-1, 0, \ldots, 0, p)^t$; define $R := (\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_{s-1}, \underline{e}_0)$, and $\underline{\psi}_i := \underline{\psi}_0 \cdot R^{-i}$, i.e.,

$$E = \begin{pmatrix} -1 & p & & & \\ & -1 & p & & \\ & & \ddots & \ddots & \\ & & & -1 & p \\ p & & & & -1 \end{pmatrix}, \; R = \begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix},$$

and $\underline{\psi}_i = (p^{s-i}, p^{s-i+1}, \ldots, p^{s-1}, 1, \ldots, p^{s-i-1})$.

Lemma 3.4.1 ([She98, Lemma 3.3, Lemma 4.2])**.** *Let $s \geq 2$. For a vector X, we denote by X_j the j-th coordinate of X.*

(a) For $n \in \mathbb{N}$, we have that $n \equiv \underline{\psi}_0 \cdot \Gamma(n) \pmod{p^s - 1}$.

(b) For $X \in \mathbb{Q}^s$, we have that $\underline{\psi}_i \cdot EX = X_i(p^s - 1)$.

(c) Let I_s be the identity matrix of size $s \times s$. We have that $E + I_s = p \cdot R^{-1}$ and $RE = ER$.

(d) For $X \in \mathbb{Z}^s$, we have that $\underline{\psi}_0 \cdot RX \equiv p \cdot \underline{\psi}_0 \cdot X \pmod{p^s - 1}$.

(e) For $X \in \mathbb{Z}^s$, we have that $\underline{\psi}_0 \cdot X \equiv p^i \cdot \underline{\psi}_i \cdot X \pmod{p^s - 1}$.

(f) For any $k \in \mathbb{N}$, we have that $R^k\Gamma(n) = \Gamma(p^k n)$.

Recall that we associate a partial ordering to the vector space $\mathbb{Q}^s$ or $\mathbb{Q}^m$. The following lemma concerns some basic properties of E with respect to this partial ordering.

Lemma 3.4.2 ([She98, Lemma 4.2])**.** *The following holds:*

(a) $\{E^{-1}X : X > 0\} \subseteq (\mathbb{Q}^+)^s$.

(b) If $X > Y$, then $E^{-1}X > E^{-1}Y$.

We define $\mathfrak{J}$ to be the set of all $\Gamma(n)$ where n is a positive multiple of $p^s - 1$.

Lemma 3.4.3 ([She98, Lemma 3.4])**.** *We have that*

$$\mathfrak{J} = (E\mathbb{Z}^s) \cap (\mathbb{N}^s \backslash \{\underline{0}\}).$$

In other words, $\mathfrak{J}$ is a submonoid under '+' consisting of all positive elements of the $\mathbb{Z}$-lattice generated by the $\underline{\epsilon}_i$'s.

Corollary 3.4.4. *The set $\mathfrak{J}$ is stable under left multiplication by R, i.e., $R\mathfrak{J} = \mathfrak{J}$.*

Proof. This follows directly from Lemma 3.4.3 and Lemma 3.4.1 (c). □

Lemma 3.4.5. *Let $B = (\underline{b}_0, \underline{b}_1, \ldots, \underline{b}_{m-1})$ be an $s \times m$-matrix with integral entries. Then $U_m^B(n)$ is nonempty if and only if the following two conditions are fulfilled:*

(a) the columns of B sum up to $\Gamma(n)$;

(b) for $i = 0, 1, \ldots, m-2$, we have $\underline{b}_i \in \mathfrak{J}$.

Proof. If $U_m^B(n)$ is nonempty, then there exists some $X = (X_0, X_1, \ldots, X_{m-1})$ such that $\Gamma(X) = B$, i.e., $b_i = \Gamma(X_i)$. Conditions (a) and (b) follow directly from the definition of a valid composition. The inverse follows directly from the surjectivity of Γ. □

Remark 3.4.6. One may notice that the above Lemma is quite similar to Lemma 3.5 in [She98], but we should remember that in our case, the last column of the matrix B can be the zero vector.

Proposition 3.4.7. *Suppose $X = (X_0, X_1, \ldots, X_{m-1})$ is optimal (or greedy) in $U_m(n)$, then*

(a) If $p^k \in \tau(X_{m-1})$, then $(X_0, X_1, \ldots, X_{m-2}, X_{m-1} - p^k)$ is optimal (or greedy) in $U_m(n - p^k)$.

(b) If n' is an integer such that $\tau(n') \subset \Gamma(X_{m-1})$, then $(X_0, X_1, \ldots, X_{m-2}, X_{m-1} - n')$ is optimal (or greedy) in $U_m(n-n')$. In particular, in the case of $n' = X_{m-1}$, the tuple $(X_0, X_1, \ldots, X_{m-2}, 0)$ is optimal (or greedy) in $U_m(n - X_{m-1})$.

(c) *For any integer $k \geq 0$, the tuple $(p^k X_0, p^k X_1, \ldots, p^k X_{m-1})$ is optimal (or greedy) in $U_m(p^k n)$.*

Proof. The greedy parts for all three statements are clear. We only need to show that these hold for optimal elements.

(a) Suppose $X' = (X_0, X_1, \ldots, X_{m-2}, X_{m-1} - p^k)$ is not optimal, then there exists some $Z = (Z_0, Z_1, \ldots, Z_{m-1}) \in U_m(n - p^k)$ such that $wt(Z) > wt(X')$. We consider $Z' = (Z_0, Z_1, \ldots, Z_{m-2}, Z_{m-1} + p^k)$. It clearly lies in $U_m(n)$ and we can compute its weight as

$$wt(Z') = wt(Z) + \varphi_{m-1} p^k > wt(X') + \varphi_{m-1} p^k = wt(X),$$

and this contradicts the optimality of X.

(b) This follows directly from (a).

(c) It is easy to see that $X' = (p^k X_0, p^k X_1, \ldots, p^k X_{m-1})$ is indeed a valid composition of $p^k n$, since when looking at the p-adic expansion of n, multiplying p^k just means adding k to all exponents, while the coefficients stay invariant. Therefore, for any p-power in $\tau(p^k n)$, the exponent must be larger than k, i.e., each element in $\tau(p^k n)$ is a multiple of p^k.

Suppose that X' is not optimal, then there exists some $Z = (Z_0, Z_1, \ldots, Z_{m-1})$ which is optimal in $U_m(p^k n)$ and $wt(Z) > wt(X')$. We define

$$Z' := (p^{-k} Z_0, p^{-k} Z_1, \ldots, p^{-k} Z_{m-1}).$$

Note that for any i, $p^{-k} Z_i$ is an integer, since all elements in $\tau(Z_i) \subset \tau(p^k n)$ are divisible by p^k. Hence Z lies in $U_m(n)$, and

$$wt(Z') = p^{-k} wt(Z) > p^{-k} wt(X') = wt(X),$$

which contradicts the optimality of X.

□

Now, we introduce two sets of vectors and will try to fully characterize them.

Definition 3.4.8. For any $m \in \mathbb{Z}_{>0}$, we define:

$$I_m := \{\Gamma(n) : n \in \mathbb{N} \text{ and } U_m(n) \neq \emptyset\},$$
$$J_m := \mathfrak{J} \cap (I_m \backslash I_{m+1}).$$

In other words, I_m contains all vectors corresponding to those k's which have valid compositions of length m, and J_m is the set of all vectors corresponding to the positive multiples of $p^s - 1$ whose longest valid decompositions have length exactly m. Note that $J_1 = \emptyset$, and for $m \geq 2$, for any k such that $\Gamma(k) \in J_m$, its valid compositions of length m always has 0 as the last entry. The relations among different m's are

$$\begin{aligned} &I_1 \supset I_2 \supset \ldots \supset I_m \supset I_{m+1} \supset \ldots, \\ &\mathfrak{J} = \sqcup_{m \geq 1} J_m. \end{aligned}$$

Remark 3.4.9. Recall that in [She98], Sheats defined similar subsets, also denoted by I_m and J_m. To distinguish these from the sets we defined here, let us denote the sets defined by Sheats by I_m^S and J_m^S respectively. The main difference between I_m^S and I_m (resp. J_m^S and J_m) is that the vectors in I_m^S (resp. J_m^S) have by definition nonzero last entries, but this condition does not apply to those in I_m (resp. J_m). However, there is a simple relation between I_m^S and I_m (resp. J_m^S and J_m), which will be given as follows:

$$\begin{aligned} &I_m = I_m^S \cup J_m; \\ &J_m = \{(X_0, \ldots, X_{m-2}, 0) : (X_0, \ldots, X_{m-2}) \in J_{m-1}^S\}. \end{aligned}$$

Proposition 3.4.10. *Let I_m and J_m be defined as above. Then for $m \geq 2$, we have:*

$$\begin{aligned} I_m =& \{\underline{u} \in \mathbb{N}^s : \exists\, \underline{v}_0, \ldots, \underline{v}_{m-2} \in \mathfrak{J} \text{ s.t. } \underline{u} \geq \underline{v}_0 + \ldots + \underline{v}_{m-2}\} \\ =& \{\underline{u} \in \mathbb{N}^s : \exists\, \underline{\eta}_0, \ldots, \underline{\eta}_{m-2} \in \mathfrak{J} \text{ s.t. } \underline{u} \geq \underline{\eta}_{m-2} > \ldots > \underline{\eta}_0\} \\ =& \{E\underline{a} \in \mathbb{N}^s : \underline{a} \in \mathbb{Q}^s, m-1 \leq \min\{a_0, \ldots, a_{s-1}\}\}; \\ J_m =& \{E\underline{a} \in \mathbb{N}^s : \underline{a} \in \mathbb{Z}^s, m-1 = \min\{a_0, \ldots, a_{s-1}\}\}. \end{aligned}$$

Proof. The proof follows from Remark 3.4.9 and [She98, p. 136]. In the first equation, suppose that $(X_0, X_1, \ldots, X_{m-1}) \in U_m(n)$, then we can just choose those $\underline{v}_i$'s to be the $\Gamma(X_i)$'s; the $\underline{\eta}_j$'s in the second equation are partial sums of $\sum \underline{v}_i$; and the third equation follows from Lemma 3.4.2 and Lemma 3.4.3; the last one follows directly from the third one. □

Note that for any $E\underline{a} \in I_m$ or J_m, we always have that $a_i \leq mq^{s-1}$.

Definition 3.4.11. According to Proposition 3.4.10, we can define a sequence of subsets: for $i = 0, 1, \ldots, s-1$, we define

$$J_m^i := \{E\underline{a} \in \mathbb{N}^s : \underline{a} \in \mathbb{Z}^s, a_i = m-1 = \min\{a_0, \ldots, a_{s-1}\}\}.$$

Note that J_m is the union of all J_m^i's, but this is not necessarily a disjoint union!

Lemma 3.4.12. *Suppose that $X = (X_0, X_1, \dots, X_{m-1}) \in U_m(n)$ is greedy or optimal. Then $\Gamma(X_i) \in J_2$ for $i = 0, 1, \dots, m-2$.*

Proof. Suppose that there exists some i such that $X_i \notin J_2$. Then there exists a valid composition of X_i of length 3, say (y_0, y_1, y_2), where y_0 and y_1 are positive multiples of p^s-1 and y_2 is either 0 or a positive multiple of p^s-1. We can construct a new composition X' of n, namely $X'_j = X_j$ for any $j \neq i, m-1$, $X'_i = y_0$ and $X'_{m-1} = X_{m-1} + y_1 + y_2$. It is clear that X' is again a valid composition and $X'_i < X_i$, $X'_{m-1} > X_{m-1}$.

Then X cannot be greedy since $(X'_{m-1}, \dots, X'_0)$ is lexicographically larger than X; on the other hand, X cannot be optimal either, since

$$\begin{aligned} wt(X') - wt(X) =& (\varphi_0 X'_0 + \dots + \varphi_i X'_i + \dots + \varphi_{m-2} X'_{m-2} + \varphi_{m-1} X'_{m-1}) \\ & - (\varphi_0 X_0 + \dots + \varphi_i X_i + \dots + \varphi_{m-2} X_{m-2} + \varphi_{m-1} X_{m-1}) \\ =& \varphi_i (X'_i - X_i) + \varphi_{m-1}(X'_{m-1} - X_{m-1}) \\ =& (\varphi_{m-1} - \varphi_i)(y_1 + y_2) > 0. \end{aligned}$$

□

Lemma 3.4.13. *Let $\underline{u} \in J_m$ for some $m \geq 2$. Suppose that $\underline{v} \in \mathbb{N}^s$ such that $\underline{v} \leq (p-1, p-1, \dots, p-1)^t$ and $\underline{v} < \underline{u}$. Then $\underline{u} - \underline{v} \in I_{m-1}$.*

Proof. By Lemma 3.4.3, we know that $\underline{u} = E\underline{a}$ for some $\underline{a} \in \mathbb{Z}^s$ and $\underline{v} = E\underline{b}$ for some $\underline{b} \in \mathbb{Q}^s$. Then $\underline{u} - \underline{v} = E(\underline{a} - \underline{b})$. Since $\underline{v} \leq (p-1, p-1, \dots, p-1)^t$, Lemma 3.4.2 implies that $\underline{b} \leq E^{-1}(p-1, p-1, \dots, p-1)^t = (1, 1, \dots, 1)^t$. On the other hand, since $\underline{u} \in J_m$, we know that $m - 1 = \min\{a_0, \dots, a_{m-1}\}$. Since $\underline{v} < \underline{u}$, we have that $a_i - b_i \geq m-2$ for any i, thus $\underline{u} - \underline{v} \in I_{m-1}$. □

Proposition 3.4.14. *Suppose that n is a positive multiple of $p^s - 1$, such that $\Gamma(n) \in I_{m+1}$. Let X be optimal or greedy in $U_m(n)$. Then we have*

$$\phi_m n \leq wt(X) \leq \varphi_{m-1} n,$$

where the ϕ_m's are given as follows:

$$\begin{aligned} \phi_1 =& 0,\ \phi_2 = \frac{q+p-2}{q+p}\varphi_1, \\ \phi_m =& \frac{q+p-2}{q+p}\left(\left(\frac{2}{q+p}\right)^{m-2}\varphi_1 + \dots + \frac{2}{q+p}\varphi_{m-2} + \varphi_{m-1}\right). \end{aligned}$$

Remark 3.4.15. The reason to require $\Gamma(n)$ lying in I_{m+1} is that in this case, for $G = (G_0, G_1, \ldots, G_{m-1})$ the greedy element in $U_m(n)$, we have that G_{m-1} must be nonzero. Because $U_{m+1}(n) \neq \emptyset$, there exists some $(X_0, X_1, \ldots, X_{m-1}, X_m) \in U_{m+1}(n)$, where $X_{m-1} > 0$ and $X_m \geq 0$, hence $(X_0, X_1, \ldots, X_{m-2}, X_{m-1} + X_m)$ lies in $U_m(n)$ and $X_{m-1} + X_m \geq X_{m-1} > 0$. By the greediness of G, we must have $G_{m-1} \geq X_{m-1} + X_m > 0$.

Proof to Proposition 3.4.14. The upper bound is trivial since $\varphi_i < \varphi_{m-1}$ for all $i < m-1$, and

$$\begin{aligned} wt(X) = &\varphi_0 X_0 + \varphi_1 X_1 + \ldots + \varphi_{m-1} X_{m-1} \\ < &\varphi_{m-1}(X_0 + X_1 + \ldots + X_{m-1}) = \varphi_{m-1} n. \end{aligned}$$

Note that the upper bound is reached if and only if $m = 2$.

To prove the lower bound, it suffices to take only the greedy element G into consideration. Let G be $(G_0, G_1, \ldots, G_{m-1})$. Then $G_{m-1} > 0$ by Remark 3.4.15. Let $n = n_0 p^0 + \ldots + n_l p^l$ be the p-adic expansion of n, then let

$$n' = n_l p^l + \ldots + n_{l-s+1} p^{l-s+1} + \min\{n_{l-s}, (p-1) - n_l\} p^{l-s}.$$

Clearly we have

$$\Gamma(n') \leq (p-1, p-1, \ldots, p-1)^t.$$

By the greediness of G and the fact that G_{m-1} must be a positive multiple of $p^s - 1$, we have that $G_{m-1} \geq n'$.

Let us now compare n' and $n - n'$. Denote by $m := \min\{n_{l-s}, (p-1) - n_l\}$. Then $n' \geq (n_l q + m) p^{l-s}$ and $n - n' \leq (n_{l-s} + 1 - m) p^{l-s}$. Hence

$$\frac{n'}{n - n'} \geq \frac{n_l q + m}{n_{l-s} + 1 - m}.$$

And we can estimate the right hand side in the following two cases; denote $i := n_l$ for abbreviation:

1. when $n_{l-s} = 0, \ldots, p - 1 - i$, then $m = n_{l-s}$, hence

   $$RHS = \frac{iq + n_{l-s}}{n_{l-s} + 1 - n_{l-s}} = iq + n_{l-s}.$$

   In this case, the lower bound is iq;

2. when $n_{l-s} > p-1-i$, then $m = p-1-i$, hence

$$RHS = \frac{iq+p-1-i}{n_{l-s}+1-p+1+i} = \frac{i(q-1)+p-1}{n_{l-s}+2-p+i}.$$

   In this case, the lower bound is

$$\frac{i(q-1)+p-1}{p-1+2-p+i} = q-1-\frac{q-p}{i+1}.$$

Vary i and we can get a lower bound of the right hand side:

$$RHS \geq \frac{q+p}{2} - 1,$$

and we achieve this lower bound when $n_l = 1$, $n_{l-s} = p-1$. Hence $\frac{n'}{n-n'} \geq \frac{q+p}{2} - 1$ and $\frac{n'}{n} \geq \frac{q+p-2}{q+p}$.

Now we prove the lower bound of $wt(X)$ by induction:

for any m and the greedy element $G = (G_0, G_1, \ldots, G_{m-1})$, we know that $G' = (G_0, G_1, \ldots, G_{m-2})$ is the greedy element in $U_{m-1}(n - G_{m-1})$, hence

$$\begin{aligned} wt(G) &= wt(G') + \varphi_{m-1}G_{m-1} \\ &\geq \phi_{m-1}(n - G_{m-1}) + \varphi_{m-1}G_{m-1} \\ &= \phi_{m-1}n + (\varphi_{m-1} - \phi_{m-1})G_{m-1} \\ &\geq (\phi_{m-1} + (\varphi_{m-1} - \phi_{m-1})\frac{q+p-2}{q+p})n. \end{aligned}$$

The proposition follows straightforwardly. □

The next lemma concerns the size of ϕ_m compared with φ_m's. Recall that we always assume that $q \neq p$. Let χ be $\frac{2}{p+q}$.

Lemma 3.4.16. *For any g and $m \geq g+2$, we have that*

$$\phi_m > \varphi_{m-2}.$$

Proof. Recall that

$$\begin{aligned} \phi_1 &= 0,\ \phi_2 = \frac{q+p-2}{q+p}\varphi_1 = (1-\chi)\varphi_1, \\ \phi_m &= \frac{q+p-2}{q+p}((\frac{2}{q+p})^{m-2}\varphi_1 + \ldots + \frac{2}{q+p}\varphi_{m-2} + \varphi_{m-1}) \\ &= (1-\chi)(\chi^{m-1}\varphi_1 + \ldots + \chi\varphi_{m-2} + \varphi_{m-1}). \end{aligned}$$

Then

$$\begin{aligned}\phi_m - \varphi_{m-2} =& (1-\chi)(\chi^{m-2}\varphi_1 + \ldots + \chi\varphi_{m-2} + \varphi_{m-1}) - \varphi_{m-2}\\ =& (1-\chi)\chi^{m-2}\varphi_1 + \ldots + (1-\chi)\chi\varphi_{m-2} + (1-\chi)\varphi_{m-1} - \varphi_{m-2}\\ =& \varphi_{m-1} - \varphi_{m-2} - \chi(\varphi_{m-1} - \varphi_{m-2}) - \chi^2(\varphi_{m-2} - \varphi_{m-3}) - \ldots\\ & - \chi^{m-2}(\varphi_2 - \varphi_1) - \chi^{m-1}\varphi_1\\ =& (1-\chi)\tilde{\varphi}_{m-2} - \chi^2\tilde{\varphi}_{m-3} - \chi^3\tilde{\varphi}_{m-4} - \ldots - \chi^{m-1}\tilde{\varphi}_0.\end{aligned}$$

When $m-2$ is at least g, then by Corollary 3.2.3 and the fact that $\chi < 1$, we have an immediate lower bound of the above sum, which is reached when $\tilde{\varphi}_i = 2$ for $i = 0, 1, \ldots, g-1$, and we have:

$$\begin{aligned}\phi_m - \varphi_{m-2} \geq& (1-\chi) - \chi^2 - \chi^3 - \ldots - \chi^{m-g-1} - 2\chi^{m-g} - \ldots - 2\chi^{m-1}\\ =& 2 - \frac{1-\chi^m}{1-\chi} - \frac{\chi^{m-g} - \chi^m}{1-\chi}\\ \geq& 1 - \frac{\chi + \chi^{m-g}}{1-\chi}\\ =& \frac{1-2\chi-\chi^2}{1-\chi}.\end{aligned}$$

Since $0 < \chi \leq \frac{1}{3}$, $1 - 2\chi - \chi^2$ must be positive, hence $\phi_m > \varphi_{m-2}$. □

The same holds for all m if we bound the genus g.

Lemma 3.4.17. *Suppose that $g < \chi^{-2} - \chi^{-1} - 1$, then for any $m \geq 2$, we always have*

$$\phi_m > \varphi_{m-2}.$$

Proof. Same as above, we can compute the difference of ϕ_m and φ_{m-2} as:

$$\phi_m - \varphi_{m-2} = (1-\chi)\tilde{\varphi}_{m-2} - \chi^2\tilde{\varphi}_{m-3} - \chi^3\tilde{\varphi}_{m-4} - \ldots - \chi^{m-1}\tilde{\varphi}_0.$$

If $m-2 \geq g$, then we can use the same argument as in the proof to Lemma 3.4.16 to obtain

$$\phi_m - \varphi_{m-2} \geq 1 - \frac{\chi + \chi^{m-g}}{1-\chi}.$$

As $\chi < 1$, and $m - 2 \geq g$, we have

$$\phi_m - \varphi_{m-2} \geq 1 - \frac{\chi + \chi^2}{1-\chi} > 0.$$

If $m-2 < g$, then all $\tilde{\varphi}_j$'s must lie between 1 and $g+1$, and we achieve the lower bound when $\tilde{\varphi}_i = \frac{m-2+g}{m-2}$ for $i = 0, 1, \ldots, m-3$ and $\tilde{\varphi}_i = 1$ for $i \geq m-2$, then we have

$$\begin{aligned}
\phi_m - \varphi_{m-2} \geq & (1-\chi) - \frac{m-2+g}{m-2}\chi^2 - \frac{m-2+g}{m-2}\chi^3 - \ldots - \frac{m-2+g}{m-2}\chi^{m-1} \\
= & 1 - \chi - \chi^2 - \ldots - \chi^{m-1} - \frac{g}{m-2}(\chi^2 + \ldots + \chi^{m-1}) \\
= & 1 - \frac{\chi - \chi^m}{1-\chi} - \frac{g}{m-2}\frac{\chi^2 - \chi^m}{1-\chi} \\
\geq & 1 - \frac{\chi - \chi^3}{1-\chi} - g\chi^2.
\end{aligned}$$

As $g < \chi^{-2} - \chi^{-1} - 1$, then $\phi_m < \varphi_{m-2}$. □

From now on, we fix g_0 to be $\chi^{-2} - \chi^{-1} - 1$.

Proposition 3.4.18. *Suppose that $g < g_0$ or $m \geq g+2$. If X is optimal or greedy in $U_m(n)$, then $\Gamma(n - X_{m-1}) \in J_m$.*

Proof. Let $X = (X_0, X_1, \ldots, X_{m-1})$ be optimal or greedy in $U_m(n)$. Clearly $\Gamma(n - X_{m-1})$ lies in $\mathfrak{J} \cap I_m$ since $(X_0, X_1, \ldots, X_{m-2}, 0) \in U_m(n - X_{m-1})$, and $n - X_{m-1}$, which is the sum of $X_0, \ldots, X_{m-2}$, must be a positive multiple of $p^s - 1$.

If $\Gamma(n - X_{m-1}) \notin J_m$, then $\Gamma(n - X_{m-1}) \in \mathfrak{J} \cap I_{m+1}$, in particular, $U_{m+1}(n - X_{m-1})$ is nonempty. Let $G = (G_0, \ldots, G_{m-1})$ be the greedy element in $U_m(n - X_{m-1})$, then $G_{m-1} > 0$, by Remark 3.4.15. We define $G' := (G_0, G_1, \ldots, G_{m-2}, G_{m-1} + X_{m-1}) \in U_m(n)$. Then by Proposition 3.4.14, we have

$$wt(G') = wt(G) + \varphi_{m-1}X_{m-1} \geq \phi_m(n - X_{m-1}) + \varphi_{m-1}X_{m-1}.$$

On the other hand, we have a natural upper bound for the weight of X:

$$wt(X) = \sum_{i=0}^{m-2} \varphi_i X_i + \varphi_{m-1}X_{m-1} \leq \varphi_{m-2}(n - X_{m-1}) + \varphi_{m-1}X_{m-1}.$$

Since $m \geq g+2$ (resp. $g < g_0$), we have by Lemma 3.4.16 (resp. Lemma 3.4.17) that $\phi_m > \varphi_{m-2}$, hence $wt(X) < wt(G')$, contradicting the optimality of X. □

Corollary 3.4.19. *Suppose that $g < g_0$ or $m \geq g+2$. Let $O = (O_0, \ldots, O_{m-1})$ resp. $G = (G_0, \ldots, G_{m-1})$ be optimal resp. greedy in $U_m(n)$. Then $O_{m-1} = 0$ if and only if $G_{m-1} = 0$.*

Proposition 3.4.20. *Suppose that $g < g_0$ or $m \geq g+2$. If X is optimal or greedy in $U_m(n)$, then there exists some i such that $\Gamma(X_j) \in J_2^i$ for all $0 \leq j \leq m-2$.*

Proof. By Lemma 3.4.12, for $0 \leq j \leq m-2$, we always have $\Gamma(X_j) \in J_2$, i.e.,

$$\min_{i=0,1,\ldots,s-1} (E^{-1}\Gamma(X_j))_i = 1$$

where $(E^{-1}\Gamma(X_j))_i$ denotes the i-th coordinate of $E^{-1}\Gamma(X_j)$.

But by Proposition 3.4.18, we know that $\Gamma(n - X_{m-1}) \in J_m$, i.e.,

$$\min_i (E^{-1}\Gamma(n - X_{m-1}))_i = m-1.$$

Since there is no carryover of p-adic digits in the sum $n = \sum_{i=0}^{m-1} X_i$, we can rewrite $E^{-1}\Gamma(n - X_{m-1})$ as:

$$\begin{aligned} E^{-1}\Gamma(n - X_{m-1}) &= E^{-1}\Gamma(X_0 + X_1 + \ldots + X_{m-2}) \\ &= E^{-1}\Gamma(X_0) + E^{-1}\Gamma(X_1) + \ldots + E^{-1}\Gamma(X_{m-2}), \end{aligned}$$

hence the i-th coordinate of $E^{-1}\Gamma(n - X_{m-1})$ is the sum of all i-th coordinates of $E^{-1}\Gamma(X_j)$ for $0 \leq j \leq m-2$. But each of them is at least 1, so there must exist at least one i such that $(E^{-1}\Gamma(X_j))_i = 1$ for all $0 \leq j \leq m-2$, i.e., $\Gamma(X_j) \in J_2^i$. □

Corollary 3.4.21. *Suppose that $g < g_0$ or $m \geq g+2$. If X is optimal or greedy in $U_m(n)$, then $(X_0, \ldots, X_{m-2})$ is optimal or greedy in $U_{m-1}(n - X_{m-1})$.*

Corollary 3.4.22. *Suppose that $g < g_0$ or $m \geq g+2$. Let m be such that $\Gamma(n) \in I_m \backslash I_{m+1}$ and $G = (G_0, \ldots, G_{m-1})$ be the greedy element in $U_m(n)$. Then the greedy element in $U_i(n)$ for any $i \leq m$ is*

$$(G_0, \ldots, G_{i-2}, G_{i-1} + \ldots + G_{m-1}).$$

Proposition 3.4.23. *Suppose that $q \neq p$ and $g < g_0$. If there exists some n' and m' such that in $U_{m'}(n')$ exists an optimal element $O' = (O'_0, \ldots, O'_{m'-1})$ which is different from the greedy element. Then there exist an n, an m and an $O = (O_0, O_1, \ldots, O_{m-1})$ optimal in $U_m(n)$ satisfying the following properties:*

(i) $\Gamma(O_j) \in J_2^0$, *for* $0 \leq j \leq m-2$.

(ii) $\deg_p(O_{m-1}) < \deg_p(G_{m-1})$, *where $G = (G_0, G_1, \ldots, G_{m-1})$ is the greedy element in $U_m(n)$.*

(iii) $\Gamma(O_{m-1}) \neq \Gamma(G_{m-1})$.

(iv) $O_{m-1} = p^{\tilde{\omega}}$ *for some* $\tilde{\omega} \in \mathbb{N}$.

(v) $\underline{\psi}_0 \cdot \Gamma(O_{m-1}) = \underline{\psi}_0 \cdot \Gamma(G_{m-1})$.

Remark 3.4.24. We first make some observations on the size of m if there exists an optimal element in $U_m(n)$ which is not greedy. Firstly, m cannot be 1 since $U_1(n) = \{(n)\}$, which is a singleton-set. It means that there is no room for optimal elements being different from the greedy element. Secondly, m cannot be 2 either, since $U_2(n) = \{(n-a, a) \mid 0 \leq a < n, a \equiv n \pmod{p^s - 1}, \tau(a) \subset \tau(n)\}$, and the weight of such a typical element $(n-a, a)$ is $wt(n-a, a) = \varphi_1 a$, which is fully determined by a, so the maximality of weight is equivalent to the maximality of a, i.e., an optimal element must be greedy in $U_2(n)$. Therefore, m must be at least 3. We will see some examples for $m = 3$ in Section 3.7.

Proof of Proposition 3.4.23. Recall that we denote by $\mathrm{digsum}_p(n)$ the p-adic digit sum of n, i.e., if the p-adic expansion of n is $\sum_{i=0}^{l} a_i p^i$ with $0 \leq a_i \leq p-1$ for all i, then $\mathrm{digsum}_p(n) := \sum_{i=0}^{l} a_i$.

Let Θ be the set of pairs of integers (m, n) satisfying the hypothesis. It is nonempty by assumption. Let (m, n'') be such that $(m, \mathrm{digsum}_p(n''))$ is lexicographically minimal. Note that in this case, the last entry of any optimal element in $U_m(n'')$ is nonzero. Suppose the contrary, i.e., we have $(O_0, \ldots, O_{m-2}, 0)$ optimal in $U_m(n'')$. By Corollary 3.4.19, the greedy element G is of the form $(G_0, \ldots, G_{m-2}, 0)$. Then by Corollary 3.4.21, $(O_0, \ldots, O_{m-2})$ resp. $(G_0, \ldots, G_{m-2})$ is optimal resp. greedy in $U_{m-1}(n'')$. Clearly they are different and both have last entries being nonzero, thus $(m-1, n'') \in \Theta$ and it contradicts the choice of (m, n''). is not greedy. Also, G'_{m-1} must be positive since O'_{m-1} must be so.

(i) By Proposition 3.4.20, there exists some h such that $\Gamma(O_j) \in J_2^h$ for $0 \leq j \leq m-2$. If $h = 0$, then we just take n to be n''. Otherwise, let $n := p^{s-h} n''$. Then by Proposition 3.4.7(c), we know that $O := (p^{s-h} O'_0, \ldots, p^{s-h} O'_{m-1})$ resp. $G := (p^{s-h} G'_0, \ldots, p^{s-h} G'_{m-1})$ is optimal resp. greedy in $U_m(n)$. It is clear from construction that $O \neq G$ and $\Gamma(O_j) \in J_2^0$ for $0 \leq j \leq m-2$.

We fix such an n from now on. Note that $\mathrm{digsum}_p(n) = \mathrm{digsum}_p(n'')$, so $(m, \mathrm{digsum}_p(n))$ remains lexicographically minimal. Note that for any pair of integers (m_1, n_1), if either $m_1 < m$ or $m_1 = m$ and $\mathrm{digsum}_p(n_1) > \mathrm{digsum}_p(n)$, we have $(m_1, n_1) \notin \Theta$.

Before continuing, we introduce the following notation:

$$\begin{aligned} \underline{o} &:= (o_0, \ldots, o_{s-1})^t := \Gamma(O_{m-1}) \\ \underline{g} &:= (g_0, \ldots, g_{s-1})^t := \Gamma(G_{m-1}) \\ \underline{n} &:= (n_0, \ldots, n_{s-1})^t := \Gamma(n). \end{aligned}$$

As $O_{m-1} > 0$, we have that $G_{m-1} \geq O_{m-1} > 0$. We also define indices $0 \leq \omega, \gamma \leq s-1$ such that $\omega \equiv \tilde{\omega} := \deg_p(O_{m-1}) \pmod{s}$ and $\gamma \equiv \tilde{\gamma} := \deg_p(G_{m-1})$.

(ii) By the greediness of G, we have $\tilde{\gamma} \geq \tilde{\omega}$.

Suppose equality holds, then $\omega = \gamma$, in particular, both g_ω and o_ω are positive. This contradicts the following lemma:

Lemma 3.4.25 ([She98, Lemma 5.3])**.** *For any $0 \leq i \leq s-1$, we always have either $g_i = 0$ or $o_i = 0$.*

(iii) By Lemma 3.4.25, we can also conclude that $\underline{o} \neq \underline{g}$, i.e., $\Gamma(O_{m-1}) \neq \Gamma(G_{m-1})$.

(iv)-(v) To show the rest, we need to show the following two lemmas first.

Lemma 3.4.26. *For any k such that $o_k > 0$, we have*

$$\underline{n} - \underline{e}_\gamma - \underline{e}_k \notin I_m.$$

Proof. By Lemma 3.4.25, if $o_k > 0$, then g_k must be 0. In particular, $k \neq \gamma$ and $\underline{n} - \underline{e}_\gamma - \underline{e}_k > 0$.

Suppose that $\underline{n} - \underline{e}_\gamma - \underline{e}_k \in I_m$. Then there exist $\underline{v}_0, \ldots, \underline{v}_{m-2} \in \mathfrak{J}$ such that $\underline{v}_0 + \ldots + \underline{v}_{m-2} \leq \underline{n} - \underline{e}_\gamma - \underline{e}_k$. Let p^σ be the largest element in $\tau_k(n)$. Then $\Gamma(n - p^\sigma) = \underline{n} - \underline{e}_k$. Set $\underline{v}_{m-1} := (\underline{n} - \underline{e}_k) - (\underline{v}_0 + \ldots + \underline{v}_{m-2}) \geq \underline{e}_\gamma > 0$. Let B be the matrix $(\underline{v}_0, \ldots, \underline{v}_{m-1})$, then $U_m^B(n - p^\sigma)$ is not empty by Lemma 3.4.5. Let $X = (X_0, \ldots, X_{m-1})$ be the τ-monotonic element in $U_m^B(n - p^\sigma)$. Since $\underline{v}_{m-1} \geq \underline{e}_\gamma$, the γ-th entry in $\Gamma(X_{m-1})$ must be nonzero. By the τ-monotonicity of X as well as the greediness of G, the largest p-power in $\tau_\gamma(n - p^\sigma)$, which is also the largest p-power in $\tau_{\ gamma}(n)$, must land in $\tau(X_{m-1}) \cap \tau(G_{m-1})$.

On the other hand, as assumed, $o_k > 0$, hence $p^\sigma \in \tau(O_{m-1})$ by the τ-monotonicity of O. Thus $Y := (O_0, \ldots, O_{m-2}, O_{m-1} - p^\sigma)$ is optimal in $U_m(n - p^\sigma)$ by Proposition 3.4.7(a). Since $\mathrm{digsum}_p(n - p^\sigma) < \mathrm{digsum}_p(n)$, the pair $(m, n - p^\sigma)$ cannot be in Θ, hence Y must at the same time be the greedy element in $U_m(n - p^\sigma)$. But this cannot be since

$$\begin{aligned}\deg_p(Y_{m-1}) = \deg_p(O_{m-1} - p^\sigma) &\leq \deg_p(O_{m-1}) \\ &< \deg_p(G_{m-1}) = \deg_p(X_{m-1}),\end{aligned}$$

which contradicts the greediness of Y in $U_m(n - p^\sigma)$. □

Recall that for $i = 0, 1, \ldots, s-1$, we defined the following row vectors:

$$\underline{\psi}_i = (p^{s-i}, \ldots, p^{s-1}, 1, p, \ldots, p^{s-1-i}).$$

Lemma 3.4.27 ([She98, Lemma 5.5]). *Let k be such that $o_k > 0$, and set*

$$\underline{v} := (v_0, \ldots, v_{s-1})^t := E^{-1}(\underline{n} - \underline{e}_k - \underline{e}_\gamma).$$

Then there exists an h such that $v_h < m - 1$.

Furthermore, for any such h we have

(a) $\underline{\psi}_h \cdot \underline{g} = \underline{\psi}_h \cdot \underline{o}$;

(b) $\underline{\psi}_h \cdot \underline{o} < \underline{\psi}_h \cdot \underline{e}_k + \underline{\psi}_h \cdot \underline{e}_\gamma$;

(c) $\underline{\psi}_h \cdot \underline{e}_\gamma < \underline{\psi}_h \cdot \underline{e}_k$.

(iv) Let k be ω in Lemma 3.4.27, we have

$$\underline{\psi}_{h_\omega} \cdot \underline{o} < \underline{\psi}_{h_\omega} \cdot \underline{e}_\omega + \underline{\psi}_{h_\omega} \cdot \underline{e}_\gamma$$
$$\underline{\psi}_{h_\omega} \cdot \underline{e}_\gamma < \underline{\psi}_{h_\omega} \cdot \underline{e}_\omega$$

Combining the above two inequalities leads to

$$\underline{\psi}_{h_\omega} \cdot \underline{o} < 2\underline{\psi}_{h_\omega} \cdot \underline{e}_\omega,$$

so $o_\omega < 2$, hence must be 1.

Now we need to show that only o_ω is nonzero. If $s = 2$, then it holds automatically since $\omega, \gamma \in \{0, 1\}$ and they are distinct. Otherwise, suppose there exists some $\omega' \neq \omega$ such that $o_{\omega'} \neq 0$. Then there exists an $h_{\omega'}$ such that

$$\underline{\psi}_{h_{\omega'}} \cdot \underline{o} < \underline{\psi}_{h_{\omega'}} \cdot \underline{e}_{\omega'} + \underline{\psi}_{h_{\omega'}} \cdot \underline{e}_\gamma$$
$$\underline{\psi}_{h_{\omega'}} \cdot \underline{e}_\gamma < \underline{\psi}_{h_{\omega'}} \cdot \underline{e}_{\omega'}$$

Since $\omega' \neq \omega$ and $o_{\omega'} \neq 0$, as shown in the proof to Lemma 3.4.27(c), we have

$$\underline{\psi}_{h_{\omega'}} \cdot \underline{e}_\omega < \underline{\psi}_{h_{\omega'}} \cdot \underline{e}_\gamma, \ \underline{\psi}_{h_\omega} \cdot \underline{e}_{\omega'} < \underline{\psi}_{h_\omega} \cdot \underline{e}_\gamma.$$

Then we have

$$\underline{\psi}_{h_\omega} \cdot \underline{e}_{\omega'} < \underline{\psi}_{h_\omega} \cdot \underline{e}_\gamma < \underline{\psi}_{h_\omega} \cdot \underline{e}_\omega$$
$$\underline{\psi}_{h_{\omega'}} \cdot \underline{e}_\omega < \underline{\psi}_{h_{\omega'}} \cdot \underline{e}_\gamma < \underline{\psi}_{h_{\omega'}} \cdot \underline{e}_{\omega'}$$

but this is impossible because of the following observation: for any a and i such that $0 \leq a, i \leq s-1$, let $p^{a'}$ be $\underline{\psi}_i \cdot \underline{e}_a$, then $0 \leq a' \leq s-1$ and $a' - a + i \equiv 0 \pmod{s}$. More precisely, if $a \leq i$, then $a' = i - a$; if $a > i$, then $a' = i - a + s$.

(v) Again, let k be ω in Lemma 3.4.27. Then it suffices to show that we can choose h to be 0, i.e., $v_0 < m-1$, since if so, then we can deduce (v) directly from Lemma 3.4.27(a) with $h = 0$.

By (iv), we have that $O_{m-1} = p^{\tilde{\omega}}$, hence $\Gamma(O_{m-1}) = \underline{o} = \underline{e}_\omega$. Thus

$$\underline{n} - \underline{e}_\omega = \Gamma(n - O_{m-1}) = \Gamma(O_0) + \ldots + \Gamma(O_{m-2}),$$

hence

$$\underline{v} = E^{-1}(\underline{n} - \underline{e}_\omega - \underline{e}_\gamma) = \sum_{j=0}^{m-2} E^{-1}\Gamma(O_j) - E^{-1}\underline{e}_\gamma.$$

By (i), $\Gamma(O_j) \in J_2^0$ for all $0 \le j \le m-2$, thus

$$v_0 = m - 1 - \frac{p^\gamma}{p^s - 1} < m - 1.$$

□

Now we can construct some $Z \in U_m(n)$ as follows:

- $\underline{\theta}_j := \sum_{i=0}^{j} \Gamma(O_i)$ for $0 \le j \le m-1$;
- $(t_{i,j})_{i,j} := (\underline{t}_0, \ldots, \underline{t}_{m-1}) := E^{-1}(\underline{\theta}_0, \ldots, \underline{\theta}_{m-1}) = E^{-1}(\theta_{i,j})_{i,j}$.

We will need the following lemma to proceed. First recall that we have defined:

$$\begin{aligned}\underline{n} &:= \Gamma(n) = (n_0, \ldots, n_{s-1})^t;\\ \underline{o} &:= \Gamma(O_{m-1}) = (o_0, \ldots, o_{s-1})^t;\\ \underline{g} &:= \Gamma(G_{m-1}) = (g_0, \ldots, g_{s-1})^t.\end{aligned}$$

Lemma 3.4.28 ([She98, Lemma 6.1]). *There exists some α with $0 \le \alpha \le \omega$ such that*

(a) $t_{i,m-2} > m-1$ for $\alpha < i \le \omega$;

(b) $t_{\alpha,m-2} = m-1$;

(c) if $g_i > 0$, then $\alpha \le i < \omega$;

Fix such an α from now on. Now we can continue the construction of Z.

- Define a matrix $(d_{ij})_{i,j} = (\underline{d}_0, \ldots, \underline{d}_{m-1})$ as follows:

$$\underline{d}_{m-1} := E^{-1}\Gamma(n) = \underline{t}_{m-1}$$

$$d_{i,m-2} := \begin{cases} t_{i,m-2} & \text{if } 0 \leq i \leq \alpha \text{ or } \omega < i \leq s-1; \\ \min\{t_{i,m-2} - 1, pd_{i+1,m-2}\} & \text{if } \alpha < i \leq \omega. \end{cases}$$

$$d_{i,j} := \begin{cases} t_{ij} & \text{if } 0 \leq i \leq \alpha \text{ or } \omega < i \leq s-1 \\ \min\{d_{i,j+1} - 1, pd_{i+1,j}\} & \text{if } \alpha < i \leq \omega. \end{cases}$$

- $(\delta_{ij})_{i,j} = (\underline{\delta}_0, \ldots, \underline{\delta}_{m-1}) = E(d_{ij})_{i,j}$;

- $\underline{b}_0 := \underline{\delta}_0$, and for $i = 1, 2, \ldots, m-1$, define $\underline{b}_i := \underline{\delta}_i - \underline{\delta}_{i-1}$. Define $B = (\underline{b}_0, \ldots, \underline{b}_{m-1})$;

Definition 3.4.29. With same notation as above, we define Z to be the τ-monotonic element of $U_m^B(n)$.

An immediate question arousing is whether such a Z really exists or not, i.e., whether $U_m^B(n)$ is nonempty or not. We will show this in Proposition 3.4.32. Before we can do this, we will need some preparations. The next lemma concerns some properties of the δ_{ij}'s.

Lemma 3.4.30 ([She98, Lemma 6.2])**.** *As defined, $\underline{\delta}_{m-1} = \underline{n} = \Gamma(n)$.*

For $\underline{\delta}_{m-2}$, we have

(a) $\delta_{h,m-2} = n_h$, for $0 \leq h < \alpha$ or $\omega \leq h \leq s-1$;

(b) $0 \leq \delta_{h,m-2} \leq \max\{n_h - (p-1), 0\}$, for $\alpha < h < \omega$;

(c) $0 \leq \delta_{\alpha,m-2} \leq n_\alpha - p$.

For $0 \leq j \leq m-3$, we have

(d) $\delta_{hj} = \theta_{hj}$, for $0 \leq h < \alpha$ or $\omega < h \leq s-1$;

(e) $0 \leq \delta_{h,j} \leq \max\{\delta_{h,j+1} - (p-1), 0\}$, for $\alpha \leq h \leq \omega$.

For simplicity, from now on, $\tau_h^i := \tau_h^i(n)$.

Corollary 3.4.31. *For $0 \leq j \leq m-3$, we have* *(a)* $\tau_h^{\delta_{h,j+1}} \geq p^s \tau_h^{\delta_{h,j}}$;

(b) $\sum_{i=0}^{j} \tau_h^{\delta_{h,i}} \leq \frac{p^s}{p^s-1}\tau_h^{\delta_{h,j}} \leq \frac{1}{p^s-1}\tau_h^{\delta_{h,j+1}}$;

(c) $\sum_{i=0}^{\delta_{h,j}} \tau_h^{i} \leq \frac{p^s(p-1)}{p^s-1}\tau_h^{\delta_{h,j}} \leq \frac{p-1}{p^s-1}\tau_h^{\delta_{h,j+1}}$.

Now we are ready to prove the existence of such a Z, i.e., the set $U_m^B(n)$ is nonempty.

Proposition 3.4.32. *We use the same notation as above. Then the set $U_m^B(n)$ is nonempty, i.e., the Z defined in Definition 3.4.29 exists.*

Proof. By Lemma 3.4.5, $U_m^B(n)$ is nonempty if and only if the matrix B satisfies the following two conditions:

(i) $\underline{b}_0 + \underline{b}_1 + \ldots + \underline{b}_{m-1} = \Gamma(n) = \underline{n}$;

(ii) $\underline{b}_j \in \mathfrak{J}$ for $j = 0, 1, \ldots, m-2$.

The first condition is fulfilled by construction:

$$\underline{b}_0 + \underline{b}_1 + \ldots + \underline{b}_{m-1} = \underline{\delta}_{m-1} = E^{-1}\underline{d}_{m-1} = \Gamma(n).$$

To show the second condition, we recall that $\underline{b}_j = \underline{\delta}_{j+1} - \underline{\delta}_j = E(\underline{d}_{j+1} - \underline{d}_j)$. By Lemma 3.4.3, $\mathfrak{J} = E\mathbb{Z}^s \cap (\mathbb{N}^s\backslash\{0\})$, so it suffices to show that $\underline{d}_{j+1} - \underline{d}_j \in \mathbb{Z}^s$ and $\underline{b}_j \in \mathbb{N}^s\backslash\{0\}$. The first one is immediate by the definition of $\underline{d}$. To show $\underline{b}_j > 0$ for $0 \leq j \leq m-2$, it is equivalent to show that $\underline{\delta}_{j+1} > \underline{\delta}_j$.

For $0 \leq j \leq m-3$, we know from Lemma 3.4.30(e) that $0 \leq \delta_{h,j} \leq \max\{\delta_{h,j+1} - (p-1), 0\}$ for $\alpha \leq h \leq \omega$, thus $\delta_{h,j} \leq \delta_{h,j+1}$ for these h's and the equality holds when $\delta_{h,j} = \delta_{h,j+1} = 0$. By Lemma 3.4.30(d), for $0 \leq h < \alpha$ or $\omega < h \leq s-1$, $\delta_{h,j} = \theta_{h,j} \leq \theta_{h,j+1} = \delta_{h,j+1}$. If $\underline{b}_j = 0$, then $\underline{\delta}_j = \underline{\delta}_{j-1}$, but this cannot be since $d_{0,j} = w_{0,j} = j$ for all j. So $\underline{b}_j > 0$ for $0 \leq j \leq m-3$.

For $j = m-2$:

(1) for $0 \leq h < \alpha$ and $\omega < h \leq s-1$, by Lemma 3.4.30(a),

$$\delta_{h,m-2} = n_h = \delta_{h,m-1};$$

(2) for $\alpha < h \leq \omega$, by Lemma 3.4.30(b),

$$\delta_{\omega,m-2} \leq \max\{n_h - (p-1), 0\} \leq u_h = \delta_{h,m-1};$$

(3) for $h = \alpha$, by Lemma 3.4.30(c),

$$\delta_{\alpha,m-2} \leq n_\alpha - p < n_\alpha = \delta_{\alpha,m-1}.$$

So $\delta_{m-1} > \delta_{m-2}$. □

3.5 Proof of the main theorem

In this section, we will use the tools developed from the previous sections to prove the main theorems given below. Suppose now $g_1 = \frac{p^s+p}{2}$.

Theorem 3.5.1. *Suppose that $g \leq g_1$. For any pair (m, n), if $U_m(n)$ is nonemtpy, then any optimal element must be greedy.*

We will prove it by contradiction. Suppose that there exists a pair (m, n) such that $U_m(n)$ is nonempty and contains an optimal element which is different from the greedy element, such that the last entry in the optimal element is nonzero, then we can construct a Z as in Definition 3.4.29. We will show that such a Z has a larger weight than O. Before getting our hands on the proof, we first make some observations.

Lemma 3.5.2 ([She98, Lemma 7.2])**.** $\deg_p(Z_{m-1}) = \deg_p(G_{m-1}) > \tilde{\omega}$.

Define

$$Q := \sum_{h=\alpha}^{\omega-1} \tau_h^{\delta_{h,m-2}}. \tag{3.2}$$

If $Q \neq 0$, then we define r to be its p-degree, and $\tilde{r} \equiv r \pmod{s}$ with $0 \leq \tilde{r} \leq s-1$. The upcoming lemmas concern the p-degree of Q.

Lemma 3.5.3. *Suppose Q is not zero, then*

$$\deg_p(Z_{m-1}) \geq r + s.$$

Proof. Note that if $\delta_{h,m-2} = 0$, then $\tau_h^{\delta_{h,m-2}} = 0$ by definition. If nonzero, τ_h^j is a power of p whose exponent is congruent to h mod s. So the sum at the right hand side of 3.2 is a sum of distinct p-powers, in particular, there can never be carryovers. So r must be the exponent of some $\tau_h^{\delta_{h,m-2}}$, say $p^r = \tau_{h'}^{\delta_{h',m-2}}$ with $\alpha \leq h' \leq \omega - 1$. In particular, $\delta_{h',m-2}$ is positive. By Lemma 3.4.30 (b) and (c),

$0 \leq \delta_{h',m-2} \leq \max\{n_{h'} - (p-1), 0\}$ if $h' \neq \alpha$, or $0 \leq \delta_{h',m-2} \leq n_{h'} - p$ otherwise. In both cases, $n'_h - (p-1)$ must be at least $\delta_{h',m-2}$, hence

$$b_{h',m-2} = n_{h'} - \delta_{h',m-2} \geq p-1,$$

i.e., there exist at least $p-1$ terms in $\tau_{h'}(Z_{m-1})$. Since $p^r \in \tau_{h'}(Z_{m-2})$, we get

$$\max \tau(Z_{m-1}) \geq \max \tau_{h'}(Z_{m-1}) \geq p^{r+s}$$

by the τ-monotonicity of Z. □

Lemma 3.5.4. *Suppose Q is nonzero with p-degree r. Suppose $k' \not\equiv r \pmod{s}$ and $p^{k'} \in \tau(Z_{m-1})$, then*

$$\deg_p(Z_{m-1} - p^{k'}) \geq r+s.$$

Proof. Let h' be such that $\tau_{h'}^{\delta_{h',m-2}} = p^r$. Then it is easy to see that $r \equiv h' \not\equiv k' \pmod{s}$, hence $\tau_{h'}(Z_{m-1} - p^{k'}) = \tau_{h'}(Z_{m-1})$. The rest of the proof is exactly the same as above. □

Corollary 3.5.5. *Suppose Q is nonzero with p-degree r. Recall that $O_{m-1} = p^{\tilde{\omega}}$. Suppose $p^{\tilde{\omega}+1} \in \tau(Z_{m-1})$, then*

$$\deg_p(Z_{m-1} - p^{\tilde{\omega}+1}) \geq r+s.$$

Proof. If $\tilde{\omega}+1 \not\equiv r \pmod{s}$, then it follows directly from Lemma 3.5.4.

Otherwise, if $\tilde{\omega}+1 \equiv r \pmod{s}$, then we must have

$$\omega = s-1,\ \alpha = 0, \text{ and } r \equiv \alpha \pmod{s}.$$

By Lemma 3.4.30 (c), we have that

$$p \leq n_\alpha - \delta_{\alpha,m-2}.$$

As $p^{\tilde{\omega}+1} \in \tau(Z_{m-1})$, it must lie in $\tau_\alpha(Z_{m-1})$. Hence

$$\tau_\alpha(Z_{m-1} - p^{\tilde{\omega}+1}) = \tau_\alpha(Z_{m-1}) \backslash \{p^{\tilde{\omega}+1}\}$$

contains at least $p-1$ terms. By the τ-monotonicity of Z, we have

$$\deg_p(Z_{m-1} - p^{\tilde{\omega}+1}) \geq \log_p(\max \tau_\alpha(Z_{m-1} - p^{\tilde{\omega}+1})) \geq r+s.$$

□

Next, we need some estimates on the weights. Let Z be as above. Then for $0 \leq j \leq m-2$, we define $\tilde{Z}_j$ and $\tilde{O}_j$'s in the same fashion as $\tilde{X}$ in Section 3.2.5, i.e.,

$$\begin{aligned}\tilde{Z}_j &:= Z_j + Z_{j-1} + \ldots + Z_0 \\ \tilde{O}_j &:= O_j + O_{j-1} + \ldots + O_0.\end{aligned}$$

Lemma 3.5.6. *We have*

$$\sum_{j=0}^{m-3} \tilde{\varphi}_j(\tilde{Z}_j - \tilde{O}_j) \leq \frac{p^s(p-1)}{(p^s-1)^2}(1+c)(Q + p^{\tilde{\omega}}),$$

where

$$c = \begin{cases} p^{-s(m-2-g)} & \text{if } m-3 \geq g; \\ g & \text{otherwise.} \end{cases}$$

Proof. For $0 \leq j \leq m-3$, $\tilde{\varphi}_j \leq g$, and by definition,

$$\begin{aligned}\tilde{Z}_j &= Z_j + Z_{j-1} + \ldots + Z_0 = \sum_{h=0}^{s-1}\sum_{i=0}^{\delta_{h,j}} \tau_h^i \\ \tilde{O}_j &= O_j + O_{j-1} + \ldots + O_0 = \sum_{h=0}^{s-1}\sum_{i=0}^{\theta_{h,j}} \tau_h^i\end{aligned}$$

Note that $\delta_{h,i}$ and $\theta_{h,i}$ might be 0 for some h and i. By Lemma 3.4.30 (d), we have that $\delta_{h,i} = \theta_{h,i}$ for $0 \leq h < \alpha$ or $\omega < h \leq s-1$, so

$$\begin{aligned}\tilde{\varphi}_j(\tilde{Z}_j - \tilde{O}_j) &= \tilde{\varphi}_j \sum_{h=0}^{s-1}(\sum_{i=0}^{\delta_{h,j}} \tau_h^i - \sum_{i=0}^{\theta_{h,j}} \tau_h^i) \\ &= \tilde{\varphi}_j \sum_{h=\alpha}^{\omega}(\sum_{i=0}^{\delta_{h,j}} \tau_h^i - \sum_{i=0}^{\theta_{h,j}} \tau_h^i) \\ &\leq \tilde{\varphi}_j \sum_{h=\alpha}^{\omega}\sum_{i=0}^{\delta_{h,j}} \tau_h^i.\end{aligned}$$

By Corollary 3.4.31(c), we have

$$\sum_{i=0}^{\delta_{h,j}} \tau_h^i \leq \frac{p^s(p-1)}{p^s-1}\tau_h^{\delta_{h,j}} \leq \frac{p-1}{p^s-1}\tau_h^{\delta_{h,j+1}}.$$

Now we plug these arguments into the above estimate of $\sum_{j=0}^{m-3}\tilde{\varphi}_j(\tilde{Z}_j-\tilde{O}_j)$, we have

$$\begin{aligned}\sum_{j=0}^{m-3}\tilde{\varphi}_j(\tilde{Z}_j-\tilde{O}_j) &\leq \sum_{j=0}^{m-3}\tilde{\varphi}_j(\sum_{h=\alpha}^{\omega}\sum_{i=1}^{\delta_{h,j}}\tau_h^i)\\ &\leq \sum_{j=0}^{m-3}\tilde{\varphi}_j(\sum_{h=\alpha}^{\omega}\frac{p-1}{p^s-1}\tau_h^{\delta_{h,j+1}})\\ &\leq \sum_{h=\alpha}^{\omega}\frac{p-1}{p^s-1}(\sum_{j=0}^{m-3}\tau_h^{\delta_{h,j+1}}+\sum_{j=0}^{\min\{m-3,g\}}(\tilde{\varphi}_j-1)\tau_h^{\delta_{h,j}}).\end{aligned}$$

If $m-3\geq g$, then

$$\begin{aligned}\sum_{j=0}^{m-3}\tilde{\varphi}_j(\tilde{Z}_j-\tilde{O}_j) \leq&\sum_{h=\alpha}^{\omega}\frac{p-1}{p^s-1}(\sum_{j=0}^{m-3}\tau_h^{\delta_{h,j+1}}+\sum_{j=0}^{\min\{m-3,g\}}\tau_h^{\delta_{h,j}})\\ \leq&\sum_{h=\alpha}^{\omega}\frac{p-1}{p^s-1}\frac{p^s}{p^s-1}(1+c)\tau_h^{\delta_{h,m-2}},\end{aligned}$$

where $c=p^{-s(m-2-g)}$;

if $m-3<g$, then

$$\begin{aligned}\sum_{j=0}^{m-3}\tilde{\varphi}_j(\tilde{Z}_j-\tilde{O}_j) \leq&\sum_{h=\alpha}^{\omega}\frac{p-1}{p^s-1}(1+\frac{g}{m-2})\sum_{j=0}^{m-3}\tau_h^{\delta_{h,j+1}}\\ \leq&\sum_{h=\alpha}^{\omega}\frac{p-1}{p^s-1}(1+\frac{g}{m-2})\frac{p^s}{p^s-1}\tau_h^{\delta_{h,m-2}}\end{aligned}$$

In particular, we have that $\delta_{\omega,m-2}=n_\omega$, hence $\tau_\omega^{\delta_{\omega,m-2}}=p^{\tilde{\omega}}$. Therefore,

$$\sum_{j=0}^{m-3}\tilde{\varphi}_j(\tilde{Z}_j-\tilde{O}_j) \leq\frac{p^s(p-1)}{(p^s-1)^2}(1+c)(Q+p^{\tilde{\omega}}),$$

where

$$c=\begin{cases}p^{-s(m-2-g)} & \text{if } m-3\geq g;\\ g & \text{otherwise.}\end{cases}$$

Hence we have the desired inequality. □

Now we are ready to prove Theorem 3.5.1.

Proof to Theorem 3.5.1: Recall that as in Remark 3.2.5, for any $X = (X_0, \ldots, X_{m-1})$ in $U_m(n)$, we can write the weight of X as:

$$wt(X) = \varphi_{m-1}n - \sum_{j=0}^{m-2} \tilde{\varphi}_j \tilde{X}_j,$$

where $\tilde{\varphi}_j = \varphi_j - \varphi_{j-1}$, and $\tilde{X}_j = X_0 + \ldots + X_j$ for $j = m-2, \ldots, 0$. Note that $\tilde{X}_{m-2} = n - X_{m-1}$.

Then with the help of $\tilde{Z}$'s and $\tilde{O}$'s, we can write the difference of the weights as:

$$wt(Z) - wt(O) = \sum_{j=0}^{m-2} \tilde{\varphi}_j(\tilde{O}_j - \tilde{Z}_j).$$

For $j = m-2$, since $\tilde{O}_{m-2} = n - O_{m-1}$ and $\tilde{Z}_{m-2} = n - Z_{m-1}$, where $O_{m-1} = p^{\tilde{\omega}}$ by Proposition 3.4.23(v),

$$\tilde{\varphi}_{m-2}(\tilde{O}_{m-2} - \tilde{Z}_{m-2}) = \tilde{\varphi}_{m-2}(Z_{m-1} - p^{\tilde{\omega}}).$$

And it is at least $Z_{m-1} - p^{\tilde{\omega}}$ since $\tilde{\varphi}_{m-2} \geq 1$. Together with Lemma 3.5.6 we have

$$wt(Z) - wt(O) \geq Z_{m-1} - p^{\tilde{\omega}} - (p-1)\frac{p^s}{(p^s-1)^2}(1+c)(Q + p^{\tilde{\omega}}).$$

Since $g \leq \frac{p^s+p}{2}$ where $s \geq 2$. it is easy to see that when $q \neq 4$, we always have

$$\frac{p^s}{(p^s-1)^2}(1+c) \leq \frac{p^s}{(p^s-1)^2}(1+g) \leq 1.$$

Hence by Lemma 3.5.6:

$$wt(Z) - wt(O) \geq Z_{m-1} - p^{\tilde{\omega}+1} - (p-1)Q.$$

We want to show that this is positive. If it is true, then we get a contradiction to the optimality of O.

Recall that we denote by $Q := \sum_{h=\alpha}^{\omega-1} \tau_{h,\delta_{h,m-2}}$ and $r = \deg_p(Q)$.

If $p^{\tilde{\omega}+1} \not\in \tau(Q)$, then in the summation $p^{\tilde{\omega}+1} + (p-1)Q$, the greatest coefficient of any p-power is at most $p-1$, there cannot be any carryovers, hence

$$\deg_p(p^{\tilde{\omega}+1} + (p-1)Q) = \max\{\tilde{\omega}+1, r\}.$$

As shown in Lemma 3.5.2 and Lemma 3.5.3, both $\tilde{\omega}$ and r are smaller than $\deg_p(Z_{m-1})$. Hence we consider the following two cases:

- if $\deg_p(Z_{m-1}) > \tilde{\omega}+1$, then we have

$$\deg_p(Z_{m-1}) > \deg_p(p^{\tilde{\omega}+1} + (p-1)Q);$$

- if $\deg_p(Z_{m-1}) = \tilde{\omega}+1$, then by Corollary 3.5.5 we have

$$\deg_p(Z_{m-1} - p^{\tilde{\omega}+1}) \geq r+s > r = \deg_p((p-1)Q).$$

Otherwise, if $p^{\tilde{\omega}+1} \in \tau(Q)$, then there will be carryovers, and we have

$$\deg_p(p^{\tilde{\omega}+1} + (p-1)Q) \leq r+1 < r+s < \deg_p(Z_{m-1}).$$

Either way, we always get that $Z_{m-1} > p^{\tilde{\omega}+1} + (p-1)Q$, hence

$$wt(Z) - wt(O) > 0.$$

When $q=4$, then for elements in J_2 must have the shape $(1,1)^t$, $(3,0)^t$ or $(0,3)^t$. By Proposition 3.4.23, for $j=0,1,\dots,m-2$, $\Gamma(O_j)$ must lie in J_2^0, hence must of the form $(1,1)^t$ or $(3,0)^t$. Moreover, $\Gamma(G_{m-1}) = (2,0)^t$ by (iii) and (v).

Claim 1. *For O, we have $\Gamma(O_0) = (3,0)^t$ and $\Gamma(O_j) = (1,1)^t$ for $j = 1,\dots,m-2$. For G, we have $\Gamma(G_j) = (1,1)^t$ for $j=0,1,\dots,m-2$.*

Proof. If $\Gamma(O_j) = (1,1)^t$ for all $j = 0,1,\dots,m-2$, then $\Gamma(n) = (m-1,m)^t$ and $\Gamma(n-G_{m-1}) = (m-3,m)^t \in J_{m-1}$ which contradicts to the existence of $\tilde{G} := (G_0,\dots,G_{m-2},0) \in U_m(n-G_{m-1})$.

Now let i be the largest such that $\Gamma(O_i) = (3,0)^t$. Suppose that $i > 0$. Observe that $n' := O_i + \ldots + O_{m-1}$, together with an optimal element $(O_i, O_{i+1}, \dots, O_{m-1})$ satisfies Proposition 3.4.23, but smaller than n, which contradicts to the minimality of n as in the construction.

The statement concerning G is a direct consequence. □

We can write down O and G explicitly

$$\begin{aligned}
O_0 &= \tau_0^1 + \tau_0^2 + \tau_0^3;\\
O_j &= \tau_0^{j+3} + \tau_1^{j+1}, \text{ for } j = 1,\dots,m-2;\\
O_{m-1} &= \tau_1^m;\\
G_j &= \tau_0^{j+1} + \tau_1^{j+1}, \text{ for } j = 0,1,\dots,m-2;\\
G_{m-1} &= \tau_0^m + \tau_0^{m+1}.
\end{aligned}$$

Now let us compare the weights of O and G:

$$\begin{aligned} wt(G) - wt(O) =& \tilde{\varphi}_{m-2}(\tau_0^{m+1} - \tau_1^{m-1}) - \sum_{i=1}^{m-2} \tilde{\varphi}_{i-1}\tau_1^i + \sum_{i=3}^{m} (\tilde{\varphi}_{i-2} + \tilde{\varphi}_{i-3})\tau_0^i \\ >& (\tau_0^{m+1} - \tau_1^{m-1}) - \sum_{i=1}^{m-2} \tilde{\varphi}_{i-1}\tau_1^i. \end{aligned}$$

The aim is to show that $wt(G) - wt(O) > 0$, which contradicts to the optimality of O.

If $m - 3 > 0$, follow the above strategy and we can get the desired; if $m = 3$, then

$$wt(G) - wt(O) > \tau_0^4 - \tau_1^2 - \tilde{\varphi}_0\tau_1^1 \geq 0.$$

□

Theorem 3.5.7. *Suppose that $p \neq q$ and $g \leq \frac{p+q}{2}$. Let n be a fixed positive integer.*

(a) The x-coordinates of the break points of the Newton polygon associated to $\zeta_A(-n, T)$ are φ_i for all $i = 0, 1, \ldots$.

(b) The slope of the i-th segment between φ_{i-1} and φ_i is G_i^i, where G_i^i appears as the last entry of the greedy element in $U_{i+1}(n)$. In particular, the sequence $(G_i^i)_i$ is strictly increasing.

Let $m \leq g$ be the smallest positive integer such that $\tilde{\varphi}_i = 1$ for all $i > m$. Except for the φ_m zeros of lowest valuations, all other zeros of $\zeta_A(-n, T)$ are simple with pairwise distinct valuations.

Proof. Recall that the definition of Goss-Thakur zeta function $\zeta_A(-n, T)$ is

$$\zeta_A(-n, T) := \sum_{d \geq 0} T^d S_d(n),$$

where $S_d(n) := \sum_{a \in A_{+,d}} a^n$.

Thanks to those $f_0, \ldots, f_d, \ldots$ we defined before, we can rewrite $S_d(n)$ as follows:

- if $d \notin \varphi(\mathbb{N})$, then $S_d(n) = 0$;

- if there exists some $m \in \mathbb{N}$ such that $d = \varphi(m)$, then

$$\begin{aligned} S_d(n) &= \sum_{a \in A_{+,d}} a^n = \sum_{a \in A_{+,\varphi_m}} a^n \\ &= \sum_{a_0,\ldots,a_{m-1} \in \mathbb{F}_q} (a_0 f_0 + \ldots + a_{m-1} f_{m-1} + f_m)^n \\ &= \sum_{a_0,\ldots,a_{m-1} \in \mathbb{F}_q} \sum_{X_0 + \cdots + X_m = n} \binom{n}{X_0, \ldots, X_m} a_0^{X_0} \ldots a_{m-1}^{X_{m-1}} f_0^{X_0} \ldots f_m^{X_m} \\ &= \sum_{X \in U_{m+1}(n)} \binom{n}{X_0, \ldots, X_m} (-1)^m f_0^{X_0} \ldots f_m^{X_m}. \end{aligned}$$

Denote by T_X the term corresponding to X. Clearly, $v(T_X) = -wt(X)$. By Theorem 3.5.1, when $g \leq \frac{p+q}{2}$, there exists a unique term with maximal weight, which is the greedy element in $U_m(n)$. Hence

$$v(S_{\varphi_{m-1}}(n)) = -wt(G^m),$$

where G^m denotes the greedy element in $U_m(n)$.

Now we want to compare the differences of weights of G^m's. By greediness and Corollary 3.4.22, for $G^{m-1} = (G_0^{m-1}, \ldots, G_{m-1}^{m-1})$ and $G^m = (G_0^m, \ldots, G_m^m)$, we have

$$G_i^{m-1} = \begin{cases} G_i^m, & \text{for } i = 0, \ldots, m-2; \\ G_{m-1}^m + G_m^m, & \text{for } i = m-1. \end{cases}$$

Hence

$$\begin{aligned} & wt(G^m) - wt(G^{m-1}) \\ =& \varphi_0 G_0^m + \ldots + \varphi_{m-1} G_{m-1}^m + \varphi_m G_m^m - (\varphi_0 G_0^{m-1} + \ldots + \varphi_{m-1} G_{m-1}^{m-1}) \\ =& \varphi_{m-1} G_{m-1}^m + \varphi_m G_m^m - \varphi_{m-1}(G_{m-1}^m + G_m^m) \\ =& (\varphi_m - \varphi_{m-1}) G_m^m = \tilde{\varphi}_{m-1} G_m^m. \end{aligned}$$

This implies that when we look at the Newton polygon attached to $\zeta_A(-n, T)$, the points are $(\varphi_m, -wt(G^m))$ and the line segments have slopes $-G_m^m$ and horizontal width $\tilde{\varphi}_{m-1}$ for $m = 1, 2, \ldots$. They are clearly of strictly increasing order, hence the Newton polygon consists of all these line segments.

Recall that the definition of m, $\tilde{\varphi}_i = 1$ for all $i > m$. Hence except for the first m slopes, all the line segments in the Newton polygon have horizontal width 1. This is equivalent to say, that except for the zeroes of the lowest m valuations, which mount to φ_m zeros, all other zeroes of $\zeta_\infty(-n, T)$ are simple and have pairwise distinct valuations. □

Remark 3.5.8. By Lemma 3.2.1, $\tilde{\varphi}_i = 1$ for $i \geq g$. Hence a somewhat weaker version of Theorem 3.5.7 states that all the zeros except for the $2g$ zeros with smallest valuations are simple with pairwise distinct valuations.

3.6 Examples: Non-rational Class Number One Curves With a Rational Point

In this section, we will look at those curves of class number 1. In these cases, we have a better understanding of the slopes as well as the zeros.

Example 3.6.1. Our first example is the curve defined by $y^2+y = x^3+x+1$ over $\mathbb{F}_2$. This is the curve occurred in [Böc13]. Note that in this case, $p = q = 2$, and this curve is an elliptic curve, i.e., $g = 1$. We can conclude from Theorem 3.3.2:

Proposition 3.6.2. *Let $n = 2^{n_0} + 2^{n_1} + \ldots + 2^{n_l}$ be the 2-adic expansion of a positive integer n with $n_0 < n_1 < \ldots < n_l$. Then the Newton polygon of $\zeta_A(-n, T)$ has slopes*

$$-(2^{n_1} + \ldots + 2^{n_l}), -(2^{n_2} + \ldots + 2^{n_l}), \ldots, -2^{n_l},$$

of increasing order. Furthermore, apart from the first one which has width 2, all the other slopes have horizontal width 1.

In terms of zeros of $\zeta_A(-n, T)$, except for the two zeros of smallest valuation, all the other zeros are simple with pairwise distinct valuations.

Compare with [Böc13, Corollary 6.3], we need to remember that an interpolation form of $\zeta_A(-n, T)$ is treated there. Using the formula $\zeta_A(-n, T) = z_A(-n, T\pi_\infty^{-n})$ with π_∞ a uniformizer at ∞, it is easy to see that they imply the same result.

Example 3.6.3. Let $\mathcal{C}$ be defined by $y^2 + y = x^3 + \zeta_3$ over $\mathbb{F}_4$ where ζ_3 is a primitive 3rd root of unity. In this case, $q = 4 = p^2$ and the curve is also elliptic, i.e., $g = 1$. Similar as the above example, we have

Proposition 3.6.4. *Let n be a positive integer and $n = n_0 + n_1 + \ldots + n_l$ where $n \in I_{l+1} \backslash I_{l+2}$ and $(n_0, n_1, \ldots, n_l)$ is the greedy element in $U_{l+1}(n)$. Then the slopes of Newton polygon of $\zeta_A(-n, T)$ are*

$$-(n_1 + \ldots + n_l), -(n_2 + \ldots + n_l), \ldots, -n_l,$$

of increasing order. Furthermore, apart from the first one which has width 2, all the other slopes have horizontal width 1.

In terms of zeros of $\zeta_A(-n, T)$, except for the two zeros of smallest valuation, all the other zeros are simple with pairwise distinct valuations.

Example 3.6.5. Let $\mathcal{C}$ be defined by $y^2 = x^3 - x - 1$ over $\mathbb{F}_3$. In this case, $p = q = 3$ and the curve is elliptic, i.e., $g = 1$. Similarly, we have

Proposition 3.6.6. *Let n be a positive integer and $n = \sum_{i=0}^{l} 3^{k_i}$ where $l = \mathrm{digsum}_3(n)$, $k_0 \leq k_1 \leq \ldots \leq k_l$ and at most two k_i's are the same. Set $n_i := 3^{k_{2i}} + 3^{k_{2i+1}}$ for $i = 0, 1, \ldots, \lfloor (l-1)/2 \rfloor$, and $n_l := n - (n_0 + \ldots + n_{l-1})$. Then the slopes of Newton polygon of $\zeta_A(-n, T)$ are*

$$-(n_1 + \ldots + n_l), -(n_2 + \ldots + n_l), \ldots, -n_l,$$

of increasing order. Furthermore, apart from the first one which has width 2, all the other slopes have horizontal width 1.

In terms of zeros of $\zeta_A(-n, T)$, except for the two zeros of smallest valuation, all the other zeros are simple with pairwise distinct valuations.

Example 3.6.7. Let $\mathcal{C}$ be defined by $y^2 + y = x^5 + x^3 + 1$ over $\mathbb{F}_2$. Unlike the previous cases, this curve has genus 2, and the gap numbers are 1 and 3.

Proposition 3.6.8. *Let $n = 2^{n_0} + 2^{n_1} + \ldots + 2^{n_l}$ be the 2-adic expansion of a positive integer n with $n_0 < n_1 < \ldots < n_l$. Then the Newton polygon of $\zeta_A(-n, T)$ has slopes*

$$-(2^{n_1} + \ldots + 2^{n_l}), -(2^{n_2} + \ldots + 2^{n_l}), \ldots, -2^{n_l},$$

of increasing order. Furthermore, apart from the first two both of which have width 2, all the other slopes have horizontal width 1.

In terms of zeros of $\zeta_A(-n, T)$, except for the four zeros of smallest valuation, all the other zeros are simple with pairwise distinct valuations.

3.7 Some (Counter-)Examples

As we have seen from previous discussion, this method may fail for curves whose genera are large with respect to p and q, where $q \neq p$. We first observe the following examples.

Example 3.7.1. As the first counterexample, let us first consider the case $q = 4$ and the point ∞ is an $\mathbb{F}_4$-rational non-Weierstrass point. Hence its Weierstrass gap sequence is by definition $\{1, 2, 3, \cdots, g\}$. Then $\varphi_i = g + i$ for $i \geq 1$, hence $\tilde{\varphi}_i = 1$, $i \geq 1$, $\tilde{\varphi}_0 = g + 1$. We would like to find a 'small' counterexample in the sense of the 2-digit sum of n. By Remark 3.4.24, we can only expect counterexamples when m is at least 3. Hence let us set m to be 3, i.e., $\Gamma(n) \in I_4$.

Observe that in this case, for any $\underline{a} \in J_3$, it must be of one of the following forms: $(1,1)$, $(3,0)$ or $(0,3)$. To get a small $\mathrm{digsum}_2(n)$, it is natural to consider $2 \not| n$ and $\Gamma(n) = (3,0)+(1,1)+(1,1) = (5,2)$, i.e., $n = 2^0+2^{i_1}+2^{i_2}+2^{i_3}+2^{i_3}+2^{i_4}+2_{j_1}+2^{j_2}$ where $0 < i_1 < i_2 < i_3 < i_4$ are even and $j_1 < j_2$ are odd. To get an optimal O different from the greedy G, $O_0 \neq G_0$, hence $\Gamma(O_0) \neq \Gamma(G_0)$ by the τ-monotonicity. Therefore, we have $\Gamma(G)$ is either

$$\begin{pmatrix} 3 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 & 3 \\ 1 & 1 & 0 \end{pmatrix}.$$

If it is the first case, then we have $j_2 > i_3$ and $j_1 > i_2$. And it is easy to check that O must be the same as G. So we can conclude that

$$G = \begin{pmatrix} 1 & 1 & 3 \\ 1 & 1 & 0 \end{pmatrix}, O = \begin{pmatrix} 3 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

By the τ-monotonicity of G, we must have $i_3 > j_2$. Now let us compare the weights of G and O:

$$\begin{aligned} wt(G) &= (g+2)n - (2^0 + 2^{j_1} + 2^{i_1} + 2^{j_2}) - (g+1)(2^0 + 2^{j_1}) \\ wt(O) &= (g+2)n - (2^0 + 2^{i_1} + 2^{i_2} + 2^{j_1} + 2^{i_3}) - (g+1)(2^0 + 2^{i_1} + 2^{i_2}). \end{aligned}$$

Then $wt(O) - wt(G) = (g+1)(2^{j_1} - 2^{i_2} - 2^{i_1}) - (2^{i_3} + 2^{i_2} - 2^{j_2})$. Hence $j_1 > i_2$. Therefore we get the ordering of $\tau(n)$:

$$2^{i_4} > 2^{i_3} > 2^{j_2} > 2^{j_1} > 2^{i_2} > 2^{i_1} > 2^0,$$

and thus a candidate of n as $n = 2^0 + 2^2 + 2^4 + 2^5 + 2^7 + 2^8 + 2^{10}$. It is easy to see that the greedy element in $U_3(n)$ is $G = (2^0 + 2^5, 2^2 + 2^7, 2^4 + 2^8 + 2^{10})$, and the element $O = (2^0 + 2^2 + 2^4, 2^5 + 2^8, 2^7 + 2^{10})$ lies in $U_3(n)$ and is the only optimal element in $U_3(n)\backslash\{G\}$. By comparing the difference of the weights, we can see that when $g \geq 11$, $wt(O) \geq wt(G)$, i.e., an optimal element is not necessary to be the greedy one. In particular, when $g = 11$, we obtain two optimal elements, G and O.

When $g = 11$, by computation, we can see that there are exactly two optimal elements, namely O and G. Both of them have weight 18432, while the sum of the corresponding terms has degree 18428, which is exactly the degree of the coefficient S_{g+2}.

For $g > 11$, the above optimal element O is the only optimal one and hence the degree of the coefficient S_{g+2} is just $wt(O)$.

Example 3.7.2. Suppose that ∞ a non-Weierstrass point as in last example. For any prime p and $q = p^2$, we consider n as follows:

$$\begin{aligned} n =&(p-1)p^0 + (p-1)p^2 + \ldots + (p-1)p^{2p} \\ &+ (p-1)p^{2p+1} + (p-1)p^{2p+3} \\ &+ (p-1)p^{2p+4} + (p-1)p^{2p+6}. \end{aligned}$$

The greedy element is

$$\begin{aligned} G = (&(p-1)p^0 + \ldots + (p-1)p^{2p-4} + (p-2)p^{2p-2} + p^{2p+1}, \\ &p^{2p-2} + (p-2)p^{2p} + (p-2)p^{2p+1} + p^{2p+3}, \\ &p^{2p} + (p-2)p^{2p+3} + (p-1)p^{2p+4} + (p-1)p^{2p+6}). \end{aligned}$$

Its weight is

$$\begin{aligned} wt(G) =&(g+2)n - ((p-1)p^0 + \ldots + (p-1)p^{2p-2} + (p-2)p^{2p} + (p-1)p^{2p+1} \\ &+ p^{2p+3}) - (g+1)((p-1)p^0 + \ldots + (p-1)p^{2p-4} + (p-2)p^{2p-2} + p^{2p+1}). \end{aligned}$$

And the only optimal element in $U_3(n)\backslash\{G\}$ is

$$\begin{aligned} O = (&(p-1)p^0 + \ldots + (p-1)p^{2p}, \\ &(p-1)p^{2p+1} + (p-1)p^{2p+4}, \\ &(p-1)p^{2p+3} + (p-1)p^{2p+6}). \end{aligned}$$

Its weight is

$$\begin{aligned} wt(O) =&(g+2)n - ((p-1)p^0 + \ldots + (p-1)p^{2p} + (p-1)p^{2p+1} + (p-1)p^{2p+4}) \\ &- (g+1)((p-1)p^0 + \ldots + (p-1)p^{2p}). \end{aligned}$$

By observing the difference of the weight, we can conclude that

(i) if $g = p^5 - p^4 - p^2 - 1$, then there exist two optimal elements in $U_3(n)$, namely O and G;

(ii) if $g < p^5 - p^4 - p^2 - 1$, then there exists a unique optimal element in $U_3(n)$, and it coincides with the greedy element G;

(iii) if $g > p^5 - p^4 - p^2 - 1$, then there exists a unique optimal element in $U_3(n)$, which is just O.

In order to achieve a better bound of g, we vary n such that it is of the form

$$\begin{aligned} n =&(p-1)p^0 + \ldots + (p-1)p^{2p} \\ &+ (p-1)p^i + (p-1)p^{i+2} \\ &+ (p-1)p^j + (p-1)p^{j+2}, \end{aligned}$$

where $i > 2p$ odd and $j > i+2$ even. Using same method as above, the greedy element G is given by

$$\begin{aligned}
G_2 &= (p-1)p^{j+2} + (p-1)p^j + (p-2)p^{i+2} + p^{2p},\\
G_1 &= (p-2)p^{2p} + p^{2p-2} + p^{i+2} + (p-2)p^i,\\
G_0 &= (p-2)p^{2p-2} + (p-1)p^{2p-4} + \ldots + (p-1)p^0 + p^i,
\end{aligned}$$

and the only optimal element in $U_3(n)\backslash\{G\}$, denoted by O, is given by

$$\begin{aligned}
O_2 &= (p-1)p^{j+2} + (p-1)p^{i+2},\\
O_1 &= (p-1)p^j + (p-1)p^i,\\
O_0 &= (p-1)p^{2p} + \ldots + (p-1)p^0.
\end{aligned}$$

Their weights are

$$\begin{aligned}
wt(G) =&(g+2)n - ((p-1)p^0 + \ldots + (p-1)p^{2p-2} + (p-2)p^{2p} + (p-1)p^i + p^{i+2})\\
&- (g+1)((p-1)p^0 + \ldots + (p-1)p^{2p-4} + (p-2)p^{2p-2} + p^i);\\
wt(O) =&(g+2)n - ((p-1)p^0 + \ldots + (p-1)p^{2p} + (p-1)p^i + (p-1)p^j)\\
&- (g+1)((p-1)p^0 + \ldots + (p-1)p^{2p}).
\end{aligned}$$

Look at the difference and we can see that in order to assure the element O having a larger weight than the greedy element, we must have that

$$g > \frac{(p-1)p^j - p^{i+2} - p^{2p}}{p^i - (p-1)p^{2p} - p^{2p-2}}.$$

When $j = i+3$ and i tends to ∞, we get a lower bound of the right hand side, which is

$$p^4 - p^3 - p^2.$$

Therefore, as long as $g > p^4 - p^3 - p^2 - 1$, we can always find some n of this form such that $wt(O) > wt(G)$. In particular, when $p = 2$, this bound coincides with the bound we already have in the previous sections, namely $(p+q)/2 = 3$.

Example 3.7.3. When $m = 4$, suppose now that ∞ is a non-Weierstrass point and n is an integer such that $E^{-1}\Gamma(n) = (4, 2p+2)$. Then clearly $\Gamma(m) \in \mathfrak{J}_5$. By computation, we see that the following n contributes to an interesting example

$$\begin{aligned}
n =&(p-1)p^0 + \ldots + (p-1)p^{2p}\\
&+ (p-1)p^i + (p-1)p^{i+2}\\
&+ (p-1)p^j + \ldots + (p-1)p^{j+2p+4},
\end{aligned}$$

where $i > 2p$ odd and $j > i+2$ even.

Comparing with the above example, we see that gives the same bound on g in order to make sure that the element O has a larger weight than the greedy one, where O is given by

$$\begin{aligned} O_3 &= (p-1)p^{j+2p+4} + \ldots + (p-1)p^{j+4}, \\ O_2 &= (p-1)p^{j+2} + (p-1)p^{i+2}, \\ O_1 &= (p-1)p^{j} + (p-1)p^{i}, \\ O_0 &= (p-1)p^{2p} + \ldots + (p-1)p^{0}, \end{aligned}$$

and G is

$$\begin{aligned} G_3 &= (p-1)p^{j+2p+4} + \ldots + (p-1)p^{j+4}, \\ G_2 &= (p-1)p^{j+2} + (p-1)p^{j} + p^{2p} + (p-2)p^{i+2}, \\ G_1 &= (p-2)p^{2p} + p^{2p-2} + p^{i+2} + (p-2)p^{i}, \\ G_0 &= (p-2)p^{2p-2} + (p-1)p^{2p-4} + \ldots + (p-1)p^{0} + p^{i}. \end{aligned}$$

In this case, the weights are computed as follows:

$$\begin{aligned} wt(O) =&(g+3)n - ((p-1)p^0 + \ldots + (p-1)p^{2p} + (p-1)p^i + (p-1)p^{i+2} \\ &+ (p-1)p^j + (p-1)p^{j+2}) - ((p-1)p^0 + \ldots + (p-1)p^{2p} + (p-1)p^i \\ &+ (p-1)p^j) - (g+1)((p-1)p^0 + \ldots + (p-1)p^{2p}); \\ wt(G) =&(g+3)n - ((p-1)p^0 + \ldots + (p-1)p^{2p} + (p-1)p^i + (p-1)p^{i+2} \\ &+ (p-1)p^j + (p-1)p^{j+2}) - ((p-1)p^0 + \ldots + (p-1)p^{2p-2} + (p-2)p^{2p} \\ &+ (p-1)p^i + p^{i+2}) - (g+1)((p-1)p^0 + \ldots + (p-1)p^{2p-4} + (p-2)p^{2p-2} \\ &+ p^i). \end{aligned}$$

It is clear that we get the same asymptotic bound of g as in the above example, namely

$$p^4 - p^3 - p^2 - 1.$$

Example 3.7.4. Let m and ∞ be as above. Suppose now p is an odd prime. Let n be

$$\begin{aligned} n =&(p-1)p^0 + \ldots + (p-1)p^{2p} \\ &+ (p-1)p^i + (p-1)p^{i+2} + (p-1)p^{i+4} \\ &+ (p-1)p^j + (p-1)p^{j+2} + (p-1)p^{j+4} \end{aligned}$$

where $i > 2p$ odd and $j > i + 4$ even. Then as in the second example, the greedy element G is given by

$$\begin{aligned} G_3 &= (p-1)p^{j+4} + (p-1)p^{j+2} + (p-1)p^{j} + 2p^{2p} + (p-3)p^{i+4}, \\ G_2 &= (p-3)p^{2p} + 2p^{2p-2} + 2p^{i+4} + (p-3)p^{i+2}, \\ G_1 &= (p-3)p^{2p-2} + 2p^{2p-4} + 2p^{i+2} + (p-3)p^{i}, \\ G_0 &= (p-3)p^{2p-4} + (p-1)p^{2p-6} + \ldots + (p-1)p^{0} + 2p^{i}. \end{aligned}$$

There exists a unique optimal element O in $U_4(n)\backslash\{G\}$, which is

$$\begin{aligned}
O_3 &= (p-1)p^{j+4} + (p-1)p^{i+4},\\
O_2 &= (p-1)p^{j+2} + (p-1)p^{i+2},\\
O_1 &= (p-1)p^{j} + (p-1)p^{i},\\
O_0 &= (p-1)p^{2p} + \ldots + (p-1)p^{0}.
\end{aligned}$$

Their weights are

$$\begin{aligned}
wt(G) =& (g+3)n - ((p-1)p^0 + \ldots + (p-1)p^{2p-2} + (p-3)p^{2p} + (p-1)p^i\\
&+ (p-1)p^{i+2} + 2p^{i+4}) - ((p-1)p^0 + \ldots + (p-1)p^{2p-4} + (p-3)p^{2p-2}\\
&+ (p-1)p^i + 2p^{i+2}) - (g+1)((p-1)p^0 + \ldots + (p-1)p^{2p-6} + (p\\
&- 3)p^{2p-4} + 2p^i);\\
wt(O) =& (g+3)n - ((p-1)p^0 + \ldots + (p-1)p^{2p} + (p-1)p^i + (p-1)p^{i+2}\\
&+ (p-1)p^j + (p-1)p^{j+2}) - ((p-1)p^0 + \ldots + (p-1)p^{2p} + (p-1)p^i\\
&+ (p-1)p^j) - (g+1)((p-1)p^0 + \ldots + (p-1)p^{2p}).
\end{aligned}$$

The difference of the weights $wt(O) - wt(G)$ is

$$\begin{aligned}
wt(O) - wt(G) =& - (2p^{2p} - 2p^{i+4} + (p-1)p^j + (p-1)p^{j+2})\\
&- (2p^{2p-2} + (p-1)p^{2p} - 2p^{i+2} + (p-1)p^j)\\
&+ (g+1)(-2p^{2p-4} - (p-1)p^{2p-2} - (p-1)p^{2p} + 2p^i).
\end{aligned}$$

In order to get that $wt(O) > wt(G)$, we will need

$$g+1 > \frac{(p-1)p^{j+2} + 2(p-1)p^j - 2p^{i+4} - 2p^{i+2} + (p+1)p^{2p} + 2p^{2p-2}}{2p^i - (p-1)p^{2p} - (p-1)p^{2p-2} - 2p^{2p-4}}.$$

Let $j = i+5$ and i tend to infinity and we get a lower bound of the right hand side, hence an asymptotic bound of the upper bound of g, which is

$$\frac{p-1}{2}p^7 - (p-1)p^5 - p^4 - p^2 - 1.$$

This bound is clearly worse than the one in the last example.

Example 3.7.5. Now let $p = 2$ and $s = 3$, i.e., $q = 8$. Same as above, we suppose that ∞ is a non-Weierstrass point. Let

$$n = 2^0 + \ldots + 2^{18} + 2^{19} + 2^{20} + 2^{22} + 2^{23} + 2^{24} + 2^{27}.$$

Clearly, it lies in $\mathfrak{J}_4$. When we consider $U_3(n)$, we can see that the greedy element $G = (G_0, G_1, G_2)$ is given by

$$\begin{aligned} G_2 &= 2^{18} + 2^{23} + 2^{24} + 2^{27} \\ G_1 &= 2^{15} + 2^{20} + 2^{22} \\ G_0 &= 2^0 + \ldots + 2^{12} + 2^{19}. \end{aligned}$$

It is of weight

$$\begin{aligned} wt(G) =&(g+2)n - (2^0 + \ldots + 2^{15} + 2^{19} + 2^{20} + 2^{22}) \\ &- (g+1)(2^0 + \ldots + 2^{12} + 2^{19}). \end{aligned}$$

One can show that there exists a unique optimal element in the set $U_3(n)\backslash\{G\}$, denoted by $O = (O_0, O_1, O_2)$, where

$$\begin{aligned} O_2 &= 2^{22} + 2^{23} + 2^{27} \\ O_1 &= 2^{19} + 2^{20} + 2^{24} \\ O_0 &= 2^0 + \ldots + 2^{18}. \end{aligned}$$

Its weight is

$$wt(O) = (g+2)n - (2^0 + \ldots + 2^{18} + 2^{19} + 2^{20} + 2^{24}) - (g+1)(2^0 + \ldots + 2^{18}).$$

Now we look at the difference of the weights:

$$wt(O) - wt(G) = -(2^{24} - 2^{22} + 2^{18}) + (g+1)(2^{19} - 2^{18} - 2^{15}).$$

Hence, when $g \geq 55$, the weight of O is not smaller than that of G. In particular, when $g = 55$, there exists exactly two optimal elements in $U_3(n)$, namely O and G.

Similar as above, we can generalize this to arbitrary p and get an asymptotic bound of the genus. Here

$$\begin{aligned} n =&(p-1)p^0 + \ldots + (p-1)p^{3i} + (p-1)p^{3j_1+1} + (p-1)p^{3j_1+2} + (p-1)p^{3j_2+1} \\ &+ (p-1)p^{3j_2+2} + (p-1)p^{3k_1} + (p-1)p^{3k_2}, \end{aligned}$$

where $i = p^2 + p \leq j_1 < j_2 < k_1 < k_2$.

The greedy element G is given by

$$\begin{aligned} G_3 &= p^{3i} + (p-2)p^{3j_2+1} + (p-1)p^{3j_2+2} + (p-1)p^{3k_1} + (p-1)p^{3k_2} \\ G_2 &= p^{3(i-1)} + (p-2)p^{3i} + (p-2)p^{3j_1+1} + (p-1)p^{3j_1+2} + p^{3j_2+1} \\ G_0 &= (p-1)p^0 + \ldots + (p-1)p^{3(i-2)} + (p-2)p^{3(i-1)} + p^{3j_1+1}. \end{aligned}$$

And the unique optimal element O in $U_3(n)\backslash\{G\}$ is given by

$$\begin{aligned} O_2 &= (p-1)p^{3j_2+1} + (p-1)p^{3j_2+2} + (p-1)p^{3k_2} \\ O_1 &= (p-1)p^{3j_1+1} + (p-1)p^{3j_1+2} + (p-1)p^{3k_1} \\ O_0 &= (p-1)p^0 + \ldots + (p-1)p^{3i}. \end{aligned}$$

Compare the weights and we get

$$\begin{aligned} wt(O) - wt(G) = &- ((p-1)p^{3k_1} - p^{3j_2+1} + p^{3i} \\ &+ (g+1)(p^{3j_1+1} - (p-1)p^{3i} - p^{3(i-1)}). \end{aligned}$$

Hence we can get an asymptotic bound for g:

$$(p-1)p^5 - p^3 - 1.$$

3.8 Example: Hyperelliptic curves and more

In this section, let $\mathcal{C}$ be a hyperelliptic curve. Then the gap sequence is $\{1, 3, \ldots, 2g-1\}$, i.e., $\tilde{\varphi}_i = 2$ for $i < g$. Recall that we have shown in Proposition 3.4.14 that the weight of optimal or greedy element is bounded as follows:

$$\phi_m n \leq wt(X) \leq \varphi_{m-1}(n),$$

where ϕ_m are given as follows:

$$\begin{aligned} \phi_1 =&0,\ \phi_2 = \frac{q+p-2}{q+p}\varphi_1, \\ \phi_m =&\frac{q+p-2}{q+p}((\frac{2}{q+p})^{m-2}\varphi_1 + \ldots + \frac{2}{q+p}\varphi_{m-2} + \varphi_{m-1}). \end{aligned}$$

Lemma 3.8.1. *For a hyperelliptic curve, we always have $\phi_m > \varphi_{m-2}$.*

Proof. Same as in the proof to Lemma 3.4.16, we have that

$$\phi_m - \varphi_{m-2} = (1-\chi)\tilde{\varphi}_{m-2} - \chi^2\tilde{\varphi}_{m-3} - \ldots - \chi^{m-1}\tilde{\varphi}_0.$$

If $m-2 < g$, then

$$\phi_m - \varphi_{m-2} = 2(1-\chi) - 2\chi^2 - \ldots - 2\chi^{m-1} = 2(2 - \frac{1-\chi^m}{1-\chi}) > 0$$

since $\chi = \frac{2}{p+q} \leq \frac{1}{3}$.

If $m-2 \geq g$, then the statement follows directly from Lemma 3.4.16. □

Hence we have an unconditional version of Lemma 3.4.17 or Lemma 3.4.16. Analogously, we can conclude that if X is either optimal or greedy in $U_m(n)$, then there exists some h such that $\Gamma(X_i) \in J_0^h$ for all $i = 0, \dots, m-1$. Hence we can get an unconditional version of Proposition 3.4.23:

Proposition 3.8.2. *If there exists some n' and m' such that in $U_{m'}(n')$, there exists an optimal element $O' = (O'_0, \dots, O'_{m'-1})$ which is different from the greedy element. Then there exist an n, an m and an optimal element $O = (O_0, O_1, \dots, O_{m-1})$ in $U_m(n)$ such that*

(i) $\Gamma(O_j) \in J_2^0$*, for* $0 \leq j \leq m-2$.

(ii) $\deg_p(O_{m-1}) < \deg_p(G_{m-1})$*, where* $G = (G_0, G_1, \dots, G_{m-1})$ *is the greedy element in* $U_m(n)$.

(iii) $\Gamma(O_{m-1}) \neq \Gamma(G_{m-1})$.

(iv) $O_{m-1} = p^{\tilde{\omega}}$ *for some* $\tilde{\omega} \in \mathbb{N}$.

(v) $\underline{\psi}_0 \cdot \Gamma(O_{m-1}) = \underline{\psi}_0 \cdot \Gamma(G_{m-1})$.

Furthermore, assume that there exists such a pair m and n, then we can construct an element Z in $U_m(n)$ as in Section 3.4. Lemma 3.5.2, 3.5.3, 3.5.4 and Corollary 3.5.5 still hold. Then we have an analogue to Lemma 3.5.6 as follows

Lemma 3.8.3. *The difference of the weight of Z and O is bounded by*

$$wt(Z) - wt(O) > Z_{m-1} - 2p^{\tilde{\omega}} - Q.$$

Proof. Using the same method as in the proof to Lemma 3.5.6, we have

$$\begin{aligned}
wt(Z) - wt(O) =& \tilde{\varphi}_{m-2}(Z_{m-1} - p^{\tilde{\omega}}) - \sum_{j=0}^{m-3} \tilde{\varphi}_j(\tilde{Z}_j - \tilde{O}_j) \\
\geq& Z_{m-1} - p^{\tilde{\omega}} - \sum_{j=0}^{m-3} \tilde{\varphi}_j(\tilde{Z}_j - \tilde{O}_j) \\
\geq& Z_{m-1} - p^{\tilde{\omega}} - \sum_{j=0}^{m-3} 2(\sum_{h=\alpha}^{\omega} \frac{p-1}{p^s-1} \tau_h^{\delta_{h,j+1}}) \\
\geq& Z_{m-1} - p^{\tilde{\omega}} - \sum_{h=\alpha}^{\omega} \frac{2(p-1)}{p^s-1} \sum_{j=0}^{m-3} \tau_h^{\delta_{h,j+1}}
\end{aligned}$$

$$
\begin{aligned}
&\geq Z_{m-1} - p^{\tilde{\omega}} - \sum_{h=\alpha}^{\omega} \frac{2(p-1)}{p^s-1}\frac{p^s}{p^s-1}\tau_h^{\delta_{h,m-2}} \\
&= Z_{m-1} - p^{\tilde{\omega}} - \frac{2(p-1)p^s}{(p^s-1)^2}(Q+p^{\tilde{\omega}}) \\
&> Z_{m-1} - 2p^{\tilde{\omega}} - Q.
\end{aligned}
$$

□

Theorem 3.8.4. *For any pair (m, n), if $U_m(n)$ is nonemtpy, then any optimal element must be greedy.*

Proof. Suppose the contrary, then we can find a pair (m, n) and an optimal element O satisfying Proposition 3.8.2. Then we can construct a Z as described in Section 3.4.

Recall that by Lemma 3.5.2 and Lemma 3.5.3, we have that

$$\deg_p(Z_{m-1}) = \deg_p(G_{m-1}) > \tilde{\omega}$$

and

$$\deg_p(Z_{m-1}) \geq r + s$$

where $r := \deg_p(Q)$ if Q is nonzero.

If $p \geq 3$, then in the sum $2p^{\tilde{\omega}} + Q$, the multiplicity of a single p-power is at most 2, hence

$$\deg_p(2p^{\tilde{\omega}} + Q) = \max\{\tilde{\omega}, r\} < \deg_p(Z_{m-1}).$$

Thus $Z_{m-1} - 2p^{\tilde{\omega}} - Q > 0$.

If $p = 2$, then $2p^{\tilde{\omega}} = p^{\tilde{\omega}+1}$. Recall that any p-power in Q is congruent to some p^i mod $p^s - 1$, for $i = \alpha, \dots, \omega - 1$, and $p^{\tilde{\omega}} \equiv p^{\omega} \pmod{p^s - 1}$.

If $p^{\tilde{\omega}+1} \notin \tau(Q)$, then in the summation $p^{\tilde{\omega}+1} + Q$, the greatest coefficient of any p-power is at most 1, there cannot be any carryovers, hence

$$\deg_p(p^{\tilde{\omega}+1} + (p-1)Q) = \max\{\tilde{\omega} + 1, r\}.$$

As shown in Lemma 3.5.2 and Lemma 3.5.3, both $\tilde{\omega}$ and r are smaller than $\deg_p(Z_{m-1})$. Hence we consider the following two cases:

- if $\deg_p(Z_{m-1}) > \tilde{\omega} + 1$, then we have

$$\deg_p(Z_{m-1}) > \deg_p(p^{\tilde{\omega}+1} + (p-1)Q);$$

- if $\deg_p(Z_{m-1}) = \tilde{\omega} + 1$, then by Corollary 3.5.5 we have

$$\deg_p(Z_{m-1} - p^{\tilde{\omega}+1}) \geq r + s > r = \deg_p((p-1)Q).$$

Otherwise, if $p^{\tilde{\omega}+1} \in \tau(Q)$, then there will be carryover, and we have

$$\deg_p(p^{\tilde{\omega}+1} + (p-1)Q) \leq r + 1 < r + s < \deg_p(Z_{m-1}).$$

Either way, we always have that

$$Z_{m-1} - 2p^{\tilde{\omega}} - Q > 0.$$

Hence Z has a larger weight than O, which contradicts to the optimality of O. □

Now we can formulate the Riemann hypothesis for hyperelliptic curves.

Theorem 3.8.5. *For any positive integer n, the break points of the Newton polygon of $\zeta_\infty(-n, T)$ have x-coordinates φ_i for $i = 0, 1, \ldots$ with slopes G_i^i, where G_i^i denotes the last entry of the greedy element in $U_{i+1}(n)$. Hence for $0 \leq i \leq g-1$, there exist exactly two zeros of valuation G_i^i; for $i > g$, there exist a simple zero of valuation G_i^i.*

Similarly, if the curve has gap sequence $\{1, 2, 4, 5, \ldots\}$, i.e., $\tilde{\varphi}_i = 3$ for $i = 0, 1, \ldots, \lfloor \frac{2g}{3} \rfloor - 1$. Note that for $i = \lfloor \frac{2g}{3} \rfloor$, we have

$$\tilde{\varphi}_i = \begin{cases} 1 & \text{if } g \equiv 0, 1 \pmod 3; \\ 2 & \text{else.} \end{cases}$$

Using the same method, we can show that the same result holds.

4. Some Results on Partial zeta Functions

4.1 Introduction

In Chapter 3, we have seen the Riemann hypothesis for global Goss zeta functions. In this chapter, we will consider instead the Riemann hypothesis for partial Goss zeta functions. As we have seen, when dealing with the global Goss zeta functions, we can only expect the zeros to be simple when they have relatively large valuations when applying the method of Newton polygons. But luckily, based on some numerical tests, this disturbing phenomenon will not occur when we turn to partial Goss zeta functions.

Recall that we fix two distinct places ∞ and v of the function field K of a smooth geometrically irreducible curve over $\mathbb{F}_q$, where ∞ is $\mathbb{F}_q$-rational. Denote by A the ring of functions regular away from ∞. On this ring, we have a sign function and a degree function with respect to the place ∞. Hence for any $d \in \mathbb{N}$, we can define a subset $A_{+,d}$ consisting of ∞-positive functions of degree d. Let $\bar{b}$ be a nonzero congruence class with respect to v, then we can define the partial zeta function with respect to $\bar{b}$ as follows:

$$\zeta_A(-n, T, \bar{b}) := \sum_{d \geq 0} T^d S_d(n, \bar{b})$$

where $S_d(n, \bar{b}) = \sum_{a \in A_{+,d}, a \in \bar{b}} a^n$.

Suggested by various numerical experiments, the Newton polygon of $\zeta_A(-n, T, \bar{b})$ for a given positive integer n and a fixed nonzero congruence class $\bar{b}$ behaves much better than that of $\zeta_A(-n, T)$, in the sense that all the slopes have width 1, which means that all the zeros are simple with pairwise distinct valuations. Moreover, we observe from the data that the Newton polygons are independent of the choice of the congruence class $\bar{b}$, and this suggests that we should expect some carryover of the leading coefficients when summing up all the partial zeta functions to get the global one.

Throughout this chapter, we always assume that $A = \mathbb{F}_q[t]$, and $v = (f)$ with $f \in A_+$. We denote by s_d the valuation of $S_d(n, \bar{b})$ at v.

In this Chapter, we will concentrate on the following two cases: Section 4.2 is devoted to the case when $\deg(v) = 1$, where we have a complete understanding of s_d's based on the results from Chapter 3. The main results in this part are formulated as Theorem 4.2.6 and Theorem 4.2.7. The first one states that there exists a unique so-called t-optimal element, which is an analogue of optimal element in Chapter 3, and it must be t-greedy, which is, similarly, an analogue of greedy element in Chapter 3, while the latter concerns the zero distribution of the value of $\zeta_A(-n, T, \bar{b})$ at a given positive n, and it states that all zeros are simple of pairwise distinct valuations. In the next section, we focus on the case when $\deg(v) = 2$, and try to look at the problem from two different aspects. In Section 4.3.1 we state a recursive formula and then apply it to get a nice result when $q = 2$. In Section 4.3.2 we will investigate the $\tilde{S}$'s appearing in the expansion of $S_d(n, \bar{b})$ as in Remark 4.3.1, and Theorem 4.3.9 offers a close formula to the valuations and leading coefficients of $\tilde{S}$'s. However, this could not settle the general problem on s_d, since the formula of the valuation of $\tilde{S}(n)$ depends significantly on the p-adic expansion of n, on which we have not gained enough information.

4.2 Degree 1 place case

Throughout this section, we suppose that the place $v = (f)$ is $\mathbb{F}_q$-rational, i.e. $\deg(f) = 1$. We fix a representative b of $\bar{b}$ such that $\deg(b) < \deg(v)$, i.e. $b \in \mathbb{F}_q^*$. Then we can expand the sum as

$$\begin{aligned} S_d(n, \bar{b}) &= \sum_{a \in A_{+,d}, a \equiv b(f)} a^n \\ &= \sum_{a_1, \ldots, a_{d-1} \in \mathbb{F}_q} (b + a_1 f + a_2 f^2 + \ldots + a_{d-1} f^{d-1} + f^d)^n \\ &= \sum_{\substack{a_1, \ldots, a_{d-1} \in \mathbb{F}_q \\ X_0 + \ldots + X_d = n}} \binom{n}{X_0, \ldots, X_d} b^{X_0} a_1^{X_1} \ldots a_{d-1}^{X_{d-1}} f^{X_1 + \ldots + (d-1)X_{d-1} + dX_d}. \end{aligned}$$

Definition 4.2.1. For any element X in $\mathbb{N}^{m+1}$, we define the *t-weight* as

$$wt_t(X) = X_1 + 2X_2 + \ldots + mX_m.$$

Let V be any subset of $\mathbb{N}^{m+1}$. We call an element $X = (X_0, X_1, \dots, X_m)$ in V *t-optimal* (resp. *t-greedy*) if it has minimal weight (resp. it is lexicographically maximal).

Definition 4.2.2. We define the following subset of $\mathbb{N}^{m+1}$:

$$\begin{aligned} V_m(n) = \{X = (X_0, \dots, X_d) \in \mathbb{N}^{m+1} \,| X_0 + \dots + X_m = n, \\ p \nmid \binom{n}{X_0, X_1, \dots, X_m}, \\ X_i \text{ is a positive multiple of } q-1 \text{ for } i = 1, 2, \dots, m-1\}. \end{aligned}$$

The elements in $V_m(n)$ are called the *t-valid compositions of n of length m.*

Remark 4.2.3. Since we consider the partial zeta functions in this chapter, the t occuring in the above definitions is merely an abbreviation of ‘teil’, the German word for ‘partial’.

Remark 4.2.4. Note that the definition of the t-weight here coincides with the definition of weight in Definition 3.2.4 for the case $g = 0$.

Remark 4.2.5. Recall that in Definition 3.2.7, we have defined the set of valid compositions of n of length m as follows:

$$\begin{aligned} U_m(n) := \{X = (X_0, X_1, \dots, X_{m-1}) \in \mathbb{N}^m : X_0 + \dots + X_{m-1} = n, \\ p \nmid \binom{n}{X_0, X_1, \dots, X_{m-1}}, \\ X_i \text{ is a positive multiple of } q-1, \text{ for } i = 0, 1, \dots, m-2\}. \end{aligned}$$

Hence for n' such that $\tau(n') \subset \tau(n)$, we can embed $U_m(n')$ into $V_m(n)$ by sending $(X_0, X_1, \dots, X_{m-1})$ to $(X_{m-1}, \dots, X_0, n-n')$. In this way, we can say that $V_m(n)$ is the disjoint union of $U_m(n')$ for all n' such that $\tau(n') \subset \tau(n)$. For any $X \in V_m(n)$, we have $wt_t(X) = mn - n' - wt(X')$ with $X' = (X_{m-1}, X_{m-2}, \dots, X_0) \in U_m(n')$, $n' = n - X_0$ and wt is defined as in Definition 3.2.4 for $g = 0$. Based on this observation, it is immediate to see that $\Gamma(n) \in I_m$ if and only if $V_m(n) \neq \emptyset$.

Theorem 4.2.6. *There exists a unique t-optimal element in $V_m(n)$ which is the t-greedy element.*

Proof. Let $X = (X_0, X_1, \dots, X_m)$ be a t-optimal element in $V_m(n)$. We claim that $X_m = 0$. Otherwise, let $\tilde{X}$ be $(X_0 + X_m, X_1, \dots, X_{m-1}, 0)$. It lies in $V_m(n)$ by definition and has a smaller t-weight than X does since $wt_t(\tilde{X}) - wt_t(X) = -mX_d < 0$. Thus for any t-optimal element $X = (X_0, X_1, \dots, X_m)$ in $V_m(n)$, we have $X' := (X_{m-1}, \dots, X_1, X_0)$ lying in $U_m(n)$. In Remark 4.2.5, we have that

$wt_t(X) = mn - n - wt(X') = (m-1)n - wt(X')$, hence X' must be optimal in $U_m(n)$ in the sense of Definition 3.2.6. By Theorem 3.5.1, when $g = 0$, there exists a unique optimal element in $U_m(n)$, and it must be the greedy one. Hence there must exist a unique t-optimal element O in $V_m(n)$, which arises from the unique optimal, hence the greedy element in $U_m(n)$, thus O must be t-greedy in $V_m(n)$ by definition. □

We can now conclude the following theorem concerning the distribution of zeros:

Theorem 4.2.7. *Suppose that both ∞ and v are $\mathbb{F}_q$-rational places. Let n be any positive integer and $\bar{b}$ be a nonzero congruent class with respect to v.*

(a) All the segments of the Newton polygon associated to $\zeta_{\mathbb{F}_q[t]}(-n, T, \bar{b})$ have width 1.

(b) The d-th slope is $\sum_{j=1}^{d-1} G_{m-j}$ where m is defined such that $\Gamma(n) \in I_m \backslash I_{m+1}$ and $G = (G_0, \ldots, G_{m-1}, 0)$ is the t-greedy element in $V_m(n)$.

Hence all zeros of $\zeta_{\mathbb{F}_q[t]}(-n, T, \bar{b})$ are simple. Furthermore, all of the zeros have pairwise distinct valuations at v.

Proof. From Theorem 4.2.6, we know that

$$v_v(S_d(n, \bar{b})) = wt_p(X^d)$$

where X^d is the t-greedy element in $V_d(n)$. Since m is defined such that $n \in I_m \backslash I_{m+1}$, we have $V_m(n) \neq \emptyset$ and $V_{m+1}(n) = \emptyset$. Let $G = (G_0, G_1, \ldots, G_{m-1}, 0)$ be the t-greedy element in $V_m(n)$. Then $d \leq m$ and for $X^d = (X_0^d, \ldots, X_d^d) \in V_d(n)$ t-greedy, we have

$$\begin{aligned} X_d^d &= 0, \\ X_i^d &= G_{m-d+i}, \text{ for } i = d-1, \ldots, 1, \\ X_0^d &= G_{m-d} + \ldots + G_0. \end{aligned}$$

Hence we can compute $s_d := v_v(S_d(n, \bar{b}))$ as

$$s_d = \sum_{i=1}^{d-1} i G_{m-d+i}.$$

Then the slope of the d-th line segment between (d, s_d) and $(d-1, s_{d-1})$ is

$$s_d - s_{d-1} = \sum_{i=1}^{d-1} i G_{m-d+i} - \sum_{i=1}^{d-2} i G_{m-d+1+i} = \sum_{j=1}^{d-1} G_{m-j}.$$

So for $1 \le d < m$, the difference of the $d+1$-th and the d-th slopes is

$$(s_{d+1} - s_d) - (s_d - s_{d-1}) = \sum_{j=1}^{d} G_{m-j} - \sum_{j=1}^{d-1} G_{m-j} = G_{m-d} > 0,$$

which means that the horizontal width of each line segment in the Newton polygon of $\zeta_\infty^{(v)}(-n, T, \bar{b})$ is always one, hence the statement follows. □

4.3 Degree 2 Place

Suppose now that v is of degree 2, then $\bar{b} \in (\mathbb{F}_q/v)^* \cong \mathbb{F}_{q^2}^*$ and $\deg(f) = 2$. As in the last section, we fix a representative b of $\bar{b}$, such that $\deg(b) < 2$. For any $n \in \mathbb{N}$, we define

$$\tilde{S}(n) := \sum_{a \in \mathbb{F}_p[t]_{+,\le 1}} a^n = 1 + \sum_{i \in \mathbb{F}_p} (t+i)^n.$$

Recall that in Chapter 3, we defined $\mathfrak{J}$ and I_m, J_m for $m \in \mathbb{Z}_{>0}$ as follows:

$$\begin{aligned}
&\mathfrak{J} = \{\Gamma(n) \mid n \text{ is a positive multiple of } p-1\};\\
&I_m = \{\Gamma(n) \mid U_m(n) \neq \emptyset\} = \{\Gamma(n) \mid V_m(n) \neq \emptyset\};\\
&J_m = \mathfrak{J} \cap (I_m \backslash I_{m+1}).
\end{aligned}$$

Remark 4.3.1. Observe that similar as in the previous section, we can expand the summands in the definition of $S_d(n, \bar{b})$ as follows.

- If the degree is even, i.e., of the form $2d$, then

$$\begin{aligned}
S_{2d}(n, \bar{b}) &= \sum_{\substack{a \in A_{+,2d} \\ a \equiv b \pmod{f}}} a^n = \sum_{a_1, \ldots, a_{d-1} \in \mathbb{F}_q[t]_{\le 1}} (b + a_1 f + \ldots + a_{d-1} f^{d-1} + f^d)^n \\
&= \sum_{\substack{a_1, \ldots, a_{d-1} \in \mathbb{F}_q[t]_{\le 1} \\ X_0 + \ldots + X_d = n}} \binom{n}{X_0, \ldots, X_d} b^{X_0} a_1^{X_1} \ldots a_{d-1}^{X_{d-1}} f^{X_1 + \ldots + dX_d} \\
&= \sum_{X_0 + \ldots + X_d = n} \binom{n}{X_0, \ldots, X_d} \left(\prod_{i=1}^{d-1} \left(\sum_{a \in \mathbb{F}_q[t]_{\le 1}} a^{X_i} \right) \right) b^{X_0} f^{X_1 + \ldots + dX_d} \\
&= \sum_{X \in W_d(n)} \binom{n}{X_0, \ldots, X_d} (-1)^{d-1} \tilde{S}(X_1) \ldots \tilde{S}(X_{d-1}) b^{X_0} f^{X_1 + \ldots + dX_d},
\end{aligned}$$

where

$$\begin{aligned} W_d(n) := \{X = (X_0, \ldots, X_d) \in \mathbb{N}^{d+1} \,| & X_0 + \ldots + X_d = n, \\ & p \nmid \binom{n}{X_0, \ldots, X_d} \\ & \Gamma(X_i) \in \mathfrak{J} \cap I_3 \text{ for } i = 1, \ldots, d-1\}. \end{aligned}$$

In particular, to guarantee $S_{2d}(n, \bar{b})$ not vanishing, we need

$$\Gamma(n) = \Gamma(X_0) + \ldots + \Gamma(X_d) \in I_{2d-1}.$$

- If the degree is odd, i.e., of the form $2d+1$, then

$$\begin{aligned} S_{2d+1}(n, \bar{b}) &= \sum_{\substack{a \in A_{+,2d+1} \\ a \equiv b \pmod f}} a^n \\ &= \sum_{\substack{a_1, \ldots, a_{d-1} \in \mathbb{F}_q[t]_{\leq 1} \\ a_d \in \mathbb{F}_q[t]_{+,1}}} (b + a_1 f + \ldots + a_{d-1} f^{d-1} + a_d f^d)^n \\ &= \sum_{\substack{a_1, \ldots, a_{d-1} \in \mathbb{F}_q[t]_{\leq 1} \\ a_d \in \mathbb{F}_q[t]_{+,1}}} \sum_{X_0 + \ldots + X_d = n} \binom{n}{X_0, \ldots, X_d} b^{X_0} a_1^{X_1} \ldots a_{d-1}^{X_{d-1}} a_d^{X_d} f^{X_1 + \ldots + dX_d} \\ &= \sum_{X_0 + \ldots + X_d = n} \binom{n}{X_0, \ldots, X_d} \prod_{i=1}^{d-1} \left(\sum_{a \in \mathbb{F}_q[t]_{\leq 1}} a^{X_i} \right) \left(\sum_{a \in \mathbb{F}_q[t]_{+,1}} a^{X_d} \right) b^{X_0} f^{X_1 + \ldots + dX_d} \\ &= \sum_{X \in W'_d(n)} \binom{n}{X_0, \ldots, X_d} (-1)^{d-1} \tilde{S}(X_1) \ldots \tilde{S}(X_{d-1}) S_1(X_d) b^{X_0} f^{X_1 + \ldots + dX_d}, \end{aligned}$$

where

$$\begin{aligned} W'_d(n) := \{X = (X_0, \ldots, X_d) \in \mathbb{N}^{d+1} \,| & X_0 + \ldots + X_d = n, \\ & p \nmid \binom{n}{X_0, \ldots, X_d}, \\ & X_i \in \mathfrak{J} \cap I_3 \text{ for } i = 1, \ldots, d-1, \\ & X_d \in I_2\}. \end{aligned}$$

In particular, we need $\Gamma(n) \in I_{2d}$ to make sure that $S_{2d+1}(n, \bar{b})$ does not vanish.

Therefore, $S_d(n, \bar{b}) \neq 0$ only if $n \in I_{d-1}$.

By convention, for any polynomial $g \in \mathbb{F}_p[t]$, by the *leading coefficient of f with respect to v*, we mean the coefficient of $f^{v_v(g)}$ in the v-adic expansion of g. Denote the leading coefficient of $\tilde{S}(n)$ with respect to v by $\tilde{l}_v(n)$. Sometimes we drop the index v if it is clear from the context.

4.3.1 A Recursive Formula Within the same Congruence Class And Its Application

In this section, we will first establish a recursive formula which connects partial zeta functions with respect to the same congruence class. Afterwards, we will apply this recursive formula to the case $A = \mathbb{F}_2[t]$ to get a nice result.

Let $c \in \mathbb{F}_p[t]_{\leq 1}$ be such that $bt + c \equiv b \pmod{f}$. Then we have

$$\{a \mid a \in A_{+,d},\, a \in \bar{b}\} = \{at + c + if \mid a \in A_{+,d-1},\, a \in \bar{b},\, i \in \mathbb{F}_q\}.$$

Then we can rewrite the definition of $S_d(n, \bar{b})$ as

$$\begin{aligned} S_d(n,\bar{b}) &= \sum_{\substack{a \in A_{+,d} \\ a \equiv b \pmod{f}}} a^n \\ &= \sum_{\substack{a \in A_{+,d-1} \\ a \equiv b \pmod{f}}} \sum_{i \in \mathbb{F}_q} (at + c + if)^n \\ &= \sum_{k_0+k_1+k_2=n} \binom{n}{k_0, k_1, k_2} \Big(\sum_{\substack{a \in A_{+,d-1} \\ a \equiv b \pmod{f}}} a^{k_0} \Big) t^{k_0} c^{k_1} \Big(\sum_{i \in \mathbb{F}_q} i^{k_2}\Big) f^{k_2} \\ &= - \sum_{\substack{k_0+k_1+k_2=n \\ q-1 \mid k_2, k_2>0}} \binom{n}{k_0, k_1, k_2} S_{d-1}(k_0, \bar{b}) t^{k_0} c^{k_1} f^{k_2}. \end{aligned} \tag{4.1}$$

Now let $A = \mathbb{F}_2[t]$, then the only degree 2 place is $(v) = (t^2 + t + 1)$, i.e., we have in this case $f = t^2 + t + 1$ and $b \in \{1, t, t+1\}$. Note that in this case, $p = q = 2$, hence $\Gamma(n) \in I_m$ is equivalent to that $\operatorname{digsum}_2(n) \geq m - 1$. By Remark 4.3.1, if $S_d(n, \bar{b}) \neq 0$, we must have $\operatorname{digsum}_2(n) \geq d - 2$.

To get the result, we will need the following conjecture:

Conjecture 4.1. *Denote by $\tilde{n_d}$ the sum of the first $d-2$ summands appeared in the 2-adic expansion of n. Then we have*

$$v_v(S_d(n, \bar{b})) = v_v(S_d(\tilde{n_d}, \bar{b})).$$

We have computed for all n up to 2^{10} and the results suggest the above conjecture.

Theorem 4.3.2. *Assuming Conjecture 4.1, we have*

$$v_v(S_d(n, \bar{b})) = \sum_{i=1}^{d-2} \mu_i 2^{n_i},$$

where n_i's are those appeared in the 2-adic expansion of n, i.e., $n = \sum_{i=1}^{l} 2^{n_i}$ with $n_1 < n_2 < \ldots < n_l$, and μ_i is defined as

$$\mu_i := \#\{j \mid i \leq j \leq d-2,\ 2 \mid n_j - n_i\}.$$

Proof. As we have seen above, $S_d(n, \bar{b}) = 0$ when $\mathrm{digsum}_2(n) < d - 2$. Assuming the conjecture, w.l.o.g we can assume that $\mathrm{digsum}_2(n) = d - 2$. Then in the recursive formula (4.1), the only summands which are nonzero are those with $k_1 = 0$ and $k_2 \in \tau(n)$. Hence we have

$$S_d(n, \bar{b}) = -\sum_{k \in \tau(n)} S_{d-1}(n - k, \bar{b}) t^{n-k} f^k.$$

Apply this recursively and we get:

$$\begin{aligned} S_d(n, \bar{b}) =& (-1)^2 \sum_{k_1, k_2 \in \tau(n), k_1 \neq k_2} S_{d-2}(n - k_1 - k_2, \bar{b}) t^{n-k_1} t^{n-k_1-k_2} f^{k_1+k_2} \\ =& \cdots \\ =& (-1)^{d-3} \sum_{\sigma \in \Sigma_{d-2}} S_3(2^{n_{\sigma(d-2)}}, \bar{b}) t^{m_\sigma} f^{n - 2^{n_{\sigma(d-2)}}} \end{aligned} \tag{4.2}$$

where Σ_{d-2} is the set of permutations of $\{1, 2, \ldots, d-2\}$, and m_σ is defined as follows:

$$\begin{aligned} m_\sigma &= n - 2^{n_{\sigma(1)}} + (n - 2^{n_{\sigma(1)}}) - 2^{n_{\sigma(2)}} + \ldots + (n - \sum_{j=1}^{d-4} 2^{n_{\sigma(j)}}) - 2^{n_{\sigma(d-3)}} \\ &= (2^{n_{\sigma(2)}} + \ldots + 2^{n_{\sigma(d-2)}}) + \ldots + 2^{n_{\sigma(d-2)}} \\ &= \sum_{j=1}^{d-2} (j-1) \cdot 2^{n_{\sigma(j)}}. \end{aligned}$$

By the definition of $S_d(n, \bar{b})$, we can compute the $S_3(2^{n_{\sigma(d-2)}}, \bar{b})$ directly:

$$\begin{aligned} S_3(2^{n_{\sigma(d-2)}}, \bar{b}) &= \sum_{a \in A_{+,3}, a \in \bar{b}} a^{2^{n_{\sigma(d-2)}}} = \sum_{a \in A_{+,1}} (fa+b)^{2^{n_{\sigma(d-2)}}} \\ &= (tf+b)^{2^{n_{\sigma(d-2)}}} + ((t+1)f+b)^{2^{n_{\sigma(d-2)}}} \\ &= f^{2^{n_{\sigma(d-2)}}} t^{2^{n_{\sigma(d-2)}}} + f^{2^{n_{\sigma(d-2)}}} (t+1)^{2^{n_{\sigma(d-2)}}} \\ &= f^{2^{n_{\sigma(d-2)}}}. \end{aligned}$$

Plug the above into equation (4.2), we have

$$S_d(n, \bar{b}) = (-1)^{d-3} f^n \sum_{\sigma \in \Sigma_{d-2}} t^{\sum_{j=1}^{d-2} (j-1) 2^{n_{\sigma(j)}}}. \tag{4.3}$$

Now the question is how to compute the valuation of $\sum_{\sigma \in \Sigma_{d-2}} t^{\sum_{j=1}^{d-2} (j-1) 2^{n_{\sigma(j)}}}$, which is the determinant of the following $(d-2) \times (d-2)$ matrix

$$A = \begin{pmatrix} t^{0 \cdot 2^{n_1}} & t^{0 \cdot 2^{n_2}} & \dots & t^{0 \cdot 2^{n_{d-2}}} \\ t^{1 \cdot 2^{n_1}} & t^{1 \cdot 2^{n_2}} & \dots & t^{1 \cdot 2^{n_{d-2}}} \\ \vdots & \vdots & \ddots & \vdots \\ t^{(d-3) \cdot 2^{n_1}} & t^{(d-3) \cdot 2^{n_2}} & \dots & t^{(d-3) \cdot 2^{n_{d-2}}} \end{pmatrix}.$$

The above is a Vandermonde matrix, hence its determinant is

$$\pm \prod_{1 \le i < j \le d-2} (t^{2^{n_j}} - t^{2^{n_i}}).$$

Combine all the discussions above, we have now:

$$\begin{aligned} S_d(n, \bar{b}) &= (-1)^{d-1} f^n \cdot \det(A) \\ &= \pm f^n \cdot \prod_{1 \le i < j \le d-2} (t^{2^{n_j}} - t^{2^{n_i}}) \end{aligned}$$

Its valuation at v is:

$$\sum_{i=1}^{d-2} \mu_i 2^{n_i}$$

with μ_i defined as in the statement. □

Theorem 4.3.3. *Assuming Conjecture 4.1, let n be a fixed positive integer and $\bar{b}$ be a nonzero congruent class with respect to v. The we have the following:*

(a) All of the segments of the Newton polygon associated to $\zeta^{(t^2+t+1)}_{\mathbb{F}_2[t]}(-n, T, \bar{b})$ have width 1.

(b) The d-th slope is

$$\sum_{\substack{i=1 \\ 2|n_{d-2}-n_i}}^{d-2} 2^{n_i}$$

where $n = 2^{n_1} + \ldots + 2^{n_l}$, $n_0 < n_1 < \ldots < n_l$ is the 2-adic expansion of n. In particular, the slopes form a strictly increasing sequence.

Hence all zeros of $\zeta^{(t^2+t+1)}_{\mathbb{F}_2[t]}(-n, T, \bar{b})$ are simple. Furthermore, all of the zeros have pairwise distinct valuations at v.

Proof. By Theorem 4.3.2, we can directly compute the d-th slope of the Newton polygon, which is

$$s_d - s_{d-1} = \sum_{i=1}^{d-2} \mu_i 2^{n_i} - \sum_{i=1}^{d-3} \mu_i 2^{n_i} = \sum_{\substack{i=1 \\ 2|n_{d-2}-n_i}}^{d-2} 2^{n_i}.$$

Hence

$$\begin{aligned}(s_{d+1} - s_d) - (s_d - s_{d-1}) &= \sum_{\substack{i=1 \\ 2|n_{d-1}-n_i}}^{d-1} 2^{n_i} - \sum_{\substack{i=1 \\ 2|n_{d-2}-n_i}}^{d-2} 2^{n_i} \\ &\geq 2^{n_{d-1}} - \sum_{\substack{i=1 \\ 2|n_{d-2}-n_i}}^{d-2} 2^{n_i} > 0.\end{aligned}$$

Then the statement follows. □

Remark 4.3.4. Unfortunately this method cannot be applied to cases when $q \neq 2$, since in these cases, we will need to face the fact that the elements in $\tau(n)$ may have multiplicity at most $p-1$, hence in equation (4.3), there may be more terms with the same minimal valuations, therefore if we want to apply this method, we also need to take the leading coefficients into consideration.

4.3.2 The Valuation of $\tilde{S}$

As we have seen, the method of Section 4.3.1 does not apply to the general case, so we turn back to the expansion of $S_d(n, \bar{b})$ in Remark 4.3.1. In this section, we will investigate the valuation of $\tilde{S}$'s and the leading coefficients. Although the results cannot be applied directly to get the valuation of $S_d(n, \bar{b})$, this may help to get a deeper insight into the problem. As an outline of this section, the first part provides an important division of $\mathbb{N}$ and the main result will be stated as Theorem 4.3.9. Sections 4.3.2.2 to 4.3.2.6 make up the proof to the main result.

Throughout this section, we always assume that $p = q$.

4.3.2.1 The Main Result

Definition 4.3.5. (1) We define the following subsets of $\mathbb{N}$: for any $i \in \mathbb{N}$,

$$C_i := \{n \in \mathbb{N} \mid (p+1)(p-1)p^i \leq n < (p+1)(p-1)p^{i+1}\}$$
$$C_{-\infty} := \{n \in \mathbb{N}^* \mid n < (p+1)(p-1)\}.$$

(2) For any $i \in \mathbb{N} \cup \{-\infty\}$, we define subsets of C_i as follows:

$$\begin{aligned}
C_i^0 :=&\{n \in C_i \mid p-1 \nmid n\};\\
C_i^1 :=&\{n \in C_i \mid \operatorname{digsum}_p(n) = p-1\};\\
C_i^2 :=&\{n \in C_i \mid (p+1)(p-1) \mid n\};\\
C_i^3 :=&\{n \in C_i \mid n \equiv \sum_{k=1}^{p-1} p^{j_k} \pmod{(p^2-1)p^i} \text{ with } 0 \leq j_1 \leq \ldots \leq j_{p-1}\\
&\leq i+1, \text{ and } \operatorname{digsum}_p(n) \geq 2(p-1)\};\\
C_i^4 :=&C_i \backslash (C_i^0 \cup C_i^1 \cup C_i^2 \cup C_i^3).
\end{aligned}$$

Moreover, for any $n \in C_i^3$, we denote by $Z_m = Z_m(n)$ the number of k's such that $j_k = m$.

The following are a few facts regarding the definition of C_i and C_i^j's.

Remark 4.3.6. Note that for $n \in \mathbb{N}$, $p-1$ divides n if and only if $p-1$ divides $\operatorname{digsum}_p(n)$.

Remark 4.3.7. For any $n \in C_i^3$, we can write n as $j(p^2-1)p^i + \sum_{k=1}^{p-1} p^{j_k}$, then $0 < j \leq p-1$ by the definition of C_i, and we can substitute the condition $\operatorname{digsum}_p(n) \geq 2(p-1)$ by

$$Z_i < j.$$

The reason is that writing out the p-adic expansion of n, we have

$$\begin{aligned}
n =& j(p^2-1)p^i + \sum_{k=1}^{p-1} p^{j_k} \\
=& (j-1)p^{i+2} + (p-1)p^{i+1} + (p-j)p^i + Z_{i+1}p^{i+1} + Z_i p^i \\
&+ \sum_{k=1}^{p-1-Z_{i+1}-Z_i} p^{j_k}.
\end{aligned}$$

So if $Z_i \geq j$, then

$$n = jp^{i+2} + Z_{i+1}p^{i+1} + (Z_i - j)p^i + \sum_{k=1}^{p-1-Z_{i+1}-Z_i} p^{j_k}.$$

Clearly, the p-digit sum of n must be $p-1$.

Moreover, we can also conclude from the p-adic expansion above that $n \in C_i^3$ has p-digit sum either $2(p-1)$ or $3(p-1)$, where the former holds if and only if $Z_{i+1} > 0$. In this case, we always have $p^{i+2} \in \tau(n)$.

Proposition 4.3.8. *Following the definition, we have*

$$\begin{aligned}
&C_{-\infty}^2 = C_{-\infty}^3 = C_{-\infty}^4 = C_0^4 = \emptyset; \\
&C_{-\infty} = C_{-\infty}^0 \sqcup C_{-\infty}^1; \\
&C_i = \sqcup_{j=0}^4 C_i^j \text{ for } i \in \mathbb{N}.
\end{aligned}$$

Proof. The first line is clear from definition. It suffices to show that $C_i^j \bigcap C_{i'}^{j'} = \emptyset$ for any $(i,j) \neq (i',j')$. Clearly, $C_i^j \bigcap C_{i'}^{j'} = \emptyset$ for any $i \neq i'$. So we only need to show that $C_i^j \bigcap C_i^{j'} = \emptyset$ for $j \neq j'$. For $i = -\infty$, it is clear that $C_i^0 \bigcap C_i^1 = \emptyset$. From now on, we assume that $i \in \mathbb{N}$.

By definition of C_i^4 and C_i^0, together with Remark 4.3.6, they are disjoint with any other set. For C_i^1, we have that $C_i^1 \bigcap C_i^3 = \emptyset$ since each element in C_i^3 by definition has p-digit sum not smaller than $2(p-1)$. So we are left with the only nontrivial parts of this statement, which are that $C_i^1 \bigcap C_i^2 = \emptyset$ and $C_i^2 \bigcap C_i^3 = \emptyset$.

For any n, we can always write n as $\sum_{p^i \in \tau(n)} p^i$. Observe that

$$\sum_{p^i \in \tau(n)} p^i \equiv \sum_{p^i \in \tau(n)} p^{i \bmod 2} \pmod{p^2-1}.$$

Now for $n \in C_i^2$, we have $n \equiv (p-1)p + (p-1) \pmod{p^2-1}$. While for $n \in C_i^1$, we have $n \equiv a_1 p + a_0 \pmod{p^2-1}$ with $a_1 + a_0 = p-1$. Clearly $C_i^1 \bigcap C_i^2 = \emptyset$.

For any $n \in C_i^3$, $n \equiv \sum_{k=1}^{p-1} p^{j_k} \pmod{p^2-1}$. By definition, $\sum_{k=1}^{p-1} p^{j_k} \in C_{i'}^1$ for some i' and it cannot be a multiple of p^2-1 since $C_{i'}^1 \bigcap C_{i''}^2$ is empty for any i'', hence $n \notin C_i^2$. We have therefore $C_i^2 \bigcap C_i^3 = \emptyset$.

□

Recall that $\tilde{S}(n) = 1 + \sum_{i \in \mathbb{F}_p} (t+i)^n$ and $\tilde{s}(n)$ denotes the valuation of $\tilde{S}(n)$ at v, while $\tilde{l}(n)$ denotes the corresponding leading coefficient. Define D to be the discriminant of f. The following theorem describes $\tilde{s}$ and $\tilde{l}$.

Theorem 4.3.9. *For any $i \in \mathbb{N} \bigcup \{\infty\}$ and any $n \in C_i$, we have the following recursive recipe:*

(0) if $n \in C_i^0$, then $\tilde{s}(n) = 0$;

(1) if $n \in C_i^1$, then $\tilde{S}(n) = 0$;

(2) if $n \in C_i^2$, then $\tilde{s}(n) = 0$ and $\tilde{l}(n) = 1$;

(3) if $n \in C_i^3$, i.e., $n \equiv \sum_{k=1}^{p-1} p^{j_k} := n' \pmod{(p^2-1)p^i}$ for some $0 \le j_1 \le j_2 \le \ldots \le j_{p-1} \le i+1$, such that $\operatorname{digsum}(n) \ge 2(p-1)$, then

$$\tilde{s}(n) = p^i + \sum_{\substack{p^k \in \tau(n') \\ k \equiv i \pmod 2}} p^k = p^i + \sum_{\substack{k=1 \\ j_k \equiv i \pmod 2}}^{p-1} p^{j_k},$$

and

$$\tilde{l}(n) = \binom{j}{Z_i + 1} \binom{p-1}{Z_{i-2}} \cdots \binom{p-1}{Z_{i'}} D^{-(1+Z_i+Z_{i-2}+\ldots+Z_{\bar{i}})},$$

where $\bar{i} \in \{0,1\}$ such that $\bar{i} \equiv i \pmod 2$ and $Z_k := \#\{p^k \in \tau(n')\}$;

(4) for $n \in C_i^4$, then let n' be such that $n \equiv n' \pmod{(p^2-1)p^i}$ and $n' \in C_{i'}$ for some $i' < i$, then $\tilde{s}(n) = \tilde{s}(n') < \infty$ and $\tilde{l}(n) = \tilde{l}(n')$.

The theorem will be proved in Sections 4.3.2.2 till 4.3.2.6.

Let us first make the following observation regarding case (4).

Lemma 4.3.10. *The procedure in case (4) always results in $n' \in C_{i'}^j$ for some $i' < i$ and $j \in \{3, 4\}$.*

Proof. Recall that for any $n \in C_i^4$, we let $n' \in C_{i'}$ for some $i' < i$ be such that $n' \equiv n \pmod{(p^2-1)p^i}$. By Proposition 4.3.8, the subsets C_i^j's are disjoint, so we only need to show that n' does not belong to $C_{i'}^0 \bigcup C_{i'}^1 \bigcup C_{i'}^2$. It is easy to see that $n' \notin C_{i'}^0 \bigcup C_{i'}^2$ since the mod action preserves the divisibility of $p-1$ and p^2-1. If $n' \in C_{i'}^1$, then $n' = \sum_{k=1}^{p-1} p^{j_k}$, with $j_k \leq i'+2 \leq i+1$, hence $n = j(p^2-1)p^i + n'$. But n cannot be in C_i^3, hence by Remark 4.3.7, we must have $\#\{k \mid j_k = i\} \geq j$ and the p-digit sum of n is $p-1$, thus $n \in C_i^1$ which contradicts the disjointness of C_i^1 and C_i^4. □

Remark 4.3.11. Since i' is strictly smaller than i, the procedure in case (4) of the theorem stops after finitely many steps, which means that after finitely many steps, we can get some n' which belongs to case (3), i.e. there exists some $n' \in C_{i'}^3$ for some $i' < i$ such that $n' \equiv n \pmod{p^2-1}$.

To end this section, we present here a corollary to the theorem. This is merely a special case of the above when $\mathrm{digsum}_p(n)$ is exactly $2(p-1)$, i.e. $n \in J_3$. The reason to focus on these n's is that as we have seen in Remark 4.3.1, those terms occurring in the final formula of $S_d(n, \bar{b})$ are of the shape $\tilde{S}(X_i)$ where $\gamma(X_i) \in \mathfrak{J} \cap I_3 \supset J_3$.

Corollary 4.3.12. *If $n \in C_i$ has p-digit sum exactly $2(p-1)$, then we have the following possibilities:*

(1) $n \in C_i^2$ iff $\#\{k|p^k \in \tau(n), k \text{ even}\} = \#\{k|p^k \in \tau(n), k \text{ odd}\} = p-1$. In this case, $\tilde{s}(n) = 0$ and $\tilde{l}(n) = 1$.

(2) $n \in C_i^3 \sqcup C_i^4$ iff $\#\{k|p^k \in \tau(n), k \text{ even}\} \neq p-1$. In this case, let l be the largest integer such that $c_l(n) := \#\{k|p^k \in \tau(n), k \geq l, k \equiv l \bmod 2\} \geq p$ and $p^l \in \tau(n)$, then

$$\tilde{s}(n) = (1-p+c_l)p^l + \sum_{\substack{p^k \in \tau(n), k<l \\ k \equiv l \pmod{2}}} p^k.$$

Proof. Note that when $\mathrm{digsum}_p(n) = 2(p-1)$, we always have $n \in C_i^j$ for some $i \in \mathbb{N}$ and $j \in \{2,3,4\}$.

The first parts of both statements follow directly from the fact that $n = \sum_{p^k \in \tau(n)} p^k \equiv \sum_{p^k \in \tau(n)} p^{k \bmod 2} \pmod{p^2-1}$ and that the sets C_i^2, C_i^3 and C_i^4 are disjoint by Proposition 4.3.8.

The part concerning the valuation $\tilde{s}(n)$ and the leading coefficient in (1) follows directly from the theorem. In (2), it suffices to show that

(i) if $n \in C_i^3$, then $i = l$;

(ii) if $n \in C_i^4$, then there exists some $m \in C_l^3$ such that $\tilde{s}(n) = \tilde{s}(m)$.

In case (i), following Remark 4.3.7, we know that the p-adic expansion of n is

$$n = jp^{i+2} + (Z_{i+1} - 1)p^{i+1} + (p - j + Z_i)p^i + \sum_{k=0}^{i-1} Z_k p^k,$$

where $Z_{i+1} \geq 1$, $Z_k \geq 0$ for $k = 0, 1, \ldots, i$ and $\sum_{k=0}^{i} Z_k = p - 1 - Z_{i+1}$. Then it is easy to see that $l = i$. The statement is just a reformulation of case (3) of Theorem 4.3.9. Otherwise, following case (4) of Theorem 4.3.9 and Remark 4.3.11, there exists some n' such that $n \equiv n' \pmod{p^2 - 1}$ and $n' \in C_{i'}^3$ for some $i' < i$, then $\tilde{s}(n) = \tilde{s}(n')$. Note also that in this procedure, the p-digit sum remains invariant. Also in this case, $i > l$, i.e. $\#\{p^{i+2} \in \tau(n)\} + \#\{p^i \in \tau(n)\} < p$, hence we have that for any l, $c_l(n) = c_l(n')$, i.e. we get the same l for n and n'. Then by case (i), $l = i'$ and we define m such that $m \equiv n \pmod{(p^2-1)p^{l+1}}$ and $m \in C_l$. It is easy to show that m lies in C_l^3 and $\tilde{s}(n) = \tilde{s}(m)$ by case (4) of Theorem 4.3.9. □

4.3.2.2 A proof of case (2)

To prove (2), we need to look at $\tilde{S}(n)$ from a different perspective.

We know that in $\mathbb{F}_p[t]/f$ with f an irreducible polynomial of degree 2, every nonzero element has order dividing $p^2 - 1$. Thus for any $a \in \mathbb{F}_p$, we always have $(t+a)^{p^2-1} \equiv 1 \pmod{f}$, i.e. we can write $(t+a)^{p^2-1} = 1 + \zeta_a f$ with some $\zeta_a \in \mathbb{F}_p[t]$. Therefore if $n \in C_i^2$, say $n = n'(p+1)(p-1)$, then

$$\begin{aligned}
\tilde{S}(n) &= \sum_{a \in \mathbb{F}_p[t]_{\leq 1,+}} a^n = 1 + \sum_{a \in \mathbb{F}_p} (t+a)^n \\
&= 1 + \sum_{a \in \mathbb{F}_p} ((t+a)^{p^2-1})^{n'} \\
&= 1 + \sum_{a \in \mathbb{F}_p} (1 + \zeta_a f)^{n'} \\
&= 1 + \sum_{a \in \mathbb{F}_p} \left(1 + \sum_{k=1}^{n'} \binom{n'}{k} \zeta_a^k f^k \right) \\
&= 1 + \sum_{k=1}^{n'} \binom{n'}{k} f^k \left(\sum_{a \in \mathbb{F}_p} \zeta_a^k \right) \in 1 + f\mathbb{F}_p[t].
\end{aligned}$$

Therefore,

$$\tilde{s}(n) = v_f(\tilde{S}(n)) = 0,' , \tilde{l}(n) = 1.$$

4.3.2.3 A proof of case (1)

Recall that for p a prime, we always have

$$\sum_{i \in \mathbb{F}_p^*} i^n = \begin{cases} -1, & \text{if } p-1 \mid n \\ 0, & \text{else.} \end{cases}$$

By Lucas' lemma, if $a = \sum\limits_m a_m p^m$ and $b = \sum\limits_m b_m p^m$ are their p-adic expansions, then we have

$$\binom{a}{b} = \prod_m \binom{a_m}{b_m}.$$

Hence the above binomial coefficient is nonzero if and only if $\tau(a) \subseteq \tau(b)$.

The following lemma shows a simplified expansion of $\tilde{S}$.

Lemma 4.3.13 ([Gos98])**.** *The following holds:*

$$\tilde{S}(n) = 1 - \sum_{\substack{k=0 \\ p-1 \mid n-k}}^{n-1} \binom{n}{k} t^k.$$

Hence for any $n \in C_i^1$, i.e. $\mathrm{digsum}_p(n) = p - 1$, the only choice of k such that $\tau(k) \subseteq \tau(n)$ and $p - 1 \mid n - k$ is 0, hence

$$\tilde{S}(n) = 1 - 1 = 0.$$

4.3.2.4 A proof of case (0)

The following lemma will be of great importance to proving the rest of the theorem.

Lemma 4.3.14. *For $n' \equiv n \pmod{(p^2-1)p^i}$, and $\tilde{s}(n') < p^i$, we have*

$$\tilde{S}(n) \equiv \tilde{S}(n') \pmod{f^{p^i}}.$$

Proof. For $n' \equiv n \pmod{(p^2-1)p^i}$, say $n = n' + m \cdot (p^2-1)p^i$, we have:

$$\begin{aligned}
\tilde{S}(n) - \tilde{S}(n') &= \sum_{a \in \mathbb{F}_p[t]_{\leq 1,+}} a^n - \sum_{a \in \mathbb{F}_p[t]_{\leq 1,+}} a^{n'} \\
&= \sum_{a \in \mathbb{F}_p} (t+a)^{n'}((t+a)^{m(p^2-1)p^i} - 1) \\
&= \sum_{a \in \mathbb{F}_p} (t+a)^{n'}(((t+a)^{p^2-1})^{mp^i} - 1) \\
&= \sum_{a \in \mathbb{F}_p} (t+a)^{n'}((1+\zeta_a f)^{mp^i} - 1) \\
&= \sum_{a \in \mathbb{F}_p} (t+a)^{n'} \left(\sum_{k=1}^{mp^i} \binom{mp^i}{k} \zeta_a^k f^k \right) \\
&= \sum_{a \in \mathbb{F}_p} (t+a)^{n'} \left(\sum_{k'=1}^{m} \binom{m}{k'} \zeta_a^{k'p^i} f^{k'p^i} \right).
\end{aligned}$$

Hence the valuation of $\tilde{S}(n) - \tilde{S}(n')$ is at least p^i. Since we assume that $\tilde{s}(n')$ is smaller than p^i, we hence have the desired equivalence. □

By Lemma 4.3.14, we only need to show that $\tilde{s}(n) = 0$ for $n \in C_0^0$. Using the expansion of $\tilde{S}(n)$ in Lemma 4.3.13

$$\tilde{S}(n) = 1 - \sum_{\substack{k=0 \\ p-1 \mid n-k}}^{n-1} \binom{n}{k} t^k,$$

it is easy to see that there exists no non-zero summand, hence $\tilde{S}(n) = 1$, i.e., $\tilde{s}(n) = 0$ and $\tilde{l}(n) = 1$.

4.3.2.5 A proof of case (3) and case (4)

Before we present the complete proof to case (3), we need to show some useful lemmas first.

Lemma 4.3.15. *For $\tilde{S}$ defined as above, and any r, $s \in \mathbb{N}$, we have:*

$$\tilde{S}(m)(t^{p^s} - t^{p^r}) = t^{p^s} - t^{p^r} + \tilde{S}(m+p^s) - \tilde{S}(m+p^r).$$

Moreover, we have:

$$\begin{aligned}\tilde{S}(n)(t^{p^{i+1}} - t^{p^i}) =&\tilde{S}(n + p^{i+1} - p^{i+2})(t^{p^{i+2}} - t^{p^i}) - \tilde{S}(n + p^i - p^{i+2})\\ &(t^{p^{i+2}} - t^{p^{i+1}}).\end{aligned}$$

Proof. The first statement follows directly from the definition of $\tilde{S}$:

$$\begin{aligned}\tilde{S}(m)(t^{p^s} - t^{p^r}) :=&(1 + \sum_{a\in\mathbb{F}_p}(t+a)^m)(t^{p^s} - t^{p^r})\\ =&t^{p^s} - t^{p^r} + \sum_{a\in\mathbb{F}_p}(t+a)^m(t^{p^s} - t^{p^r})\\ =&t^{p^s} - t^{p^r} + \sum_{a\in\mathbb{F}_p}(t+a)^m((t+a)^{p^s} - (t+a)^{p^r})\\ =&t^{p^s} - t^{p^r} + \sum_{a\in\mathbb{F}_p}(t+a)^{m+p^s} - \sum_{a\in\mathbb{F}_p}(t+a)^{m+p^r}\\ =&t^{p^s} - t^{p^r} + \tilde{S}(m+p^s) - \tilde{S}(m+p^r).\end{aligned}$$

In particular, if we take $m = n$, $s = r + 1 = i + 1$, then

$$\begin{aligned}\tilde{S}(n)(t^{p^{i+1}} - t^{p^i}) =&t^{p^{i+1}} - t^{p^i} + \tilde{S}(n + p^{i+1}) - \tilde{S}(n + p^i)\\ =&t^{p^{i+2}} - t^{p^i} + \tilde{S}(n + p^{i+1}) - \tilde{S}(n + p^{i+1} - p^{i+2} + p^i)\\ &- t^{p^{i+2}} + t^{p^{i+1}} - \tilde{S}(n + p^i) + \tilde{S}(n + p^i - p^{i+2} + p^{i+1})\\ =&\tilde{S}(n + p^{i+1} - p^{i+2})(t^{p^{i+2}} - t^{p^i}) - \tilde{S}(n + p^i - p^{i+2})(t^{p^{i+2}}\\ &- t^{p^{i+1}}).\end{aligned}$$

□

The following two lemmas provide us the essential ingredients to prove the argument concerning the leading coefficients.

Lemma 4.3.16. *The leading coefficient of $\frac{t^{p^2}-t}{t^p-t}$ with respect to any degree 2 irreducible polynomial over $\mathbb{F}_p$ always lies in $\mathbb{F}_p^*$. Moreover, the leading coefficient equals to $1/\Delta$ where Δ denotes the discriminant of the chosen irreducible polynomial.*

Proof. Since $t^{p^2} - t$ (resp. $t^p - t$) is the product of all degree less or equal to 2 (resp. degree 1) irreducible polynomials over $\mathbb{F}_p$, it is easy to see that the quotient $\frac{t^{p^2}-t}{t^p-t}$ has valuation 1 at any degree 2 irreducible polynomial, say f, thus the leading coefficient is just $\frac{t^{p^2}-t}{(t^p-t)f} \bmod f$. On the other hand, if we consider f as a polynomial over $\mathbb{F}_{p^2}$, it can be factored into a product of two degree 1 polynomials, i.e., $f = (t-\alpha)(t-\alpha^p)$. Hence $F := \frac{t^{p^2}-t}{(t^p-t)f} = \prod_{\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \cup \{\alpha, \alpha^p\}} (t-\beta)$.

We can first compute $F \bmod (t-\alpha)$ as follows:

$$\begin{aligned} F \bmod (t-\alpha) &= \prod_{\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \cup \{\alpha, \alpha^p\}} (\alpha - \beta) \\ &= \prod_{\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \cup \{\alpha, \alpha^p\}} (\alpha - \frac{\alpha^{p+1}}{\beta}) = \prod_{\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \cup \{\alpha, \alpha^p\}} \frac{\alpha}{-\beta}(\alpha^p - \beta) \\ &= \prod_{\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \cup \{\alpha, \alpha^p\}} \frac{\alpha}{-\beta} \cdot \prod_{\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \cup \{\alpha, \alpha^p\}} (\alpha^p - \beta). \end{aligned}$$

Claim: $\prod_{\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \cup \{\alpha, \alpha^p\}} \frac{\alpha}{-\beta} = 1$.

The proof of the claim follows directly from computation:

$$\begin{aligned} LHS = (-\alpha)^{p^2-p-2} & \prod_{\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \cup \{\alpha, \alpha^p\}} \beta^{-1} = \alpha^{p^2-p-2+p+1} \cdot \prod_{\mathbb{F}_{p^2} \setminus \mathbb{F}_p} \beta^{-1} \\ &= \prod_{\beta \mathbb{F}_{p^2} \setminus \mathbb{F}_p} \beta^{-1} = \prod_{\beta \in \mathbb{F}_{p^2}} \beta^{-1} \prod_{\gamma \in \mathbb{F}_p} \gamma \\ &= \frac{-1}{-1} = 1. \end{aligned}$$

Therefore, we know that $F \bmod (t-\alpha) = F \bmod (t-\alpha^p)$, hence by CRT, we have that the residue equals to that of F modulo f, hence must lie in $\mathbb{F}_p^*$.

We can get the explicit value of the residue by some further computation:

$$\begin{aligned} \prod_{\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \cup \{\alpha, \alpha^p\}} (\alpha - \beta) &= \frac{1}{\alpha - \alpha^p} \prod_{\gamma \in \mathbb{F}_p} (\alpha - \gamma)^{-1} \prod_{\beta \in \mathbb{F}_{p^2} \setminus \{\alpha\}} (\alpha - \beta) \\ &= \frac{1}{\alpha - \alpha^p} \cdot \prod_{\gamma \in \mathbb{F}_p} (t-\gamma) \mid_{t=\alpha} \cdot \prod_{\beta' \in \mathbb{F}_{p^2} \setminus \{0\}} \beta \\ &= \frac{1}{\alpha - \alpha^p} \cdot \frac{1}{\alpha^p - \alpha} \cdot (-1) = \frac{1}{(\alpha - \alpha^p)^2} \\ &= 1/\Delta. \end{aligned}$$

□

Recall that $v = (f)$ with $\deg(f) = 2$, and we denote by Δ the discriminant of f.

Lemma 4.3.17. *Given any degree 2 irreducible polynomial f over $\mathbb{F}_p$, the leading coefficient of $(t^p - t)^{p-1}$ with respect to f is always -1.*

Proof. It is easy to see that $(t^p - t)^{p-1}$ has valuation 0 at f, hence its leading coefficient is the residue modulo f. Moreover, we have

$$\begin{aligned}(t^p - t)^{p-1} &= \frac{t^{p^2} - t^p}{t^p - t} \\ &= \frac{t - t^p}{t^p - t} + \frac{t^{p^2} - t}{t^p - t} \\ &\equiv -1 \pmod{f}.\end{aligned}$$

□

Remark 4.3.18. An immediate consequence of the previous lemma is that for any $i \in \mathbb{N}$, the residue of $(t^p - t)^{(p-1)p^i}$ modulo f is always -1.

Before giving the proof to case (3), we need to note in particular that if $S = S_1 + S_2$ with $v_v(S_1) = v_v(S_2)$, then by the ultrametric triangle inequality, we always have $v_v(S) \geq v_v(S_1)$. Moreover, if we can show that the leading coefficients of S_1 and S_2 with respect to v do not cancel, then the equality holds. In our case, following Lemma 4.3.15, we can always write $\tilde{S}(n)$ as the sum of $\tilde{S}(n_1)(\frac{t^{p^2}-t}{t^p-t})^{p^i}$ and $-\tilde{S}(n_2)(t^p - t)^{(p-1)p^i}$, where $n_1 = n - p^{i+2} + p^{i+1}$ and $n_2 = n - (p^2 - 1)p^i$. If we have $\tilde{s}(n_1) + p^i = \tilde{s}(n_2)$, then we can conclude that $\tilde{s}(n) = \tilde{s}(n_2)$ provided $\tilde{l}(n_1)\Delta^{-1} + \tilde{l}(n_2)$ does not vanish in $\mathbb{F}_p$; if so, then $\tilde{l}(n) = \tilde{l}(n_1)\Delta^{-1} + \tilde{l}(n_2)$.

Now we can give the full proof to case (3) of Theorem 4.3.9 by induction on i and j.

First recall that for any $n \in C_i^3$, we can write n by definition as

$$n = j(p-1)p^{i+1} + j(p-1)p^i + \sum_{k=0}^{i+1} Z_k p^k$$

satisfying the following:

(i) $1 \leq j \leq p - 1$;

(ii) $\sum_{k=0}^{i+1} Z_k = p - 1$ and $Z_i < j$.

- For $i = 0$ and $j = 1$, we have $Z_0 = 0$ and $Z_1 = p - 1$, then
$$n = (p^2 - 1) + (p - 1)p.$$
Following Lemma 4.3.15, we have:
$$\begin{aligned}\tilde{S}(n) &= \tilde{S}(n - p^2 + p)\frac{t^{p^2} - t}{t^p - t} - \tilde{S}(n - (p^2 - 1))(t^p - t)^{p-1} \\ &= \tilde{S}(p^2 - 1)\frac{t^{p^2} - t}{t^p - t} - \tilde{S}((p - 1)p)(t^p - t)^{p-1} \\ &= \tilde{S}(p^2 - 1)\frac{t^{p^2} - t}{t^p - t},\end{aligned}$$
hence $\tilde{S}(n)$ has valuation 1 and leading coefficient Δ^{-1} by case (2) and Lemma 4.3.16.

- Now let $n \in C_0^3$ be such that $j := \lfloor n/(p^2 - 1)\rfloor > 1$, then we have $Z_0 < j$ and $Z_1 = p - 1 - Z_0$. Suppose that the statement holds for all $n' \in C_0^3$ with $j' < j$. Following Lemma 4.3.15, we have:
$$\begin{aligned}\tilde{S}(n) =&\tilde{S}(n - p^2 + p)\frac{t^{p^2} - t}{t^p - t} - \tilde{S}(n - (p^2 - 1))(t^p - t)^{p-1} \\ =&\tilde{S}((j - 1)(p^2 - 1) + (p - 1 - Z_0)p + (p + Z_0 - 1))\frac{t^{p^2} - t}{t^p - t} \\ &- \tilde{S}((j - 1)(p^2 - 1) + (p - 1 - Z_0)p + Z_0)(t^p - t)^{p-1} \\ =:& \tilde{S}(n_1)\frac{t^{p^2} - t}{t^p - t} - \tilde{S}(n_2)(t^p - t)^{p-1}.\end{aligned}$$
Hence
$$n_1 = \begin{cases}\text{divisible by } p^2 - 1 & \text{if } Z_0 = 0; \\ (j - 1)(p^2 - 1) + (p - Z_0)p + Z_0 - 1 & \text{if } Z_0 \geq 1.\end{cases}$$
Meanwhile, $n_2 \in C^3$ if $Z_0 < j - 1$ and $n_2 \in C^1$ otherwise. Recall that $\frac{t^{p^2} - p}{t^p - t}$ has valuation 1 with leading coefficient Δ^{-1}, and $(t^p - t)^{p-1}$ has valuation 0 with leading coefficient -1. Then we can calculate the valuation and the leading coefficient of $\tilde{S}(n)$:

  (i) if $Z_0 = 0$, then $\tilde{S}(n_1)$ has valuation 0 and leading coefficient 1, while $\tilde{S}(n_2)$ has valuation 1 and leading coefficient $(j - 1)\Delta^{-1}$, hence the valuation of $\tilde{S}(n)$ is $1 = Z_0 + 1$ and the leading coefficient is $j\Delta^{-1} = \binom{j}{1}\Delta^{-1} = \binom{j}{Z_0 + 1}\Delta^{-1(Z_0 + 1)}$;

(ii) if $0 < Z_0 < j-1$, then by the induction assumption, $\tilde{S}(n_1)$ has valuation Z_0 and leading coefficient $\binom{j-1}{Z_0}\Delta^{-Z_0}$, while $\tilde{S}(n_2)$ has valuation Z_0+1 and leading coefficient $\binom{j-1}{Z_0+1}\Delta^{-(Z_0+1)}$, hence the valuation of $\tilde{S}(n)$ is Z_0+1 and the leading coefficient is $(\binom{j-1}{Z_0}+\binom{j-1}{Z_0+1})\Delta^{-(Z_0+1)} = \binom{j}{Z_0+1}\Delta^{-(Z_0+1)}$;

(iii) if $Z_0 = j-1$, then $\tilde{S}(n_1)$ has valuation Z_0 and leading coefficient $\binom{j-1}{Z_0}\Delta^{-Z_0} = \Delta^{-Z_0}$, while $\tilde{S}(n_2) = 0$, hence the valuation of $\tilde{S}(n)$ is Z_0+1 and the leading coefficient is $\Delta^{-(Z_0+1)} = \binom{j}{Z_0+1}\Delta^{-(Z_0+1)}$.

- Let $n \in C_i^3$ be such that $i > 0$ and $j := \lfloor n/(p^2-1)p^i \rfloor = 1$, then we have $Z_i = 0$ and $Z_{i+1} + Z_{i-1} + Z_{i-2} + \ldots + Z_0 = p-1$. Suppose now that the statement holds for all $n' \in C_{i'}^3$ for $i' < i$. Recall that we denote by $\bar{i}$ the residue of i modulo 2. Following Lemma 4.3.15, we have:

$$\begin{aligned}\tilde{S}(n) =&\tilde{S}(n-p^{i+2}+p^{i+1})(\frac{t^{p^2}-t}{t^p-t})^{p^i} - \tilde{S}(n-(p^2-1)p^i)(t^p-t)^{(p-1)p^i}\\ =&\tilde{S}(Z_{i+1}p^{i+1}+(p-1)p^i+Z_{i-1}p^{i-1}+\ldots+Z_0)(\frac{t^{p^2}-t}{t^p-t})^{p^i}\\ &-\tilde{S}(Z_{i+1}p^{i+1}+Z_{i-1}p^{i-1}+Z_{i-2}p^{i-2}+\ldots+Z_0)(t^p-t)^{(p-1)p^i}\\ =&\tilde{S}(Z_{i+1}p^{i+1}+(p-1)p^i+Z_{i-1}p^{i-1}+\ldots+Z_0)(\frac{t^{p^2}-t}{t^p-t})^{p^i}\\ =:&\ \tilde{S}(n_1)(\frac{t^{p^2}-t}{t^p-t})^{p^i}.\end{aligned}$$

It is easy to see that $n_1 \in C^2$ if $Z_{i-2} = Z_{i-4} = \ldots = Z_{\bar{i}} = 0$; otherwise, let k be the largest integer such that $k \equiv i \pmod 2$ and $Z_k \neq 0$. Note that $k \equiv i \equiv \bar{i} \pmod 2$. Then we have:

$$\begin{aligned}n_1 =&Z_{i+1}(p^2-1)p^{i-1}+(p-1)(p^2-1)p^{i-2}\\ &+(Z_{i+1}+Z_{i-1})(p^2-1)p^{i-3}+(p-1)(p^2-1)p^{i-4}+\ldots\\ &+(Z_{i+1}+Z_{i-1}+Z_{i-3}+\ldots+Z_{k+3})(p^2-1)p^{k+1}+(p-1)(p^2-1)p^k\\ &+(Z_{i+1}+Z_{i-1}+Z_{i-3}+\ldots+Z_{k+1}+1)p^{k+1}+(Z_k-1)p^k+Z_{k-1}p^{k-1}\\ &+\ldots+Z_0,\end{aligned}$$

hence the valuation is

$$\tilde{s}(n_1) = Z_kp^k + Z_{k-2}p^{k-2} + \ldots + Z_{\bar{i}}p^{\bar{i}}$$

with leading coefficient

$$\tilde{l}(n_1) = \binom{p-1}{Z_k}\binom{p-1}{Z_{k-2}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(Z_k+Z_{k-2}+\ldots+Z_{\bar{i}})}.$$

Then we can calculate the valuation and leading coefficient of $\tilde{S}(n)$:

(i) if $Z_{i-2} = Z_{i-4} = \ldots = Z_{\bar{i}} = 0$, then $\tilde{S}(n_1)$ has valuation 0 and leading coefficient 1, hence the valuation of $\tilde{S}(n)$ is

$$p^i = p^i + Z_i p^i + Z_{i-2}p^{i-2} + Z_{i-4}p^{i-4} + \ldots + Z_{\bar{i}}p^{\bar{i}}$$

and the leading coefficient is

$$\Delta^{-1} = \binom{j}{Z_i + 1}\binom{p-1}{Z_{i-2}}\binom{p-1}{Z_{i-4}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(1+Z_i+Z_{i-2}+Z_{i-4}+\ldots+Z_{\bar{i}})};$$

(ii) otherwise, let k be as above, then the valuation of $\tilde{S}(n)$ is

$$\begin{aligned} &p^i + Z_k p^k + Z_{k-2}p^{k-2} + \ldots + Z_{\bar{i}}p^{\bar{i}} \\ &= p^i + Z_i p^i + Z_{i-2}p^{i-2} + Z_{i-4}p^{i-4} + \ldots + Z_{\bar{i}}p^{\bar{i}}, \end{aligned}$$

and the leading coefficient is

$$\begin{aligned} &\binom{p-1}{Z_k}\binom{p-1}{Z_{k-2}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(1+Z_k+Z_{k-2}+\ldots+Z_{\bar{i}})} \\ &= \binom{j}{Z_i+1}\binom{p-1}{Z_{i-2}}\binom{p-1}{Z_{i-4}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(1+Z_i+Z_{i-2}+Z_{i-4}+\ldots+Z_{\bar{i}})}. \end{aligned}$$

- Now let $n \in C_i^3$ be such that $i > 0$ and $j := \lfloor n/(p^2-1)p^i \rfloor > 1$, then we have $Z_i < j$. Suppose that the statement holds for all $n' \in C_{i'}^3$ for $i' < i$, as well as for $n' \in C_i^3$ with $j' < j$. Following Lemma 4.3.15, we have:

$$\begin{aligned} \tilde{S}(n) =& \tilde{S}(n - p^{i+2} + p^{i+1})(\frac{t^{p^2} - t}{t^p - t})^{p^i} - \tilde{S}(n - (p^2-1)p^i)(t^p - t)^{(p-1)p^i} \\ =& \tilde{S}((j-1)(p^2-1)p^i + Z_{i+1}p^{i+1} + (p-1)p^i + Z_{i-1}p^{i-1} + \ldots + Z_0) \\ & (\frac{t^{p^2} - t}{t^p - t})^{p^i} - \tilde{S}((j-1)(p^2-1)p^i + Z_{i+1}p^{i+1} + Z_{i-1}p^{i-1} + Z_{i-2}p^{i-2} \\ & + \ldots + Z_0)(t^p - t)^{(p-1)p^i} \\ =:& \tilde{S}(n_1)(\frac{t^{p^2} - t}{t^p - t})^{p^i} - \tilde{S}(n_2)(t^p - t)^{(p-1)p^i}. \end{aligned}$$

Similar as above, we have that $n_1 \in C^2$ if $Z_i = Z_{i-2} = \ldots = Z_{\bar{i}} = 0$, and $n_1 \in C^4$ otherwise; regarding n_2, we have that $n_2 \in C_i^3$ if $Z_i < j-1$ and $n_2 \in C^2$ if $Z_i = j-1$.

In particular, if $Z_i = 0$, then as we can see from the above case, the valuation of $\tilde{S}(n_1)$ cannot exceed $(p-1)p^{i-2}$. By Lemma 4.3.14, we can apply the above analysis of valuation and leading coefficient of $\tilde{S}(n_1)$ directly. If $Z_i \neq 0$, then $n_1 = (j-1)(p^2-1)p^i + (Z_{i+1}+1)p^{i+1} + (Z_i-1)p^i + Z_{i-1}p^{i-1} + \ldots + Z_0$, hence by induction assumption, $\tilde{S}(n_1)$ has valuation $Z_ip^i + Z_{i-2}p^{i-2} + \ldots + Z_{\bar{i}}p^{\bar{i}}$ with leading coefficient $\binom{j-1}{Z_i}\binom{p-1}{Z_{i-2}}\binom{p-1}{Z_{i-4}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(Z_i+Z_{i-2}+\ldots+Z_{\bar{i}})}$. To sum up, we have the following cases for $\tilde{S}(n_1)$:

- if $Z_i = Z_{i-2} = \ldots = Z_{\bar{i}} = 0$, then $\tilde{S}(n_1)$ has valuation 0 with leading coefficient 1;
- if $Z_i \neq 0$, then $\tilde{S}(n_1)$ has valuation $Z_ip^i + Z_{i-2}p^{i-2} + \ldots + Z_{\bar{i}}p^{\bar{i}}$ with leading coefficient $\binom{j-1}{Z_i}\binom{p-1}{Z_{i-2}}\binom{p-1}{Z_{i-4}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(Z_i+Z_{i-2}+\ldots+Z_{\bar{i}})}$;
- if $Z_i = 0$ but not all $Z_{i'}$ for $i' \equiv i \pmod 2$ are zero, then let k be the biggest integer such that $k \equiv i \pmod 2$ and $Z_k \neq 0$, then $\tilde{S}(n_1)$ has valuation $Z_kp^k + Z_{k-2}p^{k-2} + \ldots + Z_{\bar{i}}p^{\bar{i}}$ with leading coefficient
$$\binom{p-1}{Z_k}\binom{p-1}{Z_{k-2}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(Z_k+Z_{k-2}+\ldots+Z_{\bar{i}})}.$$

For $\tilde{S}(n_2)$, we have:

- if $Z_i < j-1$, then by the induction assumption, $\tilde{S}(n_2)$ has valuation $p^i + Z_ip^i + Z_{i-2}p^{i-2} + Z_{i-4}p^{i-4} + \ldots + Z_{\bar{i}}p^{\bar{i}}$ with leading coefficient
$$\binom{j-1}{Z_i+1}\binom{p-1}{Z_{i-2}}\binom{p-1}{Z_{i-4}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(1+Z_i+Z_{i-2}+Z_{i-4}+\ldots+Z_{\bar{i}})};$$
- if $Z_i = j-1$, then by case (2), $\tilde{S}(n_2)$ is zero.

Finally we can calculate the valuation and the leading coefficient of $\tilde{S}(n)$:

(1) if $Z_i < j-1$ and $Z_i = Z_{i-2} = \ldots = Z_{i \bmod 2} = 0$, then the valuation of $\tilde{S}(n)$ is
$$\tilde{s}(n) = p^i = p^i + Z_ip^i + Z_{i-2}p^{i-2} + \ldots + Z_{\bar{i}}p^{\bar{i}}$$
and the leading coefficient is
$$\begin{aligned}\tilde{l}(n) &= \Delta^{-1} + \binom{j-1}{1}\Delta^{-1} = j\Delta^{-1}\\ &= \binom{j}{Z_i+1}\binom{p-1}{Z_{i-2}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(1+Z_i+Z_{i-2}+\ldots+Z_{\bar{i}})};\end{aligned}$$

(2) if $Z_i = j-1 \neq 0$, then $\tilde{S}(n_2) = 0$, hence $\tilde{S}(n) = \tilde{S}(n_1)(\frac{t^{p^2}-t}{t^p-t})^{p^i}$. Therefore we have

$$\tilde{s}(n) = p^i + \tilde{s}(n_1) = p^i + Z_i p^i + Z_{i-2}p^{i-2} + Z_{i-4}p^{i-4} + \ldots + Z_{\bar{i}}p^{\bar{i}}$$

and

$$\begin{aligned}\tilde{l}(n) &= \tilde{l}(n_1) \cdot \Delta^{-1} \\ &= \binom{j-1}{Z_i}\binom{p-1}{Z_{i-2}}\binom{p-1}{Z_{i-4}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(1+Z_i+Z_{i-2}+Z_{i-4}+\ldots+Z_{\bar{i}})} \\ &= \binom{j}{Z_i+1}\binom{p-1}{Z_{i-2}}\binom{p-1}{Z_{i-4}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(1+Z_i+Z_{i-2}+Z_{i-4}+\ldots+Z_{\bar{i}})};\end{aligned}$$

(3) if $0 < Z_i < j-1$, then the valuation of $\tilde{S}(n)$ is

$$\tilde{s}(n) = p^i + Z_i p^i + Z_{i-2}p^{i-2} + Z_{i-4}p^{i-4} + \ldots + Z_{\bar{i}}p^{\bar{i}}$$

and the leading coefficient is

$$\begin{aligned}\tilde{l}(n) &= (\binom{j-1}{Z_i} + \binom{j-1}{Z_i+1})\binom{p-1}{Z_{i-2}}\binom{p-1}{Z_{i-4}}\cdots\binom{p-1}{Z_{\bar{i}}} \\ &\Delta^{-(1+Z_i+Z_{i-2}+\ldots+Z_{\bar{i}})} \\ &= \binom{j}{Z_i+1}\binom{p-1}{Z_{i-2}}\binom{p-1}{Z_{i-4}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(1+Z_i+Z_{i-2}+\ldots+Z_{\bar{i}})};\end{aligned}$$

(4) if $Z_i = 0$ and there exists at least one $i' < i$ such that $i' \equiv i \pmod 2$ and $Z_{i'} \neq 0$. Let k be as above, then the valuation of $\tilde{S}(n)$ is

$$\tilde{s}(n) = p^i + Z_i p^i + Z_{i-2}p^{i-2} + Z_{i-4}p^{i-4} + \ldots + Z_{\bar{i}}p^{\bar{i}}$$

since

$$\begin{aligned}&p^i + Z_k p^k + Z_{k-2}p^{k-2} + \ldots + Z_{\bar{i}}p^{\bar{i}} \\ &= p^i + Z_i p^i + Z_{i-2}p^{i-2} + Z_{i-4}p^{i-4} + \ldots + Z_{\bar{i}}p^{\bar{i}},\end{aligned}$$

and the leading coefficient is

$$\begin{aligned}\tilde{l}(n) &= (1 + \binom{j-1}{1})\binom{p-1}{Z_k}\binom{p-1}{Z_{k-2}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(1+Z_k+Z_{k-2}+\ldots+Z_{\bar{i}})} \\ &= \binom{j}{Z_i+1}\binom{p-1}{Z_{i-2}}\binom{p-1}{Z_{i-4}}\cdots\binom{p-1}{Z_{\bar{i}}}\Delta^{-(1+Z_i+Z_{i-2}+Z_{i-4}+\ldots+Z_{\bar{i}})}.\end{aligned}$$

4.3.2.6 A proof of case (4)

For case (4), we first observe the following:

Remark 4.3.19. According to the Lemma 4.3.10, we know that for any $n \in C_i^4$ for some i, the corresponding n' always satisfies that $\tilde{s}(n')$ exists. Moreover, assuming (3), $\tilde{s}(n')$ is always smaller than p^i.

Remark 4.3.20. The proof to case (4) therefore follows directly from case (3), Remark 4.3.19 and Lemma 4.3.14.

5. A cohomological approach

5.1 Introduction

In Chapter 3, we have seen that the Riemann hypothesis holds for the Goss-Thakur zeta functions attached to certain curves. In particular, we explored some examples in Section 3.6, where we used the same method to consider those curves whose function fields have class number 1 and have at least one rational place. In this chapter, we will look at one of these examples from another perspective, namely using a cohomological method introduced by Böckle in his paper [Böc13]. To be more precise, the special value of Goss zeta function at a negative integer can be viewed as the dual characteristic polynomial of certain Cartier dual action on the global sections of a locally free τ-sheaf. Hence by investigating the τ-sheaf and its dual, we can gain some information on the corresponding Goss zeta function. In particular, the leading coefficient is just the determinant of the matrix representing the Cartier dual action.

In this chapter, we only consider the curve given by $y^2 = x^3 - x - 1$ over $\mathbb{F}_3$. This is one of the only four non-trivial curves of class number 1 with a rational point given in [Hay79]. As we have seen from Section 2.2.5, the number of Drinfeld-Hayes modules attached to a given A is the same as the strict class number of A. Hence there exists a unique Drinfeld-Hayes module attached to the coefficient ring of this curve. The main result in this chapter provides a precise formula of the slopes of the Newton polygon of $z_A(-n, T)$ with n of shape $\sum_{i=1}^{l} 2 \cdot 3^{n_i}$ with $n_1 < n_2 < \ldots < n_l$, and in particular, apart from the first slope, all other slopes occur with multiplicity 1.

Note that the above theorem is a special case of Example 2.6.5 of Section 3.6, but we will approach with a different method.

This chapter begins by determining the unique Drinfeld-Hayes module, thus the corresponding τ-sheaf and the Cartier operator. Next, we fix an integer n of a special form and determine the locally free τ-sheaf which is nil-isomorphic to the n-th tensor power of the τ-sheaf. Then we determine bases of the global sections of the dual sheaf which provides us a matrix description of the Cartier dual action. Therefore the leading coefficient of the dual characteristic polynomial can be described by the discriminant of the very matrix, which is very explicit to compute.

5.2 The Drinfeld-Hayes Module and τ-sheaf

Let us first recall some notation from Chapter 2. Let q be a prime power, $q = p^s$ with p a prime and s a positive integer. Denote by k the finite field $\mathbb{F}_q$. By $\mathcal{C}$ we mean a smooth projective curve over k whose function field is K, and we write $g = g_{\mathcal{C}} = g_K$ for its genus. Fix a place ∞ of K and denote by A the ring of functions in K which are regular away from ∞. Assume that ∞ is k-rational. exact sequence $0 \to A_+ \to A\backslash\{0\} \to \mathbb{F}_q^* \to 0$. For any $d \in \mathbb{N}$ we define the set $A_d := \{a \in A \mid \deg(a) = d\}$ where $\deg(a) := \log_q(| A/(a) |)$. Define $A_{+,d}$ to be the intersection $A_+ \cap A_d$. Let B be the normalization of the ring A in the strict Hilbert class field of K with respect to ∞. Then there exits a Drinfeld-Hayes module over Spec(B) as we have discussed in Section 2.2.5. Moreover, the number of Drinfeld-Hayes modules equals to the strict class number of A by Proposition 2.2.26. These Drinfeld-Hayes modules give rise to certain A-motives over B as described in [And86, Section 1]. In this section, we will construct and try to have a deep insight into this A-motive for $A = \mathbb{F}_3[x, y]/(y^2 - x^3 + x + 1)$. Note that the strict class number of A is 1, hence $B = A$ and we have a unique Drinfeld-Hayes module, thus a unique corresponding τ-sheaf.

The construction follows [Böc13]. More details concerning properties of A-motives and τ-sheaves are referred to [Gos98, Chapter 5],[And86] and [BP09].

We consider the elliptic curve defined by $y^2 = x^3 - x - 1$ over $\mathbb{F}_3$. Let ∞ be the natural infinite place. Hence $A = \mathbb{F}_3[x, y]/(y^2 - x^3 + x + 1)$ has strict class number 1 ,thus we have a unique Drinfeld-Hayes module. We first compute its corresponding Drinfeld-Hayes module. To distinguish the base ring from the coefficient ring, we use bold letters for the base ring $\mathbf{A} = k[\mathbf{x}, \mathbf{y}]/(\mathbf{y}^2 - \mathbf{x}^3 + \mathbf{x} + 1)$. Similarly, we denote by $\mathbf{E}$ the elliptic curve defined by $\mathbf{y}^2 = \mathbf{x}^3 - \mathbf{x} - 1$ over $\mathbb{F}_3$. The Drinfeld-Hayes module attached to A is the ring homomorphism

$$\begin{aligned} \rho : \ A &\to \mathbf{A}\{\tau\} \\ a &\mapsto \rho_a \end{aligned}$$

where τ is the Frobenius homomorphism and $\mathbf{A}\{\tau\}$ is the ring of skew polynomials over $\mathbf{A}$, given by

$$\begin{aligned}\rho_x &= \mathbf{x} + \left(\mathbf{y}^2+1\right)\tau + \tau^2,\\ \rho_y &= \mathbf{y} + \left(\mathbf{y}^3-\mathbf{y}\right)\mathbf{y}\tau + \mathbf{y}\left(\mathbf{y}^2-1\right)\left(\mathbf{y}^6+\mathbf{y}^4+\mathbf{y}^2-1\right)\tau^2 + \tau^3.\end{aligned}$$

This Drinfeld-Hayes module was computed by Hayes in [Hay91]. To outline the computation briefly, we first note that it suffices to identify ρ_x and ρ_y. Let $\rho_x = \mathbf{x} + a_1\tau + \tau^2$ and $\rho_y = \mathbf{y} + b_1\tau + b_2\tau + \tau^3$ with $a_1, b_1, b_2 \in \mathbf{A}$. By the commutativity of ρ_x and ρ_y, we can get the above expressions for ρ_x and ρ_y.

Now we want to give the explicit construction of the corresponding A-motive following [Böc13]. Define $S := \mathbf{A} \otimes_k A$. We consider $M := \mathbf{A}\{\tau\}$ as the $\mathbf{A}$-A-bimodule such that an element $\mathbf{a}$ of $\mathbf{A}$ (resp. an element a of A) acts on M via multiplication from the left by $\mathbf{a}$ (resp. via composition with ρ_a from the right). It is easy to see that the actions of $\mathbf{A}$ and A commute, hence M can be viewed as an S-module. In fact, it is a projective S-module of rank 1. Next we would like to describe M explicitly. In order to distinguish from τ in $\mathbf{A}\{\tau\}$, we denote by Φ the Frobenius as an element of M.

Following the same method as in [Böc13], we compute a minimal set of generator of M over S, which is $\{1, \beta/\alpha\}$, where α and β are computed by the formula $\alpha\Phi = \beta \cdot 1$ in M, hence we have

$$\begin{aligned}\beta &= -\mathbf{y}\left(x-\mathbf{x}\right) - \mathbf{y} + y\\ \alpha &= x - \mathbf{x} - 1.\end{aligned}$$

In terms of these generators, the action of τ on M from the left is given by

$$\begin{aligned}\tau\left(1\right) &= \Phi = \beta/\alpha,\\ \tau\left(\beta/\alpha\right) &= \left(x-\mathbf{x}\right)\cdot 1 - \left(\mathbf{y}^2+1\right)\mathbf{y}\cdot\frac{\beta}{\alpha}.\end{aligned}$$

Note that the map $E \to \mathbf{E} : (x,y) \mapsto (x-1,y)$ is an isomorphism with inverse $\mathbf{E} \to E : (\mathbf{x},\mathbf{y}) \mapsto (\mathbf{x}+1,\mathbf{y})$. Let D' be the restriction of the graph of the above isomorphism to $\operatorname{Spec} S$. Then we can show that the locally free sheaf $\mathscr{L}$ associated to the projective module M is $\mathcal{O}_{\operatorname{Spec} S}(D')$. And let $D = D' \cup \{\infty \times \infty\}$ be the closure of D' in $\mathbf{E} \times E$. Then it is a divisor of degree 1 over both factors $\mathbf{E}$ and E.

To compute the associated τ-sheaf, we first let $\sigma_{\mathbf{E}}$ be the absolute Frobenius endomorphism of $\mathbf{E}$. For a divisor $\mathcal{D}$ of $\mathbf{E} \times E$, its pullback under $(\sigma_{\mathbf{E}} \times \mathrm{id}_E)^*$ is again a divisor of $\mathbf{E} \times E$. Let $\overline{\mathbf{X}}$ (resp. $\overline{X}$) to be the smooth projective curve obtained by base change $\mathbf{E}$ (resp. E) to the algebraic closure of K (resp. $\mathbf{K}$). For any $n \in \mathbb{Z}$ and $\mathcal{D}$ a divisor on $\overline{\mathbf{E}}$ (resp. on $\overline{X}$), we define $\mathcal{D}^{(n)}$ (resp. ${}^{(n)}\mathcal{D}$) by $(a,b)^{(n)} := (a^{p^n}, b^{p^n})$ (resp. ${}^{(n)}(\mathbf{a},\mathbf{b}) := (\mathbf{a}^{p^n}, \mathbf{b}^{p^n})$) on closed points. Note that for a divisor $\mathcal{D}$ of $\mathbf{E} \times E$, we can base change it to $\overline{\mathbf{X}}$ or $\overline{X}$. Following [Böc13], the base change of $(\sigma_{\mathbf{E}} \times \mathrm{id}_E)^* \, \mathcal{D}$ to $\overline{\mathbf{X}}$ is $3\mathcal{D}^{(-1)}$ and to $\overline{X}$ is ${}^{(1)}\mathcal{D}$. In particular, the degree of $(\sigma_{\mathbf{E}} \times \mathrm{id}_E)^* \, \mathcal{D}$ as a divisor on $\overline{\mathbf{X}}$ is triple of the degree of $\mathcal{D}$ as a divisor on $\overline{\mathbf{X}}$, and its degree as a divisor on $\overline{X}$ is the same as the degree of $\mathcal{D}$ as a divisor on $\overline{X}$. In particular, the base change of $(\sigma_{\mathbf{E}} \times \mathrm{id}_E)^* \, [\infty]$ to $\overline{\mathbf{X}}$ is $3[\infty]$ and to $\overline{X}$ is $[\infty]$.

Let Δ be the diagonal divisor on $\mathbf{E} \times E$ and D be the divisor defined by $\alpha = 0$ and $\beta \neq 0$. Let f be the section β/α. Then we can compute the divisors of f at $\overline{\mathbf{X}}$ and $\overline{X}$ respectively (note that the order of ∞ as a pole of β is 3 on $\overline{X}$ and 5 on $\overline{\mathbf{X}}$ respectively):

$$\mathrm{div}_{\overline{\mathbf{X}}}(f) = [\Delta] + 3[D^{(1)}] - [D] - 3[\infty],$$
$$\mathrm{div}_{\overline{X}}(f) = [\Delta] + [{}^{(1)}D] - [D] - [\infty].$$

We have a τ-sheaf $(\mathcal{O}_{\overline{\mathbf{X}}}(D - 3\infty), s \mapsto f \cdot s)$ on $\mathbf{E}$ on $\overline{K}$, which means that $\mathcal{O}_{\overline{\mathbf{X}}}(D - 3\infty)$ is a coherent sheaf on $\mathbf{E} \times \operatorname{Spec} \overline{K}$, and $s \mapsto f \cdot s$ is a homomorphism from $(\sigma_{\mathbf{E}} \times \mathrm{id}_E)^* \left(\mathcal{O}_{\overline{\mathbf{X}}}\left(D - 3\infty\right)\right)$ to $\mathcal{O}_{\overline{\mathbf{X}}}\left(D - 3\infty\right)$ with cokernel $\mathcal{O}_{\Delta + 3\infty}$.

By the equation of $\mathcal{C}$, we have that $\mathrm{d}\mathbf{x} = \mathbf{y}\mathrm{d}\mathbf{y}$ and $\Omega = \mathbf{A}\mathrm{d}\mathbf{y}$. We need to describe the Cartier operator $C : \mathbf{A}\mathrm{d}\mathbf{y} \to \mathbf{A}\mathrm{d}\mathbf{y}$ as defined in [Böc13, Lemma 2.5]. In our case, it is characterized by the following formulas:

$$C(\mathrm{d}\mathbf{y}) = 0, \quad C(\mathbf{x}\mathrm{d}\mathbf{y}) = -\mathrm{d}\mathbf{y}, \quad C(\mathbf{x}^2\mathrm{d}\mathbf{y}) = \mathbf{x}\mathrm{d}\mathbf{y},$$
$$C(\mathbf{y}\mathrm{d}\mathbf{y}) = 0, \quad C(\mathbf{x}\mathbf{y}\mathrm{d}\mathbf{y}) = 0, \quad C(\mathbf{x}^2\mathbf{y}\mathrm{d}\mathbf{y}) = \mathbf{y}\mathrm{d}\mathbf{y}.$$

Furthermore, $C(f^3 g) = fC(g)$ for any $f \in \mathbf{A}$ and $g \in \mathbf{A}\mathrm{d}\mathbf{x}$. By abuse of notation, we denote also by C the induced endomorphism $C \otimes \mathrm{id}$ on $\mathbf{A} \otimes \overline{K}\mathrm{d}\mathbf{x}$. Then we have $C(f^3 g) = f^{(1)}C(g)$ for any $f \in \mathbf{A} \otimes \overline{K}$ and $g \in \mathbf{A} \otimes \overline{K}\mathrm{d}\mathbf{x}$.

5.3 The Special Value at Certain Integers

From now on, we fix a positive integer n such that $n = \sum_{j=1}^{l} 2p^{n_j}$ for $n_1 < n_2 < \ldots < n_l$. Then $\zeta_A(-n, T)$ has degree l. To simplify the notation, we denote by Q_j the twist $Q^{(i_j)}$ of a point Q in X, and by h_j the twist $h^{(i_j)}$ of a function. Recall that $D = (x-1, y)$, $\Delta = (x, y)$ and $f = \left(-\mathbf{y}\left(x - \mathbf{x}\right) - \mathbf{y} + y\right) / \left(x - \mathbf{x} - 1\right)$. The divisor of f on $\overline{\mathbf{X}}$ is $\mathrm{div}_{\overline{\mathbf{X}}}(f) = [\Delta] + 3[D^{(-1)}] - [D] - 3[\infty]$. For simplicity, we define $x_i := x^{p^{n_i}}$, $y_i := y^{p^{n_i}}$, $D_i := D^{(n_i)}$, $\Delta_i := \Delta^{(n_i)}$, and $f_i := f^{(n_i)}$. From now on, the divisors mentioned will be the divisors on $\overline{\mathbf{X}}$ unless stated otherwise.

Recall that Theorem 2.3.18 states the relation between Goss zeta function and the global L-function associated to certain τ-sheaf. As stated in [Böc13, Remark 3.4], it suffices to know $\overline{\mathscr{H}}_n$ after change of coefficients to $\overline{K}$. Hence in our case, we can take

$$\overline{\mathscr{H}}_n = \otimes_j(\mathcal{O}_{\overline{\mathbf{X}}}(2D_j - 3\infty), s \mapsto f_j^2 s).$$

We consider the line bundle $L_n(3l\infty) = \mathcal{O}_{\overline{\mathbf{X}}}(2[D_1] + 2[D_2] + \cdots + 2[D_l] - 3l\infty)$, whose dual is $L_n^\vee(-3l\infty) = \mathcal{O}_{\overline{\mathbf{X}}}(3l\infty - 2[D_1] - 2[D_2] - \cdots - 2[D_l])\, \mathrm{d}\mathbf{x}$. Then

$$\mathcal{H}\mathrm{om}(\overline{\mathscr{H}}_n, \Omega_{\mathbf{X}\times \mathrm{Spec}\,\overline{K}}) = L_n^\vee(-3l\infty).$$

Set $W_n := H^0(L_n^\vee(-3l\infty))$ to be the vector space of global sections of $L_n^\vee(-3l\infty)$. The Riemann-Roch theorem implies that $\dim_{\overline{K}}(W_n) = l$. For simplicity, we sometimes drop $\mathrm{d}\mathbf{y}$ from the notation of sections of $L_n^\vee(-3l\infty)$.

By Theorem 2.3.18(e), let $\kappa : (\sigma \times \mathrm{id})_* D(\overline{\mathscr{H}}_n) \to D(\overline{\mathscr{H}}_n)$ denote the Cartier dual action on $D(\overline{\mathscr{H}}_n) = \mathcal{H}\mathrm{om}(\overline{\mathscr{H}}_n, \Omega_{X\times\mathrm{Spec}\,K})$ induced from τ. Then κ-action on W_n gives rise to the special value of Goss zeta function at $-n$. The next two propositions describe the action of κ and the structure of W_n as a $\overline{K}$-vector space.

Proposition 5.3.1. *The homomorphism $\kappa : (\sigma \times \mathrm{id})_* L_n^\vee(-3l\infty) \to L_n^\vee(-3l\infty)$ is given on sections as:*

$$s \mapsto C\left((f_1 f_2 \cdots f_l)^2 s\right)$$

where C is the Cartier operator.

Proposition 5.3.2. *The following are bases of W_n:*

- *(i) $\{s_1, s_2, \cdots, s_l\}$ where s_k is the unique global section of $L_n^\vee(-3l\infty)$ with simple zeros at $\Delta_1, \Delta_2, \cdots, \widehat{\Delta_k}, \cdots, \Delta_l$ and with value 1 at Δ_k, for $k = 1, 2, \cdots, l$;*
- *(ii) $\{\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_l\}$ where $\tilde{s}_k$ is the unique global section of $L_n^\vee(-3l\infty)$ with simple zeros at $\Delta_1^{(1)}, \Delta_2^{(1)}, \cdots, \widehat{\Delta_k^{(1)}}, \cdots, \Delta_l^{(1)}$ and with value 1 at $\Delta_k^{(1)}$, for $k = 1, 2, \cdots, l$;*
- *(iii) $\{b_1, b_2, \cdots, b_l\}$ defined as follows: let $\tilde{b}_k$ be the function defining the line with a double zero at the point D_k and (thus) a single zero at $-2P_k$ (defined under the group law of elliptic curve) for $k = 1, 2, \cdots, l$; let $\tilde{b}_{jk}$ be the function defining the line with single zeros at D_j, D_k and (thus) $-D_j - D_k$. Set:*

$$b_k := \begin{cases} \displaystyle\prod_{j=1}^{l} \tilde{b}_j & \text{when } k = 1; \\ \displaystyle\prod_{j=2, j\neq k}^{l} \tilde{b}_j \cdot \tilde{b}_{1k}^2 & \text{when } k \geq 2. \end{cases}$$

Remark 5.3.3. To make life easier, we compute the divisors of the above sections:

(i) $\operatorname{div}(s_k) = \sum_{j=1}^{l} (2[D_j] + [\Delta_j]) - [\Delta_k] + [R_k] - 3l\infty$ where $R_k := -\left(\sum_{j=1}^{l} (2D_j + \Delta_j)\right) + \Delta_k$ defined by the group law of the elliptic curve;

(ii) $\operatorname{div}(\tilde{s}_k) = \sum_{j=1}^{l} \left(2[D_j] + [\Delta_j^{(1)}]\right) - [\Delta_k^{(1)}] + [\widetilde{R}_k] - 3l\infty$ where $\widetilde{R}_k := -\left(\sum_{j=1}^{l} (2D_j + \Delta_j^{(1)})\right) + \Delta_k^{(1)}$;

(iii) $\operatorname{div}(b_1) = \sum_{j=1}^{l} (2[D_j] + [-2D_i]) - 3l\infty$; for $k \geq 2$, $\operatorname{div}(b_k) = \sum_{j=2,\, j\neq k}^{l} (2[D_j] + -2D_j]) + 2[-D_1 - D_k] - [-2D_1] - [-2D_k] - 3l\infty$.

Remark 5.3.4. We can write down the explicit functions of b_k's as follows: it is easy to see that $\tilde{b}_k = -y_k\mathbf{y} + \mathbf{x} + 1 - x_k + y_k^2$ and $\tilde{b}_{jk} = (x_j - x_k)\,\mathbf{y} - (y_j - y_k)\,\mathbf{x} + x_k y_j - x_j y_k - y_k + y_j$. Thus for $k = 1$, we have

$$b_1 = \prod_{j=1}^{l} \left(-y_j\mathbf{y} + \mathbf{x} + 1 - x_j + y_j^2\right);$$

and for $k \geq 2$, we have

$$\begin{aligned} b_k = \prod_{j=2, j\neq k}^{l} &\left(-y_j\mathbf{y} + \mathbf{x} + 1 - x_j + y_j^2\right) \cdot ((x_1 - x_k)\,\mathbf{y} - (y_1 - y_k)\,\mathbf{x} \\ &+ x_k y_1 - x_1 y_k - y_1 + y_k)^2 . \end{aligned}$$

Proof of Proposition 5.3.2. The first and second parts are straightforward. And (iii) follows from Remark 5.3.3. □

In the next step, we will look at the action of κ on these bases.

The Action of κ on $\{s_1, s_2, \cdots, s_l\}$

By Proposition 5.3.1, we know that $\kappa(s_k) = C((f_1 f_2 \cdots f_l)^2 s_k)$ where

$$\begin{aligned}
\operatorname{div}\left((f_1 f_2 \cdots f_l)^2 s_k\right) =& 2\sum_{j=1}^{l}\left([\Delta_j] + 3[D_j^{(-1)}] - [D_j] - 3\infty\right) + \sum_{j=1}^{l}(2[D_j] + [\Delta_j]) \\
& - [\Delta_k] + [R_k] - 3l\infty \\
=& 3\sum_{j=1}^{l}\left([\Delta_j] + 2[D_j^{(-1)}]\right) - [\Delta_k] + [R_k] - 9l\infty \\
=& 3\sum_{j=1}^{l}\left([\Delta_j] + 2[D_j^{(-1)}] + [T] - (3l+1)\infty\right) + [R_k] - [\Delta_k] \\
& - 3[T] + 3\infty
\end{aligned}$$

with $T := -\sum_{j=1}^{l}\left(\Delta_j + 2D_j^{(-1)}\right)$. Thus let t be a meromorphic section such that

$$\operatorname{div}(t) = \sum_{j=1}^{l}[\Delta_j] + 2[D_j^{(-1)}] + [T_k] - (3l+1)\infty,$$

and let $t_k := (f_1 f_2 \cdots f_l)^2 s_k t^{-3}$. By the properties of Cartier operator, we have $\kappa(s_k) = C(t^3 t_k) = t^{(1)} C(t_k)$. Following the definition of t, we know that $t^{(1)}$ has simple zeros at $\Delta_j^{(1)}$'s and double zeros at D_j's. Again by the properties of the Cartier operator, we have that $C(t_k)$ has a simple pole at $\Delta_k^{(1)}$ and the residue $\operatorname{Res}_{\Delta_k^{(1)}} C(t_k) = \operatorname{Res}_{\Delta_k} t_k$. Hence $\kappa(s_k)$ has simple zeros at all $\Delta_j^{(1)}$'s except $\Delta_k^{(1)}$, i.e., it is a nonzero multiple of $\tilde{s}_k$, and the constant is $\kappa(s_k)(\Delta_k^{(1)})$:

$$\begin{aligned}
\kappa(s_k)(\Delta_k^{(1)}) =& t^{(1)} C(t_k) = (t^{(1)})'(\Delta_k^{(1)}) \cdot \operatorname{Res}_{\Delta_k^{(1)}} C(t_k) \\
=& (t'(\Delta_k))^3 \cdot \operatorname{Res}_{\Delta_k} t_k \\
=& \left(\frac{t}{\pi_k}(\Delta_k)\right)^3 \cdot (-\pi_k^2 t_k')(\Delta_k) = -(t^3 t_k' \cdot \pi_k^{-1})(\Delta_k) \\
=& -\left((t^3 t_k)' \cdot \pi_k^{-1}\right)(\Delta_k) \\
=& -\left(((f_1 f_2 \cdots f_l)^2 s_k)' \cdot \pi_k^{-1}\right)(\Delta_k) \\
=& -\left((f_1 f_2 \cdots f_k)^2 s_k'\right)(\Delta_k) + \sum_{j=1}^{l}\left(\frac{(f_1 f_2 \cdots f_l)^2}{f_j} f_j' s_k \pi_k^{-1}\right)(\Delta_k)
\end{aligned}$$

$$= \left(\frac{(f_1 f_2 \cdots f_l)^2}{f_k} f_k' s_k \pi_k^{-1} \right) (\Delta_k) \neq 0$$

with π_k a uniformizer at Δ_k. Define $\mu_k := \left(\frac{(f_1 f_2 \cdots f_l)^2}{f_k} f_k' s_k \pi_k^{-1} \right) (\Delta_k)$. Note that by definition, Δ_k is neither a zero nor a pole of s_k (resp. f_j for $j \neq k$), but it is a simple zero of f_k, hence it is neither a zero nor a pole of $f_k f_k' \cdot \pi_k^{-1}$, i.e. $\mu_k \neq 0$ or ∞. Define $\mu := \operatorname{diag}(\mu_1, \ldots, \mu_l)$.

Therefore we have the action of κ on $\{s_1, s_2, \cdots, s_l\}$ represented as

$$\kappa(s_1, s_2, \cdots, s_l) = (\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_l) \cdot \mu.$$

The Action of κ on $\{b_1, b_2, \cdots, b_l\}$

Let ν (resp. $\tilde{\nu}$) be the $l \times l$ matrix with the (i,j)-th entry defined to be $b_j(\Delta_i)$ (resp. $b_j(\Delta_i^{(1)})$). It is easy to see that

$$(s_1, s_2, \cdots, s_l)\, \nu = (b_1, b_2, \cdots, b_l)\,, \qquad (\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_l)\, \tilde{\nu} = (b_1, b_2, \cdots, b_l)\,.$$

Therefore, we can represent the action of κ with respect to $\{b_1, b_2, \cdots, b_l\}$ by the matrix

$$\tilde{\nu}^{-1} \mu \nu.$$

Valuations of the Determinants

The special value of our zeta function at n is the characteristic polynomial of the action of κ at the corresponding linear system W_n, which is just the characteristic polynomial of the matrix $\tilde{\nu}^{-1}\mu\nu$. In particular, the leading coefficient of the special value is just the determinant.

Our aim is to compute the valuation with respect to the place ∞. Note that we have $v(x) = -2$ and $v(y) = -3$, hence by the definition of x_i and y_i, we have $v(x_i) = -2 \cdot p^{n_i}$ and $v(y_i) = -3 \cdot p^{n_i}$. We will eventually show the following proposition.that the valuation of the determinant of $\tilde{\nu}^{-1}\mu\nu$ is

Proposition 5.3.5. *Let the matrices μ, ν and $\tilde{\nu}$ be defined as above. Then we have*

$$v(\det(\tilde{\nu}^{-1}\mu\nu)) = -\sum_{k=2}^{l} 2kp^{n_k}.$$

Proof. The proof will be divided into two steps. Firstly, we compute the valuation of the determinants of each matrix.

Lemma 5.3.6. *We have*

$$v(\det(\mu)) = -\sum_{k=1}^{l}(8k+4)p^{n_k} + \sum_{\substack{k=2\\ n_k=n_{k-1}+1}} 4p^{n_k}.$$

Proof. Since μ is a diagonal matrix, its determinant is just the product of all diagonal entries

$$\det(\mu) = \prod_{k=1}^{l}\mu_k,$$

where $\mu_k = \left(\prod_{j=1,j\neq k}^{l} f_j\right)^2 \cdot f_k' \cdot \frac{f_k}{\pi_k} \cdot s_k(\Delta_k)$. By definition $f_j = \frac{-\mathbf{y}(x_j-\mathbf{x})-\mathbf{y}+y_j}{x_j-\mathbf{x}-1}$, which has a simple zero at Δ_j, a triple zero at $P_j^{(-1)}$ and a simple pole at P_j, and s_k by definition takes value 1 at Δ_k.

Hence we have for $j \neq k$

$$f_j(\Delta_k) = \frac{-y_k(x_j-x_k)-y_k+y_j}{x_j-x_k-1}$$

whose valuation is

$$v(f_j(\Delta_k)) = \begin{cases} -3p^{n_k} & \text{if } j<k; \\ p^{n_j} & \text{if } j=k+1 \text{ and } n_j=n_k+1; \\ -p^{n_j} & \text{else.} \end{cases}$$

We still need to compute $f_k' \cdot \frac{f_k}{\pi_k}(\Delta_k)$. Since Δ_k is a simple zero of f_k, we have that $f_k'(\Delta_k) = \frac{f_k}{\pi_k}(\Delta_k)$. To compute this, we take an explicit uniformizer at Δ_k, namely $\pi_k = \mathbf{y} - y_k$. We first compute the Taylor expansion of $\mathbf{x} - x_k$ at π_k: since

$$\begin{aligned}(\mathbf{x}-x_k)^3 - (\mathbf{x}-x_k) &= \mathbf{x}^3 - \mathbf{x} - 1 - \left(x_k^3 - x_k - 1\right) = \mathbf{y}^2 - y_k^2 \\ &= \pi_k^2 - y_k\pi_k,\end{aligned}$$

we have

$$\begin{aligned}\mathbf{x} - x_k =& y_k\pi_k - \pi_k^2 + (\mathbf{x}-x_k)^3 \\ =& y_k\pi_k - \pi_k^2 + \left(y_k\pi_k - \pi_k^2 + (\mathbf{x}-x_k)^3\right)^3 \\ =& y_k\pi_k - \pi_k^2 + O\left(\pi_k^3\right)\end{aligned}$$

It yields:

$$\begin{aligned}
f_k &= \frac{-\mathbf{y}\left(\mathbf{x}-x_k\right)+\left(\mathbf{y}-y_k\right)}{1+\left(\mathbf{x}-x_k\right)} = \frac{-\left(\pi_k+y_k\right)\left(\mathbf{x}-x_k\right)+\pi_k}{1+\left(\mathbf{x}-x_k\right)} \\
&= \left(-\left(\pi_k+y_k\right)\left(y_k\pi_k-\pi_k^2+O\left(\pi_k^3\right)\right)+\pi_k\right)\left(1-\left(y_k\pi_k-\pi_k^2+O\left(\pi_k^3\right)\right)\right. \\
&\quad \left.+\left(y_k\pi_k-\pi_k^2+O\left(\pi_k^3\right)\right)^2+O\left(\pi^3\right)\right) \\
&= \left(\left(1-y_k^2\right)\pi_k-y_k\pi_k^2+O\left(\pi_k^3\right)\right)\left(1-y_k\pi_k+\left(1+y_k^2\right)\pi_k^2+O\left(\pi_k^3\right)\right) \\
&= \left(1-y_k^2\right)\pi_k+\left(1-y_k-y_k^3\right)\pi_k^2+O\left(\pi_k^3\right)
\end{aligned}$$

Hence we have

$$f_k'\left(\Delta_k\right)=\frac{f_k}{\pi_k}\left(\Delta_k\right)=1-y_k^2.$$

Thus for any k, we have

$$\begin{aligned}
v(\mu_k) &= 2\left(-6p^{n_k}-\sum_{j=1}^{k-1}3p^{n_k}-\sum_{j=k+1}^{l}p^{n_j}+\begin{cases}2p^{n_{k+1}} & \text{if } n_{k+1}=n_k+1\\ 0 & \text{else}\end{cases}\right) \\
&= -6(k+1)p^{n_k}-2\sum_{j=k+1}^{l}p^{n_j}+\begin{cases}4p^{n_{k+1}} & \text{if } n_{k+1}=n_k+1\\ 0 & \text{else}\end{cases}.
\end{aligned}$$

Therefore we have the valuation of the determinant of μ:

$$v\left(\det\left(\mu\right)\right)=\sum_{k=1}^{l}v\left(\mu_k\right)=-\sum_{k=1}^{l}(8k+4)p^{n_k}+\sum_{\substack{k=2\\ n_k=n_{k-1}+1}}4p^{n_k}.$$

□

Lemma 5.3.7. *We have*

$$v(\det(\nu))=3p^{n_1}-\sum_{k=2}^{l}\left(6k-7\right)p^{n_k}.$$

Proof. Recall that the matrix ν is defined to be the $l\times l$ matrix whose (i,j)-th entry is $b_j\left(\Delta_i\right)$, where

$$\begin{aligned}
b_1\left(\Delta_i\right) &= \prod_{k=1}^{l}\left(\frac{x_i-y_ky_i+y_k^2-x_k+1}{y_k}\right); \\
b_j\left(\Delta_i\right) &= \prod_{k=2,k\neq j}^{l}\left(\frac{x_i-y_ky_i+y_k^2-x_k+1}{y_k}\right)\cdot\left(\frac{1}{x_1-x_j}\left(\left(y_1-y_j\right)x_i-\left(x_1-x_j\right)y_i\right.\right. \\
&\quad \left.\left.+x_1y_j-x_jy_1+y_1-y_j\right)\right)^2 \text{ for } j>1.
\end{aligned}$$

In order to compute the determinant, we write ν as $\gamma\rho$ where

$$\begin{aligned}\rho &:= \operatorname{diag}\left(\rho_i\right) := \operatorname{diag}\left(\prod_{k=2}^{l} \frac{x_i - y_k y_i + y_k^2 - x_k + 1}{y_k}\right),\\ \gamma &:= \left(\gamma_{ij}\right)_{i,j},\end{aligned}$$

where

$$\begin{aligned}\gamma_{i1} &:= \frac{x_i - y_1 y_i + y_1^2 - x_1 + 1}{y_1};\\ \gamma_{ij} &:= \left(\frac{\left(y_1 - y_j\right) x_i - \left(x_1 - x_j\right) y_i + x_1 y_j - x_j y_1 + y_1 - y_j}{x_1 - x_j}\right)^2 \cdot\\ &\quad \left(\frac{x_i - y_j y_i + y_j^2 - x_j + 1}{y_j}\right)^{-1}.\end{aligned}$$

For ρ, we have for any $i \geq 2$

$$v\left(\rho_i\right) = \sum_{k=2}^{i-1} \left(-3p^{n_i}\right) + 3p^{n_i} + \sum_{k=i+1}^{l} \left(-3p^{n_k}\right) = -3(i-3)p^{n_i} - \sum_{k=i+1}^{l} 3p^{n_k},$$

and

$$v\left(\rho_1\right) = -\sum_{k=2}^{l} 3p^{n_k}.$$

Therefore the valuation of the determinant of ρ is:

$$\begin{aligned}v\left(\det\left(\rho\right)\right) &= \sum_{i=1}^{l} v\left(\rho_i\right)\\ &= -\sum_{k=2}^{l} 3p^{n_k} + \sum_{i=2}^{l} \left(-3(i-3)p^{n_i} - \sum_{k=i+1}^{l} 3p^{n_k}\right)\\ &= -\sum_{k=2}^{l} 3(2k-4)p^{n_k}.\end{aligned}$$

On the other hand, for γ, we have for any i:

$$v\left(\gamma_{i1}\right) = \begin{cases} 3p^{n_1} & \text{for } i = 1;\\ -3p^{n_i} & \text{else;}\end{cases}$$

and for any i and any $j \geq 2$, we have

$$\begin{aligned} v\left(\gamma_{ij}\right) = & -v\left(\frac{1}{y_j}\left(x_i - y_j y_i + y_j^2 - x_j + 1\right)\right) + 2v\left(\frac{1}{x_1 - x_j}\left(\left(y_1 - y_j\right)x_i - \right.\right. \\ & \left.\left.\left(x_1 - x_j\right)y_i + x_1 y_j - x_j y_1 + y_1 - y_j\right)\right) \\ := & \left(I\right) + 2\left(II\right) \end{aligned}$$

where

$$\left(I\right) = \begin{cases} -3p^{n_j} & \text{if } i < j; \\ 3p^{n_j} & \text{if } i = j; \\ -3p^{n_i} & \text{if } i > j. \end{cases}$$

$$\left(II\right) = \begin{cases} -p^{n_j} & \text{if } i = 1 \text{ or } j; \\ -p^{n_j} - 2p^{n_i} & \text{if } 1 < i < j; \\ -3p^{n_i} & \text{if } i > j. \end{cases}$$

hence we have for $j \geq 2$:

$$v\left(\gamma_{ij}\right) = \begin{cases} p^{n_j} & \text{if } i = 1; \\ p^{n_j} - 4p^{n_i} & \text{if } 1 < i < j; \\ -5p^{n_i} & \text{if } i = j; \\ -3p^{n_i} & \text{if } i > j. \end{cases}$$

Therefore, there exists a unique permutation $\sigma \in \Sigma_l$ such that the valuation of $\prod_{k=1}^{l} \gamma_{k\,\sigma(k)}$ is minimal, which is $\sigma = \mathrm{id}$. The valuation of the determinant of γ is

$$v\left(\det\left(\gamma\right)\right) = v\left(\prod_{k=1}^{l} \gamma_{kk}\right) = 3p^{n_1} - \sum_{k=2}^{l} 5p^{n_k}.$$

Thus

$$\begin{aligned} v\left(\det\left(\nu\right)\right) &= v\left(\det\left(\rho\right)\right) + v\left(\det\left(\gamma\right)\right) \\ &= -\sum_{k=2}^{l} 3(2k-4)p^{n_k} + 3p^{n_1} - \sum_{k=2}^{l} 5p^{n_k} \\ &= 3p^{n_1} - \sum_{k=2}^{l} \left(6k-7\right)p^{n_k}. \end{aligned}$$

□

Lemma 5.3.8. *We have*

$$v(\det(\tilde{\nu})) = -\sum_{k=1}^{l}(12i-3)p^{n_k} + \sum_{\substack{k=2 \\ n_k=n_{k-1}+1}} 4p^{n_k}.$$

Proof. Recall that the matrix $\tilde{\nu}$ is defined as the $l \times l$ matrix $\left(b_j\left(\Delta_i^{(1)}\right)\right)_{i,j}$. Similar as above, we can write $\tilde{\nu}$ as the product of $\tilde{\rho}$ and $\tilde{\gamma}$ with $\tilde{\rho} = \operatorname{diag}_l(\tilde{\rho}_i)$ where

$$\tilde{\rho}_i = \prod_{k=2}^{l}\left(\frac{x_i^3 - y_k y_i^3 + y_k^2 - x_k + 1}{y_k}\right)$$

and $\tilde{\gamma} = (\tilde{\gamma}_{ij})$ where for any i and $j \geq 2$:

$$\begin{aligned}\tilde{\gamma}_{i1} :=& \frac{x_i^3 - y_1 y_i^3 + y_1^2 - x_1 + 1}{y_1};\\ \tilde{\gamma}_{ij} :=& \left(\frac{(y_1 - y_j)\, x_i^3 - (x_1 - x_j)\, y_i^3 + x_1 y_j - x_j y_1 + y_1 - y_j}{x_1 - x_j}\right)^2 \cdot \\ & \left(\frac{x_i^3 - y_j y_i^3 + y_j^2 - x_j + 1}{y_j}\right)^{-1}.\end{aligned}$$

For $\tilde{\rho}$: since

$$v\left(\frac{x_i^3 - y_k y_i^3 + y_k^2 - x_k + 1}{y_k}\right) = \begin{cases} -3p^{n_k} & \text{if } i < k-1; \\ -3p^{n_k} & \text{if } i = k-1 \text{ and } n_i + 1 < n_k; \\ 3p^{n_k} & \text{if } i = k-1 \text{ and } n_i + 1 = n_k; \\ -3p^{n_i+1} & \text{if } i > k-1, \end{cases}$$

we have:

$$\begin{aligned} v(\tilde{\rho}_i) &= -\sum_{k=2}^{i} 9p^{n_i} - \sum_{k=i+1}^{l} 3p^{n_k} + \begin{cases} 6p^{n_{i+1}} & \text{if } n_{i+1} = n_i + 1 \\ 0 & \text{else} \end{cases} \\ &= -9(i-1)p^{n_i} - \sum_{k=i+1}^{l} 3p^{n_k} + \begin{cases} 6p^{n_{i+1}} & \text{if } n_{i+1} = n_i + 1 \\ 0 & \text{else} \end{cases}. \end{aligned}$$

Hence

$$\begin{aligned} v(\det(\tilde{\rho})) =& \sum_{i=1}^{l} -9(i-1)p^{n_i} - \sum_{k=i+1}^{l} 3p^{n_k} + \begin{cases} 6p^{n_{i+1}} & \text{if } n_{i+1} = n_i + 1 \\ 0 & \text{else} \end{cases} \\ =& -12\sum_{k=1}^{l}(i-1)p^{n_i} + \sum_{\substack{k=2 \\ n_k=n_{k-1}+1}}^{l} 6p^{n_k}. \end{aligned}$$

On the other hand, for $\tilde{\gamma}$, we have for any i and $j \geq 2$:

$$\begin{aligned}
v\left(\tilde{\gamma}_{i1}\right) =& -3p^{n_i+1}\\
v\left(\tilde{\gamma}_{ij}\right) =& -v\left(\frac{1}{y_j}\left(x_i^3 - y_j y_i^3 + y_j^2 - x_j + 1\right)\right) + 2v\left(\frac{1}{x_1 - x_j}\left(\left(y_1 - y_j\right) x_i^3\right.\right.\\
&\left.\left. - \left(x_1 - x_j\right) y_i^3 + x_1 y_j - x_j y_1 + y_1 - y_j\right)\right)\\
&=: -\left(I\right) + 2\left(II\right)
\end{aligned}$$

where

$$\left(I\right) = \begin{cases} -3p^{n_i+1} & \text{if } j \leq i \\ 3p^{n_i+1} & \text{if } j = i+1 \text{ and } n_j = n_i + 1 \\ -3p^{n_j} & \text{if } j = i+1 \text{ and } n_j > n_i + 1 \\ -3p^{n_j} & \text{if } j > i+1. \end{cases}$$

$$\left(II\right) = \begin{cases} -3p^{n_i+1} & \text{if } j \leq i \\ -p^{n_i+1} & \text{if } j = i+1 \text{ and } n_j = n_i + 1 \\ -p^{n_j} - 2p^{n_i+1} & \text{if } j = i+1 \text{ and } n_j > n_i + 1 \\ -p^{n_j} - 2p^{n_i+1} & \text{if } j > i+1. \end{cases}$$

Hence we have

$$v\left(\tilde{\gamma}_{ij}\right) = \begin{cases} -3p^{n_i+1} & \text{if } j \leq i \\ -5p^{n_i+1} & \text{if } j = i+1 \text{ and } n_j = n_i + 1 \\ -4p^{n_i+1} + p^{n_j} & \text{if } j = i+1 \text{ and } n_j > n_i + 1 \\ -4p^{n_i+1} + p^{n_j} & \text{if } j > i+1. \end{cases}$$

Therefore, there exists a unique permutation $\sigma \in \Sigma_l$ such that the valuation of $\prod_{i=1}^{l} \tilde{\gamma}_{i\sigma(i)}$ is minimal, which is the product of $(i-1, i)$ for all i such that $n_i = n_{i-1} + 1$. The valuation of the determinant of $\tilde{\gamma}$ is

$$\begin{aligned}
v\left(\det\left(\tilde{\gamma}\right)\right) &= -\sum_{\substack{i=1\\ n_{i+1} \neq n_i + 1}} 9p^{n_i} - \sum_{\substack{i=1\\ n_{i+1} = n_i + 1}}^{l-1} 15p^{n_i}\\
&= -\sum_{k=1}^{l} 9p^{n_k} - \sum_{\substack{k=2\\ n_k = n_{k-1}+1}} 2p^{n_k}.
\end{aligned}$$

Thus

$$\begin{aligned}v\left(\det\left(\tilde{\nu}\right)\right) =& v\left(\det\left(\tilde{\rho}\right)\right) + v\left(\det\left(\tilde{\gamma}\right)\right)\\ =& -12\sum_{k=1}^{l}(i-1)p^{n_i} + \sum_{\substack{k=2\\ n_k=n_{k-1}+1}}^{l} 6p^{n_k} - \sum_{k=1}^{l} 9p^{n_k} - \sum_{\substack{k=2\\ n_k=n_{k-1}+1}} 2p^{n_k}\\ =& -\sum_{k=1}^{l}(12i-3)p^{n_k} + \sum_{\substack{k=2\\ n_k=n_{k-1}+1}} 4p^{n_k}.\end{aligned}$$

□

Now we can compute the valuation of the determinant of $\tilde{\nu}^{-1}\mu\nu$ directly:

$$\begin{aligned}v(\det(\tilde{\nu}^{-1}\mu\nu)) =& -v(\det(\tilde{\nu})) + v(\det(\mu)) + v(\det(\nu))\\ =& \sum_{k=1}^{l}(12i-3)p^{n_k} - \sum_{\substack{k=2\\ n_k=n_{k-1}+1}} 4p^{n_k} - \sum_{k=1}^{l}(8k+4)p^{n_k} + \sum_{\substack{k=2\\ n_k=n_{k-1}+1}} 4p^{n_k}\\ &+ 3p^{n_1} - \sum_{k=2}^{l}(6k-7)\,p^{n_k}\\ =& -\sum_{k=2}^{l} 2kp^{n_k}.\end{aligned}$$

□

5.4 The Main result

We take $\pi_\infty := x/y \in K$ as a uniformizer at ∞ and recall that we define $z_A(-n,T) := \zeta_A(-n, T\pi_\infty^n)$. We have the following interpolating lemma for z:

Lemma 5.4.1 (Goss). *The polynomials $z_A(-n,T)$ lie in $\mathcal{O}_\infty[T]$ for $n \in \mathbb{N}$. If $n, n' \in \mathbb{N}$ satisfy that $n \equiv n' \pmod{3^k}$, then*

$$z_A(-n,T) \equiv z_A(-n',T) \pmod{\pi_\infty^{3^k}}.$$

Now let us consider $z_A(-n,T)/(1-T\pi_\infty^n)$ and $\zeta_A(-n,T)/(1-T)$. They are both polynomials since the L-function possesses Euler product. Moreover, since the degree of $\zeta_A(-n,T)$ is $l+1$ for $n=\sum_{i=1}^{l} 2\cdot 3^{n_i}$ with $n_1<n_2<\ldots<n_l$, the degree of $\zeta_A(-n,T)/(1-T)$ is l and we define the coefficients to be $\tilde{a}_{i,n}$: $\zeta_A(-n,T)/(1-T)=\sum_{i=0}^{l}\tilde{a}_{i,n}T^i$. By definition of $z_A(-n,T)$, we have that $z_A(-n,T)/(1-T\pi_\infty^n)$ is also a polynomial of degree l. We define the coefficients to be $z_A(-n,T)/(1-T\pi_\infty^n)=:\sum_{i=0}^{l}a_{i,n}T^i$. Then we have that $\tilde{a}_{i,n}=a_{i,n}\pi_\infty^n$. Moreover, $z_A(-n,T)/(1-T\pi_\infty^n)$ satisfies the same congruence property as $z_A(-n,T)$ in Lemma 5.4.1.

Theorem 5.4.2. *We have $a_{0,n}=1$, $a_{1,n}=\pi_\infty^n$, and for $2\le j\le l$, we have*

$$v(a_{j,n})=2\cdot 3^{n_1}+\sum_{i=1}^{j-1}2(j-i)3^{n_i}.$$

Proof. Since the constant term of $\zeta_A(-n,T)$ is 1, we have the constant term of $z_A(-n,T)/(1-T\pi_\infty^n)$ is also 1, i.e., $a_{0,n}=1$. Since $A_{+,1}=\emptyset$, the coefficient of T in $\zeta_A(-n,T)$ is 0, thus $a_{1,n}=\pi_\infty^n$. Moreover, if $l\ge 2$, then we can compute the valuation of the leading coefficient following Proposition 5.3.5:

$$\begin{aligned} v(a_{l,n})=v(\tilde{a}_{l,n})+ln&=l\cdot\sum_{i=1}^{l}2\cdot 3^{n_i}-\sum_{i=2}^{l}2i\cdot 3^{n_i}\\ &=2\cdot 3^{n_1}+\sum_{i=1}^{l-1}2(l-i)3^{n_i}<n<3^{n_l+1}. \end{aligned}$$

If $l=1$, then we have nothing else to prove. If $l\ge 2$, we apply induction on n. Observe that for any $n'=\sum_{i=1}^{l'}2\cdot 3^{n'_i}$ with $n'_1<n'_2<\ldots<n'_{l'}$ and $l'\ge 2$, we have $v(a_{l',n'})<3^{n_{l'}+1}$. Now let $n'=\sum_{i=1}^{l'}2\cdot 3^{n_i}$, then $n'\equiv n \pmod{3^{n_{l'}+1}}$. Then by the congruence property, we have

$$z_A(-n,T)/(1-T\pi_\infty^n)\equiv z_A(-n',T)/(1-T\pi_\infty^{n'}) \pmod{3^{n_{l'}+1}}.$$

Therefore we have for any $2\le l'\le l$:

$$v(a_{l',n})=v(a_{l',n'})=2\cdot 3^{n_1}+\sum_{i=1}^{l'-1}2(l'-i)3^{n_i}.$$

□

Remark 5.4.3. For $A=\mathbb{F}_p[t]$, we have a closed formula for the leading coefficient of $\zeta_A(-n,T)$ for $n=\sum_{i=1}^{l}(p-1)p^{n_i}$ with $n_1<n_2<\ldots<n_l$ following Thakur [Tha13, Corollary 6], which is

$$(-1)^l\prod_{1\le i<j\le l}(t^{p^{n_j}}-t^{p^{n_i}})^{p-1}.$$

In particular, the valuation of the leading term is no other than $\sum_{i=1}^{l-1}(p-1)(l-i)p^{n_i}$.

The next corollary follows directly from Theorem 5.4.2 and the fact that $z_A(-n,T) = (1 - T\pi_\infty^n)(\sum_{i=0}^{l} a_{i,n}T^i)$.

Corollary 5.4.4. *The slopes of the Newton polygon of $z_A(-n,T)$ are:*

$$2 \cdot 3^{n_1},\ 2 \cdot 3^{n_1},\ 2 \cdot 3^{n_1} + 2 \cdot 3^{n_2},\ 2 \cdot 3^{n_1} + 2 \cdot 3^{n_2} + 2 \cdot 3^{n_3},\ \ldots,$$

in increasing order. In particular, apart from the first slope, all slopes occur with multiplicity 1.

6. On the Comparison of Goss ∞-adic and v-adic Zeta Functions

6.1 Introduction

In Chapter 2, we have defined the Goss ∞-adic and v-adic zeta functions. However, we only dealt with the ∞-adic zeta functions in the previous chapters. In this chapter, we will focus on setting up a relation between them.

Let ∞ and v be two distinct fixed places and S be a finite set of places containing v but not ∞. Define $S' := (S\backslash\{v\}) \cup \{\infty\}$. Denote by $\mathfrak{I}^{\infty,S}$ (resp. $\mathfrak{I}^{v,S'}$) the group of nonzero fractional ideals of A^∞ (resp. A^v) which are prime to all places in S (resp. S'). We first show that there exists an isomorphism ϕ between these two groups. Let $\mathfrak{J}$ be a subgroup of $\mathfrak{I}^{\infty,S}$ of finite index and let $\mathfrak{J}' := \phi(\mathfrak{J})$. We prove the main result of this chapter as follows:

Theorem 6.1.1. *Let (χ, χ') be any pair of characters such that the diagram*

$$\begin{tikzcd}
\mathfrak{I}^{\infty,S} \arrow[r, "\chi"] \arrow[d, "\phi"'] & K^{\mathrm{alg}} \\
\mathfrak{I}^{v,S'} \arrow[ur, "\chi'"'] &
\end{tikzcd} \tag{6.1}$$

commutes. Let $\tilde{\omega} : \mathfrak{I}^{\infty,S} \to \mathbb{F}_q^{\mathrm{alg}}$ be the character of finite order sending any $\mathfrak{a}$ to $\omega(\sigma(\mathfrak{a}^1_\infty))$ with ω as in the definition of v-adic exponentiation of an ideal. Then we have:

$$z^S_{A^v}(-n, T, \varphi(\mathfrak{a}) \pmod{\mathfrak{J}'}, \chi') = z^{S',(v)}_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi\tilde{\omega}^{-1})$$

for any $\mathfrak{a} \in \mathfrak{I}^{\infty,S}$.

The first step is to fix a joint uniformizer which allows us to compare the v-adic and ∞-adic exponentiations, as we will do in Section 6.3.1. The next section is devoted to recalling the definition of Goss zeta functions and its twist by a character. Then we will state the main theorem and the proof is given in Section 6.5.

6.2 Notation

In this chapter, we will consider ∞-adic and v-adic zeta functions, thus we will slightly alter the notation of previous chapters. From now on, we fix two different places ∞ and v.

- The ring of functions regular away from ∞ (resp. v) is denoted by A^∞ (resp. A^v). The group of nonzero fractional ideals of A^∞ is denoted by $\mathcal{I}^\infty$. Denote by K_∞ (resp. K_v) the completion of K at ∞ (resp. v). Let $\mathcal{O}_\infty$ (resp. $\mathcal{O}_v$) be the ring of integers in K_∞ (resp. K_v), and denote by $k_\infty := \mathcal{O}_\infty/\mathfrak{m}_\infty$ (resp. $k_v := \mathcal{O}_v/\mathfrak{m}_v$). We define a sign function $\operatorname{sgn}_\infty : K_\infty^* \to k_\infty^*$ (resp. $\operatorname{sgn}_v : K_v^* \to k_v^*$). An element a of K_∞^* (resp. K_v^*) is said to be *∞-positive* or *positive at* ∞ (resp. *v-positive* or *positive at* v) if and only if $\operatorname{sgn}_\infty(a) = 1$ (resp. $\operatorname{sgn}_v(a) = 1$). We say an element of K is ∞-positive or v-positive if its image under the canonical inclusion into K_∞ or K_v is so. In particular, an element of K^* can be positive at both ∞ and v, or in short, *doubly-positive*.

- Let d_∞ be the degree of ∞ and d_v be the degree of v. Denote by h the class number of K. Then by [NX02, Proposition 1.2.5], the class number of A^∞ (resp. A^v) is hd_∞ (resp. hd_v) and the narrow class number is $hd_\infty(q^{d_\infty} - 1)/(q - 1)$ (resp. $hd_v(q^{d_v} - 1)/(q - 1)$).

- Let S be a finite set of places of K such that $\infty \notin S$. Later we will assume that $v \in S$. The subgroup of $\mathcal{I}^\infty$ consisting of fractional ideals prime to all the places in S is denoted by $\mathcal{I}^{\infty,S}$. The subgroup of $\mathcal{I}^{\infty,S}$ consisting of principal fractional ideals is denoted by $\mathcal{P}^{\infty,S}$. For a positive integer d, we define $\mathcal{P}^{\infty,S,(d)}$ to be the subgroup of $\mathcal{P}^{\infty,S}$, consisting of all principal ideals whose order at ∞ is a multiple of d. Note that for an ideal (α) in $\mathcal{P}^{\infty,S}$, we have by definition that the order of α at any place in S is 0.

- The subgroup of $\mathcal{P}^{\infty,S}$ generated by ∞-positively generated principal ideals is denoted by $\mathcal{P}^{\infty,S}_{+_\infty}$. Its intersection with $\mathcal{P}^{\infty,S,(d)}$ is denoted by $\mathcal{P}^{\infty,S,(d)}_{+_\infty}$.

- We define the group of doubly-positively generated principal ideals, denoted by $\mathcal{P}^{\infty,S}_{+_\infty,+_v}$, to be the group of principal ideals in $\mathcal{I}^{\infty,S}$ which have doubly-positive generators.

- We denote by $\mathcal{J}$ a subgroup of $\mathcal{I}^{\infty,S}$ of finite index. Some possible $\mathcal{J}$'s can be $\mathcal{P}^{\infty,S}$, $\mathcal{P}^{\infty,S}_{+\infty}$ and $\mathcal{P}^{\infty,S}_{+\infty,+v}$ defined above.
- Let S' be a finite set of places of K such that $v \notin S$. Then we can define verbatimly the groups of ideals $\mathcal{I}^{v,S'}$, $\mathcal{P}^{v,S'}$, $\mathcal{P}^{v,S',(d)}$, $\mathcal{P}^{v,S'}_{+v}$, and $\mathcal{P}^{v,S',(d)}_{+v}$.

6.3 Comparison of the Exponentiations

6.3.1 Joint Uniformizer

Recall that as we have seen in Section 2.3.1, the ∞-adic (resp. v-adic) exponentiation depends on the choice of the uniformizer π_∞ (resp. the uniformizers π_∞ and π_v). In order to make the exponentiations 'comparable', our first aim should be to find suitable uniformizers.

Firstly we want to find a divisor of K satisfying the following properties:

(i) it is principal;

(ii) its support contains only v and ∞;

(iii) it is the divisor of a doubly-positive element in K^*.

The existence of such a divisor satisfying these properties is as follows. Let D be a divisor defined as:

$$D = d' \cdot v - d'' \cdot \infty, \ \text{ with } d' := \frac{d_\infty}{\gcd(d_v, d_\infty)}, \ d'' := \frac{d_v}{\gcd(d_v, d_\infty)}.$$

Clearly the divisor D is of degree 0. But it is not necessarily principal. The following is an example.

Example 6.3.1. We choose the curve $\mathcal{C}$ to be $y^2 = x^3 - x - 1$ over $\mathbb{F}_5$, and the places $\infty := (x^2+3x+3, y+x-1)$ and $v := (x^4+3x^3+3x^2+x-1, y+3x^3+x^2+x-1)$. The degree of the place ∞ is 2 and the degree of v is 4, but the divisor $v-2\infty$ is not principal. In fact by computation, we know that in this case, the principal divisor of shape $n \cdot v - 2n \cdot \infty$ with smallest positive n is $8v - 16\infty$ and $8v - 16\infty = (f)$ with f given as follows

$$(xy + x + 2)^{-8} \cdot (x + 4)^8 \cdot (x^4 + 3x^3 + 3x^2 + x + 4)^8 \cdot ((x^3 + 2x^2 + 3x + 1)y + x^6 + 2x^5 + x^4 + 3x^3 + x^2 + 1)^{-4} \cdot (x^2 + 2)^4 \cdot ((x^2 + x + 3)y + 2x^4 + 4x^3 + 2x^2)^{-1}.$$

Although D is not necessarily principal, we always have that $h{\cdot}D$ must be principal, hence satisfies both (i) and (ii). To satisfy (iii), we need to turn to the narrow class groups, i.e., we consider instead $h\frac{q^{d_v}-1}{q-1}\frac{q^{d_\infty}-1}{q-1}\cdot D$, which has support $\{v,\infty\}$ and is the divisor of some doubly-positive element in K^*. Hence there exists a factor m of $h\frac{q^{d_v}-1}{q-1}\frac{q^{d_\infty}-1}{q-1}$ which is minimal such that $m \cdot D$ satisfies the above properties. Let α be in K^* such that $\operatorname{div}(\alpha) = mD$ and α is positive at both places. Define $l := \operatorname{lcm}(d_v, d_\infty)$. Fix a 1-unit lm-th root $\alpha_* \in K^{\mathrm{alg}}$ of α, then we define:

$$\begin{aligned} \pi_{\infty,*} &:= \alpha_*^{-1}, & \pi_{v,*} &:= \alpha_*; \\ \pi_\infty &:= \pi_{\infty,*}^{d_\infty}, & \pi_v &:= \pi_{v,*}^{d_v}. \end{aligned}$$

Observe that by construction π_∞ (resp. π_v) has valuation 1 at ∞ (resp. v) for any embedding $K^{\mathrm{alg}} \hookrightarrow K_\infty^{\mathrm{alg}}$ (resp. $K^{\mathrm{alg}} \hookrightarrow K_v^{\mathrm{alg}}$).

Remark 6.3.2. By definition, α_*, $\pi_{\infty,*}$ and $\pi_{v,*}$ are all doubly-positive.

Remark 6.3.3. Note that α_* may not lie in K, but only in a finite field extension. Thus it is possible that π_∞ and π_v are not in K. However, we always have that certain powers of π_∞ and π_v lie in K, namely $\pi_\infty^{lm/d_\infty} \in K$ and $\pi_v^{lm/d_v} \in K$. Hence in this case, we can compare the v-adic zeta functions and ∞-adic zeta functions when restricted to some $c\mathbb{Z}$ for c being lm/d_∞ or lm/d_v. We will see more details later.

To have a clearer idea of all the elements defined above, we can look at the following diagram of fields:

$$\begin{tikzcd}
K'_\infty(\pi_{\infty,*}) \arrow[dr, dash] \arrow[dd, dash] & & K'_v(\pi_{v,*}) \arrow[dl, dash] \arrow[dd, dash] \\
& K'(\alpha_*) \arrow[dd, dash] & \\
K'_\infty := K_\infty(\pi_{\infty,*}^{1/l_p m_p}) \arrow[dr, dash] \arrow[dd, dash] & & K'_v := K_v(\pi_{v,*}^{1/l_p m_p}) \arrow[dl, dash] \arrow[dd, dash] \\
& K' := K(\alpha_*^{1/l_p m_p}) \arrow[dd, dash] & \\
K_\infty \arrow[dr, dash] & & K_v \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

where l_p (resp. m_p) is defined to be the p-power part of l (resp. m). And we "connect" the fields on the right hand side and those on the left hand side via the fields in the middle, where on the top row the correspondence is given by $\alpha_* \mapsto \pi_{\infty,*}^{-1}$, $\alpha_* \mapsto \pi_{v,*}$. In this diagram, the lower extensions are purely inseparable, and the upper layer is separable and tamely ramified.

Recall that S is a finite set of places of K such that $v \in S$ and $\infty \notin S$, and we define S' to be $(S\backslash\{v\}) \cup \{\infty\}$. Then we have the following isomorphisms:

$$\begin{tikzcd}
\mathcal{I}^{v,S'} \arrow[r, "\cong"] \arrow[d, dotted] & \bigoplus\limits_{w \notin S' \cup \{v\}} \mathbb{Z} \arrow[d, "="] \\
\mathcal{I}^{\infty,S} \arrow[r, "\cong"] & \bigoplus\limits_{w \notin S \cup \{\infty\}} \mathbb{Z}.
\end{tikzcd}$$

This induces an isomorphism between $\mathcal{I}^{\infty,S}$ and $\mathcal{I}^{v,S'}$, denoted by ϕ. We will show that π_∞ and π_v give a description of this isomorphism.

Before proceeding, we first consider the restriction of ϕ to the following subgroups of $\mathcal{I}$:

$$\mathcal{P}^{\infty,S,(md'')} = \{(a) \in \mathcal{I}^{\infty,S} \mid v_\infty(a) \in md''\mathbb{Z}\};$$
$$\mathcal{P}^{v,S',(md')} = \{(b) \in \mathcal{I}^{v,S'} \mid v_v(b) \in md'\mathbb{Z}\}.$$

Lemma 6.3.4. *The subgroups $\mathcal{P}^{\infty,S,(md'')}$ and $\mathcal{P}^{v,S',(md')}$ are isomorphic under the restriction of ϕ (when by abuse of the notation, this map is also denoted by ϕ):*

$$\begin{tikzcd}
\mathcal{P}^{\infty,S,(md'')} \arrow[r] & \mathcal{P}^{v,S',(md')} \\
(a) \arrow[r, mapsto, "\phi"] & (a \cdot \pi_\infty^{-v_\infty(a)}) \\
(b \cdot \pi_v^{-v_v(b)}) & (b). \arrow[l, mapsto, "\phi'"']
\end{tikzcd}$$

Note that one should keep in mind that by the definition of the π_∞ and π_v, we have

$$\pi_\infty^{-md''} = \pi_v^{md'} = \alpha \in K^*.$$

Proof. It is quite straightforward to show that ϕ is well-defined: firstly, it is clear that this map is independent of the choice of the generator. For any element in $\mathcal{P}^{\infty,S,(md'')}$, say (a), define $a' := a \cdot \pi_\infty^{-v_\infty(a)}$. Note that $a' \in K^*$ since $v_\infty(a)$ is by definition a multiple of md''. Now we show that (a') lies in $\mathcal{P}^{v,S',(md')}$ by computing the valuations of a' at v and ∞. Observe that $v_v(\pi_\infty) = v_v(\alpha_*^{-d_\infty}) = -\frac{d_v}{d_\infty}$. Hence we have

$$\begin{aligned} v_\infty(a') &= v_\infty(a \cdot \pi_\infty^{-v_\infty(a)}) = v_\infty(a) - v_\infty(a) \cdot v_\infty(\pi_\infty) = 0; \\ v_v(a') &= v_v(a \cdot \pi_\infty^{-v_\infty(a)}) = v_v(a) - v_\infty(a) \cdot v_v(\pi_\infty) \\ &= \frac{d_\infty \cdot v_\infty(a)}{d_v} \in md'\mathbb{Z}, \end{aligned} \tag{6.2}$$

since $v_\infty(a) \in md''\mathbb{Z}$ and $d_\infty d'' = d_v d'$. Clearly, this ϕ is a homomorphism.

For any element in $\mathcal{P}^{v,S',(md')}$, say (b), the order of b at v is divisible by md'. We define $b' := b \cdot \pi_v^{-v_v(b)}$. Same as above, we can show that (b') lies in $\mathcal{P}^{\infty,S,(md'')}$ and that ϕ' is a homomorphism.

The fact that they are inverse to each other follows directly from the fact that $\pi_{\infty,*} = \pi_{v,*}^{-1}$.

The claim that the ϕ is the restriction of the isomorphism $\mathcal{I}^{\infty,S} \to \mathcal{I}^{v,S'}$ is shown by checking the divisor maps:

$$\begin{aligned} \mathrm{div}_{A^v}(\phi((a))) &= \mathrm{div}_{A^v}(a \cdot \pi_\infty^{-v_\infty(a)}) \\ &= \sum_{w \neq v} v_w(a \cdot \pi_\infty^{-v_\infty(a)}) \cdot w \\ &= \sum_{w \notin S \cup \{\infty\}} v_w(a \cdot \pi_\infty^{-v_\infty(a)}) \cdot w + v_\infty(a \cdot \pi_\infty^{-v_\infty(a)}) \cdot \infty \\ &= \sum_{w \notin S \cup \{\infty\}} v_w(a) \cdot w + (v_\infty(a) - v_\infty(a) \cdot v_\infty(\pi_\infty)) \cdot \infty \\ &= \sum_{w \notin S \cup \{\infty\}} v_w(a) \cdot w = \mathrm{div}_{A^\infty}(a). \end{aligned}$$

□

Lemma 6.3.5. *The following holds:*

(a) For any $\mathfrak{a} \in \mathcal{I}^{\infty,S}$, we have $\deg_\infty(\mathfrak{a}) = \deg_v(\phi(\mathfrak{a}))$.

(b) When restricted to $\mathcal{P}^{\infty,S,(md'')}$, ϕ preserves the signs at both ∞ and v, i.e., for some a in A^∞ such that $(a) \in \mathcal{P}^{\infty,S,(md'')}$, there exists some $b \in A^v$ such that $(b) = \phi((a))$, and $\mathrm{sgn}_v(b) = \mathrm{sgn}_v(a)$, $\mathrm{sgn}_\infty(b) = \mathrm{sgn}_\infty(a)$.

Proof. For (a), it suffices to consider the principal ideals, hence the statement follows directly from (6.2). For (b), the b in the statement can be chosen to be as in Lemma 6.3.4. □

We define the following important subgroups of $\mathcal{P}^{\infty,S}$ and $\mathcal{P}^{v,S'}$:

$$\mathcal{P}^{\infty,S}_{+_\infty,+_v} := \{(a) \in \mathcal{P}^{\infty,S,(md'')}_{+_\infty} \mid \operatorname{sgn}_\infty(a) = \operatorname{sgn}_v(a) = 1\};$$
$$\mathcal{P}^{v,S'}_{+_v,+_\infty} := \{(b) \in \mathcal{P}^{v,S',(md')}_{+_v} \mid \operatorname{sgn}_v(b) = \operatorname{sgn}_\infty(b) = 1\}.$$

By Lemma 6.3.5 (b), they are isomorphic under ϕ and ϕ' . Note that we omit the degree constraints in the notation since m, d'' and d' are uniquely determined by the places v and ∞. Both subgroups are of finite index in $\mathcal{J}^\infty$ and $\mathcal{J}^v$ respectively.

Moreover, let $\mathscr{J}$ be a subgroup of $\mathcal{P}^{\infty,S}_{+_\infty,+_v}$. We define

$$K_{\mathscr{J}} := \{\alpha \in K^* | \operatorname{sgn}_\infty(\alpha) = 1, (\alpha) \in \mathscr{J}\},$$

and for any fractional ideal $\mathfrak{a}$ of A^∞, we define

$$\mathfrak{a}_{\mathscr{J}} := \mathfrak{a} \cap K_{\mathscr{J}}.$$

6.3.2 Comparison of Exponentiations

Thanks to the π_∞, $\pi_{\infty,*}$, π_v and $\pi_{v,*}$ defined above, we can define the corresponding ∞- and v-adic exponentiations following Section 2.3.1.

For an integer n, we define the ∞-adic exponentiation of a nonzero fractional ideal $\mathfrak{a}$ as

$$\mathfrak{a}^n_\infty := \langle\mathfrak{a}\rangle^n_\infty \cdot \pi_{\infty,*}^{-n\deg_\infty(\mathfrak{a})}.$$

where $\langle\cdot\rangle_\infty$ sends any $\mathfrak{a}$ to $\langle\mathfrak{a}\rangle_\infty := (b \cdot \pi_\infty^{-v_\infty(b)})^{\frac{1}{h(q^{d_\infty}-1)}} \in \mathfrak{U}^1$ with b an ∞-positive generator of $\mathfrak{a}^{h(q^{d_\infty}-1)}$ such that it is ∞-positive. We define the v-adic exponentiation of $\mathfrak{a}$ as

$$\mathfrak{a}^n_{\infty,v} := \langle\sigma(\mathfrak{a}^1_\infty)\rangle^n_{\infty,v} \cdot \omega(\sigma(\mathfrak{a}^1_\infty))^n,$$

where $\langle\cdot\rangle_{\infty,v}$ sends $\sigma(\mathfrak{a}^1_\infty)$ to $\langle\sigma(\mathfrak{a}^1_\infty)\rangle_{\infty,v} := (b \cdot \pi_v^{-v_v(b)})^{\frac{1}{h(q^{d_\infty}-1)(q^{d_v}-1)}} \in \mathfrak{U}^1$ where b is a generator of $\sigma(\mathfrak{a}^1_\infty)^{h(q^{d_\infty}-1)(q^{d_v}-1)}$ such that it is positive at ∞ and v. We can give an explicit description of $\langle\sigma(\mathfrak{a}^1_\infty)\rangle_{\infty,v}$ as follows: for $\mathfrak{a}$ in $\mathcal{J}^{v,S'}$, let b be a doubly positive generator of $\mathfrak{a}^{h(q^{d_\infty}-1)(q^{d_v}-1)}$, then

$$\langle\sigma(\mathfrak{a}^1_\infty)\rangle_{\infty,v} = (b \cdot \pi_\infty^{-v_\infty(b)})^{\frac{1}{h(q^{d_\infty}-1)(q^{d_v}-1)}} \cdot \pi_{v,*}^{\deg_\infty(\mathfrak{a})},$$

where we take the 1-unit root. By definition, the sign part ω is a character of finite order.

Lemma 6.3.6. *We have the following*

$$\langle\phi(\mathfrak{a})\rangle_v = \langle\sigma(\mathfrak{a}^1_\infty)\rangle_{\infty,v}.$$

Proof. Let b be a doubly-positive generator of $\mathfrak{a}^{h(q^{d_\infty}-1)(q^{d_v}-1)}$. Then $\deg_w(b) = h(q^{d_\infty}-1)(q^{d_v}-1)\deg_w(\mathfrak{a})$ for $w \in \{v, \infty\}$. We have

$$\begin{aligned}\langle \phi(\mathfrak{a})\rangle_v &= \left(b \cdot \pi_{\infty,*}^{n\deg_\infty(b)} \cdot \pi_{v,*}^{\deg_v(\phi(b))}\right)^{\frac{1}{h(q^{d_\infty}-1)(q^{d_v}-1)}} \\ &= \left(b \cdot \pi_{\infty,*}^{\deg_\infty(\mathfrak{a})h(q^{d_\infty}-1)(q^{d_v}-1)}\right)^{\frac{1}{h(q^{d_\infty}-1)(q^{d_v}-1)}} \cdot \pi_{v,*}^{\deg_\infty(\mathfrak{a})} \\ &= \langle \sigma(\mathfrak{a}_\infty^1)\rangle_{\infty,v}.\end{aligned}$$

□

Combining the above lemma with Lemma 6.3.5 (b), we have

Lemma 6.3.7. *For any $\mathfrak{a}$ in $\mathcal{I}^{\infty,S}$, we have*

$$\phi(\mathfrak{a})_v^n \cdot \pi_{v,*}^{n\deg_\infty(\mathfrak{a})} = \mathfrak{a}_{\infty,v}^n \omega(\sigma(\mathfrak{a}_\infty^1))^{-n}.$$

6.4 Goss Zeta Functions Twisted by a Character

Recall that we have seen Goss zeta functions in Chapter 2, as well as partial Goss zeta functions in Chapter 4. In this section, we would like to introduce partial Goss zeta function twisted by characters.

Note that we have defined π_∞ and π_v in Section 6.3.1 which may not be in K. Nevertheless we can consider the corresponding ∞- and v-adic exponentiations. To be more precise, the so-called ∞- or v-adic integral exponentiations of a fractional ideal may not lie in K but in a finite field extension of K. Hence the following definitions may not agree with the original definitions by Goss, but there is a close relation between them.

Definition 6.4.1. Let $\mathfrak{J}$ be a subgroup of $\mathcal{I}^{\infty,S}$ of finite index, χ be a character which factors through $\mathcal{I}^{\infty,S}/\mathfrak{J}$. Let $\mathfrak{a}$ be a representative of any equivalent class of $\mathcal{I}^{\infty,S}/\mathfrak{J}$ such that $\mathfrak{a}$ is an ideal of A^∞. We can define the partial ∞-adic zeta function twisted by χ resp. the partial v-adic zeta function twisted by χ as:

$$\zeta_{A^\infty}^S(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi) = \chi(\mathfrak{a})^n \mathfrak{a}_\infty^n \sum_{d\geq 0} T^d \left(\sum_{\substack{\mathfrak{b}\in\mathfrak{J}\cap[\mathfrak{a}]^{-1}, \mathfrak{b}\subset A^\infty \\ \deg_\infty(\mathfrak{b})=d-\deg_\infty(\mathfrak{a})}} \mathfrak{b}_\infty^n \right);$$

$$\zeta_{A^\infty}^{S,(v)}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi) = \chi(\mathfrak{a})^n \mathfrak{a}_{\infty,v}^n \sum_{d\geq 0} T^d \left(\sum_{\substack{\mathfrak{b}\in\mathfrak{J}\cap[\mathfrak{a}]^{-1}, \mathfrak{b}\subset A^\infty \\ \deg_\infty(\mathfrak{b})=d-\deg_\infty(\mathfrak{a})}} \mathfrak{b}_{\infty,v}^n \right).$$

Remark 6.4.2. Here are some remarks on the indices of the zeta functions.

(1) The index S in $\zeta^S_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi)$ or $\zeta^{S,(v)}_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi)$ means that we consider the ideals which are prime to all the places contained in S. Note that in the definition of ∞-adic zeta functions the set S can be empty but in the definition of v-adic zeta functions the place v must lie in S;

(2) the index (v) in $\zeta^{S,(v)}_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi)$ means that we apply the v-adic exponentiation to the ideals;

(3) the index A^∞ in $\zeta^S_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi)$ or $\zeta^{S,(v)}_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi)$ refers to the open curve we work with in Definition 6.4.1;

(4) the index ∞ of $\mathfrak{a}^n_\infty$ is to remind us that we define the exponentiation of ideal $\mathfrak{a}$ with respect to the particularly chosen π_∞ and $\pi_{\infty,*}$ in Section 6.3.1;

(5) the index ∞, v of $\mathfrak{a}^n_{\infty,v}$ is to remind us that we define the exponentiation of ideal $\mathfrak{a}$ by first defining the ∞-adic exponentiation $\cdot^m_\infty$ as above and then refining it with respect to the place v and $\pi_{v,*}$ as in Section 6.3.1.

Remark 6.4.3. The definition of the partial zeta functions are independent of the choice of the representative $\mathfrak{a}$. Given two different representatives of the same equivalent class, say $\mathfrak{a}$ and $\mathfrak{a}'$, then there exists some $\tilde{\mathfrak{a}} \in \mathfrak{J}$ such that $\mathfrak{a} = \mathfrak{a}' \cdot \tilde{\mathfrak{a}}$. Then $\deg_\infty(\mathfrak{a}) = \deg_\infty(\mathfrak{a}') + \deg_\infty(\tilde{\mathfrak{a}})$. Now let us compare each term in the definition. Since χ factors through $\mathfrak{J}$, we have $\chi(\mathfrak{a}) = \chi(\mathfrak{a}')$. By the multiplicativity of ∞-adic exponentiations, $\mathfrak{a}^n_\infty = \mathfrak{a}'^n_\infty \cdot \tilde{\mathfrak{a}}_\infty$. And the two sets $\{\mathfrak{b} \in \mathfrak{J} \cap [\mathfrak{a}]^{-1} \mid \deg_\infty(\mathfrak{b}) = d - \deg_\infty(\mathfrak{a})\}$ and $\{\mathfrak{b}' \in \mathfrak{J} \cap [\mathfrak{a}']^{-1} \mid \deg_\infty(\mathfrak{b}') = d - \deg_\infty(\mathfrak{a}')\}$ coincide by sending each $\mathfrak{b}$ in the first set to $\mathfrak{b}' := \mathfrak{b} \cdot \tilde{\mathfrak{a}}^{-1}$ in the latter one. Thus $\zeta^S_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi) = \zeta^S_{A^\infty}(-n, T, \mathfrak{a}' \pmod{\mathfrak{J}}, \chi)$. The same applies to partial v-adic zeta functions.

We introduce some variations of the ∞-adic and v-adic Goss zeta functions.

Definition 6.4.4. Use the notation as above, we can define the following Goss zeta functions.

(1) If the character χ is trivial, we call for abbreviation the partial ∞-adic and v-adic zeta function, i.e.,

$$\zeta^S_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}) := \zeta^S_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, 1),$$
$$\zeta^{S,(v)}_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}) := \zeta^{S,(v)}_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, 1).$$

(2) We define the global ∞-adic and v-adic zeta functions twisted by a character as:

$$\zeta^S_{A^\infty}(-n,T,\chi) := \sum_{[\mathfrak{a}]\in\mathcal{I}^{\infty,S}/\mathfrak{J}} \zeta^S_{A^\infty}(-n,T,\mathfrak{a} \pmod{\mathfrak{J}},\chi),$$
$$\zeta^{S,(v)}_{A^\infty}(-n,T,\chi) := \sum_{[\mathfrak{a}]\in\mathcal{I}^{\infty,S}/\mathfrak{J}} \zeta^{S,(v)}_{A^\infty}(-n,T,\mathfrak{a} \pmod{\mathfrak{J}},\chi).$$

(3) The ∞-adic and v-adic global Goss zeta functions are defined as follows:

$$\zeta^S_{A^\infty}(-n,T) := \zeta^S_{A^\infty}(-n,T,1);$$
$$\zeta^{S,(v)}_{A^\infty}(-n,T) := \zeta^{S,(v)}_{A^\infty}(-n,T,1).$$

Remark 6.4.5. Since χ is chosen such that it factors through $\mathcal{I}^{\infty,S}/\mathfrak{J}$, we have the following

$$\zeta^S_{A^\infty}(-n,T,\chi) = \sum_{[\mathfrak{a}]\in\mathcal{I}^{\infty,S}/\mathfrak{J}} \chi(\mathfrak{a})^n \zeta^S_{A^\infty}(-n,T,\mathfrak{a} \pmod{\mathfrak{J}}),$$
$$\zeta^{S,(v)}_{A^\infty}(-n,T,\chi) = \sum_{[\mathfrak{a}]\in\mathcal{I}^{\infty,S}/\mathfrak{J}} \chi(\mathfrak{a})^n \zeta^S_{A^\infty}(-n,T,\mathfrak{a} \pmod{\mathfrak{J}}).$$

Remark 6.4.6. Equivalently, we can define the global Goss zeta functions as the sum of the partial ones:

$$\zeta^S_{A^\infty}(-n,T) := \sum_{[\mathfrak{a}]\in\mathcal{I}^{\infty,S}/\mathfrak{J}} \zeta^S_{A^\infty}(-n,T,\mathfrak{a} \pmod{\mathfrak{J}});$$
$$\zeta^{S,(v)}_{A^\infty}(-n,T) := \sum_{[\mathfrak{a}]\in\mathcal{I}^{\infty,S}/\mathfrak{J}} \zeta^{S,(v)}_{A^\infty}(-n,T,\mathfrak{a} \pmod{\mathfrak{J}}).$$

The following diagram describes the relations between the above variations of ∞-adic zeta functions:

$$\begin{tikzcd}
 & \zeta^S_{A^\infty}(-n,T,\mathfrak{a} \pmod{\mathfrak{J}},\chi) \arrow[dl, "\chi=1"'] \arrow[dr, "\sum_{[\mathfrak{a}]\in\mathcal{I}^{\infty,S}/\mathfrak{J}}"] & \\
\zeta^S_{A^\infty}(-n,T,\mathfrak{a} \pmod{\mathfrak{J}}) \arrow[dr, "\sum_{[\mathfrak{a}]\in\mathcal{I}^{\infty,S}/\mathfrak{J}}"'] & & \zeta^S_{A^\infty}(-n,T,\chi) \arrow[dl, "\chi=1"] \\
 & \zeta^S_{A^\infty}(-n,T) &
\end{tikzcd}$$

and we have a similar diagram for the v-adic zeta functions.

For interpolating purpose, we introduce also the z functions as follows.

$$z^S_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi) := \zeta^S_{A^\infty}(-n, T \cdot \pi^n_{\infty,*}, \mathfrak{a} \pmod{\mathfrak{J}}, \chi);$$
$$z^{S,(v)}_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi) := \zeta^{S,(v)}_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi).$$

And we can also define the global ∞-adic and v-adic z functions in a similar manner. It is easy to see that the z functions interpolate by Lemma 2.3.2 and Lemma 2.3.9.

Lemma 6.4.7. *Given m and n in $\mathbb{Z}_p$ such that $m \equiv n \pmod{p^k}$, we have*

$$z^S_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi) \equiv z^S_{A^\infty}(-m, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi) \pmod{\pi^{p^k}_\infty}.$$

Given m and n in $\mathbb{Z}_p$ such that $m \equiv n \pmod{p^k(q^{d_v f} - 1)}$, for any ideal $\mathfrak{a}$ we have

$$z^{S,(v)}_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi) \equiv z^{S,(v)}_{A^\infty}(-m, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi) \pmod{\pi^{p^k}_v}.$$

6.5 The Main Result

We hope to establish the comparison between v-adic Goss zeta functions and ∞-adic Goss zeta functions. Recall that we assume S to be a finite set of places of C such that $v \in S$ and $\infty \notin S$, and define S' to be $(S\backslash\{v\}) \cup \{\infty\}$. Throughout this section, we will assume that

$$\mathfrak{J} = \mathcal{P}^S_{+\infty,+v}, \qquad \mathfrak{J}' = \mathcal{P}^{S'}_{+v,+\infty}.$$

Recall that we have an isomorphism ϕ from $\mathcal{I}^{\infty,S}$ to $\mathcal{I}^{v,S'}$ and $\phi(\mathfrak{J}) = \mathfrak{J}'$. In Section 6.3.1 we had a detailed description of this map.

At the end of last section, we defined the z functions. Besides the interpolating property, the introduction of the z functions is also motivated by the following example.

Example 6.5.1. Let us look at the zeta functions with respect to the trivial class and twisted by the trivial character, i.e., $\zeta^{S,(v)}_{A^\infty}(-n, T, 1 \pmod{\mathfrak{J}})$ and $\zeta^{S'}_{A^v}(-n, T, 1 \pmod{\mathfrak{J}'})$. Recall that we define $K_{\mathfrak{J}} = \{\alpha \in K^* \mid \mathrm{sgn}_\infty(\alpha) = 1, (\alpha) \in$

$\mathfrak{J}\}$ and $K_{\mathfrak{J}'} = \{\alpha \in K^* \mid \operatorname{sgn}_v(\alpha) = 1,\, (\alpha) \in \mathfrak{J}'\}$. Then by definition we have:

$$\begin{aligned}
\zeta^{S'}_{A^v}(-n, T, 1 \pmod{\mathfrak{J}'}) &= \sum_{d\geq 0} T^d \Big(\sum_{\substack{b \in K_{\mathfrak{J}'} \\ \deg_v(b)=d}} b^n \Big) \\
&= \sum_{d\geq 0} T^d \Big(\sum_{\substack{a \in K_{\mathfrak{J}} \\ \deg_\infty(a)=d}} \phi(a)^n \operatorname{sgn}_v(\phi(a))^{-n} \Big) \\
&= \sum_{d\geq 0} T^d \Big(\sum_{\substack{a \in K_{\mathfrak{J}} \\ \deg_\infty(a)=d}} a^n \cdot \pi_\infty^{-nv_\infty(a)} \operatorname{sgn}_v(a)^{-n} \Big) \\
&= \sum_{d\geq 0} T^{dml} \Big(\sum_{\substack{a \in K_{\mathfrak{J}} \\ v_\infty(a)=-dmd''}} a^n \cdot \pi_\infty^{ndmd''} \operatorname{sgn}_v(a)^{-n} \Big) \\
&= \sum_{d\geq 0} (T \cdot \pi^n_{\infty,*})^{dml} \Big(\sum_{\substack{a \in K_{\mathfrak{J}} \\ v_\infty(a)=-dmd''}} a^n \operatorname{sgn}_v(a)^{-n} \Big); \\
\zeta^{S,(v)}_{A^\infty}(-n, T, 1 \pmod{\mathfrak{J}}) &= \sum_{d\geq 0} T^d \Big(\sum_{\substack{a \in K_{\mathfrak{J}} \\ \deg_\infty(a)=d}} a^n \Big) \\
&= \sum_{d\geq 0} T^{dml} \Big(\sum_{a \in K_{\mathfrak{J}}, v_\infty(a)=-dmd''} a^n \Big).
\end{aligned}$$

From the above computations it is evident that the ζ functions only differ by a 'twist' of roots of uniformizers. Note that by our choice of uniformizers, $\pi^{-1}_{\infty,*} = \pi_{v,*}$. Hence if we turn to the z functions then we have:

$$z^{S'}_{A^v}(-n, T, 1 \pmod{\mathfrak{J}'}) = z^{S,(v)}_{A^\infty}(-n, T, 1 \pmod{\mathfrak{J}}, \operatorname{sgn}_v^{-1}).$$

the relation between the partial twisted z functions can be stated as follows:

Theorem 6.5.2. *Let (χ, χ') be any pair of characters such that the diagram*

$$\begin{tikzcd}
\mathfrak{I}^{\infty,S} \arrow[r, "\chi"] \arrow[d, "\phi"'] & K^{\mathrm{alg}} \\
\mathfrak{I}^{v,S'} \arrow[ur, "\chi'"'] &
\end{tikzcd} \tag{6.3}$$

commutes. Let $\tilde{\omega} : \mathfrak{I}^{\infty,S} \to \mathbb{F}_q^{\mathrm{alg}}$ be the character of finite order sending any $\mathfrak{a}$ to $\omega(\sigma(\mathfrak{a}^1_\infty))$ with ω as in the definition of v-adic exponentiation of an ideal. Then we have:

$$z^{S}_{A^v}(-n, T, \varphi(\mathfrak{a}) \pmod{\mathfrak{J}'}, \chi') = z^{S',(v)}_{A^\infty}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi\tilde{\omega}^{-1})$$

for any $\mathfrak{a} \in \mathfrak{I}^{\infty,S}$.

Proof. We have the following

$$\zeta_{A^v}^{S'}(-n, T, \mathfrak{a}' \pmod{\mathfrak{J}'}, \chi') = \sum_{d\geq 0} T^d(\sum_{\substack{\mathfrak{b}'\in[\mathfrak{a}'], \mathfrak{b}'\subset A^v \\ \deg_v(\mathfrak{b}')=d}} (\mathfrak{b}')_v^n \cdot \chi'(\mathfrak{b}')^n)$$

$$= \sum_{d\geq 0} T^d(\sum_{\substack{\mathfrak{b}'\in\mathfrak{J}'\cap(\mathfrak{a}')^{-1}, \mathfrak{b}'\subset A^v \\ \deg_v(\mathfrak{b}')=d-\deg_v(\mathfrak{a}')}} (\mathfrak{b}')_v^n(\mathfrak{a}')_v^n\chi'(\mathfrak{b}'\mathfrak{a}')^n)$$

$$= \sum_{d\geq 0} T^d(\mathfrak{a}')_v^n\chi'(\mathfrak{a}')^n(\sum_{\substack{\mathfrak{b}'\in\mathfrak{J}'\cap(\mathfrak{a}')^{-1}, \mathfrak{b}'\subset A^v \\ \deg_v(\mathfrak{b}')=d-\deg_v(\mathfrak{a}')}} (\mathfrak{b}')_v^n\chi'(\mathfrak{b}')^n)$$

$$= \sum_{d\geq 0} T^d(\phi(\mathfrak{a}))_v^n\chi'(\phi(\mathfrak{a})^n)(\sum_{\substack{\mathfrak{b}\in\mathfrak{J}\cap\mathfrak{a}^{-1}, \mathfrak{b}\subset A^\infty \\ \deg_v(\phi(\mathfrak{b}))=d-\deg_v(\phi(\mathfrak{a}))}} (\phi(\mathfrak{b}))_v^n\chi'(\phi(\mathfrak{b}))^n)$$

$$= \sum_{d\geq 0} T^d\mathfrak{a}_{\infty,v}^n\tilde{\omega}(\mathfrak{a})^{-n}\pi_\infty^{-v_\infty(\mathfrak{a})}\chi(\mathfrak{a})^n(\sum_{\substack{\mathfrak{b}\in\mathfrak{J}\cap\mathfrak{a}^{-1}, \mathfrak{b}\subset A^\infty \\ \deg_\infty(\mathfrak{b})=d-\deg_\infty(\mathfrak{a})}} \mathfrak{b}_{\infty,v}^n\tilde{\omega}(\mathfrak{b})^{-n}\pi_\infty^{-v_\infty(\mathfrak{b})\cdot n}\chi(\mathfrak{b})^n)$$

$$= \sum_{d\geq 0} (T\cdot\pi_{\infty,*}^n)^d\mathfrak{a}_{\infty,v}^n\tilde{\omega}(\mathfrak{a})^{-n}\chi(\mathfrak{a})^n(\sum_{\substack{\mathfrak{b}\in\mathfrak{J}\cap\mathfrak{a}^{-1}, \mathfrak{b}\subset A^\infty \\ \deg_\infty(\mathfrak{b})=d-\deg_\infty(\mathfrak{a})}} \mathfrak{b}_{\infty,v}^n\tilde{\omega}(\mathfrak{b})^{-n}\chi(\mathfrak{b})^n);$$

and on the other hand, we also have

$$\zeta_{A^\infty}^{S,(v)}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi\tilde{\omega}^{-1}) = \sum_{d\geq 0} T^d(\sum_{\substack{\mathfrak{b}\in[\mathfrak{a}], \mathfrak{b}\subset A^\infty \\ \deg_\infty(\mathfrak{b})=d}} \mathfrak{b}_{\infty,v}^n \cdot \omega(\mathfrak{b})^{-n}\chi(\mathfrak{b})^n)$$

$$= \sum_{d\geq 0} T^d(\sum_{\substack{\mathfrak{b}\in\mathfrak{J}\cap\mathfrak{a}^{-1}, \mathfrak{b}\subset A^\infty \\ \deg_\infty(\mathfrak{b})=d-\deg_\infty(\mathfrak{a})}} \mathfrak{b}_{\infty,v}^n\mathfrak{a}_{\infty,v}^n \cdot \tilde{\omega}(\mathfrak{b})^{-n}\tilde{\omega}(\mathfrak{a})^{-n}\chi(\mathfrak{b}\mathfrak{a})^n)$$

$$= \sum_{d\geq 0} T^d\mathfrak{a}_{\infty,v}^n\tilde{\omega}(\mathfrak{a})^{-n}\chi(\mathfrak{a})^n(\sum_{\substack{\mathfrak{b}\in\mathfrak{J}\cap\mathfrak{a}^{-1}, \mathfrak{b}\subset A^\infty \\ \deg_\infty(\mathfrak{b})=d-\deg_\infty(\mathfrak{a})}} \mathfrak{b}_{\infty,v}^n\tilde{\omega}(\mathfrak{b})^{-n}\chi(\mathfrak{b})^n).$$

Thus by the definition of the z functions, we have:

$$\begin{aligned} z_{A^v}^{S'}(-n, T, \mathfrak{a}' \pmod{\mathfrak{J}'}, \chi') =& \zeta_{A^v}^{S'}(-n, T\cdot\pi_{v,*}^n, \mathfrak{a}' \pmod{\mathfrak{J}'}, \chi') \\ =& \zeta_{A^\infty}^{S,(v)}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi\tilde{\omega}^{-1}) \\ =& z_{A^\infty}^{S,(v)}(-n, T, \mathfrak{a} \pmod{\mathfrak{J}}, \chi\tilde{\omega}^{-1}). \end{aligned}$$

□

6.6 Examples

In this section, we present several examples of zeta functions and explicit computations of them.

Example 6.6.1. Take $\mathcal{C}$ to be the projective line over $\mathbb{F}_q$ for any q a prime power, the places ∞ and v to be $(1/t)$ and (t) respectively, and let S be $\{v\}$, then $S' = \{\infty\}$. Then both places are $\mathbb{F}_q$-rational, and the rings A^∞ and A^v are:

$$A^\infty = \mathbb{F}_q[t],\ A^v = \mathbb{F}_q[1/t],$$

both of which have strict class number 1. We choose the sign functions as:

$$\begin{aligned} \mathrm{sgn}_\infty : A^\infty \backslash \{0\} &\longrightarrow \mathbb{F}_q^\times \\ f(t) &\longmapsto \text{ the leading coefficient of } f; \\ \mathrm{sgn}_v : A^v \backslash \{0\} &\longrightarrow \mathbb{F}_q^\times \\ g(1/t) &\longmapsto \text{ the leading coefficient of } g. \end{aligned}$$

Note that in this case, the value field $\mathbb{V}$ is the same as K, thus the embedding σ is trivial and $\tilde{\omega}$ sends any (f) to $\mathrm{sgn}_v(f)$ with f an ∞-positive generator. Then α can be chosen as $1/t$, with $\mathrm{div}_K(\alpha) = 1 \cdot v - 1 \cdot \infty$, and the uniformizers are then $\pi_\infty = 1/t$, $\pi_v = t$. Note that in this case, the uniformizers π_∞ and π_v lie indeed in K, hence we have the right definitions of ∞- and v-adic Goss zeta functions. The isomorphism from $\mathcal{P}^{\infty,S,(1)} = \mathcal{P}^{\infty,S}$ to $\mathcal{P}^{v,S',(1)} = \mathcal{P}^{v,S'}$ sends (f) to $(f/t^{\deg f})$. Hence the doubly positively-generated principal ideal groups $\mathcal{P}^{\infty,S}_{+\infty,+v} = \mathcal{J}$ or $\mathcal{P}^{v,S'}_{+v,+\infty} = \mathcal{J}'$ have index $(q-1)$ in the corresponding fractional ideal groups. Thus the partial Goss zeta functions are:

$$\begin{aligned} \zeta^{S,(v)}_{A^\infty}(-n, T, 1 \pmod{\mathcal{J}}, \tilde{\omega}^{-1}) &= \sum_{d \geq 0} T^d \Big(\sum_{f \in \mathbb{F}_q[t],\, f \text{monic},\, \deg(f) = d} f^n \cdot \mathrm{sgn}_v(f)^{-n} \Big) \\ &= \sum_{d \geq 0} T^d \Big(\sum_{f \in \mathbb{F}_q[t],\, f(0)=1,\, \deg(f) = d} f^n \Big); \\ \zeta^{S'}_{A^v}(-n, T, 1 \pmod{\mathcal{J}'}) &= \sum_{d \geq 0} T^d \Big(\sum_{f \in \mathbb{F}_q[t],\, f(0)=1,\, \deg(f) = d} f^n t^{-dn} \Big) \\ &= \sum_{d \geq 0} (T \cdot \pi_v^{-n})^d \Big(\sum_{f \in \mathbb{F}_q[t],\, f(0)=1,\, \deg(f) = d} f^n \Big). \end{aligned}$$

Thus we have

$$z^{S,(v)}_{A^\infty}(-n, T, 1 \pmod{\mathcal{J}}, \tilde{\omega}^{-1}) = z^{S'}_{A^v}(-n, T, 1 \pmod{\mathcal{J}'}).$$

And the relation of the global ∞-adic zeta function and v-adic zeta function is

$$z^{S,(v)}_{A^\infty}(-n, T, \tilde{\omega}^{-1}) = z^{S'}_{A^v}(-n, T).$$

If the zeta function $z^{S'}_{A^v}$ is twisted by a character χ' which factors through $\mathcal{J}'$, then let χ be product of $\tilde{\omega}^{-1}$ and the composition of

$$\mathcal{I}^{\infty,S} \xrightarrow{\phi} \mathcal{I}^{v,S'} \xrightarrow{\chi'} K^{\mathrm{alg}},$$

then
$$z_{A^\infty}^{S,(v)}(-n,T,\chi) = z_{A^v}^{S'}(-n,T,\chi').$$

Example 6.6.2. Take $\mathcal{C}$ to be the projective line over $\mathbb{F}_2$, the places ∞ and v to be $(1/t)$ and (t^2+t+1), respectively, and $S := \{v\}$. Then we have $d_\infty = 1$, $d_v = 2$. The rings of functions A^∞ and A^v are:

$$\begin{aligned} A^\infty &= \mathbb{F}_2[t]; \\ A^v &= \mathbb{F}_2[\frac{1}{t^2+t+1}, \frac{t}{t^2+t+1}] = \mathbb{F}_2[x,y]/(y^2+xy+x^2+1). \end{aligned}$$

We choose sign functions as:

$$\begin{aligned} \mathrm{sgn}_\infty : \qquad A^\infty\backslash\{0\} &\longrightarrow \mathbb{F}_2^* = \{1\} \\ f &\mapsto \text{the leading coefficient of } f; \\ \mathrm{sgn}_v : \qquad A^v\backslash\{0\} &\longrightarrow \mathbb{F}_4^* = \{1, t, 1+t\} \\ f/(t^2+t+1)^n &\mapsto f \pmod{t^2+t+1}, \end{aligned}$$

for some integer n such that f is not divisible by t^2+t+1. Same as the above example, the value field $\mathbb{V}$ in this case is the same as K, thus the embedding σ is trivial and $\tilde{\omega}$ sends any (f) to $\mathrm{sgn}_v(f)$ with f an ∞-positive generator. Then we can choose α to be t^2+t+1, thus $\mathrm{div}(\alpha) = v - 2\cdot\infty$, where $d' = 1$ and $d'' = 2$. Then the uniformizer $\pi_{v,*}$ is a square root of α and $\pi_{\infty,*} = \pi_{v,*}^{-1}$. Let S be $\{v\}$, then $S' = \{\infty\}$.

Therefore we can write down the groups of ideals explicitly:

$$\begin{aligned} \mathcal{P}^{\infty,S} &= \{(f) | f \in \mathbb{F}_2[t], t^2+t+1 \nmid f\} = \mathcal{P}_{+\infty}^{\infty,S}; \\ \mathcal{P}^{\infty,S,(2)} &= \{(f) | f \in \mathbb{F}_2[t], t^2+t+1 \nmid f, 2 \mid \deg f\} = \mathcal{P}_{+\infty}^{\infty,S,(2)}; \\ \mathcal{P}^{v,S'} &= \{(\frac{f}{(t^2+t+1)^n}) | f \in \mathbb{F}_2[t], t^2+t+1 \nmid f, \deg f \le 2n\} = \mathcal{P}^{v,S',(1)}; \\ \mathcal{P}_{+v}^{v,S'} &= \{(\frac{f}{(t^2+t+1)^n}) | f \in \mathbb{F}_2[t], f \equiv 1 \pmod{t^2+t+1}, \deg f = 2n\} \\ &= \mathcal{P}_{+v}^{v,S',(1)}. \end{aligned}$$

And the isomorphism between $\mathcal{P}^{\infty,S,(2)}$ and $\mathcal{P}^{v,S',(1)}$ is given by:

$$\begin{tikzcd} \mathcal{P}^{\infty,S,(2)} \arrow[r] & \mathcal{P}^{v,S',(1)} & . \\ (f) \arrow[r, mapsto, "\phi"] & \left(\frac{f}{(t^2+t+1)^{\deg f/2}}\right) & \end{tikzcd}$$

Hence the doubly positively-generated principal ideal groups are:

$$\begin{aligned}\mathcal{P}^{\infty,S}_{+_\infty,+_v} &= \{(f) \mid f \in \mathbb{F}_2[t], f \equiv 1 \pmod{t^2+t+1}, 2|\deg f\};\\ \mathcal{P}^{v,S'}_{+_v,+_\infty} &= \{\left(\frac{f}{(t^2+t+1)^{\deg f/2}}\right) \mid f \in \mathbb{F}_2[t], f \equiv 1 \pmod{t^2+t+1}, 2|\deg f\},\end{aligned}$$

both of which are of index 6 in $\mathcal{I}^{\infty,S}$ and $\mathcal{I}^{v,S'}$, respectively. Let $\mathcal{J}$ be $\mathcal{P}^{v,\infty}_{+_v,+_\infty}$.

The partial Goss zeta functions are computed as below:

$$\zeta^{S,(v)}_{A^\infty}(-n,T,1 \pmod{\mathcal{J}}, \tilde{\omega}^{-1}) = \sum_{d\geq 0} T^{2d}\left(\sum_{\substack{f\in\mathbb{F}_2[t],\deg f=2d\\ f\equiv 1 \pmod{t^2+t+1}}} f^n\right);$$

$$\zeta^{S'}_{A^v}(-n,T,1 \pmod{\mathcal{J}}) = \sum_{d\geq 0} T^{2d}\left(\sum_{\substack{f\in\mathbb{F}_2[t],\deg f=2d\\ f\equiv 1 \pmod{t^2+t+1}}} f^n\cdot(t^2+t+1)^{-nd}\right).$$

Plug in the uniformizer $\pi_{v,*}$, then we get that

$$z^{S,(v)}_{A^\infty}(-n,T,1 \pmod{\mathcal{J}}, \tilde{\omega}^{-1}) = z^{S'}_{A^v}(-n,T,1 \pmod{\mathcal{J}}).$$

Example 6.6.3. Take $\mathcal{C}$ to be the projective line over $\mathbb{F}_q$, the places ∞ and v to be $(1/t)$ and (g) with g in $\mathbb{F}_q[t]$, irreducible and of degree a, respectively, and $S := \{v\}$. Then we have $d_\infty = 1$, $d_v = a$. The rings of functions A^∞ and A^v are:

$$\begin{aligned}A^\infty &= \mathbb{F}_q[t];\\ A^v &= \mathbb{F}_q[\frac{1}{g},\frac{t}{g},\cdots,\frac{t^{a-1}}{g}] = \mathbb{F}_q[x_0,\cdots,x_{a-1}]/I,\end{aligned}$$

for some I an ideal in $\mathbb{F}_q[x_0,\cdots,x_{a-1}]$. Note that this I defines the relation of the x_i's, refer to the remark below.

Remark 6.6.4. For instance if we take $\mathcal{C}$ to be the projective line over $\mathbb{F}_2$, and the place v to be (t^3+t+1). Then to write A^v in the form of $\mathbb{F}_2[x_0,x_1,x_2]/I$, we have that $x_0 = 1/g$, $x_1 = t/g$, and $x_2 = t^2/g$, and the relations which generate I are

$$\begin{aligned}x_0^2 + x_0x_1 + x_1x_2 &= 0\\ x_0x_2 + x_1^2 &= 0.\end{aligned}$$

The sign function sgn_∞ is chosen as above, and sgn_v sends f/g^n to the residue of f modulo g, where the integer n is uniquely chosen such that $g \nmid f$. Similarly the embedding σ is trivial and $\tilde{\omega}$ sends any (f) to $\operatorname{sgn}_v(f)$ with f an ∞-positive generator. Choose α to be g, thus $\operatorname{div}(\alpha) = v - a \cdot \infty$, and $d' = 1$ and $d'' = a$. Then we have that $\pi_{v,*}$ is a primitive a-th root of α and $\pi_{\infty,*} = \pi_{v,*}^{-1}$. Let S be $\{v\}$, then $S' = \{\infty\}$. Therefore we have the following groups of ideals:

$$\begin{aligned}
\mathcal{P}^{\infty,S} &= \{(f) \mid f \in \mathbb{F}_q[t], g \nmid f\};\\
\mathcal{P}^{\infty,S}_{+\infty} &= \{(f) \mid f \in \mathbb{F}_q[t], g \nmid f\} = \mathcal{P}^{\infty,S};\\
\mathcal{P}^{\infty,S} &= \{(f) \mid f \in \mathbb{F}_q[t], g \nmid f, a \mid \deg f\};\\
\mathcal{P}^{\infty,S}_{+\infty} &= \{(f) \mid f \in \mathbb{F}_q[t], g \nmid f, a \mid \deg f\} = \mathcal{P}^{\infty,S};\\
\mathcal{P}^{v,S'} &= \{(\frac{f}{g^n}) \mid f \in \mathbb{F}_q[t], g \nmid f, \deg f \le an\} = \mathcal{P}^{v,S'};\\
\mathcal{P}^{v,S'}_{+v} &= \{(\frac{f}{g^n}) \mid f \in \mathbb{F}_q[t], f \equiv 1 \pmod{g}, \deg f = an\} = \mathcal{P}^{v,S'}_{+v}.
\end{aligned}$$

And the isomorphism between $\mathcal{P}^{\infty,S}$ and $\mathcal{P}^{v,S'}$ is given by:

$$\begin{array}{ccc}
\phi : \mathcal{P}^{\infty,S} & \longrightarrow & \mathcal{P}^{v,S'} \quad . \\
 & & \\
(f) & \longmapsto & \left(\frac{f}{g^{\deg f/a}}\right)
\end{array}$$

Hence the doubly positively-generated principal ideal groups are:

$$\begin{aligned}
\mathcal{P}^{\infty,S}_{+\infty,+v} &= \{(f) \mid f \in \mathbb{F}_q[t], f \equiv 1 \pmod{g}, a|\deg f, f \text{ is monic}\};\\
\mathcal{P}^{v,S'}_{+v,+\infty} &= \{(\frac{f}{g^{\deg f/a}}) \mid f \in \mathbb{F}_q[t], f \equiv 1 \pmod{g}, a|\deg f, f \text{ is monic}\},
\end{aligned}$$

both of which are of order $a(q^a-1)$ in $\mathcal{I}^{\infty,S}$ and $\mathcal{I}^{v,S'}$, respectively. Let $\mathfrak{J}$ be $\mathcal{P}^{v,S'}_{+v,+\infty}$.

The partial Goss zeta functions are computed as below:

$$\begin{aligned}
\zeta^{S,(v)}_{A^\infty}(-n, T, 1 \pmod{\mathfrak{J}}) &= \sum_{d \ge 0} T^{ad}\Big(\sum_{\substack{f \in \mathbb{F}_q[t]_{+\infty}, \deg f = ad\\ f \text{ monic}}} f^n\Big);\\
\zeta^{S'}_{A^v}(-n, T, 1 \pmod{\mathfrak{J}}) &= \sum_{d \ge 0} T^{ad}\Big(\sum_{\substack{f \in \mathbb{F}_q[t]_{+v}, \deg f = ad\\ f \equiv 1 \pmod{g}}} f^n \cdot g^{-nd}\Big).
\end{aligned}$$

By easy computation, we can see that

$$z^{S,(v)}_{A^\infty}(-n, T, 1 \pmod{\mathfrak{J}}, \tilde{\omega}^{-1}) = z^{S'}_{A^v}(-n, T, 1 \pmod{\mathfrak{J}})$$

Example 6.6.5. Take $\mathcal{C}$ to be the projective line over $\mathbb{F}_q$, the places ∞ and v to be $v_0 := (g_0)$ and $v_1 := (g_1)$ with g_i irreducible and of degree a_i, for $i = 0, 1$, respectively. Let S be $\{v_1\}$, then $S' = \{v_0\}$. Then we have $d_{v_0} = a_0$, $d_{v_1} = a_1$. For $i \in \{0, 1, \}$, the corresponding ring of functions A^{v_i} is:

$$A^{v_i} = \mathbb{F}_q[\frac{1}{g_i}, \frac{t}{g_i}, \cdots, \frac{t^{a_i-1}}{g_i}] = \mathbb{F}_q[x_0, x_1, \cdots, x_{a_i-1}]/I_i,$$

with sign function $\mathrm{sgn}_i(f/g_i^n) = f \,\mathrm{mod} g_i$ where n is an integer such that $f \in \mathbb{F}_q[t]$ hence f is not divisible by g_i. In this case, $\tilde{\omega}$ sends any (f/g_0^n) to $\mathrm{sgn}_v(f/g_0^n)^{-1}$ with f/g_0^n the ∞-positive generator.

Then h can be chosen as $g_1^{d'} g_0^{-d''}$, with $d' := a_0/\gcd(a_0, a_1)$ and $d'' := a_1/\gcd(a_0, a_1)$, thus $\mathrm{div}(h) = d' \cdot v_1 - d'' \cdot v_0$. Therefore we can write down the groups of ideals explicitly:

$$\begin{aligned}
\mathcal{P}^{v_0,S} &= \{(\frac{f}{g_0^n}) \mid f \in \mathbb{F}_q[t], g_0 \nmid f, g_1 \nmid f, \deg f \leq na_0\};\\
\mathcal{P}^{v_0,S}_{+v_0} &= \{(\frac{f}{g_0^n}) \mid f \in \mathbb{F}_q[t], f \equiv 1 \pmod{g_0}, g_1 \nmid f, \deg f = na_0\};\\
\mathcal{P}^{v_0,S} &= \{(\frac{f}{g_0^n}) \mid f \in \mathbb{F}_q[t], g_0 \nmid f, g_1 \nmid f, \deg f \leq na_0, d'' \mid \deg f\};\\
\mathcal{P}^{v_0,S}_{+v_0} &= \{(\frac{f}{g_0^n}) \mid f \in \mathbb{F}_q[t], f \equiv 1 \pmod{g_0}, g_1 \nmid f, \deg f = na_0, d'' \mid \deg f\};\\
\mathcal{P}^{v_1,S'} &= \{(\frac{f}{g_1^n}) \mid f \in \mathbb{F}_q[t], g_1 \nmid f, g_0 \nmid f, \deg f \leq na_1\};\\
\mathcal{P}^{v_1,S'}_{+v_1} &= \{(\frac{f}{g_1^n}) \mid f \in \mathbb{F}_q[t], f \equiv 1 \pmod{g_1}, g_0 \nmid f, \deg f = na_1\};\\
\mathcal{P}^{v_1,S'} &= \{(\frac{f}{g_1^n}) \mid f \in \mathbb{F}_q[t], g_1 \nmid f, g_0 \nmid f, \deg f \leq na_1, d' \mid \deg f\};\\
\mathcal{P}^{v_1,S'}_{+v_1} &= \{(\frac{f}{g_1^n}) \mid f \in \mathbb{F}_q[t], f \equiv 1 \pmod{g_1}, g_0 \nmid f, \deg f = na_1, d' \mid \deg f\}.
\end{aligned}$$

And the isomorphism between $\mathcal{P}^{v_0,S}$ and $\mathcal{P}^{v_1,S'}$ is given by:

$$\begin{array}{ccc}
\phi : \mathcal{P}^{v_0,S} & \longrightarrow & \mathcal{P}^{v_1,S'} \quad . \\
 & & \\
\left(\frac{f}{g_0^{nd''}}\right) & \longmapsto & \left(\frac{f}{g_1^{nd'}}\right)
\end{array}$$

Hence the doubly-positivelygenerated principal ideal groups are:

$$\begin{aligned}\mathcal{P}^{v_0,S}_{+v_0,+v_1} &= \{(\frac{f}{g_0^n}) \mid f \in \mathbb{F}_q[t], f \equiv 1 \pmod{g_0}, f \equiv 1 \pmod{g_i} \text{ for } i = 0,1, \deg f = na_0,\\ &\quad d'' \mid \deg f\};\\ \mathcal{P}^{v_1,S'}_{+v_1,+v_0} &= \{(\frac{f}{g_1^n}) \mid f \in \mathbb{F}_q[t], f \equiv 1 \pmod{g_1}, f \equiv 1 \pmod{g_i} \text{ for } i = 0,1, \deg f = na_1,\\ &\quad d' \mid \deg f\}.\end{aligned}$$

The partial Goss zeta functions are computed as below:

$$\begin{aligned}\zeta^{S,(v_1)}_{A^{v_0}}(-n, T, 1 \pmod{\mathfrak{J}}) &= \sum_{d \geq 0} T^{d''d}(\sum_{\substack{f \in \mathbb{F}_q[t], \deg f = d''d\\ f \equiv 1 \pmod{g_0}}} f^n \cdot g_0^{-nd});\\ \zeta^{S'}_{A^{v_1}}(-n, T, 1 \pmod{\mathfrak{J}}) &= \sum_{d \geq 0} T^{d'd}(\sum_{\substack{f \in \mathbb{F}_q[t], \deg f = d'd\\ f \equiv 1 \pmod{g_1}}} f^n \cdot g_1^{-nd}).\end{aligned}$$

Thus if we consider the z functions, we have then

$$z^{S,(v_1)}_{A^{v_0}}(-n, T, 1 \pmod{\mathfrak{J}}, \tilde{\omega}^{-1}) = z^{S'}_{A^{v_1}}(-n, T, 1 \pmod{\mathfrak{J}}).$$

References

[And86] Greg W. Anderson. t-motives. *Duke Math. J.*, 53(2):457–502, 1986.

[Böc02] Gebhard Böckle. Global L-functions over function fields. *Math. Ann.*, 323(4):737–795, 2002.

[Böc13] Gebhard Böckle. The distribution of the zeros of the Goss zeta-function for $A = \mathbb{F}_2[x, y]/(y^2 + y + x^3 + x + 1)$. *Math. Z.*, 275(3-4):835–861, 2013.

[BP09] Gebhard Böckle and Richard Pink. *Cohomological theory of crystals over function fields*, volume 9 of *EMS Tracts in Mathematics*. European Mathematical Society (EMS), Zürich, 2009.

[Car35] Leonard Carlitz. On certain functions connected with polynomials in a Galois field. *Duke Math. J.*, 1(2):137–168, 1935.

[DH87] Pierre Deligne and Dale Husemoller. Survey of Drinfel′d modules. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp. Math.*, pages 25–91. Amer. Math. Soc., Providence, RI, 1987.

[Dri74] V. G. Drinfel′d. Elliptic modules. *Mat. Sb. (N.S.)*, 94(136):594–627, 656, 1974.

[DV96] Javier Diaz-Vargas. Riemann hypothesis for $\mathbf{F}_p[T]$. *J. Number Theory*, 59(2):313–318, 1996.

[Gos98] David Goss. *Basic Structures of Function Field Arithmetic.* Number 35 in Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Springer, 1998.

[Gos00] David Goss. A riemann hypothesis for characteristic p l-functions. *Journal of Number Theory*, 82(2):299 – 322, 2000.

[Hay79] David R. Hayes. Explicit class field theory in global function fields. In *Studies in algebra and number theory*, volume 6 of *Adv. in Math. Suppl. Stud.*, pages 173–217. Academic Press, New York-London, 1979.

[Hay91] David R. Hayes. On the reduction of rank-one Drinfel′d modules. *Math. Comp.*, 57(195):339–349, 1991.

[NX02] Harald Niederreiter and Chaoping Xing. *Rational Points on Curves over Finite Fields*. Number 285 in London Mathematical Society Lecture Note Series. Cambridge University Press, 2002.

[RS97] Imke Rust and Ortwin Scheija. A guide to explicit class field theory in global function fields. In E.-U. Gekeler, M. van der Put, M. Reversat, and J. Van Geel, editors, *Drinfeld modules, modular schemes and applications, Proceedings of the workshop held in Alden-Biesen, September 9–14, 1996*, pages 44–65. World Scientific Publishing Co., Inc., River Edge, NJ, 1997.

[She98] Jeffrey T. Sheats. The Riemann hypothesis for the Goss zeta function for $\mathbf{F}_q[T]$. *J. Number Theory*, 71(1):121–157, 1998.

[Tha95] Dinesh S. Thakur. On characteristic p zeta functions. *Compositio Math.*, 99(3):231–247, 1995.

[Tha13] Dinesh S. Thakur. Valuations of v-adic power sums and zero distribution for the Goss v-adic zeta function for $\mathbb{F}_q[t]$. *J. Integer Seq.*, 16(2):Article 13.2.13, 18, 2013.

[Tor94] Fernando Torres. Weierstrass points and double coverings of curves. *manuscripta mathematica*, 83(1):39–58, 1994.

[Wan96] Daqing Wan. On the Riemann hypothesis for the characteristic p zeta function. *J. Number Theory*, 58(1):196–212, 1996.

Index

List of Symbols