International Journal of Pure and Applied Mathematics
Volume 63 No. 3 2010, 341-353

NOTES ON THE RIEMANN HYPOTHESIS IN CHARACTERISTIC p

Víctor Bautista-Ancona[1], Javier Diaz-Vargas[2], Gabriel Villa-Salvador[3] §

[1,3]Departamento de Control Automático
Centro de Investigación y de Estudios Avanzados del I.P.N.
Apartado Postal 14-740, México, D.F., 07000, MÉXICO
[1]e-mail: vbautista@ctrl.cinvestav.mx
[3]e-mail: gvilla@ctrl.cinvestav.mx

[2]Facultad de Matemáticas
Universidad Autónoma de Yucatán
Periférico Norte Tablaje, 13615, Cordemex
Mérida, Yucatán, 97110, MÉXICO
e-mail: jdvargas@uady.mx

Abstract: In this paper we give a full view on the proof of Riemann's Hypothesis for Goss zeta function in characteristic $p > 0$. First, we present the set up of the problem. Then, we analyze the proof of J. Diaz-Vargas for the $q = p$ case. Next, we discuss the main ideas of the unpublished note of B. Poonen for the case $q = 4$ from a combinatorial point of view and how this ideas cannot be extended to more general cases. Finally we give an overview on how J. Sheats proves the general case.

AMS Subject Classification: 11R58, 11G09, 11M41
Key Words: Goss zeta function, Carlitz zeta function, Riemann Hypothesis in positive characteristic

1. Introduction

In the case of functions fields, David Goss extended the definition of Carlitz zeta function in positive characteristic to a much larger domain by defining exponentiation of monic polynomials.

Received: July 9, 2010

§Correspondence author

Let $\mathbb{F}_q$ be the finite field of $q = p^s$ elements, $A := \mathbb{F}_q[T]$ the ring of polynomials in one variable over $\mathbb{F}_q$, $K := \mathbb{F}_q(T)$ the rational function field over $\mathbb{F}_q$, and let v be the T^{-1}-adic valuation over K. The field of Laurent series $K_\infty := \mathbb{F}_q\left(\left(T^{-1}\right)\right)$ is the completion of K with respect to v. Let A_+ denote the set of monic polynomials in A. Let $\mathbb{Z}_p$ be the ring of p-adic integers and let Ω be the completion of an algebraic closure of K_∞.

The Goss exponentiation of monic polynomials is defined as follows: For $n \in A_+$, set $\langle n\rangle := nT^{-\deg n}$. For $z = (x, y) \in \Omega^* \times \mathbb{Z}_p$, we define $n^z := x^{\deg n}\langle n\rangle^y$.

Definition 1. Goss zeta function for $A = \mathbb{F}_q[T]$ is defined by

$$\zeta_A(z) := \sum_{n\in A_+} n^{-z},$$

where z belongs to $\Omega^* \times \mathbb{Z}_p$.

2. The Riemman Hypothesis for $\mathbb{F}_q[T]$

By definition, we have

$$\zeta_A(z) =: \zeta(A, (x, -y)) = 1 + \sum_{d=1}^{\infty}\left(\frac{1}{x}\right)^d \sum_{h=0}^{\infty} C_d(h),$$

where

$$C_d(h) = \sum_{a_1,\ldots,a_d\in\mathbb{F}_q}\left(a_1t + a_2t^2 + \cdots + a_dt^d\right)^h, \quad C_d(0) = 0.$$

Daqing Wan obtained in [6] an asymptotic formula for the coefficient $C_d(h)$ of $\left(\frac{1}{x}\right)^d$ described in terms of the q-digits of y. It follows that the Newton's polygon of $\zeta_A(z)$ lies above the convex hull in the plane $\mathbb{R}^2$ of the lattice $P(y)$ given by the points $(d, w_d(y))$, where $w_d(y)$ is the weight function of y. In particular, this asymptotic formula establishes when the Newton's polygon coincides with this lower bound $P(y)$.

Furthermore, Wan obtained a lower bound $P(y)$ for the Newton's polygon of the entire function $\zeta_A(z)$ in terms of q-digits of y, where the horizontal projection of each side of $P(y)$ has length 1.

When $A = \mathbb{F}_p[T]$ (i.e. $q = p$), the Newton's polygon coincides with its lower bound $P(y)$. In this case, it is also obtained an asymptotic formula for the roots of $\zeta_A(z)$. More specifically, we obtain a particular case of the next theorem.

Theorem 2. (Riemann Hypothesis for $\mathbb{F}_q[T]$) *All zeroes of the function* $\zeta_A(z)$ *are simple and belong to* $\mathbb{F}_q((1/T))$.

3. The Carlitz Problem

Carlitz investigated in [1], among other things, the zeroes of the power series

$$S'_k(N) = \sum_{n\in A_+,\deg n=k} n^N$$

for a positive integer N. He established that $S'_k(N) \neq 0$ if and only if there exists a $(k+1)$-tuple $(r_0, r_1, \dots r_k) \in \mathbb{N}^{k+1}$ whose terms sum N and satisfies the following statements:

Condition 1. No carries occur when their sum is computed in base p.

Condition 2. $r_j > 0$ and $(p^s - 1) \mid r_j$ for $0 \leq j \leq k-1$.

Note that, Condition 2 does not give any restriction to r_k other than $r_k \geq 0$.

In what follows, we use the Condition 1 and Condition 2 names, when we refer to these two statements.

Let $U_{k+1}(N)$ be the set of $(k+1)$-tuples satisfying both conditions above. Carlitz claimed that $S'_k(N) \neq 0$ if and only if $U_{k+1}(N) \neq \emptyset$. Thakur noticed in [5] that Carlitz argument also gives:

Claim 3. *The degree* $r_1 + 2r_2 + \cdots + kr_k$ *of a monomial in* $S'_k(N)$ *attains a unique maximal value when* $(r_k, r_{k-1}, \dots, r_1)$ *is the lexicographic maximum in* $U_{k+1}(N)$.

Claim 3 is the key for the proof of the Riemann Hypothesis for the Goss zeta function. The goal of this paper is to explain the main steps to prove Claim 3.

Diaz-Vargas gave in [2] an elementary proof for the $q = p$ case, based in Carlitz and Wan work.

Next, we discuss the ideas of the Diaz-Vargas proof, but first we have

Definition 4. A $k-$tuple $(r_1, \dots r_k)$ maximizing $r_1 + 2r_2 + \cdots + kr_k$ will be called an *optimal element,* and the element such that $(r_k, r_{k-1}, \dots, r_1)$ is the lexicographically maximal will be called the *greedy element.*

If $y = m_0 + m_1 + \cdots + m_d$ where the set $\{m_j\}$ satisfies Conditions 1 and 2, we select m_j maximizing $dm_0 + (d-1)m_1 + \cdots + m_{d-1}$. Note that

$$\max\left\{dm_0 + (d-1)m_1 + \cdots + m_{d-1}\right\} = dy - \min\left\{m_1 + \cdots + dm_d\right\}.$$

So m_0 plays no role in the computation and is used to adjust the computations of the other terms.

One of the tools used is to explain how to modify the greedy element and how to subtract powers of p to it in order to obtain a new element with less weight. This idea is fundamental in Sheats proof for this case.

In order to study the proof of the general case, we present an alternative proof which is closer to the language used by Carlitz.

4. Another Proof for the $q = p$ Case

Let $(n_1, n_2, \ldots n_m)$ be the greedy element and $(n'_1, n'_2, \ldots n'_m)$ be an optimal element. Suppose that they are different. Let j be the largest index such that $n_j \neq n'_j$. We write n_j and n'_j as sums of $p-$powers:

$$\begin{aligned} n_j &= \sum_{l=0}^{u} a_l p^l = \sum_k p^{i_k}, i_k \geq i_{k+1}, \\ n'_j &= \sum_{l=0}^{u} b_l p^l = \sum_k p^{i'_k}, i'_k \geq i'_{k+1}. \end{aligned}$$

We have $n_j > n'_j$. Let k be the least index such that $r := i_k > i'_k =: i$.

Note that it is possible that there is no power p^i appearing in the expression of n'_j. For instance if $n_j = (p-1)\,p + (p-1)\,p^2$ and $n'_j = (p-1)\,p^2$. In this case, $r = 1$ and there does not exist any such power p^i.

Therefore, we have two cases: when p^i appears and when it does not exist.

In the first case, when p^i appears in the expression of n'_j, we choose the last k such that $r := i_k > i := i'_k$. This implies that for some $t > j$, $p^r \in n'_t$. Define $\{\widetilde{n}_u\}$ by

$$\begin{aligned} \widetilde{n}_u &= n'_u \text{ for } u \neq j, t, \\ \widetilde{n}_j &= n'_j - p^i + p^r, \\ \widetilde{n}_t &= n'_t + p^i - p^r. \end{aligned}$$

Then,

$$\begin{aligned} f\left(\{\widetilde{n}_u\}\right) &= \widetilde{n}_1 + 2\widetilde{n}_2 + \cdots + u\widetilde{n}_u \\ &= n'_1 + \cdots + j\left(n'_j + p^i - p^r\right) \\ &\qquad + \cdots + t\left(n'_t - p^i + p^r\right) + \cdots + un'_u \end{aligned}$$

$$= f\left(\{n'_u\}\right) + (t-j)\left(p^r - p^i\right) > f\left(\{n'_u\}\right).$$

This is a contradiction to the fact that $\{n'_u\}$ is an optimal partition.

Now, let us consider the case when p^i does not appear in the expression of n'_j. Since $\{n_i\}$ and $\{n'_i\}$ are two partitions of the same number, it is not possible that $n'_k \leq n_k$ for $1 \leq k \leq j-1$, so that there exists $t < j$ such that $n'_t > n_t$ and they differ in at least a block of $(p-1)$ summands of $p-$powers. Let $n'_t = n_t + w$ where w is a block of this type. We define the partition $\{\widetilde{n}_u\}$ by:

$$\begin{aligned} \widetilde{n}_u &= n'_u \text{ for } u \neq j, t, \\ \widetilde{n}_j &= n'_j + w, \\ \widetilde{n}_t &= n'_t - w. \end{aligned}$$

Then,

$$\begin{aligned} f\left(\{\widetilde{n}_u\}\right) &= \widetilde{n}_1 + 2\widetilde{n}_2 + \cdots + u\widetilde{n}_u \\ &= n'_1 + \cdots + t\left(n'_t - w\right) + \cdots + j\left(n'_j + w\right) + \cdots + un'_u \\ &= f\left(\{n'_u\}\right) + (j-t)\,w > f\left(\{n'_u\}\right). \end{aligned}$$

This is a contradiction to the fact that $\{n'_u\}$ is an optimal partition. Therefore, the optimal partition and the greedy partition are the same.

At this point, the question is: Is it possible to modify this argument for the general case, that is, for $q = p^s$? The problem is that the (p^s-1)-divisibility and the p-adic carrying are not easily handled when we subtract or add powers of p. This problem was solved by Sheats in a matrix form.

However, before Sheats work, Bjorn Poonen, in an unpublished note, solved the next simplest case, that is, the $q = 4 = 2^2$ case, using combinatorial arguments. Inspired in Diaz-Vargas proof, Poonen shows, how the greedy and the optimal elements can be modified, to obtain a contradiction in case we assume that Theorem 2 does not hold.

5. Poonen's Proof for the $q = 2^2$ Case

Condition 2 in Section 3, was modified by Poonen:

Condition 2'. $r_j > 0$ and $(p^s-1) \mid r_j$ for $0 \leq j \leq k$.

Observe that Condition 2' implies that $(p^s-1) \mid N$ it will play an important role in J. Sheats proof. In fact, we are capable of giving a proof of the general case using this Condition 2' instead of Condition 2.

For each bit in the binary expansion of N where 1 appears, we write below the integer k corresponding to n_k such that the 1 appears in the same bit position. Then, we use two colors and we color alternatively from right to left. In symbols, we will take a color for the positions $u \equiv 1 \bmod 2$ and another color for the positions $u \equiv 0 \bmod 2$. We will distinguish the two colors using different typos (see below). For example, if $p = 2$, $s = 2$, $m = 3$, $N = 2997 = 101110110101_2$ and $n_1 = 100001_2$, $n_2 = 10000100_2$, $n_3 = 101100010000_2$, then we write,

1	**0**	1	**1**	1	**0**	1	**1**	0	**1**	0	**1**
3		3	**3**	2		1	**3**		**2**		**1**

The bottom row (with spaces) is called *the arrangement* corresponding to $\{n_1, n_2, n_3\}$.

Let $\mathcal{A}_{greedy}$ and $\mathcal{A}_{optimal}$ be the arrangements corresponding to the greedy element and an optimal element respectively. We give some important properties about these arrangements.

Now, as one moves from left to right in either $\mathcal{A}_{greedy}$ or $\mathcal{A}_{optimal}$, the first appearances of $m, m-1, \ldots, 1$ are in that order; also, if $i < j$ and i appears to the left to j, then they are in opposite colors and there is no other i to the left of this j and vice versa. One key property is: fix a number i, then there exists $l \geq 0$ such that the first l numbers of the opposite color to the right of i are $i + l, i + l - 1, \ldots, i + 1$ and such that there are no numbers greater than i to the right of i in the same color.

Our goal is prove that $\mathcal{A}_{greedy}$ and $\mathcal{A}_{optimal}$ are equal. We proceed by contradiction.

Assume that $\mathcal{A}_{greedy}$ and $\mathcal{A}_{optimal}$ are different. Reading from left to right, let k be in $\mathcal{A}_{greedy}$ the number at the first position where $\mathcal{A}_{greedy}$ and $\mathcal{A}_{optimal}$ differ. Let k' be the number in $\mathcal{A}_{optimal}$ with the same property. This position is called *the threshold*. Let $K = \max\{k, k'\}$. Each number greater than K appears in the same position in both arrangements.

Hence, proceeding by induction, we may assume that $K = k = m$ and $k > k'$. No number less than k appears to the left of the threshold in $\mathcal{A}_{greedy}$ or $\mathcal{A}_{optimal}$.

Fill the empty spaces with zeros in $\mathcal{A}_{greedy}$ and $\mathcal{A}_{optimal}$, and following Diaz-Vargas argument, we delete everything to the left of the threshold. Set $a_0, a_1, a_2, \ldots$ the resultant list of $\mathcal{A}_{greedy}$ and $b_0, b_1, b_2, \ldots$ the resultant list of $\mathcal{A}_{optimal}$, where $a_0 = k$ and $b_0 = k'$. Now, if $a_i \neq 0$ then $a_i \geq k - i$ and the inequality is strict for $i \geq 2$. If $b_i \neq 0$, then $b_i \leq k$ and the inequality is strict

for all but at most one positive value of i.

The last step is to compute $A := f(\mathcal{P}_{greedy}) - f(\mathcal{P}_{optimal})$ divided by the power of 2 corresponding to the threshold position. This is

$$\begin{aligned} A &= (a_0 - b_0) + \frac{(a_1 - b_1)}{2} + \frac{(a_2 - b_2)}{2^2} + \frac{(a_3 - b_3)}{2^3} + \cdots \\ &\geq \left(k - k'\right) + \left(\frac{(k-1) - k}{2}\right) + \left(\frac{(k-1) - (k-1)}{2^2}\right) + \\ &\quad + \left(\frac{(k-2) - (k-1)}{2^3}\right) + \left(\frac{(k-3) - (k-1)}{2^4}\right) \cdots \\ &\geq 1 - \frac{1}{2} - \frac{0}{4} - \frac{1}{8} - \frac{2}{16} - \cdots > 0. \end{aligned}$$

Thus $f(\mathcal{P}_{greedy}) > f(\mathcal{P}_{optimal})$, a contradiction and this finishes Poonen's proof.

We may ask: is it possible to generalize Poonen's approach to the general case $q = p^s$? We may think that s gives the number of colors and p the number of arrangements to be considered.

6. The $q = p^s$ Case

In this section, we give an overview of Sheats proof of the general case. It is important to emphasize that Sheats works with the two original conditions namely Condition 1 and 2, contrary to Poonen's proof.

Now, we give some elementary definitions in a combinatorial language that allow us to work in an efficient way with the colors and the number of arrangements. If $X = (X_1, \ldots, X_m)$ we define the *weight* of X as $wt(X) = X_1 + 2X_2 + \cdots + mX_m$. Given a finite subset $W \subset \mathbb{N}^m$, a tuple $O \in W$ is an *optimal element* in W if $wt(O) \geq wt(X)$ for all $X \in W$. The *greedy element* of W is that tuple $(G_1, \ldots, G_m) \in W$ such that $(G_m, \ldots, G_1)$ is the maximum in the lexicographical order.

A *composition* of $N \in \mathbb{Z}^+$ is a tuple $X = (X_1, \ldots, X_m)$ of positive integers whose sum is N. We say that an m-tuple X is a *valid composition* of N if, in addition, it satisfies Conditions 1 and 2.

Define $V_m(N)$ to be the set of all valid compositions of N of length m. Note that

$$V_m(N) = \{(X_1, \ldots, X_m) \in U_m(N) : X_m > 0\}.$$

Next statement, related to $V_m(N)$, is very useful to reduce our problem.

Proposition 5. *If the set $V_m(N)$ is not empty, then it contains a unique optimal element. Further, the optimal element is the greedy element of $V_m(N)$.*

Observe that this proposition implies the equivalent statement for $U_m(N)$. In fact, Proposition 5 turns out to be equivalent to Claim 3. We present a sketch of proof of Proposition 5.

Define Ψ to be the set of all pairs (m, N) such that $V_m(N)$ contains an optimal element that is not the greedy element. Therefore, Proposition 5 is equivalently to the statement: $\Psi = \emptyset$.

Next, we rewrite Conditions 1 and 2. For a number N, define $\sigma(N)$ as the shortest non decreasing sequence of powers of p whose terms sum N. Then, $(X_1, \ldots, X_m)$ satisfies Condition 1 if and only if, $\{\sigma(X_1), \ldots, \sigma(X_m)\}$ is a partition, as multiset, of $\sigma(N)$. In this case, define $\deg_p(N)$ to be the exponent of the largest power of p occurring in $\sigma(N)$.

We say that $X = (X_1, \ldots, X_m)$ is τ-*monotonic* if for all $0 \leq h \leq s-1$ the sequence $\tau_h(N)$ is simply the concatenation of the subsequences $\tau_h(X_1)$, ..., $\tau_h(X_m)$. Here, $\tau_i(N)$ is the subsequence of $\sigma(N)$ consisting of all $p^k \in \sigma(N)$ such that $k \equiv i \bmod s$.

We define the map $\Gamma : \mathbb{N} \to \mathbb{N}^s$ as follows. Given $N \in \mathbb{N}$ with p-adic expansion $N = \sum n_j p^j$, define $\Gamma(N) = [u_0, u_1, \ldots, u_{s-1}]^T$ where u_i is the sum of all n_j such that $j \equiv i \bmod s$. Let $\langle \cdot, \cdot \rangle$ be the standard inner product in $\mathbb{R}^s$ and let $\overline{\psi} = \left[1, p, \ldots, p^{s-1}\right]^T$. Then, $X = (X_1, \ldots, X_m)$ satisfies Condition 2 if and only if

$$(p^s - 1) \mid \left\langle \overline{\psi}, \Gamma(N) \right\rangle.$$

Now we define the matrix $\Gamma X = [\Gamma(X_1), \ldots, \Gamma(X_m)]$. By construction, this matrix reflects simultaneously the *colors* and the *number of arrangements*, discussed in the previous section.

Given an $s \times m$ matrix B, denote by $V_m^B(N)$ the set of all valid compositions X of N such that $\Gamma X = B$.

6.1. An "Algorithm" to Find Greedy and Optimal Elements

We observe that the greedy and all optimal elements of $V_m(N)$ are τ-monotonic. Furthermore, we have the following.

Proposition 6. *If the set $V_m^B(N)$ is not empty then it contains a unique*

τ-monotonic composition.

Now, we specify the conditions that B must meet in order that $V_m^B(N) \neq \emptyset$. Let $\overline{e}_0, \ldots, \overline{e}_{s-1}$ denote the standard basis of column vectors for $\mathbb{R}^s$. Define $\overline{\varepsilon}_i = p\overline{e}_{i-1} - \overline{e}_i$ for $0 \leq i \leq s-1$. Define the $s \times s$ matrix E whose columns are $\varepsilon_0, \ldots, \varepsilon_{s-1}$. Define

$$\mathfrak{J} = \{\Gamma(k) : p^s - 1 \mid k\} = (E\mathbb{Z}^s) \cap \left(\mathbb{N}^s \backslash \overline{0}\right).$$

Lemma 7. *Let $B = \left[\overline{b}_1, \ldots, \overline{b}_m\right]$ be an integer matrix. We have $V_m^B(N) \neq \emptyset$ if and only if $\overline{b}_1 + \cdots + \overline{b}_m = \Gamma(N)$, $\overline{b}_1, \ldots, \overline{b}_{m-1} \in \mathfrak{J}$ and $\overline{b}_m > \overline{0}$.*

We use Proposition 6 and Lemma 7 to find greedy and optimal elements. This "algorithm" is illustrated in the following example.

Example 8. Let $p = 5, s = 3, m = 2$, and $N = 91811337$. We construct all valid compositions of 142000430322_5 with two components. In order to satisfy Condition 1, we make a partition $\sigma(N)$ with two components (Σ_1, Σ_2). Let X_i equal to the sum of the elements of Σ_i. To satisfy Condition 2 we choose Σ_1 such that $124 \mid \left\langle \overline{\psi}_0, \Gamma(X_1) \right\rangle$. The only vectors $\overline{v} = [v_0, v_1, v_2]^T \in \mathbb{N}^3 \backslash \{0\}$ such that $\overline{v} < [4, 9, 8]^T$ and such that 124 divides $\left\langle \overline{\psi}_0, \overline{v} \right\rangle = v_0 + 5 \cdot v_1 + 5^2 \cdot v_2$ are $[3, 9, 8]^T$, $[4, 4, 4]^T$ and $[4, 9, 3]^T$. For instance, it is easy to see that $X = (142000300002_5, 130320_5) \in V_2(142000430322_5)$. For this X we have

$$\Gamma X = \begin{pmatrix} 4 & 0 \\ 4 & 5 \\ 4 & 4 \end{pmatrix}$$

and

$$\sigma(142000430322_5) = \{1, 1, 5, 5, 5^2, 5^2, 5^2, 5^4, 5^4, 5^4, 5^5, 5^5, 5^5, 5^5, 5^9, 5^9, 5^{10}, 5^{10}, 5^{10}, 5^{10}, 5^{11}\}.$$

Furthermore,

$$\begin{aligned} \tau_0(142000430322_5) &= \{1, 1, 5^9, 5^9\}, \\ \tau_1(142000430322_5) &= \{5, 5, 5^4, 5^4, 5^4, 5^{10}, 5^{10}, 5^{10}, 5^{10}\}, \\ \tau_2(142000430322_5) &= \{5^2, 5^2, 5^2, 5^5, 5^5, 5^5, 5^5, 5^{11}\}. \end{aligned}$$

We will see if X is τ-monotonic. We have

$$\begin{aligned} \tau_0(142000300002_5) &= \{1, 1, 5^9, 5^9\}, \\ \tau_1(142000300002_5) &= \{5^{10}, 5^{10}, 5^{10}, 5^{10}\}, \\ \tau_2(142000300002_5) &= \{5^5, 5^5, 5^5, 5^{11}\}, \\ \tau_0(130320_5) &= \{0\}, \end{aligned}$$

$$\begin{aligned}\tau_1(130320_5) &= \left\{5,5,5^4,5^4,5^4\right\},\\ \tau_2(130320_5) &= \left\{5^2,5^2,5^2,5^5\right\}.\end{aligned}$$

Therefore X is not τ-monotonic. Now, we will find a τ-monotonic composition $(Z_1,Z_2)\in V_2^B(142000430322_5)$ where $B=\begin{pmatrix}4&0\\4&5\\4&4\end{pmatrix}$. The sequences

$$\begin{aligned}\tau_0(Z_1) &:= \left\{1,1,5^9,5^9\right\},\\ \tau_0(Z_2) &:= \{0\},\\ \tau_1(Z_1) &:= \left\{5,5,5^4,5^4\right\},\\ \tau_1(Z_2) &:= \left\{5^4,5^{10},5^{10},5^{10},5^{10}\right\},\\ \tau_2(Z_1) &:= \left\{5^2,5^2,5^2,5^5\right\},\\ \tau_2(Z_2) &:= \left\{5^5,5^5,5^5,5^{11}\right\}.\end{aligned}$$

are given by τ-monotonicity. It follows that

$$\begin{aligned}Z_1 &:= 1+1+5+5+5^2+5^2+5^2+5^4+5^4+5^5+5^9+5^9\\ &= 2000120322_5,\\ Z_2 &:= 5^4+5^5+5^5+5^5+5^{10}+5^{10}+5^{10}+5^{10}+5^{11}\\ &= 140000310000_5.\end{aligned}$$

We want to see if $V_2^B(142000430322_5)\neq\emptyset$ where $B=\begin{pmatrix}4&0\\4&5\\4&4\end{pmatrix}$. We use Lemma 7. First, it is immediate that the sum of the columns of B equals $\Gamma(N)$. The second condition requires a little more. We have to show that the first column of B is an element of $\mathfrak{J}=(E\mathbb{Z}^s)\cap\left(\mathbb{N}^s\backslash\overline{0}\right)$ where $E=\begin{pmatrix}-1&5&0\\0&-1&5\\5&0&-1\end{pmatrix}$. This is equivalent to find a non-trivial integral solution of the following system

$$\begin{aligned}-z_1+5z_2 &= 4,\\ -z_2+5z_3 &= 4,\\ 5z_1-z_3 &= 4.\end{aligned}$$

The solution is $(1,1,1)$. Therefore $V_3^B(N)\neq\emptyset$. By Proposition 6, $V_3^B(N)$ contains a unique τ-monotonic composition. Now, the greedy and all optimal elements are τ-monotonic. We conclude that $X=(142000300002_5,130320_5)$ is the greedy element and the unique optimal element.

The proof for the elementary case $q=p$ is related to the previous example.

Remember that the problem has been reduced to: If $s = 1$, then $\Psi \neq \emptyset$. The proof consists in fixing m and N so that $V_m(N)$ is not empty. Since $s = 1$, we find a matrix B such that V_m^B is non-empty and $\Gamma G = \Gamma O = B$ where G and O are respectively the greedy and the optimal elements of $V_m(N)$. Therefore, $G = O$ is the τ-monotonic element of $V_m^B(N)$.

6.2. The Proof of the General Case

To prove Proposition 5, we proceed by contradiction. We assume $\Psi \neq \emptyset$. Therefore, there exist m and N such that $V_m(N)$ is not empty and it contains an optimal element which is different from the greedy element. Our goal is to arrive to a contradiction by constructing a composition $Z \in V_m(N)$ such that $wt(Z) > wt(O)$.

To construct Z, we first define an $s \times m$ matrix B and then define Z to be an optimal element among those valid compositions X such that $\Gamma X = B$. The reason for defining B is that, it can be shown that the greedy element and all optimal elements of $V_m(N)$ are the same if $V_m^B(N) \neq \emptyset$. Therefore, it suffices to construct a matrix B, such that $V_m^B(N)$ is not empty.

Since the construction of B is complicated we just outline it.

Proposition 9. *Let $s \geq 2$. If Ψ is not empty there exist $m > 2$, N, and an optimal element $(O_1, \ldots, O_m) \in V_m(N)$ such that,*

(a) $\Gamma(O_j) = E\overline{a}$ *for* $1 \leq j \leq m-1$, *with* $\overline{a} \in \mathbb{R}^s$ *satisfying* $a_0 = 1$.

(b) $\deg_p(O_m) < \deg_p(G_m)$

(c) $O_m = p^k$ *for some* $k \in \mathbb{N}$

(d) $\langle \overline{\psi}, \Gamma(O_m) \rangle = \langle \overline{\psi}, \Gamma(G_m) \rangle$ *yet* $\Gamma(O_m) \neq \Gamma(G_m)$.

Here $G = (G_1, \ldots, G_m)$ is the greedy element for $V_m(N)$.

Proposition 9 gives the tools to prove a variant of Claim 3.

Remark 10. Observe that if we change Condition 2 by Condition 2' used by Poonen, we can prove Claim 3 easily with this variant. In the proof of Proposition 5, Condition 2 was not used, that is, we did not use any restriction for the last component. Therefore, if we assume that $\Psi \neq \emptyset$ then, from Proposition 9 (c), $O_m = p^k$ for some $k \in \mathbb{N}$, which contradicts that $p^s - 1 \mid O_m$. In this way, we obtain Claim 3 in general, from Poonen's point of view.

Now we construct the matrix B. Let $[\theta_{i,j}] = \left[\overline{\theta}_1, \ldots, \overline{\theta}_m\right]$ be the matrix whose columns are the partial sums of the columns of ΓO :

$$\overline{\theta}_j = \sum_{i=1}^{j} \Gamma(O_i), \text{ for } 1 \leq j \leq m.$$

First, we take E^{-1} of the matrix $[\theta_{i,j}]$ to obtain a new matrix:

$$[w_{i,j}] = [\overline{w}_1, \ldots, \overline{w}_m] = E^{-1}[\theta_{i,j}].$$

Let α be given by: there exists an index $\alpha < \beta$ such that: $w_{i,m-1} > m-1$ for $\alpha < i \leq \beta$ and $w_{\alpha,m-1} = m-1$. Here $\beta \equiv \deg_p(O_m) \bmod s$. Next, we modify the rows of $[w_{i,j}]$ with indices between α and β.

Now, we use $[w_{i,j}]$ to define a matrix $[d_{i,j}]$ recursively. First, we define $\overline{d}_m := E^{-1}\Gamma(N)$. The other elements are given by

$$d_{i,m-1} = \begin{cases} w_{i,m-1} & \text{if } 0 \leq i \leq \alpha, \text{ or } \beta < i \leq s-1, \\ \min\{w_{i,m-1} - 1, pd_{i+1,m-1}\} & \text{for } i = \beta, \beta-1, \ldots, \alpha, \end{cases}$$

and for $j = m-2, m-3, \ldots, 1$, define

$$d_{i,j} = \begin{cases} w_{i,j} & \text{if } 0 \leq i \leq \alpha \text{ or } \beta < i \leq s-1, \\ \min\{w_{i,j+1} - 1, pd_{i+1,j}\} & \text{for } i = \beta, \beta-1, \ldots, \alpha. \end{cases}$$

Now, we reverse the first two steps. Set $[\delta_{i,j}] = \left[\overline{\delta}_1, \ldots, \overline{\delta}_m\right] = E[d_{i,j}]$. We define $\overline{b}_1 := \overline{\delta}_1$, $\overline{b}_2 := \overline{\delta}_2 - \overline{\delta}_1$, ..., $\overline{b}_m := \overline{\delta}_m - \overline{\delta}_{m-1}$ to obtain $B = \left[\overline{b}_1, \ldots, \overline{b}_m\right]$. Then the columns of B sum $\Gamma(N)$, this implies that, $V_m^B(N)$ is not empty. Finally we define $Z := (Z_1, \ldots, Z_m)$ to be the $\tau-$monotonic element of $V_m^B(N)$. The last step in Sheats proof is to prove that O is not optimal. This is shown by proving that $wt(Z) > wt(O)$.

For $1 \leq j \leq m$, set $\widetilde{Z}_j := Z_1 + Z_2 + \cdots + Z_j$ and $\widetilde{O}_j := O_1 + O_2 + \cdots + O_j$. It is easy to verify that $wt(Z) = mN - \left(\widetilde{Z}_1 + \cdots + \widetilde{Z}_{m-1}\right)$ and $wt(O) = mN - \left(\widetilde{O}_1 + \cdots + \widetilde{O}_{m-1}\right)$. Therefore

$$wt(Z) - wt(O) = \sum_{j=1}^{m-1} \left(\widetilde{O}_j - \widetilde{Z}_j\right).$$

Note that $\widetilde{Z}_{m-1} = N - Z_m$ and $\widetilde{O}_{m-1} = N - O_m$. It follows that, $\widetilde{O}_{m-1} - \widetilde{Z}_{m-1} = Z_m - p^k$ so that

$$wt(Z) - wt(O) = Z_m - \left(p^k + \sum_{j=1}^{m-2} \left(\widetilde{Z}_j - \widetilde{O}_j\right)\right). \tag{1}$$

Now, since Z is $\tau-$monotonic, we have that $\tau_h(N)$ is the concatenation of

the sequences $\tau_h(Z_1), \ldots, \tau_h(Z_m)$. Since $\widetilde{Z}_j = Z_1 + Z_2 + \cdots + Z_j$, we have that $\tau_h\left(\widetilde{Z}_j\right)$, for $1 \leq j \leq m$, is the concatenation of the first j sequences $\tau_h(Z_1), \ldots, \tau_h(Z_j)$. For $0 \leq h \leq s-1$ and $1 \leq i \leq u_h$ we define $\tau_{h,i}$ to be the $i^{th}-$term of $\tau_h(N)$. Define $\tau_{h,0} := 0$ for each h. Then, $\widetilde{Z}_j = \sum_{h=0}^{s-1} \sum_{i=0}^{\delta_{h,j}} \tau_{h,i}$ and $\widetilde{O}_j = \sum_{h=0}^{s-1} \sum_{i=0}^{\theta_{h,j}} \tau_{h,i}$. We have an upper bound of (1),

$$\sum_{j=1}^{m-2} \left(\widetilde{Z}_j - \widetilde{O}_j\right) \leq p^k + \sum_{h=\alpha}^{\beta-1} \tau_{h,\delta_{h,m-1}}. \tag{2}$$

From (1) and (2) we obtain

$$wt(Z) - wt(O) \geq Z_m - \left(2p^k + \sum_{h=\alpha}^{\beta-1} \tau_{h,\delta_{h,m-1}}\right). \tag{3}$$

Now, we have some lower bounds on Z_m: $\deg(Z_m) > k$ and if $\sum_{h=\alpha}^{\beta-1} \tau_{h,\delta_{h,m-1}}$ is positive, then $\deg_p(Z_m) > \deg_p\left(\sum_{h=\alpha}^{\beta-1} \tau_{h,\delta_{h,m-1}}\right) + 1$.

Finally, we set $Q := p^k + \sum_{h=\alpha}^{\beta-1} \tau_{h,\delta_{h,m-1}}$. From (3), it suffices to show $Z_m > Q + p^k$. Therefore, $wt(Z) > wt(O)$ and the proof of Claim 3 is complete.

References

[1] L. Carlitz, Finite sums and interpolation formulas over $GF[p^n, x]$, *Duke Math. J.*, **15** (1948), 1001-1012.

[2] J. Diaz-Vargas, Riemann Hypothesis for $\mathbb{F}_p[T]$, *J. Number Theory*, **59** (1996), 313-318.

[3] B. Poonen, Notes on a combinatorial problem, *Personal Correspondence with D. Thakur* (1996).

[4] J. Sheats, The Riemann Hypothesis for the Goss zeta function for $\mathbb{F}_q[T]$, *J. Number Theory*, **71** (1998), 121-157.

[5] D. Thakur, Zeta measure associated to $\mathbb{F}_q[t]$, *J. Number Theory*, **35** (1990), 1-17.

[6] D. Wan, On the Riemann Hypothesis for the characteristic p zeta function, *J. Number Theory*, **58** (1996), 196-212.