Canad. Math. Bull. Vol. 65 (1), 2022, pp. 9–29
http://dx.doi.org/10.4153/S0008439521000035

Vanishing of multizeta values over $\mathbb{F}_q[t]$ at negative integers

Shuhui Shi

Abstract. Let $\mathbb{F}_q$ be the finite field of q elements. In this paper, we study the vanishing behavior of multizeta values over $\mathbb{F}_q[t]$ at negative integers. These values are analogs of the classical multizeta values. At negative integers, they are series of products of power sums $S_d(k)$ which are polynomials in t. By studying the t-valuation of $S_d(s)$ for $s < 0$, we show that multizeta values at negative integers vanish only at trivial zeros. The proof is inspired by the idea of Sheats in the proof of a statement of "greedy element" by Carlitz.

1 Introduction

Classical multizeta values (i.e., over $\mathbb{Z}$), also known as "multiple zeta values," are defined as the convergent series

$$\zeta(\mathbf{s}) = \sum_{n_1 > n_2 > \cdots > n_r \geq 1} \frac{1}{n_1^{s_1} n_2^{s_2} \cdots n_r^{s_r}} \quad \in \mathbb{R},$$

where $\mathbf{s} = (s_1, \ldots, s_r) \in \mathbb{Z}_+^r$ with $s_1 > 1$. We call r the *depth* and $\sum_i s_i$ the *weight* of $\zeta(\mathbf{s})$. Here and in the rest of the paper, $\mathbb{Z}_+$ is the set of positive integers and $\mathbb{N} = \mathbb{Z}_+ \cup \{0\}$. Multizeta values of depth 1 are the usual Riemann zeta values. Double zeta values (i.e., $r = 2$) were first considered by Euler in 1776 [Eul75] in the study of $\zeta(3)$. After a long time of oblivion, multizeta values of higher depth were introduced independently by Hoffman [Hof92] and Zagier [Zag94] in 1992. During the last three decades, great attention has been drawn to the study of multizeta values because of their appearance in many different contexts, including the absolute Galois group [Gon01], periods of mixed Tate motives [DG05, Gon05], knot invariants, and calculations of integrals associated to Feynman diagrams in perturbative quantum field theory [BK97]. These various connections with other fields have led to big progresses in the study of classical multizeta values, although some fundamental questions still remain open (see [BGF, Preface]).

Having learned about the rich interconnections in the classical case, Thakur, in 2002, defined two types of multizeta values over function fields [Tha04, Section 5.10], one complex valued (generalizing special values of Artin–Weil zeta functions) and the other with values in Laurent series over finite field (generalizing Carlitz zeta values).

Received by the editors March 29, 2020; revised December 3, 2020.
Published online on Cambridge Core January 18, 2021.
AMS subject classification: **11M32**, **11M38**, 11R58.
Keywords: multizeta values, vanishing at negative integers, trivial zero, power sum, valuation monotonicity, modest element.

The first type was completely evaluated in [Tha04] for $\mathbb{F}_q(t)$ (see [Mas06] for a study in the higher genus case). In this paper, we focus on the second type and stick to the rational function field $\mathbb{F}_q(t)$.

Throughout this paper, p is a prime and $q := p^f$ is a power of p. We say an integer is *q-even* if it is divisible by $q-1$ and *q-odd* otherwise. Let $K := \mathbb{F}_q(t)$ be the rational function field over the finite field $\mathbb{F}_q$, ∞ be the rational place of K with uniformizer $1/t$, and $K_\infty := \mathbb{F}_q((1/t))$ be its completion at ∞. Let $A := \mathbb{F}_q[t]$ be the polynomial ring in t, $A_+ := \{\text{monics in } A\}$, and $A_{d+} := \{\text{monic in } A \text{ of degree } d\}$ for $d \geq 0$. For $d \geq 0$ and $s \in \mathbb{Z}$, we define the power sum

$$S_d(s) := \sum_{a \in A_{d+}} \frac{1}{a^s} \in K. \tag{1.1}$$

Note that $S_d(s) \in A$ if $s < 0$. The *multizeta values* at $\mathbf{s} \in \mathbb{Z}^r$ over $\mathbb{F}_q[t]$ are defined as

$$\zeta(\mathbf{s}) := \sum_{d_1 > \cdots > d_r \geq 0} S_{d_1}(s_1) \cdots S_{d_r}(s_r) \quad \in K_\infty. \tag{1.2}$$

The convergence of $\zeta(\mathbf{s})$ at positive integers, i.e., $\mathbf{s} \in \mathbb{Z}_+^r$, is clear from definition of S_d. At nonpositive integers, it follows from the fact that $S_d(0) = 0$ for $d > 0$ and $S_d(s) = 0$ for $d \gg 0$ if $s < 0$ (see Section 2 for details). At positive integers, the definition above can be restated as

$$\zeta(\mathbf{s}) = \sum_{a_1, a_2, \ldots, a_r} \frac{1}{a_1^{s_1} a_2^{s_2} \cdots a_r^{s_r}} \in K_\infty,$$

where the sum is over all $a_i \in A_{d_i+}$ with $d_1 > d_2 > \cdots > d_r \geq 0$. Following the classical case, we say $\zeta(\mathbf{s})$ is of depth r and weight $\sum_i s_i$. For general introduction of results on function field multizeta values and comparison with the classical case, we refer the reader to the survey papers [Cha14, Tha17]. In this paper, $\zeta(\mathbf{s})$ is used to denote multizeta values in both the classical and function field cases. It should be clear which one we are referring to from the context.

A natural question to ask is when $\zeta(\mathbf{s})$ vanishes. In classical case, $\zeta(\mathbf{s}) > 0$ by definition at positive integers with $s_1 > 1$. Treating s_i's as complex variables, the series defining $\zeta(\mathbf{s})$ is absolutely convergent in the region $\{(s_1, \ldots, s_r) \in \mathbb{C}^r : \mathrm{Re}(s_1 + \cdots + s_j) > j \text{ for } 1 \leq j \leq r\}$ and can be meromorphically continued to $\mathbb{C}^r$ with singular hyperplanes $\{s_1 = 1, s_1 + s_2 \in \{2, 1, 0, -2, -4, -6, \ldots\}, \sum_{i=1}^k s_i \in \mathbb{Z}_{\leq k} \text{ for } 3 \leq k \leq r\}$. In particular, all the negative integer points, except when $r = 2$ or $s_1 + s_2$ odd, lie on these hyperplanes. Moreover, they are points of indeterminacy. See [FKMT17] and the references mentioned in its "Introduction" for several different approaches to define and determine the multizeta values at these points.

In function field case, Thakur [Tha09] showed that $\zeta(\mathbf{s}) \neq 0$ at positive integers. At negative integers, the vanishing of multizeta values of depth 1 is completely understood by Goss [Gos79]. Its vanishing behavior is quite similar to that of the Riemann zeta values although lacking a functional equation. In this paper, we study the vanishing of $\zeta(\mathbf{s})$ at negative integers of higher depth.

Replacing a by $t^d + \sum_{i=1}^d \theta_i t^{d-i}$ in (1.1), we can rewrite $S_d(s)$ as a sum of monomials in t for negative s, whose sum indices are in $\mathbb{N}^{d+1}$ satisfying some restrictions. Denote the set of these indices as $U_d(-s)$. Our main result (restated as Theorem 2.8) gives an explicit description of the t-valuation of $S_d(s)$ in terms of elements in $U_d(-s)$.

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

Theorem 1.1 *Assume $U_d(-s) \neq \emptyset$, then there is a unique monomial in the sum $S_d(s)$ achieving the lowest degree. Moreover, this term corresponds to the element in $U_d(-s)$ whose reverse is lexicographically the largest.*

This result implies monotonicity of the t-valuation of $S_d(s)$ with respect to d, using which we completely solve the vanishing of $\zeta(\mathbf{s})$ at negative integers (stated as Theorem 2.10 later). See Section 2.1 for definition of "trivial zero."

Theorem 1.2 *At negative integers, $\zeta(\boldsymbol{s})$ of depth at least 2 only vanishes at trivial zeros.*

Here is the outline of the paper. In Section 2, we study the behavior of $S_d(s)$ at negative s in detail and discuss how our main result implies Theorem 1.2. Section 3 gives the proof of Theorem 1.1.

2 Main result

In this section, we study the vanishing behavior of multizeta values in detail. We continue to use the notations in the previous section. Our main object of study is $S_d(s)$, the building blocks of multizeta values. The reader will see that the vanishing of $\zeta(\mathbf{s})$ is really a reflection of properties of $S_d(s)$.

2.1 Trivial zeros

Let $s < 0$. We first take a closer look at when $S_d(s)$ vanishes. Writing out the coefficients of a in (1.1), we get

$$\begin{aligned} S_d(s) &= \sum_{\theta_i \in \mathbb{F}_q} (t^d + \theta_1 t^{d-1} + \cdots + \theta_d)^{-s} \\ &= \sum_{\theta_i \in \mathbb{F}_q} \sum_{\substack{m_0+\cdots+m_d=-s \\ m_i \geq 0}} \binom{-s}{m_0, \ldots, m_d} \theta_1^{m_1} \cdots \theta_d^{m_d}\, t^{dm_0+(d-1)m_1+\cdots+m_{d-1}} \\ &= (-1)^d \sum_{\substack{m_0+\cdots+m_d=-s \\ m_0 \geq 0,\ m_i>0 \ q\text{-even for } i>0}} \binom{-s}{m_0, \ldots, m_d} t^{dm_0+(d-1)m_1+\cdots+m_{d-1}} \\ &= (-1)^d \sum_{\substack{\oplus_{i=0}^d m_i=-s \\ m_0 \geq 0,\ m_i>0 \ q\text{-even for } i>0}} \binom{-s}{m_0, \ldots, m_d} t^{dm_0+(d-1)m_1+\cdots+m_{d-1}}, \end{aligned} \tag{2.1}$$

where $\oplus_{i=0}^d m_i$ denotes sum $\sum_{i=0}^d m_i$ with no carry over of digits base p. The third equality comes from exchanging the two sum indices and the fact that $\sum_{\theta \in \mathbb{F}_q} \theta^k = -1$ if k is a positive multiple of $q-1$ and 0 otherwise. The last equality follows from Lucas' theorem.

For $k > 0$ and $d \geq 0$, let

$$U_d(k) := \{(m_0, \ldots, m_d) \in \mathbb{N}^{d+1} : k = \oplus_{i=0}^d m_i \text{ and } m_i > 0 \text{ is } q\text{-even for } 1 \leq i \leq d\}.$$

Let $\mathcal{P}(n)$ be the multiset of p-powers adding up to n with no carry over in base p. More precisely, if $n = \sum_{i=0}^k a_i p^i$ with $0 \leq a_i < p$, $\mathcal{P}(n) := \{\{p^i\}_{a_i} : 0 \leq i \leq k\}$, where

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

$\{m\}_k$ denotes the sequence $m, \dots, m$ with m repeated k times. Then, the condition $k = \bigoplus_{i=0}^{d} m_i$ is equivalent to

$$\mathcal{P}(k) = \bigsqcup_{i=0}^{d} \mathcal{P}(m_i). \tag{2.2}$$

Note that $U_d(-s)$ is the set of sum indices in (2.1). Clearly, $S_d(s)$ vanishes if $U_d(-s) = \emptyset$. In [Car48], Carlitz claimed without proof that the converse also holds. More precisely, he asserted that if $U_d(-s) \neq \emptyset$, the term $t^{dm_0+(d-1)m_1+\cdots+m_{d-1}}$ with $(m_0, \dots, m_d)$ lexicographically largest among sum indices attains the unique maximal degree. Such $(m_0, \dots, m_d)$ is called *greedy*. This claim was not proved until 50 years later. Diaz-Vargas [DV96] gave a proof for the case $q = p$, and a general proof for any q is given by Sheats [She98].

Theorem 2.1 (Carlitz, Diaz-Vargas, Sheats) *For $s < 0$, $S_d(s) \neq 0$ if and only if $U_d(-s) \neq \emptyset$. Moreover, if $U_d(-s) \neq \emptyset$, the summand in $S_d(s)$ corresponding to the greedy element achieves the unique maximal degree.*

Böeckle pointed out that with some results in [She98], one gets a more straightforward criterion when $S_d(s)$ vanishes.

Definition 2.2 For $k \in \mathbb{Z}_+$ with base q expansion $k = a_0 + a_1 q + \cdots + a_n q^n$, let $l(k) = \sum a_i$ be the sum of base q digits of k. Recall that $q = p^f$. Define

$$L_k := \min_{i=0,\dots,f-1} \left\{ \frac{l(kp^i)}{(q-1)} \right\}.$$

We note that since $k \equiv l(k) \bmod q-1$, L_k is an integer if and only if $(q-1)|k$, i.e., k is q-even.

Proposition 2.3 [Böc13, Theorem 1.2(a)] *For s negative, $S_d(s) = 0 \Leftrightarrow d > L_{-s}$.*

For reader's convenience, we provide a proof of the result above. For $d \geq 0$ and $k > 0$, let

$$V_d(k) := \{(m_0, \dots, m_d) \in U_d(k) : m_0 > 0\}.$$

The proposition follows from the following lemma of Sheats. We note that the notations and expression of the lemma are slightly different from those in Sheats' paper, but one can check that they are equivalent.

Lemma 2.4 [She98, Proposition 4.3(a)] $V_d(k) = \emptyset \Leftrightarrow d \geq L_k$.

Proof of Proposition 2.3 By Theorem 2.1, it is enough to show that $U_d(k) = \emptyset$ iff $d > L_k$. We break it up into two cases.

If k is q-even, $U_d(k) = V_d(k) \cup \{(0, m_1, \dots, m_d) \mid (m_1, \dots, m_d) \in V_{d-1}(k)\}$. $U_d(k) = \emptyset$ iff $V_d(k) = V_{d-1}(k) = \emptyset$, i.e., $d - 1 \geq L_k$ by Lemma 2.4. Since L_k is an integer, $d - 1 \geq L_k \Leftrightarrow d > L_k$.

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

If k is q-odd, $U_d(k) = V_d(k)$; thus, $U_d(k) = \emptyset$ iff $d \geq L_k$ by Lemma 2.4. As L_k is not an integer in this case, $d \geq L_k \Leftrightarrow d > L_k$. ∎

Note that in (1.2), the least d appearing in $S_d(s_i)$ is $r - i$. Thus, if $r - i > L_{-s_i}$, all terms in the sum vanish and so does the multizeta value. With this observation, we define

Definition 2.5 Let $r > 1$ and $(s_1, \ldots, s_r) \in \mathbb{Z}_-^r$ such that $\zeta(s_1, \ldots, s_r) = 0$. We call $(s_1, \ldots, s_r)$ a *trivial zero* of ζ if there exists some $1 \leq i \leq r-1$ such that $r - i > L_{-s_i}$. Otherwise, $(s_1, \ldots, s_r)$ is a *nontrivial zero*.

2.2 Existence of nontrivial zero

We now investigate nontrivial zeros of $\zeta(\mathbf{s})$ where $s_i < 0$. The depth 1 case is completely understood by Goss [Gos79].

Theorem 2.6 (Goss, see [Tha04, Section 5.3]) *For s negative, $\zeta(s) = 0$ if and only if s is q-even.*

Note that multizeta values in this case reduce to Carlitz zeta values. The above theorem shows that the behavior of zeros of Carlitz zeta at negative integers is analogous to that of the trivial zeros of the classical Riemann zeta function. However, unlike a direct implication from the functional equation of the Riemann zeta, the vanishing of $\zeta(s)$, without any known functional equations in the function field case, follows from cancellations among monomials.

The proof of the nonvanishing of $\zeta(s)$ at q-odd s [Tha04, Theorem 5.3.2] showed that there is a unique term of least degree, 1, in the polynomial sum of $\zeta(s)$, which could not be canceled. Similarly, the fact that multizeta values at positive integers never vanish [Tha09, Theorem 4] follows from the strict monotonicity in d of the ∞-valuation of $S_d(\mathbf{s})$. We use the same strategy to show that there are no nontrivial zeros in higher depth case.

Definition 2.7 $M = (M_0, \ldots, M_d) \in U_d(k)$ is called *modest* if $(M_d, M_{d-1}, \ldots, M_0)$ is lexicographically the largest, i.e., $M_d \geq m_d$ for all $(m_0, \ldots, m_d) \in U_d(k)$, $M_{d-1} \geq m_{d-1}$ for those $(m_0, \ldots, m_d)$ with $m_d = M_d$, and so on. Such element always exists and is unique if $U_d(k) \neq \emptyset$.

Our main result is the following theorem, which characterizes the term in $S_d(s)$ with least degree. Its proof is given in Section 3.

Theorem 2.8 *Assume $S_d(s) \neq 0$. The term corresponding to the modest element in $U_d(-s)$ attains the unique minimum degree in t among all summands in $S_d(s)$.*

Recall that for $d \leq L_{-s}$, elements in $U_d(-s)$ and summands in (2.1) are in one-to-one correspondence. Take $(m_0, m_1, \ldots, m_d) \in U_d(-s)$, then its corresponding term

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

in $S_d(s)$ has degree $dm_0 + (d-1)m_1 + \cdots + m_{d-1}$. Define $v_d(s) := v_t(S_d(s))$, where v_t is the t-valuation. We have the following corollary.

Corollary 2.9 *Fix $s < 0$, then*

$$v_{\lfloor L_{-s} \rfloor}(s) > v_{\lfloor L_{-s} \rfloor - 1}(s) > \cdots > v_1(s) \geq v_0(s).$$

Proof Since $v_0(s) = v_t(1) = 0$ for all s, the last inequality is obvious. Assume $0 < d \leq L_{-s}$ and let $\mathbf{M} = (M_0, \ldots, M_d)$ be the modest element in $U_d(-s)$, then Theorem 2.8 implies $v_d(s) = dM_0 + (d-1)M_1 + \cdots + M_{d-1}$. Consider $\mathbf{N} = (M_0, \ldots, M_{d-2}, M_{d-1} + M_d)$, then $\mathbf{N} \in U_{d-1}(-s)$ and thus $v_{d-1}(s) \leq (d-1)M_0 + (d-2)M_1 + \cdots + M_{d-2} \leq v_d(s)$, where the second inequality is equality iff $d = 1$ and $M_d = -s$. ∎

With this result, we finish the discussion of the vanishing of multizeta values of higher depth at negative integers.

Theorem 2.10 *For $\mathbf{s} = (s_1, \ldots, s_r)$ with $s_i < 0$ and $r > 1$, $\zeta(\mathbf{s}) = 0$ if and only if $\mathbf{s}$ is a trivial zero.*

Proof It is equivalent to show that $\zeta(\mathbf{s}) \neq 0$ if $\mathbf{s}$ is not a trivial zero. In this case, the sum $\zeta(\mathbf{s}) = \sum_{d_1 > \cdots > d_r \geq 0} S_{d_1}(s_1) \cdots S_{d_r}(s_r)$ is nonempty. In particular, $S_{r-1}(s_1) \cdots S_0(s_r) \neq 0$ and

$$v_t(S_{r-1}(s_1) \cdots S_0(s_r)) = \sum_{i=1}^{r} v_{r-i}(s_i).$$

For any other term $S_{d_1}(s_1) \cdots S_{d_r}(s_r)$ in the sum, $d_i \geq r - i$ for all i and there exist some j such that $d_j > r - j > 0$; thus, by Corollary 2.9,

$$v_t(S_{d_1}(s_1) \cdots S_{d_r}(s_r)) = \sum_{i=1}^{r} v_{d_i}(s_i) > v_t(S_{r-1}(s_1) \cdots S_0(s_r)).$$

By strict triangle inequality, $v_t(\zeta(\mathbf{s})) = v_t(S_{r-1}(s_1) \cdots S_0(s_r)) = \sum_{i=1}^{r} v_{r-i}(s_i)$. In particular, $\zeta(\mathbf{s}) \neq 0$. ∎

Remark 2.11 We note that the same strategy fails in analyzing the vanishing of $\zeta(\mathbf{s})$ at integers of mixed signs. For both place t and ∞, s being positive and negative give opposite monotonicity of the valuation of $S_d(s)$ in d. Hence, there is no unique term with least valuation in general. For example, let $q = 3$, then

$$\begin{aligned} \zeta(-8, 2) &= S_1(-8)S_0(2) + S_2(-8)S_0(2) + S_2(-8)S_1(2) \\ &= (2t^6 + 2t^4 + 2t^2 + 2) + (t^6 + t^4 + t^2) + (1) = 0 \end{aligned}$$

is a "nontrivial zero" in the sense of Definition 2.5. In the sum, $S_1(-8)S_0(2), S_2(-8)S_1(2)$ attain the least valuation at t and $S_1(-8)S_0(2), S_2(-8)S_0(2)$ attain the least valuation at ∞.

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

3 Proof of Theorem 2.8

The proof of Theorem 2.8 is quite complicated and combinatorial. This is because the two conditions on elements of $U_d(-s)$ are with respect to p and q each while p and q are different in general. Major difficulty of the proof arises from how to track these two conditions simultaneously.

3.1 Special case

When $q = p$ is a prime, the problem mentioned above disappears and the theorem can be proved in a way similar to the proof of Theorem 2.1 for $q = p$ case by Diaz-Vargas. Another simple case, without restriction on q, is where s is q-even, which follows directly from the result on greedy element. We first prove these two special cases.

Proof of Theorem 2.8 for special cases. Let $k = -s$ and $\mathbf{M} = (M_0, \dots, M_d) \in U_d(k)$ be the modest element. For $\mathbf{m} = (m_0, \dots, m_d) \in U_d(k)$, define

$$\mathrm{wt}(\mathbf{m}) := dm_0 + (d-1)m_1 + \cdots + m_{d-1}$$

to be its weight, which equals the degree of its corresponding term in $S_d(s)$. For both cases, we need to show $\mathbf{M}$ achieves the unique minimum weight.

(1) $q = p$ is a prime: We show that given any nonmodest element $\mathbf{m}$, one can always adjust it to get another $\mathbf{m'}$ of smaller weight. Let $l > 0$ be the largest index such that $M_l > m_l$. Then, $M_i = m_i$ for $i > l$ by the choice of $\mathbf{M}$. Recall that $\mathcal{P}(n)$ is the multiset of p-powers represented by the base p digits of n. When $q = p$, n is q-even iff $(q-1)|\#\mathcal{P}(n)$. We split the discussion into two cases.

(a) If $\#\mathcal{P}(M_l) \le \#\mathcal{P}(m_l)$, then there exist some $p^e \in \mathcal{P}(m_l)$ and $p^{e'} \in \mathcal{P}(M_l)\backslash\mathcal{P}(m_l)$ such that $p^e < p^{e'}$. By (2.2), $p^{e'} \in \mathcal{P}(m_{l'})$ for some $l' < l$. Let

$$\mathbf{m'} = (m_0, \dots, m_{l'} - p^{e'} + p^e, \dots, m_l - p^e + p^{e'}, \dots, m_d),$$

then it is easy to check that $\mathbf{m'} \in U_d(k)$ and $\mathrm{wt}(\mathbf{m'}) < \mathrm{wt}(\mathbf{m})$.

(b) If $\#\mathcal{P}(M_l) > \#\mathcal{P}(m_l)$, then $\#\mathcal{P}(M_l) - \#\mathcal{P}(m_l) \ge q-1$, since both M_l and m_l are q-even. Note that $\sum_{i=0}^{d} \#\mathcal{P}(M_i) = \sum_{i=0}^{d} \#\mathcal{P}(m_i) = \#\mathcal{P}(k)$; thus, there exists $l' < l$ such that $\#\mathcal{P}(m_{l'}) - \#\mathcal{P}(M_{l'}) \ge q-1$. Write $\mathcal{P}(m_{l'}) = P_1 \sqcup P_2$, where $\#P_1 = q-1$, and this implies $m_{l'} = n_1 \oplus n_2$ with $n_1 q$-even. If $l' > 0$, then $n_2 > 0$ and is also q-even. Consider

$$\mathbf{m'} = (m_0, \dots, m_{l'} - n_1, \dots, m_l + n_1, \dots, m_d),$$

then $\mathbf{m'} \in U_d(k)$ and $\mathrm{wt}(\mathbf{m'}) < \mathrm{wt}(\mathbf{m})$.

(2) s is q-even: Recall that

$$V_d(k) = \{(m_0, \dots, m_d) \in U_d(k) : m_0 > 0\}.$$

In this case, $\mathbf{M} \in U_d(k) \setminus V_d(k)$, since otherwise $(0, M_1, \dots, M_d + M_0)$ is also contained in $U_d(k)$ whose reverse is lexicographically larger. Similar argument shows that $\mathbf{m} \in U_d(k) \setminus V_d(k)$ if $\mathbf{m}$ is of minimum weight. Consider the bijective map

$$\varphi : (0, m_1, \dots, m_d) \mapsto (m_d, \dots, m_1)$$

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

between $U_d(k) \setminus V_d(k)$ and $V_{d-1}(k)$. Note that $k = \sum_i m_i$; thus, for $\mathbf{m} \in U_d(k) \setminus V_d(k)$,

$$\mathrm{wt}(\mathbf{m}) = (d-1)m_1 + \cdots + m_{d-1} = (d-1)k - \mathrm{wt}(\varphi(\mathbf{m})).$$

$\mathrm{wt}(\mathbf{m})$ being minimum indicates that $\varphi(\mathbf{m}) = (m_d, \ldots, m_1)$ achieves the largest weight in $V_{d-1}(k)$. By Theorem 2.1, $\varphi(\mathbf{m})$ has to be the greedy element in $U_{d-1}(k)$. This implies that the reverse of $\mathbf{m}$ is lexicographically the largest in $U_d(k) \setminus V_d(k)$; hence, $\mathbf{m} = \mathbf{M}$. ∎

3.2 General case

Our proof for general case is inspired by Sheats' proof [She98] of Theorem 2.1 on greedy element. We prove by contradiction. Roughly speaking, assuming there exists a tuple not modest in $U_d(-s)$ gives a term of lowest degree in $S_d(s)$, we construct another term with smaller degree.

We fix a prime power $q = p^f$. In this section, $\bar{x}$ denotes a column vector of length f, where x is either an English or Greek letter, with or without subscript. If not mentioning explicitly, its entries are denoted as x_i with $0 \le i < f$, e.g., $\bar{u} = [u_0, u_1, \ldots, u_{f-1}]^t$. Note that the subscripts start from 0. The zero vector is denoted as $\bar{0}$.

3.2.1 Setup and preliminaries

Before the proof, we change to a different notation for easy expression. A d-tuple $(X_1, \ldots, X_d) \in \mathbb{N}^d$ is said to be a *composition* of N if $N = \sum_{i=1}^d X_i$. For $d > 0$ and $N \in \mathbb{Z}_+$, let

$$\begin{aligned} W_d(N) &= \{(X_1, X_2, \ldots, X_d) \in \mathbb{N}^d : (X_d, X_{d-1}, \ldots, X_1) \in U_{d-1}(N)\} \\ &= \{(X_1, X_2, \ldots, X_d) \in \mathbb{N}^d : N = \bigoplus_{i=1}^d X_i, \text{ and } X_i > 0 \text{ is } q\text{-even for } i < d\}. \end{aligned}$$

In this new setup, the modest element in $U_{d-1}(N)$ corresponds to be the lexicographically largest composition in $W_d(N)$, which we again call it modest.

Definition 3.1 Let $\mathbf{X} = (X_1, \ldots, X_d) \in W_d(N)$. Define its *weight*, denoted as $\mathrm{wt}(\mathbf{X})$, by

$$\mathrm{wt}(\mathbf{X}) = X_1 + 2X_2 + \cdots + dX_d.$$

Any composition $\mathbf{X}$ achieving the minimum weight in $W_d(N)$ is called *optimal*.

One can check that Theorem 2.8 is equivalent to the following.

Theorem 3.2 *For $W_d(N) \neq \emptyset$, the modest composition is the only optimal composition.*

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

Remark 3.3 The theorem holds for $d = 1$ trivially, since $W_1(N) = \{(N)\}$ has only one composition. For $d = 2$, $\mathrm{wt}(\mathbf{X}) = 2N - X_1$ for any $\mathbf{X} \in W_2(N)$ and hence the modest composition is the only optimal element.

The following proposition consists of some observations on how to get new modest or optimal compositions from old ones.

Proposition 3.4 *Suppose $W_d(N) \neq \emptyset$. $\boldsymbol{X} = (X_1, \ldots, X_d)$ is the modest composition in $W_d(N)$. Then*

(i) $(X_1, X_2, \ldots, X_{d-1})$ *is the modest composition in* $W_{d-1}(N - X_d)$;
(ii) $(X_2, X_3, \ldots, X_d)$ *is the modest composition in* $W_{d-1}(N - X_1)$;
(iii) *for any* $n \geq 0$, $(p^n X_1, \ldots, p^n X_n)$ *is the modest composition in* $W_d(p^n N)$.

These three statements remain true when replacing "the modest composition" with "an optimal composition".

Proof (i) and (ii) are obvious from definition in each case. To show (iii), we observe that all p-powers in $\mathcal{P}(p^n N)$ are divisible by p^n. Thus, for $(Y_i) \in W_d(p^n N)$, $p^n \mid Y_i$ for all i since $\mathcal{P}(Y_i) \subset \mathcal{P}(p^n N)$. Moreover, $(Y_i) \mapsto (p^{-n} Y_i)$ gives a 1-to-1 correspondence between compositions in $W_d(p^n N)$ and $W_d(N)$. (iii) follows from this observation easily in both cases. ∎

Given base p expansion $n = \sum_{j \geq 0} a_j p^j$, we define $\Gamma(n) \in \mathbb{N}^f$ to be the column vector $[\mu_0, \ldots, \mu_{f-1}]^t$, where

$$\mu_i = \sum_{j \equiv i \bmod f} a_j.$$

Let $\bar{\psi}_0 := [1, p, \ldots, p^{f-1}]^t$, then

$$\langle \bar{\psi}_0, \Gamma(n) \rangle = \mu_0 + \cdots + p^{f-1} \mu_{f-1}$$

is the sum of base q digits of N. In particular, n is q-even iff $(q-1) \mid \langle \bar{\psi}_0, \Gamma(n) \rangle$. Then, $\mathbf{X} \in W_d(N)$ if and only if

(1) $\Gamma(N) = \Gamma(X_1) + \Gamma(X_2) + \cdots + \Gamma(X_d)$,
(2) for $1 \leq i \leq (d-1)$, $(q-1) \mid \langle \bar{\psi}_0, \Gamma(X_i) \rangle \neq 0$.

For a composition $\mathbf{X} = (X_1, \ldots, X_d)$ of N, define $\Gamma(\mathbf{X})$ to be the $f \times d$ matrix with columns $\Gamma(X_1), \ldots, \Gamma(X_d)$.

Example Let $q = 9$ and $N = 131$. In base 3, $N = 11212_3$. Thus, $\Gamma(N) = [5, 2]^t$. For any $\mathbf{X} \in W_2(N)$, $\Gamma(\mathbf{X})$ is one of the two matrices: $\begin{bmatrix} 5 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 3 \\ 2 & 0 \end{bmatrix}$. $(128, 3) = (11202_3, 10_3)$, $(104, 27) = (10212_3, 1000_3) \in W_2(N)$ correspond to the first one, and the rest correspond to the second one.

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

In the example above, we give a partition of compositions in $W_d(N)$ with respect to matrix representation. Given $B \in \mathrm{Mat}_{f\times d}(\mathbb{N})$, define

$$W_d^B(N) := \{\mathbf{X} \in W_d(N) : \Gamma(\mathbf{X}) = B\}.$$

We call B a *valid matrix* of $W_d(N)$ if $W_d^B(N) \neq \emptyset$. Let $B_1, \ldots, B_d$ be columns of B, then B is valid if and only if

(1) $\Gamma(N) = B_1 + \cdots + B_d$,
(2) for $1 \le i \le (d-1)$, $(q-1) \mid \langle \bar{\psi}_0, B_i \rangle \neq 0$.

For $n > 0$, denote $\tau(n)$ the nonincreasing sequence of p-powers in $\mathcal{P}(n)$ and $\tau_k(n)$ be its subsequence consisting of those p^i with $i \equiv k \bmod f$ for $0 \le k < f$.

Example Take $q = 9$ and $N = 131 = 11212_3$. Then,

$$\tau(N) = (3^4, 3^3, 3^2, 3^2, 3^1, 3^0, 3^0),\ \tau_0(N) = (3^4, 3^2, 3^2, 3^0, 3^0),\ \tau_1(N) = (3^3, 3^1).$$

Given $\mathbf{X} \in W_d(N)$, $\tau_k(X_i)$'s give a partition of p-powers in $\tau_k(N)$ for each k. We call $\mathbf{X}$ is *τ-monotonic* if the sequence $\tau_k(N)$ is the concatenation of the subsequences $\tau_k(X_1), \tau_k(X_2), \ldots, \tau_k(X_d)$ for all $0 \le k < f$. Note that there is a unique τ-monotonic composition in $W_d^B(N)$ for each valid B.

Lemma 3.5 *Suppose B is a valid matrix of $W_d(N)$, then the τ-monotonic composition with respect to B is lexicographically the largest and achieves the unique minimum weight in $W_d^B(N)$. In particular, both modest and optimal compositions are τ-monotonic.*

Proof Take $\mathbf{X} = (X_1, \ldots, X_d) \in W_d^B(N)$ which is not τ-monotonic. Then, there exist some k, i, j, m, n such that $i < j, m < n$, with $p^m \in \tau_k(X_i), p^n \in \tau_k(X_j)$. Consider the composition $\mathbf{Y} = (X_1, \ldots, X_i - p^m + p^n, \ldots, X_j - p^n + p^m, \ldots, X_d)$. Then, $\mathbf{Y} \in W_d^B(N)$ since $m \equiv n \equiv k \bmod f$. Clearly, $\mathbf{Y}$ is lexicographically larger than $\mathbf{X}$. Easy computation shows that $\mathrm{wt}(\mathbf{Y}) = \mathrm{wt}(\mathbf{X}) - (j-i)(p^n - p^m) < \mathrm{wt}(\mathbf{X})$. ∎

Define

$$\mathfrak{J} := \{\Gamma(n) : n > 0 \text{ is } q\text{-even}\}.$$

Given $B = [B_1, \ldots, B_d]$ an $f \times d$ matrix with columns B_i, the conditions for B being valid for $W_d(N)$ can be translated as

(1) $\Gamma(N) = B_1 + \cdots + B_d$,
(2) $B_i \in \mathfrak{J}$ for $1 \le i \le (d-1)$.

We follow Sheats' discussion in [She98] to give a characterization of vectors in $\mathfrak{J}$. Let $\bar{e}_0, \ldots, \bar{e}_{f-1}$ be the standard basis of $\mathbb{R}^f$, i.e., $[\bar{e}_0, \ldots, \bar{e}_{f-1}] = I$, the identity matrix. Define matrix $E = [E_0, E_1, \ldots, E_{f-1}]$ with columns

$$E_i := p\bar{e}_{i-1} - \bar{e}_i.$$

Here and from now on, subscripts which should range from 0 to $f-1$ are evaluated modulo f, e.g., $\bar{e}_{-1} = \bar{e}_{f-1}$ and $E_0 = p\bar{e}_{f-1} - \bar{e}_0$. Given vectors $\bar{u}$ and $\bar{v} = E\bar{u}$, we have,

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

for all i,

$$v_i = pu_{i+1} - u_i.$$

Let $R = [\bar{e}_1, \bar{e}_2, \dots, \bar{e}_{f-1}, \bar{e}_0]$ be the permutation matrix such that $R\bar{e}_i = \bar{e}_{i+1}$. Then, $R^f = I$ and $\langle R\bar{u}, R\bar{v}\rangle = \langle \bar{u}, \bar{v}\rangle$ for any $\bar{u}$ and $\bar{v}$. Recall that $\bar{\psi}_0 = [1, p, \dots, p^{f-1}]^t$. Define

$$\bar{\psi}_i := R^i\bar{\psi}_0 = [p^{f-i}, \dots, p^{f-1}, 1, \dots, p^{f-1-i}]^t$$

for $1 \le i < f$. Then,

$$\langle \bar{\psi}_i, E_j\rangle = \begin{cases} q-1 & \text{if } i = j \\ 0 & \text{otherwise,} \end{cases}$$

which implies

$$E^{-1} = (q-1)^{-1}[\bar{\psi}_0, \bar{\psi}_1, \dots, \bar{\psi}_{f-1}]^t.$$

Given two vectors $\bar{u}$ and $\bar{v}$, we denote $\bar{u} \ge \bar{v}$ if $u_i \ge v_i$ for all i, $\bar{u} > \bar{v}$ if $\bar{u} \ge \bar{v}$ and $u_i > v_i$ for some i, and $\bar{u} \gg \bar{v}$ if $u_i > v_i$ for all i.

Lemma 3.6 *Let $\bar{u} = E\bar{a}$ and $\bar{v} = E\bar{b}$, then*

(i) *$\bar{u} > \bar{v} \Rightarrow \bar{a} \gg \bar{b}$. In particular, if $\bar{u} > \bar{0}$, then $\bar{a} \gg \bar{0}$.*
(ii) *Let $\bar{1} = [1, \dots, 1]^t$. If $\bar{0} < \bar{u} < (p-1)\bar{1}$, then $\bar{0} \ll \bar{a} \ll \bar{1}$.*

Proof $\bar{a} - \bar{b} = E^{-1}(\bar{u} - \bar{v})$. Since all components of E^{-1} are positive, $\bar{u} - \bar{v} > \bar{0}$ implies $\bar{a} - \bar{b} \gg \bar{0}$. This proves (i). (ii) is a direct application of (i) as $[p-1, \dots, p-1]^t = E[1, \dots, 1]^t$. ∎

Take a positive integer n. Let $E\bar{\alpha} = \Gamma(n)$, then we have, for each i,

$$\alpha_i = (q-1)^{-1}\langle \bar{\psi}_0, \Gamma(p^{f-i}n)\rangle,$$

since $R\Gamma(n) = \Gamma(pn)$ and $\langle \bar{\psi}_i, \Gamma(n)\rangle = \langle R^i\bar{\psi}_0, \Gamma(n)\rangle = \langle \bar{\psi}_0, R^{f-i}\Gamma(n)\rangle$. In particular,

$$\bar{\alpha} \in \mathbb{Z}^f \Leftrightarrow n \text{ is } q\text{-even}.$$

The above discussion can be rephrased as following.

Proposition 3.7 [She98, Lemma 3.4] $\mathfrak{J} = (E\mathbb{Z}^f) \cap (\mathbb{N}^f \backslash \{\bar{0}\})$.

3.2.2 Criterion for $W_d(N) \neq \emptyset$

For $d > 0$, define

$$I_d := \{\Gamma(n) : \exists\, \bar{v}_1, \dots, \bar{v}_{d-1} \in \mathfrak{J} \text{ such that } \Gamma(n) > \bar{v}_1 + \cdots + \bar{v}_{d-1}\},$$

$$J_d := \mathfrak{J} \cap (I_d \backslash I_{d+1}).$$

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

For $d = 0$, we set $J_0 = \emptyset$. By definition, J_d consists of those $\Gamma(n)$ such that n can be written as a sum of d many, but not $d+1$ many, positive q-even numbers without carry over in base p. Then,

$$W_d(N) \neq \emptyset \Leftrightarrow \Gamma(N) \in J_{d-1} \cup I_d. \tag{3.1}$$

The next proposition by Sheats characterizes elements in I_m and J_m.

Proposition 3.8 [She98, Proposition 4.3] *For $m \geq 1$,*

(i) $I_m = \{E\bar{x} \in \mathbb{N}^f \backslash \{\bar{0}\} : \bar{x} \in \mathbb{R}^f$ *and* $\min_{0 \leq i < f}(x_i) > m-1\}$,

(ii) $J_m = \{E\bar{a} \in \mathbb{N}^f \backslash \{\bar{0}\} : \bar{a} \in \mathbb{R}^f$ *and* $\min_{0 \leq i < f}(a_i) = m\}$.

With (3.1), it implies the following result which is indeed equivalent to Proposition 2.3.

Corollary 3.9 *Let $\Gamma(N) = E\bar{\alpha}$, then $W_d(N) \neq \emptyset$ iff $\min_{0 \leq i < f}(\alpha_i) \geq d-1$.*

3.2.3 Modest/optimal composition

The following results give estimation on components of the modest and optimal compositions.

Proposition 3.10 *Let $\mathbf{X} = (X_1, \ldots, X_d) \in W_d(N)$ be modest or optimal. Then, $\Gamma(X_i) \in J_1$ for $2 \leq i \leq d-1$, $X_d = 0$ if N is q-even, or $\Gamma(X_d) \in I_1 \backslash I_2$ if N is q-odd.*

Proof We prove by contrapositive.

N is q-even: If $X_d \neq 0$, then $\mathbf{X}$ is neither modest nor optimal from the discussion in Section 3.1. If $\Gamma(X_i) = \bar{\nu}_1 + \bar{\nu}_2$ for some $2 \leq i \leq d-1$ and vectors $\bar{\nu}_1, \bar{\nu}_2 \in \mathfrak{J}$, define

$$\mathbf{Y} := (X_1 + a_1, \ldots, X_{i-1}, a_2, X_i, \ldots, X_d).$$

Since $\bar{\nu}_i \in \mathfrak{J}$, both a_i's are q-even. The sum of entries in $\mathbf{Y}$ has no carry over in base p. So $\mathbf{Y} \in W_d(N)$. Moreover, $\mathbf{Y}$ is lexicographically larger than $\mathbf{X}$ and $\mathrm{wt}(\mathbf{Y}) = \mathrm{wt}(\mathbf{X}) - (i-1)a_1 < \mathrm{wt}(\mathbf{X})$.

N is q-odd: Suppose $\Gamma(X_d) = \bar{w}_1 + \bar{w}_2$ with $\bar{w}_1 \in \mathfrak{J}, \bar{w}_2 \in I_1$. We have $X_d = b_1 \oplus b_2$ with $\Gamma(b_i) = \bar{w}_i$ and $b_1 q$-even. Define $\mathbf{Y} := (X_1 + b_1, X_2, \ldots, X_{d-1}, b_2)$. Then, similar argument as above shows that $\mathbf{Y} \in W_d(N)$, $\mathbf{Y}$ is lexicographically larger than $\mathbf{X}$, and $\mathrm{wt}(\mathbf{Y}) < \mathrm{wt}(\mathbf{X})$. ∎

Take $N \in \mathbb{Z}_+$, let $\bar{u} = \Gamma(N)$ and $\bar{\beta} = E^{-1}\bar{u}$.

Lemma 3.11 *Let $\bar{\nu} = E\bar{\alpha} \in \mathbb{N}^f$ with $\bar{0} < \bar{\nu} < \bar{u}$. Suppose $\min_{0 \leq i < f}(\lfloor \beta_i \rfloor - \lceil \alpha_i \rceil) = k$ for some $k \in \mathbb{N}$, then there exists some $\bar{w} \in \mathfrak{J}$ with $\bar{\nu} \leq \bar{w} \leq \bar{u}$ and $\bar{u} - \bar{w} \in J_k \cup I_{k+1}$.*

Proof To find such an $\bar{w}$ is equivalent to find a $\bar{\gamma}$ with $\bar{w} = E\bar{\gamma}$. Recall that if $\bar{x} = E\bar{a}$, $x_i = pa_{i+1} - a_i$. By Propositions 3.7 and 3.8, we get the following conditions on $\bar{\gamma}$:

(1) $v_i \leq p\gamma_{i+1} - \gamma_i \leq u_i$,

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

(2) $\gamma_i \in \mathbb{Z}$ and $\min_{0\le j<f}(\beta_j - \gamma_j) \ge k$.

To construct $\bar{\gamma}$, take an l such that $\lfloor \beta_l \rfloor - \lceil \alpha_l \rceil = k$. Let $\gamma_l = \lceil \alpha_l \rceil$. For $i = l-1, l-2, \dots, l-f+1$, define inductively

$$\gamma_i = \min(\lfloor \beta_i \rfloor - k, p\gamma_{i+1} - \nu_i).$$

Condition (2) holds automatically by the construction of γ_i. The construction also implies $\nu_i \le p\gamma_{i+1} - \gamma_i$ for $i \ne l$. To prove it for $i = l$, we first show that $\gamma_i \ge \lceil \alpha_i \rceil$ for all i. By definition, $\gamma_l = \lceil \alpha_l \rceil$. We prove the rest by backward induction. Suppose $\gamma_{i+1} \ge \lceil \alpha_{i+1} \rceil$. If $\gamma_i = \lfloor \beta_i \rfloor - k$, then clearly $\gamma_i \ge \lceil \alpha_i \rceil$ since $\lfloor \beta_i \rfloor - \lceil \alpha_i \rceil \ge k$; otherwise,

$$\begin{aligned} \gamma_i &= p\gamma_{i+1} - \nu_i \\ &= p\gamma_{i+1} - p\alpha_{i+1} + \alpha_i \ge \alpha_i. \end{aligned}$$

Since γ_i is an integer, we have $\gamma_i \ge \lceil \alpha_i \rceil$. Now, we have $\nu_l \le p\gamma_{l+1} - \gamma_l$, since

$$p\gamma_{l+1} - \nu_l = p\gamma_{l+1} - p\alpha_{l+1} + \alpha_l \ge \lceil \alpha_l \rceil = \gamma_i.$$

Next, we show $p\gamma_{i+1} - \gamma_i \le u_i$. For $i = l$,

$$\begin{aligned} u_l - (p\gamma_{l+1} - \gamma_l) &= p\beta_{l+1} - \beta_l - (p\gamma_{l+1} - \gamma_l) \\ &= p(\beta_{l+1} - \gamma_{l+1}) - (\beta_l - \gamma_l) \\ &= p(\beta_{l+1} - \gamma_{l+1}) - (\beta_l - \lceil \alpha_l \rceil) \\ &> p(\beta_{l+1} - \gamma_{l+1}) - k - 1 \ge -1, \end{aligned}$$

where the last inequality comes from that $\beta_{l+1} - \gamma_{l+1} \ge k$ and $p \ge 2$. Since the left-hand side is an integer, we have

$$u_l - (p\gamma_{l+1} - \gamma_l) \ge 0.$$

Now, let $i \ne l$. If $\gamma_i = p\gamma_{i+1} - \nu_i$, then $p\gamma_{i+1} - \gamma_i = \nu_i \le u_i$; otherwise, $\gamma_i = \lfloor \beta_i \rfloor - k$, then a similar computation as in the $i = l$ case shows $p\gamma_{i+1} - \gamma_i \le u_i$. ∎

Proposition 3.12 *Take N with base p-expansion $N = \sum_{i=0}^{n} a_i p^i$, where $a_n \ne 0$. Suppose $W_d(N) \ne \emptyset$. Let $\boldsymbol{X} = (X_1, \dots, X_d) \in W_d(N)$ be modest or optimal, then*

(i) $X_1 \ge a_n p^n$. *In particular,* $X_1 > N/2$.
(ii) $N \le wt(\boldsymbol{X}) < 2N$.
(iii) $W_d(N - X_1) = \emptyset$ *if* $d \ge 2$. *In particular, by (3.1),* $\Gamma(N - X_1) \notin I_d$.

Proof We prove each case separately.

X modest: Let $\bar{u} = \Gamma(N)$ and $\bar{\alpha} = E^{-1}\bar{u}$. By Corollary 3.9, $\min_i(\lfloor \alpha_i \rfloor) = m \ge d - 1$. Let $k = n \bmod f$ and $\bar{\beta} = E^{-1}(a_n \bar{e}_k)$. Lemma 3.6 implies $\lceil \beta_i \rceil = 1$ for each i. By Lemma 3.11, we can extend $\bar{\nu} = a_n \bar{e}_k$ to some $\bar{w}_1 \in \mathfrak{J}$ with $\bar{u} - \bar{w}_1 \in J_{m-1} \cup I_m$. In particular, we can write $\bar{u} - \bar{w}_1$ as $\bar{u} - \bar{w}_1 = \bar{w}_2 + \cdots + \bar{w}_{d-1} + \bar{w}_d$, where $\bar{w}_i \in \mathfrak{J}$ for $2 \le i \le d-1$ and $\bar{w}_d \in \mathbb{N}^d$. Take $B = [\bar{w}_1, \dots, \bar{w}_d]$, then B is a valid matrix, i.e., $W_d^B(N) \ne \emptyset$. Let $\mathbf{Y}$ be the τ-monotonic element in $W_d^B(N)$, then $Y_1 \ge a_n p^n$ since $\bar{w}_1 \ge a_n \bar{e}_k$. X is modest so $X_1 \ge Y_1 \ge a_n p^n$. This proves (i).

We prove (ii) by induction on d. For $d = 1$, $\mathbf{X} = (N)$ and $\mathrm{wt}(\mathbf{X}) = N$. Suppose (ii) holds for $d-1$. By Proposition 3.4 (ii), $\mathbf{Y} = (X_2, \dots, X_d)$ is modest in $W_{d-1}(N - X_1)$.

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

By induction, $N - X_1 \le \mathrm{wt}(\mathbf{Y}) < 2(N - X_1) < N$. Thus, $N \le \mathrm{wt}(\mathbf{X}) = N + \mathrm{wt}(\mathbf{Y}) < 2N$.

Suppose (iii) fails. Take $(X_1', \dots, X_d') \in W_d(N - X_1)$, then $(X_1 + X_1', X_2', \dots, X_d') \in W_d(N)$. But this contradicts that $\mathbf{X}$ is modest.

$\mathbf{X}$ optimal: (ii) holds automatically by the minimum weight property.

To prove (i), we first show that $X_1 \ge p^n$. If N is q-even or $d < 3$, by Section 3.1 and Remark 3.3, optimal is equivalent to modest, and thus (1) holds. We assume N is q-odd and $d \ge 3$. Then, $X_1 + X_2 > p^n$, since otherwise $X_1 + X_2 < p^n < N/2$ and $\mathrm{wt}(\mathbf{X}) > N + 2(N - X_1 - X_2) > 2N$. For $\mathrm{wt}(\mathbf{X})$ being minimal, $X_1 \ge X_2$ which implies $X_1 \ge p^n$. Now, suppose $X_1 = \sum_{i=0}^{n} b_i p^i$ with $0 < b_n < a_n$, then $N - X_1 > p^n$. Note that $(X_2, \dots, X_d)$ is optimal in $W_{d-1}(N - X_1)$. Thus $X_2 \ge p^n$ and $N - X_d > (b_n + 1)p^n$. But by Proposition 3.4 (i), $(X_1, \dots, X_{d-1}) \in W_{d-1}(N - X_d)$ is optimal and thus modest since $N - X_d$ is q-even. In particular, $X_1 \ge (b_n + 1)p^n$. Contradiction.

At last, we show (iii) holds. If not, let $(X_1', \dots, X_d') \in W_d(N - X_1)$ be optimal. Then, $X_1' > (N - X_1)/2$ by (i). $(X_2', \dots, X_d')$ being optimal in $W_{d-1}(N - X_1 - X_1')$, $\mathrm{wt}(X_2', \dots, X_d') < 2(N - X_1 - X_1\prime) < N - X_1$. Let $\mathbf{Y} = (X_1 + X_1', X_2', \dots, X_d')$, then $\mathbf{Y} \in W_d(N)$ and $\mathrm{wt}(\mathbf{Y}) = N + \mathrm{wt}(X_2', \dots, X_d') < 2N - X_1$. However, $\mathrm{wt}(\mathbf{X}) = N + \mathrm{wt}(X_2, \dots, X_d) \ge 2N - X_1$. Contradiction. ∎

3.2.4 Constructing composition of smaller weight

Suppose Theorem 3.2 fails. Then, $q = p^f$ with $f > 1$. Take the least d and some N such that there exist $\mathbf{M} = (M_i), \mathbf{O} = (O_i) \in W_d(N)$ with $\mathbf{M}$ modest, $\mathbf{O}$ optimal, and $\mathbf{M} \ne \mathbf{O}$. Then, N is q-odd, $d \ge 3$, and $M_1 > O_1$ by Section 3.1, Remark 3.3, and Proposition 3.4 (ii), respectively. Let p^a be the largest p-power in $\mathcal{P}(M_1) \setminus \mathcal{P}(O_1)$. By Proposition 3.4 (iii), we may assume $a \equiv f - 1 \bmod f$. Let

$$\begin{aligned} \tilde{u} &:= \Gamma(N), & \tilde{x} &:= \Gamma(M_1), & \tilde{y} &:= \Gamma(O_1), \\ \tilde{\eta} &:= E^{-1}\tilde{u}, & \tilde{\alpha} &:= E^{-1}\tilde{x}, & \tilde{\beta} &:= E^{-1}\tilde{y}. \end{aligned}$$

By our construction, $x_{f-1} > y_{f-1}$ since both $\mathbf{M}$ and $\mathbf{O}$ are τ-monotonic. Define

$$\tilde{v} = [v_i]^t := [\min(x_i, y_i)]^t, \quad \tilde{w} = [w_i]^t := \tilde{y} - \tilde{v}.$$

Then, $w_{f-1} = 0$. Note that $\tilde{w} > \tilde{0}$, since otherwise $\tilde{x} > \tilde{y}$ and $\tilde{x} - \tilde{y} \in \mathfrak{J}$, $\Gamma(N - O_1) = (\tilde{x} - \tilde{y}) + \Gamma(M_2) + \cdots + \Gamma(M_d) \in I_d$, contradicting Proposition 3.12 (iii). Let $0 \le k \le f - 2$ be the least subscript such that $w_k > 0$. We have the following result.

Lemma 3.13 (i) $\langle \tilde{\psi}_i, \tilde{w} \rangle < \langle \tilde{\psi}_i, \tilde{e}_{f-1} \rangle$ *for* $0 \le i \le k$.

(ii) $\lfloor \eta_i \rfloor - \beta_i \ge d - 2$ *for all* i, *and there exists* $k < l \le f - 1$ *such that* $\lfloor \eta_l \rfloor - \beta_l = d - 2$ *and* $\lfloor \eta_i \rfloor - \beta_i \ge d - 1$ *for* $l - f < i \le k$, *i.e.,* $i = l + 1, l + 2, \dots, f - 1, 0, 1, \dots, k$.

Proof We show (i) by contradiction. For each $0 \le i \le k$, by definition of $\tilde{\psi}_i$,

$$\langle \tilde{\psi}_i, \tilde{e}_{f-1} \rangle = p^{f-1-i}$$

and $\langle \tilde{\psi}_i, \tilde{w} \rangle$ is a sum of p-powers less than p^{f-1-i} since $w_j = 0$ for $-1 \le j < i$. Suppose $\langle \tilde{\psi}_i, \tilde{w} \rangle \ge \langle \tilde{\psi}_i, \tilde{e}_{f-1} \rangle$ for some $0 \le i \le k$. Then, there is a subset of p-powers in the sum

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

$\langle \bar{\psi}_i, \bar{w} \rangle$ whose terms add up to p^{f-1-i}. In other words, there exists some $\bar{w}' \le \bar{w}$ such that

$$\langle \bar{\psi}_i, \bar{w}' \rangle = \langle \bar{\psi}_i, \bar{e}_{f-1} \rangle. \tag{3.2}$$

Another observation is that $\bar{w}$ represents those p-powers p^b in $\mathcal{P}(O_1) \setminus \mathcal{P}(M_1)$. In particular, $b < a$ for each b since $O_1 < M_1$. $\bar{w}' \le \bar{w}$ represents a subset of such p-powers. Let M be the sum of p-powers represented by $\bar{w}'$, then $M < p^a$ and $\Gamma(M) = \bar{w}'$. Note that $\Gamma(p^a) = \bar{e}_{f-1}$, then (3.2) implies

$$M \equiv p^a \bmod q - 1.$$

By the choice of p^a, we can find some $j > 1$ such that $p^a \in \mathcal{P}(O_j)$. Consider composition

$$\mathbf{X} = (O_1 - M + p^a, \dots, O_j - p^a + M, \dots, O_d),$$

then $\mathbf{X} \in W_d(N)$ and $\mathrm{wt}(\mathbf{X}) < \mathrm{wt}(\mathbf{O})$. Contradiction.

To prove (ii), we note that $E(\bar{\eta} - \bar{\beta}) = \Gamma(N - O_1) = \Gamma(O_2) + \cdots + \Gamma(O_d) \in I_{d-1}$. Hence, by Proposition 3.8 (i), $\eta_i - \beta_i > d - 2$. Thus,

$$\lfloor \eta_i \rfloor - \beta_i \ge d - 2,$$

for all i. On the other hand, $\Gamma(N - O_1) \notin I_d$ implies $\min_i(\lfloor \eta_i \rfloor - \beta_i) = d - 2$. Let l be the largest subscript such that $\lfloor \eta_l \rfloor - \beta_l = d - 2$. Then, for $l < i < f$,

$$\lfloor \eta_i \rfloor - \beta_i \ge d - 1.$$

To finish the proof, we show $\lfloor \eta_i \rfloor - \beta_i \ge d - 1$ for $0 \le i \le k$. By construction, we have

$$\bar{x} = \bar{v} + \bar{w}_1, \quad \bar{y} = \bar{v} + \bar{w},$$

where $\bar{w}_1 \ge \bar{e}_{f-1}$. For $0 \le i \le k$,

$$\begin{aligned}
\beta_i &= (q-1)^{-1} \langle \bar{\psi}_i, \bar{y} \rangle \\
&= (q-1)^{-1} (\langle \bar{\psi}_i, \bar{v} \rangle + \langle \bar{\psi}_i, \bar{w} \rangle) \\
(\text{by (i)}) &< (q-1)^{-1} (\langle \bar{\psi}_i, \bar{v} \rangle + \langle \bar{\psi}_i, \bar{e}_{f-1} \rangle) \\
&\le (q-1)^{-1} (\langle \bar{\psi}_i, \bar{v} \rangle + \langle \bar{\psi}_i, \bar{w}_1 \rangle) \\
&= (q-1)^{-1} \langle \bar{\psi}_i, \bar{x} \rangle = \alpha_i.
\end{aligned}$$

Note that $E(\bar{\eta} - \bar{\alpha}) = \Gamma(N - M_1) \in I_{d-1}$, then by Proposition 3.8 (i), we have $\lfloor \eta_i \rfloor - \alpha_i > d - 2$ for all $0 \le i < f$. For $0 \le i \le k$, $\beta_i < \alpha_i$ by the above calculation, and thus $\lfloor \eta_i \rfloor - \beta_i \ge d - 1$. ∎

Define, for $1 \le j \le d$,

$$\bar{u}_j = [u_{0,j}, \dots, u_{f-1,j}]^t := \sum_{s=j}^{d} \Gamma(O_s), \quad \bar{\theta}_j = [\theta_{0,j}, \dots, \theta_{f-1,j}]^t := E^{-1} \bar{u}_j.$$

Note that $\bar{u}_1 = \bar{u}$ and $\bar{\theta}_1 = \bar{\eta}$. By Lemma 3.13 (ii), we have

$$\lfloor \theta_{l,2} \rfloor = d - 2, \quad \lfloor \theta_{i,2} \rfloor \ge d - 1 \text{ for } l - f < i \le k. \tag{3.3}$$

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

The following construction uses $\bar{\theta}_j$ to get a new composition $\mathbf{Z} \in W_d(N)$ whose weight is less than that of $\mathbf{O}$. Let $\bar{\phi}_1 = [\phi_{i,1}]^t := \bar{\theta}_1$. Define $\bar{\phi}_2 = [\phi_{i,2}]^t$ inductively as following.

$$\phi_{i,2} = \begin{cases} \theta_{i,2} & \text{for } k < i \le l \\ \min(\theta_{i,2} - 1, p\phi_{i+1,2}) & i = k, k-1, \ldots, 0, f-1, f-2, \ldots, l+1. \end{cases}$$

For $j = 3, \ldots, d$, define $\bar{\phi}_j = [\phi_{i,j}]^t$ recursively as

$$\phi_{i,j} = \begin{cases} \theta_{i,j} & \text{for } k < i \le l \\ \min(\phi_{i,j-1} - 1, p\phi_{i+1,j}) & i = k, k-1, \ldots, 0, f-1, f-2, \ldots, l+1. \end{cases}$$

Proposition 3.14 *For $1 \le j \le d$, let*

$$\bar{z}_j = [z_{0,j}, \ldots, z_{f-1,j}]^t := E\bar{\phi}_j.$$

Then

(i) $\bar{\phi}_j - \bar{\phi}_{j+1} \in \mathbb{Z}_+^f$ *for* $1 \le j \le d-1$.
(ii) $\bar{z}_j \in \mathbb{Z}^f$ *for all* j.
(iii) $\min_{0 \le i \le f-1}(\lfloor \phi_{i,j} \rfloor) = \lfloor \phi_{l,j} \rfloor = d - j$ *for* $2 \le j \le d$.
(iv) $z_{k,2} = u_{k,2} + 1 \le u_k$.
(v) $0 \le z_{l,2} \le u_{l,2} - p$.
(vi) $0 \le z_{i,2} \le \max(u_{i,2} - (p-1), 0)$ *for* $l - f < i < k$.
(vii) $z_{i,j} = u_{i,j}$ *for* $k < i < l$ *and* $2 \le j \le d$.
(viii) $0 \le z_{i,j} \le \max(z_{i,j-1} - (p-1), 0)$ *for* $l - f \le i \le k$ *and* $3 \le j \le d$.

Proof (i): By construction, $\phi_{i,j} - \phi_{i,j+1} > 0$ for all i, j. Hence, it is enough to show

(a) $\bar{\theta}_j - \bar{\theta}_{j+1} \in \mathbb{Z}^f$ for $1 \le j \le d-1$;
(b) $\{\phi_{i,j}\} = \{\theta_{i,j}\}$ for all i, j, where $\{x\}$ is the fractional part of x.

We note that for $1 \le j \le d-1$,

$$E(\bar{\theta}_j - \bar{\theta}_{j+1}) = \Gamma(O_j) \in \mathfrak{J}.$$

This implies (a) by Proposition 3.7. (a) says $\{\theta_{i,j}\} = \{\theta_{i,j+1}\}$ for all i and j. Also $p\{\theta_{i+1,j}\} - \{\theta_{i,j}\} \in \mathbb{Z}$ since $p\theta_{i+1,j} - \theta_{i,j} = u_{i,j} \in \mathbb{N}$. With these two properties in mind, starting with the initial case $\{\phi_{i,1}\} = \{\theta_{i,1}\}$ since $\bar{\phi}_1 = \bar{\theta}_1$, following the inductive construction of $\phi_{i,j}$, one can check that (b) holds.

(ii): Since $\bar{\phi}_1 = \bar{\eta}$, $\bar{z}_1 = E\bar{\eta} = \bar{u} \in \mathbb{Z}^f$. For $j > 1$,

$$\bar{z}_j = E\bar{\phi}_1 - \sum_{s=1}^{j-1} E(\bar{\phi}_s - \bar{\phi}_{s+1}).$$

By (i), $\bar{\phi}_s - \bar{\phi}_{s+1} \in \mathbb{Z}^f$ for each s; hence, $\bar{z}_j \in \mathbb{Z}^f$.

(iii): We first show that $\lfloor \phi_{i,j} \rfloor \ge d - j$ for $2 \le j \le d$ and $k < i \le l$. This is the same as showing

$$\lfloor \theta_{i,j} \rfloor \ge d - j$$

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

for $2 \le j \le d$, since $\phi_{l,j} = \theta_{i,j}$ by construction. Note that for each j, $E\bar{\theta}_j = \sum_{s=j}^{d} \Gamma(O_j) \in I_{d-j+1}$. Thus, the statement follows from Proposition 3.8.

Next, we prove $\lfloor \phi_{l,j} \rfloor = d - j$ for each j. The $j = 2$ case is given by (3.3). For $3 \le j \le d$, $\bar{\theta}_2 - \bar{\theta}_j = \sum_{s=2}^{j-1} E^{-1}\Gamma(O_s)$. By Propositions 3.8 and 3.10, $\theta_{l,2} - \theta_{l,j} \ge j - 2$, which implies $\lfloor \theta_{l,j} \rfloor \le \lfloor \theta_{l,2} \rfloor - (j-2) = d - j$. Thus, the statement follows since $\lfloor \theta_{l,j} \rfloor \ge d - j$.

Last, we show $\lfloor \phi_{i,j} \rfloor \ge d - j$ for $l - f < i \le k$ by induction on j. For $j = 2$, we have

$$\lfloor \theta_{i,2} - 1 \rfloor \ge d - 2$$

for $l - f < i \le k$ by (3.3). Taking $i = k$, since $\lfloor p\phi_{k+1,2} \rfloor = \lfloor p\theta_{k+1,2} \rfloor \ge d - 2$, we get

$$\lfloor \phi_{k,2} \rfloor = \min(\lfloor \theta_{k,2} - 1 \rfloor, \lfloor p\phi_{k+1,2} \rfloor) \ge d - 2.$$

Note that

$$\begin{aligned} \lfloor \phi_{i+1,2} \rfloor \ge d - 2 &\Rightarrow \lfloor p\phi_{i+1,2} \rfloor \ge d - 2 \\ &\Rightarrow \lfloor \phi_{i,2} \rfloor = \min(\lfloor \theta_{i,2} - 1 \rfloor, \lfloor p\phi_{i+1,2} \rfloor) \ge d - 2. \end{aligned}$$

Hence, a backward induction on i starting from k implies that for $k \ge i > l - f$,

$$\lfloor \phi_{i,2} \rfloor \ge d - 2.$$

Suppose $\lfloor \phi_{i,j-1} \rfloor \ge d - j + 1$ for $l - f < i \le k$. Then, $\lfloor \phi_{k,j-1} - 1 \rfloor \ge d - j$ and $\lfloor p\phi_{k+1,j} \rfloor \ge d - j$, since $\lfloor \phi_{k+1,j} \rfloor \ge d - j$ by previous statement. This implies $\lfloor \phi_{k,j} \rfloor = \min(\lfloor \phi_{k,j-1} - 1 \rfloor, \lfloor p\phi_{k+1,j} \rfloor) \ge d - j$. Similarly, we have

$$\begin{aligned} \lfloor \phi_{i+1,j} \rfloor \ge d - j &\Rightarrow \lfloor p\phi_{i+1,j} \rfloor \ge d - j \\ &\Rightarrow \lfloor \phi_{i,j} \rfloor = \min(\lfloor \phi_{i,j-1} - 1 \rfloor, \lfloor p\phi_{i+1,j} \rfloor) \ge d - j. \end{aligned}$$

Again, a backward induction on i shows that $\lfloor \phi_{i,j} \rfloor \ge d - j$ for $k \ge i > l - f$.

(iv): Since

$$p\phi_{k+1,2} - (\theta_{k,2} - 1) = p\theta_{k+1,2} - \theta_{k,2} + 1 = u_{k,2} + 1 > 0,$$

$\phi_{k,2} = \theta_{k,2} - 1$ and $z_{k,2} = u_{k,2} + 1$. By construction,

$$u_{k,2} = u_k - y_k \le u_k - w_k \le u_k - 1,$$

so $u_{k,2} + 1 \le u_k$.

(v): The second inequality is given by

$$z_{l,2} = p\phi_{l+1,2} - \phi_{l,2} \le p(\theta_{l+1,2} - 1) - \theta_{l,2} = u_{l,2} - p.$$

To show $z_{l,2} \ge 0$, we have $\min_{0 \le i \le f-1}(\lfloor \phi_{i,2} \rfloor) = \lfloor \phi_{l,2} \rfloor = d - 2$ by (iii). This implies

$$z_{l,2} = p\phi_{l+1,2} - \phi_{l,2} \ge p(d-2) - (d-2) - \{\phi_{l,2}\} \ge 0.$$

(vi): For $l - f < i < k$, if $\phi_{i,2} = p\phi_{i+1,2}$, $z_{i,2} = p\phi_{i+1,2} - \phi_{i,2} = 0$; otherwise, $\phi_{i,2} = \theta_{i,2} - 1$ and $z_{i,2} = p\phi_{i+1,2} - (\theta_{i,2} - 1) \le p(\theta_{i+1,2} - 1) - (\theta_{i,2} - 1) = u_{i,2} - (p-1)$.

(vii): This follows directly from the construction of the ϕ_j's.

(viii): We break up the proof into three cases.

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

For $l - f < i < k$, we only need to check for the case where $\phi_{i,j} = \phi_{i,j-1} - 1$, since otherwise $z_{i,j} = 0$. In this case, $\phi_{i,j} - 1 \le p\phi_{i+1,j}$ and

$$0 \le z_{i,j} = p\phi_{i+1,j} - (\phi_{i,j-1} - 1) \le p(\phi_{i+1,j-1} - 1) - (\phi_{i,j-1} - 1) = z_{i,j-1} - (p-1).$$

For $i = k$, again, we may assume $\phi_{k,j} = \phi_{k,j-1} - 1$, then

$$\begin{aligned} 0 \le z_{k,j} &= p\theta_{k+1,j} - (\phi_{k,j-1} - 1) \\ &\le p(\theta_{k+1,j-1} - 1) - (\phi_{k,j-1} - 1) = z_{k,j-1} - (p-1), \end{aligned}$$

where the second inequality follows from the fact that $\tilde{\theta}_{j-1} - \tilde{\theta}_j = E^{-1}\Gamma(O_{j-1}) \ge 1$ by Propositions 3.8 and 3.10.

For $i = l$, by (iii), we have

$$z_{l,j} = p\phi_{l+1,j} - \phi_{l,j} \ge p(d-j) - (d-j) - \{\phi_{l,j}\} \ge 0.$$

Finally, $z_{l,j} = p\phi_{l+1,j} - \theta_{l,j} \le p(\phi_{l+1,j-1} - 1) - (\theta_{l,j-1} - 1) = z_{l,j-1} - (p-1)$. ∎

Proposition 3.14 implies that the matrix

$$B = [\tilde{z}_1 - \tilde{z}_2, \dots, \tilde{z}_{d-1} - \tilde{z}_d, \tilde{z}_d]$$

is a valid matrix of $W_d(N)$. Let $\mathbf{Z} = (Z_1, \dots, Z_d)$ be the τ-monotonic element in $W_d^B(N)$. We show that $\mathrm{wt}(\mathbf{Z}) < \mathrm{wt}(\mathbf{O})$ and hence get a contradiction.

3.2.5 Estimation on wt(Z)

For $2 \le j \le d$, define

$$\begin{aligned} Z'_j &:= Z_j + Z_{j+1} + \cdots + Z_d, \\ O'_j &:= O_j + O_{j+1} + \cdots + O_d. \end{aligned}$$

Then, $\Gamma(Z'_j) = \tilde{z}_j$ and $\Gamma(O'_j) = \tilde{u}_j$. And weights of $\mathbf{Z}$ and $\mathbf{O}$ can be expressed as

$$\begin{aligned} \mathrm{wt}(\mathbf{Z}) &= N + Z'_2 + \cdots + Z'_d, \\ \mathrm{wt}(\mathbf{O}) &= N + O'_2 + \cdots + O'_d. \end{aligned}$$

To describe these Z'_j, O'_j explicitly, for each $0 \le i \le f-1$, denote

$$\tau_i(N) = (\tau_{i,u_i}, \tau_{i,u_i-1}, \dots, \tau_{i,1}).$$

We recall that $\tau_i(N)$ is defined as the subsequence of the nonincreasing sequence of p-powers in $\mathcal{P}(n)$, where the exponents of powers in it are congruent to i modulo f.

Let $\tau_{i,0} = 0$. Then, by τ-monotonicity, we have

$$Z'_j = \sum_{i=0}^{f-1} \sum_{s=0}^{z_{i,j}} \tau_{i,s}, \qquad O'_j = \sum_{i=0}^{f-1} \sum_{s=0}^{u_{i,j}} \tau_{i,s}.$$

By Proposition 3.14 (vii),

$$O'_j - Z'_j = \sum_{i \in I} \left(\sum_{s=0}^{u_{i,j}} \tau_{i,s} - \sum_{s=0}^{z_{i,j}} \tau_{i,s} \right),$$

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

where

$$I = \{l, \dots, f-1, 0, \dots, k\}.$$

For $j = 2$ and $i \in I$, we have the following:

(1) By Proposition 3.14 (iv–vi), $z_{k,2} = u_{k,2} + 1$ and for $i \in I \backslash \{k\}$, $z_{i,2} \le u_{i,2}$, where "=" holds iff $z_{i,2} = u_{i,2} = 0$.

(2) $\tau_{f-1,u_{f-1,2}} = p^a$ since it is the largest p-power not in $\mathcal{P}(O_1)$ whose exponent is $f-1 \bmod n$. In particular, $u_{f-1,2} > 0$; hence, $z_{f-1,2} < u_{f-1,2}$ by (1).

(3) Let $\tau_{k,z_{k,2}} = p^b$, then $z_{k,2} = u_{k,2} + 1$ implies that p^b is the last p-power in $\tau_k(O_1)$. By our choice of k, $p^b \in \mathcal{P}(O_1) \setminus \mathcal{P}(M_1)$. In particular, $p^b < p^a$.

With these observations, we have

$$O_2' - Z_2' \ge \tau_{f-1,u_{f-1,2}} - \tau_{k,z_{k,2}} + \sum_{i \in I \backslash \{k,f-1\}} \tau_{i,z_{i,2}} = p^a - p^b + \sum_{i \in I \backslash \{k,f-1\}} \tau_{i,z_{i,2}}.$$

Thus,

$$\mathrm{wt}(\mathbf{O}) - \mathrm{wt}(\mathbf{Z}) = \sum_{j=2}^{d} O_j' - Z_j' \ge p^a - p^b + \sum_{i \in I \backslash \{k,f-1\}} \tau_{i,z_{i,2}} + \sum_{j=3}^{d} O_j' - Z_j'. \tag{3.4}$$

The next lemma gives a lower bound for $\sum_{j=3}^{d} O_j' - Z_j'$.

Lemma 3.15 *Let $I = \{l, \dots, f-1, 0, \dots, k\}$, then*

$$\sum_{j=3}^{d} O_j' - Z_j' > -\sum_{i \in I} \tau_{i,z_{i,2}}.$$

Proof We note that $\tau_{k,z_{k,2}} > 0$ since $z_{k,2} > 0$ by Proposition 3.14 (iv). The statement is trivial if $z_{i,j} = 0$ for all $i \in I$ and $3 \le j \le d$. Assuming they are not all vanishing, the statement follows from the following calculation:

$$\begin{aligned}
\sum_{j=3}^{d} O_j' - Z_j' &= \sum_{j=3}^{d} \sum_{i \in I} \left(\sum_{s=0}^{u_{i,j}} \tau_{i,s} - \sum_{s=0}^{z_{i,j}} \tau_{i,s} \right) \\
&> -\sum_{i \in I} \sum_{j=3}^{d} \sum_{s=0}^{z_{i,j}} \tau_{i,s} \\
&> -p \sum_{i \in I} \sum_{j=3}^{d} \tau_{i,z_{i,j}} \\
&> -p^2/q \sum_{i \in I} \tau_{i,z_{i,2}} \\
&\ge -\sum_{i \in I} \tau_{i,z_{i,2}}.
\end{aligned}$$

The first inequality is trivial. The last one follows from the assumption $f \ge 2$. For the second inequality, we note that each p-power appearing in the sum $\sum_{s=0}^{z_{i,j}} \tau_{i,s}$ repeats at most $p-1$ times and the largest term is $\tau_{i,z_{i,j}}$, which indicates $\sum_{s=0}^{z_{i,j}} \tau_{i,s} < p\tau_{i,z_{i,j}}$.

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press

By a similar argument and Proposition 3.14 (viii), for all $i \in I$ and $3 \le j \le d$, we have $\tau_{i,z_{i,j}} \le q^{-1}\tau_{i,z_{i,j-1}}$; thus,

$$\sum_{j=3}^{d} \tau_{i,z_{i,j}} \le q^{-1} \sum_{j=2}^{d-1} \tau_{i,z_{i,j}} < \frac{p}{q}\tau_{i,z_{i,2}}.$$

This gives the third inequality. ∎

Now, we are ready to claim the contradiction, which finishes the proof of Theorem 3.2.

Proposition 3.16 $wt(\boldsymbol{Z}) < wt(\boldsymbol{O})$.

Proof We first show $\tau_{f-1,z_{f-1,2}} < p^a$. Assume $z_{f-1,2} > 0$ since otherwise $\tau_{f-1,z_{f-1,2}} = 0$. Then, $\tau_{f-1,z_{f-1,2}} \le q^{-1}\tau_{f-1,u_{f-1,2}}$ because $z_{f-1,2} \le u_{f-1,2} - (p-1)$ by Proposition 3.14. Note that $\tau_{f-1,u_{f-1,2}} = p^a$ as we mentioned earlier, and thus $\tau_{f-1,z_{f-1,2}} < p^a$.

Putting together (3.4) and Lemma 3.15, we have

$$\mathrm{wt}(\mathbf{O}) - \mathrm{wt}(\mathbf{Z}) > p^a - 2p^b - \tau_{f-1,z_{f-1,2}}.$$

Here p^b and $\tau_{f-1,z_{f-1,2}}$ are p-powers less than p^a, and they are distinct since their exponents fall into different residue classes mod f. We break up the proof into three cases.

(1) $p \ge 3$: $\mathrm{wt}(\mathbf{O}) - \mathrm{wt}(\mathbf{Z}) > 0$ since $2p^b + \tau_{f-1,z_{f-1,2}} < p^a$.

(2) $p = 2$ and $b + 1 < a$: $2p^b + \tau_{f-1,z_{f-1,2}} = p^{b+1} + \tau_{f-1,z_{f-1,2}} \le p^a$; thus, $\mathrm{wt}(\mathbf{O}) - \mathrm{wt}(\mathbf{Z}) > 0$.

(3) $p = 2$ and $b + 1 = a$: In this case, we have $k + 1 = l = f - 1$ and $I = \{0, \dots, f-1\}$. By Proposition 3.14 (v), $u_{f-1,2} - z_{f-1,2} \ge 2$. Hence,

$$\begin{aligned} O'_2 - Z'_2 &= \left(\sum_{s=0}^{u_{f-1,2}} \tau_{i,s} - \sum_{s=0}^{z_{f-1,2}} \tau_{i,s}\right) + \sum_{i=0}^{k}\left(\sum_{s=0}^{u_{i,2}} \tau_{i,s} - \sum_{s=0}^{z_{i,2}} \tau_{i,s}\right) \\ &\ge p^a + \tau_{f-1,1+z_{f-1,2}} - p^b + \sum_{i=0}^{k-1} \tau_{i,z_{i,2}}, \end{aligned}$$

and by Lemma 3.15,

$$\begin{aligned} \mathrm{wt}(\mathbf{O}) - \mathrm{wt}(\mathbf{Z}) &= \sum_{j=2}^{d} O'_j - Z'_j \\ &> p^a + \tau_{f-1,1+z_{f-1,2}} - p^b + \sum_{i=0}^{k-1} \tau_{i,z_{i,2}} - \sum_{i\in I} \tau_{i,z_{i,2}} \\ &= p^a + \tau_{f-1,1+z_{f-1,2}} - p^b - p^b - \tau_{f-1,z_{f-1,2}} \\ &= \tau_{f-1,1+z_{f-1,2}} - \tau_{f-1,z_{f-1,2}} \ge 0. \end{aligned}$$

∎

Acknowledgment. The results of this paper are a part of the author's Ph.D. thesis at the University of Rochester. The author would like to express her sincere gratitude

for her advisor, Prof. Dinesh Thakur, for suggesting this problem and for all of his guidance and encouragement.

References

[Böc13] G. Böckle, *The distribution of the zeros of the Goss zeta-function forA = $F_2[x, y]/\left(y^2 + y + x^3 + x + 1\right)$*. Math. Z. **275**(2013), nos. 3–4, 835–861.

[BK97] D. J. Broadhurst and D. Kreimer, *Association of multiple zeta values with positive knots via Feynman diagrams up to 9 loops*. Phys. Lett. B. **393**(1997), nos. 3–4, 403–412.

[BGF] J. I. Burgos Gil and J. Fresán, *Multiple zeta values: from numbers to motives*, to appear in Clay Mathematics Proceedings. http://javier.fresan.perso.math.cnrs.fr/mzv.pdf.

[Car48] L. Carlitz, *Finite sums and interpolation formulas over GF $[p^n, x]$*. Duke Math. J. **15**(1948), 1001–1012.

[Cha14] C.-Y. Chang, *On characteristic p multizeta values, Algebraic number theory and related topics 2012*. RIMS Kôkyûroku Bessatsu, B51, Research Institute For Mathematical Sciences, Kyoto, 2014, pp. 177–202.

[DG05] P. Deligne and A. B. Goncharov, *Groupes fondamentaux motiviques de Tate mixte*. Ann. Sci. École Norm. Sup. **38**(2005), no. 1, 1–56, Series 4.

[DV96] J. Diaz-Vargas, *Riemann hypothesis for $F_p[T]$*. J. Number Theory **59**(1996), no. 2, 313–318.

[Eul75] L. Euler, *Meditationes circa singulare serierum genus*. Novi Comm. Acad. Sci. Petropol. **20**(1775), 140–186, Reprinted in "Opera Omnia", ser. 1, vol. 15, B. G. Teubner, Berlin, 1927, pp. 217–267.

[FKMT17] H. Furusho, Y. Komori, K. Matsumoto, and H. Tsumura, *Desingularization of complex multiple zeta-functions*. Amer. J. Math. **139**(2017), no. 1, 147–173.

[Gon01] A. B. Goncharov, *Multiple ζ-values, Galois groups, and geometry of modular varieties*. In: European Congress of Mathematics, Vol. I (Barcelona, 2000), Progr. Math., 201, Birkhäuser, Basel, 2001, pp. 361–392.

[Gon05] A. B. Goncharov, *Galois symmetries of fundamental groupoids and noncommutative geometry*. Duke Math. J. **128**(2005), no. 2, 209–284.

[Gos79] D. Goss, *v-Adic zeta functions, L-series and measures for function fields*. Invent. Math. **55**(1979), 107–119.

[Gos96] D. Goss, *Basic structures of function field arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 35, Springer-Verlag, Berlin, 1996.

[Hof92] M. E. Hoffman, *Multiple harmonic series*. Pacific J. Math. **152**(1992), no. 2, 275–290.

[Mas06] R. Masri, *Multiple zeta values over global function fields*. In: Multiple Dirichlet series, automorphic forms, and analytic number theory, Proc. Sympos. Pure Math., 75, American Mathematical Society, Providence, RI, 2006, pp. 157–175.

[She98] J. T. Sheats, *The Riemann hypothesis for the Goss zeta function for $F_q[T]$*. J. Number Theory **71**(1998), no. 1, 121–157.

[Tha04] D. S. Thakur, *Function field arithmetic*. World Scientific Publishing, River Edge, NJ, 2004.

[Tha09] D. S. Thakur, *Power sums with applications to multizeta and zeta zero distribution for $F_q[t]$*. Finite Fields Appl. **15**(2009), no. 4, 534–552.

[Tha17] D. S. Thakur, *Multizeta values for function fields: a survey*. J. Théor. Nombres Bordeaux **29**(2017), no. 3, 997–1023.

[Zag94] D. Zagier, *Values of zeta functions and their applications*. In: First European Congress of Mathematics, Vol. II (Paris, 1992), Progr. Math., 120, Birkhäuser, Basel, 1994, pp. 497–512.

Department of Mathematics, Texas A&M University, College Station, TX 77843, USA
e-mail: shuhui@math.tamu.edu

https://doi.org/10.4153/S0008439521000035 Published online by Cambridge University Press