Finite Fields and Their Applications 15 (2009) 534–552

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Power sums with applications to multizeta and zeta zero distribution for $\mathbb{F}_q[t]$

Dinesh S. Thakur [1]

University of Arizona, Tucson, AZ 85721, United States

ARTICLE INFO

Article history:
Received 18 November 2008
Revised 1 April 2009
Available online 22 April 2009
Communicated by Neal Koblitz

Keywords:
Zeta
Function field
Riemann hypothesis
Multizeta
Duality

ABSTRACT

We study the sum of integral powers of monic polynomials of a given degree over a finite field. The combinatorics of cancellations are quite complicated. We prove several results on the degrees of these sums giving direct or recursive formulas, congruence conditions and degree bounds for them. We point out a 'duality' between values for positive and negative powers. We show that despite the combinatorial complexity of the actual values, there is an interesting kind of a recursive formula (at least when the finite field is the prime field) which quickly leads to many interesting structural facts, such as Riemann hypothesis for Carlitz–Goss zeta function, monotonicity in degree, non-vanishing and special identity classification for function field multizeta, as easy consequences.

1. Introduction

We study some basic questions on the behavior of $S_d(k)$ defined as the sum of $1/a^k$ as a runs through all the monic polynomials of degree d in $\mathbb{F}_q[t]$. (In the literature, the notation $S_d(-k)$ for this sum is also common. Though we allow k to be any integer, because of the zeta connection, we follow this particular sign convention here.)

We will be interested in (i) getting simple formulas (direct or recursive in k or d) for these sums and for their degrees, (ii) understanding how these degrees behave as functions of d and k.

While the degree of the term $1/a^k$, being just $-dk$, has extremely simple behavior, the degree we are interested in behaves quite erratically, because of complicated cancellation possibilities. Apart from their intrinsic interest, these questions have applications to the non-vanishing of the multizeta

E-mail address: thakur@math.arizona.edu.

[1] The author was supported by NSA grant H98230-08-1-0049.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2009.04.002

values defined [8, Sec. 5.10] by the author and to the zero distribution results for the Goss zeta function for $\mathbb{F}_q[t]$, namely the Riemann hypothesis analog in this context, proved for q prime by Daqing Wan [10], with another proof by Diaz-Vargas [3], [8, Sec. 5.8] and for general q by Sheats [6], see also [4, Sec. 8.24], [5]. While they used values for k negative, we show a 'duality' between positive and negative k and explain how to calculate values for positive k similarly and approach the zero distribution this way.

Let k be positive for this paragraph. While $-dk$ is clearly a strictly decreasing function of d or k, the degree of $S_d(k)$ is not a strictly decreasing as a function of k. The statement that it is a strictly decreasing function of d is a subtle claim which implies non-vanishing of all the multizeta values. As d jumps by one, $-dk$ changes by k. But again the claim that the jumps in the degree of $S_d(k)$ strictly increase with d easily implies the Riemann hypothesis analog mentioned above.

When q is a prime, we describe (and prove in Theorem 1) a simple recursion formula (1) (for $k \in \mathbb{Z}$) for the degree of $S_d(k)$, which has immediate implications this analog of Riemann hypothesis as well as many other applications and it also allows fast calculations of the degrees. The recursive formula reduces all its complexities to $s_1(k)$ which being simple for $q = 2$, we have a simple direct proof in the case $q = 2$, $k > 0$. If we could generalize this, it would lead to another proof of Riemann hypothesis coming from power sums for positive k. The proof we give in general uses the results of Carlitz, the author and Diaz-Vargas [3] for negative k. We also see that the simple recursive formula underlies the zero distribution phenomena with the 'initial values' $s_1(k)$ being almost irrelevant, except for the trivial fact $s_1(k) > k$, for positive k.

The recursion formula (1) sometimes fails, when q is not a prime and we plan to investigate the case of general q in the near future.

2. Power sums

2.1. Notation

$$\mathbb{Z} = \{\text{integers}\},$$

$$\mathbb{Z}_+ = \{\text{positive integers}\},$$

$$\mathbb{Z}_{\geqslant 0} = \{\text{non-negative integers}\},$$

$$q = \text{a power of a prime } p, \quad q = p^f,$$

$$A = \mathbb{F}_q[t],$$

$$A+ = \{\text{monics in } A\},$$

$$A_d+ = \{\text{monics in } A \text{ of degree } d\},$$

$$K = \mathbb{F}_q(t),$$

$$K_\infty = \mathbb{F}_q\big((1/t)\big) = \text{completion of } K \text{ at } \infty,$$

$$C_\infty = \text{the completion of an algebraic closure of } K_\infty,$$

$$[n] = t^{q^n} - t,$$

$$d_n = \prod_{i=0}^{n-1} \big(t^{q^n} - t^{q^i}\big),$$

$$\ell_n = \prod_{i=1}^{n} \big(t - t^{q^i}\big),$$

$$\ell(k) = \text{sum of the digits of the base } q \text{ expansion of } k,$$

$$\deg = \text{function assigning to } a \in A \text{ its degree in } t, \quad \deg(0) = -\infty.$$

2.2. Power sums

2.2.1. For $k \in \mathbb{Z}$ and $d \in \mathbb{Z}_{\geqslant 0}$, write

$$S_d(k) := \sum_{\substack{a \in A_+ \\ \deg a = d}} \frac{1}{a^k} \in K, \qquad s_d(k) := -\deg S_d(k).$$

Hence $s_d(k)$ is the valuation of $S_d(k)$ at the infinite place of $\mathbb{F}_q[t]$.

2.2.2. Zeta and multizeta
For $k \in \mathbb{Z}$, put

$$\zeta(k) := \sum_{d=0}^{\infty} S_d(k) \in K_\infty.$$

These are the *Carlitz–Goss zeta values*. See [2,4,8] and references there for more details on interpolations and properties. Let $s_i \in \mathbb{Z}_{>0}$. Then

$$\zeta(s_1, \ldots, s_r) := \sum_{d_1 > \cdots > d_r \geqslant 0} S_{d_1}(s_1) \cdots S_{d_r}(s_r) \in K_\infty$$

are the multizeta values defined in [8]. See [1,9] for more details and results on their properties and interpolations.

2.2.3. Note $S_0(k) = 1$ and thus $s_0(k) = 0$, for $k \in \mathbb{Z}$.

If $k > 0$, then $S_d(k)$ does not vanish (as we can see using P-adic valuation for prime P of degree d) and $s_d(k) > 0$, if further $d > 0$.

Let $k \leqslant 0$. If $S_d(k)$ does not vanish, then $s_d(k) \leqslant 0$. But $S_d(k)$ does vanish (and then $s_d(k)$ is infinite) for d large enough, for example if $d > \ell(k)/(q-1)$ (this is 'if and only if' when q is a prime, but not in general). We refer to [8, 5.6] and references there for this fact, history and some formulas, when $k \leqslant 0$, by Carlitz, Lee, Gekeler etc. But note that $S_d(k)$ in this reference corresponds to our $S_d(-k)$ and also that Theorem 5.6.3 there has two misprints: both in the statement and the proof (i) the exponent of x in the first sum should be $-n-1$ rather than $-n+1$, (ii) the minus sign is missing in front of the second sum.

2.2.4. Since we are in characteristic p, we have

$$S_d\big(kp^n\big) = S_d(k)^{p^n}.$$

So we can often restrict to k's not divisible by p without loss of generality, in many situations. Observe also that $S_d(k) \in \mathbb{F}_p(t)$, by considering $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$-invariance.

2.2.5. Since $S_d(k)$, for $d > 0$, is the sum of $S_1(k)$'s evaluated at t replaced by all the monic polynomials of degree d with zero constant coefficient, we have (i) a simple bound $s_d(k) \geqslant ds_1(k)$, (ii) if $S_d(k_1) = S_d(k_2)$ holds for $d = 1$, then it holds for all d.

2.3. Carlitz' generating function

By a generating function approach, Carlitz (see [2], [8, 5.6.3]) proved:

Let $k \geqslant 0$ and $d \geqslant 0$. Then $S_d(k+1)$ is the coefficient of x^k in $(1+\sum+\sum^2+\cdots+\sum^k)/\ell_d$, where $\sum = \sum_{i=0}^d x^{q^i}/d_i \ell_{d-i}^{q^i}$, i.e.,

$$S_d(k+1) = \frac{1}{\ell_d} \sum_{\sum_{i=0}^d k_i q^i = k,\, k_i \geqslant 0} \binom{\sum k_i}{k_0, \ldots, k_d} \prod \left(\frac{1}{d_i \ell_{d-i}^{q^i}}\right)^{k_i}$$

$$= \frac{1}{\ell_d^{k+1}} \sum_{\sum_{i=0}^d k_i q^i = k,\, k_i \geqslant 0} \binom{\sum k_i}{k_0, \ldots, k_d} \prod \left(\frac{(\ell_d/\ell_{d-i})^{q^i}}{d_i}\right)^{k_i}$$

$$= \frac{1}{\ell_d^{k+1}} \sum_{k = k_d q^d + \cdots + k_0,\, k_i \geqslant 0} \binom{k_d + \cdots + k_0}{k_d, \ldots, k_0} \prod_{i=1}^d \left(\frac{(-1)^i([d]\cdots[d-i+1])^{q^i}}{d_i}\right)^{k_i}.$$

2.3.1. Remarks

(1) While the number of terms in $S_d(k)$, as defined in 2.2.1, is q^d, in these formulas the number of terms does not grow with d, for sufficiently large d, because $k_i = 0$ for $i > \log_q k$.

(2) Lucas theorem says that if $k = \sum k_i p^i$ and $m_j = \sum m_{ji} p^i$ are base p expansions, then

$$\binom{k}{m_1, \ldots, m_r} = \prod \binom{k_i}{m_{1i}, \ldots, m_{ri}}.$$

Since we have $\binom{a}{b} = 0$ if $b > a$, we see as a corollary that the multinomial coefficient displayed above is zero, if there is a carry over base p in the sum $k = \sum m_i$. So only terms where there is no carry over base p in the sum of k_i's need to be considered.

(3) When $d = 1$, we see that $s_1(k+1) = (k_1 + k_0 + 1)q = k + q + k_0(q-1)$, where k_0 is the minimum possible such that $k = k_1 q + k_0$, $k_i \geqslant 0$, with no carry over base p in the sum $k_1 + k_0$. For example, if the last two digits in the base q expansion of k add without carry over base p, then k_0 is the last digit. In particular, if q divides k, then $s_1(k+1) = k + q$. This together with 2.2.4 takes care of $d = 1$, $q = 2$ case.

(4) Let us write, for $0 \leqslant i \leqslant d$,

$$b(i,d) := \deg 1/\left(\ell_{d-i}^{q^i} d_i\right) = -\left(\frac{q^{d+1} - q^{i+1}}{q-1} + iq^i\right).$$

Hypothesis (H1). In the sum in 2.3, there is unique term of maximum degree among the terms corresponding to various decompositions of k.

Under Hypothesis (H1), we see that $s_d(k+1) = -(b(0,d) + \sum k_i b(i,d))$ where the k_i's correspond to this unique term. We do not have a proof, but only numerical evidence, gathered by David Roe for small q, k, d, that there is no clash for the maximum degree contribution.

3. Recursion in d for $s_d(k)$

Let $k > 0$ in this section. We have $S_0(k) = 1$, so $s_0(k) = 0$.

3.1. Case $d = 1$

The next case $d = 1$ is already a little complicated:

Claim: $s_1(k) = k + j$ where j is the least positive integer divisible by $q - 1$ for which $\binom{-k}{j} = (-1)^j\binom{k+j-1}{j} = (-1)^j\binom{k+j-1}{k-1}$ is non-zero modulo p:

We have

$$S_1(k) = \frac{1}{t^k}\sum_{\theta \in \mathbb{F}_q}\left(1 + \frac{\theta}{t}\right)^{-k} = -\sum_{j=1,(q-1)|j}^{\infty}\binom{-k}{j}\frac{1}{t^{k+j}}.$$

Here we use that $\sum \theta^j$ is 0 if $q - 1$ does not divide j and is -1 if $j > 0$ is divisible by $q - 1$. Note that the sum starts with $j = 1$ rather than $j = 0$, because the $j = 0$ contribution is $\sum 1 = q = 0$, as we are in characteristic p.

When $q = 2$, $s_1(k) = k + 2^{\mathrm{ord}_2(k)}$ as can be seen directly from this or by reducing, using 2.2.4, to k odd, when $j = 1$ clearly works.

3.2. Recursion in d

Consider the calculation

$$S_{d+1}(k) = \sum_{n \in A_d+, \theta \in \mathbb{F}_q}\frac{1}{(tn + \theta)^k} = -\sum_{j=1,(q-1)|j}^{\infty}\binom{-k}{j}\frac{S_d(k+j)}{t^{k+j}}.$$

As we see from the $d = 1$ case above, the binomial coefficients are zero for $j < s_1(k) - k$, so we can replace j by $s_1(k) - k + j$. Consider

Hypothesis (H2). When q is a prime, '$\min s_{d-1}(s_1(k) + j) + s_1(k) + j$, where the minimum is taken over $j \geqslant 0$, with $(q - 1) \mid j$ and $\binom{s_1(k)+j-1}{k-1}$ non-zero modulo p, is unique and occurs at $j = 0$'.

If it holds, then we have the *main recursion formula* (for q a prime):

$$s_d(k) = s_{d-1}\big(s_1(k)\big) + s_1(k). \tag{1}$$

Using this iteratively leads to (for q a prime)

$$s_d(k) = s_1^{(d)}(k) + \cdots + s_1^{(2)}(k) + s_1(k), \tag{2}$$

where $s_1^{(i)}$ is the ith iteration of s_1 map.

We do not yet know whether Hypothesis (H2) holds, but we will prove this recursion in Theorem 1 for any prime q and $k \in \mathbb{Z}$.

3.2.1. By 2.2.4, the recursion works for $k = m$ if and only if it works for all $k = mp^n$.

3.3. Reformulation for $q = 2$

When $q = 2$, combining the formula (at the end of 3.1) for $s_1(k)$ with our recursive formula for s_d we can describe $s_d(k)$ as follows:

Consider the base 2 expansion of k written in the usual way, except for the infinitely many zeros at the left end. Let 2^{e_0} be the place value of the first one from the right, 2^{e_1} be the place value of the first zero to its left and $2^{e_{i+1}}$ be the place value of the next zero to the left of the zero corresponding to e_i. In other words, the base 2 expansion of k looks (with the subscripts corresponding to the exponents of the place value, and where some of the in–between strings of 1's or 0's can be empty) like

$$k = \cdots 0_{e_{m+1}} 0_{e_m} 1 \cdots 10_{e_3} 1 \cdots 10_{e_2} 1 \cdots 10_{e_1} 1 \cdots 11_{e_0} 0 \cdots 0.$$

Then $s_1^{(i)}(k) = k + 2^{e_0} + \cdots + 2^{e_{i-1}}$ and so

$$s_d(k) = dk + d2^{e_0} + (d-1)2^{e_1} + \cdots + 1 * 2^{e_{d-1}}.$$

3.3.1. Remark

Note that when $d \geqslant k$, the terms can be combined by arithmetic geometric sum formula, since e_i's all increase by one at each step eventually, so the number of terms does not grow with d, as it seems at first.

4. Proof of the recursion (1) for any prime q and $k \in \mathbb{Z}$

We first recall some facts about $S_d(k)$ for k negative. See [8, 5.6] for more on this, Carlitz generating function, special evaluations and references to earlier works by Carlitz, Lee, Goss, Paley, Gekeler etc.

4.1. Carlitz, Diaz-Vargas, Poonen, Sheats result

Put $y = -k$. Then y is positive. We have

$$S_d(k) = \sum_{f_i \in \mathbb{F}_q} \left(t^d + f_{d-1}t^{d-1} + \cdots + f_0\right)^y = \sum \binom{y}{m_0, \ldots, m_d} \left(t^d\right)^{m_0} \cdots (f_0)^{m_d}.$$

Using this, Carlitz, without full justification, gave the following non-vanishing criterion for $S_d(k)$:

(C1) $S_d(k)$ is non-zero if and only if there is decomposition

$$y = m_0 + \cdots + m_d \text{ without carry over base } p, m_i \in \mathbb{Z}_{\geqslant 0}, \quad \text{for } 1 \leqslant i \leqslant d,\ (q-1) \mid m_i > 0.$$

It was noticed in [7] that Carlitz argument also gives

(C2) $-s_d(k) = \max(dm_0 + \cdots + m_{d-1}) = -dk - \min(m_1 + \cdots + dm_d)$, where the minimum is among the lists of m_i's as in (C1).

This is assuming (as Carlitz does) that there is unique maximum. After Daqing Wan's proof [10] of Riemann hypothesis for Carlitz–Goss zeta function for $\mathbb{F}_p[t]$, the author realized that $\mathbb{F}_q[t]$ case can be reduced easily to this assertion. It was justified in Diaz-Vargas thesis (see [3,4,8]) for $q = p$ and later by Sheats [6] in full generality. The general q case turned out to be much more difficult and combinatorially involved than the p case! They proved (in the $q = p$ case and in general respectively), as Carlitz hinted, that

(C3) The maximum in (C2) is unique and is given by the 'greedy' algorithm, namely: arrange possible sets of m_i's in (C1) as $m_d \leqslant m_{d-1} \leqslant \cdots \leqslant m_1$ and then choose one with minimum m_d, then among those with minimum m_{d-1} and so on.

For the proof of Theorem 1, we only need easier $q = p$ case.

Theorem 1. *Let q be a prime. Let $k \in \mathbb{Z}$ and $d > 0$. Then we have*

$$s_d(k) = s_{d-1}\big(s_1(k)\big) + s_1(k),$$

where both sides are either finite or both infinite (*see* 2.2.3).

Proof. We deal with general prime power q and point out exactly which parts of the argument need q to be a prime. The rest of the arguments work for general q.

The trivial case $k = 0$ is taken care by 2.2.3, as both sides are then infinite. For $k \neq 0$, we will make heavy use of (C1)–(C3) above, without specific mention at each instance of the use. We denote by $\oplus$ sum without carry over base p.

(I) Let us first consider $k < 0$ and $y = -k > 0$.

First we look at the case when some term can be infinite.

(i) If $s_1(k)$ is infinite, then there is no m_0, m_1 valid decomposition, and thus no decomposition for higher d also and thus $s_d(k)$ is also infinite. (Alternately, use 2.2.5.)

Now assume $s_1(k)$ is finite and let $y = \overline{m}_0 \oplus \overline{m}_1$ be the corresponding greedy decomposition, so that $s_1(k) = \overline{m}_0$.

(ii) If $s_{d-1}(s_1(k))$ is finite corresponding to greedy decomposition $\overline{m}_0 = \bigoplus_0^{d-1} m_{0i}$, then $y = \bigoplus m_{0i} \oplus \overline{m}_1$ is a valid decomposition so that $s_d(k)$ is finite.

(iii) Finally we claim that if q is a prime and $s_d(k)$ is finite, then $s_{d-1}(s_1(k))$ is finite and the equality of the Theorem holds.

Let $\bigoplus_0^d m_i$ be the optimum (greedy) decomposition of y corresponding to $s_d(k)$. First $m_d = \overline{m}_1$, since otherwise by the greedy property, $m_d > \overline{m}_1$, and then we get a contradiction as we can exchange then two appropriate p-powers between m_d and the rest lowering the minimum m_d. Note that (see [8, p. 180] for very similar argument) such an exchange retains $\oplus$ and also divisibility by $q-1$, as $p^i \equiv p^j$ modulo $q-1$, as $q = p$. So we get $m_d = \overline{m}_1$ and also $\overline{m}_0 = m_0 \oplus \cdots \oplus m_{d-1}$ is the optimum greedy decomposition corresponding to $s_{d-1}(s_1(k))$. The claimed equality follows by using (C2).

We remark that the recipe to find the optimum decomposition (when q is prime) is just that one fills up $m_d, m_{d-1}, \ldots, m_1$ in that order by putting $p-1$ lowest possible p powers each in order corresponding to the base p digits of y and the remaining part of y (if any) is m_0.

(II) Now consider $k > 0$. Now

$$\begin{aligned} S_d(k) &= \frac{1}{t^{dk}} \sum \left(1 + \frac{f_1}{t} + \cdots + \frac{f_d}{t^d}\right)^{-k} \\ &= \frac{1}{t^{dk}} \sum \binom{-k}{y} \left(\frac{f_1}{t} + \cdots + \frac{f_d}{t^d}\right)^{y} \\ &= \frac{1}{t^{dk}} \sum \binom{-k}{y} \sum \binom{y}{m_1, \ldots m_d} \left(\frac{f_1}{t}\right)^{m_1} \cdots \left(\frac{f_d}{t^d}\right)^{m_d}. \end{aligned}$$

Since $\binom{-k}{y} = \pm\binom{k+y-1}{y}$, the only y's that contribute are such that the sum $(k-1)+y$ has no carry over base p and the inner sum contribution comes from m_i such that $y = \bigoplus_1^d m_i$ with m_i positive and divisible by $q-1$.

In this case, y varies among the multiples of $q-1$, but it is big enough so that decompositions exist and by minimization it is small enough so that 'm_0' in the notation above is zero. For each such y, there is unique optimum decomposition by (C1)–(C3).

Thus $s_d(k) = dk + m_1 + \cdots + dm_d$ with m_i's corresponding to the unique minimum, when there is one. Consider n large enough so that $s_d(k - q^n)$ is finite, as the corresponding decomposition as in (C1)–(C3) of $q^n - k$ exists. Then as $(q^n - k) + (k-1) = q^n - 1$ is the sum with no carry over giving 'complementary' digits, so that we see that same decomposition m_i's ($i > 0$) can be used both in (I) and (II) for the two numbers, and hence by Sheats result there is a unique minimum giving similar recipe for $s_d(k)$ with positive k.

When q is a prime, we can do better directly: all p-powers (i.e., place values in the expansions) being congruent to one modulo $q-1$, if each $m_d, m_{d-1}, \dots, m_1$ is filled in order using $p-1$ of lowest possible p-powers to add to $k-1$ without carry over, we clearly reach the unique minimum.

So if q is a prime, $s_1(k) = k + \overline{m}_1$, we consider $(k-1) + \overline{m}_1 + y'$ with $y' = \bigoplus_1^{d-1} m'_i$ optimum decomposition corresponding to $s_{d-1}(s_1(k))$, then we have $m_d = \overline{m}_1$ and $m_i = m'_i$, for $1 \leqslant i \leqslant d-1$.

$$\begin{aligned} s_{d-1}\big(s_1(k)\big) + s_1(k) &= \big((d-1)s_1(k) + (d-1)m'_{d-1} + \cdots + m'_1\big) + (k + \overline{m}_1) \\ &= dk + d\overline{m}_1 + (d-1)m'_{d-1} + \cdots + m'_1 \\ &= s_d(k), \end{aligned}$$

as claimed. □

As pointed out in this proof, optimal m_i's ($i > 0$) match for k and $q^n - k$ and thus comparing the formulas for s_d at negative and positive powers mentioned above, we immediately see 'duality' result as follows.

Theorem 2. *Let $k > 0$, q be a prime power, then we have*

$$\big|s_d(-k)\big| + \big|s_d\big(q^n - k\big)\big| = dq^n, \quad \textit{for } q^n > k,$$

if $s_d(-k)$ is finite. In particular, under these conditions we have $s_d(q^{n+m} - k) - s_d(q^n - k) = d(q^{n+m} - q^n)$.

5. Applications to zeta zero distribution and multizeta

5.1. Applications to zeta zero distribution

The Carlitz–Goss zeta values are in fact special values of Goss zeta function defined on $C_\infty \times \mathbb{Z}_p$. We refer to [4, Ch. 8], [8, 5.5, 5.8] for the definitions, motivation and discussion. Its zeros, for a fixed value of the second variable (in $\mathbb{Z}_p$), can a priori lie in the 'complex plane' C_∞, but do lie on the 'real line' K_∞. This analog of the Riemann hypothesis in this case was proved in [3,6,10], see also [4,8].

Theorem 3. *The analog of Riemann hypothesis for $\mathbb{F}_p[t]$ follows easily from recursion* (1)*.*

Proof. We claim that $2s_d(k) < s_{d-1}(k) + s_{d+1}(k)$ or equivalently the jump inequality $s_d(k) - s_{d-1}(k) < s_{d+1}(k) - s_d(k)$: The formula (1) reduces this statement to the statement with d replaced by $d-1$ and k replaced by $s_1(k)$, and the base case $2s_1(k) < s_0(k) + s_2(k) = s_2(k) = s_1(s_1(k)) + s_1(k)$ is equivalent to $s_1(k) < s_1(s_1(k))$. This is clear since $s_1(k) > k$ for any k from any of the above descriptions. This proves the claim.

As explained in the references above, e.g. [8, 5.8], our analog of the Riemann hypothesis follows from this degree jump behavior, because it implies that the Newton polygon for Carlitz–Goss zeta function has slopes increasing at every integral step and hence has simple zeros in K_∞ (analog of the set of real numbers), rather than its algebraic closure where they would be a priori. □

5.1.1. Remark

Since the analog of the Riemann hypothesis is already known as mentioned before, the only point of this theorem is that it is an easy consequence of (1) and easy, different proof of (1) would thus give an easy and different proof for it. We provide in Section 8 such a proof for $q = 2$ only and our general proof unfortunately uses ideas of Carlitz, Sheats etc. in the original proof. Proof of our theorem also shows that rather than actual (initial) value of s_1, it is the recursion that implies the zero distribution. And plausibly some direct recursion for general prime power q case might simplify the proof by Sheats.

5.2. Applications to multizeta values

In contrast to the case of the Riemann zeta and the Euler multizeta values at positive integers, where they are defined as sums of positive terms and thus are non-zero, in the function field case, the non-vanishing is not obvious. Indeed, the Carlitz–Goss zeta, at negative integers, are also given by sums, but vanish for negative 'even' integers. At positive k, $\zeta(k)$ does not vanish for the simple reason that $d=0$ term, being 1, is of degree zero, whereas the terms for $d>0$ are of negative degree and thus there is no chance of cancellation. For the depth two multizeta (i.e., with $r=2$ in 2.2.2), similarly, we can see using 2.2.5, that the $d_2=0$, $d_1=1$ term is the only term of the largest degree and thus these values are non-zero.

Theorem 4. *The multizeta values $\zeta(s_1,\ldots,s_k)$, with $s_i>0$, are never zero.*

Proof. When q is a prime, the recursion formula (1) implies strict monotonicity in d of $s_d(k)$, namely $s_d(k)<s_{d+1}(k)$. This is because the formula reduces the statement for d, to the statement for $d-1$ (and with k replaced by $s_1(k)$), and the base case $d=0$ is clear.

This proves the non-vanishing of the multizeta values defined above by showing that they have the degree of the 'lowest' term.

We can deduce the general case by either (i) appealing to the formula in the proof of Theorem 1 for $s_d(k)$: Taking d components of the minimal decomposition corresponding to $s_{d+1}(k)$ gives valid decomposition for d and thus gives the contribution at least that of minimal one, thus we get $s_{d+1}(k)>s_d(k)$ again, (ii) appealing to Riemann hypothesis inequality $s_{d+1}(k)-s_d(k)>s_d(k)-s_{d-1}(k)$ noted above together with the obvious base case $s_1(k)-s_0(k)>0$ for $k>0$. □

6. Degree bounds and divisibilities

6.1. General q, $k>0$

Trivial bounds for $s_d(k+1)$ are

$$\max\big((k+1)d, q\big(q^d-1\big)/(q-1)\big)\leqslant s_d(k+1)\leqslant (k+1)q\big(q^d-1\big)/(q-1)$$

where the right inequality follows from the second generating function formula (and $k=k_0$ term), the first term of the left inequality follows by looking at terms in the definition of $S_d(k+1)$ and the second term by noting that in the first generating formula, we have terms of negative degree.

We can do a little better by looking more closely at second generating function in whose notation

$$\begin{aligned} s_d(k+1) &\geqslant (k+1)q\frac{q^d-1}{q-1}-\max\sum k_i\left(q^{d+1}\frac{q^i-1}{q-1}-iq^i\right)\\ &=\min\left(\frac{q^{d+1}}{q-1}\left(1+\sum k_i\right)+\sum ik_iq^i\right)-\frac{(k+1)q}{q-1} \end{aligned}$$

since $\sum k_iq^i=k$. Here the minimum is over all the decompositions $k=\sum_{i=0}^d k_iq^i$, with no carries in the sum of k_i's base p, i.e., multinomial coefficient of $\sum k_i$ with respect to k_i's is non-zero modulo p.

(1) Here $\sum k_i$ is at least the sum $\ell(k)$ which is the sum of the digits base q of k.
(2) The inequality is equality, e.g. if the maximum is unique, i.e., under Hypothesis (H1) of 2.3.1.
(3) Once d is large enough, choice of k_i's is independent of d and, e.g. if the maximum is unique we thus get a clear asymptotics in d.

The upper and lower bound is best possible as $k=q^m$ shows.

When $d \geqslant 1$ is fixed and k can be large, $s_d(k) > dk$ is better than the other lower bound. (Note that for $d = 0$ we have equality, but for $d \geqslant 1$ we can claim strict inequality as the leading degree contribution occurs multiple of characteristic times.) In fact, by 3.1, we have $s_1(k) \geqslant k + (q-1)$. By 3.2, iteration of this gives $s_d(k) \geqslant dk + d(d+1)(q-1)/2$, for q prime, from our main recursion. For $q = 2$, $s_d(k) \geqslant ds_1(k) \geqslant d(k+q-1)$ by 2.2.5 and 3.1.

6.2. When $q = 2$, $k > 0$

Let $q = 2$. For k odd, $s_1(k) = k + 1$ (we have $s_1(k) \geqslant k + q - 1$ in general) and thus the inequality $ds_1(k) \geqslant d(k + q - 1)$ is best possible for $d = 1$. For all k of the form $4n + 1$, $s_2(k) = 2k + 4$. More generally, our formula in terms of e_i's shows that

$$s_d(k) = dk + d + (d-1)2 + (d-2)2^2 + \cdots + 1 * 2^{d-1} = dk + 2\big(2^d - 1\big) - d, \quad \text{if } k = 2^d n + 1,$$

and that the right side is thus the best lower bound in general for $s_d(k)$ when $q = 2$. For an upper bound, we have $s_1(k) \leqslant 2k$, with equality for k a power of 2. So using the iteration formula, $s_1^{(i)}(k) \leqslant 2^i k$ and so $s_d(k) \leqslant 2(2^d - 1)k$, with equality for the k a power of 2 agreeing as it should with what we get for generating function approach. In summary, we have

Theorem 5.

$$dk + 2\big(2^d - 1\big) - d \leqslant s_d(k) \leqslant 2\big(2^d - 1\big)k, \quad \textit{if } q = 2,$$

with each inequality being an equality for infinitely many k's.

6.3. Asymptotic in d for a fixed $k > 0$

There are only finitely many choices for $k_i > 0$, where k_i are as in 2.3 and thus for d large, $s_d(k)$ is asymptotic to $q^{d+1}/(q-1)(1 + \sum k_i)$, e.g., if Hypothesis (H1) of 2.3.1 holds and there is no clash for maximum degree contribution.

6.4. Divisibility by q

We have seen (2.3.1 Remark (3)) that q divides $s_1(k)$. The main recursion (1) (or also Hypothesis (H1), i.e., equality in the second displayed formula in 8.1) implies that q divides $s_d(k)$, if q is a prime.

6.5. Congruence conditions

We have seen that $s_1(k)$ is congruent to k modulo $q - 1$. So the recursion relation implies that $s_d(k)$ is congruent to dk modulo $q - 1$, when q is a prime. (This fact easily generalizes to any q, by the recipe for $S_d(k)$ given in the proof of Theorem 1, as m_i are divisible by $q - 1$ there.)

Combining the above two, we get

Theorem 6. *We have $s_d(k) \equiv dk \bmod (q-1)$, for $d \geqslant 0$ and $k > 0$, and further q divides $s_d(k)$ if q is a prime.*

The referee points out following nice easy consequence of the recursion (1) and (2) which follows directly by induction.

Theorem 7. *We have $s_1^{(i)}(k)$ is divisible by q^i and $s_d(k) - s_{d-1}(k)$ divisible by q^d, when q is a prime.*

7. Applications to sum shuffle relations for multizeta

7.1. In the study of multizeta identities, we are interested in when sum shuffle $\zeta(a)\zeta(b) = \zeta(a+b) + \zeta(a,b) + \zeta(b,a)$ works and in particular when it works term by term (for motivation and reason for this, see [9]), or equivalently when $S_d(a)S_d(b) = S_d(a+b)$. We know that this works when $a = b$ and $p = 2$, or when $a + b \leqslant q$ for example. There are other examples known, when $q > 2$. For example, $q > p$, $a = q - 1$, $b = p + 1$.

Theorem 8. *When $q = 2$, $S_d(a)S_d(b) = S_d(a+b)$ if and only if $a = b$.*

Proof. In fact, we show a priori stronger statement that $s_d(a) + s_d(b) = s_d(a+b)$ for all d implies that $a = b$. For $d = 1$, our $q = 2$ formula in 3.1 for $s_1(k)$ and the hypothesis imply that ord_2 is the same for both a and b. In other words, in the notation above, e_0's are the same. The $d = 2$ equality then implies that s_1's of a and b are the same, which means e_1 are the same and so on, so that $a = b$. □

7.2. The easiest sum shuffle source in general comes when $i = a, b$ satisfy $S_d(i) = 1/\ell_d^i$.

Theorem 9. *Consider the following statements*:

(i) $S_d(k+1) = 1/\ell_d^{k+1}$,
(ii) $s_d(k+1) = (k+1)q(q^d - 1)/(q-1)$,
(iii) $s_d(k+1) \geqslant (k+1)q(q^d - 1)/(q-1)$,
(iv) $k + 1 = cq^n$, *with* $0 < c < q$, $n \geqslant 0$,
(v) *whenever* $k = \sum k_i q^i$, $k_i \geqslant 0$, $k_0 \neq k$, *there is a carry over base p in* $\sum k_i$.

Then (v) $\Rightarrow$ (iv) $\Rightarrow$ (i) $\Rightarrow$ (ii) $\Leftrightarrow$ (iii).

Under Hypothesis (H1) *of* 2.3, *i.e., assuming that the maximum degree term is unique in decomposition for $S_d(k+1)$ in* 2.3, (ii) $\Rightarrow$ (i) $\Rightarrow$ (v), *so that all the statements are equivalent.*

Proof. (v) implies (iv): Notice that we can take the p-powers out, so it is enough to prove that if (v) holds for $k+1$ not divisible by p, then $k + 1 \leqslant q$. So assume $k + 1 > q$ and let $\sum a_j q^j$ be the base q expansion of k. Then there is $j \geqslant 1$ with $a_j > 0$. Then the sum of $k_j = 1$ and $k_0 = k - q^j$ has no carry over base p, as $a_0 \neq p - 1$ by the assumption.

(iv) implies (i): Use 2.2.4 and 2.3.

(i) implies (ii): It is straight degree calculation and (ii) is equivalent to (iii) follows from the trivial bounds in 6.1.

Assuming unique maximum, the claims follow as then there is unique contribution corresponding to $k_0 = k$. □

8. Direct proof of (1) when $q = 2$, $k > 0$ and equivalent formulas

8.1. Direct proof of the recursion when $q = 2$, $k > 0$

Theorem 10. *When $q = 2$, $k > 0$, the recursion* (1) *holds, i.e., $s_d(k) = s_{d-1}(s_1(k)) + s_1(k)$.*

Proof. We prove (1), when $q = 2$, by proving the minimizing condition in 3.2. In fact, using (2), it is enough to show that $s_1^{(i)}(s_1(k) + j) \geqslant s_1^{(i)}(s_1(k))$ for j's as in the condition.

In terms of the expansion of k as in 3.3, we have

$$k - 1 = \cdots 0_{e_{m+1}} 0_{e_m} 1 \cdots 10_{e_3} 1 \cdots 10_{e_2} 1 \cdots 10_{e_1} 1 \cdots 10_{e_0} 1 \cdots 1,$$

$$s_1^{(i)}(k) = \cdots 0_{e_{m+1}} 0_{e_m} 1 \cdots 0_{e_{i+1}} 1 \cdots 11_{e_i} 0 \cdots 0.$$

So the binomial non-divisibility condition that $\binom{s_1(k)+j-1}{k-1}$ is odd, allows us, by Lucas theorem, to restrict positive j's to j such that

$$s_1(k)+j-1=\cdots *_{e_{m+1}} *_{e_m} 1\cdots\cdots 1 *_{e_3} 1\cdots 1 *_{e_2} 1\cdots 1 *_{e_1} 1\cdots 1 *_{e_0} 1\cdots 1$$

where $*$ can either stand for a 0 or 1 with at least one $*$ being 1 at e_uth place with $u \geqslant 1$ (since it is at least $s_1(k)$). (Note $j \geqslant 2^{e_0}$.)

Consider the three cases (i) $*_{e_0}=0$, (ii) $*_{e_0}=1, *_{e_1}=0$ and (iii) $*_{e_0}=1, *_{e_1}=1$.

Now note that by 3.1, $s_1^{(i)}$ applied successively to $s_1(k)=k+2^{e_0}$ adds to it $2^{e_1}, 2^{e_2}, \ldots$ in turn.

In the first case,

$$s_1(k)+j=\cdots *_{e_1} 1\cdots 1_{e_0} 0\cdots 0$$

so that $s_1^{(i)}$ applied successively to $s_1(k)+j \geqslant k+2^{e_u}$ adds in turn $2^{e_0}, 2^{e_1}, \ldots, 2^{e_u-1}$ and then at least 2^{e_u+1} and so on.

In the second case, $s_1(k)+j=\cdots 1_{e_1} 0\cdots 0$, so that we add successively 2^{e_1} and at least $2^{e_2}, \ldots.$

In the third case, we add at least $2^{e_2}, \ldots.$

So in each case, the claimed inequality follows and hence the unique minimum is at $j=0$ and the recursion formula (1) is proved when $q=2$. □

8.2. The inequality needed above for the analog of the Riemann hypothesis can be checked directly from the formula for $s_d(k)$ in 3.3 and it shows that the difference between the two sides is in fact 2^{e_d}.

8.3. Equivalent formula

(This formula, and its generalization in the next section for prime q, was found by Greg Anderson, by computer experimentation trying to solve a recursion in k.)

Theorem 11. *We have, when $q=2$, $k>0$,*

$$s_d(k+1)=2^{d+1}-2^d+\sum\bigl(\min(e_i-i+1,d)-2\bigr)2^{e_i}+2^{\max(e_i+1,d+i)},$$

where the notation now is $k=\sum_{i=1}^{\ell(k)} 2^{e_i}$, with $0 \leqslant e_1 < e_2 < \cdots.$

Proof. We need only check that right side satisfies the recursion (1). Using 2.2.4, it is sufficient to check for k even, when $k+1=\sum_{i=1}^{\ell(k)+1} 2^{e_i'}$, with $e_1'=0$ and $e_i'=e_{i-1}$ for $i>1$. So it is sufficient to check that the right side of the displayed formula above is the same as $k+2+s_{d-1}(k+2)$, which is $\sum 2^{e_i}+2+2^d-2$ plus the $\sum$ above with e_i replaced by e_i' and d replaced by $d-1$. This sum has $-2+2^d$ as a contribution from e_1' term and $\sum_{i=2}^{\ell(k)+1}((\min(e_{i-1}-i+1,d-1)-2)2^{e_{i-1}}+2^{\max(e_{i-1}+1,d-1+i)})$ which matches perfectly, when you re-index i to $i-1$. □

8.3.1. Remark

By Remark 3.3.1, we see that the number of terms in the formula for $s_d(k)$ given in 3.3 is the number of zeros in the base 2 expansion of k to the left of the first one from the right, whereas the number of terms in the formula above (when rewritten for $s_d(k)$ rather than for $s_d(k+1)$ for better comparison) is the number of 1's in the base 2 expansion of $k-1$.

9. Equivalent formulas for prime *q*

While the formulas explained for $s_d(k)$ in the proof of Theorem 1 are very simple and efficient for prime q, here we discuss another formula.

9.1. The case $d = 1$

Let q be a prime and let us temporarily write u and v for best k_0, k_1 as in 2.3.1, remark (3), so that $k = vq + u$ and $s_1(k+1) = (u + v + 1)q$. Let $m = \sum m_i q^i$ be the base q expansions of m, so that now k_i (u_i, v_i respectively) stands for ith digit of the base q expansion of k (u, v respectively). Here is a recipe to find u, v and hence $s_1(k)$:

Claim. *$u_0 = k_0$ and $u_j = k_j - \min(q - 1 - u_{j-1}, k_j)$. (Note that when u_j is zero for some j, then it is zero for higher j's.)*

Proof. This follows from $u_j + v_j < q$ and $u_j + v_{j-1} = k_j$ as we now show (this does not generalize to non-prime case, see the last section): We have to rule out the only other possibility that $u_j + v_{j-1} = k_j + q$. Let j be smallest such that this happens. Then changing u and v by only replacing v_j by $v_j + 1$, u_j by zero and v_{j-1} by k_j is legal:

(i) $v_i + 1$ is legitimate digit, since otherwise $v_j = q - 1$ and thus $u_j = 0$ making assumed carry over impossible.

(ii) Earlier sums are preserved: earlier $u_{j+1} + v_j + 1$ where 1 was from carry over is now the same digit sum without carry over.

But this change decreases u contrary to the minimality assumption. □

9.2. Another formula for $d = 1$

We continue to assume that q is a prime. We now show that this formula is equivalent to

$$s_1(k+1) = q + q \sum_{e_i'=0} q^{e_i} + \sum_{e_i'>0} q^{e_i}$$

where we write $k = \sum_{i=1}^{m} q^{e_i}$, with e_i monotonically increasing with i and no more than $q - 1$ consecutive values being the same and where

$$e_i' = e_i - \left\lfloor \frac{i-1}{q-1} \right\rfloor.$$

This recipe is equivalent to the one above, because u prescribed above is the same as $\sum q^{e_i}$ where the sum is over i such that $e_i' = 0$ and $e_i' > 0$ exactly when q^{e_i} can be forced into v-part satisfying the carry-over restrictions.

9.3. Formula for general d and equivalence to recursion

Theorem 12. *Let $q = p$ be prime. Let $k > 0$ and let e_i, e_i' be defined as above. Then recursive formula (1) is equivalent to*

$$s_d(k+1) = \frac{q^{d+1} - q}{q-1} + \sum \left(\min\left(e_i', d\right) + \frac{q}{q-1}\left(q^{\max(d - e_i', 0)} - 1\right) \right) q^{e_i}.$$

Proof. Since in the last subsection, we have checked that the starting case $d = 1$ of the recursion agrees with the claimed formula which is therefore correct in the case, to show the equivalence it is enough to show that the formula above satisfies the recursion. So we want to show that with $s_d(k)$ defined by this formula, we have $s_d(k+1) - s_1(k+1) = s_{d-1}(s_1(k+1))$.

Let $\bar{e}_i$ and $\bar{e}_i'$ be defined as e_i and e_i' respectively when k is replaced by $s_1(k+1) - 1$.

The left side of the claimed equality is

$$\left[\frac{q^{d+1}-q}{q-1}-q\right]+\frac{q(q^{d-1}-1)}{q-1}\left(\sum_{e_i'=0}q^{e_i+1}+\sum_{e_i'=1}q^{e_i}\right)+\sum_{e_i'>1}\left(\min(e_i',d)-1+\frac{q(q^{\max(d-e_i',0)}-1)}{q-1}\right)q^{e_i}$$

whereas the right side is

$$\left[\frac{q^d-q}{q-1}\right]+\frac{q(q^{d-1}-1)}{q-1}\sum_{\bar{e}_i'=0}q^{\bar{e}_i}+\sum_{\bar{e}_i'>0}\left(\min(\bar{e}_i',d-1)+\frac{q}{q-1}\left(q^{\max(d-1-\bar{e}_i',0)}-1\right)\right)q^{\bar{e}_i}.$$

Now the difference between the square bracket terms is $q(q^{d-1}-1)/(q-1)$ times $q-1$. We have $s_1(k+1)-1=\sum_{e_i'=0}q^{e_i+1}+\sum_{e_i'>0}q^{e_i}+q-1$.

We see from the recipe above that the sequence of $\bar{e}_i$'s is obtained by appending to $q-1$ first zeros the sequence of e_i's and by replacing e_i by e_i+1 whenever $e_i'=0$. This results into shifting by $q-1$ of the indexing of i's in e_i to $\overline{e_i}$ correspondence, which causes extra subtraction of 1 in calculating $\bar{e}_i'$ whenever corresponding $e_i'>0$. When $e_i'=0$, $\bar{e}_i$ is obtained by increasing by 1, so $\bar{e}_i'=0$.

The two sides are thus equal by matching the terms as follows: (i) The $q-1$ difference coming from square brackets matches with the 0th digit of $s_1(k+1)-1$, i.e., the first $q-1$ $\bar{e}_i$'s which are zero. (ii) The terms with $e_i'>1$ match with $\bar{e}_{i+q-1}'=e_i'-1>0$ and $e_i=\bar{e}_{i+q-1}$. (iii) The terms with $e_i'=0,1$ match with those with $\bar{e}_i'=0$: In more detail, $e_i+1=\bar{e}_{i+q-1}$ when $e_i'=0$ and $e_i=\bar{e}_{i+q-1}$ when $e_i'=1$. □

9.4. Recursion in k for $s_1(k)$

Theorem 13. *For general q, and $k>0$, we have $s_1(k+1)=k+q$, if q divides k. Let $q=p$ be a prime. If q does not divide k, then $s_1(k+1)=s_1(k)+q^{\mathrm{ord}_q(s_1(k))}$.*

Proof. We use 2.3. The first statement is proved there in the remark (3). For notational convenience, we replace k by $k+1$, and write $k=k_1q+k_0$ and $k+1=\bar{k}_1q+\bar{k}_0$ for the minimum decompositions in the notation of the remark. Let $r:=\mathrm{ord}_q(s_1(k+1))$. Then we have $s_1(k+1)=(k_1+k_0+1)q$ exactly divisible by q^r. Hence the 'no carry over' and 'minimization' conditions imply that $\bar{k}_0=k_0+q^{r-1}+\cdots+1$. (Here we use that since q does not divide $k+1$, by hypothesis, the last digit of k is not $q-1$ and can be increased by one). Thus $s_1(k+2)=(\bar{k}_1+\bar{k}_0+1)q=s_1(k+1)+q^r$ as claimed. □

Acknowledgments

I thank the Ellentuck Fund and the von Neumann Fund for their support for my stay during Spring 2008 at the Institute for Advanced study, Princeton, where most of this paper was written. I thank Noam Elkies for helping with my baby steps at programming the small computations, Angelo Mingarelli and Robert Israel for help with maple syntax, David Roe and Alejandro Lara Rodriguez for much more extensive check of the conjectural formula using SAGE, for general q and for equivalent version for prime q in Section 9 respectively and Gebhard Boeckle for pointing out peculiarities of $q=4$, $k=-181$ that he found during the computer verifications and simplifications of the formulas for the zeta values developed using Taguchi–Wan–Anderson–Pink–Boeckle cohomological approach. I am also grateful to Greg Anderson for communicating and allowing me to use in Theorem 12 the formula he found. I thank the referee for the suggestions to improve the exposition.

Appendix A. Special evaluations and observations

In this appendix, we collect some special examples, counterexamples, observations and open questions for the benefit of the reader.

A.1. Special simple evaluations of $S_d(k)$, $k > 0$

Here are some special cases of 2.3:

$$S_d(a) = 1/\ell_d^a, \quad 0 < a \leqslant q,$$

$$S_d(q+b) = \frac{1}{\ell_d^{q+b}}\left(1 - b\frac{[d]^q}{[1]}\right), \quad b < q,$$

$$S_d(aq+b) = \frac{1}{\ell_d^{aq+b}}\left(1 + \sum_{j=1}^{a}(-1)^j \binom{b+j-1}{j}\frac{[d]^{jq}}{[1]^j}\right), \quad 0 < a, b < q,$$

$$S_d\left(q^2+1\right) = \frac{1}{\ell_d^{q^2+1}}\left(1 + \sum_{j=1}^{q}(-1)^j\frac{[d]^{jq}}{[1]^j} + \frac{[d]^{q^2}[d-1]^{q^2}}{[2][1]^q}\right).$$

The following is a little harder to prove directly, but follows from straight manipulations. (See also [9].)

$$S_d\left(q^i - 1\right) = \frac{\ell_{d+i-1}}{\ell_{i-1}\ell_d^{q^i}} = \frac{[d+i-1]\cdots[d+1]}{[i-1]\cdots[1]\ell_d^{q^i-1}}.$$

A.2. Special simple evaluations of $s_d(k)$, $k > 0$

It follows from simple manipulations from above formulas, with $\deg(\ell_d) = (q^{d+1} - q)/(q-1)$,

(1) $s_d(q^n - 1) = (q^n - 1)\deg(\ell_d) - (q^{d+n-1} + \cdots + q^{d+1}) + (q^{n-1} + \cdots + q) = q^n(q^d - 1)$.

(2) $0 \leqslant a, b < q$, $1 \leqslant aq + b$, $s_d(aq+b) = (aq+b)\deg(\ell_d) - (q^{d+1} - q)\mathrm{Max}\ j$, where the maximum is over $1 \leqslant j \leqslant a$ with $\binom{b+j-1}{j}$ being non-zero.

(A simple corollary is that $s_d(b+1) = s_d(q+b)$, if $b < q$ and b prime to p).

(3) We have $s_d(q^n + 1) = dq^n + q^d + \cdots + q = dq^n + (q^{d+1} - q)/(q-1)$, when $n \geqslant d$, as follows from our minimization formula because the minimum is achieved for $q^n = \sum k_i q^i$, with the conditions above, when $k_d = q^{n-d}$ and with all other $k_i = 0$. Our recursion works under this condition: Since $s_1(q^n+1) = q^n + q = q(q^{n-1}+1)$, the pair (d, n) is taken to $(d-1, n-1)$, so that the inequality is justified.

Note that explicit evaluation above gives $s_d(q^0 + 1) = s_d(q^1 + 1) = 2(q^{d+1} - q)/(q-1)$ (which do not agree with the formula above when $d > n$) and $s_d(q^2+1) = (q^2+1)(q^{d+1} - q)/(q-1) - q^{d+2} - q^{d+1} + 2q^2$, for $d \geqslant 2$ (it works for $d = 1$ but not for $d = 0$).

(4) Let us give a short table for the reader's convenience, when $q = 3$. Note $s_1(3k) = 3s_1(k)$ and $s_1(k) = k + 2$, if k is 1 mod 3.

k	1	2	4	5	7	8	10	11	13	14	16	17	19	20	22	23
$s_1(k)$	3	6	6	9	9	18	12	15	15	18	18	27	21	24	24	27
$s_2(k)$	12	24	24	36	36	72	30	42	42	72	72	108	48	78	78	108

k	25	26	28	29	31	32	34	35	37	38	40	41	43	44	46	47
$s_1(k)$	27	54	30	33	33	36	36	45	39	42	42	45	45	54	48	51
$s_2(k)$	108	216	66	78	78	90	90	126	84	96	96	126	126	216	102	132

k	49	50	52	53	55	56	58	59	61	62	64	65	67	68	70
$s_1(k)$	51	54	54	81	57	60	60	63	63	72	66	69	69	72	72
$s_2(k)$	132	216	216	324	120	132	132	144	144	234	138	150	150	234	234

(4) Here is a short table for $q=4$.

k	1	3	5	7	9	11	13	15	17	19	21	23	29
$s_1(k)$	4	12	8	16	12	32	16	48	20	28	24	32	32
$s_2(k)$	20	60	40	80	60	160	80	240	52	92	120	160	160

A.3. Special $S_d(k)$ and $s_d(k)$ with k negative

Using Carlitz–Lee results [8, 5.6.4]

$$S_d\big(1-\big(q^{a_1}+\cdots+q^{a_s}\big)\big)=\big([a_1]_d\cdots[a_s]_d\big)/\ell_d,$$

where $[a]_m := D_a/D_{a-m}^{q^m}$ if $m \leqslant a$ and 0 otherwise, we have

$$s_d\big(1-\big(q^{a_1}+\cdots+q^{a_s}\big)\big)=q\frac{q^d-1}{q-1}-d\sum q^{a_i},\quad \text{when } s<q, d\leqslant a_i.$$

A.4. $s_d(k)$ with k negative: short tables

We record some values of $s_d(k)$ calculated directly. The dash represents infinite value.

For $q=2$, with k divisible by 2 omitted because of 2.2.4, we have

$-k$	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
$-s_1(k)$	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
$-s_2(k)$	–	2	4	10	8	18	20	26	16	34	36	42	40	50	52	58
$-s_3(k)$	–	–	–	10	–	18	20	34	–	34	36	58	40	66	68	82

For $q=3$, with k divisible by 3 omitted because of 2.2.4, we have

$-k$	1	2	4	5	7	8	10	11	13	14	16	17	19	20	22	23	25
$-s_1(k)$	–	0	0	3	3	6	0	9	9	12	12	15	9	18	18	21	21
$-s_2(k)$	–	–	–	–	–	6	–	–	–	12	12	24	–	18	18	30	30

and the first few finite values for $-s_3$ are $42, 78, 84, 84, 123$ at $-k$ being $26, 44, 50, 52, 53$, respectively.

For $q=4$, with k divisible by 2 omitted because of 2.2.4, we have

$-k$	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
$-s_1(k)$	–	0	–	4	0	8	4	12	–	16	0	20	16	24	20	28	0

and first few finite values for $-s_2$ are $12, 24, 24, 44, 36, 36, 76, 48, 48, 68$ at $-k$ being $15, 27, 30, 31, 39, 45, 47, 51, 54, 55$ respectively, and $-s_3(63) = -108$ is the only finite value for $-k \leqslant 110$. (Note $\ell(63)/3 = 3$.)

A.5. Properties of $s_d(k)$ for $k<0$

We can use the 'duality' to study these properties also. But we proceed directly.

The special case $d=1$ of the Carlitz–Sheats recipe follows directly exactly as in 3.1, i.e., existence of greedy property of minimum is obvious in this case. Thus we have (when finite) $-s_1(k) = \max(m_0)$, where the decompositions $-k = m_0 + m_1$, with $(q-1) \mid m_1 > 0$, have no carry over base p. Thus $s_1(k) \equiv -m_0 \equiv k \bmod (q-1)$ and thus by the recursion we have that $s_d(k) \equiv dk \bmod (q-1)$, when it is finite and q a prime. For general q, the formula for $s_d(k)$ in Section 4 implies this congruence, as m_i are divisible by $q-1$.

Note $s_0(k) \leqslant 0$, $s_1(k) = -m_0 > k$ and also $|s_{d+1}(k)| \geqslant |s_d(k)|$ (when all finite) exactly as in the proof of Theorem 1, when q is a prime.

Finally, we see that q divides $s_d(k)$, when it is finite, and q a prime, as follows.

By looking at $d=1$ case of the Carlitz generating function theorem [8, 5.6.3] (with sign corrections as mentioned in 2.2.3 and with $w = 1/x$, $y = -k$) we see that for $k \leqslant 0$, $S_1(k+1)$ is the coefficient of w^y in $-w^q \sum_{j=0}^{\infty}(w^{q-1} + (t^q - t)w^q)^j$. This implies that $s_1(k+1) = -rq$, where $y - q = rq + (j-r)(q-1)$, with r maximum possible (clearly unique) such that $r, j-r \geqslant 0$ and that there is no carry over base p in the sum $r + (j-r)$, if such decompositions exist. (In particular, if q divides k, $s_1(k+1) = k+q$ parallel to 2.3.1(3).) The assertion for d follows from $d=1$ case by the recursion, exactly as before.

As for the bounds when $s_d(k)$ is finite, we see that when q is a prime, 4.1 implies that $m_i \geqslant (q-1)q^{d-i}$ for $i > 0$ and $m_0 \geqslant 0$, and so

$$(q-1)\sum_{i=1}^{d-1}(d-i)q^{d-i} \leqslant \left|s_d(k)\right| \leqslant |dk| - (q-1)\left(q^{d-1} + 2q^{d-2} + \cdots + d\right) = |dk| - q\left(q^d - 1\right)/(q-1) - d$$

and these bounds are reached when $k = 1 - q^d$. We see that for a fixed d and k large, $|s_d(k)|$ can be as large as $|dk|$ asymptotically, e.g. for $k = 1 - q^{d+m}$, with m large, where $s_d(k)$ is recalled in the next section. Note $s_1(k)$ is zero if k has $q-1$ digits and q is prime, as $k = m_1$ then. (This was proved long ago by Thomas and Goss by another method.)

We collect these facts in

Theorem 14. *Let $k < 0$. Then $s_d(k) \equiv dk \bmod (q-1)$.*
If further q is prime, then

(i) *q divides $s_d(k)$, if it is finite,*
(ii) *$|s_{d+1}(k)| \geqslant |s_d(k)|$, and*
(iii) *$|s_d(k)|$ is bounded as in the displayed formula above, assuming all the values are finite.*

Note that given a d, $|s_d(k)|/|k|$ tends to d as the sum of the base q digits of k tends to infinity, by the recipe (C1)–(C3) of Section 4.

It is known (2.2.3 and 2.2.4) that $S_d(k) = 0$, if $d > L := \min\lfloor \ell(kp^s)/(q-1)\rfloor$. Gebhard Boeckle has informed us that $S_L(k) \neq 0$ follows easily from [6] and also from his cohomological approach.

A.6. Case $q = 4$

Complicated nature of s_1 for general q makes the general case difficult. We discuss s_1 in more detail now.

We do not have a nice 'formula' in general, but the following 'recipe' for $q = 4$ case is almost as simple computationally.

Recipe for $s_1(k+1)$ when $q = 4$.

Case 0, $k+1$ is even: We can take out power of 2 by using 2.2.4, so we assume that $k+1$ is odd. Even when it is even, sometimes it is better to get direct answer. For example,

$$u = 1 \text{ when } k+1 \text{ is } 2 \bmod 8 \quad \text{and} \quad u = 3 \text{ when it is } 4 \bmod 16.$$

Case I, $k+1$ is odd: From the carry over minimization description in 2.3.1, remark (3), it follows immediately that

Sub-case Ia: u is 0 (resp. 2), if $k+1$ is 1 mod 4 (resp. 3 or 7) mod 16.

So we need to look at $k+1$ which are either 11 or 15 modulo 16 only.

Sub-case Ib: $k \equiv 10 = 2^3 + 2$ modulo 16.

For $k = \cdots + 0 * 2^{2\ell+1} + \sum_{i=4}^{2\ell} 2^i + 2^3 + 2$, $\ell \geqslant 2$, we have $u = \sum_{j=3}^{\ell} 2^{2j-1} + 2^3 + 2$.

(This is because 2 is forced into u and if you put 2^2 in it, all even powers are forced and you get a bigger u than claimed, if you do not put 2^2 in then one by one all odd powers up to $2\ell - 1$ are so forced, on the other hand, for this u we have decomposition without carry.)

For $k = \cdots + 0 * 2^{2\ell} + \sum_{i=4}^{2\ell-1} 2^i + 2^3 + 2$, $\ell \geqslant 2$, we have $u = \sum_{j=2}^{\ell-1} 2^{2j} + 2^2 + 2$.

(This is because this u gives good decomposition and if the minimal u has no 2^2 in it, then it has 2^3 and thus all odd powers up to $2\ell - 1$ forced into it and is then not minimum.)

Sub-case Ic: $k \equiv 14 = 2^3 + 2^2 + 2$ modulo 16.

For $k = \cdots + 0 * 2^{\ell+1} + \sum_{i=m}^{\ell} 2^i + 2^3 + 2^2 + 2$, with ℓ even and $m = 4$ or 5, then u is the sum of all odd power of 2 from first to $\ell - 1$th.

For $k = \cdots + 0 * 2^{\ell+1} + \sum_{i=5}^{\ell} 2^i + 2^3 + 2^2 + 2$, with ℓ odd, then u is $2 + 2^3$ plus all higher even powers up to $\ell - 1$th.

Now let ℓ be odd.

For $k = \cdots + 0 * 2^{\ell+2} + 0 * 2^{\ell+1} + \sum_{i=1}^{\ell} 2^i$, we have $u = \sum_{i=0}^{(\ell-1)/2} 2^{2i+1}$.

For $k = \cdots + 0 * 2^{\ell+m+1} + \sum_{i=2}^{m} 2^{\ell+i} + \sum_{i=1}^{\ell} 2^i$, with $m \geqslant 2$, we have $u =$ the sum of all odd powers of 2 up to $2^{\ell+m-1}$, if m is odd and $u =$ the sum of all odd powers up to 2^ℓ plus all even powers from $2^{\ell+1}$ up to $2^{\ell+m-1}$, if m is even.

(Proofs are similar as above. We always use the simple principle that if some u, with highest power 2^ℓ in it, works for a given k then the same u works for k' obtained from k by changing powers higher than $2^{\ell+2}$.)

A.7. Remark on monotonicity

As a function of $k > 0$, $s_d(k)$ may not monotonically increase, as the example $q = 3$, $d = 1$ and $k = 3, 4$ already shows. In fact, if $q = 2$, by 2.2.4, $s_1(2^n) = 2^{n+1}$ and we will see below that $s_1(2^n + 1) = 2^n - 2$.

A.8. Remark on Hypothesis (H1)

First note that since q divides $b(i,d)$, under Hypothesis (H1), we see that q divides $s_d(k)$ for positive k and then by duality (Theorem 2), the same holds for negative k also.

Note though that $qb(i,d) - b(i+1,d) = q^{i+1} - q^{d+1} < 0$, for $i < d$. Hence when we move contribution to $k = \sum k_i q^i$ from higher i term to lower i's, we lose degree. But since we can also simultaneously move up terms from lower i's to compensate, there can be clash of degrees even retaining 'no carry over' condition. Here is an example: Consider the two decompositions $1 * q^6 + q^2 * q^4 + (2q) * q^2$ and $(2q) * q^5 + 1 * q^3 + q^2 * q$ of $k = 2q^6 + 2q^3$ when $q > 2$: There is no carry over in digit sums, but the contributions are the same by the calculation above. Hence, e.g. if $q = 4$, because the degrees match and top coefficients are one (as they are in $\mathbb{F}_p$), the total degree of the two terms is less.

A.9. Remark on Hypothesis (H2)

The minimum in Hypothesis (H2) is not necessarily at $j = 0$ if we drop the binomial coefficient condition: e.g. take $q = d = 2$, $k = 4$, $j = 0, 1$. The uniqueness of minimum and strict increase of $s_d(k)$ as a function of d would have easily followed if $s_d(k) < s_d(k + q - 1) + q - 1$. But this is not true, e.g. for $q = 2$, $d = 2$, $k = 2^d$.

A.10. Hypothesis (H3)

The numerical data suggests

Hypothesis (H3). $s_d(k) < s_d(k+1)$ when k is not divisible by p.

We have proved more refined version of the special case, $d=1$, q prime, in Theorem 13.

A.11. Counter-examples when q is not a prime

The converse of (I)(ii) in proof of Theorem 1 is not true, e.g. if $q=4$, $-k=181$, $d=2$, where $181=160\oplus 21=16\oplus 132\oplus 33$ are greedy decompositions for $d=1,2$ respectively, giving $s_2(k)=164$.

When $q=4$, $d=2$ and k is negative, odd, there are exactly 8 counter-examples to the recursion for $y\leqslant 1000$ with $y=-k$ being 181, $437=256+181$, $565=128+437$, 661, $693=512+181$, 709, 721, $949=512+437$.

There are 'dual' counter-examples at positive k. For example, for $k=75$ the recursion and Hypothesis (H2) fails. (Minimum is at $j=12$ rather than $j=0$.)

In contrast to the prime q case, when q is not a prime, the u and v corresponding to $s_d(k+1)$ as in the last section need not be 'sub-sums' in the expansion of k:

Example. $q=4$, $k+1=11$, $k=2^3+2$, but $u=2^2+2$ giving $s_1(11)=32$. Other such examples when $q=4$ are e.g. when $k+1$ are 43, 47, 59, 75, 107, 139 and 2 power multiples of these examples.

Consider naive generalized formula, when $q=p^f$, for $s_d(k+1)$, namely

$$s_d(k+1)=\frac{q^{d+1}-q}{q-1}+\sum\left(\min\left(e_i',d\right)+\frac{q}{q-1}\left(q^{\max(d-e_i',0)}-1\right)\right)p^{e_i},$$

where $k=\sum_{i=1}^N p^{e_i}$ with monotonically increasing e_i and with no more than $p-1$ consecutive values being the same and with

$$e_i'=\left\lfloor\frac{e_i}{f}\right\rfloor-\left\lfloor\frac{\#\{j: j<i, e_j\equiv e_i \bmod f\}}{p-1}\right\rfloor.$$

When $k+1=2*4^n+4^n-1$, it fails, even for $d=1$ (e.g. for $k+1=11$, it gives wrong answers 44 and 220 for $d=1$, 2, respectively).

A.12. Open questions

It would be nice to settle the status of Hypotheses (H1)–(H3) (note that we have not used them in any proofs or theorems, but they are just interesting observations), get simple recursion or formulas of the type of Section 9, for general q (and also for negative k's) and see whether the applications (which are easy consequences of our recursion when q is prime) generalize for any q, say by generating function approach or by direct applications of Sheats' and our algorithm for k negative and positive, respectively.

References

[1] G. Anderson, D. Thakur, Multizeta values for $F_q[t]$, their period interpretation and relations between them, Int. Math. Res. Not., in press.
[2] L. Carlitz, On certain functions connected with polynomials in a Galois field, Duke Math. J. 1 (1935) 139–158.
[3] J. Diaz-Vargas, Riemann hypothesis for $F_q[t]$, J. Number Theory 59 (2) (1996) 313–318.
[4] D. Goss, Basic Structures of Function Field Arithmetic, Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas (3)), vol. 35, Springer-Verlag, Berlin, 1996.
[5] D. Goss, A Riemann hypothesis for characteristic p L functions, J. Number Theory 82 (2000) 299–322.
[6] J. Sheats, The Riemann hypothesis for the Goss zeta function for $F_q[t]$, J. Number Theory 71 (1) (1998) 121–157.
[7] D. Thakur, Zeta measure associated to $\mathbb{F}_q[t]$, J. Number Theory 35 (1990) 1–17.
[8] D. Thakur, Function Field Arithmetic, World Scientific Publ., 2004.
[9] D. Thakur, Relations between multizeta values for $\mathbb{F}_q[t]$, Int. Math. Res. Not., in press.
[10] D. Wan, On the Riemann hypothesis for the characteristic p zeta function, J. Number Theory 58 (1) (1996) 196–212.