JP Journal of Algebra, Number Theory and Applications
Published Online: June 2014
Available online at http://pphmj.com/journals/jpanta.htm
Volume 32, Number 2, 2014, Pages 141-164

A NOTE ON POWER SUMS OVER FINITE FIELDS

Javier Diaz-Vargas and Eduardo Hernandez-Mezquita

Facultad de Matemáticas
Universidad Autónoma de Yucatán
Periférico Norte Tablaje 13615, 97119
Mérida, Yucatán, México
e-mail: jdvargas@uady.mx
megacamilo@msn.com

Abstract

We study basic aspects of the sums of nonpositive integral powers of monic polynomials of degree one over a finite field. The combinatorics of cancelation in these sums is rather complicated. The focus is basically on the valuations of these sums in the infinite place of $\mathbb{F}_q(t)$, where q is a power of a prime p. We present the concept of integer with inner q carry over of depth j. For exponents of the form $(k+1)$ relative prime to p and k relative prime to q, where k presents inner q carry over of depth j, we give a result to find the valuation at the infinite place of $\mathbb{F}_q(t)$ of the sums of powers under study, for any finite field.

1. Introduction

We study some basic questions on the behavior of $S_d(k)$ defined as the sum of $\dfrac{1}{a^k}$ as a runs through all the monic polynomials of degree d in $\mathbb{F}_q[t]$,

Received: January 25, 2014; Accepted: March 26, 2014
2010 Mathematics Subject Classification: 11T55, 11R58.
Keywords and phrases: finite fields, power sums, zeta function.

being q the power of a prime and k a nonnegative integer. The focus is basically on the valuation of these sums at the infinite place of $\mathbb{F}_q(t)$, designated by $s_d(k)$. Guided by the fact that when the finite field is a prime field, there exists a recursive formula to get $s_d(k)$ from $s_1(k)$ [4], we directed our efforts to obtain a formula or method to calculate $s_1(k)$ for any finite field. While the degree of the term $\frac{1}{a^k}$, being just $-dk$, has extremely simple behavior, the degree we are interested in behaves quite erratically because of complicated cancelation possibilities. Apart from their intrinsic interest, these questions have applications to the non-vanishing of the multizeta function values [5] 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 Wan [6], with another proof by Diaz-Vargas [2] and for general q by Sheats [3]. After analysis of certain amount of $s_1(k)$ values for various $\mathbb{F}_q$, we conjectured and finally proved that, under certain assumptions, when the coefficients of the q-base expansion of k can be made to display a particular arrangement, there is an easy way to obtain $s_1(k+1)$ from these coefficients. That particular arrangement for the q-base expansion of k we mentioned, leads us to define integer with inner q carry over of certain depth. We give some examples for the existence of these particular exponents and the way to achieve $s_1(k+1)$ from their q-base expansion coefficients.

2. Notation

Some standard notation used along the paper are settled:

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

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

$\mathbb{Z}_{\geq 0} = \{\text{nonnegative integers}\}$,

$q =$ power of a prime p, $q = p^\lambda$, $\lambda > 0$,

$\mathbb{F}_q$ = finite field with q elements,

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

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

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

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

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

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

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

deg = degree of $a \in K$, $\deg(0) = -\infty$.

3. Definitions and Preliminary Results

We define the objects we work on.

Definition 1. For $k \in \mathbb{Z}$ and $d \in \mathbb{Z}_{\geq 0}$, write

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

Since we are in characteristic p, we have

$$S_d(kp^n) = S_d(k)^{p^n}. \tag{3.1}$$

The property (3.1) enables us to restrict our research to exponents not divisible by p without loss of generality.

Proposition 1. *Let k, u, v be nonnegative integers with base q expansions* *given by*

$$k = \sum_{i=0}^{m} \alpha_i q^i, \quad 0 \le \alpha_i \le q - 1,$$

$$u = \sum_{i=0}^{m} \beta_i q^i, \quad 0 \le \beta_i \le q - 1,$$

$$v = \sum_{i=0}^{m} \gamma_i q^i, \quad 0 \le \gamma_i \le q - 1$$

such that $k = u + qv$ *and* $\alpha_i, \beta_i, \gamma_i = 0$ *for* $i > m$. *Then*

$$\alpha_0 = \beta_0$$

and $u \ge \alpha_0$.

Proof. If we substitute in the expression $k = u + qv$ the respective base q expansions, then we have

$$\sum_{i=0}^{m} \alpha_i q^i = \sum_{i=0}^{m} \beta_i q^i + q \sum_{i=0}^{m} \gamma_i q^i$$

$$= \beta_0 + \left(\sum_{i=1}^{m} \beta_i q^i + \sum_{i=1}^{m+1} \gamma_{i-1} q^i \right), \tag{3.2}$$

by comparing terms on both sides of (3.2), we get

$$\alpha_0 = \beta_0.$$

As we have $u \ge \beta_0$, then $u \ge \alpha_0$. □

The occurrence of carry over in base q or in base p, when performing an addition, is an essential fact we have to take care. The following two results enable us, under certain conditions, to be sure of the occurrence or lack of such carry over.

Proposition 2. *If the sum of two digits base q equals* $(q-1)$, *then the same addition performed in base p has no carry over.*

Proof. For $q = 2$, the proposition is trivial; henceforth, we can assume $q > 2$. By contradiction let us suppose that we are given two base q digits a, b, whose sum in base q equals $q-1$, but the same sum performed in base p has carry over. As we have supposed $q = p^{\lambda}$, $\lambda > 0$, then $a = \sum_{i=0}^{\lambda-1} a_i p^i$, $b = \sum_{i=0}^{\lambda-1} b_i p^i$ with $0 \le a_i, b_i \le p-1$, are p base representations for a and b. Let $q - 1 = \sum_{i=0}^{\lambda-1}(p-1)p^i$ be the p-base expansion for $q-1$. By hypothesis $a + b = (q-1) = \sum_{i=0}^{\lambda-1}(p-1)p^i$, but at the same time, when summing the p-base representations for a and b, there exists carry over base p. Let j, $0 \le j \le \lambda - 1$, the first position where there exists carry over base p when performing $a+b$ base p. Then $a_j + b_j > p-1$, that is, $a_j + b_j = p + r$, where r is the base p digit that remains at the j position in the base p expansion for $a + b$. Neither a_j nor b_j are zero, then we have

$$1 \le a_j \le p-1,$$

$$1 \le b_j \le p-1;$$

therefore,

$$2 \le a_j + b_j \le 2p - 2 = p + (p-2).$$

Hence, $r \le p-2$. However, the base p representation for $q-1$ is unique; so, we must have $r = (p-1)$, which is contradictory, and we have finished. □

Proposition 3. *If the sum of two base q digits has carry over base q, then the same sum performed in base p has carry over base p.*

Proof. Let $0 \leq a, b \leq q - 1$ be base q digits and by contradiction suppose that the sum $a + b \geq q$, but the same sum performed in base p has no carry over. Again, we can take $a = \sum_{i=0}^{\lambda-1} a_i p^i$, $b = \sum_{i=0}^{\lambda-1} b_i p^i$ with $0 \leq a_i, b_i \leq p - 1$ as base p representations for a and b, respectively. As we have supposed that the sum $a + b$ has no carry over base p, then we have

$$a + b = \sum_{i=0}^{\lambda-1} (a_i + b_i) p^i,$$

because

$$(a_i + b_i) \leq p - 1 \text{ for } i = 0, 1, \ldots, \lambda - 1.$$

Hence,

$$\begin{aligned} a + b &\leq \sum_{i=0}^{\lambda-1} (p - 1) p^i \\ &= p^{\lambda} - 1 \\ &= q - 1, \end{aligned}$$

and the supposed carry over base q does not exist. We can conclude that carry over base q implies carry over base p. □

As we mentioned in the introduction, $s_1(k + 1)$ can be readily obtained from k when it accomplishes certain conditions; the following definition gives, explicitly, these conditions.

Definition 2. Let k be a positive integer, with base q expansion:

$$k = \sum_{i=0}^{m} \alpha_i q^i, \; 0 \leq \alpha_i \leq q - 1, \; \alpha_i = 0 \text{ for } i > m,$$

where we define $c_0 = \alpha_0$. If we can make the following arrangement with the $\alpha_i's$, for some $0 \leq j \leq m$:

$$c_0 + \alpha_1 = (q-1) + c_1,\ c_1 \geq 1$$

$$c_1 + \alpha_2 = (q-1) + c_2,\ c_2 \geq 1$$

$$\vdots$$

$$c_{j-1} + \alpha_j = (q-1) + c_j,\ c_j \geq 1$$

$$c_j + \alpha_{j+1} \leq (q-1),$$

with the sum $c_j + \alpha_{j+1}$ free of carry over base p, then we say that k has inner q carry over of depth j.

We now give some examples of integers that fulfill Definition 2.

Example 1. For $q = 9,$ consider $k = 2725 = 3657_9,$ then

$$c_0 + \alpha_1 = 7 + 5 = 8 + 4 = (q-1) + c_1$$

$$c_1 + \alpha_2 = 4 + 6 = 8 + 2 = (q-1) + c_2$$

$$c_2 + \alpha_3 = 2 + 3 < 8,$$

where the last sum, $c_2 + \alpha_3,$ has no carry over base 3. Therefore, according to Definition 2, $k = 2725$ has inner 9 carry over of depth 2.

Example 2. Now, for $q = 8,$ consider $k = 253814 = 757566_8,$ then

$$c_0 + \alpha_1 = 6 + 6 = 7 + 5 = (q-1) + c_1$$

$$c_1 + \alpha_2 = 5 + 5 = 7 + 3 = (q-1) + c_2$$

$$c_2 + \alpha_3 = 3 + 7 = 7 + 3 = (q-1) + c_3$$

$$c_3 + \alpha_4 = 3 + 5 = 7 + 1 = (q-1) + c_4$$

$$c_4 + \alpha_5 = 1 + 7 = 7 + 1 = (q-1) + c_5$$

$$c_5 + \alpha_6 = 1 + 0 < 7,$$

where the last sum, $c_5 + \alpha_6,$ has no carry over base 2. Therefore, according to Definition 2, $k = 253814$ has inner 8 carry over of depth 5.

Example 3. Let $q = 27$ with $k = 825892 = (1)(14)(25)(24)(16)_{27}$. Then

$$c_0 + \alpha_1 = 16 + 24 = 26 + 14 = (q - 1) + c_1$$

$$c_1 + \alpha_2 = 14 + 25 = 26 + 13 = (q - 1) + c_2$$

$$c_2 + \alpha_3 = 13 + 14 = 26 + 1 = (q - 1) + c_3$$

$$c_3 + \alpha_4 = 1 + 1 < 26,$$

with the last sum, $c_3 + \alpha_4$, free of carry over base 3. Then, in concordance with Definition 2, $k = 825892$, has inner 27 carry over of depth 3.

As a consequence of Definition 2, we establish the following lemma which is going to be useful in the proof of our main result.

Lemma 1. *If* $(k, q) = 1$, $(k + 1, p) = 1$, $q > 2$ *and k has inner q carry over of depth j* (*Definition* 2), *then*:

$$1 \le c_0 \le q - 2$$

$$1 \le c_1 \le q - 2$$

$$\vdots$$

$$1 \le c_j \le q - 2,$$

and

$$\alpha_i - c_i > 0, \quad i = 1, 2, \ldots, j.$$

Proof. For c_0, we have $c_0 \ge 1$, because, if $c_0 = 0$, then $(k, q) \ne 1$ which is contradictory. Also, $c_0 \le q - 2$, because, if $c_0 = (q - 1)$, then $q \mid (k + 1)$ $\Rightarrow (k + 1, p) \ne 1$ contrary to what we have assumed. Then $1 \le c_0 \le q - 2$. If $j = 0$, then we have concluded. In case that $j \ge 1$, we must have

$$c_0 + \alpha_1 = (q - 1) + c_1, \ c_1 \ge 1$$

$$c_1 + \alpha_2 = (q - 1) + c_2, \ c_2 \ge 1$$

$$\vdots$$

$$c_{j-1} + \alpha_j = (q-1) + c_j,\ c_j \geq 1$$

$$c_j + \alpha_{j+1} \leq (q-1),$$

without carry over base p in the last sum. Then

$$1 \leq c_0 \leq q-2$$

$$0 \leq \alpha_1 \leq q-1,$$

which implies

$$1 \leq c_0 + \alpha_1 \leq (q-1) + (q-2),$$

hence

$$c_1 = (c_0 + \alpha_1) - (q-1) \leq q-2.$$

Therefore,

$$1 \leq c_1 \leq q-2.$$

Following an identical procedure, we can conclude

$$1 \leq c_0 \leq q-2$$

$$1 \leq c_1 \leq q-2$$

$$\vdots$$

$$1 \leq c_j \leq q-2.$$

Now, if we suppose $\alpha_i - c_i \leq 0$ for some $i \in \{1, 2, \ldots, j\}$, then we should have

$$c_{i-1} + (\alpha_i - c_i) = (q-1),$$

implying that $c_{i-1} \geq (q-1)$, contrary to what we have just proved. □

4. Main Result

By a generating function approach, Carlitz [1] proved that

$$S_d(k+1) = \frac{1}{l_d^{k+1}} \sum \left(\sum_{\substack{i=0 \\ k_0, k_1, \ldots, k_d}}^{d} k_i \right) \prod_{i=0}^{d} \left(\frac{\left(\frac{l_d}{l_{d-i}} \right)^{q^i}}{D_i} \right)^{k_i},$$

where the sum is made over all $(d+1)$-tuples $(k_0, k_1, \ldots, k_d)$ of nonnegative integers such that $\sum_{i=0}^{d} k_i q^i = k$. Thakur [4] pointed out and claimed that

- For $S_d(k+1)$ only terms where there is no carry over base p in the sum of k_i's need to be considered.
- When $d = 1$, $s_1(k+1) = (k_1 + k_0 + 1)q = k + q + k_0(q-1)$, where k_0 is the minimum possible such that $k = k_1 q + k_0$, $k_i \geq 0$, with no carry over base p in the sum $k_1 + k_0$.
- When the last two digits in the base q expansion of k add without carry over base p, the minimum k_0 is the last digit. Giving a formula for $s_1(k+1)$ in case that k has inner q carry over of depth 0.
- This last statement, together with the property (3.1), takes care of $s_1(k+1)$ for $q = 2$.

For convenience, let us write u and v for best k_0, k_1. Then $k = vq + u$ and $s_1(k+1) = (v+u+1)q = k + q + u(q-1)$. The following result gives us the value of $s_1(k+1)$ when k accomplishes the conditions of Lemma 1.

Proposition 4. *Suppose $(k, q) = 1$, $(k+1, p) = 1$, $q > 2$ and k has inner q carry over of depth j. Then $s_1(k+1) = k + q + (c_0 + c_1 q + c_2 q^2 + \cdots + c_j q^j)(q-1)$, where $c_0, c_1, c_2, \ldots, c_j$ are those from Definition* 2.

Proof. By Definition 2 and Lemma 1, we have: $k = \alpha_0 + \alpha_1 q + \cdots +$

$\alpha_j q^j + \sum_{i=j+1}^{m} \alpha_i q^i$, and

$$\begin{aligned} & c_0 + \alpha_1 = (q-1) + c_1,\ 1 \le c_1 \le q-2,\ \alpha_1 - c_1 > 0 \\ & c_1 + \alpha_2 = (q-1) + c_2,\ 1 \le c_2 \le q-2,\ \alpha_2 - c_2 > 0 \\ & \qquad \vdots \\ & c_{j-1} + \alpha_j = (q-1) + c_j,\ 1 \le c_j \le q-2,\ \alpha_j - c_j > 0 \\ & c_j + \alpha_{j+1} \le (q-1) \text{ without carry over base } p. \end{aligned} \tag{4.1}$$

Taking $u = c_0 + c_1 q + c_2 q^2 + \cdots + c_j q^j$, if we assume that $k = u + qv$, then we have

$$\begin{aligned} v &= (k-u)q^{-1} \\ &= \left[\left(\sum_{i=0}^{j} \alpha_i q^i + \sum_{i=j+1}^{m} \alpha_i q^i\right) - \sum_{i=0}^{j} c_i q^i\right] q^{-1} \\ &= \sum_{i=1}^{j} (\alpha_i - c_i) q^{i-1} + \sum_{i=j+1}^{m} \alpha_i q^{i-1}. \end{aligned}$$

Note that, by construction $k = u + qv$, $u, v \ge 0$ and the sum $u + v$ has no carry over base p because

$$u = \sum_{i=0}^{j} c_i q^i = \sum_{i=1}^{j} c_{i-1} q^{i-1} + c_j q^j,$$

$$\begin{aligned} u + v &= \sum_{i=1}^{j} (c_{i-1} + (\alpha_i - c_i)) q^{i-1} + (c_j + \alpha_{j+1}) q^j + \sum_{i=j+2}^{m} \alpha_i q^{i-1} \\ &= \sum_{i=1}^{j} (q-1) q^{i-1} + (c_j + \alpha_{j+1}) q^j + \sum_{i=j+2}^{m} \alpha_i q^{i-1}, \end{aligned}$$

where we have made use of (4.1) in the last step. The sums $(c_{i-1} + (\alpha_i - c_i))$ for $j = 1, \ldots, j$ are free of carry over base p by Proposition 2, because digits add to $(q-1)$ exactly. The sum $(c_j + \alpha_{j+1})$ also is free of carry over base p by definition, given that k has inner q carry over of depth j. Then we have integers $u, v \geq 0,$ such that $k = u + qv$ and the sum $u + v$ is free of carry over base p. Let us see that the proposed u is the minimal one that accomplishes $k = u + qv,\ u, v \geq 0$ and the sum $u + v$ has no carry over base p. By contradiction suppose that there exist integers $u' < u, v',$ such that $k = u' + qv'$ and the sum $u' + v'$ is free of carry over base p. As we have supposed $u' < u,$ u' must have no more that $(j+1)$ base q digits, let us say $u' = (c'_j c'_{j-1} \cdots c'_1 c'_0)_q$. By Proposition 1, $c_0 = c'_0$. If we suppose that $c'_i \leq c_i$ for $i = 1, 2, \ldots, j,$ let $\eta \in \{1, 2, \ldots, j\}$ be the least integer such that $c'_\eta < c_\eta,$ this implies $c'_i = c_i$ for $i < \eta.$ As we have supposed $k = u' + qv',$ then

$$
\begin{aligned}
v' &= (k - u')q^{-1} \\
&= \left(\sum_{i=0}^{m} \alpha_i q^i - \sum_{i=0}^{j} c'_i q^i\right) q^{-1} \\
&= \left(\sum_{i=0}^{m} \alpha_i q^i - \sum_{i=0}^{\eta-1} c'_i q^i - c'_\eta q^\eta - \sum_{i=\eta+1}^{j} c'_i q^i\right) q^{-1} \\
&= \sum_{i=1}^{\eta-1} (\alpha_i - c'_i) q^{i-1} + (\alpha_\eta - c'_\eta) q^{\eta-1} + \sum_{i=\eta+1}^{j} (\alpha_i - c'_i) q^{i-1} + \sum_{i=j+1}^{m} \alpha_i q^{i-1},
\end{aligned}
$$

note that it is possible to perform the subtraction term by term in the same way we made it for u because $c'_i \leq c_i$ for $i = 1, 2, \ldots, j.$ Even more, for $i < \eta$ the result is the same given that $c'_i = c_i$ for these places. We see that for v' the digit on the $\eta - 1$ position equals $(\alpha_\eta - c'_\eta) > (\alpha_\eta - c_\eta)$. Summing

$u' + v',$ we obtain

$$u' + v' = \sum_{i=0}^{j} c_i' q^i + \sum_{i=1}^{\eta-1} (\alpha_i - c_i') q^{i-1} + (\alpha_\eta - c_\eta') q^{\eta-1}$$

$$+ \sum_{i=\eta+1}^{j} (\alpha_i - c_i') q^{i-1} + \sum_{i=j+1}^{m} \alpha_i q^{i-1},$$

rearranging the sum and taking into account that $c_i' = c_i$ for $i < \eta,$ we arrive to

$$u' + v' = \sum_{i=1}^{\eta-1} c_{i-1} q^{i-1} + c_{\eta-1} q^{\eta-1} + \sum_{i=\eta}^{j} c_i' q^i$$

$$+ \sum_{i=1}^{\eta-1} (\alpha_i - c_i) q^{i-1} + (\alpha_\eta - c_\eta') q^{\eta-1}$$

$$+ \sum_{i=\eta+1}^{j} (\alpha_i - c_i') q^{i-1} + \sum_{i=j+1}^{m} \alpha_i q^{i-1}$$

$$= \sum_{i=1}^{\eta-1} (c_{i-1} + (\alpha_i - c_i)) q^{i-1} + (c_{\eta-1} + (\alpha_\eta - c_\eta')) q^{\eta-1}$$

$$+ \sum_{i=\eta}^{j} c_i' q^i + \sum_{i=\eta+1}^{j} (\alpha_i - c_i') q^{i-1} + \sum_{i=j+1}^{m} \alpha_i q^{i-1}$$

$$= \sum_{i=1}^{\eta-1} (q-1) q^{i-1} + (c_{\eta-1} + (\alpha_\eta - c_\eta')) q^{\eta-1}$$

$$+ \sum_{i=\eta}^{j} c_i' q^i + \sum_{i=\eta+1}^{j} (\alpha_i - c_i') q^{i-1} + \sum_{i=j+1}^{m} \alpha_i q^{i-1},$$

where we have made use of (4.1) as in the u case. For the sum $c_{\eta-1} +$

$(\alpha_\eta - c'_\eta)$, we have

$$c_{\eta-1} + (\alpha_\eta - c'_\eta) > c_{\eta-1} + (\alpha_\eta - c_\eta) > q - 1,$$

then for this case the sum $u' + v'$ has carry over q and therefore carry over base p. The existence or lack of carry over base p in the sum $\sum_{i=\eta}^{j} c'_i q^i + \sum_{i=\eta+1}^{j} (\alpha_i - c'_i) q^{i-1} + \sum_{i=j+1}^{m} \alpha_i q^{i-1}$ does not change the result of this part of the proof. Hence to suppose $u' < u$ with $c'_i \le c_i$ for $i = 1, 2, \ldots, j$, leads us to a contradiction. Then, for some $i = 1, 2, \ldots, j-1$, we must have $c'_i > c_i$. Let $\eta \in \{1, 2, \ldots, j-1\}$ be the biggest index for which $c'_\eta > c_\eta$; remembering that necessarily $c'_0 = c_0 = \alpha_0$ and also $c'_j \le c_j$, because $c'_j > c_j$ implies that $u' > u$. By the choice of η, we have that $c'_i \le c_i$, for $i = \eta + 1, \eta + 2, \ldots, j$. Nevertheless, if for all $i \in \{\eta + 1, \eta + 2, \ldots, j\}$, $c'_i = c_i$, then $u' > u$, which is contradictory. Therefore, for some $i \in \{\eta + 1, \eta + 2, \ldots, j\}$ we must have $c'_i < c_i$. Let us designate by $\xi \in \{\eta + 1, \eta + 2, \ldots, j\}$ the least integer such that $c'_\xi < c_\xi$. If $\xi - \eta > 1$, then $c'_{\eta+1}, c'_{\eta+2}, \ldots, c'_{\xi-1}$ necessarily accomplish

$$\begin{gathered} c'_{\eta+1} = c_{\eta+1} \\ c'_{\eta+2} = c_{\eta+2} \\ \vdots \\ c'_{\xi-1} = c_{\xi-1}. \end{gathered}$$

Then u' and k have for this case the following arrangement:

$$\begin{aligned} u' &= c'_0 c'_1 \cdots c'_\eta c'_{\eta+1} \cdots c'_{\xi-1} c'_\xi c'_{\xi+1} \cdots c'_j \\ &= \alpha_0 c'_1 \cdots c'_\eta c_{\eta+1} \cdots c_{\xi-1} c'_\xi c'_{\xi+1} \cdots c'_j, \\ k &= \alpha_0 \alpha_1 \cdots \alpha_\eta \alpha_{\eta+1} \cdots \alpha_{\xi-1} \alpha_\xi \alpha_{\xi+1} \cdots \alpha_j \cdots \alpha_m. \end{aligned}$$

As we have supposed $k = u' + qv'$, it follows that $v' = (k - u')q^{-1}$. The indicated subtraction $(k - u')$, can be settled down as

$$
\begin{array}{rcccccccccccc}
 & \alpha_0 & \alpha_1 & \cdots & \alpha_\eta & \alpha_{\eta+1} & \cdots & \alpha_{\xi-1} & \alpha_\xi & \alpha_{\xi+1} & \cdots & \alpha_j & \cdots \ \alpha_m \\
- & \alpha_0 & c'_1 & \cdots & c'_\eta & c_{\eta+1} & \cdots & c_{\xi-1} & c'_\xi & c'_{\xi+1} & \cdots & c'_j. &
\end{array}
$$

At the η position, we have to subtract c'_η from $(\alpha_\eta - \varepsilon)$, where $\varepsilon = 1$ or 0 whether or not a borrowing has been made from the prior position $\eta - 1$, note that $(\alpha_\eta - \varepsilon) \geq 0$ (see Remark 1).

If $\alpha_\eta - \varepsilon \geq c'_\eta$, then it is possible to perform the subtraction $(\alpha_\eta - \varepsilon) - c'_\eta$ without the need to make a borrowing from the next position $\eta + 1$, and therefore, the following subtractions $\alpha_i - c_i$ for $i = \eta + 1, \ldots, \xi - 1$, are also possible without the need to make a borrowing from the next position. This last can be justified by (4.1). Following with the subtraction, under the assumption $\alpha_\eta - \varepsilon \geq c'_\eta$, we reach the ξ position where we have

$$\alpha_\xi - c'_\xi > \alpha_\xi - c_\xi > 0,$$

and then this difference will remain as a valid digit for u' in the $\xi - 1$ position because of the position shift that occurs in the product $(k - u')q^{-1}$. When performing the sum $u' + v'$, if there occurs carry over base p when summing the digits that correspond to the $0, 1, \ldots, \xi - 2$ positions, we have finished, on the contrary for the $\xi - 1$ position we will have

$$c'_{\xi-1} + (\alpha_\xi - c'_\xi) = c_{\xi-1} + (\alpha_\xi - c'_\xi) > c_{\xi-1} + (\alpha_\xi - c_\xi) = q - 1,$$

having carry over base q and therefore carry over base p.

In case of $\alpha_\eta - \varepsilon < c'_\eta$, it is necessary to make a borrowing from the $\eta + 1$ position, and so the valid digit position η for $k - u'$ is

$$(\alpha_\eta - \varepsilon) + q - c'_\eta.$$

At the $\eta + 1$ position, for k y u', we have as valid digits, respectively, $\alpha_{\eta+1} - 1$ and $c'_{\eta+1} = c_{\eta+1}$. In addition, the definition of u and the supposed structure for u' allows us to claim

$$\alpha_{\eta+1} - c_{\eta+1} = \alpha_{\eta+1} - c'_{\eta+1} > 0,$$

then

$$(\alpha_{\eta+1} - 1) - c'_{\eta+1} \geq 0,$$

therefore the subtraction in the $\eta + 1$ position can be performed without borrowing from the next position. The latter implies that for the $\eta + 2, \ldots, \xi - 1$ positions, the subtraction can be made term by term without borrowing, that is for in these positions we have as valid digits

$$\begin{aligned} \alpha_{\eta+2} - c'_{\eta+2} &= \alpha_{\eta+2} - c_{\eta+2} > 0, \\ &\vdots \\ \alpha_{\xi-1} - c'_{\xi-1} &= \alpha_{\xi-1} - c_{\xi-1} > 0, \end{aligned}$$

which are the same subtractions that were made for $k - u$, at the same positions. Reaching the ξ position, the digits to be subtracted are α_ξ and $c'_\xi < c_\xi$ and then

$$\alpha_\xi - c'_\xi > \alpha_\xi - c_\xi > 0$$

will be a valid digit for v' at the $\xi - 1$ position because of the position shift when $(k - u')$ is multiplied by q^{-1}. Performing the addition $u' + v'$, if there occurs carry over base p when summing the digits that correspond to the $0, 1, \ldots, \xi - 2$ positions, we have finished, on the contrary for the $\xi - 1$ position we will have

$$c'_{\xi-1} + (\alpha_\xi - c'_\xi) = c_{\xi-1} + (\alpha_\xi - c'_\xi) > c_{\xi-1} + (\alpha_\xi - c_\xi) = q - 1,$$

having carry over base q and therefore carry over base p.

Now, if $\xi - \eta = 1,$ then u' and k will have for this case the following arrangement:

$$u' = c_0' c_1' c_3' \cdots c_n' c_{\eta+1}' \cdots c_j'$$

$$= \alpha_0 c_1' c_2' \cdots c_\eta' c_{\eta+1}' \cdots c_j',$$

$$k = \alpha_0 \alpha_1 \alpha_2 \cdots \alpha_\eta \alpha_{\eta+1} \cdots \alpha_j \cdots \alpha_m,$$

with $c_\eta' > c_\eta$ and $c_{\eta+1}' < c_{\eta+1}.$ Once again, for this u' we suppose $k = u' + qv',$ hence $v' = (k - u')q^{-1}.$ Performing the subtraction $k - u',$ when we reach the η position, for k we will have for this position $\alpha_\eta - \varepsilon \geq 0,$ where $\varepsilon = 1$ or 0, whether or not there has been made a borrowing from the prior position $\eta - 1.$ If $\alpha_\eta - \varepsilon \geq c_\eta',$ then the subtraction $(\alpha_\eta - \varepsilon) - c_\eta'$ can be made without borrowing from the following position $\eta + 1,$ then in that position the subtraction $k - u'$ can be made term by term because $c_{\eta+1}' < c_{\eta+1}.$ Hence the digit of v' in η position would be $(\alpha_{\eta+1} - c_{\eta+1}') > (\alpha_{\eta+1} - c_{\eta+1}),$ taking into account the position shift when multiplied by $q^{-1}.$ When summing $u' + v',$ if there occurs carry over base p at positions $0, 1, ..., \eta - 1,$ we have finished. If not when performing the sum at η position, then we will have

$$c_\eta' + (\alpha_{\eta+1} - c_{\eta+1}') > c_\eta + (\alpha_{\eta+1} - c_{\eta+1}') > c_\eta + (\alpha_{\eta+1} - c_{\eta+1}) = q - 1,$$

with carry over base q and therefore carry over base p. In case of $\alpha_\eta - \varepsilon < c_\eta'$ to perform the subtraction at this position, it is necessary to take a borrowing from the next position $\eta + 1.$ The actual subtraction to perform at η position will be

$$(\alpha_\eta - \varepsilon) + q - c_\eta'$$

and for $\eta + 1$ position, as digits for k and $u',$ we will have $(\alpha_{\eta+1} - 1)$ and

$c'_{\eta+1} < c_{\eta+1}$, respectively. As we defined u and by k definition, it is known that $\alpha_{\eta+1} - c_{\eta+1} > 0$. To find out the subtraction in $\eta + 1$ position, consider

$$c'_{\eta+1} < c_{\eta+1}$$

$$c'_{\eta+1} + 1 \leq c_{\eta+1}$$

$$-c'_{\eta+1} - 1 \geq -c_{\eta+1}$$

$$[(\alpha_{\eta+1} - 1) - c'_{\eta+1}] \geq \alpha_{\eta+1} - c_{\eta+1} > 0,$$

this last shows that at $\eta + 1$ position, it is valid a term by term subtraction without borrowing. Hence the digit at η position for v' will be $[(\alpha_{\eta+1} - 1) - c'_{\eta+1}]$, remembering the position shift when it is multiplied by q^{-1}. When we sum $u' + v'$ in this case, if there exists carry over base p at positions $0, 1, \ldots, \eta - 1$ we have finished. If not, when performing the sum at η position, then we have

$$\begin{aligned} c'_{\eta} + [(\alpha_{\eta+1} - 1) - c'_{\eta+1}] &\geq c'_{\eta} + (\alpha_{\eta+1} - c_{\eta+1}) \\ &> c_{\eta} + (\alpha_{\eta+1} - c_{\eta+1}) \\ &= q - 1, \end{aligned}$$

with carry over base q and therefore carry over base p. Given this last argumentation, we can conclude that for an integer k with inner q carry over of depth j, the minimum u that accomplishes, $k = u + qv,\ u,\ v \geq 0,$ with no carry over base p in the sum $u + v$ is given by $u = (c_0 + c_1 q + c_2 q^2 + \cdots + c_j q^j)$, where $c_0, c_1, c_2, \ldots, c_j$ are those from Definition 2. Then

$$s_1(k + 1) = k + q + (c_0 + c_1 q + c_2 q^2 + \cdots + c_j q^j)(q - 1). \qquad \square$$

Remark 1. If k has inner q carry over of depth j, then $\alpha_i > 0$ for $i \leq j$.

Because if for some integer $\zeta < j, \alpha_\zeta = 0,$ then we would have

$$c_{\zeta-1} + \alpha_\zeta = c_{\zeta-1} < q - 1,$$

without carry over base p, which implies that k has inner q carry over of depth $(\zeta - 1) < j,$ contradicting what we have assumed.

The following two corollaries are a formal statement for when an integer k having inner q carry over of depth j is such that $j = m$ or $j = m - 1$, where m is the exponent of the most significative digit in the base q representation of k, we can build from it an infinite set of integers, sharing all of them, the same depth and the same value of u that is used to obtain $s_1(k + 1)$.

Corollary 1. *If k is an integer with base q representation*

$$k = \sum_{i=0}^{m} \alpha_i q^i,\ 0 \leq \alpha_i \leq q - 1,\ \alpha_i = 0 \ \mathit{for}\ i > m,\ m \geq 1,$$

such that it has inner q carry over of depth $m - 1$, *then all the elements of the form* $k + aq^{m+1}$, *for any* $a \in \mathbb{Z}_{\geq 0}$ *have the same depth and use the same value of u to obtain* $s_1(k' + 1), k' = k + aq^{m+1}$.

Proof. This follows from the way we construct the value of u from the $\alpha_i's$ and $c_i's$ in Proposition 4 for k. Given that k has inner q carry over of depth $m - 1,$ we must have

$$c_{m-1} + \alpha_m < q - 1$$

with no carry over base p in the sum. The addition to k of a positive multiple of q^{m+1} does not change, for the new formed integer k', the property of having inner q carry over of depth $m - 1.$ The latter implies via Proposition 4 that to obtain $s_1(k' + 1),$ we take the same value of u we have used to calculate $s_1(k + 1)$. □

Corollary 2. *If k is an integer with base q representation*

$$k = \sum_{i=0}^{m} \alpha_i q^i, \; 0 \le \alpha_i \le q-1, \; \alpha_i = 0 \text{ for } i > m,$$

such that it has inner q carry over of depth m, then all the elements of the form $k + aq^{m+2}$, *for any* $a \in \mathbb{Z}_{\ge 0}$ *have the same depth and use the same value of u to obtain* $s_1(k'+1)$, $k' = k + aq^{m+2}$.

Proof. Given that k has inner q carry over of depth m and $\alpha_i = 0$ for $i > m$, we must have

$$c_m + 0 < q - 1,$$

clearly with no carry over base p in the sum. The addition to k of a positive multiple of q^{m+2}, keeps for the new formed integer k', a zero in position $m+1$. Then k' has also inner q carry over of depth m. The latter implies via Proposition 4 that to obtain $s_1(k'+1)$, we take the same value of u we have used to calculate $s_1(k+1)$. □

The following examples show the way we can use Proposition 4 and Corollaries 1, 2 in order to calculate $s_1(k+1)$, when k has inner q carry over of certain depth.

Example 4. Let $q = 9$, $k = 11410 = 16577_9$. Then

$$c_0 + \alpha_1 = 7 + 7 = 8 + 6 = (q-1) + c_1$$

$$c_1 + \alpha_2 = 6 + 5 = 8 + 3 = (q-1) + c_2$$

$$c_2 + \alpha_3 = 3 + 6 = 8 + 1 = (q-1) + c_3$$

$$c_3 + \alpha_4 = 1 + 1 < (q-1)$$

without carry over base 3 in the last sum. Then $11410 = 16577_9$ has inner 9 carry over of depth 3. Then to calculate $s_1(11411) = -\deg \sum_{\alpha \in \mathbb{F}_9} \frac{1}{(t+\alpha)^{11411}}$, we set

$$u = (c_0 + c_1 q + c_2 q^2 + c_3 q^3)$$

$$= (7 \cdot 9^0 + 6 \cdot 9^1 + 3 \cdot 9^2 + 1 \cdot 9^3),$$

therefore

$$s_1(11411) = 11410 + 9 + (7 + 6 \cdot 9^1 + 3 \cdot 9^2 + 1 \cdot 9^3) \cdot 8$$

$$= 11410 + 9 + 1033 \cdot 8$$

$$= 19683.$$

Example 5. From Example 1, we know that $k = 2725$ has inner 9 carry over of depth 2; with $c_0 = 7$, $c_1 = 4$, $c_2 = 2$. So in order to calculate $s_1(2726) = -\deg \sum_{\alpha \in \mathbb{F}_9} \frac{1}{(t+\alpha)^{2726}}$, we take

$$u = c_0 + c_1 q + c_2 q^2$$

$$= 7 + 4 \cdot 9 + 2 \cdot 9^2,$$

then

$$s_1(2726) = 2725 + 9 + (7 + 4 \cdot 9 + 2 \cdot 9^2) \cdot 8$$

$$= 2734 + 1640$$

$$= 4374.$$

Example 6. In Example 2, we saw that $k = 253814$ has inner 8 carry over of depth 5, with $c_0 = 6$, $c_1 = 5$, $c_2 = 3$, $c_3 = 3$, $c_4 = 1$, $c_5 = 1$. From these numbers, we can find $s_1(253815) = -\deg \sum_{\alpha \in \mathbb{F}_8} \frac{1}{(t+\alpha)^{253815}}$, calculating first

$$u = 6 + 5 \cdot 8 + 3 \cdot 8^2 + 3 \cdot 8^3 + 1 \cdot 8^4 + 1 \cdot 8^5$$

and then

$$\begin{aligned} s_1(253815) &= 253814 + 8 + (6 + 5 \cdot 8 + 3 \cdot 8^2 + 3 \cdot 8^3 + 1 \cdot 8^4 + 1 \cdot 8^5) \cdot 7 \\ &= 253822 + (38638) \cdot 7 \\ &= 253822 + 270466 \\ &= 524288. \end{aligned}$$

Example 7. Let $q = 8$, $k = 124 = 174_8$. Then $m = 2$. Easily we can see that k has inner 8 of depth $m - 1 = 1$

$$c_0 + \alpha_1 = 4 + 7 = 7 + 4 = (q - 1) + c_1$$

$$c_1 + \alpha_2 = 4 + 1 < (q - 1) \text{ with no carry over base 2;}$$

from Proposition 4 we have

$$u = c_0 + c_1 q = 4 + 4(8) = 36$$

and

$$s_1(k + 1) = s_1(125) = 124 + 8 + 7(36) = 384.$$

Then, according to Corollary 1, $s_1(k' + 1)$, for any $k' = k + aq^{m+1} = 124 + a(8^3)$ with $a \in \mathbb{Z}_{\geq 0}$, is just

$$\begin{aligned} s_1(k' + 1) &= k' + q + (q - 1)u \\ &= k' + 8 + 7(36) \\ &= 124 + a(8^3) + 8 + 252,\ a \in \mathbb{Z}_{\geq 0} \\ &= s_1(k + 1) + a(8^3) \\ &= 384 + 512a. \end{aligned}$$

Example 8. Consider $q = 9$ and let $k = 58 = 64_9$. We can see that k has inner 9 of depth $m = 1$ as follows:

$$c_0 + \alpha_1 = 4 + 6 = 8 + 2 = (q - 1) + c_1$$

$$c_1 + \alpha_2 = 2 + 0 < (q - 1) \text{ with no carry over base 3;}$$

from Proposition 4 we have

$$u = c_0 + c_1 q = 4 + 2(9) = 22$$

and

$$s_1(k + 1) = s_1(59) = 58 + 9 + 8(22) = 243.$$

Then when calculating $s_1(k' + 1)$, for any $k' = k + aq^{m+2} = 58 + a(9^3)$ with $a \in \mathbb{Z}_{\geq 0}$, we use the same value for best u, in this example $u = 22$. Then

$$\begin{aligned} s_1(k' + 1) &= k' + q + (q - 1)u \\ &= k + aq^{m+2} + q + (q - 1)u, \; a \in \mathbb{Z}_{\geq 0} \\ &= 58 + a(9^3) + 9 + 8(22) \\ &= s_1(k + 1) + a(9^3) \\ &= 243 + 243a. \end{aligned}$$

References

[1] L. Carlitz, On certain functions connected with polynomials in a Galois field, Duke Math. 1 (1935), 139-158.

[2] J. Diaz-Vargas, Riemann hypothesis for $\mathbb{F}_q[t]$, J. Number Theory 59(2) (1996), 313-318.

[3] J. Sheats, The Riemann hypothesis for the Goss zeta function for $\mathbb{F}_q[t]$, J. Number Theory 71(1) (1998), 121-157.

[4] D. Thakur, Power sums with applications to multizeta and zeta zero distributions for $\mathbb{F}_q[t]$, Finite Fields Appl. 15 (2009), 534-552.

[5] D. Thakur, Function Field Arithmetic, World Scientific Publ., 2004.

[6] D. Wan, On the Riemann hypothesis for the characteristic p zeta function, J. Number Theory 58(1) (1996), 196-212.