JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Gebhard BÖCKLE et Dinesh S. THAKUR

Leading coefficient of the Goss Zeta value and p-ranks of Jacobians of Carlitz cyclotomic covers

Tome 29, n° 3 (2017), p. 963-995.

<http://jtnb.cedram.org/item?id=JTNB_2017__29_3_963_0>

Journal de Théorie des Nombres
de Bordeaux **29** (2017), 963–995

Leading coefficient of the Goss Zeta value and p-ranks of Jacobians of Carlitz cyclotomic covers

par Gebhard BÖCKLE et Dinesh S. THAKUR

Dedicated to Ernst-Ulrich Gekeler and to the memory of David M. Goss

Résumé. Soit $\mathbb{F}_q$ un corps fini de caractéristique p. Nous étudions la variation de la multiplicité de la pente nulle dans les composantes du module de Dieudonné (c'est-à-dire, du groupe p-divisible) associé à la Jacobienne de l'extension cyclotomique de Carlitz d'ordre $\wp$ de $\mathbb{F}_q(t)$ quand on fait varier l'idéal premier $\wp$ de $\mathbb{F}_q[t]$. Nous donnons quelques applications aux questions d'ordinarité et de calcul du p-rang des facteurs de ces Jacobiennes. Guidé par des expériences numériques, nous arrivons à nos résultats en démontrant et en conjecturant des propriétes structurales de la décomposition en facteurs premiers des sommes de puissances donnant les coefficients directeurs des valeurs de la fonction zêta de Goss aux entiers négatifs.

Abstract. Let $\mathbb{F}_q$ be a finite field of characteristic p. We study variations in slope zero multiplicities of the components of the Dieudonné module (or equivalently the p-divisible group) of the Jacobian of the $\wp$-th Carlitz cyclotomic extension of $\mathbb{F}_q(t)$, as we vary the prime $\wp$ of $\mathbb{F}_q[t]$. We also give some applications to the question of ordinariness and of p-ranks of the factors of these Jacobians. We do this, guided by numerical experiments, by proving and guessing some interesting structural patterns in prime factorizations of power sums representing the leading terms of the Goss zeta function at negative integers.

1. Introduction

The Herbrand–Ribet theorem [15], generalizing Kummer's work componentwise, connects divisibilities by a prime p of certain Bernoulli numbers

Manuscrit reçu le 2 octobre 2016, révisé le 29 janvier 2017, accepté le 3 février 2017.
2010 *Mathematics Subject Classification.* 11M38, 14H05, 11R60, 14H40.
Mots-clefs. Bernoulli number, Artin–Schreier polynomial, Herbrand–Ribet theorem, Carlitz cyclotomic field, Hasse–Witt invariant, Goss ζ-function, power sum, ordinariness.
G.B. was supported by the DFG programs FG 1920 and SPP 1489 (in a joint project with FNR Luxembourg). D.T. was supported in part by NSA grants 98230-14-1-0162 and 98230-15-10318.

(or rather zeta values at negative integers) with non-vanishing of certain p-parts of class group components for the cyclotomic fields $\mathbb{Q}(\zeta_p)$.

We have analogs of these results in the function field arithmetic by [10] of Goss and Sinnott, connecting the Carlitz–Goss zeta values $\zeta(-k,1) \in \mathbb{F}_q[t]$, in the notation introduced below, at negative integers $-k$, to certain class group components for the Carlitz cyclotomic fields. Due to the lack of a known functional equation, the corresponding questions for zeta values at positive integers, studied for instance by Okada, Goss and Taelman [9, 20, 22], are not known to be easily connected. For more discussion on the two sets of Bernoulli analogs, and on the arithmetic and analytic properties of this zeta function, we refer the interested reader to [9, Ch. 8], [22, Ch. 5].

The class group of a smooth curve over $\mathbb{F}_q$ is the group of $\mathbb{F}_q$-rational points of its Jacobian. Following Shiomi [17, 18], we look instead at the p-torsion, and study related questions of ordinariness and p-rank of the Jacobian. But we look at the finer component analysis: a vague analogy being that of moving to the Herbrand–Ribet type component analysis from the Kummer type aggregate analysis.

A cohomological analysis of L-values is well-known, by works of Weil, Artin, or by Serre, Manin in this context. Related explicit calculations in the Carlitz cyclotomic case, by Galovich and Rosen, and "double congruences", by Goss and Sinnott, were applied by Shiomi to show that the divisibility of the leading coefficient $\overline{S}(k)$ of Goss' zeta value $\zeta(-k,X) \in \mathbb{F}_q[t,X]$ (for negative integers $-k$ in a certain range), as a polynomial in X, by a prime $\wp$ of $\mathbb{F}_q[t]$ is linked to the question of ordinariness of the Jacobian of the $\wp$-th Carlitz cyclotomic cover.

We will recall more details of the above geometric interpretation in Section 3. There we will see that for q a prime, the divisibility of $\overline{S}(k)$ by $\wp$ for some $k < q^{\deg \wp} - 1$ indicates whether the slope zero multiplicity of the k-th component of the Dieudonné module of the Jacobian for $\wp$ is lower than a natural "generic multiplicity" for k. We call $\wp$ *exceptional for* k if $k < q^{\deg \wp} - 1$ and if $\wp$ divides $\overline{S}(k)$, and we call k *exceptional* if some $\wp$ is exceptional for k, cf. Definition 5.1. We also have results if q is not a prime, but for simplicity, throughout the introduction, we will often assume that q is prime.

The main technique of this article is to explore and exploit the factorization of the leading term $\overline{S}(k)$. This investigation begins in Section 4 and continues for the remainder of the article. Our methods are mainly of combinatorial nature, and so from Section 4 on, we will only use the elementary language of power sum factorization, except to record implications for the geometric questions.

Section 4 starts with an important combinatorial formula from [24] (Theorem 4.2) for power sums, in terms of the base q digit expansion of the

exponent. We use it in the proof of Theorem 4.6 which identifies a large "regular" part of the prime factorization in $\mathbb{F}_q[t]$ of the leading coefficient $\overline{S}(k)$ in X of $\zeta(-k, X)$.

Let us briefly explain this result which is one of the main novelties of the present article: Let $k \in \mathbb{Z}_{\geq 0}$ have base q expansion $k = \sum_{i \geq 0} c_i q^i$ with $0 \leq c_i \leq q-1$. Set $r_{i,j} := \max(c_i + c_j - (q-1), 0)$. The *regular part* for k is defined as

$$R(k) := \prod_{0 \leq j < i} (t^{q^i} - t^{q^j})^{r_{i,j}}.$$

Note that since "the bracket" $[m] := t^{q^m} - t$ is the product of all monic irreducible polynomials of $\mathbb{F}_q[t]$ of degree dividing m, we understand the prime factorization of $R(k)$ very well.

Theorem A (Theorem 4.6)**.** *If q is a prime, then $R(k)$ divides $\overline{S}(k)$.*

If q is prime, we call k *regular* if $\overline{S}(k)/R(k) \in \mathbb{F}_q^*$, and *irregular* otherwise. The *irregular part of* k is defined as $I(k) = \overline{S}(k)/R(k)$. If $q = 2$, then any k is regular (Corollary 4.4). For general q we give various families of k which are regular (Corollary 4.4, Corollary 4.10). We completely characterize (Corollary 5.11) the regular k's, for $q = 3$ and give partial results and conjectures in general.

In Sections 5 and 6, we focus on studying various aspects of the "exceptional" part responsible for the drop of generic multiplicity, by proving and conjecturing its relations (Proposition 5.5, Hypothesis (H6.1), Corollary 5.11) with the "irregular" part and on applying our results to geometric questions (Proposition 6.5, Corollary 5.13). Here is one example:

Theorem B (Proposition 5.5 (1))**.** *If k is exceptional, then k is irregular.*

What we find remarkable but are unable to prove is that if $q = p$ is a prime, then a strong partial converse (see Hypothesis (H6.1) and remarks following it) seems to hold as well. More precisely, Hypothesis (H6.1) (2) says that when q is a prime, then k irregular implies k is "weakly exceptional" in the sense that the irregular part $I(k)$ is divisible by some prime (but not by all primes of that degree), which is exceptional for some k' (but not necessarily exceptional for k). More striking is the particular case of irregular k that are not divisible by q, and that have the highest and the lowest base q digits different from $q-1$. According to Hypothesis (H6.1) (1) these k are exceptional. Theorem 5.9 and Proposition 5.5 (7) explain the link between the two. (See also Remark 6.2 (a)).

Computations show further interesting phenomena related to these divisibility questions, and thus to the geometric questions indicated above, with similar complexity and flavor as well-known questions about Bernoulli numbers. For example, while we can show (Theorem 5.4) infinitude of "exceptional" primes, the question of infinitude of "non-exceptional" primes

(analogous to classical regular primes) is open. Computations also reveal interesting connections (some of which we can prove) of this geometric phenomena to combinatorics of digits of k base q (Proposition 5.6, Theorems 5.7 and 5.9, Corollary 5.10, Hypothesis (H6.4)) and special primes such as Artin–Schreier primes (Theorems 5.17 and 5.19). We prove some results, raise many questions and provide some guesses. Let us give one example of a surprising result that we guessed based on data and that eventually we could prove:

Theorem C (Theorem 5.9)**.** *Suppose the base q expansions of $k, k' \in \mathbb{Z}_{\geq 0}$ differ in one place where the digits are 0 and $q-1$, respectively, and that q is prime. Then $I(k)$ and $I(k')$ agree up to a (predictable) sign.*

We end this introduction by expressing the hope that some of these structural results will turn out to have interesting Iwasawa theoretic number field analogs in view of the well-known analogies due to Weil and Iwasawa.

Acknowledgments. We thank Ching-Li Chai for explanations regarding the Section 3, and Alejandro Lara Rodriguez for some corrections. Many results presented here are based on experiments with the computer algebra systems Magma, Maple, Maxima and Sage, [4, 13, 14, 25].

It is our pleasure to dedicate this work to David Goss and Ernst-Ulrich Gekeler. David's work [9, 10] on zeta, and Ernst's work [8] on power sums and their factorization beyond Carlitz–Lee, are intimately related to the theme of this paper. We are both saddened by the untimely recent death of our friend David during the revisions of this work.

2. Goss zeta values for $\mathbb{F}_q[t]$

2.1. Notation.

$$\begin{aligned}
\mathbb{Z} &= \{\text{integers}\}\\
\mathbb{Z}_{\geq 0} &= \{\text{nonnegative integers}\}\\
q &= \text{a power of a fixed prime number } p\\
A &= \mathbb{F}_q[t]\\
A_+ &= \{\text{monics in } A\}\\
A_{d+} &= \{\text{monics in } A \text{ of degree } d\}\\
K &= \mathbb{F}_q(t)\\
[n] &= t^{q^n} - t\\
k &= \text{a positive integer}\\
\ell(k) &= \text{sum of the digits of the base } q \text{ expansion of } k\\
\mathcal{L}(k) &= \min_{i=0}^{e-1} \lfloor \ell(p^i k)/(q-1) \rfloor, \text{if } q = p^e\\
\deg &= \text{function assigning to } a \in A \text{ its degree in } t, \deg(0) = -\infty\\
(c_0, \ldots, c_m)_q &= \textstyle\sum_{i=0}^{m} c_i q^i \text{ for } c_i \text{ with } 0 \leq c_i < q
\end{aligned}$$

2.2. Power sums and Zeta values. For $d \in \mathbb{Z}_{\geq 0}$, put

$$S_d(-k) := \sum_{a \in A_{d+}} a^k \in A, \quad s_d(-k) = \deg(S_d(-k)) \in \mathbb{Z}_{\geq 0} \cup \{-\infty\}.$$

Observe the elementary but useful formula $S_d(-kp^i) = S_d(-k)^{p^i}$ for $i \geq 0$. It follows [22, Cor. 5.6.2] from Carlitz' work that for $k > 0$, $S_d(-k) = 0$ if $d > \ell(k)/(q-1)$, so that

$$\zeta(-k, X) := \sum_{d=0}^{\infty} S_d(-k) X^d$$

lies in $A[X]$. From the work of Carlitz (q prime case) and Sheats (general case stated by Carlitz and proved by Sheats), we know that $S_d(-k) = 0$ if and only if $d > \mathcal{L}(k)$ (see [1], [8, Rk. 2.11] and [23, A.5]). When q is prime, this condition simplifies to $d > \lfloor \ell(k)/(q-1) \rfloor$. Hence

$$\deg_X \zeta(-k, X) = \mathcal{L}(k) \tag{2.1}$$

and the "leading term" of the Goss zeta value $\zeta(-k, X)$ is

$$\overline{S}(k) = S_{\mathcal{L}(k)}(-k).$$

We also put $\overline{s}(k) = \deg(\overline{S}(k)) \in \mathbb{Z}_{\geq 0}$.

Definition 2.1. *For a given q, we call k* optimum*, if*

$$\mathcal{L}(k) = \lfloor \ell(k)/(q-1) \rfloor.$$

Note that all k are optimum, when q is a prime. If $\mathcal{L}(k) = \lfloor \frac{\ell(p^i k)}{q-1} \rfloor$, then

$$\overline{S}(k) = S_{\lfloor \ell(p^i k)/(q-1) \rfloor}(-p^i k)^{1/p^i}. \tag{2.2}$$

This allows us to reduce calculations to only optimum k's.

We record the following result on digit permutation of optimum k whose proof we leave as an exercise in expressing $\ell(k)$ in terms of the base p expansion of k.

Lemma 2.2. *Let $k, f \in \mathbb{Z}_{\geq 0}$ with $0 \leq k < q^f - 1$. For $i \in \mathbb{Z}_{\geq 0}$, let $k' \in \mathbb{Z}_{\geq 0}$ be unique with $0 \leq k' < q^f - 1$ and $k' \equiv p^i k \pmod{(q^f - 1)}$. Then $\ell(p^{i+j} k) = \ell(p^j k')$ for all $j \in \mathbb{Z}_{\geq 0}$, and hence $\mathcal{L}(k) = \mathcal{L}(p^i k) = \mathcal{L}(k')$, and $p^i k$ is optimum if and only if k' is so.*

3. Geometric interpretation of Zeta leading coefficient divisibility

Let F be a global function field with constants $\mathbb{F}_q$ with corresponding non-singular projective model X and Jacobian J. The dimension λ_F of the group of p-torsion points $J[p](\overline{\mathbb{F}}_p)$ over $\mathbb{Z}/p\mathbb{Z}$ is called the p-rank or the Hasse–Witt invariant of F, X or J. The Jacobian is *ordinary* if λ_F is maximal possible, i.e., equal to the genus g_X of X, or, equivalently, to the

dimension of J. It is well-known (see e.g., [12, Thm.1], [19, Satz 1], [16, Prop. 11.20], [17], [18]) that λ_F is the degree of the reduction mod p of the numerator $L_F(u)$ of the classical Hasse–Weil zeta function $Z_F(u) = L_F(u)/(1-u)(1-uq)$ of F. A simple proof is given in [19].

The polynomials $L_F(u)$ have been calculated, starting with Artin for F a quadratic cover of K, for many global function fields F. For Carlitz cyclotomic extensions of K (see e.g., [7]), $L_F(u)$ can be expressed in terms of character sums of A_{d+}. To explain this, we fix some notation. For a (monic) prime $\wp$ of A, denote by $(F =)K_\wp$ the function field obtained by adjoining to K the $\wp$-torsion of the Carlitz A-module, by $G_\wp$ its Galois group $\mathrm{Gal}\,(K_\wp/K)$, by $\alpha_\wp\colon (A/\wp)^\times \to G_\wp$ the canonical isomorphism defined by the action of $A/\wp$ on the $\wp$-torsion points in $K_\wp$, by $X_\wp$ the cover of $\mathbb{P}^1_{\mathbb{F}_q}$ corresponding to $K \to K_\wp$, and by $J_\wp$ the Jacobian of $X_\wp$. Observe that $G_\wp$ is cyclic of order $q^{\deg \wp} - 1$. For a character $\chi\colon G_\wp \to \overline{\mathbb{Q}}^\times$, let $s_d(\chi) = \sum_{a\in A_{d+}} \chi(\alpha_\wp(a))$ and $L_\chi(u) = \sum_{d=0}^{\deg\wp - 1} s_d(\chi) u^d \in \overline{\mathbb{Q}}[u]$ as in [7]. Set $\Phi_\chi(u) = L_\chi(u)/(1-u)$ if $\chi(\alpha_\wp(\mathbb{F}_q^*)) = \{1\}$, and $\Phi_\chi(u) = L_\chi(u)$ otherwise; see [18, p. 526]. Then by [7] one has the factorization

$$L_{K_\wp}(u) = \prod_{\chi\in \mathrm{Hom}(G_\wp,\overline{\mathbb{Q}}^\times)\setminus\{\mathrm{triv}\}} \Phi_\chi(u)\,.$$

For a suitable embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, one can identify the characters χ with powers $\chi_\wp^k$ of the Teichmüller lift $\chi_\wp\colon G_\wp \to \overline{\mathbb{Q}}_p^\times$ of the isomorphism $\alpha_\wp^{-1}$. By the double congruences of Goss and Sinnott [9, 10] this gives for any $k \in \{1,\dots,\#G_\wp - 1\}$ the formula

$$\zeta(-k,X) \pmod{\wp} = L_{\chi_\wp^{-k}}(X) \pmod{p}, \tag{3.1}$$

which was explicitly noticed and exploited by Shiomi in [17, 18] to give a criterion for when $J_\wp$ is ordinary. We shall reinterpret his idea of proof to give a geometric meaning to the results we shall investigate in the remainder of this article, and also give a proof of his result after this reinterpretation.

For this we introduce some notions from covariant Dieudonné theory, see [6, App. B]. Denote by $T_p(J_\wp)$ the Dieudonné module of $J_\wp$ tensored over the central ring $\mathbb{Z}_p$ with the ring of Witt vectors $W(A/\wp)$. Thus $T_p(J_\wp)$ is a module over the (generally) non-commutative Dieudonné ring $E = W(\mathbb{F}_q)[F,V]/(FV-p) \otimes_{\mathbb{Z}_p} W(A/\wp)$, and it is free as a module over $W(\mathbb{F}_q) \otimes_{\mathbb{Z}_p} W(A/\wp)$. Recall that any Dieudonné module has a set of slopes with multiplicities; if $q = p^e$, then $\frac{1}{e}$ times the p-valuation of any eigenvalue of the $W(\mathbb{F}_q) \otimes_{\mathbb{Z}_p} W(A/\wp)$-linear operator F^e acting on such a module is called a slope, and for each slope, the sum of the dimensions of the corresponding eigenspaces is called its multiplicity. The slopes lie in the closed interval $[0,1]$, and the formation of the Cartier dual $M^\vee$ of a Dieudonné

module, exchanges the multiplicity of slope s of M with that of slope $1-s$ of $M^\vee$.

The action of $G_\wp$ on $J_\wp$ gives rise to an action of $W(A/\wp)[G_\wp]$ on $T_p(J_\wp)$ that commutes with the action of E. Moreover for each character $\chi_\wp^k$ one obtains an idempotent $e_{\chi_\wp^k} \in W(A/\wp)[G_\wp]$ such that $e_{\chi_\wp^k} W(A/\wp)[G_\wp]$ is free over $W(A/\wp)$ of rank 1. Consequently we have a direct sum decomposition $T_p(J_\wp) = \bigoplus_k e_{\chi_\wp^k} T_p(J_\wp)$ where each factor $T_p(J_\wp)_k := e_{\chi_\wp^k} T_p(J_\wp)$, $k \in \mathbb{Z}/(\#G_\wp)$, is again a Dieudonné module; note that $J_\wp$ does not allow for such a decomposition.

The pairing on $T_p(J_\wp)$ induced by the canonical principal polarization on $J_\wp$, identifies $T_p(J_\wp)_{\#G_\wp - k}$ with the Cartier dual of $T_p(J_\wp)_k$. We call a Dieudonné module $M \neq 0$ *ordinary* if the slope zero multiplicity of M is half of the dimension of M. Then Dieudonné theory yields that $J_\wp$ is ordinary if and only if the associated module $T_p(J_\wp)$ is ordinary. The pairing on $T_p(J_\wp)$ now immediately yields:

Proposition 3.1. *The Jacobian $J_\wp$ is ordinary if and only if the Dieudonné modules $M_{\wp,\pm k} := T_p(J_\wp)_k \oplus T_p(J_\wp)_{\#G_\wp - k}$ are ordinary for all k.*

Let $\varepsilon_{k,q} := 1$, if $q-1$ divides k, and $\varepsilon_{k,q} := 0$, otherwise.

Lemma 3.2.

(1) $\dim T_p(J_\wp)_k = \deg_u \Phi_{\chi_\wp^k}(u) = \deg \wp - 1 - \varepsilon_{k,q}$.

(2) *The slope zero multiplicity of $T_p(J_\wp)_k$ is equal to the $A/\wp$-dimension of the $\chi_\wp^k$-component of $J_\wp[p](\overline{\mathbb{F}}_p) \otimes_{\mathbb{F}_q} A/\wp$, which in turn is equal to*

$$\deg_X(\zeta(-k,X) \pmod{\wp}) - \varepsilon_{k,q} = \deg_u(L_{\chi_\wp^{-k}}(u) \pmod{p}) - \varepsilon_{k,q}\,.$$

Sketch of proof: Part (1) follows by comparison of the characteristic polynomials of Frobenius for ℓ-adic and p-adic Tate-modules of abelian varieties. The bridge between the two is given by the Tate conjecture, which is known over finite fields, cf. [26, §1]. It links ℓ- and p-adic Frobenii to the Frobenius in the endomorphism ring $\mathrm{End}(J_\wp)$ of $J_\wp$. Enlarging the latter ring to $\mathrm{End}(J_\wp) \otimes_{\mathbb{Z}} \mathbb{Q}(\zeta_\wp)$, which contains $\mathbb{Q}(\zeta_\wp)[G_\wp]$ in its center, where $\zeta_\wp$ is a primitive $\#G_\wp$-th root of unity, one can naturally decompose the characteristic polynomial of Frobenius in its $\chi_\wp^k$-components. Part (2) follows from [2, Thm. 9.11] (we note that in part (c) of the quoted theorem the symbol $C_{K,\mathfrak{p}}$ has to be replaced by C_{H^+}). □

Remark 3.3. For fixed k, we have $\deg_X(\zeta(-k,X) \pmod{\wp}) = \mathcal{L}(k)$ for all but finitely many $\wp$, and so $\mathcal{L}(k)$ can be regarded as the *generic slope zero multiplicity* of $T_p(J_\wp)_k$.

If we fix $\wp$, then for all $k, m \geq 0$ a simple congruence argument shows $S_d(-k) \equiv S_d(-k - m\#G_\wp)$ for all $d \geq 0$, and hence

$$\deg_X(\zeta(-k,X) \pmod{\wp}) = \deg_X(\zeta(-k - m\#G_\wp, X) \pmod{\wp})\,.$$

Therefore for fixed $\wp$, only the $k \in \{1, \dots, \#G_\wp - 1\}$ carry interesting information, and for k outside this range, the number $\mathcal{L}(k)$ cannot be regarded as the generic slope zero multiplicity.

Turning things around, we call $\wp$ exceptional for k if $k < q^{\deg \wp} - 1$ and if the leading term of $\zeta(-k, X)$ vanishes modulo $\wp$, cf. Definition 5.1. Such $\wp$ are analogous to Kummer's irregular primes in number theory; cf. Proposition 3.4.

Let us begin by a simple but key observation contained in [18], whose proof is straightforward: If $0 < k < \#G_\wp$, then

$$\left\lfloor \tfrac{\ell(k)}{q-1} \right\rfloor + \left\lfloor \tfrac{\ell(\#G_\wp - k)}{q-1} \right\rfloor = \deg \wp - 1 + \varepsilon_{k,q}. \tag{3.2}$$

Proposition 3.4. *For $0 < k < \#G_\wp$, the Dieudonné module $M_{\wp,\pm k}$ is ordinary if and only if k and $\#G_\wp - k$ are optimum and not exceptional for $\wp$, i.e., if and only if*

$$\deg_X \zeta(-k, X) \pmod{\wp} = \left\lfloor \tfrac{\ell(k)}{q-1} \right\rfloor \quad \textit{and}$$
$$\deg_X \zeta(k - \#G_\wp, X) \pmod{\wp} = \left\lfloor \tfrac{\ell(\#G_\wp - k)}{q-1} \right\rfloor.$$

Proof. Consider the chain of (in)equalities

$$\begin{aligned}
&\tfrac{1}{2} \dim M_{\wp,\pm k} \\
&\overset{\text{Lemma 3.2(1)}}{=} \deg \wp - 1 - \varepsilon_{k,q} \\
&\overset{(3.2)}{=} \Big(\left\lfloor \tfrac{\ell(k)}{q-1} \right\rfloor - \varepsilon_{k,q} \Big) + \Big(\left\lfloor \tfrac{\ell(\#G_\wp - k)}{q-1} \right\rfloor - \varepsilon_{k,q} \Big) \\
&\overset{(2.1)}{\geq} \Big(\deg_X \zeta(-k, X) - \varepsilon_{k,q} \Big) + \Big(\deg_X \zeta(-(\#G_\wp - k), X) - \varepsilon_{k,q} \Big) \\
&\overset{\text{Lemma 3.2(2)}}{\geq} \text{slope zero multiplicity of } M_{\wp,\pm k}.
\end{aligned}$$

Now $M_{\wp,\pm k}$ is ordinary if and only if there exists an equality between the outer terms, and this is precisely the equivalence of the first and last assertion of the proposition. The equivalence of the last to the middle assertion is immediate from equation (2.1) and the definition of optimum. □

Corollary 3.5 ([18, Thm. 1.1])**.** *The Jacobian $J_\wp$ is ordinary if and only if for all $k \in \{1, \dots, \#G_\wp - 1\}$ one has $\deg_X \zeta(-k, X) \pmod{\wp} = \lfloor \frac{\ell(k)}{q-1} \rfloor$.*

Note that when q is prime, exceptionality is the only source for non-ordinariness in Proposition 3.4, but when q is not a prime, non-optimality in the pair matters.

Suppose $0 < k < \#G_\wp$ is optimum, but kp^i is not. Then equation (3.2) together with Lemma 2.2 imply that $\#G_\wp - k$ cannot be optimum. Thus we deduce from Proposition 3.4 also the following result:

Corollary 3.6. *Let $\wp$ be a prime of A and $k \in \mathbb{Z}$ with $0 < k < \#G_\wp$. Suppose kp^i is not optimum for some $i \in \mathbb{Z}_{\geq 0}$. Then $M_{\wp,\pm k'}$ is non-ordinary for all $0 < k' < \#G_\wp$ such that $k' \equiv kp^i \pmod{q^{\deg \wp} - 1}$ for some $i \in \mathbb{Z}_{\geq 0}$.*

Now if q is not a prime, there is always a $k < q^2 - 1$ that is not optimum, for instance $k = (p, q-p)_q$, so that $k/p = (1, \frac{q}{p} - 1)_q$. It follows that $J_\wp$ is never ordinary if $q \neq p$ and $\deg \wp > 1$, see [18, Cor. 3.1].

One can also directly decompose $J_\wp$ under the action of $G_\wp$ induced from its action on the (ramified) covering $X_\wp$ over $\mathbb{P}^1_{\mathbb{F}_q}$. This allows one to identify the group ring $\mathbb{Q}[G_\wp]$ as a subring of the rational endomorphism ring $\mathrm{End}(J_\wp) \otimes_{\mathbb{Z}} \mathbb{Q}$. The ring $\mathbb{Q}[G_\wp]$ is isomorphic to the product $\times_{d|\#G_\wp} \mathbb{Q}(\zeta_d)$ of cyclotomic fields, where ζ_d is the $\#G_\wp/d$-th power of $\zeta_\wp$. If e_d denotes the idempotent corresponding to $\mathbb{Q}(\zeta_d)$, then $J_\wp$ is isogenous to $\times_{d|\#G_\wp} J_{\wp,d}$ with $J_{\wp,d} = e_d J_\wp$; see [11] for further details on this type of decomposition. For the associated Dieudonné module, one verifies $T_p(J_{\wp,d}) \cong \bigoplus_{k:\mathrm{ord}(\chi_\wp^k)=d} T_p(J_\wp)_k \cong \bigoplus_{k:\mathrm{ord}(\chi_\wp^k)=d} M_{\wp,\pm k}$, where the sum is over all k such that $\chi_\wp^k$ has some fixed order d. In particular, the decomposition of $J_\wp$ under $G_\wp$ is less fine than that of $T_p(J_\wp)$ into its k-components.

Let us recall yet another geometric interpretation of $\zeta(-k, X)$ via the cohomology of function field crystals from [3], as detailed in [2, Sects. 8 and 9]. It is the (dual) characteristic polynomial of the cohomology of a function field crystal over $\mathbb{P}^1_{\mathbb{F}_q}$ which arises from the k-th tensor power of the Carlitz t-motive. This cohomology takes values in a category of A-modules that carry a linear endomorphism. The reduction of the cohomology modulo a prime $\wp$ of A arises from a function field crystal built out of the k-th tensor power of the Carlitz t-motive modulo $\wp$, and its (dual) characteristic polynomial is $\zeta(-k, X) \pmod{\wp}$. The cohomological approach also gives an explicit expression for $\zeta(-k, X)$. Write $k = \sum c_n q^n$ in base q-expansion, and let M_k denote the square matrix of size $\lfloor \frac{\ell(k)}{q-1} \rfloor$ whose (i,j)-th entry is the $(jq - i)$-th coefficient of $g(x) := \prod (t^{q^n} - x)^{c_n}$. Then

$$\zeta(-k, X) = \det(1 - XM_k)\,.$$

If in particular k is optimum for q, then $\lfloor \frac{\ell(k)}{q-1} \rfloor = \mathcal{L}(k) = \deg_X \zeta(-k, X)$, so that $\overline{S}(k) = \det(-M_k)$. For non-optimum k, we use formula (2.2). This allows one to compute $\overline{S}(k)$ as the determinant of a square matrix of size $\mathcal{L}(k)$, which is typically small, though possibly with large degree entries in A. We used the above formula for $\overline{S}(k)$ in our computer calculations.

The following sections will investigate the property of $\wp$ being exceptional in detail. We focus on the individual components $T_p(J_\wp)_k$ for k fixed whose generic slope zero multiplicity is $\mathcal{L}(k)$ and investigate for which $\wp$ the actual multiplicity is smaller. We do not calculate the exact decrement of

ranks, but focus instead on when (rather than how much) the degree drops from the maximum generic one. We will find a lot of interesting arithmetic information in this question. For explicit results (and conjectures) on k-components, see for instance Corollary 4.10 (in combination with Proposition 5.5), Corollaries 5.10 and 5.11, and Hypothesis (H6.1)(1).For further results on ordinariness, see Proposition 6.5 for $J_{\wp}$, and Corollary 5.13 for some $J_{\wp,d}$.

4. Zeta leading coefficient

Theorem 4.2 below recalls an explicit formula for the zeta leading coefficient $\overline{S}(k)$. The formula has many applications. One important consequence is a partial factorization of $\overline{S}(k)$ derived in Theorem 4.6.

As we shall use the terminology of multisets, we wish to clarify some notation.

Definition 4.1. *Let M be a set and $D \subset \mathbb{Z}_{\geq 1}$ be a finite subset.*

An indexed multiset over M with index set D *is a map $f\colon D \to M$ (or more precisely, a triple (D, M, f)).*

An ordered partition *of an indexed multiset (D, M, f) is an ordered partition $(D_0, \dots, D_d)$ of D; its* type *is the tuple $(|D_0|, \dots, |D_d|)$. For every D_i this defines the indexed multiset $(D_i, M, f|_{D_i})$.*

The multiset corresponding to an indexed multiset (D, M, f) is the pair (M, g) with the map $g\colon M \to \mathbb{Z}_{\geq 0}, m \mapsto |f^{-1}(m)|$. Each $m \in M$ then occurs with multiplicity $g(m)$ in the multiset (M, g).

From now on we write the base q expansion of k as $k = \sum c_i q^i$, with $0 \leq c_i < q$. We also write k as $\sum q^{k_i}$, where k_i is a monotonically increasing sequence of non-negative integers with no more than $q-1$ of the k_i's being the same. We shall regard $k_\bullet\colon D = \{1, \dots, \ell(k)\} \to M = \mathbb{Z}_{\geq 0}, i \mapsto k_i$ as an indexed multiset. If $(D_0, \dots, D_d)$ is a partition of D of type $(t_0, \dots, t_d)$ (with $t_i \in \mathbb{Z}_{\geq 1}$), let $k_{i,\bullet}\colon \{1, \dots, t_i\} \to M$ be the composition of $k_\bullet|_{D_i}$ with the unique increasing bijection $\{1, \dots, t_i\} \to D_i$.

Theorem 4.2 ([24, Thm. 12])**.** *Let $k > 0$ and $\ell(k) = (q-1)d + r$, with $0 \leq r < (q-1)$, so that $d = \lfloor \ell(k)/(q-1) \rfloor$. Write the base q-expansion $k = \sum_{i=1}^{d(q-1)+r} q^{k_i}$. Then*

$$S_d(-k) = (-1)^d \sum t^{\sum_{i=1}^{d} (d-i) \sum_{j=1}^{q-1} q^{k_{i,j}} + d \sum_{j=1}^{r} q^{k_{0,j}}}$$

where the sum is over all ordered partitions $(D_0, \dots, D_d)$ of type $(r, q-1, q-1, \dots, q-1)$ of $(D, M, k_\bullet)$, and with the $k_{i,\bullet}$ as introduced above.

This formula allows us to write the leading term $\overline{S}(k) = S_{\mathcal{L}(k)}(-k)$ immediately as a polynomial, when q is a prime or more generally when $\mathcal{L}(k) = \lfloor \ell(k)/(q-1) \rfloor$. In the general case $q = p^e$, we get the leading term

by replacing k by any $p^i k$ $(0 \le i < e)$ such that $\mathcal{L}(k) = \lfloor \ell(p^i k)/(q-1) \rfloor$ and using that $S_d(-p^i k) = S_d(-k)^{p^i}$. Thus, in general, the power sum in Theorem 4.2 represents either $\overline{S}(k)$ or zero.

Examples 4.3. Let $q = 3, k = 38 = 27 + 9 + 1 + 1$, so that $d = 2$ and our formula gives $S_d(-k) = t^{27+9} + 2t^{27+1} + 2t^{9+1} + t^2$. Similarly, for example, if $q = 3$, $k = 3^5 + 3^4 + \cdots + 1$, so that $\ell(k) = 6$ and $d = 3, r = 0$, then $\overline{S}(k)$ has $6!/(2!2!2!) = 90$ terms.

Our evaluation factorizes $S_2(-38) = [3][2]$. Note the fact that $[n]$ is the product of all the irreducible polynomials in A_+ of degree dividing n. So we understand prime factorization immediately. We will see that this is a much more general phenomenon.

Corollary 4.4 ([24, Cor. 13])**.** *Suppose $k = (q-1)\sum_1^d q^{u_i} > 0$, with $u_i \in \mathbb{Z}_{\ge 0}$ distinct and increasing with i. Then we have the leading term*

$$S_d(-k) = (-1)^d \prod_{d \ge n > m} (t^{q^{u_n}} - t^{q^{u_m}})^{q-1} = \prod [u_n - u_m]^{q^{u_m}(q-1)}.$$

Remarks 4.5.

(a) For $q = 2$, any k is of the form in the corollary. In this case the product formula was obtained earlier by Richard Pink using a cohomological formula for the leading power sum. See [1, 7.1] for this as well as the proof of Corollary 4.4 using the Vandermonde determinant formula combined with the cohomological machinery.

(b) When $q > 2$, we do not have a product formula involving only monomials in $[n]$'s, in the general case, for the leading term, even if q is a prime. For example, when $q = 3$, $k = 13$, $S_1(-13) = -(t^3 - t)(t^3 - t + 1)(t^3 - t - 1)$.

Let us put

$$r_{i,j} := \max(c_i + c_j - (q-1), 0),$$

and consider the *regular part*

$$R(k) := \prod_{i>j} (t^{q^i} - t^{q^j})^{r_{i,j}} = \prod_{i>j} [i-j]^{q^j r_{i,j}}, \tag{4.1}$$

where the product is over all $0 \le j < i$. Note that $r_{i,j} = 0$ as soon as $i > \max\{s \mid c_s \ne 0\}$. The following is the first main result.

Theorem 4.6. *Let the notation be as in Theorem 4.2. Then $R(k)$ divides $S_d(-k)$. In particular, for optimum k, $R(k)$ divides $\overline{S}(k)$.*

Example 4.7. We warn the reader that if k is not optimum, then $R(k)$ need not divide $\overline{S}(k)$: Let $q = 4$ and $k = 21 = (1\,1\,1)_4$. Then $R(k) = \overline{S}(k) = \overline{S}(2k) = 1$, but $R(2k) = t^{36} + t^{33} + t^{24} + t^{18} + t^9 + t^6$. Here $2k$ is not optimum and $R(2k)$ does not divide $\overline{S}(2k)$. The next such k are 23, 29, 69, 71 etc.

For the proof of Theorem 4.6, we need a lemma. We use the following notation. For an $m \times n$-matrix M we denote by $\sum_c M$ and $\sum_r M$ the sum of the columns and rows of M, respectively, so that for instance $\sum_c M$ is an $m \times 1$ column vector. The notation also applies to row and columns vectors, regarded as $1 \times n$- and $m \times 1$-matrices.

Lemma 4.8. *The following formulas hold for binomial and multinomial coefficients:*

(1) *Let $a, b \in \mathbb{Z}_{\geq 0}$, and let $\underline{f} = (f_0, \dots, f_d) \in \mathbb{Z}_{\geq 0}^{d+1}$ with $\sum_c \underline{f} = a + b$. Then*

$$\sum_{a_0=0}^{f_0} \sum_{a_1=0}^{f_1} \cdots \sum_{a_{d-1}=0}^{f_{d-1}} \binom{a}{\underline{a}} \binom{b}{\underline{f} - \underline{a}} = \binom{a+b}{\underline{f}},$$

where $\underline{a} = (a_0, \dots, a_d)$ and a_d is determined by $\sum_c \underline{a} = a$.

(2) *Let $n_1, \dots, n_d, j \in \mathbb{Z}_{\geq 0}$. Then*

$$\binom{n_1 + \cdots + n_d}{j} = \sum_{\substack{\underline{j}=(j_1,\dots,j_d) \in \mathbb{Z}_{\geq 0}^d \\ \sum_c \underline{j} = j}} \binom{n_1}{j_1} \cdot \dots \cdot \binom{n_d}{j_d}.$$

(3) *Let $d \geq 1$ and $j \geq 0$ be integers. Then there exist integers $a_{d,j,i}$, $0 \leq i \leq j$, such that for all $n \in \mathbb{Z}_{\geq 0}$ one has*

$$\binom{dn}{j} = \sum_{i=0}^{j} \binom{n}{i} a_{d,j,i}\,.$$

(4) *Let $\underline{a} = (a_0, \dots, a_d), \underline{b} = (b_0, \dots, b_d) \in \mathbb{Z}_{\geq 0}^{d+1}$, $a = \sum_c \underline{a}$ and $b = \sum_c \underline{b}$. Then*

$$\binom{a}{\underline{a}} \cdot \binom{a_0}{b_0} \cdot \dots \cdot \binom{a_d}{b_d} = \binom{a}{b} \binom{a-b}{\underline{a} - \underline{b}}.$$

Proof. Part (1) is independently due to Carlitz and Tauber; see [5] or [21]. Part (2) for $k = 2$ is a special case of (1), also known as the Cauchy summation formula or the Vandermonde convolution formula. The result for general k follows from $k = 2$ by a straightforward induction. To see (3) note that the left hand side is an integer valued polynomial in n of degree j. The set of such have the $\mathbb{Z}$-basis $n \mapsto \binom{n}{i}$, $i = 0, \dots, j$. Regarding (4) we may assume $\underline{a} \geq \underline{b}$ (entry-wise), since otherwise both sides are zero. Note

that

$$\binom{a}{\underline{a}}\binom{a_0}{b_0} = \binom{a}{a_0}\binom{a-a_0}{a_1,\dots,a_d}\binom{a_0}{b_0} = \binom{a}{b_0}\binom{a-b_0}{a_0-b_0}\binom{a-a_0}{a_1,\dots,a_d}$$
$$= \binom{a}{b_0}\binom{a-b_0}{a_0-b_0,a_1,\dots,a_d}.$$

Now (4) follows from an obvious induction that uses that $\binom{j_0+\cdots+j_d}{j_0,\dots,j_d}$ is independent of the order of the bottom entries. □

Proof of Theorem 4.6. Let us temporarily write $X_j := t^{q^j}$ and let $e = \lfloor \log_q k \rfloor$. Then Theorem 4.2 gives

$$S_d(-k) = \sum_{\underline{C}} \binom{c_0}{\underline{c}_0} \cdot \dots \cdot \binom{c_e}{\underline{c}_e} \prod_{j=0}^{e} X_j^{\sum_{i=0}^{d}(d-i)c_{ji}}, \tag{4.2}$$

where the sum is over all matrices $\underline{C} = (c_{ji})_{j=0,\dots,e,i=0,\dots,d}$ with j-th row $\underline{c}_j$, such that $\sum_r \underline{C} = (r, q-1, q-1, \dots, q-1)$, $\sum_c \underline{C} = (c_0, \dots, c_e)^t$.

We fix indices $0 \le i_0 < i_1 \le e$ as well as vectors $\underline{c}_i$ for all $i \ne i_0, i_1$, and we define the row vector $\underline{f}$ as $(r, q-1, \dots, q-1) - \sum_{j \notin \{i_0,i_1\}} \underline{c}_j$. Note that $0 \le f_0 \le r$ and $0 \le f_i \le q-1$ for $i \ge 1$. We need to show that $(X_{i_0} - X_{i_1})^{r_{i_0,i_1}}$ divides

$$\sum_{\underline{c}_{i_0},\underline{c}_{i_1}} \binom{c_{i_0}}{\underline{c}_{i_0}}\binom{c_{i_1}}{\underline{c}_{i_1}} X_{i_0}^{\sum_{i=0}^{d}(d-i)c_{i_0,i}} X_{i_1}^{\sum_{i=0}^{d}(d-i)c_{i_1,i}},$$

where the sum is over all pairs of row vectors $\underline{c}_{i_0}, \underline{c}_{i_1} \in \mathbb{Z}_{\ge 0}^{d+1}$ with $\underline{c}_{i_0} + \underline{c}_{i_1} = \underline{f}$ and $\sum_c \underline{c}_{i_j} = c_{i_j}$ for $j = 0, 1$. Let us replace X_{i_0} by $(X_{i_0} - X_{i_1}) + X_{i_1}$, write δ_X for $X_{i_0} - X_{i_1}$, apply binomial expansion, and reduce modulo $\delta_X^{r_{i_0,i_1}}$. This yields

$$X_{i_1}^{\sum_{i=0}^{d}(d-i)f_i} \sum_{\underline{c}_{i_0},\underline{c}_{i_1}} \binom{c_{i_0}}{\underline{c}_{i_0}}\binom{c_{i_1}}{\underline{c}_{i_1}} \sum_{j=0}^{r_{i_0,i_1}-1} \delta_X^j X_{i_1}^{-j} \binom{\sum_{i=0}^{d}(d-i)c_{i_0,i}}{j}.$$

We need to show that for $j = 0, \dots, r_{i_0,i_1} - 1$ the following expression vanishes

$$\sum_{\substack{0 \le \underline{c}_{i_0} \le \underline{f} \\ \sum_i c_{i_0,i} = c_{i_0}}} \binom{c_{i_0}}{\underline{c}_{i_0}}\binom{c_{i_1}}{\underline{f} - \underline{c}_{i_0}}\binom{\sum_{i=0}^{d}(d-i)c_{i_0,i}}{j}.$$

If we apply (2), (3) and (4) from Lemma 4.8, then we need to show that

$$\sum_{\substack{0 \le \underline{c}_{i_0} \le \underline{f} \\ \sum_i c_{i_0,i} = c_{i_0}}} \binom{c_{i_0} - i}{\underline{c}_{i_0} - (i_0, \dots, i_d)}\binom{c_{i_1}}{\underline{f} - \underline{c}_{i_0}} \tag{4.3}$$

vanishes for any $(i_0,\dots,i_d)\in\mathbb{Z}_{\geq 0}^{d+1}$ such that $i=i_0+\cdots+i_d\leq j\leq r_{i_0,i_1}-1$. By (1) of Lemma 4.8, the expression (4.3) is equal to

$$\binom{c_{i_0}+c_{i_1}-i}{\underline{f}-(i_0,\dots,i_d)}. \tag{4.4}$$

However $c_{i_0}+c_{i_1}-i\geq (q-1)+r_{i_0,i_1}-i\geq q$ while all entries of $\underline{f}-(i_0,\dots,i_d)$ are at most of size $q-1$, and hence the expression (4.4) is zero modulo p.

This shows that $\prod_{i<j}(X_i-X_j)^{r_{i,j}}$ divides expression (4.2) in the unique factorization domain $\mathbb{F}_q[X_0,\dots,X_e]$. Substituting back t^{q^i} for X_i, the theorem follows. □

Remarks 4.9.

(a) Note that different $t^{q^i}-t^{q^j}$'s are not relatively prime, and that is one reason we introduced variables X_i for t^{q^i}, and then proved a divisibility for a polynomial in the variables X_i, before substituting back. For the polynomial in X_i, the divisibility is often, but not always optimal. The polynomial $S_d(-k)/R(k)$ (as a polynomial in t) may well be divisible by further terms of the form $[m]$, $m\geq 1$. See Remark 5.18, Remark 6.2(f) and Hypothesis (H6.3) in Section 6.

(b) Let $q=p^e$. For $a=\prod \wp_i^{m_i}\in A$, with $\wp_i$ being distinct monic primes, we temporarily write $a\langle r\rangle=\prod \wp_i^{\lceil m_i/p^r\rceil}\in A$. Thus if a divides S^{p^i}, for some $S\in A$, then $a\langle i\rangle$ divides S. Now for $0\leq i\leq e$ such that kp^i is optimum, Theorem 4.6 shows that $R(kp^i)$ divides $S_{\mathcal{L}(kp^i)}(-kp^i)=\overline{S}(k)^{p^i}$. For k not divisible by p, we define

$$\overline{R}(k):=\operatorname{lcm}\big\{R(kp^i)\langle i\rangle \mid i\in\{0,\dots,e-1\}, kp^i \text{ is optimum}\big\},$$

and then $\overline{R}(kp^i):=\overline{R}(k)^{p^i}$ for $i\geq 1$. Then $\overline{R}(k)$ divides $\overline{S}(k)$, and $\overline{R}(kp)=\overline{R}(k)^p$ by definition. Clearly $\overline{R}(k)=R(k)$ if q is prime. For general q, even if k is optimum, it need not hold that $\overline{R}(k)=R(k)$. For instance, for $q=4$ and $k=25=(1\,2\,1)_4$ one has $R(k)=1$ and $\overline{R}(k)=t^{16}+t=\overline{S}(k)$.

While $R(k)$ is a simple monomial in the brackets, $\overline{R}(k)\in A$ can be expressed as a ratio of such monomials in a complicated way, since all primes of the same degree divide it to the same exponent. For instance, let $q=4$ and $k=155=(3\,2\,1\,2)_4$. Then $R(k)=[1]^2[2]^5[3]^2$, $R(2k)=[1]^4[2]^{18}$ and $\overline{R}(k)=[2]^9[3]^2[1]^{-2}$. Below we shall mainly focus on cases where $\overline{R}(k)=R(k)$, e.g. when q is prime.

For many families of q,k, we can prove $\overline{S}(k)=cR(k)$, with $c\in\mathbb{F}_q^*$ (which often can be made explicit, but we will ignore it as it is irrelevant

for our purpose). We write $r(k) := \deg(R(k))$, $\overline{r}(k) := \deg(\overline{R}(k))$, and recall $\overline{s}(k) = \deg \overline{S}(k)$.

Corollary 4.10. *Suppose that one of the following two conditions holds:*

(1) $k = (\sum_{i=1}^{s} q^{a_i}) - 1$ *with* $a_1 > \cdots > a_s > 0$ *and* $s < q$;
(2) $k = \sum_{i=0}^{d} a_i q^{n_i}$ *with* $0 \leq a_i \leq q-1$, $0 \leq n_0 < n_1 < \cdots < n_d$ *such that* $\mathcal{L}(k) = d$; *i.e., we require* $\mathcal{L}(k) + 1 \geq \#\{i \mid c_i \neq 0\}$ *if* $k = (c_0 \ \ldots \ c_m)_q$.

Then $\overline{S}(k)/R(k) \in \mathbb{F}_q^*$ *(and thus also* $\overline{R}(k) = R(k)$*).*

Proof. By Theorem 4.6 the term $R(k)$ divides $\overline{S}(k)$ for all k. Hence in either of the cases it suffices to show that $r(k) = \overline{s}(k)$.

Under the hypothesis of (1), we have $\mathcal{L}(k) = a_s$, and a result of Lee, [22, 5.6.4] gives

$$\overline{S}(k) = \frac{1}{L_{a_s}} \prod_{i=1}^{s} \frac{D_{a_i}}{D_{a_i - a_s}^{q^{a_s}}} = \pm \frac{\prod_{i=1}^{s} [a_i][a_i - 1]^q \ldots [a_i - a_s + 1]^{q^{a_s - 1}}}{[a_s] \ldots [1]},$$

where $L_s = \prod_{j=1}^{s} [j]$ and $D_s = \prod_{j=1}^{s} [j]^{q^{s-j}}$. To prove (1), one can either check directly that this factorization matches with $R(k)$, or, as we shall do now, one can compute degrees: For the calculation it will be useful to remember that $\deg[i] = \deg[i-j]^{q^j} = q^i$ for $0 \leq j \leq i$. We first compute

$$\begin{aligned} \overline{s}(k) &= -\deg L_{a_s} + \sum_{i=1}^{s} \deg(D_{a_i} / D_{a_i - a_s}^{q^{a_s}}) \\ &= -\sum_{i=1}^{a_s} \deg[i] + \sum_{i=1}^{s} \sum_{j=0}^{a_s - 1} \deg[a_i - j]^{q^j} \\ &= \sum_{i=1}^{s} a_s q^{a_i} - \sum_{i=1}^{a_s} q^i. \end{aligned}$$

To find $R(k)$ we use $k = \sum_{i=1}^{s-1} q^{a_i} + (q-1)(q^{a_s - 1} + \cdots + q + 1)$, so that $r_{i,j} = 1$ if $i \in \{a_1, \ldots, a_{s-1}\}$ and $0 \leq j < a_s$, $r_{i,j} = (q-1)$ if $0 \leq j < i < a_s$ and $r_{i,j} = 0$ otherwise. Thus

$$\begin{aligned} r(k) = \sum_{i<j} r_{ij} q^i &= \sum_{t=1}^{s} \sum_{j=0}^{a_s - 1} q^{a_t} + (q-1) \sum_{0 \leq j < i < a_s} q^i \\ &= a_s \sum_{i=1}^{s-1} q^{a_i} + (q-1) \sum_{i=1}^{a_s - 1} i q^i. \end{aligned}$$

Using $\sum_{i=1}^{t} iq^i = \frac{q}{(q-1)^2}\big(tq^{t+1} - (t+1)q^t + 1\big)$, the expressions for $r(k)$ and $\overline{s}(k)$ are easily seen to be equal.

To prove (2), first note that under the hypothesis, $r_{n_i,n_j} = a_i + a_j - (q-1)$ is non-negative for $d \geq i > j \geq 0$, and $r_{i,j} = 0$ for all other pairs of indices. Hence

$$\begin{aligned} r(k) &= \sum_{d\geq i>j\geq 0} (a_i + a_j - (q-1))q^{n_i} = \sum_{i=1}^{d} q^{n_i} \sum_{j=0}^{i-1} (a_i + a_j - (q-1)) \\ &= \sum_{i=1}^{d} q^{n_i} \left(i(a_i - (q-1)) + \sum_{j=0}^{i-1} a_j \right) \\ &= \sum_{i=1}^{d} q^{n_i} \left((d-i)(q-1) + r - \sum_{j=i+1}^{d} a_j + (i-1)(a_i) \right), \end{aligned}$$

where in the last step we use $d(q-1) + r - \sum_{j=i}^{d} a_j = \sum_{j=0}^{i-1} a_j$.

On the other hand the hypothesis also implies for all i that $a_i \geq r$, $a_i + a_{i-1} \geq r + (q-1), \ldots, a_i + \cdots + a_0 \geq r + (i-1)(q-1)$. Thus Theorem 4.2 gives

$$\begin{aligned} \overline{s}(k) &\overset{\mathcal{L}(k)=d}{=} s_d(k) \\ &\leq drq^{n_d} + (d-1)\big((a_d - r)q^{n_d} + ((q-1) - (a_d - r))q^{n_{d-1}}\big) + \cdots \\ &\qquad \cdots + (d-i)\big((a_d + \cdots + a_{d-i+1} - r - (q-1)(i-1)) \\ &\qquad\qquad \times (q^{n_{d-i+1}} - q^{n_{d-i}}) + (q-1)q^{n_{d-i}}\big) + \cdots \\ &= drq^{n_d} + (q-1)\sum_{i=1}^{d-1} iq^{n_i} \\ &\qquad + \sum_{i=1}^{d} (i-1)(q^{n_i} - q^{n_{i-1}}) \left(\sum_{j=0}^{d-i} a_{d-j} - ((d-i)(q-1) + r) \right), \end{aligned}$$

where the last step uses a substitution $d - i \leftrightarrow i - 1$. By sorting the summands according to the powers q^{n_i}, it follows that $\overline{s}(k) \leq r(k)$, and hence they must be equal. Note that initially we only get an upper bound for $\overline{s}(k)$ because the terms in Theorem 4.2 have coefficients, and a priori these may vanish.

Finally note that for $k = (c_0 \ldots c_m)_q$ the condition $\mathcal{L}(k) + 1 \geq \#\{i \mid c_i \neq 0\}$ is directly equivalent to the first assumption given in (2) if not all non-zero c_i are equal to $q-1$; then one takes these as the a_i. In the latter case, one has to include one further $a_i = 0$. □

Remark 4.11. In some cases it is possible to determine the factor $\overline{S}(k)/R(k)$ in $\mathbb{F}_q^*$ explicitly. For instance, for a, b with $0 \le a, b < q$ and $a+b = q-1+r > q-1$, one can show that

$$S_1(aq^m + b) = -\binom{a}{r}[m]^r,$$

where for general q, the term $\binom{a}{r}$ can be zero. To see that the formula holds up to a unit by Corollary 4.10(1), requires the following two facts:

(a) the binomial coefficient $\binom{a}{r}$ is non-zero if and only if in base p expansion all digits of a are greater or equal to the corresponding one of b;

(b) the condition $\mathcal{L}(k) = 1$ (this is the maximum possible) holds if and only if, again in base p expansion, the sum of any digit of a and the corresponding one of b is at least $p-1$, i.e., the digits of r are the sum of those of a and of b minus $p-1$.

In particular any digit of r is at most as large as the corresponding one of a, and hence $\binom{a}{r}$ is non-zero.

5. Exceptional factorization of Zeta leading coefficient

Fix A (and thus q). By k we always denote a positive integer.

Definition 5.1. *We say that $\wp$ is* exceptional *for k, if $k < q^{\deg(\wp)} - 1$ and $\wp$ divides $\overline{S}(k)$.*

We call k exceptional*, if there is $\wp$ exceptional for k.*

We call k regular*, if $\overline{S}(k)/\overline{R}(k) \in \mathbb{F}_q^*$, and we call k* irregular *otherwise.*[1]

We define $I(k) := \overline{S}(k)/\overline{R}(k) \in A \setminus \{0\}$ as the irregular part of $\overline{S}(k)$.[2]

We recall from Section 3 that k being non-exceptional is equivalent to the slope zero multiplicity of $T_p(J_\wp)_k$ being equal to $\mathcal{L}(k)$ for all $\wp$ with $q^{\deg \wp} - 1 \ge k$.

We will assume $q > 2$ below without mention, as Corollary 4.4 shows that there are no exceptional or irregular k's or $\wp$'s in the case $q = 2$.

Examples 5.2. Let $q = 3$. Then $k = 38$ is not exceptional by Example 4.3, while $k = 13$ is, by Remark 4.5(b), with $\wp = t^3 - t \pm 1$ the two corresponding exceptional primes.

Remarks 5.3.

(a) The connection between irregular and exceptional is explained in Proposition 5.5 and in Hypothesis (H6.1) in Section 6. If q is prime, so that $\overline{R}(k) = R(k)$, or if we assume that $R(k) = \overline{R}(k)$, our results are more complete.

[1] We are not certain whether using $\overline{S}(k)/R(k) \in \mathbb{F}_q^*$ would be more sensible.

[2] We know by Remark 4.9(b) that $\overline{S}(k)/\overline{R}(k)$ lies in $A \setminus \{0\}$.

(b) Corollary 4.4 and Corollary 4.10 give many families of k which are not exceptional by Proposition 5.5(1) below. Note also that in the definition, we could have included case the $k = 0$ as being non-exceptional.
(c) Clearly, any k can be exceptional for only finitely many $\wp$'s (even when we vary q). We guess but cannot prove yet that for a given $q > 2$, there are infinitely many non-exceptional $\wp$'s (in fact, we guess there are some in every degree).

Theorem 5.4. *For $q > 2$, there are infinitely many exceptional primes. In fact, there are some in every degree qm.*

Proof. Let $q > 2$ and $k = 1+q^m+q^{2m}+\cdots+q^{(q-1)m}$. Then $\ell(k) = \mathcal{L}(k) = 1$ and the leading term, which we temporarily write as $-X$, is

$$\overline{S}(k) = \sum_{\theta\in\mathbb{F}_q} (t+\theta)^k = -\sum_{k-r\equiv 0 \bmod q-1} \binom{k}{r} t^r = -\sum_{i=0}^{q-1} t^{q^{im}},$$

where the second equality follows by the basic fact on power sums over finite fields, and the third equality follows by straight-forward application of Lucas' theorem to our case.

Then $X^{q^m} - X = [qm]$. So all primes dividing X are of degree dividing qm. But by taking the derivative with respect to t, we see that X is multiplicity free. So a straight degree count shows that it is divisible by many primes of degree qm which are all exceptional. □

Proposition 5.5. *We have*

(1) *If k is regular, then k is not exceptional.*
(2) *k is irregular if and only if $\overline{s}(k) > \overline{r}(k)$.*
(3) *Assume k is optimum. If $\overline{S}(k)/R(k) \in \mathbb{F}_q^*$, then $\overline{S}(k')/R(k') \in \mathbb{F}_q^*$ for any k' obtained by permuting the base q digits of k. In particular, if k is regular and $\overline{R}(k) = R(k)$, then k' is regular and $\overline{R}(k') = R(k')$.*
(4) *If $\wp(t)$ is exceptional for k, then so are $\wp(t+\theta)$ and $\wp(\theta t)$, for any $\theta \in \mathbb{F}_q^*$.*
(5) *Any exceptional (or irregular) k satisfies $\ell(k) \geq q$. If q is prime and $\ell(k) \geq q$, and $r_{ij} = 0$ for k, then k is irregular.*
(6) *Primes of degree 1 or 2 are never exceptional.*
(7) *k is irregular if and only if $p^i k$ is irregular, for some or any $i \geq 0$. If $p^i k$ is exceptional with $i \geq 0$, then k is exceptional. If k is exceptional, then $\overline{S}(p^i k)$ ($i \geq 0$) is divisible by some exceptional prime (for k).*

Proof. For (1) let $k = c_0 + \cdots + c_s q^s$ be the q-adic expansion of k with $c_s \neq 0$. Let $\wp$ be a prime that divides $\overline{S}(k)$. Because of $\overline{S}(k'p) = \overline{S}(k')^p$, and similarly for $\overline{R}(k'p)$, we may assume that p does not divide k. Assume

that k is regular. Then $\wp$ divides a factor $[i-j]$ that is part of the product for $R(kp^a)$, some $a \in \{0, \dots, e-1\}$ where $q = p^e$. We have $0 \le j \le i$ and i is bounded by the largest non-vanishing base q digit of kp^a. If $a = 0$, then $i \le s$ and so $[i-j] = [m]$ for some $m \le s$. It follows that $\deg \wp$ divides m, i.e., that $q^{\deg \wp} - 1 \le q^s - 1 < k$.

If $0 < a < e$ it can happen that kp^a has highest non-zero digit c'_{s+1} at position $s+1$. It satisfies $c'_{s+1} \le p^a - 1$. At the same time, the lowest digit c'_0 is of the form $p^a x$ for some $x \in \{0, \dots, p^{e-a} - 1\}$. It follows that $c'_{s+1} + c'_0 - (q-1) \le p^a - 1 + p^e - p^a - (p^e - 1) = 0$ and hence the resulting $r_{s+1\,0}$ of kp^a is zero. Thus for $p^a k$ the largest possible $[m]$ is still $[m] = [s]$ and this completes the proof of (1).

Part (2) follows from Remark 4.9 (b) and the definition of regular.

Part (3) holds because when we interchange i-th and jth base q digits of k, the recipe of the Theorem 4.2 shows that X_i, X_j just get interchanged in the leading term $\overline{S}(k)$ formula. The same clearly also happens to $R(k)$, up to sign. So the claim follows by the definition and writing a general permutation as a product of transpositions. The second part also uses $R(k)|\overline{R}(k)|\overline{S}(k)$.

To see (4) note that $t \mapsto t+\theta$ (or $t \mapsto \theta t$, respectively) is an automorphism of A that preserves degrees. It takes A_{d+} to A_{d+} (or to $\theta^d A_{d+}$, respectively). Therefore $S_d(-k)|_{t \mapsto t+\theta} = S_d(-k)$ and $S_d(-k)|_{t \mapsto t\theta} = \theta^{dk} S_d(-k)$, and the claim follows.

Next we prove (5). If $\ell(k) < q-1$, then $d = 0$, and $S_d(-k) = 1$ for the leading term. If $\ell(k) = q-1$, then $d = 1$, and $S_d(-k) = -1$, e.g. by Theorem 4.2. (From [23, p. 539 (C2)], it is known that these are the only cases of non-zero constant values of the leading term.) Since $S_d(-k)$ is thus constant for $\ell(k) \le q-1$, it is clear that such k are regular. Hence the exceptional and irregular k have at least q digits. The last claim follows since in this case $R(k) = 1$ while $\overline{S}(k)$ is not in $\mathbb{F}_q^*$ (here q is prime!).

For (6) note that the corresponding exceptional k would satisfy $k < q^2 - 1$. However this is not possible by (1), (5) and Corollary 4.10.

To see (7) recall that $\overline{S}(p^i k) = \overline{S}(k)^{p^i}$ and $\overline{R}(p^i k) = \overline{R}(k)^{p^i}$. □

Proposition 5.6. *Suppose $\wp$ is exceptional for k. Let $e = \log_p(q)$ and $f = \deg \wp$, and let $k = (d_0, \dots, d_{fe-1})_p$ be the base p expansion of $k \le p^{ef} - 1$. Let $k' = (d'_0, \dots, d'_{ef-1})_p$ be a cyclic permutation of the digits of the base p expansion of k. Then $\wp$ is exceptional for k'. In particular, if $p|k$, then $\wp$ is exceptional for $\frac{k}{p}$.*

Note that the last assertion also has the simple proof $\overline{S}(k) = \overline{S}(\frac{k}{p})^p$.

Proof. By an inductive procedure, it suffices to show that $\wp$ is exceptional for $k' = (d_{ef-1}, d_0, \dots, d_{ef-2})_p$. Let $0 < i \le e$ be minimal such that $p^i k$

is optimum. From the definition of $\overline{S}(\,\cdot\,)$ we have $\overline{S}(k)^{p^i} = S_d(p^i k)$ for $d = \lfloor \frac{\ell(p^i k)}{q-1} \rfloor$. By Lemma 2.2, also $p^{i-1}k'$ is optimum, and thus $\overline{S}(k')^{p^{i-1}} = S_d(p^{i-1}k')$.

Now consider formula (4.2) for $S_d(p^i k)$ and $S_d(p^{i-1}k')$. Writing $p^i k = (c_0, \dots, c_f)_q$ and $p^{i-1}k' = (c'_0, \dots, c'_f)_q$, the key observation is that (in the notation of the proof of Theorem 4.2 with $e = f$) the two formulas are congruent modulo the bracket $[f] = t^{q^f} - t$, using that

$$\binom{c_t}{\underline{c}_t} = \binom{c'_t}{\underline{c}'_t} \quad \text{for } t = 1, \dots, f-1\,,$$

and that

$$\binom{c_0}{\underline{c}_0} \cdot \binom{c_f}{\underline{c}_f} = \binom{c'_0}{\underline{c}'_0} \cdot \binom{c'_f}{\underline{c}'_f}$$

by Lucas' theorem. I.e., we have $S_d(p^i k) \equiv S_d(p^{i-1}k') \pmod{[f]}$. Since $\wp$ divides $[f]$ and $\wp$ divides $S_d(p^i k)$ by assumption, it divides $S_d(p^{i-1}k') \pmod{[f]}$, and hence $\wp$ divides $\overline{S}(k')$, as was to be shown. □

Theorem 5.7. *If $p > 2$, the lowest k for which the leading coefficient $\overline{S}(k)$ is divisible by an exceptional prime is $k_0 = q^2 + q + (q-2)$ (with digit sum q).*

For $p = 3$, the corresponding exceptional primes have degree 3. For $p \geq 5$, the degrees of the corresponding exceptional primes divide $p - 1$.

If $p = 2$ and $q = 4$, the smallest exceptional k_0 is $q^3 + q^2 + q + 1$. The degrees of all the corresponding exceptional primes is 4.

If $q = 2^e$ with $e \geq 3$, $k_0 = 3q^2 + 3q + (q-5)$ is exceptional, the degrees of the corresponding exceptional primes being 3 or 4.

Proof. We first treat the case $p > 2$. First we show that no k smaller than k_0 is exceptional. By Proposition 5.5 (5), it is enough to look at $k = (c_0\, c_1)_q$, with $c_0 + c_1 > q - 1$ or $k = q^2 + (q-1)$. By Corollary 4.10 (2), none of these k is exceptional, because either $\mathcal{L}(k) = 0$ or else $\mathcal{L}(k) = 1 \geq \#\{i \mid c_i \neq 0\} - 1 = 2 - 1$.

By Theorem 4.2, since $d = r = 1$, the leading coefficient is $t^{q^2} + t^q + (q-2)t = [2] + [1] = [1]([2]/[1] + 1)$. It is divisible by a prime of degree more than two, and thus exceptional.

If we have a relation $t^{q^2} = -t^q + 2t$, raising it to q-th power and simplifying repeatedly, we see that $t^{q^n} = a_n t^q + (-a_n + 1)t$, where a_n satisfies the recursion $a_{n+1} = 1 - 2a_n$ with $a_0 = 0$. One deduces $a_n = \frac{1}{3}(1 - (-2)^n)$, and this can be regarded as a sequence of integers. For $n = p - 1$ and $p \geq 5$, we deduce $a_{p-1} \equiv 0 \pmod{p}$, and so $t^{q^{p-1}} - t = 0$. For $p = 3$, the sequence vanishes for the first time for $n = 3$, in accordance with Example 4.3.

Second case $p = 2$: We first consider $q = 4$. Theorem 4.2 gives the leading term as $t^{q^3} + t^{q^2} + t^q + t$ for $k = k_0$, which is

$$[2] + [2]^q = [2]\Big(1 + [2]^{q-1}\Big),$$

as we are in characteristic 2. Now modulo primes $\wp$ dividing it, $t^{q^3} = t^{q^2} + t^q + t$, implies, by raising to q-th power and back substituting this, that $t^{q^4} = t$, so that prime divisors $\wp$ have degree dividing 4. But primes of degree dividing two are prime to $1+[2]^{q-1}$, thus proving the claim. (We also know directly that primes of degree one and two are never exceptional, for example, by Proposition 5.5(6). (Note that exceptional degree calculation for this k_0 works for any $q = 2^e$, $e > 1$.)

Suppose now $q = 2^e$ for some $e \geq 3$. Let $k_0 = 3q^2+3q+q-5$. Theorem 4.2 gives the leading term (since the relevant binomial coefficients 3 and $\binom{q-5}{2}$ are odd, and thus one) as $f = t^{2q^2} + t^{q^2+q} + t^{q^2+1} + t^{2q} + t^{q+1} + t^2 = [1]^2 + [1]^q[2]$. We claim that f divides $[3][4]$. Because all prime factors of $[3]/[1]$ and $[4]/[2]$ have degrees 3 or 4, respectively, and because $\deg f = 2q^2 > q^2 + q = \deg[1][2]$, this implies that f has a prime factor of degree 3 or 4.

We now prove the claim. Using $[m]^q = [m+1] - [1]$ for $m \geq 1$ repeatedly, by a simple but straightforward computation one finds (since we are in characteristic 2) that

$$f^q + f = [3]\left([3] + [2] + [1]\right).$$

Let now $g = [3] + [2] + [1]$. A similar computation shows $g^q + g = [4]$, so that g divides $[4]$. It follows that $f^q + f$ divides $[3][4]$, and hence that f divides $[3][4]$. □

Remark 5.8. The proof shows that when $p \geq 5$ the degrees of exceptional primes will divide the least $k \geq 2$ such that $a_k = 0$, i.e., the order of -2 in $\mathbb{F}_p^*$. The data shows that for $q \leq 49$, the exceptional degree is equal to this k. Moreover the non-exceptional part is $[1]$. For example, for $p = 11$, these exceptional primes have degree 5.

When $p = 2$, $q > 2$, the data shows that the non-exceptional part seems to be $[2]$ for $q = 4$ and $[1]^2$ for $q > 4$. The exceptional primes occur to multiplicity 1, as can be checked by a derivative calculation (after dividing by the observed non-exceptional part). Moreover if $q = 2^e$ with $e \geq 3$, computer experiments suggest that $k_0 = 3q^2 + 3q + (q - 5)$ is the smallest exceptional k and all the exceptional primes for k_0 have degree 4 if e is odd, and degree 3, if e is even.

Theorem 5.9. *Suppose $k' = (c_0, \dots, c_{e+1})_q$ has digit $c_{j_0} = q-1$ for some $0 \le j_0 \le e+1$. Let $k = k' - (q-1)q^{j_0}$ and write $\ell(k') = \sum_{j=0}^{e+1} c_j = (d+1)(q-1)+r$ with $0 \le r < q-1$. Then*

$$S_{d+1}(-k') = (-1)^{\sum_{j=0}^{j_0-1} c_j} \cdot S_d(-k) \cdot \prod_{j=0}^{j_0-1} [j_0-j]^{q^j c_j} \cdot \prod_{j=j_0+1}^{j-j_0} [j-j_0]^{q^{j-j_0} c_j}. \tag{5.1}$$

Proof. From the definitions it is clear that $R(k)$ divides $R(k')$, and using that the j_0-th coefficient of k' is $q-1$ it follows that

$$\begin{aligned} R(k')/R(k) &= \prod_{\substack{j=0,\dots,e+1 \\ j \ne j_0}} \left(t^{q^{\max\{j,j_0\}}} - t^{q^{\min\{j,j_0\}}} \right)^{c_j} \\ &= \prod_{j=0}^{j_0-1} (X_{j_0} - X_j)^{c_j} \cdot \prod_{j=j_0+1}^{e+1} (X_j - X_{j_0})^{c_j}, \end{aligned}$$

where as in the proof of Theorem 4.6, we write X_j for t^{q^j}. The reformulation of Theorem 4.2 in the proof of Theorem 4.6 gives

$$\begin{aligned} S_{d+1}(-k') &= f(X_0, \dots, X_{e+1}) \\ &:= \sum_{\underline{C}'} \binom{c_0}{c'_0} \cdot \dots \cdot \binom{c_{e+1}}{c'_{e+1}} \prod_{j=0}^{e+1} X_j^{\sum_{i=0}^{d+1} (d+1-i) c'_{ji}}, \end{aligned} \tag{5.2}$$

where the sum is over all matrices $\underline{C}' = (c'_{ji})_{j=0,\dots,e+1, i=0,\dots,d+1}$ with j-th row $\underline{c}'_j$, $\sum_r \underline{C}' = (r, q-1, q-1, \dots, q-1)$, $\sum_c \underline{C}' = (c_0, \dots, c_{e+1})^t$. The proof also shows that $R(k')$, considered as a polynomial in $X_0, \dots, X_{e+1}$, divides $f \in \mathbb{F}_p[X_0, \dots, X_{e+1}]$, and hence

$$g(X_0, \dots, X_{e+1}) := \prod_{j=0}^{j_0-1} (X_{j_0} - X_j)^{c_j} \cdot \prod_{j=j_0+1}^{e+1} (X_j - X_{j_0})^{c_j}$$

divides f. Thus there exists $h(X_0, \dots, X_{e+1}) \in \mathbb{F}_p[X_0, \dots, X_{e+1}]$ such that $f = gh$.

Now the maximal exponent of X_{j_0} that occurs in the polynomial f is $s := \sum_{i=0}^{d+1} (d+1-i) c'_{j_0\, i}$ for

$$\underline{c}'_{j_0} = (r, q-1-r, 0, \dots, 0), \tag{5.3}$$

i.e., $s = (d+1)r + d(q-1-r) = d(q-1)+r = \ell(k)$, and s is also the maximal exponent of X_{j_0} in g. Hence h lies in $S = \mathbb{F}_p[X_0, \dots, X_{j_0-1}, X_{j_0+1}, \dots, X_{e+1}]$. Since g has leading term $(-1)^{\sum_{j=j_0+1}^{e+1} c_j}$ as a polynomial in X_{j_0} with coefficients in S, it follows that $(-1)^{\sum_{j=j_0+1}^{e+1} c_j} h$ is the coefficient of $X_{j_0}^{\ell(k)}$

of f regarded as a polynomial in X_{j_0} with coefficients in S. By (5.2) this coefficient is

(5.4)
$$\sum_{\underline{C}'} \binom{c_0}{c'_0} \cdot \ldots \cdot \binom{c_{j_0}}{r, q-1-r, 0, \ldots, 0} \cdot \ldots \cdot \binom{c_{e+1}}{c'_{e+1}} \prod_{\substack{j=0\ldots e+1 \\ j\neq j_0}} X_j^{\sum_{i=0}^{d+1}(d+1-i)c'_{ji}},$$

where the sum is over all matrices $\underline{C}' = (c'_{ji})_{j=0,\ldots,e+1, i=0,\ldots,d+1}$ with $\sum_r \underline{C}' = (r, q-1, q-1, \ldots, q-1)$, $\sum_c \underline{C}' = (c_0, \ldots, c_{e+1})^t$ and $\underline{c}'_{j_0}$ as in (5.3).

The multinomial with $c_{j_0} = q-1$ in the numerator has value $(-1)^r = (-1)^{\ell(k)}$, since $q - i = -i$ in characteristic p. The main observation is that if we define the matrix $\underline{C}$ as $(c'_{ji})_{j=0,\ldots,e+1, j\neq j_0, i=1,\ldots,d+1}$, and if we use the shape in (5.3) of $\underline{c}'_{j_0}$ and the analog of (5.2) for $S_d(-k)$, then it is immediate that expression (5.4) is equal to $(-1)^{\ell(k)} S_d(-k)$, and this completes the proof. □

The following result is a direct consequence of Theorem 5.9.

Corollary 5.10. *Suppose $k' = (c_0, \ldots, c_{e+1})_q$ has digit $c_{j_0} = q-1$ for some $0 \leq j_0 \leq e+1$. Let $k = k' - (q-1)q^{j_0}$. Then $\overline{S}(k)/R(k) \in \mathbb{F}_q^*$ if and only if $\overline{S}(k')/R(k') \in \mathbb{F}_q^*$. Moreover if k' is exceptional, then so is k, and if $j_0 \leq e$, the converse also holds.*

Corollary 5.11. *For $q = 3$, the integer k is irregular if and only if its base q expansion contains the digit 1 at least q times.*

Proof. We see, for instance by Proposition 5.5 (5), that 1_m is irregular if and only if $m \geq 3$. Adding 0 digit at the end is multiplication by the prime q and preserves regularity and irregularity. By Corollary 5.10, when $q = 3$, adding 2 in front also preserves regularity and irregularity. By (3) of Proposition 5.5 permuting digits also preserves regularity and irregularity. Combining these, the corollary is proved. □

Remarks 5.12.

(a) For $q = 3$, the irregular k's thus have the asymptotic density one.
(b) For generalizations of Corollary 5.11, see Hypothesis (H6.1) (3).

Recall from Section 3 that for a prime $\wp$ of A we denote by $J_{\wp,d}$ the factor of the Jacobian $J_\wp$ characterized by having associated Dieudonné module consisting of all k-components such that $k = k' \cdot \#G_\wp/d$, $0 < k' < d$ and $\gcd(k', d) = 1$.

Corollary 5.13. *Let $q = 3$. If $\deg \wp$ is even then $J_{\wp,4}$ is ordinary of dimension $\deg \wp - 2$. If $\deg \wp$ is divisible by 4 then $J_{\wp,10}$ is ordinary of dimension $2 \deg \wp - 4$.*

Proof. For $d = 4$, there are two k to consider, namely $k = \frac{j}{4}(3^{\deg \wp} - 1)$ for $j \in \{1, 3\}$. Their base 3 expansion is a sequence of the digit pair $0, 2$ or $2, 0$, respectively. For $d = 10$ the k are $\frac{j}{10}(3^{\deg \wp} - 1)$ for $j \in \{1, 3, 7, 9\}$ and their base 3 expansion is a repetition of $0, 0, 2, 2$, or $0, 2, 2, 0$, or $2, 0, 0, 2$ or $2, 2, 0, 0$, respectively. In both cases all such k are regular by Corollary 4.4. This implies the ordinariness of $J_{\wp,d}$.

The dimensions are computed by the Hurwitz formula from the known ramification properties of $K_\wp/K$, e.g. [9, Sect. 7.4], and by a recursion using that $\prod_{d'|d} J_{\wp,d'}$ is the Jacobian of the subcover of $X_\wp \to \mathbb{P}^1_{\mathbb{F}_3}$ corresponding to the (unique) quotient of $\#G_\wp$ of order d. All covers involved, of degrees $d \in \{2, 4, 5, 10\}$, have decomposition group $\mathbb{Z}/(d)$ at $\wp$ and are unramified away from $\wp$. □

Remark 5.14. We note that Hypothesis (H6.3) implies, for example, that $J_{\wp,2}$ is never ordinary for $q = 3$ and a prime $\wp$ of degree at least 3.

Computer experiments relying crucially on Corollary 5.11 suggest that for $q = 3$ and large $f \in \mathbb{Z}_{\geq 0}$ one cannot expect the components $J_{\wp,d}$ to be ordinary for all $\wp$ of degree f for pairs (d, f) not covered by Corollary 5.13.

For $q = 5$ a family similar to the first one in Corollary 5.13 exists, namely $J_{\wp,6}$ for $\wp$ of even degree. For larger primes q we have no evidence for the existence of such families.

From Corollary 5.10 and Proposition 5.6 we deduce the following result.

Corollary 5.15. *For a given exceptional prime, the lowest k for which it is an exceptional prime has no $q-1$ digit in its base q expansion and is not divisible by p.*

Definition 5.16. *An* Artin–Schreier polynomial *for q is a polynomial of the form $t^q - t - \theta$ for $\theta \in \mathbb{F}_q^*$. If $q = p$ is a prime number, then $t^q - t - \theta$ is irreducible and is then called an* Artin–Schreier prime.

Theorem 5.17. *Let $p > 2$. Put $c := (q-1)/2$. When $k = q^2 + cq + (q-2)$, the leading coefficient $\overline{S}(k)$ is $-c[1]^c([1]^{q-1} - 1)$, and thus it factors as the product over all Artin–Schreier polynomials for q to multiplicity one times $[1]^c$.*

Hence when q is prime, the exceptional primes for this k are exactly the Artin–Schreier primes $t^q - t - \theta$, $\theta \in \mathbb{F}_q^*$ occurring to multiplicity one.

Proof. Since $d = 1$, $r = (q-1)/2$, Theorem 4.2 gives the leading term as

$$(-1)^1 \left(\sum_{a=0}^{c-1} \binom{c}{a} \binom{q-2}{c-a-1} t^{q^2 + aq + (c-a-1)} + \sum_{a=0}^{c} \binom{c}{a} \binom{q-2}{c-a} t^{aq + (c-a)} \right).$$

The claimed term is

$$-c[1]^{c-1}(t^{q^2}-2t^q+t)$$
$$=-c\left(\sum_{a=0}^{c-1}\binom{c-1}{a}t^{aq+c-a-1}(-1)^{c-a-1}(t^{q^2}-2t^q+t)\right).$$

These are the same: Note that $\binom{q-2}{j}=(-1)^j(j+1)$ in characteristic p. After straight manipulations, the terms in the first sum of the first expression match with those of the second using t^{q^2} term, while the second sum of the first expression matches with that of second with terms $-2t^q+t$, which leads to combine terms for a and $a-1$ and reduces to $c-a+1=a-c-2a$. □

Remark 5.18. Note that Theorem 4.6 only shows that $[1]^{c-1}$ divides $\overline{S}(k)$ under the hypothesis of Theorem 5.17.

Theorem 5.19. *Let q be a prime and $0<k=\sum_{i=0}^{q-1}c_iq^i<q^q-1$ with $0\le c_i\le q-1$.*

(1) *If one Artin–Schreier prime is exceptional for k, then all are.*
(2) *Let k' be obtained from k by reversing the digits $c_0,\dots,c_{q-1}$. If an Artin–Schreier prime is exceptional for k, then it is also exceptional for k'.*

Proof. Let $\wp_\alpha(t):=t^q-t-\alpha$, with $\alpha\in\mathbb{F}_q^*$. Then $\wp_\alpha(\theta t)=\theta(t^q-t-\alpha/\theta)$, and so assertion (1) follows from Proposition 5.5 (4).

To prove (2), note that modulo $\wp_\alpha$ we have $t^{q^i}\equiv t+i\alpha$. Then Theorem 4.2 shows that modulo $\wp_\alpha$ we have

$$\overline{S}(k)\equiv\sum_{\underline{C}}\binom{c_0}{\underline{c}_0}\cdot\ldots\cdot\binom{c_{q-1}}{\underline{c}_{q-1}}\prod_{j=0}^{q-1}(t+j\alpha)^{\sum_{i=0}^d(d-i)c_{ji}},$$

where the sum is over all matrices $\underline{C}=(c_{ji})_{j=0,\dots,q-1,i=0,\dots,d}$ with j-th row $\underline{c}_j$, such that the rows sum to $(r,q-1,q-1,\dots,q-1)$ and the columns sum to the transpose of $(c_0,\dots,c_{q-1})$, and the expressions $\binom{c_j}{\underline{c}_j}$ are multinomial coefficients with $d+1$ entries in the bottom. We consider the substitution $t\mapsto -t-(q-1)\alpha$. By the proof of Proposition 5.5 (4), it changes $\overline{S}(k)$ only by a factor in $\mathbb{F}_q^*$. Moreover

$$\prod_{j=0}^{q-1}(-1)^{\sum_{i=0}^d(d-i)c_{ji}}=(-1)^{\sum_{i=0}^d(d-i)\sum_j c_{ji}}=(-1)^{dr+(q-1)\binom{d}{2}}=(-1)^{dr}$$

is independent of $\underline{C}$. Hence $\overline{S}(k)\equiv 0 \pmod{\wp_\alpha}$ if and only if

$$\sum_{\underline{C}}\binom{c_0}{\underline{c}_0}\cdot\ldots\cdot\binom{c_{q-1}}{\underline{c}_{q-1}}\prod_{j=0}^{q-1}(t+(q-1-j)\alpha)^{\sum_{i=0}^d(d-i)c_{ji}}=\overline{S}(k')\equiv 0 \pmod{\wp_\alpha}.$$

To show that $k' < q^q - 1$, note first that by Proposition 5.5(1) not all $c_j = q-1$. But then clearly $k' = \sum_{i=0}^{q-1} c_{q-1-i} q^i < q^q - 1$, we are done. □

6. Data/Guesses/Observations/Questions

6.1. Data. Let $\pi(q,d)$ ($a(q,d)$ respectively) be the number of primes of A of degree d (that are exceptional respectively). Let $e(q,d)$ be the number of exceptional k's for degree d primes, out of total $q^d - 1$ possible. Then we know that $a(q,1) = a(q,2) = 0$. Note that

$$\pi(q,d) = \frac{1}{d} \sum_{i|d} \mu(d/i) q^i$$

is, for a fixed q, asymptotic to q^d/d. Then

$$\begin{array}{lll}
a(3,3) = 2, & \pi(3,3) = 8, & e(3,3) = 1 \\
a(3,4) = 6, & \pi(3,4) = 18, & e(3,4) = 1 \\
a(3,5) = 12, & \pi(3,5) = 48, & e(3,5) = 1 \\
a(3,6) = 71, & \pi(3,6) = 116, & e(3,6) = 41 \\
a(3,7) = 96, & \pi(3,7) = 312, & e(3,7) = 15 \\
a(3,8) = 329, & \pi(3,8) = 810, & e(3,8) = 689
\end{array}$$

$$a(5,3) = 0, \quad a(7,5) = 0, \quad a(13,4) = 0, \quad a(11,3) = 0, \quad a(17,3) = 0$$

$$\begin{array}{lll}
a(5,4) = 90, & \pi(5,4) = 150, & e(5,4) = 103 \\
a(5,5) = 224, & \pi(5,5) = 624, & e(5,5) = 373 \\
a(5,6) = 1600, & \pi(5,6) = 2580, & e(5,6) = 1153
\end{array}$$

$$\begin{array}{ll}
a(7,3) = 28, & \pi(7,3) = 112 \\
a(7,4) = 462, & \pi(7,4) = 588 \\
a(7,6) = 454, & \pi(7,6) = 19544
\end{array}$$

$$\begin{array}{ll}
a(13,3) = 104, & \pi(13,3) = 728
\end{array}$$

$$\begin{array}{ll}
a(17,3) = 952, & \pi(17,3) = 1632
\end{array}$$

6.2. Guesses. In Proposition 5.5 we showed that exceptional k are irregular. Based on large computations, mainly for small primes q and for $q = 4$, we formulate the following hypothesis toward a converse.

Hypothesis (H6.1). *Suppose for* (0)–(3) *that* q *is a prime number.*

(0) *If* $\overline{S}(k)$ *is (constant times) a product of brackets* $[i]$*'s, then* k *is regular (the converse holds by definition of regular).*

(1) *If* k *is irregular, not divisible by* q *and with highest and lowest digits different than* $q-1$ *in the base* q *expansion of* k*, then* k *is exceptional.*

(2) *For irregular* k*, the irregular part* $I(k)$ *is a non-trivial ("maximal bracket part") product of some* $[n]$*'s with* $q^n - 1 \leq k$ *times a non-trivial product of some exceptional primes (for some* k'*). If* d *is a degree of such an exceptional prime, then not all primes of degree* d *occur in the second product.*
If furthermore the conditions in part (1) *hold, then at least one (but may be not all) of the factors of the second product are exceptional for the given* k*.*

(3) k *is irregular if the base* q *expansion of* k *contains sub-multiset of (non-zero) digits with total (at least)* q *but any pair of digits from it adding to less than* q*.*

(4) *Suppose that* $q = 4$ *and that* k *is optimum. Then* $R(k)$ *is a proper divisor of* $\overline{S}(k)$ *if and only if its base* 4 *expansion contains either the sub-multiset* $[1,1,2]$ *or* $[1,1,1,1]$*.*

Remarks 6.2.

(a) If indeed (H6.1)(1) holds, then for k satisfying conditions there, k being exceptional for q a prime is reduced via regularity to a purely numerical criterion, namely to

$$k \text{ is not exceptional} \iff \overline{s}(k) = r(k)\,.$$

Note that $\overline{s}(k) \geq r(k)$, and the "if part" follows from Proposition 5.5(1). For q prime one has explicit expressions for $\overline{s}(k)$, from [2, p. 71], and for any q for $r(k)$, from formula (4.1). While they can be efficiently computed and compared for a given fixed k and q, it is hard to derive general conclusions.

We note that conditions on the k in (H6.1)(1) cannot be removed as we can see from the following examples: When $q = 3$, and $k = 41 = (2111)_3$ or $k = 67 = (1112)_3$ are irregular, but not exceptional as their irregular part consists of two degree 3 primes, which are exceptional for $13 = (111)_3$, but not for k's above. Theorem 5.9 and Proposition 5.5(7), explain the passage from $41, 67$ to 13 (via $39 = 13*3$ in the case of 41), and explain in general how the leading terms of k's considered in (H6.1)(2) are related to leading terms of k's considered in (H6.1)(1). In fact, by Theorem 5.9 it suffices to check (H6.1)(1) only for k not divisible by q and with no digit $q-1$ in its base q expansion.

(b) Because of the Corollary 5.11, for $q = 3$ and for k as in Hypothesis (H6.1)(1), k is exceptional if and only if the base 3 expansion of k contains the digit 1 at least 3 times.

(c) Note that k with all digits one, and more than $q-1$ digits is irregular (when $q > 2$, of course), thus exceptional, for q a prime, under (H6.1)(1). See (H6.3) below for a more explicit guess.

(d) Note $r(k) = \sum_{i>j} r_{i,j} q^i$. Since [23, Thm. 14] implies that when q is prime, $\overline{s}(k)$ is also a multiple of q, our (H6.1)(2) implies that the total degree of exceptional divisor is a multiple of q. For $q = 3$, data seems to suggest that the total exceptional degree is of form $q^a - q^b$. On the other hand, for $q = 5$, $k = 62$, the total exceptional degree is 40, there being 4 degree 10 exceptional primes.

(e) Let q be prime. By [23, Thm. 14], modulo $q-1$, $s_{\mathcal{L}(k)}(-k)$ is $k\mathcal{L}(k)$ (this also follows directly from Theorem 4.2, since $d = \mathcal{L}(k)$ and q^u is 1 modulo $q-1$), whereas $r(k)$ is $\sum_{i>j} r_{i,j}$, so if they do not match, k is irregular.

(f) We can have k exceptional, even if whenever $c_i c_j \neq 0$, we have $r_{ij} > 0$. An example is given by $q = 5$ and $k = 343$. In this case, $\overline{S}(k)/R(k)$ is product of [1] and 5 primes of degree 24.

(g) Using the explicit formulas mentioned in (a), it might be possible to give a proof of $\overline{s}(k) > r(k)$ under the conditions of (H6.1)(3).

(h) Our data suggests that hypothesis (H6.1)(2) on $I(k)$ can be strengthened. We did not see any factors $[n]$ occur in $I(k)$ for $n \geq \frac{1}{2}\log_q(k+1)$. But we did not collect enough data to formulate a hypothesis in general; but see (H6.4), for $q = 3$.

(i) Part (4) is not the generalization of (3) to $q = 4$. That would ask for a characterization of k such that $\overline{R}(k)$ properly divides $\overline{S}(k)$. We only know that $R(k)|\overline{R}(k)|\overline{S}(k)$.

(j) Hypothesis (H6.1)(0, 1, 2) do not generalize to prime power q's. In fact, if all $r_{i,j} = 0$ (e.g., all $c_i < (q-1)/2$), but $\mathcal{L}(k) > 1$, so that [23, p. 539] $\overline{s}(k) > 0$, then k would be irregular. But the conclusions of these parts, extended for q non-prime in general are false, for example, if $q = 4$, and $k = 25$ or 37 respectively, when $r(k) = 0$, but $\overline{S}(k)$ is [2] or [1] respectively.

Explicit exceptional family. Put $k_m = (q^m - 1)/(q-1)$, which has m digits all 1, so that the corresponding $\mathcal{L}(k)$ is $\lfloor m/(q-1) \rfloor$. Note that $R(k_m) = 1$ in this case.

Hypothesis (H6.3). *If $m \geq q > 2$, then $\overline{S}(k_m)$ is divisible by exceptional prime of degree m. More precisely, if $q = 3$, and $m > 2 = 3-1$, then $\overline{S}(k_m)$ is divisible by an exceptional prime of degree m and in fact,*

$$\overline{S}(k_m) = (-1)^{\mathcal{L}(k)} Q([1]^{1+3+\cdots+3^{m-3}}[2]^{1+3+\cdots+3^{m-5}} \ldots [r]^s),$$

where $[r]^s = [(m-1)/2]$ *or* $[m/2-1]^{1+3}$ *depending on whether* m *is odd or even, and where* Q *is a product of some monic exceptional primes, at least one of them is of degree* m.

Some exceptional primes in Q are not exceptional for k and some occur with multiplicity. We denote by (a,b) a product of a distinct exceptional primes of degree b. Then Q takes the shapes $(2,3)$, $(6,4)$, $(12,5)(15,6)$, $(60,6)(24,7)$, $(15,6)^3(96,7)(90,8)(78,9)$, $(24,7)^3(270,8)(312,9)(240,10)$ and $(2,3)(90,8)^3(78,9)^4(702,9)(666,10)(660,11)(472,12)$, respectively, for $m = 3,\dots,9$. Moreover, e.g., $(78,9)$ represents the same product in both cases, whereas the 702 other primes of degree 9 are distinct from those 78. The primes of degree at least m in Q are exceptional for k_m, but those of the lower degree are not exceptional for k_m.

Conjectural prediction of bracket factors of the irregular part for q = 3. Let $q = 3$ in this part. Let k be irregular, i.e., (by Corollary 5.11) k has at least three 1's as digits. We define the "*irregular bracket part*" $I_b(k)$ to be the divisor of $I(k)$ of the form $\prod_{i\geq 1}[i]^{n_i}$ which is largest lexicographically (i.e., for the order where the divisor with the largest i (with a positive exponent) larger, or with larger n_i, if the largest such i's are the same, gives the larger divisor). Then by Hypothesis (H6.1), every prime factor, say $\wp$, of $I(k)/I_b(k)$ is exceptional and not all primes of degree that of $\wp$ divide $I(k)/I_b(k)$. We would like to give conjectural prediction for $I_b(k)$, but we can do this only in part in the following Hypothesis.

By Theorem 5.9, $I_b(k)$ does not change if we drop the digits 2 from k, so that we can assume, without loss of generality, that all the digits of k are 0 or 1. Write $k = \sum_{i=0}^{d} q^{k_i}$, with k_i strictly increasing with respect to i.

Hypothesis (H6.4). *Write* $I_b(k) = \prod_{i\geq 1}[i]^{n_i}$. *Then* $n_i = 0$ *for* $i > k_d/2$, *and* $\sum n_i = \sum_{r=1}^{\lfloor d/2\rfloor}\sum_{i=0}^{d-2r} q^{k_i}$. *Further,* $[n]$ *divides* $I_b(k)$ *if and only if there exist* $0 \leq a < b < c \leq d$ *such that* n *divides the greatest common divisor of* $k_b - k_a$ *and* $k_c - k_b$.

The simplest example is $k = 1+q^m+q^n$, with $0 < m < n$, then $I_b(k) = [r]$, where r is the gcd of m and n. This is seen as follows. As in the proof of Theorem 4.6, the leading term is $-X = -(t^{3^n} + t^{3^m} + t) = -[m] - [n]$, since $q = 3$. Hence, $\gcd(X,[r]) = [r]$, if and only if r divides the gcd of m,n. (In more detail, the "if" direction is immediate, since then $[r]$ divides $[m],[n]$ and thus divides X. Conversely, let q_1, q_2 be quotients of m,n respectively, under division by r, then modulo $[r]$, $0 \equiv X \equiv [m - q_1 r] + [n - q_2 r]$ would give a contradiction by degree inequalities unless r divides m or n, hence both).

The next simplest family is $k = 1+q^m+q^{m+n}+q^{m+n+s}$. There are 4 gcd's a,b,c,d of $(m,n+s),(m+n,s),(n,s),(m,n)$ respectively. The hypothesis

implies that the total number of brackets in $I_b(k)$ is $1+q^m$. It seems that $I_b(k)$ is either $[u]^{q^m}[v]$, or $[u]^{q^m-1}[v][w]$ or $[u]^{q^m-2}[v][w][x]$, where u, v, w, x, which may or may not be distinct, are among these 4 gcd's.

An example with 5 digits 1's is $k = 2299 = 1+q+q^3+q^4+q^7$, and so $d = 4$ and $k_d = 7$, which has $I_b(k) = [3]^3[2]^3[1]^{27-1}$ giving in total 32 brackets as predicted.

6.3. Observations.

Absence of exceptional primes in certain low degrees. By Proposition 5.5(6), primes of degree one or two are never exceptional. Hypothesis (H6.3) suggests that for any $m \geq q$, we can find exceptional primes of degree m. We observed that for $q = p = 5, 11, 17$, and for $q = 4$ primes $\wp$ of degree 3 are not exceptional. The following proposition summarizes our computations for odd primes q:

Proposition 6.5. *Let $q = p$ be an odd prime, $\wp$ a prime of A and $J_\wp$ the Jacobian of the Carlitz $\wp$-cyclotomic extension of $\mathbb{F}_q(t)$. Then the following hold:*

1. *If $q \in \{5, 11, 17\}$, then $J_\wp$ is ordinary for all $\wp$ of degree 3. For all other $q \leq 61$, there is some $\wp$ of degree 3, such that $J_\wp$ is non-ordinary.*
2. *If $q = 7$, then $J_\wp$ is ordinary for all $\wp$ of degree 4. For all other $q \leq 41$, there is some $\wp$ of degree 4, such that $J_\wp$ is non-ordinary.*
3. *For every $q \leq 41$, there is some $\wp$ of degree 5 such that $J_\wp$ is non-ordinary.*

Checking primes $\wp$ of degrees larger than 5 systematically seemed computationally very difficult.

Orbits of exceptional primes and their size. Let us now fix q a prime number and d the degree of possibly exceptional primes $\wp \subset A$. The prime $\wp$ can be exceptional for many $k < q^{\deg \wp} - 1$. So for each $\wp$ let $\mathrm{Exc}_\wp$ be the list of such k. In experimental computations (for many q, mostly prime, and many degrees) it turns out that the sets $\mathrm{Exc}_\wp$ were the same for many (exceptional) primes $\wp$. We therefore partition the set $\mathrm{Exc}_d := \bigcup_\wp \mathrm{Exc}_\wp \subset \{0, \ldots, q^{\deg \wp} - 2\}$ as $\mathrm{Exc}_d = \bigcup_i O_i$ into subsets O_i of maximal size with the following property: the set of $\wp$ (of still fixed degree d) that is exceptional for k in O_i is independent of the k in O_i. We call the O_i *orbits* of $k's$ for a fixed set of exceptional $\wp$. An orbit has a length, the cardinality $\#O_i$ of the relevant k, and a prime set P_{O_i} of exceptional $\wp$ for all $k \in O_i$. Suppose $d \leq 2q-2$ and q is a prime number. Our data supports the following properties:

1. $\#P_{O_i}$ is a multiple of q if $d \neq q$ and a multiple of $q-1$ is $d = q$.
2. Many orbits have length a multiple of d. But there are exceptions.

(3) The Artin–Schreier primes occur for many k's.

Some of the above phenomena might be explained by Proposition 5.5(4) which says that if $\wp(t)$ is exceptional then so are $\wp(t+\theta)$ and $\wp(\theta t)$. Another phenomenon is that many orbits are invariant under $k \mapsto k^p \mod q^d$.

Short polynomials. Fix a prime q. Let $I(k) := \overline{S}(k)/R(k)$ be the "irregular" part. If one puts all the $I(k)$ into a list and strips of q-powers, say for all k up to a certain bound, one obtains a relatively small list of exceptional parts. It is much smaller then one might expect. Its members of minimal degree (or of minimal number of terms) are Artin–Schreier polynomials. Those with more terms are more complicated. We tried to write these parts in way as simple as possible. These are polynomials in the expressions $[i]$ with possibly few terms. Let us give two examples:

Let first $q = 7$ and $k = 116 = (2\,2\,4)_7$. Then

$$I(k) = 6t^{98} + 3t^{56} + 6t^{50} + 6t^{14} + 6t^8 + t^2 = -[2]^2 + 3[2][1] + [1]^2.$$

Let next $q = 3$ and $k = 121 = (1\,1\,1\,1\,1)_3$. Then

$$\begin{aligned} I(k) &= t^{198} + t^{192} + t^{190} + t^{174} + t^{172} + t^{166} + t^{144} + t^{138} + t^{136} + t^{126} \\ &\quad + t^{114} + t^{110} + t^{102} + t^{100} + t^{96} + t^{92} + t^{88} + t^{86} + t^{66} + t^{64} + t^{58} \\ &\quad + t^{48} + t^{46} + t^{42} + t^{38} + t^{34} + t^{32} + t^{22} + t^{16} + t^{14} \\ &= [4]^2[3][2] + [4]^2[3][1] + [4]^2[2][1] + [4][3]^2[2] + [4][3]^2[1] + [4][3][2]^2 \\ &\quad + [4][3][1]^2 + [4][2]^2[1] + [4][2][1]^2 + [3]^2[2][1] + [3][2]^2[1] + [3][2][1]^2. \end{aligned}$$

While the expression for $I(121)$ in "brackets" $[i]$ is not short, it has an obvious simple pattern in it. We observe also, that in both cases the expressions in brackets are homogeneous and wonder if there are indeed simple predictions of polynomials in the $[i]$'s that would give the exceptional parts.

k with many symmetries. From our data it seems that certain k with high symmetry also have a tendency for a large set of exceptional primes. We have no explanation and except for (H6.3) no general patterns when this occurs. Here is an example.

Let $q = 5$. Then:

(1) for $k = 312 = (2\,2\,2\,2)_5$ the polynomial $\overline{S}(312)$ is the product of $[1]^{12}$ with 60 degree 4 exceptional primes;
(2) for $k = 781 = (1\,1\,1\,1\,1)_5$ the polynomial $\overline{S}(781)$ is the product of $[1]$ with 124 degree 5 exceptional primes (in accordance with Hypothesis (H6.3));
(3) for $k = 1302 = (2\,0\,2\,0\,2)_5$ the polynomial $\overline{S}(1302)$ is the product of $[2]^2$ with 200 degree 6 exceptional primes.

6.4. Questions.

(1) What is the full characterization of irregular or exceptional k's? We know it for $q = 2$ and have characterized irregular k's for $q = 3$ and have conjectured relations between irregular and exceptional, for q a prime.
(2) What is full characterization of exceptional primes? We only know for $q = 2$. We have proved infinitude of exceptional primes and have conjectured explicitly many exceptional primes for each $q > 2$ in each degree $m \geq q$. But the questions of existence of infinitely many non-exceptional primes for a given $q > 2$ seems to be open and seem to be of the flavor of classical open problem of infinitude of regular primes, in analogy with Herbrand–Ribet mentioned in the introduction. What are the asymptotics? The data above shows that for $q = 3$, $d = 6$ and in a few more cases, there are more exceptional primes than non-exceptional. We guess that there is a non-exceptional prime for every q and every degree d.
(3) What is a recipe for irregular non-exceptional part of the leading terms?
(4) What is the (geometric) meaning of multiplicities of the exceptional primes?
(5) What are direct geometric proofs of "no drop in rank" for $q = 2$ or of other theorems?
(6) Is the case $q \neq p$ closest to the case $q = p$ in those cases where $\lfloor \ell(p^i k)/(q-1) \rfloor$ is independent of i?

References

[1] G. Böckle, "The distribution of the zeros of the Goss zeta-function for $A = \mathbb{F}_2[x, y]/(y^2 + y + x^3 + x + 1)$", *Math. Z.* **275** (2013), no. 3-4, p. 835-861.
[2] ———, "Cohomological theory of crystals over function fields and applications", in *Arithmetic Geometry over Global Function Fields (CRM Barcelona 2010)*, Advanced Courses in Mathematics, Birkhäuser, 2014.
[3] G. Böckle & R. Pink, *Cohomological theory of crystals over function fields*, EMS Tracts in Mathematics, vol. 9, European Mathematical Society, 2009, viii+187 pages.
[4] W. Bosma, J. J. Cannon, C. Fieker & A. Steel (eds.), *Handbook of Magma functions*, 2010, Edition 2.16, 5017 pages.
[5] L. Carlitz, "Sums of products of multinomial coefficients", *Elem. Math.* **18** (1963), p. 37-39.
[6] C.-L. Chai, B. Conrad & F. Oort, *Complex multiplication and lifting problems*, Mathematical Surveys and Monographs, vol. 195, American Mathematical Society, 2014, ix+387 pages.
[7] S. Galovich & M. Rosen, "The class number of cyclotomic function fields", *J. Number Theory* **13** (1981), p. 363-375.
[8] E.-U. Gekeler, "On power sums of polynomials over finite fields", *J. Number Theory* **30** (1988), no. 1, p. 11-26.
[9] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3, vol. 35, Springer, 1996, xiii+422 pages.
[10] D. Goss & W. Sinnott, "Class groups of function fields", *Duke Math. J.* **52** (1985), p. 507-516.

[11] H. Lange & S. Recillas Pishmish, "Abelian varieties with group action", *J. Reine Angew. Math.* **575** (2004), p. 135-155.
[12] Y. I. Manin, "On the Hasse-Witt matrix of an algebraic curve", *Izv. Akad. Nauk SSSR, Ser. Mat.* **25** (1961), p. 1513-172, English translation in *Amer. Math. Soc. Transl.* **45** (1965), p. 245-264.
[13] Maplesoft, "Maple mathematics software", a division of Waterloo Maple Inc., Waterloo, Ontario.
[14] Maxima, "Maxima, a Computer Algebra System. Version 5.34.1", 2014, `http://maxima.sourceforge.net/`.
[15] B. Mazur, "How can we construct abelian Galois extensions of basic number fields?", *Bull. Am. Math. Soc.* **48** (2011), no. 2, p. 155-209.
[16] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer, 2002, xii+358 pages.
[17] D. Shiomi, "The Hasse-Witt invariant of cyclotomic function fields", *Acta Arith.* **150** (2011), no. 3, p. 227-240.
[18] ———, "Ordinary cyclotomic function fields", *J. Number Theory* **133** (2013), no. 2, p. 523-533.
[19] H. Stichtenoth, "Die Hasse-Witt Invariante eines Kongruenzfunktionenkörpers", *Arch. Math.* **33** (1980), p. 357-360.
[20] L. Taelman, "A Herbrand-Ribet theorem for function fields", *Invent. Math.* **188** (2012), no. 2, p. 253-275.
[21] S. Tauber, "On multinomial coefficients", *Am. Math. Mon.* **70** (1963), p. 1058.1063.
[22] D. S. Thakur, *Function Field Arithmetic*, World Scientific, 2004, xv+388 pages.
[23] ———, "Power sums with applications to multizeta and zeta zero distribution for $\mathbb{F}_q[t]$", *Finite Fields Appl.* **15** (2009), no. 4, p. 534-552.
[24] ———, "Valuations of ν-adic power sums and zero distribution for the Goss' v-adic zeta function for $\mathbb{F}_q[t]$", *J. Integer Seq.* **16** (2013), no. 2, Article 13.2.13, 18 p.
[25] The Sage Developers, "SageMath, the Sage Mathematics Software System (Version 6.2)", 2014, `http://www.sagemath.org/`.
[26] W. C. Waterhouse, "Abelian varieties over finite fields", *Ann. Sci. Éc. Norm. Supér.* **2** (1969), p. 521-560.

Gebhard Böckle
IWR, Universität Heidelberg
69120 Heidelberg, Germany
E-mail: `gebhard.boeckle@iwr.uni-heidelberg.de`

Dinesh S. Thakur
Department of Mathematics
University of Rochester
Rochester, NY 14627, USA
E-mail: `dinesh.thakur@rochester.edu`