Math. Z. (2013) 275:835–861
DOI 10.1007/s00209-013-1162-9

Mathematische Zeitschrift

The distribution of the zeros of the Goss zeta-function for $A = \mathbb{F}_2[x, y]/(y^2 + y + x^3 + x + 1)$

Gebhard Böckle

Received: 10 June 2012 / Accepted: 6 February 2013 / Published online: 16 April 2013

Abstract Let F be a global function field over a finite constant field and ∞ a place of F. The ring A of functions regular away from ∞ in F is a Dedekind domain. For such A Goss defined a ζ-function which is a continuous function from $\mathbb{Z}_p$ to the ring of entire power series with coefficients in the completion F_∞ of F at ∞. He asks what one can say about the distribution of the zeros of the entire function at any parameter of $\mathbb{Z}_p$. In the simplest case A is the polynomial ring in one variable over a finite field. Here the question was settled completely by J. Sheats, after previous work by J. Diaz-Vargas, B. Poonen and D. Wan: for any parameter in $\mathbb{Z}_p$ the zeros of the power series have pairwise different valuations and they lie in F_∞. In the present article we completely determine the distribution of zeros for the simplest case different from polynomial rings, namely $A = \mathbb{F}_2[x, y]/(y^2 + y + x^3 + x + 1)$—this A has class number 1, it is the affine coordinate ring of a supersingular elliptic curve and the place ∞ is $\mathbb{F}_2$-rational. The answer is slightly different from the above case of polynomial rings. For arbitrary A such that ∞ is a rational place of F, we describe a pattern in the distribution of zeros which we observed in some computational experiments. Finally, we present some precise conjectures on the fields of rationality of these zeroes for one particular hyperelliptic A of genus 2.

1 Introduction

The theme of this article goes back to the mid 1990's when D. Wan, J. Diaz-Vargas, B. Poonen and J. Sheats in [8,17,24] determined the distribution of the zeros of the Goss ζ-function for all rational function fields over a finite field and a chosen rational point. Prior to [24], Goss had given an interpretation of the distributions of these zeros as an analog of the classical Riemann hypothesis, see [24, p. 198f.] or [13]. A slightly different function field Riemann hypothesis had been formulated by Wan in [24, p. 197f.]. Since [17], no distribution of zeros

G. Böckle (✉)
Interdisciplinary Center for Scientific Computing, Heidelberg University,
Im Neuenheimer feld 368, 69120, Heidelberg, Germany
e-mail: gebhard.boeckle@iwr.uni-heidelberg.de

of a further function field or non-rational chosen place had been determined, see however [24, p. 199]. Due to examples of Thakur in [21] and observations of Goss in [14] it is clear that the results will be different from the rational case.

In the present article we go in two ways beyond the results mentioned above. First, we completely determine for one non-rational function field of class number one and a rational place the distribution of zeros. Except for the two zeros of smallest absolute value (which occur for the smallest slope of the Newton polygon of the power series), the distributions are as in the rational case. Second we did some numerical experiments. These suggest that if the chosen place of the function field is rational, then again apart from the initial small zeros, the distribution of zeros is regular. We also computed for one particular field and chosen place ∞, experimentally, the fields of definition of the roots as an extension of the completion F_∞ of the function field at ∞. This gives strong evidence that the compositum of these fields in a fixed algebraic closure of F_∞, for all parameters in $\mathbb{Z}_p$ at once, is of infinite degree over F_∞. This is strikingly different from the case of rational function fields and the usual chosen place ∞; here Sheats' results (and the method of Newton polygons) imply that all roots lie in F_∞. The question about the degrees of these splitting fields was raised in [13, Conj. 4]; see also Remark 8.1.

To describe the contents of this article in greater detail let us introduce some notation. We fix a prime number p, denote by q a power p^e of p and write $\mathbb{F}_q$ for a field of q elements. By F we denote a global function field with $\mathbb{F}_q$ as its field of constants. By X we denote the smooth projective curve over $\mathbb{F}_q$ with function field F and we write $g = g_F = g_X$ for its genus. We fix a place ∞ of F and then define A as the ring of functions in F regular outside ∞, so that $X = \operatorname{Spec} A \cup \{\infty\}$, set-theoretically.

Assumption 1.1 Throughout this article, we assume that ∞ is $\mathbb{F}_q$-rational.

We shall say nothing in cases when the hypothesis of Assumption 1.1 is not met. The completion of F at ∞ will be F_∞. We fix a uniformizer π_∞ of F_∞ and write $\mathcal{O}_\infty$ for its ring of integers. The uniformizer π_∞ defines a sign-homomorphism $\operatorname{sgn}\colon F_\infty^* \longrightarrow \mathbb{F}_q^*$, which is defined by the rule that it sends a product $\pi_\infty^n u$ with $n \in \mathbb{Z}$ and $u \in \mathcal{O}_\infty^*$ to $u \pmod{\pi_\infty} \in \mathbb{F}_q^*$ (since ∞ is $\mathbb{F}_q$-rational, $\mathbb{F}_q$ is naturally isomorphic to the residue field at ∞). The sign homomorphism allows one to define $A_+ := \{a \in A \setminus \{0\} \mid \operatorname{sgn}(a) = 1\}$ as the set of positive elements of A. For any $d \in \mathbb{N}_0$ we set $A_{+,d} := \{a \in A_+ \mid \deg(a) = d\}$ where $\deg(a) \in \mathbb{N}_0$ is defined so that $q^{\deg(a)} = \#A/(a)$. Note that for $F = \mathbb{F}_q(t)$, $\pi_\infty = 1/t$ (and ∞ the place at which π_∞ vanishes) the set $A_{+,d}$ consists of all monic polynomials in $\mathbb{F}_q[t]$ of degree d. Finally for $n \in \mathbb{N}$ with base q expansion $n = a_0 + a_1 q + \cdots + a_\ell q^\ell$ we define $\operatorname{dig}_q(n) := a_0 + \cdots + a_\ell$ as the sum of its digits in base q expansion.

Following [21], we define for any $n \in \mathbb{Z}$ the power series

$$\zeta_A(n, T) := \sum_{d \in \mathbb{N}_0} T^d \left(\sum_{a \in A_{+,d}} a^{-n} \right) \in 1 + TF[[T]].$$

In the terminology of Goss [12, Ch. 8] this is the ζ-function for the principal (positively generated) ideals of A. In [21] one finds that the sum $S_A(-n, d) := \sum_{a \in A_{+,d}} a^n$ is zero whenever

$$n \geq 0 \quad \text{and} \quad \dim H^0(X, \mathcal{O}_X(d\infty)) - 1 > \frac{\operatorname{dig}_q(n)}{q-1} \tag{1}$$

Hence for all $n \leq 0$ the expression $\zeta_A(n, T)$ is a polynomial.

To describe a simple improvement of the degree bound on $\zeta_A(-n,T)$ derived from (1), consider the function

$$d \mapsto \dim H^0(X, \mathcal{O}_X(d\infty)) - 1.$$

The function is obviously increasing in d of slope at most one. It takes the value zero for $d = 0$. By the definition of the genus g of X the function is linear of slope 1 for $d \geq 2g$. Let $h_A : \mathbb{N} \to \mathbb{N}, x \mapsto \max\{d \in \mathbb{N} \mid \dim H^0(X, \mathcal{O}_X(d\infty)) - 1 \leq x\}$. The function $x \to h_A(x)$ is linear of slope 1 for $x \geq g$ and increases from 0 to $2g-1$ for $0 \leq x \leq g$. The estimate derived from (1) yields $\deg_T \zeta_T(-n,T) \leq h_A(\lfloor(\mathrm{dig_q}(n))/(q-1)\rfloor)$. Taking further into account the elementary formula $\zeta_A(n,T)^p = \zeta_A(pn, T^p)$ which implies that the degree in T for $-n$ and for $-pn$ is the same, one obtains the bound:

$$\deg_T \zeta_A(-n,T) \leq d_A(n) := h_A\Big(\min_{i=1,\ldots,e} \lfloor \frac{\mathrm{dig_q}(np^i)}{q-1} \rfloor\Big) \tag{2}$$

which in particular yields $d_A(n) = O(\log_q(n))$. If one renormalizes the $\zeta_A(n,T)$ and defines

$$z_A(n,T) := \zeta_A(n, T\pi_\infty^{-n})$$

then it is quite elementary to see that the coefficients of the power series $z_A(n,T)$ in T satisfy congruences. Using the logarithmic degree bound in n on the $\zeta_A(-n,T)$, this observation was sharpened by Goss in [12, Ch 8] to the following result: the power series $z_A(n,T)$, $n \in \mathbb{Z}$, can be interpolated to a continuous function with domain $\mathbb{Z}_p$ and image the entire power series in T with coefficients in F_∞.

The special values $z_A(n,T)$ being entire power series, it makes sense to ask about the distribution of their zeros. The following result summarizes what is known due to [8,17,24] in the case of rational function fields with ∞ the usual place:

Theorem 1.2 (Wan, Diaz-Vargas, Poonon, Sheats). *Let $A = \mathbb{F}_q[t]$. Then*

(a) $\deg_T \zeta_A(-n,T) = d_A(n) = \min_{i=1,\ldots,e} \lfloor \frac{dig_q(np^i)}{q-1} \rfloor$.
(b) *For all $n \in \mathbb{Z}_p$, all slopes of the Newton polygon of $z_A(n,T)$ have width* 1.
(c) *For all $n \in \mathbb{Z}_p$, all roots of the Newton polygon $z_A(n,T)$ are simple and have pairwise distinct valuations and in particular, they are all distinct and lie in F_∞.*

We note that part (a) is not explicitly stated in [17], but is an immediate consequence of the computations there. We shall explain this in Sect. 7. Thinking of F_∞ as the analog of the line $\frac{1}{2} + i\mathbb{R}$, in [13] Goss interprets (c) as an analog of the Riemann hypothesis of the classical Riemann ζ-function.

The main result of the present article is the following:

Theorem 1.3 *Let $A = \mathbb{F}_2[x,y]/(y^2 + y + x^3 + x + 1)$. Then*

(a) *For $n = 2^k$ and $k \geq 0$, one has $\zeta_A(-n,T) = (1-T)^2$; cf.* [21, §3].
(b) *For any $n \in \mathbb{N}$ one has $\deg_T \zeta_A(-n,T) = 1 + dig_2(n) = d_A(n)$.*
(c) *For $n = 2^{k_1} + \cdots + 2^{k_\ell}$ with $0 \leq k_1 < k_2 < \cdots < k_\ell$ and $\ell \geq 1$, the Newton polygon of $z_A(-n,T)$ has slopes 2^{k_1}, $2^{k_1} + 2^{k_2}$, $2^{k_1} + 2^{k_2} + 2^{k_3}, \ldots, 2^{k_1} + 2^{k_2} + \cdots + 2^{k_\ell}$; the smallest slope occurs with multiplicity two, all other slopes with multiplicity one. In particular, the x-coordinates of the break points of the Newton polygon are independent of n.*
(d) *Except for the two roots of smallest absolute value, all roots have pairwise different valuations and thus lie in F_∞.*

Note that A is the coordinate ring of the affine part of a supersingular elliptic curve over $\mathbb{F}_2$ minus its unique $\mathbb{F}_2$-rational point. Moreover A has class number one, which is very useful in the proof of the above theorem. Finally part (c) also holds for arbitrary $n \in \mathbb{Z}_2$, and infinite 2-adic expansions, by the continuity of the map $n \mapsto z_A(n, T)$.

We cannot say much in this introduction about the proof of the Theorem 1.3: It is obtained by analyzing the action of a Cartier linear endomorphism on a dual of the A-motive attached to certain tensor powers of the Drinfeld Hayes module for A. It builds on the work of Anderson, Böckle and Pink, and Taguchi and Wan, cf. [2,5,19]. The proof covers Sects. 2–6. It may well be that a combinatorial proof can also be given. To explain some ideas of the proof, we give in Sect. 7 in a much simpler setting by similar methods a proof of a leading term formula due to Pink and Thakur.

Following a suggestion of D. Thakur, we investigated the four roots of lowest absolute value in the case $A' = \mathbb{F}_2[x, y]/(y^2 + y + x^5 + x + 1)$. We report our findings in Sect. 8. The computations suggest that the conductor of the splitting field of $\zeta_{A'}(n, T)$ over F_∞, which is of degree at most 4, can be arbitrarily large; this is based on a conjectural formula for the conductor of the splitting field above F_∞ which depends on the lowest three non-zero 2-adic digits of n only. In Sect. 8 we also comment on some patterns for the x-coordinates of the break points of the Newton polygons of $\zeta_A(n, T)$ for some rings A that arise from curves X of small genus with a chosen rational point ∞.

2 The Drinfeld–Hayes-motive for A

For a smooth projective, geometrically irreducible curve X over the field $\mathbb{F}_q$ and a choice of a closed (not necessarily $\mathbb{F}_q$-rational) point ∞, Drinfeld and Hayes have explained, independently, the existence of an integral model for a rank 1 sign-normalized Drinfeld A-module over Spec B, where B is the normalization of the ring A in the strict Hilbert class field of F with respect to the place ∞ – see for instance [12, Ch. 7] or [22, Ch. 3]. The number of such modules is equal to the strict class number of A. Using Anderson's dictionary between Drinfeld A-modules and certain A-motives, each such Drinfeld–Hayes module defines an A-motive on Spec B. These A-motives will be key to our approach of computing special values of the Goss L-function of (F, ∞) at negative integers. Therefore we shall need a precise description of these A-motives or at least a good understanding of the associated τ-sheaf, in the sense of [5], on Spec B with coefficients in $\overline{F}$, a fixed algebraic closure of F. Moreover we shall need its maximal extension, in the sense of [9], from Spec B to the smooth projective curve with function field the field of fractions $Q(B)$ of B.

In the present section we determine this τ-sheaf for the particular ring

$$A = \mathbb{F}_2[x, y]/(y^2 + y + x^3 + x + 1).$$

It has the simplifying feature that its strict class number is one, see [15], so that $B = A$ and there is exactly one τ-sheaf as above.

The places of the fraction field F of A are in bijection with the non-zero prime ideals of A together with the place ∞ of the elliptic curve $E/\mathbb{F}_2$ defined by A. The ring A has strict class number one with respect to the place ∞ because ∞ is $\mathbb{F}_2$-rational and $\mathrm{Cl}(A) \cong E(\mathbb{F}_2) = \{\infty\}$. Thus the corresponding strict Hilbert class field is F itself. Its ring of integers away from ∞ is A. The general theory of Drinfeld–Hayes modules tells us that this ring of integers is the base of a rank-1 sign-normalized Drinfeld–Hayes module and that there is a unique such module. To distinguish the base ring from the coefficients we use bold notation, i.e., we

define

$$\mathbf{A} = \mathbb{F}_2[\mathbf{x}, \mathbf{y}]/(\mathbf{y}^2 + \mathbf{y} + \mathbf{x}^3 + \mathbf{x} + 1),$$

and refer to Spec $\mathbf{A}$ as our base scheme. The Drinfeld–Hayes module for A is then the ring homomorphism

$$A \longrightarrow \mathbf{A}\{\tau\} : f \mapsto \rho_f$$

where the expressions for ρ_x and ρ_y are given explicitly by

$$\rho_x = \mathbf{x} + (\mathbf{x}^2 + \mathbf{x})\tau + \tau^2 \quad \rho_y = \mathbf{y} + (\mathbf{y}^2 + \mathbf{y})\tau + \mathbf{x}(\mathbf{y}^2 + \mathbf{y})\tau^2 + \tau^3;$$

see [10, p. 345].

We also consider the elliptic curve $\mathbf{E}/\mathbb{F}_2$ given in homogeneous coordinates by

$$\mathbf{y}^2\mathbf{z} + \mathbf{y}\mathbf{z}^2 = \mathbf{x}^3 + \mathbf{x}\mathbf{z}^2 + \mathbf{z}^3.$$

The differential $\omega = \frac{\mathrm{d}\mathbf{y}}{\mathbf{x}^2+1} = \mathbf{d}\mathbf{x}$ is nowhere vanishing and a global section of the sheaf of differentials $\Omega_{\mathbf{E}/\mathbb{F}_2}$. Clearly $\mathbf{E} \setminus \{\infty\} = \operatorname{Spec}\mathbf{A}$ and one finds

$$\Omega_{\mathbf{A}/\mathbb{F}_2} := \Gamma(\operatorname{Spec}\mathbf{A}, \Omega_{\mathbf{E}/\mathbb{F}_2}) = \mathbf{A}\mathbf{d}\mathbf{x}$$

To pass from the Drinfeld A-module to its corresponding A-motive, we follow the procedure described in [1, §1]: we consider $P := \mathbf{A}\{\tau\}$ as a module over $\mathbf{A} \otimes_{\mathbb{F}_2} A = \mathbf{A}[x, y]/(y^2 + y + x^3 + x + 1)$ such that

(a) Elements $\mathbf{a}$ of $\mathbf{A}$ act on P via multiplication from the left by $\mathbf{a}$.
(b) Elements a of A act on P via composition with ρ_a from the right.

This makes P into an $\mathbf{A}$-A-bimodule where the action of $\mathbf{A}$ and A commute and thus into an $\mathbf{A} \otimes_{\mathbb{F}_2} A$-module. Essentially from the results in [1] it follows that P is a projective $\mathbf{A} \otimes_{\mathbb{F}_2} A$-module of rank 1.

We want to distinguish between the indeterminate τ in the skew-polynomial ring $\mathbf{A}\{\tau\}$ and the powers of τ as elements of P. Therefore we write Φ^i for the element τ^i of P. The Φ^i, $i \in \mathbb{N}_0$, form an $\mathbf{A}$-basis of P. The left action by $\tau \in \mathbf{A}\{\tau\}$ on P is thus given by left multiplication by τ on P, i.e., we have $\tau(\mathbf{a}\Phi^i) = \mathbf{a}^2\Phi^{i+1}$. Note that we usually write 1 for Φ^0.

Our first aim is to describe the module P over $\mathbf{A} \otimes_{\mathbb{F}_2} A$ in various explicit ways. In a first step we consider P over $\mathbf{A}[x] = \mathbf{A} \otimes_{\mathbb{F}_2} \mathbb{F}_2[x]$. Over it, the module P is free of rank 2 with basis 1 and Φ, i.e., $P = \mathbf{A}[x] \oplus \mathbf{A}[x]\Phi$. The endomorphism τ is given with respect to this $\mathbf{A}[x]$-basis by

$$\tau = \begin{pmatrix} 0 & x+\mathbf{x} \\ 1 & \mathbf{x}^2+\mathbf{x} \end{pmatrix} (\sigma_{\mathbf{A}} \otimes \mathrm{id}_{\mathbb{F}_2[x]}).$$

Observe that since $\mathbf{A}$ is factorial, so is the polynomial ring $\mathbf{A}[x]$ over it. We note the following formulas for multiplication of an element $\mathbf{a}(\Phi) \in \mathbf{A}\{\Phi\}$ by elements in $\mathbf{A}$ and A:

$$\mathbf{x} \cdot \mathbf{a}(\Phi) = (\mathbf{x}\mathbf{a})(\Phi), \quad \tau \cdot \mathbf{a}(\Phi) = (\tau \circ \mathbf{a})(\Phi) \tag{3}$$

$$x \cdot \mathbf{a}(\Phi) = \mathbf{a}(\tau)(\mathbf{x} + (\mathbf{x}^2 + \mathbf{x})\Phi + \Phi^2) \tag{4}$$

$$y \cdot \mathbf{a}(\Phi) = \mathbf{a}(\tau)(\mathbf{y} + (\mathbf{y}^2 + \mathbf{y})\Phi + \mathbf{x}(\mathbf{y}^2 + \mathbf{y})\Phi^2 + \Phi^3) \tag{5}$$

and thus, using the equality $\mathbf{y}^2+\mathbf{y}=\mathbf{x}^3+\mathbf{x}+1$ and that we are over $\mathbb{F}_2$, we obtain

$$\begin{aligned} x\cdot\Phi &= \tau(\mathbf{x}+(\mathbf{x}^2+\mathbf{x})\Phi+\Phi^2) = \mathbf{x}^2\Phi+(\mathbf{x}^4+\mathbf{x}^2)\Phi^2+\Phi^3\\ y\cdot 1 &= \mathbf{y}+(\mathbf{y}^2+\mathbf{y})\Phi+\mathbf{x}(\mathbf{y}^2+\mathbf{y})\Phi^2+\Phi^3\\ \mathbf{x}x\cdot 1 &= \mathbf{x}(\mathbf{x}+(\mathbf{x}^2+\mathbf{x})\Phi+\Phi^2) = \mathbf{x^2}+(\mathbf{x^3}+\mathbf{x^2})\Phi+x\Phi^2\\ x\cdot\Phi+y\cdot 1+\mathbf{x}x\cdot 1 &= \mathbf{y}+\mathbf{x^2}+(\mathbf{1}+\mathbf{x})\Phi \end{aligned}$$

In other words, if we set $\alpha := 1+x+\mathbf{x}$ and $\beta = y+\mathbf{y}+\mathbf{x}(x+\mathbf{x})$, then we have the relation

$$\beta\cdot 1 = \alpha\,\Phi.$$

To understand P as a module over $\mathbf{A}\otimes_{\mathbb{F}_2} A$, we first give an algebraic description: since $\mathbf{A}$ is geometrically irreducible over $\mathbb{F}_2$, the ring $\mathbf{A}\otimes_{\mathbb{F}_2} F$ is a Dedekind domain over F and in particular $S := \mathbf{A}\otimes_{\mathbb{F}_2} A$ is an integral domain. For any non-zero elements $u, v\in S$ we denote by $\frac{u}{v}$ the fraction of u divided by v in a fixed quotient field $Q(S)$ of S. The formula $\alpha\Phi=\beta\cdot 1$ in P allows us to identify P with

$$P = \Big(1,\frac{\beta}{\alpha}\Big) := S+S\frac{\beta}{\alpha}\subset Q(S).$$

Observe that $\frac{\beta}{\alpha}$ is the shtuka function in [20, Ex. 2.3.(a)]. In terms of the generators $1,\ \frac{\beta}{\alpha}$ of P, the action of τ from the left is given by

$$\begin{aligned} \tau(1) &= \Phi = 1\cdot\frac{\beta}{\alpha},\\ \tau\Big(\frac{\beta}{\alpha}\Big) &= \tau^2(1) = \Phi^2 = x\cdot 1+\mathbf{x}+(\mathbf{x}^2+\mathbf{x})\Phi = (x+\mathbf{x})\cdot 1+(\mathbf{x}^2+\mathbf{x})\cdot\frac{\beta}{\alpha}. \end{aligned}$$

Geometrically, $\operatorname{Spec} S = \operatorname{Spec}\mathbf{A}\times\operatorname{Spec} A = (\mathbf{E}\smallsetminus\{\infty\})\times(E\smallsetminus\{\infty\})$ is the product of two affine elliptic curves $\operatorname{Spec}\mathbf{A}$ and $\operatorname{Spec} A$. The locally free sheaf $\mathcal{L}$ associated with the projective S-module P is the sheaf $\mathcal{O}_{\operatorname{Spec} S}(D)$ containing the structure sheaf $\mathcal{O}_{\operatorname{Spec} S}$ and with D the reduced subscheme of $\operatorname{Spec} S$ defined by

$$0\overset{!}{=}\frac{\alpha}{\beta} = \frac{1+x+\mathbf{x}}{y+\mathbf{y}+\mathbf{x}(x+\mathbf{x})}.$$

For any given x, the hyperplane $1+x+\mathbf{x}=0$ in $\mathbb{A}^4=\mathbb{A}^2\times\mathbb{A}^2$ intersects $\operatorname{Spec}\mathbf{A}\times\operatorname{Spec} A$ in two lines:

$$\mathbf{y}=1+x+y \quad\text{and}\quad \mathbf{y}=x+y.$$

The hypersurface $0=\beta=y+\mathbf{y}+\mathbf{x}(x+\mathbf{x})$ contains $\mathbf{y}=1+x+y$ but not $\mathbf{y}=x+y$ (assuming $1+x+\mathbf{x}=0$). We find that D is the restriction to $\operatorname{Spec}\mathbf{A}\times\operatorname{Spec} A$ of the graph of the isomorphism $E\to\mathbf{E}: (x,y)\mapsto(1+x,x+y)$ with inverse $\mathbf{E}\to E: (\mathbf{x},\mathbf{y})\mapsto(1+\mathbf{x},1+\mathbf{x}+\mathbf{y})$. In particular the closure $D\cup\{\infty\times\infty\}\subset\mathbf{E}\times E$ of D, which by slight abuse of notation we denote again by D, is a divisor of degree 1 over $\mathbf{E}$ and over E.

For later we observe that the dual of P is $P^\vee=\Gamma(\operatorname{Spec}\mathbf{A}\times\operatorname{Spec} A,\mathcal{O}_{\operatorname{Spec} S}(-D)) = \alpha S+\beta S\subset S$; the verification of the latter we leave to the reader. We summarize the results on P:

Lemma 2.1 *Let $P := \mathbf{A}\{\tau\}$ as a module over $S=\mathbf{A}\otimes_{\mathbb{F}_2} A$. Then $P=(1,\frac{\beta}{\alpha})\subset Q(S)$ for $\alpha=1+x+\mathbf{x}$ and $\beta=(y+\mathbf{y}+\mathbf{x}(x+\mathbf{x}))$, with*

$$\tau(1)=\frac{\beta}{\alpha},\qquad\text{and}\qquad \tau\Big(\frac{\beta}{\alpha}\Big)=(x+\mathbf{x})\cdot 1+(\mathbf{x}^2+\mathbf{x})\cdot\frac{\beta}{\alpha}.$$

Let $D \subset \mathbf{E} \times E$ be the graph of the isomorphism $E \to \mathbf{E} : (x, y) \mapsto (1 + x, x + y)$ with inverse $\mathbf{E} \to E : (\mathbf{x}, \mathbf{y}) \mapsto (1 + \mathbf{x}, 1 + \mathbf{x} + \mathbf{y})$. As a divisor it has degree 1 over both factors $\mathbf{E}$ and E of $\mathbf{E} \times E$.

As a set of global sections we have

$$P = \Gamma((\mathbf{E} \smallsetminus \{\infty\}) \times (E \smallsetminus \{\infty\}), \mathcal{O}_{\mathbf{E}\times E}(D))$$

Furthermore the dual $P^\vee$ is the submodule $\alpha S + \beta S$ of S.

Up to this point, the above analysis is very similar to that of shtuka functions of Thakur as in [20] except that we work integrally over the base and coefficients whereas in op.cit. the base considered was simply Spec $\mathbf{F}$—or rather Spec $\overline{\mathbf{F}}$ where $\overline{\mathbf{F}}$ denotes an algebraic closure of $\mathbf{F}$. For us the opposite viewpoint will be important. To study special values of the ζ-function of A at negative integers, we will require the base to be integral but may replace the coefficients A by F, or for simplicity by $\overline{F}$. This explains the difference in our treatment from that in [20].

Let $\sigma_{\mathbf{E}}$ denote the absolute Frobenius endomorphism of $\mathbf{E}$. For a divisor $\mathcal{D} \subset \mathbf{E} \times E$ (or $\mathcal{D} \subset \operatorname{Spec} \mathbf{A} \times \operatorname{Spec} A$), its pullback under $(\sigma_{\mathbf{E}} \times \mathrm{id}_E)^*$ is again a divisor on $\mathbf{E} \times E$. In terms of composition of correspondences, one can equivalently define this pullback as $\mathcal{D} \circ \operatorname{Graph}(\sigma_{\mathbf{E}})^t$, where for a divisor on a product of curves $C \times C'$ the superscript ^{t} indicates that we pass to its dual on $C' \times C$. For D the latter shows that $(\sigma_{\mathbf{E}} \times \mathrm{id}_E)^* D$ is the dual of the graph of $\sigma_{\mathbf{E}} \circ i : E \to \mathbf{E}$ for i the isomorphism $E \to \mathbf{E}$, $(x, y) \mapsto (1 + x, x + y)$.

Set $\overline{\mathbf{X}} := \mathbf{E} \times \operatorname{Spec} \overline{F}$ and $\overline{X} := \operatorname{Spec} \overline{\mathbf{F}} \times E$. These are smooth projective curves over $\overline{F}$ or $\overline{\mathbf{F}}$, respectively. Motivated by the notation in [20], for any $n \in \mathbb{Z}$ we define ${}^{(n)}\mathcal{D}$ for a divisor $\mathcal{D}$ on $\overline{X}$ by ${}^{(n)}(\mathbf{a}, \mathbf{b}) := (\mathbf{a}^{2^n}, \mathbf{b}^{2^n})$ on closed points, and $\mathcal{D}^{(n)}$ for a divisor $\mathcal{D}$ on $\overline{\mathbf{X}}$ by $(a, b)^{(n)} := (a^{2^n}, b^{2^n})$ on closed points; note that the Frobenius endomorphism is an automorphism on algebraically closed fields. Suppose now that a divisor on $\overline{X}$ or $\overline{\mathbf{X}}$ arises by base change from a divisor $\mathcal{D}$ on $\mathbf{E} \times E$ (which is neither vertical or horizontal); we keep the notation $\mathcal{D}$ for the base change. Then the base change of $(\sigma_{\mathbf{E}} \times \mathrm{id}_E)^*\mathcal{D}$ to $\overline{X}$ is ${}^{(1)}\mathcal{D}$ while that to $\overline{\mathbf{X}}$ is $2\mathcal{D}^{(-1)}$. Note in particular that the degree of $(\sigma_{\mathbf{E}} \times \mathrm{id}_E)^*\mathcal{D}$ as a divisor on $\overline{X}$ is the same as the degree of $\mathcal{D}$ on $\overline{X}$, while over $\overline{\mathbf{X}}$ the degree gets multiplied by the degree of Frobenius, i.e. by 2. Abstractly this can be deduced from the fact that the divisor $\operatorname{Graph}(\sigma_{\mathbf{E}})^t$ has degree 2 over $\mathbf{E}$ and degree 1 over E.

We recall the situation from [20, 2.3(a)]: Let $\Delta \subset \mathbf{E} \times E$ denote the diagonal divisor (called ξ in [20, 2.3(a)]); the divisor D defined by $\alpha = 0$ and $\beta \neq 0$ is called $\xi + 1$ in [20, 2.3(a)]. Following [20], we set $V := \mathcal{O}_{\overline{X}}(D)$ and $f := \frac{\beta}{\alpha}$. A simple calculation shows that the divisor of f is

$$\operatorname{div}(f) = \operatorname{div}\left(\frac{y + \mathbf{y} + \mathbf{x}(x + \mathbf{x})}{1 + x + \mathbf{x}}\right) = [\Delta] + [{}^{(1)}D] - [D] - [\infty]; \tag{6}$$

to make computations more transparent, we use [__] in the notation for divisors, since it will be useful to distinguish the negative sign of the group law from that on divisors, e.g., to distinguish $[-\Delta]$ from $-[\Delta]$—even though as classes we have $-[\mathcal{D}] \equiv [-\mathcal{D}]$. Regarding the computation of $\operatorname{div}(f)$ we note that $\beta = 0$ is satisfied for $(x, y) = (\mathbf{x}, \mathbf{y})$, $(x, y) = (1 + \mathbf{x}^2, 1 + \mathbf{x}^2 + \mathbf{y}^2)$ and $(x, y) = (1 + \mathbf{x}, \mathbf{x} + \mathbf{y})$, i.e., β vanishes on Δ, ${}^{(1)}D$ and $-D$. From (6) we deduce the short exact sequence

$$0 \longrightarrow {}^{(1)}V(-\infty) \xrightarrow{s \mapsto f \cdot s} V \longrightarrow \mathcal{O}_\Delta \longrightarrow 0.$$

Let us consider the situation over $\overline{\mathbf{X}}$ and set $\mathbf{V} := \mathcal{O}_{\overline{\mathbf{X}}}(D)$. This means that we regard the bold indeterminates as variables and the others as constants. The following result is straightforward:

Lemma 2.2 *The affine vanishing locus of β base changed to $\overline{\mathbf{X}}$ (here β has degree 2) is the divisor $[\Delta] + 2[D^{(-1)}] + [-D]$; that of α is given by $[D] + [-D]$. Thus for $f = \frac{\beta}{\alpha}$ one has*

$$\mathbf{div}(f) = [\Delta] + 2[D^{(-1)}] - [D] - 2[\infty].$$

Multiplication by f occurs in the short exact sequence

$$0 \longrightarrow (\sigma \times \mathrm{id})^*\big(\mathcal{O}_{\overline{\mathbf{X}}}(D-2\infty)\big) \xrightarrow{s \mapsto f \cdot s} \mathcal{O}_{\overline{\mathbf{X}}}(D-2\infty) \longrightarrow \mathcal{O}_{\Delta} \longrightarrow 0. \tag{7}$$

Finally there is an isomorphism $(\sigma \times \mathrm{id})^*\mathcal{O}_{\overline{\mathbf{X}}}(D - 2\infty) \cong \mathcal{O}_{\overline{\mathbf{X}}}(2D^{(-1)} - 4\infty)$.

Remark 2.3 In the notation of [5], the pair $(\mathcal{O}_{\overline{\mathbf{X}}}(D - 2\infty), s \mapsto f \cdot s)$ is a τ-sheaf on $\mathbf{E}$ over $\overline{F}$, i.e.,

(a) $\mathcal{O}_{\overline{\mathbf{X}}}(D - 2\infty)$ is a coherent sheaf on $\mathbf{E} \times \mathrm{Spec}\,\overline{F}$ and
(b) $s \mapsto f \cdot s$ is a homomorphism $(\sigma \times \mathrm{id})^*\big(\mathcal{O}_{\overline{\mathbf{X}}}(D - 2\infty)\big) \longrightarrow \mathcal{O}_{\overline{\mathbf{X}}}(D - 2\infty)$.

The underlying sheaf $\mathcal{O}_{\overline{\mathbf{X}}}(D - 2\infty)$ is locally free, so that it is a locally free τ-sheaf. The τ-sheaf is a maximal extension from $\mathbf{E} \setminus \{\infty\}$ to $\mathbf{E}$ in the sense of Gardeyn, cf. [9, § 2], because the morphism on ∞ is an isomorphism (and this is a sufficient condition for maximality). Also note that (7) is defined on $\mathbf{E}$ over A – and even on $\mathbf{E} \times E$ with the exception of $\infty \times \infty$.

Definition 2.4 For any divisor $\mathcal{D}$ on $\overline{\mathbf{X}}$ and line bundle $L = \mathcal{O}_{\overline{\mathbf{X}}}(\mathcal{D})$ we define $L^{(n)} := \mathcal{O}_{\overline{\mathbf{X}}}(\mathcal{D}^{(n)})$. In particular $(\sigma \times \mathrm{id})^*L = (L^{(-1)})^{\otimes 2}$.

We end this section by stating some computations regarding the **Cartier operator** on A, leaving details for the reader to verify:

Lemma 2.5 *Consider the diagram*

$$\begin{array}{ccc} \mathbb{F}_2[\mathbf{x},\mathbf{y}]/(\mathbf{y}^2+\mathbf{y}+\mathbf{x}^3+\mathbf{x}+1) & \xrightarrow{0} & \mathbb{F}_2[\mathbf{x},\mathbf{y}]/(\mathbf{y}^2+\mathbf{y}+\mathbf{x}^3+\mathbf{x}+1)\mathrm{d}\mathbf{x} \\ \downarrow{\scriptstyle \sigma_0} & & \downarrow{\scriptstyle \sigma_1} \\ \mathbb{F}_2[\mathbf{x},\mathbf{y}]/(\mathbf{y}^2+\mathbf{y}+\mathbf{x}^3+\mathbf{x}+1) & \xrightarrow{d} & \mathbb{F}_2[\mathbf{x},\mathbf{y}]/(\mathbf{y}^2+\mathbf{y}+\mathbf{x}^3+\mathbf{x}+1)\mathrm{d}\mathbf{x} \end{array}$$

with $\sigma_0(f) = f^2$ and $\sigma_1(g\,\mathrm{d}f) = g^2 f\,\mathrm{d}f$ and the morphism 0 as the top horizontal arrow and $d : f \mapsto \mathrm{d}f$ as the bottom horizontal arrow. Then

(a) *The above diagram commutes and the maps σ_i, $i = 0, 1$, are injective.*
(b) *One has $\mathrm{Ker}(d) = \mathrm{Im}(\sigma_0)$ and $\mathrm{Im}(d) \oplus \mathrm{Im}(\sigma_1) = \mathbb{F}_2[\mathbf{x},\mathbf{y}]/(\mathbf{y}^2+\mathbf{y}+\mathbf{x}^3+\mathbf{x}+1)\mathrm{d}\mathbf{x}$.*
(c) *The Cartier operator $C : \mathbb{F}_2[\mathbf{x},\mathbf{y}]/(\mathbf{y}^2+\mathbf{y}+\mathbf{x}^3+\mathbf{x}+1)\mathrm{d}\mathbf{x} \longrightarrow \mathbb{F}_2[\mathbf{x},\mathbf{y}]/(\mathbf{y}^2+\mathbf{y}+\mathbf{x}^3+\mathbf{x}+1)\mathrm{d}\mathbf{x}$ is the composition of the projection of $\mathbb{F}_2[\mathbf{x},\mathbf{y}]/(\mathbf{y}^2+\mathbf{y}+\mathbf{x}^3+\mathbf{x}+1)\mathrm{d}\mathbf{x}$ onto $\mathrm{Im}(\sigma_1)$ with the inverse of σ_1. It is completely characterized by the formulas*

$$C(\mathrm{d}\mathbf{x}) = 0, \quad C(\mathbf{x}\mathrm{d}\mathbf{x}) = \mathrm{d}\mathbf{x}, \quad C(\mathbf{y}\mathrm{d}\mathbf{x}) = (\mathbf{x}+1)\mathrm{d}\mathbf{x}, \quad C(\mathbf{x}\mathbf{y}\mathrm{d}\mathbf{x}) = (\mathbf{y}+1)\mathrm{d}\mathbf{x}, \tag{8}$$

and $C(f^2 g) = f C(g)$ for all $f \in \mathbf{A}$ and $g \in \mathbf{A}\mathrm{d}\mathbf{x}$.
(d) *The induced endomorphism $C \otimes \mathrm{id}$ on $\overline{F}[\mathbf{x},\mathbf{y}]/(\mathbf{y}^2+\mathbf{y}+\mathbf{x}^3+\mathbf{x}+1)\mathrm{d}\mathbf{x}$, which we also denote by C is characterized by (8) and $C(f^2 g) = f^{(1)} C(g)$ for all $f \in \mathbf{A} \otimes \overline{F}$ and $g \in \mathbf{A} \otimes \overline{F}\mathrm{d}\mathbf{x}$.*

3 A cohomological formula for $\zeta_A(n, T)$ at negative integers

Recall from Sect. 1, that for any $n \in \mathbb{Z}$ we defined the power series

$$\zeta_A(n, T) := \sum_{d \geq 0} T^d \sum_{a \in A_{d,+}} a^{-n} \in 1 + TF[[T]].$$

Its definition uses that ∞ is rational over $\mathbb{F}_q$. For $n \in \mathbb{N}_0$ the value $\zeta_A(-n, T)$ lies in $1 + TA[T]$. Its degree in T satisfies a logarithmic bound in n. This is at the basis of the following important result of Goss [12, Thm. 8.9.2], in which $F_\infty[[T]]^{\text{ent}}$ denotes the set of entire power series over F_∞, i.e., power series with coefficients in F_∞ and infinite radius of convergence:

Theorem 3.1 *There exists a (unique) continuous function*

$$L_A(\_) : \mathbb{Z}_p \longrightarrow F_\infty[[T]]^{\text{ent}}$$

such that for all $n \in \mathbb{N}_0$ the power series $L_A(-n)$ is the polynomial

$$L_A(-n) : T \longmapsto \zeta_A(-n, T\pi_\infty^n) = z_A(-n, T).$$

Remark 3.2 The continuity is meant with respect to the usual p-adic topology on $\mathbb{Z}_p$ and the Fréchet topology on $L_\infty[[T]]^{\text{ent}}$, which is defined so that a sequence in $L_\infty[[T]]^{\text{ent}}$ is convergent if it is uniformly convergent with respect to the supremum norms on all bounded subsets of $\mathbb{C}_\infty$, see [4, p. 765ff.].

For T sufficiently small, it is not difficult to see that the power series $z_A(n, T)$ satisfy a uniform convergence condition for all $n \in \mathbb{Z}_p$. The continuity stated in Theorem 3.1, expresses congruence conditions for the coefficients of the special value polynomials $z_A(n, T)$ for $n \in -\mathbb{N}_0$: if $n \equiv m \pmod{p^k}$ for some $k \in \mathbb{N}$, then the coefficient of any monomial T^d in $L(-n) - L(-m)$ is divisible by $\pi_\infty^{p^k}$. The logarithmic growth of the special values $L_A(-n)$ for $n \in \mathbb{N}$, then implies that the interpolated power series are entire for all $n \in \mathbb{Z}_p$ and not just convergent on some bounded disc around zero.interpolated by $\{L_A(-n)\}_{n \in \mathbb{N}_0}$.

Suppose now that A has strict class number one – there are exactly 4 such rings A different from rings of the form $\mathbb{F}_q[t]$, see [15]. For such A there exists exactly one sign-normalized Drinfeld A-module of rank 1. Specializing work of Anderson [2], Böckle and Pink [5] and Böckle [4] (we use the notation as in [4, 1.40, 1.42, 4.1] or [6, Ch. 9, Ch. 10(3)]) to such A, one obtains the following result:

Theorem 3.3 *Let A have strict class number one. Let $n \in \mathbb{N}_0$. Let $\overline{\mathcal{H}}_n$ be a locally free τ-sheaf on X over F whose restriction to* Spec A *is* **nil***-isomorphic to the n-th tensor power of the A-motive corresponding to the sign-normalized Drinfeld A-module of rank* 1. *Let*

$$L(\infty, \overline{\mathcal{H}}_n, T)^{-1} \in 1 + TA[T]$$

be the characteristic polynomial of the restriction of $\overline{\mathcal{H}}_n$ to Spec$(k_\infty \times F)$. *Then we have:*

(a) $\zeta_A(-n, T) = L(\text{Spec } A, \overline{\mathcal{H}}_n, T)$.
(b) $L(X, \overline{\mathcal{H}}_n, T)L(\infty, \overline{\mathcal{H}}_n, T)^{-1} = L(\text{Spec } A, \overline{\mathcal{H}}_n, T)$.
(c) $H^1(X \times \text{Spec } F, \overline{\mathcal{H}}_n)$ *is a free finitely generated F-vector space which carries an action $H^1(\tau)$ induced from the action of τ on $\overline{\mathcal{H}}_n$ via the functoriality of cohomology.*
(d) $L(X, \overline{\mathcal{H}}_n, T) = \det_F(1 - TH^1(\tau) \mid H^1(X \times \text{Spec } F, \overline{\mathcal{H}}_n)) \in 1 + A[T]$.

(e) *Let* $\kappa : (\sigma \times \mathrm{id})_* D(\underline{\overline{\mathcal{H}}}_n) \to D(\underline{\overline{\mathcal{H}}}_n)$ *denote the Cartier dual action on* $D(\underline{\overline{\mathcal{H}}}_n) = \mathcal{H}om(\underline{\overline{\mathcal{H}}}_n, \Omega_{X\times \mathrm{Spec}\, F})$ *induced from* τ. *Then* $\Gamma(X \times \mathrm{Spec}\, F, D(\underline{\overline{\mathcal{H}}}_n))$ *is a free finitely generated* F*-vector space and for the action induced from* κ *on global sections,* $\kappa : \Gamma(X \times \mathrm{Spec}\, F, D(\underline{\overline{\mathcal{H}}}_n)) \to \Gamma(X \times \mathrm{Spec}\, F, D(\underline{\overline{\mathcal{H}}}_n))$, *one has*

$$L(X, \underline{\overline{\mathcal{H}}}_n, T) = \det_F(1 - T\kappa \mid \Gamma(X \times \mathrm{Spec}\, F, D(\underline{\overline{\mathcal{H}}}_n))).$$

Remark 3.4 It suffices to know $\underline{\overline{\mathcal{H}}}_n$ after change of coefficients to $\overline{F}$, i.e. the algebraic closure of F since this does not affect the values of the characteristic polynomials of τ or κ, respectively.

For the following result, we introduce some notation. Namely for $f \in \mathbf{A} \otimes A$ we set $f^{(i)} := (\sigma^i \otimes \mathrm{id})(f)$. This extends to elements in $\mathbf{F} \otimes A$ or sections of $\mathcal{O}_{\mathbf{X}}$ in the obvious way. Now Remark 2.3 together with [4, Proof of Lemma 4.7] yields:

Lemma 3.5 *Let* $A = \mathbb{F}_2[x, y]/(y^2+y+x^3+x+1)$. *Let* $n = \sum_j 2^{i_j}$ *be the base* 2 *expansion of* $n \in \mathbb{N}$, *where the* i_j *form a finite increasing sequence of integers. Then in the previous theorem one can take*

$$\underline{\mathcal{H}}_n = \bigotimes_j \left(\mathcal{O}_{\overline{\mathbf{X}}}(D - 2\infty), s \mapsto f \cdot s\right)^{(i_j)} = \bigotimes_j \left(\mathcal{O}_{\overline{\mathbf{X}}}(D^{(i_j)} - 2\infty), s \mapsto f^{(i_j)} \cdot s\right).$$

For rational function fields, the following result which is similar to but simpler than the above can be found in [6, §10.5, in part. Cor. 10.25].

Lemma 3.6 *Let* $A = \mathbb{F}_q[t]$. *Let* $n = \sum_j a_j q^j$ *be the base* q *expansion of* $n \in \mathbb{N}$ *with* $a_j \in \{0, 1, \ldots, q-1\}$. *Then for*

$$\left(\underline{\mathcal{H}}_n = \mathcal{O}_{\mathbb{P}^1_F}(-d_{\mathbb{F}_q[t]}(n)\,\infty), s(\mathbf{x}) \mapsto \prod_j (t^{q^j} - \mathbf{t})^{a_j} \cdot s(\mathbf{t})\right)$$

one has

$$\zeta_{\mathbb{F}_q[T]}(-n, T) = (1-T)^{\delta_n} \det\left(1 - T\kappa \mid H^0(\mathbb{P}^1_F, D(\underline{\mathcal{H}}_n))\right)$$

where $\delta_n = 1$ *if* $q-1$ *divides* n, *i.e., if* n *is* q*-even, and* $\delta_n = 0$ *if* n *is* q*-odd.*

4 Special values as characteristic polynomials of matrices

In Theorem 3.3 we displayed a cohomological expression for ζ_A at negative integers in terms of an A-motive closely related to tensor powers of the Drinfeld–Hayes module for A. A candidate for such an A-motive was given in Lemma 3.5 which is based on Lemma 2.2. Combining both results, in this section we shall derive for each positive n a matrix whose characteristic polynomials compute $\zeta_A(-n, T)$.

We work over the curve $\overline{\mathbf{X}} = \mathbf{X} \times \mathrm{Spec}\, \overline{F}$. It is an elliptic curve with affine equation $\mathbf{y}^2 + \mathbf{y} = \mathbf{x}^3 + \mathbf{x} + 1$. It contains the points $\Delta = (x, y)$ and $P = (1+x, x+y)$ for x, y in the ring $A = \mathbb{F}_2[x, y]/(y^2 + y + x^3 + x + 1)$. On $\overline{\mathbf{X}}$ we have the line bundle $L = \mathcal{O}_{\overline{\mathbf{X}}}(D - 2\infty)$ and multiplication by $f = \frac{\beta}{\alpha}$ on sections induces an injective homomorphism $L^{(-1)} \xrightarrow{f\cdot} L$ with cokernel $\mathcal{O}_\Delta$. This defines a locally free τ-sheaf on $\overline{\mathbf{X}}$ in the sense of Remark 2.3. We have observed in Lemma 3.5 that for a sequence $\underline{i} = (i_1 < \cdots < i_\ell)$ in $\mathbb{N}$ and $n = \sum_{j=1}^{\ell} 2^{i_j}$ the line bundle $L_{\underline{i}} = L^{(i_1)} \otimes \cdots \otimes L^{(i_\ell)}$ with the induced τ is a τ-sheaf that can be used to compute the special polynomial $\zeta_A(-n, T)$.

The dual $L^\vee = \mathcal{O}_{\overline{\mathbf{X}}}(2\infty - D)$ has degree 1. For a tuple $\underline{i} = (i_1 < \cdots < i_\ell)$ in $\mathbb{N}$ we define

$$L_{\underline{i}}^\vee := D(L_{\underline{i}}) := (L^{(i_1)})^\vee \otimes \cdots \otimes (L^{(i_\ell)})^\vee \otimes \Omega_{\overline{\mathbf{X}}} = \mathcal{O}_{\overline{\mathbf{X}}}(2\ell\infty - D^{(i_1)} - D^{(i_2)} - \cdots - D^{(i_\ell)})\mathrm{d}\mathbf{x}.$$

It has degree ℓ, so that $W_{\underline{i}} := H^0(L_{\underline{i}}^\vee)$ has dimension ℓ over $\overline{F}$. Given a tuple $\underline{i}$, we write P_k for $P^{(i_k)}$ and $\Delta_k := \Delta^{(i_k)}$. We mostly drop $\mathrm{d}\mathbf{x}$ from the notation for sections of $L_{\underline{i}}^\vee$.

Lemma 4.1 *The following sets are bases of $W_{\underline{i}}$:*

(a) $\{s_1, \ldots, s_\ell\}$ *where s_k is the unique section of $L_{\underline{i}}^\vee$ with zeros at $\Delta_1, \ldots, \Delta_{k-1}$, $\Delta_{k+1}, \ldots, \Delta_\ell$ and with value 1 at Δ_k.*

(b) $\{\widetilde{s}_1, \ldots, \widetilde{s}_\ell\}$ *where $\widetilde{s}_k$ is the unique section of $L_{\underline{i}}^\vee$ with zeros at $\Delta_1^{(1)}, \ldots, \Delta_{k-1}^{(1)}$, $\Delta_{k+1}^{(1)}, \ldots, \Delta_k^{(1)}$ and with value 1 at $\Delta_\ell^{(1)}$.*

(c) $\{b_1, \ldots, b_\ell\}$ *where the b_k are defined as follows: Observe first that $1 + x_k + \mathbf{x}$ vanishes on P_k and $-P_k$ and has a double pole at ∞. Consider next the linear form $\ell_{ij} = \mathbf{y} + m_{ij}\mathbf{x} + b_{ij}$. It vanishes on P_i, P_j and $-P_i - P_j$ and has a triple pole at ∞. Writing $P_i = (1 + x_i, x_i + y_i)$ we have*

$$\ell_{1j} = \mathbf{y} + y_1 + x_1 + (\mathbf{x} + x_1 + 1)\left(\frac{y_j + y_1}{x_j + x_1} + 1\right)$$

for $j \geq 2$. Set now $b_1 := \prod_{k=1}^{\ell}(1 + x_k + \mathbf{x})$ and for $2 \leq j \leq \ell$

$$b_j := \prod_{\substack{k=1 \\ k \neq 1, j}}^{\ell} (1 + x_k + \mathbf{x})\ell_{1j}.$$

Proof The proof of (a), (b) being straightforward, we only prove part (c): The function b_1 has a pole of order 2ℓ at ∞, the functions b_k with $k > 1$ of order $2\ell - 1$. They have no other poles. All these functions vanish on the points $P_1, \ldots, P_\ell$ and hence they are global sections of $W_{\underline{i}}$. Let us argue that they form a basis over $\overline{F}$:

For any divisor $\mathcal{D}$ of $\overline{\mathbf{X}}$ of degree ℓ such that $L_{\underline{i}} \ncong \mathcal{O}_{\overline{\mathbf{X}}}(\mathcal{D})$, the theorem of Riemann-Roch combined with the six-term exact sequence for coherent cohomology of a curve yield an isomorphism $W_{\underline{i}} \cong L_{\underline{i}}^\vee/\mathcal{D}L_{\underline{i}}^\vee$ under evaluation. It follows that evaluation for a suitable $\mathcal{D}$ yields the isomorphism

$$\mathrm{eval}\colon W_{\underline{i}} \xrightarrow{\cong} \oplus_{j=2}^{\ell} L_{\underline{i}}^\vee/L_{\underline{i}}^\vee(-[-P_j]) \oplus L_{\underline{i}}^\vee/L_{\underline{i}}^\vee(-\Delta).$$

Denote by $\mathrm{eval}(b_k)$ the row vector of length ℓ in $\overline{F}$ whose last entry is $b_k(\Delta)$ and whose further entries are $b_k(-P_2)$, …, $b_k(-P_\ell)$. Then $\mathrm{eval}(b_1) = (0, \ldots, 0, b_1(\Delta))$, $\mathrm{eval}(b_2) = (b_2(-P_2), 0, \ldots, 0, b_2(\Delta))$, $\mathrm{eval}(b_3) = (0, b_3(-P_3), 0, \ldots, 0, b_3(\Delta))$, …, , $\mathrm{eval}(b_\ell) = (0, \ldots, 0, b_\ell(-P_\ell), b_\ell(\Delta))$. We claim that $b_k(P_k)$ is non-zero for all $k \geq 2$. Then the row vectors $\mathrm{eval}(b_k)$ are linearly independent, because $b_1(\Delta) \neq 0$, and so it follows that the sections $b_1, \ldots, b_n$ form a basis.

To prove the claim recall that b_k vanishes exactly at $\pm P_2, \ldots, \pm P_{k-1}, \pm P_{k+1}, \ldots, \pm P_\ell$ and P_1, P_k, $-P_1 - P_k$. Suppose $b_k(-P_k) = 0$. Since the x-coordinates of $\pm P_k$ and $\pm P_j$ are different for $k \neq j$ – they are $1 + x_k$ and $1 + x_j$ –, it follows that $-P_k \in \{P_k, -P_k - P_1\}$. The former condition is not possible since $\pm P_k$ have the same x-coordinates but different

y-coordinates, namely $1 + x_k + y_k$ and $x_k + y_k$. The latter leads to $0 = -P_1$ which is absurd as well and hence the claim is shown. □

Given any meromorphic function g on $\overline{\mathbf{X}}$ such as $f = \frac{\alpha}{\beta}$, we denote for $n \in \mathbb{Z}$ by $g^{(n)}$ the meromorphic section where the n-th power of the absolute Frobenius automorphism on $\overline{F}$ is applied to the coefficients. The following assertion is clear from the description of the Cartier operator C in [2]; see also [6, § 10.5].

Lemma 4.2 *The homomorphism $\kappa\colon (\sigma \times \mathrm{id})_* L_{\underline{i}}^{\vee} \to L_{\underline{i}}^{\vee}$ is given on sections as*

$$s \mapsto C(f^{(i_1)} f^{(i_2)} \cdot \ldots \cdot f^{(i_\ell)} s)$$

where C is the Cartier operator on $\Omega_{\overline{\mathbf{X}}} = \mathcal{O}_{\overline{\mathbf{X}}} \mathrm{d}\mathbf{x}$ which has $\frac{\mathrm{d}\mathbf{x}}{\mathbf{x}}$ as a fixed point, extends uniquely to the meromorphic differentials on $\overline{\mathbf{X}}$ and satisfies $C(g^2\omega) = g^{(1)} C(\omega)$ for any meromorphic function g and meromorphic differential ω on $\overline{\mathbf{X}}$.

In the following we write f_k instead of $f^{(i_k)}$, so that $\mathbf{div}(f_k) = [\Delta_k] + 2[P_k^{(-1)}] - [P_k] - 2[\infty]$.

Lemma 4.3 *For $j = 1, \ldots, \ell$ let*

$$\alpha_j := \prod_{\substack{k=1 \\ k \neq j}}^{\ell} f_k(\Delta_j) = \prod_{\substack{k=1 \\ k \neq j}}^{\ell} \frac{y_k + y_j + x_j(x_k + x_j)}{1 + x_j + x_k}.$$

Define μ as the diagonal $\ell \times \ell$-matrix with α_j as the entry at (j, j). Then

$$\kappa(s_1, \ldots, s_\ell) = (\widetilde{s}_1, \ldots, \widetilde{s}_\ell)\mu.$$

Proof Using the group law on $\overline{\mathbf{X}}$ we define $R_j := -(P_1 + \cdots + P_\ell + \Delta_1 + \cdots + \Delta_\ell) + \Delta_j$, so that we have $\mathbf{div}(s_j) = [R_j] - [\Delta_j] + \sum_i ([P_i] + [\Delta_i] - 2\infty)$. The divisor of a meromorphic function on the elliptic curve $\overline{\mathbf{X}}$ has degree zero and sums as a set of points on the curve to 0. This proves the first equality in

$$\begin{aligned}
\mathbf{div}(s_j f_1 f_2 \ldots f_\ell) &= \sum_{k=1}^{\ell} ([\Delta_k] + [P_k]) - [\Delta_j] + [R_j] - 2\ell[\infty] \\
&\quad + \sum_{k=1}^{\ell} \left([\Delta_k] + 2\left[P_k^{(-1)}\right] - [P_k] - 2[\infty] \right) \\
&= 2\left(-[\infty] + \sum_{k=1}^{\ell} \left([\Delta_k] + \left[P_k^{(-1)}\right] - 2[\infty] \right) \right) - [\Delta_j] + [R_j] + 2[\infty].
\end{aligned}$$

Let t be a meromorphic section such that

$$\mathbf{div}(t) = -[\infty] + \sum_{k=1}^{\ell} \left([\Delta_k] + \left[P_k^{(-1)}\right] - 2[\infty] \right) + [T]$$

for $T = -\sum_{k=1}^{\ell} (\Delta_k + P_k^{(-1)})$ under the group law of $\overline{\mathbf{X}}$. Define $t_j := s_j f_1 \ldots f_\ell t^{-2}$, so that $\mathbf{div}(t_j) = -2[T] + [R_j] - [\Delta_j] + 2[\infty]$. We claim that Δ_j is different from R_j and from T and that the $P_j^{(-1)}$ are different from T.

First we explain $\Delta_j \neq R_j$. Suppose on the contrary, that the two are equal. From the definition of R_j it follows that $\sum_{i=1}^{\ell} (P_i + \Delta_i) = 0$. Noticing that $P_i + \Delta_i$ under the group

law is equal to $-P_i^{(1)}$, and writing Φ for the Frobenius endomorphism of the elliptic curve, it follows that $-(\sum_{i=1}^{\ell} \Phi^{\iota_i+1})(P) = 0$. This contradicts Lemma 4.4(c) below since all coefficients of $-(\sum_{i=1}^{\ell} \Phi^{\iota_i+1})$ are odd.

Now we explain $T \neq \Delta_j$. The divisor of β is $[\Delta] + 2[P^{(-1)}] - [P] - 2[\infty]$, so that $\Delta + P^{(-1)} = P - P^{(-1)}$ under the group law of E. The formula $\Delta + P + P^{(1)} = 0$ from the previous paragraph yields $\Delta = -P^{(1)} - P$. Therefore using the Frobenius Φ, the equality $T = \Delta_j$ can expressed as $\sum_k (\Phi^{i_k} - \Phi^{i_k-1})P = (-\Phi^{i_j+1} - \Phi^{i_j})P$. Writing this as $f(\Phi)P = 0$ for some $f \in \mathbb{Z}[u^{\pm 1}]$ we see that the lowest non-vanishing coefficient of f is odd. Again this contradicts Lemma 4.4(c). The argument for $P_j^{(-1)} \neq T$ is similar.

The point of introducing t, t_j above is the following simple calculation using the Cartier linearity of κ:

$$\kappa(s_j) = C(s_j f_1 \dots f_\ell) = C(t^2 t_j) = t^{(1)} C(t_j).$$

Now $t^{(1)}$ has simple zeros at all P_j and $\Delta_k^{(1)}$—since the Δ_k are different from T and the P_j. Because of Sublemma 4.5 below, $C(t_j)$ is non-zero and has a simple pole at $\Delta_j^{(1)}$, and the last part of Sublemma 4.5 easily yields $t^{(1)}C(t_j) \in \Gamma(\overline{\mathbf{X}}, L_{\underline{i}}^{\vee})$. Hence $\kappa(s_j) = t^{(1)}C(t_j)$ is a non-zero multiple of $\widetilde{s}_j$ by a constant. To determine this constant we now evaluate $\kappa(s_j)$ at $\Delta_j^{(1)}$ (π_j denotes a uniformizer at Δ_j):

$$\begin{aligned}
\big(t^{(1)}C(t_j)\big)(\Delta_j^{(1)}) &= (t^{(1)})'(\Delta_j^{(1)}) \cdot \mathrm{Res}_{\Delta_j^{(1)}} C(t_j) \\
&\overset{4.5}{=} (t'(\Delta_j))^{(1)} \cdot \mathrm{Res}_{\Delta_j}(t_j) \;=\; (t'(\Delta_j))^2 \cdot \mathrm{Res}_{\Delta_j}(t_j) \\
&= (t/\pi_j)^2(\Delta_j) \cdot (\pi_j^2 t_j')(\Delta_j) \;=\; (t^2 t_j)'(\Delta_j) \\
&= (s_j f_1 \cdot \ldots \cdot f_\ell)'(\Delta_j) \;= (f_1 \cdot \ldots \cdot \widehat{f_j} \cdot \ldots \cdot f_\ell)(\Delta_j) f_j'(\Delta_j)\,;
\end{aligned}$$

the passage from line 1 to line 2 also uses the formula $(t^{(1)})'(\Delta_j^{(1)}) = (t'(\Delta_j))^{(1)}$ which holds since differentiation commutes with the Frobenius on $\overline{F}$. Now, at $\Delta_j = (x_j, y_j)$ an explicit uniformizer is given by $\mathbf{x} - x_j$. Computing the Taylor expansion for $\mathbf{y} - y_j$ of the equation for $\mathbf{E}$ at Δ_j using implicit differentiation, one finds

$$\mathbf{y} - y_j = (1 + x_j)(\mathbf{x} + x_j) + (1 + x_j + x_j^4)(\mathbf{x} + x_j)^2 + O((\mathbf{x} + x_j)^4).$$

Substituting this expression in $f_j = \frac{y_i + \mathbf{y} + \mathbf{x}(x_i + \mathbf{x})}{1 + x_i + \mathbf{x}}$ we deduce $f_j'(\Delta_j) = 1$. This in turn allows us to evaluate $(s_j f_1 \cdot \ldots \cdot \widehat{f_j} \cdot \ldots \cdot f_k) x f_j'$ at Δ_j, yielding α_j as the value, and thus to prove the lemma. □

We now state the two auxiliary results used in the proof of the previous lemma:

Lemma 4.4 *For the Frobenius endomorphism $\Phi \in \mathrm{End}(\mathbf{E})$ and $f = \sum_{i=M}^{N} a_i u^i \in \mathbb{Z}[u^{\pm 1}]$ one has*

(a) *The minimal polynomial of Φ is $u^2 - 2u + 2 \in \mathbb{Z}[u]$; it has roots $1 \pm i$ in $\mathbb{C}$ with $i = \sqrt{-1}$.*
(b) *One has the equivalences: $f(\Phi)P = 0$ in $\mathbf{E}(\overline{F}) \iff f(\Phi) = 0$ in $\mathrm{End}(\mathbf{E}) \iff f(1 - i) = 0$.*
(c) *If a_M is an odd integer, then $f(1 - i)$ is non-zero, and so $f(\Phi)P \in \mathbf{E}(\overline{F})$ is non-zero.*

Proof For (a) recall that the minimal polynomial of the Frobenius endomorphism Φ of an elliptic curve over a finite prime field $\mathbb{F}_p$ is $u^2 - au + p \in \mathbb{Z}[u]$ where the value of this

polynomial at $u = 1$ is the number of $\mathbb{F}_p$-rational points of the curve. In the case at hand we have $\#\mathbf{E}(\mathbb{F}_2) = 1$ and so $a = 2$ and (a) follows immediately.

To see $\Rightarrow$ of the first implication of (b) note that if $f(\Phi)$ is non-zero, then it is an isogeny of $\mathbf{E}$. As such its kernel consists of torsion points only. But the torsion points of $\mathbf{E}$ are defined over $\overline{\mathbb{F}_2}$ while P, having coordinates (x, y), is not. This gives a contradiction. The remaining assertions of (b) are immediate or follow from (a).

For (c) note that by multiplying from the left by a suitable power of Φ, which commutes with $\mathbb{Z}$, we can assume that $M = 0$ so that $f(1-i)$ lies in $\mathbb{Z}[i]$. Now in the latter ring $1-i$ is a generator of the maximal ideal above $(2) \subset \mathbb{Z}$. Reduction modulo $(1-i)$ of $f(1-i)$ yields the non-zero value $a_0 \pmod 2$ and thus that f is non-zero. The remaining claim follows from (b). □

The following result follows from [18, Exer, 4.12ff.] by composing the Cartier endomorphism considered there with the automorphism on $\mathbf{E}_{\overline{F}}$ induced by the inverse of the Frobenius automorphism on the coefficient field $\overline{F}$:

Sublemma 4.5 *Let ω be a meromorphic differential on $\mathbf{E}_{\overline{F}}$ with a simple pole at $P \in \mathbf{E}(\overline{F})$. Then*

(a) *$C(\omega)$ has a simple pole at $P^{(1)}$ and in particular it is non-zero.*
(b) *$Res_{P^{(1)}} C(\omega) = Res_P(\omega)$.*

Moreover if ω is regular at $P \in \mathbf{E}(\overline{F})$, then $C(\omega)$ is regular at $P^{(1)}$.

From Lemma 4.1 we know that the s_j as well as the $\widetilde{s}_j$ form a basis of $W_{\underline{i}}$. Since the α_j are all non-zero the determinant of the matrix μ in Lemma 4.3 is non-zero. It follows that the characteristic polynomial of κ on $W_{\underline{i}}$ has full rank. Since the pointwise L-factor of $L_{\underline{i}}$ at ∞ is equal to $1 + T$, Lemma 3.5 and Theorem 3.3 yield the following result:

Theorem 4.6 *Let $A = \mathbb{F}_2[x, y]/(y^2 + y + x^3 + x + 1)$. Then for $n \in \mathbb{N}$ one has*

$$\deg_T \zeta_A(-n, T) = dig_2(n) + 1.$$

So far we have obtained a matrix representative for τ on $W_{\underline{i}}$ with respect to two different bases. This allows us to deduce that κ is non-singular on $W_{\underline{i}}$. But it does not allow one to compute its characteristic polynomial, and thus the value $\zeta_A(-n, T)$ for $n = \sum_j 2^{i_j}$. To achieve this, we define the base change matrices ν and $\widetilde{\nu}$ in $M_{\ell\times\ell}(\overline{F})$ of the vector space $W_{\underline{i}}$ as follows:

$$(s_1\ s_2\ \ldots\ s_\ell)\nu = (b_1\ b_2\ \ldots\ b_\ell) \qquad (\widetilde{s}_1\ \widetilde{s}_2\ \ldots\ \widetilde{s}_\ell)\widetilde{\nu} = (b_1\ b_2\ \ldots\ b_\ell).$$

We have defined the s_i so that evaluated at the point Δ_j one obtains the Kronecker symbol δ_{ij}, and similarly for the $\widetilde{s}_i$. Thus we find

$$\nu = (b_j(\Delta_i))_{i,j=1,\ldots,\ell} \qquad \widetilde{\nu} = (b_j(\Delta_i^{(1)}))_{i,j=1,\ldots,\ell}.$$

Here i is the row and j is the column index. The explicit expressions for the b_i in Lemma 4.1 allow one to evaluate these:

Lemma 4.7 *The first column of ν has entries*

$$\prod_{k=1}^{\ell}(1 + x_k + x_i)$$

and that of $\widetilde{\nu}$ *has the entries* $\prod_{k=1}^{\ell}(1+x_k+x_i^2)$ *for* $i=1,\ldots,\ell$. *Columns* $j=2,\ldots,\ell$ *of* ν *have entries*

$$\Big(y_i+y_1+x_1+(x_i+x_1+1)\Big(\frac{y_j+y_1}{x_j+x_1}+1\Big)\Big)\prod_{\substack{k=1\\k\neq 1,j}}^{\ell}(1+x_k+x_i),$$

and those of $\widetilde{\nu}$ *have entries* $\Big(y_i^2+y_1+x_1+(x_i^2+x_1+1)\Big(\frac{y_j+y_1}{x_j+x_1}+1\Big)\Big)\prod_{k=1\,k\neq 1,j}^{\ell}(1+x_k+x_i^2)$, *for* $i=1,\ldots,\ell$.

Having defined ν, $\widetilde{\nu}$ and μ, elementary linear algebra now yields:

Lemma 4.8 *With respect to the basis* $(b_1\ldots,b_\ell)$ *of* $W_{\underline{i}}$, *the endomorphism* κ *is given by the matrix*

$$\widetilde{\nu}^{-1}\mu\nu.$$

We do not know how to compute the characteristic polynomial of the matrix $\widetilde{\nu}^{-1}\mu\nu$. However to obtain its Newton polygon, it will be sufficient to compute the ∞-adic valuation of its determinant. This will be the content of the following section.

5 The valuations of $\det(\nu)$, $\det(\widetilde{\nu})$ and $\det(\mu)$

We let the notation be as in the previous section and define the following $\ell\times\ell$-matrices: ρ is the diagonal matrix with entry

$$\prod_{k=1}^{\ell}(1+x_k+x_i)$$

at (i,i) and $\widetilde{\rho}$ the diagonal matrix with entry $\prod_{k=1}^{\ell}(1+x_k+x_i^2)$ at (i,i). Next, ε is the diagonal matrix with entry 1 at $(1,1)$ and $(x_1+x_i)^{-1}$ at (i,i) for all $i\geq 2$; we also define $\widetilde{\varepsilon}:=\varepsilon$. Finally, γ is the matrix with $c_{i1}=1$ in the first column and

$$c_{ij}=\frac{(x_1+x_j)(x_1+y_1+y_i)+(1+x_1+x_i)(x_1+y_1+x_j+y_j)}{(1+x_1+x_i)(1+x_i+x_j)}$$

for $j\geq 2$ and similarly $\widetilde{\gamma}$ is is obtained from γ be replacing all x_i by x_i^2 and y_i by y_i^2. The reason for introducing these matrices is that

$$\nu=\rho\gamma\varepsilon,\qquad \widetilde{\nu}=\widetilde{\rho}\widetilde{\gamma}\widetilde{\varepsilon}. \tag{9}$$

Our aim will be to compute the valuations of the determinants of the above matrices at the place ∞ of F. Since $(x_i,y_i)=(x,y)^{(n_i)}$, we have $v(x_i)=-2\cdot 2^{n_i}$ and $v(y_i)=-3\cdot 2^{n_i}$. We leave the following elementary result as an exercise to the reader:

Lemma 5.1 *The entries* c_{ij} *of* γ *have the following valuations:*

(a) *For* $j=1$ *(column* 1*):* $v(c_{i1})=0$.

(b) *For* $i=1$ *and* $j>1$ *(row* 1*):* $v(c_{1j})=\begin{cases}2^{n_j+1}, & \text{if } n_j=n_1+1\\ -2^{n_j}, & \text{if } n_j>n_1+1\end{cases}$.

(c) *For* $i>1$ *(row* ≥ 2*):* $v(c_{ij})=\begin{cases}2^{n_i}-2\cdot 2^{n_j}, & \text{if } i>j\\ -2\cdot 2^{n_j}, & \text{if } i=j\\ -2^{n_j}, & \text{if } i<j\end{cases}$.

Using the above and the Leibniz formula for the determinant, it is not hard to see that the most negative valuation among all $c_{i\alpha(1)} \cdot \ldots \cdot c_{\ell\alpha(\ell)}$, for α a permutation of $\{1, \ldots, \ell\}$, occurs for $\alpha = \mathrm{id}$ and thus it follows that

$$v(\det(\gamma)) = -2 \cdot (2^{n_2} + \cdots + 2^{n_\ell}).$$

A very simple computation yields $v(\det(\varepsilon)) = -\sum_{i\geq 2} v(x_i) = \sum_{i\geq 2} 2 \cdot 2^{n_i} = -v(\det(\gamma))$. For ρ we find

$$v(\det(\rho)) = \sum_{i,j\geq 1} v(1 + x_i + x_j) = 2 \sum_{1\leq i<j\leq \ell} v(x_j) = 2 \sum_{j=1}^{\ell} (-2)(j-1)2^{n_j}.$$

In light of (9) we have proved:

Corollary 5.2

$$v(\det(\nu)) = (-4) \sum_{j=1}^{\ell} (j-1)2^{n_j}.$$

The same type of analysis also yields $v(\det(\widetilde{\nu}))$. We simply give the relevant intermediate results and again leave the details to the reader:

Lemma 5.3 *The entries $\widetilde{c}_{ij}$ of $\widetilde{\gamma}$ have the following valuations:*

(a) *For $j = 1$ (column 1) : $v(\widetilde{c}_{i1}) = 0$.*

(b) *For $j > 1$:* $v(\widetilde{c}_{ij}) = \begin{cases} -2 \cdot 2^{n_j}, & \text{if } n_j = n_i + 1 \text{ (and thus } j > i) \\ -2^{n_j}, & \text{if } n_j > n_i + 1 \text{ (and thus } j > i) \\ 2(2^{n_i} - 2^{n_j}), & \text{if } i \geq j \end{cases}.$

One computes $v(\det(\widetilde{\gamma}))$ by the same argument as $v(\det(\gamma))$ to

$$v(\det(\widetilde{\gamma})) = \sum_{i\geq 2} -2^{n_i} + \sum_{i\geq 2, n_{i-1}+1=n_i} -2^{n_i},$$

where this time the optimal permutation is the cyclic permutation (1 2 3 ... n) in cycle representation. Note that $\widetilde{\varepsilon} = \varepsilon$, so that $v(\det(\widetilde{\varepsilon})) = \sum_{i\geq 2} 2 \ldots 2_i^n$. Finally one has

$$v(\det(\widetilde{\rho})) = \sum_{i=1}^{\ell} (-4)i2^{n_i} + \sum_{j=2, n_{j-1}<n_j-1}^{\ell} (-2)2^{n_j} + \sum_{j=3}^{\ell} (-2)(j-2)2^{n_j}.$$

Thus

Corollary 5.4

$$v(\det(\widetilde{\nu})) = -2 \cdot 2^{n_1} - \sum_{i=1}^{\ell} (6i-4)2^{n_i} - \sum_{i\geq 2, n_i-1>n_{i-1}} 2^{n_i}.$$

A similar argument shows for μ from Lemma 4.3 that

$$v(\det(\mu)) = -\sum_{j=1}^{k} (3j+1)2^{n_j} + \sum_{k=2, n_k-1=n_{k-1}}^{\ell} 2^{n_k}. \tag{10}$$

From Lemma 4.8 and the above values for the valuations of $\det(\nu)$, $\det(\widetilde{\nu})$ and $\det(\mu)$, we obtain the valuation of $\det(\kappa)$. Since we have $\det(1 - T\kappa) = (1+T)\zeta_A(-n, T)$, we deduce:

Theorem 5.5 *The valuation of the leading term of* $\zeta_A(-n, T)$ *is*

$$v(\det \kappa) = -\sum_{j=2}^{k} j \cdot 2^{n_j}.$$

6 The Newton polygon of $\zeta_A(-n, T)$

Using the congruence properties of the functions $z_A(-n, T)$ and the valuation of its leading term, in this section we shall recursively deduce a formula for the Newton polygon for $z_A(-n, T)$ for all $n \in \mathbb{Z}_p$. This is the main result of the present article.

We take $\pi_\infty := \frac{x}{y} \in F$ as a uniformizer at ∞ and recall that $z_A(-n, T) := \zeta_A(-n, T\pi_\infty^n)$.

Lemma 6.1 *(Goss). The polynomials* $z_A(-n, T)$ *lie in* $\mathcal{O}_\infty[T]$ *for* $n \in \mathbb{N}_0$. *If* $n, n' \in \mathbb{N}$ *satisfy* $n \equiv n' \pmod{2^k}$, *then* $z_A(n, T) \equiv z_A(n', T) \pmod{\pi_\infty^{2^k}}$.

Proof From its definition, we deduce

$$z_A(-n, T) = \prod_{a \in A_{d,+} \text{ irred}} \left(1 - (T\pi_\infty^n)^{\deg a} a^n\right)^{-1} = \prod_{a \in A_{d,+} \text{ irred}} \left(1 - T^{\deg a}(\pi_\infty^{\deg a} a)^n\right)^{-1}.$$

The first thing to note is that $\pi_\infty^{\deg a} a$ lies in $\mathcal{O}_\infty^*$ and hence so does $z_A(-n, T)$. Next observe that $\pi_\infty^{\deg a} a$ must be a 1-unit, since the residue field of $\mathcal{O}_\infty$ is $\mathbb{F}_2$. In particular $(\pi_\infty^{\deg a} a)^{2^k} \equiv 1 \pmod{\pi_\infty^{2^k}}$. Therefore if $n' = n + 2^k m$, then

$$1 - T^{\deg a}(a\pi_\infty^{\deg a})^{n'} = 1 - T^{\deg a}(a\pi_\infty^{\deg a})^n (a\pi_\infty^{\deg a})^{2^k m} \equiv 1 - T^{\deg a}(a\pi_\infty^{\deg a})^n \pmod{\pi_\infty^{2^k}}.$$

The congruence property is immediate. □

For any $n \in \mathbb{N}_0$ with base 2 expansion $n = \sum_{i=1}^{\ell} 2^{n_i}$ for a strictly increasing sequence of $n_i \in \mathbb{N}$, we name the coefficients of $z_A(-n, T))/(1 + T\pi_\infty^n)$ and $\zeta_A(-n, T)/(1 + T)$ by

$$z_A(-n, T)/(1 + T\pi_\infty^n) =: \sum_{i=0}^{\ell} a_{i,n} T^i \qquad \zeta_A(-n, T)/(1 + T) =: \sum_{i=0}^{\ell} \widetilde{a}_{i,n} T^i;$$

note that by Theorem 4.6 the degree in T of both polynomials is equal to ℓ. Note also that $\widetilde{a}_{i,n} = a_{i,n}\pi_\infty^{ni}$. Obviously $z_A(-n, T)/(1 + T\pi_\infty^n)$ satisfies the same congruence condition as $z_A(-n, T)$.

Theorem 6.2 *One has* $a_{0,n} = 1$, $a_{1,n} = \pi_\infty^n$ *and for* $2 \le i \le \ell$:

$$v(a_{i,n}) = 2^{n_{i-1}} + 2 \cdot 2^{n_{i-2}} + 3 \cdot 2^{n_{i-3}} + \ldots + (i-2) \cdot 2^{n_2} + i2^{n_1} = \sum_{j=1}^{i-1} (i-j) 2^{n_j} + 2^{n_1}$$

Proof The constant coefficient of $\zeta_A(-n, T)$ is 1, and the coefficient of T^1 is zero (because $A_{+,1} = \emptyset$). We immediately deduce the formulas $a_{0,n} = 1$, $a_{1,n} = \pi_\infty^n$. Next, from Theorem 5.5 we deduce

$$v(a_{\ell,n}) = v(\det(\kappa)) + \ell \cdot n = \ell \cdot \left(\sum_{j=1}^{\ell} 2^{n_j}\right) - \sum_{j=2}^{\ell} j 2^{n_j} = 2^{n_1} + \sum_{j=1}^{\ell-1} (\ell - j) 2^{n_j}.$$

In particular this completes the proof for $\ell = 1$ and so from now on, we assume $\ell \geq 2$ and proceed by induction on n. Let us first observe that for any $n' = \sum_{i=1}^{\ell'} 2^{n'_i}$ with strictly increasing n'_i and $\ell' \geq 2$ we have

$$v(a_{\ell',n'}) \leq n' - (\ell' - 1)2^{n'_1},$$

as follows from

$$\begin{aligned} v(a_{\ell',n'}) = {} & 2^{n'_{\ell'-1}} + 2^{n'_{\ell'-2}} + \cdots + 2^{n'_1} \\ & + 2^{n'_{\ell'-2}} + \cdots + 2^{n'_1} \\ & \qquad \ddots \\ & \qquad\quad + 2^{n'_1} \\ & \qquad\quad + 2^{n'_1} \\ \leq {} & (2^{n'_{\ell'}} - 2^{n'_1}) + \cdots + (2^{n'_2} - 2^{n'_1}) + (2^{n'_1} - 2^{n'_1}) + 2^{n'_1} \\ \leq {} & 2^{n'_{\ell'}} + \cdots + 2^{n'_1} - 2^{n'_1}(\ell' - 1) \;=\; n' - (\ell' - 1)2^{n'_1}. \end{aligned}$$

Let now $n' = \sum_{j=1}^{\ell'} 2^{n_j}$ for some $1 \leq \ell' < \ell$, so that $v(a_{\ell',n'}) \leq n' - (\ell' - 1)2^{n_1} < n'$. Lemma 6.1 gives

$$z_A(n, T) \equiv z_A(n', T) \pmod{\pi_\infty^{2^{n'_\ell+1}}}.$$

Since $n' < 2^{n'_\ell+1}$, we deduce $v(a_{\ell',n}) = v(a_{\ell',n'}) \overset{\text{ind. hyp.}}{=} 2^{n_1} + \sum_{j=1}^{\ell'-1}(\ell' - j)2^{n_j}$, completing the proof. □

We note the following immediate consequence of the above theorem:

Corollary 6.3 *The slopes of the Newton polygon of $z_A(-n, T)$ are, in increasing order:*

$$2^{n_1}, 2^{n_1}, 2^{n_1} + 2^{n_2}, 2^{n_1} + 2^{n_2} + 2^{n_3}, \ldots, 2^{n_1} + 2^{n_2} + \cdots + 2^{n_{\ell-1}}.$$

In particular, apart from the first slope, all slopes occur with multiplicity 1.

Using the interpolation property of Lemma 6.1, we deduce

Corollary 6.4 *Let n be in $\mathbb{Z}_p$. The slopes of the Newton polygon of $z_A(n, T)$, except for the lowest one, all have width* 1. *In particular, except for those of lowest order, all roots of $z_A(n, T)$ are simple, have pairwise different valuation and lie in $\mathbb{F}_2((\pi_\infty))$.*

7 Two results on $\zeta_{\mathbb{F}_q[t]}(-n, T)$

In this section we prove two results on $\zeta_{\mathbb{F}_q[t]}(-n, T)$: the first result is a closed formula for the leading term of $\zeta_{\mathbb{F}_p[t]}(-n, T)$ for n whose only digits in base p expansion are 0 and $p - 1$. Such a formula was first suggested for $p = 2$ by some computer experiments of the author, then proved and made precise for $p = 2$ and all n by R. Pink and then generalized to arbitrary p by D. Thakur. The method is the same as the one to obtain the main results of the earlier part of the article. We hope that the simplicity of the situation to which we apply these methods will make the proof given in the previous sections more transparent. The second result is the determination of the degree of $\zeta_{\mathbb{F}_q[t]}(-n, T)$ given in Theorem 1.2(a) for arbitrary $n \in \mathbb{N}$ and prime powers q by a careful analysis of the results of Sheats in [17]. For computational results in this direction, see [3]

7.1 A closed formula for the leading term of $\zeta_{\mathbb{F}_p[t]}(-n, T)$ for certain n

Recall from Lemma 3.6 that we have

$$\zeta_{\mathbb{F}_p[T]}(-n, T) = (1-T)^{\delta_n} \det\left(1 - T\kappa \mid H^0(\mathbb{P}^1_F, D(\underline{\mathcal{H}}_n))\right)$$

for

$$\underline{\mathcal{H}}_n = \mathcal{O}_{\mathbb{P}^1_F}(-d_{\mathbb{F}_p[t]}(n)[\infty]), s(\mathbf{t}) \mapsto \prod_j (t^{p^j} - \mathbf{t})^{a_j} \cdot s(\mathbf{t})\big)$$

where $D(\_)$ denotes the dual $\mathcal{H}om_{\mathbb{P}^1_F}(\_, \Omega_{\mathbb{P}^1_F/F})$ and κ the Cartier linear endomorphism on this sheaf. Using $\Omega_{\mathbb{P}^1_F/F} = \mathcal{O}_{\mathbb{P}^1_F}(-2)\mathrm{d}\mathbf{t}$ and the well-known formula for the Cartier operator C on function fields, i.e.,

$$C\left(\mathbf{t}^n \frac{\mathrm{d}\mathbf{t}}{\mathbf{t}}\right) = \mathbf{t}^{n/q} \frac{\mathrm{d}\mathbf{t}}{\mathbf{t}} \tag{11}$$

where $\mathbf{t}^{n/q} = 0$ if q does not divide n, one finds

$$(D(\underline{\mathcal{H}}_n), \kappa) = \left(\mathcal{O}_{\mathbb{P}^1_F}(d_{\mathbb{F}_p[t]}(n)[\infty] - 2), s(\mathbf{t}) \mapsto C\left(\prod_j (t^{p^j} - \mathbf{t})^{a_j} \cdot s(\mathbf{t})\right)\right).$$

It is not hard to see that if we define $(\mathcal{F}_n, \kappa)$ as the pair

$$\left(\mathcal{O}_{\mathbb{P}^1_F}(d_{\mathbb{F}_p[t]}(n)[\infty] - 1), s(\mathbf{t}) \mapsto C\left(\prod_j (t^{p^j} - \mathbf{t})^{a_j} \cdot s(\mathbf{t})\right)\right),$$

then for any q-even n one has

$$\zeta_{\mathbb{F}_p[T]}(-n, T) = \det\left(1 - T\kappa \mid H^0(\mathbb{P}^1_F, \mathcal{F}_n)\right). \tag{12}$$

We will use (12) to obtain a proof of the following leading term formula:

Proposition 7.1 (Pink ([16], $p = 2$), Thakur ([23, Sec. 11], general p)). *For $n = (p-1)\left(p^{k_1} + \cdots + p^{k_\ell}\right)$ with $0 \le k_1 < \cdots < k_\ell$, the degree of $\zeta_{\mathbb{F}_p}(-n, T)$ is ℓ and the leading term is*

$$\prod_{1 \le i < j \le m} \left(t^{p^{k_j}} - t^{p^{k_i}}\right)^{p-1}.$$

Proof In the case at hand we have $d_{\mathbb{F}_p}(n) = \ell$. We consider the following three bases of $W := H^0(\mathbb{P}^1_F, \mathcal{F}_n)$:

(a) $\underline{B}_0 := (1, \mathbf{t}, \ldots, \mathbf{t}^{\ell-1})\mathrm{d}\mathbf{t}$.
(b) $\underline{B}_1 := (b_1, \ldots, b_\ell)\mathrm{d}\mathbf{t}$ for $b_j = \prod_{i=1,\ldots,\ell, i \ne j} (t^{p^{k_i}} - \mathbf{t})$.
(c) $\underline{B}_2 := (\widetilde{b}_1, \ldots, \widetilde{b}_\ell)\mathrm{d}\mathbf{t}$ for $\widetilde{b}_j = \prod_{i=1,\ldots,\ell, i \ne j} (t^{p^{k_i+1}} - \mathbf{t}) = b_j^{(1)}$.

Observe first that $\kappa(b_j \mathrm{d}\mathbf{t}) = \widetilde{b}_j \mathrm{d}\mathbf{t}$ for $j = 1, \ldots, \ell$ (this shows in particular that κ is an automorphism!):

$$\begin{aligned}\kappa(b_j \mathrm{d}\mathbf{t}) &= C\left(\prod_{i=1,\dots,\ell} (t^{p^{k_i}} - \mathbf{t})^{p-1} \cdot \prod_{i=1,\dots,\ell, i\neq j} (t^{p^{k_i}} - \mathbf{t}) \mathrm{d}\mathbf{t}\right) \\ &= C\left((t^{p^{k_j}} - \mathbf{t})^{p-1} \cdot \prod_{i=1,\dots,\ell, i\neq j} (t^{p^{k_i+1}} - \mathbf{t}^p) \mathrm{d}\mathbf{t}\right) \\ &= \prod_{i=1,\dots,\ell, i\neq j} (t^{p^{k_i+1}} - \mathbf{t}) \cdot C\big((t^{p^{k_j}} - \mathbf{t})^{p-1} \mathrm{d}\mathbf{t}\big) \overset{(11)}{=} \widetilde{b}_j \mathrm{d}\mathbf{t}.\end{aligned}$$

Next define the change of bases matrix $\nu \in \mathrm{GL}_n(F)$ from $\underline{B}_1$ to $\underline{B}_0$ by

$$(1, \mathbf{t}, \dots, \mathbf{t}^{\ell-1}) \mathrm{d}\mathbf{t} = (b_1, \dots, b_\ell) \mathrm{d}\mathbf{t} \cdot \nu$$

where the tuples are considered as row vectors. Define analogously $\widetilde{\nu}$ for the change of basis from $\underline{B}_2$ to $\underline{B}_0$. By evaluating the defining relation for ν successively at $\mathbf{t} = t^{p^{k_i}}$, $i = 1, \dots, \ell$, one obtains for the matrix coefficients a_{ij} of ν the conditions:

$$\prod_{j=1,\dots,\ell, i\neq j} (t^{p^{k_j}} - t^{p^{k_i}}) \cdot \text{ row } i \text{ of } \nu = \left(1, t^{p^{k_i}}, \dots, \left(t^{p^{k_i}}\right)^{\ell-1}\right)$$

Using the formula for the van der Monde determinant, it follows that

$$\det(\nu) \prod_{i,j=1,\dots,\ell; i\neq j} (t^{p^{k_j}} - t^{p^{k_i}}) = \prod_{1\leq i<j\leq \ell} (t^{p^{k_j}} - t^{p^{k_i}})$$

and thus $\det(\nu) = \prod_{1\leq i<j\leq \ell} (t^{p^{k_i}} - t^{p^{k_j}})^{-1}$. By the same line of reasoning one finds $\det(\widetilde{\nu}) = \det(\nu)^{(1)}$. Finally using that ν and $\widetilde{\nu}$ are change of bases matrices, for κ we find that κ with respect to the basis $\underline{B}_0$ is represented by $(\widetilde{\nu})^{-1}\nu$. It follows that $\det(\kappa)$ is the expression given in the proposition. □

7.2 The degree of $\zeta_{\mathbb{F}_q[t]}(-n, T)$ for $n \in \mathbb{N}$

Fix $A = \mathbb{F}_q[t]$ with $q = p^e$ for the remainder of this section. We recall some notation from [17]: a *valid composition* of $n \in \mathbb{N}$ of length d is a tuple $\underline{r} = (r_1, \dots, r_d) \in \mathbb{N}^d$ of positive non-zero integers such that

(a) $n = \sum_{i=1}^d r_i$,
(b) when summing $n = \sum_{i=1}^d r_i$ as integers in base p expansion, there are no carry over digits and
(c) for $i = 1, \dots, d-1$ the integer r_i is a positive multiple of $q-1$.

The set of all such compositions is denoted by $V_d(n)$. Note that if $\underline{r}$ is a valid composition, then the same is true for $(r_1, \dots, r_{i-1}, r_i + r_{i+1}, r_{i+2}, \dots, r_d)$ for any $i \in 1, \dots, d-1$.

Recall that $S_A(n, d)$ was defined as the sum $\sum_{a\in A_{+,d}} a^{-n}$. From [17, Thm. 1.4] one deduces:

Theorem 7.2 (Sheats). *$S_A(-n, d) \neq 0$ if and only if either*

(a) *$(q-1)|n$ and $V_d(n) \neq \emptyset$ or*
(b) *$(q-1) \nmid n$ and $V_{d+1}(n) \neq \emptyset$.*

Following Sheats, we define $\Gamma : \mathbb{N}_0 \longrightarrow \mathbb{N}_0^e$ as the function which maps $n \in \mathbb{N}_0$ with base p expansion

$$n = \sum_{i \geq 0} a_i \, p^i,$$

so that $0 \leq a_i \leq p-1$, to the column vector $(u_0, \ldots, u_{e-1})^t$ where

$$u_j = \sum_{i \equiv j \pmod e} a_i. \tag{13}$$

We consider the indices $0, 1, \ldots, e-1$ of $(u_0, \ldots, u_{e-1})$ as elements in $\mathbb{Z}/(e)$. Define as in [17]

$$I_d := \{\Gamma(n) \mid n \in \mathbb{N} \text{ and } V_d(n) \neq 0\}.$$

From [17, Lem. 3.5, and (4.1)] one easily deduces that[1]

$$V_d(n) \neq 0 \Longleftrightarrow \Gamma(n) \in I_d. \tag{14}$$

In particular, the non-vanishing of $V_d(n)$ only depends on $\Gamma(n)$.

We next recall a simple direct characterization of I_d due to Sheats: regard $\mathbb{Z}^e$ as a space of column vectors over $\mathbb{Z}$ and denote by $f_1, \ldots, f_e$ its standard basis. Define R as the $e \times e$-Matrix whose columns are the vectors $f_e, f_1, \ldots, f_{e-1}$, in this order, and set $E := -1_e + R$ where 1_e is the unit for matrix multiplication in $M_{e\times e}(\mathbb{Z})$. A simple computation shows that

$$E^{-1} = \frac{-1}{q-1}(1 + pR + p^2R^2 + \cdots + p^{e-1}R^{e-1}).$$

We restate [17, Prop. 4.3]:

Proposition 7.3

$I_d = \{Ex \in \mathbb{N}_0^e \mid x = (x_1, \ldots, x_e) \in E^{-1}\mathbb{Z}^e \subset \mathbb{Q}^e$ such that $d - 1 < \min\{x_0, \ldots, x_{e-1}\}\}$.

To make the above proposition more explicit, we shall now derive an explicit expression for $E^{-1}\Gamma(n)$: let $(u_0, \ldots, u_{e-1})$ be as in (13). Then

$$\begin{aligned}
E^{-1}\Gamma(n) &= \frac{1}{q-1}\Big(\sum_{i=0}^{e-1} p^i R^i (u_0, \ldots, u_{e-1})^t\Big) \\
&= \frac{1}{q-1}\Big(p^0(u_0, \ldots, u_{e-1})^t + p^1(u_1, u_2, \ldots, u_{e-1}, u_0)^t + \ldots \\
&\quad + p^{e-1}(u_{e-1}, u_0, \ldots, u_{e-2})\Big)^t \\
&= \frac{1}{q-1}\Big(\sum_{i=0}^{e-1} p^i u_i, \sum_{i=0}^{e-1} p^i u_{i-1}, \ldots, \sum_{i=0}^{e-1} p^i u_{i-e+1}\Big)^t \\
&= \frac{1}{q-1}\Big(\mathrm{dig}_q(n), \mathrm{dig}_q(pn), \ldots, \mathrm{dig}_q(p^{e-1}n)\Big)^t.
\end{aligned}$$

[1] For the convenience of the reader we indicate a proof of the non-trivial direction $\Leftarrow$ using the notation from [17]: Suppose $\Gamma(n) = \Gamma(n')$ for some $n' \in \mathbb{N}$ with $V_d(n') \neq \emptyset$. Then n' has a valid composition $(r_1, \ldots, r_d)$. Define B as the matrix with columns $\Gamma(r_i)$, $i = 1, \ldots, d$. From property (ii) of a valid composition one deduces that the columns of B sum to $\Gamma(n') = \Gamma(n)$. Moreover $\Gamma(r_i)$ lies in $\mathcal{J}$ for $i = 1, \ldots, d-1$. Now [17, Lem. 3.5] yields $V_d(n) \supset V_d^B(n) \neq \emptyset$.

And thus we have

$$\min E^{-1}\Gamma(n) = \frac{1}{q-1}\big(\min_{i=0,\dots,e-1} \mathrm{dig}_q(p^i n)\big) \quad \text{and} \quad d_{\mathbb{F}_q[t]}(n) = \lfloor \min E^{-1}\Gamma(n) \rfloor.$$

We note a simple consequence: It is well-known and a simple exercise that $q-1$ divides n if and only if $q-1$ divides $\mathrm{dig}_q(n)$. It follows that

$$(q-1)|n \text{ if and only if } \min E^{-1}\Gamma(n) \text{ is an integer.}$$

Proof of Theorem 1.2(a) We break up the computation of $\deg_T \zeta_{\mathbb{F}_q[t]}(-n, T)$ into two cases:

Case $(q-1) \not| n$: Then $\min E^{-1}\Gamma(n)$ is not an integer and so $d < \min E^{-1}\Gamma(n)$ is equivalent to $d \leq \lfloor \min E^{-1}\Gamma(n) \rfloor$. We deduce

$$\begin{aligned}\deg_T \zeta_{\mathbb{F}_q}(-n, T) &\overset{Thm.\ 7.2}{=} \max\{d \in \mathbb{N}_0 \mid V_{d+1}(n) \neq \emptyset\} \overset{(14)}{=} \max\{d \in \mathbb{N}_0 \mid \Gamma(n) \in I_{d+1}\} \\ &\overset{Prop.\ 7.3}{=} \max\{d \in \mathbb{N}_0 \mid d < \min E^{-1}\Gamma(n)\} = \lfloor \min E^{-1}\Gamma(n) \rfloor = d_{\mathbb{F}_q[t]}(n).\end{aligned}$$

Case $(q-1)|n$: Then $\min E^{-1}\Gamma(n)$ is an integer and now we deduce

$$\begin{aligned}\deg_T \zeta_{\mathbb{F}_q}(-n, T) &\overset{Thm.\ 7.2}{=} \max\{d \in \mathbb{N}_0 \mid V_d(n) \neq \emptyset\} \overset{(14)}{=} \max\{d \in \mathbb{N}_0 \mid \Gamma(n) \in I_d\} \\ &\overset{Prop.\ 7.3}{=} \max\{d \in \mathbb{N}_0 \mid d-1 < \min E^{-1}\Gamma(n)\} = \min E^{-1}\Gamma(n) \\ &= d_{\mathbb{F}_q[t]}(n).\end{aligned}$$

□

8 The field of definition of the roots of $z_A(n, T)$ for some particular A and open questions

The purpose of this section is twofold. First we report on some numerical computations of the author with regards to the Newton polygons of $\zeta_A(-n, T)$ for A different than the ones considered above. These computations display some pattern. But we think it too premature, due to the few computations made, to make any kind of conjecture. Second, for an elliptic and a hyperelliptic A, we determine the fields of definition of the roots of small valuation of $\zeta_A(-n, T)$. For one A we obtain a complete answer, for the other this is done experimentally. We conjecture that the experimentally observed behavior for *small* n holds for all n. If so, this shows that there is now bound on the degree of ramification of the fields of definitions of the roots of $\zeta_A(-n, T)$ over $\mathbb{F}_q((\pi_\infty))$. We think that with some combinatorial effort the conjecture could be proven rigorously. This and the computation of further examples is currently considered by Yujia Qiu, a PhD student of the author. We owe D. Thakur the suggestion to investigate the fields of definition in the second part.

8.1 Experimental study of the break points of Newton plygons

Fix an arbitrary ring A as in Sect. 1, let X be the smooth projective geometrically irreducible curve over $\mathbb{F}_q$ such that $A = \Gamma(X \smallsetminus \{\infty\}, \mathcal{O}_X)$ and consider for any $n \in \mathbb{Z}_p$ the following two sets:

$$\mathrm{NB}_n := \big\{x \in \mathbb{N}_0 \mid x \text{ is not the } x\text{-coordinate of a break point of the Newton polygon of } \zeta_A(-n, T)\big\},$$

$$\mathrm{WP} := \Big\{x \in \mathbb{N} \mid x \text{ is a Weierstrass gap at } \infty, \text{ i.e., } \dim H^0(X, \mathcal{O}_X(x\infty)) = H^0(X, \mathcal{O}_X((x-1)\infty))\Big\}$$

For the rings A listed below, we have experimentally observed the following patterns for all $n \in \mathbb{N}$ between 1 and 100 (note that for all these A we have $q = p$):

(a) For any n we have $\deg_T \zeta_A(-n, T) = d_A(n) \in \mathbb{N}_0 \setminus \mathrm{WP}$ with $d_A(n)$ from from (2)
(b) The number of break points of the Newton polygon of $\zeta_A(-n, T)]$ is $\lfloor \frac{\mathrm{dig_q}(n)}{q-1} \rfloor$.
(c) For any n we have $\mathrm{NB}_n = \mathrm{WP} \cap [0, \deg_T \zeta_A(-n, T)]$.

Besides $\mathbb{F}_q[t]$ and the ring considered in the main part of this paper, the above holds for the following rings A (the class numbers were computed using MAGMA, see [7]):

(i) The elliptic curves $A = \mathbb{F}_2[x, y]/(y^2 + y + x^3)$, $A = \mathbb{F}_3[x, y]/(y^2 - x^3 + x + 1)$, $A = \mathbb{F}_3[x, y]/(y^2 - x^3 - x^2 + x)$, $A = \mathbb{F}_3[x, y]/(y^2 - x^3 - x^2 + 1)$ of genus $g = 1$ with Weierstrass gaps at 1 and class numbers 3, 4, 6 and 3, respectively.
(ii) The hyper-elliptic curves $A = \mathbb{F}_2[x, y]/(y^2 + y + x^5 + x^3 + 1)$ and $A = \mathbb{F}_3[x, y]/(y^2 - x^5 - x^3 - 1)$ of genus $g = 2$ with Weierstrass gaps at 1 and 3 and class numbers 1 and 10, respectively.
(iii) The curve $A = \mathbb{F}_2[x, y]/(y^3 + x^4 + x + 1)$ of genus $g = 3$ with Weierstrass gaps at 1, 2 and 5 and class number 21.
(iv) The curve $A = \mathbb{F}_3[x, y]/(y^3 - y - x^5 + x^3 + 1)$ of genus $g = 4$ with Weierstrass gaps at 1, 2, 4 and 7 and class number 28.

8.2 Experimental study of the field of definition of the roots of ζ_A for one A

We now consider the ring $A' = \mathbb{F}_2[x, y]/(y^2 + y + x^5 + x + 1)$ with $p = q = 2$. This ring A' is the affine coordinate ring of a hyperelliptic curve of genus 2 minus one rational point ∞. Its class number is 1. The ring A' is listed in (ii) in the examples above. In particular, experimentally the break points of any Newton polygon of any $\zeta_{A'}(-n, T)$ occur at $x = 2, 4, 5, 6, 7, 8, 9, \ldots$. Or in other words, the width of the projections of these Newton polygons onto the x-axis seem to be $2, 2, 1, 1, 1, \ldots, 1$ where the number of constant slope segments is $\mathrm{dig}_2(n)$. For the degree we expect

$$\deg_T \zeta_{A'}(-n, T) = \begin{cases} 2, & \text{if } \mathrm{dig}_2(n) = 1 \\ 2 + \mathrm{dig}_2(n), & \text{if } \mathrm{dig}_2(n) \geq 2. \end{cases}$$

By [21] we know that $\zeta_{A'}(-n, T) = (1 + T)^2$ for $\mathrm{dig}_2(n) = 1$ and that $(1 + T)^2$ divides $\zeta_{A'}(-n, T)$ for $\mathrm{dig}_2(n) = 2$. Computations suggest that for $\mathrm{dig}_2(n) = 2$ the polynomial $\zeta_{A'}(-n, T)/(1+T)^2$, which is of degree 2 in T, has either roots in F_∞ or its unique inseparable extension of degree 2.

To describe what was experimentally observed[2] for $\mathrm{dig}_2(n) \geq 3$, write n as

$$n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_\ell}$$

with $i_1 < i_2 < \cdots < i_\ell$ and $\ell = \mathrm{dig}_2(n)$. Then over F_∞ the polynomial splits into 2 quadratic and $\ell - 2$ linear isoclinic polynomials of pairwise different slopes. The experiments also suggest that for $\ell \geq 3$

- at least one of the quadratic factors is irreducible
- both factors are irreducible if and only if $i_2 + 2 \leq i_3$
- the irreducible degree 2 factors are Artin-Schreier polynomials.

[2] We thank Ralph Butenuth for writing MAGMA code that performed the factorization of precomputed special values.

The splitting fields of these Artin-Schreier extensions are ramified extensions of F_∞. The conductor of the more ramified field is

$$1 + 2^{i_3 - i_1} + 2^{i_2 + 1 - i_1}.$$

The conductor of the less ramified field, which exists precisely if $i_2 + 3 \leq i_3$, is

$$1 + 2^{i_3 - i_1 - 1} - 2^{i_2 + 1 - i_1}.$$

In particular, the experimental results suggest that the splitting field of $\zeta_{A'}(-n, T)$ over F_∞ can have arbitrarily large degree, or in other words, that there cannot exist a finite extension of F_∞ which splits $\zeta_{A'}(n, T)$ for all $n \in \mathbb{Z}_p$. We expect that the quadratic factors of small slope for $A' = \mathbb{F}_2[x, y]/(y^2 + y + x^5 + x + 1)$ can be analyzed completely by combinatorial methods. This may however be quite involved.

Remark 8.1 The observations reported in the previous section suggest that for fixed $n \in \mathbb{Z}_p$ the splitting field of the entire power series $T \mapsto z_{A'}(n, T)$ is finite over F_∞ and that the degree is bounded independently of n. This agrees with the expectation of [13, Conj. 4]. However the experimental data also suggests that the conductors of these fields are unbounded, so that the union of all these fields is unbounded. This is strikingly different from the situation in characteristic zero. If K is a finite extension of $\mathbb{Q}_p$, then the subfield of an algebraic closure $\overline{\mathbb{Q}_p}$ generated by all extension of K, whose degree is at most a fixed bound, is a finite extension of K. Thus for a continuous family of entire power series in characteristic zero (say over K), if the splitting field of each member of the family is of a uniformly bounded degree over K, then there is a finite extension of K that contains all roots of all power series. Going back to positive characteristic p, what can be said is the following: If all roots of all $z_A(-n, T)$ are of degree strictly less than p, then there exists a finite extension of F_∞ that contains all of them. If the degrees assume the value p, then this can fail. In particular one has to be careful when comparing the characteristic zero with the characteristic p situation. We owe this remark a question of Kevin Buzzard who considered questions of a similar flavor in characteristic zero, on coefficient fields of modular forms in p-adic families.

We end this section with an explicit result on the splitting fields of the quadratic factors of $\zeta_A(-n, T)$ for A as in Sects. 2–6.

Proposition 8.2 *Let $A = \mathbb{F}_2[x, y]/(y^2 + y + x^3 + x + 1)$. Let $n \in \mathbb{N}$ have base 2 expansion*

$$n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_\ell}$$

with $i_1 < i_2 < \cdots < i_\ell$ and $\ell = dig_2(n)$ and assume that $\ell \geq 2$. Then the splitting field of $\zeta_A(-n, T)$ is F_∞ if $i_3 \geq i_2 + 2$ and it is $F_\infty[\zeta]/(\zeta^2 + \zeta + 1)$ if $i_3 = i_2 + 1$.

Proof We define coefficients $\widetilde{a}_{d,n} \in A$ by $\zeta_A(-n, T) =: \sum_{d=0,\ldots,\ell+1} \widetilde{a}_{d,n} T^d$. The coefficient $\widetilde{a}_{1,n}$ is zero and, by Theorem 1.3, for $d \geq 2$ we have

$$v(\widetilde{a}_{d,n}) = 2^{i_1} + (d-1)2^{i_1} + (d-2)2^{i_2} + \cdots + 2^{i_{d-1}} - dn.$$

By the theory of the Newton polygon we can thus factor

$$\sum_{d=0,\ldots,\ell+1} \widetilde{a}_{d,n} T^d = \Big(1 + b_{1,n} T + b_{2,n} T^2\Big)\Big(\sum_{d=0,\ldots,\ell-1} c_{d,n} T^d\Big)$$

where $v(b_{2,n}) = 2 \cdot 2^{i_1} - 2n$, $v(b_{1,n}) \geq 2^{i_1} - n$, and

$$v(c_{d,n}) = d2^{i_1} + d2^{i_2} + (d-1)2^{i_3} + \cdots + 2^{i_{d+1}} - dn.$$

Recall that $\pi_\infty = x/y$ is a uniformizer at ∞. Substituting in the above product decomposition for T the expression $T \cdot \pi_\infty^{n-2^{i_1}}$, all coefficients will come to lie in $\mathcal{O}_\infty$ and moreover the quadratic factor will have slope zero while all slopes of the other factors will be strictly positive. We set $a'_{d,n} := \widetilde{a}_{d,n}\pi_\infty^{d(n-2^{i_1})}$, $b'_{d,n} := b_{d,n}\pi_\infty^{d(n-2^{i_1})}$ and $c'_{d,n} := c_{d,n}\pi_\infty^{d(n-2^{i_1})}$ and note that $v(b'_{1,n}) \geq 0$, $v(b'_{2,n}) = 0$, $v(c'_{d,n}) = d2^{i_2} + (d-1)2^{i_3} + \ldots + 2^{i_{d+1}} > 0$. For convenience of reference, we write down the composition in this renormalization also:

$$\sum_{d=0,\ldots,\ell+1} a'_{d,n}T^d = \left(1 + b'_{1,n}T + b'_{2,n}T^2\right)\Big(\sum_{d=0,\ldots,\ell-1} c'_{d,n}T^d\Big). \tag{15}$$

Comparing coefficients in the factorization modulo $\pi_\infty^{v(c_{2,n})} = 2 \cdot 2^{i_2} + 2^{i_3}$ shows that

$$b'_{1,n} \equiv c'_{1,n} \pmod{\pi_\infty^{2\cdot 2^{i_2}+2^{i_3}}} \text{ and } b'_{1,n} \cdot b'_{2,n} \equiv a'_{3,n} \pmod{\pi_\infty^{2\cdot 2^{i_2}+2^{i_3}}}.$$

In particular this shows that $v(b'_{1,n}) = v(c'_{1,n}) = 2^{i_2}$, so that the roots of the quadratic factor in the $b'_{d,n}$ satisfy an Artin-Schreier extension. Introducing $S = T\frac{b'_{2,n}}{b'_{1,n}}$ gives the Artin-Schreier equation

$$S^2 + S = \frac{b'_{2,n}}{(b'_{1,n})^2}.$$

To determine the splitting field of the latter Artin-Schreier equation, by Krasner's lemma we may replace the expression $\frac{b'_{2,n}}{(b'_{1,n})^2} \in F_\infty = \mathbb{F}_q((\pi_\infty))$ by the sum of its principal part together with its constant coefficient. Thus it suffices to know the lowest $2^{i_2+1}+1$ coefficients of the Taylor series of $b'_{2,n}$ in π_∞ and, similarly, the lowest $2^{i_2}+1$ coefficients of $b'_{1,n}$. In particular, due to their valuations, it suffices to know both, $b'_{2,n}$ and $b'_{1,n}$ modulo $\pi_\infty^{2^{i_2+1}+1}$ only. From here it is easy to deduce that one only needs to know $a'_{2,n}$ and $a'_{3,n}$ modulo $\pi_\infty^{2^{i_2+1}+1}$ and modulo $\pi_\infty^{2^{i_2+1}+1}$, respectively. Thus modulo $\pi_\infty^{2^{i_2+1}+1}$ the formulae

$$b'_{1,n} = c'_{1,n}, \quad b'_{1,n}b'_{1,n} + b'_{2,n} = a'_{2,n}, \quad b'_{1,n}b'_{2,n} = a'_{3,n}$$

suffice to determine $b'_{2,n}$ and $b'_{1,n}$ to a sufficient precision. From these formulae one readily deduces

$$b'_{1,n} = \frac{a'_{3,n}}{a'_{2,n}}\left(1 + \mathcal{O}\left(\pi_\infty^{2v(b'_{1,n})}\right)\right)$$

In turn it follows that the splitting field of the equation for S, and hence for T, is the same as that of

$$S^2 + S = 1 + \frac{(a'_{2,n})^2}{(a'_{3,n})^3} = 1 + \frac{\widetilde{a}^2_{2,n}}{\widetilde{a}^3_{3,n}}, \tag{16}$$

where the second equality follows from the homogeniety of degree 0 of the expression.

Because of the congruences among the coefficients of the $z_A(n,T)$, it suffices to know $\frac{\widetilde{a}^2_{2,n}}{\widetilde{a}^3_{3,n}}$ only for some n' nearby n. Here 'nearby' depends on the precision needed for $a'_{3,n}$ and $a'_{3,n}$. We have

$$a'_{2,n} \equiv \widetilde{a}_{2,n'} \pmod{\pi_\infty^{2^k-2\cdot 2^{i_1}}} \quad \text{and} \quad a'_{3,n} \equiv \widetilde{a}_{3,n'} \pmod{\pi_\infty^{2^k-3\cdot 2^{i_1}}}$$

if $n \equiv n' \pmod{2^k}$. Our precision needed for $a'_{3,n}$ and $a'_{3,n}$ leads to the conditions

$$2^k - 2 \cdot 2^{i_1} \geq 2^{i_2+1} + 1 \quad \text{and} \quad 2^k - 3 \cdot 2^{i_1} \geq 2^{i_2+1} + 1,$$

i.e., we need $2^k \geq 2^{i_2+1} + 3 \cdot 2^{i_1} + 1$. This means that $k = i_2 + 2$ is sufficient. This leads to two cases:

Case $i_3 \geq i_2 + 2$: Then we may replace n by $n' = 2^{i_1} + 2^{i_2}$ without changing the splitting field of (16). Then $\mathrm{dig}_2(n') = 2$ and $\zeta_A(-n', T)$ has degree 3. To compute this polynomial, observe that $A_{+,1} = \emptyset$, $A_{+,2} = \{x, x+1\}$ and $A_{+,3} = \{y, y+1, y+x, y+x+1\}$ and we find

$$\zeta_A(-n', T) = 1 + (1 + x^{i_1} + x^{i_2})T^2 + (x^{i_1} + x^{i_2})T^3 = (1 + T)(1 + T + (x^{i_1} + x^{i_2})T^2).$$

In this case, Eq. (16) becomes $S^2 + S = x^{i_1} + x^{i_2}$ whose roots

$$\alpha := x^{2^{i_1}} + x^{2^{i_1}+1} + \cdots + x^{2^{i_2}-1} \quad \text{and} \quad \alpha + 1 \quad \text{lie in } F_\infty.$$

Case $i_3 = i_2 + 1$: Then we may replace n by $n' = 2^{i_1} + 2^{i_2} + 2^{i_3}$ without changing the splitting field of (16). We compute $a'_{d,n'}$ for $d = 2, 3$:

$$a'_{2,n'} = 1 + x^{2^{i_1}} + x^{2^{i_2}} + x^{2^{i_3}} + x^{2^{i_1}+2^{i_2}} + x^{2^{i_1}+2^{i_3}} + x^{2^{i_2}+2^{i_3}},$$
$$a'_{3,n'} = 1 + x^{2^{i_1}} + x^{2^{i_2}} + x^{2^{i_3}} + x^{2^{i_1}+2^{i_2}} + x^{2^{i_1}+2^{i_3}} + x^{2^{i_2}+2^{i_3}} + \sum_{\substack{1 \leq j,k \leq 3 \\ j \neq k}} y^{2^{i_j}} x^{2^{i_k}}.$$

The double sum on the right in the expression for $a'_{3,n'}$ is equal to

$$\begin{aligned}
&(y^{2^{i_3}} + y^{2^{i_2}})(x^{2^{i_1}} + x^{2^{i_2}}) + (y^{2^{i_1}} + y^{2^{i_2}})(x^{2^{i_2}} + x^{2^{i_3}}) \\
&= (y^2 + y)^{2^{i_2}}(x^{2^{i_1}} + x^{2^{i_2}}) + ((y^2 + y)^{2^{i_1}} + (y^2 + y)^{2^{i_1+1}} + \cdots \\
&\quad + (y^2 + y)^{2^{i_2}-1})(x^{2^{i_2}} + x^{2^{i_3}}) \\
&= (x^3 + x + 1)^{2^{i_2}}(x^{2^{i_1}} + x^{2^{i_2}}) + ((x^3 + x + 1)^{2^{i_1}} + + \cdots \\
&\quad + (x^3 + x + 1)^{2^{i_2}-1})(x^{2^{i_2}} + x^{2^{i_3}})
\end{aligned}$$

The term of $a'_{2,n'}$ of most negative valuation is $x^{2^{i_2}+2^{i_3}}$. Krasner's lemma requires us to know the coefficients of $x^{2^{i_2}+2^{i_3}-m}$ for $m = 0, \ldots, (2^{i_2} + 2)/2$ – note that $v(x) = -2$. The term of $a'_{3,n'}$ of most negative valuation is $x^{3 \cdot 2^{i_2}+2^{i_2}}$ and this time we need to know the coefficients of $x^{4 \cdot 2^{i_2}-m}$ for $m = 0, \ldots, (2^{i_2+1} + 2)/2 = 2i_2 + 1$. Thus we may approximate $a'_{2,n'}$ by $x^{2^{i_3}}(x^{2^{i_2}} + x^{2^{i_1}} + 1)$ and $a'_{3,n'}$ by $x^{3 \cdot 2^{i_2}}(x^{2^{i_2}} + x^{2^{i_2-1}} + 2^{i_1})$. Again by Krasner's lemma, it suffices to know $\frac{\widetilde{a}^2_{2,n}}{\widetilde{a}^3_{3,n}}$ modulo $\pi_\infty \mathcal{O}_\infty$ and a simple computation, left to the reader shows now that

$$\frac{\widetilde{a}^2_{2,n}}{\widetilde{a}^3_{3,n}} \equiv 1 + x^{2^{i_1}} + x^{2^{i_2}} \equiv 1 + \sum_{m=0}^{i_2-i_1-1} (x^{2^{i_1+m}} + x^{2^{i_1+m+1}}) \pmod{\pi_\infty \mathcal{O}_\infty}.$$

Hence if α is a root of (16), then $\alpha - \sum_{m=0}^{i_2-i_1-1} x^{2^{i_1+m}}$ is a root of $S^2 + S = 1$, and the claim of the proposition is thus proved. □

Acknowledgments I would like to thank Dinesh Thakur for several helpful conversations on the theme of the present article. In particular he suggested the calculations carried out in Sect. 8. For help with these calculations I thank Ralf Butenuth who wrote an efficient MAGMA routine to analyze polynomials over the field F_∞. The article was also influenced by the original proof of Proposition 7.1 by Richard Pink, turning cohomology into explicit formulas for ζ-values. For a careful reading of the manuscript, I thank Yujia Qui. For its hospitality and the inspiring environment during spring of 2010, I thank the CRM Barcelona, where important initial work on this article took place. In this work, the author was supported by the SFB/TR45 and the SPP 1489 of the German Science Foundation DFG.

References

1. Anderson, G.: t-motives. Duke Math. J. **53**, 457–502 (1986)
2. Anderson, G.: An elementary approach to L-functions mod p. J. Number Theory **80**(2), 291–303 (2000)
3. Bautista-Ancona, V., Diaz-Vargas, J.: Index of maximality and Goss zeta function, preprint 2010
4. Böckle, G.: Global L-functions over function fields. Math. Ann. **323**(4), 737–795 (2002)
5. Böckle, G., Pink, R.: Cohomological theory of crystals over function fields. In: Tracts in Mathematics, vol. 5. European Mathematical Society (2009)
6. Böckle, G.: Cohomological theory of crystals over function fields and applications. In: Bars, F., Longhi, I., Trihan, F. (eds.) Arithmetic Geometry in Positive Characteristic. Advanced Courses in Mathematics—CRM Barcelona. Birkhäuser, Basel. http://www.iwr.uni-heidelberg.de/groups/arith-geom/boeckle/Crystals-Barca.pdf. (2013, to appear)
7. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997)
8. Diaz-Vargas, J.: Riemann hypothesis for $\mathbb{F}_q[t]$. J. Number Theory **59**(2), 313–318 (1996)
9. Gardeyn, F.: The structure of analytic τ-sheaves. J. Number Theory **100**(2), 332–362 (2003)
10. Hayes, D.: On the reduction of rank-one Drinfeld modules. Math. Comput. **57**(195), 339–349 (1991)
11. Goss, D.: L-series of t-motives and Drinfeld modules. In: Goss, D., et al. (eds.) The Arithmetic of Function Fields, Proceedings of the Workshop at Ohio State University 1991, pp. 313–402. Walter de Gruyter, Berlin (1992)
12. Goss, D.: Basic Structures of function field arithmetic. In: Ergebnisse, vol. 35. Springer, Berlin etc. (1996)
13. Goss, D.: A Riemann hypothesis for characteristic p L-functions. J. Number Theory **82**(2), 299–322 (2000)
14. Goss, D.: The impact of the infinite primes on the Riemann hypothesis for characteristic p valued L-series. In: Algebra, Arithmetic and Geometry with Applications (West Lafayette, IN, 2000). Springer, Berlin (2004)
15. Leitzel, J.R.C., Madan, M.L., Queen, C.S.: Algebraic function fields with small class number. J. Number Theory **7**, 11–27 (1975)
16. Pink, R.: Private communication
17. Sheats, J.: The Riemann hypothesis for the Goss zeta function for $\mathbb{F}_q[T]$. J. Number Theory **71**(1), 121–157 (1998)
18. Stichtenoth, H.: Algebraic function fields and codes. In: Graduate Texts in Mathematics, vol. 254. Springer, Berlin (2009)
19. Taguchi, Y., Wan, D.: L-functions of φ-sheaves and Drinfeld modules. J. Am. Math. Soc. **9**(3), 755–781 (1996)
20. Thakur, D.: Shtukas and Jacobi sums. Invent. Math. **111**, 557–570 (1993)
21. Thakur, D.: On characteristic p zeta functions. Compositio Math. **99**(3), 231–247 (1995)
22. Thakur, D.: Function Field Arithmetic. World Scientific (2004)
23. Thakur, D.: Valuations of v-adic power sums and zero distribution for Goss' v-adic zeta for $\mathbb{F}_q[t]$, preprint 2011
24. Wan, D.: On the Riemann hypothesis for the characteristic p zeta function. J. Number Theory **58**(1), 196–212 (1996)