DYNAMICS ON ABELIAN VARIETIES IN POSITIVE CHARACTERISTIC

JAKUB BYSZEWSKI AND GUNTHER CORNELISSEN

Abstract. We study periodic points and orbit length distribution for endomorphisms of abelian varieties in characteristic $p > 0$. We study rationality, algebraicity and the natural boundary property for the dynamical zeta function (the latter using a general result on power series proven by Royals and Ward in the appendix), as well as analogues of the prime number theorem, also for tame dynamics, ignoring orbits whose order is divisible by p. The behaviour is governed by whether or not the action on the local p-torsion group scheme is nilpotent.

Contents

Introduction

The study of the orbit structure of a dynamical system starts by considering periodic points, which, as advocated by Smale in [37, Section 1.4] and Artin–Mazur [1], can be approached by considering *dynamical zeta functions*. More precisely, let S denote a set (typically, a topological space, differentiable manifold, or an algebraic variety), let $f\colon S \to S$ be a map on a set S (typically, a homeomorphism, a diffeomorphism, or a regular map), and denote by f_n the number of fixed points of the n-th iterate $f^n = f \circ f \circ \cdots \circ f$ (n times), i.e., the number of *distinct* solutions in S of the equation $f^n(x) = x$. Let us say that f is *confined* if f_n is finite for all n, and use the notation $f \circlearrowright S$ to indicate that f satisfies this assumption. For such f, the basic question is to find patterns in the sequence $(f_n)_{n\geqslant 1}$: Does it grow in some controlled way? Does it satisfy a recurrence relation, so that finitely many f_n suffice to determine all? These questions are recast in terms of the (full) dynamical zeta function, defined as $\zeta_f(z) := \exp(\sum f_n z^n/n)$. Typical questions are:

(Q1) Is ζ_f (generically) a rational function? (Smale [37, Problem 4.5]);
(Q2) Is ζ_f algebraic as soon as it has a nonzero radius of convergence? (Artin and Mazur [1, Question 2 on p. 84]).

2010 *Mathematics Subject Classification.* 37P55, 14K02, 37C30. (11N45, 14G17, 37C25.)

Key words and phrases. Abelian variety, inseparability, fixed points, Artin–Mazur zeta function, recurrence sequence, natural boundary.

We thank Fryderyk Falniowski, Marc Houben, Jakub Konieczny, Dominik Kwietniak, Frans Oort, Zeév Rudnick and Tom Ward for feedback on previous versions, Bartosz Naskręcki and Jeroen Sijsling for pointing us to the LMFDB, Jan-Willem van Ittersum for crucial corrections in Sagemath code, and Damaris Schindler for help with identifying main and error terms in the final section. JB gratefully acknowledges the support of National Science Center, Poland under grant no. 2016/23/D/ST1/01124.

Answers to these questions vary widely depending on the situation considered; we quote some results that provide context for our study. The dynamical zeta function $\zeta_f(z)$ is rational when f is an endomorphism of a real torus ([2, Thm. 1]); f is a rational function of degree $\geqslant 2$ on $\mathbf{P}^1(\mathbf{C})$ (Hinkkanen [24, Thm. 1]); or f is the Frobenius map on a variety X defined over a finite field $\mathbf{F}_q$, so that f_n is the number of $\mathbf{F}_{q^n}$-rational points on X and $\zeta_f(z)$ is the Weil zeta function of X (Dwork [13] and Grothendieck [22, Cor. 5.2]). Our original starting point for this work was Andrew Bridy's automaton-theoretic proof that $\zeta_f(z)$ is transcendental for separable dynamically affine maps on $\mathbf{P}^1(\overline{\mathbf{F}}_p)$, e.g., for the power map $x \mapsto x^m$ where m is coprime to p ([8, Thm. 1], [9, Thm. 1.2 & 1.3]). Finally, we mention that $\zeta_f(z)$ has natural boundary (namely, it does not extend analytically beyond the disk of convergence) for some explicit automorphisms of solenoids, e.g., the map dual to doubling on $\mathbf{Z}[1/6]$ (Bell, Miles, and Ward [5]).

In this paper, we deal with these questions in a rather "rigid" algebraic situation, when $S = A(K)$ is the set of K-points on an abelian variety over an algebraically closed field of characteristic $p > 0$, and $f = \sigma$ is a confined endomorphism $\sigma \in \mathrm{End}(A)$ (reserving the notation f for the general case). It is plain that ζ_σ has nonzero radius of convergence (Proposition 5.2). We provide an *exact dichotomy* for rationality of zeta functions in terms of an arithmetical property of $\sigma \circlearrowright A$. Call σ *very inseparable* if $\sigma^n - 1$ is a separable isogeny for all $n \geqslant 1$. The terminology at first may appear confusing, but notice that the multiplication-by-m map for an integer m is very inseparable precisely when $p|m$, i.e., when it is an inseparable isogeny or zero. For another example, if A is defined over a finite field, the corresponding (inseparable) Frobenius is very inseparable.

Theorem A (= Theorem 4.3 & Theorem 6.3)**.** *Suppose that $\sigma\colon A \to A$ is a confined endomorphism of an abelian variety A over an algebraically closed field K of characteristic $p > 0$. Then σ is very inseparable if and only if it acts nilpotently on the local p-torsion subgroup scheme $A[p]^0$. Furthermore, the following dichotomy holds:*

(i) *If σ is very inseparable, then (σ_n) is linear recurrent, and $\zeta_\sigma(z)$ is rational.*
(ii) *If σ is not very inseparable, then (σ_n) is non-holonomic (cf. Definition 1.1 below), and $\zeta_\sigma(z)$ is transcendental.*

Since the local p-torsion group scheme has trivial group of K-points, in the given characterisation of very inseparability it is essential to use the scheme structure of $A[p]^0$. When A is ordinary—which happens along a Zariski dense subspace in the moduli space of abelian varieties—very inseparable endomorphisms form a proper ideal in the endomorphism ring. Thus, in relation to question (Q1) above, in our case rationality is *not* generic at all.

The proofs proceed as follows: the number σ_n is the quotient of the degree of $\sigma^n - 1$ by its inseparability degree. We use arithmetical properties of the endomorphism ring of A and the action of its elements on the p-divisible subgroup to study the structure of these degrees as a function of n, showing that their ℓ-valuations are of the form "(periodic sequence) $\times$ (periodic power of $|n|_\ell$)" (Propositions 2.3 and 2.7). The emerging picture is that the degree is a very regular function of n essentially controlled by linear algebra/cohomology, but to study the inseparability degree, one needs to use geometry. The crucial tool is a general commutative algebra lemma (Lemma 2.1). We find that for some positive integers q, ϖ,

$$\begin{aligned} &d_n \coloneqq \deg(\sigma^n - 1) = \sum_{i=1}^{r} m_i \lambda_i^n \text{ for some } m_i \in \mathbf{Z} \text{ and distinct } \lambda_i \in \mathbf{C}^*; \text{ and} \\ &\deg_i(\sigma^n - 1) = r_n |n|_p^{s_n} \text{ for } \varpi\text{-periodic sequences } r_n \in \mathbf{Q}^*, s_n \in \mathbf{Z}_{\leqslant 0}\,. \end{aligned} \tag{1}$$

Note in particular that this implies that the *degree zeta function*

$$D_\sigma(z) \coloneqq \exp(\sum d_n z^n/n) = \prod_{i=1}^{r} (1 - \lambda_i z)^{-m_i}$$

(called the "false zeta function" by Smale [37, p. 768]) is rational. In Theorem 3.1, we then prove an adaptation of the Hadamard quotient theorem in which one of the series displays such periodic behaviour, but

the other is merely assumed holonomic. From this, we can already deduce the rationality or transcendence of ζ_σ. In contrast to Bridy's result, we make no reference to the theory of automata.

Example B. We present as a warm up example the case where E is an ordinary elliptic curve over $\mathbf{F}_3$ and let $\sigma = [2]$ be the doubling map and $\tau = [3]$ the tripling map, where everything can be computed explicitly. Although the example lacks some of the features of the general case, we hope this will help the reader to grasp the basic ideas. For this example, some facts follow from general theory in Bridy [9]; and, since $\zeta_\sigma(z)$ equals the dynamical zeta function induced by doubling on the direct product of the circle and the solenoid dual to $\mathbf{Z}[1/6]$ ([5]), some properties could be deduced from the existing literature, which we will not do.

First of all, $\deg(\sigma^n - 1) = (2^n - 1)^2 = 4^n - 2 \cdot 2^n + 1$ and $\deg(\tau^n - 1) = (3^n - 1)^2 = 9^n - 2 \cdot 3^n + 1$. The corresponding degree zeta functions are

$$D_\sigma(z) = \frac{(1-2z)^2}{(1-4z)(1-z)} \text{ and } D_\tau(z) = \frac{(1-3z)^2}{(1-9z)(1-z)}.$$

From the definition, σ is not very inseparable but τ is. In fact, $\tau_n = \deg(3^n - 1)$ and $\zeta_\tau = D_\tau$ but, since we are on an ordinary elliptic curve (where $E[p^m]$ is of order p^m), we find

$$\begin{aligned} &\sigma_n = (2^n - 1)^2 |2^n - 1|_3 = (2^n - 1)^2 r_n^{-1} |n|_3^{-s_n} \\ &\text{with } \varpi = 2; r_{2k} = 3, s_{2k} = -1; r_{2k+1} = 1, s_{2k+1} = 0. \end{aligned}$$

In our first proof of transcendence of $\zeta_\sigma(z)$, we use the fact that σ_{2n} differs from a linear recurrence by a factor $|n|_3$ to argue that it is not holonomic.

Since we are on an ordinary curve, the local 3-torsion group scheme is $E[3]^0 = \mu_3$, which has $\mathrm{End}(E[3]^0) = \mathbf{F}_3$ in which the only nilpotent element is the zero element. Thus, we can detect very inseparability of σ or τ by their image under $\mathrm{End}(E) \to \mathrm{End}(E[3]^0) = \mathbf{F}_3$ being zero, and indeed, $\tau = [3]$ maps to zero, but $\sigma = [2]$ does not. ◊

In some cases, we prove a stronger result. Let Λ denote a dominant root of the linear recurrence (1) satisfied by $\deg(\sigma^n - 1)$, i.e., $\Lambda \in \{\lambda_i\}$ has $|\Lambda| = \max |\lambda_i|$. In Proposition 5.1, we prove some properties of Λ, e.g., that $\Lambda > 1$ is real and $1/\Lambda$ is a pole of ζ_σ.

Theorem C (= Theorem 5.5)**.** *If $\sigma\colon A \to A$ is a confined, not very inseparable endomorphism of an abelian variety A over an algebraically closed field K of characteristic $p > 0$ such that Λ is the unique dominant root, then the dynamical zeta function $\zeta_\sigma(z)$ has a natural boundary along $|z| = 1/\Lambda$.*

This result implies non-holonomicity and hence transcendence for such functions; our proof of Theorem C is independent of that of Theorem A. The existence of a natural boundary follows from the fact that the logarithmic derivative of ζ_σ can be expressed through certain "adelically perturbed" series that satisfy Mahler-type functional equations in the sense of [3], and hence have accumulating poles (proven in the appendix by Royals and Ward). From the theorem we see, in connection with question (Q2) above, that a "generic" ζ_σ is far from algebraic (not even holonomic), despite having a positive radius of convergence.

Example B (continued). The dominant roots are $\Lambda_\sigma = 4$ and $\Lambda_\tau = 9$, which are simple. Since ζ_τ is rational, it extends meromorphically to $\mathbf{C}$. We prove that $\zeta_\sigma(z)$ has a natural boundary at $|z| = 1/4$, as follows. It suffices to prove this for the function $Z(z) = z\zeta_\sigma'(z)/\zeta_\sigma(z) = \sum \sigma_n z^n$, which we can expand as

$$Z(z) = \sum_{2 \nmid n} (2^n - 1)^2 z^n + \frac{1}{3} \sum_{2 | n} |n|_3 (2^n - 1)^2 z^n;$$

if we write $f(t) = \sum |n|_3 t^n$, then

$$Z(z) = \frac{z(1 + 28z^2 + 16z^4)}{(1-16z^2)(1-4z^2)(1-z^2)} + \frac{1}{3}\left(f(16z^2) - 2f(4z^2) + f(z^2)\right).$$

It suffices to prove that $f(t)$ has a natural boundary at $|t| = 1$, and this follows from the fact that f satisfies the functional equation

$$f(z) = \frac{z^2 + z}{1 - z^3} + \frac{1}{3} f(z^3),$$

and hence acquires singularities at the dense set in the unit circle consisting of all third power roots of unity. $\Diamond$

Section 6 constitutes a purely arithmetic geometric study of the notion of very inseparability. We prove that very inseparable isogenies are inseparable and that an isogeny $\sigma\colon E \to E$ of an elliptic curve E is very inseparable if and only if it is inseparable. We give examples where very inseparability is not the same as inseparability even for simple abelian varieties. We study very inseparability using the description of $A[p]^0$ through Dieudonné modules, from which it follows that very inseparable endomorphisms are precisely those of which a power factors through the Frobenius morphism.

Example D. Let E denote an ordinary elliptic curve over a field of characteristic 3 and set $A = E \times E$; then the map $[2] \times [3]$ is inseparable but not very inseparable, since there exist n for which $2^n - 1$ is divisible by 3. In this case, $\mathrm{End}(A[3]^0)$ is the two-by-two matrix algebra over $\mathbf{F}_3$, which contains non-invertible non-nilpotent elements, and under $\mathrm{End}(A) \to \mathrm{End}(A[3]^0) = M_2(\mathbf{F}_3)$, $[2] \times [3]$ is mapped to the matrix $\mathrm{diag}(2, 0)$, which is such an element. $\Diamond$

We then introduce the *tame zeta function* ζ^*_σ, defined as

$$\zeta^*_\sigma(z) \coloneqq \exp\left(\sum_{p \nmid n} \sigma_n \frac{z^n}{n}\right), \tag{2}$$

summing only over n that are not divisible by p. The full zeta function ζ_σ is an infinite product of tame zeta functions of p-power iterates of σ (Proposition 7.2). Thus, one "understands" the full zeta function by understanding those tame zeta functions. Our main result in this direction says that the tame zeta function belongs to a cyclic extension of the field of rational functions:

Theorem E (= Theorem 7.3)**.** *For any (very inseparable or not) $\sigma \circlearrowright A$, a positive integer power of the tame zeta function ζ^*_σ is rational.*

The minimal such integral power $t_\sigma > 0$ seems to be an interesting arithmetical invariant of $\sigma \circlearrowright A$; for example, on an ordinary elliptic curve E, one can choose t_σ to be a p-th power for $\sigma \circlearrowright E$, but for a certain endomorphism of a supersingular elliptic curve, $t_\sigma = p^2(p + 1)$ (cf. Proposition 7.4).

Example B (continued). The tame zeta function for σ is, by direct computation,

$$\begin{aligned}\zeta^*_\sigma(z) &= \exp\left(\frac{1}{3}\sum_{\substack{3\nmid n\\ 2\mid n}} (2^n - 1)^2 \frac{z^n}{n} + \sum_{\substack{3\nmid n\\ 2\nmid n}} (2^n - 1)^2 \frac{z^n}{n}\right) \\ &= \sqrt[9]{\frac{F_2(z)^9 F_{64}(z^6)}{F_8(z^3)^3 F_4(z^2)^3}}, \text{ where } F_a(z) \coloneqq \frac{(1 - az)^2}{(1 - a^2 z)(1 - z)},\end{aligned}$$

and hence $t_\sigma = 9$. Note that even for the very inseparable τ, $\zeta^*_\tau(z) = D_\tau(z)/\sqrt[3]{D_{\tau^3}(z^3)}$ is not rational, and $t_\tau = 3$. $\Diamond$

In Section 8, we investigate functional equations for ζ_σ and ζ^*_σ under $z \mapsto 1/(\deg(\sigma) z)$. For very inseparable σ, there is such a functional equation (which can also be understood cohomologically), but not for ζ_σ having a natural boundary. On the other hand, we show that all tame zeta functions satisfy a functional equation when continued to their Riemann surface (see Theorem 8.3).

In Section 9, we study the distribution of prime orbits for $\sigma \circlearrowright A$. Let P_ℓ denote the number of prime orbits of length ℓ for σ. In case of a unique dominant root, we deduce sharp asymptotics for P_ℓ of the form

$$P_\ell = \frac{\Lambda^\ell}{\ell r_\ell |\ell|_p^{s_\ell}} + O(\Lambda^{\Theta\ell}) \text{ where } \Theta := \max\{\mathsf{Re}(s) : D_\sigma(\Lambda^{-s}) = 0\}. \tag{3}$$

We average further like in the Prime Number Theorem (PNT). Define the *prime orbit counting function* $\pi_\sigma(X)$ and the *tame prime orbit counting function* $\pi_\sigma^*(X)$ by

$$\pi_\sigma(X) := \sum_{\ell \leqslant X} P_\ell \text{ and } \pi_\sigma^*(X) := \sum_{\substack{\ell \leqslant X \\ p \nmid \ell}} P_\ell.$$

Again, whether or not σ is very inseparable is related to the limit behaviour of these functions.

Theorem F (= Theorem 9.5 and Theorem 9.9)**.** *If $\sigma \circlearrowright A$ has a unique dominant root $\Lambda > 1$, then, with ϖ as in* (1) *and for X taking integer values, we have:*

(i) *If σ is very inseparable, $\lim_{X \to +\infty} X\pi_\sigma(X)/\Lambda^X$ exists and equals $\Lambda/(\Lambda - 1)$.*

(ii) *If σ is not very inseparable, then $X\pi_\sigma(X)/\Lambda^X$ is bounded away from zero and infinity, its set of accumulation points is a union of a Cantor set and finitely many points (in particular, it is uncountable), and every accumulation point is a limit along a sequence of integers X for which (X, X) converges in the topological group*

$$\{(a, x) \in \mathbf{Z}/\varpi\,\mathbf{Z} \times \mathbf{Z}_p : a \equiv x \bmod |\varpi|_p^{-1}\}.$$

(iii) *For any $k \in \{0, \ldots, p\varpi - 1\}$, the limit $\lim_{\substack{X \to +\infty \\ X \equiv k \bmod p\varpi}} X\pi_\sigma^*(X)/\Lambda^X =: \rho_k$ exists.*

An expression for ρ_k in terms of arithmetic invariants can be found in Formula (39). We also present an analogue of Mertens' second theorem (Proposition 9.10) on the asymptotics of

$$\mathrm{Mer}(\sigma) := \sum_{\ell \leqslant X} P_\ell/\Lambda^\ell$$

in X. It turns out that, in contrast to the PNT analogue, such type of averaged asymptotics is insensitive to the endomorphism being very inseparable or not.

Example B (continued). Including a subscript for σ or τ in the notation, Möbius inversion relates $P_{\sigma,\ell}$ to the values of σ_ℓ, and hence of λ_i, r_n, s_n; we find for the very inseparable τ that $P_{\tau,\ell} = 9^\ell/\ell + O(3^\ell)$, which we can sum to the analogue of the prime number theorem $\pi_\tau(X) \sim 9/8 \cdot 9^X/X$. The situation is different for the not very inseparable σ, where

$$P_{\sigma,\ell} = \frac{4^\ell}{\ell} \cdot \left\{ \begin{array}{ll} |3\ell|_3 & \text{if } \ell \text{ is even} \\ 1 & \text{if } \ell \text{ is odd} \end{array} \right\} + O(2^\ell), \tag{4}$$

and $\pi_\sigma(X)X/4^X$ has uncountably many limit points in the interval $[1/12, 4/3]$ (following the line of thought set out in [14]).

We find as main term in $\mathrm{Mer}(\tau)$ the X-th harmonic number $\sum_{\ell \leqslant X} 1/\ell$, and, taking into account the constant term from summing error terms in (3), we get $\mathrm{Mer}(\tau) \sim \log X + c$ for some $c \in \mathbf{R}$. On the other hand, a more tedious computation gives $\mathrm{Mer}(\sigma) \sim 5/8 \log X + c'$ for some $c' \in \mathbf{R}$.

Concerning the tame case, Figure 1 shows a graph (computed in SageMath [11]) of the function $\pi_\sigma^*(X)X/4^X$, in which one sees six different accumulation points. The values ρ_k can be computed in closed form as rational numbers by noticing that if we sum Equation (4) only over ℓ not divisible by 3, we can split it into a

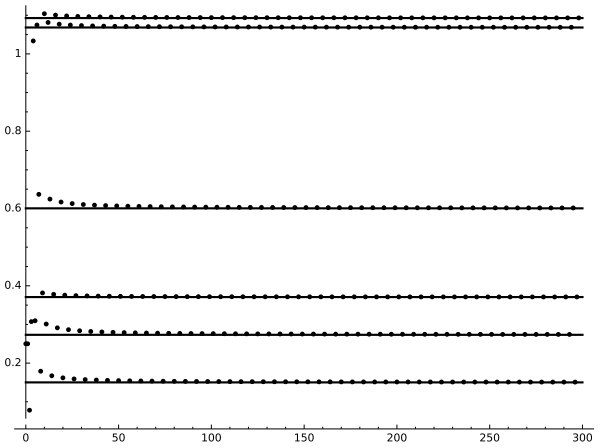

FIGURE 1. Plot of $X \mapsto X\pi^*_\sigma(X)/4^X$, where σ is doubling on an ordinary elliptic curve in characteristic 3 (dots) and the six limit values as computed from Formula (39) (horizontal solid lines)

$k \bmod 6$	$\rho_k \cdot 2^{-2} \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$	ρ_k (numerical)
0	839	0.27317867317867
1	$17 \cdot 193$	1.06829466829467
2	$2^2 \cdot 461$	0.60040700040700
3	461	0.15010175010175
4	$17 \cdot 67$	0.37085877085877
5	$2^2 \cdot 839$	1.09271469271469

TABLE 1. Exact and numerical values of the six limit values in Figure 1

finite sum over different values of ℓ modulo 6. We show the computed values in Table 1, which match the asymptotics in the graph.[1] ♢

We briefly discuss convergence rates in the above theorem (compare, e.g., [33]) in relation to analogues of the Riemann Hypothesis (see Proposition 9.11): there is a function $M(X)$ determined by the combinatorial information $(p, \Lambda, \varpi, (r_n), (s_n))$ associated to $\sigma \circlearrowright A$ as in Equation (1), such that for integer values X, we have

$$\pi_\sigma(X) = M(X) + O(\Lambda^{\Theta X})$$

where the "power saving" Θ is determined by the real part of zeros of the degree zeta function $D_\sigma(\Lambda^{-s})$. Said more colloquially, the main term reflects the growth rate (analogue of entropy) and inseparability, whereas the error term is insensitive to inseparability and determined purely by the action of σ on the total cohomology.

Example B (continued). If we collect the main terms using the function, for $k \in \{0, 1\}$,

$$F_k(\Lambda, X) = \sum_{\substack{\ell \leqslant X \\ \ell \equiv k \bmod 2}} \Lambda^\ell / \ell$$

[1] An amusing observation is the similarity between Figure 1 and the final image in the notorious Fermi–Pasta–Ulam–Tsingou paper (see the very suggestive Figures 4.3 and 4.5 in the modern account [7]): the time averaged fraction of the energy per Fourier mode in the epynomous particle system seems to converge to distinct values, whereas mixing would imply convergence to a unique value; by work of Izrailev–Chirikov the latter seems to happen at higher energy densities. This suggests an analogy (not in any way mathematically precise) between "very inseparable" and "ergodic/mixing/high energy density".

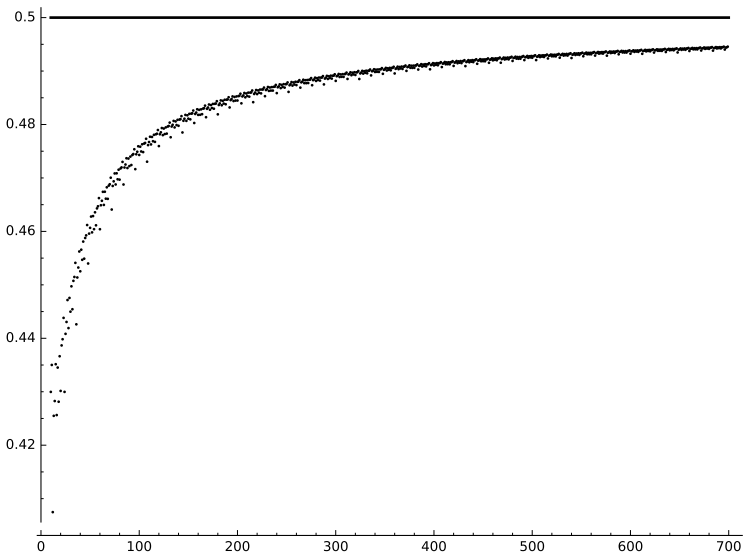

FIGURE 2. Plot of $X \mapsto \log_4 |\pi_\sigma(X) - M(X)| / X$ (dots) for integer $X \in [10, 700]$ and the solid line $\Theta = 1/2$, where σ is doubling on an ordinary elliptic curve in characteristic 3

we arrive at the following analogue of the Riemann Hypothesis for σ:

$$\pi_\sigma(X) = M(X) + O(2^X) \text{ with } M(X) \coloneqq \frac{1}{3}F_0(4, X) + F_1(4, X) - \sum_{i=1}^{\lfloor \log_3(X) \rfloor} \frac{2}{9^i} F_0\left(4^{3^i}, \left\lfloor \frac{X}{3^i} \right\rfloor\right).$$

See Figure 2 (computed in SageMath [11]) for an illustration. ◊

Example G. All our results apply to the situation where A is an abelian variety defined over a finite field $\mathbf{F}_q$ and σ is the Frobenius of $\mathbf{F}_q$, which is very inseparable. This implies known results about curves $C/\mathbf{F}_q$ when applied to the Jacobian $A = \mathrm{Jac}(C)$ of C, such as rationality of the zeta function and analogues of PNT (compare [34, Thm. 5.12]).

We finish this introduction by discussing some open problems and possible future research directions. In the near future, we hope to treat the case of linear algebraic groups, which will require different techniques. Our methods in this paper rest on the presence of a group structure preserved by the map. What happens in absence of a group structure is momentarily unclear to us, but we believe that the study of the tame zeta function in such a more general setup merits consideration. We will consider this for dynamically affine maps on $\mathbf{P}^1$ in the sense of [9] (not equal to, but still "close to" a group) in future work. It would be interesting to study direct relations between our results and that of compact group endomorphisms and S-integer dynamical systems—we briefly touch upon this at the end of Section 5.

1. Generalities

Rationality and holonomicity. We start by recalling some basic facts about recurrence sequences.

Definition 1.1. A power series $f = \sum_{n \geqslant 1} a_n z^n \in \mathbf{C}[\![z]\!]$ is *holonomic* (or *D-finite*) if it satisfies a linear differential equation over $\mathbf{C}(z)$, i.e., if there exist polynomials $q_0, \ldots, q_d \in \mathbf{C}[z]$, not all zero, such that

$$q_0(z)f(z) + q_1(z)f'(z) + \ldots + q_d(z)f^{(d)}(z) = 0. \tag{5}$$

A sequence $(a_n)_{n \geqslant 1}$ is called *holonomic* if its associated generating function $f = \sum_{n \geqslant 1} a_n z^n \in \mathbf{C}[\![z]\!]$ is holonomic.

In the following lemma, we collect some well-known equivalences between properties of a sequence and its generating series:

Lemma 1.2. *Let $(a_n)_{n\geqslant 1}$ be a sequence of complex numbers.*

(i) *The following conditions are equivalent:*
  (a) *The sequence $(a_n)_{n\geqslant 1}$ satisfies a linear recurrence.*
  (b) *The power series $\sum_{n\geqslant 1} a_n z^n$ is in $\mathbf{C}(z)$.*
  (c) *There exist complex numbers λ_i and polynomials $q_i \in \mathbf{C}[z]$, $1 \leqslant i \leqslant s$, such that we have $a_n = \sum_{i=1}^{s} q_i(n)\lambda_i^n$ for n large enough.*

(ii) *The following conditions are equivalent:*
  (a) *The power series $f(z) = \exp\left(\sum_{n\geqslant 1} \frac{a_n}{n} z^n\right)$ is in $\mathbf{C}(z)$.*
  (b) *There exist integers m_i and complex numbers λ_i, $1 \leqslant i \leqslant s$, such that the sequence a_n can be written as $a_n = \sum_{i=1}^{s} m_i \lambda_i^n$ for all $n \geqslant 1$.*

  Furthermore, if all a_n are in $\mathbf{Q}$, then $f(z)$ is in $\mathbf{Q}(z)$.

(iii) *The following conditions are equivalent:*
  (a) *The sequence $(a_n)_{n\geqslant 1}$ is holonomic.*
  (b) *There exist polynomials $q_0, \ldots, q_d \in \mathbf{C}[z]$, not all zero, such that for all $n \geqslant 1$ we have $q_0(n)a_n + \ldots + q_d(n)a_{n+d} = 0$.*

  Furthermore, if a power series $f(z) \in \mathbf{C}[\![z]\!]$ is algebraic over $\mathbf{C}(z)$, then it is holonomic.

Proof. Statement (i) follows from [39, Thm. 4.1.1 & Prop. 4.2.2]. Statement (ii) is [39, Ex. 4.8]; the final claim holds since $\mathbf{C}(z) \cap \mathbf{Q}(\!(z)\!) = \mathbf{Q}(z)$ (see, e.g., [29, Lemma 27.9]). Statement (iii) is [38, Thm. 1.5 & 2.1]. □

Initial reduction from rational maps to confined endomorphisms. Let A denote an abelian variety over an algebraically closed field K. Rational maps on abelian varieties are automatically regular [28, I.3.2], and are always compositions of an endomorphism and a translation [28, I.3.7]. We say that a regular map $\sigma\colon A \to A$ is *confined* if the set of fixed points of σ^n is finite for all n, which we assume from now on. We use the notations from the introduction: σ_n is the number of fixed points of σ^n and ζ_σ is the Artin–Mazur dynamical zeta function of σ.

If σ is an endomorphism of A, confinedness is equivalent to the finiteness of the kernel $\ker(\sigma^n - 1)$ for all n, or the fact that all $\sigma^n - 1$ are isogenies [28, I.7.1]. For arbitrary maps, the following allows us to restrict ourselves to the study of zeta funtions of confined endomorphisms (where case (i) can effectively occur, for example when σ is a translation by a non-torsion point):

Proposition 1.3. *Let $\sigma\colon A \to A$ be a confined regular map and write $\sigma = \tau_b\psi$, where τ_b is a translation by $b \in A(K)$ and ψ is an endomorphism of A. Then either*

(i) *$\sigma_n = 0$ for all n and hence $\zeta_\sigma(z) = 1$; or else*
(ii) *ψ is confined and $\zeta_\sigma(z) = \zeta_\psi(z)$.*

Proof. Iterates of σ are of the form

$$\sigma^n = \tau_{b^{(n)}}\psi^n, \text{ where } b^{(n)} = \sum_{i=0}^{n-1} \psi^i(b).$$

Thus, $\sigma_n = \psi_n$ if $b^{(n)} \in \mathrm{im}(\psi^n - 1)$ and $\sigma_n = 0$ otherwise. If $\sigma_n = 0$ for all n, then $\zeta_\sigma(z) = 1$. Otherwise, for some $m \geqslant 1$ we have $\sigma_m > 0$ and thus $b^{(m)} \in \mathrm{im}(\psi^m - 1)$, $\sigma_m = \psi_m$, and $\psi^m - 1$ is an isogeny. It follows that for all $k \geqslant 1$ we have $b^{(km)} = \sum_{i=0}^{k-1} \psi^{im}(b^{(m)})$ and hence $b^{(km)} \in \mathrm{im}(\psi^{km} - 1)$,

$\sigma_{km} = \psi_{km}$, and $\psi^{km} - 1$ is an isogeny. Since $\psi^k - 1$ is a factor of $\psi^{km} - 1$, we conclude that ψ is a confined endomorphism, and hence $\psi^k - 1$ is surjective. In particular, $b^{(k)} \in \mathrm{im}(\psi^k - 1)$, so $\sigma_n = \psi_n$ for all n, and hence $\zeta_\sigma(z) = \zeta_\psi(z)$. □

We make the following standing assumptions from now on, that we will not repeat in formulations of results. Only in Section 6 shall we temporarily drop the assumption of confinedness, since this will make exposition smoother (this will be clearly indicated).

Standing assumptions. K is an algebraically closed field of characteristic $p > 0$; A is an abelian variety over K of dimension g; $\sigma\colon A \to A$ is a confined endomorphism.

2. Periodic patterns in (in)separability degrees

For now, we will consider ζ_σ as a *formal power series*

$$\zeta_\sigma(z) \coloneqq \exp\left(\sum_{n\geqslant 1} \sigma_n \frac{z^n}{n}\right),$$

and postpone the discussion of complex analytic aspects to Section 5. Let $\deg_{\mathrm{i}}(\tau)$ denote the inseparability degree of an isogeny $\tau \in \mathrm{End}(A)$ (a pure p-th power). We then have the basic equation

$$\sigma_n = \frac{\deg(\sigma^n - 1)}{\deg_{\mathrm{i}}(\sigma^n - 1)}. \tag{6}$$

The strategy is to first consider the "false" (in the terminology of Smale [37]) zeta function with σ_n replaced by the degree of $\sigma^n - 1$. This turns out to be a rational function. We then turn to study the inseparability degree, which is determined by the p-valuations of the other two sequences.

We start with a general lemma in commutative algebra that is our crucial tool for controlling the valuations of certain elements of sequences:

Lemma 2.1. *Let S denote a local ring with maximal ideal $\mathfrak{m}$ and residue field k of characteristic $p > 0$ such that the ring S/pS is artinian. For $\sigma \in S$ and a positive integer n, let $I_n \coloneqq (\sigma^n - 1)S$. Let $\overline{\sigma}$ denote the image of σ in k.*

(i) *If $\sigma \in \mathfrak{m}$, then $I_n = S$ for all n.*
(ii) *If $\sigma \in S^*$, let e be the order of $\overline{\sigma}$ in k^*. Then:*
  (a) *if $e\nmid n$, then $I_n = S$ (this happens in particular if $e = \infty$);*
  (b) *if $e|n$ and $p\nmid m$, then $I_{mn} = I_n$;*
  (c) *there exists an integer n_0 such that for all n with $e|n$ and $\mathrm{ord}_p(n) > n_0$, we have $I_{pn} = pI_n$.*

Proof. Part (i) is clear, so assume $\sigma \in S^*$. If $e\nmid n$, then $\sigma^n - 1$ is invertible in S, since $\overline{\sigma}^n - 1 \neq 0$ in k and hence $I_n = S$.

If $e|n$, we can assume without loss of generality that $e = 1$ (replacing σ by σ^e). Write $\sigma^n = 1 + \varepsilon$ for $\varepsilon \in \mathfrak{m}$. Then for m coprime to p, we immediately find

$$\sigma^{mn} - 1 = \varepsilon u$$

for a unit $u \in S^*$, and hence $I_{mn} = I_n$, which proves (b). On the other hand,

$$\sigma^{pn} - 1 = p\varepsilon v + \varepsilon^p \tag{7}$$

for some unit $v \in S^*$. This shows that $\sigma^{pn} - 1 = \varepsilon(pv + \varepsilon^{p-1}) \subseteq \varepsilon\mathfrak{m}$, which already implies that we get

$$I_{pn} \subseteq I_n\mathfrak{m} \text{ for all } n. \tag{8}$$

Since S/pS is artinian, there exists an integer n_0 such that $\mathfrak{m}^{n_0} \subseteq pS$. By iterating (8) $n_0 + 1$ times, we have

$$I_n \subseteq p\mathfrak{m} \text{ for all } n \text{ with } \mathrm{ord}_p(n) > n_0.$$

Assuming now that $\mathrm{ord}_p(n) > n_0$, we have $\varepsilon \in p\mathfrak{m}$, so $\varepsilon^p \in p\varepsilon\mathfrak{m}$. Hence we conclude from (7) that $\sigma^{pn} - 1 = p\varepsilon w$ for some unit $w \in S^*$, and hence $I_{pn} = pI_n$. □

The degree zeta function. We start by considering the following zeta function with σ_n replaced by the degree of $\sigma^n - 1$.

Definition 2.2. The *degree zeta function* is defined as the formal power series

$$D_\sigma(z) \coloneqq \exp\left(\sum_{n\geqslant 1} \frac{\deg(\sigma^n - 1)}{n} z^n\right).$$

Proposition 2.3.

(i) $D_\sigma(z) \in \mathbf{Q}(z)$.

(ii) *Let ℓ be a prime (which might or might not be equal to p). Then the sequence of ℓ-adic valuations $(|\deg(\sigma^n - 1)|_\ell)_{n\geqslant 1}$ is of the form*

$$|\deg(\sigma^n - 1)|_\ell = r_n \cdot |n|_\ell^{s_n}$$

for some periodic sequences (r_n) and (s_n) with $r_n \in \mathbf{Q}^*$ and $s_n \in \mathbf{N}$. Furthermore, there is an integer ω such that we have

$$r_n = r_{\gcd(n,\omega)} \quad \textit{for } \ell\nmid n.$$

Proof. By [21, Cor. 3.6], the degree of σ and the sequence $\deg(\sigma^n - 1)$ can be computed as

$$\deg\sigma = \prod_{i=1}^{k} \mathrm{Nrd}_{R_i/\mathbf{Q}}(\alpha_i)^{\nu_i}, \quad \deg(\sigma^n - 1) = \prod_{i=1}^{k} \mathrm{Nrd}_{R_i/\mathbf{Q}}(\alpha_i^n - 1)^{\nu_i},$$

where R_i are finite dimensional simple algebras over $\mathbf{Q}$, α_i are elements of R_i, $\mathrm{Nrd}_{R_i/\mathbf{Q}}$ is the reduced norm, and ν_i are positive integers. These formulæ come from replacing the variety A by an isogenous one that is a finite product of simple abelian varieties and applying the well-known results on the structure of endomorphism algebras of simple abelian varieties.

After tensoring with $\overline{\mathbf{Q}}$, the algebras R_i become isomorphic to a finite product of matrix algebras over $\overline{\mathbf{Q}}$. For matrix algebras the notion of reduced norm coincides with the notion of determinant, and since the determinant of a matrix is equal to the product of its eigenvalues, we obtain formulæ of the form

$$\deg(\sigma) = \prod_{i=1}^{q} \xi_i, \quad \deg(\sigma^n - 1) = \prod_{i=1}^{q} (\xi_i^n - 1), \tag{9}$$

with $\xi_i \in \overline{\mathbf{Q}}$ (with possible repetitions to take care of multiplicities) and $q = 2g$ (since $\deg$ is a polynomial function of degree $2g$). Multiplying out the terms in this expression, we finally obtain a formula of the form

$$\deg(\sigma^n - 1) = \sum_{i=1}^{r} m_i \lambda_i^n, \tag{10}$$

for some $m_i \in \mathbf{Z}$ and $\lambda_i \in \overline{\mathbf{Q}}$. Now (i) follows from 1.2.(ii).

In order to prove (ii), we will use Formula (9). Consider a finite extension L of the field of ℓ-adic numbers $\mathbf{Q}_\ell$ obtained by adjoining all ξ_i with $1 \leqslant i \leqslant q$. There is a unique extension of the valuation $|\cdot|_\ell$ to L that we continue to denote by the same symbol. Then we have

$$|\deg(\sigma^n - 1)|_\ell = \prod_{i=1}^{q} |\xi_i^n - 1|_\ell.$$

We now claim that for $\xi \in L$, we have

$$|\xi^n - 1|_\ell = \begin{cases} |\xi|_\ell^n & \text{if } |\xi|_\ell > 1, \\ r_n^\xi |n|_\ell^{s_n^\xi} & \text{if } |\xi|_\ell = 1, \\ 1 & \text{if } |\xi|_\ell < 1, \end{cases} \tag{11}$$

where $(r_n^\xi)_n$ and $(s_n^\xi)_n$ are certain periodic sequences, $r_n^\xi \in \mathbf{R}^*$, $s_n^\xi \in \{0, 1\}$. The first and the last line of the claim are immediate, and the second one follows from applying Lemma 2.1 to the ring of integers $S = \mathscr{O}_L$ with $\sigma = \xi$, as follows: set $a_n = |\xi^n - 1|_\ell^{-1}$ and let e_ξ be the order of ξ in the residue field of S (note that e_ξ is not divisible by ℓ). Then by Lemma 2.1 there exists an integer N such that $a_n = 1$ if $e_\xi \nmid n$; $a_{mn} = a_n$ if $e_\xi | n$ and $\ell \nmid m$; and $a_{\ell n} = \ell a_n$ if $e_\xi | n$ and $\operatorname{ord}_\ell(n) \geqslant N$. Therefore, it suffices to set $(r_n^\xi, s_n^\xi) = (1, 0)$ for $e_\xi \nmid n$; $(r_n^\xi, s_n^\xi) = (a_{e_\xi l^\nu}^{-1}, 0)$ for $e_\xi | n$ and $\nu := \operatorname{ord}_\ell(n) < N$; and $(r_n^\xi, s_n^\xi) = (a_{e_\xi \ell^N}^{-1} \ell^N, 1)$ for $e_\xi | n$ and $\operatorname{ord}_\ell(n) \geqslant N$. Note that for $\ell \nmid n$ we have

$$r_n^\xi = \begin{cases} 1 & \text{if } e_\xi \nmid n, \\ a_{e_\xi}^{-1} & \text{if } e_\xi | n. \end{cases}$$

Multiplying together formulæ (11) for $\xi = \xi_1, \dots, \xi_q$, we obtain

$$|\deg(\sigma^n - 1)|_\ell = \rho^n r_n |n|_\ell^{s_n},$$

where

$$\rho = \prod_{i=1}^q \max(|\xi_i|_\ell, 1) \geqslant 1$$

and (r_n) and (s_n) are periodic sequences, $r_n \in \mathbf{R}^*$, $s_n \in \mathbf{N}$. We claim that $\rho = 1$ (that is, there is no i such that $|\xi_i|_\ell > 1$). Indeed, we know that $\deg(\sigma^n - 1)$ is an integer, and hence $\rho^n r_n |n|_\ell^{s_n} \leqslant 1$ for all n. Thus, taking $n \to \infty$, $\ell \nmid n$, we get $\rho = 1$ and $r_n \in \mathbf{Q}^*$. This finishes the proof of the formula for $|\deg(\sigma^n - 1)|_\ell$. Furthermore, we have

$$r_n = \prod_{e_{\xi_i} | n} a_{e_{\xi_i}}^{-1} \quad \text{for } \ell \nmid n,$$

and hence the final formula holds with $\omega = \operatorname{lcm}(e_{\xi_1}, \dots, e_{\xi_q})$. □

Remark 2.4. We present an alternative, cohomological description of the degree zeta function $D_\sigma(z)$. Fix a prime $\ell \neq p$ and let $\mathrm{H}^i := \mathrm{H}^i_{\text{ét}}(A, \mathbf{Q}_\ell) = \bigwedge^i (V_\ell A)^\vee$ denote the i-th ℓ-adic cohomology group of A, ($V_\ell A = T_\ell A \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$, $T_\ell A$ is the Tate module and $^\vee$ denotes the dual); then

$$D_\sigma(z) = \prod_{i=1}^{2g} \det(1 - \sigma^* z | \mathrm{H}^i)^{(-1)^{i+1}}. \tag{12}$$

This follows in the same way as for the Weil zeta function: let $\Gamma_{\sigma^n} \subseteq A \times A$ denote the graph of σ^n and $\Delta \subseteq A \times A$ is the diagonal [29, 25.6]. The Lefschetz fixed point theorem [29, 25.1] implies that

$$(\Gamma_{\sigma^n} \cdot \Delta) = \sum_{i=0}^{2g} (-1)^i \operatorname{tr}(\sigma^n | \mathrm{H}^i).$$

Now Γ_{σ^n} intersects Δ precisely along the (finite flat) group torsion group scheme $A[\sigma^n - 1]$, and hence the intersection number $(\Gamma_{\sigma^n} \cdot \Delta)$ is the order of this group scheme, which is $\deg(\sigma^n - 1)$. Then the standard determinant-trace identity [29, 27.5] implies the result (12).

The characteristic polynomial of σ_* acting on H^1 has integer coefficients independent of the choice of ℓ and its set of roots is precisely the set of algebraic numbers ξ_i from the proof of Proposition 2.3 (with multiplicities), see, e.g., [30, IV.19, Thm. 3 & 4].

Example 2.5. Suppose A is an abelian variety over a finite field $\mathbf{F}_q$ and σ is the q-Frobenius. Then $\sigma^n - 1$ is separable for all n, so $\sigma_n = \deg(\sigma^n - 1)$ for all n, and $\zeta_\sigma(z) = D_\sigma(z)$ is exactly the Weil zeta function of $A/\mathbf{F}_q$. Thus, we recover the rationality of that function for abelian varieties; note that this is an "easy" case: by cutting A with suitable hyperplanes, we are reduced to the case of (Jacobians of) curves, hence essentially to the Riemann–Roch theorem for global function fields proven by F.K. Schmidt in 1927.

The inseparability degree. Similarly to Proposition 2.3, we can control the regularity in the sequence of inseparability degrees, with some more (geometric) work; this is relevant in the light of Formula (6). We start with a decomposition lemma in commutative algebra:

Lemma 2.6. *Let R be a (commutative) ring and let M be an R-module such that for every $m \in M$ the ring $R/\mathrm{ann}(m)$ is artinian. Let $\mathfrak{m}$ be a maximal ideal of R. Then the localisation $M_\mathfrak{m}$ is equal to*

$$M_\mathfrak{m} = M[\mathfrak{m}^\infty] \coloneqq \{m \in M : \mathfrak{m}^k m = 0 \text{ for some } k \geqslant 1\}$$

and

$$M = \bigoplus_\mathfrak{m} M_\mathfrak{m},$$

the direct sum being taken over all maximal ideals $\mathfrak{m}$ of R.

Proof. Assume first that the module M is finitely generated, say, with generators $m_1, \ldots, m_s$. Set $I = \mathrm{ann}(M)$. Then M is of finite length as a surjective image of the module $\bigoplus_{i=1}^s R/\mathrm{ann}(m_i)$ and hence the ring R/I is artinian, since it can be regarded as a submodule of M^s via the embedding $r \mapsto (rm_1, \ldots, rm_s)$. Therefore, the ideal I is contained in only finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ of R, and for the remaining maximal ideals $\mathfrak{m}$ of R we have $M_\mathfrak{m} = 0$. The artinian ring R/I decomposes as the product

$$R/I \simeq \prod_{i=1}^s R_{\mathfrak{m}_i}/IR_{\mathfrak{m}_i}. \tag{13}$$

Since $I = \mathrm{ann}(M)$, we have $M \otimes_R R/I \simeq M$ and $M \otimes_R R_{\mathfrak{m}_i}/IR_{\mathfrak{m}_i} \simeq M_{\mathfrak{m}_i}$. Thus, tensoring (13) with M, we obtain an isomorphism

$$M \to M_{\mathfrak{m}_1} \oplus \ldots \oplus M_{\mathfrak{m}_s}.$$

Since the modules $M_{\mathfrak{m}_i}$ are also of finite length, we see that each $M_{\mathfrak{m}_i}$ is annihilated by some power of the maximal ideal $\mathfrak{m}_i$.

We now turn to the case of an arbitrary module M. Consider the canonical map

$$\Phi\colon M \to \prod_\mathfrak{m} M_\mathfrak{m},$$

the product being taken over all maximal ideals $\mathfrak{m}$ of R. Restricting Φ to finitely generated submodules $N \subseteq M$, and using the (already established) claim for finitely generated modules, we conclude that the image of Φ is in fact contained in $\bigoplus_\mathfrak{m} M_\mathfrak{m}$ and that the induced map

$$\Phi\colon M \to \bigoplus_\mathfrak{m} M_\mathfrak{m}$$

(that we continue to denote by the same letter) is an isomorphism. For a maximal ideal $\mathfrak{n}$ of R, multiplication by elements outside of $\mathfrak{n}$ is bijective on $M_\mathfrak{n}$. Therefore, restricting Φ to $M[\mathfrak{m}^\infty]$ shows that $M[\mathfrak{m}^\infty] = M_\mathfrak{m}[\mathfrak{m}^\infty]$. Finally, we conclude from the case of finitely generated modules that every element in $M_\mathfrak{m}$ is anihilated by some power of the maximal ideal $\mathfrak{m}$. Thus, $M[\mathfrak{m}^\infty] = M_\mathfrak{m}$. □

Proposition 2.7. *The inseparability degree of $\sigma^n - 1$ satisfies*

$$\deg_{\mathrm{i}}(\sigma^n - 1) = r_n \cdot |n|_p^{s_n} \tag{14}$$

for periodic sequences (r_n) and (s_n) with $r_n \in \mathbf{Q}^*$ and $s_n \in \mathbf{Z}$, $s_n \leqslant 0$. Furthermore, there is an integer ω such that we have

$$r_n = r_{\gcd(n,\omega)} \quad \textit{for } p\nmid n.$$

Proof. The strategy of the proof is as follows: since $\deg_{\mathrm{i}}(\sigma^n - 1)$ is a power of p, it is sufficient to compute $|\deg(\sigma^n - 1)|_p$ and $|\sigma_n|_p$. The former number has been already computed in Proposition 2.3.(ii); for the latter, we study the p-primary torsion of A as an R-module, where, not to have to worry about noncommutative arithmetic, we work with the ring $R = \mathbf{Z}[\sigma] \subseteq \mathrm{End}(A)$. Note that R need not be a Dedekind domain. Let $X \coloneqq A(K)_{\mathrm{tor}}$ denote the subgroup of torsion points of $A(K)$. It has a natural structure of an R-module, and as an abelian group is divisible; in fact,

$$X \simeq \left(\mathbf{Z}\left[\frac{1}{p^\infty}\right]/\mathbf{Z}\right)^f \oplus \bigoplus_{q\neq p}\left(\mathbf{Z}\left[\frac{1}{q^\infty}\right]/\mathbf{Z}\right)^{2g},$$

where f is the p-rank of A, and

$$\mathbf{Z}\left[\frac{1}{q^\infty}\right] = \bigcup_{k\geqslant 1}\mathbf{Z}\left[\frac{1}{q^k}\right].$$

As R acts on X, the localisation $R_{\mathfrak{m}}$ acts on $X_{\mathfrak{m}}$ for each maximal ideal $\mathfrak{m}$ of R. Since X is torsion as an abelian group, the conditions of Lemma 2.6 are satisfied, and hence we have $X_{\mathfrak{m}} = X[\mathfrak{m}^\infty]$ and

$$X = \bigoplus_{\mathfrak{m}} X_{\mathfrak{m}},$$

the sum being taken over all maximal ideals $\mathfrak{m}$ of R. For an element $\tau \in R$, we have

$$X[\tau] = \bigoplus_{\mathfrak{m}} X_{\mathfrak{m}}[\tau].$$

Since $X_{\mathfrak{m}} = X[\mathfrak{m}^\infty]$, for any prime number q we have $X_{\mathfrak{m}}[q^\infty] = 0$ if $q \notin \mathfrak{m}$ and $X_{\mathfrak{m}}[q^\infty] = X_{\mathfrak{m}}$ if $q \in \mathfrak{m}$, and hence we get

$$X[q^\infty] = \bigoplus_{q\in\mathfrak{m}} X_{\mathfrak{m}}.$$

Thus the groups $X_{\mathfrak{m}}$ for $q \in \mathfrak{m}$ are q-power torsion. It follows that for $\tau \in R$, $\tau \neq 0$, we can compute

$$|X[\tau]|_q = \prod_{q\in\mathfrak{m}} |X_{\mathfrak{m}}[\tau]|_q. \tag{15}$$

Since X is a divisible abelian group, the groups $X_{\mathfrak{m}}$, being quotients of X, are also divisible. Thus, the surjectivity of $p\colon X_{\mathfrak{m}} \to X_{\mathfrak{m}}$ implies that there is a short exact sequence

$$0 \longrightarrow X_{\mathfrak{m}}[p] \longrightarrow X_{\mathfrak{m}}[p\tau] \xrightarrow{\ p\ } X_{\mathfrak{m}}[\tau] \longrightarrow 0. \tag{16}$$

Let σ be an element of R, let $e_{\mathfrak{m}}$ denote the order of $\overline{\sigma}$ in $(R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}})^*$ for maximal ideals $\mathfrak{m}$ of R with $p \in \mathfrak{m}$ and $\sigma \notin \mathfrak{m}$. Note that $e_{\mathfrak{m}}$ is then coprime with p. Applying (16) to $\tau = \sigma^n - 1$ and using Lemma 2.1, we get

$$|X_{\mathfrak{m}}[\sigma^{mn} - 1]|_p = \begin{cases} 1 & \text{for } \sigma \in \mathfrak{m}, \\ 1 & \text{for } \sigma \notin \mathfrak{m} \text{ and } e_{\mathfrak{m}}\nmid mn, \\ |X_{\mathfrak{m}}[\sigma^n - 1]|_p & \text{for } \sigma \notin \mathfrak{m},\ p\nmid m \text{ and } e_{\mathfrak{m}}\mid n, \\ |X_{\mathfrak{m}}[\sigma^n - 1]|_p \cdot |X_{\mathfrak{m}}[p]|_p & \text{for } \sigma \notin \mathfrak{m},\ m = p,\ e_{\mathfrak{m}}\mid n, \text{ and } \mathrm{ord}_p(n) \gg 0. \end{cases}$$

Arguing in the same way as in the proof of Proposition 2.3, we conclude that there exist periodic sequences $(r_n^{\mathfrak{m}})_n$ and $(s_n^{\mathfrak{m}})_n$ with $r_n^{\mathfrak{m}} \in \mathbf{Q}^*$ and $s_n^{\mathfrak{m}} \in \mathbf{N}$ such that

$$|X_{\mathfrak{m}}[\sigma^n - 1]|_p = r_n^{\mathfrak{m}}|n|_p^{s_n^{\mathfrak{m}}} \quad \text{for } n \geqslant 1. \tag{17}$$

Furthermore, $r_n^{\mathfrak{m}} = 1$ and $s_n^{\mathfrak{m}} = 0$ for all n if $\sigma \in \mathfrak{m}$, and

$$r_n^{\mathfrak{m}} = r_{\gcd(n,e_{\mathfrak{m}})}^{\mathfrak{m}} \quad \text{for } \sigma \notin \mathfrak{m} \text{ and } p \nmid n.$$

Applying (15) to $\tau = \sigma^n - 1$ and $q = p$, we get the equality

$$|\sigma_n|_p = \prod_{p \in \mathfrak{m}} |X_{\mathfrak{m}}[\sigma^n - 1]|_p.$$

Taking the product of the Formulæ (17) over all maximal ideals $\mathfrak{m}$ of R with $p \in \mathfrak{m}$, we obtain periodic sequences $(r'_n)_n$ and $(s'_n)_n$ with $r'_n \in \mathbf{Q}^*$ and $s'_n \in \mathbf{N}$ such that

$$|\sigma_n|_p = r'_n |n|_p^{s'_n}$$

and

$$r'_n = r'_{\gcd(n,\omega')} \quad \text{for } p \nmid n,$$

where

$$\omega' = \operatorname{lcm}\{e_{\mathfrak{m}} \mid \sigma \notin \mathfrak{m}\}.$$

Writing

$$\deg_{\mathrm{i}}(\sigma^n - 1) = \frac{\deg(\sigma^n - 1)}{\sigma_n} = \frac{|\sigma_n|_p}{|\deg(\sigma^n - 1)|_p}$$

and using Proposition 2.3.(ii), we get sequences (r_n) and (s_n) satisfying having all stated properties except that it might be that $s_n > 0$ for some n. However, since $\deg_{\mathrm{i}}(\sigma^n - 1)$ is an integer, letting ϖ be the common period of (r_n) and (s_n), we automatically get $s_n \leqslant 0$ for all n such that the arithmetic sequence $n + \varpi\,\mathbf{N}$ contains terms divisible by arbitrarily high powers of p. For all the remaining n we have $\operatorname{ord}_p(n) < \operatorname{ord}_p(\varpi)$, and thus whenever $s_n > 0$, we replace s_n by 0 and r_n by $r_n |n|_p^{s_n}$, obtaining the claim. □

3. A holonomic version of the Hadamard quotient theorem

The next proposition is our basic tool from the theory of recurrent sequences. It bears some resemblance to the Hadamard quotient theorem (which is used in its proof), and to conjectural generalisations of it as proposed by Bellagh and Bézivin [6, "Question" in Section 1] (using holonomicity instead of linear recurrence) and Dimitrov [12, Conjecture in 1.1] (using algebraicity instead of linear recurrence). In our special case, the proof relies on the quotient sequence having a specific form.

Proposition 3.1. *Let $(a_n)_{n\geqslant 1}$, $(b_n)_{n\geqslant 1}$, $(c_n)_{n\geqslant 1}$ be sequences of nonzero complex numbers such that*

$$a_n = b_n c_n$$

for all n. Assume that:

(i) *$(a_n)_{n\geqslant 1}$ satisfies a linear recurrence;*
(ii) *$(b_n)_{n\geqslant 1}$ is holonomic;*
(iii) *$(c_n)_{n\geqslant 1}$ is of the form $c_n = r_n |n|_p^{s_n}$ for a prime p and periodic sequences $(r_n)_{n\geqslant 1}$, $(s_n)_{n\geqslant 1}$ with $r_n \in \mathbf{Q}^*$, $s_n \in \mathbf{Z}$.*

Then the sequence $(c_n)_{n\geqslant 1}$ is bounded.

Proof. Note that $c_n \neq 0$ for all n. Since the sequence $(b_n)_{n\geqslant 1}$ given by $b_n = a_n/c_n$ is holonomic, by Lemma 1.2.(iii) there exist polynomials $q_0, \dots, q_d \in \mathbf{C}[z]$ such that

$$q_0(n)\frac{a_n}{c_n} = -\sum_{i=1}^{d} q_i(n+i)\frac{a_{n+i}}{c_{n+i}} \quad \text{for } n \geqslant 1. \tag{18}$$

We may further assume that $q_0 \neq 0$ (otherwise, replace for $i = 1, \dots, d$ the polynomials q_i by $(z-1)q_i$ and shift the relation by one). Suppose $c_n = r_n |n|_p^{s_n}$ is not bounded and let ϖ be the common period of both (r_n) and (s_n). The unboundedness of $(c_n)_{n\geqslant 1}$ means that there exists an integer $j \geqslant 1$ with $s_j < 0$ such

that there are elements in the arithmetic sequence $\{j + \varpi n \mid n \geqslant 0\}$ which are divisible by an arbitrarily high power of p. Fix such j and write $s := s_j$. Let ν be an integer such that $p^\nu > \max(d, \varpi)$ and let $\Pi = \operatorname{lcm}(\varpi, p^\nu)$. Note that $\operatorname{ord}_p \Pi = \nu$. By the assumption on $\{j + \varpi n \mid n \geqslant 0\}$, there exists an integer J such that $J \equiv j \pmod{\varpi}$ and $J \equiv 0 \pmod{p^\nu}$. By the definition of the sequence $(c_n)_{n\geqslant 1}$, for $n \equiv J \pmod{\Pi}$ the values $c_{n+1}, \ldots, c_{n+d}$ are uniquely determined (i.e., do not depend on n). Substituting such n to the equation (18), we obtain a formula of the form

$$\frac{a'_n}{|n|_p^s} = b'_n \quad \text{for } n \equiv J \pmod{\Pi},$$

where

$$a'_n = q_0(n)\frac{a_n}{r_j} \quad \text{and} \quad b'_n = -\sum_{i=1}^{d} q_i(n+i)\frac{a_{n+i}}{c_{n+i}}$$

are linear recurrence sequences along the arithmetic sequence $n \equiv J \pmod{\Pi}$ (here we use the fact that the values $c_{n+1}, \ldots, c_{n+d}$ do not depend on n, and that linear recurrence sequences form an algebra). Note that the values of $(a'_n)_{n\geqslant 1}$ are nonzero for sufficiently large n, and hence so are $(b'_n)_{n\geqslant 1}$. By Lemma 1.2.(i), a subsequence of a linear recurrence sequence along an arithmetic sequence is a linear recurrence sequence. Since the sequence

$$|n|_p^s = \frac{a'_n}{b'_n}$$

takes values in a finitely generated ring (namely $\mathbf{Z}[1/p]$), we conclude from the Hadamard quotient theorem (van der Poorten [40, Théorème], [36]) that the sequence $(|J + \Pi n|_p^s)_{n\geqslant 0}$ satisfies a linear recurrence, say

$$\gamma_0|J + \Pi n|_p^s + \gamma_1|J + \Pi(n+1)|_p^s + \ldots + \gamma_e|J + \Pi(n+e)|_p^s = 0 \quad \text{for } n \text{ large enough}, \tag{19}$$

where $\gamma_0, \ldots, \gamma_e \in \mathbf{C}$, $\gamma_0 \neq 0$. Let μ be an integer such that $p^\mu > \Pi d$. Since $\nu = \operatorname{ord}_p(\Pi) \leqslant \operatorname{ord}_p(J)$, we can find an integer $\Pi' > 0$ such that $\Pi\Pi' \equiv -J \pmod{p^\mu}$. Then for $n \equiv \Pi' \pmod{p^{\mu-\nu}}$ the values of

$$|J + \Pi(n+1)|_p^s, \ldots, |J + \Pi(n+e)|_p^s$$

are independent of n (actually, $|J + \Pi(n+j)|_p^s = p^{-\nu s}|j|_p^s$ for $j = 1, \ldots, e$), and hence by (19) so is the value of $\gamma_0|J + \Pi n|_p^s$ for n sufficiently large. Substituting $n = \Pi' + ip^{\mu-\nu}$ with $i = 0, \ldots, p-1$, we get a contradiction, since there is exactly one value of i for which $|J + \Pi(\Pi' + ip^{\mu-\nu})|_p^s < p^{-\mu s}$. □

4. Rationality properties of dynamical zeta functions

We prove a general rational/transcendental dichotomy in terms of the following arithmetical property:

Definition 4.1. An endomorphism $\sigma \in \operatorname{End}(A)$ is called *very inseparable* if $\sigma^n - 1$ is a separable isogeny for all n.

Note that the zero map is very inseparable. The notion "very inseparable" makes sense for arbitrary (not necessarily confined) endomorphisms, but such very inseparable endomorphisms are then automatically confined. We will study the geometric meaning of very inseparability in greater detail in Section 6; here we content ourselves with discussing the case of elliptic curves.

Example 4.2. In case $A = E$ is an elliptic curve, things simplify greatly (compare [9, Section 5]): there exists a (nonarchimedean) absolute value $|\cdot|$ on the ring $\operatorname{End}(E)$ such that $\deg_{\mathrm{i}}(\tau) = |\tau|^{-1}$ for $\tau \in \operatorname{End}(E)$. It is immediate that inseparable isogenies together with the zero map form an ideal in $\operatorname{End}(E)$ and that an inseparable isogeny σ (i.e., $|\sigma| < 1$) is very inseparable (i.e., $|\sigma^n - 1| = 1$ for all n). Neither of these statements is true in general for higher dimensional abelian varieties.

Theorem 4.3.

(i) *If σ is very inseparable, then $\zeta_\sigma(z) \in \mathbf{Q}(z)$ is rational.*

(ii) *If σ is not very inseparable, the sequence (σ_n) is not holonomic, and $\zeta_\sigma(z)$ is transcendental over $\mathbf{C}(z)$.*

Proof. Suppose we are in case (i), so $\sigma^n - 1$ is separable for all n. Since $\sigma_n = \deg(\sigma^n - 1)$, Proposition 2.3.(i) implies that $\zeta_\sigma(z)$ is a rational function of z.

In case (ii), set $a_n = \deg(\sigma^n - 1)$, $b_n = \sigma_n$, and $c_n = \deg_{\mathrm{i}}(\sigma^n - 1)$. By Proposition 2.3.(i), (a_n) is linear recurrent. By Proposition 2.7, $c_n = r_n |n|_p^{s_n}$ for periodic $r_n \in \mathbf{Q}^*$ and $s_n \in \mathbf{Z}$. Assume, by contradiction, that b_n is holonomic, i.e., that the sequence (b_n) is holonomic. The sequences $(a_n), (b_n)$, and (c_n) then satisfy all the conditions of Proposition 2.7, and we conclude that the sequence (c_n) is bounded. However, the following proves that (c_n) is unbounded:

Lemma 4.4. *If σ is not very inseparable, then the sequence $\deg_{\mathrm{i}}(\sigma^n - 1)$ is unbounded.*

Proof. By assumption, there exists n_0 for which $\sigma^{n_0} - 1$ is inseparable. Write $\sigma^{n_0} = 1 + \psi$ with ψ inseparable; then

$$\sigma^{n_0 p} - 1 = (1 + \psi)^p - 1 = \psi(\psi^{p-1} + p\chi)$$

for some endomorphism $\chi \colon A \to A$. Since p has identically zero differential, the map $\psi^{p-1} + p\chi$ is inseparable, and hence

$$\deg_{\mathrm{i}}(\sigma^{n_0 p} - 1) \geqslant 1 + \deg_{\mathrm{i}}(\psi) = 1 + \deg_{\mathrm{i}}(\sigma^{n_0} - 1),$$

and the result follows by iteration. □

To show the transcendence of $\zeta_\sigma(z)$ over $\mathbf{C}(z)$, suppose it is algebraic. Then so would be

$$z\frac{\zeta_\sigma'(z)}{\zeta_\sigma(z)} = z(\log(\zeta_\sigma(z)))' = \sum \sigma_n z^n.$$

This contradicts the fact that σ_n is not holonomic. □

Corollary 4.5. *At most one of the functions*

$$\zeta_\sigma(z) = \exp\left(\sum_{n\geqslant 1} \sigma_n \frac{z^n}{n}\right) \text{ and } \frac{1}{\zeta_\sigma(z)} = \exp\left(\sum_{n\geqslant 1} -\sigma_n \frac{z^n}{n}\right)$$

is holonomic.

Proof. Assume that both these functions are holonomic. Since the class of holonomic functions is closed under taking the derivative and the product [38, Thm. 2.3], we conclude that $z\frac{\zeta_\sigma'(z)}{\zeta_\sigma(z)}$ is holonomic, contradicting Theorem 4.3.(ii). □

Remark 4.6. It is not true that the multiplicative inverse of a holonomic function is necessarily holonomic. Harris and Shibuya [23] proved that this happens precisely if the logarithmic derivative of the function is algebraic. We do not know whether $\zeta_\sigma(z)$ is holonomic for not very inseparable σ, but Theorem 5.5 will show that $\zeta_\sigma(z)$ is not holonomic for a large class of maps.

Remark 4.7. If σ is not assumed to be confined, we could change the definition of σ_n by considering σ_n to be the number of fixed points of σ^n whenever it is finite, and 0 otherwise. This is in the spirit of [1], where only isolated fixed points of diffeomorphisms of manifolds were considered. In this case, we could still prove a variant of Theorem 4.3 saying that if σ is a (not-necessarily confined) endomorphism of A such that there exist n such that $\sigma^n - 1$ is an isogeny of arbitrarily high inseparability degree, then (σ_n) is not holonomic; one needs to use the fact that (the proof of) Proposition 3.1 holds even if we do not insist that a_n, b_n be nonzero and instead demand that $c_n = 1$ if $a_n = 0$. Note, however, that without the assumption that

σ is confined, $\zeta_\sigma(z)$ could be an algebraic but not rational function. For example, let E be a supersingular elliptic curve over a field of characteristic 2, let $A = E \times E$, and $\sigma = [2] \times [-1]$. Then

$$\zeta_\sigma(z) = \frac{1-2z}{1+2z}\sqrt{\frac{(1+z)(1+4z)}{(1-z)(1-4z)}}.$$

5. Complex analytic aspects

We now turn to questions of convergence and analytic continuation.

Radius of convergence. From the proof of Proposition 2.3, we pick up the formula

$$\deg(\sigma^n - 1) = \prod_{i=1}^{q}(\xi_i^n - 1) = \sum_{i=1}^{r} m_i \lambda_i^n, \tag{20}$$

where we note for future use that $q = 2g$, $\prod_{i=1}^{q} \xi_i = \deg(\sigma)$, and λ_i are of the form $\lambda_i = \prod_{j\in I} \xi_j$ for some $I \subseteq \{1, \dots, q\}$, each occurring with sign $(-1)^{|I|}$. Recall that $\{\lambda_i\}$ are called the *roots* of the linear recurrence, and λ_i is called a *dominant root* if it is of maximal absolute value amongst the roots. The roots $\{\lambda_i\}$ of the recurrence should not be confused with the roots $\{\xi_i\}$ of the characteristic polynomial of σ on H^1 (the dual of the ℓ-adic Tate module for any choice of $\ell \neq p$).

The following proposition follows from Formula (20) and the fact that $\deg(\sigma^n - 1)$ takes only positive values.

Proposition 5.1.

(i) *The ξ_i are not roots of unity.*
(ii) *The linear recurrent sequence $\deg(\sigma^n - 1)$ has a dominant positive real root, denoted Λ.*
(iii) $\Lambda = \prod_{i=1}^{q} \max\{|\xi_i|, 1\} \geqslant 1$ *is the Mahler measure of the characteristic polynomial of σ acting on H^1.*
(iv) $\Lambda = 1$ *if and only if σ is nilpotent.*
(v) $\deg(\sigma^n - 1)$ *has a unique dominant root if and only if there is no ξ_i with $|\xi_i| = 1$.*
(vi) *If $\deg(\sigma^n - 1)$ has a unique dominant root Λ, then Λ has multiplicity 1.*

Proof. (i) This is clear since σ is confined.

(ii) If not, then $\deg(\sigma^n - 1)$ would be negative infinitely often by a result of Bell and Gerhold [4, Thm. 2].

(iii) Denote temporarily $\tilde{\Lambda} = \prod_{i=1}^{q} \max\{|\xi_i|, 1\}$. We will prove shortly that $\tilde{\Lambda} = \Lambda$. Formula (20) implies that $\Lambda \leqslant \tilde{\Lambda}$ and

$$a_1(n) \coloneqq \sum_{|\lambda_j| = \tilde{\Lambda}} m_j \lambda_j^n$$

equals

$$a_1(n) = (-1)^t P^n \prod_{j\in J}(\xi_j^n - 1), \tag{21}$$

where t is the number of indices i such that $|\xi_i| < 1$, $P \coloneqq \prod_{|\xi_i|>1} \xi_i$, and $J \subseteq \{1, \dots, q\}$ denotes the set of indices i such that $|\xi_i| = 1$. Since the right hand side of Formula (21) is nonzero, we conclude that $\tilde{\Lambda} = \Lambda$. Finally, by Remark 2.4, ξ_i are the roots of the indicated characteristic polynomial.

(iv) Since none of the ξ_i is a root of unity, and since the set $\{\xi_i\}$ is closed under Galois conjugation, Kronecker's theorem implies that either some ξ_i has absolute value $|\xi_i| > 1$, in which case $\Lambda > 1$, or else all ξ_i are 0. The latter is equivalent to σ acting nilpotently on H^1, and hence σ is nilpotent since $\mathrm{End}(A)$ embeds into (the opposite ring of) $\mathrm{End}(\mathrm{H}^1)$.

(v) From Formula (21) we immediately get that if $J = \emptyset$, then $\deg(\sigma^n - 1)$ has a unique dominant root. Conversely, if $J \neq \emptyset$, then substituting $n = 0$ into Formula (21) gives $\sum m_j = 0$, and hence in the formula there are at least two distinct values of λ_j occurring, and the dominant root is not unique.

(vi) We have already proved that if there is a unique dominant root, then $J = \emptyset$. Thus we read from Formula (21) that the multiplicity of Λ is ± 1. Since $\deg(\sigma^n - 1)$ takes only positive values, the multiplicity is in fact 1. □

Proposition 5.2. *The radius of convergence of the power series defining $\zeta_\sigma(z)$ is $1/\Lambda > 0$.*

Proof. Note first that we have a trivial bound $\sigma_n = O(\Lambda^n)$, which implies that the power series $\zeta_\sigma(z)$ is majorised by $\exp(\sum_{n \geqslant 1} C\Lambda^n z^n/n) = (1 - \Lambda z)^{-C}$ for some constant $C > 0$. Thus the radius of convergence of $\zeta_\sigma(z)$ is at least $1/\Lambda$. If σ is nilpotent, the maps $\sigma^n - 1$ are all invertible, and hence $\sigma_n = 1$ and $\zeta_\sigma(z) = 1/(1 - z)$. Assume thus that σ is not nilpotent, and hence by Proposition 5.1.(iv), $\Lambda > 1$.

For the other inequality, we write the linear recurrence sequence $\deg(\sigma^n - 1) = \sum_{i=1}^r m_i \lambda_i^n$ as the sum of two linear recurrence sequences $a_1(n)$ and $a_2(n)$, $a_1(n)$ as in Formula (21) containing the terms with λ_i of absolute value $\tilde{\Lambda} = \Lambda$, and $a_2(n)$ containing the terms where λ_i is of strictly smaller absolute value.

Since all ξ_j with $j \in J$ are algebraic numbers on the unit circle but not roots of unity, a theorem of Gel'fond [19, Thm. 3] implies that for any $\varepsilon > 0$ and $n = n(\varepsilon)$ sufficiently large,

$$\prod_{j \in J} |\xi_j^n - 1| > \Lambda^{-n\varepsilon}$$

and hence $|a_1(n)| > \Lambda^{n(1-\varepsilon)}$ for sufficiently large n. The formula in Proposition 2.7 implies that $\deg_{\mathrm{i}}(\sigma^n - 1) = O(n^s)$ for some integer s, and hence it follows from Formula (6) that $\sigma_n > \Lambda^{n(1-2\varepsilon)}$ for sufficiently large n. An analogous reasoning as for the upper bound proves that the radius of convergence of $\zeta_\sigma(z)$ is at most $1/\Lambda^{1-2\varepsilon}$, implying the claim. □

Remark 5.3. The value $\log \Lambda$ describes the growth rate of the number of periodic points and plays the role of entropy as defined in the presence of a topology or a measure. It is the logarithm of the spectral radius of σ acting on the total (ℓ-adic) cohomology of A—even in the not very inseparable case—similarly to a result of Friedland's in the context of complex dynamics [18].

The degree zeta function. The degree zeta function $D_\sigma(z)$ is a rational function, and hence admits a meromorphic continuation to the entire complex plane. Actually,

$$D_\sigma(z) = \prod_{i=1}^r (1 - \lambda_i z)^{-m_i},$$

written in terms of the parameters in Equation (20), immediately provides the extension. Poles (with multiplicity m_i) occur at $1/\lambda_i$ with $m_i > 0$; zeros (with multiplicity m_i) occur at $1/\lambda_i$ with $m_i < 0$. We may describe the behaviour of zeros and poles more precisely.

Proposition 5.4. *Assume that σ is not nilpotent. Let $\Lambda' \coloneqq \max\{|\lambda_i| : |\lambda_i| < \Lambda\} < \Lambda$.*

(i) *The function $D_\sigma(z)$ has a pole at $1/\Lambda$.*
(ii) *The function $D_\sigma(z)$ has a zero z_0 with $|z_0| = 1/\Lambda'$ and is holomorphic in the annulus $1/\Lambda < |z| < 1/\Lambda'$.*
(iii) $\Lambda' \geqslant \sqrt{\Lambda}$.

Proof. In order to prove (i), we need to show that the multiplicity m of Λ is positive. If Λ is a dominant root, this follows from Proposition 5.1.(vi). If Λ is not a dominant root and $m < 0$, the sequence $\deg(\sigma^n - 1) - m\Lambda^n$ is a linear recurrent sequence with positive values and no dominant positive real root, contradicting [4, Thm. 2].

Let us now prove (ii). Let ρ denote the minimal value of $|\xi_i|$ and $|\xi_i|^{-1}$ that is strictly larger than 1, i.e.,

$$\rho = \min(\min\{|\xi_i| : |\xi_i| > 1\}, \min\{|\xi_i|^{-1} : 0 < |\xi_i| < 1\});$$

it exists since by Proposition 5.1.(iv), $\Lambda > 1$. Write the set of indices $\{1, \dots, q\} = J^-_< \cup J^- \cup J \cup J^+ \cup J^+_>$, where membership $i \in J^*_*$ is defined by the corresponding condition in the second row of the following table

$J^-_<$	J^-	J	J^+	$J^+_>$
$\lvert\xi_i\rvert < \rho^{-1}$	$\lvert\xi_i\rvert = \rho^{-1}$	$\lvert\xi_i\rvert = 1$	$\lvert\xi_i\rvert = \rho$	$\lvert\xi_i\rvert > \rho$

From Equation (20) we see that there is no λ_j with $\Lambda/\rho < |\lambda_j| < \Lambda$ and that the terms λ_j with $|\lambda_j| = \Lambda/\rho$ arise as products $\prod_{i\in I} \xi_i$ where I contains $J^+_>$, I is disjoint from $J^-_<$, $I \cap J$ can be anything and *either* I contains all except one $i \in J^+$ *or* I contains all $i \in J^+$ and exactly one $i \in J^-$.

Setting as before $P \coloneqq \prod_{i\in J^+\cup J^+_>} \xi_i$ and $t = \#(J^-_< \cup J^-)$, we get

$$\sum_{|\lambda_j|=\Lambda/\rho} m_j \lambda_j^n = (-1)^{t-1} P^n \prod_{j\in J} (\xi_j^n - 1) \left(\sum_{i\in J^+} \xi_i^{-n} + \sum_{i\in J^-} \xi_i^n \right). \tag{22}$$

Since the right hand side is not identically zero as a function of n, we conclude that $\Lambda' = \Lambda/\rho$. We consider two cases.

Case 1: $J = \emptyset$. Then by Proposition 5.1.(vi), $P = \Lambda$ has multiplicity 1 and hence from Formula (21) we conclude that t is even. Therefore by Formula (22) all λ_i with $|\lambda_i| = \Lambda'$ have multiplicity $m_i < 0$, and hence correspond to zeros of $D_\sigma(z)$.

Case 2: $J \neq \emptyset$. Substituting $n = 0$ into Formula (21) shows that the sum of multiplicities m_i of λ_i with $|\lambda_i| = \Lambda$ is 0. By Formula (22), the same is true for multiplicities m_j of λ_j with $|\lambda_j| = \Lambda'$. Thus there is some λ_i with $|\lambda_i| = \Lambda'$ and $m_i < 0$.

For the proof of (iii), note that since $\Lambda' = \Lambda/\rho$, the stated inequality is equivalent to $\Lambda \geqslant \rho^2$. Since $\Lambda = \prod \max\{|\xi_i|, 1\}$, it is enough to prove that there are at least two elements in the (non-empty) set $J^+ \cup J^+_>$. Since $q = 2g$ is even, it suffices to prove that both $\#J$ and $t = \#(J^- \cup J^-_<)$ are even. Since ξ_i with $|\xi_i| = 1$ occur in complex conjugate pairs, $\#J$ is even, and the corresponding term in (21) is real positive. In the course of proof of Proposition 5.2 we have shown that the sum $a_1(n)$ dominates the remaining terms, and hence is positive for large n. Hence we find from Formula (21) that $P > 1$ and t is even. □

Analytic continuation/natural boundary. When σ is very inseparable, $\zeta_\sigma(z)$ coincides with the degree zeta function $D_\sigma(z)$ and hence is a rational function. One may wonder whether a Pólya–Carlson dichotomy holds for the functions $\zeta_\sigma(z)$, meaning that, when they are not rational as above, they admit a natural boundary as complex function (and hence they are non-holonomic; in this context also called "transcendentally transcendental").

We confirm this for a large class of such maps, providing at the same time another proof of their transcendence (and even non-holonomicity). The crucial tool is Theorem A.1 that Royals and Ward prove in Appendix A of this paper.

Theorem 5.5. *Suppose that σ is not very inseparable and that Λ is the unique dominant root. Then the function $\zeta_\sigma(z)$ has the circle $|z| = 1/\Lambda$ as its natural boundary. In particular, $\zeta_\sigma(z)$ is not holonomic.*

Proof. We start by the observation that $\zeta_\sigma(z)$ has the same natural boundary as $Z_\sigma(z) \coloneqq \sum \sigma_n z^n$ if the latter function has natural boundary [5, Lemma 1]. Next, we find an expression

$$Z_\sigma(z) = \sum_{i=1}^{r} m_i \sum_{n\geqslant 1} r_n^{-1} |n|_p^{-s_n} (\lambda_i z)^n,$$

where m_i, λ_i are as in (10) and r_n, s_n are as in Proposition 2.7. We now apply Theorem A.1: in the notation of that theorem, we choose S to be the set of primes containing p and all primes ℓ for which $|r_n|_\ell \neq 1$ for some n. By periodicity of (r_n), the set S is finite. Let $a_n := \deg_{\mathrm{i}}(\sigma^n - 1) = r_n |n|_p^{s_n}$. Suppose ϖ is a common period for (r_n) and (s_n). For $\ell \in S$, set $n_\ell = \varpi$, $c_{\ell,k} = |r_k|_\ell$; for $\ell \neq p$, set $e_{\ell,k} = 0$, and set $e_{p,k} = -s_k$. Then $|a_n|_S = a_n^{-1}$, and hence we can write

$$Z_\sigma(z) = \sum_{i=1}^{r} m_i f(\lambda_i z),$$

where f is the function associated to (a_n) as in Theorem A.1. Since σ is not very inseparable, by Remark 4.4 the sequence (a_n) takes infinitely many values. We find that the term $f(\lambda_i z)$ has a natural boundary along $|z| = \frac{1}{|\lambda_i|}$. If Λ is the *unique* λ_i of maximal absolute value, then the dense singularities along this circle cannot be cancelled by other terms, and we conclude that $Z_\sigma(z)$ has a natural boundary along $|z| = 1/\Lambda$, and the same holds for $\zeta_\sigma(z)$. Since a holonomic function has only finitely many singularities (corresponding to the zeros of $q_0(z)$ if the series function satisfies Equation (5), compare [16, Thm. 1]), $\zeta_\sigma(z)$ cannot be holonomic. □

Question 5.6. Is $|z| = 1/\Lambda$ a natural boundary for $\zeta_\sigma(z)$ for any not very inseparable σ (even without the assumption of a unique dominant root)?

Metrisable group endomorphisms with the same zeta function. Given the analogy between our results and some properties of metrizable group endomorphisms, one may ask for the following more formal relationship:

Question 5.7. Can one associate to an action of $\sigma \circlearrowright A$ an endomorphism of a compact metrisable abelian group $\tau \circlearrowright G$ with the same Artin–Mazur zeta function, i.e., $\zeta_\sigma = \zeta_\tau$?

The analogue of this question over the complex numbers is trivial, as one may take $G = A(\mathbf{C})$. The degree zeta function $D_\sigma(z)$ artificially equals the Artin–Mazur zeta function of an endomorphism τ of a $2g$-dimensional real torus whose matrix has the same characteristic polynomial as that of σ acting on $T_\ell(A)$ for any $\ell \neq p$ (e.g., the companion matrix). This implies that for a very inseparable $\sigma \circlearrowright A$, indeed, $\zeta_\sigma(z) = \zeta_\tau(z)$.

Even in the not very inseparable case, it is sometimes possible to construct such $\tau \circlearrowright G$, like we did for the example in the introduction.

In general, it would be natural to consider the induced action of σ on the torsion subgroup $A(K)_{\mathrm{tor}}$ (dual of the total Tate module $\prod T_\ell(A)$). This provides the correct contribution $|\sigma_n|_\ell$ at all primes $\ell \neq p$; for such ℓ, the size of the cokernel of $\sigma^n - 1$ acting on $T_\ell(A)$ is precisely $|\sigma_n|_\ell^{-1}$. However, at $\ell = p$, we found no such natural group in general, and it seems that $|\sigma_n|_p$ is genuinely determined by the geometry of the p-torsion subgroup scheme.

6. Geometric characterisation of very inseparable endomorphisms

In this section, we analyse the condition of very inseparability from a geometric point of view as well as its relation to inseparability. For this, it is advantageous to *temporarily drop the assumption of confinedness* and consider a general $\sigma \in \mathrm{End}(A)$.

Elementary properties. We start by listing properties of very inseparability that follow more or less directly from the definition. For this, we first write out a very basic property:

Lemma 6.1. *Whether $\sigma \in \mathrm{End}(A)$ is a separable isogeny or not is determined by its action on the finite commutative group scheme $A[p]$, i.e., by its image under the map $\mathrm{End}(A) \to \mathrm{End}(A[p])$.*

Proof. If two endomorphisms $\sigma, \tau\colon A \to A$ induce the same map on $A[p]$, then $\sigma - \tau$ vanishes on the group scheme $A[p]$, and hence it factors through the map $[p]\colon A \to A$. Thus $\sigma - \tau = p\nu$ for some $\nu\colon A \to A$, and hence the map $\operatorname{End}(A)/p\operatorname{End}(A) \hookrightarrow \operatorname{End}(A[p])$ is injective. Since an endomorphism $A \to A$ is a separable isogeny if and only if it induces an isomorphism on the tangent space, and since every map of the form $p\nu$ induces the zero map on the tangent space, we conclude that σ is a separable isogeny if and only if τ is a separable isogeny. □

Proposition 6.2. *Let $\sigma \in \operatorname{End}(A)$.*

(i) *The endomorphism σ is very inseparable if and only if $\sigma^n - 1$ is a separable isogeny for all $n \leqslant p^{4g^2}$.*
(ii) *If $A = A_1 \times A_2$ with A_1, A_2 abelian varieties and $\sigma = \sigma_1 \times \sigma_2$ is a product morphism with $\sigma_i \in \operatorname{End}(A_i)$, then σ is very inseparable if and only if σ_1 and σ_2 are both very inseparable.*
(iii) *Multiplication $[m]\colon A \to A$ by an integer m is very inseparable if and only if m is divisible by p.*
(iv) *An endomorphism of an elliptic curve is very inseparable if and only if it is either an inseparable isogeny or zero.*
(v) *If E is an elliptic curve over a field of characteristic 3, then the isogeny $\sigma := [2]\times[3]$ on $A := E\times E$ is inseparable but not very inseparable.*

Proof. To prove (i), observe that by Lemma 6.1, it suffices to look at the images of $\sigma^n - 1$ in the ring $\operatorname{End}(A)/p\operatorname{End}(A)$. Since $\operatorname{End} A$ is finite free of rank at most $4g^2$, this ring is finite of cardinality $\leqslant p^{4g^2}$, and hence the sequence of images of $\sigma^n - 1$ is ultimately periodic (i.e., periodic except for a finite number of n) with all possible values already occuring for $n \leqslant p^{4g^2}$.

Property (ii) is immediate from the definition.

Since an endomorphism of an abelian variety is a separable isogeny if and only if its differential is surjective, to prove (iii), observe that the differential of the multiplication by $m^n - 1$ map is still given by multiplication by $m^n - 1$ and hence is surjective if and only if it is nonzero, i.e., when p does not divide $m^n - 1$. The latter happens for all $n \geqslant 1$ if and only if $p|m$.

Statement (iv) was already discussed in Remark 4.2.

Property (v) follows immediately from (ii) and (iii). □

Using the local group scheme $A[p]^0$. The category of finite commutative group schemes over K is abelian and decomposes as the product of the category of finite étale and the category of finite local group schemes (see, e.g., [20, A §4]). The group scheme $A[p]$ decomposes canonically as the product of the étale part $A[p]_{\text{ét}}$ and the local part $A[p]^0$. We now provide a geometric characterisation of (very) inseparability using the local p-torsion subgroup scheme, as in Theorem A in the introduction.

Theorem 6.3. *Let $\sigma \in \operatorname{End}(A)$.*

(i) *σ is a separable isogeny if and only if it induces an isomorphism on $A[p]^0$.*
(ii) *σ is very inseparable if and only if it induces a nilpotent map on $A[p]^0$.*

Proof. Under the splitting $A[p] = A[p]_{\text{ét}} \times A[p]^0$, the morphism $\sigma[p]$ induced by σ on $A[p]$ splits as a product morphism $\sigma[p] = \sigma[p]_{\text{ét}} \times \sigma[p]^0$. Therefore, we have

$$\ker \sigma[p] = \ker \sigma[p]_{\text{ét}} \times \ker \sigma[p]^0. \tag{23}$$

An isogeny σ is separable if and only if $\ker \sigma$ is étale.

We turn to the proof of (i). In one direction, first assume that σ is a separable isogeny. Then $\ker \sigma$ is étale, and hence so is its subgroup scheme $\ker \sigma[p]$. From the decomposition (23), we conclude that $\ker \sigma[p]^0$ is both étale and local, hence trivial. Since $A[p]^0$ is a finite group scheme, the map $\sigma[p]^0$ is an isomorphism.

For the other direction, assume first that σ is *not an isogeny.* Let B be the reduced connected component of 0 of $\ker \sigma$. Then B is an abelian subvariety, $B[p]^0$ is a nontrivial group scheme (because multiplication by p on B is not étale) and is contained in the kernel of $\sigma[p]^0$ and hence $\sigma[p]^0$ is not an isomorphism.

Secondly, assume that σ is an *inseparable isogeny.* Then $\ker\sigma$ is not étale. We have $\ker\sigma \subseteq A[n]$ for $n = \deg\sigma$. Writing $n = p^t u$ with u coprime with p, we get a decomposition $\ker\sigma = \ker\sigma[p^t] \times \ker\sigma[u]$. The group scheme $\ker\sigma[u]$ is étale (as a subgroup scheme of $A[u]$), and hence $\ker\sigma[p^t]$ cannot be étale, which means that $\ker\sigma[p^t]^0$ is nontrivial. For each integer r, we have an exact sequence

$$0 \longrightarrow \ker\sigma[p^{r-1}]^0 \longrightarrow \ker\sigma[p^r]^0 \xrightarrow{p^{r-1}} \ker\sigma[p]^0.$$

Applying this inductively for $r = t, t-1, \ldots, 2$, we conclude that $\ker\sigma[p]^0$ is nontrivial, and hence the morphism $\sigma[p]^0$ is not an isomorphism. This proves (i).

For the proof of (ii), consider the natural homomorphism $\varphi\colon \mathrm{End}(A) \to \mathrm{End}(A[p]^0)$. Since $\mathrm{End}(A)$ is a finite $\mathbf{Z}$-algebra, and since $p \in \ker\varphi$, the ring $R \coloneqq \mathrm{im}(\varphi)$ is a finite $\mathbf{F}_p$-algebra. By part (i), the map $\sigma^n - 1$ is a separable isogeny if and only if its image $\varphi(\sigma^n - 1)$ is a unit in $\mathrm{End}(A[p]^0)$. We claim that $\varphi(\sigma^n - 1)$ is then a unit in R; in fact, the ring R is a finite $\mathbf{F}_p$-algebra, and hence there exists a monic polynomial $f \in \mathbf{F}_p[t]$, $f = t^d + a_{d-1}t^{d-1} + \ldots + a_0$ of lowest degree such that $f(\sigma^n - 1) = 0$. If the constant term a_0 of f is different than zero, then we easily see that $\sigma^n - 1$ is invertible in R, its inverse being $-a_0^{-1}\sum_{i=0}^{d-1}(\sigma^n - 1)^i$. If on the other hand $a_0 = 0$, then $\sigma^n - 1$ is a two-sided zero-divisor in R, hence in $\mathrm{End}(A[p]^0)$, and therefore cannot be a unit in $\mathrm{End}(A[p]^0)$. Thus, our claim is now reduced to the proof of the following lemma.

Lemma 6.4. *Let R be a finite (not necessarily commutative) $\mathbf{F}_p$-algebra and let $r \in R$. Then the following conditions are equivalent:*

(i) *For all positive integers n $r^n - 1$ is invertible.*
(ii) *The element r is nilpotent.*

Proof. Let J denote the Jacobson radical of R. The ring R is artinian and hence the ring $\overline{R} = R/J$ is semisimple [26, 4.14]. For an element $s \in R$, denote the image of s in $\overline{R}$ by $\overline{s}$. Then s is invertible in R if and only if $\overline{s}$ is invertible in $\overline{R}$ [26, 4.18] and s is nilpotent if and only if $\overline{s}$ is nilpotent (this follows from the fact that the Jacobson radical of an artinian ring is nilpotent, see [26, 4.12]). Thus we have reduced the claim to the case of a semisimple ring $\overline{R}$.

By the Wedderburn–Artin theorem [26, 3.5], a semisimple ring is a product of matrix rings over division rings which in our case need to be finite, and hence by another theorem of Wedderburn [26, 13.1] are commutative. Thus we can decompose the ring $\overline{R}$ as a product of matrix rings over finite fields

$$\overline{R} \simeq \prod_{i=1}^{s} \mathrm{M}_{n_i}(\mathbf{F}_{q_i}).$$

Clearly, each of the properties in the statement of the lemma can be considered separately for each term in this product, and we are reduced to proving that a matrix N over a finite field has the property that $N^n - 1$ is invertible for all $n \geqslant 1$ if and only if N is nilpotent.

If N is nilpotent, then all the matrices $N^n - 1$ are invertible, since in any ring the sum of a unit and a nilpotent that commute with each other is a unit. Conversely, if N is not nilpotent, then N has some eigenvalue $\lambda \neq 0$, perhaps in a larger (but still finite) field. Let $n \geqslant 1$ be such that $\lambda^n = 1$ (such n always exists in a *finite* field). Then the matrix $N^n - 1$ is not invertible. □

We have some immediate corollaries (where 6.5.(i) refines Lemma 6.1):

Corollary 6.5. *Let $\sigma \in \mathrm{End}(A)$.*

(i) *Whether σ is a separable isogeny or not, or very inseparable or not, is determined by its action on $A[p]^0$, i.e., on its image under the map*

$$\mathrm{End}(A) \to \mathrm{End}(A[p]^0).$$

(ii) *Very inseparable isogenies are inseparable.*

(iii) *There exists a simple abelian surface with a confined isogeny that is inseparable but not very inseparable and for which inseparable isogenies together with the zero map do not form an ideal.*

Proof. Statement (i) is immediate from Theorem 6.3. Statement (ii) follows from Theorem 6.3, since nilpotents are not invertible. Concerning (iii), the following is an example of a simple abelian variety A and an inseparable but not very inseparable isogeny σ (all computational data used can be found at [27]). Consider the isogeny class of supersingular abelian surfaces over $\mathbf{F}_5$ of p-rank 0 with characteristic polynomial of the Frobenius π equal to $x^4 + 25 = 0$. The splitting field $L \coloneqq \mathbf{Q}(\pi) = \mathbf{Q}(i, \sqrt{10})$ has no real embeddings, hence by Waterhouse [41, Thm. 6.1] there exists a simple abelian surface A with endomorphism ring $\mathscr{O}_L = \mathbf{Z}[i, \pi]$ (the ring of integers in L, containing both π and $5/\pi = -i\pi$). Consider $\sigma = i - 2 = \frac{\pi^2}{5} - 2$, with characteristic polynomial $\sigma^2 + 4\sigma + 5 = 0$. The endomorphism σ is a confined isogeny since on a simple abelian variety these are exactly the endomorphisms that are neither zero nor roots of unity. Denoting the reduction of σ modulo 5 by $\overline{\sigma}$, we find that

$$\overline{\sigma}^2 = \overline{\sigma}. \tag{24}$$

Note that $A[p] = A[p]^0$ and hence there is an injective map $\mathscr{O}_L/5\mathscr{O}_L \hookrightarrow \mathrm{End}(A[p]^0)$. Now σ is separable if and only if $\overline{\sigma}$ is an isomorphism on $A[p]^0$, which, by (24), happens exactly if $\overline{\sigma} = 1$. But then $\sigma = 5\psi + 1$ for some $\psi \in \mathscr{O}_L$, which does not hold. Hence σ is inseparable. On the other hand, σ is very inseparable if and only if $\overline{\sigma}$ is nilpotent on $A[p]^0$, which, by (24), happens exactly if $\overline{\sigma} = 0$. This means that $\sigma = 5\psi$ for some $\psi \in \mathscr{O}_L$, which does not hold either. Hence σ is not very inseparable.

Let $\sigma' = -i - 2$. We similarly prove that σ' is inseparable, and yet the map $\sigma + \sigma' = -4$ is a separable isogeny. Hence the set of inseparable isogenies together with the zero map is not closed under addition. □

Using Dieudonné modules. The structure of the endomorphism ring of the local group scheme $A[p]^0$ can be computed explicitly using the theory of Dieudonné modules, and we will use this to deduce some more results on very inseparability.

The group schemes $A[p]$ and $A[p]^0$ are objects in the category $\mathscr{C}_K$ of finite commutative group schemes over K annihilated by p. By covariant Dieudonné theory [20, A §5] there is an equivalence of categories

$$D\colon \mathscr{C}_K \to \text{Finite length left } \mathbf{E}\text{-modules},$$

where $\mathbf{E} = K[F, V]$ denotes the non-commutative ring of polynomials with relations

$$FV = VF = 0, F\lambda = \lambda^p F \text{ and } V\lambda^p = \lambda V \text{ for } \lambda \in K.$$

We may consider being a very inseparable endomorphism or a separable isogeny as a property of the image of an endomorphism under the map $\mathrm{End}(A) \to \mathrm{End}_{\mathbf{E}}(D(A[p]^0))$.

Example 6.6. If A is an ordinary elliptic curve, then $A[p]^0 \cong \mu_p$, so $\mathrm{End}(A[p]^0) = \mathbf{F}_p$. If A is a supersingular elliptic curve, the local group scheme $A[p]^0$ is the unique non-split self-dual extension of α_p by α_p. The Dieudonné module is $D(A[p]^0) = \mathbf{E}/\mathbf{E}(V + F)$ [20, A.5.4] and a computation [20, A.5.8] gives a ring isomorphism

$$\mathrm{End}(A[p]^0) \cong \mathrm{End}_{\mathbf{E}}(\mathbf{E}/\mathbf{E}(V + F)) \cong \left\{ \begin{pmatrix} a^p & b \\ 0 & a \end{pmatrix} : a \in \mathbf{F}_{p^2}, b \in K \right\}.$$

From these computations, one also sees directly that non-invertible elements are nilpotent in $\mathrm{End}(A[p]^0)$ in both the ordinary and the supersingular case, giving an alternative proof of 6.2.(iv).

Proposition 6.7. *Let $\sigma \in \mathrm{End}(A)$ and set $\mathbf{D} \coloneqq D(A[p])^0)$.*

(i) *σ is a separable isogeny (respectively, very inseparable endomorphism) if and only if its image in $\mathrm{End}_{K[F]}(\mathbf{D}/V\mathbf{D})$ is invertible (respectively, nilpotent).*

(ii) *σ is very inseparable if and only if a power of σ factors through the p-Frobenius map $\mathrm{Fr}\colon A \mapsto A^{(p)}$.*

(iii) *If $\mathrm{End}(A)$ is commutative, the set of very inseparable endomorphisms forms an ideal in $\mathrm{End}(A)$.*

(iv) *There exists an abelian variety for which the set of very inseparable endomorphisms is not closed under either addition or multiplication (in particular, it is not an ideal).*

(v) *Let A denote a simple ordinary abelian variety defined over a finite field $\mathbf{F}_q \subseteq K$ with (commutative) endomorphism ring $\mathscr{O} \coloneqq \mathrm{End}(A)$ and Frobenius endomorphism π. Set $R \coloneqq \mathbf{Z}[\pi, q/\pi]$. Then $R \subseteq \mathscr{O}$ and if $p \nmid [\mathscr{O}:R]$, then any isogeny of A is very inseparable if and only if it is inseparable. This is in particular true if $q = p \geqslant 5$.*

Proof. We first prove (i). The relations in $\mathbf{E}$ imply that $V\mathbf{E}$ is a two-sided ideal in $\mathbf{E}$. In this way, σ, as an $\mathbf{E}$-endomorphism of $\mathbf{D}$, gives rise to an endomorphism $\tilde{\sigma}$ of the $\mathbf{E}/V\mathbf{E} = k[F]$-module $\mathbf{D}/V\mathbf{D}$. The first claim is that σ is nilpotent if and only if $\tilde{\sigma}$ is. The interesting direction is where $\tilde{\sigma}$ is nilpotent, meaning that $\sigma^n(\mathbf{D}) \subseteq V\mathbf{D}$ for some n. Since V is nilpotent on $\mathbf{D}$ [20, A.5], say $V^d\mathbf{D} = 0$, we can iterate the equation to get $\sigma^{nd}(\mathbf{D}) \subseteq V^d\mathbf{D} = 0$. Secondly, we claim that σ is invertible if and only if $\tilde{\sigma}$ is so. Again, the interesting direction is when $\tilde{\sigma}$ is invertible. If we let $\mathbf{D}'$ denote the image of $\sigma\colon \mathbf{D} \to \mathbf{D}$, then $\mathbf{D}'$ is an $\mathbf{E}$-submodule of $\mathbf{D}$ and $\mathbf{D} = \mathbf{D}' + V\mathbf{D}$. Iterating this sufficiently many times, we find that

$$\mathbf{D} = \mathbf{D}' + V\mathbf{D} = \mathbf{D}' + V\mathbf{D}' + V^2\mathbf{D} = \ldots = \mathbf{D}' + V\mathbf{D}' + \cdots + V^{d-1}\mathbf{D}' \subseteq \mathbf{D}'.$$

This shows that σ is surjective, and, since it is an endomorphism of the underlying finite dimensional vector space, it is then automatically injective.

In order to prove (ii), note that the Dieudonné module $D(A^{(p)}[p]^0)$ can be identified with $\mathbf{D} = D(A[p]^0)$ with the $\mathbf{E}$-action twisted by the geometric Frobenius map $\psi\colon K \to K$, $\psi(\lambda) = \lambda^{1/p}$. Under this identification, the map induced by the p-Frobenius $\mathrm{Fr}\colon A \to A^{(p)}$ on the Dieudonné modules is the ψ-semilinear map $V\colon \mathbf{D} \to \mathbf{D}$ [20, A.5]. Moreover, the map V is nilpotent.

If σ is very inseparable, there exists n with $\sigma^n|_{A[p]^0} = 0$. Since $A[\mathrm{Fr}] \subseteq A[p]^0$, we have $\sigma^n|_{A[\mathrm{Fr}]} = 0$ and hence σ^n factors through Fr. Conversely, suppose that $\sigma^n = \tau \circ \mathrm{Fr}$ for some $\tau\colon A^{(p)} \to A$. Passing to the Dieudonné modules, and using the fact that the map $D(\tau)$ is ψ^{-1}-semilinear (and hence commutes with V), we see that $D(\sigma^n)\mathbf{D} \subseteq V\mathbf{D}$, so $D(\sigma)$ is nilpotent modulo V. By part (i), we find that σ is very inseparable.

For the proof of (iii), note that, without any assumptions on the ring $\mathrm{End}(A)$, the set I of maps in $\mathrm{End}(A)$ that factor through the p-Frobenius Fr is a left ideal in $\mathrm{End}(A)$. Therefore by (ii), if the ring $\mathrm{End}(A)$ is commutative, the set of very inseparable maps in $\mathrm{End}(A)$ coincides with the radical of I, and hence is an ideal.

For (iv), consider $A = E \times E$ for an ordinary elliptic curve E. Then $\mathrm{End}(A) = \mathrm{M}_2(\mathrm{End}(E))$ surjects onto $\mathrm{End}(A[p]^0) = \mathrm{M}_2(\mathbf{F}_p)$ (see Example 6.6). The set of very inseparable endomorphisms corresponds under this map to matrices whose image in $\mathrm{M}_2(\mathbf{F}_p)$ is nilpotent, and it suffices to remark that the set of nilpotent elements in $\mathrm{M}_2(\mathbf{F}_p)$ is not closed under neither addition nor multiplication.

For (v), we indeed have $R \subseteq \mathscr{O}$ by [41, 7.4]. Let $\sigma \in \mathscr{O}$ and observe that the coprimality of $[\mathscr{O}:R]$ to p implies that there exists an integer N coprime to p with $N\sigma \in R$. Therefore, it suffices to prove the equivalence of inseparability and very inseparability for elements of R. Represent such an element $\sigma \in R$ by

$$\sum_{i \geqslant 1} a_i \pi^i + \sum_{j \geqslant 0} b_j (\pi')^j,$$

with $\pi' = q/\pi$ and $a_i, b_i \in \mathbf{Z}$ (the terms containing both π and π' may be omitted since they do not change the image of σ in $\mathrm{End}(\mathbf{D})$). Since A is defined over $\mathbf{F}_q$ with $q = p^r$, we have $\pi = \mathrm{Fr}^r$ and $\pi' = \mathrm{Ver}^r$, where $\mathrm{Ver}\colon A^{(p)} \to A$ is the Verschiebung. On the level of Dieudonné modules, Fr maps to V and Ver maps to F [20, A.5], so σ maps to the endomorphism

$$\tilde{\sigma} \coloneqq \sum b_j F^{rj} \in \mathrm{End}_{K[F]}(\mathbf{D}/V\mathbf{D}).$$

In the ordinary case, the Dieudonné modules of $A[p]$ and $A[p]^0$ are

$$D(A[p]) = (\mathbf{E}/(V, 1-F) \oplus \mathbf{E}/(F, 1-V))^g$$

and

$$\mathbf{D} = D(A[p]^0) = (\mathbf{E}/(V, 1-F))^g$$

(since this is the subgroup scheme of $D(A[p])$ on which V is nilpotent [20, A.5]). Hence $F = 1$ in $\mathrm{End}(\mathbf{D}/V\mathbf{D}) = \mathrm{M}_g(\mathbf{F}_p)$, and $\tilde{\sigma} \coloneqq \sum b_j$ is a scalar multiplication; therefore, it is nilpotent if and only if it is zero (i.e., non-invertible).

The final claim follows from a result of Freeman and Lauter [17, Prop. 3.7]. □

We were unable to answer the following natural questions:

Question 6.8.

(i) Construct a *simple* abelian variety for which very inseparable endomorphisms do not form an ideal.

(ii) Consider the subset of the moduli space of abelian varieties of given dimension and given degree of polarisation consisting of those abelian varieties A for which inseparable isogenies are very inseparable. Is this locus dense in the moduli space? Recall that, by a result of Norman and Oort, the ordinary locus is dense [31, Thm. 3.1].

7. The tame zeta function

We revert to our standard assumptions and define the following general "tame" version of the Artin–Mazur zeta function for varieties over fields of positive characteristic (the construction is somewhat reminiscent of that of the Artin–Hasse exponential):

Definition 7.1. Let K denote an algebraically closed field of positive characteristic $p > 0$, X/K an algebraic variety, and let $f\colon X \to X$ denote a confined morphism. The *tame zeta function* ζ_f^* is defined as the formal power series

$$\zeta_f^*(z) \coloneqq \exp\left(\sum_{p\nmid n} f_n \frac{z^n}{n}\right), \tag{25}$$

summing only over n that are not divisible by p.

A basic observation is:

Proposition 7.2. *We have identities of formal power series*

$$\zeta_{X,f}(z) = \prod_{i\geqslant 0} \sqrt[p^i]{\zeta^*_{X,f^{p^i}}(z^{p^i})} \tag{26}$$

and

$$\zeta^*_{X,f}(z) = \zeta_{X,f}(z) / \sqrt[p]{\zeta_{X,f^p}(z^p)}. \tag{27}$$

Proof. For the first identity (26), we do a formal computation, splitting the sum over n into parts where n is exactly divisible by a given power p^i of p (denoted $p^i \| n$):

$$\begin{aligned}\zeta_{X,f}(z) &= \exp\left(\sum_{i\geqslant 0}\sum_{p^i\| n} \frac{f_n}{n} z^n\right) = \exp\left(\sum_{i\geqslant 0}\sum_{p\nmid m} \frac{f_{p^i m}}{p^i m} z^{p^i m}\right)\\ &= \exp\left(\sum_{i\geqslant 0}\frac{1}{p^i}\sum_{p\nmid m}\frac{(f^{p^i})_m}{m}\left(z^{p^i}\right)^m\right) = \prod_{i\geqslant 0}\exp\left(\frac{1}{p^i}\log\left(\zeta^*_{f^{p^i}}(z^{p^i})\right)\right).\end{aligned}$$

For the second identity (27), we compute as follows:

$$\zeta^*_{X,f}(z) = \exp\left(\sum_{n\geqslant 1}\frac{f_n}{n}z^n - \sum_{k\geqslant 1}\frac{f_{pk}}{pk}z^{pk}\right) = \exp\left(\sum_{n\geqslant 1}\frac{f_n}{n}z^n\right) \Big/ \exp\left(\frac{1}{p}\sum_{k\geqslant 1}\frac{(f^p)_k}{k}z^{pk}\right). \qquad \square$$

Theorem 7.3. *For $\sigma \circlearrowright A$, there exists an integer $t > 0$ (depending on σ) such that $(\zeta_\sigma^*)^t$ is a rational function. In particular, ζ_σ^* is algebraic.*

Proof. Proposition 2.7 implies that for $p \nmid n$ the inseparability degree $\deg_{\mathrm{i}}(\sigma^n - 1) = r_n$ is periodic of period ω with $r_n = r_{\gcd(n,\omega)}$. Let μ denote the Möbius function. For $n|\omega$, define rational numbers α_n by

$$\alpha_n = \frac{1}{n} \sum_{e|n} \frac{\mu(n/e)}{r_e}. \tag{28}$$

By Möbius inversion and the equality $r_n = r_{\gcd(n,\omega)}$, we get

$$\frac{1}{r_n} = \sum_{d|\gcd(n,\omega)} d\alpha_d \quad \text{for all } n \geqslant 1.$$

Therefore,

$$\begin{aligned} \zeta_\sigma^*(z) &= \exp\left(\sum_{p\nmid n} \frac{\deg(\sigma^n - 1)}{nr_n} z^n \right) = \exp\left(\sum_{d|\omega} \alpha_d \sum_{p\nmid m} \frac{\deg(\sigma^{dm} - 1)}{m} z^{dm} \right) \\ &= \prod_{d|\omega} \left(\exp\left(\sum_{p\nmid m} \frac{\deg(\sigma^{dm} - 1)}{m} z^{dm} \right) \right)^{\alpha_d}. \end{aligned}$$

Using the notation of Proposition 2.3.(i), we can rewrite this as

$$\zeta_\sigma^*(z) = \prod_{d|\omega} \left(D_{\sigma^d}(z^d) / \sqrt[p]{D_{\sigma^{pd}}(z^{pd})} \right)^{\alpha_d} \tag{29}$$

and hence the result follows from the rationality of the degree zeta functions. □

The minimal exponent $t_\sigma > 0$ for which $\zeta_\sigma^*(z) \in \mathbf{Q}(z)$ is an invariant of the dynamical system $\sigma \circlearrowright A$. We briefly discuss the arithmetic significance of such t_σ, by considering both ordinary and supersingular elliptic curves.

Proposition 7.4. *Let E denote an elliptic curve, $\sigma \in \mathrm{End}(E)$, and let t_σ be the minimal positive integer for which $\zeta_\sigma^*(z)^{t_\sigma} \in \mathbf{Q}(z)$.*

(i) *If E is ordinary, t_σ is a pure p-th power.*
(ii) *There exists a (supersingular) E and $\sigma \circlearrowright E$ for which t_σ is not a pure p-th power.*

Proof. If σ is an endomorphism of an ordinary elliptic curve, then there is a valuation $|\cdot|$ on the quotient field L of the endomorphism ring that extends the p-valuation and such that $\deg_{\mathrm{i}} \sigma = |\sigma|$ (cf. Remark 4.2). If σ is very inseparable, $\zeta_\sigma^*(z)$ is rational, and the claim is clear. Otherwise, let s be the minimal positive integer for which $M \coloneqq |\sigma^s - 1| < 1$. We find that for integers n not divisible by p,

$$r_n = \deg_{\mathrm{i}}(\sigma^n - 1) = \begin{cases} 1 & \text{if } s\nmid n, \\ M & \text{if } s|n. \end{cases} \tag{30}$$

Substituting this into Formula (28), we get $\omega = s$. If $s = 1$, we have $\alpha_1 = 1/M$, and if $s > 1$, we find

$$\alpha_n = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n|s,\ 1 < n < s, \\ (1 - M)/(Ms) & \text{if } n = s. \end{cases} \tag{31}$$

Since p splits in L [10, §2.10], the valuation $|\cdot|$ has residue field $\mathbf{F}_p$, and hence $s|(p-1)$. From Formula (29), it follows that $\zeta_\sigma^*(z)$ is a product of rational functions to powers $1/p$ and $(1-M)/(Mps)$ (and $1/(Mp)$ if $s = 1$). Now with $M = p^{-r}$ for some $r \geqslant 1$, we find that $(1 - M)/(Mps) = (p^r - 1)/p^{r+1}s$, which has denominator a power of p, since s divides $p - 1$. This proves (i).

For (ii) consider a supersingular elliptic curve $A = E$. We have already seen in Remark 4.2 that the inseparability degree of an isogeny is detected by a valuation on the quaternion algebra $\mathrm{End}(E) \otimes \mathbf{Q}$, on which we now briefly elaborate. The ring $\mathscr{O} = \mathrm{End}(E)$ is a maximal order in a quaternion algebra, and its completion $\mathscr{O}_p = \mathrm{End}(E) \otimes_{\mathbf{Z}} \mathbf{Z}_p$ is an order in the unique quaternion division algebra D over $\mathbf{Q}_p$ [10]. There exists a valuation $v\colon D \to \mathbf{Z}$ on D with the property that $\mathscr{O}_p = \{x \in D : v(x) \geqslant 0\}$. Let $\mathfrak{p} = \{x \in \mathscr{O} : v(x) \geqslant 1\}$. Then $\mathfrak{p}$ is a two-sided maximal ideal in $\mathscr{O}$ with $p\mathscr{O}_p = \mathfrak{p}^2\mathscr{O}_p$ and we have an isomorphism $\mathscr{O}/\mathfrak{p} \simeq \mathbf{F}_{p^2}$. The inseparable degree of an isogeny $\sigma \in \mathscr{O}$ is given by the formula $\deg_{\mathrm{i}}(\sigma) = p^{v(\sigma)}$, cf. [9, Prop. 5.5].

Let $\sigma \in \mathscr{O}$ be an endomorphism such that its image in $\mathscr{O}/\mathfrak{p} \simeq \mathbf{F}_{p^2}$ generates the multiplicative group of the field and such that $v(\sigma^{p^2-1} - 1) = 1$. Then for integers n not divisible by p we have

$$\deg_{\mathrm{i}}(\sigma^n - 1) = \begin{cases} 1 & \text{if } (p^2-1) \nmid n, \\ p & \text{if } (p^2-1) \mid n. \end{cases} \tag{32}$$

Let us prove that such σ exists: choose elements $\sigma_0, \tau \in \mathscr{O}$ such that the image of σ_0 in $\mathscr{O}/\mathfrak{p} \simeq \mathbf{F}_{p^2}$ generates the multiplicative group of the field and $v(\tau) = 1$. Then one of the elements $\sigma_0, \sigma_0 + \tau$ satisfies the desired conditions.

Furthermore, the degree is of the form $\deg(\sigma^n - 1) = m^n - \lambda^n - (\lambda')^n + 1$ for $\lambda, \lambda' \in \overline{\mathbf{Q}}$ and $m \coloneqq \lambda\lambda' \in \mathbf{Z}$. Using the convenient notation

$$\mathscr{Z}(z) \coloneqq \frac{\sqrt[p]{1 - z^p}}{1 - z},$$

a somewhat tedious computation, splitting the terms in $\log \zeta^*_\sigma(z)$ to take into account the cases in Formula (32), gives that

$$\zeta^*_\sigma(z) = \frac{g_1(z)}{\sqrt[p(p+1)]{g_{p^2-1}(z)}}, \text{ where } g_i(z) \coloneqq \frac{\mathscr{Z}(z^i)\,\mathscr{Z}((mz)^i)}{\mathscr{Z}((\lambda z)^i)\,\mathscr{Z}((\lambda' z)^i)}.$$

Note that $\mathscr{Z}(z)$ is itself a p-th root of a rational function. We conclude that $t = p^2(p+1)$ suffices to have $\zeta^*_\sigma(z)^t \in \mathbf{Q}(z)$ but $\zeta^*_\sigma(z)^t$ is not rational for any choice of t as a pure p-th power. □

8. Functional equations

In this section, we study the existence of functional equations for full and tame zeta functions on abelian varieties. Assume throughout the section that σ is an isogeny. Under the transformation $z \mapsto 1/\deg(\sigma)z$, we will find a functional equation for zeta functions of very inseparable endomorphisms, and a "Riemann surface" version of a functional equation for the tame zeta function. Since this transformation does not make sense for ζ_σ as a formal power series, D_σ, ζ_σ, and ζ^*_σ are therefore considered as genuine functions of a complex variable, and the symbols are understood to refer to their (maximal) analytic continuations.

Proposition 8.1. *The degree zeta function $D_\sigma(z)$ (cf. 2.2) satisfies a functional equation of the form*

$$D_\sigma\left(\frac{1}{\deg(\sigma)z}\right) = D_\sigma(z).$$

Proof. We use the notations from Equation (20). It is clear that the multiset of λ_i is stable under the involution $\lambda \mapsto \deg(\sigma)/\lambda$. From this symmetry, we obtain a functional equation for the exponential generating function $D_\sigma(z) = \prod_{i=1}^r (1 - \lambda_i z)^{-m_i}$ of the form

$$D_\sigma\left(\frac{1}{\deg(\sigma)z}\right) = (-z)^{\sum_{i=1}^r m_i} \prod_{i=1}^r \lambda_i^{m_i} D_\sigma(z).$$

Subsituting $n = 0$ into (20) gives $\sum_{i=1}^r m_i = 0$ and a direct computation using the form of λ_i and the fact that q is even shows that $\prod_{i=1}^r \lambda_i^{m_i} = 1$, which gives the claim. □

Remark 8.2. The functional equation for $D_\sigma(z)$ can be placed in the cohomological framework from Remark 2.4: consider the Poincaré duality pairing $\langle \cdot, \cdot \rangle \colon \mathrm{H}^i \times \mathrm{H}^{2g-i} \otimes \mathbf{Q}_\ell(g) \to \mathbf{Q}_\ell$, under which $\langle \sigma_* x, y \rangle = \langle x, \sigma^* y \rangle$, with $\sigma_* \sigma^* = [\deg \sigma]$. Hence if σ^* has eigenvalues α_i on H^i, then σ_* has eigenvalues $\deg(\sigma)/\alpha_i$ on H^{2g-i}, but these sets are the same by duality. In this way the functional equation picks up a factor $z^{\chi(A)}$, where $\chi(A)$ is the ℓ-adic Euler characteristic of A. But here, $\chi(A) = 0$ (since the i-th ℓ-adic Betti number of an abelian variety of dimension g is the binomial coefficient $\binom{2g}{i}$).

Theorem 8.3.

(i) *If σ is very inseparable, then $\zeta_\sigma(z)$ extends to a meromorphic function on the entire complex plane and satisfies a functional equation of the form*

$$\zeta_\sigma\left(\frac{1}{\deg(\sigma) z}\right) = \zeta_\sigma(z).$$

(ii) *If σ is not very inseparable and Λ is the unique dominant root, then $\zeta_\sigma(z)$ cannot satisfy a functional equation under $z \mapsto 1/\deg(\sigma) z$; actually, the intersection of the domains of $\zeta_\sigma(z)$ and $\zeta_\sigma(1/\deg(\sigma) z)$ is empty.*

(iii) *For any confined σ, let X_σ denote the concrete Riemann surface of the algebraic function $\zeta_\sigma^*(z)$ (a finite covering of the Riemann sphere). Then there exists an involution $\tau \in \mathrm{Aut}(X_\sigma)$ such that the meromorphic extension $\zeta_\sigma^* \colon X_\sigma \to \widehat{\mathbf{C}}$ fits into a commutative diagram of the form*

$$\begin{array}{ccc} X_\sigma & \xrightarrow{\tau} & X_\sigma \\ {\scriptstyle \zeta_\sigma^*}\downarrow & & \downarrow{\scriptstyle \zeta_\sigma^*} \\ \widehat{\mathbf{C}} & \xrightarrow{\mathrm{id}} & \widehat{\mathbf{C}}. \end{array} \tag{33}$$

Proof. If σ is very inseparable, then $\zeta_\sigma = D_\sigma$, and the result follows from Proposition 8.1.

If σ is not very inseparable and Λ is the unique dominant root, then by Theorem 5.5 the function $\zeta_\sigma(z)$ has a natural boundary on $|z| = 1/\Lambda$. Thus $\zeta_\sigma(z)$ and $\zeta_\sigma(\frac{1}{\deg(\sigma) z})$ are commonly defined only on $\frac{\Lambda}{\deg(\sigma)} < |z| < \frac{1}{\Lambda}$ which is empty when $\Lambda^2 \geqslant \deg(\sigma)$. By Proposition 5.1.(iii), we have $\Lambda^2 \geqslant \Lambda \geqslant \prod |\xi_i| = \deg \sigma$, so this always holds.

For the third part of the theorem, consider equation (29) that expresses the function ζ_σ^* in terms of degree zeta functions. Write $\alpha_d/p = A_d/B_d$ for coprime integers A_d, B_d, let N denote the least common multiple of B_d over all $d|\omega$ and set $\beta_d \coloneqq N\alpha_d/p \in \mathbf{Z}$. Then ζ_σ^* entends to a function on the Riemann surface X_σ corresponding to the projective curve defined by the affine equation

$$y^N = \prod_{d|\omega} \left(\frac{D_{\sigma^d}(x^d)^p}{D_{\sigma^{pd}}(x^{pd})} \right)^{\beta_d}$$

given by $\zeta_\sigma^*(x, y) = y$. By the fact that all D_σ satisfy the functional equation as in Proposition 8.1, the map $\tau \colon X_\sigma \to X_\sigma, \tau(x, y) = \left(\frac{1}{\deg(\sigma) x}, y\right)$ is an involution of X_σ (we use that $\deg(\sigma^r) = \deg(\sigma)^r$ for any integer r). The same functional equations then prove that the diagram (33) commutes. □

9. Prime orbit growth

In this section, we consider the prime orbit growth for a confined endomorphism $\sigma \colon A \to A$. We are interested in possible analogues of the Prime Number Theorem ("PNT"), much like Parry and Pollicott proved for Axiom A flows [32]. In our case, it follows almost immediately from the rationality of their zeta functions that such an analogue holds for very inseparable σ. In general, however, as we will see, the prime orbit counting function displays infinitely many forms of limiting behaviour. Nevertheless, the (weaker) analogue of Chebyshev's bounds and Mertens' second theorem hold. In accordance with our philosophy, we also consider counting only "tame" prime orbits (i.e, of length coprime to p), and in this case we see

finitely many forms of limiting behaviour, detectable from properties of the p-divisible group. Finally, we briefly discuss good main and error terms reflecting analogues of the Riemann Hypothesis.

Notations/Definitions 9.1. A *prime orbit* O of length $\ell =: \ell(O)$ of $\sigma\colon A \to A$ is a set $O = \{x, \sigma x, \sigma^2 x, \ldots, \sigma^\ell x = x\} \subseteq A(K)$ of exact cardinality ℓ. Letting P_ℓ denote the number of prime orbits of length ℓ for σ, the *prime orbit counting function* is $\pi_\sigma(X) \coloneqq \sum_{\ell \leqslant X} P_\ell$.

As formal power series, the zeta function of σ admits a product expansion

$$\zeta_\sigma(z) = \prod_O \frac{1}{1 - z^{\ell(O)}},$$

where the product runs over all prime orbits. Since $\sigma_n = \sum_{\ell | n} \ell P_\ell$, Möbius inversion implies that $P_\ell = \frac{1}{\ell} \sum_{n|\ell} \mu\left(\frac{\ell}{n}\right) \sigma_n$. Our proofs will exploit the fact that the numbers σ_n differ from the linear recurrent sequence $\deg(\sigma^n - 1)$ only by a multiplicative factor, the inseparable degree, that grows quite slowly.

Not to complicate matters, we make the following assumption:

Standing assumption/notations.
The dominant root $\Lambda > 1$ is unique.
The ϖ-periodic sequences (r_n) and (s_n), $s_n \leqslant 0$, are as in Formula (14).
All asymptotic formulæ in this section hold for integer values of the parameter.

By Proposition 5.1.(vi), this implies that $\Lambda > 1$ is of multiplicity one. We start with a basic proposition describing the asymptotics of P_ℓ. Interestingly, the error terms are determined by the zeros of the degree zeta function. This appears to be a rather strong result with a very easy proof, dependent on the exponential growth.

Proposition 9.2. $P_\ell = \dfrac{\Lambda^\ell}{\ell r_\ell |\ell|_p^{s_\ell}} + O(\Lambda^{\Theta\ell})$, *where* $\Theta \coloneqq \max\{\mathsf{Re}(s) : D_\sigma(\Lambda^{-s}) = 0\} \in [\frac{1}{2}, 1)$.

Proof. From Formula (10), we get $\deg(\sigma^n - 1) = \Lambda^n + O(\Lambda^{\Theta\ell})$ for

$$\Theta \coloneqq \max_{|\lambda_i| \neq \Lambda} \frac{\log|\lambda_i|}{\log(\Lambda)}.$$

By Proposition 5.4, this equals the largest real part of a zero of $D_\sigma(\Lambda^{-s})$, and $1/2 \leqslant \Theta < 1$. Hence

$$\sigma_\ell = \frac{\deg(\sigma^\ell - 1)}{\deg_{\mathrm{i}}(\sigma^\ell - 1)} = \frac{\Lambda^\ell}{r_\ell |\ell|_p^{s_\ell}} + O(\Lambda^{\Theta\ell}).$$

Expressing the number of prime orbits in terms of the number of fixed points, we get

$$P_\ell = \frac{1}{\ell} \sum_{n|\ell} \mu\left(\frac{\ell}{n}\right) \sigma_n = \frac{\sigma_\ell}{\ell} + \frac{1}{\ell} \sum_{\substack{n|\ell \\ n<\ell}} \mu\left(\frac{\ell}{n}\right) \sigma_n.$$

Since $|\mu(\ell/n)\sigma_n| \leqslant \deg(\sigma^n - 1) \leqslant M\Lambda^n$ for some constant M depending only on σ, we get

$$\left| \sum_{\substack{n|\ell \\ n<\ell}} \mu\left(\frac{\ell}{n}\right) \sigma_n \right| \leqslant \ell M \Lambda^{\ell/2},$$

and since $\Theta \geqslant 1/2$, the claim follows. □

The remainder of this section is dedicated to a study of what happens to the asymptotics if we further average in ℓ, like in the prime number theorem or Mertens' theorem. We will see that between PNT and Mertens' theorem, information about σ being very inseparable or not gets lost.

The next lemma is formulated in a general way and will be applied several times in order to asymptotically replace factors "$1/\ell$" for $\ell \leqslant X$ by "$1/X$". This leads to simplified main terms at the cost of worse error terms (we will discuss another approach leading to a "complicated main term with good error term" at the end of the section).

Lemma 9.3. *Let (a_ℓ) be a bounded sequence and let $\Lambda > 1$ be a real number. Then*

$$\sum_{\ell \leqslant X} \frac{a_\ell}{\ell} \Lambda^{\ell - X} = \frac{1}{X} \sum_{\ell \leqslant X} a_\ell \Lambda^{\ell - X} + O(1/X^2).$$

Proof. Write

$$\sum_{\ell \leqslant X} \frac{a_\ell}{\ell} \Lambda^{\ell - X} - \frac{1}{X} \sum_{\ell \leqslant X} a_\ell \Lambda^{\ell - X} = \sum_{\ell \leqslant X} \frac{a_\ell (X - \ell)}{X \ell} \Lambda^{\ell - X}.$$

With $M \coloneqq \sup |a_\ell| < +\infty$, the "top half" of this sum can be bounded as follows:

$$\left| \sum_{X/2 \leqslant \ell \leqslant X} \frac{a_\ell (X - \ell)}{X \ell} \Lambda^{\ell - X} \right| \leqslant \frac{2M}{X^2} \sum_{i \geqslant 0} i \Lambda^{-i} = O(1/X^2)$$

while the "bottom half" is easily seen to be $O(X \Lambda^{-X/2})$, whence the claim. □

(Non-)analogues of PNT and analogues of Chebyshev's estimates. The first application is to the following "fluctuating" asymptotics for the prime orbit counting function:

Proposition 9.4. $$\frac{X \pi_\sigma(X)}{\Lambda^X} = \sum_{\ell \leqslant X} \frac{1}{r_\ell |\ell|_p^{s_\ell}} \Lambda^{\ell - X} + O(1/X).$$

Proof. By Proposition 9.2 we see that

$$\frac{X \pi_\sigma(X)}{\Lambda^X} = X \sum_{\ell \leqslant X} P_\ell \Lambda^{-X} = X \sum_{\ell \leqslant X} \left(\frac{1}{\ell r_\ell |\ell|_p^{s_\ell}} \Lambda^{\ell - X} + \Lambda^{-X} O(\Lambda^{\Theta \ell}) \right).$$

The error terms in this sum form a geometric series and hence decrease exponentially. Applying Lemma 9.3 to the main term, we find the stated result. □

The next theorem discusses the analogue of the PNT in our setting; an analogue of Chebyshev's 1852 determination of the order of magnitude of the prime counting function holds in general, but the analogue of the PNT holds only for very inseparable endomorphisms. The result for general endomorphisms is similar in spirit to that for the 3-adic doubling map considered in [15, Thm. 3], S-integer dynamical systems in [14] (from which we take the terminology "detector group"), or to Knieper's theorem [25, Thm. B] on the asymptotics of closed geodesics on rank one manifolds of non-positive curvature.

Theorem 9.5.

(i) *The order of magnitude of $\pi_\sigma(X)$ is $\pi_\sigma(X) \asymp \Lambda^X / X$, in the sense that the function $X \pi_\sigma(X) / \Lambda^X$ is bounded away from 0 and ∞.*

(ii) *Consider the "detector" group*

$$G_\sigma \coloneqq \{(a, x) \in \mathbf{Z}/\varpi \mathbf{Z} \times \mathbf{Z}_p : a \equiv x \bmod |\varpi|_p^{-1}\}.$$

If (X_n) is a sequence of integers such that $X_n \to +\infty$ and (X_n, X_n) has a limit in the group G_σ, then the sequence $X_n \pi_\sigma(X_n) / \Lambda^{X_n}$ converges, and every accumulation point of $X \pi_\sigma(X) / \Lambda^X$ arises in this way.

(iii) (a) *If σ is very inseparable, $\lim_{X \to +\infty} X \pi_\sigma(X) / \Lambda^X$ exists and equals $\Lambda / (\Lambda - 1)$.*

(b) *If σ is not very inseparable, then the set of accumulation points of $X \pi_\sigma(X) / \Lambda^X$ is a union of a Cantor set and finitely many points. In particular, it is uncountable.*

Proof. For (i), we estimate the value of $X\pi_\sigma(X)/\Lambda^X$ in terms of the sum in Proposition 9.4. The bound from above is trivial; for the bound from below we consider the terms with $\ell = X-1$ and $\ell = X$ and note that for at least one of these indices we have $|\ell|_p = 1$. We thus obtain the bounds

$$\frac{1}{\Lambda \max(r_\ell)} \leqslant \liminf_{X\to+\infty} \frac{X\pi_\sigma(X)}{\Lambda^X} \leqslant \limsup_{X\to+\infty} \frac{X\pi_\sigma(X)}{\Lambda^X} \leqslant \frac{\Lambda}{\Lambda-1}. \tag{34}$$

To prove (ii), the formula in Proposition 9.4 may be rewritten as

$$\frac{X\pi_\sigma(X)}{\Lambda^X} = \sum_{\ell=0}^{X-1} \frac{1}{r_{X-\ell}|X-\ell|_p^{s_{X-\ell}}} \Lambda^{-\ell} + O(1/X). \tag{35}$$

If (X_n) is as indicated, i.e., if $X_n \bmod \varpi$ stabilises (say at the value $\varpi_0 \bmod \varpi$) and X_n converges to some x in $\mathbf{Z}_p$, then individual summands in Formula (35) have a well-defined limit while the whole sum is bounded uniformly in n by the convergent series $\sum_{t=0}^\infty \Lambda^{-t}$. Thus

$$\lim_{n\to+\infty} \frac{X_n\pi_\sigma(X_n)}{\Lambda^{X_n}} = \sum_{\ell=0}^{\infty} \frac{1}{r_{\varpi_0-\ell}|x-\ell|_p^{s_{\varpi_0-\ell}}} \Lambda^{-\ell}, \tag{36}$$

where (r_n) and (s_n) are prolonged to periodic sequences for $n \in \mathbf{Z}$ in an obvious manner; if x is a positive integer, then the term corresponding to $\ell = x$ should be construed as $\frac{\Lambda^{-\ell}}{r_{\varpi_0-\ell}}$ if $s_{\varpi_0-\ell} = 0$, and 0 otherwise.

We now prove (iii). When σ is very inseparable, $\varpi = 1, r_n = 1$, $s_n = 0$, and Proposition 9.4 implies the result by summing the geometric series $\sum_{k\geqslant 0} \Lambda^{-k} = 1/(1-1/\Lambda)$ in (36). Note that the result also follows by Tauberian methods applied to the rational zeta function $\zeta_\sigma = D_\sigma$.

In the case of general σ, we consider the map $\varphi\colon G_\sigma \to \mathbf{R}$ which associates to an element $(\varpi_0, x) \in G_\sigma$ the limit

$$\varphi(\varpi_0, x) = \lim_{n\to+\infty} \frac{X_n\pi_\sigma(X_n)}{\Lambda^{X_n}}$$

for a sequence (X_n) of integers such that $X_n \to +\infty$ and X_n has the limit (ϖ_0, x) in G_σ. By Formula (36), this map is continuous. We will show that in some neighbourhood of each point the map φ is either constant or a homeomorphism. Note that since G_σ is compact, the set of accumulation points of $X\pi_\sigma(X)/\Lambda^X$ is equal to the image of φ.

Choose $\varpi_0 \bmod \varpi$, two distinct elements $x, y \in \mathbf{Z}_p$ and two sequences of integers (X_n) and (Y_n) which tend to infinity and such that $X_n \bmod \varpi = Y_n \bmod \varpi = \varpi_0$ and $X_n \to x$ and $Y_n \to y$ in $\mathbf{Z}_p$. Then by (36) we have

$$\varphi(\varpi_0, x) - \varphi(\varpi_0, y) = \sum_{\ell=0}^{\infty} a_\ell, \tag{37}$$

where

$$a_\ell = \frac{1}{r_{\varpi_0-\ell}} \left(\frac{1}{|x-\ell|_p^{s_{\varpi_0-\ell}}} - \frac{1}{|y-\ell|_p^{s_{\varpi_0-\ell}}} \right) \Lambda^{-\ell}.$$

Let $k \geqslant 0$ be such that $|x-y|_p = p^{-k}$. The terms a_ℓ are nonzero if and only if $\ell \equiv x \pmod{p^{k+1}}$ or $\ell \equiv y \pmod{p^{k+1}}$ and furthermore $s_{\varpi_0-\ell} \neq 0$. Note that whether such ℓ exists depends only on the values of $x - \varpi_0$ and $y - \varpi_0$ modulo $\gcd(p^{k+1}, \varpi)$. For ℓ with $a_\ell \neq 0$, the terms a_ℓ can be bounded from below:

$$|a_\ell| \geqslant \frac{1}{r_{\varpi_0-\ell}} \left(p^{ks_{\varpi_0-\ell}} - p^{(k+1)s_{\varpi_0-\ell}} \right) \Lambda^{-\ell} \geqslant \frac{1}{2r_{\varpi_0-\ell}} p^{ks_{\varpi_0-\ell}} \Lambda^{-\ell}$$

while clearly $|a_\ell| \leqslant \Lambda^{-\ell}$ for any ℓ.

We now consider two cases depending on whether or not there exists ℓ such that $a_\ell \neq 0$.

Case 1: Assume first that there exists ℓ such that $a_\ell \neq 0$ and let ℓ_0 be the smallest such ℓ. Since any other such ℓ differs from ℓ_0 by a multiple of p^k, we get

$$\left|\sum_{\ell=0}^{\infty} a_\ell\right| \geqslant \left(\frac{1}{2r_{\varpi_0-\ell_0}} p^{ks_{\varpi_0-\ell_0}} - \frac{\Lambda^{-p^k}}{1-\Lambda^{-p^k}}\right)\Lambda^{-\ell_0}.$$

Since the sequences (r_ℓ) and (s_ℓ) take only finitely many values, the expression on the right is positive for k larger than a constant K_0 which depends only on σ but not on x, y, or ϖ_0. Therefore from (37) we conclude that if $|x-y|_p \leqslant p^{-K_0}$, then $\varphi(\varpi_0, x) \neq \varphi(\varpi_0, y)$.

Case 2: If $a_\ell = 0$ for all ℓ, then by Formula (37) we have $\varphi(\varpi_0, x) = \varphi(\varpi_0, y)$. Let p^ν be the largest power of p dividing ϖ. Recall that whether $a_\ell = 0$ for all ℓ depends only on the values of $x - \varpi_0$ and $y - \varpi_0$ modulo $\gcd(p^{k+1}, \varpi)$. Therefore if $a_\ell = 0$ for all ℓ and $|x-y| = p^{-k}$ with $k \geqslant \nu$, then the map φ is locally constant in a neighbourhood of (ϖ_0, x).

Replacing K_0 with $\max(K_0, \nu)$ if necessary, we see that the map $\varphi\colon G_\sigma \to \mathbf{R}$ restricted to open compact subsets

$$B(\varpi_0, x) = \{(\varpi_0, y) \in G_\sigma : |x-y|_p \leqslant p^{-K_0}\} \subseteq G_\sigma$$

is either injective (corresponding to Case 1) or constant (corresponding to Case 2). Since G_σ is a disjoint union of finitely many subsets $B(\varpi_0, x)$, and since each $B(\varpi_0, x)$ is topologically a Cantor set, we conclude that the image of φ is a union of finitely many (possibly no) Cantor sets and finitely many points.

In order to finish the proof, it is enough to note that if σ is very inseparable, then there exists $(\varpi_0, x) \in G_\sigma$ for which Case 1 holds, so the image of φ contains a Cantor set. Indeed, by Lemma 4.4 there exists an integer ϖ_0 such that $s_{\varpi_0} < 0$. It is then easy to see that Case 1 holds for this choice of ϖ_0 and $x = 0$. □

Example 9.6. If σ is the (very inseparable) Frobenius (relative to $\mathbf{F}_q$) on an abelian variety $A/\mathbf{F}_q$ of dimension g, then $\Lambda = q^g$ and we find that $\sum_{\ell \leqslant X} P_\ell \sim q^{g(X+1)}/(X(q^g-1))$, where P_ℓ is the number of closed points of A with residue field $\mathbf{F}_{q^\ell}$.

Our warm up example from the introduction illustrates what happens in the not very inseparable case.

Tame prime orbit counting. Now consider the analogous question in the tame case.

Definition 9.7. The *tame prime orbit counting function* is $\pi^*_\sigma(X) \coloneqq \sum_{\substack{\ell \leqslant X \\ p \nmid \ell}} P_\ell$.

Remark 9.8. The tame zeta function $\zeta^*_\sigma(z)$ is not exactly equal to the formal Euler product over orbits of length coprime to p, but rather (notice the difference with Formula (26)):

$$\prod_{p \nmid \ell(O)} \frac{1}{1-z^{\ell(O)}} = \prod_{i \geqslant 0} \sqrt[p^i]{\zeta^*_\sigma(z^{p^i})}.$$

We find only finitely many possible kinds of limiting behaviour, governed by the values of the periodic sequence (r_n) (the warm up example from the introduction illustrates this).

Theorem 9.9. *For any $k \in \{0, \ldots, p\varpi - 1\}$ the limit*

$$\lim_{\substack{X \to +\infty \\ X \equiv k \bmod p\varpi}} \frac{X\pi^*_\sigma(X)}{\Lambda^X} = \rho_k \tag{38}$$

exists (so there is convergence along sequences of values of X that converge in the "tame detector group" $G^*_\sigma \coloneqq \mathbf{Z}/p\varpi$) and is given by

$$\rho_k = \frac{1}{\Lambda^{p\varpi}-1} \sum_{\substack{1 \leqslant n \leqslant p\varpi \\ p \nmid n}} \frac{\Lambda^{\langle n-k\rangle}}{r_n}, \tag{39}$$

where $\langle x \rangle$ denotes the representative for x mod $p\varpi$ in $\{1, \ldots, p\varpi\}$.

Proof. By Proposition 9.2 we have

$$\pi_\sigma^*(X) = \sum_{\substack{\ell \leqslant X \\ p \nmid \ell}} \left(\frac{\Lambda^\ell}{\ell r_\ell} + O(\Lambda^{\Theta \ell}) \right).$$

The error terms in this formula form a geometric progression and hence are $O(\Lambda^{\Theta X})$. Multiplying by Λ^{-X} and applying Lemma 9.3, we get

$$\frac{\pi_\sigma^*(X)}{\Lambda^X} = \frac{1}{X\Lambda^X} \sum_{\substack{\ell \leqslant X \\ p \nmid \ell}} \Lambda^\ell \frac{1}{r_\ell} + O(1/X^2).$$

We split the sum by values of r_n, as follows:

$$\begin{aligned} \lim_{X \to +\infty} \frac{X \pi_\sigma^*(X)}{\Lambda^X} &= \lim_{X \to +\infty} \frac{1}{\Lambda^X} \left(\sum_{\substack{1 \leqslant n \leqslant p\varpi \\ p \nmid n}} \frac{1}{r_n} \sum_{s=0}^{\left\lfloor \frac{X-n}{p\varpi} \right\rfloor} \Lambda^{n+sp\varpi} \right) \\ &= \lim_{X \to +\infty} \left(\sum_{\substack{1 \leqslant n \leqslant p\varpi \\ p \nmid n}} \frac{\Lambda^{p\varpi \left\lfloor \frac{X-n}{p\varpi} \right\rfloor + p\varpi + n - X}}{r_n(\Lambda^{p\varpi} - 1)} \right). \end{aligned}$$

The limit does not converge in general, but if we put $X = Yp\varpi + k$ for fixed k and $Y \to +\infty$, we find the indicated result, since $p\varpi \left\lfloor \frac{k-n}{p\varpi} \right\rfloor + p\varpi + n - k = \langle n - k \rangle$. □

We refer to the example in the introduction for some explicit computations and graphs.

Analogue of Mertens' theorem. The PNT is equivalent to the statement that the reciprocals of the primes up to X sum, up to a constant, to $\log \log X + o(1/\log X)$. Mertens' second theorem is the same statement but with the weaker error term $O(1/\log X)$. It turns out that the analogue of this last theorem in our setting does hold, and very inseparable and not very inseparable endomorphisms behave in the same way.

Proposition 9.10. *For some $c \in \mathbf{Q}$ and $c' \in \mathbf{R}$ we have* $\sum_{\ell \leqslant X} P_\ell / \Lambda^\ell = c \log X + c' + O(1/X)$.

Proof. From Proposition 9.2 we find

$$\sum_{\ell \leqslant X} P_\ell / \Lambda^\ell = \sum_{\ell \leqslant X} \left(\frac{1}{\ell r_\ell |\ell|_p^{s_\ell}} + O(\Lambda^{(\Theta-1)\ell}) \right).$$

The error terms in this formula sum to $c'' + O(\Lambda^{(\Theta-1)X})$ for some $c'' \in \mathbf{R}$ and the main terms sum to

$$\sum_{j=1}^{\varpi} \frac{1}{r_j} B_{-s_j, j}(X),$$

where for integers $s \geqslant 0$, $\varpi > 0$, and j, we set

$$B_{s,j}(X) \coloneqq \sum_{\substack{n \leqslant X \\ n \equiv j \bmod \varpi}} \frac{|n|_p^s}{n}.$$

The proposition follows from

$$B_{s,j}(X) = c_{s,j} \log X + c'_{s,j} + O(1/X) \tag{40}$$

for constants $c_{s,j} \in \mathbf{Q}$ and $c'_{s,j} \in \mathbf{R}$. The case $s = 0$ is well-known and we will thus limit ourselves to the case $s > 0$. To prove (40), we first consider the related sum

$$A_{s,j}(X) = \sum_{\substack{n \leqslant X \\ n \equiv j \bmod \varpi}} |n|_p^s$$

and we claim that

$$A_{s,j}(X) = c_{s,j} X + O(1) \text{ with } c_{s,j} \in \mathbf{Q}\,. \tag{41}$$

Then Abel summation gives

$$B_{s,j}(X) = \frac{A_{s,j}(X)}{X} + \int_1^X \frac{A_{s,j}(t)}{t^2} dt,$$

so (40) follows, setting $c'_{s,j} = c_{s,j} + \int_1^\infty (A_{s,j}(t) - c_{s,j} t) dt/t^2 \in \mathbf{R}$. To prove (41), observe that the arithmetic sequence $j + \varpi \mathbf{N}$ might or might not contain terms divisible by arbitrarily high power of p depending on whether $|j|_p \leqslant |\varpi|_p$ or $|j|_p > |\varpi|_p$. In the latter case the sequence $|n|_p$ for $n \equiv j \pmod{\varpi}$ is constant, and the asymptotic formula for $A_{s,j}$ is clear. In the former case we write k for the power of p dividing ϖ. In the formula defining $A_{s,j}$, we isolate terms with a given value of $|n|_p$. For each integer $q \geqslant k$ the number of terms $n \equiv j \pmod{\varpi}$ with $n \leqslant X$ and $|n|_p = p^{-q}$ is $\frac{p-1}{p^{q-k+1}\varpi} X + O(1)$, the implicit constant being independent of q. We thus get the asymptotic formula

$$A_{s,j} = \sum_{q \geqslant k} p^{-sq} \left(\frac{p-1}{p^{q-k+1}\varpi} X + O(1) \right) = c_{s,j} X + O(1)$$

with $c_{s,j} = (p-1) p^{s(1-k)} / ((p^{s+1} - 1)\varpi)$. □

Error terms in the PNT. We now briefly discuss how to identify good main terms and error terms in the asymptotics for the number of prime orbits. From Proposition 9.2, it is immediate that

$$\pi_\sigma(X) = M(X) + O(\Lambda^{\Theta X})$$

with "main term"

$$M(X) \coloneqq \sum_{\ell \leqslant X} \frac{\Lambda^\ell}{\ell r_\ell |\ell|_p^{s_\ell}}$$

depending only on the data $(p, \Lambda, \varpi, (r_n), (s_n))$ and the power saving in the error term is dictated by the zeros of the degree zeta function D_σ.

Finding Θ geometrically. Finding Θ can sometimes be approached geometrically, as follows. Recall that ξ_i are roots of the characteristic polynomial of σ acting on H^1 and all λ_i are products of such roots (corresponding to the characteristic polynomial of σ acting on $\mathrm{H}^i = \wedge^i \mathrm{H}^1$ for various i). Suppose that

$$|\xi_i|^2 = a \tag{42}$$

for all i and a fixed integer a. Then $\Lambda = a^g$ and $\Theta = 1 - 1/(2g)$, so we get an error term of the form $O(a^{g-1/2})$. By [30, Chapter 4, Application 2], condition (42) happens if for some polarisation on A with Rosati involution $'$, we have $\sigma\sigma' = a$ in $\mathrm{End}(A)$. In Weil's proof of the analogue of the Riemann hypothesis for abelian varieties $A/\mathbf{F}_q$, it is shown that this holds for σ the q-Frobenius with $a = q^g$.

Another expression for the main term. One may express the main term $M(X)$ as follows. For $k \in \{0, \dots, \varpi - 1\}$, define

$$F_k(\Lambda, X) = \sum_{\substack{\ell \leqslant X \\ \ell \equiv k \bmod \varpi}} \Lambda^\ell / \ell; \tag{43}$$

then

$$M(X) = \sum_{k=0}^{\varpi-1} r_k^{-1} \left(F_k(\Lambda, X) + \sum_{i \geqslant 1} p^{(s_k-1)i}(1-p^{-s_k}) \sum_{\substack{0 \leqslant k' < \varpi \\ p^i k' \equiv k \bmod \varpi}} F_{k'}\left(\Lambda^{p^i}, \left\lfloor \frac{X}{p^i} \right\rfloor\right) \right). \tag{44}$$

We collect the information in the following proposition.

Proposition 9.11. *With $M(X)$ the function defined in* (44) *using* (43)*, depending only on the data $(p, \Lambda, \varpi, (r_n), (s_n))$ (i.e., the growth rate Λ and the inseparability degree pattern), we have for integer values of X,*

$$\pi_\sigma(X) = M(X) + O(\Lambda^{\Theta X})$$

where

$$\Theta = \{\mathsf{Re}(s) : s \text{ is a zero of } D_\sigma(\Lambda^{-s})\}. \qquad \square$$

A worked example is in the introduction.

The tame case. In the tame setting, one similarly finds $\pi^*_\sigma(X) = M^*(X) + O(\Lambda^{\Theta X})$ with

$$M^*(X) = \sum_{k=0}^{\varpi-1} r_k^{-1} \left(F_k(\Lambda, X) - \frac{1}{p} \sum_{\substack{0 \leqslant k' < \varpi \\ pk' \equiv k \bmod \varpi}} F_{k'}\left(\Lambda^p, \left\lfloor \frac{X}{p} \right\rfloor\right) \right).$$

Remark 9.12. Due to its exponential growth as a function of a real variable X, it is not possible to approximate $M(\lfloor X \rfloor)$ by a continuous function with error $O(\Lambda^{\vartheta X})$ for any $\vartheta < 1$. Note that $F_k(\Lambda, X)$ can be evaluated using the Lerch transcendent.

Appendix A. Adelic perturbation of power series

ROBERT ROYALS AND THOMAS WARD

The result in this appendix comes from the thesis [35] of the first author, and arose there in connection with the following question about 'adelic perturbation' of linear recurrence sequences. Write $|m|_S = \prod_{\ell \in S} |m|_\ell$ for $m \in \mathbf{Q}$ and S a set of primes, and for an integer sequence $a = (a_n)$ define a function $f_{a,S}$ by $f_{a,S}(z) = \sum_{n=1}^{\infty} |a_n|_S a_n z^n$. If a is an integer linear recurrence sequence, does $f_{a,S}$ satisfy a Pólya–Carlson dichotomy? That is, does $f_{a,S}$ admit a natural boundary whenever it does not define a rational function? This remains open, but for certain classes of linear recurrence and for $|S| < \infty$, the following theorem is the key step in the argument.

Theorem A.1. *Let $a = (a_n)$ be an integer sequence with the property that for every prime ℓ there exist constants n_ℓ in $\mathbf{Z}_{>0}$, $(c_{\ell,i})_{i=0}^{n_\ell-1}$ in $\mathbf{Q}^{n_\ell}$, and $(e_{\ell,i})_{i=0}^{n_\ell-1}$ in $\mathbf{Z}_{\geqslant 0}^{n_\ell}$ such that $|a_n|_\ell = c_{\ell,k}|n|_\ell^{e_{\ell,k}}$ if $n \equiv k \bmod n_\ell$. Let S be a finite set of primes and write $f(z) = \sum_{n \geqslant 1} |a_n|_S z^n$. If the sequence $(|a_n|_S)$ takes infinitely many values, then f admits the unit circle as a natural boundary. Otherwise, f is a rational function.*

The method of proof is reminiscent of Mahler's, in which functional equations allow one to conclude that certain functions have singularities along a dense set of roots of unity (compare [3]).

For the proof, it is necessary to consider a slightly more general setup. Assume that S is a finite set of primes and for each $\ell \in S$ there is an associated positive integer e_ℓ, write e for the collection $(e_\ell)_{\ell \in S}$, and write $F_{S,e,r}(z) = \sum_{n \geqslant 0} |n - r|_{S,e} z^n$ for some $r \in \mathbf{Q}$, where $|n|_{S,e} = \prod_{\ell \in S} |n|_\ell^{e_\ell}$. Notice that there is always a bound of the shape

$$\frac{A}{n^B} \ll |n - r|_\ell \leqslant \max\{1, |r|_\ell\}$$

for constants $A, B > 0$, so the radius of convergence of $F_{S,e,r}$ is 1. If $|r|_\ell > 1$ for some $\ell \in S$ then $|n-r|_\ell = |r|_\ell$ for all $n \in \mathbf{N}$, and so

$$F_{S,e,r}(z) = |r|_\ell^{e_\ell} \sum_{n \geqslant 0} |n-r|_{S-\{\ell\},e} z^n = |r|_\ell^{e_\ell} F_{S-\{\ell\},e,r}(z)$$

wherever these series are defined. Thus as far as the question of a natural boundary is concerned, we may safely assume that $|r|_\ell \leqslant 1$ for all $\ell \in S$.

Now let $\ell \in S$ be fixed. Since $|r|_\ell \leqslant 1$, we can write

$$r = r_0 + r_1\ell + r_2\ell^2 + \dots$$

with $r_i \in \{0, 1, \dots, \ell-1\}$ for all $i \geqslant 0$. For $r \in \mathbf{Q}$ write $r \bmod \ell^e$ for the positive integer $r_0 + r_1\ell + \dots + r_{e-1}\ell^{e-1}$. In particular, $r \bmod \ell^e$ is the smallest non-negative integer with

$$|r - (r \bmod \ell^e)|_\ell \leqslant \ell^{-e}.$$

If $n = p_1^{e_1} \cdots p_j^{e_j}$ for distinct primes p_i, then write $r \bmod n$ for the smallest non-negative integer satisfying

$$|r - (r \bmod n)|_{p_i} \leqslant p_i^{-e_i}$$

for $i = 1, \dots, j$ (which exists by the Chinese remainder theorem).

Next we will obtain some functional equations for $F_{S,e,r}$. For $m \geqslant 0$, we write $t_m = \frac{r-(r \bmod \ell^m)}{\ell^m}$. Note that $|t_m|_p \leqslant 1$ for all $p \in S$ and $m \geqslant 0$. We claim that for any $m \geqslant 1$ we have the equality

$$F_{S,e,t_{m-1}}(z) = F_{S-\{\ell\},e,t_{m-1}}(z) + \ell^{-e_\ell} z^{r_{m-1}} F_{S,e,t_m}(z^\ell) - z^{r_{m-1}} F_{S-\{\ell\},e,t_m}(z^\ell). \tag{45}$$

Indeed, we compare directly the coefficients at z^n on both sides of this equation. The coefficient on the left is $|n - t_{m-1}|_{S,e}$. The coefficient on the right is $|n - t_{m-1}|_{S-\{\ell\},e}$ if $\ell \nmid (n - t_{m-1})$ and

$$|n - t_{m-1}|_{S-\{\ell\},e} + \ell^{-e_\ell} \left| \frac{n - r_{m-1}}{\ell} - t_m \right|_{S,e} - \left| \frac{n - r_{m-1}}{\ell} - t_m \right|_{S-\{\ell\},e}$$

otherwise. Since $\frac{n-r_{m-1}}{\ell} - t_m = \frac{n-t_{m-1}}{\ell}$ and $|\ell|_{S-\{\ell\},e} = 1$, after an easy manipulation we see that both these coefficients are equal and hence we get (45).

Combining formulæ (45) for $m = 1, \dots, s$, we obtain the equality

$$\begin{aligned} F_{S,e,r}(z) = F_{S-\{\ell\},e,r}(z) - (\ell^{e_\ell} - 1) \sum_{k=1}^{s-1} \frac{1}{\ell^{ke_\ell}} z^{r \bmod \ell^k} F_{S-\{\ell\},e,t_k}(z^{\ell^k}) \\ - \ell^{-(s-1)e_\ell} z^{r \bmod \ell^s} F_{S-\{\ell\},e,t_s}(z^{\ell^s}) + \ell^{-se_\ell} z^{r \bmod \ell^s} F_{S,e,t_s}(z^{\ell^s}). \end{aligned} \tag{46}$$

Since we have $|t_s|_p \leqslant 1$ for all $p \in S$ and $s \geqslant 0$, the coefficients in the power series $F_{S-\{\ell\},e,t_s}(z^{\ell^s})$ and $F_{S,e,t_s}(z^{\ell^s})$ are bounded by 1, and hence for $|z| < 1$ we can bound the two latter terms in (46) by

$$\begin{aligned} \left| -\ell^{-(s-1)e_\ell} z^{r \bmod \ell^s} F_{S-\{\ell\},e,t_s}(z^{\ell^s}) + \ell^{-se_\ell} z^{r \bmod \ell^s} F_{S,e,t_s}(z^{\ell^s}) \right| \\ \leqslant (\ell^{-(s-1)e_\ell} + \ell^{-se_\ell}) \sum_{n \geqslant 0} |z|^{n\ell^s}. \end{aligned}$$

Thus by passing in (46) with s to infinity, we obtain

$$F_{S,e,r}(z) = F_{S-\{\ell\},e,r}(z) - (\ell^{e_\ell} - 1) \sum_{k \geqslant 1} \frac{1}{\ell^{ke_\ell}} z^{r \bmod \ell^k} F_{S-\{\ell\},e,t_k}(z^{\ell^k}). \tag{47}$$

Lemma A.2. *Let S be a finite set of primes, $e = \{e_\ell \mid \ell \in S\}$ the associated exponents, and $n > 1$ an integer divisible by some prime $q \notin S$. Then there is a constant $c_{n,e,S} > 0$ such that for any primitive nth root of unity μ and for all $\lambda \in [0, 1)$ we have $|F_{S,e,r}(\lambda\mu)| < c_{n,e,S}$.*

The constant $c_{n,e,S}$ does not depend on r under the assumption that $|r|_\ell \leqslant 1$ for all $\ell \in S$.

Proof. We proceed by induction on the cardinality of S. For $S = \emptyset$ we have

$$F_{S,e,r}(z) = \sum_{m \geqslant 0} |m - r|_{\emptyset,e} z^m = \frac{1}{1-z},$$

and the existence of the claimed constant is clear. Now suppose that $|S| \geqslant 1$, let $p \in S$ and write

$$F_{S,e,r}(z) = F_{S-\{p\},e,r}(z) - (p^{e_p} - 1) \sum_{k \geqslant 1} \frac{1}{p^{ke_p}} z^{r \bmod p^k} F_{S-\{p\},e,t_k}(z^{p^k}).$$

So,

$$\begin{aligned} |F_{S,e,r}(z)| &\leqslant |F_{S-\{p\},e,r}(z)| \\ &\qquad + (p^{e_p} - 1) \sum_{k \geqslant 1} \frac{1}{p^{ke_p}} |z^{r \bmod p^k}| |F_{S-\{p\},e,t_k}(z^{p^k})| \\ &\leqslant (p^{e_p} - 1) \sum_{k \geqslant 0} \frac{1}{p^{ke_p}} |F_{S-\{p\},e,t_k}(z^{p^k})| \end{aligned}$$

for $|z| \leqslant 1$. If $z = \lambda\mu$ for some $\lambda \in [0,1)$ and μ is a primitive nth root of unity with $q|n$, then $z^{p^k} = \lambda'\mu'$ where $\lambda' \in [0,1)$ and μ' is a primitive n'th root of unity with $q|n'$, and n' is one of finitely many possible values. Thus by the inductive hypothesis there is a constant c with $|F_{S-\{p\},e,t_k}(z^{p^k})| < c$ for all k, and hence $|F_{S,e,r}(z)| < (p^{e_p} - 1)c\frac{p^{e_p}}{p^{e_p}-1}$. Taking this as $c_{n,e,S}$ gives the lemma. □

Lemma A.3. *Let S be a finite set of primes and let $r \in \mathbf{Q}$ be such that $|r|_p \leqslant 1$ for all $p \in S$. Suppose that $n \geqslant 1$ is an integer divisible only by primes in S, and that μ is a primitive nth root of unity. Writing $n = p_1^{f_1} \cdots p_j^{f_j}$ where $p_1, \ldots, p_j$ are distinct primes in S and $f_i \geqslant 1$ for all $i = 1, \ldots, j$, we have*

$$|F_{S,e,r}(\lambda\mu)| \longrightarrow \infty$$

as $\lambda \to 1^-$. More precisely,

$$\mathsf{Re}\big((-1)^j \mu^{-(r \bmod n)} F_{S,e,r}(\lambda\mu)\big) \longrightarrow \infty$$

as $\lambda \to 1^-$ and there exists a constant $c'_{n,e,S}$ (which does not depend on r and λ) such that

$$|\mathsf{Im}\big((-1)^j \mu^{-(r \bmod n)} F_{S,e,r}(\lambda\mu)\big)| < c'_{n,e,S}$$

and

$$\mathsf{Re}\big((-1)^j \mu^{-(r \bmod n)} F_{S,e,r}(\lambda\mu)\big) > -c'_{n,e,S}.$$

Proof. We again write $z = \lambda\mu$ and define the function $\varphi_{S,e,r,\mu}(\lambda)$ by the formula

$$\varphi_{S,e,r,\mu}(\lambda) = (-1)^j \mu^{-(r \bmod n)} F_{S,e,r}(\lambda\mu),$$

where j is the number of prime factors of n.

We proceed by induction on the number of distinct prime factors in n starting with $n = 1$. In this case $\varphi_{S,e,r,\mu}(\lambda) = \sum_{m \geqslant 0} |m - r|_{S,e} \lambda^m$ for each m, $\lambda^m \to 1^-$ as $\lambda \to 1^-$, and $|m - r|_{S,e} = 1$ infinitely often. This shows that the real part tends to infinity as $\lambda \to 1^-$ and is bounded from below by 0. The imaginary part is bounded as $F_{S,e,r}(\lambda)$ is real for all $\lambda \in [0,1)$.

Now let $p_1, \ldots, p_j \in S$ be distinct, and let $n = \prod_{i=1}^j p_i^{f_i}$ with $f_i \geqslant 1$ for all i. Let $p = p_1$ and use the variables $r_0, r_1, \ldots$ to indicate the p-adic coefficients of r and $t_0, t_1, \ldots$ to indicate the values $t_k =$

$\frac{r-r \bmod p^k}{p^k}$ for all k. Assume first that $f_1 = 1$. We will apply the functional equation (47). For all $k \geqslant 1$, μ^{p^k} is a primitive (n/p)th root of unity and the formula $t_k = \frac{r-r \bmod p^k}{p^k}$ implies that

$$r \bmod n \equiv r \bmod p^k + p^k(t_k \bmod (n/p)) \pmod n.$$

Thus Formula (47) after some manipulation gives

$$\varphi_{S,e,r,\mu}(\lambda) = \varphi_{S-\{p\},e,r,\mu}(\lambda) + (p^{e_p} - 1) \sum_{k=1}^{\infty} \frac{\lambda^{r \bmod p^k}}{p^{ke_p}} \varphi_{S-\{p\},e,t_k,\mu^{p^k}}(\lambda^{p^k}).$$

The leading term in this expression is bounded by Lemma A.2, and the inductive hypothesis applied to the terms $\varphi_{S-\{p\},e,r,\mu^{p^k}}(\lambda^{p^k})$ shows that their real part tends to $+\infty$ as $\lambda \to 1^-$ and is bounded away from $-\infty$ independently of r and λ. Since these terms appear within the geometric progression $\sum_{k=1}^{\infty} p^{-ke_p}$, we obtain that

$$\varphi_{S,e,r,\mu}(\lambda) \to \infty$$

as $\lambda \to 1^-$ and the same argument proves the latter claim. This proves the inductive step for the case $f_1 = 1$.

We will use this as the base case for a second inductive proof for $f_1 > 1$. The argument in this case is similar except that we will use the functional equation (45) instead of (47). As before, μ^p is a primitive (n/p)th root of unity and

$$r \bmod n \equiv r \bmod p + p(t_1 \bmod (n/p)) \pmod n.$$

Thus Formula (45) after some manipulation gives

$$\varphi_{S,e,r,\mu}(\lambda) = \varphi_{S-\{p\},e,r,\mu}(\lambda) + p^{-e_p}\lambda^{r \bmod p}\varphi_{S,e,t_1,\mu^p}(\lambda^p) - \lambda^{r \bmod p}\varphi_{S-\{p\},e,t_1,\mu^p}(\lambda^p).$$

The first and the third terms in this expression are bounded by Lemma A.2, and hence the claim follows immediately from the inductive hypothesis applied to the term $\varphi_{S,e,t_1,\mu^p}(\lambda^p)$. This concludes the induction. □

Proof of Theorem A.1. If $c_{\ell,k} = 0$ for some $\ell \in S$ and k we will automatically take $e_{\ell,k} = 0$ as the power of $|n|_\ell$ plays no role. Another case we wish to avoid is if for some ℓ and $k \in \{0, 1, \ldots, n_\ell - 1\}$, the value $|n|_\ell$ is constant for all $n \equiv k \bmod n_\ell$. Writing v_ℓ for the ℓ-adic order, this happens exactly when $v_\ell(n_\ell) > v_\ell(k)$, and in this case $|n|_\ell = |k|_\ell$. If this is the case and $e_{\ell,k} \neq 0$, then we will set $e_{\ell,k} = 0$ and substitute $c_{\ell,k}|k|_\ell^{e_{\ell,k}}$ for $c_{\ell,k}$. Let $N = \operatorname{lcm}\{n_p \mid p \in S\}$. For each $j \in \{0, 1, \ldots, N-1\}$ consider the value of $|a_n|_S$ when $n \equiv j \bmod N$. For each p, $n \equiv j \bmod N$ and thus $n \equiv j \bmod n_p$ as $n_p | N$. Let $k_{p,j}$ be the unique element of $\{0, 1, \ldots, n_p - 1\}$ such that $k_{p,j} \equiv j \bmod n_p$. So

$$|a_n|_S = \prod_{p \in S} |a_n|_p = \prod_{p \in S} c_{p,k_{p,j}} |n|_p^{e_{p,k_{p,j}}}$$

as $n \equiv j \equiv k_{p,j} \bmod n_p$ for all $p \in S$. If for any nonzero n with $n \equiv j \bmod N$ we have $|a_n|_S = 0$, or equivalently $a_n = 0$, we define $S_j = \emptyset$ and $d_j = 0$. If this is the case, then it follows that for this value n

$$0 = \prod_{p \in S} c_{p,k_{p,j}} |n|_p^{e_{p,k_{p,j}}}$$

and $|n|_p^{e_{p,k_{p,j}}} \neq 0$ implies that $c_{p,k_{p,j}} = 0$ for some $p \in S$. This in turn implies that $|a_m|_S = 0$ and hence $a_m = 0$ for any $m \equiv j \bmod N$. If, on the other hand, for some $n \equiv j \bmod N$ we have $|a_n|_S \neq 0$ then for all $m \equiv j \bmod N$ we have $|a_m|_S \neq 0$ and hence $c_{p,k_{p,j}} \neq 0$ for all $p \in S$. If for a prime $p \in S$ we have $v_p(N) > v_p(j)$, then for all $n \equiv j \bmod N$ we have $|n|_p = |j|_p$. We will split S into the disjoint union $S_j \sqcup S'_j \sqcup S''_j$, where

$$S_j = \{p \in S \mid v_p(N) \leqslant v_p(j) \text{ and } e_{p,k_{p,j}} \neq 0\},$$

$$S'_j = \{p \in S \mid v_p(N) > v_p(j) \text{ and } e_{p,k_{p,j}} \neq 0\},$$

and

$$S_j'' = \{p \in S \mid v_p(N) > v_p(j) \text{ and } e_{p,k_{p,j}} = 0\}.$$

Thus for all $n \equiv j \bmod N$ we have

$$|a_n|_S = \prod_{p \in S} c_{p,k_{p,j}} \cdot \prod_{p \in S_j'} |j|_p^{e_{p,k_{p,j}}} \cdot |n|_{S_j, e^{(j)}},$$

where $e^{(j)}$ denotes the collection of exponents $\{e_{p,k_j} \mid p \in S_j\}$. Set

$$d_j = \prod_{p \in S} c_{p,k_{p,j}} \cdot \prod_{p \in S_j'} |j|_p^{e_{p,k_{p,j}}}$$

and $|a_n|_S = d_j |n|_{S_j, e^{(j)}}$ for all $n \equiv j \bmod N$.

Assume that the sequence $(|a_n|_S)$ takes infinitely many values. This implies that there exists some j for which S_j is non-empty. By our assumption, for such j we have $d_j \neq 0$. Consider the family of sets $\{S_j \mid 0 \leqslant j < N\}$, partially ordered by inclusion. Since it is finite and the S_j are not all empty, there is a non-empty maximal element S_{j_0}. Write

$$f(z) = \sum_{n=1}^{\infty} |a_n|_S z^n = \sum_{j=0}^{N-1} \sum_{n \equiv j\,(N)} |a_n|_S z^n = \sum_{j=0}^{N-1} f_j(z)$$

where

$$f_j(z) = \sum_{n \equiv j\,(N)} |a_n|_S z^n = \sum_{n \equiv j\,(N)} d_j |n|_{S_j, e^{(j)}} z^n = \sum_{k=0}^{\infty} d_j |kN + j|_{S_j, e^{(j)}} z^{kN+j}$$

$$= d_j |N|_{S_j, e^{(j)}} \sum_{k=0}^{\infty} |k + j/N|_{S_j, e^{(j)}} z^{kN+j} = d_j |N|_{S_j, e^{(j)}} z^j g_j(z^N)$$

with $g_j(z) = F_{S_j, e^{(j)}, -j/N}(z)$. Thus $f = h_1 + h_2$, where h_1 is the sum of the f_j with $S_j = S_{j_0}$ and h_2 is the sum of the f_j with $S_j \neq S_{j_0}$. Let $n = \prod_{q \in S_{j_0}} q^{f_q}$ be an integer divisible by every prime in S_{j_0} and by no other primes such that for each $q \in S_{j_0}$ we have $f_q > v_q(N)$ and let μ be a primitive nth root of unity. If j with $0 \leqslant j < N$ has $S_j \neq S_{j_0}$ then $f_j(\lambda\mu) = d_j |N|_{S_j, e^{(j)}} (\lambda\mu)^j g_j(\lambda^N \mu^N)$ is bounded as $\lambda \to 1^-$ by Lemma A.2 as μ^N is an $\frac{n}{N}$th root of unity and $\frac{n}{N}$ is divisible by every prime in S_{j_0} and hence by some prime not in S_j by maximality of S_{j_0}. Thus $|h_2(\lambda\mu)|$ is bounded as $\lambda \to 1^-$. Suppose instead that $S_j = S_{j_0}$. By Lemma A.3 we have that

$$\mathsf{Re}\big((-1)^m (\mu^N)^{-(-j/N \bmod n/N)} g_j(z^N)\big) \longrightarrow \infty$$

as $\lambda \to 1^-$ where $m = |S_{j_0}|$. Equivalently,

$$\mathsf{Re}\big((-1)^m \mu^{(j \bmod n)} g_j(z^N)\big) \longrightarrow \infty,$$

and thus

$$\mathsf{Re}\big((-1)^m z^j g_j(z^N)\big) \longrightarrow \infty$$

as $\lambda \to 1^-$. As the real part of every term in $h_1(z)$ goes to ∞, this means that

$$\mathsf{Re}\big((-1)^m f(\lambda\mu)\big) \longrightarrow \infty$$

as $\lambda \to 1^-$. Since this is true for any μ that is a ($\prod_{q \in S_{j_0}} q^{f_q}$)th root of unity with each $f_q > v_q(N)$, these singularities form a dense set on the unit circle. It follows that f admits a natural boundary on the unit circle.

For the second part of the theorem, assume that the sequence $(|a_n|_S)$ takes only finitely many values. Then $(|a_n|_S)$ is periodic modulo N, and thus

$$f(z) = \sum_{j=1}^{N} \sum_{n \equiv j\ (N)} |a_j|_S z^n = \sum_{j=1}^{N} |a_j|_S \sum_{m=0}^{\infty} z^{mN+j} = \sum_{j=1}^{N} |a_j|_S \frac{z^j}{1-z^N},$$

completing the proof. □

Appendix author information:

Ziff Building, University of Leeds, Leeds LS2 9JT, UK
E-mail address: t.b.ward@leeds.ac.uk

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK
E-mail address: aradesh@gmail.com

References

1. Michael Artin and Barry C. Mazur, *On periodic points*, Ann. of Math. (2) **81** (1965), 82–99.
2. Michael Baake, Eike Lau, and Vytautas Paskunas, *A note on the dynamical zeta function of general toral endomorphisms*, Monatsh. Math. **161** (2010), no. 1, 33–42.
3. Jason P. Bell, Michael Coons, and Eric Rowland, *The rational-transcendental dichotomy of Mahler functions*, J. Integer Seq. **16** (2013), no. 2, Article 13.2.10, 11.
4. Jason P. Bell and Stefan Gerhold, *On the positivity set of a linear recurrence sequence*, Israel J. Math. **157** (2007), 333–345.
5. Jason P. Bell, Richard Miles, and Thomas Ward, *Towards a Pólya-Carlson dichotomy for algebraic dynamics*, Indag. Math. (N.S.) **25** (2014), no. 4, 652–668.
6. Abdelaziz Bellagh and Jean-Paul Bézivin, *Quotients de suites holonomes*, Ann. Fac. Sci. Toulouse Math. (6) **20** (2011), no. 1, 135–166.
7. Giancarlo Benettin, Andrea Carati, Luigi Galgani, and Antonio Giorgilli, *The Fermi-Pasta-Ulam problem and the metastability perspective*, The Fermi-Pasta-Ulam problem, Lecture Notes in Phys., vol. 728, Springer, Berlin, 2008, pp. 152–189.
8. Andrew Bridy, *Transcendence of the Artin-Mazur zeta function for polynomial maps of* $\mathbb{A}^1(\overline{\mathbb{F}}_p)$, Acta Arith. **156** (2012), no. 3, 293–300.
9. Andrew Bridy, *The Artin-Mazur zeta function of a dynamically affine rational map in positive characteristic*, J. Théor. Nombres Bordeaux **28** (2016), no. 2, 301–324.
10. Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. (= Abh. Math. Sem. Univ. Hamburg) **14** (1941), 197–272.
11. The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 8.0)*, 2017, http://www.sagemath.org.
12. Vesselin Dimitrov, *A note on a generalization of the Hadamard quotient theorem*, preprint, arxiv:1309.1920 (2013).
13. Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.
14. Graham Everest, Richard Miles, Shaun Stevens, and Thomas Ward, *Orbit-counting in non-hyperbolic dynamical systems*, J. Reine Angew. Math. **608** (2007), 155–182.
15. Graham Everest, Victoria S. Stangoe, and Thomas Ward, *Orbit counting with an isometric direction*, in: Algebraic and topological dynamics, Contemp. Math., vol. 385, Amer. Math. Soc., Providence, RI, 2005, pp. 293–302.
16. Philippe Flajolet, Stefan Gerhold, and Bruno Salvy, *On the non-holonomic character of logarithms, powers, and the nth prime function*, Electron. J. Combin. **11** (2004/06), no. 2, Article 2, 16.
17. David Freeman and Kristin Lauter, *Computing endomorphism rings of Jacobians of genus 2 curves over finite fields*, in: Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 29–66.
18. Shmuel Friedland, *Entropy of polynomial and rational maps*, Ann. of Math. (2) **133** (1991), no. 2, 359–368.
19. Alexander O. Gel'fond, *Transcendental and algebraic numbers*, Translated from the first Russian edition by Leo F. Boron, Dover Publications, Inc., New York, 1960.
20. Eyal Z. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Series, vol. 14, American Mathematical Society, Providence, RI, 2002.
21. Nathan Grieve, *Reduced norms and the Riemann-Roch theorem for Abelian varieties*, New York J. Math. **23** (2017), no. 3, 1087–1110.
22. Alexander Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki, Vol. 9, Exp. No. 279, Soc. Math. France, Paris, 1995 (1965), pp. 41–55.

23. William A. Harris, Jr. and Yasutaka Sibuya, *The reciprocals of solutions of linear ordinary differential equations*, Adv. in Math. **58** (1985), no. 2, 119–132.
24. Aimo Hinkkanen, *Zeta functions of rational functions are rational*, Ann. Acad. Sci. Fenn. Ser. A I Math. **19** (1994), no. 1, 3–10.
25. Gerhard Knieper, *On the asymptotic geometry of nonpositively curved manifolds*, Geom. Funct. Anal. **7** (1997), no. 4, 755–782.
26. Tsit Yuen Lam, *A first course in noncommutative rings*, Graduate Texts Math., vol. 131, Springer, New York, 1991.
27. The LMFDB Collaboration, *The L-functions and Modular Forms Database,* Home page of the abelian variety isogeny class 2.5.a_a over $\mathbf{F}_5$, online, accessed 22 Oct 2017, `www.lmfdb.org/Variety/Abelian/Fq/2/5/a_a`.
28. James S. Milne, *Abelian varieties (v2.00)*, 2008, Available at www.jmilne.org/math, 172 pp.
29. James S. Milne, *Lectures on etale cohomology (v2.21)*, 2013, Available at www.jmilne.org/math, 202 pp.
30. David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, corrected reprint of the second edition, Hindustan Book Agency, New Delhi, 2008.
31. Peter Norman and Frans Oort, *Moduli of abelian varieties*, Ann. of Math. (2) **112** (1980), no. 3, 413–439.
32. William Parry and Mark Pollicott, *An analogue of the prime number theorem for closed orbits of Axiom A flows*, Ann. of Math. (2) **118** (1983), no. 3, 573–591.
33. Mark Pollicott and Richard Sharp, *Exponential error terms for growth functions on negatively curved surfaces*, Amer. J. Math. **120** (1998), no. 5, 1019–1042.
34. Michael Rosen, *Number theory in function fields*, Graduate Texts Math., vol. 210. Springer, New York, 2002.
35. Robert Royals, *Arithmetic and dynamical systems*, 2015, Doctoral thesis, University of East Anglia, Available at https://ueaeprints.uea.ac.uk/57191 (64 pp.).
36. Robert Rumely, *Notes on van der Poorten's proof of the Hadamard quotient theorem. I, II*, Séminaire de Théorie des Nombres, Paris 1986–87, Progr. Math., vol. 75, Birkhäuser Boston, Boston, MA, 1988, pp. 349–382, 383–409.
37. Stephen Smale, *Differentiable dynamical systems*, Bull. Amer. Math. Soc. **73** (1967), 747–817.
38. Richard P. Stanley, *Differentiably finite power series*, European J. Combin. **1** (1980), no. 2, 175–188.
39. Richard P. Stanley, *Enumerative combinatorics. Volume 1*, second ed., Cambridge Studies in Adv. Math., vol. 49, Cambridge University Press, Cambridge, 2012.
40. Alfred J. van der Poorten, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sci. Paris Sér. I Math. **306** (1988), no. 3, 97–102.
41. William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.

Wydział Matematyki i Informatyki Uniwersytetu Jagiellońskiego, ul. S. Łojasiewicza 6, 30-348 Kraków, Polska
E-mail address: `jakub.byszewski@uj.edu.pl`

Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 TA Utrecht, Nederland
E-mail address: `g.cornelissen@uu.nl`