ARTIN-MAZUR ZETA FUNCTIONS IN ARITHMETIC DYNAMICS

EVAN WARNER

How should we define the zeta function of a rational map $f : \mathbb{P}^1(k) \to \mathbb{P}^1(k)$, k a field? All we need is a sequence of numbers, and it makes sense to consider the sequence $|\mathrm{Per}_n(f)|$, where

$$\mathrm{Per}_n(f) = \{x \in \mathbb{P}^1(k) : f^n(x) = x\}.$$

Then we construct a zeta function in the usual way:

$$\zeta(f;t) = \exp\left(\sum_{n=1}^{\infty} |\mathrm{Per}_n(f)| \frac{t^n}{n}\right).$$

This is a special case of an Artin-Mazur zeta function, which is defined for certain dynamical systems (and in general counts the number of *isolated* fixed points). Note that we are, as usual, *not* counting fixed points with multiplicity, which in this case would be something like the Lefschetz index. In fact, if we did count with multiplicity and $\deg f = d$, then $|\mathrm{Per}_n(f)| = d^n + 1$ for all n, and after summing the geometric series we would get

$$\zeta(f;t) = \frac{1}{(1-t)(1-dt)}.$$

In general, we at least have $|\mathrm{Per}_n(f)| \leq d^n + 1$, so the zeta function is certainly defined as a formal power series and even converges on a positive radius around the origin if k is a normed field. The usual formal manipulations give rise to an Euler product over cycles, and in particular $\zeta(f;t) \in \mathbb{Z}[[t]]$.

Over $\mathbb{C}$, these zeta functions aren't too hard to calculate:

Theorem 1 (Hinkkanen)**.** *If $f : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ has degree $d \geq 2$, then $\zeta(f;t)$ is a rational function. Specifically,*

$$\zeta(f;t) = \frac{\prod_{\substack{parabolic \\ cycles\ P}} (1 - t^{pq})^{\ell}}{(1-t)(1-dt)}.$$

□

We have to define a few things: a *parabolic fixed point* is a fixed point with multiplier exactly one, and a *parabolic cycles* is a cycle of distinct points

$$P = \{z, f(z), f^2(z), \ldots, f^{p-1}(z)\},$$

where $f^p(z) = z$ and each $y \in P$ is a parabolic fixed point of some iterate f^n. This implies that the multiplier of f^p is a primitive qth root of unity for some q, and we define ℓ to be the first nonzero index in the power series expansion of $f^{pq}(y)$ around any $y \in P$ other than the constant and linear terms.

The proof is not long or difficult, and it does not really rely on the field being $\mathbb{C}$; really, the crucial point is the following: if P is a parabolic cycle of length p,

then we have noted that for any $y \in P$, $(f^p)'(y)$ is a root of unity. There are only finitely many $z \in \mathbb{P}^1(\mathbb{C})$ such that $(f^n)'(z)$ is a root of unity, where n ranges over all positive integers. Therefore there are only finitely many parabolic cycles, so if $\zeta(f;t)$ is given by the above formula it really is a rational function.

This fails badly for, say, $k = \overline{\mathbb{F}_p}$, as every element of this field is a root of unity. In fact, we have the following conjecture:

Conjecture 2. *If $f \in \overline{\mathbb{F}_p}[t]$ is a separable polynomial, then $\zeta(f;t)$ is transcendental over $\mathbb{Q}(t)$.*

Incidentally, the "separable" criterion is really necessary: if $f \in \overline{\mathbb{F}_p}[t]$ is inseparable, then $f^n(z) - z$ has constant derivative -1 and therefore has distinct roots for every n, so $|\mathrm{Per}_n(f)| = d^n + 1$ and $\zeta(f;t) = \frac{1}{(1-t)(1-dt)}$ is a rational function by the above calculation.

This conjecture has been verified by Andrew Bridy for all *dynamically affine* maps; that is, all maps "coming from" (one-dimensional) algebraic groups. These fall into five classes in characteristic p: we have the Lattés maps, coming from an elliptic curve, the power and Chebyshev maps, coming from the multiplicative group $\mathbb{G}_m$, and additive and subadditive polynomial maps, coming from the additive group $\mathbb{G}_a$. These last two classes are special to characteristic p.

In this talk I'll go through the proof for power maps, which is the simplest case but contains all the ideas of the proof for all dynamically affine maps. We will rely heavily on the fact that the simplicity of the map implies that we can describe the sequence of numbers $|\mathrm{Per}_n(f)|$ fairly precisely.

A power map on $\mathbb{P}^1$ is always conjugate to the map $x \mapsto x^d$ and the zeta-function is conjugation invariant, so without loss of generality assume that $f(x) = x^d$.

Lemma 3.

$$|\mathrm{Per}_n(f)| = \begin{cases} 2 + |\ker(g)| & \text{if } d > 0, \\ 1 + (-1)^n + |\ker(g)| & \text{if } d < 0, \end{cases}$$

where $g : \mathbb{G}_m \to \mathbb{G}_m$ is the map $x \mapsto x^{d^n-1}$.

Proof. Essentially trivial: a point of $\mathbb{P}^1$ is either a point of $\mathbb{G}_m$ or 0 or ∞. The latter two are both fixed points of f if $d > 0$ and are swapped by f if $d < 0$. Thus in the former case we add 2 to the number of fixed points in $\mathbb{G}_m$ proper, and in the latter case we add 2 if n is even and 0 if n is odd (because only if n is even will f^n fix 0 and ∞). □

As for $|\ker(g)|$, it is easy to count using the following equality on $\mathbb{G}_m$:

$$|\ker(x \mapsto x^m)| = \frac{|m|}{p^{v_p(|m|)}}.$$

We are just counting $|m|$th roots of unity. The denominator arises because we recall that there are no nontrivial pth roots of unity in characteristic p, so we have to excise them in our count.

Here's the outline of the proof in steps. We will start by assuming that $\zeta(f;t)$ is algebraic and derive the following consequences:

(1) The sequence $(|\mathrm{Per}_n(f)|)_n$ is ℓ-automatic, where $\ell \neq p$ is a prime.
(2) The sequence $d_n = p^{v_p((\ell-1)n+1)}$ is ℓ-automatic.
(3) The sequence d_n is eventually periodic.

(4) But the sequence d_n cannot be eventually periodic, contradiction.

The main concept here is that of an ℓ-automatic sequence, which by definition is a sequence a_n produced as the output of a discrete finite automaton that takes as input the base-ℓ expansion of n. Fortunately, we will be able to use this concept as a black box, merely employing the following facts:

Theorem 4 (Christol)**.** *If $\sum a_n t^n \in \mathbb{Z}[[t]]$ is algebraic, then the sequence $(a_n \mod \ell)_n$ is ℓ-automatic for each prime ℓ.* □

This theorem follows from the following characterization of elements of $\mathbb{F}_p[[t]]$ that are algebraic over $\mathbb{F}_p(t)$: such elements are precisely those that are formal generating functions for p-automatic sequences. As an example, consider the famous Thue-Morse sequence 1001011001101001..., created by starting with 1 and at each step appending the bit flip of the current string. This sequence is 2-automatic, and its generating function Z satisfies the algebraic equation

$$Z + (1+Z)^2 t + (1+Z)^3 t^2 = 0.$$

The following theorem severely restricts the kind of sequences that can be automatic with respect to two different bases:

Theorem 5 (Cobham)**.** *If ℓ and p are multiplicatively independent positive integers and a_n is both an ℓ-automatic and a p-automatic sequence, then a_n is eventually periodic.* □

Finally, the following are easy and very believable closure properties of ℓ-automatic sequences:

Proposition 6. *The set of ℓ-automatic sequences is closed under elementwise addition, multiplication, inversion (when defined), and taking linearly-indexed subsequences (i.e. if a_n is ℓ-automatic, so is a_{bn+c} for positive integers b, c).* □

Now we can start the proof in earnest.

Step 1 is easy enough with what we know so far. If $\zeta(f;t)$ were algebraic, then its logarithmic derivative

$$\frac{\zeta'}{\zeta}(f;t) = \sum_{n \geq 1} |\mathrm{Per}_n(f)| t^{n-1}$$

certainly will be as well. Hence Christol's theorem implies that the sequence $(|\mathrm{Per}_n(f)| \mod \ell)_n$ is ℓ-automatic for any prime ℓ.

Step 2 consists of massaging our formula for $|\mathrm{Per}_n(f)|$. First, re-index by an even multiple m, letting

$$a_n = |\mathrm{Per}_{mn}(f)| \mod \ell.$$

Then the distinction between even and odd n in our formula disappears, so by previous calculation

$$a_n = 2 + \frac{d^{mn}-1}{p^{v_p(d^{mn}-1)}} \mod \ell$$

is ℓ-automatic. Now subtract two, which certainly preserves ℓ-automaticness, by the proposition:

$$b_n = \frac{d^{mn}-1}{p^{v_p(d^{mn}-1)}} \mod \ell.$$

Now we want to simplify this formula as much as possible while still retaining its ℓ-automatic character.

Claim: if $p > 2$ and if we chose m such that $d^m \equiv 1 \bmod p$, which we are certainly free to do, then

$$v_p(d^{mn} - 1) = v_p(d^m - 1) + v_p(n).$$

Proof of claim: first let's verify the case where $v_p(n) = 0$. Then

$$\frac{d^{mn} - 1}{d^m - 1} = 1 + d^m + \ldots + d^{m(n-1)}.$$

Mod p, the right hand side is equal to n, because each term is equal to 1 mod p. So if $v_p(n) = 0$, the p-valuation of the right hand side is zero, and we have $v_p(d^{mn} - 1) = v_p(d^m - 1)$ as desired. By induction, to prove the remaining cases it suffices to prove the formula when $p = n$, which will be an application of the binomial theorem. Write $d^m = z + 1$ (so, of course, $z = d^m - 1$). Then the binomial formula yields

$$d^{mp} = \sum_{i=0}^{p} \binom{p}{i} z^i.$$

The first term is equal to one and the second is equal to pz. Claim: all other terms are equal to zero modulo $p^{v_p(z)+2}$. This is clear for all $2 \leq i < p$. It is true for $i = p$ as well because $v_p(z^p) = pv_p(z) \geq v_p(z) + 2$, by the fact that $v_p(z)$ is nonzero and $p > 2$.

If $p = 2$, we repeat the above process but instead pick $m = 2$, so $d^m \equiv 1 \bmod 4$ (which is true because if d were even then $x \mapsto x^d$ would not be separable mod p, so d must be odd, so $d^2 \equiv 1 \mod 4$). Then $v_p(z) \geq 2$ in the above proof and everything goes through as before.

By the claim, we can write

$$b_n = \frac{d^{mn} - 1}{p^{v_p(d^m-1)+v_p(n)}}.$$

Now we take a further subsequence to simplify the numerator. Note that $d^{mn} - 1 \equiv d^m - 1 \bmod \ell$ whenever $n \equiv 1 \bmod \ell - 1$, by Fermat's little theorem. So take the subsequence

$$c_n = b_{(\ell-1)n+1} = \frac{d^m - 1}{p^{v_p(d^m-1)+v_p((\ell-1)n+1)}} \mod \ell.$$

(If $p = 2$ we instead take the subsequence $b_{(\ell-1)n+2}$, for reasons that will soon become clear in Step 4.) Finally, multiply by the obvious constant sequences and invert to conclude that

$$d_n = p^{v_p((\ell-1)n+1)} \mod \ell$$

is ℓ-automatic (with the aforementioned slight modification if $p = 2$).

Step 3: It is easy to show that any sequence that is a function of the equivalence class mod d of $v_p(n)$ is p-automatic; we can build a simple finite automaton by hand to output it. So if we let d be the multiplicative order of p mod ℓ, we see that d_n is p-automatic. Therefore by Cobham's theorem, d_n is eventually periodic.

Step 4: Claim: the sequence $p^{v_p(\alpha n+\beta)} \mod \ell$ is not periodic if $v_p(\alpha) \leq v_p(\beta)$. If we show the claim, we're done: if $p \neq 2$, then we just choose ℓ so that, say, $\ell \equiv 2 \bmod p$, so $v_p(\ell - 1) = v_p(1) = 0$ and the hypotheses are satisfied. If $p = 2$, then we choose $\ell \equiv 3 \mod 4$, so $v_p(\ell - 1) = v_p(2) = 1$.

Proof of claim: assume the sequence is periodic. Then for all sufficiently large n and for all x, we have

$$p^{v_p(\alpha n+\beta)} = p^{v_p(\alpha(n+xc)+\beta)} \mod \ell.$$

This implies that

$$v_p(\alpha n+\beta) = v_p(\alpha(n+xc)+\beta) \mod d,$$

where as above d is the multiplicative order of p mod ℓ. Without loss of generality, we can assume that $v_p(\alpha) = 0$, just by subtracting $v_p(\alpha)$ from both sides and bringing it inside the valuation. We have the freedom to choose n and x (so long as n is sufficiently large), and we will do this in such a way as to derive a contradiciton. First, using that α has no p-part, choose n large enough and such that

$$\alpha n \equiv -\beta + p^{v_p(c)} \mod p^{v_p(c)+2}.$$

This immediately implies that $v_p(\alpha n+\beta) = v_p(c)$. Next, again using that α has no p-part, choose x to solve the congruence

$$\alpha \frac{c}{p^{v_p(c)}} x \equiv p-1 \mod p^{v_p(c)+2}.$$

This implies that $\alpha cx \equiv p^{v_p(c)+1} - p^{v_p(c)}$ modulo the same quantity. Adding these two equivalences mod $p^{v_p(c)+2}$, we get

$$\alpha(n+cx) \equiv -\beta + p^{v_p(c)+1} \mod p^{v_p(c)+2}.$$

Taking valuations,

$$v_p(\alpha(n+cx)+\beta) = v_p(c)+1.$$

By our original assumption of eventual periodicity, the left hand side is equivalent to $v_p(\alpha n+\beta)$ mod d, and by our choice of n we know that $v_p(\alpha n+\beta) = v_p(c)$. Therefore we get

$$v_p(c) \equiv v_p(c)+1 \mod d.$$

As $d > 1$, this is a contradiction, and we're done.

References:

Allouche, J.-P. and Shallit, J., *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge University Press, 2003.

Bridy, A., *The Artin-Mazur zeta function of a dynamically affine rational map in positive characteristic*, preprint at `http://arxiv.org/abs/1306.5267`, 2013.

Bridy, A., *Transcendence of the Artin-Mazur zeta function for polynomial maps of* $\mathbb{A}^1(\overline{\mathbb{F}}_p)$, Acta Arith., 156 no. 3, 293-300, 2012.

Hinkkanen, A., *Zeta functions of rational functions are rational*, Ann. Acad. Sci. Fenn., Ser. AI Math., 19(1):3-10, 1994.