The Artin-Mazur Zeta Function of a Rational Map in Positive Characteristic

Andrew Bridy
Department of Mathematics
University of Wisconsin-Madison
bridy@math.wisc.edu

May 7, 2013
The Artin-Mazur Zeta Function

Let $X$ be a set and $f : X \to X$ be a function. The pair $(X, f)$ defines a discrete dynamical system. The Artin-Mazur zeta function of this dynamical system is defined as

$$\zeta_f(X; t) := \exp \left( \sum_{n=1}^{\infty} |\text{Fix}(f^n)| \frac{t^n}{n} \right).$$

Here $f^n$ is the $n$-fold composition of $f$ with itself and $\text{Fix}(f^n)$ is the set of fixed points of $f^n$. This zeta function keeps track of the number of periodic points of $(X, f)$ of all possible periods, and it is also given by the product formula

$$\zeta_f(X; t) = \prod_{\text{cycles } C} (1 - t^{|C|})^{-1}.$$
The Main Question

**Question**

When is $\zeta_f(X; t)$ a rational function?

Rationality of $\zeta_f$ means that a finite amount of information determines $|\text{Fix}(f^n)|$ for all $n$.

Artin and Mazur studied the case of $X$ a manifold and $f$ a diffeomorphism. In this setting there is a large class of diffeomorphisms $f$ such that $\zeta_f$ is rational (Guckenheimer, Manning). It can also be shown that $\zeta_f$ is rational when $X = \mathbb{P}^1(\mathbb{C})$ and $f$ is a rational function (Hinkkanen).
Dwork’s Theorem and Beyond

Let $X$ be a variety over $\mathbb{F}_q$ and let $f : X \to X$ be the Frobenius morphism, i.e. the $q$th power map on coordinates. Then $\text{Fix}(f^n)$ is exactly the set of $\mathbb{F}_{q^n}$-valued points of $X$. Therefore $\zeta_f(X; t) = \zeta_X(t)$, the Hasse-Weil zeta function of $X$, which is a rational function (Dwork).

**Question**

Let $X$ be a variety over $\mathbb{F}_q$ and let $f : X \to X$ be a rational map. Under what conditions on $X$ and $f$ is $\zeta_f(X; t)$ rational?

A simple case of this question that is already interesting is when $X = \mathbb{A}^1(\overline{\mathbb{F}}_q)$ or $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ and $f \in \overline{\mathbb{F}}_q[x]$ or $\overline{\mathbb{F}}_q(x)$ is a map from $X$ to itself with $\deg f \geq 2$. 
Counting Periodic Points

Let $f \in \overline{\mathbb{F}}_q(x)$, $d = \deg f \geq 2$, and regard $f$ as a map $f : \mathbb{P}^1(\overline{\mathbb{F}}_q) \to \mathbb{P}^1(\overline{\mathbb{F}}_q)$. The set $\text{Fix}(f^n)$ consists of the solutions of $f^n(x) = x$ counted without multiplicity. If we count with multiplicity, then $|\text{Fix}(f^n)| = d^n + 1$ for all $n$ and

$$
\zeta_f(X; t) = \exp \left( \sum_{n=1}^{\infty} (d^n + 1) \frac{t^n}{n} \right) = \frac{1}{(1 - t)(1 - dt)},
$$

which makes the question of rationality very uninteresting. (However, one must take care in higher dimensions, where it is not necessarily true that $\deg(f^n) = (\deg f)^n$.)
First Example: Power Maps

Let \( f(x) = x^m \) for \( m \geq 2 \), \( X = \mathbb{P}^1(\mathbb{F}_q) \), and \( p = \text{char } \mathbb{F}_q \). The set \( \text{Fix}(f^n) \) consists of \( \infty \) and the roots of \( x^{m^n} - x \). Therefore

\[
|\text{Fix}(f^n)| = \begin{cases} 
    m^n + 1 & : p \mid m \\
    \frac{m^n-1}{p^{v_p(m^n-1)}} + 2 & : p \nmid m 
\end{cases}
\]

It follows that \( \zeta_f(X; t) \) is rational when \( p \) divides \( m \). The case where \( p \nmid m \) is less clear.
Transcendence Results

Theorem (B.)

Let \( X = \mathbb{P}^1(\overline{\mathbb{F}_q}) \) and \( p = \text{char } \mathbb{F}_q \).

1. Let \( f(x) = x^m, \ m \geq 2 \). If \( p \mid m \), then \( \zeta_f(X; t) \in \mathbb{Q}(t) \). If \( p \nmid m \), then \( \zeta_f(X; t) \) is transcendental over \( \mathbb{Q}(t) \).

2. Let \( f(x) = x^{p^m} + ax, \ p \text{ odd and } a \in \mathbb{F}_{p^m}^{\times} \). Then \( \zeta_f(X; t) \) is transcendental over \( \mathbb{Q}(t) \).
By the same argument as in the above theorem, it follows that when \( p \nmid m \), the set of periodic points of \((\mathbb{P}^1(\overline{\mathbb{F}}_q), x^m)\) is not a variety. Let \( X = (\cup_{n=1}^{\infty} \text{Fix}(f^n)) \). Then

\[
\zeta_X(t) = \exp \left( \sum_{n=1}^{\infty} \frac{|X(\mathbb{F}_{q^n})|}{n} t^n \right)
\]

is not rational. By Dwork’s Theorem, \( X \) is not a variety, that is, it is not cut out by finitely many polynomial equations.
Automatic Sequences

The proof of transcendence uses tools from the theory of automatic sequences, in particular the following:

**Theorem (Christol)**

The formal power series $\sum_{n=0}^{\infty} a_n t^n \in \mathbb{F}_\ell[[t]]$ is algebraic over $\mathbb{F}_\ell(t)$ iff its coefficient sequence $(a_n)$ is $\ell$-automatic.

**Theorem (Cobham)**

Let $k$ and $\ell$ be multiplicatively independent positive integers (that is, $\log k / \log \ell \notin \mathbb{Q}$). The sequence $(a_n)$ is both $k$-automatic and $\ell$-automatic if and only if it is eventually periodic.
If \( \zeta_f(X; t) \) is algebraic, then its logarithmic derivative

\[
\frac{\zeta_f'}{\zeta_f} = \sum_{n=1}^{\infty} |\text{Fix}(f^n)| t^{n-1}
\]

is algebraic. By Christol’s theorem, for any prime \( \ell \) the sequence \(|\text{Fix}(f^n)| \pmod{\ell}\) is \( \ell \)-automatic. With some work it can be shown that the sequence is \( p \)-automatic. For a suitable choice of \( \ell \), Cobham’s theorem produces a contradiction.
Another Example: Lattès Maps

A rational map \( f : \mathbb{P}^1 \to \mathbb{P}^1 \) with \( \deg f \geq 2 \) is a Lattès map if there exist an elliptic curve \( E \), a morphism \( \psi : E \to E \), and a finite separable cover \( \pi : E \to \mathbb{P}^1 \) such that the following diagram commutes.

\[
\begin{array}{ccc}
E & \xrightarrow{\psi} & E \\
\downarrow{\pi} & & \downarrow{\pi} \\
\mathbb{P}^1 & \xrightarrow{f} & \mathbb{P}^1
\end{array}
\]

Lattès maps enjoy many special dynamical properties. For example, any Lattès map is postcritically finite, and over \( \mathbb{C} \), its Julia set is all of \( \mathbb{P}^1(\mathbb{C}) \).
Another Transcendence Result

Theorem (B.)

Let $f : \mathbb{P}^1(\overline{F}_q) \to \mathbb{P}^1(\overline{F}_q)$ be a Lattès map.

1. If $f$ is inseparable, then $\zeta_f(\mathbb{P}^1(\overline{F}_q); t) \in \mathbb{Q}(t)$.
2. If $f$ is separable, then $\zeta_f(\mathbb{P}^1(\overline{F}_q); t)$ is transcendental.
Ingredients in the Proof

- The map $\pi : E \to \mathbb{P}^1$ factors as $\pi : E \to E/\Gamma \cong \mathbb{P}^1$ for a nontrivial subgroup $\Gamma \subseteq \text{Aut}(E)$ (Milnor, Ghioca-Zieve). There are only finitely many possibilities for $\text{Aut}(E)$.
- The solutions in $\mathbb{P}^1$ of $f^n(x) = x$ can be determined from the solutions in $E$ of $\psi^n(P) = \gamma(P)$ for $\gamma \in \Gamma$.
- The size of $\ker(\psi^n - \gamma)$ is the separable degree of $\psi^n - \gamma$, which can be determined from the arithmetic of $\text{End}(E)$. The ring $\text{End}(E)$ is isomorphic to either an order in an imaginary quadratic field or a maximal order in a quaternion algebra (Deuring).
A Unified Conjecture

The above theorems suggest the following dichotomy:

Conjecture

If \( f : \mathbb{P}^1(\overline{\mathbb{F}}_q) \to \mathbb{P}^1(\overline{\mathbb{F}}_q) \) ia a rational map, \( \zeta_f(\mathbb{P}^1(\overline{\mathbb{F}}_q); t) \) is

- rational if \( f \) is inseparable
- transcendental if \( f \) is separable

The inseparable case is much more general than Dwork’s theorem. Consider rational maps such as

\[
f(x) = \frac{x^{3p} + 5x^{2p} + x^p}{x^{4p} + 1}
\]
Testing Rationality

Given the first $N$ terms of the sequence $a_n = |\text{Fix}(f^n)|$, how do we test whether $\zeta$ is rational?

**Proposition**

If $\exp(\sum_{n \geq 1} a_n t^n/n)$ is rational, the sequence $(a_n)$ satisfies a linear recurrence relation with constant coefficients.

One approach is to reduce $a_n \mod \ell$ for a large prime $\ell$ and use the Berlekamp-Massey algorithm to determine the shortest linear recurrence that outputs $(a_1, \ldots, a_N) \mod \ell$. If its length stays bounded as $N$ increases, with any luck $\zeta$ is rational.
How do we compute $|\text{Fix}(f^n)|$? In principle, this is done by factoring $f^n(x) - x$, but this becomes slow as the degree grows exponentially in $n$. Storing large polynomials in memory is already a problem for many computer algebra systems...

Another approach is to hunt for $n$-cycles directly in finite fields. Here the size of the field needed is not entirely obvious, and grows superexponentially in $n$ on average (Dixon-Panario).
Some Further Questions

- The rational maps considered in the above theorems are strongly related to group homomorphisms (they are \textit{dynamically affine} in the sense of Silverman), so they are very special among rational maps. What is the nature of \( \zeta_f(\mathbb{P}^1(\overline{\mathbb{F}}_q); t) \) for a randomly chosen rational function? What about \( f(x) = x^2 + 1 \) (\( p \) odd)?

- All \( f \in \mathbb{F}_q(x) \) commute with \( \phi(x) = x^q \), so their periodic points have additional Galois structure, that is, \( \phi \) permutes the points of period \( n \). Could a “mixed zeta function” correctly capture this structure?
The Artin-Mazur Zeta Function of a Rational Map in Positive Characteristic

Andrew Bridy
Department of Mathematics
University of Wisconsin-Madison
bridy@math.wisc.edu

May 7, 2013