ARITHMETIC DYNAMICS

NATHAN SHKOLNIK

Abstract. We look at general theory behind dynamic systems of rational functions as well as the height function on Diophantine equations. Then from those definitions we look at integer points in orbits of rational functions. Then we look at a way to approximate the amount of periodic points on elliptic curves as well as the entropy of transformations on said elliptic curves.

1. Introduction

Arithmetic dynamics combines the study of dynamical systems and the study of Diophantine equations to study the arithmetic properties of certain dynamical systems. To begin to understand dynamical systems we will need to define such a system.

Definition 1.1. *We call the pair (K, φ) a* dynamical system *where φ will be a rational map and K a field of numbers.*

Suppose we have a function $\varphi : S \to S$ where S is any set then we define $\varphi^n(P)$ of a point $P \in S$ to be

$$\varphi^n(P) := \varphi \cdot \varphi \cdot \cdots \cdot \varphi \cdot \varphi(P)$$

where we iterate φ n times The orbit $\mathcal{O}_\varphi(x) = \{x, \varphi(x), \varphi^2(x), \dots \varphi^n(x)\}$ We say x is *preperiodic* if $\mathcal{O}_\varphi(x)$ is finite. We call x *periodic* if x appears more than once in $\mathcal{O}_\varphi(x)$ Let x be a periodic point. The *period* of x is n where $\varphi^n(x) = x$. The multiplier of a function φ at a periodic point a is the value λ_a such that

$$\lambda_a(\varphi) = (\varphi^n)'(x)$$

we call λ_a superattracing if it equals 0, attracting is it's norm is less than one, neutral if it is of norm one and repelling in if it's norm is grater than one.
We will put a topology on the complex projective line $\mathbb{P}^{1\!\!\not\!K}(\mathbb{C})$ with the chordal metric.

$$\rho_{ch}(z, w) := \frac{|z - w|}{\sqrt{|z^2| + 1}\sqrt{|w^2| + 1}} = \frac{1}{2}|z^* - w^*|$$

We call a function equicontinous if for every $\varepsilon > 0$ there exists a $\delta > 0$ such that if

$$\rho_{ch}(a, b) < \delta \text{ then } \rho_{ch}(\varphi^{(n)}a, \varphi^{(n)}(b)) \text{for all n} \geq 0$$

The Fatou set, $\mathcal{F}(\varphi)$ of a function φ is the largest open subset of $\mathbb{P}^1(\mathbb{C})$ such that φ is equicontinous on every point in $\mathcal{F}(\varphi)$. The Julia set is the complement of the Fatou set. The points in the Julia set behave *chaotically*.

Example: Let $\varphi(z) = z^d$ for some d ≥ 2. Then the Julia set is the unit circle in $\mathbb{C}$, or

$$\mathcal{J}(\varphi) = \{z \in \mathbb{C} : |z| = 1\}$$

Date: Dec 2023.

Proof. First we show that $S^1 \subset \mathcal{J}(\varphi)$. Since, if a $\notin S^1$, then there is a neighborhood U of a such that $\lim_{n\to\infty} \varphi^{(n)}(U)$ converges to 0 or ∞. Therefore $S^1 \subset \mathcal{J}(\varphi)$. If $a \in S^1$ then there exists a neighborhood that goes to 0 and part that goes to ∞. Therefore S^1 is the Julia set of φ □

Height Functions: Let B $\in \bar{\mathbb{Q}}$. The define

$$F_B(X) = a_0X^d + a_1x^{d-1} \cdots + a_d \in \mathbb{Z}X \text{ where } \gcd(a_0..a_d) = 1$$

Then factor $F_B(X) = (X - B_1)(X - B_2) \dots (X - B_d)$. The absolute multiplicative height of $F_B(X)$ is

$$F_B(X) = (|a_0| \prod_{i=1}^{d} \max\{1, |B_i|\})^{1/d}$$

The absolute logarithmic height is defined to be

$$h(B) = \log(H(B))$$

Theorem 1.2. *Let $\varphi(x)$ be a rational function of degree d≥ 1. Then*

$$h(\varphi(B)) = dh(B) + O(1) \text{ for all } B \in \mathbb{P}^1(\bar{\mathbb{Q}})$$

For all $C > 0$ and $D > 0$ the set

$$\{B \in \mathbb{P}^1(\bar{\mathbb{Q}}) : h(B) \leq C and [\mathbb{Q}(\mathbb{B}) : \mathbb{Q}] \leq D\}$$

A subset U $\subset \mathbb{P}^1(\mathbb{C})$ is completely invariant with respect to φ if $\varphi(U) = U = \varphi^{-1}(U)$

Theorem 1.3. *Let $\varphi(z)$ be a polynomial of degree $d \geq 2$with complex coefficients.*

We will briefly touch on the subject of hantine approximation which asks how close can we get a rational number $\frac{a}{b} \in \mathbb{Q}$ to a number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$

Proposition 1.4. *Let $\beta \in \mathbb{R} \setminus \mathbb{Q}$ then there are infinitely many rational numbers such $\frac{a}{b} \in \mathbb{Q}$ such that*

$$|\frac{a}{b} - \beta| \leq \frac{1}{b^2}$$

.

However, a theorem by Roth shows that this is about as good as we could do.

Theorem 1.5. *Let $\beta \in \bar{\mathbb{Q}} \setminus \mathbb{Q}$ and let $\varepsilon > 0$ then there is a constant c such that*

$$\frac{a}{b} - \beta| \geq \frac{c}{b^{2+\varepsilon}} for \text{ all } \frac{a}{b} \in \mathbb{Q}$$

Theorem 1.6. *Let K be a field and let $\varphi(z) \in K(z)$ be a rational function within degree $d \geq 2$ then the set of of preperiodic points of φ, PrePer(φ) is a set of bounded height.*

Proof. Theorem 1.6 implies that there exists a constant C such that

$$h(\varphi(\alpha)) \geq dh(\alpha) - C$$

Applying this inequality to $\varphi^1 \dots \varphi^n$ we get

$$h(\varphi^2(\alpha)) \geq d^2h(\alpha) - (d + 1)C$$
$$h(\varphi^3(\alpha)) \geq d^3h(\alpha) - (d^2 + d + 1)C$$
$$\vdots$$

$$h(\varphi^n(\alpha)) \geq d^n h(\alpha) - (d^{n-1} + \cdots + d + 1)C$$

we can rewrite

$$d^{n-1} + \cdots + d + 1 = \frac{d^n - 1}{d-1} \leq \frac{d^n}{d-1}$$

which implies, after dividing by d^n that

$$\frac{C}{d-1} \geq h(\alpha) - \frac{1}{d^n} h(\varphi^n(a)) \quad (1)$$

Now suppose that we have a point $\beta \in \text{PrePer}(\varphi)$ such that

$$\varphi^{i+n}(\beta) = \varphi^i(\beta) \text{ for some n}\geq 1 \text{ and } i \geq 0$$

We substitute $\alpha = \varphi^i(\beta)$ into (1) to get

$$\frac{C}{d-1} \geq h(\varphi^i(\beta)) - \frac{1}{d^n} h(\varphi^{i+n}(\beta)) = (1 - \frac{1}{d^n}) h(\varphi^i(\beta))$$

Which mans that $h(\varphi(\beta)$ is bounded by $\frac{Cd}{(d-1)^2}$ Finally, substituting $\beta = \alpha$ and n = i into (1) gives us

$$\frac{C}{d-1} \geq h(\beta) - \frac{1}{d^i} h(\varphi^i(\alpha))$$

Therefore

$$h(\beta) \leq \frac{C}{d-1} + h(\varphi^i(\beta)) \leq \frac{C}{d-1} + \frac{Cd}{(d-1)^2} = \frac{(2d-1)C}{(d-1)^2}$$

which shows that preperiodic points of φ have a height bounded by a constant that depends only on φ Then, by the second part of theorem 1, since PrePer(φ, K) is a set of bounded height, it is finite. □

2. Canonical Height

There ares cases where we want to modify the height such that $h(\alpha) = dh(\alpha)$ without the addition of a constant. So we define it as the following:

Definition 2.1. *Le $\varphi(z) \in \bar{\mathbb{Q}}$ be a function of degree $d \geq 2$. The for any $\beta \in \mathbb{P}^1(\bar{\mathbb{Q}})$ we define*

$$\hat{h}_\varphi(\beta) = \lim_{n\to\infty} \frac{1}{d^n} h(\varphi^n(\beta))$$

Theorem 2.2. *$\hat{h}$ as defined above has the following properties:*
(a)

$$\hat{h}_\varphi(\beta) = h(\beta) + O(1)$$

(b)

$$\hat{h}_\varphi(\varphi(\beta)) = d\hat{h}_\varphi(\beta)$$

(c)

$$\hat{h}_\varphi(\beta) \geq 0 \textit{and is only equal to 0 if and only if } \beta \textit{ is preperiodic point of } \varphi$$

Proof. (a) By (1) we know that

$$\frac{C}{d-1} \geq |h(\beta) - \frac{1}{d^n} h(\varphi^n(\beta))|$$

letting $n \to \infty$ we get

$$|\hat{h}_\varphi(\beta) - h(\beta)| \leq \frac{C}{d-1}|$$

(b)This follows directly from the definition $\hat{h}$ (c) $\hat{h}_\varphi(\beta) \geq 0$ since it is the limit of non negative quantities. Furthermore, since $h(\varphi^n(\beta))$ takes on only a finite number of quantities as $n \to \infty$ when β is preperiodic, by the limit definition, $\hat{h}_\varphi = 0$ when β is preperiodic. Suppose now that $\beta \in \mathbb{P}^1(K)$ with $\hat{h}(\beta) = 0$ then

$$h(\varphi^n(\beta)) = \hat{h}_\varphi(\varphi^n(\beta)) + C = d^n \hat{h}(\beta) + C = C$$

therefore the points in $\mathcal{O}_\varphi(\beta)$ have bounded height. Letting $\varphi(z) \in K(z)$, $\mathcal{O}_\varphi(\beta)$ is contained in $\mathbb{P}^1(K)$. By the second part of theorem 1, $\mathcal{O}$ is finite and therefore β is preperiodic. □

3. Integer points in orbits

A natural question to [1] ask, given a rational function of degree d≥ 2 and $\beta \in \mathbb{P}(K)$, is how many integer points $(O)_\varphi(\beta)$ can contain. Obviously, if φ us a a polynomial the answer is an infinite amount. However, even if we don't consider polynomials there are still rational functions with an infinite number of integers in their orbit. In many of these cases we have that φ^n is a polynomial, but if this happens, that means that $\varphi^2(\alpha)$ is already a polynomial.

Proposition 3.1. *Let $\varphi(z) \in \mathbb{C}(z)$ be a rational function of degree d, and suppose that $\varphi^n(z)$ is a polynomial for some n. Then either*

$$\varphi(z) \in \mathbb{C}[z]$$

or

$$\varphi^2(z) \in \mathbb{C}[z], \textit{and there exists a linear function } f = az+b \textit{ such that } \varphi^f(z) = z^{-d}$$

Proof. If $\varphi^n(z)$ is a polynomial that implies that $(\varphi^n)^{-1}(\infty)$ consists of the single point at ∞. Let

$$\varphi^i(\infty) = a_i \text{ for i} \leq n$$

and let m be the smallest integer such that $\varphi^m(\infty) = \infty$ so, $a_o \cdots a_m$ are distinct points. Applying the Reiman-Hurwitz formula* we get

$$\begin{aligned} 2d - 2 &= \sum_{\beta \in \mathbb{P}^1(\mathbb{C})} (e_\beta(\varphi) - 1) \\ &\geq \sum_{i=0}^{m-1} (e_{a_1}(\varphi) - 1) \\ &= m(d-1) \end{aligned}$$

Thus, m ≤ 2. Now there are two cases where m=1 and therefore φ is a polynomial. The other case is that m = 2, which means $a_0 = a_2 = \infty$ and $a_1 \neq \infty$. Conjugating $\varphi(z)$ by $f(z) = z + a_1$, we may assume that$a_1 = 0$. Therefore $\varphi^-1(0) = \infty$ and $\varphi^{-1}(\infty) = 0$. The

[1]Proof in [Sil07] theorem 1.1

only rational function of degree d that behave like this are of the form$g(z) = az^{-d}$ and conjugating by f(z) =$a^{1/(d+1)}z$ puts g in the for z^{-d} □

This proposition hints at the following result.

Theorem 3.2. *Let $\varphi(z) \in \mathbb{Q}(z)$ be a rational map such that $\varphi^2(z)$ is not a polynomial and let $a \in \mathbb{P}^1(\mathbb{Q})$ Then*

$$\mathcal{O}_\varphi(a) \cap \mathbb{Z}$$

is a finite set.

In fact, there is a stronger theorem.

Theorem 3.3. *Let φ be a rational map with φ^2 not a polynomial and a wandering point $\alpha \in \mathbb{P}^1(\mathbb{Q})$ For all $n \geq 0$,write*

$$\varphi^n(\alpha) = \frac{a_n}{b_n} \in \mathbb{Q}$$

as a fraction in lowest terms. Then

$$\lim_{n\to\infty} \frac{a_n}{b_n} = 1$$

This means that as n increases, the number of digits in the denominator is the same as the number of digits in the numerator.

Proof. Let $\varepsilon > 0$. We need to show that only finitely many points satisfy

$$|b_n| \leq |a_n|^{1-\varepsilon}$$

Such points satisfy $|a_n| \geq |b_n|$, so

$$H(\varphi^n(a)) := max\{|a_n, b_n\} = |a_n|$$

Where H is the multiplicative height. We can now write that

$$\varphi^n(a) \geq H(\varphi^n(a))^\varepsilon$$

Using the chordal metric and the fact that H($\varphi^n(a) \approx d^n \hat{h}_\varphi(a)$)we can make the approximate calculation that

$$\rho_{ch}(\varphi^n(a), \infty) \approx \frac{1}{|\varphi^n(a)|} \leq H(\varphi^n * (a)^{-\varepsilon} \approx e^{-\varepsilon d^n \bar{h}_\varphi(a)}$$

Since $\varphi^n(a)$ is close to ∞ the rational number $\varphi^{n-k}(a)$ should be close to an algebraic number β in the inverse image of $\varphi^{-k}(\infty)$. Let $d^k > 6/\varepsilon$ and let $\beta \in \mathbb{Q}$ be the aforementioned algebraic number. Assume for now that φ is unramified(i.e has no critical points). Unramified somewhat preserve distances ans so we can say that

$$\rho_{ch}(\varphi^{n-k}(a), \beta) \approx \rho_{ch}(\varphi^n(a), \varphi^k(\beta) = \rho_{ch}(\varphi^n(a), \infty$$

Now we compute where the C_i's are constants

$$\begin{aligned}
&\frac{1}{|a_n|^{\varepsilon}} \geq |\frac{b_n}{a_n}| \\
&= \frac{1}{\varphi^n(a)} \\
&\geq C_1 \rho_{ch}(\varphi^n(a), \infty) \\
&= C_1 \rho_{ch}(\varphi^n(a), \varphi^k(\beta)) \\
&\geq C_2 \rho_{ch}(\varphi^{n-k}, \beta) \\
&\geq C_3 |\varphi^{n-k}(a) - \beta| \\
&\geq \frac{C_4}{H(\varphi^{n-k}(a))^3} \text{ Roth's theorem with} \varepsilon = 1 \\
&\geq \frac{C_5}{H(\varphi^n(a))^{3/d^k}} \\
&= \frac{C_5}{|a_n|^{3/d^k}} \\
&\geq \frac{C_6}{|a_n|^{\varepsilon/2}} \text{ Since } d^k \geq 6/\varepsilon
\end{aligned}$$

The details and what happens at ramification points can be found in [Sil07] □

4. Dynamical Systems on Elliptic Curves

We will need a tool for this section and that is p-adic valuation and the closure of $\mathbb{Q}$ based on that metric. Under the usual $|\cdot|$ valuation $\mathbb{R}$ is the closure of $\mathbb{Q}$. We will use the p-adic valuation.

Definition 4.1. *The p-adic valuation, notated $|\cdot|_p$, of a number $n = p_1^{r_1} \cdot \ldots p_b^{r_n}$. We define $|n|_p = p^{-r_p}$ where p is the largest prime that divides n. The closure of $\mathbb{Q}$ under the metric induced my this valuation is called $\mathbb{Q}_p$*

Definition 4.2. *Let λ_p be the local height relative to the p-adic valuation. The global height $\hat{h}$ can be written as:*

$$\hat{h} = \sum_{p \leq \infty} \lambda_p(Q) for\ Q \in E(\mathbb{Q})$$

Let $E_1(\mathbb{R})$ denote the connected component of the identity. We will now consider a monic polynomial $v_n(x)$ of degree n-1 with coefficients which are real algebraic numbers:

$$v_n(x) = \prod_{nQ=\infty Q \in E_1(\mathbb{R}) \neq \infty} (x - x(Q))$$

For notational simplicity $\mathrm{Per}_n(T)$ will denote the group of a space X which consists of elements of order n under a homeomorphic transformation T. We also define q-transformation as a transformation $T_q(x) = qx \mod (1)$

Theorem 4.3. *Let $q \in \mathbb{Q}_p \setminus U$, where U is the set of unit roots in $\mathbb{Q}$ Then*

$$\log Per_n(T_q) = n log^+ |q|_p$$

Proof. First, consider $|q|_p < 1$. The as $n \to \infty, T_q^n(x) \to 0$ for all $x \in \mathbb{Z}_p$. Therefore T_q has only a preperiodic point at zero. When $|q| = 1$, $T_q(x)$ on $\mathbb{Z}_p$ is multiplication, so periodic points are solutions of $q^n x = x$. Since q is not a root of unity the only solution is q = 0.

Finally suppose that $|q|_p > 1$. If q= p^{-k} with $k > 0$. We have $T_q^n(x) = \sum_{i=0}^{n=\infty} a_{i+nk} p^i$ and the solutions of $T_q^n x = x$ are given by the p^{kn} with $a_{i+nk} = a_i$ for $1 \leq i \leq kn - 1$. Thus, both sides of the assumed equation are equal to nk log p. Suppose that $|q|_p$. Then, we can claim that for any integer $0 \leq a < p^{nk}$, there exists a unique y$\in \mathbb{Z}_p$ such that $T_q^n(a + p^{nk}y) = (a + p^{nk}y)$. This is true because the left hand side is of the form $b + q^n p^{nk} y$ for some $b \in \mathbb{Z}_p$. If we write v = $q^n p^{nk}$ for some p-adic unit v, then the equation b+vy $= a + p^{nk}y$ has a unique solution for y $\in \mathbb{Z}_p$. This shows that there are at least p^{nk} solutions to $T_q^n x = x$. There can't be anymore because if we can take a to be the coset representative of $\mathbb{Z}_p/p^{nk}\mathbb{Z}_p$ meaning that ever element x $\in \mathbb{Z}_p$ is represented by an a. □

Theorem 4.4. *Let T_Q be a dynamical system (T,Q) with T being a transformation and Q $\in E(\mathbb{Q})$ a non torison point. Then*

(1)

The entropy of T_Q is given by h(T_Q) = $2\hat{h}(Q)$

(2)

the asymptotic growth of periodic point is given by$\log |Per_n(T_Q)\ \log |b^n v_n(q)|$*as* $n \to \infty$

Proof. By theorem 4.1 in [DEMW99] the entropy of each component of T_Q is given by $\log \beta_p$ where $\beta_p = \beta$ if $p = \infty$ and $\beta_p = 2\lambda_p(Q)$ if p is finite. Applying theorem 4.23 in [Wal82]

$$h(T_Q) = h(T_\beta) + \sum_{p<\infty} (h(T_q)) = 2 \sum_p \lambda_p(Q) = 2\hat{h}(Q)$$

For the growth rate, note that if dynamical systems $T_i : X_i \to X_i$ are given and the point x_i has period m in T_i for $1 \leq i \leq r$ then x_i has period m in $\Pi_i T_i$. Thus we must consider the contribution to the periodic point from each prime on their own. For a finite prime

$$\log |\mathrm{Per}_n(T_Q) = n \log^+ |q|_p = -nlog|b|_p$$

Since Q isn't a torison point we know that q is not an integer, and thus, not a root of unity. Summing over all finite primes we get a total contribution of $nlog|b|$. Considering the prime at infinity by a result from [FLP94]

$$\log |\mathrm{Per}_n(T_Q)| = n \log \beta + O(n)$$

and from the previous to statements we have that

$$\log |\mathrm{Per}|(T_Q) = nlog|b| + nlog\beta = o(n)$$

Finally, from theorem 6.24 in [EW99],

$$\log |v_n(q)| = nlog\beta + o(n)$$

From the previous two equations we get that $|b^n v_n(q)|$ is asymptotically equivalent to $\mathrm{Per}|_n(T_Q)|$. □

This gives us a way to count the size of the set consisting of points of period n under a $Q-$transformation.

References

[DEMW99] P. D'Ambros, G. Everest, R. Miles, and T. Ward. Dynamical systems arising from elliptic curves, 1999.

[EW99] Graham Everest and Thomas Ward. *Heights of polynomials and entropy in algebraic dynamics*. Universitext. London: Springer, 1999.

[FLP94] Leopold Flatto, Jeffrey C. Lagarias, and Bjorn Poonen. The zeta function of the beta transformation. *Ergodic Theory Dyn. Syst.*, 14(2):237–266, 1994.

[Sil07] J.H. Silverman. *The Arithmetic of Dynamical Systems*. Graduate Texts in Mathematics. Springer New York, 2007.

[Wal82] Peter Walters. *An introduction to ergodic theory*, volume 79 of *Grad. Texts Math.* Springer, Cham, 1982.