An arithmetic dynamical Mordell-Lang conjecture

Rafe Jones

Carleton college

August 15, 2015

Silvermania!
Warmup: squares in polynomial orbits

For a field $K$, $f \in K(x)$, and $\alpha \in K$, the orbit $O_f(\alpha)$ is $\{f^n(\alpha) : n \geq 0\}$. 
Let \( f \in \mathbb{Q}[x] \) be monic and quadratic, and let \( S \) be the set of rational squares. Suppose there is \( \alpha \in \mathbb{Q} \) such that \( O_f(\alpha) \cap S \) is infinite. What can be said about \( f \)?

Motivation:

- If \( f \in \mathbb{Q}(x) \) has degree at least two and there is \( \alpha \in \mathbb{Q} \) with \( O_f(\alpha) \cap \mathbb{Z} \) infinite, then \( f^2(x) \in \mathbb{Q}[x] \) (Silverman 1993)

- If \( f, g \in \mathbb{C}[x] \) have degree at least two and there are \( \alpha, \beta \in \mathbb{C} \) with \( O_f(\alpha) \cap O_g(\beta) \) infinite, then \( f \) and \( g \) have a common iterate (Ghioca-Tucker-Zieve 2008)
Theorem (Cahn-RJ-Spear 2015)

If \( f \in \mathbb{Q}[x] \) is monic and quadratic and \( O_f(\alpha) \cap S \) is infinite for some \( \alpha \in \mathbb{Q} \), then either

- \( f(x) = (x + c)^2 \) for some \( c \in \mathbb{Q} \), or
- \( f(x) = x^2 + 4x \).

Remarks (let \( f(x) = x^2 + 4x \)):

- \( O_f(1/2) = \{1/2, (3/2)^2, (15/4)^2, (255/16)^2, \ldots \} \)
- \( f^2(x) = (x^2 + 4x)(x + 2)^2 \)
- \( f(x) = T_2(x + 2) - 2 \), where \( T_2(x) = x^2 - 2 \). Critical orbit of \( f(x) \) is \(-2 \mapsto -4 \mapsto 0 \mapsto 0\).
- For any monic, quadratic \( f \in \mathbb{Q}[x] \) and any \( \alpha \in \mathbb{Q} \), \( \{n : f^n(\alpha) \in S\} \) is a finite union of arithmetic progressions.
Conjecture (Dynamical Mordell-Lang)

Let $X/\mathbb{C}$ be a quasi-projective variety, $V \subseteq X$ a subvariety, and $f : X \to X$ a morphism. Then for all $\alpha \in X(\mathbb{C})$, the set 
\{$n : f^n(\alpha) \in V(\mathbb{C})$\} is a finite union of arithmetic progressions.

Singletons are considered arithmetic progressions. So if 
\{$n : f^n(\alpha) \in V(\mathbb{C})$\} is finite, then the conjecture holds.
Theorem (Skolem-Mahler-Lech)

If \( F(x_0, \ldots, x_{\ell-1}) = \sum_{i=0}^{\ell-1} a_i x_i \) is a linear form on \( \mathbb{C}^\ell \) and \( a_{n+\ell} = F(a_n, \ldots, a_{n+\ell-1}) \) for all \( n \geq 0 \), then \( \{ n : a_n = 0 \} \) is a finite union of arithmetic progressions.

Special case of dynamical M-L conjecture: \( f : \mathbb{A}^\ell \to \mathbb{A}^\ell \),

\( f(x_0, \ldots, x_{\ell-1}) = (x_1, \ldots, x_{\ell-1}, F(x_0, \ldots, x_{\ell-1})) \), \( V = \{ x_0 = 0 \} \).
The dynamical M-L conjecture is known to hold for

- $X = \mathbb{A}^n$ and $f$ an automorphism of $X$ (Bell 2006)
- $X$ a semi-abelian variety (Ghioca-Tucker 2009)
- $X$ arbitrary and $f$ étale (Bell-Ghioca-Tucker 2010)
- $X = \mathbb{A}^2$ (Xie 2015)
- $X = \mathbb{A}^n$, $V$ is a curve, and $f = (f_1, \ldots, f_n)$ with $f_i \in \mathbb{C}[x]$ (Xie 2015)
From now on, $K$ is a number field.

A $K$-endomorphism of a variety $X$ is a morphism $X \to X$ defined over $K$.

**Question:** Let $X/K$ be a quasi-projective variety, $V \subset X(K)$ the value set $\lambda(X(K))$ of a $K$-endomorphism $\lambda$ of $X$, and $f$ a $K$-endomorphism of $X$. For $\alpha \in X(K)$, must $\{n : f^n(\alpha) \in V\}$ be a finite union of arithmetic progressions?
Proposition

Let $G$ be a finitely generated abelian group, $H \leq G$, and $f : G \to G$ a homomorphism. Then for any $\alpha \in G$, 
\[ \{ n : f^n(\alpha) \in H \} \] is a finite union of arithmetic progressions.

Consequence: if $X$ is an abelian variety, $f$ and $\lambda$ are isogenies on $X$, and $\alpha \in X(K)$, then 
\[ \{ n : f^n(\alpha) \in \lambda(X(K)) \} \] is a finite union of arithmetic progressions.
**Bad example:** \( K = \mathbb{Q}, X = \mathbb{A}^1, \lambda(y) = y^2, V = \{ \text{squares in } \mathbb{Q} \}, f(x) = x + 1, \alpha = 0. \)

Then \( f^n(0) = n \) for all \( n \geq 0 \), so

\[
\{ n : f^n(0) \in V \} = \{ 0, 1, 4, 9, \ldots \}.
\]
Revised Question: Let $X/K$ be a quasi-projective variety, $\lambda$ a $K$-endomorphism of $X$, $V = \lambda(X(K))$, and $f$ a sufficiently complicated $K$-endomorphism of $X$. For $\alpha \in X(K)$, must $\{n : f^n(\alpha) \in V\}$ be a finite union of arithmetic progressions?

Suppose there is $i$ with $f^i = \lambda \circ g$, where $g$ is a $K$-endomorphism of $X$.
Then for $n \geq i$, we have $f^n(\alpha) = \lambda(g(f^{n-i}(\alpha))) \in \lambda(X(K))$.

So if an iterate of $f$ has a “close functional relationship” to $\lambda$, we should expect the question to have an affirmative answer.
For $n \geq 1$, let $Z_n$ be the subvariety of $X \times X$ given by $f^n(x) = \lambda(y)$.

Then there is a natural $K$-morphism $f : Z_{n+1} \to Z_n$ taking $(x, y)$ to $(f(x), y)$. Thus if $i > j$, a point in $Z_i(K)$ maps to a point in $Z_j(K)$.

Suppose that $\{n : f^n(\alpha) \in \lambda(X(K))\}$ is infinite.

Then $Z_n(K)$ is infinite for all $n \geq 1$. 

First leap of faith: For each $n$, the infinitely many points in $Z_n(K)$ are Zariski dense in $Z_n$.

Second leap of faith: The Bombieri-Lang conjecture is true: if a variety has a Zariski-dense set of $K$-rational points, then it is not of general type (i.e. not of full Kodaira dimension). Therefore $Z_n$ is not of general type for any $n$.

Third leap of faith: Because $f$ is sufficiently complicated, the varieties $Z_n$ will be of general type for large $n$ unless some iterate of $f$ has a “close functional relationship” to $\lambda$. 
Conjecture (Arithmetic dynamical Mordell-Lang conjecture)

Let $X = (\mathbb{P}^1)^g$ and let $f = (f_1, \ldots, f_g)$ with $f_i \in K(x)$, $\deg f_i \geq 2$. Then for any $K$-endomorphism $\lambda$ of $X$ and any $\alpha \in X(K)$, the set \[ \{ n : f^n(\alpha) \in \lambda(X(K)) \} \] is a finite union of arithmetic progressions.

If $\lambda = (\lambda_1, \ldots, \lambda_g)$ with $\lambda_i \in K(x)$, then the conjecture may be proved one coordinate at a time, and reduces to the case where $X = \mathbb{P}^1$.

**Theorem (Cahn-RJ-Spear)**

*The conjecture holds for $X = \mathbb{P}^1$ and $\lambda(y) = y^m$, where $m \in \mathbb{Z}$.***
Proof Sketch

Let \( f \in K(x) \), and note \( Z_n \) is the curve \( f^n(x) = y^m \). Suppose that \( O_f(\alpha) \cap (\mathbb{P}^1(K))^m \) is infinite, so that \( Z_n(K) \) is infinite for each \( n \).

**First leap of faith** First fact: For each \( n \), the infinitely many points in \( Z_n(K) \) are Zariski-dense in \( Z_n \).

**Second leap of faith** Second fact: The Bombieri-Lang conjecture is true for curves (Faltings’ Theorem). Therefore \( Z_n \) is not of general type for any \( n \), i.e. the genus of \( Z_n \) is \( \leq 1 \).
**Third leap of faith** Third step: Show the genus of $Z_n : f^n(x) = y^m$ is at least two unless some iterate of $f$ has a “close functional relationship” to $\lambda$.

**Definition**

For $\beta \in \mathbb{P}^1(\mathbb{C})$, define $\rho_n(\beta)$ to be the number of $z \in f^{-n}(\beta)$ with $e_{fn}(z)$ not divisible by $m$. Call $\beta$ $m$-branch abundant for $f$ if $\rho_n(\beta)$ is bounded as $n \to \infty$.

From genus formulae for superelliptic curves, the genus of $Z_n$ is bounded if and only if 0 and $\infty$ are $m$-branch abundant for $f$. 
We classified all rational functions over $\mathbb{C}$ with two $m$-branch abundant points, and showed their components are defined over $K$.

First attempt: determine all possible ramification structures of pre-image trees of an $m$-branch abundant point.

**Figure 1.** Ramification structures for $O^-(\alpha)$, where $\alpha$ is $p$-branch abundant for $f \in \mathbb{C}(z)$ and $p \nmid \deg f$. 
FIGURE 2. Ramification structures for $O^-(\alpha)$, where $\alpha$ is $p$-branch abundant for $f \in \mathbb{C}(z)$ and $p \mid \deg f$. 
The dynamical Mordell-Lang conjecture
A question over number fields
An arithmetic dynamical Mordell-Lang conjecture

Theorem (Cahn-RJ-Spear)

Let \( f \in K(x) \) and fix \( m \geq 2 \). Then the genus of \( Z_n : f^n(x) = y^m \) is bounded as \( n \to \infty \) if and only if one of the following holds:

- \( f(x) = cx^j(g(x))^m \) with \( g(x) \in K(x), \ 0 \leq j \leq m - 1, \ c \in K^* \);
- (requires \( m \in \{2, 3, 4\} \)) \( f \) is a Lattès map with 0 and \( \infty \) in its post-critical set;
- (requires \( m = 2 \)) Either \( f(x) \) or \( 1/f(1/x) \) can be written in one of the following ways (\( B, C \in K^*, \ p, q, r \in K[x] \setminus \{0\} \)):
  1. \( -\frac{p(x)^2}{(x-C)q(x)^2} \) with \( p(x)^2 + C(x-C)q(x)^2 = Cx r(x)^2 \);
  2. \( -\frac{(x-C)p(x)^2}{q(x)^2} \) with \( (x-C)p(x)^2 + Cq(x)^2 = xr(x)^2 \);
  3. \( B \frac{(x-C)p(x)^2}{q(x)^2} \) with \( B(x-C)p(x)^2 - Cq(x)^2 = -Cr(x)^2 \);
  4. \( B \frac{x(x-C)p(x)^2}{q(x)^2} \) with \( Bx(x-C)p(x)^2 - Cq(x)^2 = -Cr(x)^2 \);

In each case of the theorem, the genus of \( Z_n \) is at most 1 for all \( n \).
Theorem (Cahn-RJ-Spear)

Let $f \in K(x)$ and fix $m \geq 2$. Then the genus of $Z_n : f^n(x) = y^m$ is bounded as $n \to \infty$ if and only if one of the following holds:

- $f(x) = cx^j(g(x))^m$ with $g(x) \in K(x)$, $0 \leq j \leq m - 1$, $c \in K^*$;
- (requires $m \in \{2, 3, 4\}$) $f$ is a Lattès map with $0$ and $\infty$ in its post-critical set;
- (requires $m = 2$) Either $f(x)$ or $1/f(1/x)$ can be written in one of the following ways ($B, C \in K^*, p, q, r \in K[x] \setminus \{0\}$):
  1. $-\frac{p(x)^2}{(x-C)q(x)^2}$ with $p(x)^2 + C(x - C)q(x)^2 = Cx r(x)^2$;
  2. $-\frac{(x-C)p(x)^2}{q(x)^2}$ with $(x - C)p(x)^2 + Cq(x)^2 = xr(x)^2$;
  3. $B \frac{(x-C)p(x)^2}{q(x)^2}$ with $B(x - C)p(x)^2 - Cq(x)^2 = -Cr(x)^2$;
  4. $B \frac{x(x-C)p(x)^2}{q(x)^2}$ with $Bx(x - C)p(x)^2 - Cq(x)^2 = -Cr(x)^2$;

In each case of the theorem, the genus of $Z_n$ is at most 1 for all $n$. 
Theorem (Cahn-RJ-Spear)

Let \( f \in K(x) \) and fix \( m \geq 2 \). Then the genus of \( Z_n : f^n(x) = y^m \) is bounded as \( n \to \infty \) if and only if one of the following holds:

1. \( f(x) = cx^j(g(x))^m \) with \( g(x) \in K(x), 0 \leq j \leq m-1, c \in K^* \);
2. (requires \( m \in \{2, 3, 4\} \)) \( f \) is a Lattès map with 0 and \( \infty \) in its post-critical set;
3. (requires \( m = 2 \)) Either \( f(x) \) or \( 1/f(1/x) \) can be written in one of the following ways (\( B, C \in K^*, p, q, r \in K[x] \setminus \{0\} \)):
   1. \[ -\frac{p(x)^2}{(x-C)q(x)^2} \text{ with } p(x)^2 + C(x - C)q(x)^2 = Cx^2 \]
   2. \[ -\frac{(x-C)p(x)^2}{q(x)^2} \text{ with } (x - C)p(x)^2 + Cq(x)^2 = xr(x)^2 \]
   3. \[ B\frac{(x-C)p(x)^2}{q(x)^2} \text{ with } B(x - C)p(x)^2 - Cq(x)^2 = -Cr(x)^2 \]
   4. \[ B\frac{x(x-C)p(x)^2}{q(x)^2} \text{ with } Bx(x - C)p(x)^2 - Cq(x)^2 = -Cr(x)^2 \]

In each case of the theorem, the genus of \( Z_n \) is at most 1 for all \( n \).
Lattès maps

We say $f \in \mathbb{C}(z)$ is a Lattès map if there is an elliptic curve $E$, a morphism $\mu : E \to E$, and a finite separable map $\pi$ such that the following diagram commutes:

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

Natural choices: $\pi$ is the $x$-coordinate projection and $\mu = [j]$. 
Question

Let $X = \mathbb{A}^2$ and $\lambda(y_1, y_2) = (y_1^{m_1}, y_2^{m_2})$ with $m_1, m_2 \geq 2$. Are there interesting examples of $f : \mathbb{A}^2 \to \mathbb{A}^2$ not of the form $(f_1(x_1), f_2(x_2))$ such that $Z_n : f^n(x_1, x_2) = (y_1^{m_1}, y_2^{m_2})$ is a surface of Kodaira dimension $\leq 2$ for all $n$?

Corollary

Let $f \in K(x)$, fix $m \geq 2$, and suppose that the genus of $Z_n$ is bounded as $n \to \infty$. Then there exist $a > b \geq 0$ with $f^a(x) = f^b(x)(g(x))^m$ for some $g(x) \in K(x)$.

Corollary

$\{n : f^n(\alpha) \in (\mathbb{P}^1(K))^m\}$ is a finite union of arithmetic progressions, of modulus bounded by $a - b$. 
Maximum modulus?

Example: let

\[ f(x) = \frac{2(x - 2)(x + 2)^3}{x(x - 4)^3}. \]

Then \( a = 3, b = 0 \) (\( f^3(x) = x(g(x))^3 \)), and no smaller \( a, b \) suffice.

\[ O_f(6) = \left\{ 6, \frac{4}{3} \cdot 4^3, \left( \frac{655}{488} \right)^3, 6 \left( -\frac{129900299507}{120418942015} \right)^3, \ldots \right\} \]

Indeed, for all \( m \geq 3 \) the modulus is bounded by \( m \), and this is best possible (independent of \( K \)):

Let \( f(x) = cx(x + 1)^m \), where \( c \notin K^p \) for each prime \( p \) dividing \( m \).

Then \( f^i(1) = c^i(k_i)^m \) for \( k_i \in K \), for all \( 1 \leq i \leq m - 1 \). But \( c^i \notin K^m \), and so \( \{ n : f^n(1) \in (\mathbb{P}^1(K))^m \} = \{ 0, m, 2m, 3m, \ldots \} \).
For \( m = 2 \) one must have \( a - b \leq 4 \). This is attained by certain Lattès maps descending from CM elliptic curves.

Example:

\[
f(x) = (8 + 4\sqrt{3}) \frac{(x - 1)(x - (4 + 4\sqrt{3}))^2}{x(x - (6 + 4\sqrt{3}))^2}
\]

has post-critical orbit

\[
0 \to \infty \to 8 + 4\sqrt{3} \to 1 \to 0.
\]

Thus \( f^4(x) = x(g(x))^4 \), but \( f^i(x) \) is not of this form for \( i = 1, 2, 3 \).

This map arises from taking \( E \) to have CM by \( \mathbb{Z}[\sqrt{-3}] \),

\[
\mu(P) = [\sqrt{-3}]P + T,
\]

where \( T \) is a non-trivial 2-torsion point, and \( \pi \) to be projection onto the \( x \)-coordinate.
Question 1: Is it possible for a Lattès map with a post-critical four-cycle to have $\alpha \in K$ with $\{ n : f^n(\alpha) \in (\mathbb{P}^1(K))^2 \}$ an arithmetic progression of modulus 4?

Question 2: Can Lattès maps with a post-critical four-cycle be defined over $\mathbb{Q}$?
Thank you!