The dynamical Mordell-Lang conjecture and related problems

Thomas J. Tucker
University of Rochester

The cyclic case of the dynamical Mordell-Lang conjecture

Conjecture

(Dynamical Mordell-Lang conjecture) Let X be an algebraic variety defined over $\mathbb{C}$, let V be a closed subvariety of X, let $\Phi : X \longrightarrow X$, and let $\mathbf{z} \in X(\mathbb{C})$. Then the set of n such that $\Phi^n(\mathbf{z}) \in V$ is a finite union of arithmetic sequences.

This was onjectured by Denis, Bell, Ghioca-Tucker. We will often call it the DML conjecture. We will denote the set of all iterates of $\mathbf{z}$ as $\mathrm{Orb}(\mathbf{z})$.

Two quick points;

- An arithmetic sequence is sequence of the form $\ell, \ell + m, \ell + 2m, \ldots, \ell + km, \ldots$.
- The "modulus" m can be zero, so singleton sets are allowed. In fact....

Conjecture, continued

- If the DML conjecture is true then any time $V \cap \text{Orb}(\mathbf{z})$ is infinite, V must contain $\Phi^{\ell}(\mathbf{z}), \Phi^{\ell+m}(\mathbf{z}), \ldots, \Phi^{\ell+km}(\mathbf{z}), \ldots$ which is invariant under Φ^m. Taking the Zariski closure of these gives a positive dimensional subvariety of V that is periodic under Φ.
- One motivation for the conjecture were the analogies

$$\text{periodic subvarieties} \longleftrightarrow \text{group subvarieties}$$

$$\text{arithmetic sequences} \longleftrightarrow \text{cosets of subgroups}$$

Abelian varieties and the Mordell-Lang conjecture

Theorem (Mordell-Lang conjecture, Faltings-Vojta, 1991)

Let A be an abelian variety over a field of characteristic 0, let G be a finitely generated subgroup of A, and let V be a subvariety of A. Then

$$V \cap G \text{ is a finite union of cosets of subgroups of } G.$$

When A is defined $\mathbb{Q}$, one may talk about the $\mathbb{Q}$-points on A (these are literally the points on A with rational coordinates under some embedding), which are denoted as $A(\mathbb{Q})$, which is finitely generated (Mordell-Weil). Thus, in particular, it says that if a curve in A contains infinitely many points, then the curve must be translate of a group subvariety and thus must have genus 1. That gives the Mordell conjecture. (Note: taking the closures of the cosets of subgroups gives translated group subvarieties.)

The theorem of Skolem-Mahler-Lech

The cyclic case of Mordell-Lang was proved by Chabauty in 1941. His method dates back even earlier to Skolem, in 1933.

Theorem (Skolem-Mahler-Lech theorem)

Suppose we have a linear recurrence sequence $(\alpha_n)_{n=1}^{\infty}$ *where*

$$\alpha_{m+i} = a_1\alpha_{m+i-1} + \cdots + a_i\alpha_m,$$

where $a_j \in \mathbb{C}$*. Then, for any* $\gamma \in \mathbb{C}$*, the set of* n *such that* $\alpha_n = \gamma$ *is a finite union of arithmetic sequences.*

(Again, singleton arithmetic sequences are allowed and the union could be an empty union.)

SML continued

The Skolem-Mahler-Lech is equivalent to the following dynamical statement.

Theorem

Let $A \in \mathrm{GL}_r(\mathbb{C})$, V a subvariety of $\mathbb{C}^r$, and $\mathbf{z}$ a point in $\mathbb{C}^r$. Then either

- *there are finitely n such that $A^n\mathbf{z} \in V$; or*
- *There is an entire coset $i + m\mathbb{Z}$ of $\mathbb{Z}$ such that $A^n\mathbf{z} \in V$ for all n in this coset.*

A few notes:

- There are many important quantitative refinements (Beukers, Evertse, Schlickewei, Schmidt) using diophantine approximation.
- The original method here seems to always be effective in practice...is there a proof in general? (See Terry Tao's blog.)

One very simple example

Let's just do one very simple example.

Example

Let $A = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}$ and let $s = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Let V be the subspace consisting of all vectors of the form $\begin{pmatrix} x \\ -x \end{pmatrix}$. Then $A^n s \in V$ if and only if n is odd, i.e. if $n \in 1 + 2\mathbb{Z}$.

Note that A^2 sends V to itself, so once you get some $A^i s \in V$, you must get $A^{i+2k} s \in V$ for any k (this is why you do not get any "singleton cosets" here).

p-adics and Skolem-Mahler-Lech theorem

The proof of the Skolem-Mahler-Lech theorem, is fairly easy to describe.

The idea is to use p-adic analytic parametrization. Here is the key observation.

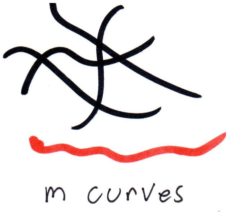
$\mathbb{Z}$ is in the closed unit disc of radius 1 in $\mathbb{Q}_p$.

(Henceforth, we denote the unit disc in $\mathbb{Q}_p$ as $\mathbb{D}_p$).

Since $\mathbb{Z}$ is in the closed unit disc $\mathbb{D}_p$ in $\mathbb{Q}_p$, *any p-adic analytic power series on $\mathbb{Z}$ will have finitely many zeros*. That is the key to the proof of the Skolem-Mahler-Lech theorem. It is always possible to embed the entries of A, the coordinates of our point $\mathbf{z}$, and the polynomials defining V into $\mathbb{Z}_p$ for some p.

p-adic analytic parametrization

It turns out that there exists some p such that the p-adic closure of $\mathbf{z}, A\mathbf{z}, \ldots, A^n\mathbf{z}, \ldots$ has the following structure.



More concretely, there is a prime p and a modulus m such that for each congruence class i modulo m, there is a p-adic analytic map

$$\theta_i : \mathbb{D}_p \longrightarrow \mathbb{Q}_p^r \quad \text{such that} \quad \theta_i(k) = A^{i+mk}(\mathbf{z}).$$

Each "curve" above corresponds to a an analytic θ_i which corresponds to a congruence class in $m\mathbb{Z}$.

p-adic analytic parametrization and the method of Skolem-Mahler-Lech

For each polynomial F that vanishes on V, we have that

$$F \circ \theta_i : \mathbb{D}_p \longrightarrow \mathbb{Q}_p$$

is a one variable analytic power series. Thus $F \circ \theta_i$ is either has at most finitely many zeroes or is itself *identically zero*. Since for $n = mk + i$, we have $A^n(\mathbf{z}) \in V$ if and only if $F \circ \theta_i(k) = 0$ for all F vanishing on V, we see that

- $A^{i+mk}(\mathbf{z}) \in V$ **at most for finitely many** k (these give "singleton" cosets); *or*
- $A^{i+mk}(\mathbf{z}) \in V$ **for all** k (these give infinite cosets).

This produces either finitely many elements in a congruence class or entire cosets $i + m\mathbb{Z}$, and thus gives the Skolem-Mahler-Lech theorem.

A very simple example of p-adic parametrization

One can define p-adic logarithm and exponential maps using the usual power series definition

$$\log_p(z) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(z-1)^n}{n}$$

and

$$\exp_p(z) = \sum_{n=1}^{\infty} \frac{z^n}{n!}$$

Then for, say, $z \in \mathbb{Z}$ with $z \equiv 1 \pmod{p}$ (where the power series for $\log_p$ converges), we can write

$$\theta(n) = \exp_p(n \log z) = z^n$$

to get an analytic function "parametrizing" powers of z.
Note that for any $z \in \mathbb{Z}$ prime to p, we have $z^m \equiv 1 \pmod{p}$ for some m, so we can always break $\{z, z^2, \dots\}$ up into m "parametrizable orbits". And of course you can do the same thing when you have a diagonalizable matrix, by treating each eigenvalue, *as long as each eigenvalue is a p-adic unit*.

Notes on Skolem-Mahler-Lech

A few points about the Skolem-Mahler-Lech theorem:

- The reason we get cosets of $\mathbb{Z}$ (rather than all of $\mathbb{Z}$) is precisely because we have to raise eigenvalues to a power m in order to take p-adic logarithms.
- Won't work over the usual absolute value, see $\sin \pi z$.
- Everything works the same for taking logarithms of matrices in more complicated (non-diagonalizable) Jordan canonical forms.
- Everything here generalizes to étale maps of any algebraic variety, via a generalization of p-adic logarithms.

The étale case

Theorem

(Bell-Ghioca-T) Let X be an algebraic variety defined over $\mathbb{C}$, let V be a closed subvariety of X, let $\Phi : X \longrightarrow X$ be an étale map, and let $\mathbf{z} \in X(\mathbb{C})$. Then the set of n such that $\Phi^n(\mathbf{z}) \in V$ is a finite union of arithmetic sequences.

Recall that an étale map is one that induces an isomorphism at the tangent space of each point. Thus there is no ramification.

Intuitively, one might think of applying the Skolem-Mahler-Lech p-adic logarithm technique (sort of) to the Jacobian matrix J for Φ at a suitable point *as long as* $p \nmid \det J$. (A very short actual proof of p-adic parametrization can be found in a recent paper of Poonen's.)

Generalizing the étale method

In fact, one can apply the method of Skolem method whenever the orbit of $\mathbf{z}$ avoids the ramification locus of Φ modulo p, the analog of *being able to take p-adic logs of all your eigenvalues*.

Since one only needs a *single* p with this "avoidance of ramification" property, it would seem that there should always exist *some* suitable p.

But in fact in general it is unlikely that there is always a p where this works!

Avoiding ramification and the birthday problem

If X has dimension r, then it has about p^r points modulo p. By the "birthday problem", it should therefore take about $\sqrt{p^d}$ iterations for an orbit to start to cycle.

The ramification locus R of a map $\Phi : X \longrightarrow X$ has codimension 1 in X, so it has p^{r-1} points in it modulo p. So each iterate has a $1/p$ chance of hitting R modulo p (regardless of r).

Moral: when the dimension of X is large and p is large, any given orbit probably goes through R. But..you probably can avoid ramification in dimensions 1, 2, and 3. (Benedetto/Ghioca/Hutz/Kurlberg/Scanlong-T).

Another approach

Here is another way of approach the dynamical Mordell-Lang conjecture:

The Lang-Vojta conjectures say that in a variety of general type, the rational points are not dense. (General type means that the canonical divisor is quasi-ample. For curves, this means genus > 1.)

The inverse images of V under Φ "should" become general type under sufficiently high inverse images if V if the images meet the ramification divisor.

Unfortunately, there are counterexamples to making this argument work in general.

However, the idea of analyzing V and its inverse images can be fruitful, especially when V is a curve.

Another approach, continued

Ghioca-T-Zieve showed that the Mordell-Lang conjecture is true for maps of the form $\Phi : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ by $\Phi(x, y) = (f(x), g(y))$, for f and g polnomials, when V is a line. The idea is to show that high inverse images of V cannot have infinitely many integral points unless V is periodic. This uses Siegel's theorem which says if C is an affine curve with infinitely many integral points, then C has genus 0 and at most two points at infinity.

More generally, Xie showed the following.

Theorem

(Xie) The dynamical Mordell-Lang conjecture holds for any morphism $\Phi : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ *be defined over a number field.*

The proof uses an analysis of dynamics near the points at infinity via deep Berkovich space techniques developed by Favre-Jonsson.

A more general dynamical Mordell-Lang question

Question DML

Let X be an algebraic variety defined over $\mathbb{C}$, let V be a closed subvariety of X, let G be a finitely generated commutative semigroup of morphisms from X to itself, and let $\mathbf{z} \in X(\mathbb{C})$. Can the set

$$\{g \in G \mid g\mathbf{z} \in V\}$$

be written as a finite union of cosets of subsemigroups of G?

Is there a reasonable conjecture to be made here?

Counterexample

The simplest counterexample may be the following.

Example

Let X be $\mathbb{C}^2$ and let S be the group of translations generated by:

$$\sigma_1(a, b) = (a + 1, b)$$

and

$$\sigma_2(a, b) = (a, b + 1)$$

Let $\mathbf{z} = (0, 0)$ and let V be a curve coming from a *Pell's equation*:

$$x^2 - dy^2 = 1 \text{ for some square-free positive integer } d \; .$$

Then it is known that there are infinitely many integer solutions (m, n) to $m^2 - dn^2 = 1$, but they do not form a finite set of cosets of subgroups of S.

Thus, we say that the dynamical Mordell-Lang question has a negative answer for groups of additive translations.

Another counterexample

Example

(Ghioca) Working in $\mathbb{C}^3$, let V be the subspace given by the yz-plane, i.e. the set of all $(0, y, z)$, and let G be the group generated by the matrices $A = \begin{pmatrix} 2 & -1 & 0 \\ 0 & 2 & -2 \\ 0 & 0 & 2 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & 2 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 2 \end{pmatrix}$. This gives a commutative abelian group isomorphic to $\mathbb{Z}^2$. But we do not get the desired coset intersection result.

By exponentiating, this gives counterexamples for endomorphisms of the multiplicative group. Scanlon and Yasufuku were able to generalize this to show much more pathological counterexamples.

Characteristic p – bad news

Even the one-parameter version of dynamical Mordell-Lang is false in characteristic p.

Example

Let

- $X = \mathbb{F}_p(T)^2$ (two dimensional affine space over the function field $\mathbb{F}_p(T)$)
- $V = \{(x, y) \mid x - y = 1\}$
- $\Phi : X \longrightarrow X$ be the map given by $\Phi(x, y) = ((T + 1)x, Ty)$
- $\mathbf{z} = (1, 1)$

Since $(T + 1)^n - T^n = 1$ if and only if n is a power of p, we have

$$\{n \mid \Phi^n(\mathbf{z}) \in V\} = \{p^m \mid m \in \mathbb{N}\}$$

This is clearly an infinite but sparse set, one which does *not* contain any infinite arithmetic progressions.

Characteristic p – good news

Note that the set of powers of p, while not *finite*, does have zero density in the set of natural numbers.

Theorem

(Gignac, Petsche, Bell-Ghioca-T) Let X be an algebraic variety defined over any field, let V be a closed subvariety of X, let $\Phi : X \longrightarrow X$, and let $\mathbf{z} \in X$. Then the set of n such that $\Phi^n(\mathbf{z}) \in V$ is a finite union of arithmetic sequences along with a set of density zero.

The techniques probably don't seem to extend to an attack on the full dynamical Mordell-Lang in characteristic 0...because they work in characteristic p!

Ghioca and Scanlon have a characteristic p dynamical Mordell-Lang conjecture essentially saying that "Frobenius-type" sequences as on the previous page are the only new feature.

Other questions

The dynamical Mordell-Lang conjecture says that, in characteristic 0, if V is a subvariety of X, then the set of points $V(\mathbb{C})$ has the property that for any morphism has the property that for any $\Phi : X \longrightarrow X$ and $\mathbf{z} \in X(\mathbb{C})$, the n such that $\Phi^n(\mathbf{z})$ form a finite union of arithmetic sequences.

Are there other natural subsets of varieties with this sort of property?

One natural such subset is the set of integral points. The Mordell-Lang conjecture admits an analog for integral points on semiabelian varieties, which was also proved by Faltings and Vojta.

Is there an integral points analog of the dynamical Mordell-Lang conjecture? For this, and other questions, we will need some extra hypotheses.

Integral points, continued

Recall that if S is a set of places of a number field K including all the archimedean places, we say that α is an S-integer if $|\alpha|_v \leq 1$ for all places v outside of S. When $K = \mathbb{Q}$, this just means that the denominator of α has no factors outside of primes in S.

We say that a point in $\mathbb{P}^N(K)$ is S-integral (relative to the hyperplane at infinity) if its coordinates are $[\alpha_1 : \cdots : \alpha_N : 1]$ where α_i is an S-integer for $i = 1, \ldots, N$. (This generalizes the natural notion that the integer points in $\mathbb{P}^1(\mathbb{Q})$ are those that can be written as $[n : 1]$ for n an integer.)

DML for integral points

Question

Let K be a number field, let $\Phi : \mathbb{P}^N \longrightarrow \mathbb{P}^N$ be a morphism defined over K with $\deg \Phi > 1$, and let $\mathbf{z} \in \mathbb{P}^N(K)$. Let S be a finite set of places of K including all the archimedean places and all the places of bad reduction for Φ. Is it true that the set of n such that $\Phi^n(\mathbf{z})$ is S-integral must be a finite union of arithmetic sequences.

The rough idea here is that the only way one can get infinitely many such n at all is if some power of Φ comes from a polynomial map in the first n coordinates (which naturally sends S-integral points to S-integral points and fixes the hyperplane at infinity)

There is partial progress towards on this question due to Yasufuku and Yasufuku-Levin (assuming Vojta's conjecture), and on related questions by Corvaja-Sookdeo-Tucker-Zannier. Idea: The degree of high iterate inverse images of the hyperplane at infinity gets large, and a conjecture of Vojta says there are few integral points relative to hypersurfaces of high degree.

Other questions, continued

The good reduction condition in the question above is necessary (there's a fairly simple counterexample due to Benedetto-Briend-Perdry).

The condition $\deg \Phi > 1$ can be explained even more simply. If $\Phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ by $\Phi([x : y]) = [x : y + p]$ and S is the set of primes of $\mathbb{Q}$ consisting of the archimedean place and p, then the set of n such that $\Phi^n([1 : 0])$ is S-integral consists of $\{p, p^2, p^3, \dots\}$ so is not a finite union of arithmetic progressions.

This sort of example arises in other contexts too. More generally, Zhang has emphasized the importance of the condition of "polarizability" of morphisms of projective varieties which is equivalent to morphisms that extend to morphisms of projective space of degree greater than one.

Dynamical Mordell-Lang for value sets

Cahn, Jones, and Spear made the following conjecture.

Conjecture

Let K be a number field, let $f : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be defined over K with $\deg f > 1$. Let $g : V \longrightarrow \mathbb{P}^1$ be any finite morphism defined over K, and let $\mathbf{z} \in \mathbb{P}^1(K)$. Then set of n such that $f^n(\mathbf{z}) \in g(V(K))$ forms a finite union of arithmetic progressions.

There is a very nice proof of this conjecture due to Hyde and Zieve.

There are also counterexamples when K, instead of being a number field, is a non-finitely generated field (due to Zieve) and when $g : V \longrightarrow \mathbb{P}^1$ is not a finite map (due to Bell).

Dynamical Mordell-Lang for value sets, continue

Are there similar results in higher dimension?

Question

Let K be a number field, let $f : \mathbb{P}^N \longrightarrow \mathbb{P}^N$ be defined over K with $\deg f > 1$. Let $g : V \longrightarrow \mathbb{P}^N$ be any finite morphism defined over K, and let $\mathbf{z} \in \mathbb{P}^N(K)$. Is it true that the set of n such that $f^n(\mathbf{z}) \in g(V(K))$ must form a finite union of arithmetic progressions?

Here is the rationale for this question. For each n, we let V_n be set of points $(x, y) \in \mathbb{P}^N \times V$ such that $f^n(x) = g(y)$. We have a map $V_n \longrightarrow V_{n-1}$ by sending (x, y) to $(f(x), y)$.

If there are infinitely many n such that $f^n(\mathbf{z}) \in g(V(K))$ then all of the V_n must contain infinitely many K-points. But intuitively, their canonical divisors get "bigger", unless there is some kind of periodicity relation among the V_n, so this shouldn't happen (by Lang-Vojta conjecture),

One conjecture to rule them all?

Is there a nice way to put the dynamical Mordell-Lang conjecture, its integral points version, and its value set version all into one conjecture?

Density of orbits

We mention one more conjecture with a close relationship to the dynamical Mordell-Lang conjecture.

Conjecture

(Zhang, Amerik-Campana, Medvedev-Scanlon) Let $\Phi : X \longrightarrow X$ *be defined over a number field* K. *Then there is some* $\mathbf{z} \in X(\bar{\mathbb{Q}})$ *such that* $\mathrm{Orb}(\mathbf{z})$ *is Zariski dense in* X *unless there is a nonconstant rational map* $g : X \longrightarrow P^1$ *such that* $g \circ \Phi = g$ *on a dense open subset of* X *(that is, unless* Φ *preserves the fibers of a nonconstant rational map to* $\mathbb{P}^1$*).*

Of course, if Φ preserves fibers of a map, then every orbit stays within one of these orbits, and cannot possibly be dense.

While, this conjecture says that there is a dense orbit, the dynamical Mordell-Lang conjecture says that any infinite sequence of a dense orbit is itself dense (in other words, any dense orbit is generic). Partial progress on this has been made by several people (Amerik, Bell, Bogomolov, Campana, Ghioca, Levy, Medvedev, Reichstein, Rovinsky, Scanlon, Voisin, Xie, for example).

Outline

In the next two talks we will study the following problems:

1. Classifying preperiodic subvarieties. If we knew what all the preperiodic subvarieties looked like it would help with both the Zhang density conjecture and some aspects of DML. We will touch on a classification theorem of Medvedev-Scanlon as well as on the uniform boundedness conjecture of Morton-Silverman (and subsequent work by Pezda, Zieve, Benedetto, Hutz, Bell/Ghioca/T).
2. Avoiding ramification mod primes via iterated Galois groups in the case of "split maps" (more on this later). This ties in with a dynamical variant of the Serre open image conjecture, first suggested by Boston and Jones.