Back and Forth from Model Theory to Number Theory: Structures of Lang-type

Andrew Harrison-Migochi

University of Manchester

March 2023

Contents

O-minimality

O-minimality

Definition

We call an expansion of the real field, $\mathcal{R} = (\mathbb{R}, +, \cdot, \leq, \ldots)$ o-minimal if every definable subset of the real line is a finite union of point and intervals.

Examples

- $\overline{\mathbb{R}} = (\mathbb{R}, +, -, \cdot, 0, 1, \leq)$
- $\mathbb{R}_{\exp} = (\overline{\mathbb{R}}, \exp)$ (Wilkie)
- $\mathbb{R}_{\text{an}} = (\overline{\mathbb{R}}, (f|_{[0,1]^n} : f \in C^\infty(U),\ [0,1]^n \subseteq U)_{n\in\mathbb{N}})$ (Gabrielov)

Elliptic curves

Definition

Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be a complex lattice with ω_1, ω_2 linearly independent over $\mathbb{R}$. We call the quotient $\mathbb{C}/\Lambda$ an elliptic curve.

Definition

An elliptic curve, $\mathcal{E}$, is a projective variety given by the zero set of the homogenisation of a non-singular cubic polynomial in the form $y^2 = 4x^3 + ax + b$ equipped with an algebraic group structure.

Weierstrass $\wp$

Definition (Weierstrass $\wp$-function)

For any elliptic curve $\mathbb{C}/\Lambda$ we can define its Weierstrass $\wp$ function.

$$\wp(z,\Lambda) := \frac{1}{z^2} \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

Let $\exp_{\mathcal{E}} : \mathbb{C}/\Lambda \to \mathcal{E}$ be the map $\exp_{\mathcal{E}} : z \mapsto [1 : \wp(z) : \frac{1}{2}\wp'(z)]$.

Fact

Every lattice Λ is isomorphic to one with generators $\{1, \tau\}$ for some $\tau \in \mathbb{H}$. Furthermore $\tau_1, \tau_2 \in \mathbb{H}$ define isomorphic lattices if and only if there exists some $g \in \mathrm{SL}(2, \mathbb{Z})$ such that $\tau_1 = g\tau_2$.

Fact

Let $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$. The torsion points of $\mathbb{C}/\Lambda$ are the points of the form $\mathbb{Q} + \tau\mathbb{Q}$.

the j-function

The j-function is an $\mathrm{SL}(2,\mathbb{Z})$-periodic function from $\mathbb{H} \to \mathbb{C}$.
In other words, the j-function is a bijective map from the space of isomorphism classes of elliptic curves to $\mathbb{C}$.

Fact

The restriction $j|_{\mathcal{F}}$ is holomorphic.

Fact

The point $(\tau, j(\tau))$ is algebraic if and only if τ is a quadratic integer.

O-minimal structures

Fact

The restriction of $\wp$ to a compact set is definable in $\mathcal{R}_{\mathrm{an}}$.

Fact (Peterzil and Starchenko)

The structure $(\overline{\mathbb{R}}, j|_{\mathcal{F}})$ is o-minimal.

Definitions

Definition

Let $X \subseteq \mathbb{R}^n$ be definable in some o-minimal expansion of $\overline{\mathbb{R}}$. We define the algebraic part of X, X^{alg} as the union of all connected semi-algebraic subsets of X with dimension greater than or equal to 1. Define $X^{\mathrm{trans}} = X \setminus X^{\mathrm{alg}}$.

Definition (Height)

- For $q \in \mathbb{Q}$ with $q = a/b$ and $\gcd(a, b) = 1$ define $H(q) = \max\{|a|, |b|\}$.
- For $p \in \overline{\mathbb{Q}}$ with minimal polynomial over $\mathbb{Q}$, $q_0 + \ldots + q_{n-1}x^{n-1} + x^n$, define $H(p) = \max\{H(q_0), H(q_1), \ldots H(q_{n-1}), 1\}$.

Pila-Wilkie

Definition

Let $X \subset \mathbb{R}^n$ be a set. Let K be a number field and let $H > 1$. We define $\#X(K, H)$ as number of K-points in X of height at most H.

Theorem (Pila-Wilkie[3])

Let $X \subseteq \mathbb{R}^n$ be definable in some o-minimal expansion of $\overline{\mathbb{R}}$. Let $\varepsilon > 0$ and let K be a number field of degree d. Let $H > 1$. Then there exist $c(\varepsilon, d)$ such that

$$\#X^{trans}(K, H) \leq c(\varepsilon, d) H^{\varepsilon}$$

Special Point Conjectures

Special Point Theorems

Statement

Let $A \subset \mathbb{C}^n$ be a semi-algebraic set and let S be a set of special points. Let $X \subset A^n$ be an algebraic variety. Then the Zariski closure $X \cap S^n$ is a finite union of special varieties.

Semi-Algebraic Set	Special Points	Special Varieties
$\mathbb{C}^\times$	roots of unity	gH
$\mathbb{C}$	j-invariants of CM curves	σ, $\Phi_N(X, Y) = 0$
$\mathcal{E}$	torsion points	$c \oplus H$

Examples

Theorem (Mordell-Lang (Faltings, Hrushovski))

Let $A \subseteq \mathbb{C}^n$ be an abelian variety. Let Γ be a finitely generated subgroup of A. Let $X \subseteq A$ be a subvariety of A. Then the Zariski closure of $X \cap \Gamma$ is the union of finitely many translates of abelian subvarieties of A.

Theorem (Manin-Mumford (Raynaud, Hrushovski))

Let $A \subseteq \mathbb{C}^n$ be an abelian variety. Let $X \subseteq A$ be a subvariety of A defined over some number field. Then the Zariski closure of $X \cap A_{tors}$ is the union of finitely many translates of abelian subvarieties of A by torsion points.

Theorem (André-Oort (j-function) (Pila [2]))

Let $X \subseteq \mathbb{C}^n$ be a variety. Let Σ be the j-invariants of CM-elliptic curves. Let $\Phi_N(X, Y)$ be the Nth modular polynomial for each $N \in \mathbb{N}$. Then the Zariski closure of $X \cap \Sigma^n$ is a finite union of irreducible components of special subvarieties of X defined using modular polynomials and points from Σ.

Pila-Zannier Strategy

1. Move to an o-minimal setting with definable function, f such that $f^{-1}(S^n)$ belongs to some number field.
2. Let $Y = f^{-1}(X)$.
3. Show that $\overline{f(Y^{\text{alg}}) \cap S}$ is union of irreducible components of special subvarieties by using Ax-Schanuel/functional transcendence argument. In his paper on the André-Oort conjecture, Pila also makes use of Pila-Wilkie during this step.
4. Show that Y^{trans} contains the pre-image of finitely many special points. This part combines Pila-Wilkie with Galois bounds.
5. Show that $\overline{f(Y^{\text{alg}}) \cap S}$ is a finite union, usually by a degree bounds on the special subvarieties.

Examples

Set	S	f	Structure	$f^{-1}(S)$
$\mathbb{C}^\times$	roots of unity	$\exp(2\pi i x)$	$\mathbb{R}_{\exp}$	$\mathbb{Q}$
$\mathbb{C}$	singular moduli	$j(x)$	$(\overline{\mathbb{R}}, j\|_{\mathcal{F}})$	quadratic integers
$\mathcal{E}$	torsion points	$\exp_{\mathcal{E}}$	$\mathbb{R}_{\text{an}}$	$\mathbb{Q} \times \mathbb{Q}$[1]

[1] In reality $exp_{\mathcal{E}}^{-1}(S)$ will be the set $\mathbb{Q} + \tau\mathbb{Q}$ for some $\tau \in \mathbb{H}$ so some additional work must be done to arrive at $\mathbb{Q} \times \mathbb{Q}$

Applications to Model Theory

Quantifier Elimination

Definition

An L-theory T has quantifier elimination if every L-formula is equivalent to a quantifier free formula.

Examples

- Let $L = \{+, -, \cdot, 0, 1\}$. The L-theory of algebraically closed fields has quantifier elimination.
- Let $L = \{+, -, \cdot, 0, 1, \leq\}$. The L-theory of real closed ordered fields quantifier elimination.

Stability

Definition (Stability)

A complete first order theory T is said to be κ-stable for some cardinal κ if for any subset A of the monster model such that $|A| < \kappa$ the set of complete types over A has cardinality κ. T is called stable if it is stable for some cardinal κ.

Examples

- Let $L = \{+, -, \cdot, 0, 1\}$. The L-theory of algebraically closed fields is ω-stable.
- Let $L = \{+, -, \cdot, 0, 1, \leq\}$. The L-theory of real closed ordered fields is not stable

Structures of Lang-Type

Definition (Lang-type (Pillay [4]))

Let K be an algebraically closed field, and A a commutative algebraic group over K. Let Γ be a subgroup of A. We say that the triple (K, A, Γ) is of Lang-type if for every $n < \omega$ and every subvariety X of A^n, $X \cap \Gamma^n$ is a finite union of cosets.

Theorem (Manin-Mumford (Raynaud, Hrushovski))

Let $A \subseteq \mathbb{C}^n$ be an abelian variety. Let $X \subseteq A$ be a subvariety of A defined over some number field. Then the Zariski closure of $X \cap A_{tors}$ is the union of finitely many translates of abelian subvarieties of A by torsion points.

Structures of Lang-type

Theorem ((Pillay [4]))

Let K be an algebraically closed field, A a commutative algebraic group over K, and Γ a subgroup of A. Then (K, A, Γ) is of Lang-type if and only if Th$(K, +, ., \Gamma, a)_{a \in K}$ is stable, and the formula $x \in \Gamma$ is one-based.

Mordell-Lang Property

Definition (Mordell-Lang Property[1])

Let K be a field and $G \subseteq K^n$ be a subgroup of a one dimensional group definable in K, $(A, \oplus)$. Let L be a subfield of K. We say that G has the Mordell-Lang property over L if for any $p \in L[X_1, \ldots X_{mn}]$ there exists $t \in \mathbb{N}$, $g_1, \ldots, g_t \in A^m$ and $H_1, \ldots H_m$ subgroups of G^m such that

$$V(p) = \bigcup_{i=1}^{t} g_i \oplus (H_i \cap G^m)$$

and each H_i is the kernel of a system of linear equations over A.

Expansions of the Real Field

Theorem (Günaydin and Hieronymi[1])

Let $\mathcal{R}$ be a real closed field. Let $(\mathbb{A}, \oplus)$ be a 1-dimensional t-connected group definable in R^n. Let L be the language of ordered rings together with an n-ary predicate P. Let Γ be a t-dense subgroup of $\mathbb{A}(\mathbb{R})$ satisfying a Mordell-Lang Condition. If the theory, T of $(\mathcal{R}, \mathcal{G})$ where P is a predicate for G models:

- *G is a t-dense subgroup of $\mathbb{A}(R)$,*
- *for all $n > 0$ for all $g \in G$ if $ng \in \Gamma$, then $g \in \Gamma$,*
- *for all $n > 0$, $|G/nG| = |\Gamma/n\Gamma|$,*
- *G satisfies the same Mordell-Lang condition as Γ*

then every L-formula is equivalent modulo T to a boolean combination of ones in the form

$$\exists x_1^1 \dots \exists x_n^m \bigwedge Q(x_1^i, \dots, x_n^i) \wedge \varphi(x, y)$$

where φ is a quantifier free formula in the language of ordered rings.

References

[1] Ayhan Gunaydin and Philipp Hieronymi. "The real field with the rational points of an elliptic curve". In: (June 2010). URL: http://arxiv.org/abs/0906.0528.

[2] Jonathan Pila. "O-minimality and the André-Oort conjecture for Cn". In: *Annals of Mathematics* 173.3 (2011), pp. 1779–1840. ISSN: 0003486X. DOI: 10.4007/annals.2011.173.3.11.

[3] Jonathan Pila. "On the algebraic points of a definable set". In: *Selecta Mathematica, New Series* 15.1 (2009), pp. 151–170. ISSN: 10221824. DOI: 10.1007/s00029-009-0527-8.

[4] Anand Pillay. "The model-theoretic content of Lang's conjecture". In: *Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture*. Ed. by Elisabeth Bouscaren. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 101–106. ISBN: 978-3-540-68521-0. DOI: 10.1007/978-3-540-68521-0{_}6. URL: https://doi.org/10.1007/978-3-540-68521-0_6.