O-minimality and Diophantine applications

What is... o-minimality? Here's an impressionistic answer:

- A type of geometry or topology, lying between algebraic geometry (very rigid) and topology (very flexible), in which the spaces and functions under consideration are restricted through a deceptively simple condition
- Tarski '40s - implicitly present in his work concerning semi-algebraic geometry
- van der Dries '80s - formulated o-minimality using model theory
- Pila, Zannier '00s - arithmetic applications
- Habegger, Gao, Pillay, Tsimerman, and many others - o-minimality has surprisingly wide reach! (look at this IAS special year!)

$\S\, 1$. Set up: basic notions of model theory

Definition (Languages and structures).

A *language* is a set $\mathscr{L}$ consisting of constant symbols c, relation symbols (r, n), and function symbols (f, m).

An $\mathscr{L}$*-structure* is a set M endowed with distinguished constants, relations, and functions that give meaning to symbols in $\mathscr{L}$. (More precisely, for any constant symbol c an element $c_M \in M$; for any relation symbol (r, n) a subset $r_M \subset M^n$; and for any function symbol (f, m) a map $f : M^m \to M$.)

Example.

- $\mathscr{L} = \emptyset$. Then $\mathscr{L}$-structures = sets.
- $\mathscr{L} = \mathscr{L}_{\text{ring}} = \{(+, 2), (-, 1), (\cdot, 2), 0, 1\}$ "the language of rings". Then $\mathscr{L}$-structures are sets M together with two named elements $0_M \in M$ and $1_M \in M$, as well as maps $M \times M \xrightarrow{+} M$, $M \xrightarrow{-} M$, $M \times M \xrightarrow{\cdot} M$.
- $\mathscr{L} = \mathscr{L}_{\text{or}}$ " the language of ordered rings" - important for us today

NB: Through any ring is an $\mathscr{L}_{\text{ring}}$-structure in the obvious way, an arbitrary $\mathscr{L}_{\text{ring}}$-structure might have nothing to do with a ring!

Definition (Terms, formulas and sentences).

Let $\mathscr{L}$ be a language.

An $\mathscr{L}$-term is a "syntactical" expression obtained by finitely many uses of the following rules: (1) any free variable, any constant symbol is a term, (2) if (f, n) is a function symbol and $t_1, \ldots, t_n$ are $\mathscr{L}$-terms, then $f(t_1, \ldots, t_n)$ is a term.

An $\mathscr{L}$-formula is a syntactical expression obtained by finitely many uses of the following rules: (1) for terms t_1 and t_2, $t_1 = t_2$ is a formula; (2) for any relation symbol (r, n) and terms $t_1, \ldots, t_n$, $r(t_1, \ldots, t_n)$ is a formula; (3) boolean combinations $\wedge$, $\vee$, $\neg$, implications $\rightarrow$ and quantifiers $\exists$, $\forall$ can be applied to formulas to produce new formulas.

Formulas without free variables are called sentences.

Given a ring R viewed as an $\mathscr{L}_{\text{or}}$-structure, any term can be interpreted as a polynomial function with *integral* coefficients, e.g. $t : +(v_1, \cdot(v_2, +(1, v_3)))$ means

$$t_R(x, y, z) = x + y \cdot (1 + z).$$

Formulas $\varphi(\boldsymbol{v})$ can be interpreted as subsets $\varphi(M)$ of M^m including semi-algebraic sets $f = 0$, $f > 0$. Such subsets are called **definable sets**. Sentences are statements about these structures that can be true or false, e.g. $\exists x, f(x) > 0$
.

For the sake of exposition we will identify the symbols in a language with their interpretation in a structure.

Notation. For a sentence φ, by $\varphi \models M$ we mean that φ is true in M. More generally, for any formula φ in m variables and $a \in M^m$ we write $M \models \varphi(\boldsymbol{a})$ iff $\boldsymbol{a} \in \varphi(M)$.

Definition (Definable sets with parameters).

For a formula $\varphi(\boldsymbol{x}, \boldsymbol{y})$ with two sets of variables, and $\boldsymbol{b}$ a $\boldsymbol{y}$-tuple in M, we write

$$\varphi(M, \boldsymbol{b}) = \{\boldsymbol{a} : M \models \varphi(\boldsymbol{a}, \boldsymbol{b})\}.$$

Sets of this form are called definable sets with parameters.

Definable sets with parameters in M include algebraic sets defined by polynomial equations with arbitrary coefficients in M, but also things like

$$\{x \in M : \exists\, y,\ f(x, y) = 0\}$$

which are usually not algebraic sets. However, Tarski and Seidenberg showed that, definable sets with parameters in $\mathbb{R}$ in $\mathscr{L}_{\text{or}}$ are precisely semi-algebraic sets, that is, finite union of

$$\{\mathbf{x} \in \mathbb{R}^m : f_1(\mathbf{x}) = 0, f_2(\mathbf{x}) > 0, \ldots, f_k(\mathbf{x}) > 0\}$$

with $f_i(\mathbf{x}) \in \mathbb{R}[x_1, \ldots, x_m]$. We will always refer to definability with parameters.

A *theory* $\mathscr{T}$ in the language $\mathscr{L}$ is a collection of $\mathscr{L}$-sentences. A *model* for $\mathscr{T}$ is an $\mathscr{L}$-structure that satisfies every sentence in $\mathscr{T}$. For instance, in $\mathscr{L}_{\text{ring}}$ one can express the axioms of a ring, commutative ring, field, etc.
Two of the main objectives of model theory:

- Given a language $\mathscr{L}$ and a theory $\mathscr{T}$, classify the models of $\mathscr{T}$;
- Given a language $\mathscr{L}$ and a structure M, analyze the definable sets of M.
  We will focus here on the second one.

Why this formalism...? Model theory is a new way of doing or thinking about mathematics! Unfortunately I do not have time to go further along this direction in today's talk.

§ 2. O-minimal structures

Semi-algebraic subsets of $\mathbb{R}$ are particularly simple -- finite union of points and open intervals. This basic fact is the starting point of the modern model-theoretic approach to $\mathbb{R}$.

Definition (O-minimal structures).

Let $\mathscr{L}$ be a language containing a binary relation $\leq$. Then an $\mathscr{L}$-structure M is called o-minimal if

- $\leq$ is interpreted as a dense, linear (a.k.a. total) order without end points.
- The definable sets $X \subset M$ are finite unions of points and open intervals $\{x \in M : a < x < b\}$ (a (resp. b) is allowed to be $-\infty$ (resp. $+\infty$)).

Why o-minimality? Definable sets over o-minimal structures are very well-behaved -- they have many of the good topological and geometric properties of the semi-algebraic sets, which allows for a rich theory that generalizes real algebraic geometry. Some results that can be proved in this generality are

- existence of cell decompositions,
- a good theory of dimension,
- finiteness of connected components,
- and parametrization results,
- $\cdots$

  A cool result by Pillay: if G is a definable group, then it is definably isomorphic to a Lie group.

Remark. Unlike algebraic geometry (resp. differential topology) where one has a powerful toolkit of commutative algebra (resp. calculus), working with foundations of o-minimal structures can often be technical and tedious :((e.g. try to express continuity by a 1st order formula)

What are examples of o-minimal structures?

- Of course, Tarski--Seidenberg implies that $\mathbb{R}$ is o-minimal as an $\mathscr{L}_{\text{or}}$-structure.
- If the language is simple enough, e.g. $\mathscr{L} = \{(\leq, 2)\}$, then $\mathbb{Q}$ is o-minimal. But are there other interesting ones?
- (Denef--van der Dries, '88) the first new example of an o-minimal structure: $\mathbb{R}$ is o-minimal as an $\mathscr{L}_{\text{an}}$-structure, where $\mathscr{L}_{\text{an}}$ is expanded from $\mathscr{L}_{\text{or}}$ by

"adding all analytic functions" on $[0,1]^n$. *Looks unnatural, but maybe one motivation comes from the study of sub-analytic sets, which were well-understood at that time*

- (Wilkie, '91) Let $\mathscr{L}_{\exp} = \mathscr{L}_{\text{or}} \cup \{\exp\}$, then $\mathbb{R}$ is o-minimal also as an $\mathscr{L}_{\exp}$-structure, where $\exp$ is interpreted as the usual exponential function on $\mathbb{R}$.
- $\mathbb{R}$ is o-minimal as an $\mathscr{L}_{\text{an,exp}}$-structure.
  We will see that these results are useful!

§ 3. The Pila--Wilkie Theorem and its applications

Theorem (Pila--Wilkie, '06).

Let $\mathscr{L}$ be a language extending $\mathscr{L}_{\text{or}}$ such that $\mathbb{R}$ is o-minimal as an $\mathscr{L}$-structure. Let $X \subset \mathbb{R}^m$ be a definable set. Then for any $\epsilon > 0$, there exists $c = c(X, \epsilon) \geq 0$ such that

$$\# X^{\text{tr}}(B) \leq c B^{\epsilon}$$

for all $B \geq 1$. Where, X^{tr} denotes the "transcendental part" of X and $X^{\text{tr}}(B)$ denotes points of height bounded by B.

Given a subset $X \subset \mathbb{R}^m$, an **algebraic piece** of X is an infinite, connected, $\mathscr{L}_{\text{or}}$-definable (thus semi-algebraic) subset of X. The union of all algebraic pieces of X is called the **algebraic part** of X, denoted X^{alg}. The complement $X \setminus X^{\text{alg}} =: X^{\text{tr}}$ is called the **transcendental part** of X. For instance, consider

$$X = \{(x, y, z) \in \mathbb{R}^3 : x > 0, z = x^y\}.$$

Its algebraic part would be $X^{\text{alg}} = \bigcup_{y \in \mathbb{Q}} \{(x, y, z) \in \mathbb{R}^3 : x > 0, z = x^y\}$ since $z = x^r \Leftrightarrow z^b = x^a$ for $r = a/b \in \mathbb{Q}$.

Point-counting theorems in o-minimal structures like this have found remarkable and unexpected applications in Diophantine geometry, in the context of **unlikely intersections**. Prototype:

Theorem (Laurent, '79).

Let $X \subset (\mathbb{C}^\times)^n$ be an irreducibe algebraic variety. If X_{tors} is Zariski-dense in X, then there exists some $x_0 \in X_{\mathrm{tors}}$ and $G \subset (\mathbb{C}^\times)^n$ an algebraic group such that

$$X = x_0 G.$$

Remark.

1. If X is of the form $x_0 G$, then not hard to see that X_{tors} is dense in X.
2. This is a special case of the Mordell--Lang conjecture: Let X be a complex subvariety of a complex Abelian variety A and let Γ be a subgroup of finite rank in A. If $X \cap \Gamma$ is Zariski-dense in X, then X is a translate of an Abelian subvariety by a point in Γ.

How does Pila--Wilkie come into play?

Key idea: consider the surjective map

$$e : \mathbb{C}^n \to (\mathbb{C}^\times)^n, (z_j) \mapsto (e^{2\pi i z_j})$$

and the pre-image $\widetilde{X} := e^{-1}(X)$ of X. Set $D = ([0,1) + i\mathbb{R})^n \subset \mathbb{C}^n$. Note that e induces a bijection between rational points of D and torsion points of $(\mathbb{C}^\times)^n$.

- (Point counting) Note that the set

  $$Y = \widetilde{X} \cap D \subset \mathbb{C}^n \simeq \mathbb{R}^{2n}$$

  is definable in the language

  $$\mathscr{L}_{\mathrm{exp,sin}} = \mathscr{L}_{\mathrm{exp}} \cup \{\sin|_{[0,2\pi]}\}.$$

  By Pila--Wilkie, $Y^{\mathrm{tr}}(B) \le cB^\epsilon$ for all $B \geq 1$ ($\mathbb{R}$ is o-minimal w.r.t. $\mathscr{L}_{\mathrm{exp,sin}}$ (Wilkie--Miller, '94)).
- (Large Galois orbits) If X_{tors} is Zariski-dense, then can show that $Y(B)$ grows faster than above by considering Galois orbits of these points, so $\widetilde{X}^{\mathrm{alg}} \neq \emptyset$. Thus, $\widetilde{X}^{\mathrm{alg}}$ contains an infinite semi-algebraic set A such that $e(A) \subset X$ is algebraic}.
- (Functional Transcendence) However, transcendental number theory us that this should not happen frequently (c.f. Lindemann--Weierstrass 1880: if α_i's

are algebraic and linearly independent over $\mathbb{Q}$, then e^{α_i}'s are algebraically independent over $\mathbb{Q}$).

This is now referred to in the literature as the "Pila--Zannier strategy".

Further generalizations.

- The Manin--Mumford conjecture (Raynaud's theorem, '83) -- If C is a curve of genus ≥ 2 over a number field K, embedded in its Jacobian J, then the set $C(\overline{K}) \cap J(\overline{K})_{\text{tors}}$ is finite. **Hrushovski '95 gave a different proof using model theory.**
- The André--Oort conjecture -- non-Abelian analogue of Manin–-Mumford, "if a subvariety of a Shimura variety contains too many special points, then it must be special". Partial results by Klingler, Ullmo, Yafaev, ... **Pila, Shankar, and Tsimerman announced a full proof in 2021 using the Pila--Zannier strategy.**
- The Zilber--Pink conjecture -- a far-reaching generalization of many famous Diophantine conjectures and statements including all above... wide open

Flavor: Given an ambient algebraic object G and an algebraic subvariety $X \subset G$. In G, there are certain "special points" and "special subvarieties". If X contains many special points, then it should contain a special subvariety.

$\S\, 4$. Leftovers

- Fun with model theory
  - Sela; Kharlampovich--Myasnkov '06: "1st logic can not tell free groups on n ($n \geq 2$) generators apart"!
  - Hilbert's 17th problem: Is every non-negative polynomial in $\mathbb{R}[x_1, \ldots, x_n]$ a sum of squares of rational polynomials? (Yes, Artin '30; beautiful model-theoretic proof)
  - a model-theoretic proof of Hilbert's Nullstellensatz.
  - Ax--Grothendieck theorem: Let X be an algebraic variety over an algebraically closed field k. If a morphism $X \to X$ is injective, then it is also surjective.
- O-minimal structures

- lattice counting problems -- (Barroero--Widmer, '12) o-minimality is applied to improve results on asymptotic lattice points counting formulas
- Diophantine equations -- (Frei--Pieropan, '13) using the previous result, certain case of Manin's conjecture is proved (using $\mathscr{L}_{\mathrm{exp}}$)
- Harmonic analysis -- (Basu--Guo--Zhang--Zorin-Karnich, '21) estimate oscillatory integrals better (using $\mathscr{L}_{\mathrm{an,exp}}$)
- Hodge theory -- (Peterzil--Starchenko, '09) "o-minimal Chow's theorem"; (Bakker--Brunebarbe--Tsimerman) "o-minimal GAGA type theorem", and there are important applications to Hodge theory, e.g. Ax--Schanuel theorem ---> Lawrence & Venkatesh's new proof of Mordell's conjecture
- o-minimal algebraic topology, o-minimality and differential equations, o-minimal homogeneous dynamics, motivic integration(?)