The Unreasonable Effectiveness of Model Theory in Number Theory

John T. Baldwin
University of Illinois at Chicago

May 19, 2016

Unreasonable Effectiveness

Wigner 

Wigner writes,

> *The first point is that ~~mathematical~~ model theoretic concepts turn up in entirely unexpected connections. Moreover, they often permit an unexpectedly close and accurate description of the phenomena in these connections.*

We mean effective in Wigner's colloquial sense, not constructive or recursive.

Section I

Axiomatization vrs Formalization

Bourbaki on Axiomatization:

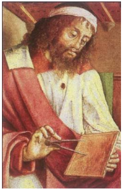
Dieudonne  Bourbaki  Cartan 

Bourbaki wrote:

> *'We emphasize that it [formalization] is but one aspect of this [the axiomatic] method, indeed the least interesting one.'*

We reverse Bourbaki's aphorism to argue.
Full formalization is an important tool for modern mathematics.

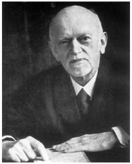
Euclid-Hilbert formalization 1900:

Euclid  Hilbert 

The Euclid-Hilbert (the Hilbert of the Grundlagen) framework has the notions of axioms, definitions, proofs and, with Hilbert, models.

But the arguments and statements take place in natural language. For Euclid-Hilbert logic is a means of proof.

Hilbert-Gödel-Tarski-Vaught formalization 1917-1956:

Hilbert  Gödel  Tarski  Vaught 

In the Hilbert (the founder of proof theory)-Gödel-Tarski framework, logic is a mathematical subject.

There are explicit rules for defining a formal language and proof. Semantics is defined set-theoretically.

Formalization

Anachronistically, *full formalization* involves the following components.

1. Vocabulary: specification of primitive notions.
2. Logic
   - a Specify a class of well formed formulas.
   - b Specify truth of a formula from this class in a structure.
   - c Specify the notion of a formal deduction for these sentences.
3. Axioms: specify the basic properties of the situation in question by sentences of the logic.

Item 2c) is the least important from our standpoint.

Two theses

Theses

1. Contemporary model theory makes formalization of specific mathematical areas a powerful tool to investigate both mathematical problems and issues in the philosophy of mathematics (e.g. methodology, axiomatization, purity, categoricity and completeness).
2. Contemporary model theory enables systematic comparison of local formalizations for distinct mathematical areas in order to organize and do mathematics, and to analyze mathematical practice.

II. The Methods of Model Theory

The ingredients of effectiveness

1. interpretation Hilbert- Malcev-Tarski – everywhere
2. formal definability – quantifier reduction
3. theories - understanding families of related structures
4. The paradigm shift: the partition of first order theories by syntactic properties specifying mathematically significant properties of the theories;
5. structure of definable sets
   - a stable theories: rank, one based, chain conditions; geometric analysis of models
   - b o-minimal theories: cell decomposition, uniformly bounded fibrations
   - c p-adics: cell decomposition

Interpretation I:

Borovik  Nesin 

In Borovik-Nesin: Groups of Finite Morley Rank:

> *The notion of interpretation in model theory corresponds to a number of familiar phenomena in algebra which are often considered distinct: coordinatization, structure theory, and constructions like direct product and homomorphic image.*

1. a Desarguesian projective plane is coordinatized by a division ring
2. Artinian semisimple rings are finite direct products of matrix rings over division rings;
3. classifying abstract groups as a standard family of matrix groups

Interpretation II

> *All of these examples have a common feature: certain structures of one kind are somehow encoded in terms of structures of another kind.*
> *All of these examples have a further feature which plays no role in algebra but which is crucial for us: in each case the encoded structures can be recovered from the encoding structures definably.*

'plays no role': written in 1994 -no longer true

Structures and Definability

A vocabulary τ is collection of constant, relation, and function symbols.

A τ-structure is a set in which each τ-symbol is interpreted.

A subset A of a τ-structure M is definable in M if there is $\mathbf{n} \in M$ and a τ-formula $\phi(x, \mathbf{y})$ such that

$$A = \{m \in M : M \models \phi(m, \mathbf{n})\}.$$

Note that if property is defined without parameters in M, then it is uniformly defined in all models of $\mathrm{Th}(M)$.

The Significance of Classes of Theories : Definability

Tarski  Robinson 

Quantifier Elimination and Model Completeness

Every definable formula is equivalent to quantifier-free (resp. existential) formula.

The Significance of Classes of Theories : Definability

Tarski  Robinson 

Quantifier Elimination and Model Completeness

Every definable formula is equivalent to quantifier-free (resp. existential) formula.

Tarski proved quantifier elimination of the reals in 1931.

Such a condition provides a general format for Nullstellensatz-like theorems.

Robinson provides a unified treatment of Hilbert's Nullstellensatz and the Artin-Schreier theorem which led to the notion of differentially closed fields.

The Paradigm Shift

The paradigm around 1950

the study of logics; the principal results were completeness, compactness, interpolation and joint consistency theorems.

Various semantic properties of theories were given syntactic characterizations but there was no notion of partitioning all theories by a family of properties.

The Paradigm Shift

The paradigm around 1950

the study of logics; the principal results were completeness, compactness, interpolation and joint consistency theorems.

Various semantic properties of theories were given syntactic characterizations but there was no notion of partitioning all theories by a family of properties.

After the paradigm shift

There is a systematic search for a finite set of syntactic conditions which divide first order theories into disjoint classes such that models of different theories in the same class have similar mathematical properties.

After the shift one can compare different areas of mathematics by checking where theories formalizing them lie in the classification.

The significance of classes of Theories

The breakthroughs of model theory as a tool for organizing mathematics come in several steps.

1. The significance of (complete) first order theories.
2. The significance of classes of (complete) first order theories: Quantifier reduction

The significance of classes of Theories

The breakthroughs of model theory as a tool for organizing mathematics come in several steps.

1. The significance of (complete) first order theories.
2. The significance of classes of (complete) first order theories: Quantifier reduction

East Coast Quantifier reduction in a natural vocabulary is crucial for applications.

West Coast Quantifier elimination by fiat exposes the fundamental model theoretic structure.

The significance of classes of Theories

The breakthroughs of model theory as a tool for organizing mathematics come in several steps.

1. The significance of (complete) first order theories.
2. The significance of classes of (complete) first order theories: Quantifier reduction

   East Coast: Quantifier reduction in a natural vocabulary is crucial for applications.

   West Coast: Quantifier elimination by fiat exposes the fundamental model theoretic structure.

3. The significance of classes of (complete) first order theories: syntactic dividing lines

Shelah on Dividing Lines: Shelah 

I am grateful for this great honour. While it is great to find full understanding of that for which we have considerable knowledge, I have been attracted to trying to find some order in the darkness, more specifically,
finding meaningful dividing lines among general families of structures.
This means that there are
meaningful things to be said on both sides of the divide:
characteristically, understanding the tame ones and giving evidence of being complicated for the chaotic ones.

Shelah on Dividing Lines

> *It is expected that this will eventually help*
>
> *in understanding even specific classes and even specific structures.*
>
> *Some others see this as the aim of model theory, not so for me.*
>
> *Still I expect and welcome such applications and interactions. It is a happy day for me that this line of thought has received such honourable recognition. Thank you*

on receiving the Steele prize for seminal contributions.

Properties of classes of theories

The Stability Hierarchy

Every complete first order theory falls into one of the following 4 classes.

1. ω-stable
2. superstable but not ω-stable
3. stable but not superstable
4. unstable

Stability is Syntactic

Definition

T is stable if no formula has the order property in any model of T.

ϕ is unstable in T just if for every n the sentence
$\exists x_1, \ldots x_n \exists y_1, \ldots y_n \bigwedge_{i<j} \phi(x_i, y_i) \wedge \bigwedge_{j \geq i} \neg\phi(x_i, y_i)$ is in T.

This formula changes from theory to theory.

1. dense linear order: $x < y$;
2. real closed field: $(\exists z)(x + z^2 = y)$,
3. $(\mathbb{Z}, +, 0, \times)$:$(\exists z_1, z_2, z_3, z_4)(x + (z_1^2 + z_2^2 + z_3^2 + z_4^2) = y)$.
4. infinite boolean algebras: $x \neq y$ & $(x \wedge y) = x$.

These syntactic conditions are Wigner's connections.

The stability hierarchy: examples: Conant

http://www.forkinganddividing.com/

ω-stable

Algebraically closed fields (fixed characteristic), differentially closed fields (infinite rank), compact complex manifolds

strictly superstable

$(\mathbb{Z}, +)$, $(2^\omega, +) = (Z_2^\omega, H_i)_{i<\omega}$.

strictly stable

$(\mathbb{Z}, +)^\omega$, separably closed fields, the free group on 2 generators

Saturated Models

Saturated models

Saturated models are a natural generalization of Weil's notion of 'universal domain', that clarify concepts and simplify proofs in many situations.

The syntactic definition of saturation is a crucial tool.

The wild world of mathematics

Point

Martin Davis wrote, ”Gödel showed us that the wild infinite could not really be separated from the tame mathematical world where most mathematicians may prefer to pitch their tents.”

The wild world of mathematics

Point

Martin Davis wrote, "Gödel showed us that the wild infinite could not really be separated from the tame mathematical world where most mathematicians may prefer to pitch their tents."

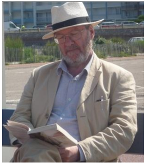
Counterpoint

In fact we show how to systematically make this separation in important cases.
What "Gödel showed us that the wild infinite could not really be separated from the tame mathematical world if we insist on starting with the wild worlds of arithmetic or set theory.

The crucial contrast is between a foundationalist approach – a demand for global foundations
and a foundational approach – a search for mathematically important foundations of different topics.

Tame theories

1. superstable
   1. ranks - that interact with ones defined by algebraists
   2. definable chain conditions on subgroups; this gives a notion of closed subgroup in model theory corresponding to the Zariski closure in algebraic geometry.
   3. NO pairing function – some chance at dimension
   4. structure of definable sets
2. stable
   1. an independence relation (non-forking)
   2. general notion of ‘generic element’ (realizes a non-forking extension)
   3. dimension on ‘regular’ types
3. o-minimal ordered structures
4. neo-stability theory: simple and NIP (no independence property)
5. local tameness – a tame piece of a model can be exploited



o-minimality Wilkie

Wilkie to Bourbaki:

> *It [o-minimality] is best motivated as being a candidate for Grothendieck's idea of tame topology as expounded in his Esquisse d'un Programme. It seems to me that such a candidate should satisfy (at least) the following criteria.*

A A flexible framework to carry out many geometrical and topological constructions on real functions and on subsets of real euclidean spaces.

B It should have built in restrictions to block pathological phenomena. There should be a meaningful notion of dimension for all sets under consideration and any that can be constructed from these by use of the operations allowed under (A).

o-minimality continued

C One must be able to prove finiteness theorems that are uniform over fibred collections.

Rather than enumerate analytic conditions on sets and functions sufficient to guarantee the criteria (A), (B) and (C) however, we shall give one succinct axiom, the o-minimality axiom, which implies them.

Above paraphased/quoted from a Wilkie Bourbaki seminar.

o-minimality continued

C One must be able to prove finiteness theorems that are uniform over fibred collections.

Rather than enumerate analytic conditions on sets and functions sufficient to guarantee the criteria (A), (B) and (C) however, we shall give one succinct axiom, the o-minimality axiom, which implies them.

Above paraphased/quoted from a Wilkie Bourbaki seminar.

Note Bene

o-minimality is not an axiom.

It is a syntactic property defining a class of theories – just as the stability conditions above.
Every definable set is a Boolean combination of intervals

O-minimal structures: examples

$\mathfrak{R}_{\mathsf{alg}} = (\mathfrak{R}; <, 0, 1, +, \times)$

TARSKI, 1940s

O-minimal structures: examples

$\mathfrak{R}_{\mathrm{an}} = \left(\mathfrak{R}_{\mathrm{alg}}, \left\{f\colon [-1,1]^n \to \mathfrak{R}\right.\right.$ restricted analytic, $\left.\left. n \in \mathbb{N}^{\geq 1}\right\}\right)$

VAN DEN DRIES, 1986

VAN DEN DRIES-DENEF, 1988

$\mathfrak{R}_{\mathrm{alg}} = (\mathfrak{R}; <, 0, 1, +, \times)$

TARSKI, 1940s

O-minimal structures: examples

$\mathfrak{R}_{\text{an}} = \big(\mathfrak{R}_{\text{alg}}, \{f \colon [-1,1]^n \to \mathfrak{R}$ restricted analytic, $n \in \mathbb{N}^{\geq 1}\}\big)$

VAN DEN DRIES, 1986

VAN DEN DRIES-DENEF, 1988

$\mathfrak{R}_{\text{exp}} = (\mathfrak{R}_{\text{alg}}, \exp)$

WILKIE, 1991

$\mathfrak{R}_{\text{alg}} = (\mathfrak{R}; <, 0, 1, +, \times)$

TARSKI, 1940s

O-minimal structures: examples

$\mathfrak{R}_{\text{an,exp}} = (\mathfrak{R}_{\text{an}}, \exp)$

VAN DEN DRIES-MILLER, 1992

MACINTYRE-MARKER-VAN DEN DRIES, 1994

$\mathfrak{R}_{\text{an}} = \left(\mathfrak{R}_{\text{alg}}, \left\{f\colon [-1,1]^n \to \mathfrak{R} \text{ restricted analytic, } n \in \mathbb{N}^{\geq 1}\right\}\right)$

VAN DEN DRIES, 1986

VAN DEN DRIES-DENEF, 1988

$\mathfrak{R}_{\text{exp}} = (\mathfrak{R}_{\text{alg}}, \exp)$

WILKIE, 1991

$\mathfrak{R}_{\text{alg}} = (\mathfrak{R}; <, 0, 1, +, \times)$

TARSKI, 1940s

O-minimal structures: examples

$\Re_{\text{an,exp}} = (\Re_{\text{an}}, \exp)$

VAN DEN DRIES-MILLER, 1992

MACINTYRE-MARKER-VAN DEN DRIES, 1994

$\Re_{\text{an}} = \left(\Re_{\text{alg}}, \left\{f\colon [-1,1]^n \to \Re \text{ restricted analytic, } n \in \mathbb{N}^{\geq 1}\right\}\right)$

VAN DEN DRIES, 1986

VAN DEN DRIES-DENEF, 1988

$\Re_{\text{exp}} = (\Re_{\text{alg}}, \exp)$

WILKIE, 1991

semialgebraic sets →

$\Re_{\text{alg}} = (\Re; <, 0, 1, +, \times)$

TARSKI, 1940s

III. Unreasonable effectiveness in number theory

III.A From Diophantus to the 20th century

Diophantine geometry

Diophantus: Find integer solutions to an equation: e.g. $x^n + y^n = z^n$.

Modern approach: Solve the wild by embedding in the tame

Study a variety $V \subseteq \mathcal{C}^n$ and look at its integral solutions.

The integer solutions are in a wild structure.

Diophantine geometry

Diophantus: Find integer solutions to an equation: e.g. $x^n + y^n = z^n$.

Modern approach: Solve the wild by embedding in the tame

Study a variety $V \subseteq \mathcal{C}^n$ and look at its integral solutions.

The integer solutions are in a wild structure.

The variety is studied in the tame structure $\mathcal{C}$.

From varieties to groups

Motivated by the natural addition on elliptic curves, Mordell and Weil transformed the problem into finding rational solutions of algebraic groups

Theorem: Jacobians exist

To a curve C of genus $g \geq 1$ there is a naturally associated g-dimensional abelian variety, J_C, called the Jacobian of C.

Then $C(\mathbb{Q})$ is infinite if and only if $C'(\mathbb{Q}) = C'(\mathcal{C}) \cap J_C(\mathbb{Q})$ is infinite, where the associated C' is biregularly isomorphic to C.

Abelian varieties

Definition/Theorem: Abelian variety

An abelian variety is a connected projective algebraic group.

Mordell-Weil Theorem

In an abelian variety A over a number field K, the group $A(K)$ of K-rational points of A is a finitely-generated abelian group, Γ.

III.B. Mordell-Lang conjectures: stable theories

Application to Mordell-Lang

Pillay 

Pillay explains the diophantine geometry connection as follows.

> *The use of model-theoretic and stability-theoretic methods should not be so surprising, as the full Lang conjecture itself is equivalent to a purely model-theoretic statement. The structure $(\mathbb{Q}, +, \cdot)$ is wild (undecidable, definable sets have no structure, etc.), as is the structure $(\mathcal{C}, +, \cdot)$ with a predicate for the rationals. What comes out of the diophantine type conjectures however is that* certain *enrichments of the structure $(\mathcal{C}, +, \cdot)$ . . . are not wild, in particular are stable.*

Consider $(\mathcal{C}, +, \cdot, \Gamma)$ where Γ is the finitely generated group from Mordell-Weil.

The Mordell-Lang conjectures

Hrushovski

Falting's theorem

Let G be a semiabelian variety defined over the field of complex numbers $\mathcal{C}$. Let $X \subset G$ be a closed subvariety and $\Gamma \subset G(\mathcal{C})$ a finitely generated subgroup of the group of $\mathcal{C}$-points on G.

Then $X(\mathcal{C}) \cap \Gamma$ is a finite union of cosets of subgroups of Γ.

The Mordell-Lang conjectures

Hrushovski 

Falting's theorem

Let G be a semiabelian variety defined over the field of complex numbers $\mathcal{C}$. Let $X \subset G$ be a closed subvariety and $\Gamma \subset G(\mathcal{C})$ a finitely generated subgroup of the group of $\mathcal{C}$-points on G.

Then $X(\mathcal{C}) \cap \Gamma$ is a finite union of cosets of subgroups of Γ.

Rephrased by Pillay (Moosa-Scanlon)

Let G be a semiabelian variety defined over the field of complex numbers $\mathcal{C}$ and $\Gamma \subset G(\mathcal{C})$ is a finitely generated subgroup of the group of $\mathcal{C}$-points on G.

Then the induced structure on Γ is stable and weakly normal.

This doesn't mean there is a model theoretic proof.

The Model theoretic connection

Definition

A definable set X is weakly normal if the intersection of every infinite family of distinct conjugates of X is empty.

A theory is weakly normal if each formula is a Boolean combination of weakly minimal formulas.

General Model Theoretic Fact

In a weakly normal group G, every definable subset of G^n is a Boolean combination of $\mathrm{acl}(\emptyset)$-definable subgroups of G^n.

Characteristic p -case Moosa  Scanlon 

The direct translation of Mordell-Lang to characteristic p is blatantly false. Hrushovski proved a relativized version. The following later version makes the analogies closer.

Moosa-Scanlon version

Let G be a semiabelian variety defined over a finite field, $F : G \rightarrow G$ the corresponding Frobenius morphism, and K an algebraically closed field extending the field of definition of G.

If $\Gamma \leq G(K)$ is a finitely generated $Z[F]$-submodule of $G(K)$ and $X \subset G$ is a closed subvariety, then $X(K) \cap \Gamma$ is a finite union of (cycle-free) F-sets.

Hrushovski's proof used the model theoretic analysis of differentially closed field (ω-stable) and separably closed fields (strictly stable).

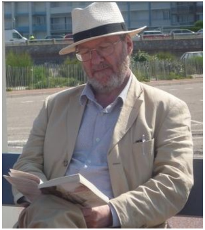
III.C. André-Oort conjecture: o-minimality

Half of the 2013 Karp prize was awarded to Kobi Peterzil, Jonathan Pila, Sergei Starchenko, and Alex Wilkie for 'their efforts in turning the theory of o-minimality into a sharp tool for attacking conjectures in number theory, which culminated in the solution of important special cases of the André-Oort Conjecture by Pila.'

KOBI PETERZIL

JONATHAN PILA

SERGEI STARCHENKO



ALEX WILKIE

The next group of slides are borrowed with permission for Matthias Aschenbrenner wonderful talk presenting the prize.

21st century: Special points and varieties

Contemporary approach: Given an interesting set $\Gamma \subset \mathcal{C}$, how does the geometry of V influence the structure of $V(\Gamma \cap C^n)$?

A general principle

If V is a special variety and $X \subset V$ is a variety which contains a dense set of special points, then X, too, has to be special. (Whatever special means.)

Diophantine Geometry

Here is an archetypical example of the “general principle.” Pila’s theorem requires to much terminology to be stated here.
Put

$$\mathbb{U} := \left\{ z \in \mathcal{C} : z^n = 1 \text{ for some } n \geq 1 \right\} \qquad \text{(roots of unity).}$$

The elements of $\mathbb{U}$ are our *special points.*

Diophantine Geometry

Here is an archetypical example of the "general principle." Pila's theorem requires to much terminology to be stated here.
Put

$$\mathbb{U} := \left\{ z \in \mathcal{C} : z^n = 1 \text{ for some } n \geq 1 \right\} \qquad \text{(roots of unity).}$$

The elements of $\mathbb{U}$ are our *special points.*

Theorem (Laurent, 1984)

Let $X \subseteq (\mathcal{C}^\times)^n$ be irreducible. If $X(\mathbb{U})$ is dense in X, then X is defined by equations

$$X_1^{\alpha_1} \cdots X_n^{\alpha_n} = b \qquad (\alpha_1, \ldots, \alpha_n \in \mathbb{Z},\ b \in \mathbb{U}).$$

Diophantine Geometry

Here is an archetypical example of the "general principle." Pila's theorem requires to much terminology to be stated here.
Put

$$\mathbb{U} := \{z \in \mathcal{C} : z^n = 1 \text{ for some } n \geq 1\} \qquad \text{(roots of unity)}.$$

The elements of $\mathbb{U}$ are our *special points.*

Theorem (LAURENT, 1984)

Let $X \subseteq (\mathcal{C}^\times)^n$ be irreducible. If $X(\mathbb{U})$ is dense in X, then X is defined by equations

$$X_1^{\alpha_1} \cdots X_n^{\alpha_n} = b \qquad (\alpha_1, \ldots, \alpha_n \in \mathbb{Z},\ b \in \mathbb{U}).$$

This is an instance of the MANIN-MUMFORD Conjecture (= RAYNAUD's Theorem). The PILA-ZANNIER method (extended by PETERZIL-STARCHENKO) gives (yet) another proof.

The method of PILA-ZANNIER

The main idea

- We have an analytic surjection

$$e\colon \mathcal{C}^n \to (\mathcal{C}^\times)^n, \qquad e(z_1,\dots,z_n) = (e^{2\pi i z_1},\dots,e^{2\pi i z_n}).$$

The method of Pila-Zannier

The main idea

- We have an analytic surjection

$$e\colon \mathcal{C}^n \to (\mathcal{C}^\times)^n, \qquad e(z_1, \ldots, z_n) = (e^{2\pi i z_1}, \ldots, e^{2\pi i z_n}).$$

Note: $\zeta \in \mathbb{U}^n \iff \zeta = e(z)$ for some $z \in \mathbb{Q}^n$.

The method of PILA-ZANNIER

The main idea

- We have an analytic surjection

$$e\colon \mathcal{C}^n \to (\mathcal{C}^\times)^n, \qquad e(z_1, \ldots, z_n) = (e^{2\pi i z_1}, \ldots, e^{2\pi i z_n}).$$

Note: $\zeta \in \mathbb{U}^n \iff \zeta = e(z)$ for some $z \in \mathbb{Q}^n$.

- e has a fundamental domain:

$$D := \{(z_1, \ldots, z_n) \in \mathcal{C}^n : 0 \leq \mathrm{Re}(z_i) < 1 \text{ for each } i\}.$$

The method of PILA-ZANNIER

The main idea

- We have an analytic surjection

$$e\colon \mathcal{C}^n \to (\mathcal{C}^\times)^n, \qquad e(z_1, \ldots, z_n) = (e^{2\pi i z_1}, \ldots, e^{2\pi i z_n}).$$

  Note: $\zeta \in \mathbb{U}^n \iff \zeta = e(z)$ for some $z \in \mathbb{Q}^n$.
- e has a fundamental domain:

$$D := \{(z_1, \ldots, z_n) \in \mathcal{C}^n : 0 \leq \mathrm{Re}(z_i) < 1 \text{ for each } i\}.$$

  Then with $\tilde{e} := e \restriction D$, we still have

$$\zeta \in \mathbb{U}^n \iff \zeta = \tilde{e}(z) \text{ for some } z \in D \cap \mathbb{Q}^n.$$

The method of PILA-ZANNIER

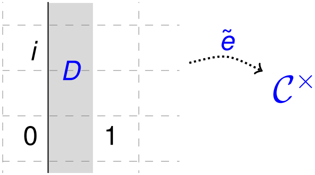
e is "logically" badly behaved (its kernel is $\mathbb{Z}^n$), but $\tilde{e}$ and thus

$$\tilde{X} := \tilde{e}^{-1}(X)$$

are definable in the o-minimal structure

$$(\Re; <, 0, 1, +, \times, \exp, \sin \restriction [0, 2\pi]),$$

with $\tilde{X}(\mathbb{Q}) = \tilde{e}^{-1}(X(\mathbb{U}))$.



(Identify $\mathcal{C}$ with $\Re^2$.)

$$e^{a+ib} = e^a(\cos b + i \sin b)$$

The method of PILA-ZANNIER

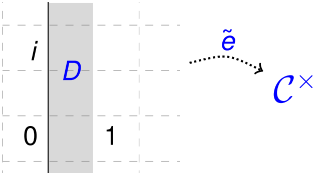
e is "logically" badly behaved (its kernel is $\mathbb{Z}^n$), but $\tilde{e}$ and thus

$$\tilde{X} := \tilde{e}^{\,-1}(X)$$

are definable in the o-minimal structure

$$(\Re; <, 0, 1, +, \times, \exp, \sin \restriction [0, 2\pi]),$$

with $\tilde{X}(\mathbb{Q}) = \tilde{e}^{-1}(X(\mathbb{U}))$.



(Identify $\mathcal{C}$ with $\Re^2$.)

$$e^{a+ib} = e^a(\cos b + i \sin b)$$

(Definability in an o-minimal structure is obvious in this case, but by far non-obvious in many other applications of the PILA-ZANNIER method $\rightarrow$ PETERZIL-STARCHENKO.)

The method of PILA-ZANNIER

Split $$\tilde{X} = \underbrace{\tilde{X}^{\text{alg}}}_{\text{algebraic part}} \ \dot{\cup} \ \underbrace{\tilde{X}^{\text{trans}}}_{\text{transcendental part}}$$ (to be defined).

The method of PILA-ZANNIER

Split $\tilde{X} = \underbrace{\tilde{X}^{\text{alg}}}_{\text{algebraic part}} \dot{\cup} \underbrace{\tilde{X}^{\text{trans}}}_{\text{transcendental part}}$ (to be defined).

Strategy

1. The upper bound: *Prove that $\tilde{X}^{\text{trans}}(\mathbb{Q})$ is "small."*

The method of PILA-ZANNIER

Split $\tilde{X} = \underbrace{\tilde{X}^{\text{alg}}}_{\text{algebraic part}} \dot{\cup} \underbrace{\tilde{X}^{\text{trans}}}_{\text{transcendental part}}$ (to be defined).

Strategy

1. The upper bound: *Prove that $\tilde{X}^{\text{trans}}(\mathbb{Q})$ is "small."*
2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that $\tilde{X}^{\text{trans}}(\mathbb{Q})$ actually is finite.*

The method of PILA-ZANNIER

Split $\tilde{X} = \underbrace{\tilde{X}^{\text{alg}}}_{\text{algebraic part}} \dot{\cup} \underbrace{\tilde{X}^{\text{trans}}}_{\text{transcendental part}}$ (to be defined).

Strategy

1. The upper bound: *Prove that $\tilde{X}^{\text{trans}}(\mathbb{Q})$ is "small."*
2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that $\tilde{X}^{\text{trans}}(\mathbb{Q})$ actually is finite.*
3. Analyze $\tilde{X}^{\text{alg}}(\mathbb{Q})$: Let A be a variety contained in $e^{-1}(X)$; take such A maximal and irreducible. *Show that A is an affine subspace of $\mathcal{C}^n$ defined over $\mathbb{Q}$.*

The method of PILA-ZANNIER

Split $\tilde{X} = \underbrace{\tilde{X}^{\text{alg}}}_{\text{algebraic part}} \dot{\cup} \underbrace{\tilde{X}^{\text{trans}}}_{\text{transcendental part}}$ (to be defined).

Strategy

1. The upper bound: *Prove that* $\tilde{X}^{\text{trans}}(\mathbb{Q})$ *is "small."*
   [Follows from definability of $\tilde{X}$ and a theorem of PILA-WILKIE.]
2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that* $\tilde{X}^{\text{trans}}(\mathbb{Q})$ *actually is finite.*
3. Analyze $\tilde{X}^{\text{alg}}(\mathbb{Q})$: Let A be a variety contained in $e^{-1}(X)$; take such A maximal and irreducible. *Show that A is an affine subspace of* $\mathcal{C}^n$ *defined over* $\mathbb{Q}$.

The method of PILA-ZANNIER

Split $\tilde{X} = \underbrace{\tilde{X}^{\mathrm{alg}}}_{\text{algebraic part}} \,\dot{\cup}\, \underbrace{\tilde{X}^{\mathrm{trans}}}_{\text{transcendental part}}$ (to be defined).

Strategy

1. The upper bound: *Prove that $\tilde{X}^{\mathrm{trans}}(\mathbb{Q})$ is "small."*
   [Follows from definability of $\tilde{X}$ and a theorem of PILA-WILKIE.]
2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that $\tilde{X}^{\mathrm{trans}}(\mathbb{Q})$ actually is finite.*
   [Involves an automorphism argument and some number theory; here, only simple properties of EULER's φ-function.]
3. Analyze $\tilde{X}^{\mathrm{alg}}(\mathbb{Q})$: Let A be a variety contained in $e^{-1}(X)$; take such A maximal and irreducible. *Show that A is an affine subspace of $\mathcal{C}^n$ defined over $\mathbb{Q}$.*

The method of PILA-ZANNIER

Split $$\tilde{X} = \underbrace{\tilde{X}^{\text{alg}}}_{\text{algebraic part}} \;\dot{\cup}\; \underbrace{\tilde{X}^{\text{trans}}}_{\text{transcendental part}}$$ (to be defined).

Strategy

1. The upper bound: *Prove that $\tilde{X}^{\text{trans}}(\mathbb{Q})$ is "small."*
   [Follows from definability of $\tilde{X}$ and a theorem of PILA-WILKIE.]
2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that $\tilde{X}^{\text{trans}}(\mathbb{Q})$ actually is finite.*
   [Involves an automorphism argument and some number theory; here, only simple properties of EULER's φ-function.]
3. Analyze $\tilde{X}^{\text{alg}}(\mathbb{Q})$: Let A be a variety contained in $e^{-1}(X)$; take such A maximal and irreducible. *Show that A is an affine subspace of $\mathcal{C}^n$ defined over $\mathbb{Q}$.*
   [Uses AX' functional analogue of LINDEMANN-WEIERSTRASS.]

The method of PILA-ZANNIER

Split $\tilde{X} = \underbrace{\tilde{X}^{\text{alg}}}_{\text{algebraic part}} \dot{\cup} \underbrace{\tilde{X}^{\text{trans}}}_{\text{transcendental part}}$ (to be defined).

Strategy

1. The upper bound: *Prove that* $\tilde{X}^{\text{trans}}(\mathbb{Q})$ *is "small."*
   [Follows from definability of $\tilde{X}$ and a theorem of PILA-WILKIE.]
2. The lower bound: Suppose that X contains a dense set of special points (here: that $X(\mathbb{U})$ is dense in X). *Show that this implies that* $\tilde{X}^{\text{trans}}(\mathbb{Q})$ *actually is finite.*
   [Involves an automorphism argument and some number theory; here, only simple properties of EULER's φ-function.]
3. Analyze $\tilde{X}^{\text{alg}}(\mathbb{Q})$: Let A be a variety contained in $e^{-1}(X)$; take such A maximal and irreducible. *Show that A is an affine subspace of* $\mathbb{C}^n$ *defined over* $\mathbb{Q}$.
   [Uses AX' functional analogue of LINDEMANN-WEIERSTRASS.]

This is enough

Given $X \subseteq \Re^n$ we let

$$X^{\mathrm{alg}} := \left\{ \begin{array}{l} \text{union of all infinite connected semial-} \\ \text{gebraic subsets of } X \end{array} \right\} \quad \textit{algebraic part of } X$$

$$X^{trans} := X \setminus X^{\mathrm{alg}} \quad \textit{transcendental part of } X.$$

The finitely many transcendental points are handled by equations $x = y$.
And the affine subspaces are mapped by the exponential maps to tori.

O-minimal structures: diophantine properties

Fix an o-minimal expansion $\mathbf{R} = (\Re; <, 0, 1, +, \times, \ldots)$ of $\mathbb{R}_{\text{alg}}$.

O-minimal structures: diophantine properties

Fix an o-minimal expansion $\mathbf{R} = (\Re; <, 0, 1, +, \times, \ldots)$ of $\mathbb{R}_{\text{alg}}$.

More than ten years ago, WILKIE realized that the geometry of definable sets influences the distribution of integer points (= points with integer coordinates) on 1-dimensional definable sets.

O-minimal structures: diophantine properties

Fix an o-minimal expansion $\mathbf{R} = (\Re; <, 0, 1, +, \times, \dots)$ of $\mathbb{R}_{\text{alg}}$.

More than ten years ago, WILKIE realized that the geometry of definable sets influences the distribution of integer points (= points with integer coordinates) on 1-dimensional definable sets.

Around the same time, and developing earlier ideas of BOMBIERI-PILA (1989), PILA studied rational points on curves and surfaces definable in $\mathbb{R}_{\text{an}}$.

O-minimal structures: diophantine properties

Fix an o-minimal expansion $\mathbf{R} = (\Re; <, 0, 1, +, \times, \dots)$ of $\mathbb{R}_{\text{alg}}$.

More than ten years ago, WILKIE realized that the geometry of definable sets influences the distribution of integer points (= points with integer coordinates) on 1-dimensional definable sets.

Around the same time, and developing earlier ideas of BOMBIERI-PILA (1989), PILA studied rational points on curves and surfaces definable in $\mathbb{R}_{\text{an}}$.

These developments culminated in the theorem of PILA-WILKIE (2006):

Definable sets which are sufficiently "transcendental" contain few rational points.

O-minimal structures: diophantine properties

Notation

Given non-zero coprime $a, b \in \mathbb{Z}$ *define the* **height** *of* $x = \frac{a}{b}$ *by* $H(x) := \max\{|a|, |b|\}$, *and set* $H(0) := 0$.

O-minimal structures: diophantine properties

Notation

Given non-zero coprime $a, b \in \mathbb{Z}$ *define the* **height** *of* $x = \frac{a}{b}$ *by* $H(x) := \max\{|a|, |b|\}$, *and set* $H(0) := 0$.

We also define a height function $\mathbb{Q}^n \to \mathbb{N}$, *still denoted by* H:

$$H(x_1, \ldots, x_n) := \max\left\{H(x_1), \ldots, H(x_n)\right\}.$$

O-minimal structures: diophantine properties

Notation

Given non-zero coprime $a, b \in \mathbb{Z}$ *define the* **height** *of* $x = \frac{a}{b}$ *by* $H(x) := \max\{|a|, |b|\}$, *and set* $H(0) := 0$.

We also define a height function $\mathbb{Q}^n \to \mathbb{N}$, *still denoted by* H:

$$H(x_1, \ldots, x_n) := \max\left\{H(x_1), \ldots, H(x_n)\right\}.$$

Given $X \subseteq \Re^n$ *and* $t \in \Re$, *put*

$$X(\mathbb{Q}, t) \ := \ \left\{x \in X \cap \mathbb{Q}^n : H(x) \leq t\right\} \quad \textit{(a finite set)}.$$

O-minimal structures: diophantine properties

Notation

Given non-zero coprime $a, b \in \mathbb{Z}$ *define the* **height** *of* $x = \frac{a}{b}$ *by* $H(x) := \max\{|a|, |b|\}$*, and set* $H(0) := 0$*.*

We also define a height function $\mathbb{Q}^n \to \mathbb{N}$*, still denoted by* H*:*

$$H(x_1, \ldots, x_n) := \max\left\{H(x_1), \ldots, H(x_n)\right\}.$$

Given $X \subseteq \Re^n$ *and* $t \in \Re$*, put*

$$X(\mathbb{Q}, t) \ := \ \left\{x \in X \cap \mathbb{Q}^n : H(x) \leq t\right\} \quad \textit{(a finite set).}$$

We'd like to understand the asymptotic behavior of $|X(\mathbb{Q}, t)|$.

O-minimal structures: diophantine properties

Example

$$\left\{\begin{array}{l} X \text{ is graph of } P \text{ where } P\colon \Re^{n-1} \to \Re \text{ is a polynomial function with integer coefficients of degree } d \end{array}\right\} \Rightarrow |X(\mathbb{Q}, t)| \sim Ct^{2(n-1)/d}$$

O-minimal structures: diophantine properties

Example

$$\left\{\begin{array}{l} X \text{ is graph of } P \text{ where } P\colon \Re^{n-1} \to \Re \text{ is a polynomial function with integer coefficients of degree } d \end{array}\right\} \Rightarrow |X(\mathbb{Q}, t)| \sim Ct^{2(n-1)/d}$$

Question

When does $|X(\mathbb{Q}, t)|$ grow sub-polynomially as $t \to \infty$?

O-minimal structures: diophantine properties

Theorem (Pila-Wilkie, 2006)

Let $X \subseteq \Re^n$ be definable. Then for each $\varepsilon > 0$ there is some $t_0 = t_0(\varepsilon)$ such that

$$|X^{\text{trans}}(\mathbb{Q}, t)| \leq t^{\varepsilon} \qquad \textit{for all } t \geq t_0.$$

O-minimal structures: diophantine properties

Theorem (PILA-WILKIE, 2006)

Let $X \subseteq \Re^n$ be definable. Then for each $\varepsilon > 0$ there is some $t_0 = t_0(\varepsilon)$ such that

$$|X^{\text{trans}}(\mathbb{Q}, t)| \leq t^{\varepsilon} \qquad \text{for all } t \geq t_0.$$

Remark

- *The theorem continues to hold if given $d \geq 1$, we replace*

$$\mathbb{Q} \rightsquigarrow \text{set of algebraic numbers of degree} \leq d$$
$$H \rightsquigarrow \text{a suitable height function on } \mathbb{Q}^{\text{alg}}.$$

(PILA, 2009)

Aschenbrenner's slides.

`https://www.math.ucla.edu/~matthias/pdf/Wien.pdf`

Unreasonable effectiveness of model theory in number theory

Model theory succeeds by studying tame structures; arithmetic is quintessentially NOT tame.

What's going on?

Arithmetic is non-definably embedded in an appropriate tame structure.
Earlier the reals, p-adics, or complexes. But now more sophisticated structures.

Bourbaki again

Bourbaki's vision

Bourbaki has some beginning notions of combining the 'great mother-structures' (group, order, topology). They write:

'the organizing principle will be the concept of a hierarchy of structures, going from the simple to complex, from the general to the particular.'

Bourbaki again

Bourbaki's vision

Bourbaki has some beginning notions of combining the 'great mother-structures' (group, order, topology). They write:

'the organizing principle will be the concept of a hierarchy of structures, going from the simple to complex, from the general to the particular.'

fulfilling the vision

1. Divide the task according to whether there is a definable order
2. Find sufficient conditions for definable groups
3. Use topology as a unifying technique – sometimes definable
4. Add the 4th great mother structure – 'Geometry' – the existence of dimension.

Unreasonable effectiveness

There have been significant applications of the themes above in:

1. groups of finite Morley rank
2. differential algebra
3. real algebraic geometry
4. algebraically closed valued fields
5. Banach spaces (continuous logic and metric AEC)
6. approximate groups
7. combinatorial graph theory

Notation for Pila's theorem

Recall that the Weierstrass j function, $j\colon \mathbb{H} \to \mathcal{C}$ satisfies

$$j(\sigma) = j(\tau) \iff E_\sigma \cong E_\tau$$

so it parameterizes elliptic curves.

The nth classical modular polynomial ($n \in \mathbb{N}^{\geq 1}$)

There is an irreducible $\Phi_n \in \mathbb{Z}[X, Y]$ such that for $x, y \in \mathcal{C}$:

$$\Phi_n(x, y) = 0 \iff x = j(\tau),\ y = j(n\tau) \text{ for some } \tau \in \mathbb{H}.$$

The Φ_n are symmetric in X and Y.

Pila's actual theorem

Theorem: Pila, 2011

Let $X \subseteq \mathcal{C}^n$ be an irreducible variety. If X contains a dense set of special points, then X is special.

where

1. The $j(\tau) \in \mathcal{C}$ with $\tau \in \mathbb{H}$ quadratic over $\mathbb{Q}$ ("E has CM") will be our *special points.*
2. A variety $V \subseteq \mathcal{C}^n$ is *special* if it is an irreducible component of a variety defined by equations of the form

$$\Phi_n(x_i, x_j) = 0 \quad \text{or} \quad x_i = a \text{ where } a \in \mathcal{C} \text{ is special.}$$