Chapter VIII

Applications of o-minimality

We will finally discuss some applications of o-minimality to number theory. We first do a quick survey before focusing on the Pila-Wilkie counting theorem and its appearance in the "Pila-Zannier approach" to various questions (André-Oort, Manin-Mumford, Zilber-Pink, etc, conjectures).

1. Quick survey

a) Lattice point problems [Barroero-Widmer, 2012]

A classical problem in analytic number theory, with many applications, is to estimate $|\Lambda \cap X|$ where $\Lambda \subset \mathbb{R}^n$ is a lattice (i.e. free ab. grp of rank n ex. $\Lambda = \mathbb{Z}^n$) and X is a "big" open set. Typically, X varies with a parameter $t \to +\infty$ and the goal is to have an asymptotic formula for $|\Lambda \cap X_t|$ as $t \to +\infty$.

The simplest case is when $X_t = tU$ for some fixed $U \subset \mathbb{R}^n \left\{ \begin{array}{l} \underline{\text{open}} \\ \underline{\text{convex}} \end{array} \right.$ (e.g. $U =$ unit ball), in which case it is not too hard to show

$$|\mathbb{Z}^n \cap tU| \underset{t \to \infty}{\sim} \mathrm{Vol}(U)\, t^n$$

[Ex. (Gauss) $n=2$, $U =$ unit disc, $|\mathbb{Z}^2 \cap tU|$ is the number of $(a,b) \in \mathbb{Z}^2$ s.t. $a^2 + b^2 \leq t^2$]

However, in many cases the situation is not so nice.

Theorem. (Barroero – Widmer)

Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and let $Z \subset \mathbb{R}^{m+n}$ be a definable set in some o-minimal structure expanding $\mathbb{R}$ and semialgebraic sets.

For $t \in \mathbb{R}^m$ we have

$$\left| \, |\Lambda \cap \underbrace{Z_t}_{\{x \in \mathbb{R}^n \,|\, (t,x) \in Z\}}| - \frac{\mathrm{Vol}(Z_t)}{\det(\Lambda)} \right| \leq c_Z \cdot \underbrace{\delta(Z,t)}_{\text{explicit in terms of the geometry of } \Lambda \text{ and } Z_t}.$$

provided all fibers Z_t are bounded.

This turns out to improve many previous results.

b) Diophantine equations [Frei – Pieropan, 2013]

Using the previous result, the following case of the so-called "Manin-(Batyrev-Peyre-Tschinkel)" conjecture is proved

Theorem – (Frei – Pieropan)

Let $S \subset \mathbb{P}^4$ be the algebraic surface with equations

"del Pezzo surface of type $A_3 + A_1$"

$$\begin{cases} x_0 x_3 - x_2 x_4 = 0 \\ x_0 x_1 + x_1 x_3 + x_2^2 = 0. \end{cases}$$

Let $U \subset S$ be the complement of the set of lines included in S. (One can show that there are 3 lines.)

Let $K/\mathbb{Q}$ be a finite extension of degree d. For $B \geq 2$ we have

some "height" function

$$|\{x \in U(K) \mid \boxed{H}(x) \leq B\}|$$

$$= c\, B (\log B)^5 + O\left(B (\log B)^{5-\frac{2}{d}}\right)$$

For $K = \mathbb{Q}$ this was proved in 2009 by Deren-

-that (for $K/\mathbb{Q}$ imaginary quadratic, by Derenthal and Frei); the crucial fact is that the theorem holds for *any* (fixed) K, and it is for this purpose that o-minimality is used. The underlying o-minimal structure is $\mathbb{R}_{exp}$, i.e., the set $\mathbb{R}$ in the language $(+, -, \cdot, 0, 1, \leq, exp)$, where exp is a function symbol interpreted in $\mathbb{R}$ as the exponential function.

Theorem. ("Tarski's Problem"; Wilkie, 1996).

The structure $\mathbb{R}_{exp}$ is o-minimal.

c) *Oscillatory integrals* [Basu, Guo, Zhang, Zorin-Kranich (2021)]

Here the context is quite different:

Theorem. (B - G - Z - Z)

Let $Q : [0,1]^d \longrightarrow \mathbb{R}$ be bounded and semialgebraic with "$\underbrace{\text{complexity} \leq k}_{\text{e.g. polynomial of degree } \leq k}$". We then have

$$\left| \int_{[0,1]^d} e^{2i\pi Q(x)} \, dx \right| \leq C_{d,k} \sup_{\mu \in \mathbb{R}} \overbrace{\left| \left\{ x \in [0,1]^d \,/\, Q(x) \in [\mu, \mu+1] \right\} \right|}^{\text{Lebesgue measure of} \ldots}$$

Here the o-minimal structure used is $\mathbb{R}$ with the language $\mathcal{L}_{an,exp}$ (involving exp and analytic functions restricted to $[0,1]^d$).

d) o-minimal Chow / GAGA

Here we have very different types of applications!

Theorem (Peterzil - Starchenko, 2009)

Let $X_{/\mathbb{C}}$ be a quasi-projective algebraic variety. Let $Z \subset X$ be a closed analytic subset. If there exists an o-minimal expansion of $\mathbb{R}_{an}$ ($= \mathbb{R}$ with $(+, -, \cdot, 0, 1, \leq, (f))$ where f are function symbols representing all restrictions to $[0,1]$ of analytic functions; this is o-minimal by a result of Gabrielov from 1968) such that Z is definable. Then Z is algebraic.

More generally, Bakker, Brunebarbe and Tsimerman have extended this to a "GAGA"-type theorem.

"Theorem." (B-B-T, 2018)

Let $X/_{\mathbb{C}}$ be an algebraic variety. One can define an associated "definable space" X^{def} and a category of coherent "definable" sheaves $\underline{Coh}(X^{def})$. The natural functor $\underline{Coh}(X) \longrightarrow \underline{Coh}(X^{def})$ is exact and fully-faithful; it is not essentially surjective in general [e.g. for $\mathbb{P}^1 \setminus \{0, \infty\}$] but the (essential) image is stable by subobjects and subquotients.

There are important applications of this to Hodge Theory.

2. The Pila-Wilkie Theorem

We now present the result which is the source of much of the arithmetic interest in o-minimality. This concerns the number of rational points in definable sets in $\mathbb{R}^n$ for some o-minimal structure.

More precisely, we consider here a language $\mathcal{L}$ extending $(+, -, \cdot, 0, 1, \leq)$ and a structure with underlying set $\mathbb{R}$, with its usual interpretations as an ordered ring. Given $n \geq 1$ and $X \subset \mathbb{R}^n$ definable, we let

$$X(\mathbb{Q}) = X \cap \mathbb{Q}^n.$$

This set is often infinite. But if we further filter according to the *height*, we get finite sets.

Definition. If $\frac{a}{b} \in \mathbb{Q}$ with a coprime to b, then we put $h(a/b) = \max(|a|, |b|)$.
If $x = (x_1, \dots, x_n) \in \mathbb{Q}^n$, then we put

$$h(x) = \max(h(x_i)).$$

Observe the following elementary fact:

Lemma. For any $B \geq 1$, the set

$$\{x \in \mathbb{Q}^n \mid H(x) \leq B\}$$

is finite and has size $\boxed{\asymp}\ B^{2n}$.

between $c_1 B^{2n}$ and $c_2 B^{2n}$ with $c_1, c_2 > 0$

Proof. The definition means that we can assume that $n = 1$. Then

$$|\{x \in \mathbb{Q} \mid H(x) \leq B\}| = \sum\sum_{\substack{|a|,|b| \leq N \\ (a,b)=1}} 1$$

$$\leq (2N+1)^2$$

gives the upper-bound, while the "standard" formula

$$\sum\sum_{\substack{(a,b)=1 \\ 1 \leq a,b \leq N}} 1 \sim \frac{6}{\pi^2} N^2, \quad N \to +\infty$$

gives the lower-bound

□

(Note. A slightly weaker lower bound is

$$\sum\sum_{\substack{(a,b)=1 \\ a,b \leq N}} 1 \geq \sum_{\substack{p \leq N \\ \text{prime}}} \sum_{1 \leq a < p} 1$$

$$\geq \sum_{p \leq N} (p-1) \gg \frac{N^2}{\log N}$$

using the Chebychev bound $\sum_{p \leq N} 1 \gg \frac{N}{\log N}$.)

Now let $X \subset \mathbb{R}^n$ be any set. Define

$$X(B) = \{x \in X \cap \mathbb{Q}^n \mid H(x) \leq B\}.$$

It could of course be that $X(B)$ contains all $x \in \mathbb{Q}^n$ of height $\leq B$, even while X is "a curve".

However, when X is described by concrete (in) equations, and one can compute what happens, one finds that $X(B)$ is typically smaller, *unless* X contains a line, or some graph $x_n = f(x_1, \dots, x_{n-1})$ with $f \in \mathbb{Q}[X_1, \dots, X_{n-1}]$, or something similar. The Pila-Wilkie Theorem confirms that this *is* the case.

To state it, one uses the following definition:

Definition — $n \geq 1$, $X \subset \mathbb{R}^n$

An *algebraic piece* of X is an *infinite*, *connected* (for the classical topology), *$\mathcal{L}_{or}$-definable* (with parameters) subset of X.
"semi-algebraic"

The *algebraic part* of X is the *union* of all

algebraic pieces of X; it is denoted X^{alg}.
The complement $X - X^{alg}$ is denoted X^{tr} (the "transcendental part").

Example.

(1) $X_1 = \{ (x,y) \in \mathbb{R}^2 \mid y = e^x \}$, the graph of the exponential $\rightsquigarrow$ $X_1^{alg} = \emptyset$.

(2) $X_2 = \{ (x,y) \in \mathbb{R}^2 \mid 0 \leq y \leq e^x \}$: here $X_2^{alg} = X_2$, although X_2 is <u>not</u> definable in $\mathcal{I}_{or}$: each segment $\{x\} \times [0, e^x]$ is semi-algebraic and their union is X_2.

(3) $X_3 = \{ (x,y,z) \in \mathbb{R}^3 \mid x > 0, \ z = x^y \}$

One can show that

$$X_3^{alg} = \{ (x,y,z) \in \mathbb{R}^3 \mid x > 0, \ z = x^y, \text{ with } y \in \mathbb{Q} \}$$

a union of countably many curves.

cf. Pila-Wilkie, Duke Math. J. 133

Bhardwaj - van den Dries, arXiv: 2010.14046

<u>Theorem</u>. (Pila-Wilkie, 2006)

Let $\mathcal{L}$ be a language extending $\mathcal{L}_{or}$ such that $\mathbb{R}$ is an o-minimal $\mathcal{L}$-structure. Let $n \geq 1$ and $X \subset \mathbb{R}^n$ an $\mathcal{L}$-definable set (with parameters). For any $\varepsilon > 0$, there exists $c \geq 0$, depending on X and ε, such that for all $B \geq 1$, we have

$$|X^{tr}(B)| \leq c B^{\varepsilon}.$$

<u>Note</u>. In <u>some</u> cases, but not all, one can replace B^{ε} by $(\log B)^{\alpha}$ for some $\alpha \geq 0$, which is important in a number of applications.

3. How is the Pila-Wilkie Theorem used?

We recall the theorem of Laurent:

[Mordell-Lang conjecture]

<u>Theorem</u> (Laurent). $X \subset (\mathbb{C}^{\times})^n$ irreducible algebraic variety. If X_{tors} (= points on X with

coordinates roots of unity] is Zariski-dense, then $X = x_0 H$ for some $x_0 \in X$ and $H < (\mathbb{C}^*)^n$ algebraic subgroup.

We will explain the specific instance of the "Pila-Zannier strategy" that gives a proof of this (there are simpler approaches).

The key idea is to consider the surjective (holomorphic) map

$$e : \mathbb{C}^n \longrightarrow (\mathbb{C}^\times)^n$$

$$(z_j)_{1 \leq j \leq n} \longmapsto (e^{2i\pi z_j})_{1 \leq j \leq n}$$

and the preimage $\tilde{X} = e^{-1}(X) \subset \mathbb{C}^n$. Then one observes that e induces a <u>bijection</u>

$$\tilde{e} : \mathbb{Q}^n \cap \Big(\big(\underbrace{[0,1[^n + i\mathbb{R}^n}_{\subset \mathbb{C}^n = \mathbb{R}^{2n}} \big) \cap \tilde{X} \Big) \longrightarrow X_{\text{tors}} .$$

Now we note that the set

$$Y = \tilde{X} \cap \left([0,1[^n + i\,\mathbb{R}^n \right) \subset \mathbb{R}^{2n}$$

is $\mathcal{L}$ - definable, where

$$\mathcal{L} = (+, -, \cdot, 0, 1, \leq, \exp, \sin|[0,2\pi]).$$

So, according to Pila - Wilkie

$$|Y^{tr}(B)| \leq c_\varepsilon B^\varepsilon$$

for $\varepsilon > 0$.

<u>However</u>: if X_{tors} is dense, one shows that in fact $|Y(B)|$ grows <u>faster</u>, so that $Y^{alg} \neq \emptyset$: Y contains an infinite (positive-dimension) <u>semialgebraic</u> set A; then X contains $e(A)$; some additional information leads to the conclusion, of "transcendental nb. theory" flavor: A is "algebraic" and $e(A) \subset X$ also, which shouldn't happen frequently. (Compare with the Lindemann - Weierstrass Theorem: if $\alpha_1, \dots, \alpha_m$ are $\mathbb{Q}$ - linearly independent <u>algebraic</u> numbers, then $(e^{\alpha_1}, \dots, e^{\alpha_m})$ are algebraically independent

over $\mathbb{Q}$.)

4. The determinant method

The first step to prove the Pila-Wilkie Theorem is:

Step 1. ("Determinant method" of Bombieri-Pila)

This says that, under suitable conditions, the points in $X \cap \mathbb{Q}^m$ are contained in finitely many hypersurface.

Def. $H \subset \mathbb{R}^m$ is a hypersurface if there exists $f \in \mathbb{R}[X_1, \dots, X_m]$, $f \neq 0$, such that

$$H = \{x \in \mathbb{R}^m \mid f(x) = 0\}.$$

The minimal possible degree of f is called the degree of H.

The statement is then the following:

Th. 1. (P-W; inspired by Bombieri-Pila)

Let $\varphi :]0,1[^n \longrightarrow \mathbb{R}^m$ be a function of class C^r for some $r \geq 1$, and let

$$X = \varphi(]0,1[^n) \subset \mathbb{R}^m.$$

Suppose that $n < m$ and that

$$|\partial_\beta \varphi(x)| \leq 1$$

for all $\beta \in \mathbb{N}^n$ with $|\beta| = \sum \beta_i \leq r$.

Let $d \geq 1$ be an integer.

There exist $r_0 \geq 1$ depending on (n, m, d)

$C \geq 0$ ———————— (n, m, d)

$\varepsilon > 0$ ———————— (n, m, d)

such that if $r \geq r_0$, then for all $B \geq 1$, the set $X(B)$ is contained in the union of $\leq C B^{\varepsilon}$ hypersurfaces of degree $\leq d$.

Furthermore, we have $\varepsilon \to 0$ when $d \to \infty$.

Once this is proved, the second step is to show that any definable set can be represented as the union of finitely many sets of the previous type (essentially).

But we begin by this first step.

This involves some notation.

Consider $m \geqslant 0$, $d \geqslant 0$. Let:

$$\mathbb{N}^m(d) = \{ \alpha \in \mathbb{N}^m \mid \sum \alpha_i \leqslant d \}$$

(nb. of monomials of deg. $\leq d$ in m variables)

$$\alpha(m,d) = |\mathbb{N}^m(d)| = \binom{m+d}{d}$$

(nb. of monomials of deg. d in m variable)

$$\beta(m,d) = |\mathbb{N}^m(d) - \mathbb{N}^m(d-1)| = \binom{m+d-1}{d-1}$$

For $S \subset \mathbb{R}^m$, finite, $I \subset \mathbb{N}^d$, we write

$$V(S, I) = (x^\alpha)_{\substack{x \in S \\ \alpha \in I}} \qquad \begin{pmatrix} |S| \times |I| \\ \text{matrix} \end{pmatrix}$$

where

$$x^\alpha = \prod x_i^{\alpha_i}.$$

<u>Lemma 1</u>. Let $m \geqslant 1$, $d \geqslant 1$, $S \subset \mathbb{R}^m$ arbitrary.

Suppose that for any $T \subset S$ with $|T| = \alpha(d,m)$, we have $\det(\underbrace{V(T, \mathbb{N}^m(d))}_{\substack{\alpha(m,d) \times \alpha(m,d), \\ \text{defined up to sign}}}) = 0$.

Then S is contained in a hypersurface of degree $\leqslant d$.

Proof. We may assume that $S \neq \{0\}$. Pick $T \subset S$ with $|T| = \alpha(m,d)$ such that the matrix $V(T, \mathbb{N}^m(d))$ has maximal rank. By assumption, this is $< \alpha(m,d)$, and it is ≥ 1 because $S \neq \{0\}$, so there exists $T_1 \subsetneq T$ and $A \subset \mathbb{N}^m(d)$ with $|T_1| = |A|$ such that $\det(V(T_1, A)) \neq 0$ (such matrices are minors of $V(T, \mathbb{N}^m(d))$, and one must be $\neq 0$).

There exists $\beta \in \mathbb{N}^m(d) - A$. Define

$$f(y_1, \dots, y_m) = \det\left(V(T_1 \cup \{y\}, A \cup \{\beta\})\right).$$

By the expansion formula for determinants along columns (or rows), we see that f is a polynomial of degree $\leq d$ (in variables $y_1, \dots, y_m$). Moreover, the coefficient of y^β is

$$\pm \det(V(T_1, A)) \neq 0$$

so $f \neq 0$.

Finally, let $x \in S$. Then $f(x) = 0$ since it is $\det\left(V\left(\underbrace{T_1 \cup \{x\}}_{\subset S}, A \cup \{\beta\}\right)\right)$ is a minor of size $|T_1| + 1$ of $V(T, \mathbb{N}^m(d))$.

□

The issue is now to construct sets of points satisfying the assumptions. This will be done by combining

(i) an analytic upper bound

(ii) a lower bound coming from integrality: if $x \in \mathbb{Z}$ and $x \neq 0$, then $|x| \geq 1$ (integrality will arise from rational points by clearing denominators).

Here is the analytic step:

Lemma 2 – Pick $m \geq 1$, $n \geq 1$, $d \geq 1$. Let $\varphi :]0,1[^n \longrightarrow \mathbb{R}^m$ be of class C^r with

r sufficiently large (see below) such that

$$|\partial_\alpha \varphi(x)| \leq 1, \qquad |\alpha| \leq \mu, \quad x \in]0,1[^n.$$

Let $\delta \in]0,1[$ be fixed.

There exists $\begin{cases} E \geq 0 \\ C \geq 0, \end{cases}$ depending on (m,n,d), such that

$$\overset{(\varphi(x))_{x\in S}}{}$$

$$\det\left(V\left(\widetilde{\varphi(S)}, \mathbb{N}^m(d)\right)\right) \leq C\delta^E$$

for any $S \subset]0,1[^n$ such that

$$\|x-y\| \leq r \quad \text{for} \quad x, y \quad \text{in} \quad S.$$

Proof.- Fix S, and some $x_0 \in S$.

Let $x \in S$. We write $\varphi = (\varphi_1, \ldots, \varphi_m)$ and

$$\varphi_j(x) = \sum_{\substack{|\beta| \leq r-1 \\ \beta \in \mathbb{N}^d}} (x - x_0)^\alpha \frac{(\partial^\alpha \varphi_j)(x_0)}{\boxed{\alpha!}} \to \prod \alpha_i!$$

$$+ \psi_{j,r}(x)$$

by Taylor expansion, with

$$|\psi_{j,r}(x)| \leq \max_{|\beta|=r}\left(\frac{|x-x_0|^\beta}{\beta!} \sup_y |\partial_\beta \varphi_j(y)|\right)$$

(e.g. from the integral form of the remainder).

So $\varphi_j(x) = p_{j,x}(x - x_0)$ for some polynomial $p_{j,x} \in \mathbb{R}[Y_1, \dots, Y_n]$ of degree $\leqslant r$ with coefficients all bounded by 1 (in absolute value), by our hypothesis. It follows that for $\alpha \in \mathbb{N}^m(d)$, and $x \in S$, we can write $\varphi(x)^\alpha$ as $q_{x,\alpha}(x - x_0)$ where $q_{x,\alpha}$ is a polynomial with coefficients bounded by d^m in $\mathbb{R}[Y_1, \dots, Y_n]$.

We express

$$q_{x,\alpha} = \sum_{k=0}^{r} q_{x,\alpha,k}$$

where $q_{x,\alpha,k}$ is the homogeneous part of degree k if $k < r$, and the remainder (of degree $\geqslant r$) if $k = r$; all are in $\mathbb{R}[Y_1, \dots, Y_n]$.

Correspondingly, we have

$$V(\varphi(s), \mathbb{N}^m(d)) = \sum_{k=0}^{r} V_k$$

with $V_k = (q_{x,\alpha,k}(x - x_0))_{\substack{x \in S \\ |\alpha| \in \mathbb{N}^m(d)}}$.

We now use:

Sublemma - Let V be an N-dimensional real vector space (or over any base field). Let $(u_k)_{k \in I}$ be a finite family of endomorphisms of V.

We have

$$\det\left(\sum_{k \in I} u_k\right) = \sum_{\substack{\sigma : \{1, \dots, N\} \longrightarrow I \\ |\sigma^{-1}(k)| \leq \operatorname{rank}(u_k) \\ \text{for all } k}} u_{\sigma(1)} \wedge \dots \wedge u_{\sigma(N)}$$

where we identify $\operatorname{End}\left(\overset{N}{\Lambda} V\right) = \mathbb{R}$.

We apply this to $V = \mathbb{R}^{\alpha(m,d)}$ with the u_k given by multiplication by the matrix V_k (after ordering the rows/columns). If $k < r$, then note that $\operatorname{rank}(V_k) \leq \beta(n, k)$ since $\beta(n,k)$ is the dimension of the space of homogeneous polynomials of degree k in n variables.

So

$$\det\left(V\left(\varphi(s), \mathbb{N}^m(d)\right)\right) = \sum_{\substack{\sigma : \mathbb{N}^m(d) \longrightarrow \{0, \dots, r\} \\ |\sigma^{-1}(k)| \leq \beta(n,k) \\ \text{if } 0 \leq k < r}} \bigwedge_{\alpha} V_{\sigma(\alpha)} .$$

Fix a $\sigma : \mathbb{N}^m(d) \longrightarrow \{0, \dots, r\}$. By "inspection", one sees that $\bigwedge_\alpha V_{\sigma(\alpha)}$, if non zero, is multiplication by a number bounded by

$$C_1 \left(\max_x \|x - x_0\| \right)^{\sum \sigma(\alpha)} \leq C_1 \delta^{\sum_\alpha \sigma(\alpha)}$$

for some constant C_1 depending on m, n, d only.

The <u>worse</u> bound, since $\delta \leq 1$ by assumption, is when $\sum_\alpha \sigma(\alpha)$ is smallest. But

$$\sum_\alpha \sigma(\alpha) = \sum_{k<r} k \sum_{\sigma(\alpha)=k} 1$$
$$+ r \sum_{\sigma(\alpha)=r} 1 .$$

So we want to have as many $\sigma(\alpha) = 1$ as possible, etc; hence the worse occurs when

$$|\sigma^{-1}(k)| = \beta(n, k) \quad , \quad 0 \leq k < r,$$

provided r is large enough that this is possible. This will be the case if $r \geq b+1$, where b is chosen so that

$$\alpha(n, b) \leq \alpha(m, d) \leq \alpha(n, b+1).$$

There is a unique such b, and we assume $r = b+1$ exactly. Then the exponent E is

$$E = \sum_{k=0}^{b} k\,\beta(n,k) + (b+1)\big(\alpha(m,d) - \alpha(n,b)\big).$$

□

And now :

<u>Proof of Th. 1</u> _ We take r_0 to be the r of Lemma 2, which determines the exponent E above. Let C be also as in Lemma 2. Let $d \geq 1$. Let $B \geq 1$.

Let $S \subset \,]0,1[^n$ be a set of size $\alpha(m,d)$ and suppose $\varphi(x) \in X(B)$ for all $x \in S$. Then $\det\big(V(\varphi(S), \mathbb{N}^m(d))\big) \in \mathbb{Q}$, and in fact, since for each x there is an integer $1 \leq b_{x,j} \leq B$ such that $b_{x,j}\varphi_j(x) \in \mathbb{Z}$, we have $\det\big(V(\varphi(S), \mathbb{N}^m(d))\big) \in \frac{1}{b_S}\mathbb{Z}$ where $1 \leq b_S \leq B^{md\,\alpha(m,d)}$ (because if $b_j(x) \leq B$

is a "denominator" of $\varphi_j(x)$, then one of $\varphi(x)^\alpha$ is $\prod_{j=1}^{m} b_j(x)^{\alpha_j}$,

so a common denominator $b(x)$ of $\varphi(x)^\alpha$ for $|\alpha| \leq d$ is $\left(\prod_{j=1}^{m} b_j(x)\right)^d$

which is $\leq B^{md}$; then $b_S = \prod_x b(x) \leq B^{md\,\alpha(m,d)}$

satisfies $b_S \det(\_) = \sum_{\sigma : S \xrightarrow{\sim} \mathbb{N}^m(d)} \varepsilon(\sigma) \prod_x \underbrace{b(x)\,\varphi(x)^{\sigma(x)}}_{\in \mathbb{Z}} \in \mathbb{Z})$.

So <u>either</u> $\det V(\varphi(S), \mathbb{N}^m(d)) = 0$

<u>or</u> $|\det V(\varphi(S), \mathbb{N}^m(d))| \geq \dfrac{1}{B^{md\,\alpha(m,d)}}$

If we pick $\delta \in \,]0,1[$ such that

$$C\,\delta^E < \frac{1}{B^{md\,\alpha(m,d)}}$$

then this means, by contrasting with Lemmas $\left.\begin{matrix}1\\2\end{matrix}\right\}$,

we deduce that for any box $V \subset \,]0,1[^n$

of diameter $\leq \delta$, we have

$$X(B) \cap \varphi(V) \subset H$$

for some hypersurface H of degree $\leq d$.

We can cover $]0,1[^n$ by $\approx \delta^{-n}$ such

boxes, hence we get $X(B)$ in the union

of <u>approximately</u> (up to multiplicative constant)

$$\delta^{-n} \simeq \left(C B^{md\,\alpha(m,d)}\right)^{n/E}$$

$$= C' \; B^{\varepsilon}$$

where

$$\varepsilon = \frac{mnd\,\alpha(m,d)}{E}.$$

It remains to check that $\varepsilon \longrightarrow 0$ as $d \longrightarrow \infty$ if m, n are fixed. In that case,

$$\alpha(m, d) \asymp d^{m}$$

whereas $E = \sum_{k=0}^{b} k\,\beta(m,k) + (b+1)\big(\alpha(m,d) - \alpha(n,b)\big)$

and one can see that

$$b \asymp d^{\frac{m}{n}}$$

so that $E \asymp d^{m+\frac{m}{n}}$ and

$$\varepsilon \asymp \frac{d^{m+1}}{d^{m+m/n}} = d^{1-\frac{m}{n}} \longrightarrow 0$$

because we assumed that $m > n$.

$\square$

5. Reparameterization

The second step of the proof of the Pila-

Wilkie Theorem is the following, which shows how to "recover" all definable sets from those of the type allowed by Theorem 1.

Theorem 2 - Let $\mathcal{L} \supset \mathcal{L}_{or}$ be a language s.t. $\mathbb{R}$ is an o-minimal $\mathcal{L}$-structure.

Let $A \subset \mathbb{R}^n$ be definable and $X \subset A \times [-1,1]^m$ be definable. Assume $\dim(X_a) < m$ for all $a \in A$.

Let $r \geq 1$ be given.

There exists $C \geq 0$ such that for every $a \in A$, the fiber $X_a \subset [-1,1]^m$ is the union of at most C sets of the form $\varphi(]-1,1[^n)$ for some $n < m$ and some $\varphi :]-1,1[^n \longrightarrow \mathbb{R}^m$ of class C^r s.t. $\|\partial^\beta \varphi(y)\|_\infty \leq 1$ for all $\beta \in \mathbb{N}^n(r)$ and all $y \in]-1,1[^n$.

Results of this kind go back to Yomdin, then Gromov, in the semi-algebraic setting (with very different applications in mind). The proof is rather tricky and lengthy; we omit it entirely (for the moment at least), with the justification that for certain specific sets, it might be possible to prove it directly...

6. Proof of the Pila-Wilkie

We combine Th. 1 and Th. 2. The actual argument uses induction on $\dim(X)$, and for the induction step, it is useful/necessary to prove a stronger statement.

Theorem. (P-W, bis)

Let $\mathcal{L}$ be a language as above. Let $n \geq 0$ and $A \subset \mathbb{R}^n$ be definable, and $X \subset A \times \mathbb{R}^m$ definable.

For $\varepsilon > 0$, there exists $C_\varepsilon \geq 0$ s.t. for all $a \in A$ and $B \geq 1$, we have $|X_a^{tr}(B)| \leq C_\varepsilon B^\varepsilon$.

Proof (Using Th. 1, Th. 2) - We use induction on m.

For $m = 0$, the result is clear.

Suppose now that $m \geq 1$ and the result is true for $A \times \mathbb{R}^{m'}$ if $m' < m$.

Step 1 - Since $\mathring{Y} \subset Y^{alg}$ for any definable set Y, we can assume that $\mathring{X}_a = \emptyset$ for all a (replace X by $X - \{(a,x) \mid x \in \mathring{X}_a\}$, which is still definable).

In particular, it follows that $\dim(X_a) < m$ for all $a \in A$.

Step 2 - One also assume that $X \subset A \times [-1,1]^m$: indeed, we can decompose

$$X = \bigcup_{I \subset \{\pm 1\}^m} X_I$$

where $(a,x) \in X_I \iff \forall j, \ |x_j^{\varepsilon_j}| \leq 1$.

It suffices to prove the result for each X_I. But we have a definable homeomorphism

$$\varphi_I \left\{ \begin{tikzcd} X_I \arrow[r] & Y_I \\ (a,x) \arrow[r, mapsto] & \left(a, \left(x_j^{\varepsilon_j}\right)\right) \end{tikzcd} \right.$$

where $Y_I \subset [-1,1]^m$, and because φ_I is $\mathcal{L}_{or}$-definable, in fact

$$\varphi_I\left(X^{tr}_{I,a}\right) = Y^{tr}_{I,a}.$$

Moreover, from $H(y^{-1}) = H(y)$ for any $y \in \mathbb{Q}^{\times}$, we get $Y_{I,a}(B) = \varphi_I(X_{I,a}(B))$ also, so the P-W bound for X_I will follow from that for Y_I.

Step 3. Assume $X \subset A \times [-1,1]^m$ and $\mathring{X}_a = \emptyset$ for all a. Pick $\varepsilon > 0$, then pick r and d so that Theorem 1 applies for sets of the form $\varphi(]-1,1[^n)$ for all $n < m$, and so that the corresponding exponent is $\leq \varepsilon$.

By Theorem 2, we find a constant C and for $a \in A$, at most C functions $\varphi_k :]-1,1[^{n_k} \longrightarrow \mathbb{R}^m$ $(n_k < m)$

such that $X_a = \bigcup \varphi_k(]-1,1[^{n_k})$ and

$$\| \partial^\beta \varphi_k \|_\infty \leq 1 \quad , \quad |\beta| \leq r.$$

Now let $B \geq 1$. By Theorem 1 applied to each φ_k we find a set of $\leq C' B^\varepsilon$ hypersurfaces $\{f_i = 0\}$ of degree $\leq d$ such that

$$X_a(B) \subset \bigcup_i (X_a \cap \{f_i = 0\})(B)$$

Step 4. Consider the space $\mathbb{R}^{\alpha(m,d)} - \{0\} = H_{m,d}$ parameterizing (equations of) hypersurfaces of degree $\leq d$ in $\mathbb{R}^m$. Then consider the "(uni)versal" hypersurface

$$\mathcal{H}_{m,d} \subset \mathbb{R}^m \times H_{m,d}$$

where $\mathcal{H}_{m,d} = \{ (x, f) \mid f(x) = 0 \}$. Note that $\mathcal{H}_{m,d}$ is semi-algebraic. By the Cell Decomposition Theorem (for the o-minimal $\mathcal{L}_{or}$ - structure $\mathbb{R}$) we can find a (semi-algebraic) cell decomposition

$$\mathcal{H}_{m,d} = \bigcup_{\underline{c}} C_{\underline{c}}$$

where $C_{\underline{c}}$ is a $\underline{c}$-cell in the language $\mathcal{L}_{or}$ for each $\underline{c}$. For any $f \in H_{m,d}$, we get

$$(\mathcal{H}_{m,d})_f = \bigcup_{\underline{c}} C_{\underline{c},f}$$

$\overset{\simeq}{\{x \in \mathbb{R}^m \mid f(x)=0\}}$ and by properties of cell decompositions, the non-empty among the $C_{\underline{c},f}$ form a cell decomposition of $(\mathcal{H}_{m,d})_f$.

As a consequence

$$|X_a^{tr}(B)| \leq \sum_i \left|(X_a \cap \{f_i=0\})^{tr}(B)\right|$$

$$\leq \sum_i \sum_{C_{\underline{c},f_i} \neq \emptyset} \left|(X_a \cap C_{\underline{c},f_i})^{tr}(B)\right|.$$

The cells $C_{\underline{c},f_i} \subset \{f_i = 0\}$ are not open (because hypersurface have dimension $m-1$). Let

$$p_{\underline{c}} : C_{\underline{c},f_i} \xrightarrow{\sim} \mathbb{R}^{m_i}, \quad m_i < m$$

be the definable homeomorphic projection (as in the proof of the Cellular Decomposition Theorem) with image an open cell in $\mathbb{R}^{m_i}$.

We have $|(X_a \cap C_{\le, f_i})^{tr}(B)|$

$p_\le$ is semialgebraic

$$= \left| p_\le\left((X_a \cap C_{\le, f_i})^{tr}(B)\right) \right|$$

$$\le \left| p_\le(X_a \cap C_{\le, f_i})^{tr}(B) \right|$$

[because $p_\le(\mathbb{Q}^m) \subset \mathbb{Q}^{m_i}$ and $H(p_\le(x)) \le H(x)$ for all $x \in \mathbb{Q}^m$]. But $p_\le(X_a)$ is definable in a space $\mathbb{R}^{m_i}$ with $m_i < m$, so we can apply induction on m to get

$$|(X_a \cap C_{\le, f_i})^{tr}(B)| \le C'' B^{\varepsilon},$$

and then we are done (here C'' is independent of f_i because we can use the equation as a parameter).

□

7 - Setting up the proof of Laurent's Th.

Recall once more the Theorem:

Theorem. $n \geq 1$, $X \subset (\mathbb{C}^\times)^n$ irreducible.

If $X_{tors} = \{x \in X \mid \exists n \geq 1, x^n = 1\} \subset X$ is dense, then $X = x_0 H$ for some $x_0 \in X_{tors}$

and some subgroup $H \subset (\mathbb{C}^\times)^n$.

For the proof, we may assume $\dim(X) \geq 1$.

Consider the homomorphism

$$\begin{aligned} e : \mathbb{C}^n &\longrightarrow (\mathbb{C}^\times)^n \\ (z_j)_j &\longmapsto \left(e^{2i\pi z_j}\right)_j \end{aligned}$$

Define $D = \left([0,1[+ i\mathbb{R}\right)^n \subset \mathbb{C}^n$.

Lemma. The map e induces bijections

$$D \longrightarrow (\mathbb{C}^\times)^n,$$

$$D \cap \mathbb{Q}^n \longrightarrow (\mathbb{C}^\times)^n_{tors}.$$

Proof. This is simply because exp is a bijection $\mathbb{R} + i[0,2\pi[\xrightarrow{\sim} \mathbb{C}^\times$ and because $z^n = 1 \iff z = e^{2i\pi k/n}$ for some integer $k \in \mathbb{Z}$. $\square$

Then comes another easy observation.

Lemma. Let $\mathcal{L} = (+,-,\cdot,0,1,\leq,\overbrace{\exp,\sin}^{\text{unary functions}})$ and $\mathbb{R}$ the $\mathcal{L}$-structure where exp is interpreted as the usual exponential and sin as the function $\tilde{\sin}$ $\begin{cases} x \longmapsto \sin(x), & 0 \leq x \leq 2\pi \\ x \longmapsto 0, & \text{otherwise} \end{cases}$.

Then the sets

$$D \subset \mathbb{R}^{2n}, \quad (\mathbb{C}^\times)^n \subset \mathbb{R}^{2n} - \{0\}$$

are $\mathcal{L}$-definable and the map

$$e|D : D \longrightarrow (\mathbb{C}^\times)^n$$

is $\mathcal{L}$-definable.

Proof. Identify $\mathbb{C}^n$ with $\mathbb{R}^{2n}$ by

$$(z_j) \longmapsto (x_j, y_j).$$

Then $(x_j, y_j) \in D \iff 0 \leq x_j < 1$ for all j

and $(x_j, y_j) \in (\mathbb{C}^\times)^n \iff (x_j \neq 0 \vee y_j \neq 0)$ for all j.

Consider $\Gamma_{e|D} \subset D \times (\mathbb{C}^\times)^n$:

$$(x_j, y_j, u_j, v_j) \in \Gamma_e \iff \begin{cases} (x_j, y_j) \in D \\ (u_j, v_j) \in \Gamma_e \end{cases}$$

and $$\begin{cases} e^{-2\pi y_j} \cos(2\pi x_j) = u_j, \\ e^{-2\pi y_j} \sin(2\pi x_j) = v_j. \end{cases}$$

Now note that $\alpha = \pi$ can be defined in $\mathcal{L}$ by

$$\varphi(\alpha) : \left(\widetilde{\sin}\left(\frac{\alpha}{2}\right) = 1 \wedge \left(\forall x, \left(0 < x < \alpha \to \widetilde{\sin}\left(\frac{\alpha}{2}\right) \neq 1\right)\right)\right)$$

so that $x \mapsto e^{-2\pi x}$ is $\mathcal{L}$-definable, as well as $x \longmapsto \sin(2\pi x)$ on $[0,1[$, and also $x \longmapsto \cos(2\pi x)$ on $[0,1[$: the graph is defined as the (x,y) such that

$$\begin{aligned} &((0 \leq x < 1) \wedge (y^2 = 1 - x^2) \\ &\qquad \wedge \left(\left(0 \leq x < \tfrac{1}{4}\right) \vee \left(\tfrac{3}{4} \leq x < 1\right) \to y \geq 0\right) \\ &\qquad \wedge \left(\left(\left(\tfrac{1}{4} \leq x \leq \tfrac{3}{4}\right) \longrightarrow (y \leq 0)\right)\right). \end{aligned}$$

□

Corollary. Let $\tilde{X} = e^{-1}(X) \subset D$. Then $\tilde{X}$ is $\mathcal{L}$-definable.

Proof. Since $X \subset (\mathbb{C}^{\times})^n$ is algebraic, it is also as a subset of $\mathbb{R}^{2n}$ in $\mathcal{L}_{or}$; since $e|D$ is definable, $\tilde{X}$ is definable.

□

Now we have:

Theorem. (van den Dries-Miller, 1994)

The $\mathcal{L}$-structure $\mathbb{R}$ is o-minimal.

(This is quite deep, as it contains Wilkie's Theorem from 1991 that $\mathbb{R}$ is o-minimal for the "simpler" language $(+, \cdot, -, 0, 1, \leq, \exp)$.)

It follows that we can apply the Pila-Wilkie Theorem to $\tilde{X} \cap \mathbb{Q}^n$, which means getting bounds on $|\tilde{X}^{tr}(B)|$.

8. Application of the Pila-Wilkie Theorem

Proposition. Assume X_{tors} is dense $\dim(X) \geq 1$.

Then $\tilde{X}^{alg} \neq \emptyset$.

Proof. Step 1: assume that X is defined by equations $f(x) = 0$ with $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ for some finite algebraic extension $K/\mathbb{Q}$ (what is called a number field).

Then the key observation is the following: if $x \in X_{tors}$, then for any $\sigma \in Aut(\mathbb{C})$ such that $\sigma|K = Id$, we have $\sigma(x) \in X_{tors}$:

first, $\sigma(x) \in X$ because σ fixes the coefficients of the equations defining X, then $\sigma(x) \in X_{tors}$ because $\sigma(\xi)$ is a root of unity for any root of unity ξ. Moreover, $\sigma(\xi)$ is of the same order as ξ. This translates to the following: if $z \in \tilde{X}^{tr} \cap \mathbb{Q}^n$ has "large" height, then we get many other $z' = e^{-1}(\sigma(z))$, which will be in $\tilde{X}^{tr}(B)$ for the same B, and ultimately too many for the Pila - Wilkie bound.

Now the details...

Step 1.1. Let $z \in \tilde{X}(B)$ and $x = e(z)$. Let x_j be a coordinate of x of order $b = H(z)$ $(= \max H(z_j))$. If b is large enough, then

$\mathbb{Q}(x_j)$ is not contained in K and in fact

$$[K(x_j) : K] \geq \frac{\varphi(b)}{[K:\mathbb{Q}]}$$

where φ is the Euler function $\left(\varphi(b) = \left| (\mathbb{Z}/b\mathbb{Z})^\times \right| \right)$.

Indeed, one knows that $[\mathbb{Q}(x_j) : \mathbb{Q}] = \varphi(b)$, because $\mathbb{Q}(x_j)/\mathbb{Q}$ is Galois (splitting field of $X^b - 1 \in \mathbb{Q}[X]$) with an isomorphism

$$\left\{ \begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(x_j)/\mathbb{Q}) & \xrightarrow{\sim} & (\mathbb{Z}/b\mathbb{Z})^\times \\ \sigma & \longmapsto & \dfrac{\sigma(x_j)}{x_j} \end{array} \right.$$

(The tricky part is to prove that this is surjective: this is the irreducibility of the b-th cyclotomic polynomial over $\mathbb{Q}$).

Now, by multiplicativity of the degree in towers, we have

$$[K(x_j) : \mathbb{Q}] = [K(x_j) : K]\,[K : \mathbb{Q}]$$

so $$[K(x_j) : K] = \frac{[K(x_j) : \mathbb{Q}]}{[K:\mathbb{Q}]}$$

$$\geq \frac{[\mathbb{Q}(x_j) : \mathbb{Q}]}{[K:\mathbb{Q}]} = \frac{\varphi(b)}{[K:\mathbb{Q}]}.$$

Step 1.2. Pick $x \in X_{tors}$, $z \in \tilde{X}(\mathbb{Q})$ such that $x = e(z)$, $b = H(x)$ and j s.t. $b = H(x_j)$. Then b is a primitive b-th root of unity.

For all $\sigma \in Gal(K(x_j)/K)$, we have $e^{-1}(\sigma(x)) \in \tilde{X}(b)$ (because if ξ is a root of unity of order d, then $\sigma(\xi)$ also).

Therefore
$$|\tilde{X}(b)| \geq \frac{\varphi(b)}{[K:\mathbb{Q}]} \geq \frac{c_1}{[K:\mathbb{Q}]} \frac{b}{\log\log b}$$
according to the next lemma.

Lemma. There exists $c_1 > 0$ such that for $b \geq e^e$ we have $\varphi(b) \geq c_1 \dfrac{b}{\log\log b}$.

from Pila-Wilkie

Taking $\varepsilon = \frac{1}{2}$ in the Pila-Wilkie Theorem, we have
$$|\tilde{X}^{tr}(b)| \leq \boxed{C_{1/2}}\, b^{1/2}.$$

Since $\dim(X) \geq 1$, X_{tors} must be infinite to be dense, so we can find $x \in X_{tors}$ with b arbitrarily large. But then for b sufficiently big, the bounds above give $\tilde{X}(b) \neq \tilde{X}^{tr}(b)$, so $\tilde{X}^{alg} \neq \emptyset$.

Proof of the Lemma. We use the formula

$$\varphi(b) = b \prod_{\boxed{p \mid b}} \left(1 - \frac{1}{p}\right),$$

which follows

primes dividing b

from the Chinese Remainder Theorem $(\mathbb{Z}/b\mathbb{Z})^{\times} \simeq \prod_{p \mid b} (\mathbb{Z}/p^{v_p}\mathbb{Z})^{\times}$ and the elementary fact $|\varphi(p^n)| = p^n - p^{n-1}$ for p prime and $n \geq 1$. So we need a lower bound for

$$\prod_{p \mid b} \left(1 - \frac{1}{p}\right)$$

and we observe

$$\prod_{p \mid b} \left(1 - \frac{1}{p}\right) \geq \prod_{1 \leq j \leq \omega} \left(1 - \frac{1}{p_j}\right)$$

where ω is the number of prime factors of b and $p_1 = 2 < p_2 = 3 < \dots$ are the first ω primes. We have $2^{\omega} \leq b$ so $\omega \leq \frac{\log(b)}{\log(2)}$.

Finally

$$\prod_{j=1}^{\omega} \left(1 - \frac{1}{p_j}\right) \prod_{j=1}^{\omega} \left(1 + \frac{1}{p_j}\right) \geq \alpha > 0$$

(because the produc $\prod \left(1 - \frac{1}{p^2}\right)$ converges to a >0 value) so

$$\prod_{j=1}^{\omega}\left(1-\frac{1}{p_j}\right) \geq \frac{\alpha}{\prod_{j=1}^{\omega}\left(1+\frac{1}{p_j}\right)}$$

but

$$\prod_{j=1}^{\omega}\left(1+\frac{1}{p_j}\right) \leq \exp\left(\sum_{j=1}^{\omega}\frac{1}{p_j}\right).$$

It a consequence of the elementary results of Chebychev that $\sum_{j=1}^{\omega}\frac{1}{p_j} \leq 2\log\log p_\omega$

$$\leq c \log\log \omega$$

so

$$\prod_{j=1}^{\omega}\left(1+\frac{1}{p_j}\right) \leq (\log \omega)^c$$

and finally

$$\varphi(b) \geq c_1 \frac{b}{(\log\log b)}$$

for some $c_1 > 0$, as claimed.

□

We now finish this part with: .

<u>Step 2</u> - Reduction to Step $\underline{1}$: we know that $X \subset (\mathbb{C}^\times)^n$ is defined by polynomial equations in $X_j^{\pm 1}$, $1 \leq j \leq n$; by Hilbert's Theorem, it is enough to use finitely many equations, but a priori they

might have transcendental coefficients. However, this is not the case:

<u>Lemma</u>. Let $X \subset (\mathbb{C}^\times)^n$ be such that X contains a dense set of points with <u>algebraic</u> coordinates. Then X is the zero set of (finitely many) polynomials with coefficients in a number field.

<u>Proof</u>. (Sawin)

Let $(\alpha_i)_{i \in I}$ be a basis of $\mathbb{C}$ as $\bar{\mathbb{Q}}$-vector space. Let $f \in \mathbb{C}[x_j^{\pm 1}]$ be a polynomial vanishing on X. We expand the coefficients and write

$$f = \sum_{j \in J} \alpha_j f_j$$

for some $J \subset I$ finite and $f_j \in \bar{\mathbb{Q}}[x_j^{\pm 1}]$.

Let $x \in X \cap \bar{\mathbb{Q}}^n$; then $0 = f(x) = \sum \alpha_j f_j(x)$, so $f_j(x) = 0$ for all j (definition of a basis), and since $X \cap \bar{\mathbb{Q}}^n$ is Zariski-dense (par hypothèse) it follows that f_j vanishes on X.

This means $X \subset \{$ zeros of all f_j associated to all $f\}$ and since the converse inclusion is automatic, we conclude that the polynomials f_j, for f varying, define X. By Hilbert's Theorem, we only need finitely many, and their coefficients generate a number field.

$\square$

9_ Understanding the algebraic part

To finish the proof one needs to understand the following situation:

given

$$\begin{tikzcd} \mathbb{C}^n \arrow[r, "e"] & (\mathbb{C}^\times)^n \\ Y \arrow[u, phantom, "\cup"] & \end{tikzcd}$$

with Y (semi)algebraic, what are the algebraic subsets containing $e(Y)$? (In the case above, $Y \subset \tilde{X}^{alg}$ is a connected semialgebraic set of dim ≥ 1 and $e(Y) \subset X$) We expect these to be very restricted (often $e(Y)$ is Zariski-dense !)

This is a question of "transcendance" flavor: want to prove that the exponential of algebraic data is rarely algebraic.

The basic result is:

Theorem (Ax, 1971; "Ax-Lindemann-Weierstrass")

Let $Y \subset \mathbb{C}^n$ be algebraic and suppose

$$z_1, \dots, z_n : Y \longrightarrow \mathbb{C}$$

are $\mathbb{Q}$-linearly independend modulo $\mathbb{C}$ [if $\sum \alpha_i z_i$ is constant on Y, then $\alpha_i = 0$ for all i]. Then

$$e^{z_1}, \dots, e^{z_n} : Y \longrightarrow \mathbb{C}$$

are algebraically independent over $\mathbb{C}$.

Remark. The "Lindemann-Weierstrass" name comes by reference to one of the first big transcendance theorems:

Th. (Lindemann, Weierstrass ~ 1880). If $z_1, \dots, z_n$ are algebraic over $\mathbb{Q}$ and linearly independent over $\mathbb{Q}$, then $e^{z_1}, \dots, e^{z_n}$ are algebraically independent over $\mathbb{Q}$.

(E.g., 1 is $\mathbb{Q}$-lin. indep. so $e^1 = e$ is transcendental; $e^{i\pi} = -1$ is not transcendental, so $i\pi$ cannot be algebraic)

How does this apply to our question? First, there is a relatively simple lemma:

Lemma. If $X \subset \mathbb{C}^n$ is a complex-analytic set (= solution of holomorphic equations) and $Y \subset X$ is semialgebraic (viewing $\mathbb{C}^n$ as $\mathbb{R}^{2n}$), then there exists a complex algebraic $Y \subset Y' \subset X$.

In particular, $\tilde{X}^{alg} \subset D$ is contained in $e^{-1}(X)$, which is a complex-analytic variety (defined by $e(f(z)) = 0$ for f vanishing on X), so $e^{-1}(X)$ contains an algebraic subvariety $Y \subset e^{-1}(X)$.

If $X \neq (\mathbb{C}^\times)^n$ [which would be fine], then

$e(Y) \subset X$ implies that $e^{z_1}, \dots, e^{z_n}$ are not algebraically independent on Y, so by Ax's Theorem, the functions $z_1, \dots, z_n$ on Y satisfy a linear relation $\sum_{j=1}^{n} \alpha_j z_j = \alpha$ with α, α_j in $\mathbb{C}$, and $(\alpha_j) \neq 0$. This means that Y is contained in a proper affine hyperplane (with rational coefficients), so $e(Y)$ is contained in an algebraic subgroup $H \neq (\mathbb{C}^*)^n$ (because $\sum \frac{a_j}{b_j} z_j = \alpha$ implies that $\prod (e^{z_j})^{a_j} = \alpha^{\sum b_j}$ for all $z \in Y$). This is the first step.

In fact, we will proceed through a more geometric statement, which is in fact equivalent to Ax's Theorem, but somewhat more easily applicable.

Theorem – Let $Y \subset \mathbb{C}^n$ be an irreducible algebraic variety. The Zariski closure $\overline{e(Y)}$ is a translate of an algebraic subgroup $H \subset (\mathbb{C}^\times)^n$.

To apply this, we take Y of dimension ≥ 1 containing an algebraic piece of $\tilde{X}$ and contained in $e^{-1}(X)$; then $\overline{e(Y)} \subset X$, so X contains a coset $x_0 H$ for some $x_0 \in X$ and some H of dimension ≥ 1 (connected). From there, it is relatively easy to conclude by induction on $\dim(X)$ (take the quotient modulo H, etc).

Remarkably, while the original proof of Ax is based on differential algebra, Pila, Zannier and others discovered that it (and generalizations/variants) could also be proved using o-minimality. First, this was done through Pila-Wilkie, but there is now a simpler proof by Peterzil-Starchenko, which we now explain.

10. The Peterzil - Starchenko approach

Recall the setup : $n \geq 1$, $Y \subset \mathbb{C}^n$ is an irreducible algebraic variety, and we want to find $x_0 \in (\mathbb{C}^\times)^n$ and $H \subset (\mathbb{C}^\times)^n$ connected algebraic subgroup such that

$$\overline{e(Y)} = x_0 H \qquad (*)$$

(i.e. $x_0^{-1} e(Y)$ does not satisfy any polynomial equation except those defining H, which are of the form $\prod x_j^{a_j} = \alpha$).

How can we go in this direction ? A good first step would be to identify a candidate for H. And we can : if $(*)$ holds, then H can be recovered as the stabilizer of $\overline{e(Y)}$ in $(\mathbb{C}^\times)^n$.

More precisely let $Z = \overline{e(Y)}$ and

$$\tilde{H} = \{ x \in (\mathbb{C}^\times)^n \mid x Z = Z \}.$$

It is straightforward that $\tilde{H} < (\mathbb{C}^\times)^n$ is an (algebraic) subgroup, but for general Z, it might not be connected, so let H be the connected component of the identity. Let further

$$W = e^{-1}(H) \subset \mathbb{C}^n$$

which is a $\mathbb{C}$-vector subspace. (In Lie-theoretic terms, W can be identified to the Lie algebra of the Lie group H, as e is the Lie-theoretic exponential map.)

We can weaken the goal of showing $Z = x_0 H$ a bit:

Lemma 1 - We have $Z = x_0 H$ for some x_0 if and only if $e(Y) \subset x_1 H$ for some x_1.

Proof - "Only if" is clear; conversely, assume $e(Y) \subset x_1 H$; then $Z \subset x_1 H$; pick $x_0 \in Z$, to get

$$x_0 H \subset HZ \subset Z \subset x_1 H.$$

Since $x_0 H$, $x_1 H$ and Z are irreducible algebraic varieties, we get $x_0 H = Z = x_1 H$. □

Now we begin by the following definition (already used by Pila - Zannier):

$$\Sigma = \{ \lambda \in \mathbb{C}^n \mid (\lambda + Y) \cap D \neq \emptyset \text{ and } (\lambda + Y) \cap D \subset e^{-1}(Z) \}.$$

Lemma 2 - The following properties hold:

(1) Σ is $\mathcal{L}$-definable [where $\mathcal{L} = (+, -, \cdot, 0, 1, \leq, \exp, \sin)$ as before]

(2) If $\lambda \in \mathbb{Z}^n$ satisfies $\underbrace{(\lambda + D) \cap Y}_{\text{not } (\lambda + Y) \cap D} \neq \emptyset$, then $-\lambda \in \Sigma$.

(3) $Y \subset D - (\Sigma \cap \mathbb{Z}^n)$.

(4) $\lambda \in \Sigma \Rightarrow \lambda + Y \subset e^{-1}(Z)$.

(5) $e(\Sigma) \subset \tilde{H} = \mathrm{Stab}(Z)$.

Proof - (1) is straightforward.

(2) If $z \in D$ satisfies $\lambda + z = y \in Y$, then

$$-\lambda + y = z \in (\lambda + Y) \cap D \text{ and}$$

$$e((\lambda + Y) \cap D) \subset e(\lambda + Y) = e(Y)$$

since $e(\mathbb{Z}^n) = \{1\}$.

(3) Let $y \in Y$; there is a $\lambda \in \mathbb{Z}^n$ s.t.

$$y - \lambda \in D$$

so that $y \in (\lambda + D) \cap Y$, hence $-\lambda \in \Sigma$ by (2) and $y = (y-\lambda) + \lambda \in D - (\Sigma \cap \mathbb{Z}^n)$.

(4) If $\lambda \in \Sigma$ then $e((\lambda + Y) \cap D) \subset Z$; but $(\lambda + Y) \cap D$ is Zariski-dense in $\lambda + Y$ (open in the euclidean topology and not empty, and $\lambda + Y$ is irreducible), so $e(\lambda + Y) \subset Z$.

(5) Let $\lambda \in \Sigma$; by (4) we have $e(\lambda + Y) \subset Z$ hence $e(Y) \subset e(-\lambda) Z$; since $e(-\lambda) Z$ is an algebraic variety, we get $Z = \overline{e(Y)} \subset e(-\lambda) Z$ and then $Z = e(-\lambda) Z$, or $e(\lambda) Z = Z$.

□

Proposition 1 – There exists a finite set $F \subset \mathbb{C}^n$ such that $Y \subset W + F + D$.

This is where o-minimality will appear.

Proof - Pick $\tilde{C}$ representatives of $\tilde{H}/H$, and pick C s.t. $e(C) = \tilde{C}$, C finite.

Then $e\left(\bigcup_{\lambda \in C} (\lambda + W)\right) =: H$, so by part (5) of Lemma 2

$$e(\Sigma) \subset e(H) = e\left(\bigcup_{\lambda \in C} (\lambda + W)\right),$$

hence $\Sigma \subset W + \bigcup_{\lambda \in C} (\lambda + \mathbb{Z}^n)$.

But $\bigcup_{\lambda \in C} (\lambda + \mathbb{Z}^n)$ is discrete and Σ is definable in an o-minimal structure, so there is a finite subset $F \subset \bigcup_{\lambda \in C} (\lambda + \mathbb{Z}^n)$ such that

$$\Sigma \subset W - F$$

(Σ has only finitely many connected components)

and then by Part (3) of Lemma 2, we get

$$Y \subset D - (\Sigma \cap \mathbb{Z}^n)$$

$$\subset D + W - F.$$

□

Proposition 2 - There exists $\lambda \in \mathbb{C}^n$ such that $Y - \lambda \subset W$.

This concludes the proof, since it follows that

$$e(Y) \subset e(\lambda) H$$

and so we can apply Lemma 1.

Proof. By Prop. 1, we have

$$Y \subset W + D + \overset{\text{finite}}{\boxed{F}}$$

and we can find a compact subset $K \subset \mathbb{C}^n$ such that

$$Y \subset W + K + (i\mathbb{R})^n = M + K$$

where $M = W + (i\mathbb{R})^n \subset \mathbb{C}^n$.

The space M is an $\mathbb{R}$-linear subspace. Because Y is irreducible, we deduce (elementary linear algebra) that in fact $Y \subset M + \lambda$ for some λ in $\mathbb{C}^n$. Then $Y - \lambda \subset M$, but $Y - \lambda$ is a complex algebraic variety, and deduces (also elementarily) that $Y - \lambda \subset iM$

so

$$Y - \lambda \subset M \cap iM.$$

Finally, check that $M \cap iM = W$...

□

Let us prove some of the last small step above:

(1) $Y \subset M + K \Rightarrow Y \subset M + \lambda$

To see this, note that by linear algebra, it amounts to the same to prove that for any $\mathbb{R}$-linear form $\xi : \mathbb{C}^n \longrightarrow \mathbb{R}$ such that $\xi(M) = \{0\}$, the restriction of ξ to Y is constant. We know that $\xi(Y) \subset \xi(K)$, which is bounded. But moreover, there is a $\mathbb{C}$-linear form $\tilde{\xi} : \mathbb{C}^n \longrightarrow \mathbb{C}$ such that $\xi = \mathrm{Re}(\tilde{\xi})$, namely

$$\tilde{\xi}(\mu) = \xi(\mu) - i\,\xi(i\mu) \qquad \text{(check!)}$$

so that $\tilde{\xi}(Y) \subset \mathbb{C}$ is bounded also, and because $\tilde{\xi}(Y)$ is an irreducible complex algebraic variety, it must be a single point so $\xi(Y) = \mathrm{Re}(\tilde{\xi}(Y))$ also.

□

(2) $Y - \lambda \subset M \Rightarrow Y - \lambda \subset iM$

The point is again that $Y - \lambda$ is a complex alge-

-braic variety, whereas M is an $\mathbb{R}$-vector space; but then the $\mathbb{R}$-subspace of $\mathbb{C}^n$ generated by $Y-\lambda$ is in fact a $\mathbb{C}$-linear subspace (if ξ is an $\mathbb{R}$-linear form vanishing on $Y-\lambda$, then $\tilde{\xi}$ $\mathbb{C}$-linear with $\mathrm{Re}(\tilde{\xi}) = \xi$ will vanish on $Y-\lambda$). So

$$iY \subset M$$

(3) $\underline{M \cap iM = \omega}$

The point here is that ω has a basis in $\mathbb{R}^n$ (even in $\mathbb{Z}^n$), so $\omega = \tilde{\omega} \oplus i\tilde{\omega}$ for some real-vector space $\tilde{\omega} \subset \mathbb{C}^n$. Let then $\lambda \in M \cap iM$; write

$$\lambda = w_1 + i v_1, \qquad w_1 \in \omega,\ v_1 \in i\mathbb{R}^n$$

$$= i w_2 - v_2, \qquad w_2 \in \omega,\ v_2 \in i\mathbb{R}^n$$

so that $$w_1 - i w_2 = -v_2 - i v_1 \in \tilde{\omega} \oplus i\tilde{\omega}$$

implies that v_1 and v_2 are in $\tilde{\omega}$ and

$$\lambda = w_1 + i v_1 \in \omega .$$