Rational points on definable sets

Lectures by Prof. Alex Wilkie, University of Manchester
Typeset by Adam Gutter, Carnegie Mellon University

These notes are based on lectures and a handout given by Professor Alex Wilkie as part of an LMS-EPSRC Short Course held at the University of Manchester from July 8th to 12th, 2013. Many thanks to the LMS, EPSRC, University of Manchester, and Prof. Wilkie for these lectures.

1 Introduction

The aim of these lectures is to prove the following:

1.1 Theorem (Pila-Wilkie [PW])

Let $S \subseteq \mathbb{R}^n$ be a set definable in some o-minimal expansion of the order field of real numbers. Assume that S contains no infinite semi-algebraic subset. Let $\epsilon > 0$ be given. Then for all sufficiently large H, the set S contains at most H^ϵ rational points of height at most H.

- The underlined terms will be defined below.

1.2

For $q \in \mathbb{Q}$, say $q = a/b$ in lowest terms, the height of q, denoted $\mathrm{ht}(q)$, is defined as $\max\{|a|, |b|\}$. For $\overline{q} = \langle q_1, \ldots, q_n \rangle \in \mathbb{Q}^n$, $\mathrm{ht}(\overline{q}) := \max\{\mathrm{ht}(q_1), \ldots, \mathrm{ht}(q_n)\}$.

1.3

A set $S \subseteq \mathbb{R}^n$ is called basic semi-algebraic if it is of the form $\{\overline{a} \in \mathbb{R}^n : P(\overline{a}) > 0\}$ for some polynomial $P(\overline{x}) \in \mathbb{R}[\overline{x}]$.

The collection $\mathcal{A}_n$ of all semi-algebraic subsets of $\mathbb{R}^n$ is defined inductively as follows:

(1) Every basic semi-algebraic subset of $\mathbb{R}^n$ is in $\mathcal{A}_n$;

(2) If $X \in \mathcal{A}_n$, then $\mathbb{R}^n \setminus X \in \mathcal{A}_n$;

(3) If $X, Y \in \mathcal{A}_n$, then $X \cup Y \in \mathcal{A}_n$ and $X \cap Y \in \mathcal{A}_n$;

(4) Nothing else is in $\mathcal{A}_n$.

1.4 Exercises

(1) Let $P(\overline{x}) \in \mathbb{R}[\overline{x}]$ (where $\overline{x} = x_1, \ldots, x_n$). Prove that $Z(P) \in \mathcal{A}_n$, where $Z(P) := \{\overline{a} : P(\overline{a}) = 0\}$.

(2) Suppose that $X \in \mathcal{A}_n$ and $Y \in \mathcal{A}_m$. Prove that $X \times Y \in \mathcal{A}_{n+m}$.

(3) Find an example of a polynomial $P(x) \in \mathbb{R}[x]$ (in the single variable x) such that the closure of the set $\{x \in \mathbb{R} : P(x) > 0\}$ is not the set $\{x \in \mathbb{R} : P(x) \geq 0\}$. Show, however, that (for your example) the closure of $\{x \in \mathbb{R} : P(x) > 0\}$ is a semi-algebraic subset of $\mathbb{R}$.

2 Some semi-algebraic geometry

In fact, it is the case that the closure of any semi-algebraic set is semi-algebraic, but this is very difficult to prove directly. Instead we appeal to the fundamental result of the subject.

2.1 Theorem (Tarski-Seidenberg, see e.g. [vdD])

Let $Y \in \mathcal{A}_{n+m}$ and let $X := \pi_n^{n+m}[Y]$ be the projection of Y onto the first n coordinates, i.e.

$$X = \{\bar{x} \in \mathbb{R}^n : \exists \bar{y} \in \mathbb{R}^m \langle \bar{x}, \bar{y} \rangle \in Y\}.$$

Then $X \in \mathcal{A}_n$.

2.2 Exercise

Let $Y \in \mathcal{A}_{n+m}$ and set $X' := \{\bar{x} \in \mathbb{R}^n : \forall \bar{y} \in \mathbb{R}^m \langle \bar{x}, \bar{y} \rangle \in Y\}$. Prove that $X' \in \mathcal{A}_n$.

Now, for any set $X \subseteq \mathbb{R}^n$, observe that the closure $\overline{X}$ of X in $\mathbb{R}^n$ satisfies, for all $\bar{x} \in \mathbb{R}^n$,

$$\bar{x} \in \overline{X} \iff \forall \epsilon \in \mathbb{R}(\epsilon > 0 \implies \exists \bar{y} \in \mathbb{R}^n(\|\bar{x} - \bar{y}\|^2 < \epsilon \text{ and } \bar{y} \in X)).$$

So if $X \in \mathcal{A}_n$, the expression on the right-hand side here provides a recipe for showing (via uses of 2.1 and of the rules 1.3(1), (2), and (3)) that $\overline{X} \in \mathcal{A}_n$.

2.3 Exercises

(1) Complete the proof that $\overline{X} \in \mathcal{A}_n$ whenever $X \in \mathcal{A}_n$. Use a similar method to show that the interior X° of X is in $\mathcal{A}_n$ whenever X is.

(2) Convince yourself that if $f : \mathbb{R}^n \to \mathbb{R}$ is a semi-algebraic function (meaning that its graph is a semi-algebraic subset of $\mathbb{R}^{n+1}$), then the set $\{\bar{x} \in \mathbb{R}^n : f \text{ is continuous at } \bar{x}\}$ is a semi-algebraic subset of $\mathbb{R}^n$.

There are many structure theorems for semi-algebraic sets. For example, every $X \in \mathcal{A}_n$ has the form $X = \bigcup_{i=1}^{N} X_i$, where each X_i is in $\mathcal{A}_n$ and is connected. This is fairly clear for $n = 1$, and it turns out that one can actually deduce the general case from this using little more than the properties 1.3(1), (2), (3), and 2.1. This suggests an axiomatic treatment.

3 O-minimal structures ([PS], [vdD])

Let A be any non-empty set and suppose we are given, for each $n \geq 1$, a collection $\mathcal{S}_n$ of subsets of A^n. We write $\mathcal{S}$ for the disjoint union $\dot{\bigcup}_{n \geq 1} \mathcal{S}_n$. We call $\mathcal{S}$ a structure (on A).

3.1 Definition

The <u>definable hull</u>, $\tilde{\mathcal{S}} = \dot{\bigcup_{n\geq 1}} \tilde{\mathcal{S}}_n$, of $\mathcal{S}$ is the collection of sets defined inductively as follows:

(1) $\mathcal{S}_n \subseteq \tilde{\mathcal{S}}_n$ (and each $X \in \tilde{\mathcal{S}}_n$ is a subset of A^n);

(2) $\{a\} \in \tilde{\mathcal{S}}_1$ for each $a \in A$;

(3) For each i, j with $1 \leq i, j \leq n$, $\{\langle a_1, \ldots, a_n\rangle \in A^n : a_i = a_j\} \in \tilde{\mathcal{S}}_n$;

(4) If $X \in \tilde{\mathcal{S}}_n$ and $Y \in \tilde{\mathcal{S}}_m$ then $X \times Y \in \tilde{\mathcal{S}}_{n+m}$;

(5) If $X, Y \in \tilde{\mathcal{S}}_n$, then $X \cup Y, X \cap Y$, and $A^n \setminus X$ are all in $\tilde{\mathcal{S}}_n$;

(6) If $X \in \tilde{\mathcal{S}}_{n+m}$, then $\pi_n^{n+m}[X] \in \tilde{\mathcal{S}}_n$;

(7) Nothing else is in $\tilde{\mathcal{S}}_n$.

Sets in $\tilde{\mathcal{S}}$ are called <u>definable</u> (from, or in, $\mathcal{S}$). Functions whose graphs are in $\tilde{\mathcal{S}}$ are called <u>definable functions</u>.

3.2 Examples and exercises

(1) Say $A = \mathbb{C}$ and $\mathcal{S}_n = \{Z(P) : P(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]\}$. By quoting a suitable famous theorem, prove that $\tilde{\mathcal{S}}_n$ consists precisely of the <u>constructible</u> sets (i.e. $\tilde{\mathcal{S}}_n$ is just the Boolean closure of $\mathcal{S}_n$).

(2) Say $A = \mathbb{N}$ and $\mathcal{S}_n = \{Z(P) \cap \mathbb{N}^n : P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]\}$. By quoting a suitable famous theorem, prove that $\mathcal{S}_1$ contains a non-computable set.

(3) For arbitrary $A, \mathcal{S}$, and $X \in \tilde{\mathcal{S}}_n$, prove that $X_\sigma \in \tilde{\mathcal{S}}_n$, where σ is any permutation of $\{1, \ldots, n\}$ and $X_\sigma := \{\langle x_{\sigma(1)}, \ldots, x_{\sigma(n)}\rangle \in A^n : \langle x_1, \ldots, x_n\rangle \in X\}$.

Henceforth, we shall assume that $A = \mathbb{R}$ (thereby abandoning most model-theoretic methods) and consider only those structures $\mathcal{S}$ on $\mathbb{R}$ with $\mathcal{A}_n \subseteq \mathcal{S}_n$ for all n.

3.3 Definition

A structure $\mathcal{S}$ (on $\mathbb{R}$) is called <u>$o-minimal$</u> if every set $X \in \tilde{\mathcal{S}}_1$ is a finite union of open intervals and singleton sets.

The underlying assumption that $\mathcal{A}_n \subseteq \mathcal{S}_n$ for all n is precisely what is meant by saying that "$\mathcal{S}$ is an o-minimal expansion of the ordered field of real numbers" in 1.1. Thus, all the terms in our main theorem have now been explained.

3.4 Remarks and examples

(1) It is crucial in 3.3 that the condition on X (which is equivalent to saying that X has finite boundary) holds for all X in $\tilde{\mathcal{S}}_1$ and not just those X in $\mathcal{S}_1$.

(2) We have seen that $\mathcal{A}$ $(= \tilde{\mathcal{A}})$ is an o-minimal structure, so at least one exists.

(3) Another example (see [W]) is $\mathcal{A}^{\mathrm{exp}}$, where

$\mathcal{A}_n^{\mathrm{exp}} := \{Z(F) : F(x_1, \ldots, x_n) = P(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n})$ for some $P(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{R}[x_1, \ldots, x_n, y_1, \ldots, y_n]\}$.

The definable sets here are precisely the projections of sets in $\mathcal{A}^{\mathrm{exp}}$.

(4) In [Mi], Miller shows that if $\mathcal{S}$ is o-minimal and some function $f : \mathbb{R} \to \mathbb{R}$ of greater than polynomial growth (at ∞) is definable (from $\mathcal{S}$), then $\mathcal{A}^{\mathrm{exp}} \subseteq \tilde{\mathcal{S}}$ (so, of course, $\tilde{A}^{\mathrm{exp}} \subseteq \tilde{\mathcal{S}}$).

(5) Another example (van den Dries-Denef [DD], Gabrielov [G]) is $\mathcal{A}^{\mathrm{an}}$. Here we take $\mathcal{A}_n^{\mathrm{an}}$ to be the union of $\mathcal{A}_n$ and the collection of all bounded subanalytic subsets of $\mathbb{R}^n$. I won't define this collection here, but suffice it to say that if U is an open subset of $\mathbb{R}^n$ and $f : U \to \mathbb{R}$ is a real analytic function (i.e. it is infinitely differentiable, and for each $\bar{a} \in U$, the Taylor series of f at $\bar{a}$ converges to $f(\bar{x})$ for each $\bar{x} \in \mathbb{R}^n$ sufficiently close to $\bar{a}$), then $f \restriction_K$ is definable in $\mathcal{A}^{\mathrm{an}}$ for each closed box $K \subseteq U$. (Exercise: exhibit an analytic function $f : (0,1) \to \mathbb{R}$ which is not definable in any o-minimal structure).

(6) The largest o-minimal structure required for application in this course is $\mathcal{A}^{\mathrm{an,\,exp}}$ ($:= \mathcal{A}^{\mathrm{an}} \cup \mathcal{A}^{\mathrm{exp}}$). The o-minimality here is due to van den Dries and Miller (see [DM]).

(7) There is no largest o-minimal structure. Indeed, in [RSW] it is shown that if $f : [0,1] \to \mathbb{R}$ is any infinitely differential function, then there exists o-minimal structures $\mathcal{S}_1$ and $\mathcal{S}_2$ and functions $f_i : [0,1] \to \mathbb{R}$ definable in $\mathcal{S}_i$ (for $i = 1, 2$), such that $f = f_1 + f_2$. (Exercise: Why does this justify the claim here?)

(8) (Pila-Bombieri) Theorem 1.1 is the best result possible in the sense that the "ϵ" cannot be replaced by any function $\epsilon(H) > 0$ which tends monotonically to 0 as $H \to \infty$. This is already the case for the o-minimal structure $\mathcal{A}^{\mathrm{an}}$. However, for the structure $\mathcal{A}^{\mathrm{exp}}$, I conjecture that "$H^{\epsilon}$" may be replaced by $(\log H)^c$ for some constant c (depending on the set S). This is known for definable curves and some surfaces (see Jones-Thomas [JT], Butler [B]).

4 Some 1-dimensional o-minimal theory

Throughout this section, $\mathcal{S}$ is an arbitrary o-minimal structure. For those not used to working "inside" o-minimal structures, the following exercise provides good practice as well as containing an important result.

4.1 Exercise

Let $a < b$ and suppose that $f : (a,b) \to \mathbb{R}$ is a definable function (in $\mathcal{S}$). Prove that $\lim\limits_{x \to b^-} f(x)$ exists (an an element of $\mathbb{R} \cup \{\pm\infty\}$).

The first major result in the subject is:

4.2 The Monotonicity Theorem

Let $f : \mathbb{R} \to \mathbb{R}$ be a definable function. Then there exist real numbers $a_1 < a_2 < \cdots < a_N$ such that (setting $a_0 = -\infty$ and $a_{N+1} = +\infty$) for each $i = 0, \ldots, N$, $f \restriction_{(a_i, a_{i+1})}$ is continuous and either strictly monotonic or constant.

4.3

It is a remarkable fact of o-minimality (due to Pillay and Steinhorn [PS]) that when a finiteness theorem has been established, then it usually holds *uniformly*. More precisely, suppose that $F : \mathbb{R}^{n+m} \to \mathbb{R}^k$ is a definable map. This gives rise to a family

$$\mathcal{F}_F := \{F(\bar{x}, \cdot) : \bar{x} \in \mathbb{R}^n\}$$

of definable maps from $\mathbb{R}^m$ to $\mathbb{R}^k$ *parameterized by* $\mathbb{R}^n$. Such a family is called a *definable family of maps.*

Now if, in 4.2, $f \in \mathcal{F}_F$, then the N may be chosen to depend only on F. I.e., one may take the same N for all $f \in \mathcal{F}_F$. (We are in the case $m = k = 1$ here). Further, for each $i = 1, \dots, N$, the correspondence $f \mapsto a_i$ may be chosen to be definable in the sense that if $f(\cdot) = F(\bar{x}, \cdot)$, then the $a_1, \dots, a_N$ can be chosen to be definable functions of the parameter $\bar{x}$.

4.4 Exercises

(1) (a) Make precise the notion of a definable family of *subsets* (of $\mathbb{R}^n$) and deduce (from 4.2, 4.3) a uniformity result for definable families of subsets of $\mathbb{R}$. (*Further exercise for model theorists*: Now deduce the Pillay-Steinhorn fundamental theorem for o-minimal structures, namely that any structure (not necessarily with domain $\mathbb{R}$) which is elementarily equivalent to an o-minimal structure is also o-minimal.)
(b) Prove this uniformity result directly in the semi-algebraic case (i.e. the case $\mathcal{S} = \mathcal{A}$).

(2) Let $f : \mathbb{R} \to \mathbb{R}$ be definable. Prove that the set

$$C'_f := \{x \in \mathbb{R} : f \text{ is continuously differentiable on some open neighbourhood of } x\}$$

is definable (and uniformly so in definable families of functions). Deduce that C'_f is cofinite (and hence uniformly so). [Hint: a monotone function (defined on an open interval) is differentiable (Lebesgue-) almost everywhere. Question for model theorists: why is this cheating?]. Show further that the derivative, $f' \restriction_{C'_f}$, of f, is definable.

5 Reparameterization (one variable case)

Theorem 1.1 is proved by first reducing to the case that $S \subseteq (0,1)^n$ (which is easy upon observing that the four functions $x \mapsto \pm x^{\pm 1}$ preserve height (and definability)), and then to the case that S is the image of some definable map $F : (0,1)^m \to (0,1)^n$ for some $m < n$. (We assume that $n \geq 2$. I leave the case $n = 1$ as an exercise!)

The idea now is to *reparameterize* F so that its derivatives, up to some order p, exist and are bounded by 1. This means that we look for a finite set, Φ say, of definable C^p (= p-times continuously differentiable) maps $\phi : (0,1)^m \to (0,1)^m$ such that $F \circ \phi$ is also C^p and both ϕ and $F \circ \phi$ have derivatives (of all orders $\leq p$) bounded by 1. We also require that $\bigcup_{\phi \in \Phi} \mathrm{Im}(\phi) = (0,1)^m$. In this section, I consider the case $m = 1$.

So let $F : (0,1) \to (0,1)^n, x \mapsto \langle F_1(x), \dots, F_n(x) \rangle$ be a definable map. (In fact, everything must be uniform in definable families of such maps, but we suppress the parameters and simply observe that this is the case.) We assume that one of the F_i's is the identity function. By 4.4.(2), there exist $a_0 = 0 < a_1 < \cdots < a_N < 1 = a_{N+1}$ such that each F_i is C^1 on each interval (a_j, a_{j+1}).

Further, by considering the definable sets $\{x \in \mathbb{R} : |F_i'(x)| < |F_k'(x)|\}$ (for $1 \leq i, k \leq n$) and using the definition of o-minimality (3.3) or, more precisely, 4.4(1)(a), we may suppose (after further subdivision) that for each $j = 0, \ldots, N$ and each $i, k = 1, \ldots, n$ that $|F_i'(x)| - |F_k'(x)|$ has constant sign (positive, negative, or zero) throughout (a_j, a_{j+1}).

Fix some j with $1 \leq j \leq N$. We first find the set Φ, as described above, for the case $p = 1$.

Let $x_0 \in (a_j, a_{j+1})$ and choose i_0 so that

$$|F_{i_0}'(x_0)| \geq |F_i'(x_0)| \quad \text{for } i = 1, \ldots, n.$$

Then for all $x \in (a_j, a_{j+1})$ we have

$$|F_{i_0}'(x)| \geq |F_i'(x)| \quad \text{for } i = 1, \ldots, n, \text{ and so also} \tag{5.1}$$

$$|F_{i_0}'(x)| \geq 1. \tag{5.2}$$

In particular, F_{i_0} maps (a_j, a_{j+1}) strictly monotonically onto some interval (c, d), where $0 \leq c < d \leq 1$. Now define $\phi_j : (0,1) \to (0,1)$ by $x \mapsto F_{i_0}^{-1}(c + (d-c)x)$. Clearly ϕ_j is definable and satisfies, for all $x \in (0,1)$,

$$F_{i_0}(\phi_j(x)) = c + (d-c)x \tag{5.3}$$

$$\text{and } \operatorname{Im}(\phi_j) = (a_j, a_{j+1}). \tag{5.4}$$

Then, for $x \in (0,1)$, $|\phi_j'(x)| = \left|\frac{d-c}{F_{i_0}'(\phi_j(x))}\right| \leq |d-c|$ (by (5.2), (5.4)). Further, for $i = 1, \ldots, n$,

$$\begin{aligned} |(F_i \circ \phi_j)'(x)| &= |F_i'(\phi_j(x))| \cdot |\phi_j'(x)| \\ &= \frac{|F_i'(\phi_j(x))| \cdot |d-c|}{|F_{i_0}'(\phi_j(x))|} \\ &\leq |d-c| \quad \text{(by (5.1), (5.4))} \\ &\leq 1. \end{aligned}$$

So, taking Φ to be $\{\phi_0, \ldots, \phi_N\}$ together with the constant functions $x \mapsto a_j$ (for $j = 1, \ldots, N$), we have established the following:

5.5 Lemma (The C^1-1-reparameterization lemma)

Let $F : (0,1) \to (0,1)^n$ be any definable map. Then there exists a finite set Φ of definable, C^1 functions mapping $(0,1)$ to $(0,1)$ such that $\bigcup_{\phi \in \Phi} \operatorname{Im}(\phi) = (0,1)$ and such that for each $\phi \in \Phi$ and $i = 1, \ldots, n$, both $|\phi'|$ and $|(F_i \circ \phi)'|$ are bounded by 1 on $(0,1)$, where F_i denotes the ith coordinate function of F.

We now aim to improve C^1 to C^p in 5.5. We use the following:

5.6 Lemma

Let $p \geq 1$ and let I be a bounded open interval in $\mathbb{R}$. Suppose that $f : I \to (0,1)$ is *any* (not necessarily definable) C^{p+1} function having the property that for all $x \in I$ and all $j = 0, \ldots, p+1$, $f^{(j)}(x) \neq 0$. Then for $j = 0, \ldots, p$ and all $x \in I$,

$$|f^{(j)}(x)| \leq \left(\frac{j+1}{\delta_I(x)}\right)^j,$$

where $\delta_I(x) := \min\{x-a, b-x\}$ (where $I = (a,b)$).
<u>Proof</u>

By linear rescaling it is sufficient to consider $I = (0,1)$ and to prove that, for all $x \in (0, \frac{1}{2}]$,

$$|f^{(j)}(x)| \leq \left(\frac{j+1}{x}\right)^j$$

for $j = 0, \ldots, p$.

We use induction on j (for all f satisfying the hypotheses). The case $j = 0$ being clear, assume that the lemma holds for some j with $0 \leq j < p$. Since neither $f^{(j+1)}$ nor $f^{(j+2)}$ has a zero (note that $j+2 \leq p+1$), it follows that $|f^{(j+1)}|$ is montonic on $(0,1)$. Assume first that $|f^{(j+1)}|$ is decreasing on $(0,1)$. Let $x \in (0, \frac{1}{2}]$. Define $x_0 := \frac{j+1}{j+2} \cdot x$, so that $0 < x_0 < x \leq \frac{1}{2}$. By the Mean Value Theorem, there is some $\xi \in [x_0, x]$ such that

$$f^{(j)}(x) - f^{(j)}(x_0) = f^{(j+1)}(\xi) \cdot (x - x_0). \qquad (1)$$

Since $f^{(j)}$ has no zeros, it follows that $|f^{(j)}(x) - f^{(j)}(x_0)|$ is at most $\max\{|f^{(j)}(x)|, |f^{(j)}(x_0)|\}$ which, by the inductive hypothesis, is bounded by $\left(\frac{j+1}{x_0}\right)^j = \left(\frac{j+2}{x}\right)^j$. Further, since $|f^{(j+1)}|$ is decreasing, $|f^{(j+1)}(\xi)| \geq |f^{(j+1)}(x)|$. Also, $|x - x_0| = \frac{x}{j+2}$. Putting the last three remarks into equation (1), we obtain $\left(\frac{j+2}{x}\right)^j \geq |f^{(j+1)}(x)|$, as required.

Now if $|f^{(j+1)}|$ is increasing on $(0,1)$, we consider the function $g : (0,1) \to (0,1), x \mapsto f(1-x)$. This satisfies all the hypotheses of the theorem, and hence too the inductive hypothesis: $|g^{(j)}(x)| \leq \left(\frac{j+1}{x}\right)^j$ (for all $x \in (0, \frac{1}{2}]$). But $|g^{(j+1)}(x)|$ is decreasing on $(0,1)$, so we may apply the argument above to obtain $|g^{(j+1)}(x)| \leq \left(\frac{j+2}{x}\right)^{j+1}$ (for all $x \in (0, \frac{1}{2}]$).

Now for $x \in (0, \frac{1}{2}]$, $x \leq 1 - x$, so $|f^{(j+1)}(x)| \leq |f^{(j+1)}(1-x)|$ (as $|f^{(j+1)}|$ is increasing on $(0,1)$). But $|f^{(j+1)}(1-x)| = |g^{(j+1)}(x)|$, so we obtain that $|f^{(j+1)}(x)| \leq \left(\frac{j+2}{x}\right)^{j+1}$ in this case, too. □

5.7 Exercises

(1) Formulate and prove a many variable version of 5.6. (Unfortunately, this does not seem to help in proving the many variable reparamterization lemma.)

(2) Suppose that $f : (0,1) \to (0,1)$ satisfies the hypotheses of 5.6 for *all* p. Prove that the series

$$U(z) = U(x + \sqrt{-1}y) := \sum_{j=0}^{\infty} \frac{f^{(j)}(x)}{j!} \cdot (\sqrt{-1}y)^j$$

converges absolutely and uniformly on any compact subset of the region $\{x + \sqrt{-1}y : e \cdot |y| < x \leq \frac{1}{2}\}$. Deduce that f has a complex-analytic continuation to this region and hence that f itself, which was only assumed to be a C^∞ function, is in fact real-analytic. (An old theorem of Bernstein asserts that if $f : (0,1) \to (0,1)$ is a C^∞ function with $f^{(j)}(x) > 0$ for all $j = 0, 1, 2, \ldots$ and all $x \in (0,1)$, then f is real-analytic.)

5.8 Lemma

Let $p \geq 1$ and I be any bounded open interval in $\mathbb{R}$. Suppose that $f : I \to (0,1)$ is any C^{p+1} function having the property that for all $x \in I$ and all $j = 0, \ldots, p+1$, $f^{(j)}(x) \neq 0$. Assume further that $|f'(x)| \leq 1$ for all $x \in I$. Then for $j = 1, \ldots, p$ and all $x \in I$ we have

$$|f^{(j)}(x)| \leq \left(\frac{j}{\delta_I(x)}\right)^{j-1}.$$

Proof

Apply 5.6 with f' in place of f. $\square$

The previous lemmas suggest a reparameterization of the form $f((\delta_I(x))^p)$. So we need a formula for the higher derivatives of composite functions.

5.9 Exercise

Let $f : I \to \mathbb{R}, g : J \to I$ be any C^p functions, where I, J are open subsets of $\mathbb{R}$. Then for any $x \in J$ and $q = 1, \ldots, p$, $(f \circ g)^{(q)}(x)$ has the form

$$\sum_{k=1}^{q} f^{(k)}(g(x)) \cdot \left[\sum_{(q,k)} B_q(k_1, \ldots, k_q) \cdot \prod_{\nu=1}^{q} (g^{(\nu)}(x))^{k_\nu}\right]$$

for some positive integers $B_q(k_1, \ldots, k_q)$ (independent of f, g) and where the inner summation is over all q-tuples $\langle k_1, \ldots, k_q \rangle$ of non-negative integers satisfying the conditions

$$k_1 + k_2 + \cdots + k_q = k \quad \text{and} \quad k_1 + 2k_2 + \cdots + qk_q = q.$$

5.10 Remark

A formula attributed to the Blessed Francesco Faà di Bruno (1825-1888) gives the value for the coefficients:

$$B_q(k_1, \ldots, k_q) = \frac{q!}{\prod_{\nu=1}^{q} k_\nu!(\nu!)^{k_\nu}}$$

(where $0! = 1$).

5.11 Theorem (The C^p-1-reparameterization theorem)

Let $F : (0,1) \to (0,1)^n$ be any definable map. Then for any $p \geq 1$, there exists a finite set Φ of C^p functions mapping $(0,1)$ to $(0,1)$ such that $\bigcup_{\phi \in \Phi} \operatorname{Im}(\phi) = (0,1)$ and such that for each $\phi \in \Phi$, $i = 1, \ldots, n$, and $q = 1, \ldots, p$, both $|\phi^{(q)}|$ and $|(F_i \circ \phi)^{(q)}|$ are bounded by 1 on $(0,1)$, where F_i is the ith coordinate function of F. (Further, $|\Phi|$ depends only on p and uniformly on F, as do the functions in Φ.)

Proof

It is easily seen (exercise) that it is sufficient to prove the theorem with the bound 1 in the conclusion replaced with some function of p (independent of F). This being said, we may assume, by 5.5, that F is a C^1 function with the derivatives of its coordinate functions bounded by 1.

Now, by repeated use of 4.4(2) and the usual subdivision method, there exist $a_0 = 0 < a_1 < \cdots < a_N < a_{N+1} = 1$ such that F is a C^{p+1} map on each interval (a_j, a_{j+1}) and for $\nu = 1, \ldots, p+1$, each coordinate function of $F^{(\nu)}$ is either identically zero or has no zeros on (a_j, a_{j+1}). Define $\phi_j : (0,1) \to (a_j, a_{j+1})$ by $\phi_j(x) := a_j + \frac{1}{2}(a_{j+1} - a_j)x^p$. Then $|\phi_j^{(q)}| \leq p!$ on $(0,1)$ for each $q = 1, \ldots, p$. Also, for $\langle k_1, \ldots, k_q \rangle$ a q-tuple as in 5.9, we have

$$\begin{aligned}\left|\prod_{\nu=1}^{q} (\phi_j^{(\nu)}(x))^{k_\nu}\right| &= \left|\prod_{\nu=1}^{q} ((p(p-1)\cdots(p-\nu+1)\cdot(\frac{a_{j+1}-a_j}{2})\cdot x^{p-\nu})^{k_\nu}\right| \\ &\leq \prod_{\nu=1}^{q} p^{\nu\cdot k_\nu}\cdot(\frac{a_{j+1}-a_j}{2})^{k_\nu}\cdot x^{pk_\nu-\nu k_\nu} \\ &= p^q\cdot(\frac{a_{j+1}-a_j}{2})^k\cdot x^{pk-q} \qquad (\text{for } x\in(0,1)).\end{aligned}$$

We now apply 5.9 and 5.6 with $I = (a_j, a_{j+1})$, $J = (0,1)$, $g = \phi_j$, and $f = F_i \restriction_{(a_j,a_{j+1})}$, where F_i is some coordinate function of F.

Note that ϕ_j actually maps into (and in fact, onto) the left open half of the interval I, so that $\delta_I(\phi_j(x)) = \frac{1}{2}(a_{j+1} - a_j)x^p$ for all $x \in (0,1)$. So it follows from 5.6 that for all $x \in (0,1)$ and all $k = 1, \ldots, q$, $|f^{(k)}(\phi_j(x))| \leq \left(\frac{2k}{(a_{j+1}-a_j)x^p}\right)^{k-1}$. Applying 5.9, we obtain

$$\begin{aligned}|(f\circ\phi_j)^{(q)}(x)| &\leq \sum_{k=1}^{q}\left(\frac{2k}{(a_{j+1}-a_j)x^p}\right)^{k-1}\cdot p^q\cdot x^{pk-q}\cdot\left(\frac{a_{j+1}-a_j}{2}\right)^k\cdot B'_q(k) \\ &= x^{p-q}\cdot p^q\cdot(\frac{a_{j+1}-a_j}{2})\cdot\sum_{k=1}^{q}k^{k-1}\cdot B'_q(k) \\ &\leq B''(p) \qquad (\text{since } q\leq p).\end{aligned}$$

[<u>Exercise</u>: Show that $B''(p)$ may be taken to be $c_1 \cdot p^{c_2 p}$ for some small explicit constants c_1, c_2.] A similar calculation applies to the function $a_{j+1} - \phi_j$, which maps onto the right open half of the interval I. Thus, the proof of 5.11 is now complete upon taking Φ to be $\{\phi_j, a_{j+1} - \phi_j : j = 0, \ldots, N\}$ together with the constant functions with values $a_1, \ldots, a_N, \frac{a_0+a_1}{2}, \ldots, \frac{a_N+a_{N+1}}{2}$. $\square$

5.12 Remark

The parenthetical comment in the statement of 5.11 amounts to this: for F ranging over a definable family of maps $F(\bar{x}, \cdot) : (0,1) \to (0,1)^n$, the number N of subintervals in the above proof stays bounded (i.e. has an upper bound independent of $\bar{x}$) and the endpoints a_j are given by N definable functions of the parameters $\bar{x}$. It follows that the reparameterizing functions in Φ depend definably on $\bar{x}$. (Of course, this is all for a fixed given $p \geq 1$.)

6 Proof of 1.1 in the 1-dimensional case

There is a well-defined notion of dimension for definable sets which we shall come to later. It turns out that definable subsets of $(0,1)^n$ having dimension 1 are precisely the images of definable functions $f : (0,1) \to (0,1)^n$. The 1-dimensional case of 1.1 thus reduces to the following:

6.1 Theorem

Let $f : (0,1) \to (0,1)$ be definable and assume that graph(f) contains no infinite semi-algebraic subset. Then for any $\epsilon > 0$, there exists $C = C(\epsilon)$ such that for all $H > C$, there are fewer than H^ϵ pairs $\langle q_1, q_2 \rangle$ of rational numbers of height at most H such that $f(q_1) = q_2$.

6.2 Exercises

(1) Show that graph(f) (f as above) contains no infinite semi-algebraic subset if and only if for all a, b with $0 < a < b < 1$ and all non-zero polynomials $P(x,y) \in \mathbb{R}[x,y]$, there exists $\alpha \in (a,b)$ such that $P(\alpha, f(\alpha)) \neq 0$.

(2) Show that it is indeed sufficient to prove 6.1 in order to establish 1.1 in the 1-dimensional case (i.e. why may we take $n = 1$).

The proof of 6.1 has three stages. The second of these stages is pure transcendental number theory and requires no o-minimality (nor definability) at all:

6.3 Lemma

Let p and d be integers satisfying $100 \leq 4p \leq d^2 \leq 5p$ and let $\phi, \psi : (0,1) \to (0,1)$ be C^p functions whose derivatives (of all orders $\leq p$) are bounded by 1.

Then for all $\alpha \in (0,1)$ and all $H > 4 \cdot (2d-2)^{d/4}$, there exists a non-zero polynomial $P(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ of degree at most $d-1$ in each variable such that $P(q_1, q_2) = 0$ for all rationals $q_1, q_2 \in (0,1)$ satisfying

(1) $\mathrm{ht}(\langle q_1, q_2 \rangle) \leq H$ and

(2) there exists $\beta \in (0,1)$ with $|\beta - \alpha| < H^{-20/d}$ such that $\phi(\beta) = q_1$ and $\psi(\beta) = q_2$.

For the proof, we use the following version of the Dirichlet Box Principle (i.e. the Pigeon Hole Principle). I leave the proof as an exercise, or see [Wa] (page 132, Lemma 4.11).

6.4 Proposition (Thue-Siegel)

Let $\nu \geq 1, \mu \geq 0$ be integers and for each i, j with $1 \leq i \leq \nu, 0 \leq j \leq \mu$, let $v_{i,j}$ be a real number. Let u, X, ℓ be positive integers satisfying

(1) $u \geq \max\limits_{0 \leq j \leq \mu} \sum\limits_{i=1}^{\nu} |v_{i,j}|$, and

(2) $\ell^{\mu+1} < (X+1)^\nu$.

Then there exist integers $A_1, \ldots, A_\nu$ such that

(3) $0 < \max\limits_{1 \leq i \leq \nu} |A_i| \leq X$, and

(4) $\max\limits_{0 \leq j \leq \mu} \left| \sum\limits_{i=1}^{\nu} A_i \cdot v_{i,j} \right| \leq \frac{uX}{\ell}$.

□

6.5 Proof of 6.3

Let $\theta_1(x), \ldots, \theta_{d^2}(x)$ be an enumeration of the functions $\phi(x)^s\psi(x)^t$ $(0 \le s, t < d)$ and consider the function $G : (0,1) \to \mathbb{R}$ defined by

$$G(x) := \sum_{i=1}^{d^2} A_i \theta_i(x),$$

where the A_i are integers (to be chosen later) satisfying $|A_i| \le H^d$ for $i = 1, \ldots, d^2$.

Now, the point is that if $\beta \in (0,1)$ is such that both $\phi(\beta)$ and $\psi(\beta)$ are rationals of height $\le H$, then either $G(\beta) = 0$ or else $|G(\beta)| \ge \frac{1}{H^{2d-2}}$. (Because if $\phi(\beta) = \frac{a_1}{b_1}, \psi(\beta) = \frac{a_2}{b_2}$, then $G(\beta) = \frac{L}{b_1^{d-1} b_2^{d-1}}$ for some $L \in \mathbb{Z}$.) So if we can choose the A_i's so that $|G(\beta)| < \frac{1}{H^{2d-2}}$ for such β that also satisfy $|\beta - \alpha| < H^{-20/d}$, then we are done: just take $P(X_1, X_2) = \sum_{\substack{0 \le s < d \\ 0 \le t < d}} A_{\lceil \langle s,t \rangle \rceil} X_1^s X_2^t$ (where $\lceil \langle s,t \rangle \rceil$ denotes the i such that $\theta_i(x) = \phi(x)^s \psi(x)^t$). In fact, we shall choose the A_i's so that $|G(\beta)| < \frac{1}{H^{2d-2}}$ for *all* $\beta \in (0,1)$ with $|\beta - \alpha| < H^{-20/d}$. To do this, we apply Taylor's Theorem around α:

$$G(x) = \sum_{i=1}^{d^2} A_i \left(\sum_{j=0}^{p-1} \frac{\theta_i^{(j)}(\alpha)}{j!} \cdot (x-\alpha)^j + \frac{\theta_i^{(p)}(\xi_x^i)}{p!} (x-\alpha)^p \right) \qquad (*)$$

for some ξ_x^i's lying between α and x.

6.6 Exercise

Check that $|\theta_i^{(j)}| \le (2d-2)^j$ on $(0,1)$ for $j = 1, \ldots, p$ and for $i = 1, \ldots, d^2$.

We first bound the remainder term in $(*)$:

$$\left| \sum_{i=1}^{d^2} A_i \frac{\theta_i^{(p)}(\xi_x^i)}{p!} (x-\alpha)^p \right|.$$

If $|x - \alpha| < H^{-20/d}$, then using 6.6 and the bound $|A_i| \le H^d$, we see that it is at most

$$d^2 \cdot H^d \cdot (2d-2)^p \cdot H^{-20p/d}.$$

Since $4p \le d^2 \le 5p$, this is bounded by

$$\begin{aligned} & d^2 \cdot (2d-2)^{d^2/4} \cdot H^{-3d} \\ =& \frac{d^2 \cdot (2d-2)^{d^2/4}}{H^{d+2}} \cdot \frac{1}{H^{2d-2}} \\ \le& \left(\frac{2 \cdot (2d-2)^{d/4}}{H} \right)^d \cdot \frac{1}{H^{2d-2}} \\ <& \tfrac{1}{2 \cdot H^{2d-2}}. \end{aligned}$$

We shall be done if we can choose the A_i's so that the main term in $(*)$ has the same bound. By interchanging the order of summation in $(*)$ we see that this main term is

$$\left|\sum_{j=0}^{p-1}(x-\alpha)^j\left(\sum_{i=1}^{d^2}A_i\cdot\frac{\theta_i^{(j)}(\alpha)}{j!}\right)\right| \qquad (**)$$

This suggests applying 6.4 with $\nu=d^2, \mu=p-1, v_{i,j}=\frac{\theta_i^{(j)}(\alpha)}{j!}, \ell=H^{4d}, X=H^d$, and $u=d^2\cdot e^{2d-2}$, which is justified since (by 6.6)

$$\max_{0\le j\le\mu}\sum_{i=1}^{\nu}|v_{i,j}|\le\max_{0\le j\le p-1}\sum_{i=1}^{d^2}\frac{(2d-2)^j}{j!}\le d^2\cdot e^{2d-2}$$

and

$$\ell^p=H^{4dp}\le H^{d^3}\le(H^d+1)^{d^2}=(X+1)^{\nu},$$

so 6.4(1), (2) both hold.

So we may indeed find integers A_i (for $1\le i\le d^2$) satisfying $\max_{1\le i\le d^2}|A_i|\le H^d$ and

$$\max_{0\le j\le\mu}\left|\sum_{i=1}^{d^2}A_i\cdot\frac{\theta_i^{(j)}(\alpha)}{j!}\right|\le\frac{uX}{\ell}=\frac{d^2\cdot e^{2d-2}}{H^{3d}}\le\frac{(2e^2)^d}{H^{3d}}.$$

With this choice of the A_i's, it follows (upon using the trivial estimate $|(x-\alpha)^j|<1$) that the main term $(**)$ is bounded (for any $x\in(0,1)$) by

$$p\cdot\frac{(2e^2)^d}{H^{3d}}\le\left(\frac{4e^2}{H}\right)^d\cdot\frac{1}{2H^{2d-2}}<\frac{1}{2\cdot H^{2d-2}},$$

as required. $\square$

The first stage in the proof of 6.1 involves reducing the problem to the situation of 6.3. So let $\epsilon>0$ be given. Let d be an integer such that $d\ge 10$ and $\frac{20}{d}<\frac{\epsilon}{2}$. Then we may choose an integer p such that $100\le 4p\le d^2\le 5p$. Let $f:(0,1)\to(0,1)$ be as in the hypotheses of 6.1. For $H>4\cdot(2d-2)^{d/4}$ define

$$S_H:=\{\langle q_1,q_2\rangle\in\mathbb{Q}^2: f(q_1)=q_2 \text{ and } \mathrm{ht}(\langle q_1,q_2\rangle)\le H\}$$

and assume, for a contradiction, that $|S_H|\ge H^{\epsilon}$ for infinitely many H.

Now apply 5.11 (with $n=1$) and let $c_\epsilon=|\Phi|^{-1}$. [Note that f is now fixed and so d and p, and hence $|\Phi|$, depend only on ϵ. This is also true for f rangings over some fixed definable famliy of functions.] Then by the Pigeon Hole Principle, there is some fixed $\phi\in\Phi$ such that

$$|S_H\cap\{\langle\phi(\beta),f(\phi(\beta))\rangle:\beta\in(0,1)\}|\ge c_\epsilon H^{\epsilon}$$

for infinitely many H.

By subdividing $(0,1)$ into $1+\left[\frac{H^{20/d}}{2}\right]$ intervals of length at most $2\cdot H^{-20/d}$, it follows, again by the Pigeon Hole Principle, that there is some $\alpha_H\in(0,1)$ such that, setting

$$Y_H:=S_H\cap\{\langle\phi(\beta),f(\phi(\beta))\rangle:\beta\in(0,1)\text{ and }|\alpha_H-\beta|<H^{-20/d}\}$$

we have

$$|Y_H| \geq \frac{c_\epsilon \cdot H^\epsilon}{1 + \left[\frac{H^{20/d}}{2}\right]} \geq c_\epsilon \cdot H^{\epsilon - 20/d} > c_\epsilon \cdot H^{\epsilon/2} \qquad (***)$$

for infinitely many H.

This completes stage one.

We now apply 6.3 (with $\psi = f \circ \phi$) to obtain a polynomial $P_H(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ (though real coefficients actually suffice here) of degree at most $d-1$ in each variable, which vanishes on Y_H.

Now stage three, the final contradiction, involves what is known as "a zero estimate" in transcendental number theory. One requires an upper bound on the number of zeros of the function

$$\sum_{0 \leq s,t < d} A_{\lceil \langle s,t \rangle \rceil} \cdot y^s \cdot f(y)^t$$

which depends only on d (and not on the coefficients). Usually one has much more information about the function f and good bounds (using complex analysis, say, if f is known to have an entire analytic continuation) may be found, giving rise to much sharper bounds in place of H^ϵ in our main theorem here. However, for our purposes we only need to know that *some* such bound exists, N_d say. For then we have our contradiction to the inequality $(***)$ simply by choosing $H > \left(\frac{N_d}{c_\epsilon}\right)^{2/\epsilon}$ (and H satisfying $(***)$).

The existence of N_d follows from our discussion in 4.3 (see also 4.4.1(a)). Just consider the definable family

$$\mathcal{F} := \{\{y : \sum_{0 \leq s,t < d} x_{s,t} \cdot y^s \cdot f(y)^t = 0\} : x_{s,t} \in \mathbb{R} \text{ for } 0 \leq s,t < d\}$$

of subsets of $\mathbb{R}$. We choose N_d greater than the number of connected components of any member of $\mathcal{F}$ and observe, via 6.2(1), that such components are, in fact, singleton sets. □

7 Some remarks on the proof of the general case of 1.1

7.1

One requires some deeper o-minimality theory. In particular, we require a generalization of 5.11 for definable functions $F : (0,1)^n \to (0,1)$, and also a result telling us that in order to prove 1.1, it is sufficient to consider the case that S is the graph of such a function.

The first and second stages of the argument discussed in section 6 may now be generalized in a routine manner: under the assumption that graph(F) contains more than H^ϵ rational $(n+1)$-tuples of height $\leq H$, we end up with a polynomial $P_H(X_1, \ldots, X_n, X_{n+1})$ (with integer coefficients) of degree depending only on ϵ, such that at least H^{ϵ^r} (say) of these points lie in the set $Z(P_H) \cap$ graph(F), where r is a sufficiently large positive integer depending on n.

7.2

The third stage, however, requires an inductive argument for which we require a good notion of dimension for definable sets. The proof is then completed as follows.

If, for some sufficiently large H as above, $\dim(Z(P_H) \cap \mathrm{graph}(F)) = \dim(\mathrm{graph}(f))\ (= n)$, then it is easily shown that for some sufficiently small open box in $(0,1)^{n+1}$, Δ_H say,

$\dim(\Delta_H \cap Z(P_H)) = n$ and $\Delta_H \cap Z(P_H) = \Delta_H \cap \text{graph}(F)$. Thus, graph$(F)$ contains the infinite semi-algebraic set $\Delta_H \cap Z(P_H)$, contrary to our assumptions.

Thus, we may assume that there are infinitely many H such that $Z(P_H) \cap \text{graph}(F)$ contains at least H^{ϵ^r} rational points of height $\leq H$ *and* such that $\dim(Z(P_H) \cap \text{graph}(F)) < \dim(\text{graph}(F))$. It might now appear that, by the obvious inductive argument, we have reached the desired contradiction. However, the inductive hypothesis is being applied to a set, $Z(P_H) \cap \text{graph}(F)$, whose definition depends on H, which is not exactly how theorem 1.1 is stated. But, as I have been emphasizing throughout these notes, all our arguments have been uniform over definable families and, indeed, all the sets $Z(P_H) \cap \text{graph}(F)$ do lie in one fixed family (depending on ϵ, but not on H). So the correct formulation of 1.1 is as follows:

7.3 A uniform version of Theorem 1.1

Let $\{S_{\bar{x}} : \bar{x} \in \mathbb{R}^k\}$ be a definable family of subsets of $\mathbb{R}^n$. Then for each $\epsilon > 0$ there exists an integer $D_\epsilon > 0$ such that for all $\bar{x} \in \mathbb{R}^k$ and all $H \geq D_\epsilon$,

either $(1)_{\bar{x}}$ $S_{\bar{x}}$ contains an infinite semi-algebraic subset

or $(2)_{\bar{x}}$ $S_{\bar{x}}$ contains at most H^ϵ rational points of height at most H.

Further, which of cases $(1)_{\bar{x}}, (2)_{\bar{x}}$ holds depends definably on $\bar{x}$, and in case $(1)_{\bar{x}}$, the infinite semi-algebraic subset may be chosen to depend definably on $\bar{x}$.

7.4 Exercise

Check that our proof in section 6 does in fact establish 7.3 in the case that each $S_{\bar{x}}$ is 1-dimensional.

7.5 The transcendental part of a set

The other lectures in this course will probably need a slightly different formulation of 1.1.

7.6 Definition

For $S \subseteq \mathbb{R}^n$, S^{alg} denotes the union of all infinite, connected, semi-algebraic subsets of S. We also define $S^{\text{trans}} := S \setminus S^{\text{alg}}$.

Our methods also give the following version of 1.1.

7.7 Theorem

Let $S \subseteq \mathbb{R}^n$ be a set definable in some o-minimal expansion of the ordered field of real numbers. Let $\epsilon > 0$. Then for all sufficiently large H, S^{trans} contains at most H^ϵ rational points of height at most H.

In order to complete our discussion of the proof of 1.1 it now only remains for me to indicate the argument that establishes the general case of the reparameterization theorem.

8 Some higher-dimensional o-minimal theory

This is based on the notions of cell and cell decomposition. We treat only bounded cells here. All definability is with respect to a fixed o-minimal expansion of the real field.

8.1 Definition

For $n \geq 1$ and $n \geq m \geq 0$ we define the notion of an m-dimensional cell in $\mathbb{R}^n$ inductively as follows:

(1) (i) A 0-dimensional cell in $\mathbb{R}$ is a singleton set $\{a\}$ (for $a \in \mathbb{R}$).
  (ii) A 1-dimensional cell in $\mathbb{R}$ is an open interval (a, b) (for $a, b \in \mathbb{R}, a < b$).

(2) For $n \geq 2$, an $(m+1)$-dimensional cell in $\mathbb{R}^n$ has one of the following forms:

  (i) graph(f), where $f : C \to \mathbb{R}$ is a definable, bounded, continuous function and C is an $(m+1)$-dimensional cell in $\mathbb{R}^{n-1}$, or
  (ii) $(f, g)_C := \{\langle \bar{x}, y\rangle \in \mathbb{R}^n : \bar{x} \in C \text{ and } f(\bar{x}) < y < g(\bar{x})\}$, where $f, g : C \to \mathbb{R}$ are definable, bounded, continuous functions with $f(\bar{x}) < g(\bar{x})$ (for all $\bar{x} \in C$) and C is an m-dimensional cell in $\mathbb{R}^{n-1}$.

8.2 Definition

(1) A finite collection, $\mathcal{C}$ say, of cells in $\mathbb{R}^n$ (of various dimensions) is called a *cell-decomposition of* $(0, 1)^n$ if it partitions $(0, 1)^n$ and, in the case that $n > 1$, the collection $\{\pi^n_{n-1}[C] : C \in \mathcal{C}\}$ is a cell-decomposition of $(0, 1)^{n-1}$.

(2) A cell-decomposition $\mathcal{C}$ of $(0, 1)^n$ is called *compatible* with a set $B \subset (0, 1)^n$ if B is the union of a subcollection of $\mathcal{C}$ (i.e. for all $C \in \mathcal{C}$, either $C \subseteq B$ or $C \cap B = \emptyset$).

The main foundational result of the subject, due to Pillay and Steinhorn (see [PS] or [vdD]), is the following:

8.3 Theorem (The Cell Decomposition Theorem)

Suppose that $B_1, \ldots, B_k$ are definable subsets of $(0, 1)^n$. Then there exists a cell-decomposition of $(0, 1)^n$ that is compatible with each B_i (for $i = 1, \ldots, k$).

8.4 Definition

The *dimension* of a definable set $B \subseteq (0, 1)^n$ is defined to be the largest m such that B contains an m-dimensional cell in $\mathbb{R}^n$.

8.5 Exercises

(1) Prove by induction that an m-dimensional cell in $\mathbb{R}^n$ is definably homeomorphic to $(0, 1)^m$.

(2) Prove that an m-dimensional cell in $\mathbb{R}^n$ is open if and only if $m = n$.

8.6

One now shows that this notion of dimension has good properties with respect to definable sets and definable functions. For example

$$\dim(A \cup B) = \max\{\dim(A), \dim(B)\}, \qquad \dim(A \times B) = \dim(A) + \dim(B)$$

$$dim(f[A]) \leq \dim(A), \qquad \dim(\bar{A}) = \dim(A), \qquad \dim(\bar{A} \setminus A) < \dim(A)$$

(where we set $\dim(\emptyset) := -1$).

8.7

Further, for any definable map $F : (0,1)^m \to \mathbb{R}^n$ and $p \geq 0$, there exists a cell decomposition $\mathcal{C}_p$ of $(0,1)^m$ such that F is C^p on each open cell in $\mathcal{C}_p$. In general, this is the best one can do: we cannot replace C^p by C^∞ here. However, in all the o-minimal structures of interest in this course (in particular, for $\mathcal{A}^{\text{an, exp}}$) one can replace C^p by C^ω (i.e. real-analytic).

8.8

There is one further result that we need for the next section, namely the *Principle of Definable Choice*. This states that if $S \subseteq \mathbb{R}^{n+m}$ is any definable set, then there exists a definable function $g : \mathbb{R}^n \to \mathbb{R}^m$ such that for all $\bar{x} \in \mathbb{R}^n$, if there exists $\bar{y} \in \mathbb{R}^m$ such that $\langle \bar{x}, \bar{y} \rangle \in S$, then $\langle \bar{x}, f(\bar{x}) \rangle \in S$.

9 Reparameterization (many variable case)

I conclue these notes with a brief sketch of the proof of the following:

9.1 Theorem (The C^p-m-reparameterizaiton theorem)

Let $F : (0,1)^m \to (0,1)^n$ be any definable map. Then for any $p \geq 1$, there exists a finite set Φ of C^p maps mapping $(0,1)^m$ to $(0,1)^m$, such that $\bigcup_{\phi \in \Phi} \operatorname{Im}(\phi) = (0,1)^m$ and such that for each $\phi \in \Phi$ and $\alpha \in \mathbb{N}^m$ with $|\alpha| \leq p$, we have that both $\|\phi^{(\alpha)}\|_m$ and $\|(F \circ \phi)^{(\alpha)}\|_n$ are bounded by 1 on $(0,1)^m$. (Further, $|\Phi|$ depends only on p and uniformly on F, as do the functions in Φ.)

9.2 Remarks

(1) $\|\cdot\|_k : \mathbb{R}^k \to \mathbb{R}$ denotes the sup norm, $\|\langle x_1, \ldots, x_k \rangle\|_k := \max\{|x_1|, \ldots, |x_k|\}$, on $\mathbb{R}^k$.

(2) We are using the usual multi-index notation: for $\alpha = \langle \alpha_1, \ldots, \alpha_m \rangle \in \mathbb{N}^m$, $|\alpha| := \alpha_1 + \cdots + \alpha_m$ and, for a $C^{|\alpha|}$ map $f : (0,1)^m \to (0,1)^\ell$, $f^{(\alpha)} := \frac{\partial^{(\alpha)} f}{\partial x_1^{\alpha_1} \cdots \partial x_m^{\alpha_m}}$.

9.3

The reparameterization theorem is due, at least in the semi-algebraic case, to Yomdin and Gromov (see [Gr]). However, the inductive part of the argument, which I now sketch, is due entirely to Yomdin, and once one has the basics of o-minimality in place (section 8), one has to change very little in generalizing his argument from the semi-algebraic to the o-minimal case.

Firstly (exercise), it follows quite easily by induction (using 8.7 and a C^p version of 8.5(1)) that one may assume that F (in 9.1) is already C^p on $(0,1)^m$. The problem is to bound the derivatives. We may assume that $m \geq 2$ (by 5.11). Let $k \geq 0$.

Now assume that $\Phi = \Phi_k$ has been found to satisfy the conclusion of 9.1 except that this conclusion is weakened from "for all $\alpha \in \mathbb{N}^m$ with $|\alpha| \leq p$" to

$$\text{"for all } \alpha \in \mathbb{N}^m \text{ with } |\alpha| \leq p \text{ and } \alpha_m \leq k\text{"} \qquad (*)_k$$

We complete the proof by showing how to construct Φ_{k+1} to satisfy $(*)_{k+1}$. (The case $k = 0$ is dealt with by using a subsidiary induction on m. This involves a standard use of uniformity (relegating the variable x_m to parameter status) and is quite routine.) To this end we consider the map $\tilde{F} : (0,1)^m \to (0,1)^{\tilde{n}}$, where $\tilde{n} = |\Phi_k|(|\Delta| \cdot n + m)$ and where

$$\Delta := \{\alpha = \langle \alpha_1, \ldots, \alpha_m \rangle \in \mathbb{N}^m : |\alpha| \le p-1, |\alpha_m| \le k\}.$$

The map $\tilde{F}$ then takes $\bar{x} \in (0,1)^m$ to an enumeration of the values $(F \circ \phi)^{(\alpha)}$ for $\alpha \in \Delta$ and $\phi \in \Phi_k$ as well as $\phi(\bar{x})$ for $\phi \in \Phi_k$. Notice that $\tilde{F}$ is a C^1 map and (because of the condition "$|\alpha| \le p-1$" in the definition of Δ) that $\|\frac{\partial \tilde{F}}{\partial x_i}(\bar{a})\|_{\tilde{n}} \le 1$ for each $i = 1, \ldots, m-1$ and $\bar{a} \in (0,1)^m$. The required construction of Φ_{k+1} is now easily obtained from the

<u>Main Lemma</u>

Let $G : (0,1)^m \to (0,1)^\ell$ be a definable C^1 map and suppose that $\|\frac{\partial G}{\partial x_i}\|_\ell \le 1$ on $(0,1)^m$ for $i = 1, \ldots, m-1$. Then for any $p \ge 0$, there exists a finite set Φ of C^p functions $\phi : (0,1) \to (0,1)$ with $\bigcup_{\phi \in \Phi} \mathrm{Im}(\phi) = (0,1)$ such that for each $\phi \in \Phi$ and $j = 0, \ldots, p$, $|\phi^{(j)}| \le 1$ on $(0,1)$ and for each $i = 1, \ldots, m$, $\|\frac{\partial}{\partial x_i}(G \circ \tilde{\phi})\|_\ell \le 1$ on $(0,1)^m$, where $\tilde{\phi} : (0,1)^m \to (0,1)^m : \langle x_1, \ldots, x_m \rangle \mapsto \langle x_1, \ldots, x_{m-1}, \phi(x_m) \rangle$.

<u>Proof sketch</u>

I give the proof in the case that $\frac{\partial G}{\partial x_m}$ is bounded. (The general case follows by considering the restriction of G to the set $(\eta, 1-\eta)^m$ and then letting $\eta \to 0$. The limiting process is quite routine as the set Φ may be constructed uniformly in η. One also uses 4.1 here.)

So, for each $x_m \in (0,1)$ we consider a point $\theta(x_m) = \langle \theta_1(x_m), \ldots, \theta_{m-1}(x_m) \rangle \in (0,1)^{m-1}$ such that

$$\|\frac{\partial G}{\partial x_m}(\theta(x_m), x_m)\|_\ell \ge \frac{1}{2} \sup \left\{ \|\frac{\partial G}{\partial x_m}(x', x_m)\|_\ell : x' \in (0,1)^{m-1} \right\} \qquad (*)$$

By Definable Choice (8.8) we may suppose that $\theta : (0,1) \to (0,1)^{m-1}$ is definable. Apply 5.11 to the map $H : (0,1) \to (0,1)^{m-1+\ell}$ given by $y \mapsto \langle \theta(y), G(\theta(y), y) \rangle$. I claim that the finite set Φ of functions provided by 5.11 also (nearly) works here as well. For let $\phi \in \Phi$. We must show that

$$\|\frac{\partial (G \circ \tilde{\phi})}{\partial x_m}(a', a_m)\|_\ell \le 1 \qquad \text{for all } \langle a', a_m \rangle \in (0,1)^m,$$

the other bounds being straightforward.

Now, the conclusion of 5.11 tells us, in particular, that the derivative of the map $y \mapsto G(\theta(\phi(y)), \phi(y))$ is bounded by 1 on $(0,1)$, as is the derivative of the map $\theta \circ \phi$. Thus, for each $b \in (0,1)$,

$$\begin{aligned} 1 &\ge \|\sum_{i=1}^{m-1} \frac{\partial G}{\partial x_i}(\theta(\phi(b)), \phi(b)) \cdot (\theta_i \circ \phi)'(b) + \frac{\partial G}{\partial x_m}(\theta(\phi(b)), \phi(b)) \cdot \phi'(b)\|_\ell \\ &\ge \|\frac{\partial G}{\partial x_m}(\theta(\phi(b)), \phi(b)) \cdot \phi'(b)\|_\ell - \|\sum_{i=1}^{m-1} \frac{\partial G}{\partial x_i}(\theta(\phi(b)), \phi(b)) \cdot (\theta_i \circ \phi)'(b)\|_\ell \\ &\ge \|\frac{\partial G}{\partial x_m}(\theta(\phi(b)), \phi(b)) \cdot \phi'(b)\|_\ell - (m-1). \end{aligned}$$

(The last inequality follows from the above together with the Lemma hypothesis on $\frac{\partial G}{\partial x_i}$ for $i = 1, \ldots, m-1$.)

Now let $\langle a', a_m\rangle \in (0,1)^m$. Then

$$\begin{aligned} m &\geq \left\| \frac{\partial G}{\partial x_m}(\theta(\phi(a_m)), \phi(a_m)) \cdot \phi'(a_m) \right\|_\ell \\ &\geq \frac{1}{2} \cdot \left\| \frac{\partial G}{\partial x_m}(a', \phi(a_m)) \cdot \phi'(a_m) \right\|_\ell && \text{(by } (*)) \\ &= \frac{1}{2} \cdot \left\| \frac{\partial (G \circ \tilde{\phi})}{\partial x_m}(a', a_m) \right\|_\ell \end{aligned}$$

This gives the bound $2m$ instead of the required 1. However, just as in 5.11 (see the first paragraph of the proof there), this can be easily dealt with by a suitable linear substitution. □

References

[B] Butler, Lee A., "Some cases of Wilkie's conjecture", Bull. London Math. Soc., Vol. 44, No. 4, 2012, pp. 642-660.

[vdD] van den Dries, L., "Tame topology and o-minimal structures", LMS Lecture Notes Series 248, CUP, 1998.

[DD] Denef, J. and van den Dries, L., "p-adic and real subanalytic sets", Annals of Mathematics (2nd series) 128, 1988, pp. 80-138.

[DM] van den Dries, L. and Miller, C., "On the real exponential field with restricted analytic functions", Israel J. of Math., 85, 1994, pp. 19-56.

[G] Gabrielov, A., "Projections of semianalytic sets", Funct. Anal. Appl., 2, 1968, pp. 282-291.

[Gr] Gromov, M., "Entropy, homology and semialgebraic geometry", Astérisque 145-146, 1987, pp. 225-250.

[JT] Jones, G. O. and Thomas, M. E. M., "The density of algebraic points on certain Pfaffian surfaces", Q. J. Math., 63, 2012, pp. 637-651.

[Mi] Miller, C., "Exponentiation is hard to avoid", Proc. AMS, 122, No. 1, 1994, pp. 257-259.

[PS] Pillay, A. and Steinhorn, C., "Definable sets and ordered structures I", Trans. AMS, 295, 1986, pp. 565-592.

[PW] Pila, J. and Wilkie, A. J., "The rational points of a definable set", Duke Math. J., 133, No. 3, 2006, pp. 591-616.

[RSW] Rolin, J-P., Speisegger, P. and Wilkie, A. J., "Quasianalytic Denjoy-Carleman classes and o-minimality", J. AMS, 16, 2003, pp. 751-777.

[W] Wilkie, A. J., "Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function", J. AMS, 9, 1996, pp. 1051-1094.

[Wa] Waldschmidt, M., "Diophantine approximation on linear algebraic groups", Grund. Math. Wiss., 326, Springer, 2000.