AN INTRODUCTION TO SEMIALGEBRAIC GEOMETRY

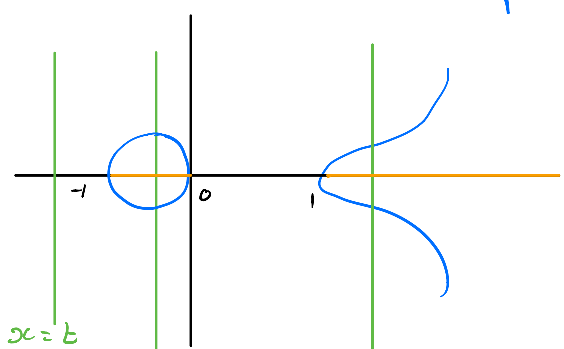
Michel COSTE
Institut de Recherche Mathématique de Rennes
michel.coste@univ-rennes1.fr

Octobre 2002

SEMI-ALGEBRAIC AND REAL ALGEBRAIC SETS

- $\mathbb{R}$ is an ordered field:
  - if $P \in \mathbb{R}[X_1, \dots, X_n]$, "$P > 0$" $= \{x \in \mathbb{R}^n : P(x) > 0\}$ makes sense too!
- $\mathbb{R}$ is not algebraically closed:
  - some varieties may be empty: $x^2+1=0$
  - irreducible varieties may have several connected components

Example: $\mathcal{C} : y^2 = x^3 - x$
$= x(x^2-1)$



Intersection of $\mathcal{C}$ with lines $x = t$ (when not tangent)

- 0 or 2 points ($\mathbb{R}$ not alg. closed)
- number of intersecting points is even (related to complex conjugation)
- set where the intersection is not empty: union of intervals (related to the order).

↳ Euclidean topology will play a role too.

1. REAL ALGEBRAIC SETS

Definition A subset $V \subseteq \mathbb{R}^n$ is a real algebraic set if

$\exists B \subseteq \mathbb{R}[X_1, \dots, X_n]$, $\quad V = Z(B) := \{x \in \mathbb{R}^n : \forall P \in B, P(x) = 0\}$

Notation Let $S \subseteq \mathbb{R}^n$ be a subset. Then

$$I(S) = \{P \in \mathbb{R}[X_1, \dots, X_n] : \forall x \in S, \; P(x) = 0\}$$

Example: $B = \{x^2 + y^2\}$

$$I(Z(B)) = (x, y) \neq \sqrt{(x^2 + y^2)}$$

irreducible polynomial

$\rightsquigarrow$ Nullstellensatz not valid.

Proposition Let $V \subseteq \mathbb{R}^n$ be an algebraic set. There exists $P \in \mathbb{R}[X_1, \dots, X_n]$ such that $V = Z(P)$.

Proof: . It is still true that $V = Z(I(V))$

. $I(V) = (P_1, \dots, P_k)$ because $\mathbb{R}[\underline{X}]$ is Noetherian

. $P = P_1^2 + \dots + P_k^2$ is convenient.

$\square$

A fact in complex algebraic geometry:

. Let $V \subseteq \mathbb{C}^n$ be given by $P_1 = \dots = P_k = 0$, $P_i \in \mathbb{C}[X_1, \dots, X_n]$

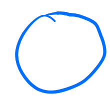
. View $V \subseteq \mathbb{R}^{2n}$ via $\begin{cases} \mathrm{Re}\, P_i = 0 \\ \mathrm{Im}\, P_i = 0 \end{cases}$

Theorem Assume V irreducible of complex dimension d.

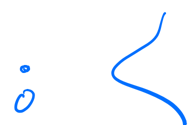
Then:
- V is connected
- V is not bounded
- $\forall x \in V$, $\dim V_x = 2d$

Some examples of real algebraic sets:

- $\{x^2 + y^2 = 1\} \subseteq \mathbb{R}^2$: a circle bounded!



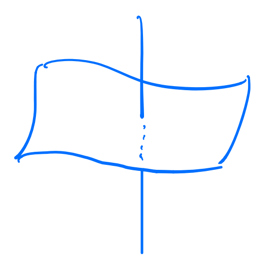
- $y^2 = x^2(x-1)$ a singular cubic
  - not connected
  - dimension at 0 is 0



- $y^2 = x(x^2-1)$ a nonsingular cubic

not connected

- $z(x^2+y^2) = x^3$ Cartan umbrella

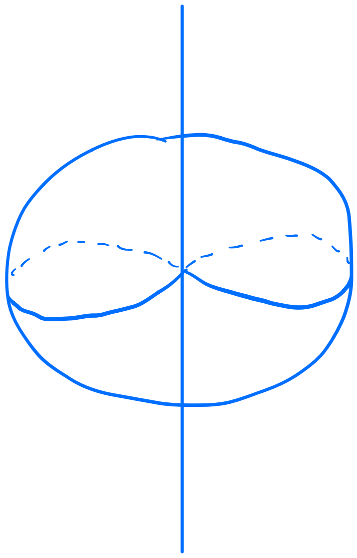


Irreducible, but the local dimension changes.

$\cdot\ x^2(1-z^2) = x^4+y^2$

I dem.

compactified Whitney umbrella



2. Semialgebraic sets

2.1 Stability properties of the class of semialgebraic sets

2.1.1 Definition and first examples

A *semialgebraic subset* of $\mathbb{R}^n$ is the subset of $(x_1, \ldots, x_n)$ in $\mathbb{R}^n$ satisfying a boolean combination of polynomial equations and inequalities with real coefficients. In other words, the semialgebraic subsets of $\mathbb{R}^n$ form the smallest class $\mathcal{SA}_n$ of subsets of $\mathbb{R}^n$ such that:

1. If $P \in \mathbb{R}[X_1, \ldots, X_n]$, then $\{x \in \mathbb{R}^n \ ; \ P(x) = 0\} \in \mathcal{SA}_n$ and $\{x \in \mathbb{R}^n \ ; \ P(x) > 0\} \in \mathcal{SA}_n$.

2. If $A \in \mathcal{SA}_n$ and $B \in \mathcal{SA}_n$, then $A \cup B$, $A \cap B$ and $\mathbb{R}^n \setminus A$ are in $\mathcal{SA}_n$.

Example ($n=1$) : finite union of points and intervals.

Proposition 2.1 *Every semialgebraic subset of $\mathbb{R}^n$ is the union of finitely many semialgebraic subsets of the form*

$$\{x \in \mathbb{R}^n \ ; \ P(x) = 0 \ \text{ and } \ Q_1(x) > 0 \ \text{ and } \ \ldots \ \text{ and } \ Q_\ell(x) > 0\} \ ,$$

where $\ell \in \mathbb{N}$ and $P, Q_1, \ldots, Q_\ell \in \mathbb{R}[X_1, \ldots, X_n]$.

"ensemble semi-algébrique basique"

Examples

- The semialgebraic subsets of $\mathbb{R}$ are the unions of finitely many points and open intervals.

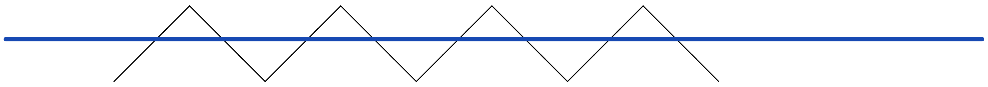
- An algebraic subset of $\mathbb{R}^n$ (defined by polynomial equations) is semialgebraic.

- Let $F : \mathbb{R}^m \to \mathbb{R}^n$ be a polynomial mapping: $F = (F_1, \ldots, F_n)$, where $F_i \in \mathbb{R}[X_1, \ldots, X_n]$. Let A be a semialgebraic subset of $\mathbb{R}^n$. Then $F^{-1}(A)$ is a semialgebraic subset of $\mathbb{R}^m$.

- If A is a semialgebraic subset of $\mathbb{R}^n$ and $L \subset \mathbb{R}^n$ a line, then $L \cap A$ is the union of finitely many points and open intervals.

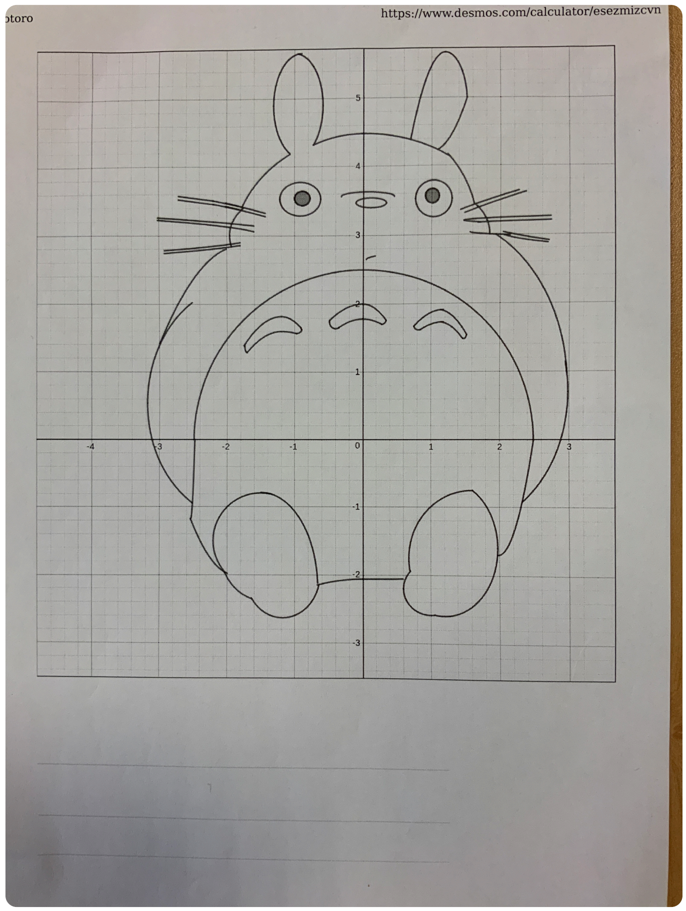
- If $A \subset \mathbb{R}^m$ and $B \subset \mathbb{R}^n$ are semialgebraic, $A \times B$ is a semialgebraic subset of $\mathbb{R}^m \times \mathbb{R}^n$.

Counter-example: the infinite zigzag



is not semialgebraic (proof later)

<u>Another escample:</u>



(equations on www.desmos.com)

The following result is extremely important in semi-algebraic geometry.

"Elimination of quantifiers"

Theorem 1.9 (Tarski-Seidenberg – first form) *There exists an algorithm which, given a system of polynomial equations and inequalities in the variables $T = (T_1, \ldots, T_p)$ and X with coefficients in $\mathbb{R}$*

$$\mathcal{S}(T,X) \ : \quad \begin{cases} S_1(T,X) \rhd_1 0 \\ S_2(T,X) \rhd_2 0 \\ \cdots \\ S_\ell(T,X) \rhd_\ell 0 \end{cases}$$

(where the $\rhd_i$ are either $=$ or $\neq$ or $>$ or $\geq$), produces a finite list $\mathcal{C}_1(T)$, $\ldots$, $\mathcal{C}_k(T)$ of systems of polynomial equations and inequalities in T with coefficients in $\mathbb{R}$ such that, for every $t \in \mathbb{R}^p$, the system $\mathcal{S}(t,X)$ has a real solution if and only if one of the $\mathcal{C}_j(t)$ is satisfied.

Proof: accepted □

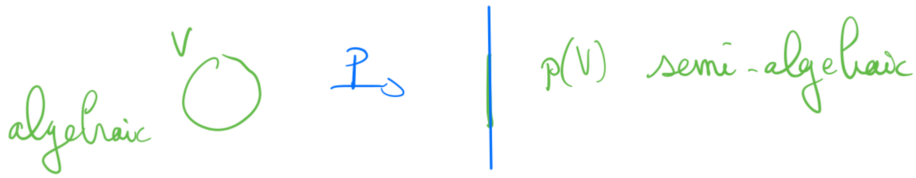
In other words, the formula "$\exists X \ \mathcal{S}(T,X)$" is equivalent to the disjunction "$\mathcal{C}_1(T)$ or $\ldots$ or $\mathcal{C}_k(T)$". The Tarski-Seidenberg theorem means that there is an algorithm for eliminating the real variable X. A well known example of elimination of a real variable is

$$\begin{aligned} &\exists X \ AX^2 + BX + C = 0 \quad \Leftrightarrow \\ &(A \neq 0 \text{ and } B^2 - 4AC \geq 0) \text{ or } (A = 0 \text{ and } B \neq 0) \text{ or } (A = B = C = 0)\,. \end{aligned}$$

Here $T = (A,B,C)$

2.1.2 Consequences of Tarski-Seidenberg principle

We have seen that the class of all semialgebraic subsets is closed under finite unions and intersections, taking complement, inverse image by a polynomial mapping, cartesian product. It is also closed under projection.



Theorem 2.3 (Tarski-Seidenberg – second form) *Let A be a semialgebraic subset of $\mathbb{R}^{n+1}$ and $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$, the projection on the first n coordinates. Then $\pi(A)$ is a semialgebraic subset of $\mathbb{R}^n$.*

Proof. Since A is the union of finitely many subsets of the form

$$\{x = (x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1} \ ; \ P(x) = 0, \ Q_1(x) > 0, \ldots, \ Q_k(x) > 0\} ,$$

we may assume that A itself is of this form. It follows from the Tarski-Seidenberg theorem (first form, 1.9) that there is a boolean combination $\mathcal{C}(X_1, \ldots, X_n)$ of polynomial equations and inequalities in $X_1, \ldots, X_n$ such that

$$\pi(A) = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \ ; \ \exists x_{n+1} \in \mathbb{R} \ (x_1, \ldots, x_n, x_{n+1}) \in A\}$$

is the set of $(x_1, \ldots, x_n)$ which satisfy $\mathcal{C}(x_1, \ldots, x_n)$. This means that $\pi(A)$ is semialgebraic. □

Remark Over $\mathbb{C}$, it will be a Zariski constructible set by Chevalley Theorem.

We now show some consequences of the Tarski-Seidenberg theorem.

Corollary 2.4 *1. If A is a semialgebraic subset of $\mathbb{R}^{n+k}$, its image by the projection on the space of the first n coordinates is a semialgebraic subset of $\mathbb{R}^n$.*

2. If A is a semialgebraic subset of $\mathbb{R}^m$ and $F : \mathbb{R}^m \to \mathbb{R}^n$, a polynomial mapping, then the direct image $F(A)$ is a semialgebraic subset of $\mathbb{R}^n$.

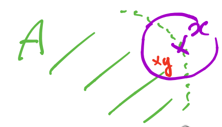
Proof. The first statement is easily obtained by induction on k. For the second statement, note that

$$\mathrm{Graph}\,F_{|A} = \{(x,y) \in \mathbb{R}^m \times \mathbb{R}^n \ ; \ x \in A \ \text{ and } \ y = F(x)\}$$

is a semialgebraic subset of $\mathbb{R}^m \times \mathbb{R}^n$ and that $F(A)$ is its projection onto $\mathbb{R}^n$.

□

Corollary 2.5 *If A is a semialgebraic subset of $\mathbb{R}^n$, its closure in $\mathbb{R}^n$ is again semialgebraic.*



Proof. The closure of A is

$$\mathrm{clos}(A) = \left\{x \in \mathbb{R}^n \ ; \ \forall \varepsilon \in \mathbb{R}, \ \varepsilon > 0 \Rightarrow \exists y \in \mathbb{R}^n, \ y \in A \ \text{ and } \ \|x-y\|^2 < \varepsilon^2\right\}$$

and can be written as

$$\mathrm{clos}(A) = \mathbb{R}^n \setminus \left(\pi_1\left(\{(x,\varepsilon) \in \mathbb{R}^n \times \mathbb{R} \ ; \ \varepsilon > 0\} \setminus \pi_2(B)\right)\right) \ ,$$

where

$$B = \left\{(x,\varepsilon,y) \in \mathbb{R}^n \times \mathbb{R} \times \mathbb{R}^n \ ; \ y \in A \ \text{ and } \ \sum_{i=1}^{n}(x_i - y_i)^2 < \varepsilon^2)\right\} \ ,$$

$\pi_1(x,\varepsilon) = x$ and $\pi_2(x,\varepsilon,y) = (x,\varepsilon)$. Then observe that B is semialgebraic.

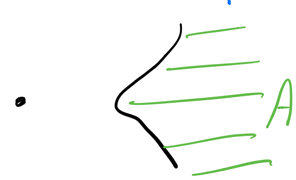
□

Remarks ① The same is true for the interior ...

② From A to $\mathrm{clos}\,A = \bar{A}$, it is not enough to relax inequalities.

example: $A = \{(x,y) \in \mathbb{R}^2 : y^2 < x^2(x-1)\}$

But $0 \notin \bar{A}$.



The example above shows that it is usually boring to write down projections in order to show that a subset is semialgebraic. We are more used to write down formulas. Let us make precise what is meant by a *first-order formula* (of the language of ordered fields with parameters in $\mathbb{R}$). A first-order formula is obtained by the following rules.

1. If $P \in \mathbb{R}[X_1, \ldots, X_n]$, then $P = 0$ and $P > 0$ are first-order formulas.
2. If Φ and Ψ are first-order formulas, then "Φ and Ψ", "Φ or Ψ", "not Φ" (often denoted by $\Phi \wedge \Psi$, $\Phi \vee \Psi$ and $\neg\Phi$, respectively) are first order formulas.
3. If Φ is a formula and X, a variable ranging over $\mathbb{R}$, then $\exists X \Phi$ and $\forall X \Phi$ are first-order formulas.

The formulas obtained by using only rules 1 and 2 are called *quantifier-free formulas*. By definition, a subset $A \subset \mathbb{R}^n$ is semialgebraic if and only if there is a quantifier-free formula $\Phi(X_1, \ldots, X_n)$ such that

$$(x_1, \ldots, x_n) \in A \Longleftrightarrow \Phi(x_1, \ldots, x_n).$$

The Tarski-Seidenberg theorem has the following useful formulation.

Theorem 2.6 (Tarski-Seidenberg – third form) *If $\Phi(X_1, \ldots, X_n)$ is a first-order formula, the set of $(x_1, \ldots, x_n) \in \mathbb{R}^n$ which satisfy $\Phi(x_1, \ldots, x_n)$ is semialgebraic.*

Proof. By induction on the construction of formulas. Rule 1 produces only semialgebraic sets. Rule 2 produces only semialgebrais sets from semialgebraic sets. For rule 3, if

$$\{(x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1} \; ; \; \Phi(x_1, \ldots, x_{n+1})\}$$

$\exists x_{n+1} \; \phi(x)$

is semialgebraic, then

$$\{(x_1, \ldots, x_n) \in \mathbb{R}^n \; ; \; \exists x_{n+1} \, \Phi(x_1, \ldots, x_{n+1})\}$$

is its projection onto $\mathbb{R}^n$ and, hence, it is also semialgebraic. The case of $\forall X \Phi$ follows by observing that $\forall X \Phi$ is equivalent to $\neg \exists X \neg \Phi$. $\square$

The preceding theorem can be formulated as follows.

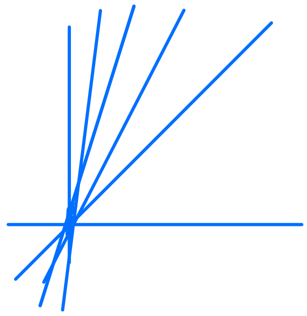
Every first-order formula is equivalent to a quantifier-free formula, or, in other words,

> $\mathbb{R}$ *admits the elimination of quantifiers in the language of ordered fields.*

Remark. One should pay attention to the fact that the quantified variables (or n-tuples of variables) have to range over $\mathbb{R}$, or $\mathbb{R}^n$, or possibly over a *semialgebraic* subset of $\mathbb{R}^n$. For instance,

$$\{(x,y) \in \mathbb{R}^2 \ ; \ \exists n \in \mathbb{N} \ y = nx\}$$

is not semialgebraic.



2.2 Semialgebraic functions

2.2.1 Definition and first properties

Let $A \subset \mathbb{R}^m$ and $B \subset \mathbb{R}^n$ be semialgebraic sets. A mapping $f : A \to B$ is said to be *semialgebraic* if its graph

$$\Gamma_f = \{(x,y) \in A \times B \ ; \ y = f(x)\}$$

is a semialgebraic subset of $\mathbb{R}^m \times \mathbb{R}^n$.

For instance:

- If $f : A \to B$ is a polynomial mapping (all its coordinates are polynomial), it is semialgebraic.
- If $f : A \to B$ is a regular rational mapping (all its coordinates are rational fractions whose denominators do not vanish on A), it is semialgebraic.

$f = \frac{P}{Q}$ avec $\forall a \in A$ $Q(a) \neq 0$

- If $f : A \to \mathbb{R}$ is a semialgebraic function, then $|f|$ is semialgebraic.
- If $f : A \to \mathbb{R}$ is semialgebraic and $f \geq 0$ on A, then $\sqrt{f}$ is a semialgebraic function.

Exemple **2.7** Let $A \subset \mathbb{R}^n$, $A \neq \emptyset$, be a semialgebraic set. Then the function

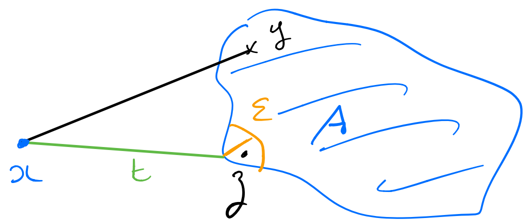
$$d(\cdot, A) : \begin{array}{ccc} \mathbb{R}^n & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \mathrm{dist}(x,A) = \inf\{\|x-y\| \ ; \ y \in A\} \end{array}$$

is continuous semialgebraic.

Actually the graph of $d(\cdot, A)$ is $\{(x,t) \in \mathbb{R}^{n+1} : t = d(x,A)\}$,

that is

$$\{(x,t) \in \mathbb{R}^{n+1} : t \geq 0 \wedge \left(\forall y \in A,\ \ t^2 \leq \|x-y\|^2\right) \wedge \left(\forall \varepsilon \in \mathbb{R},\ \varepsilon > 0 \Rightarrow \exists z \in A : t^2 + \varepsilon > \|x-z\|^2\right)\}$$



It is a first order formula in the language of ordered field.

So the graph is semi-algebraic.

Important properties of semialgebraic mappings follow from the Tarski-Seidenberg theorem.

Corollary 2.9 *1. The direct image and the inverse image of a semialgebraic set by a semialgebraic mapping are semialgebraic. For instance, if $P(X_1, \ldots, X_n)$ is a polynomial and f, a semialgebraic mapping from $A \subset \mathbb{R}^m$ to $B \subset \mathbb{R}^n$, the set $\{y \in B \ ; \ P(f(y)) > 0\}$ is semialgebraic.*

2. The composition of two semialgebraic mappings is semialgebraic.

3. The semialgebraic functions from A to $\mathbb{R}$ form a ring.

Elements of proof

1. Let $f : A \to B$ be s.a. and $S \subseteq A$ be s.a.

Then $f(S)$ is the image of

$$(S \times B) \cap \operatorname{graph} f$$

under the projection $A \times B \to B$.

2.

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ \cap & & \cap & & \cap \\ \mathbb{R}^m & & \mathbb{R}^n & & \mathbb{R}^p \end{array}$$

Then $\operatorname{graph}(g \circ f)$ is the projection of

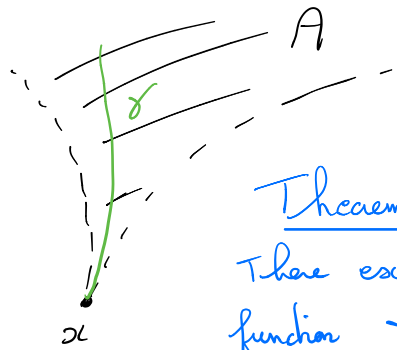
$$(\operatorname{graph} f) \times \mathbb{R}^p \cap \mathbb{R}^m \times (\operatorname{graph} g) \subseteq \mathbb{R}^{m+n+p}$$

on $\mathbb{R}^{m+p}$.

3. Consequence of 2. and the fact that $\begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x+y \end{array}$

and $\begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & & xy \end{array}$ are semi-algebraic. $\square$

• A first important result about semi-algebraic functions: <u>the curve selection lemma</u>



<u>Theorem</u> $A \subseteq \mathbb{R}^n$ semi-algebraic, $x \in \bar{A}$.
There exists a continuous semi-algebraic function $\gamma : [0,1) \longrightarrow \mathbb{R}^n$ such that

- $\gamma(0) = x$
- $\gamma((0,1)) \subseteq A$

<u>Remarks</u> (1) One can even ask γ to be analytic (i.e. of class Nash).

(2) Probably first proof by Milnor (via singularity theory).

• A second: <u>Łojasiewicz inequality</u>

First a preliminary result.

<u>Lemma</u> $P = a_0 X^d + \dots + a_{d-1} X + a_d \in \mathbb{R}[X]$ of degree d.
If $c \in \mathbb{C}$ is a root of P, then $|c| \leq \max\limits_i \left(d \left| \frac{a_i}{a_0} \right| \right)^{1/i} = M$

<u>Proof</u> Let $z \in \mathbb{C}$ with $|z| > M$, i.e. $|z^i| > d \left| \frac{a_i}{a_0} \right|$ and $|a_i| < \frac{1}{d} |a_0| |z|^i$.

So $|a_1 z^{d-1} + \dots + a_d| \leq |a_1| |z|^{d-1} + \dots + |a_d| < \frac{|a_0| |z|^d}{d} + \dots + \frac{|a_0| |z|^d}{d} = |a_0 z^d|$

Therefore $P(z) \neq 0$. □

The Łojasiewicz inequality gives information concerning the relative rate of growth of two continuous semialgebraic functions. First, we shall estimate the rate of growth of a semialgebraic function of one variable.

Proposition 2.11 *Let $f : (A, +\infty) \to \mathbb{R}$ be a semialgebraic (not necessarily continuous) function. There exist $B \geq A$ and an integer $N \in \mathbb{N}$ such that $|f(x)| \leq x^N$ for all $x \in (B, +\infty)$.*

Proof. Let Γ be the graph of f. It is a semialgebraic subset of $\mathbb{R}^2$, so $\Gamma = G_1 \cup \ldots \cup G_p$, where each G_i is a nonempty subset of the form

$$G_i = \{(x, y) \in \mathbb{R}^2 \ ; \ P_i(x, y) = 0, \ Q_{i,1}(x, y) > 0, \ldots, \ Q_{i,k_i}(x, y) > 0\} .$$

All polynomials P_i have degree > 0 with respect to y: otherwise $\dim G_i = 0$ or 2,

which is impossible since Γ is a graph. Let

$$P(x, y) = a_0(x)y^d + a_1(x)y^{d-1} + \cdots + a_d(x)$$

be the product of all $P_i(x, y)$, where $d > 0$ and $a_0 \neq 0$. Choose $C \geq A$ big enough so that $a_0(x)$ does not vanish on $(C, +\infty)$. By Lemma $*$, we obtain

$$|f(x)| \leq \max_{i=1,\ldots,d} \left(d \left| \frac{a_i(x)}{a_0(x)} \right| \right)^{1/i} .$$

As x tends to $+\infty$, the right-hand side of the equality is equivalent to λx^α, where $\lambda > 0$ and $\alpha \in \mathbb{Q}$. Taking N to be a nonnegative integer $> \alpha$, we obtain $B \geq C$, such that $|f(x)| \leq x^N$ for all $x > B$. $\square$

Theorem 2.12 (Łojasiewicz inequality) *Let $K \subset \mathbb{R}^n$ be a compact semi-algebraic set, and let $f, g : K \to \mathbb{R}$ be continuous semialgebraic functions , such that*

$$\forall x \in K \quad (f(x) = 0 \Rightarrow g(x) = 0) \ .$$

Then there exist an integer $N \in \mathbb{N}$ and a constant $C \geq 0$, such that

$$\forall x \in K \quad |g(x)|^N \leq C|f(x)| \ .$$

$$\left|\frac{g(x)}{f(x)}\right|^N \leq C$$

Proof. For $t > 0$, set $F_t = \{x \in K \ ; \ t|g(x)| = 1\}$. Since F_t is closed in K, it is compact. Assume $F_t \neq \emptyset$; then f does not vanish on F_t and the continuous function $x \mapsto 1/|f(x)|$ has a maximum on F_t, which we denote by $\theta(t)$. If $F_t = \emptyset$, we set $\theta(t) = 0$.

The function $\theta : (0, +\infty) \to \mathbb{R}$ is semialgebraic (check this fact by writing a formula which describes its graph). By Proposition 2.11, there exist $B > 0$ and $N \in \mathbb{N}$ such that

$$\forall t > B \quad |\theta(t)| \leq t^N \ .$$

$$t = \frac{1}{|g(x)|} > B \Rightarrow \frac{1}{|f(x)|} \leq \theta(t) \leq t^N = \frac{1}{|g(x)|^N}$$

This is equivalent to

$$\forall x \in K \quad \left(0 < |g(x)| < \frac{1}{B} \Rightarrow \frac{1}{|f(x)|} \leq \frac{1}{|g(x)|^N} \right) \ .$$

Let D be the maximum of the continuous function $|g(x)|^N/|f(x)|$ on the compact set

$$\{x \in K \ ; \ |g(x)| \geq 1/B\}$$

and set $C = \max(D, 1)$. Then

$\forall x \in K \quad |g(x)|^N \leq C|f(x)|$ □

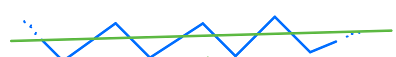
3. DECOMPOSITION OF A SEMI-ALGEBRAIC SET

Semi-algebraic sets can be cut into a finite number of "basic" semi-algebraic sets, called "cells"
$\rightsquigarrow$ cell decomposition theorem.

As a consequence:

<u>Theorem</u> A semi-algebraic set is a finite union of semi-algebraic sets each s.a. homeomorphic to some open hypercube $]0,1[^d \subseteq \mathbb{R}^d$ (with the convention $]0,1[^0$ is a point).

<u>Corollary</u> A semi-algebraic set has a finite number of connected components.

<u>Remarks</u> ① 

is not semi-algebraic.

② cosinus is not a semi-algebraic function.

③ All what we have seen (except last corollary) is still valid on any real closed field R (and not only on $\mathbb{R}$). But such a field is not connected in general

Example of such fields: $\mathbb{R}_{alg}$, $\mathbb{R}((t^{\frac{1}{\mathbb{N}}}))$

$]-\infty, \pi[$ is open and closed

$\{x : \exists r \in \mathbb{R}_+^*, x > r\}$ idem

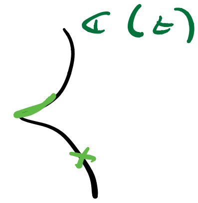
They are not semi-algebraic!

$\gamma \in \mathbb{C}((t^{\frac{1}{\mathbb{N}}}))$ corps des séries de Puiseux

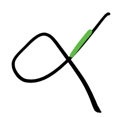
$$\gamma(t) = \sum_{m \geq q} a_m \underbrace{t^{m/p}}_{(t^{\frac{1}{p}})^m} \quad , \quad a_m \in \mathbb{C} \quad , \quad p \in \mathbb{N}^* , \; q \in \mathbb{Z}$$

Théorème $\mathbb{C}_{alg}((t^{\frac{1}{\mathbb{N}}}))$ est un corps alg. clos.
c'est la clôture algébrique de $\mathbb{C}((t))$.

Exemples ① $y^2 - x^3 \in \mathbb{C}[x][y]$



$y = \sqrt{x^3} = x^{3/2}$

② 

$y^2 = x^2(x+1)$

$$y = \sqrt{x^2(x+1)} = x \underbrace{\sqrt{1+x}}_{\dots}$$

COMPLEMENTS :

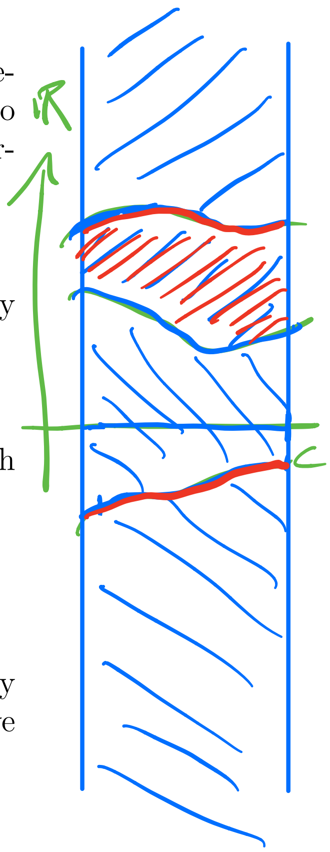
2.3 Decomposition of a semialgebraic set

We have seen that a semialgebraic subset of $\mathbb{R}$ can be decomposed as the union of finitely many points and open intervals. We shall see that every semialgebraic set can be decomposed as the disjoint union of finitely many pieces which are semialgebraically homeomorphic to open hypercubes $(0,1)^d$ of different dimensions. A semialgebraic homeomorphism $h : S \to T$ is a bijective continuous semialgebraic mapping from S onto T, such that $h^{-1} : T \to S$ is continuous.

Exercise 2.14 Check that h^{-1} is also semialgebraic.

The method of decomposition by using successive codimension 1 projections is the main tool for studying semialgebraic sets, and it is used in the foundational paper of S. Łojasiewicz (1964). We now explain the cylindrical algebraic decomposition of Collins [Cl], which makes precise the algorithmic content of this method.

2.3.1 Cylindrical algebraic decomposition



A *cylindrical algebraic decomposition* (abbreviated to *c.a.d.*) of $\mathbb{R}^n$ is a sequence $\mathcal{C}_1, \ldots, \mathcal{C}_n$, where, for $1 \le k \le n$, $\mathcal{C}_k$ is a finite partition of $\mathbb{R}^k$ into semialgebraic subsets (which are called *cells*), satisfying the following properties:

a) Each cell $C \in \mathcal{C}_1$ is either a point, or an open interval.

b) For every k, $1 \le k < n$, and for every $C \in \mathcal{C}_k$, there are finitely many continuous semialgebraic functions

$$\xi_{C,1} < \ldots < \xi_{C,\ell_C} : C \longrightarrow \mathbb{R} ,$$

and the cylinder $C \times \mathbb{R} \subset \mathbb{R}^{k+1}$ is the disjoint union of cells of $\mathcal{C}_{k+1}$ which are:

– either the *graph* of one of the functions $\xi_{C,j}$, for $j = 1, \ldots, \ell_C$:

$$A_{C,j} = \{(x', x_{k+1}) \in C \times \mathbb{R} \ ; \ x_{k+1} = \xi_{C,j}(x')\} ,$$

– or a *band* of the cylinder bounded from below and from above by the graphs of functions $\xi_{C,j}$ and $\xi_{C,j+1}$, for $j = 0, \ldots, \ell_C$, where we take $\xi_{C,0} = -\infty$ and $\xi_{i,\ell_C+1} = +\infty$:

$$B_{C,j} = \{(x', x_{k+1}) \in C \times \mathbb{R} \ ; \ \xi_{C,j}(x') < x_{k+1} < \xi_{C,j+1}(x')\} .$$

Proposition 2.15 *Every cell of a c.a.d. is semialgebraically homeomorphic to an open hypercube* $(0,1)^d$ *(by convention,* $(0,1)^0$ *is a point).*

Proof. We prove the property of the proposition for cells of $\mathcal{C}_k$, by induction on k. The key point is to observe that, using the notation above, every graph $A_{C,j}$ is semialgebraically homeomorphic to C and every band $B_{C,j}$ is semialgebraically homeomorphic to $C \times (0,1)$. In the case of $A_{C,j}$, the homeomorphism is simply

$$C \ni x' \longmapsto (x', \xi_{C,j}(x')) \in A_{C,j} \; .$$

For $B_{C,j}$ we take

$$\begin{array}{rcl} C \times (0,1) \ni (x',t) & \mapsto & (x', (1-t)\xi_{C,j}(x') + t\xi_{C,j+1}(x')) \text{ if } 0 < j < \ell_C \; , \\ & & \left(x', \dfrac{t-1}{t} + \xi_{C,1}(x')\right) \text{ if } j = 0,\; \ell_C \neq 0 \; , \\ & & \left(x', -\dfrac{1}{t} + \dfrac{1}{1-t}\right) \text{ if } j = \ell_C = 0 \; , \\ & & \left(x', \dfrac{t}{1-t} + \xi_{C,\ell_C}(x')\right) \text{ if } j = \ell_C \neq 0 \; . \end{array}$$

□

It is time to explain what we want to do with a c.a.d.. We shall use the following terminology: given a finite family $P_1, \ldots, P_r$ of polynomials in $\mathbb{R}[X_1, \ldots, X_n]$, we say that a subset C of $\mathbb{R}^n$ is $(P_1, \ldots, P_r)$-*invariant* if every polynomial P_i has a constant sign (> 0, < 0, or $= 0$) on C. We want to construct, from a finite family $P_1, \ldots, P_r$ of polynomials in $\mathbb{R}[X_1, \ldots, X_n]$, a c.a.d. of $\mathbb{R}^n$ such that:

c) Each cell $C \in \mathcal{C}_n$ is $(P_1, \ldots, P_r)$-invariant.

A c.a.d. of $\mathbb{R}^n$ satisfying this property will be called *adapted to* $(P_1, \ldots, P_r)$.

What is a c.a.d. adapted to $(P_1, \ldots, P_r)$ good for? First, the condition c) shows that every semialgebraic subset of $\mathbb{R}^n$ which is described by a boolean combination of equations $P_i = 0$ and inequalities $P_j > 0$ or $P_j < 0$, where P_i and P_j are among $P_1, \ldots, P_r$, is the union of some cells of $\mathcal{C}_n$. It follows that every semialgebraic set can be decomposed as the disjoint union of finitely many pieces, each semialgebraically homeomorphic to an open hypercube $(0,1)^d$. Moreover, the cylindrical arrangement of cells (property b) allows one to see that every semialgebraic subset of $\mathbb{R}^k$ described by a formula $Q_{k+1}x_{k+1} \ldots Q_n x_n \Phi$, where $Q_{k+1}, \ldots, Q_n$ are existential or universal quantifiers and Φ, a boolean combination of equations $P_i = 0$ and inequalities $P_j > 0$ or $P_j < 0$, is the union of some cells of $\mathcal{C}_k$. This can be useful, for instance, to decide whether such a formula is true or false.

2.3.2 Construction of an adapted c.a.d.

The definition of a c.a.d. shows the importance of the functions $\xi_{C,j}$ whose graphs cut the cylinders $C\times\mathbb{R}$. Since we want the bands of a cylinder contained in $\mathbb{R}^n$ to be $(P_1,\ldots,P_r)$-invariant, the $\xi_{C,j}$ have to describe the roots of the polynomials P_i, as functions of $(x_1,\ldots,x_{n-1})\in C$. We give now a first result in this direction.

Proposition 2.16 *Let $P(X_1,\ldots X_n)$ be a polynomial in $\mathbb{R}[X_1,\ldots X_n]$. Let $C\subset\mathbb{R}^{n-1}$ be a connected semialgebraic subset and $k\le d$ in $\mathbb{N}$ such that, for every point $x'=(x_1,\ldots,x_{n-1})\in C$, the polynomial $P(x',X_n)$ has degree d and exactly k distinct roots in $\mathbb{C}$. Then there are $\ell\le k$ continuous semialgebraic functions $\xi_1<\ldots<\xi_\ell : C\to\mathbb{R}$ such that, for every $x'\in C$, the set of real roots of $P(x',X_n)$ is exactly $\{\xi_1(x'),\ldots,\xi_\ell(x')\}$. Moreover, for $i=1,\ldots,\ell$, the multiplicity of the root $\xi_i(x')$ is constant for $x'\in C$.*

Proof. The argument relies on the "continuity of roots", in the following form (a proof is proposed in the next exercise):

CR Choose $a'\in C$ and let $z_1,\ldots,z_k$ be the distinct roots of $P(a',X_n)$, with multiplicities $m_1,\ldots,m_k$, respectively. Choose $\varepsilon>0$ so small that the open disks $D(z_i,\varepsilon)\subset\mathbb{C}$ with centers z_i and radius ε are disjoint. If $b'\in C$ is sufficiently close to a', the polynomial $P(b',X_n)$ has exactly m_i roots, counted with multiplicities, in the disk $D(z_i,\varepsilon)$, for $i=1,\ldots,k$.

Since $P(b',X_n)$ has k distinct roots and $d=m_1+\cdots+m_k$ roots counted with multiplicities, it follows that each $D(z_i,\varepsilon)$ contains exactly one root ζ_i of multiplicity k of $P(b',X_n)$. If z_i is real, ζ_i is real (otherwise, its conjugate $\overline{\zeta}_i$ would be another root of $P(b',X_n)$ in $D(z_i,\varepsilon)$). If z_i is nonreal, ζ_i is nonreal, since $D(z_i,\varepsilon)$ is disjoint from its image by conjugation. Hence, if $b'\in C$ is sufficiently close to a', $P(b',X_n)$ has the same number of distinct real roots as $P(a',X_n)$. Since C is connected, the number of distint real roots of $P(x',X_n)$ is constant for $x'\in C$. Let ℓ be this number. For $1\le i\le\ell$, denote by $\xi_i : C\to\mathbb{R}$ the function which sends $x'\in C$ to the i-th real root (in the increasing order) of $P(x',X_n)$. The argument above, with ε as small as we want, shows, moreover, that the functions ξ_i are continuous. It follows from the connectedness of C that each $\xi_i(x')$ has constant multiplicity. If C is described by the formula $\Theta(x')$, the graph of ξ_i is described by the formula

$$\begin{aligned}&\Theta(x')\ \text{ and }\ \exists y_1\ldots\exists y_\ell(y_1<\ldots<y_\ell\ \text{ and}\\&\qquad P(x',y_1)=0\ \text{ and }\ \ldots\ \text{ and }\ P(x',y_\ell)=0\ \text{ and }\ x_n=y_i)\ ,\end{aligned}$$

which shows that ξ_i is semialgebraic. ☐

Exercise 2.17 We identify monic polynomials $X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{C}[X]$ of degree d with points $(a_1, \dots, a_d) \in \mathbb{C}^d$. With this identification, let

$$\begin{array}{rcl} \mu : \mathbb{C}^e \times \mathbb{C}^{d-e} & \longrightarrow & \mathbb{C}^d \\ (R, S) & \longmapsto & RS \end{array}$$

be the mapping defined by the multiplication of monic polynomials.
1) Fix $R^0 \in \mathbb{C}^e$ and $S^0 \in \mathbb{C}^{d-e}$. Show that the jacobian determinant of μ at (R^0, S^0) is equal to $\pm$ the resultant of R^0 and S^0.
2) Let $Q^0 \in \mathbb{C}^d$ and assume that $Q^0 = R^0S^0$, where R^0 and S^0 are relatively prime monic polynomials of degrees e and $d-e$, respectively. Show that for every Q sufficiently close to Q^0, there is a unique factorization $Q = RS$ with R close to R^0 and S close to S^0.
3) Assume $Q^0 = (X - z_1)^{m_1} \cdots (X - z_k)^{m_k}$, where $z_1, \dots, z_k$ are the distinct roots of Q^0. Show that, for every Q close to Q^0, there is a unique factorization $Q = R_1 \cdots R_k$, where the R_i are monic polynomials close to $(X - z_i)^{m_i}$.
4) Fix $\varepsilon > 0$. Show that every monic polynomial sufficently close to X^m has its roots in $D(0, \varepsilon)$ (use Proposition 1.3). Deduce that every monic polynomial sufficiently close to $(X - z)^m$ has its roots in $D(z, \varepsilon)$.
5) Let Q^0 be a monic polynomial with distinct roots $z_1, \dots, z_k$ of multiplicities $m_1, \dots, m_k$, respectively. Choose $\varepsilon > 0$ such that all disks $D(z_i, \varepsilon)$ are disjoint. Show that every monic polynomial close to Q^0 has exactly m_i roots counted with multiplicities in $D(z_i, \varepsilon)$, for $i = 1, \dots, k$.
6) Prove property CR above (if $P = a_0(x')X_n + \cdots + a_d(x')$, set $Q = P/a_0(x')$).

If we have several polynomials P_i, we have also to take care that the roots of the different P_i do not get mixed.

Proposition 2.18 *Let P and Q be polynomials of $\mathbb{R}[X_1, \dots X_n]$. Let C be a connected semialgebraic subset of $\mathbb{R}^{n-1}$. Assume that the degree and the number of distinct roots of $P(x', X_n)$ (resp. $Q(x', X_n)$) and the degree of the gcd of $P(x', X_n)$ and $Q(x', X_n)$ are constant for all $x' \in C$. Let $\xi, \zeta : C \to \mathbb{R}$ be continuous semialgebraic functions such that $P(x', \xi(x')) = 0$ and $Q(x', \zeta(x')) = 0$ for every $x' \in C$. If there is $a' \in C$ such that $\xi(a') = \zeta(a')$, then $\xi(x') = \zeta(x')$ for every $x' \in C$.*

Proof. We use the same method of proof as in the preceding proposition. Let $z_1 = \xi(a') = \zeta(a'), \dots, z_k$ be the distinct roots in $\mathbb{C}$ of the product

$P(a', X_n)Q(a', X_n)$. Let m_i (resp. p_i) be the multiplicity of z_i as a root of $P(a', X_n)$ (resp. $Q(a', X_n)$), where multiplicity zero means "not a root". The degree of $\gcd(P(a', X_n), Q(a', X_n))$ is $\sum_{i=1}^{k} \min(m_i, p_i)$, and each z_i has multiplicity $\min(m_i, p_i)$ as a root of this gcd. Choose $\varepsilon > 0$ such that all disks $D(z_i, \varepsilon)$ are disjoint. For every $x' \in C$ sufficiently close to a', each disk $D(z_i, \varepsilon)$ contains a root of multiplicity m_i of $P(x', X_n)$ and a root of multiplicity p_i of $Q(x', X_n)$. Since the degree of $\gcd(P(x', X_n), Q(x', X_n))$ is equal to $\sum_{i=1}^{k} \min(m_i, p_i)$, this gcd must have one root of multiplicity $\min(m_i, p_i)$ in each disk $D(z_i, \varepsilon)$ such that $\min(m_i, p_i) > 0$. In particular, it follows that $\xi(x') = \zeta(x')$. Since C is connected, this equality holds for every $x' \in C$. $\square$

We have seen in Chapter 1 that the number of distinct complex roots of P and the degree of the gcd of P and Q, can be computed from the fact that the principal subresultant coefficients $\mathrm{PSRC}_i(P, P')$ and $\mathrm{PSRC}_i(P, Q)$ are zero or nonzero, as long as the degrees (with respect to X_n) of P and Q are fixed (cf. Corollary 1.21 and Proposition 1.19). For the values of the parameters (here, $X_1, \dots, X_{n-1}$) such that some leading coefficients vanish, we have to use the principal subresultant coefficients for the truncated polynomials. This leads us to the following definition.

If P is a polynomial in $\mathbb{R}[X_1, \dots, X_n]$, we consider it as a polynomial in the variable X_n with coefficients in $\mathbb{R}[X_1, \dots, X_{n-1}]$. We denote by $\mathrm{lc}(P)$ its leading coefficient and by $\mathrm{trunc}(P)$ the truncated polynomial obtained by deleting its leading term. Let $P_1, \dots, P_r$ be a family of polynomials in $\mathbb{R}[X_1, \dots, X_n]$. We define $\mathrm{PROJ}(P_1, \dots, P_r)$ to be the smallest family of polynomials in $\mathbb{R}[X_1, \dots, X_{n-1}]$ satisfying the following rules:

- If $\deg_{X_n} P_i = d \geq 2$, $\mathrm{PROJ}(P_1, \dots, P_i, \dots, P_r)$ contains all nonconstant polynomials among $\mathrm{PSRC}_j(P_i, \partial P_i/\partial X_n)$ for $j = 0, \dots, d-1$.

- If $1 \leq d = \min(\deg_{X_n}(P_i), \deg_{X_n}(P_k))$, $\mathrm{PROJ}(P_1, \dots, P_i, \dots, P_k, \dots, P_r)$ contains all nonconstant $\mathrm{PSRC}_j(P_i, P_k)$ for $j = 0, \dots, d$.

- If $\deg_{X_n} P_i \geq 1$ and $\mathrm{lc}(P_i)$ is not constant, $\mathrm{PROJ}(P_1, \dots, P_i, \dots, P_r)$ contains $\mathrm{lc}(P_i)$ and $\mathrm{PROJ}(P_1, \dots, \mathrm{trunc}(P_i), \dots, P_r)$.

- If $\deg_{X_n} P_i = 0$ and P_i is not constant, $\mathrm{PROJ}(P_1, \dots, P_i, \dots, P_r)$ contains P_i.

The following theorem is a consequence of the results previously proved in this section.

Theorem 2.19 *Let $(P_1, \ldots, P_r)$ be a family of polynomials in $\mathbb{R}[X_1, \ldots, X_n]$, and let C be a connected, $\mathrm{PROJ}(P_1, \ldots, P_r)$-invariant, semialgebraic subset of $\mathbb{R}^{n-1}$. Then there are continuous semialgebraic functions $\xi_1 < \ldots < \xi_\ell : C \to \mathbb{R}$, such that, for every $x' \in C$, the set $\{\xi_1(x'), \ldots, \xi_\ell(x')\}$ is the set of real roots of all nonzero polynomials $P_1(x', X_n), \ldots, P_r(x', X_n)$. The graph of each ξ_i, and each band of the cylinder $C \times \mathbb{R}$ bounded by these graphs, are connected semialgebraic sets, semialgebraically homeomorphic to C or $C \times (0,1)$, respectively, and $(P_1, \ldots, P_r)$-invariant.*

If we have constructed a c.a.d. of $\mathbb{R}^{n-1}$ adapted to $\mathrm{PROJ}(P_1, \ldots, P_r)$, the preceding theorem can be used to extend this c.a.d. to a c.a.d. of $\mathbb{R}^n$ adapted to $(P_1, \ldots, P_r)$. On the other hand, by iterating $(n-1)$ times the operation PROJ, we arrive to a finite family of polynomials in one variable X_1. It is easy to construct a c.a.d. of $\mathbb{R}$ adapted to this family: the real roots of the polynomials in the family cut the line in finitely many points and open intervals. Finally, we obtain:

Theorem 2.20 *For every finite family $P_1, \ldots, P_r$ in $\mathbb{R}[X_1, \ldots, X_n]$, there is an adapted c.a.d. of $\mathbb{R}^n$.*

We illustrate this result by constructing a c.a.d. of $\mathbb{R}^3$ adapted to the polynomial $P = X^2 + Y^2 + Z^2 - 1$. The Sylvester matrix of P and $\partial P/\partial Z$ is

$$\begin{pmatrix} 1 & 0 & X^2+Y^2-1 \\ 0 & 2 & 0 \\ 2 & 0 & 0 \end{pmatrix} .$$

Hence, $\mathrm{PSRC}_0(P, \partial P/\partial Z) = -4(X^2 + Y^2 - 1)$ and $\mathrm{PSRC}_1(P, \partial P/\partial Z) = 2$. Getting rid of irrelevant constant factors, we obtain $\mathrm{PROJ}(P) = (X^2+Y^2-1)$, then $\mathrm{PROJ}(\mathrm{PROJ}(P)) = (X^2 - 1)$. The c.a.d. obtained is represented on Figure 2.1.

Exercise 2.21 How many cells of $\mathbb{R}^3$ are there in this c.a.d.? Is it possible to have a c.a.d. of $\mathbb{R}^3$, such that the sphere is the union of cells, with less cells?

Exercise 2.22 Let $f : A \to \mathbb{R}$ be a semialgebraic function, which is not supposed to be continuous. Show that there exists a finite semialgebraic partition $A = \bigcup_{i=1}^{s} C_i$ of A such that, for every i, the restriction of f to C_i is continuous. Hint: use a c.a.d. adapted to the graph of f.

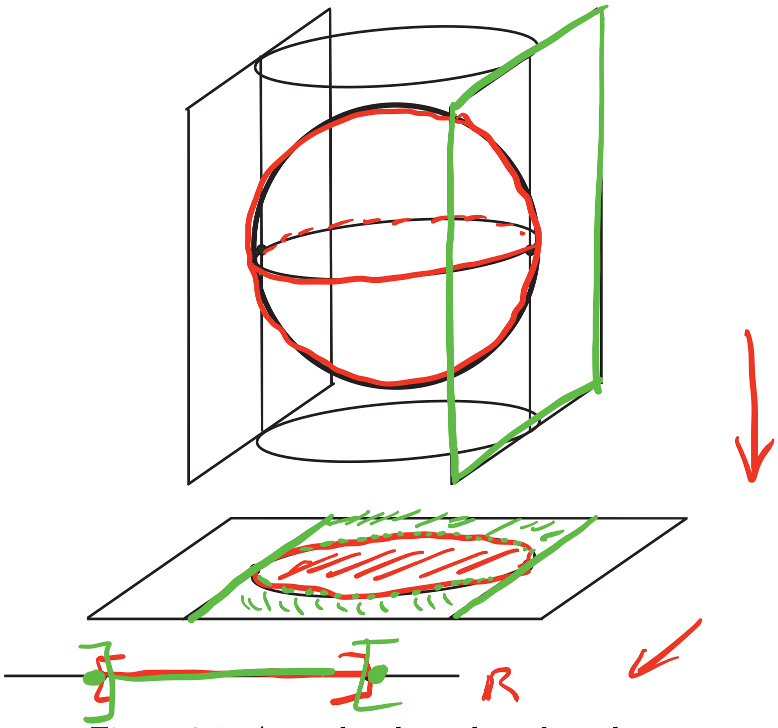


Figure 2.1: A c.a.d. adapted to the sphere

Remark. We return to the proof of Proposition 2.16. For every $x' \in C$, $\xi_i(x')$ is a root of $P(x', X_n)$, with constant multiplicity m_i. Hence, $\xi_i(x')$ is a simple root of the $(m_i - 1)^{\text{th}}$ derivative with respect to X_n. Therefore, if C is a $\mathcal{C}^\infty$ submanifold of $\mathbb{R}^{n-1}$, the function ξ_i is $\mathcal{C}^\infty$ on C. The graphs and the bands of the cylinder $C \times \mathbb{R}$ are also $\mathcal{C}^\infty$ submanifolds, diffeomorphic to C or $C \times (0,1)$, respectively (cf. the formulas in the proof of Proposition 2.15). By induction on n, one proves in this way that every semialgebraic set is the disjoint union of finitely many semialgebraic subsets C_i, which are $\mathcal{C}^\infty$ submanifolds each semialgebraically diffeomorphic to an open hypercube $(0,1)^{d_i}$. The semialgebraic $\mathcal{C}^\infty$ submanifolds are called *Nash manifolds*.