CAHIERS DU SÉMINAIRE D'HISTOIRE DES MATHÉMATIQUES

MARIE-FRANÇOISE ROY

Introduction à la géométrie algébrique réelle

Cahiers du séminaire d'histoire des mathématiques 2^e série, tome 1 (1991), p. 19-29

<http://www.numdam.org/item?id=CSHM_1991_2_1__19_0>

INTRODUCTION
A LA GEOMETRIE ALGEBRIQUE REELLE

Marie-Françoise Roy
IRMAR
Université de Rennes I

1. Définition de la géométrie algébrique réelle

La **géométrie algébrique** est, dans sa définition la plus simple, l'étude des ensembles de solutions de systèmes d'équations polynomiales. Le plus souvent,on travaille en géométrie algébrique avec des corps algébriquement clos, car la situation est plus facile à étudier : un polynôme en une variable de degré d a par exemple toujours d racines distinctes ou confondues.

La géométrie algébrique **réelle** a pour premier objet l'étude des sous-ensembles de $\mathbb{R}^n$ définis par des équations polynomiales, les ensembles algébriques réels. On veut donc rester dans le domaine des nombres réels, et non utiliser les nombres complexes. On sait bien que, dans ce cas, tous les polynômes de degré d n'auront plus d racines distinctes ou confondues.

Plus généralement, à la suite d'Artin et Schreier, on travaille avec des **corps réels clos**. La théorie des corps réels clos est la théorie qui consiste à donner une version algébrique des propriétés des réels qui sont utiles pour l'étude des polynômes.

Définition *: Un corps ordonné $(F,\leq)$ est un corps F muni d'une relation d'ordre total $\leq$ qui vérifie* :

(i) $x \leq y \Rightarrow x+z \leq y+z$,

(ii) $0 \leq x,\ 0 \leq y \Rightarrow 0 \leq xy$.

Un corps réel clos F est un corps réel qui n'admet pas d'extension algébrique non triviale $(F \subset F_1)$ réelle.

Théorème (pour une preuve, voir [B C R])
Soit F un corps. Les propriétés suivantes sont équivalentes :

(i) *F est réel clos.*

(ii) *F admet un ordre unique dont le cône positif est formé des carrés de F, et tout polynôme de $F[X]$ de degré impair a une racine dans F.*

(iii) *$F[i] = F[X] / (X^2+1)$ est un corps algébriquement clos.*

Exemples

Le corps des réels est naturellement réel clos, ainsi que le corps des nombres réels algébriques (les nombres réels qui vérifient une équation à coefficients entiers).

Le corps des séries de Puiseux $\mathbb{R}(X)^\wedge$ est réel clos. Rappelons que le corps $\mathbb{R}(X)^\wedge$ (resp. $\mathbb{C}(X)^\wedge$) des séries de Puiseux à coefficients réels (resp. complexes) a pour éléments les expressions

$\sum_{i=k}^{\infty} a_i X^{i/q}$, avec $k \in \mathbb{Z}$, $q \in \mathbb{N} \setminus \{0\}$, $a_i \in \mathbb{R}$ (resp. $a_i \in \mathbb{C}$).

Une manière de montrer que $\mathbb{R}(X)^\wedge$ est réel clos est d'utiliser le point (iii) du théorème précédent car $\mathbb{R}(X)^\wedge(i)$ coincide avec $\mathbb{C}(X)^\wedge$, dont on sait qu'il est algébriquement clos ([W]).

Un théorème fondamental en géométrie algébrique sur les corps algébriquement clos est le théorème des zéros de Hilbert, qui permet d'avoir une correspondance agréable entre objets algébriques (les idéaux radicaux des anneaux de polynômes) et objets géométriques (les ensembles algébriques). Une telle correspondance existe aussi en géométrie algébrique réelle entre idéaux réels et ensembles algébriques : c'est le **théorème des zéros réels**.

Théorème (théorème des zéros réels) (pour une preuve, voir [B C R])
Soit R un corps réel clos, I un idéal de $R[X_1, ..., X_n]$. $f \in R[X_1, ..., X_n]$ s'annule sur les zéros de I si et seulement s'il existe $m, a_1, ..., a_p$, tels que $f^{2m} + a_1^2 + ... + a_1^2 \in I$.

Donnons tout de suite un exemple très simple qui montre comment la géométrie algébrique réelle se différencie de la géométrie algébrique complexe. Considérons l'intersection de la droite $x = t$, dépendant du paramètre t, avec la cubique $y^2 = x^3 - x$. Dans le plan complexe, à part les valeurs $t = -1, 0, 1$, pour lesquelles il y a tangence, la droite coupe toujours la cubique en deux points. Il y a plus à dire sur la situation dans le plan réel.

a) Il n'y a pas toujours d'intersection.

b) L'ensemble des paramètres t pour lesquels il y a intersection est la réunion de deux intervalles. La description de cet intervalle ne peut se faire seulement au moyen d'équations et d'inéquations, elle fait intervenir nécessairement des **inégalités** polynomiales (à savoir $x^3 - x \geq 0$).

Un résultat remarquable, le **principe de Tarski-Seidenberg**, affirme que la situation décrite dans l'exemple est générale et que les inégalités polynomiales suffisent toujours à décrire les projections des ensembles algébriques réels.

On est donc tout de suite amené, si on s'intéresse aux ensembles algébriques réels, à définir les **ensembles semi-algébriques**, qui sont les sous-ensembles de $\mathbb{R}^n$ définis par une combinaison booléenne au moyen d'un nombre fini d'équations et d'inéquations polynomiales. Ces ensembles jouissent de nombre de propriétés remarquables.

Les deux propriétés essentielles sont les suivantes

Théorème (théorème de projection) (pour une preuve, voir [B C R])
Soit R un corps réel clos. Soit S un ensemble semi-algébrique de R^{n+k}. Sa projection $\Pi(S)$ sur R^n est un ensemble semi-algébrique.

Théorème (composantes connexes) (pour une preuve, voir [B C R])
Soit R un corps réel clos. Tout ensemble semi-algébrique S de R^n est réunion disjointe d'un nombre fini d'ensembles semi-algébriquement connexes $C_1, \ldots, C_s$ qui sont ouverts et fermés dans S.

Ces deux théorèmes ont un grand nombre de conséquences, qui font des ensembles semi-algébriques une classe particulièrement stable: par exemple l'adhérence et l'intérieur des ensembles semi-algébriques sont semi-algébriques, les points d'un ensemble semi-algébrique de dimension réelle fixée forment un ensemble semi-algébrique, ainsi que les composantes connexes de tous ces ensembles. Plus généralement tout ensemble décrit par une formule du premier ordre du langage des corps ordonnés (c'est-à-dire où on ne quantifie que sur des éléments du corps, pas sur des polynômes, des fonctions, des sous-ensembles, des chemins..) est semi-algébrique.

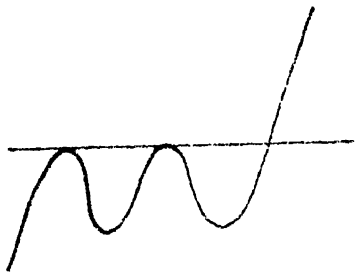
Le caractère naturel et concret de la notion d'ensemble semi-algébrique est si évident que l'on pourrait presque penser que tout est semi-algébrique. Et

en effet, la géométrie algébrique réelle offre un champ d'**applications** extrêmement variés, qui commence seulement à être exploré, et que nous aborderons dans le point 3.

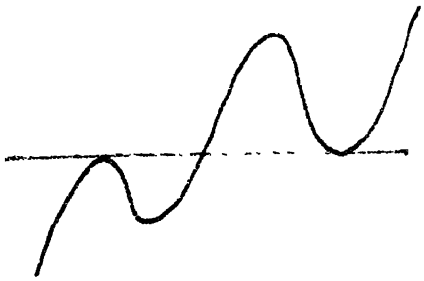
2. Interlude : Les polynômes hyperboliques

Le paragraphe suivant expose rapidement un résultat récent de géométrie algébrique réelle, qui illustre bien quelques unes des caractéristiques du domaine.

Les *polynômes hyperboliques* sont les polynômes ayant toutes leurs racines réelles (éventuellement multiples). Pour un tel polynôme on définit son vecteur multiplicité comme étant la liste ordonnée des multiplicités de ses racines, rangées dans l'ordre de R. C'est ainsi qu'un polynôme de degré 5 de vecteur multiplicité (2,2,1) aura deux racines doubles suivies d'une racine simple, et un polynôme de degré 5 de vecteur multiplicité (2,1,2) aura une racine simple entre deux racines doubles.



vecteur multiplicité (2,2,1)



vecteur multiplicité (2,1,2)

On peut observer sur les graphes de ces polynômes des propriétés assez remarquables. C'est ainsi que si on prend un polynôme P de degré 5 avec vecteur multiplicité (2,2,1), on peut trouver une constante négative c telle que la droite $y=c$ coupe 5 fois le graphe $y=P(x)$, mais aucune constante positive avec la même propriété. Par contre il existe des droites de pente positive et négative, des paraboles de coefficients directeur positif et négatif etc.... coupant 5 fois le graphe $y=P(x)$. Si on prend maintenant un polynôme P de degré 5 avec vecteur multiplicité (2,1,2), on ne peut trouver aucune constante c telle que la droite $y=c$ coupe 5 fois le graphe $y=P(x)$, ni aucune droite de pente négative qui coupe 5 fois le graphe $y=P(x)$. Par contre il existe des droites de pente positive, des paraboles de coefficients directeur positif et négatif etc.... coupant 5 fois le graphe $y=P(x)$.

Ce genre de propriété est tout à fait général. Posons une définition.

Définition :
On dit qu'un polynôme hyperbolique est
s-maximal si aucun polynôme de la forme P+Q avec Q de degré s et de coefficient dominant strictement positif n'est hyperbolique,
s-minimal si aucun polynôme de la forme P+Q avec Q de degré s et de coefficient dominant strictement négatif n'est hyperbolique.

On a le théorème suivant ([M])

Théorème :
Pour tout vecteur multiplicité v il existe un entier s (calculable par une recette très simple à partir de ce vecteur multiplicité) tel que pour tout polynôme hyperbolique P de degré p et de multiplicité v :
- pour tout $s'<s$, P est s-maximal et s-minimal,
- P est soit s-minimal et pas s-maximal, soit s-maximal et pas s-minimal,
- pour tout $s'>s$, $s'\leq p$, P n'est ni s–maximal ni s–minimal.

Il est intéressant de noter que ce résultat est de nature purement réelle. La propriété dépend bien du vecteur multiplicité, donc de l'ordre des racines, et non seulement des multiplicités des racines comme le montre l'exemple des polynômes de degré 5.

Il y a donc encore en géométrie algébrique réelle des problèmes à résoudre qui sont d'énoncé très élémentaire. Les méthodes de démonstration ne le sont pas nécessairement. C'est ainsi que l'étude des polynômes hyperboliques, dont certaines propriétés fondamentales ont été observées par Barbançon de Strasbourg, a été menée par Arnold et Givental avec des méthodes géométriques (théorie de Morse sur des variétés algébriques réelles très particulières, les variétés de Van der Monde). Leurs méthodes sont utilisées dans la démonstration du nouveau théorème ci-dessus.

3. Algorithmes et Applications

a) le théorème de Sturm

Le théorème de Sturm définit un algorithme fondamental pour connaître le nombre de racines dans R d'un polynôme P en une variable à coefficients dans un corps $K \subset R$ à l'aide de calculs qui se font uniquement dans le corps K.

Théorème (théorème de Sturm) :

Soit R un corps réel clos. Soit $f_0, .., f_1$ la suite de polynômes ainsi construite :

$$f_0 = P, f_1 = P',$$

$f_{i-2} = f_{i-1} g_i - f_i$ *avec* $deg(f_i) < deg(f_{i-1})$ *pour* $i = 2, ..., k$ *et* $f_k \in R \setminus \{0\}$.

Si $a \in R$ n'est pas racine de P, on note $v(a)$ le nombre de changements de signe dans la suite $f_0(a), f_1(a), ..., f_k(a)$: on compte un changement de signe quand $f_i(a) f_\ell(a) < 0$ avec $\ell = i+1$ ou $\ell > i+1$ et pour tout j, $i<j<\ell$, $f(a) = 0$.

Soient $a, b \in R$, $a<b$ tels que ni a ni b ne sont racines de p. Alors le nombre de racines de P sur l'intervalle $]a,b[$ est égal à $v(a) - v(b)$. p_1

b) le théorème de projection et ses conséquences

Le théorème de Sturm permet donc de décider si un polynôme d'une variable a ou non des racines réelles. Le théorème de projection qui permet de calculer les points de R^n au dessus desquels il existe des points de $S \subset R^{n+k}$ peut être considéré comme une généralisation du théorème de Sturm.

On s'est intéressé depuis longtemps au calcul explicite de la projection d'un ensemble semi-algébrique, par des algorithmes d'efficacité optimales en fonction du nombre s et du degré d des polynômes qui définissent S, et bien entendu du nombre total de variables $n+k$.

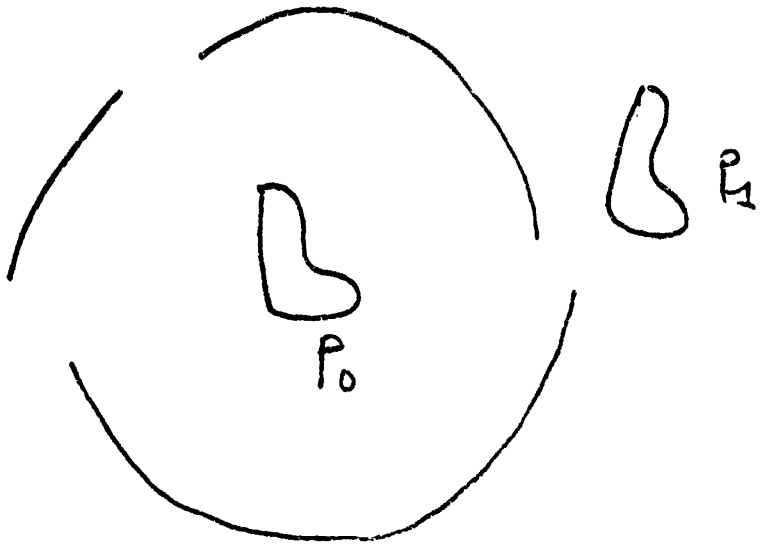
Les premières méthodes connues, basées sur les démonstrations de Tarski et Seidenberg donnaient pour complexité des tours d'exponentielle. La méthode de décomposition algébrique cylindrique de Collins donne un algorithme de complexité polynomiale en d et s, doublement exponentielle en $n+k$. Des résultats plus récents, basés sur des idées qui apparaissent dans les travaux de Grigor'ev et Vorobjov (voir leur article dans [SC]), montrent qu'on peut obtenir un algorithme de complexité polynomiale en d et s, et simplement exponentielle dans le nombre $n+k$ (voir [HRS]). Il est hors de

question de donner ici des indications précises sur ces méthodes; disons simplement qu'elles utilisent, outre des algorithmes assez précis de calcul formel sur les inégalités quelques idées et techniques issues de la géométrie différentielle (utilisation de fonctions de Morse et considération de points critiques).

Les algorithmes de calcul de projection ont de nombreuses applications, comme des méthodes explicites d'élimination des quantificateurs, qui permettent de calculer nombre d'ensembles associés à un semi-algébrique S et qui sont eux-mêmes semi-algébriques (adhérence de S, points de S de dimension réelle fixée, etc...), ou encore la démonstration automatique en géométrie réelle.

c) le problème du déménageur de piano

Considérons le problème suivant : on a dans $\mathbb{R}^n$ une pièce semi-algébrique avec des murs et des ouvertures ("portes", "fenêtres") semi-algébriques et un objet semi-algébrique (le robot, le plus souvent appelé "piano"). Existe-t-il un chemin permettant au piano de passer d'une certaine position p_0 intérieure à la pièce à une position p_1 extérieure à la pièce sans heurter les murs ? (c'est ce qu'on appelle le problème du déménageur de piano).



Ce problème ne peut pas se traduire de façon immédiate par une formule du premier ordre du langage des corps ordonnés (on ne peut pas quantifier sur les chemins).

On définit l'ensemble $\boldsymbol{M}$ des murs, l'ensemble ***Pos*** des positions du piano et l'ensemble ***PPos*** des positions permises du piano, c'est à dire des positions où le piano ne rencontre pas les murs.

Il n'est pas difficile de voir que l'ensemble ***Pos*** peut être considéré comme une partie semi-algébrique d'un certain $\mathbb{R}^N$. Si $n=2$, c'est-à-dire si le problème est plan, on peut prendre $N = 4$: on attache un repère au piano et les positions du piano sont données par l'image de ce repère; on a besoin de deux coordonnées pour déterminer l'origine du repère et de deux coordonnées supplémentaires (par exemple une matrice de rotation) pour avoir complètement sa position.

On note Pia le piano, et si p est une position, c'est-à-dire un élément de ***Pos***, on notera Pia_p le sous-ensemble de $\mathbb{R}^n$ correspondant au piano dans la position p. Comme Pia est semi-algébrique, Pia_p l'est également.

On a $\boldsymbol{PPos} = \{ p \in \boldsymbol{Pos} \mid Pia_p \cap \boldsymbol{M} = \emptyset \}$. Cet ensemble, qui est décrit par une formule du premier ordre du langage des corps ordonnés, est donc semi-algébrique et l'élimination des quantificateurs permet de décrire explicitement cet ensemble semi-algébrique.

Si on a deux positions permises p_0 et p_1 le problème de départ revient au problème suivant : p_0 et p_1 appartiennent-elles à la même composante connexe de ***PPos*** ? Si oui, le problème du déménageur sera possible, sinon il sera impossible.

On est donc ramené au problème suivant : étant donné un ensemble semi-algébrique S décrit explicitement, décider si deux éléments x_0 et x_1 de S appartiennent à la même composante connexe de S.

Là encore, après des méthodes de complexité doublement exponentielle dans le nombre de variables, basées sur la décomposition algébrique cylindrique (travaux de Schwartz et Sharir), on vient d'obtenir récemment des méthodes de complexité simplement exponentielle en ce nombre de variables, par des méthodes basées sur les mêmes principes que les nouvelles démonstrations (voir [G H R S V]).

d) le Nullstellensatz réel effectif

Les démonstrations classiques du Nullstellensatz réel font fortement intervenir le lemme de Zorn. On peut toutefois se demander s'il existe des bornes sur le nombre et le degré des sommes de carrés qui interviennent dans ce théorème, et si on peut les construire effectivement. Une méthode récente d'Henri Lombardi répond affirmativement à ces questions (voir [L]).

4. Les nombres réels existent-ils?

On vient de voir que les algorithmes de la géométrie algébrique réelle permettent de résoudre, par des calculs sur les nombres entiers, des questions de géométrie réelle. Mais dans ce cas les nombres réels dont il est question sont les nombres réels algébriques, c'est-à-dire les nombres réels qui sont solution d'un polynôme à coefficients entiers.

Le corps des nombres réels algébriques est un corps dénombrable, c'est la clôture réelle de $\mathbb{Q}$, et il est inclus dans tous les corps réels clos. On peut décrire ses éléments par une structure de donnée finie, par exemple par un polynôme à coefficients entiers et le numéro d'une de ses racines réelles. On peut aussi décrire des méthodes (basées sur une généralisation du théorème de Sturm) qui permettent de faire des calculs exacts sur ces nombres réels algébriques (voir l'article Thom's lemma dans [SC]).

Il n'en est évidemment pas de même pour les réels en général, qui ne forment pas un ensemble dénombrable et qu'on ne peut donc pas tous décrire par des structures de donnée finies.

Il est intéressant de remarquer que d'autres corps, moins familiers pour le mathématicien sont codables en machine. C'est ainsi que la clôture réelle du corps $\mathbb{Q}(X)$ (ordonné par l'ordre 0_+ où X est infiniment petit positif, c'est-à-dire positif et plus petit que tous les rationnels positifs) est le corps des séries de Puiseux à coefficients réels algébriques, qui sont algébriques sur les éléments de $\mathbb{Q}(X)$. Ce corps est dénombrable, ses éléments se décrivent grâce à une structure de donnée finie, un polynôme à coefficients dans $\mathbb{Q}(X)$ et le numéro d'une de ses racines. Il suffit de savoir faire des calculs exacts sur les entiers, pour savoir faire du calcul exact (opérations arithmétiques, décision du signe d'un élément) dans ce corps apparemment exotique, qui n'est même pas archimédien.

Le cadre général adapté à la discussion de ces questions me semble être le suivant : on fixe un anneau ordonné A, où les opérations arithmétique et la

détermination du signe d'un élément sont donnés par un oracle. On peut construire la clôture réelle R de A, les éléments de R sont décrits par une structure de donnée finie à partir d'un nombre fini d'éléments de A, et on peut répondre de manière exacte à des questions concernant les éléments de R grâce à un nombre fini d'invocations à l'oracle de A (voir [L R]).

En conclusion, les clôtures réelles d'anneaux très variés, y compris non archimédiens, existent bien, dans un sens informatique précis, mais les nombres réels des mathématiciens n'existent pas (en ce sens informatique).

Bibliographie

Les ouvrages suivant sont des manuels ou des recueils d'articles consacrés totalement ou partiellement à la géométrie algébrique réelle et peuvent donc servir de bibliothèque de base dans le domaine. Le reste de la bibliographie peut se reconstituer à partir des références qui y apparaissent.

[ARAG] *Algorithms in real algebraic geometry.* Journal of Symbolic Computation **5** (1988).

[BR] Benedetti R., Risler J.-J. : *Topologie des ensembles algébriques réels.* Hermann (1990).

[BCR] Bochnak J., Coste M., Roy M.-F. : *Géométrie algébrique réelle.* Ergebnisse des Mathematik, **12**. Berlin, Heidelberg, New York : Springer Verlag (1987).

[GAR] *Géométrie algébrique réelle et formes quadratiques.* Lecture Notes in Math. **959**. Berlin, Heidelberg, New York : Springer Verlag (1982).

[GR] *Geometry and Robotics.* Springer Lecture Notes in Computer Science **391** (1989).

[O] *Ordered fields and real algebraic geometry.* Contemp. Math. **9**. (1982).

[RAAG] *Real analytic and algebraic geometry.* Springer Lecture Notes in Math. **1420** (1990).

Dans le texte, nous avons invoqué

[G H R S V] Grigor'ev D., Heintz J., Roy M.-F., Solerno P., Vorobjov N. : *Comptage des composantes connexes des ensembles semi-algébriques en temps simplement exponentiel.* C. R. Ac. Sci. Paris **311,** 870-882 (1990).

[HRS] Heintz J., Roy M.-F., Solerno P.: *Sur la complexité du principe de Tarski-Seidenbverg.* Bull. Soc. Math. France **118,** 101-126 (1990).

[L] Lombardi H. : *Nullstelensatz réel effectif et variantes.* Mega 1990. A paraître chez Birkhauser.

[L R] Lombardi H., Roy M.-F. : *Elementary constructive theory of ordered fields.* Mega 1990. A paraître chez Birkhauser.

[M] Méguerditchian I. : *La géométrie du discriminant réel et des polynômes hyperboliques.* Thèse, Université de Rennes I (1991).

[W] Walker R. : *Algebraic curves.* Berlin, Heidelberg, New York : Springer (1978).