Le Théorème de Pila-Wilkie

Blaise Boissonneau

septembre 2018

Réalisé sous la direction de Tamara Servi,
Maître de conférences à l'Université Paris Diderot (Paris 7).

Sommaire

Introduction

La géométrie diophantienne est une branche des mathématiques qui se concentre sur les solutions entières, ou rationelles, de certaines équations. Depuis une vingtaine d'années, la théorie des modèles a eu un écho dans ce domaine, grâce à l'étude de structures dites *o-minimales*, c'est-à-dire minimales pour l'ordre.

Dans une telle structure, les ensembles définissables d'arité 1 sont par définition les unions finies d'intervalles et de points. La connaissance des seuls ensembles d'arité 1 va avoir une heureuse conséquence : les ensembles définissables d'arité quelconque sont exactement les unions finies de *cellules*, les cellules d'arité 1 étant naturellement les intervalles et les points, et les cellules d'arité n étant définies par récurrence : les graphes et les espaces entre deux graphes de fonctions définissables et continues dont le domaine est une cellule d'arité $n-1$ sont des cellules d'arité n. Les cellules vont canoniquement être munies d'une dimension ; de plus, la présence d'un ordre définissable va nous donner une topologie naturelle, pour laquelle les ouverts et les fermés sont définissables.

Dès lors que notre structure o-minimale sera de plus munie d'une structure d'anneau, elle sera automatiquement un corps réel clos ; l'analyse rudimentaire sera alors similaire à l'analyse réelle. De plus, le *théorème de décomposition cellulaire* nous permettra de dire que toute fonction définissable est C^0 et même C^r par parties. Toutes ces raisons ont mené van den Dries à considérer l'o-minimalité comme une forme de topologie modérée, comme définie par Grothendieck, et à l'étudier en détail dans [4].

Le lien avec la géométrie diophantienne apparaît lorsque l'on considère un ensemble $X \subset \mathbb{R}^n$ défini comme l'ensemble des solutions réelles d'une équation à n variables. Étudier les solutions rationnelles de cette équation revient alors à étudier l'ensemble $X(\mathbb{Q}) = X \cap \mathbb{Q}^n$. Un tel ensemble est toujours dénombrable, et n'est définissable que lorsqu'il est fini. Pour remédier à ce problème, on introduit la notion de hauteur d'un point rationnel : pour $\frac{a}{b} \in \mathbb{Q}^*$ avec $\mathrm{pgcd}(a,b) = 1$; on pose $H(\frac{a}{b}) = \max\{|a|, |b|\}$. Par convention on pose $H(0) = 0$. La hauteur d'un point $\langle \frac{a_1}{b_1}, \cdots, \frac{a_n}{b_n} \rangle$ est $\max_{1 \leqslant i \leqslant n}\{H(\frac{a_i}{b_i})\}$. On s'intéresse à $X(\mathbb{Q}, T)$, l'ensemble des points rationnels de X de hauteur $\leqslant T$, qui est toujours fini. La question est alors de savoir comment $N(X, T)$, le cardinal de $X(\mathbb{Q}, T)$, grandit en fonction de T.

On peut aisément trouver des ensembles, même bornés, contenant un grand nombre de points rationnels, par exemple, l'ensemble $(0,1)^n(\mathbb{Q}, T)$ contient $(2\sum_{2 \leqslant i \leqslant T} \varphi(i))^n \gg T^{2n}$, où φ est l'indicatrice d'Euler. En règle générale, les ensembles *semi-algébriques* contiennent un grand nombre de points rationnels. En 2006, Pila et Wilkie [8] ont démontré un théorème disant que si X est définissable dans une structure o-minimale, on a pour $N(X^{\mathrm{trans}}, T)$ une borne en $O(T^\epsilon)$, pour tout $\epsilon > 0$, où X^{trans} est l'ensemble X duquel on exclut les sous-ensembles semi-algébriques. Nous allons donner la démonstration de ce théorème telle qu'elle a été présentée dans l'article de Pila et Wilkie, depuis, Wilkie a donné une autre démonstration dans [17].

Cette démonstration repose sur une utilisation de la compacité et de la saturation pour obtenir entre autre des bornes uniformes, ou pour transformer une collection d'ensembles définissables en une *famille définissable*. Les structures o-minimales sont agréables non seulement du point de vue topologique, mais aussi du point de vue modèle-théorique ; en effet, un corps o-minimal admet des fonctions de choix définissables, ce qui rend possible lesdits arguments de saturation.

L'application de l'o-minimalité à la géométrie diophantienne ne s'arrête pas au théorème de Pila-Wilkie : en 2011, Pila a démontré dans [10] la conjecture d'André-Oort grâce à des méthodes similaires. Il est probable que d'autres résultats de théorie des nombres seront obtenus par application de l'o-minimalité. Nous nous contenterons ici d'étudier deux applications du théorème de Pila-Wilkie comme exemples de résultats obtenus par cette méthode.

1 Résultats d'o-minimalité

L'objectif de cette partie est d'énoncer les résultats classiques d'o-minimalité et de théorie des modèles utiles pour comprendre et démontrer le théorème de Pila-Wilkie. Les concepts de base et les théorèmes classiques de théorie des modèles qui ne sont pas énoncés ici se trouvent par exemple dans [3].

1.1 Définitions et exemples

Dans cette partie on se donne un langage du premier ordre $\mathcal{L}$.

Définition 1.1.1 (o-minimalité)**.** Une $\mathcal{L}$-structure M est dite o-minimale si M définit une relation d'ordre totale et si les ensembles définissables dans M sont exactements les unions finies d'intervalles ouverts et de points.

Comme nous l'allons voir, les structures o-minimales ont de nombreuses propriétés rendant leur étude agréable, particulièrement lorsque M est un anneau ; par exemple lorsque M est le corps $\mathbb{R}$ muni d'une structure bien choisie. Nous allons exposer quelques exemples de structures o-minimales.

Théorème 1.1.2. *Soit $\mathcal{L}_{anneaux} = \{0, 1, +, -, \cdot\}$ le langage des anneaux, alors $\mathbb{R}$, considéré comme une $\mathcal{L}_{anneaux}$-structure, est o-minimal.*

Démonstration. L'ordre canonique sur $\mathbb{R}$ est définissable par la $\mathcal{L}_{\text{anneaux}}$-formule $\phi(x, y) : \exists z(x - y = z^2)$. On voit bien que $\phi(x, y)$ est vérifiée seulement par les couples tels que $x \geqslant y$.

On sait d'autre part que $\mathbb{R}$, considéré comme une $\mathcal{L}_{\text{anneaux}} \cup \{<\}$-structure élimine les quantificateurs (théorème de Tarski-Seidenberg, voir [14], pages 52 à 54).

Par conséquent les seuls ensembles définissables de $\mathbb{R}$ sont ceux définis par des $\mathcal{L}_{\text{anneaux}} \cup \{<\}$-formules sans quantificateurs, c'est-à-dire des conjonctions et disjonctions d'équations et inéquations polynômiales, ce qui donne des unions finies d'intervalles et de points. □

Le fait que le corps ordonné $\mathbb{R}$ est o-minimal est un bon point de départ. Pourtant, certaines fonctions classiques comme l'exponentielle ne sont pas définissables dans cette structure. On peut se demander s'il existe des structures plus riches sur $\mathbb{R}$ qui sont elles aussi o-minimales.

On aimerait ajouter des fonctions analytiques à notre structure, cependant, celles-ci peuvent poser des problèmes : la fonction sinus par exemple définit via l'équation $sin(x) = 0$ un ensemble contenant une infinité de points isolés. On peut contourner ce problème en restreignant les fonctions analytiques à la boîte unité fermée $[-1, 1]^n$: on note $\mathbb{R}_{\text{an}}$ la structure de corps $\mathbb{R}$ munie de toutes les fonctions analytiques restreintes. On a alors le résultat suivant :

Théorème 1.1.3. *$\mathbb{R}_{an}$ est o-minimale.*

Ce résultat est une reformulation d'un théorème de Gabriélov, dans [5].

D'autre part, certaines fonctions analytiques, même non-restreintes, ne créent pas d'entrave à l'o-minimalité. Ce sont les fonctions pfaffiennes, dont l'exemple le plus évident est la fonction exponentielle. Wilkie a démontré dans [6] que $\mathbb{R}_{\mathrm{Pfaff}}$, c'est-à-dire le corps $\mathbb{R}$ muni de toutes les fonctions pfaffiennes, est une structure o-minimale. On en déduit :

Théorème 1.1.4. *$\mathbb{R}_{exp}$ est o-minimale.*

En général, deux structures o-minimale sur le même ensemble n'ont pas de raison d'être compatibles, autrement dit le fait que $\mathbb{R}_{\mathrm{an}}$ et $\mathbb{R}_{\mathrm{exp}}$ sont o-minimales ne garantit pas l'o-minimalité de $\mathbb{R}_{\mathrm{an,exp}}$. Van den Dries et Miller, en se basant sur la démonstration de Wilkie, ont démontré en 1994 dans [15] :

Théorème 1.1.5. *$\mathbb{R}_{an,exp}$ est o-minimale.*

Les exemples que nous avons donnés sont uniquement des structures sur le corps $\mathbb{R}$. Un résultat de Julia Robinson dans [12] est que $\mathbb{Q}$, en tant que corps ordonné, définit $\mathbb{Z}$; il n'y a donc pas de structure o-minimale sur le corps $\mathbb{Q}$. Comme nous le verrons dans la partie suivante, les structures o-minimales sont toujours sur des corps réels clos, l'o-minimalité est donc une théorie pertinente pour étudier les corps réels clos.

1.2 À propos des corps réels clos

Dans cette partie $\mathcal{L}$ désigne un langage du premier ordre contenant au moins $\{0, 1, +, -, \cdot, <\}$.

Définition 1.2.1 (Corps réel clos)**.** On dit qu'une $\mathcal{L}$-structure R est un corps réel clos si elle est un corps, si la relation d'ordre $<$ est compatible avec sa structure de corps et si pour chaque polynôme $P \in R[X]$ et chaque $a, b \in R$ avec $P(a) < 0 < P(b)$, on a $\exists c \in (a, b)$ tel que $P(c) = 0$.

On munit un corps réel clos de la topologie de l'ordre, engendrée par les ouverts de la forme (a, b), $(-\infty, a)$ et $(b, +\infty)$, pour chaque $a, b \in R$. Dans cette topologie le fait d'être ouvert ou fermé est exprimable par une $\mathcal{L}$-formule, et l'intérieur et l'adhérence d'un ensemble définissable sont définissables.

Comme on le verra dans cette partie, les corps réels clos ont des propriétés semblables à celle de $\mathbb{R}$. Le théorème suivant justifie l'intérêt que nous portons à ces corps :

Théorème 1.2.2. *Soit R une $\mathcal{L}$-structure qui soit aussi un anneau ordonné. Si R est o-minimale, alors R est un corps réel clos.*

Démonstration. Nous allons résumer la preuve donnée dans [4], chapitre 1 : tout d'abord, on montre que tout élément de $R^{\times}$ admet un inverse multiplicatif, en se basant sur un lemme disant que dans un groupe ordonné o-minimal, les seuls sous-groupes définissables sont le groupe trivial ou le groupe tout entier. Ainsi pour $r \in R^\times$, le groupe additif rR est définissable et o-minimal, il est donc égal à R tout entier, autrement dit r est inversible.

Ensuite, puisque $R_{\geqslant 0} = \{r \in R \mid r \geqslant 0\}$ est un groupe multiplicatif ordonné o-minimal, on sait que $Z(R_{\geqslant 0}) = R_{\geqslant 0}$, autrement dit la multiplication est commutative sur $R_{\geqslant 0}$, et par conséquent sur R tout entier. R est donc bien un corps.

Enfin on montre que, dans une structure o-minimale, l'image d'un ensemble définissablement connecté (c'est-à-dire un ensemble X définissable qui n'est pas l'union de deux ouverts relatifs à X disjoints et définissables) par une fonction définissable et continue est définissablement connectée. En particulier, cela signifie que l'image de $[a, b]$ par une fonction polynômiale (et donc définissable et continue) $P : [a, b] \to R$ est un intervalle contenant $P(a)$ et $P(b)$, donc contenant l'intervalle $[P(a), P(b)]$, lequel contient 0. □

Désormais nous allons lister certaines propriétés des corps réels clos sans les démontrer, leur démonstration étant similaire à celle dans $\mathbb{R}$.

Proposition 1.2.3. *Soit R une $\mathcal{L}$-structure qui soit aussi un corps réel clos. On a les propriétés suivantes :*

bornes atteintes *Soient $A \subset R^m$ compact (fermé et borné) et $f : A \to R^n$ définissable et continue, alors elle admet un maximum et atteint ce maximum en un point de A.*

limite aux bords *Soient $a, b \in R$, $a < b$ et $f : (a, b) \to R^n$ définissable et continue, alors f admet une limite (qui peut être $\pm\infty$) en a^+ et en b^-.*

accroissements finis *Soient $a, b \in R$, $a < b$ et $f :[a, b] \to R^n$ définissable, continue et dérivable, alors $\exists c \in (a, b)$ tel que $\frac{f(b)-f(a)}{b-a} = f'(c)$.*

Enfin, le théorème suivant, qui est une version plus forte de la décomposition cellulaire en arité 1, nous sera utile dans la démonstration du théorème de Pila-Wilkie :

Théorème 1.2.4 (monotonicité)**.** *Soit $f : (a, b) \to R^n$ définissable, alors on peut trouver $a_0 = a < a_1 < \cdots < a_k < a_{k+1} = b$ tels que f soit monotone sur (a_i, a_{i+1}), pour $0 \leqslant i \leqslant k$.*

La démonstration se trouve dans [4], chapitre 9.

1.3 Décomposition cellulaire et régularité par parties

Dans un contexte o-minimal, on sait par définition que les sous-ensembles du domaine de la structure définissables dans la structure sont les unions finies d'intervalles et de points. Les ensembles définissables en dimension plus grandes sont quant à eux les unions finies de cellules, les cellules étant définies par récurrence comme nous le verrons.

Dans cette partie et dans la partie 1.4, $\mathcal{L}$ est un langage du premier ordre qui contient $\{0, 1, +, -, \cdot, <\}$ et R est une $\mathcal{L}$-structure o-minimale et un anneau ordonné, donc un corps réel clos.

Définition 1.3.1 (Cellules)**.** Les cellules de R^n sont définies par récurrence sur n, les cellules de R étant les intervalles et les points. Désormais soient $n \geqslant 1$, $X \subset R^n$ une cellule, et $f, g : X \to R$ deux fonctions définissables et continues. Les cellules de R^{n+1} sont exactements les ensembles de la forme :

— Γ_f, le graphe de f.

— $(-\infty, f) = \{(x, y) \in X \times R \mid y < f(x)\}$ et (f, ∞) défini de manière similaire.

— Enfin, sous l'hypothèse que $f < g$ sur X, $(f, g) = \{\langle x, y\rangle \in X \times R \mid f(x) < y < g(x)\}$.

On peut définir de la même manière les cellules C^r en exigeant dans la définition que les fonctions f et g soient C^r.

Notons que les notions de continuités et dérivabilités sont exprimables par des $\mathcal{L}$-formules.

Théorème 1.3.2 (Décomposition Cellulaire)**.** *Soient $m \geqslant 1$, $r \geqslant 0$. On a les deux résultats suivants :*

(I) Quels que soient $k \geqslant 1$ et $A_1, \cdots, A_k \subset R^m$ définissables, il existe une partition de R^m en un nombre fini de cellules C^r qui sont telles que pour chaque A_i, chaque cellule est soit disjointe soit incluse dans A_i.

(II) Quelle que soient $A \subset R^m$ et $f : A \to R^n$ définissable, il existe une partition de A en un nombre fini de cellules C^r telle que f soit C^r sur chacune de ces cellules.

La preuve se fait séparément dans le cas C^0 et dans le cas C^r, ce dernier s'appuyant sur le premier. Dans les deux cas, on simplifie en prenant $n = 1$, car lorsque $n > 1$ on trouve une décomposition convenant pour chacune des fonctions coordonnées de f, et l'ensemble de leurs intersections (qui sont encore des cellules) convient pour f. Ensuite on procède par récurrence sur m.

Ici nous admettrons ce résultat, car la preuve est longue ; on renvoie vers [4], chapitres 9 et 13 pour les démonstrations des décompositions cellulaires C^0 et C^r.

Nous allons donner tout de suite un corollaire dans le cas $m = 1$:

Corollaire 1.3.3. *Soit $f : (a, b) \to R^n$ définissable, alors f admet une limite (qui peut être $\pm\infty$) en a^+, en b^-, et pour tout $c \in (a, b)$, f admet une limite en c^+ et en c^-.*

Démonstration. Par décomposition cellulaire, on a un ensemble d'intervalles et de points disjoints qui recouvrent (a, b) et tels que f soit C^0 sur chaque intervalle (et sur chaque point). On les numérote $a_0 = a < a_1 < \cdots < a_k < a_{k+1} = b$. Puisque f est C^0 sur chaque intervalle $(a_i, a_{i+1})_{0 \leqslant i \leqslant k}$, elle admet une limite en a_i^+ et en a_i^- (proposition 1.2.3), et naturellement pour chaque point $x \in (a_i, a_{i+1})$, f admet une limite à droite comme à gauche, celles-ci sont même égales par définition de la continuité. □

1.4 Dimension

Définition 1.4.1 (Dimension)**.** On définit la dimension des cellules par récurrence lors de leur construction. Dans R, les intervalles sont de dimension 1 et les points de dimension 0. Si désormais on a $X \subset R^m$ une cellule de dimension l et $f, g : X \to R$ deux fonctions définissables et C^r :

— Γ_f est une cellule de dimension l,

— $(-\infty, f)$, (f, ∞) et (f, g) sont des cellules de dimension $l + 1$.

On définit la dimension d'un ensemble définissable comme le maximum de la dimension des cellules (C^0 ou C^r, le résultat est le même) incluses dans cet ensemble.

On peut alors démontrer le théorème suivant :

Théorème 1.4.2. *Soient $r \geqslant 0$, $A \subset R^m$ ouvert et $f : A \to R^n$ définissable. Alors il existe un ensemble $B \subset A$ ouvert et définissable tel que f soit C^r sur B et $\dim(A - B) < m$.*

Démonstration. Par décomposition cellulaire C^r, on partitionne A en un nombre fini de cellules sur lesquelles f est C^r. On prend pour B l'union de l'intérieur de ces cellules. Les cellules et l'intérieur sont définissables, donc B est définissable, f est C^r sur B, et enfin $\dim(A - B) < m$; dans le cas contraire, on aurait une cellule de dimension m, notament d'intérieur non-vide, qui ne rencontre l'intérieur d'aucune cellule de notre décomposition ; c'est impossible car nous avons une décomposition finie, et que l'on ne peut pas recouvrir une cellule de dimension l avec un nombre fini de cellules de dimension $< l$: il y a donc forcément une cellule de A de dimension m qui rencontre la cellule extérieure à B, leurs intérieurs ne sont donc pas disjoints. $\square$

1.5 Fonctions de choix définissables

Pour une certaine $\mathcal{L}$-formule $\phi(x, y)$, on aimerait prendre une fonction f telle que pour y fixé, s'il y a au moins un x tel que $\phi(x, y)$ soit vraie, alors $\phi(f(y), y)$ est vraie, c'est-à-dire que f choisit un x pour chaque y. La question qui se pose alors est peut-on prendre f définissable ?

Définition 1.5.1. Soit $\mathcal{L}$ un langage, on dit qu'une $\mathcal{L}$-structure M admet des fonctions de choix (ou fonctions de Skolem) définissables si pour chaque $\mathcal{L}$-formule $\phi(x, y)$ à paramètres dans $A \subset M$ avec $x \in M^n$ et $y \in M^m$, il existe une fonction $f : M^m \to M^n$ A-définissable telle que :

$$M \vDash \forall y(\exists x \phi(x, y) \to \phi(f(y), y))$$

De manière équivalente, M admet des fonctions de choix définissables si pour chaque $Z \subset M^n \times M^m$ A-définissable, on peut trouver une fonction $f : M^m \to M^n$ A-définissable telle que pour chaque $y \in R^m$ fixé, si $Z_y = \{x \in M^n \mid \langle x, y\rangle \in Z\}$ est non-vide, alors $f(y) \in Z_y$.

Remarque. Dans le cas où la seule variable est $x \in M^n$, la fonction f devient une fonction d'arité 0, autrement dit une constante. Le théorème se reformule alors en disant qu'il existe $c \in M$ tel que $\{c\}$ est A-définissable et $M \vDash \exists x \phi(x) \to \phi(c)$.

Théorème 1.5.2. *Soit R une $\mathcal{L}$-structure o-minimale sur un corps, alors R admet des fonctions de choix définissables.*

Démonstration. On travaille à m fixé par récurrence sur n. Si $n = 1$, alors pour y fixé, $Z_y \subset R$ est A-définissable, donc est une union finie d'intervalles et de points. Le bord de Z_y est un ensemble fini A-définissable. On définit $f(y)$ comme suit :

— Si $Z_y = R$ ou $\emptyset$, on pose $f(y) = 0$.

Sinon, on note a le minimum du bord de Z_y, qui est alors non-vide, et :

— Si $a \in Z_y$, on pose $f(y) = a$.

— Si $a \notin Z_y$ et $a - 1 \in Z_y$, on pose $f(y) = a - 1$.

— Si $a \notin Z_y$, $a - 1 \notin Z_y$ et $a + 1 \in Z_y$, on pose $f(y) = a + 1$.

— Si aucune de ces quantités ne convient, alors a est forcément le bord d'un intervalle de la forme (a, b) avec $b \neq \infty$. On pose alors $f(y) = \frac{a+b}{2}$.

Ainsi, f est une fonction de choix définissable.

Désormais $n \geqslant 1$ et l'on suppose que le théorème est vrai pour tout sous-ensemble définissable de $R^n \times R^m$. Prenons alors $Z \subset R^{n+1} \times R^m$, $y \in R^m$ fixé. On définit $A_y = \{a \in R \mid \exists x \in R^n \langle x, a\rangle \in Z_y\}$. L'ensemble $A = \{\langle x, y\rangle \mid x \in A_y\} \subset R \times R^m$ est définissable, par le cas $n = 1$ on a $h : R^m \to R$ définissable telle que $h(y) \in A_y$ pour chaque A_y non vide.

On définit ensuite $B_y = \{b \in R^n \mid \langle b, h(y)\rangle \in Z_y\}$. L'ensemble $B = \{\langle x, y\rangle \mid x \in B_y\} \subset R^n \times R^m$ est définissable. Par l'hypothèse de récurrence, on a une fonction définissable $g : R^m \to R^n$ telle que $g(y) \in B_y$ pour chaque B_y non vide.

Alors la fonction $f : R^m \to R^{n+1}$ définie par $f(y) = \langle g(y), h(y)\rangle$ est définissable et telle que $f(y) \in Z_y$ pour chaque Z_y non-vide. □

1.6 $\aleph_0$-saturation

Dans cette partie on s'éloigne du domaine spécifique de l'o-minimalité pour parler de la saturation d'une structure, nous verrons ce que cela implique lorsque ce modèle est un corps ordonné.

Définition 1.6.1. Soient $\mathcal{L}$ un langage, M une $\mathcal{L}$-structure et $p(x)$ un ensemble de $\mathcal{L}$-formules en la variable x et à paramètres dans $A \subset M$. On rappelle le vocabulaire usuel :

— On dit que $p(x)$ est réalisé dans M s'il existe un certain $a \in M$ tel que pour chaque $\phi(x) \in p(x)$, $M \vDash \phi(a)$. On dit aussi que a réalise p.

— On dit que $p(x)$ est un type (à paramètres dans A) s'il est finiment satisfaisable dans M, c'est-à-dire si chaque sous-ensemble fini de $p(x)$ est réalisé dans M.

— On dit que $p(x)$ est un type complet s'il est maximal, c'est-à-dire que pour chaque formule $\phi(x)$ à paramètres dans A, si $p(x) \cup \{\phi(x)\}$ est finiment satisfaisble, alors $\phi(x) \in p(x)$. Un type incomplet est appelé type partiel.

— On définit de même les n-types en les variables $x_1, \cdots, x_n$.

Remarque. La terminologie n'est pas toujours la même selon les auteurs, certains auteurs appelant "type" ce que nous appelons ici "types complets". La terminologie que nous avons adoptée dans cette définition est la même que dans [3].

En général, finiment satisfaisable ne signifie pas réalisé. Pour s'en convaincre, on peut regarder l'exemple suivant dans $\mathbb{R}$ avec sa structure de corps :

$$p(x) = \{\phi_n(x) : x > n \mid n \in \mathbb{N}\}$$

Dans $\mathbb{R}$, $p(x)$ est finiment satisfaisable, mais n'est pas réalisé : si a réalisait p, alors a serait supérieur à tous les entiers, ce qui est impossible dans $\mathbb{R}$. On peut pourtant ajouter un élément infini dans $\mathbb{R}$ et obtenir ainsi le corps des "hyperréels", dans lequel $p(x)$ est réalisé. On peut se demander alors si l'on peut toujours réaliser un type dans une extension bien choisie, voire s'il existe une extension dans laquelle tous les types sont réalisés.

Définition 1.6.2. Soient $\mathcal{L}$ un langage et M une $\mathcal{L}$-structure. On dit que M est $\aleph_0$-saturée si tous les types à paramètres dans un ensemble fini $A \subset M$ sont réalisés dans M.

Remarque. Là encore, deux notations cohabitent, certains auteurs préférant parler d'ω-saturation. Nous noterons $\aleph_0$-saturation afin d'avoir la même notation que Pila et Wilkie dans [8].

Notons aussi que dans une structure $\aleph_0$-saturée, tous les n-types à paramètres finis sont réalisés dans M. En effet, on note $x = \langle x_1, \cdots, x_n \rangle$, et on considère le n-type $p(x, y)$. Par récurrence sur n, le $(n-1)$-type $q(x) = \{\exists y \phi(x, y) \mid \phi \in p\}$ est réalisé dans M. Si a réalise q, alors on considère le type $r(y) = \{\phi(a, y) \mid \phi \in p\}$ à paramètres finis (les paramètres de p auxquels on ajoute a). Si b réalise r, alors $\langle a, b \rangle$ réalise p.

On pourrait croire que la saturation est une propriété rare. En vérité, on peut toujours trouver une extension élémentaire $\aleph_0$-saturée :

Théorème 1.6.3. *Soient $\mathcal{L}$ un langage et M une $\mathcal{L}$-structure, il existe toujours une extension élémentaire $M^* \succcurlyeq M$ telle que M^* soit $\aleph_0$-saturée.*

Démonstration. La preuve se déroule en 2 étapes : d'abord, montrer par compacité que chaque type est réalisable dans une extension élémentaire ; ensuite, lister tous les types à paramètres finis, puis créer à l'étape i une extension élémentaire réalisant les i premiers types. Le principal problème est que cette liste n'est en général ni finie ni même dénombrable, il faut donc faire prendre des valeurs transfinies à i. Les détails se trouvent dans [3], leçon 10. $\square$

Dans la démonstration des théorèmes de (re)paramétrisation (voir 2.3), nous nous placerons dans une extension $\aleph_0$-saturée d'un corps réel clos. Ceci nous force à distinguer les ensembles bornés par un nombre quelconque et les ensembles bornés par un entier, et ce pour la raison suivante :

Proposition 1.6.4. *Soit R une structure $\aleph_0$-saturée sur un corps ordonné, alors R est non-archimédien ; c'est-à-dire qu'il existe un élément plus grand que chaque entier (où l'on identifie un entier à la somme $1 + 1 + \cdots + 1$ correspondante).*

Démonstration. On considère derechef le type $p(x) = \{\phi_n(x) : x > n \mid n \in \mathbb{N}\}$. p est finiment satisfaisable, et comme l'on écrit $n \in \mathbb{N}$ comme une somme de 1, p est à paramètres dans $\{1\}$ (voir dans $\emptyset$ si le langage contient 1). p est alors réalisé dans R par $\aleph_0$-saturation. Si $a \in R$ réalise p, alors $\forall n \in \mathbb{N}$, $a > n$. $\square$

La saturation sera utilisée à plusieurs reprises dans la démonstration des théorèmes de (re)paramétrisation, pour assurer l'uniformité de bornes. Pour n'alourdir ni la démonstration ni cette partie, les détails sont rassemblés dans l'annexe B.

2 Le théorème de Pila-Wilkie

Nous allons dans cette partie donner la démonstration du théorème de Pila-Wilkie en nous basant sur l'article original [8]. Ce théorème fournit une borne pour le nombre de points rationnels contenus dans un ensemble définissable, en fonction de leur hauteur. Il ne concerne que la partie dite transcendante de l'ensemble, car la partie algébrique contient souvent beaucoup de points rationnels.

2.1 Résultats principaux

Dans cette partie, on fixe un langage $\mathcal{L} \supset \mathcal{L}_{\text{anneaux}} \cup \{<\}$, ainsi qu'une structure o-minimale sur $\mathbb{R}$. Définissable signifiera ici définissable dans cette structure, sauf contre-indication.

Soit $X \subset \mathbb{R}^n$. On introduit les définitions suivantes :

Définition 2.1.1. — On dit que X est semi-algébrique si X est définissable par des $\mathcal{L}_{\text{anneaux}} \cup \{<\}$-formules, autrement dit X est une union finie d'intersections finies de lieux d'annulation ou de positivité de polynômes.

— On appelle partie algébrique de X et on note X^{alg} l'union de tous les ensembles semi-algébriques de dimension $\geqslant 1$ contenus dans X. On note $X^{\text{trans}} = X \setminus X^{\text{alg}}$ la partie transcendante de X.

Notons que X^{alg}, bien qu'étant l'union d'ensembles définissables, n'est en général pas semi-algébrique ou définissable, même lorsque X est définissable. Par exemple, si $X = \{\langle x, y, z\rangle \in \mathbb{R}^3 \mid z = x^y,\ x, y \in [1, 2]\}$ (définissable dans $\mathbb{R}_{\exp}$), alors chaque $y = \frac{a}{b}$ rationnel fournit l'ensemble $\{x^a = z^b\}$ qui est semi-algébrique, leur union n'est en revanche pas définissable.

Les ensembles semi-algébriques peuvent contenir un grand nombre de points rationnels. Quant à la partie transcendante, notre objectif est de montrer qu'elle contient peu de points rationnels, dans le sens suivant :

Théorème 2.1.2 (Pila-Wilkie). *Soient $X \subset \mathbb{R}^n$ définissable et $\epsilon > 0$, alors il existe $c = c(X, \epsilon) > 0$ telle que :*

$$N(X^{trans}, T) \leqslant cT^{\epsilon}$$

La démonstration se fera par récurrence sur la dimension de X, cependant nous avons besoin d'une certaine uniformité des constantes c pour la démonstration.

Soit $Z \subset \mathbb{R}^n \times \mathbb{R}^m$, pour $y \in \mathbb{R}^m$ on définit $Z_y = \{x \in \mathbb{R}^n \mid \langle x, y\rangle \in Z\}$, la fibre au-dessus de y. On pose $Y = \{y \in \mathbb{R}^m \mid \exists x \in \mathbb{R}^n \text{ tel que } \langle x, y\rangle \in Z\}$, et on dit que la famille $Z = \{Z_y\}_{y \in Y}$ est une famille définissable si l'ensemble Z est définissable dans $\mathbb{R}^n \times \mathbb{R}^m$. On peut alors reformuler le théorème de manière uniforme :

Théorème 2.1.3 (Version uniforme). *Soient $Z \subset \mathbb{R}^n \times \mathbb{R}^m$ une famille définissable et $\epsilon > 0$, alors il existe $c = c(Z, \epsilon) > 0$ telle que $\forall y \in \mathbb{R}^m$:*

$$N(Z_y, T) \leqslant cT^{\epsilon}$$

On a vu qu'en général X^{alg} n'est pas définissable, donc X^{trans} non plus. Plutôt que d'enlever toute la partie algébrique, on peut trouver un ensemble définissable inclus dans X^{alg} en dehors duquel il y a peu de points rationnels. Le version que l'on va démontrer est alors la suivante :

Théorème 2.1.4 (Version uniforme et définissable)**.** *Soient $Z \subset \mathbb{R}^n \times \mathbb{R}^m$ une famille définissable et $\epsilon > 0$, alors et il existe $c = c(Z, \epsilon) > 0$ et une famille définissable $W = W(Z, \epsilon) \subset Z$ telles que $\forall y \in \mathbb{R}^m$:*

$$W_y \subset Z_y^{alg} \text{ et } N(Z_y \setminus W_y, T) \leqslant cT^\epsilon$$

2.2 Déroulement de la preuve

La première étape de la preuve est d'établir que les points rationnels en question se trouvent dans un petit nombre (c'est-à-dire de la forme $O(T^\epsilon)$) d'hypersurfaces. Ensuite, on démontrera le théorème 2.1.4 pour une famille, construite à partir de Z, dont les fibres sont paramétrisées par y ainsi que par un nouveau paramètre t qui représente le vecteur des coordonnées définissant une hypersurface. Cette famille est telle que les points au voisinage desquels la fibre est de dimension maximale tombent dans la partie algébrique et sont donc exclus. Pour les autres, on conclut par récurrence sur la dimension.

On relie alors les fibres de Z à celles de cette famille grâce aux hypersurfaces : on sait que tous les points rationnels de hateur $\leqslant T$ d'une fibre de Z tombent dans un certain nombre, disons N, d'hypersurfaces. Chacune de ces hypersurfaces correspond à une fibre de la famille précédente, dans laquelle il y a M points rationnels de hateur $\leqslant T$ (en dehors d'un certain W). Au total il y a donc NM points rationnels de hauteur $\leqslant T$ dans une fibre de Z. Puisqu'on sait qu'il existe une borne de type $O(T^{\epsilon/2})$ pour le nombre N d'hypersurfaces et pour le nombre M de points rationnels, le théorème est finalement démontré pour Z.

Le point de départ afin d'établir le résultat sur les hypersurfaces est la proposition suivante que l'on trouve dans [9] :

Proposition 2.2.1. *Soient $k, n, d \in \mathbb{N}$ avec $k < n$ et $d \geqslant 1$, alors il existe un entier positif $r = r(k, n, d)$ et deux réels positifs $C = C(k, n, d)$ et $\epsilon = \epsilon(k, n, d)$ avec la propriété suivante :*

Pour toute fonction $\phi : (0, 1)^k \to \mathbb{R}^n$ de classe C^r dont toutes les dérivées d'ordre $\leqslant r$ sont bornées par 1, si l'on note $X = \mathrm{Im}(\phi)$, alors $X(\mathbb{Q}, T)$ est contenu dans au plus CT^ϵ hypersurfaces de degré $\leqslant d$. De plus, la quantité $\epsilon(k, n, d)$ tend vers 0 lorsque d tend vers l'infini.

Remarque. Par là on entend que lorsque l'on trouve un recouvrement de $X(\mathbb{Q}, T)$ par un grand nombre d'hypersurfaces, on peut toujours en trouver $N \leqslant CT^\epsilon$ parmi celles-ci dont l'union recouvre aussi $X(\mathbb{Q}, T)$.

Nous ne donnerons pas de preuve de ce résultat ici, nous nous contenterons d'étudier dans l'annexe A un cas en petite dimension pour avoir une représentation géométrique plus intuitive de la signification du résultat.

Cette proposition n'est pas tout à fait le résultat que l'on veut, d'abord parce qu'elle concerne seulement les ensembles X qui sont images de fonctions suffisament régulières, et ensuite parce qu'elle nous donne un ϵ qui dépend de d. Nous allons étendre ce résultat à tout X, tout ϵ et aux familles définissables :

Lemme 2.2.2 (Lemme principal)**.** *Soient $Z \subset (0,1)^n \times \mathbb{R}^m$ dont les fibres sont de dimension $\leqslant k < n$, et $\epsilon > 0$. Alors $\exists d = d(k,n,\epsilon) \in \mathbb{N}$ et $K = K(Z,\epsilon) > 0$ telles que $\forall y \in \mathbb{R}^m$ et $\forall T \geqslant 1$, $Z_y(\mathbb{Q},T)$ soit contenu dans l'union d'au plus KT^ϵ hypersurfaces de degré $\leqslant d$.*

Démonstration. On fixe d, la proposition précédente nous donne alors $\epsilon(l,n,d)$ pour chaque $l \leqslant k < n$ (car la dimension d'une fibre peut être plus petite que k). Cette quantité tend vers 0 quand d tends vers l'infini, on prend alors d suffisament grand pour avoir $\epsilon(l,n,d) \leqslant \epsilon$.

On recouvre ensuite chaque fibre Z_y par un nombre fini N, qui ne dépend pas de y, de fonctions $\phi : (0,1)^k \to \mathbb{R}^n$ dont les dérivées d'ordre $\leqslant r(k,n,d)$ sont bornées par 1. C'est possible grâce au théorème de paramétrisation que nous démontrerons dans la suite, et particulièrement grâce au corollaire 2.6.2. Les points rationnels de hauteur $\leqslant T$ de l'image de chacune des fonctions ϕ sont contenus dans au plus $C(\dim(Z_y),n,d)T^{\epsilon(\dim(Z_y),n,d)} \leqslant CT^\epsilon$ hypersurfaces de degré $\leqslant d$, avec $C = \max_{1 \leqslant l \leqslant k} C(l,n,d)$. Par conséquent les points rationnels de hauteur $\leqslant T$ de Z_y sont contenus dans au plus NCT^ϵ hypersurfaces de degré $\leqslant d$ et le lemme est démontré avec $K = NC$. □

Les parties 2.3 à 2.6 sont consacrées à la démonstration des théorèmes de paramétrisations sur lesquels repose ce résultat. La partie 2.7 applique le lemme 2.2.2 comme nous l'avons vu afin de terminer la preuve du théorème 2.1.4.

2.3 Théorèmes de paramétrisation

Dans les parties suivantes (jusqu'à 2.6) on fixe une $\mathcal{L}$-structure o-minimale sur un corps réel clos M. La raison pour laquelle on ne travaille pas sur $\mathbb{R}$ est que l'on a besoin que M soit $\aleph_0$-saturée pour démontrer le théorèmes de (re)paramétrisation. Le corollaire 2.6.2 est une conséquence de ces théorèmes, et s'exprime entièrement par des formules du premier ordre ; par conséquent puisqu'il est vrai dans une extension élémentaire $\aleph_0$-saturée de $\mathbb{R}$, il est vrai dans $\mathbb{R}$.

On dit que $x \in M$ est fini s'il existe $c \in \mathbb{N}$ tel que $x \leqslant c$, où l'on suppose que $\mathbb{Q}$ est identifié au sous-corps premier de M. On dit que $X \subset M^n$ est fortement borné s'il est borné par un certain $c \in \mathbb{N}$. Une fonction est fortement bornée si son graphe l'est ; notamment si $F : X \to Y$ est fortement bornée alors X et Y sont fortement bornés.

Définition 2.3.1 (Paramétrisation)**.** Soit $X \subset M^m$ définissable avec $\dim(X) = l$.

— Une paramétrisation partielle de X est une fonction $\phi : (0,1)^l \to X$ définissable.

— Une paramétrisation de X est un ensemble fini S de paramétrisations partielles telles que $\bigcup_{\phi \in S} \mathrm{Im}(\phi) = X$.

— Une r-paramétrisation de X est une paramétrisation S de X telle que chaque $\phi \in S$ est C^r et $\phi^{(\alpha)}$ est fortement bornée pour $\alpha = (\alpha_1, \cdots, \alpha_l) \in \mathbb{N}^l$ avec $|\alpha| = \sum_{i=1}^{m} \alpha_i \leqslant r$.

Remarque. La raison pour laquelle on considère des fonctions fortement bornées plutôt que bornées est que M est non-archimédien, puisqu'il est $\aleph_0$-saturé. À partir d'une fonction dont les dérivées sont bornées par un entier, on peut obtenir des fonctions aux propriétés similaires mais dont les dérivées sont bornées par 1, en divisant et dilatant son domaine un certain nombre (fini) de fois. Ceci serait impossible avec une borne non-finie.

Grâce au théorème de décomposition cellulaire on sait qu'il existe toujours une paramétrisation dont les fonctions sont C^r, mais a priori leur dérivées pourraient ne pas être bornées. On va démontrer le théorème suivant :

Théorème 2.3.2 (Paramétrisation)**.** *Pour $r \in \mathbb{N}$ et pour $X \subset M^m$ définissable et fortement borné, il existe une r-paramétrisation de X.*

Il existe aussi une version pour les fonctions :

Définition 2.3.3 (Reparamétrisation)**.** Soit $F : X \to M^n$ une fonction définissable et fortement bornée. On dit que S est une r-reparamétrisation de F si S est une r-paramétrisation de X telle que $\{F \circ \phi \mid \phi \in S\}$ soit une r-paramétrisation de $\mathrm{Im}(F)$.

Théorème 2.3.4 (Reparamétrisation)**.** *Pour $r \in \mathbb{N}$ et pour $F : X \to M^n$ définissable et fortement bornée, il existe une r-reparamétrisation de F.*

Dans ces théorèmes, les entiers m, l, n, et r interviennent : $X \subset M^m$, $\dim(X) = l$, $F : X \to M^n$, et r est l'entier qui détermine la régularité de la (re)paramétrisation. La démonstration dans son ensemble est une récurrence sur m des deux énoncés à la fois, mais fera intervenir des récurrences sur les autres entiers :

— Dans la partie 2.4 on démontre les théorèmes dans le cas $m = 1$ (et donc $l = 1$). Pour ce faire, on commence par démontrer une version plus forte des théorèmes, avec des propriétés supplémentaires sur les fonctions, dans le cas $n = 1$ et par réccurence sur r. Cette propriété permet d'effectuer une réccurence sur n afin de démontrer les théorèmes dans le cas $m = 1$.

— Dans la partie 2.5 on démontre un lemme permettant de passer d'une fonction dérivable (r fois) par rapport aux m premières variables, à une fonction dérivable par rapport à toutes les variables. Il s'agit d'un lemme clé dans la récurrence sur m.

— Enfin dans la partie 2.6 on effectue la réccurence sur m, ensuite on établit le corollaire que l'on souhaite.

2.4 Cas des fonctions unaires

On se place donc dans le cas $m = l = 1$. Dans un premier temps, on va aussi fixer $n = 1$ et démontrer un résultat plus fort par récurrence sur r ; ensuite nous démontrerons le théorème par récurrence sur n.

Lemme 2.4.1. *Soient $r \geqslant 2$ et $f : (0,1) \to M$ définissable et de classe C^r. On suppose que $f^{(j)}$ est fortement bornée pour $0 \leqslant j \leqslant r-1$ et que $\left|f^{(r)}\right|$ est décroissante. Soit $g : (0,1) \to M$ définie par $g(x) = f(x^2)$, alors $g^{(j)}$ est fortement bornée pour $0 \leqslant j \leqslant r$.*

Démonstration. On a pour $g^{(i)}(x) = \sum_{j=0}^{i} p_{i,j}(x) f^{(j)}(x^2)$ avec $p_{i,j}$ un polynôme à coefficients entiers. Tous les termes de la somme sont bornés par hypothèse, sauf lorsque $i = j = r$. On a alors $p_{r,r}(x) = 2^r x^r$. Par hypothèse fixons c une borne entière de $f^{(r-1)}$ et on suppose qu'il existe x_0 tel que $\left|f^{(r)}(x_0)\right| > \frac{4c}{x_0}$. Par le théorème des accroisements finis, $\exists \xi \in [\frac{x_0}{2}, x_0]$ tel que $f^{(r-1)}(x_0) - f^{(r-1)}(\frac{x_0}{2}) = f^{(r)}(\xi)(x_0 - \frac{x_0}{2})$. Puisque $\left|f^{(r)}\right|$ est décroissante, $\left|f^{(r)}(\xi)\right| \geqslant \left|f^{(r)}(x_0)\right| > \frac{4c}{x_0}$. Ainsi :

$$2c \geqslant \left|f^{(r-1)}(x_0) - f^{(r-1)}(\tfrac{x_0}{2})\right| = \left|f^{(r)}(\xi)(x_0 - \tfrac{x_0}{2})\right| > \tfrac{4c}{x_0}\tfrac{x_0}{2} = 2c$$

Par contradiction, on a alors $\forall x \; f^{(r)}(x) \leqslant \frac{4c}{x}$, et donc :

$$\left|2^r x^r f^{(r)}(x^2)\right| \leqslant 2^{r+2} x^{r-2} c \leqslant 2^{r+2} c$$

Ainsi $g^{(i)}$ est fortement bornée pour $0 \leqslant i \leqslant r$. □

Lemme 2.4.2. *Soit $F : (0,1) \to M$ définissable et fortement bornée. Alors F admet une 1-reparamétrisation S qui est de plus telle que pour $\phi \in S$, au moins une des deux fonctions ϕ et $F \circ \phi$ est un polynôme sur $(0,1)$ avec des coefficients fortement bornés.*

Démonstration. Par décomposition cellulaire, F est C^1 sur (0,1), à l'exception d'un nombre fini de points. On peut alors choisir par o-minimalité $a_0 = 0 < a_1 < \cdots < a_{p+1} = 1$ dans M tels que restreinte à (a_i, a_{i+1}), F soit C^1 et $|F'| \leqslant 1$ ou $|F'| > 1$ (qui sont des formules du premier ordre), et on définira $\phi_i : (0,1) \to M$ pour chaque i :

- Lorsque $|F'| \leqslant 1$, on pose $\phi(x) = (a_{i+1} - a_i)x + a_i$.
- Lorsque $|F'| > 1$, on note $b_i = \lim_{x \to a_i^+} F(x)$ et $b_{i+1} = \lim_{x \to a_{i+1}^-} F(x)$. Sur cet intervalle F est strictement monotone et donc injective, par conséquent on peut poser $\phi(x) = F^{-1}((b_{i+1} - b_i)x + b_i)$.

Dans le premier cas ϕ_i est un polynôme, dans le second cas $F \circ \phi_i$ est un polynôme. En ajoutant les fonctions constantes égales à a_i, on obtient une 1-reparamétrisation de F avec les propriétés voulues. □

Lemme 2.4.3. *Soit $r \geqslant 1$ et soit $F : (0,1) \to M$ définissable et fortement bornée. Alors F admet une r-reparamétrisation S qui est de plus telle que pour $\phi \in S$, ϕ ou $F \circ \phi$ est un polynôme sur $(0,1)$ avec des coefficients fortement bornés.*

Démonstration. La preuve se fait par récurrence sur r, le cas $r = 1$ étant le lemme 2.4.2. Supposons $r \geqslant 2$ et soit S une $(r-1)$-reparamétrisation de F admettant la propriété voulue. On fixe $\phi \in S$ et l'on pose $\{\phi, F \circ \phi\} = \{g, h\}$ où g est un polynôme à coefficients strictement bornés. Ainsi $g^{(i)}$ existe et est bornée pour $0 \leqslant i \leqslant r$, tandis que $h^{(i)}$ existe et est strictement bornée seulement jusqu'à $r-1$. On cherche à appliquer le lemme 2.4.1. Par le théorème 1.2.4, on choisit $a_0 = 0 < a_1 < \cdots < a_{p+1} = 1$ dans M tels que h soit C^r et que $\left|h^{(r)}\right|$ soit monotone sur (a_i, a_{i+1}). On définit alors $\theta_i : (0,1) \to (a_i, a_{i+1})$ par :

$$\theta_i = \begin{cases} (a_{i+1} - a_i)x + a_i & \text{si } \left|h^{(r)}\right| \text{ est décroissante} \\ (a_i - a_{i+1})x + a_{i+1} & \text{si } \left|h^{(r)}\right| \text{ est croissante} \end{cases}$$

$h \circ \theta_i : (0,1) \to M$ est naturellement C^r, et ses dérivées sont fortement bornées jusqu'à $r-1$. De plus, $\left|h^{(r)}\right|$ est décroissante. Si l'on note $\rho : (0,1) \to (0,1)$, $x \to x^2$; alors par le lemme 2.4.1, $h \circ \theta_i \circ \rho$ a des dérivés fortement bornées jusqu'à r. $g \circ \theta \circ \rho$ est toujours polynomiale à coefficients fortement bornés. On pose $\phi' = \phi \circ \theta \circ \rho$, et $S' = \{\phi' \mid \phi \in S\} \cup \{x \to a_i \mid 1 \leqslant i \leqslant p\}$ est une r-reparamétrisation de F ayant la propriété voulue. □

Corollaire 2.4.4. *Soit $X \subset M$ définissable et fortement borné et soit $F : X \to M$, alors F admet une r-reparamétrisation $\forall r \geqslant 1$.*

Démonstration. Par o-minimalité X est une union finie d'intervalles bornés et de points. Il admet donc une r-paramétrisation S par des fonctions linéaires et par des fonctions constantes. Pour chaque fonction ϕ de S, $F \circ \phi : (0,1) \to M$ admet une r-reparamétrisation S_ϕ par le lemme 2.4.3. Alors $S' = \{\phi \circ \psi \mid \psi \in S_\phi,\ \phi \in S\}$ est un r-reparamétrisation de F. □

Il nous reste à traiter le cas $\mathrm{Im}(F) \subset M^n$ pour n quelconque, qui sera démontré par récurrence sur n. Le lemme suivant est établi pour des fonctions m-aires car il sera aussi utilisé par la suite lors de la récurrence sur m pour nous restreindre au cas $n = 1$.

Lemme 2.4.5. *Soit $m, r \geqslant 1$ et on suppose que $\forall l \leqslant m$, $\forall X \subset M^l$ définissable, et $\forall F : X \to M$, il existe une r-reparamétrisation de F.*

Alors $\forall n \geqslant 1$, $\forall l \leqslant m$, $\forall X \subset M^l$ définissable, et $\forall F : X \to M^n$, il existe une r-reparamétrisation de F.

Démonstration. Le résultat tient naturellement pour $n = 1$. Par récurrence, fixons $n \geqslant 2$ et supposons que le résultat soit vrai jusqu'à $n-1$. On considère $G : X \subset M^m \to M^n$ définissable et fortement bornée. Par projection on peut poser $G = \langle F, f \rangle$ avec $\mathrm{Im}(F) \subset M^{n-1}$ et $\mathrm{Im}(f) \subset M$. On sait alors qu'il existe une r-reparamétrisation S de F.

Soit $\phi \in S$, on a $\phi : (0,1)^{\dim(X)} \to X$ et ainsi $f \circ \phi : (0,1)^{\dim(X)} \to M$ admet une r-reparamétrisation S_ϕ. Alors $S' = \{\phi \circ \psi \mid \psi \in S_\phi, \phi \in S\}$ est une r-reparamétrisation de G. $\square$

En appliquant le lemme 2.4.5 au cas $m = 1$, on obtient :

Corollaire 2.4.6. *Soit $n \geqslant 1$, $X \subset M$ et $F : X \to M^n$ définissable et fortement bornée, alors $\forall r \geqslant 1$, F admet une r-reparamétrisation.*

Avec ce corollaire le cas $m = l = 1$ est démontré pour r et n quelconque. La partie suivante étend le résultat à toute fonction par une récurrence sur m.

2.5 Étape de récurrence

On souhaite démontrer le théorème par réccurence sur m. Lorsque l'on traitera le cas d'un fonction F d'arité $m+1$, on travaillera avec la variable x_{m+1} fixée, et on reparamétrisera la fonction $F_u : x \in (0,1)^m \to F(x,u)$. Ainsi on obtient un certain nombre de fonctions $F_u \circ \phi$ qui sont continues et dérivables à dérivées fortement bornées par rapport aux m premières variables. À l'aide de la décomposition cellulaire et d'arguments de saturation, Pila et Wilkie démontrent que sur un certain sous-ensemble *générique* de son domaine, on peut reparamétriser une telle fonction par rapport à la dernière variable. Ce résultat se trouve dans le corollaire 2.5.3, et l'objectif de cette partie est de le démontrer, afin de pouvoir l'utiliser pour mener à bien la récurrence dans la partie suivante.

On fixe r et n dans $\mathbb{N}^*$. On considère une famille définissable de fonctions $(F_t : (0,1) \to (0,1)^n)_{t \in (0,1)}$, où pour t fixé F_t est de classe C^r et $F_t^{(i)}$ est fortement bornée pour $i = 1, \cdots, r$. Par un argument de saturation (voir l'annexe B.i), on a une borne uniforme $c \in \mathbb{N}$. On définit F_0 par $F_0(x) = \lim_{t \to 0^+} F_t(x)$. Cette limite existe par o-minimalité : puisque $\langle x, t\rangle \to F_t(x)$ est une fonction définisable, pour x fixé, $t \to F_t(x)$ est définissable et donc continue presque partout, notamment elle est continue au voisinage de $t = 0^+$ et admet donc une limite. On va voir que la fonction $F_0 : (0,1) \to [0,1]^n$ est continue :

Soient $x_1, x_2 \in (0,1)$ distincts. Comme $F_t(x_i)$ tend vers $F_0(x_i)$, on prend $t \in (0,1)$ tel que $\|F_0(x_i) - F_t(x_i)\| \leqslant |x_1 - x_2|$ pour $i = 1, 2$ (Le choix de la norme n'est pas important, car on peut vérifier que tout comme dans $\mathbb{R}$, en dimension finie les normes sont toutes équivalentes). Par le théorème des accroissements finis, on a d'autre part $\|F_t(x_1) - F_t(x_2)\| \leqslant Nc\,|x_1 - x_2|$, puisque c est une borne pour F_t'. Ainsi :

$$
\begin{aligned}
\|F_0(x_1) - F_0(x_2)\| &\leqslant \|F_0(x_1) - F_t(x_1)\| + \|F_t(x_1) - F_t(x_2)\| + \|F_t(x_2) - F_0(x_2)\| \\
&\leqslant (Nc + 2)\,|x_1 - x_2|
\end{aligned}
$$

$\square$

En itérant cette démonstration en changeant un peu les calculs, on peut montrer que F_0 est C^{r-1} et que pour $0 \leqslant i \leqslant r-1$, $F_0^{(i)}(x) = \lim_{t \to 0^+} F_t^{(i)}(x)$.

On considère désormais une famille définissable $(F_t)_{t\in(0,1)}$ comme précédemment mais aussi telle que l'ensemble S_t des fonctions coordonées de F_t soit une r-paramétrisation de $(0,1)$. On définit S_0 comme l'ensemble des fonctions $\phi|_{\phi^{-1}(0,1)}$, où ϕ est une fonction coordonnée de F_0. S_0 a les propriétés suivantes :

(A) $\bigcup_{\psi\in S_0}\mathrm{Im}(\psi) = (0,1)\setminus T$, où $T \in (0,1)$ est un ensemble fini : par o-minimalité, si T n'était pas fini il contiendrait un intervalle, qui serait donc manqué par toutes les fonctions ψ, et donc manqué par toutes les fonctions coordonnées de F_0. Mais puisque F_t tend vers F_0 et que S_t est une r-paramétrisation de $(0,1)$, ceci est impossible, étant donné le fait que les dérivées de F_t sont bornées uniformément en t.

(B) Chaque fonction $\psi \in S_0$ a pour domaine un ouvert inclus dans $(0,1)$. De plus, ψ est C^{r-1} et $\psi^{(i)}$ est fortement bornée pour $0 \leqslant i \leqslant r-1$.

Définition 2.5.1. On fixe $m \geqslant 1$ et on introduit les notations suivantes :

— Pour $U \subset M^{m+1}$ définissable et ouvert, on note $V \Subset U$ et on dit que V est générique dans U si V est définissable, ouvert, $V \subset U$ et $\dim(U\setminus V) \leqslant m$.

— Pour $\phi : (0,1) \to M$, on note $I_\phi : (0,1)^{m+1} \to (0,1)\times M$ la fonction qui est l'identité sur les m permières variables et ϕ sur la dernière : $I_\phi(x_1,\cdots,x_{m+1}) = \langle x_1,\cdots,x_m,\phi(x_{m+1})\rangle$. Pour $f : X \subset M^{m+1} \to M^n$, on note aussi $f_\phi = f\circ I_\phi$ (restreinte à $I_\phi^{-1}[X]$).

Notre objectif est alors de montrer que si f est une fonction dérivable à dérivées fortement bornées par rapport aux m premières variable, alors on peut reparamétriser la coordonnée $m+1$ afin que f soit dérivable par rapport à la variable $m+1$ presque partout. Plus formellement :

Lemme 2.5.2. *Soient $n,m \geqslant 1$, $U \Subset (0,1)^{m+1}$, et $f : U \to M^n$ définissable et fortement bornée. On suppose que pour $1 \leqslant i \leqslant m$, $\partial f/\partial x_i$ existe, est continue et fortement bornée.*

Alors il existe $\forall r \geqslant 2$ une $(r-1)$-paramétrisation S d'un ensemble cofini de $(0,1)$, et un ensemble $V \Subset U$ tels que pour chaque $\phi \in S$, $I_\phi[V] \subset U$, f_ϕ est C^1 sur V, et toutes ses dérivées $\partial f/\partial x_i$ sont fortement bornées sur V.

Démonstration. La démonstration se fait par récurrence sur n. Le cas $n=1$ demandera beaucoup de travail tandis que la récurrence elle-même sera similaire a ce qui a été fait précédemment. On se place donc dans le cas $n=1$, on fixe $m \geqslant 1$, f comme dans l'énoncé et $r \geqslant 2$ et nous allons construire le S voulu sous la forme d'un S_0 limite d'une famille bien choisie.

En appliquant le théorème 1.4.2 à f avec $r=1$, on obtient un certain $W \Subset U$ restreinte auquel f est C^1. Pour t et $y \in (0,1)$, on pose $W_t(y)$ l'ensemble des $x \in (0,1)^m$ tels que le point $\langle x,y\rangle$ soit à une distance $\geqslant t$ de l'ensemble $[0,1]^m \times \{y\}\setminus W$:

$$W_t(y) = \{x \in (0,1)^m \mid d(\langle x,y\rangle, [0,1]^m\times\{y\}\setminus W) \geqslant t\}$$

À y et t fixés, la fonction $x \to |\partial f/\partial x_{m+1}(x,y)|$ est définie est continue sur $W_t(y)$ qui est fermé, borné, et définissable ; par conséquent elle atteint son maximum en un certain point $s_t(y) \in W_t(y)$, si celui-ci n'est pas vide. Puisque M admet des fonctions de choix définissables (théorème 1.5.2), on peut choisir $s_t(y)$ comme une fonction définissable en t et y, en posant par exemple $s_t(y) = \langle \frac{1}{2}, \cdots, \frac{1}{2} \rangle$ si $W_t(y)$ est vide.

On a alors $\forall t, y \in (0,1)^2$ tels que $W_t(y)$ est non-vide, $\langle s_t(y), y \rangle \in W$ et $\forall x \in W_t(y)$, $|\partial f/\partial x_{m+1}(s_t(y),y)| \geqslant |\partial f/\partial x_{m+1}(x,y)|$.

On considère désormais la famille définissable $(g_t)_{t\in(0,1)}$ où $g_t : (0,1) \to (0,1)^m \times M$ est définie par $g_t(y) = \langle s_t(y), f(s_t(y),y) \rangle$ si $W_t(y) \neq \emptyset$ et $\langle s_t(y), 0 \rangle$ sinon. On applique le corollaire 2.4.6 pour obtenir S_t, une r-reparamétrisation de g_t. Grâce à un argument de compacité et de saturation (voir l'annexe B.ii), on peut pour un certain $N \in \mathbb{N}$ supposer que $S_t = \{{}^{(i)}\phi_t \mid 1 \leqslant i \leqslant N\}$ † avec pour chaque i, $({}^{(i)}\phi_t)_{t\in(0,1)}$ une famille définissable de fonctions. On pose $F_t = \langle {}^{(1)}\phi_t, \cdots, {}^{(N)}\phi_t \rangle$. On définit F_0 et S_0 comme décrit en début de partie.

S_0 n'est pas tout-à-fait la paramétrisation que l'on cherche. La propriété (A) nous garantit que les fonctions de S_0 recouvrent un ensemble cofini dans $(0,1)$, en revanche la propriété (B) nous dit seulement que le domaine d'une fonction de S_0 est un ouvert, là où nous souhaterions qu'il s'agissât de l'intervalle $(0,1)$ tout entier. Pour remédier à ce problème, on sépare chaque fonction de S_0 en plusieurs fonctions constantes ou injectives dont le domaine est un intervalle ouvert, quitte à perdre un nombre fini de points du domaine. On se débarasse des fonctions constantes, perdant ainsi un nombre fini de point de l'image, et l'on compose chaque fonction ψ injective de domaine $(a,b) \subset (0,1)$ avec la fonction linéaire $\lambda : (0,1) \to (a,b)$, $x \to a + bx$. L'ensemble S des fonctions $\psi \circ \lambda$ ainsi définies est alors une $r-1$-paramétrisation d'un ensemble cofini de $(0,1)$.

On cherche aussi $V \Subset U$ tel que $I_\phi[V] \subset U$ et sur lequel f_ϕ est C^1 et à dérivées fortement bornées pour chaque $\phi \in S$. On sait que f est C^1 sur $W \Subset U$, ainsi l'idéal serait d'avoir $I_\phi[V] \subset W$. On pose alors :

$$V = U \setminus \bigcup_{\phi \in S} I_\phi^{-1}[(0,1)^{m+1} \setminus W]$$

Naturellement $V \subset U$. Comme $W \Subset U \Subset (0,1)^{m+1}$, $(0,1)^{m+1} \setminus W$ est de dimension $\leqslant m$, donc pour chaque $\phi \in S$, $I_\phi^{-1}[(0,1)^{m+1} \setminus W]$ est aussi de dimension $\leqslant m$ par injectivité et continuité de ϕ, et enfin $U \setminus V \subset \bigcup_{\phi\in S} I_\phi^{-1}[(0,1)^{m+1} \setminus W]$ qui est de dimension $\leqslant m$, et $V \Subset U$.

Soit $\phi \in S$ fixée. Il nous reste à vérifier que les dérivées de f_ϕ par rapport à chacune des $m+1$ variables sont fortement bornées sur V. On fixe $\langle x_0, y_0 \rangle \in V$ et on va montrer que $\partial f_\phi/\partial x_i(x_0,y_0)$ est fini pour $1 \leqslant i \leqslant m+1$. Un argument de compacité permet de conclure qu'une borne finie existe pour la fonction toute entière.

On rappelle que $f_\phi(x_0,y_0) = f \circ I_\phi(x_0,y_0) = f(x_0,\phi(y_0))$. Comme $I_\phi[V] \subset W$, on a $\langle x_0, \phi(y_0) \rangle \in W$ et donc $\partial f_\phi/\partial x_i(x_0,y_0)$ fini par hypothèse pour $1 \leqslant$

†. Dans la notation ${}^{(i)}\phi_t$, i est simplement un indice de numérotation. Il est placé de cette manière afin d'éviter la confusion avec la dérivée ou de gêner le t en indice.

$i \leqslant m$.

Désormais $i = m+1$. On remarque que ϕ est la composée d'une fonction ψ, qui est la restriction d'une fonction de S_0 à un certain intervalle, et d'une fonction linéaire à coefficients finis λ. Enfin on sait que $\partial f_\phi/\partial x_{m+1}(x_0, y_0) = \phi'(y_0)\partial f/\partial x_{m+1}(x_0, \phi(y_0))$. En posant $y_1 = \lambda(y_0)$, on voit qu'il suffit de montrer que $\psi'(y_1)\partial f/\partial x_{m+1}(x_0, \psi(y_1))$ est fortement bornée. On se sert du fait que $\langle x_0, \psi(y_1)\rangle \in W$ et que W est ouvert pour en déduire :

(i) $x_0 \in W_t(\psi(y_1))$ pour $t \in (0,1)$ suffisamment petit.

Par définition de S_0 on sait qu'il existe une famille définissable de fonctions $(\phi_t)_{t\in(0,1)}$ avec $\phi_t \in S_t$ telle que $\lim_{t\to 0^+} \phi_t(y_1) = \psi(y_1)$ et, puisque $r \geqslant 2$, $\lim_{t\to 0^+} \phi_t'(y_1) = \psi'(y_1)$. On peut alors prendre $t \in (0,1)$ suffisamment petit pour avoir :

(ii) $\left|\frac{\partial f}{\partial x_{m+1}}(x_0, \psi(y_1)) - \frac{\partial f}{\partial x_{m+1}}(x_0, \phi_t'(y_1))\right| \leqslant 1$, par continuité de $\frac{\partial f}{\partial x_{m+1}}$ sur W.

(iii) $|\phi_t'(y_1) - \psi'(y_1)| \leqslant \left|\frac{\partial f}{\partial x_{m+1}}(x_0, \psi(y_1))\right|^{-1}$ par convergence, le membre de droite étant traité comme une constante.

(iv) $x_0 \in W_t(\phi_t(y_1))$, en effet, si t_0 satisfait (i), alors n'importe quel $t < \frac{t_0}{2}$ tel que $|\psi(y_1) - \phi_t(y_1)| < \frac{t_0}{2}$ convient.

On choisit t tel que toutes ces propriétés tiennent simultanément. On a alors :

$$\begin{aligned}
\left|\psi'(y_1)\frac{\partial f}{\partial x_{m+1}}(x_0, \psi(y_1))\right| &\overset{\text{(iii)}}{\leqslant} \left|\phi_t'(y_1)\frac{\partial f}{\partial x_{m+1}}(x_0, \psi(y_1))\right| + 1 \\
&\overset{\text{(ii)}}{\leqslant} \left|\phi_t'(y_1)\frac{\partial f}{\partial x_{m+1}}(x_0, \phi_t(y_1))\right| + |\phi_t'(y_1)| + 1 \\
&\overset{\text{(iv)}}{\leqslant} \left|\phi_t'(y_1)\frac{\partial f}{\partial x_{m+1}}(s_t(\phi_t(y_1)), \phi_t(y_1))\right| + |\phi_t'(y_1)| + 1
\end{aligned}$$

Puisque $\phi_t \in S_t$, ϕ_t' est fortement bornée. Il ne reste plus qu'à montrer que $\phi_t'(y_1)\frac{\partial f}{\partial x_{m+1}}(s_t(\phi_t(y_1)), \phi_t(y_1))$ est fini ; on se sert du fait que S_t r-reparamétrise g_t, on a :

(v) $(s_t \circ \phi_t)'$ est fortement bornée

(vi) $\frac{d}{dy} f(s_t \circ \phi_t(y), \phi_t(y))$ est fortement bornée

Le calcul de la dérivée dans (vi) donne :

$$\begin{aligned}
(s_t \circ \phi_t)'(y_1) \cdot \langle \frac{\partial f}{\partial x_1}(s_t \circ \phi_t(y_1), \phi_t(y_1)), \cdots, \frac{\partial f}{\partial x_m}(s_t \circ \phi_t(y_1), \phi_t(y_1))\rangle \\
+\phi_t(y_1)\frac{\partial f}{\partial x_{m+1}}(s_t \circ \phi_t(y_1), \phi_t(y_1))
\end{aligned}$$

Le terme de gauche est fini par (v) et par hypothèse sur f, donc puisque la somme est finie par (vi), le terme de droite est fini ; c'est ce que nous voulions montrer.

Le théorème est démontré pour $n = 1$, pour terminer la récurrence, on suppose que le théorème est vrai jusqu'à un certain $n \geqslant 1$. On prend $F : U \to M^n$ et $f : U \to M$, on pose $G = \langle F, f \rangle$ et on suppose que G vérifie les hypothèses du lemme. Par récurrence on sait que pour F il existe une r-paramétrisation S et $V \Subset U$ comme dans l'énoncé. Alors pour chaque $\phi \in S$, on applique le lemme à f_ϕ pour obtenir T_ϕ une r-paramétrisation et $V_\phi \Subset U$ comme dans l'énoncé. Alors $\mathcal{S} = \{\phi \circ \psi \mid \phi \in S, \psi \in T_\phi\}$ est la r-paramétrisation que l'on cherche, et l'ensemble $\mathcal{V} = \bigcap_{\phi \in S, \psi \in T_\phi} V_\phi \cap I_\psi^{-1}[V]$ est l'ensemble générique dans U que l'on cherche. $\square$

Corollaire 2.5.3. *Soient $r, n \geqslant 1$, $U \Subset (0,1)^{m+1}$ et $f : U \to M^n$ définissable, fortement bornée et telle que $f^{(\alpha)}$ existe, est C^0 et fortement bornée $\forall \alpha = \langle \alpha_1, \cdots, \alpha_m, 0 \rangle \in \mathbb{N}^{m+1}$ avec $|\alpha| < r$.*

Alors pour chaque $k > 0$, il existe un ensemble $V_k \Subset U$ et une r-paramétrisation, S_k, d'un certain ensemble cofini de $(0,1)$ tels que $\forall \phi \in S_k$, $I_\phi[V_k] \in U$ et $f_\phi|_{V_k}$ soit C^r et que $f_\phi^{(\alpha)}|_{V_k}$ soit fortement bornée $\forall \alpha \in \mathbb{N}^{m+1}$ avec $|\alpha| \leqslant r$ et $\alpha_{m+1} \leqslant k$.

Démonstration. La preuve se fait par récurrence sur k. Pour $k = 0$, on peut prendre $V_0 \Subset U$ sur lequel f est C^r, par décomposition cellulaire. On prend $S_0 = \{\mathrm{id}_{(0,1)}\}$ et l'on a terminé.

Soit $k \geqslant 0$ pour lequel V_k et S_k existent et ont les propriétés requises. On pose alors $\Delta = \{\alpha \in \mathbb{N}^{m+1} \mid |\alpha| \leqslant r - 1, \alpha_{m+1} \leqslant k\}$ et $\tilde{n} = \#\Delta \cdot \#S_k$. On pose $F = \langle F_1, \cdots, F_{\tilde{n}} \rangle$, où chaque F_i est une fonction $f_\phi^{(\alpha)}$, $\phi \in S_k$ et $\alpha \in \Delta$. Chaque F_j est dérivable une fois par rapport à x_i pour $1 \leqslant i \leqslant m$, car $\partial F_j / \partial x_i = f_\phi^{(\alpha)}$, avec $|\alpha| \leqslant r$ et $\alpha_{m+1} \leqslant k$. On peut alors appliquer le lemme 2.5.2 avec F pour f, V_k pour U, $n\tilde{n}$ pour n, et $r+1$ pour r ; on obtient une r-paramétrisation S d'un ensemble cofini dans $(0,1)$ et un ensemble $V_{k+1} \Subset V_k$ tel que pour chaque $\psi \in S$, $I_\psi[V_{k+1}] \subset V_k$, et sur V_{k+1} chaque fonction $(f_\phi^{(\alpha)})_\psi$ est C^1 à dérivées fortement bornées. On note que d'autre part, $(f_\phi)_\psi = f_\phi \circ I_\psi$ est une fonction C^r sur V_{k+1}, car composée de fonctions C^r. On pose $S_{k+1} = \{\phi \circ \psi \mid \phi \in S_k, \psi \in S\}$. Pour que S soit la r-paramétrisation que l'on souhaite, il nous faut que $f_{\phi \circ \psi}^{(\alpha)}$ soit fortement bornée pour $|\alpha| \leqslant r$ et $\alpha_{m+1} \leqslant k + 1$.

Si $\alpha_{m+1} = 0$, alors $f_{\phi \circ \psi}^{(\alpha)} = (f_\phi^\alpha)_\psi$ et le résultat est clair car f_ϕ^α est fortement bornée.

Si $\alpha_{m+1} > 0$, alors par le théorème de Schwarz on a $f_{\phi \circ \psi}^{(\alpha)} = \partial / \partial x_{m+1} (f_{\phi \circ \psi}^{(\beta)})$ pour un certain $\beta \in \Delta$. De plus, $f_{\phi \circ \psi}^{(\beta)}(x) = \psi^{(\alpha_{m+1}-1)}(x_{m+1})(f_\phi^{(\beta)})_\psi(x)$ pour $x \in V_{k+1}$. Donc :

$$f_{\phi \circ \psi}^{(\alpha)}(x) = \psi^{(\alpha_{m+1})}(x_{m+1})(f_\phi^{(\beta)})_\psi(x) + \psi^{(\alpha_{m+1}-1)}(x_{m+1}) \frac{\partial}{\partial x_{m+1}} (f_\phi^{(\beta)})_\psi(x)$$

$\psi \in S$, donc ses dérivées d'ordre $\leqslant r$ sont fortement bornées et $\alpha_{m+1} \leqslant r$. $f_\phi^{(\beta)}$ est fortement bornée par hypothèse, et $\frac{\partial}{\partial x_{m+1}}(f_\phi^{(\beta)})_\psi$ est fortement bornée sur V_{k+1} par définition de S. Ainsi la quantité est fortement bornée et S_{k+1} et V_{k+1} conviennent.

□

Bien que la présence de k et de U soit nécessaire à la démonstration par récurrence, le corollaire 2.5.3 sera utilisé seulement avec $U = (0,1)^{m+1}$ et $k = r$. Il peut être utile de retourner à l'énoncé afin de voir ce qu'il signifie dans ce cas précis.

2.6 Preuve des théorèmes de paramétrisation

On va désormais démontrer les théorèmes de paramétrisation par une récurrence sur deux énoncés :

$(\mathrm{I})_m$ $\forall r, n \geqslant 1$, toute fonction $F : (0,1)^m \to M^n$ définissable et fortement bornée admet une r-reparamétrisation.

$(\mathrm{II})_m$ $\forall r \geqslant 1$, tout ensemble $X \subset M^m$ définissable et fortement borné admet une r-paramétrisation.

Démonstration. $(\mathrm{I})_1$ est déjà démontré grâce au corollaire 2.4.6. On a de plus vu dans la preuve du corollaire 2.4.4 que tout ensemble définissable de M admet une r-paramétrisation, autrement dit $(\mathrm{II})_1$ est vrai. On suppose désormais que $(\mathrm{I})_l$ et $(\mathrm{II})_l$ sont vrais pour $l \leqslant m$. On va montrer que $(\mathrm{I})_{m+1}$ et $(\mathrm{II})_{m+1}$ sont vrais.

Pour $(\mathrm{II})_{m+1}$: soit $r \geqslant 1$, et $X \subset M^{m+1}$ définissable et fortement borné. Par décomposition cellulaire, X est une union finie de cellules ; on peut supposer que X est une cellule de M^{m+1}. Il y a deux cas à traiter :

— $X = \{\langle x, y\rangle \in M^m \times M \mid f(x) < y < g(x)\}$, où f et $g : Y \to M$ avec $f < g$ et Y une cellule de M^m (de dimension l). Par $(\mathrm{II})_m$ il existe une r-paramétrisation de Y, que l'on note S, et par $(\mathrm{I})_l$ pour chaque $\phi \in S$ il existe une r-reparamétrisation, que l'on note T_ϕ, de $(f \circ \phi, g \circ \phi) : (0,1)^l \to M^2$. Pour $\psi \in T_\phi$ on définit $\theta_{\phi,\psi} : (0,1)^{l+1} \to X$ par :

$$\theta_{\phi,\psi}(x_1, \cdots, x_{l+1}) = \langle \xi, (1 - x_{l+1})f(\xi) + x_{l+1}g(\xi)\rangle$$

Avec $\xi = \phi \circ \psi(x_1, \cdots, x_l)$. L'ensemble des $\theta_{\phi,\psi}$ forme alors une r-paramétrisation de X.

— X est le graphe de $f : Y \to M$. On procède de même pour obtenir S, une r-paramétrisation de Y, et pour chaque $\phi \in S$, T_ϕ une r-paramétrisation de $f \circ \phi$. On pose alors $\theta_{\phi,\psi}(x) = \langle \phi \circ \psi(x), f \circ \phi \circ \psi(x)\rangle$.

Pour $(\mathrm{I})_{m+1}$, on peut se restreindre au cas $n = 1$ grâce au lemme 2.4.5. Soit $r \geqslant 1$ et soit $F : (0,1)^{m+1} \to M$ définissable et fortement bornée. Par $(\mathrm{I})_m$, il existe pour chaque $u \in (0,1)$ fixé une r-paramétrisation, que l'on note S_u, de $F_u : (0,1)^m \to M$, $x \to F(x,u)$. Par saturation on sait qu'il existe $N \in \mathbb{N}$

tel que $\#S_u \leqslant N$, notons $S_u = \{^{(i)}\phi_u \mid 0 \leqslant i \leqslant N\}$, de manière à ce que $\{^{(i)}\phi_u \mid u \in (0,1)\}$ soit une famille définissable à i fixé.

Pour $0 \leqslant i \leqslant N$, on définit désormais $^{(i)}F : (0,1)^{m+1} \to M$ par $^{(i)}F(x,u) = F_u \circ^{(i)} \phi_u(x)$. On pose enfin :

$$^*F = \langle ^{(1)}\phi_u, \cdots ,^{(N)} \phi_u, ^{(1)} F, \cdots ,^{(N)} F\rangle \,:\, (0,1)^{m+1} \to M^{mN+N}$$

.

Les hypothèses du corollaire 2.5.3 tiennent avec $^*F$ pour f, $(0,1)^{m+1}$ pour U, et $mN+N$ pour n, car S_u est une r-reparamétrisation de F, uniformément en u. En l'applicant avec $k = r$ on obtient $V_r \Subset (0,1)^{m+1}$ et S_r une r-paramétrisation d'un certain $A \Subset (0,1)$, avec les propriétés additionnelles.

Notons que si $V_r = (0,1)^{m+1}$ et $A = (0,1)$, alors les fonctions $\langle x,u\rangle \to^{(j)} \phi_{\psi(u)}(x)$, pour $1 \leqslant j \leqslant N$ et $\psi \in S_r$, forment une r-reparamétrisation de F.

Ici on sait seulement que ces fonctions recouvrent $(0,1)^{m+1}$ à l'exception d'un nombre fini de plans $\{x_{m+1} = a\}_{a \notin A}$. De plus, si l'on les restreint à V_r, où elles sont C^r et à dérivées fortement bornées, elles recouvrent encore un ensemble W de codimension $l \leqslant m$ dans $(0,1)^{m+1}$.

On utilise $(\mathrm{II})_{m+1}$, que l'on vient de démontrer, pour obtenir une r-paramétrisation de V_r, que l'on note T_1. Ceci nous permet de nous assurer que le domaine des paramétrisations partielles sera bien $(0,1)^{m+1}$.

Toujours par $(\mathrm{II})_{m+1}$, on obtient une r-paramétrisation de $(0,1)^{m+1} \setminus W$, que l'on note T_2, afin de pouvoir couvrir la partie manquante de l'ensemble d'arrivée.

On utilise enfin $(\mathrm{I})_l$, qui tient par récurrence, pour obtenir pour chaque $\theta \in T_2$ une r-reparamétrisation de $F \circ \theta : (0,1)^l \to M$ que l'on note U_θ.

La r-reparamétrisation que l'on recherche est alors :

$$\{^{(j)}\phi_\psi \circ \chi \mid 1 \leqslant j \leqslant N,\, \psi \in S_r,\, \chi \in T_1\} \cup \{\hat{\theta} \circ \hat{\lambda} \mid \theta \in T_2,\, \lambda \in U_\theta\}$$

où ˆ signifie que l'on étend le domaine d'une fonction g à $(0,1)^{m+1}$ en posant $\hat{g}(x_1, \cdots , x_{m+1}) = g(x_, \cdots , x_l)$. □

Corollaire 2.6.1. *Soient $m, r \geqslant 1$ et $X \subset (0,1)^m$ définissable de dimension l. Alors il existe un ensemble fini S de fonctions de $(0,1)^l$ dans X définissables, C^r et telles que :*

— $\bigcup_{\phi \in S} \mathrm{Im}(\phi) = X$,

— $\forall \phi \in S,\ \alpha \in \mathbb{N}^l,\ |\alpha| \leqslant r\ ;\ \left\|\phi^{(\alpha)}\right\|_\infty \leqslant 1$.

Démonstration. Prenons S une r-paramétrisation de X, chaque fonction et chacune des dérivées, en nombre fini, est fortement bornée. Il y a donc une borne uniforme $c \in \mathbb{N}$. On recouvre $(0,1)^{\dim(X)}$ avec $(2c)^{\dim(X)}$ cubes de côté $\frac{1}{c}$ (qui se chevauchent), et pour K l'un de ces cubes on pose $\lambda_K : (0,1)^{\dim(X)} \to K$ la bijection linéaire naturelle. Alors l'ensemble $\{\phi \circ \lambda_K \mid \phi \in S,\, K \text{ un des cubes}\}$ convient. □

Comme toujours il existe une version uniforme :

Corollaire 2.6.2. *Soient $n, m, r \geqslant 1$ et $X \subset (0,1)^n \times M^m$ une famille définissable. Alors il existe $N \in \mathbb{N}$ et $\forall y \in M^m$ un ensemble S_y de N fonctions de $(0,1)^{\dim(X_y)}$ dans X_y définissables, C^r et telles que :*

— $\bigcup_{\phi \in S_y} \mathrm{Im}(\phi) = X_y$,

— $\forall \phi \in S_y$, $\alpha \in \mathbb{N}^{\dim(X_y)}$, $|\alpha| \leqslant r$; $\left\|\phi^{(\alpha)}\right\|_\infty \leqslant 1$.

Ce résultat est suffisant pour démontrer le lemme 2.2.2. Notons qu'il s'exprime uniquement grâce à des formules du premier ordre, et est par conséquent valable pour $\mathbb{R}$ comme dit précédemment. Nous pouvons alors démontrer le théorème 2.1.4.

2.7 Preuve du théorème de Pila-Wilkie

Désormais on fixe n, m et $\epsilon > 0$, et on se donne $Z \subset \mathbb{R}^n \times \mathbb{R}^m$ une famille définissable. Notre but et de trouver $W \subset Z$ et $c > 0$ satisfaisant le théorème 2.1.4. Il nous suffit de considérer le cas où $Z \subset [0,1]^n \times \mathbb{R}^m$ car l'ensemble des points rationnels de hauteur T est stable sous les opérations $x_i \to \pm x_i^{\pm 1}$. On se restreint enfin à $Z \subset (0,1)^n \times \mathbb{R}^m$ car à $y \in \mathbb{R}^m$ fixé, pour chaque $0 \leqslant i \leqslant n$, on dénombre les points de $Z_y(\mathbb{Q}, T)$ tels que $x_i = 0$ ou $x_i = 1$; ceci revient à dénombrer les points rationnels d'un ensemble de $[0,1]^{n-1}$ et par récurrence sur n on peut supposer que le résultat tient.

Considérons le cas où A, B et C sont des familles définissables incluses dans $\subset (0,1)^n \times \mathbb{R}^m$ et telles que $A \cup B = C$. On a naturellement $A_y^{\mathrm{alg}} \cup B_y^{\mathrm{alg}} \subset C_y^{\mathrm{alg}}$. Par conséquent si le théorème 2.1.4 tient pour A et B avec $W_{A,\epsilon}$, $W_{B,\epsilon}$ et $c_{A,\epsilon}$, $c_{B,\epsilon}$; alors il tient pour C avec $W_{C,\epsilon} = W_{A,\epsilon} \cup W_{B,\epsilon}$ et $c_{C,\epsilon} = c_{A,\epsilon} + c_{B,\epsilon}$. Ceci laisse penser que le résultat pourra être démontré par récurrence.

On travaille à n fixé et on commence une démonstration par récurrence sur $k = \max_{y \in \mathbb{R}^m} \dim(Z_y) \leqslant n$. Le cas $k = 0$ correspond au cas où chaque Z_y est fini, et par compacité on a une borne uniforme $N \in \mathbb{N}$ sur le nombre de points de chaque fibre. Le théorème tient avec $W = \emptyset$ et $c = N$.

On suppose désormais $k > 0$ et que le théorème tient pour tout Z dont les fibres sont de dimension $\leqslant k - 1$. On introduit la notion de point régulier : $x \in \mathrm{reg}_l(X)$ signifie que X est C^1-difféomorphe, au voisinage de x, à une variété de dimension l.

L'ensemble $R_l(Z) = \{\langle x, y\rangle \in Z \mid x \in \mathrm{reg}_l(Z_y)\}$ est alors définissable (voir [16] pour une démonstration).

Dans le cas où $k = n$, $x \in \mathrm{reg}_n(Z_y)$ pour $y \in \mathbb{R}^m$ signifie que Z_y contient un voisinage de x de dimension n, et puisque $Z_y \subset (0,1)^n$, alors $B(x, \delta) \subset Z_y$ pour un certain $\delta > 0$. Mais cette boule est un ensemble semi-algébrique, et donc $x \in Z_y^{\mathrm{alg}}$. Ainsi $A = R_n(Z)$ est définissable et $A_y^{\mathrm{alg}} = A_y$ pour chaque $y \in \mathbb{R}^m$. Le théorème tient alors pour A avec $W_{A,\epsilon} = A$. Posons $B = Z - A$, les fibres de B sont de dimension $\leqslant n - 1$, et par récurrence le résultat tient pour B et donc aussi pour $A \cup B = Z$.

Désormais $k < n$. Pour $\sigma \subset \{1, \cdots, n\}$ on note Π_σ le sous-espace vectoriel de $\mathbb{R}^n$ engendré par $\{e_i \mid i \in \sigma\}$, où $\{e_1, \cdots, e_n\}$ est la base canonique de $\mathbb{R}^n$, et π_σ la projection associée. On note $S = S_{k,n} = \{\sigma \subset \{1, \cdots, n\} \mid \#\sigma = k+1\}$ et $q = \#S$. Par le lemme 2.2.2, on sait que pour chaque $\sigma \in S$, il y a une constante $\alpha(Z, \epsilon, \sigma)$ telle que $\forall y \in \mathbb{R}^m$, $(\pi_\sigma(Z_y))(\mathbb{Q}, T)$ soit contenu dans l'union d'au plus $\alpha(Z, \epsilon, \sigma)T^{\epsilon/2q}$ hypersurfaces de degré $\leqslant d$. En posant $\alpha = \alpha(Z, \epsilon) = \max_{\sigma \in S} \alpha(Z, \epsilon, \sigma)$, on obtient que $Z_y(\mathbb{Q}, T)$ est contenu dans l'union d'au plus $\alpha^q T^{\epsilon/2}$ intersections de cylindres au-dessus de ces hypersurfaces, car pour être dans $Z_y(\mathbb{Q}, T)$ il faut être dans chacun des $(\pi_\sigma(Z_y))(\mathbb{Q}, T)$.

Une hypersurface est entièrement définie par un polynôme, on peut donc identifier une hypersurface L de Π_σ avec t_σ, un p-uplet de coefficients pour un certain $p = p(k, d)$. On notera T l'ensemble des $t = \langle t_\sigma \mid \sigma \in S \rangle$ qui correspondent à un choix d'une hypersurface $L(t_\sigma) \subset \Pi_\sigma$ pour chaque $\sigma \in S$. On pose :

$$\Sigma = \{\langle x, y, t \rangle \in \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^{pq} \mid \forall \sigma \in S,\ \pi_\sigma(x) \in L(t_\sigma)\}$$

Pour $u = \langle y, t \rangle$, la fibre Σ_u est définie par des équations polynômiales, donc est semi-algébrique. De plus comme chaque projection de Σ_u sur$k+1$ coordonnées est de dimension $\leqslant k$, la fibre est elle-même de dimension $\leqslant k$.

On considère aussi :

$$\hat{Z} = \{\langle x, y, t \rangle \in \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^{pq} \mid \langle x, y \rangle \in Z,\ t \in T\}$$

On a $\hat{Z}_u = Z_y$, et donc les fibres de $\hat{Z}$ au-dessus de u sont de dimension $\leqslant k$. Enfin les fibres de $\hat{Z} \cap \Sigma$ au-dessus de u sont elles aussi de dimension $\leqslant k$. On pose :

$$A_1 = \{\langle x, u \rangle \in \hat{Z} \cap \Sigma \mid x \notin \mathrm{reg}_k(\hat{Z} \cap \Sigma_u)\}$$

A_1 est définissable. Si $A_{1,u}$ est de dimension k, alors il existe une cellule, qui est en particulier une variété, de dimension k. Tout point de cette cellule est alors un point de $\mathrm{reg}_k(\hat{Z} \cap \Sigma_u)$, ce qui est impossible. Ainsi les fibres de A_1 au-dessus de u sont de dimension $\leqslant k-1$ et par récurrence il existe $W(A_1, \frac{\epsilon}{2})$ et $c(A_1, \frac{\epsilon}{2})$ satisfaisant le théorème (donnant une borne en $cT^{\epsilon/2}$). De même, on définit :

$$A_2 = \{\langle x, u \rangle \in \hat{Z} \cap \Sigma \mid x \notin \mathrm{reg}_k(\Sigma_u)\} \text{ et } A_3 = \{\langle x, u \rangle \in \hat{Z} \cap \Sigma \mid x \notin \mathrm{reg}_k(\hat{Z}_u)\}$$

Pour les mêmes raisons, leurs fibres au-dessus de u sont toujours de dimension $\leqslant k-1$ et il existe $W(A_i, \frac{\epsilon}{2})$ et $c(A_i, \frac{\epsilon}{2})$ satisfaisant le théorème.

Il nous reste à considérer $B = \hat{Z} \cap \Sigma - \bigcup_{i=1,2,3} A_i$, c'est-à-dire l'ensemble des points réguliers de dimension k dans $\hat{Z}$, Σ et $\hat{Z} \cap \Sigma$. Considérons un point $\langle x, u \rangle \in B$, ce qui signifie que dans un voisinage $\Delta \subset \mathbb{R}^n$ suffisament petit de x, les trois fibres $\hat{Z}_u$, Σ_u et $\hat{Z} \cap \Sigma_u$ sont des variétés C^1. Mais comme $\hat{Z} \cap \Sigma_u \subset \hat{Z}_u$ et $\hat{Z} \cap \Sigma_u \subset \Sigma_u$, elles coïncident localement :

$$\hat{Z}_u \cap \Delta = \hat{Z} \cap \Sigma_u \cap \Delta = \Sigma_u \cap \Delta$$

Or, quitte à prendre une boule ouverte pour Δ, $\Sigma_u \cap \Delta$ est semi-algébrique de dimension $k \geqslant 1$. Autrement dit $\langle x, u \rangle \in B_u^{\mathrm{alg}}$, et le théorème tient pour B avec $W(B, \epsilon) = B$, et on a démontré que $\hat{Z} \cap \Sigma$ vérifie le théorème.

Enfin, on fixe $y \in \mathbb{R}^m$, et l'on va s'intéresser aux points rationnels de Z_y :

- Pour chaque $\sigma \in S$, $(\pi_\sigma(Z_y))(\mathbb{Q}, T)$ est contenu dans l'union d'au plus $\alpha T^{\epsilon/2q}$ hypersurfaces. Ainsi à $P \in Z_y(\mathbb{Q}, T)$ on associe un vecteur $t = \langle t_\sigma \mid \sigma \in S \rangle$ tel que $\pi_\sigma(P) \in L(t_\sigma)$; puisque $\pi_\sigma(P) \in (\pi_\sigma(Z_y))(\mathbb{Q}, T)$ on peut faire en sorte que t ne prenne que $\alpha^q T^{\epsilon/2}$ valeurs distinctes lorsque P parcourt $Z_y(\mathbb{Q}, T)$.
- Pour chaque $t = \langle t_\sigma \mid \sigma \in S \rangle$ on considère la fibre $\hat{Z} \cap \Sigma_u$, où $u = \langle y, t \rangle$: cette fibre contient P, autrement dit on peut trouver $\alpha^q T^{\epsilon/2}$ fibres de $\hat{Z} \cap \Sigma$ au-dessus de u telles que chaque $P \in Z_y(\mathbb{Q}, T)$ soit dans l'une d'entre elles.
- Puisque $\hat{Z} \cap \Sigma$ vérifie le théorème, on sait qu'il existe une certaine famille définissable $\hat{W} = W(\hat{Z} \cap \Sigma, \frac{\epsilon}{2})$ et une constante $c = c(\hat{Z} \cap \Sigma, \frac{\epsilon}{2})$ telles que $N(\hat{Z} \cap \Sigma_u - \hat{W}_u, T) \leqslant c T^{\epsilon/2}$.
- En posant $W = W(Z, \epsilon) = \{\langle x, y \rangle \mid \exists t \langle x, y, t \rangle \in W\}$, alors chaque $P \in (Z_y - W_y)(\mathbb{Q}, T)$ est dans un parmi au plus $\alpha^q T^{\epsilon/2}$ ensembles de la forme $\hat{Z} \cap \Sigma_u - \hat{W}_u$; or ces ensembles contiennent au plus $c T^{\epsilon/2}$ points rationnels de hauteur $\leqslant T$, ce qui nous donne $N(Z_y - W_y, T) \leqslant c \alpha^q T^\epsilon$ et le théorème est démontré pour Z.

3 Applications

Nous allons présenter dans cette partie deux applications du théorème de Pila-Wilkie. La première est une démonstration d'un résultat dont il existe d'autres démonstration ne faisant pas appel au théorème de Pila-Wilkie, en revanche la seconde est une démonstration d'un résultat dont il n'existe pas d'autre démonstration. Nous nous basons sur un article de Scanlon [13] pour présenter ces démonstrations. La stratégie est toujours la même pour établir ces résultats : Dans un premier temps on se concentre sur la partie algébrique que l'on étudie à l'aide d'outils de géométrie algébrique, puis on s'occupe de la partie transcendante à l'aide du théorème de Pila-Wilkie. Ici nous nous concentrerons surtout sur la partie transcendante afin d'exposer en détail l'utilisation du théorème de Pila-Wilkie.

3.1 La conjecture de Manin-Mumford

Pila et Zannier ont donné dans [11] une démonstration de la conjecture de Manin-Mumford, dont il existe déjà plusieurs démonstrations différentes. Nous allons considérer un cas particulier de cette conjecture et exposer une version simplifiée de la démonstration de Pila et Zannier, en suivant l'article de Scanlon. On vise le résultat suivant :

Théorème 3.1.1. *Soient $n \in \mathbb{N}^*$ et $G \in \mathbb{C}[X_1, \cdots, X_n]$ un polynôme. On note $\mathbb{G} = (\mathbb{C}^\times)^n$, et on considère l'ensemble suivant :*

$$X = \{\langle \zeta_1, \cdots, \zeta_n \rangle \in \mathbb{G} \mid \forall i\, \zeta_i \text{ est une racine de l'unité et } G(\zeta_1, \cdots, \zeta_n) = 0\}$$

Alors X est une union finie de classes d'équivalence modulo des sous-groupes de $\mathbb{G}$.

Démonstration. Le lien entre cet ensemble et l'étude des points rationnels est obtenu grâce à la correspondance naturelle : $x \in \mathbb{C}$ est une racine de l'unité ssi $x = e^{2\pi i z}$, avec $z \in \mathbb{Q}$. Autrement dit, si l'on définit le morphisme de groupes $E : (\mathbb{C}_+)^n \to \mathbb{G}$ par $E(z_1, \cdots, z_n) = \langle e^{2\pi i z_1}, \cdots, e^{2\pi i z_n} \rangle$, alors $\zeta = \langle \zeta_1, \cdots, \zeta_n \rangle$ est un tuple de racines de l'unité ss'il existe un certain $a \in \mathbb{Q}^n$ tel que $E(a) = \zeta$. Ainsi l'étude de X devient l'étude des solutions rationnelles de l'équation $G(E(z)) = 0$.

L'étude de ces solutions n'est cependant pas forcément plus simple sous cette forme : l'équation $E(z) = \pm 1$ définit $\mathbb{Z}^n$, E n'est donc jamais définissable dans une structure o-minimale. On peut néanmoins restreindre E à un domaine fondamental afin d'éviter ce problème. On pose $D = \{z \in \mathbb{C}^n \mid 0 \leqslant Re(z_i) < 1\}$, et on note $\widetilde{E} = E|_D$. Cette fonction est bijective, et est définissable dans une structure o-minimale ; en effet, si l'on identifie $\mathbb{C}$ à $\mathbb{R}^2$, $\widetilde{E}$ est alors la fonction :

$$\langle x_1, y_1, \cdots, x_n, y_n \rangle \in ([0, 1) \times \mathbb{R})^n \to \langle e^{-2\pi y_i} cos(2\pi x_i), e^{-2\pi y_i} sin(2\pi x_i) \rangle_{1 \leqslant i \leqslant n}$$

Bien sûr, les fonctions cosinus et sinus ne sont jamais définissables dans une structure o-minimale, mais ici on peut les restreindre à $[0, 2\pi)$, et ainsi définir la fonction $\widetilde{E}$ dans la structure $\mathbb{R}_{\text{an,exp}}$, dont on sait qu'elle est o-minimale. On définit alors $\widetilde{X} = \{z \in D \mid G(\widetilde{E}(z)) = 0\}$. L'ensemble X est alors identifiable à $\widetilde{X}(\mathbb{Q})$, et puisque $\widetilde{X}$ est définissable dans une structure o-minimale, on peut lui appliquer le théorème de Pila-Wilkie (2.1.4).

On va décrire la structure de $\widetilde{X}^{\text{alg}}$ à l'aide de la proposition suivante :

Proposition 3.1.2 (Ax-Schanuel)**.** *Soient $\gamma_1(t), \cdots, \gamma_n(t) \in t\mathbb{C}[[t]]$ linéairement indépendantes sur $\mathbb{Q}$, alors $\mathbb{C}(t, \gamma_1(t), \cdots, \gamma_n(t), e^{\gamma_1(t)}, \cdots, e^{\gamma_n(t)})$ est de degré de transcendance sur $\mathbb{C}(t)$ au moins n.*

Grâce à ce résultat on peut établir le théorème 3.1.1 pour $\widetilde{X}^{\text{alg}}$, on renvoie vers l'article de Scanlon ou celui de Pila et Zannier pour les détails.

Quant à $\widetilde{X}^{\text{trans}}$, on va établir le résultat dans le cas où G est un polynôme irréductible à coefficients dans un corps de nombres K (c'est-à-dire que $[K : \mathbb{Q}]$ est fini). Une manipulation classique de géométrie algébrique nous permet de ramener le cas général à ce cas-ci, mais pour plus de concision nous nous contenterons de rajouter cette condition dans nos hypothèses. Nous allons démontrer le résultat suivant :

Théorème 3.1.3. *Soient $n \in \mathbb{N}^*$, $K \subset \mathbb{C}$ un corps de nombres, et $G \in K[X_1, \cdots, X_n]$ un polynôme irreductible. On note $\mathbb{G} = (\mathbb{C}^\times)^n$, et on considère l'ensemble suivant :*

$$\widetilde{X} = \{z \in D \mid G(\widetilde{E}(z)) = 0\}$$

Alors $\widetilde{X}^{trans}(\mathbb{Q})$ est fini.

Soient $T \geqslant 1$ et $z \in \widetilde{X}^{\text{trans}}(\mathbb{Q}, T)$. On écrit $z = \langle \frac{a_1}{b_1}, \cdots, \frac{a_n}{b_n} \rangle$ avec $0 \leqslant a_i < b_i \leqslant T$ et $\text{pgcd}(a_i, b_i) = 1$. On a donc $G(\widetilde{E}(z)) = 0$. On pose $L = K[e^{2\pi i \frac{a_1}{b_1}}, \cdots, e^{2\pi i \frac{a_n}{b_n}}]$. Puisque G est à coefficients dans K, pour $\sigma \in Gal(L/K)$, on sait que $G(\sigma(\widetilde{E}(z))) = 0$. Puisque $e^{2\pi i \frac{a_j}{b_j}}$ est une racine primitive $b_j^{\text{ème}}$ de l'unité, on sait que $\sigma(e^{2\pi i \frac{a_j}{b_j}}) = e^{2\pi i \frac{a'}{b_j}}$, avec $0 < a' \leqslant b_j$. On sait alors que l'orbite de cet élément par l'action du groupe de Galois est de cardinal au moins $\frac{\varphi(b_j)}{[K:\mathbb{Q}]}$.

Par l'absurde, on va supposer que $\widetilde{X}^{\text{trans}}(\mathbb{Q})$ est infini. Alors on peut trouver une suite d'entiers $(T_n)_{n\in\mathbb{N}}$ strictement croissante telle que $N(\widetilde{X}^{\text{trans}}, T_n) > N(\widetilde{X}^{\text{trans}}, T_n - 1)$, autrement dit il existe pour chaque n un élément de hauteur exactement T_n.

Alors, par l'action du groupe de Galois, il existe au moins $\frac{\varphi(T_n)}{[K:\mathbb{Q}]}$ éléments dans $\widetilde{X}^{\text{trans}}(\mathbb{Q}, T_n)$. Appliquons le théorème de Pila-Wilkie avec $\epsilon = \frac{1}{2}$: $\exists C \geqslant 0$ tel que $\forall n \in \mathbb{N}$, $N(\widetilde{X}^{\text{trans}}, T_n) \leqslant CT_n^{\frac{1}{2}}$. D'autre part, on a démontré auparavant $N(\widetilde{X}^{\text{trans}}, T_n) \geqslant \frac{\varphi(T_n)}{[K:\mathbb{Q}]}$; or la fonction φ est telle que $\forall \delta > 0$, $\frac{\varphi(m)}{m^{1-\delta}} \to \infty$ quand $m \to \infty$. Alors, avec $\delta = \frac{1}{2}$, on peut prendre n assez grand pour avoir $\varphi(T_n) > [K : \mathbb{Q}]CT_n^{\frac{1}{2}}$; ce qui contredit le théorème de Pila-Wilkie.

Ainsi l'on a $\widetilde{X}^{\text{trans}}(\mathbb{Q})$ est fini. $\square$

3.2 Torsion simultanée dans des courbes elliptiques

On va donner une seconde application du théorème de Pila-Wilkie. Il s'agit d'un résultat nouveau, démontré par Masser et Zannier dans [7]. Avant de l'exposer, nous allons rappeler brièvement la théorie des courbes elliptiques :

Définition 3.2.1. On se donne $\tau \in \mathbb{C}$, $\tau \neq 0$ ou 1, et l'on pose $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$. On définit la fonction de Weierstrass :

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

On pose enfin $g_2(\Lambda) = 60 \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-4}$ et $g_3(\Lambda) = 140 \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-6}$. Alors on définit la courbe elliptique E_Λ de 2 manières équivalentes :

— $E_\Lambda^{\text{tore}} = \mathbb{C}/\Lambda$, munie de la loi de groupe additif.

— $E_\Lambda^{\text{graphe}} = \{\langle x, y\rangle \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)\}$, avec un point en plus « à l'infini », noté 0_E. Les coefficients g_2 et g_3 sont définis de manière à ce que $\pi_\Lambda : E_\Lambda^{\text{tore}} \to E_\Lambda^{\text{graphe}}$, $z \to \langle \wp_\Lambda(z), \wp'_\Lambda(z)\rangle$ soit une bijection. On définit une loi de groupe sur $E_\Lambda^{\text{graphe}}$ grâce à cette bijection, qui devient alors un isomorphisme, envoyant notament le neutre de E_Λ^{tore} sur le point à l'infini, c'est-à-dire sur 0_E.

On peut aussi modifier l'équation de $E_\Lambda^{\text{graphe}}$ pour obtenir la forme réduite de Legendre : $y^2 = x(x-1)(x-\lambda)$, pour un certain $\lambda \in \mathbb{C}$ distinct de 0 ou 1 ; nous désignerons cette forme par E_λ.

L'étude des courbes elliptiques montre que pour $a \in \mathbb{C}$ fixé différent de 0 ou 1, le point $\langle a, \sqrt{a(a-1)(a-\lambda)}\rangle$ est un point de torsion dans E_λ pour un nombre infini dénombrable de $\lambda \in \mathbb{C}$. Masser et Zannier posent alors la question suivante : pour deux nombres complexes a et b distincts et différents de 0 ou 1, pour combien de $\lambda \in \mathbb{C}$ les points $\langle a, \sqrt{a(a-1)(a-\lambda)}\rangle$ et $\langle b, \sqrt{b(b-1)(b-\lambda)}\rangle$ sont simultanément des points de torsion dans E_λ ? Masser et Zannier donnent la réponse dans le cas $a = 2$ et $b = 3$:

Théorème 3.2.2. *Les deux points*

$$P_\lambda = \langle 2, \sqrt{2(2-\lambda)}\rangle \text{ et } Q_\lambda = \langle 3, \sqrt{6(3-\lambda)}\rangle$$

sont simultanément des points de torsion dans E_λ pour un nombre fini de $\lambda \in \mathbb{C}$.

Démonstration. Comme précédemment, l'objectif est de se rammener à l'étude des points rationnels d'un ensemble définissable dans une structure o-minimale. On travaille avec la bijection $\pi_\Lambda : \mathbb{C}/\Lambda \to E_\Lambda^{\text{graphe}}$. On peut l'étendre périodiquement en une fonction $\mathbb{C} \to E_\lambda^{\text{graphe}}$, puis la restreindre à un domaine fondamental $D = \{z \in \mathbb{C} \mid 0 \leqslant Re(z) < 1, 0 \leqslant Im(z) < \tau\}$. Enfin, en normalisant par τ et en modifiant la fonction pour que son espace d'arrivée soit E_λ, puis en interprétant $\mathbb{C}$ comme $\mathbb{R}^2$, on définit la fonction $\pi_\lambda : [0,1) \times [0,1) \to \mathbb{R}^2$, qui est un isomorphisme de son domaine (muni de la loi de groupe additif modulo 1) dans son image. La fonction $\langle z, \lambda \rangle \to \pi_\lambda(z)$ est alors définissable dans $\mathbb{R}_{\text{an,exp}}$, en considérant z et λ comme des couples de réels. On s'intéresse à l'ensemble suivant :

$$\widetilde{X} = \{\langle x_1, y_1, x_2, y_2\} \in [0,1)^4 \mid \exists \lambda \pi_\lambda(x_1, y_1) = P_\lambda \text{ et } \pi_\lambda(x_2, y_2) = Q_\lambda\}$$

Si λ est tel que P_λ et Q_λ sont simultanément des points de torsion dans E_λ, alors leur antécédent par π_λ est aussi de torsion dans $[0,1)^2$, ce qui signifie qu'il s'agit d'un point rationnel. Le nombre de λ tels que P_λ et Q_λ sont simultanément des points de torsion correpond alors au nombre de points rationnels de $\widetilde{X}$, qui est un ensemble définissable dans une structure o-minimale sur $\mathbb{R}$. Nous allons alors pouvoir appliquer le théorème de Pila-Wilkie.

Grâce à l'étude de la fonction $\wp$, on montre que $\widetilde{X}^{\text{alg}}$ est vide. L'étude de $\widetilde{X}^{\text{trans}}$ est plus fastidieuse, mais se déroule de la même manière que pour l'exemple précédent : on prouve que si λ est tel que P_λ et Q_λ soient des points de torsion dans E_λ, alors λ est un nombre algébrique. Si d est son degré, alors il existe au moins $\frac{d}{2}$ conjugués de λ ayant la même propriété. On établit par ailleurs un lien entre le degré d et la hauteur T du point rationnel correspondant. Enfin, on compare cette borne avec le résultat du théorème de Pila-Wilkie, et on en conclut que $\widetilde{X}^{\text{trans}}$ est fini. $\square$

Annexes

A Illustration de la proposition 2.2.1

La proposition 2.2.1 est un résultat démontré par Pila dans [9]. Nous allons donner une démonstration dans un cas de petite dimension, à savoir $k = 1$ et $n = 2$, en nous basant sur un exposé de Derya Ciray [1]. L'énoncé que l'on cherche à démontrer est alors :

Proposition A.1. *Quel que soit $d \in \mathbb{N}^*$ fixé, il existe un entier positif $r = r(d)$ et deux réels positifs $C = C(d)$ et $\epsilon = \epsilon(d)$ avec la propriété suivante :*

Pour toute fonction $\phi : (0, 1) \to \mathbb{R}^2$ de classe C^r dont toutes les dérivées d'ordre $\leqslant r$ sont bornées par 1, si l'on note $X = \mathrm{Im}(\phi)$, alors $X(\mathbb{Q}, T)$ est contenu dans au plus CT^ϵ hypersurfaces de degré $\leqslant d$. De plus, $\epsilon(d)$ tend vers 0 lorsque d tend vers l'infini.

Démonstration. On note M_d la famille de tous les monômes $m(X, Y)$ en deux variables de degré $\leqslant d$:

$$M_d = \{m(X, Y) = X^a Y^b \mid a, b \in \mathbb{N},\, a + b \leqslant d\}$$

On pose $D = \#M_d = \frac{(d+1)(d+2)}{2}$. Si $A = \{\langle x_i, y_i\rangle \in \mathbb{R}^2 \mid 1 \leqslant i \leqslant D\}$, on note $M(A)$ la matrice carrée de taille D égale à $[m(a)]_{a\in A}^{m\in M_d}$. On note enfin $\Delta(A) = \det(M(A))$.

Pour mener à bien la démonstration, nous avons besoin des trois résultats suivants :

1. Si A n'est contenu dans aucune courbe algébrique de degré $\leqslant d$, alors $\Delta(A) \neq 0$.
2. Si $A \subset \mathbb{Q}^2$, si $\forall a \in A$, $H(a) \leqslant T$, et si $\Delta(A) \neq 0$; alors $\Delta(A) \geqslant \frac{1}{T^{dD}}$.
3. $\exists r = r(d) \in \mathbb{N}$ tel que si $\phi : (0, 1) \to \mathbb{R}^2$ est une fonction de classe C^r dont toutes les dérivées d'ordre $\leqslant r$ sont bornées par 1, on prend $I \subset (0, 1)$ un intervalle et $t_1, \cdots, t_D \in I$ distincts. On considère $A = \{\phi(t_i) \mid 1 \leqslant i \leqslant D\}$; alors il existe une constante $K = K(d) \in \mathbb{R}$ telle que :

$$\Delta(A) \leqslant K \cdot |I|^{\frac{D(D-1)}{2}}$$

   Où $|I|$ dénote la longueur de l'intervalle I.

Nous allons terminer la preuve de la proposition A.1 en utilisant ces résultats que nous démontrerons par la suite.

Soient $r(d)$ comme dans l'énoncé de 3, ϕ comme dans l'énoncé de la A.1, $I \subset (0, 1)$ un intervalle, on note $X_I = \phi[I] \subset X$. On suppose que $X_I(\mathbb{Q}, T)$ n'est contenu dans aucune courbe algébrique de degré $\leqslant d$. Puisqu'une courbe algébrique de degré d peut interpoler $D-1$ points, on sait que $X_I(\mathbb{Q}, T)$ contient au moins D points distincts ; de plus si l'on prend $D - 1$ points distincts dans $X_I(\mathbb{Q}, T)$, ceux-ci définissent une courbe algébrique de degré d, on peut donc trouver un autre point de $X_I(\mathbb{Q}, T)$ qui ne soit pas dans cette courbe, autrement dit on prend $t_1, \cdots, t_D \in I$ distincts tels que $\phi(t_i) \in X_I(\mathbb{Q}, T)$ pour $1 \leqslant i \leqslant D$, et tel que $A = \{\phi(t_i) \mid 1 \leqslant i \leqslant D\}$ ne soit contenu dans aucune courbe algébrique de degré $\leqslant d$.

Par 1, on sait que $\Delta(A) \neq 0$.

Par 2 et 3, on sait que :

$$\frac{1}{T^{dD}} \leqslant \Delta(A) \leqslant K\,|I|^{\frac{D(D-1)}{2}}$$

Ce qui nous donne :

$$|I| \geqslant K^{-\frac{2}{D(D-1)}} T^{-\frac{2d}{D-1}} = B(T, d)$$

Par contaposé, si $|I| < B(T,d)$, alors $X_I(\mathbb{Q}, T)$ est contenu dans une courbe algébrique de degré $\leqslant d$. On recouvre $(0,1)$ par $1 + \frac{1}{B(T,d)}$ intervalles de longueur $< B(T,d)$; ainsi $X_I(\mathbb{Q}, T)$ est contenu dans l'union d'au plus $1 + \frac{1}{B(T,d)}$ courbes algébriques.

Or $B(T,d) \sim C(d)T^{\frac{2}{d}}$, donc le théorème est démontré avec $\epsilon(d) \sim \frac{1}{d}$, qui tend vers 0 quand d tend vers l'infini. $\square$

Preuve du 1 On va montrer la contraposée : si $\Delta(A) = 0$, alor sil existe une courbe algébrique de degré $\leqslant d$ contenant A. Ceci est dû au fait que si $\Delta(A) = 0$, alors il existe une relation algébrique entre les points de A. Comme on peut toujours définir une courbe algébrique de degré $\leqslant d$ passant par $D - 1$ points indépendants, on peut trouver une courbe algébrique passant par tous les points de A. Pour plus de détails, on peut se référer à [2].

Preuve du 2 On pose : $A' = T^d A$, qui est une matrice à coefficients dans $\mathbb{Z}$, donc son déterminant est entier. Comme $\det(A') = T^{dD} \det(A) \neq 0$, on a $|\det(A')| \geqslant 1$, donc $|\det(A')| \geqslant \left|\frac{1}{T^{dD}}\right|$.

Preuve du 3 On va montrer que $r(d) = D$ convient. Soient $I \subset (0,1)$ un intervalle et $t_1, \cdots, t_D \in I$ distincts. Soient de plus $f_1, \cdots, f_D$ des fonctions dans $C^D(I)$. On note V le déterminant de Vandermonde :

$$V = \det \begin{pmatrix} 1 & t_1 & t_1^2 & \cdots & t_1^D \\ \vdots & & & & \\ 1 & t_2 & t_2^2 & \cdots & t_D^D \end{pmatrix} = \prod_{i<j} (t_i - t_j)$$

On a alors les résultats suivants :

(a) $V \leqslant |I|^{\frac{D(D-1)}{2}}$

(b) $\forall i, j,\ \exists \zeta_{i,j} \in I$ tel que :

$$\det[f_j(t_i)]_{1 \leqslant i,j \leqslant D} = V \cdot \det[\frac{f_j^{(i)}(\zeta_{i,j})}{i!}]_{1 \leqslant i,j \leqslant D}$$

(a) vient naturellement par le calcul, et (b) est une généralisation du théorème des accroissements finis.

On considère désormais $\phi : (0,1) \to \mathbb{R}^2$ est une fonction de classe C^r dont toutes les dérivées d'ordre $\leqslant r$ sont bornées par 1, et on pose $A = \{\phi(t_i) \mid 1 \leqslant i \leqslant D\}$. Les coefficients de la matrice $M(A)$ sont donc de la forme $\phi_1(t_i)^a \phi_2(t_i)^b$, avec $a+b \leqslant d$. On définit a_i et b_i de telle sorte que $M_d = \{X^{a_i}Y^{b_i} \mid 1 \leqslant i \leqslant D\}$. On définit alors f_j pour $1 \leqslant j \leqslant D$ par :

$$f_j(x) = \phi_1(x)^{a_j}\phi_2(x)^{b_j}$$

Puisque ϕ est de classe C^D, f_j est aussi de classe C^D.

Par (b), $\Delta(A) = \det[f_j(t_i)]_{1\leqslant i,j\leqslant D} \leqslant V \cdot K$, où $K = K(d)$ est un majorant de $\det[\frac{f_j^{(i)}(x)}{i!}]_{1\leqslant i,j\leqslant D}$, qui existe et ne dépend pas de ϕ puisque toutes les dérivées de ϕ sont bornées par 1.

Enfin par (a) : $\Delta(A) \leqslant K \cdot |I|^{\frac{D(D-1)}{2}}$. □

B Utilisation de la saturation

Plusieurs fois au cours de la démonstration du théorème de Pila-Wilkie, des arguments de saturation sont utilisés pour s'assurer que l'on a des bornes finies. Nous allons développer dans le détail les arguments utilisés.

B.i Borne uniforme d'une famille définissable

Au début de la partie 2.5, nous avons une famille définissable de fonctions $(F_t)_{t\in(0,1)}$, dont on sait qu'à t fixé, elles sont C^r, fortement bornées et à dérivées fortement bornées. Autrement dit, on sait :

$$\forall t \in (0,1)\ \exists N_t \in \mathbb{N} \text{ tel que } \forall x \in (0,1)\ \forall i \in \{1, \cdots, r\}\ \left|F_t^{(i)}(x)\right| \leqslant N_t$$

Cependant, rien ne dit a priori qu'il existe une borne fonctionnant pour tous les t à la fois. N_t pourrait tendre vers l'inifini quand $t \to 0$ par exemple, nous allons montrer que ce n'est pas la cas. Nous allons raisonner par l'absurde, en supposant :

$$\forall N \in \mathbb{N}\ \exists x, t \in (0,1)\ \exists i \in \{1, \cdots, r\} \text{ tels que } \left|F_t^{(i)}(x)\right| > N$$

On considère alors le type $p(t) = \{\phi_k(t) \mid k \in \mathbb{N}\}$, où $\phi_k(t)$ est la formule « $0 < t < 1 \wedge \exists x(0 < x < 1 \wedge \bigvee_{0\leqslant i\leqslant r} \left|F_t^{(i)}(x)\right| > k)$ ». Il est finiment satisfaisable par l'hypothèse de notre raisonnement par l'absurde, d'autre part, chaque $\phi_k(t)$ a les mêmes paramètres que ceux qui entrent dans la définition de F_t ; or $(F_t)_{t\in(0,1)}$ est une famille définissable, par conséquent ces paramètres ne dépendent pas de t, et donc $p(t)$ est un type à paramètres finis. Puisque M est $\aleph_0$-saturée, il est réalisé par un certain $t_0 \in M$; on a donc $M \models \phi_N(t_0)$ pour chaque $N \in \mathbb{N}$, autrement dit :

$$\forall N\in\mathbb{N}\,\exists x\in(0,1)\,\exists i\in\{1,\cdots,r\}\text{ tels que }\left|F_{t_0}^{(i)}(x)\right|>N$$

Or ceci contredit la bornitude de F_{t_0}. $\square$

B.ii Famille définissable de reparamétrisations

On rappelle qu'une r-reparamétrisation d'une fonction $f : X \to M^n$ est un ensemble S fini de fonctions $\phi : (0,1)^{\dim(X)} \to X$ définissables et telles que ϕ et $f \circ \phi$ soient C^r, à dérivées d'ordre $\leqslant r$ fortement bornées, et avec $\bigcup_{\phi\in S} \mathrm{Im}(\phi) = X$.

À une fonction $F = \langle F_1, \cdots, F_n\rangle : (0,1)^k \to M^n$, on peut associer l'ensemble de ses fonctions coordonnées. On dira alors que F est une fonction r-reparamétrisant f si l'ensemble de ses fonctions coordonnées forme une r-reparamétrisation de f.

Dans la démonstration du lemme 2.5.2, on considère une famille définissable $(g_t)_{t\in(0,1)}$ de fonctions $g_t : (0,1) \to (0,1)^m \times M$. On souhaite obtenir une « famille définissable de r-reparamétrisations de g », c'est-à-dire un certain nombre N fini de familles définissables $({}^{(1)}\phi_t)_{t\in(0,1)}, \cdots, ({}^{(N)}\phi_t)_{t\in(0,1)}$ de fonctions ${}^{(i)}\phi_t : (0,1) \to (0,1)$ telles que l'ensemble $S_t = \{{}^{(i)}\phi_t \mid 1 \leqslant i \leqslant N\}$ soit une r-reparamétrisation de g_t pour chaque t.

De manière équivalente, on souhaite montrer qu'il existe une famille définissable $(\Phi_t)_{t\in(0,1)}$, où à t fixé Φ_t est une fonction r-reparamétrisant g_t.

À t fixé, on applique le théorème de reparamétrisation dans le cas d'arité 1 (corollaire 2.4.6) à la fonction g_t pour obtenir une r-reparamétrisation g_t, que l'on note S_t, et l'on note Φ_t la fonction r-reparamétrisant g_t dont les coordonnées sont les fonctions dans S_t. Nous allons procéder en deux étapes :

1. Montrer que l'on peut prendre, à t fixé, Φ_t définissable avec les mêmes paramètres que g_t,
2. Montrer qu'il existe une famille A-définissable de r-reparamétrisations.

Preuve du 1 Soient $f : (0,1) \to M^{m+1}$ définissable et soit A l'ensemble des paramètres intervenant dans la définition de f. En appliquant le théorème de reparamétrisation, on obtient S, une r-reparamétrisation de f. On note $k = \#S$.

Pour $\phi \in S$ et pour $0 \leqslant i \leqslant r$, les fonctions $\phi^{(i)}$ et $(f\circ\phi)^{(i)}$ sont bornées respectivement par les entiers $C_{i,\phi}$ et $C_{i,f\circ\phi}$. On pose :

$$C = \max_{0\leqslant i\leqslant r, \phi\in S}(C_{i,\phi}, C_{i,f\circ\phi})$$

On note Φ la fonction r-reparamétrisant f associée à S. Φ est définie par une certaine formule $\psi(x, y, b)$, où $x \in M$ et $y \in M^k$ sont des variables, et $b \in M^\ell$ est un vecteur de paramètres. Pour $1 \leqslant i \leqslant k$, on note $\pi_i : M^k \to M$ la projection sur la $i^{\text{ème}}$ coordonnée. Pour une variable $z \in M^\ell$, on considère la formule suivante :

$$\begin{aligned}\circledast(z) : \{\langle x,y\rangle \mid \psi(x,y,z)\} &\text{ est le graphe d'une fonction, notée } h\\ &\wedge h \text{ est } C^r \wedge \bigwedge_{0\leqslant i\leqslant r} \forall x \left|h^{(i)}(x)\right| \leqslant C\\ &\wedge f\circ\pi_1\circ h \text{ est } C^r \wedge \bigwedge_{0\leqslant i\leqslant r} \forall x \left|(f\circ\pi_1\circ h)^{(i)}(x)\right| \leqslant C\\ &\vdots\\ &\wedge f\circ\pi_k\circ h \text{ est } C^r \wedge \bigwedge_{0\leqslant i\leqslant r} \forall x \left|(f\circ\pi_k\circ h)^{(i)}(x)\right| \leqslant C\end{aligned}$$

$\circledast(z)$ est une formule à paramètres dans A par la présence de f.

Comme Φ est une fonction r-reparamétrisant f, on a $M \vDash \circledast(b)$. Autrement dit, $M \vDash \exists z \circledast(z)$; puisque M admet des fonctions de choix définissables (théorème 1.5.2), on sait qu'il existe $c \in M^\ell$ tel que $\{c\}$ est A-définissable, et $M \vDash \circledast(c)$. Ceci nous dit qu'il existe une fonction A-définissable r-reparamétrisant f .

En notant A l'ensemble des paramètres intervenant dans la définition de la famille $(g_t)_{t\in(0,1)}$ et en prenant $f = g_t$ pour un certain t fixé, on trouve qu'il existe une r-reparamétrisation $A\cup\{t\}$-définissable de g_t. □

On prend dans la suite S_t (et doncΦ_t) $A\cup\{t\}$-définissables.

Preuve du 2 On vient de montrer qu'à t fixé, il existe une fonction $\Phi_t : (0,1) \to (0,1)^{N_t}$ $A\cup\{t\}$-définissable r-reparamétrisant g_t. On souhaite montrer qu'il existe une famille définissable de fonctions r-reparamétrisant la famille $(g_t)_{t\in(0,1)}$.

Pour $C \in \mathbb{N}$ et $f : M \to (0,1)$ A-définissable, on pose :

$$\circledast_{C,t}(f) : f \text{ et } g_t\circ f \text{ sont } C^r \wedge \bigwedge_{0\leqslant i\leqslant r} \forall x \left|f^{(i)}(x)\right| \leqslant C \wedge \bigwedge_{0\leqslant i\leqslant r} \forall x \left|(g_t\circ f)^{(i)}(x)\right| \leqslant C$$

C'est une formule à paramètres dans A.

Soient $N \in \mathbb{N}^*$, $x, y \in (0,1)$ des variables, $t \in (0,1)$ fixé, et $\Psi = \langle\psi_1, \cdots, \psi_N\rangle$ un N-uplet de formules $\psi_i(x,y,t,a)$, où a est un vecteur listant les éléments de A. On considère la formule suivante :

$$\begin{aligned}\theta^{\Psi}_{N,C}(t) : &\text{ si pour chaque } 1 \leqslant i \leqslant N,\ \psi_i(x,y,t,a) \text{ définit une fonction notée } \phi_{i,t},\\ &\text{ et si } \circledast_{C,t}(\phi_{i,t})\,;\\ &\text{ alors } \bigcup_{1\leqslant i\leqslant N} \mathrm{Im}(\phi_{i,t}) \neq (0,1).\end{aligned}$$

C'est une formule à paramètres dans A qui dit entre autres que Ψ ne définit pas une r-reparamétrisation de g_t.

On suppose par l'absurde qu'il n'existe pas de famille définissable de r-reparamétrisations de g. Cela implique que si l'on a une famille $(F_t)_{t\in(0,1)}$ A-définissable de fonctions $F_t : (0,1) \to (0,1)^{N_t}$ C^r, à dérivées d'ordre $\leqslant r$ fortement bornées et telles que $g_t \circ \pi_i \circ F_t$ soit C^r, à dérivées d'ordre $\leqslant r$ fortement bornées ; alors il existe un certain t_0 pour lequel :

$$\bigcup_{1\leqslant i\leqslant N_{t_0}} \mathrm{Im}(\pi_i \circ F_{t_0}) \neq (0,1)$$

On considère alors le type suivant :

$$p(t) = \{\theta^{\Psi}_{N,C}(t) \mid N, C \in \mathbb{N}^*,\ \Psi = \langle \psi_1, \cdots, \psi_N \rangle\}$$

Ce type est à paramètres dans A et est finiment satisfaisable ; en effet, si l'on considère une formule $\theta^{\Psi}_{N,C}$ seule, deux cas sont possibles :

— Pour un certain t_0 et pour un certain i, $\psi_i(x,y,t,a)$ ne définit pas une fonction vérifiant $\circledast_{C,t}$; alors $M \vDash \theta^{\Psi}_{N,C}(t_0)$.

— Pour tout t et tout i, $\psi_i(x,y,t,a)$ définit une fonction vérifiant $\circledast_{C,t}$; alors Ψ définit une famille A-définissable de fonctions. Comme cette famille ne peut pas être une famille de fonctions r-reparamétrisant g, il y a forcément un t_0 pour lequel $M \vDash \theta^{\Psi}_{N,C}(t)$.

Désormais, on considère deux formules $\theta^{\Psi_1}_{N_1,C_1}$ et $\theta^{\Psi_2}_{N_2,C_2}$, et on suppose qu'elles ne sont jamais réalisées par le même élément simultanément. Alors la fonction définie par :

$$F_t = \begin{cases} \Psi_1(x,y,t,a) & \text{si } t \text{ réalise } \theta^{\Psi_2}_{N_2,C_2} \\ \Psi_2(x,y,t,a) & \text{sinon} \end{cases}$$

est une famille définissable de fonctions r-reparamétrisant g, ce qui contredit l'hypothèse de notre raisonnement par l'absurde. On raisonne de même pour n'importe quel nombre de formules.

Par saturation p est réalisé par un certain $t_0 \in (0,1)$, autrement dit, pour tout $N, C \in \mathbb{N}^*$, et pour tout $\Psi = \langle \psi_1, \cdots, \psi_N \rangle$, $M \vDash \theta^{\Psi}_{N,C}(t_0)$. Or ceci contredit l'existence de la fonction Φ_{t_0} A-définissable r-reparamétrisant g_{t_0}.

On a alors montré par l'absurde qu'il existe une famille A-définissable de r-reparamétrisations de g. $\square$

L'argument est similaire dans la partie 2.6, la seule différence étant qu'il est appliqué à une famille $F_u : (0,1)^m \to M$.

Références

[1] Derya Ciray. On the pila-wilkie counting theorem. 2014. Pisa seminar.

[2] Michel Coste. Systèmes d'équations linéaires et courbes passant par des points fixés. http://agreg-maths.univ-rennes1.fr/documentation/docs/CayBach.pdf. Last checked : 2018-08-26.

[3] Adrien Deloro. Logique pour mathématiciens. `https://webusers.imj-prg.fr/~adrien.deloro/teaching-archive/4M232-2015.pdf`, 2015. Last checked : 2018-08-05.

[4] L. P. D. van den Dries. *Tame Topology and O-minimal Structures*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1998.

[5] A. M. Gabriélov. Projections of semi-analytic sets. *Functional Analysis and Its Applications*, 2(4) :282–291, Oct 1968.

[6] A J. WILKIE. Model completeness results for expansions of the ordered field of real numbers by restricted pfaffian functions and the exponential function. pages 628–671, 08 2003.

[7] D. Masser and U. Zannier. Torsion anomalous points and families of elliptic curves. *American Journal of Mathematics*, 132(6) :1677–1691, 12 2010.

[8] J. Pila and A. J. Wilkie. The rational points of a definable set. *Duke Math. J.*, 133(3) :591–616, 06 2006.

[9] Jonathan Pila. Integer points on the dilation of a subanalytic surface. 55, 06 2004.

[10] Jonathan Pila. O-minimality and the André-Oort conjecture for $\mathbb{C}^n$. *Ann. of Math.*, 173(3) :1779–1840, 2011.

[11] Jonathan Pila and Umberto Zannier. Rational points in periodic analytic sets and the manin-mumford conjecture. 2008.

[12] Julia Robinson. Definability and decision problems in arithmetic. *J. Symbolic Logic*, 14(2) :98–114, 06 1949.

[13] Thomas Scanlon. Counting special points : Logic, diophantine geometry, and transcendence theory. 49, 01 2012.

[14] Katrin Tent and Martin Ziegler. *A Course in Model Theory*. Lecture Notes in Logic. Cambridge University Press, 2012.

[15] Lou van den Dries and Chris Miller. On the real exponential field with restricted analytic functions. *Israel Journal of Mathematics*, 85(1) :19–56, Feb 1994.

[16] Lou van den Dries and Chris Miller. Geometric categories and o-minimal structures. *Duke Math. J.*, 84(2) :497–540, 08 1996.

[17] A. J. Wilkie. *Rational points on definable sets*, page 41–65. London Mathematical Society Lecture Note Series. Cambridge University Press, 2015.