Trouver efficacement un point représentatif par composante connexe d'une variété algébrique réelle : l'état de l'art

Lebreton Romain encadré par
N. Vorobjov, Computer Science Departement, University of Bath
M. Giusti, Laboratoire Lix, École Polytechnique

3 octobre 2008

Notre problématique se situe dans l'étude informatisée des systèmes d'équations polynomiales à plusieurs variables et de leurs solutions, les variétés algébriques. L'étude des variétés algébriques est un domaine de mathématiques : la géométrie algébrique. Cependant les réponses de la géométrie algébrique ne sont pas toujours effectives, encore moins efficaces. La géométrie algébrique effective tend à combler cette lacune ; elle reprend les questions de la géométrie algébrique sous ce nouvel angle. Par exemple, le problème de l'appartenance à un idéal a conduit à la notion de base de Gröbner. La géométrie algébrique effective vient aussi de l'ingénierie. Elle vise à fournir des moyens de compréhension des modèles impliquant des systèmes d'équations polynomiales à plusieurs variables. La majorité des problèmes tels que la résolution des systèmes polynômiaux, la détermination de la dimension de leurs solutions ou le tracé de courbes sur une variété reliant deux points donnés, ont été résolus algorithmiquement. La recherche porte aujourd'hui d'avantage sur l'efficacité pour pouvoir traiter un plus grand champ de problèmes concrets.

La détection d'au moins un point par composante connexe d'une variété algébrique réelle est une problématique fondamentale dans l'étude informatisée des variétés algébriques réelles. Elle permet de borner le nombre de composantes connexes d'une variété. Elle ouvre la voie aux algorithmes qui calculent exactement le nombre de composantes connexes, et ceux qui décident s'il y a un chemin tracé sur une variété reliant deux points donnés. Nous tirons partie d'un nouvel algorithme de résolution des systèmes polynômiaux pour améliorer la complexité théorique et pratique de notre problème. Dans ce rapport, nous nous restreignons aux cas des variétés réelles *lisses*.

Les algorithmes de recherche d'un point par composante connexe d'une variété algébrique réelle S consistent à choisir de bonnes équations pour définir une sous-variété de S qui coupe chacune de ses composantes connexes. Rajouter des équations sert à baisser la dimension de l'objet géométrique jusqu'à ce qu'il soit un ensemble fini de points. Il ne reste plus qu'à résoudre ces équations pour avoir nos points représentatifs. Les algorithmes précédents utilisent pour la résolution des systèmes polynômiaux des outils basés sur le calcul de base de Gröbner. Les bases de Gröbner sont un outil très général qui s'applique sur tout système polynomial. En contrepartie, les algorithmes de calcul de bases de Gröbner ne tiennent pas compte des "bons" systèmes d'équations. Notre approche consiste à éviter les bases de Gröbner pour améliorer la complexité sur un certain ensemble de systèmes. Pour cela, nous utilisons *l'algorithme de résolution géométrique* pour la résolution des équations. Le premier avantage de cet algorithme

est qu'il n'utilise pas la représentation dense des polynômes. Il se sert d'une structure de données qui voit le polynôme comme une fonction qui s'évalue bien. L'autre avantage est que sa complexité est quadratique en un paramètre intrinsèque, le degré géométrique du système. Cependant l'outil ne s'applique qu'à des systèmes d'équations particuliers. C'est pourquoi nous étudions dans cet article comment trouver des équations supplémentaires qui satisfont les hypothèses de l'algorithme de résolution géométrique.

Notre approche de la question présente de nombreux avantages. D'abord nous obtenons une nouvelle complexité pour notre problème. Cette complexité tient compte de paramètres intrinsèques, tels que la complexité d'évaluation de nos équations et le degré géométrique générique des variétés polaires associées à S. Ensuite des implémentations du nouvel algorithme et d'un algorithme précédent ont été comparées sur un problème concret. Les résultats valident notre approche sur cet exemple. D'un autre côté, nos résultats ne sont valables que pour des systèmes d'équations particuliers. De plus notre approche est basé sur le fait que beaucoup de systèmes ne sont pas généraux, par exemple les polynômes sont creux. Cela convient à de nombreux problèmes de modélisation mais sans doute moins à la cryptographie multivariée où les équations sont choisies pour leur manque de bonnes propriétés. Finalement notre algorithme est probabiliste. Même si l'ensemble des paramètres de l'algorithme donnant de mauvais résultats est de mesure nulle dans les réels, le résultat n'est pas certifié.

L'approche étudiée dans ce mémoire a fourni une alternative aux algorithmes existants avec une meilleure efficacité sur une classe de problème. De plus, l'algorithme de résolution géométrique a créé une nouvelle approche plus géométrique pour la résolution d'autres problèmes de géométrie algébrique effective. La suite logique de ce mémoire est d'étendre notre algorithme aux variétés non lisses. Une autre piste est l'étude du bon comportement de l'algorithme de résolution géométrique par rapport aux systèmes d'équations invariantes sous certaines transformations.

Le corps du mémoire a été rédigé en anglais. Ceci était un des objectifs du stage qui s'est déroulé en Angleterre. Le mémoire est précédé du résumé en Français qui suit. Pour les preuves des propositions du résumé, nous renvoyons au mémoire en anglais.

Prolégomènes

L'objet de ce mémoire est d'étendre le domaine des applications de l'algorithme de résolution géométrique à la recherche d'un point représentatif par composante connexe d'une variété algébrique réelle S lisse. Pour cela nous allons introduire la notion de *variété polaire affine généralisée*, qui nous fournira les objets géométriques qu'utilisera l'algorithme de résolution géométrique.

Bien que nous souhaitons travailler avec des variétés algébriques affines réelles, la notion de variété polaire est projective et les corps algébriquement clos offrent un bon cadre pour la géométrie algébrique. Ainsi nous ferons un détour par l'espace projectif complexe. Soit $\mathbb{P}^n := \mathbb{P}^n(\mathbb{C})$ l'espace projectif complexe de dimension n. Pour tout sous-espace linéaire A et B de $\mathbb{P}^n$, nous notons $\langle A, B\rangle$ l'espace linéaire engendré par A et B. Les espaces A et B s'intersectent transversalement, ce que l'on note $A \pitchfork B$, si $\langle A, B\rangle = \mathbb{P}^n$. Dans le cas contraire, on note $A \not\pitchfork B$. Notons V une variété projective complexe de codimension pure p, *ie* telle que chacune de ses composantes irréductibles soient de codimension p, où $0 \leqslant p \leqslant n$. Écrivons V_{reg} pour l'ensemble des points réguliers (lisses) de V. Nous notons $V_{sing} := V \backslash V_{reg}$ le lieu singulier de V. Pour tout $M \in V_{reg}$, l'espace tangent $T_M V$ est vu comme un espace linéaire de $\mathbb{P}^n$ contenant M.

Viennent ensuite les notions équivalentes dans le cas affine. Nous fixons une inclusion $\mathbb{A}^n \subseteq \mathbb{P}^n$ et nous posons $H := \mathbb{P}^n \backslash \mathbb{A}^n$ l'hyperplan à l'infini. Soient $\vec{A}$ et $\vec{B}$ deux sous-espaces vectoriels de $\mathbb{A}^n$. Nous notons $\vec{A} \pitchfork \vec{B}$ si $\vec{A} + \vec{B} = \mathbb{A}^n$. Soient S une variété algébrique affine et V sa clôture projective. Nous posons $S_{reg} := V_{reg} \cap \mathbb{A}^n$ et $S_{sing} := V_{sing} \cap \mathbb{A}^n$ respectivement l'ensemble des points lisses et le lieu singulier de la variété affine S. Pour tout point lisse M de la variété affine S, nous définissons $T_M S := T_M V \cap \mathbb{A}^n$ l'espace tangent affine de S au point M.

Pour tout espace linéaire $A \subseteq \mathbb{P}^n$ de dimension a, nous notons $A^\perp$ l'orthogonal de A pour le produit scalaire usuel. La dimension de $A^\perp$ est $n - 1 - a$. Si A est un sous-espace linéaire de H, nous posons $A^* := A^\perp \cap H$ son orthogonal dans l'hyperplan. La dimension de A^* est $n - a - 2$.

Variétés Polaires Généralisées

À présent nous allons présenter la notion de variété polaire généralisée contenue dans l'espace projectif $\mathbb{P}^n$. Ces variétés polaires sont associées à un drapeau donné $\mathcal{K}$ d'espaces linéaires projectifs ainsi qu'à un hyperplan H de $\mathbb{P}^n$. Fixons pour le drapeau donné la notation

$$\mathcal{K} : \qquad \mathbb{P}^n \supsetneq K^{n-1} \supsetneq \cdots \supsetneq K^{n-p-1} \supsetneq \cdots \supsetneq K^1 \supsetneq K^0.$$

Pour tout élément K d'un drapeau $\mathcal{K}$ et pour tout hyperplan H, nous définissons la *variété polaire généralisée* $\widehat{W}_K(V)$ associé à K comme étant la clôture de Zariski de l'ensemble

$$\left\{ M \in V_{reg} \backslash (H \cup K) \mid T_M V \not\pitchfork \left(\langle M, K\rangle \cap H \right)^* \right\}. \tag{1}$$

Remarquons que $\widehat{W}_K(V)$ est inclus dans V. De plus le point M est supposé en dehors de $H \cup K$ de telle sorte que $\langle M, K\rangle \cap H$ soit toujours de dimension $\dim K$. Les variétés polaires généralisées associées à $\mathcal{K}$ forment une suite décroissante :

$$V = \widehat{W}_{K^{n-1}} = \cdots = \widehat{W}_{K^{n-p}} \supseteq \widehat{W}_{K^{n-p-1}} \supseteq \cdots \supseteq \widehat{W}_{K^1} \supseteq \widehat{W}_{K^0}.$$

Pour $1 \leqslant i \leqslant n-p$, nous notons $\widehat{W}_{K^{n-p-i}}(V)$ la *i-ème variété polaire généralisée* de V associée au drapeau $\mathcal{K}$ et à l'hyperplan H. L'indice i indique la codimension attendue de $\widehat{W}_{K^{n-p-i}}(V)$ dans V. Observons que la *partie utile* du drapeau $\mathcal{K}$ donnant lieu à des variétés polaires non triviale est comprise entre K^0 et K^{n-p-1}.

Soit K un élément de $\mathcal{K}$ et posons H l'hyperplan à l'infini de $\mathbb{A}^n \subseteq \mathbb{P}^n$. Nous posons $\widehat{W}_K(S) := \widehat{W}_K(V) \cap \mathbb{A}^n$ la variété *affine* polaire généralisée associée à K.

Deux types particuliers de drapeaux méritent d'être soulignés. Le premier type est celui des drapeaux

$$\mathcal{K} : \qquad \mathbb{P}^n \supsetneq K^{n-1} \supsetneq \cdots \supsetneq K^{n-p-1} \supsetneq \cdots \supsetneq K^1 \supsetneq K^0$$

avec $K^{n-1} = H$. Nous les appelons *drapeaux internes*. Pour un élément fixé K de $\mathcal{K}$, posons $L := K^*$. Nous déduisons facilement que la variété affine polaire généralisée $\widehat{W}_K(S)$ est la clôture de Zariski dans $\mathbb{A}^n$ de l'ensemble

$$\left\{ M \in S_{reg} \mid \overrightarrow{T_M S} \not\pitchfork \vec{L} \right\}. \tag{2}$$

Ainsi $\widehat{W}_K(S)$ est exactement la *variété polaire classique* de S associée à l'espace vectoriel $\vec{L}$. Nous renvoyons à [BGHP04] pour plus de détail sur les variétés polaires classiques.

Le deuxième type de drapeaux, nommés *drapeaux externes* sont les drapeaux

$$\mathcal{K} : \qquad \mathbb{P}^n \supsetneq K^{n-1} \supsetneq \cdots \supsetneq K^{n-p-1} \supsetneq \cdots \supsetneq K^1 \supsetneq K^0$$

où $K^0 \notin H$. Nous nommons P l'unique point de K^0. La variété polaire affine $\widehat{W}_K(S)$ correspond alors à la clôture de Zariski dans $\mathbb{A}^n$ de

$$\left\{ M \in S_{reg} \backslash (\tilde{K}) \mid \overrightarrow{T_M S} \not\pitchfork \left(\overrightarrow{MP} + \vec{K} \right)^{\perp} \right\} \tag{3}$$

où $\tilde{K} := K \cap \mathbb{A}^n$ est la partie affine de K.

Variétés polaires réelles

Une variété polaire affine réelle $\widehat{W}_K(S_{\mathbb{R}})$ peut être vide. Mais dans les cas que nous considérons, elle coupe chaque composante connexe de $S_{\mathbb{R}}$ et sera donc non vide si $S_{\mathbb{R}} \neq \emptyset$.

Considérons en premier, le cas des drapeaux externes. Nous rappelons que $K \subseteq H$ et que l'on pose $L := K^*$. Nous déduisons de l'équation (2) que $\widehat{W}_K(S_{\mathbb{R}})$ est la clôture de Zariski dans $\mathbb{A}^n$ de l'ensemble

$$\left\{ M \in (S_{\mathbb{R}})_{reg} \mid \overrightarrow{T_M S_{\mathbb{R}}} \not\pitchfork \vec{L} \right\}.$$

Proposition 1. *Soit $S_{\mathbb{R}}$ une variété algébrique réelle $\mathbb{R}$-définissable lisse et compacte. Alors $\widehat{W}_K(S_{\mathbb{R}})$ contient au moins un point par composante connexe de $S_{\mathbb{R}}$.*

Démonstration. Fixons $\vec{v} \in K \subseteq H$. Par définition $L \subseteq (\vec{v})^{\perp}$. Supposons que $\vec{v}$ soit la direction du premier axe de coordonnées. Considérons la fonction qui d'une composante connexe C de la variété $S_{\mathbb{R}}$ dans $\mathbb{R}$ associe à un point M sa première coordonnée. Cette fonction est continue et atteint son maximum sur le compact C au point P. Ainsi l'espace vectoriel $\overrightarrow{T_P S_{\mathbb{R}}}$ est inclus dans $(\vec{v})^{\perp}$. Nous avons donc $\overrightarrow{T_P S_{\mathbb{R}}} + \vec{L} \neq \mathbb{A}^n_{\mathbb{R}}$ et $P \in \widehat{W}_K(S_{\mathbb{R}}) \cap C$. □

Intéressons nous maintenant au cas des drapeaux externes. Nous pouvons alors enlever l'hypothèse S compacte.

Proposition 2. *Soit $S_{\mathbb{R}}$ une variété algébrique réelle $\mathbb{R}$-définissable lisse. Supposons que $K \not\subseteq S_{\mathbb{R}}$. Alors $\widehat{W}_K(S_{\mathbb{R}})$ contient au moins un point par composante connexe de $S_{\mathbb{R}}$.*

Démonstration. Puisque K n'est pas inclus dans $S_{\mathbb{R}}$, il existe un point $P \in K \backslash S_{\mathbb{R}}$. Fixons une composante connexe C de $S_{\mathbb{R}}$. Comme C est un fermé, sa distance au point P est atteinte en un point $M \in C$. Comme P n'appartient pas à $S_{\mathbb{R}}$, nous avons $\overrightarrow{MP} \neq 0$.

Le gradient de la fonction distance au point P en M est colinéaire à $\overrightarrow{MP}$ et est orthogonal à l'espace tangent $\overrightarrow{T_M S_{\mathbb{R}}}$ d'après le Théorème des multiplicateurs de Lagrange. C'est pourquoi l'espace vectoriel $\overrightarrow{T_M S_{\mathbb{R}}}$ est contenu dans $(\overrightarrow{MP})^{\perp}$ et ainsi M appartient à $\widehat{W}_K(S_{\mathbb{R}}) \cap C$. □

Premières équations décrivant les variétés polaires affines

Nous utilisons les coordonnées homogènes $x := (x_0 : x_1 : \ldots : x_n)$ pour les points de l'espace projectif. Quand $x_0 = 1$, nous noterons le point correspondant dans $\mathbb{A}^n$ par $(x_1, \ldots, x_n) := (1 : x_1 : \ldots : x_n)$.

Soient $F_1, \ldots, F_p \in \mathbb{Q}[X_1, \ldots, X_n]$ des polynômes à coefficients rationnels. Supposons que $F_1, \ldots, F_p$ forment une suite régulière et que l'idéal qu'ils engendrent est radical. Soit S la variété réelle qu'ils définissent. À partir de maintenant, nous supposons que la variété affine S est définie par $F_1, \ldots, F_p$, *ie* $S := V(F_1, \ldots, F_p)$. De plus, nous supposons que $F_1, \ldots, F_p$ *s'intersectent transversalement*, ce qui signifie que les équations ont une matrice jacobienne de rang maximal en tout point de S. De ce fait, S est une variété affine purement p-codimensionelle.

Fixons un indice $1 \leqslant i \leqslant n-p$ qui représente la codimension attendue de la variété polaire dans S. Choisissons des points $A_j = (a_{j,0} : \ldots : a_{j,n})$ avec $a_{j,0} \in \{0, 1\}$ et $1 \leqslant j \leqslant n-p-i+1$. Supposons que $A_1, \ldots, A_{n-p-i+1}$ engendrent un espace linéaire K de dimension $n-p-i$. Considérons la matrice

$$\Gamma^{(i)}(x) = \begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \cdots & \frac{\partial F_p}{\partial X_n} \\ a_{1,1} - a_{1,0}X_1 & \ldots & a_{1,n} - a_{1,0}X_n \\ \vdots & \vdots & \vdots \\ a_{n-p-i+1,1} - a_{n-p-i+1,0}X_1 & \ldots & a_{n-p-i+1,n} - a_{n-p-i+1,0}X_n \end{bmatrix}(x).$$

Nous notons W la variété définie par les équations $F_1, \ldots\ F_p$ et tous les $(n-i+1)$-mineurs de la $((n-i+1) \times n)$-matrice $\Gamma^{(i)}$. La proposition suivante nous donne nos premières équations pour $\widehat{W}_K(S)$.

Proposition 3. *Supposons que $K \not\subseteq S$. Alors la variété affine polaire généralisée $\widehat{W}_K(S)$ est égale à W.*

Équations et propriétés locales de $\widehat{W}_K(S)$

Dans la suite nous supposons que $K \not\subseteq S$, ce qui ne restreint pas la généralité de nos propos. Soit $s = n - i + 1$. Pour tout sous-ensemble $I = \{k_1, \ldots, k_s\}$ de $\{1, \ldots, n\}$, nous noterons $M(I)$ le s-mineur qui correspond à toutes les lignes et aux colonnes $k_1, \ldots, k_s$ de la matrice $\Gamma^{(i)}$. Notons m le $(n-i)$-mineur principal de Γ.

Lemme 4 (Lemme d'échange)**.** *Soit $J = \{k_1, \ldots, k_s\}$ un ensemble de colonnes. Alors, pour de bons $\epsilon_j \in \{-1, 1\}$, $1 \leqslant j \leqslant n$, nous avons l'égalité suivante :*

$$m\ M(I) = \sum_{l \in J \backslash \{1,\ldots,n-i\}} \epsilon_j\ M(J \backslash \{l\})\ M(1, \ldots, n-i, l).$$

Notons $M_j := M(1, \ldots, n-i, j)$ pour $n-i+1 \leqslant j \leqslant n$. Ces équations jouent un rôle fondamental.

Proposition 5. *La variété polaire affine $\widehat{W}_K(S)$ est définie par les équations $F_1, \ldots, F_p$, $M_{n-i+1}, \ldots, M_n$ en dehors de $V(m)$.*

Démonstration. Soit M un point de S de coordonnées $x = (x_1, \ldots, x_n)$. Si $m(x) \neq 0$ et $M_{n-i+1}(x) = \ldots = M_n(x) = 0$, nous déduisons du lemme d'échange que $M(J)(x) = 0$ pour tout $J \in \mathcal{P}^n_{n-i+1}$. Donc tous les $(n-i+1)$-mineurs s'annulent en M et d'après la Proposition 3, $M \in \widehat{W}_K(S)$. La réciproque est immédiate. □

Il convient alors d'étudier ces équations pour en déduire les propriétés de $\widehat{W}_K(S)$. La variété polaire $\widehat{W}_{K^{n-p-i}}(S)$ n'est pas toujours de codimension i dans S. Ceci est dû au choix d'un mauvais espace K.

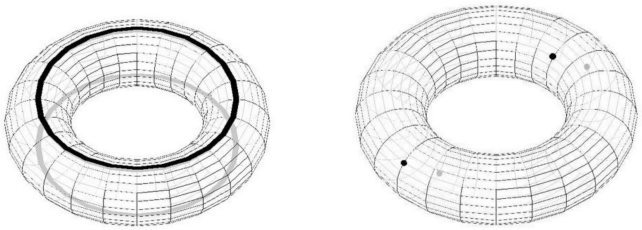

FIGURE 1 – Deux variétés polaires du tore associée chacune à une direction (i=2). À gauche, l'ensemble des points du tore où la normale est verticale est constitué de 2 courbes. La variété polaire est de mauvaise codimension. À droite, une variété pour une direction oblique est constituée de 4 points. Elle est de bonne codimension.

Dans toute la suite, l'espace K sera supposé générique. Le premier résultat est une conséquence d'un théorème de géométrie différentielle.

Proposition 6. *Pour presque tous les paramètres $a_{i,j}$ où $1 \leqslant i, j \leqslant n$, les équations $F_1, \ldots, F_p$, $M_{n-i+1}, \ldots, M_n$ se coupent transversalement sur $\widehat{W}_K(S) \backslash V(m)$.*

Ceci implique que la codimension locale de $\widehat{W}_K(S)$ dans S en tout point $M \notin V(m)$ est i. Le $(n-i)$-mineur principal m peut être remplacé par n'importe quel autre $(n-i)$-mineur supérieur de $\Gamma^{(i)}$. Il reste à voir que les ouverts $\{m \neq 0\}$, pour tous les mineurs m considérés, recouvrent S pour obtenir que $\widehat{W}_K(S)$ est bien de pure codimension i dans S.

Proposition 7. *Supposons que la variété polaire affine $\widehat{W}_{K^{n-p-i}}(S)$ est non vide. Alors pour toute composante irréductible C de $\widehat{W}_{K^{n-p-i}}(S)$ il existe un $(n-i)$-mineur supérieur m de $\Gamma^{(i)}$ tel que m ne s'annule pas identiquement sur C. Ainsi $\widehat{W}_{K^{n-p-i}}(S)$ est de pure codimension i dans S.*

Nous nous concentrons désormais sur la variété polaire zéro-dimensionnelle $\widehat{W}_{K^0}(S)$. Nous souhaitons trouver un mineur m qui ne s'annule en aucun point de $\widehat{W}_{K^0}$. Rappelons que m et $M_{p+1}, \ldots, M_n$ sont des mineurs de la matrice

$$\Gamma := \begin{bmatrix} \mathrm{Jac}(F(X)) \\ a_1 - X_1 \quad \ldots \quad a_n - X_n \end{bmatrix}$$

où $a_1, \ldots, a_n$ sont tirés au hasard pour avoir K^0 générique. En appliquant alors une transformation linéaire aléatoire $B \in \mathrm{GL}_n(\mathbb{R})$, nous définissons de nouvelles coordonnées $Z_1, \ldots, Z_n$ ainsi que de nouveaux polynômes $F_i(Z), 1 \leqslant i \leqslant p$, où l'on a remplacé $X_1, \ldots, X_n$ par leur expression en fonction de $Z_1, \ldots, Z_n$. On obtient aussi une nouvelle matrice

$$\mathrm{ExtJac} := \Gamma\ B = \begin{bmatrix} \mathrm{Jac}(F(Z)) \\ c_1 - Z_1 \quad \ldots \quad c_n - Z_n \end{bmatrix}$$

et de nouveaux mineurs m', $M'_{p+1}, \ldots, M'_n$ correspondants.

Proposition 8. *Supposons que $B \in GL_n(\mathbb{R})$ soit générique. Alors m' ne s'annule pas sur $\widehat{W}_{K^0}(S)$. Ainsi $F_1, \ldots, F_p$, $M'_{p+1}, \ldots, M'_n$ forment une suite régulière et engendrent l'idéal de définition de $\widehat{W}_{K^0}(S)$.*

Résolution réelle de systèmes polynômiaux

Les précédents résultats géométriques vont nous permettre d'étendre le champ d'application de *l'algorithme de résolution géométrique* suivant.

Soient $F_1, \ldots, F_n$ des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ tels que le système $F_1 = \ldots = F_n = 0$ ait un nombre fini de solutions complexes. Par résoudre, nous entendons calculer une représentation de l'ensemble des solutions de la forme

$$\{(v_1(T), \ldots, v_n(T)) \mid q(T) = 0\}$$

où $q \in \mathbb{Q}[T]$ est unitaire et séparable et les v_i, $1 \leqslant i \leqslant n$, sont des fonctions rationnelles univariées à coefficients rationnels. Cette présentation est appelée une *résolution géométrique*. Les racines réelles de q correspondent exactement aux solutions réelles.

L'algorithme de résolution géométrique tient compte de la complexité d'évaluation des polynômes $F_1, \ldots, F_n$. La complexité d'évaluation est le nombre d'opérations arithmétiques à effectuer pour évaluer un polynôme. Par exemple la complexité arithmétique $(X+1)(Y-2)+Z$ est au plus 4.

Nous posons $\delta = \max_i(\deg S_i)$ le degré géométrique maximum des variétés intermédiaires $S_i := \overline{V(F_1, \ldots, F_i) \backslash V(g)}$ pour $1 \leqslant i \leqslant n$. L'algorithme est incrémental sur le nombre d'équations. C'est pourquoi les variétés intermédiaires S_i interviennent. Le théorème suivant est un cas particulier du résultat principal de [GLS01] et [HMW01].

Théorème 9 (Algorithme de Résolution Géométrique)**.** *Soient $F_1, \ldots, F_n \in \mathbb{Q}[X_1, \ldots, X_n]$ de degré au plus d et dont la complexité d'évaluation est au plus L, tels que $F_1, \ldots, F_n$ forment une suite régulière et engendrent un idéal radical. Une résolution géométrique de la variété $\overline{V(F_1, \ldots, F_n) \backslash V(g)}$ peut être calculée en $\tilde{\mathcal{O}}((n^2 L + n^5) d^2 \delta^2)$ opérations arithmétiques dans $\mathbb{Q}$.*

L'algorithme sous-jacent est de type probabiliste. Sa validité dépend du choix de paramètres dans $\mathbb{Q}$. L'ensemble des mauvais choix est inclus dans une hypersurface algébrique, et donc presque tous les choix donnent lieu à un calcul valide.

Recherche d'au moins un point par composante connexe d'une variété algébrique réelle

Soit $S_{\mathbb{R}}$ une variété algébrique réelle. Supposons que $S_{\mathbb{R}} = V_{\mathbb{R}}(F_1, \ldots, F_p)$ où $F_1, \ldots, F_p \in \mathbb{Q}[X_1, \ldots, X_n]$ forment une suite régulière et engendrent un idéal radical. De ce fait, $S_{\mathbb{R}}$ est une variété algébrique affine réelle lisse de pure codimension p. Soit $S := V(F_1, \ldots, F_p)$ la variété algébrique complexe correspondante.

La variété polaire $\widehat{W}_{K^0}(S)$ pour un K^0 générique est zéro-dimensionnelle (Proposition 7) et contient au moins un point par composante connexe de S (Proposition 2). On tire au hasard le point $(1 : a_1 : \ldots : a_n) = K^0$ ainsi que la transformation $G \in \mathrm{GL}_n(\mathbb{Q})$. On obtient ainsi notre matrice ExtJac $:= \Gamma\ B$.

Une fois calculés les $(p+1)$-mineurs $M_{p+1}, \ldots, M_n$, on peut appliquer le Théorème 9 aux équations $F_1 = \ldots = F_p = M_{p+1} = \ldots = M_n = 0$ grâce à la Proposition 8. Notons $S_h := V(F_1, \ldots F_h)$, $1 \leqslant h \leqslant p$ et $\hat{S}_l := V(F_1, \ldots, F_p, M_{p+1}, \ldots, M_l)$, $1 \leqslant l \leqslant n-p$. Nous posons alors

$$\delta = max\left(max_{1 \leqslant h \leqslant p}(\deg\ S_h), max_{1 \leqslant l \leqslant n-p}(\deg\ \hat{S}_l)\right)$$

le degré géométrique maximum des variétés intermédiaires. Nous regroupons les résultats précédents dans le prochain théorème.

Théorème 10. *Soient $F_1, \ldots, F_p$ de degré au plus d et dont la complexité d'évaluation est au plus L, tels que $F_1, \ldots, F_p$ forment une suite régulière et engendrent un idéal de définition d'une variété S. Alors nous pouvons calculer en $\tilde{\mathcal{O}}(Ln^5p^2d^2\delta^2)$ opérations arithmétiques dans $\mathbb{Q}$ une résolution géométrique d'un ensemble $\hat{S}$ de points représentatifs de chaque composante connexe de S.*

Remarque 1. L'ordre des équations $F_1, \ldots, F_p, M_{p+1}, \ldots, M_n$ est important puisque pour tout $1 \leqslant l \leqslant n-p$, la variété intermédiaire $\hat{S}_l = V(F_1, \ldots, F_p, M_{p+1}, \ldots, M_l)$ est une variété polaire, donc un objet géométrique lié à S et que l'on peut espérer comprendre. D'ailleurs il apparaît que δ ne dépend pas du choix d'un drapeau externe et est donc un paramètre intrinsèque à la variété polaire S.

Remarque 2. Quand la variété S est supposé compacte, on peut alors se restreindre aux drapeaux internes d'après la Proposition 1. Ceci permet d'améliorer significativement le temps de calcul de la résolution géométrique de $\widehat{W}_{K^0}(S)$.

Contents

1 Introduction

In this paper, we intend to address the issue of finding at least one representative point in each connected component of a real algebraic variety. This is a fundamental problem of computational real algebraic geometry that appears in several other problems. It allows us to decide the emptiness of a variety. Another example : it is used to find exactly one point by connected component, hence compute the zeroth Betti number.

The paper is a sum up of previous works [BGHM97, BGHM01, BGHP04, BGHP05]. These papers were motivated by a new algorithm for efficient polynomial equation solving described in [GLS01, HMW01]. The new algorithm, called *geometric resolution algorithm*, brings with it a new philosophy. In order to understand the changes, let us recall the previous algorithms.

The basic idea of previous elimination procedures is the use of Gröbner bases so we can compute a canonical form, fixed by the choice of a monomial ordering, for every polynomial in the quotient by a given zero-dimensional ideal. We say this tool is algebraic since we do manipulations of monomials. This is a generic tool because there are none assumptions about the equations. On the other hand, the drawback of the generic aspect is that this tool does not take advantage of any 'good' system of equations to compute faster. The complexity of the algorithm depend on extrinsic parameters, such as the maximal degree d of the equations, the number n of variables. Since polynomials are manipulated through their dense representation, which has asymptotically $\Theta(d^n)$ terms, the complexity is asymptotically over d^n.

The Gröbner-free algorithm of [GLS01, HMW01] is more specific; it requires a system of equations $F_1 = \ldots = F_n = 0, g \neq 0$ that form a reduced regular sequence (see subsection 4.1). The complexity is related to the geometric object defined by the previous equations, in particular its geometric degree δ. Since this tool is intrinsic, we are prompted to think geometrically when using it. As this algorithm is iterative, we have to take into account all intermediate varieties $S_i := \overline{V(F_1, \ldots, F_i) \backslash V(g)}$. Moreover the use of a good data structure, the straight-line programs, allows the algorithm to take advantage of system of equations with good evaluation complexity, for example sparse polynomials.

We extend the range of applications of the geometric resolution algorithm to the finding of at least one point in each connected component of a real algebraic variety S. We assume the variety is smooth. The notion of *generalized polar varieties* will give us the geometric object required to apply the geometric resolution algorithm. This notion is a generalization of *classic polar varieties*. We give a non formal definition of classic polar varieties : you look at your variety S from a distance and the first polar variety is the contour of what you see. Other polar varieties are iteration of this process from different directions.

Although we want to work with real affine algebraic set, the notion of generalized polar variety is projective and algebraic geometry is nicer in algebraically closed field, so we make a detour through the complex projective space. Let $\mathbb{P}^n := \mathbb{P}^n(\mathbb{C})$ be the n-dimensional projective space over the complex numbers $\mathbb{C}$ and let, for $0 \leqslant p \leqslant n$, V be a pure p-codimensional projective algebraic variety.

The generalized polar variety of V associated with a given linear subspace K and a given hyperplane H of the ambient space $\mathbb{P}^n$ will be denoted $\widehat{W}_K(V)$. We refer to subsection 2.1 for definition. In this paper we consider mainly the case where H is the hyperplane at infinity of $\mathbb{P}^n$, fixing in this way an embedding $\mathbb{A}^n \subseteq \mathbb{P}^n$. Let $S := V \cap \mathbb{A}^n$ be the affine trace of V and suppose S is non-empty. Then S is a pure p-codimensional affine algebraic variety. The affine trace $\widehat{W}_K(S) := \widehat{W}_K(V) \cap \mathbb{A}^n$ is called the *affine* generalized polar variety of S associated with the linear subvariety K. When $K \subseteq H$, we notion of generalized affine polar variety

coincide with the notion of classic affine polar variety (see [BGHM01]).

Now we are going to outline the basic properties of $\widehat{W}_K(S)$. Let $\mathbb{Q}$ be the field of rational numbers. From now on, let a regular sequence $F_1, \ldots, F_p \in \mathbb{Q}[X_1, \ldots, X_n]$ be given such that $(F_1, \ldots, F_p)$ is the ideal of definition of the affine variety S. Assume that the projective linear variety K of dimension $n-p-i$ is spanned by $n-p-i+1$ rational points $A_j := (a_{j,0}, \ldots, a_{j,n})$ with $a_{j,1}, \ldots, a_{j,n}$ generic, for $1 \leqslant j \leqslant n-p-i+1$. Then, if S is smooth, $\widehat{W}_K(S)$ is either empty or a smooth subvariety of S having pure codimension i in S. Moreover, $\widehat{W}_K(S)$ is the variety defined by $F_1, \ldots, F_p$ and by all $(n-i+1)$-minors of the polynomial $((n-i+1) \times n)$ matrix

$$\begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \cdots & \frac{\partial F_p}{\partial X_n} \\ a_{1,1} - a_{1,0}X_1 & \cdots & a_{1,n} - a_{1,0}X_n \\ \vdots & \vdots & \vdots \\ a_{n-p-i+1,1} - a_{n-p-i+1,0}X_1 & \cdots & a_{n-p-i+1,n} - a_{n-p-i+1,0}X_n \end{bmatrix}$$

(see Proposition 4).

Let $\mathbb{R}$ be the field of real numbers and let $\mathbb{P}^n_{\mathbb{R}}$ and $\mathbb{A}^n_{\mathbb{R}}$ be respectively the real n-dimensional projective and affine spaces. Let $S_{\mathbb{R}} := S \cap \mathbb{A}^n_{\mathbb{R}}$ be the real trace of the complex algebraic variety S. From the hypothesis, we deduce that $S_{\mathbb{R}}$ is smooth and its real codimension at any point is p. Then, for generic spaces K, the generalized *real* affine polar varieties $\widehat{W}_K(S_{\mathbb{R}}) := \widehat{W}_K(S) \cap \mathbb{A}^n_{\mathbb{R}}$ is well defined and contains for each connected component of $S_{\mathbb{R}}$ at least one algebraic sample point. The same is true for the real classic polar varieties if $S_{\mathbb{R}}$ is compact (see Propositions 1 and 2).

Finally, we focus on the zero-dimensional generalized affine polar variety $\widehat{W}_K(S)$ for K a generic point in $\mathbb{P}^n$. The variety $\widehat{W}_K(S)$ will be our set of sample point that meet every connected component of $S_{\mathbb{R}}$. We can find good equations that define it. Let $c_1, \ldots, c_n$ be random real numbers and $Z_1, \ldots, Z_n$ be a random new system of coordinates. Let M_j be the $(p+1)$-minor associated with the columns $1, \ldots, p, j$ of the matrix

$$\begin{bmatrix} \frac{\partial F_1}{\partial Z_1} & \cdots & \frac{\partial F_1}{\partial Z_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial Z_1} & \cdots & \frac{\partial F_p}{\partial Z_n} \\ c_1 - Z_1 & \ldots & c_n - Z_n \end{bmatrix}$$

for $p+1 \leqslant j \leqslant n$. Then $F_1, \ldots, F_p$, $M_{p+1}, \ldots, M_n$ is a reduced regular sequence that define $\widehat{W}_K(S)$ (see Corollary 17). The geometric resolution algorithm applied on this reduced regular sequence is the final step of our algorithm for finding at least one algebraic sample point for each connected component of a given smooth, complete intersection subvariety of $\mathbb{A}^n_{\mathbb{R}}$.

2 Basics of Generalized Polar Varieties

Let the ambient space be $\mathbb{P}^n$, the n-dimensional complex projective space. For any linear subspaces A and B of $\mathbb{P}^n$, we denote $\langle A, B \rangle$ the linear space spanned by A and B. We say that A and B intersect transversally and note $A \pitchfork B$ if $\langle A, B \rangle = \mathbb{P}^n$. In the opposite case,

we note $A \not\pitchfork B$. Let V be a projective algebraic subvariety of $\mathbb{P}^n$. Suppose that V is of pure codimension p, *ie* that each irreducible component of V is of codimension p. We write V_{reg} for the regular (smooth) points of V. Observe that V_{reg} is a complex submanifold of $\mathbb{P}^n$ and that V_{reg} is Zariski-dense in V. We call $V_{sing} := V \backslash V_{reg}$ the singular locus of V. For all $M \in V_{reg}$, the tangent space $T_M V$ is viewed as a linear subspace of $\mathbb{P}^n$ containing M.

Here are by the equivalent notions in the affine case. We fix an embedding $\mathbb{A}^n \subseteq \mathbb{P}^n$ and we denote $H := \mathbb{P}^n \backslash \mathbb{A}^n$ the hyperplane at infinity. For every linear space $A \nsubseteq H$, we write $\tilde{A} := A \cap \mathbb{A}^n$ the affine trace of A. We can interpret $\tilde{A}$ as an affine space and thus write $\tilde{A} = M + \vec{A}$ where M is a point of $\tilde{A}$ and $\vec{A}$ is the vectorial part of $\tilde{A}$. If $A \subseteq H$, the vector space $\overrightarrow{\langle M, A \rangle}$ does not depend on the point $M \in \mathbb{A}^n$. Therefore we can define the vectorial part $\vec{A} := \overrightarrow{\langle M, A \rangle}$ of A. For $\vec{A}$ and $\vec{B}$ two vector subspaces of $\mathbb{A}^n$, we note $\vec{A} \pitchfork \vec{B}$ if $\vec{A} + \vec{B} = \mathbb{A}^n$. Let S be a affine algebraic variety and V its projective closure. We respectively call $S_{reg} := V_{reg} \cap \mathbb{A}^n$ and $S_{sing} := V_{sing} \cap \mathbb{A}^n$ the set of smooth (regular) points and the singular locus of the affine variety S. For any smooth point M of the affine variety S, we define $T_M S := \widetilde{T_M V}$ the affine tangent space of S at M.

For a linear subspace $A \subseteq \mathbb{P}^n$ of dimension a, we denote by $A^\perp$ the orthogonal of A with respect to the usual quadratic form $\sum_{i=0}^n X_i$. The dimension of $A^\perp$ is $n-1-a$. Let us fix a hyperplane H of $\mathbb{P}^n$. If A is a linear subspace of H, we denote by $A^* := A^\perp \cap H$ its orthogonal in the hyperplane. The dimension of A^* is $n-a-2$.

2.1 Generalized polar varieties

Now we are going to precise the notion of generalized polar varieties contained in the projective space $\mathbb{P}^n$. Such polar varieties will be associated with a given flag $\mathcal{K}$ of linear subvarieties and a hyperplane H of $\mathbb{P}^n$. Let us denote the given flag by

$$\mathcal{K} : \qquad \mathbb{P}^n \supsetneq K^{n-1} \supsetneq \cdots \supsetneq K^{n-p-1} \supsetneq \cdots \supsetneq K^1 \supsetneq K^0.$$

For a given member K of a flag $\mathcal{K}$ and a given hyperplane H, we define the *generalized polar variety* $\widehat{W}_K(V)$ associated with K as the Zariski-closure of the set

$$\left\{ M \in V_{reg} \backslash (H \cup K) \mid T_M V \not\pitchfork \left(\langle M, K \rangle \cap H \right)^* \right\}. \tag{4}$$

Note that $\widehat{W}_K(V)$ is contained in V. Moreover the point M is chosen outside of $H \cup K$ so that $\langle M, K \rangle \cap H$ is always of dimension $\dim K$. Then the generalized polar varieties associated with $\mathcal{K}$ are organized as a decreasing sequence as follows :

$$V = \widehat{W}_{K^{n-1}} = \cdots = \widehat{W}_{K^{n-p}} \supseteq \widehat{W}_{K^{n-p-1}} \supseteq \cdots \supseteq \widehat{W}_{K^1} \supseteq \widehat{W}_{K^0}.$$

For $1 \leqslant i \leqslant n-p$, we call $\widehat{W}_{K^{n-p-i}}(V)$ the *i-th generalized polar variety* of V associated with the flag $\mathcal{K}$ and the hyperplane H. The index i reflects the expected codimension of $\widehat{W}_{K^{n-p-i}}(V)$ in V. Note that the *relevant part* of the flag $\mathcal{K}$ leading to non-trivial polar varieties ranges from K^{n-p-1} to K^0.

Let K be any member of the flag $\mathcal{K}$ and assume that H is the hyperplane at infinity of $\mathbb{A}^n \subseteq \mathbb{P}^n$. Suppose V is the projective closure of S, a pure p-codimensional affine algebraic set. Then we denote by $\widehat{W}_K(S) := \widehat{W}_K(V) \cap \mathbb{A}^n$ the *affine* generalized polar variety associated to K. Hence $\widehat{W}_K(S)$ is the Zariski-closure in $\mathbb{A}^n$ of the set

$$\left\{ M \in S_{reg} \backslash (K \cap \mathbb{A}^n) \mid T_M S \not\pitchfork \left(\langle M, K \rangle \cap H \right)^* \right\}. \tag{5}$$

Two particular types of flags are noteworthy. The first type correspond to flags

$$\mathcal{K}: \qquad \mathbb{P}^n \supsetneq K^{n-1} \supsetneq \cdots \supsetneq K^{n-p-1} \supsetneq \cdots \supsetneq K^1 \supsetneq K^0$$

with $K^{n-1} = H$. We call them *internal flags*. Observe that $\langle M, K\rangle \cap H = K$. For any member K of the flag $\mathcal{K}$, we define $L := K^*$. We derive from (4) that $\widehat{W}_K(V)$ coincides with the Zariski-closure of the set

$$\{M \in V_{reg} \backslash H \mid T_M V \not\pitchfork L\}. \tag{6}$$

As before let H be the hyperplane at infinity of $\mathbb{A}^n \subseteq \mathbb{P}^n$ and let V be the projective closure of a given pure p-codimensional affine algebraic variety. Once again, we denote $L := K^*$. From (6), one easily infers that the affine generalized polar variety $\widehat{W}_K(S) := \widehat{W}_K(V) \cap \mathbb{A}^n$ is the Zariski-closure in $\mathbb{A}^n$ of the set

$$\left\{M \in S_{reg} \mid \overrightarrow{T_M S} \not\pitchfork \vec{L}\right\}. \tag{7}$$

This implies that $\widehat{W}_K(S)$ is exactly the *classic polar variety* of S associated with the linear space $\vec{L}$. Finally, let us remark that any classic polar variety of S can be obtained by a suitable choice of linear space $K \subseteq H$. For definition and basic properties of classic polar varieties, we refer to [Pie78] and the references cited therein. More details on the relations between classic and generalized polar varieties can be found in [BGHP04].

The second type of flags, referred as *external flags* are the flags

$$\mathcal{K}: \qquad \mathbb{P}^n \supsetneq K^{n-1} \supsetneq \cdots \supsetneq K^{n-p-1} \supsetneq \cdots \supsetneq K^1 \supsetneq K^0$$

with $K^0 \notin H$. We call P the (only) point of K^0. Since $K = \langle P, K \cap H\rangle$ for any $K \in \mathcal{K}$, we have

$$\langle M, K\rangle \cap H = \overrightarrow{MP} + \vec{K}.$$

Hence from (4), we conclude that the generalized polar variety $\widehat{W}_K(V)$ coincides with the Zariski-closure of the set

$$\left\{M \in V_{reg} \backslash (H \cup K) \;\middle|\; \overrightarrow{T_M V} \not\pitchfork \left(\overrightarrow{MP} + \vec{K}\right)^{\perp}\right\}. \tag{8}$$

Again, let us assume that the variety V is the projective closure of a given pure p-codimensional affine algebraic variety and that H is the hyperplane at infinity of $\mathbb{A}^n \subseteq \mathbb{P}^n$. From (8), we deduce that the affine polar variety $\widehat{W}_K(S)$ is the Zariski-closure in $\mathbb{A}^n$ of the set

$$\left\{M \in S_{reg} \backslash (\tilde{K}) \;\middle|\; \overrightarrow{T_M S} \not\pitchfork \left(\overrightarrow{MP} + \vec{K}\right)^{\perp}\right\}. \tag{9}$$

In the next subsection, we shall discuss *real* polar varieties.

2.2 Real polar varieties

In principle, a real affine polar variety $\widehat{W}_K(S_{\mathbb{R}})$ may be empty. But in our case, the polar varieties will intersect every connected component of $S_{\mathbb{R}}$ and be non-empty if $S_{\mathbb{R}} \neq \emptyset$.

Let us first consider the case of internal flags. For any member K of a given flag $\mathcal{K}$, we have $K \subseteq H$ and we write $L := K^*$. We deduce from (7) that $\widehat{W}_K(S_{\mathbb{R}})$ is the Zariski-closure in $\mathbb{A}^n$ of the set

$$\left\{M \in (S_{\mathbb{R}})_{reg} \mid \overrightarrow{T_M S_{\mathbb{R}}} \not\pitchfork \vec{L}\right\}.$$

Proposition 1. *Suppose that $S_{\mathbb{R}}$ is a $\mathbb{R}$-definable real affine algebraic variety smooth and compact. Then $\widehat{W}_K(S_{\mathbb{R}})$ contains at least one point of each connected component of $S_{\mathbb{R}}$.*

Proof. We fix $\vec{v} \in K \subseteq H$. Observe that by definition $L \subseteq (\vec{v})^{\perp}$. We can suppose that $\vec{v}$ is the direction of the first coordinate axis. Consider the function from an connected component C of the variety $S_{\mathbb{R}}$ to $\mathbb{R}$ that gives the first coordinate of a point $M \in C$. This function is continuous and reaches its maximum on the compact C at the point P. Then the vector space $\overrightarrow{T_P S_{\mathbb{R}}}$ is included in $(\vec{v})^{\perp}$. Hence we have $\overrightarrow{T_P S_{\mathbb{R}}} + \vec{L} \neq \mathbb{A}^n_{\mathbb{R}}$ and $P \in \widehat{W}_K(S_{\mathbb{R}}) \cap C$. □

Let us now consider the case of $\widehat{W}_K(S_{\mathbb{R}})$ for a external flag $\mathcal{K}$. Observe that the variety $S_{\mathbb{R}}$ is no longer supposed to be compact.

Proposition 2. *Suppose that $S_{\mathbb{R}}$ is a $\mathbb{R}$-definable real affine algebraic variety and smooth. Suppose that $K \nsubseteq S_{\mathbb{R}}$. Then the real affine polar variety $\widehat{W}_K(S_{\mathbb{R}})$ contains at least one point of each connected component of $S_{\mathbb{R}}$.*

Proof. Since K is not contained in $S_{\mathbb{R}}$, there exists a point $P \in K \backslash S_{\mathbb{R}}$. Consider now an arbitrary connected component C of $S_{\mathbb{R}}$. Then C is a smooth, closed set whose distance to the point P is realised by a point $M \in C$. Since P does not belong to $S_{\mathbb{R}}$, we have $\overrightarrow{MP} \neq 0$.

The gradient of the distance to the point P at M is collinear to $\overrightarrow{MP}$ and is orthogonal to the tangent space $\overrightarrow{T_M S_{\mathbb{R}}}$ according to the Lagrangian Multiplier Theorem. Therefore the vector space $\overrightarrow{T_M S_{\mathbb{R}}}$ is included in $(\overrightarrow{MP})^{\perp}$ and so M belongs to $\widehat{W}_K(S_{\mathbb{R}}) \cap C$. □

3 Manipulating Polar Varieties

In this section we will describe in more detail the generalized polar varieties of a pure p-codimensional affine variety S, which is given by a system of polynomial equations. We suppose that these equations intersect transversally on the variety S they define. Let K be a "sufficiently generic" linear subvariety of $\mathbb{P}^n$ of dimension at most $n-p$. We will show that the polar variety $\widehat{W}_K(S)$ of S is either empty or equidimensional of expected codimension in S. We will describe $\widehat{W}_K(S)$ locally by transversal intersections of explicitly given hypersurfaces of $\mathbb{A}^n$ and globally by explicit polynomial equations.

3.1 First equations describing affine polar varieties

Let $\mathbb{P}^n$ and $\mathbb{A}^n$ be the n-dimensional projective and affine space over $\mathbb{C}$. We use the usual homogenous coordinates $x := (x_0 : x_1 : \ldots : x_n)$ for the projective points. Moreover when $x_0 = 1$ we denote the corresponding point in the affine space $\mathbb{A}^n$ by $(x_1, \ldots, x_n) := (1 : x_1 : \ldots : x_n)$.

From now on, we suppose that the affine variety S is defined by $F_1, \ldots, F_p \in \mathbb{Q}[X_1, \ldots, X_n]$, *ie* $S := V(F_1, \ldots, F_p)$. Moreover, we ask the equations $F_1, \ldots, F_p$ to *intersect transversally*, which means that they have a Jacobian of maximal rank at every point of S. Thus S is a non-empty purely p-codimensional smooth affine variety.

We fix an index $1 \leqslant i \leqslant n-p$ that represents the expected codimension of the generalized affine polar variety in S. Let us pick some points $A_j = (a_{j,0} : \ldots : a_{j,n})$ with $a_{j,0} \in \{0, 1\}$ and $1 \leqslant j \leqslant n-p-i+1$. We assume that the points $A_1, \ldots, A_{n-p-i+1}$ span a space K of dimension $n-p-i$. Let $M = (x_1, \ldots, x_n)$ be a point of $S \backslash K$. The space $\overrightarrow{\langle M, K \rangle \cap H}$ is

spanned by the $n-p-i+1$ points at infinity $A_j - a_{j,0}M$ with $1 \leqslant j \leqslant n-p-i+1$. Let us consider the matrix

$$\Gamma^{(i)}(x) = \begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \cdots & \frac{\partial F_p}{\partial X_n} \\ a_{1,1} - a_{1,0}X_1 & \cdots & a_{1,n} - a_{1,0}X_n \\ \vdots & \vdots & \vdots \\ a_{n-p-i+1,1} - a_{n-p-i+1,0}X_1 & \cdots & a_{n-p-i+1,n} - a_{n-p-i+1,0}X_n \end{bmatrix}(x)$$

whose row vectors are the gradient vectors $(\overrightarrow{\text{grad}}\ F_i)(x)$ and the former vectors $A_j - a_{j,0}M$.

Proposition 3. *Let $M = (x_1, \ldots, x_n)$ be a point of $S\backslash K$. Then all $(n-i+1)$-minors of $\Gamma^{(i)}$ vanish at M if and only if $T_M S \not\pitchfork \left(\langle M, K\rangle \cap H\right)^*$.*

Proof. Observe that all $(n-i+1)$-minors of $\Gamma^{(i)}$ vanish at $M = (x_1, \ldots, x_n) \in S$ if and only if there exists a dependency relation between the rows of $\Gamma^{(i)}(x)$. The first p rows of $\Gamma^{(i)}(x)$ are linearly independent by hypothesis on S and the other are also independent since the points A_j have been chosen linearly independent. Hence the previous conditions are equivalent to the condition saying that the vector space spanned by the first p rows intersects the vector space spanned by the last rows. Finally, this is equivalent to the condition $T_M S \not\pitchfork \left(\langle M, K\rangle \cap H\right)^*$ from (5). □

We define the variety W_i by the equations $F_1, \ldots\ F_p$ and all $(n-i+1)$-minors of the $((n-i+1)\times n)$-matrix $\Gamma^{(i)}$. We have just shown that

$$\left\{M \in S\backslash\tilde{K} \mid T_M S \not\pitchfork \left(\langle M, K\rangle \cap H\right)^*\right\} = W\backslash\tilde{K}$$

and consequently $\widehat{W}_K(S) = \overline{W\backslash\tilde{K}}$. So $\widehat{W}_K(S)$ is equal to W without its irreducible components included in $\tilde{K}$.

Proposition 4. *Assume that $K \nsubseteq S$. Then the affine generalized polar variety $\widehat{W}_K(S)$ is equal to W.*

Proof. From the previous discussion, we have to show that no irreducible component of W_i is included in K. We begin with the following lemma.

Lemma 5. *Any irreducible component of W_i has codimension at most i in S.*

Proof. Let us denote by $\mathfrak{a}$ the ideal of the coordinate ring $\mathbb{C}[S]$ of the affine variety S, generated by all $(n-i+1)$-minors of the $((n-i+1)\times n)$-matrix induced by $\Gamma^{(i)}$ in $\mathbb{C}[S]$. Let C be a given irreducible component of the affine polar variety $\widehat{W}_K(S)$ and let $\mathfrak{p}$ be the ideal of definition of C in $\mathbb{C}[S]$. Then $\mathfrak{p}$ is an isolated prime component of the determinantial ideal $\mathfrak{a}$. From [Eag62] Theorem 3 (see also [Mat86] Theorem 13.10) we deduce that the height of the prime ideal $\mathfrak{p}$ is bounded by i. This means that the codimension of C in S is at most i. □

Assume that C is an irreducible component of W_i included in K. Since $\dim C \geqslant n-p-i$ and $\dim K = n-p-i$, we must have $C = K$. This would induce $K \subseteq S$, which contradicts the hypothesis. □

3.2 Local equations

From now on we will assume, without loss of generality, that $K \not\subseteq S$. We will now focus on finding simpler set of equations for W. We will show that W is locally described as a subvariety of S by i equations.

Let M be a $(l \times m)$-matrix and $1 \leqslant k \leqslant \min(l, m)$. Let $\mathcal{P}_k^l$ be the set of subset of cardinality k of $\{1, \ldots, l\}$. We fix $I \in \mathcal{P}_k^l$. We denote I^C its complement in $\{1, \ldots, l\}$. For $I \in \mathcal{P}_k^l, J \in \mathcal{P}_k^m$, we denote M_J^I the k-minor of M formed with the rows of index in I and the columns of index in J.

Let $s \in \{n - i, n - i + 1\}$. For any subset $I = \{k_1, \ldots, k_s\}$ of $\{1, \ldots, n\}$ we denote by $M(I) := \Gamma^{\{1,\ldots,s\}}_{\{k_1,\ldots,k_s\}}$ the s-minor that corresponds to the first s rows and to the columns $k_1, \ldots, k_s$ of the matrix $\Gamma^{(i)}$.

Lemma 6 (Exchange Lemma)**.** *Let $I_k \in \mathcal{P}_k^s$ and $I_{k-1} \in \mathcal{P}_{k-1}^s$ be two given index sets. Then, for suitable numbers $\epsilon_j \in \{-1, 1\}$ with $j \in I_k \backslash I_{k-1}$, we have the following identity:*

$$(*) \quad M(I_{k-1})M(I_k) = \sum_{j \in I_k \backslash I_{k-1}} \epsilon_j \; M(I_k \backslash \{j\}) \; M(I_{k-1} \cup \{j\}).$$

Proof. Consider the following $((2k-1) \times (2k-1))$-matrix L with entries from Γ :

$$L := \left[\begin{array}{c|c} & L_1(I_k) \\ 0 & \vdots \\ & L_{k-1}(I_k) \\ \hline L_1(I_{k-1}) & L_1(I_k) \\ \vdots & \vdots \\ L_k(I_{k-1}) & L_k(I_k) \end{array}\right].$$

Here, for any $1 \leqslant j \leqslant k$, $L_j(I_k)$ denotes the row vector of length k that we obtain selecting, from the j-th row of the matrix Γ, the k elements placed in the columns with index in I_k. Similarly, $L_j(I_{k-1})$ is obtained from the j-th row of A selecting the $k-1$ elements placed in the columns with index in I_{k-1}.

Let us recall the Laplace expansion which is the generalization of the column (or row) expansion to several columns (or rows).

Lemma 7 (Laplace Expansion)**.** *Let M be a $(n \times n)$-matrix and I be a set of rows. For suitable signs $\epsilon_J \in \{-1, 1\}$, we have the following identity*

$$\det M = \sum_{J \in \mathcal{P}_k^n} \epsilon_J \; M_J^I \; M_{J^C}^{I^C}.$$

Proof. From the formula

$$\det M = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{i,\sigma(i)} \; ,$$

you just partition $\mathfrak{S}_n$ according to the image set $\sigma(I)$. □

Now it is not difficult to verify the identity $(*)$ by calculating the determinant $\det L$ of the quadratic matrix L via Laplace expansion in two different ways. First, by expansion of $\det L$ according to the first $k-1$ columns of L, we obtain the left-hand side of $(*)$, disregarding the sign. Expansion of $\det L$ according to the first $k-1$ rows of L leads to the right-hand side of $(*)$. This implies the identity $(*)$ for an appropriate choice of the signs ϵ_j, with $j \in I_k \backslash I_{k-1}$. □

Let us fix a subset $I \in \mathcal{P}^n_{n-i}$, say $I := \{1, \ldots, n-i\}$, and let us consider the upper $(n-i)$-minor

$$m := M(I) := \det \begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_{n-i}} \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \cdots & \frac{\partial F_p}{\partial X_{n-i}} \\ r_{1,1}(X_1) & \cdots & r_{1,n-i}(X_{n-i}) \\ \vdots & \vdots & \vdots \\ r_{n-p-i,1}(X_1) & \cdots & r_{n-p-i,n-i}(X_{n-i}) \end{bmatrix}, \; r_{j,k}(X_k) := a_{j,k} - a_{j,0}X_k,$$

of the matrix $\Gamma^{(i)}$.

The Exchange Lemma implies, for any subset $J \in \mathcal{P}^n_{n-i+1}$, the identity

$$m\ M(J) = \sum_{l \in J \backslash \{1,\ldots,n-i\}} \epsilon_l\ M(J \backslash \{l\})\ M(1, \ldots, n-i, l) \tag{10}$$

with $\epsilon_l \in \{-1, 1\}$.

Let us abbreviate $M_j := M(1, \ldots, n-i, j)$ for $n-i+1 \leqslant j \leqslant n$. These equations play a fundamental role.

Proposition 8. *The affine polar variety $\widehat{W}_K(S)$ is defined by the equations $F_1, \ldots, F_p$, $M_{n-i+1}, \ldots, M_n$ outside the locus $V(m)$.*

Proof. Let M be a point of S of coordinates $x = (x_1, \ldots, x_n)$. If $m(x) \neq 0$ and $M_{n-i+1}(x) = \ldots = M_n(x) = 0$, we infer from (10) that $M(J)(x) = 0$ holds for any subset $J \in \mathcal{P}^n_{n-i+1}$. The converse is clear. □

3.3 Smoothness and generic linear space

In this section we study the smoothness of the affine polar variety $\widehat{W}_K(S)$ depending on the choice of the linear variety K. We first focus on the open set $\widehat{W}_K(S) \backslash V(m)$. We prove that almost every linear variety K leads to a smooth variety $\widehat{W}_K(S) \backslash V(m)$.

Let $Z_{n-i+1}, \ldots, Z_n$ be new indeterminates and consider the $((n-i+1) \times n)$-matrix

$$\begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_{n-i}} & \frac{\partial F_1}{\partial X_{n-i+1}} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \cdots & \frac{\partial F_p}{\partial X_{n-i}} & \frac{\partial F_p}{\partial X_{n-i+1}} & \cdots & \frac{\partial F_p}{\partial X_n} \\ r_{1,1}(X_1) & \cdots & r_{1,n-i}(X_{n-i}) & r_{1,n-i+1}(X_{n-i+1}) & \cdots & r_{1,n}(X_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r_{n-p-i,1}(X_1) & \cdots & r_{n-p-i,n-i}(X_{n-i}) & r_{n-p-i,n-i+1}(X_{n-i+1}) & \cdots & r_{n-p-i,n}(X_n) \\ r_{n-p-i+1,1}(X_1) & \cdots & r_{n-p-i+1,n-i}(X_{n-i}) & Z_{n-i+1} - a_{n-p-i+1,0}X_{n-i+1} & \cdots & Z_n - a_{n-p-i+1,0}X_n \end{bmatrix}.$$

Let $\tilde{M}_{n-i+1}, \ldots, \tilde{M}_n$ denote the corresponding $(n-i+1)$-minors of this matrix. Let $U := \{m \neq 0\}$ an affine, maybe empty, open set.

Now consider the following morphism of smooth, affine varieties

$$\Phi_i : \left\{ \begin{array}{ccc} U \times \mathbb{A}^i & \to & \mathbb{A}^p \times \mathbb{A}^i \\ (x,z) & \mapsto & \Big(F_1(x), \ldots, F_p(x), \tilde{M}_{n-i+1}(x,z), \ldots, \tilde{M}_n(x,z)\Big) \end{array} \right. .$$

Lemma 9. *The origin $(0,\ldots,0)$ of the affine space $\mathbb{A}^p \times \mathbb{A}^i$ is a regular value of the morphism Φ_i.*

Proof. If the fibre $(\Phi_i)^{-1}(0,\ldots,0)$ is empty, there is nothing to prove. Now assume that the fibre $(\Phi_i)^{-1}(0,\ldots,0)$ is non-empty. Consider a point $(x,z) \in (\Phi_i)^{-1}(0,\ldots,0)$ in the fibre and observe that the Jacobian $\mathrm{Jac}(\Phi_i)(x,z)$ of Φ_i at the point (x,z) has the form

$$\left[\begin{array}{cccccc} \frac{\partial F_1}{\partial X_1}(x) & \ldots & \frac{\partial F_1}{\partial X_n}(x) & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1}(x) & \ldots & \frac{\partial F_p}{\partial X_n}(x) & 0 & \ldots & 0 \\ * & \ldots & * & m(x) & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ * & \ldots & * & 0 & \ldots & m(x) \end{array} \right] .$$

Since x belongs to U, the first p rows of $\mathrm{Jac}(\Phi_i)(x,z)$ are linearly independent and $m(x) \neq 0$. Therefore $\mathrm{Jac}(\Phi_i)(x,z)$ is surjective for any point (x,z) in the fibre $(\Phi_i)^{-1}(0,\ldots,0)$. This means that $(0,\ldots,0)$ is a regular value of Φ_i. □

We now apply the Weak-Transversality Theorem of Thom-Sard (see e.g. [Dem89]) to Φ_i. The theorem roughly states that almost every fibre of a smooth submanifold is smooth. Here we apply it to the submanifold $(\Phi_i)^{-1}(0,\ldots,0)$, smooth thanks to Lemma 9. The fibers correspond to the choice of the parameter $z \in \mathbb{A}^i$. We deduce that there exists a residual dense set Ω of $\mathbb{A}^i$, such that for any point $z \in \Omega$ the polynomial

$$F_1, \ldots, F_p, \tilde{M}_{n-i+1}(X_1, \ldots, X_n, z), \ldots, \tilde{M}_n(X_1, \ldots, X_n, z)$$

of $\mathbb{Q}[X_1, \ldots, X_n]$ intersect transversally in any of their common zeros on the open set U. Thus, for almost all parameters $a_{1,1}, \ldots, a_{1,n}, \ldots, a_{n,1}, \ldots, a_{n,n}$ the polynomials $F_1, \ldots, F_p$, $M_{n-i+1}(X_1, \ldots, X_n), \ldots, M_n(X_1, \ldots, X_n)$ intersect transversally in any of their common zeros on the open set U.

We have therefore shown the following statement :

Lemma 10. *For almost all parameters $a_{i,j}$, with $1 \leqslant i, j \leqslant n$, the polynomial $((n-i+1)\times n)$-matrix $\Gamma^{(i)}$ satisfies the following condition :*

The equations $F_1, \ldots, F_p, M_{n-i+1}(X_1, \ldots, X_n), \ldots, M_n(X_1, \ldots, X_n)$ define the generalized polar variety $\widehat{W}_K(S)$ outside the locus $V(m)$ and intersect transversally in any point of the set $\widehat{W}_K(S) \backslash V(m)$. In particular, $\widehat{W}_K(S) \backslash V(m)$ is either empty or a smooth, complete intersection variety of dimension $n-p-i$.

We can replace m by any other upper $(n-i)$-minor of $\Gamma^{(i)}$. Observe that all upper $(n-i)$-minor of $\Gamma^{(i)}$ vanish at a point x of S if and only if x belongs to the polar variety $\widehat{W}_{K^{n-p-i-1}}(S)$ which is contained in $\widehat{W}_K(S) = \widehat{W}_{K^{n-p-i}}(S)$. Applying Lemma 10 to any upper $(n-i)$-minor of the matrix $\Gamma^{(i)}$, we conclude :

Proposition 11. *For any point $M \in \widehat{W}_{K^{n-p-i}}(S) \backslash \widehat{W}_{K^{n-p-i-1}}(S)$ a reordering $\sigma \in \mathfrak{S}_n$ of the columns of $\Gamma^{(i)}$ inducing a new matrix Γ' exists, such that the new left upper $(n-i)$-minor m' does not vanish at the point M. We define $M'_{n-i+1}, \ldots, M'_n$ for the matrix Γ' as before. Then the equations $F_1, \ldots, F_p, M'_{n-i+1}, \ldots, M'_n$ intersect transversally at M. Moreover, the polynomials $F_1, \ldots, F_p, M'_{n-i+1}, \ldots, M'_n$ define the polar variety $\widehat{W}_{K^{n-p-i}}(S)$ outside of the locus $V(m')$.*

Let us consider the case $i := n - p$. Observe that $\Gamma^{(n-p)}$ is a $((p+1) \times n)$-matrix which contains the Jacobian $J(F_1, \ldots, F_p)$ as its first p rows. Thus, for any point x of $\widehat{W}_{K^0}$, there exists an upper p-minor m of $\Gamma^{(n-p)}$ with $m(x) \neq 0$. Therefore we can define $\widehat{W}_{K^{-1}}$ as the empty set. Thus $\widehat{W}_{K^0}$ is either empty or smooth of dimension 0.

Proposition 12. *Suppose that the generalized affine polar variety $\widehat{W}_{K^{n-p-i}}(S)$ is non-empty. Then for each irreducible component C of $\widehat{W}_{K^{n-p-i}}(S)$ there exists an upper $(n-i)$-minor m of $\Gamma^{(i)}$ such that m does not vanish identically on C. Therefore $\widehat{W}_{K^{n-p-i}}(S)$ is of pure codimension i in S.*

Proof. Let C be an irreducible component of $\widehat{W}_{K^{n-p-i}}(S)$. Suppose that all upper $(n-i)$-minor of $\Gamma^{(i)}$ vanish identically on C. Proposition 11 implies that $C \subseteq \widehat{W}_{K^{n-p-i-1}}(S)$. There exists an index $0 \leqslant j < n-p-i$ such that $C \subseteq \widehat{W}_{K^j}(S)$ and $C \nsubseteq \widehat{W}_{K^{j-1}}(S)$. Let us fix $x \in C \backslash \widehat{W}_{K^{j-1}}(S)$. From Proposition 11, we deduce that there exists a unique irreducible component C' of $\widehat{W}_{K^j}(S)$ that contains the point x. Thus we have $C \subseteq C'$. We know that the codimension of C' in S is $n-p-j > i$. But the codimension of C in S is at most i according to Lemma 5. From this contradiction, we deduce that there exits an upper $(n-i)$-minor m of $\Gamma^{(i)}$ that does not vanish identically on C.

Therefore, $C \backslash V(m)$ is non-empty. From Proposition 11 we deduce that the codimension of C in S is exactly i. Hence the generalized polar variety $\widehat{W}_{K^{n-p-i}}(S)$ is of pure codimension i in S. □

3.4 Simpler Equations

In this section, we will simplify the computation of the equations of $\widehat{W}_K(S)$. We recall that the polar varieties depend on the choice of the flag. Each element K^{n-p-i} of the flag was determined by the points $A_1, \ldots, A_{n-p-i+1}$. We will explicit the procedure of picking random flags for both internal flags and external flags.

Let $F_1, \ldots, F_n, g$ be polynomials of $\mathbb{Q}[X_1, \ldots, X_n]$. We say that $F_1, \ldots, F_n$ define a *reduced regular sequence* in the open subset $\{g \neq 0\}$ of $\mathbb{C}^n$ if each variety

$$\overline{V(F_1, \ldots, F_i) \backslash V(g)}, \quad 1 \leqslant i \leqslant n,$$

has dimension $n-i$ and for each $1 \leqslant i \leqslant n$ the localized quotient

$$(\mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_i))_g$$

is reduced, *ie* in this quotient $a^m = 0$ implies $a = 0$. This notion is equivalent to $F_1, \ldots, F_n$ is a regular sequence and $F_1, \ldots, F_n$ intersect transversally on $V(F_1, \ldots, F_n) \backslash V(g)$.

3.4.1 Internal Flags

A way to choose a random internal flag is to pick some random $a^*_{i,j}$ with $1 \leqslant i \leqslant n-p-i+1$ and $1 \leqslant j \leqslant n$. Then the points $A^*_i = (0 : a_{i,1} : \ldots : a_{i,n})$ will span a $(n-p-i)$ dimensional space K^{n-p-i}. The polar variety $\widehat{W}_{K^{n-p-i}}$ is a classic polar variety (see Section 2 for details). The previous matrix $\Gamma^{(i)}$ now has the form

$$\Gamma^{(i)} = \begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \cdots & \frac{\partial F_p}{\partial X_n} \\ a^*_{1,1} & \cdots & a^*_{1,n} \\ \vdots & \vdots & \vdots \\ a^*_{n-p-i+1,1} & \cdots & a^*_{n-p-i+1,n} \end{bmatrix}.$$

The bloc $(a^*_{i,j}) \in \mathcal{M}_{n-p-i+1,n}(\mathbb{Q})$ is of maximal rank. Some basic linear algebra implies the existence of $B \in \mathrm{GL}_n(\mathbb{Q})$ and $G \in \mathrm{GL}_{n-p-i+1}(\mathbb{Q})$ such that

$$\begin{bmatrix} a^*_{i,j} \end{bmatrix} B = \begin{bmatrix} 0_{p+i-1,n-p-i+1} & G_{n-p-i+1,n-p-i+1} \end{bmatrix}.$$

The matrix $B = (b_{l,j})$ induces a change of coordinates : new coordinates $Z_1, \ldots, Z_n$ are defined by $X_j = \sum_{l=1}^{n} b_{l,j} Z_l$ with $1 \leqslant j \leqslant n$. By $F_1(Z), \ldots, F_p(Z)$ we denote the polynomials $F_1, \ldots, F_p$ rewritten in the new variables $Z_1, \ldots, Z_n$ and by

$$\mathrm{Jac}(F(Z)) := \left(\frac{\partial F_h(Z)}{\partial Z_k} \right)_{\substack{1 \leqslant h \leqslant p \\ 1 \leqslant k \leqslant n}}$$

the new Jacobian. This change of coordinate induces a new matrix

$$\check{\Gamma}^{(i)} = \Gamma^{(i)} B = \begin{bmatrix} \mathrm{Jac}(F(Z)) \\ 0_{p+i-1,n-p-i+1} \quad G_{n-p-i+1,n-p-i+1} \end{bmatrix}.$$

Now all $(n-i+1)$-minors of $\Gamma^{(i)}$ vanish at a point x if and only if all $(n-i+1)$-minors of $\check{\Gamma}^{(i)}$ vanish at x. Let M be a $(n-i+1)$-minor of $\check{\Gamma}^{(i)}$. If M does not include the last $(n-p-i+1)$ columns of $\check{\Gamma}^{(i)}$ then $M = 0$. If M does include the last $(n-p-i+1)$ columns of $\check{\Gamma}^{(i)}$ then it is a non-zero multiple of a p-minor of $\mathrm{Jac}(F_1(Z), \ldots, F_p(Z))$ associated with columns among the $(p+i-1)$ first columns. We have shown the following proposition :

Proposition 13. *The classic polar variety $\widehat{W}_{K^{n-p-i}}(S)$ for the internal flag member K^{n-p-i} is the subvariety of S where all p-minor of the following matrix vanish :*

$$Jac(F(Z_{1\ldots p+i-1})) := \left(\frac{\partial F_h(Z)}{\partial Z_k} \right)_{\substack{1 \leqslant h \leqslant p \\ 1 \leqslant k \leqslant p+i-1}}.$$

This proposition leads us to the final theorem for internal flags.

Theorem 14. *Suppose that $Z_1, \ldots, Z_n$ are in generic position with respect to the variety S. Let m be any upper $(p-1)$-minor of the Jacobian $Jac(F(Z_{1\ldots p+i-1}))$ and $M_p, \ldots, M_{p+i-1}$ the p-minors constructed as before. Then in the open subset $\{m \neq 0\}$ of $\mathbb{C}^n$, the equations $F_1, \ldots, F_p$, $M_p, \ldots, M_{p+i-1}$ form a reduced regular sequence and they define the affine variety $\widehat{W}_{K^{n-p-i}}(S) \backslash V(m)$.*

Proof. The Proposition 8 and 13 together imply that $\widehat{W}_{K^{n-p-i}}(S)$ is defined, outside of $V(m)$, by the equations $F_1, \ldots, F_p, M_p, \ldots, M_{p+i-1}$. A proof similar to the one of Lemma 10 shows that these equations intersect transversally outside of $V(m)$ (see [BGHM01] Theorem 8 for details). Therefore these equations form a reduced regular sequence. □

3.4.2 External Flags

We can now deal with external flags and generalized polar variety. The results are very similar. A way to choose a random internal flag is to pick some random $a^*_{i,j}$ with $1 \leqslant i \leqslant n-p-i+1$ and $1 \leqslant j \leqslant n$. Then the points $A^*_i = (0 : a_{i,1} : \ldots : a_{i,n})$ plus $A^*_{n-p-i+1} = (1 : a_{n-p-i+1,1} : \ldots : a_{n-p-i+1,n})$ will span a $(n-p-i)$-dimensional space K^{n-p-i}. The previous matrix $\Gamma^{(i)}$ now has the form

$$\Gamma^{(i)} = \begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \cdots & \frac{\partial F_p}{\partial X_n} \\ a^*_{1,1} & \cdots & a^*_{1,n} \\ \vdots & \vdots & \vdots \\ a^*_{n-p-i+1,1} - X_1 & \ldots & a^*_{n-p-i+1,n} - X_n \end{bmatrix}.$$

We now do the same manipulation but on the smaller bloc of lines $A^*_1, \ldots, A^*_{n-p-i}$. Hence there exists $B \in \mathrm{GL}_n(\mathbb{Q})$ and $G \in \mathrm{GL}_{n-p-i}(\mathbb{Q})$ such that

$$\check{\Gamma}^{(i)} = \Gamma^{(i)} B = \begin{bmatrix} \mathrm{Jac}(F(Z)) \\ 0_{p+i-1,n-p-i} \quad G_{n-p-i,n-p-i} \\ c_1 - Z_1 \quad \ldots \quad c_n - Z_n \end{bmatrix}.$$

If we take advantage of the bloc of 0 to reduce our minors, we will get the following proposition.

Proposition 15. *The generalized polar variety $\widehat{W}_{K^{n-p-i}}(S)$ for the external flag member K^{n-p-i} is the subvariety of S where all $(p+1)$-minor of the following extended Jacobian matrix vanish :*

$$ExtJac := \begin{bmatrix} Jac(F(Z_{1,\ldots,p+i})) \\ c_1 - Z_1 \quad \ldots \quad c_{p+i} - Z_{p+i} \end{bmatrix}.$$

This proposition leads us to the final theorem for external flags.

Theorem 16. *Suppose that $Z_1, \ldots, Z_n$ are in generic position with respect to the variety S. Let m be any upper p-minor of the Jacobian $Jac(F(Z_{1\ldots p+i}))$ and $M_{p+1}, \ldots, M_{p+i}$ the usual $(p+1)$-minors of the matrix ExtJac. Then in the open subset $\{m \neq 0\}$ of $\mathbb{C}^n$, the equations $F_1, \ldots, F_p, M_{p+1}, \ldots, M_{p+i}$ form a reduced regular sequence and define the affine variety $\widehat{W}_{K^{n-p-i}}(S) \backslash V(m)$.*

Proof. The proof is the same as Theorem 14. We can observe that in this case the intersection is transversal outside of $V(m)$ as a direct consequence of Lemma 10. □

We have the following important corollary in the case $i = n - p$.

Corollary 17. *Suppose that $Z_1, \ldots, Z_n$ are in generic position with respect to the variety S. Let $M_{p+1}, \ldots, M_{p+i}$ be the usual $(p+1)$-minors of the matrix ExtJac. Then $F_1, \ldots, F_p$, $M_{p+1}, \ldots, M_n$ form a reduced regular sequence and define the affine variety $\widehat{W}_{K^0}(S)$.*

Proof. We have to prove that if $Z_1, \ldots, Z_n$ are in generic position and $c_1, \ldots, c_n$ are random then the upper p-minor m does not vanish at any point of $\widehat{W}_{K^0}(S)$.

Let $a_1, \ldots, a_n$ be random rational numbers and define the polar variety $\widehat{W}_K(S) := \widehat{W}_{K^0}(S)$ for $K^0 = (1 : a_1 : \ldots : a_n)$. The variety $\widehat{W}_K(S)$ is defined by $F_1, \ldots, F_p$ and the $(p+1)$-minors of the matrix

$$\Gamma := \begin{bmatrix} \mathrm{Jac}(F(X)) \\ a_1 - X_1 \quad \ldots \quad a_n - X_n \end{bmatrix}.$$

Let M be a point of $\widehat{W}_K(S)$ and $x = (x_1, \ldots, x_n)$ its affine coordinates. By hypothesis we have that the vectors $\left(\frac{\partial F_1}{\partial X_i}(x), \ldots, \frac{\partial F_p}{\partial X_i}(x)\right) \in \mathbb{R}^p$ for $1 \leqslant i \leqslant n$ form a generating family.

Then we apply a random linear change of coordinates given by the matrix $B = (b_{i,j}) \in \mathrm{GL}_n(\mathbb{R})$; the new coordinates $Z_1, \ldots, Z_n$ are defined by $X_j = \sum_{l=1}^n b_{l,j} Z_l$ for $1 \leqslant j \leqslant n$. It induces new coordinates $z = (z_1, \ldots, z_n)$ for the point M and a new matrix

$$\mathrm{ExtJac}(Z) := \Gamma\ B = \begin{bmatrix} \mathrm{Jac}(F(Z)) \\ c_1 - Z_1 \quad \ldots \quad c_n - Z_n \end{bmatrix}.$$

Since the first p columns of $\mathrm{Jac}(F(Z))(z)$ are general linear combinations of all the columns of $\mathrm{Jac}(F(X))(x)$ which span $\mathbb{R}^p$, they generate $\mathbb{R}^p$ too. Hence the upper p-minor m of $\mathrm{Jac}(F(Z))$ does not vanish at M. We can do the same for a finite number of points and so the upper p-minor m of $\mathrm{Jac}(F(Z))$ does not vanish at any point of $\widehat{W}_K(S)$. □

4 Real Polynomial equation solving

The geometric and algebraic results of Sections 2 and 3 allow us to enlarge the range of applications of the new generation of elimination procedures for real algebraic varieties. We will first introduce this procedures. Then we will focus on our application.

4.1 A Gröbner-free alternative for polynomial system solving

Let $F_1, \ldots, F_n$ and g be polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ such that the system $F_1 = \ldots = F_n = 0$ with $g \neq 0$ has only a finite set of solutions over the field $\mathbb{C}$. By solving we mean computing a representation of the previous set in the form

$$\{(v_1(T), \ldots, v_n(T)) \mid q(T) = 0\}$$

where $q \in \mathbb{Q}[T]$ is monic and separable and the v_i, $1 \leqslant i \leqslant n$, are univariate rational functions with coefficients in $\mathbb{Q}$. This presentation is called a *geometric resolution*. The real roots of q give exactly the real solutions.

We are now going to introduce the basics of a data structure for the representation of polynomials of $\mathbb{Q}[X_1, \ldots, X_n]$ and its complexity measure. A straight-line program β over $\mathbb{Q}$ is a step by step evaluation program of certain output polynomials, say $F_1, \ldots, F_p$, in $\mathbb{Q}[X_1, \ldots, X_n]$. Each step of β corresponds to an arithmetic operation (addition/substraction or multiplication) between results of previous steps and/or inputs $X_1, \ldots, X_n$ and some rational constant. We represent the circuit β by a labelled *directed acyclic graph (dag)*. The

size of this dag measures the sequential time requirements of the evaluation of the output polynomials $F_1, \ldots, F_p$ performed by the circuit β.

We denote by $\delta = \max_i(\deg\ S_i)$ the maximal geometric degree of the varieties $S_i := \overline{V(F_1, \ldots, F_i) \backslash V(g)}$ for $1 \leqslant i \leqslant n$. We have to consider all varieties S_i because the algorithm is iterative and work successively on each of these varieties. The notation $f = \tilde{\mathcal{O}}(g)$ means there exist $k \in \mathbb{N}$ such as $f = \tilde{\mathcal{O}}(g \log(g)^k)$. We can now recall the main statement of the papers [GLS01] and [HMW01].

Theorem 18. *Let $F_1, \ldots, F_n, g$ be polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree at most d and given by a straight-line program of size at most L, such that $F_1, \ldots, F_n$ define a reduced regular sequence in the open subset $\{g \neq 0\}$ of $\mathbb{C}^n$. A geometric resolution of the variety $V(F_1, \ldots, F_n) \backslash V(g)$ can be computed with $\tilde{\mathcal{O}}((n^2 L + n^5) d^2 \delta^2)$ arithmetic operation in $\mathbb{Q}$.*

There is a probabilistic algorithm performing this computation. The correctness of the result relies on choices of elements of $\mathbb{Q}$. Choices for which the result is not correct are enclosed in a strict algebraic subset, hence almost all random choices lead to a correct computation.

4.2 Finding a point in every connected component of a real algebraic set

We suppose that we have a real affine variety $S_{\mathbb{R}}$ given by equations $F_1, \ldots, F_p$ such that $F_1, \ldots, F_p$ intersect transversally in every point of $S_{\mathbb{R}}$. Thus $S_{\mathbb{R}}$ is a pure p-codimensional smooth real affine variety. Let $S := V(F_1, \ldots, F_p)$ the corresponding complex affine algebraic variety.

The polar variety $\widehat{W}_{K^0}(S)$ for a generic K^0 contains a finite number of points (Proposition 12) and at least one point in each connected component of S (Proposition 2). We choose a random point $(1 : a_1 : \ldots : a_n) = K^0$. This way we get our matrix

$$\Gamma := \begin{bmatrix} & \mathrm{Jac}(F) & \\ a_1 - X_1 & \ldots & a_n - X_n \end{bmatrix}$$

on which we apply a generic change of coordinates $B \in \mathrm{GL}_n(\mathbb{Q})$ to obtain the new matrix

$$\mathrm{ExtJac}(Z) := \Gamma\ B = \begin{bmatrix} & \mathrm{Jac}(F(Z)) & \\ c_1 - Z_1 & \ldots & c_n - Z_n \end{bmatrix}.$$

We define as usual the $(p+1)$-minors $M_{p+1}, \ldots, M_n$. Corollary 17 implies that $F_1, \ldots, F_p$, $M_{p+1}, \ldots, M_n$ is a reduced regular sequence. We can then apply Theorem 18 to the equations $F_1 = \ldots = F_p = M_{p+1} = \ldots = M_n = 0$.

We note $S_h := V(F_1, \ldots F_h)$, $1 \leqslant h \leqslant p$ and $\hat{S}_l := V(F_1, \ldots, F_p, M_{p+1}, \ldots, M_l)$, $1 \leqslant l \leqslant n - p$. Observe that the $\hat{S}_l$ are polar varieties of S. We note

$$\delta = max\left(max_{1 \leqslant h \leqslant p}(\deg\ S_h), max_{1 \leqslant l \leqslant n-p}(\deg\ \hat{S}_l)\right)$$

the maximum geometric degree of the intermediate varieties.

We sum up the algorithm in the following theorem.

Theorem 19. *Let $F_1, \ldots, F_p$ be polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ of degree at most d and given by a straight-line program of size at most L. Let $S = V_{\mathbb{R}}(F_1, \ldots, F_p)$ be the corresponding real affine algebraic variety. Suppose that the polynomials $F_1, \ldots, F_p$ intersect transversally in every point of S. Then we can compute with $\tilde{\mathcal{O}}(L n^5 p^2 d^2 \delta^2)$ arithmetic operations in $\mathbb{Q}$ a geometric resolution of a zero-dimensional variety $\hat{S}$, which contains at least one point in each connected component of S.*

Proof. We only have the complexity left to prove. The degree of the minors is bounded by dp and so is the maximal degree of all equations. We need at most $5L$ operations to evaluate the gradient of a straight-line program of size L thanks to [Mor84]. Since determinants of scalar matrix of size p can be computed by a straight-line program of size $\mathcal{O}(p^3)$ and $p \leqslant n$, the minors $M_{p+1}, \ldots, M_n$ can be coded by straight-line programs of size $\mathcal{O}(n^3 L)$. Thus we have the arithmetic complexity $\tilde{\mathcal{O}}(Ln^5 p^2 d^2 \delta^2)$. □

Remark 1. The elimination procedure we use is incremental in the number of equations. The order of the equations $F_1, \ldots, F_p, M_{p+1}, \ldots, M_n$ is important since for every $1 \leqslant l \leqslant n-p$, the variety $\hat{S}_l = V(F_1, \ldots, F_p, M_{p+1}, \ldots, M_l)$ is a polar variety, which means a geometric object related to S that we can expect to control. Moreover, from the proof of Theorem 10 of [BGHP05], we deduces that δ does not depend on the choice of a external flag. So δ is an intrinsic parameter of the variety S.

When the variety S is compact, we can simplify the computations. The theoretical result is the same but there is a significative difference when implemented. Thanks to Proposition 1 we can consider only internal flags and the polar variety $\widehat{W}_{K^0}(S)$ will still be zero dimensional and have at least one point in each connected component of S.

For the computations, we first need to change coordinates $(X_1, \ldots, X_n)$ into coordinates $(Z_1, \ldots, Z_n)$ in generic position with respect to S. It is done by picking a random matrix $M \in \mathcal{M}_n(\mathbb{Q})$ that will give the coordinate change. Since the matrix is random, we can suppose that $M \in \mathrm{GL}(\mathbb{Q})$. This way we have our matrix

$$\mathrm{ExtJac} := \left[\ \mathrm{Jac}(F(Z)) \ \right].$$

We define as usual the upper $(p-1)$-minor m and the p-minors $M_p, \ldots, M_{n-1}$. Similarly to the proof of Corollary 17, the $(p-1)$-minor m does not vanish at any point of $\widehat{W}_{K^0}(S)$. From Theorem 14, we deduce that $F_1, \ldots, F_p, M_p, \ldots, M_{n-1}$ is a reduced regular sequence. We can then apply Theorem 18 to the equations $F_1 = \ldots = F_p = M_p = \ldots = M_{n-1} = 0$. We can expect a small complexity gain since the p-minors M_i are one degree less.

4.3 Experimental Results

The following results are taken from [LW01]. In this article, they apply our algorithm to the context of image compression. One class of methods for data compression uses wavelet transformations. These are invertible linear transformations that are used for exposing the local structure of natural images. By encoding this structure information a smaller representation can be obtained. The JPEG2000 standard is an exemple of wavelet transformations. The computation of optimal wavelet transformations presents a challenge to method of real root finding.

We present here results of computations obtained for the regularity index $r = 3, 4, 5$, which is related to constrains on the wavelets. The number n represents the degree of freedom for our solution. In the present case, polar varieties are also used to find the maximum of a function on a surface through the critical point method. The function associates to each wavelet an estimation of its quality. We emphasize that the equations are encoded as straight-line programs of good evaluation complexity. The varieties corresponding to the wavelet equations have dimensions from 0 to 2.

The computations of the points of the polar varieties were done with both the Kronecker-package, an implementation of our algorithm, and with Magma-internal resolution procedures

r	n	δ	δ^*	$ktime$	$kmemory$	$gtime$	$gmemory$
3	3	12	6	$3.2s$	1600 kB	$0.5s + 0.4s$	1200 kB
3	4	12	8	$7.2s$	21000 kB	$4s + 0.6s$	1700 kB
3	5	54	22	$170s$	4900 kB	$9900s + 2600s$	61700 kB/75200 kB
4	3	4	2	$1.8s$	3400 kB	$0s + 0.001s$	1300 kB
4	4	28	10	$23s$	2200 kB	$48.6s + 50.5s$	6500 kB
4	5	28	10	$42s$	3400 kB	$210s + 82s$	6800 kB/8400 kB
4	6	136	24	$2980s$	23300 kB	$> 22h$	$>$ 470 MB
4	7	136	26	$5370s$	38000 kB	$> 10h$	$>$ 300 MB
5	4	32	6	$25s$	3400 kB	$153s + 225s$	8000 kB/13000 kB
5	5	32	10	$48s$	4500 kB	$420s + 325s$	9000 kB/15500 kB
5	6	168	36	$11853s$	65107 kB	$> 10h$	$>$ 300 MB

Table 1: Computation results with Kronecker and Gröbner bases, Athlon 700MHz

for polynomial systems that use the latest developments in Gröbner bases techniques. In the latter case the triangular decomposition algorithm was used to find a univariate representation of the zero dimensional solution set, so this result has the same structure as the geometric solution in the result of the Kronecker-package. This construction was prepared by the computation of a Gröbner basis in "grevlex" order. In Table 1, δ is the number of complex solutions, δ^* the number of real solutions among them. The next two pairs of columns contain the used time and memory for computations with the Kronecker-package and the Gröbner bases procedures. The latter time is shown as sum of the "grevlex" and the triangulation time. The benchmarks show that the expected good theoretical complexity is confirmed for practical computations on this example.

5 Conclusion

We have designed a new tool for finding efficiently a representative point in each connected component of a real algebraic variety. This algorithm takes advantage of the good evaluation complexity of many systems of equations. Those systems are represented by data structures called straight-line programs, which are algorithms that evaluate polynomials. Contrary to the Gröbner bases algorithms, polynomials are never extended to a full monomial representation. This fact alone implies a lower theoretical complexity. Practical computations confirm the improvement as shown in the presented examples.

The other innovative point of this algorithmic concept consist in the introduction of a new geometric invariant, called the degree of the input system, and the proof that elimination problems have a time complexity that is polynomial in this degree δ and the length L of the input. As we reduce our problem to an elimination problem, we keep a complexity time polynomial in the degree δ and the length L. On the other hand, our algorithm is probabilistic and we can not certify the result.

References

[BGHM97] B. Bank, M. Giusti, J. Heintz, G.M. Mbakop, Polar varieties, real equation solving and data structures: the hypersurface case, J. Complexity 13 (1) (1997) 5-27 (Best Paper Award).

[BGHM01] B. Bank, M. Giusti, J. Heintz, G.M. Mbakop, Polar varieties and efficient real elimination, Math. Z. 238 (2001) 115-144.

[BGHP04] B. Bank, M. Giusti, J. Heintz, L.M. Pardo, Generalized polar varieties and efficient real elimination procedure, Kybernetika, 40 (5)(2004) 519-550.

[BGHP05] B. Bank, M. Giusti, J. Heintz, L.M. Pardo, Generalized polar varieties: geometry and algorithms, J. Complexity 21 (2005) 377-412.

[Dem89] M. Demazure, Catastrophes et bifurcations, Ellipses, Paris 1989.

[DL06] C. Durvye, G. Lecerf, A concise proof of the Kronecker polynomial system solver from scratch, Expositiones Mathematicae, 2006.

[Eag62] J.A. Eagon, D.G. Northcott, Ideals defined by matrices and a certain complex associated with them, Proc. Roy. Soc. Lond. Ser. A 269 (1962) 188-204.

[GLS01] M. Giusti, G. Lecerf, B. Salvy, A Gröbner free alternative for polynomial system solving, J. Complexity 17 (1) (2001) 154-211.

[HMW01] J. Heintz, G. Matera, A. Waissbein, On the time-space complexity of geometric elimination procedures, Appl. Algebra Eng. Commun. Comput. 11 (4)(2001) 239-296.

[LW01] L. Lehmann, A. Waissbein, Wavelets and Semi-Algebraic Sets, Proceedings of WAIT 2001, vol. 30.

[Mat86] H. Matsumura, Commutative Ring Theory, Cambridge Studies in Advanced Mathematics, vol 8., Cambridge University Press, Cambridge, UK, 1986.

[Mor84] J. Morgenstern, How to compute fast a function and all its derivative, Prépublication No. 49, Université de Nice, 1984.

[Pie78] R. Piene, Polar classes of singular varieties, Ann. Scient. Éc. Norm. Sup. 4. t. 11 (1978) 247-276.