# ÉLÉMENT DE PORTFOLIO 03

# Publication

## 1 DÉFINITION DE CET ÉLÉMENT

**Titre de l'élément :** A Nearly Optimal Algorithm for Deciding Connectivity Queries in Smooth and Bounded Real Algebraic Sets

**URL de l'élément :** `https://dl.acm.org/doi/10.1145/2996450`

## 2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

Dans cette publication [15], nous décrivons un nouvel algorithme qui compte le nombre de composantes connexes (et résout des requêtes de connectivité) de variétés algébriques réelles lisses et compactes [1]. Il s'agit d'un problème calculatoire difficile qui trouve de fortes motivations applicatives, notamment en robotique pour la planification de trajectoires et l'analyse de singularités cinématiques [11].

En 1988, J. Canny [5] introduit la notion de carte routière pour résoudre ces problèmes. Il s'agit d'une courbe algébrique dont la trace réelle est contenue dans la variété étudiée et dont l'intersection avec chaque composante connexe de cette variété est connexe. Ainsi, les requêtes de connectivité en dimension arbitraire sont réduites à des requêtes de connectivité en dimension un. L'algorithme de Canny avait pour complexité $(n\delta)^{O(n^2)}$ où $n$ est la dimension de l'espace ambiant et $\delta$ est le maximum des degrés des polynômes donnés en entrée.

Or, un résultat classique de géométrie dû à Petrovski, Oleinik [13], Milnor [12] et Thom [16] établit que le nombre de composantes connexes d'une variété algébrique réelle vit dans $\delta^{O(n)}$.

Malgré plusieurs tentatives d'amélioration, aucun algorithme n'avait été proposé pour le calcul de carte routière avec une complexité dont l'exposant est meilleur que $O(n^2)$ jusqu'à celui proposé dans [14] qui améliore l'exposant en $O\left(n^{1.5}\right)$ en introduisant un nouveau procédé géométrique de résolution. Dès lors, plusieurs algorithmes [3, 4] ont été proposés mais les seuls à avoir une complexité en exposant $\log$-linéaire en $n$ sont tels que cette complexité n'est pas polynomiale en la taille de leur sortie.

Dans la publication qui fait l'objet de ce portfolio, nous obtenons un algorithme de complexité $(n\delta)^{O(n\log(n))}$ pour une taille de sortie en $(n\delta)^{O(n\log(n))}$. Ce résultat est publié au *Journal of the ACM*, la revue porte-drapeau de l'ACM. Il est à noter que la preuve complète de ce résultat de complexité fait plus de $100$ pages.

Ce résultat illustre aussi comment nos méthodologies, combinant algèbre, géométrie, théorie de la complexité et exploitation des structures des systèmes polynomiaux sont mises en œuvre.

## 3 PRÉSENTATION DE CET ÉLÉMENT

### 3.1 Approche générale

L'approche mise en œuvre dans le calcul de cartes routières repose sur des ingrédients qui proviennent de la théorie de Morse en géométrie différentielle et qui sont utilisés ici, dans un contexte algébrique.

Comme illustré par la Figure 1, une carte routière est construite en :

(a) considérant l'ensemble des points critiques d'une projection sur un sous-espace de coordonnées bien choisi (ici la courbe rouge sur la figure) ; ce lieu a une intersection non vide mais non nécessairement connexe avec chaque composante connexe de la variété étudiée ;

(b) ajoutant à cet ensemble de points critiques des sections (en jaune sur la figure) de la variété étudiée pour réparer les défauts de connectivité.

Les résultats de [14] ont permis une plus grande flexibilité dans les choix de l'ensemble des points critiques (et donc de la projection associée). Notamment, alors que le schéma géométrique de résolution utilisé jusqu'alors imposait de choisir une projection sur un plan et donc, une courbe comme ensemble de points critiques, ce qui,

1. Une variété algébrique réelle est l'ensemble des solutions réelles de systèmes d'équations polynomiales à coefficients réels.

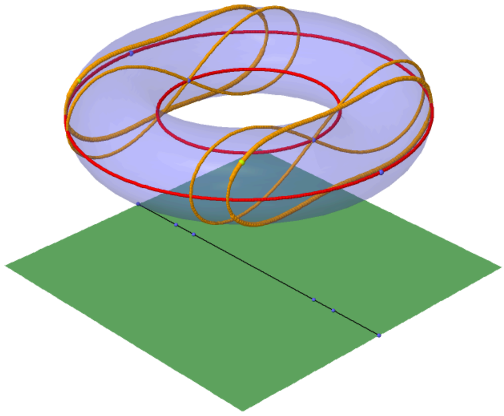

FIGURE 1 – Construction d'une carte routière sur un tore

pour des raisons intrinsèques conduisait à une complexité exponentielle en $O(n^2)$, il est devenu possible de choisir des lieux critiques de plus grande dimension.

## 3.2 Des systèmes structurés pour une meilleure complexité

Le choix fait dans cette publication, naturel au demeurant, a été d'équilibrer les dimensions des lieux critiques et sections considérés pour mettre en place une stratégie du type "diviser pour régner" : lieux critiques et sections sont alors de dimension approximativement $d/2$ où $d$ est la dimension de la variété étudiée et l'algorithme est ensuite appelé récursivement sur chacun de ces lieux géométriques. Cette stratégie est aussi facile à décrire qu'elle est difficile à mettre en place et à prouver rigoureusement.

En effet, ne serait-ce qu'un encodage naïf des lieux critiques, considérés récursivement, conduirait à des complexités doublement exponentielles en $n$. Aussi, ces appels récursifs nécessitent de garantir un certain nombre de propriétés géométriques non triviales (lissité, équidimensionnalité notamment) aux objets considérés.

Pour contourner cette difficulté, nous combinons notre expertise géométrique du problème à celle qui concerne les systèmes polynomiaux structurés, notamment les polynômes multi-homogènes en montrant comment ces lieux critiques récursifs peuvent être encodés par des systèmes que nous avons appelé systèmes de Lagrange généralisés. Ceux-ci font intervenir un nombre de variables significativement supérieur à celui de la dimension de l'espace ambient, mais, la structure naturellement multi-homogène de ces systèmes fait que les degrés de leurs ensembles de solutions sont bien maîtrisés.

La virtuosité de la preuve complète du théorème de complexité consiste alors à montrer que les propriétés requises pour les appels récursifs sont satisfaits et surtout la conception d'algorithmes dédiés permettant de résoudre ces systèmes de Lagrange généralisés dans des complexités qui sont quadratiques en le degré de leurs ensembles de solutions.

Au final, nous obtenons un algorithme de calcul de cartes routière dont la complexité arithmétique est en

$$O\tilde{}\left(16^{9d} E(n\log_2(n))^{6(2d+12\log_2(d))(\log_2(d)+7)} \delta^{3(2n+1)(\log_2(d)+5)}\right)$$

où $d$ est la dimension de la variété étudiée et $E$ la complexité d'évaluation du système étudié. Cette complexité est en fait cubique en le degré de la carte routière et donc sous-quadratique en la taille de sa sortie.

## 3.3 Impact scientifique

L'impact de ce résultat et les perspectives qu'il ouvre pour les applications en robotique sont multiples et avérées par les publications [6–8].

De manière plus marquante, mentionnons également que la publication de cet article a engendré un intérêt du côté du calcul numérique pour ces méthodes (voir [9] et [10]).

Enfin, les méthodes de résolution de systèmes polynomiaux structurés développées dans cet article ont un impact qui va bien au-delà du cadre applicatif lié à la robotique puisque ces résultats ont déjà été utilisés par une partie de la communauté de cryptologie [1, 2].

# 4 RÉFÉRENCES BIBLIOGRAPHIQUES


[1] Simon Abelard. Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus. *Journal of Complexity*, 57 :101440, 2020.

[2] Simon Abelard, Pierrick Gaudry, and Pierre-Jean Spaenlehauer. Improved complexity bounds for counting points on hyperelliptic curves. *Foundations of Computational Mathematics*, 19 :591–621, 2019.

[3] Saugata Basu and Marie-Françoise Roy. Divide and conquer roadmap for algebraic sets. *Discrete & Computational Geometry*, 52 :278–343, 2014.

[4] Saugata Basu, Marie-Françoise Roy, Mohab Safey El Din, and Éric Schost. A baby step–giant step roadmap algorithm for general algebraic sets. *Foundations of Computational Mathematics*, 14 :1117–1172, 2014.

[5] John Canny. *The complexity of robot motion planning*. MIT press, 1988.

[6] Jose Capco, Mohab Safey El Din, and Josef Schicho. Robots, computer algebra and eight connected components. In *ISSAC '20 : International Symposium on Symbolic and Algebraic Computation*, ISSAC'20 : Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation, pages 62–69, Kalamata / Virtual, Greece, 2020. ACM.

[7] Jose Capco, Mohab Safey El Din, and Josef Schicho. Positive dimensional parametric polynomial systems, connectivity queries and applications in robotics. *Journal of Symbolic Computation*, 2023.

[8] Damien Chablat, Rémi Prébet, Mohab Safey El Din, Durgesh Salunkhe, and Philippe Wenger. Deciding Cuspidality of Manipulators through Computer Algebra and Algorithms in Real Algebraic Geometry. In *2022 International Symposium on Symbolic and Algebraic Computation*, Lille, France, 2022.

[9] Changbo Chen, Wenyuan Wu, and Yong Feng. Numerical roadmap of smooth bounded real algebraic surface. *Computer Aided Geometric Design*, 79 :101858, 2020.

[10] Reza Iraji and Hamidreza Chitsaz. Nuroa : A numerical roadmap algorithm. In *53rd IEEE Conference on Decision and Control*, pages 5359–5366. IEEE, 2014.

[11] Lydia E Kavraki and Steven M LaValle. Motion planning. In *Springer handbook of robotics*, pages 139–162. Springer, 2016.

[12] John Milnor. On the Betti numbers of real varieties. *Proceedings of the American Mathematical Society*, 15(2) :275–280, 1964.

[13] I. G. Petrovskiĭ and O. A. Oleĭnik. On the topology of real algebraic surfaces. *Doklady Akad. Nauk SSSR (N.S.)*, 67 :31–32, 1949.

[14] Mohab Safey El Din and Éric Schost. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete & Computational Geometry*, 45(1) :181–220, 2011.

[15] Mohab Safey El Din and Éric Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *Journal of the ACM (JACM)*, 63(6) :48 :1–48 :37, 2017. Major revision, accepted for publication to Journal of the ACM.

[16] René Thom. Sur l'homologie des variétés algébriques réelles. *Differential and combinatorial topology*, pages 255–265, 1965.