

Décomposition Algébrique Cylindrique en Coq/Rocq

Quentin Vermande

sous la direction d'Yves Bertot et Cyril Cohen

28 Janvier 2025

Université Côte d'Azur, Inria, STAMP, École Normale Supérieure, Université PSL, Université Claude Bernard Lyon 1, ENS de Lyon, LIP, CNRS, CASH



Un aperçu de la Décomposition Algébrique Cylindrique

Constructions précises

Formalisation

Un aperçu de la Décomposition Algébrique Cylindrique

Le cadre du problème

R corps réel clos (e.g. $\mathbb{R}$, $\mathbb{R}_{\text{alg}}$), $n \in \mathbb{N}$.

Définition (cellule)

La seule cellule de R^0 est $\{R^0\}$. Pour $n \in \mathbb{N}$, les cellules de R^{n+1} sont obtenues en découpant le cylindre $C \times R$ au dessus d'une cellule C de R^n le long de graphes de fonctions semi-algébriques continues de C dans R .



Le résultat

$\mathcal{P} \subset R[X_0, \dots, X_{n-1}]$ fini.

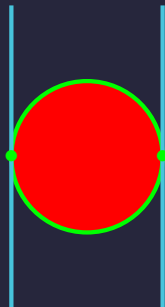
Théorème ([BPR06])

$\exists \mathcal{S}$ partition finie de R^n en cellules,

$\forall P \in \mathcal{P}, C \in \mathcal{S},$

P a un signe constant sur C .

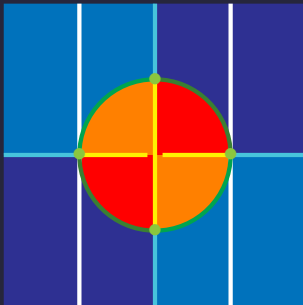
E.g. $\mathcal{P} = \{X^2 + Y^2 - 1\}$. $\mathcal{S} =$



Exemple : élimination des quantificateurs

$$\exists Y, X^2 + Y^2 < 1 \wedge 0 < XY$$

$$\text{CAD}(\{X^2 + Y^2 - 1, XY\}) =$$



$$(\exists Y, X^2 + Y^2 < 1 \wedge 0 < XY) \Leftrightarrow -1 < X < 0 \vee 0 < X < 1$$

Le pourquoi

- élimination rapide des quantificateurs [Col75]
- calcul formel
- robotique [SS83]
- systèmes dynamiques [ST11]
- systèmes hybrides [Pla22]

The dearth of efficient formally-verified support for QE is in part a consequence of the intricacy of QE algorithms. There is arguably a tradeoff [37] between the computational efficiency of an algorithm and the tractability of verification. Most notably, the CAD algorithm is efficient but complex and tremendously difficult to verify; only the significantly simpler univariate case has been fully verified (independently, in Isabelle/HOL [25] and PVS [30]). Further, in order for CAD to realize its full potential for efficiency, many further insights [3, 10, 16, 28] beyond the original development [9] are needed, and improving CAD and algorithms for real QE at large is an active area of research.

[KTP23]

Récurrance sur n , cas $n = 0$ trivial. En dimension $n + 1$, pour $\mathcal{P} \subset R[X_0, \dots, X_n]$:

1. Élimination : $\mathcal{Q} = \text{elim}(\mathcal{P}) \subset R[X_0, \dots, X_{n-1}]$
2. Récurrance : $\mathcal{T} = \text{CAD}(\mathcal{Q})$
3. Remontée : Les cellules de $\mathcal{S}$ sont obtenu en partitionnant les cylindres $C \times R$ au dessus des cellules C de $\mathcal{T}$ selon les graphes des fonctions donnant les racines des polynômes de $\mathcal{P}$ vus comme fonctions de C dans $R[X]$.

Constructions précises

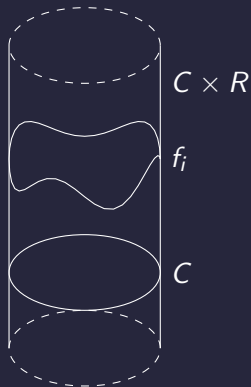
Partitions de cylindres

$$C \subset \mathbb{R}^n, f_1 < \dots < f_d : C \rightarrow \mathbb{R}$$

Définition

La partition du cylindre $C \times \mathbb{R}$ selon les f_i , $1 \leq i \leq d$ est la partition de $C \times \mathbb{R}$ contenant :

- Les graphes des f_i , $1 \leq i \leq d$
- L'intersection des épigraphes des f_i , $1 \leq i \leq d$
- L'intersection des hypographes des f_i , $1 \leq i \leq d$
- Pour $1 \leq i \leq d - 1$, l'intersection de l'épigraphe de f_i et l'hypographe de f_{i+1} .



$P \in R[X_0, \dots, X_n]$, $C \subset R^n$ cellule

Définition (évaluation partielle)

$$\begin{aligned}\overline{P} : R^n &\rightarrow R[X] \\ x &\mapsto P(x_0, \dots, x_{n-1}, X)\end{aligned}$$

$f_1 < \dots < f_d : C \rightarrow R$ racines de $\overline{P}$.

Lemme

Les f_i , $1 \leq i \leq d$ sont continues et semi-algébriques.

Partitions semi-algébriques

" $P = \sum_{i=0}^{n-1} p_i X^i \in R[X]$ ", " $r_0, \dots, r_{m-1}$ racines de P ".

$$\begin{aligned} & \left(\bigwedge_{i=0}^{n-1} p_i = 0 \wedge m = 0 \right) && \text{cas } P = 0 \\ & \vee \left(\bigwedge_{i=0}^{m-1} P(r_i) = 0 \right) && \text{les } r_i \text{ sont racines de } P \\ & \wedge \left(\bigwedge_{i=0}^{m-2} r_i < r_{i+1} \right) && \text{les } r_i \text{ sont ordonnés} \\ & \wedge \forall x, P(x) = 0 && \text{il n'y a pas d'autre racine} \\ & \quad \rightarrow \bigvee_{i=0}^{m-1} x = r_i \end{aligned}$$

Formalisation

- Système : Coq (8.18 et plus)
- Bibliothèques : mathcomp, mathcomp-real-closed et mathcomp-analysis + définition des ensembles semi-algébriques
- ~ 10000 loc
- ~ 5 mois
- Non-extractible à cause d'une mauvaise interaction entre mathcomp, le polymorphisme d'univers et le module d'extraction
- Non-efficace à cause des primitives utilisées

Spécification

```
Fixpoint isCylindricalDecomposition n (S : {fset {SAset R^n}}) :=
  SAset_partition S /\
  if n is k.+1 then
    let S' := [fset SAset_cast k s | s in S] in
    isCylindricalDecomposition S' /\
    forall (s' : S'), exists m (xi : m.-tuple {SAfun R^k -> R^1}),
      (forall i, {within [set` val s'], continuous (tnth xi i)}) /\
      sorted <%SA xi /\
      [fset s in S | SAset_cast k s == val s']
      = partition_of_graphs (val s') xi
  else Logic.True.
```

```
Definition poly_invariant n (p : {mpoly R[n]}) (s : {SASET R^n}) :=  
  {in s &, forall x y,  
    sgz p.[tnth (ngraph x)] = sgz p.[tnth (ngraph y)]}.  
  
Theorem cylindrical_decomposition n (P : {fset {mpoly R[n]}}) :  
  { S | isCylindricalDecomposition S /\  
    forall (p : P) (s : S), poly_invariant (val p) (val s)}.
```

Conclusion

Merci de votre attention.

 Saugata Basu, Richard Pollack, and Marie-Françoise Roy.
Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics).
Springer-Verlag, Berlin, Heidelberg, 2006.

 George E. Collins.
Quantifier elimination for real closed fields by cylindrical algebraic decomposition.
In H. Brakhage, editor, *Automata Theory and Formal Languages*, pages 134–183,
Berlin, Heidelberg, 1975. Springer Berlin Heidelberg.

-  Katherine Kosaian, Yong Kiam Tan, and André Platzer.
A first complete algorithm for real quantifier elimination in isabelle/hol.
In *Proceedings of the 12th ACM SIGPLAN International Conference on Certified Programs and Proofs*, CPP 2023, page 211–224, New York, NY, USA, 2023.
Association for Computing Machinery.
-  André Platzer.
Correction to : Differential dynamic logic for hybrid systems.
J. Autom. Reason., 66(1) :173, 2022.



Jacob T Schwartz and Micha Sharir.

On the “piano movers” problem. ii. general techniques for computing topological properties of real algebraic manifolds.

Advances in Applied Mathematics, 4(3) :298–351, 1983.



Thomas Sturm and Ashish Tiwari.

Verification and synthesis using real quantifier elimination.

In *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, ISSAC '11, page 329–336, New York, NY, USA, 2011. Association for Computing Machinery.