The complexity of irreducible components

Pascal Koiran

Laboratoire de l'Informatique du Parallélisme

Ecole Normale Supérieure de Lyon
Unité de recherche associée au CNRS n°1398

The Complexity of Irreducible Components

Pascal Koiran

Février 1998

Research Report N$^{\text{o}}$ 98-10

Ecole Normale Supérieure de Lyon
46 Allée d'Italie, 69364 Lyon Cedex 07, France
Téléphone : (+33) (0)4.72.72.80.00 Télécopieur : (+33) (0)4.72.72.80.80
Adresse électronique : lip@lip.ens−lyon.fr

The Complexity of Irreducible Components

Pascal Koiran

Février 1998

Abstract

We show that deciding whether an algebraic variety has an irreducible component of codimension at least d is an $\mathrm{NP}_{\mathbb{C}}$-complete problem for every fixed d (and is in the Arthur-Merlin class if we assume a bit model of computation). This is the first part of a paper which will eventually provide similar results for semi-algebraic sets.

Keywords: irreducible components, dimension, NP-completeness, Blum-Shub-Smale model.

Résumé

On montre que décider si une variété algébrique a une composante irréductible de codimension au moins d est un problème $\mathrm{NP}_{\mathbb{C}}$-complet pour toute constante d (et est dans la classe Arthur-Merlin si on travaille avec un modèle de calcul booléen). Ce rapport est la première partie d'un article qui présentera aussi des résultats similaires sur les ensembles semi-algébriques.

Mots-clés: composantes irréductibles, dimension, NP-complétude, modèle de Blum-Shub-Smale.

The Complexity of Irreducible Components

Pascal Koiran

Pascal.Koiran@ens-lyon.fr

February 4, 1998

Abstract

We show that deciding whether an algebraic variety has an irreducible component of codimension at least d is an $\mathrm{NP}_{\mathbb{C}}$-complete problem for every fixed d (and is in the Arthur-Merlin class if we assume a bit model of computation). This is the first part of a paper which will eventually provide similar results for semi-algebraic sets.

Keywords: irreducible components, dimension, NP-completeness, Blum-Shub-Smale model.

1 Introduction

It was shown in [8] that computing the dimension of algebraic varieties is $\mathrm{NP}_{\mathbb{C}}$-complete in the Blum-Shub-Smale model of computation, and that in the bit model this problem is in AM (the Arthur-Merlin class) assuming the Generalized Riemann Hypothesis. The dimension of a variety is the dimension of its largest irreducible component, and the dimensions of smaller components may also be of interest. We give here similar results for the codimension problem $\mathrm{CODIM}_{\mathbb{C}}^d$: determining whether a variety has an irreducible component of codimension at least d, where d is a given integer. For previous work on the algorithmic aspects of the decomposition of a variety into its irreducible components, see [1, 2, 3] (the first two papers assume a bit model of computation), and [4] for the determination of isolated points.

2 $\mathrm{NP}_{\mathbb{C}}$-Completeness

An instance of $\mathrm{CODIM}_{\mathbb{C}}^d$ consists of a variety $V \subseteq \mathbb{C}^n$ defined by a system

$$f_1(x) = 0, \ldots, f_s(x) = 0 \tag{1}$$

of polynomial equations (we assume that the f_i's have their exponents coded in unary). An instance is positive if V has an irreducible component of codimension at least d.

Theorem 1 *For every $d \geq 0$,* $\mathrm{CODIM}_{\mathbb{C}}^d$ *is* $\mathrm{NP}_{\mathbb{C}}$*-complete.*

For the bit model of computation we have the following result.

Corollary 1 *For every $d \geq 0$,* CODIM^d *is NP-hard and if we assume the Generalized Riemann Hypothesis,* CODIM^d *is in* AM.

The NP-hardness of CODIM^d follows from the same reduction as in the complex model of computation (see below for the details of the complex case). The second part of Corollary 1 is a direct consequence of Theorem 1 and of a general fact:

Theorem 2 *Assuming GRH,* $\mathrm{BP}(\mathrm{NP}_{\mathbb{C}}) \subseteq \mathrm{AM}$.

Proof. Let A be a boolean problem in $\mathrm{NP}_{\mathbb{C}}$. We can assume that the corresponding complex machine is parameter-free by the elimination result of [7]. It is thus possible to reduce A to HN in polynomial time in the bit model (this follows basically from the $\mathrm{NP}_{\mathbb{C}}$-completeness of $\mathrm{HN}_{\mathbb{C}}$). Since $\mathrm{HN} \in \mathrm{AM}$ under GRH (see the long version of [6]), the same is true of A. $\square$

Note that if we only want to apply this result to CODIM^d, the elimination result of [7] is not needed since the $\mathrm{NP}_{\mathbb{C}}$ algorithm for $\mathrm{CODIM}_{\mathbb{C}}^d$ exhibited in the proof of Theorem 1 is parameter-free.

The $\mathrm{NP}_{\mathbb{C}}$-hardness of $\mathrm{CODIM}_{\mathbb{C}}^d$ follows from a simple reduction from $\mathrm{HN}_{\mathbb{C}}$ to $\mathrm{CODIM}_{\mathbb{C}}^d$. To decide whether a system of the form (1) is satisfiable, we introduce d new variables $x_{n+1}, \ldots, x_{n+d}$. The variety of $\mathbb{C}^{n+d}$ defined by

$$f_1(x) = 0, \ldots, f_s(x) = 0, x_{n+1} = 0, \ldots, x_{n+d} = 0$$

is a positive instance of $\mathrm{CODIM}_{\mathbb{C}}^d$ if and only if (1) is satisfiable (indeed, the empty set does not have any irreducible component). If you are uncomfortable with proofs that rely too heavily on the properties of the empty set, write down a system of equations for the variety

$$\{f_1(x) = 0, \ldots, f_s(x) = 0, x_{n+1} = 0, \ldots, x_{n+d} = 0\} \cup \{x_{n+d} = 1\},$$

and you will be convinced that $\mathrm{CODIM}_{\mathbb{C}}^d$ is $\mathrm{NP}_{\mathbb{C}}$-hard for $d \geq 2$.

The proof that $\mathrm{CODIM}_{\mathbb{C}}^d \in \mathrm{NP}_{\mathbb{C}}$ relies on the Dimension Theorem, a classical result from algebraic geometry ([5], Chapter 1, Proposition 7.1).

Theorem 3 *Let $U, V \subseteq \mathbb{C}^n$ be two irreducible varieties of dimension p and q, respectively. Any irreducible component of $U \cap V$ has dimension at least $p+q-n$.*

This implies in particular that $U \cap V$ has dimension at least $p+q-n$ if $U \cap V \neq \emptyset$.

We also need a more algorithmic tool.

Theorem 4 *For every fixed n, the problem of deciding whether $V \subseteq \mathbb{C}^n$ has an insolated point is in* $\mathrm{P}_{\mathbb{C}}$.

In fact, Giusti and Heintz [3] have proved a much more general result: the equidimensional components of V can be constructed in time $s^{O(1)}D^{O(n^2)}$, where D is the maximum degree of the f_i's. Due to the use of (non-constructive) "correct test sequences", their algorithm is nonuniform. These sequences help determine whether certain polynomials computed by straight-line programs are identically 0. However, in fixed dimension, it turns out that these polynomials remain of polynomially bounded degree, and correct test sequences are therefore no longer needed (to determine whether a polynomial is identically 0, we can simply compute the list of its coefficients). This explains why the algorithms of Theorem 4 *are* uniform.

Proposition 1 *Let $V \subseteq \mathbb{C}^n$ be a nonempty variety. The following properties are equivalent:*

(i) There exists an affine subspace E of dimension $\geq d$ such that $V \cap E$ has an isolated point.

(ii) There exists an affine subspace E of dimension d such that $V \cap E$ has an isolated point.

(iii) V has an irreducible component of codimension $\geq d$.

Proof. We first show that (i) implies (ii). Let E be an affine subspace of dimension $\geq d$ such that $V \cap E$ has an isolated point x_0. Let F be any d-dimensional subspace of E going through x_0. This point is *a fortiori* isolated in $V \cap F$.

Next, we show that (ii) implies (iii), or rather that the negation of (iii) implies the negation of (ii). Let $V_1, \ldots, V_r$ be the irreducible components of V, and $d_i = \dim V_i$. If $d_i \geq n - d + 1$ then by the Dimension Theorem the components of $V_i \cap E$ are of dimension at least 1. It follows that if (ii) does not hold, $V \cap E$ is a (possibly empty) union of irreducible varieties of dimension at least 1, and therefore has no isolated point.

Finally, to see that (iii) implies (i) let V_i be a component of dimension $d_i \leq n - d$, and E a sufficiently "generic" affine subspace of dimension $n - d_i$. Then $V_i \cap E$ is finite and nonempty, and moreover for any $j \neq i$, $(V_i \cap E) \cap (V_j \cap E) = \emptyset$ (the genericity of E implies directly the first assertion, and also implies the second assertion if we observe that $\dim(V_i \cap V_j) < d_i$ by the irreducibility of V_i). Therefore the elements of $V_i \cap E$ are isolated in $V \cap E$. $\square$

Proof of Theorem 1. The $\mathrm{NP}_{\mathbb{C}}$ algorithm for $\mathrm{CODIM}_{\mathbb{C}}^d$ is based on the equivalence between (ii) and (iii) in Proposition 1: we guess an affine subspace E of dimension d and decide with the algorithm of Theorem 4 whether $V \cap E$ has an isolated point. More precisely, we guess $a, v_1, \ldots, v_d \in \mathbb{C}^n$ and check (in polynomial time) that $E = a + \mathrm{Vect}(v_1, \ldots, v_d)$ has dimension d. Then we obtain a system of equations for $V \cap E$ in d variables $\lambda_1, \ldots, \lambda_d$ by performing the substitution

$x = a + \sum_{i=1}^{d} \lambda_i v_i$ in (1). Verifying that $V \cap E$ has an isolated point requires only polynomial time since the dimension d is fixed. This completes the proof of Theorem 1 since we have already seen that $\mathrm{CODIM}_{\mathbb{C}}^{d}$ is $\mathrm{NP}_{\mathbb{C}}$-hard. $\square$

3 Final Remarks

A most natural question is whether the codimension problem remains in $\mathrm{NP}_{\mathbb{C}}$ if d is no longer fixed, but rather is given as input. In fact, even if we make the restriction $d = n$, we do not know if the resulting problem (deciding whether a variety has an isolated point) is in the polynomial hierarchy $\mathrm{PH}_{\mathbb{C}}$. $\mathrm{ZC}_{\mathbb{C}}$ is another related problem which is not known to be inside or outside $\mathrm{PH}_{\mathbb{C}}$: given a basic constructible set S (defined by a conjunction of polynomial equalities and disequalities), decide whether S is Zariski closed. All these problems are also open in the bit model of computation.

References

[1] A. Chistov. Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time. *Journal of Soviet Mathematics*, 34(4):1838–1882, 1986. Translated from *Zap. Nauchn. Semin. Leningrad. Odtel. Mat. Inst. Steklov (LOMI)*, 137:124-188, 1984.

[2] A. Chistov. Polynomial-time computation of the dimensions of components of algebraic varieties in zero-characteristic. *Journal of Pure and Applied Algebra*, 117/118:145–175, 1997.

[3] M. Giusti and J. Heintz. Algorithmes – disons rapides – pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. In T. Mora and C. Traverso, editors, *Effective Methods in Algebraic Geometry (MEGA'90)*, Progress in Mathematics 94, pages 169–194. Birkhäuser, 1991.

[4] M. Giusti and J. Heintz. La détermination des points isolés et la dimension d'une variété algébrique peut se faire en temps polynomial. In *Computational Algebraic Geometry and Commutative Algebra (Cortona, 1991)*, pages 216–256. Sympos. Math. XXXIV, Cambridge University Press, 1993.

[5] R. Hartshorne. *Algebraic Geometry.* Graduate Texts in Mathematics. Springer, 1977.

[6] P. Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *Journal of Complexity*, 12(4):273–286, 1996. Long version: DIMACS report 96-27 (http://lip.ens-lyon.fr/~koiran).

[7] P. Koiran. Elimination of parameters in the polynomial hierarchy. LIP Research Report 97-37, Ecole Normale Supérieure de Lyon, 1997.

[8] P. Koiran. Randomized and deterministic algorithms for the dimension of algebraic varieties. In *Proc. 38th IEEE Symposium on Foundations of Computer Science*, pages 36–45, 1997.