Laboratoire de l'Informatique du Parallélisme

École Normale Supérieure de Lyon
Unité Mixte de Recherche CNRS-INRIA-ENS LYON
n° 8512

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

The Complexity of Local Dimensions for Constructible Sets

Pascal Koiran

Janvier 1999

Research Report N° 1999-04

École Normale Supérieure de Lyon
46 Allée d'Italie, 69364 Lyon Cedex 07, France
Téléphone : +33(0)4.72.72.80.37
Télécopieur : +33(0)4.72.72.80.80
Adresse électronique : `lip@ens-lyon.fr`

The Complexity of Local Dimensions for Constructible Sets

Pascal Koiran

Janvier 1999

Abstract

We show that deciding whether an algebraic variety has an irreducible component of codimension at least d is an $NP_{\mathbb{C}}$-complete problem for every fixed d (and is in the Arthur-Merlin class if we assume a bit model of computation). However, when d is not fixed but is instead part of the input, we show that the problem is not likely to be in $NP_{\mathbb{C}}$ or in $coNP_{\mathbb{C}}$. These results are generalized to arbitrary constructible sets. We also study the complexity of a few other related problems.
This report updates LIP report 98-10.

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 $NP_{\mathbb{C}}$-complet pour toute constante d (et est dans la classe Arthur-Merlin si on travaille avec un modèle de calcul booléen). Par contre, si d n'est pas fixé mais est au contraire un entier arbitraire donné en entrée, on montre que ce problème n'est probablement pas dans $NP_{\mathbb{C}}$ ni dans $coNP_{\mathbb{C}}$. Ces résultats sont étendus aux ensembles constructibles. On étudie également la complexité de quelques problèmes connexes.
Ce rapport est une mise à jour du rapport LIP 98-10.

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

The Complexity of Local Dimensions for Constructible Sets

Pascal Koiran
Pascal.Koiran@ens-lyon.fr

15th January 1999

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). However, when d is not fixed but is instead part of the input, we show that the problem is not likely to be in $\mathrm{NP}_{\mathbb{C}}$ or in $\mathrm{coNP}_{\mathbb{C}}$. These results are generalized to arbitrary constructible sets. We also study the complexity of a few other related problems.

This report updates LIP report 98-10.

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

1 Introduction

It was shown in [14] 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 complexity class) assuming the Generalized Riemann Hypothesis (GRH). The dimension of a variety is the dimension of its largest irreducible component, and the dimensions of smaller components may also be of interest (see for instance [18]). In this paper we investigate the complexity of computing the dimensions of irreducible components, or more generally of computing local dimensions of constructible sets (given $x_0 \in \mathbb{C}^n$ and a constructible set $X \subseteq \mathbb{C}^n$, $\dim_{x_0} X$ is $\min \dim(X \cap O)$, where the minimum is taken over all Zariski open sets O containing x_0; if $\overline{X}$ denotes the Zariski closure of X, this is also the largest dimension of an irreducible component of $\overline{X}$ containing x_0). We consider both the classical model of computation and the Blum-Shub-Smale model. For previous work on the algorithmic aspects of the decomposition of a variety into its irreducible components, see [6, 7, 8] (the first two papers assume a bit model of computation), and [9] for the determination of isolated points.

The paper is organized as follows. In section 2 we recall some notions from classical and algebraic complexity theory. In section 3 we give algorithms for computing the Zariski closure of constructible sets and deciding whether a given point is isolated in a constructible set. Consider the following "codimension problem" $\mathrm{CODIM}^d_{\mathbb{C}}$: given a variety $V \subseteq \mathbb{C}^n$, decide whether V has an an irreducible component of codimension at least d (i.e., of dimension $\leq n-d$). In section 4 we show that this problem is $\mathrm{NP}_{\mathbb{C}}$-complete for any fixed d. If V is defined by polynomial equations with integer coefficients given in bits, the corresponding CODIM^d problem is NP-hard, and belongs to AM (assuming GRH). In section 5 we show that if d is no longer fixed but is instead part of the input, the codimension problem is not likely to belong either to $\mathrm{NP}_{\mathbb{C}}$ or $\mathrm{coNP}_{\mathbb{C}}$. Indeed, in both cases the classical polynomial-time hierarchy would collapse to its second level. Along the way, we show that it is coNP-hard to decide whether a variety has isolated points, and NP-hard to decide whether a system of homogeneous polynomial equations has a non-trivial solution. We also point out that $\mathrm{NP}_{\mathbb{C}} = \mathrm{coNP}_{\mathbb{C}}$ would imply the collapse of the polynomial hierarchy to its second level. Section 5 ends with a few open problems. Finally, the results of section 4 are generalized to arbitrary constructible sets in section 6 (algebraic varieties are treated separately in section 4 because there is a simpler algorithm in that case).

2 Complexity of Computations

We recall that $\mathrm{P}_{\mathbb{C}}$ denotes the class of problems of $\mathbb{C}^\infty$ which can be solved in polynomial time in the Blum-Shub-Smale model of computation over the complex numbers [3]. Roughly speaking, a problem $A \subseteq \mathbb{C}^\infty$ is in $\mathrm{P}_{\mathbb{C}}$ if there is an algorithm which on any input $x \in \mathbb{C}^n$ can decide whether $x \in A$ in a number of arithmetic operations and equality tests which is polynomial in n. More background on this model of computation can be found in [2, 5, 17].

We also recall that A is in $\mathrm{NP}_{\mathbb{C}}$ if there exists a polynomial $p(n)$ and a problem $B \in \mathrm{P}_{\mathbb{C}}$ such that for all $x \in \mathbb{C}^n$, $x \in A$ if and only if there exists $y \in \mathbb{C}^{p(n)}$ such that $(x_1, \ldots, x_n, y_1, \ldots, y_{p(n)}) \in B$. One can define the higher levels of the polynomial hierarchy over $\mathbb{C}$ in a similar way (they will not be used in this paper).

As in the classical case, there are natural $\mathrm{NP}_{\mathbb{C}}$-complete problems. Perhaps the simplest example is Hilbert's Nullstellensatz ($\mathrm{HN}_{\mathbb{C}}$): decide whether a system of polynomial equations in several complex variables has a solution. If we consider only polynomial equations with integer coefficients given in bits, the corresponding problem (call it HN) is known to be in the classical complexity class AM if we assume that the generalized Riemann hypothesis is true [12]. AM is a randomized version of NP which is located in the second level of the polynomial hierarchy (i.e., $\mathrm{NP} \subseteq \mathrm{AM} \subseteq \Pi_2$).

There is also a notion of randomization over $\mathbb{C}$: a problem $A \subseteq \mathbb{C}^\infty$ is said to be in $\mathrm{BPP}_\mathbb{C}$ if there exists a polynomial $p(n)$ and a problem $B \in \mathrm{P}_\mathbb{C}$ such that for all $x \in \mathbb{C}^n$, $x \in A$ if and only if the set of $y \in \mathbb{C}^{p(n)}$ such that $(x_1, \ldots, x_n, y_1, \ldots, y_{p(n)}) \in B$ is Zariski dense in $\mathbb{C}^{p(n)}$. However, the situation seems to be dramatically different from the classical case:

Proposition 1 $\mathrm{BPP}_\mathbb{C} = \mathrm{P}_\mathbb{C}$.

For a proof see [15], where a stronger result is established: generic quantifiers can be eliminated in polynomial time even in front of existential quantifiers (i.e., $\mathrm{AM}_c = \mathrm{NP}_\mathbb{C}$ in the terminology of that paper; polynomial-time elimination is in fact possible in front of first-order formulas with a bounded number of quantifier alternations).

3 Isolated Points

We assume that a constructible set $X \subseteq \mathbb{C}^n$ is given as a union of basic constructible sets $X_1, \ldots, X_m$. Each X_i is described by a system of polynomial equalities of inequalities:

$$f_{i,1}(x) = 0, \ldots, f_{i,s_i}(x) = 0;\ g_{i,1}(x) \neq 0, \ldots, g_{i,t_i}(x) \neq 0. \tag{1}$$

All polynomials are given in dense representation. In the sequel, $D \geq 3$ is an upper bound on the degrees of the polynomials defining X.

We now give an algorithm (essentially due to Giusti and Heintz) for computing the Zariski closure of X. This algorithm describes $\overline{X}$ as a union of intersections of zero sets of polynomials (there is one term in the union for each X_i).

Theorem 1 *For every fixed integer $n \geq 0$, the Zariski closure $\overline{X}$ of X can be computed in polynomial time.*

Proof. Since the closure of a union is the union of closures, we may assume that X is basic constructible. We therefore assume that X is described by a system of polynomial equalities and inequalities:

$$f_1(x) = 0, \ldots, f_s(x) = 0;\ g(x) \neq 0.$$

Note that if there are several inequalities $g_1(x) \neq 0, \ldots, g_t(x) \neq 0$ in the system, they can be replaced by $g(x) \neq 0$ where g is the product of the g_i's.

Now we follow closely Giusti and Heintz ([8], Proposition 4.2.5), working out the bounds in greater detail. Let $V = \{x \in \mathbb{C}^n;\ f_1(x) = 0, \ldots, f_s(x) = 0\}$, $W = \{x \in \mathbb{C}^n;\ g(x) = 0\}$, and let E' be the finite-dimensional vector space of polynomials $f \in \mathbb{C}[x_1, \ldots, x_n]$ such that there exist polynomials $p_1, \ldots, p_s \in \mathbb{C}[x_1, \ldots, x_n]$ satisfying $\deg(p_i f_i) \leq D^n(D^n + 2D + 1)$ and

$$f \cdot g^{D^n} = \sum_{i=1}^{s} p_i f_i. \tag{2}$$

We claim that E' defines the Zariski closure of X. This will yield the desired algorithm since we can compute a basis of E' by linear algebra, and the polynomials of this basis will then define $\overline{X}$.

In order to prove the claim, we first show that $\overline{X} \subseteq V(E')$, where $V(E')$ is the algebraic set defined by E'. Since $V(E')$ is closed, it suffices to show that $X \subseteq V(E')$. Let $x \in X$ and $f \in E'$. Since $f_1(x) = \cdots = f_s(x) = 0$ and $g(x) \neq 0$, it follows from (2) that $f(x) = 0$. Since this holds for an arbitrary $f \in E'$, we conclude that $x \in V(E')$.

Let us now establish the converse inclusion $V(E') \subseteq \overline{X}$. By Proposition 3 from [11], $\overline{X}$ can be defined by $n+1$ polynomials $f'_1, \ldots, f'_{n+1}$ of degree bounded by $\deg(\overline{X})$, and $\deg(\overline{X}) \leq \deg(V) \leq D^n$ (the first inequality comes from the fact $\overline{X}$ is a union of irreducible components of V, and the second from Bezout's theorem). Since each f'_j vanishes on $V - W$, the product $f'_j g$ vanishes on V, and by the effective Nullstellensatz [16] there exist polynomials $p_1, \ldots, p_s$ with $\deg(p_i f_i) \leq D^n(D^n + D + 1)$ and an integer $k \leq D^n$ such that

$$(f'_j g)^k = \sum_{i=1}^{s} p_i f_i.$$

This can be rewritten as:

$$f'^k g^{D^n} = \sum_{i=1}^{s} g^{D^n - k} p_i f_i,$$

and since $\deg(g^{D^n-k} p_i f_i) \leq D^n(D^n + D + 1) + D^{n+1}$ we conclude that $f'^k_j \in E'$. Hence f'_j vanishes on $V(E')$. Since this holds for all $j = 1, \ldots, n+1$, we conclude that $V(E') \subseteq \overline{X}$. This completes the proof of the claim, and of the theorem. □

In the above proof, the coefficients of $g = \prod_{1 \leq i \leq t} g_i$ can be computed from the coefficients of the g_i's by computing iteratively $\prod_{2 \leq i \leq j} g_i$ for j from 2 to t. This takes polynomial time since the number of variables is fixed (indeed, the number of monomials in g and in all intermediate products is bounded by $\binom{Dt+n}{n}$)). The fact that products of polynomials in a constant number of variables can be computed efficiently is also used in the proofs of Theorem 2 and Theorem 9.

We say that a point $x_0 \in \mathbb{C}^n$ is isolated in X if there exists a Zariski open set O containing x_0 such that $(X - \{x_0\}) \cap O = \emptyset$, or equivalently if $x_0 \notin \overline{X - \{x_0\}}$. Note that if x_0 is not isolated in X, this does not necessarily implies that $x_0 \in X$. Of course, we say that X has an isolated point if there exists a point $x_0 \in X$ such that x_0 is isolated in X.

Corollary 1 *For every fixed integer $n \geq 0$ the following problem can be solved in polynomial time: given a point $x_0 \in \mathbb{C}^n$ and a constructible set $X \subseteq \mathbb{C}^n$, decide whether x_0 is isolated in X.*

Proof. Compute $Y = \overline{X - \{x_0\}}$ with the algorithm of Theorem 1, and decide whether $x_0 \in Y$. Since X is given as a union of m basic constructible $X_1, \ldots, X_m$, $X - \{x_0\} = \bigcup_{1 \le i \le m}(X_i - \{x_0\})$ can be written under the same form by noticing that $X_i - \{x_0\}$ is the union of the n basic constructible sets $X_i \cap \{x_j \neq x_{0,j}\}$ $(1 \le j \le n)$ where $x_{0,1}, \ldots, x_{0,n}$ are the coordinates of x_0. □

Note that the algorithms of Theorem 1 and Corollary 1 run in single exponential time when the dimension n is not fixed (this fact will not be used in the rest of the paper). When X is an algebraic variety, Giusti and Heintz [8] have shown that all equidimensional components (and in particular the isolated points) can be computed in single exponential time. Their algorithm is non-uniform. They have further studied the complexity of computing isolated points in [9].

4 $\mathrm{NP}_{\mathbb{C}}$-Completeness for Varieties

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

$$f_1(x) = 0, \ldots, f_s(x) = 0 \tag{3}$$

of polynomial equations. Again, we assume that all polynomials are given in dense representation. An instance is positive if V has an irreducible component of codimension at least d.

Theorem 2 *For every $d \ge 0$, $\mathrm{CODIM}_{\mathbb{C}}^d$ is $\mathrm{NP}_{\mathbb{C}}$-complete.*

It will be clear from the proof that this result remains true even if we allow unions of sets of the form (3) as inputs (of course a union of algebraic sets is an algebraic set, but performing the corresponding transformation explicitly may be expensive).

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

Corollary 2 *For every $d \ge 0$, 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 2 is a direct consequence of Theorem 2 and of a general fact ([15], Theorem 5.6).

Theorem 3 *Assuming GRH, the boolean part of* $\mathrm{NP}_{\mathbb{C}}$ *is included in* AM.

The proof goes roughly as follows. 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 [13]. 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 HN $\in$ AM under GRH (see the long version of [12]), the same is true of A.

Note that if we only want to apply this result to CODIM^d, the elimination result of [13] is not needed since the $\mathrm{NP}_{\mathbb{C}}$ algorithm for $\mathrm{CODIM}^d_{\mathbb{C}}$ exhibited in the proof of Theorem 2 is parameter-free.

The $\mathrm{NP}_{\mathbb{C}}$-hardness of $\mathrm{CODIM}^d_{\mathbb{C}}$ follows from a simple reduction from $\mathrm{HN}_{\mathbb{C}}$ to $\mathrm{CODIM}^d_{\mathbb{C}}$. To decide whether a system of the form (3) 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 $\mathrm{CODIM}^d_{\mathbb{C}}$ if and only if (3) 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 $\mathrm{CODIM}^d_{\mathbb{C}}$ is $\mathrm{NP}_{\mathbb{C}}$-hard for $d \geq 2$.

The proof that $\mathrm{CODIM}^d_{\mathbb{C}} \in \mathrm{NP}_{\mathbb{C}}$ relies on the Dimension Theorem, a classical result from algebraic geometry ([10], Chapter 1, Proposition 7.1).

Theorem 4 *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 $U \cap V \neq \emptyset$.

Proposition 2 *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 $V \cap E$. □

Proof of Theorem 2. The $\mathrm{NP}_{\mathbb{C}}$ algorithm for $\mathrm{CODIM}_{\mathbb{C}}^d$ is based on the equivalence between (ii) and (iii) in Proposition 2: we guess an affine subspace E of dimension d and decide with the algorithm of Corollary 1 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 (3). 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 2 since we have already seen that $\mathrm{CODIM}_{\mathbb{C}}^d$ is $\mathrm{NP}_{\mathbb{C}}$-hard. □

5 Unrestricted Codimension

A most natural question is whether the codimension problem remains in $\mathrm{NP}_{\mathbb{C}}$ if d is no longer fixed, but rather is part of the input. We shall give strong evidence that this $\mathrm{CODIM}_{\mathbb{C}}$ problem is unlikely to be in $\mathrm{NP}_{\mathbb{C}}$ or in $\mathrm{coNP}_{\mathbb{C}}$.

Proposition 3 *If* $\mathrm{CODIM}_{\mathbb{C}} \in \mathrm{coNP}_{\mathbb{C}}$ *then* $\mathrm{NP}_{\mathbb{C}} = \mathrm{coNP}_{\mathbb{C}}$.

Proof. $\mathrm{CODIM}_{\mathbb{C}}$ is $\mathrm{NP}_{\mathbb{C}}$-hard since its restrictions $\mathrm{CODIM}_{\mathbb{C}}^d$ are hard. If a $\mathrm{NP}_{\mathbb{C}}$-hard problem is in $\mathrm{coNP}_{\mathbb{C}}$, this implies that $\mathrm{NP}_{\mathbb{C}} = \mathrm{coNP}_{\mathbb{C}}$. □

Proposition 3 can be regarded in its own right as fairly strong evidence that $\mathrm{CODIM}_{\mathbb{C}} \notin \mathrm{coNP}_{\mathbb{C}}$, but consider the following.

Proposition 4 *If* $\mathrm{NP}_{\mathbb{C}} = \mathrm{coNP}_{\mathbb{C}}$ *then (assuming the generalized Riemann hypothesis) the standard polynomial hierarchy collapses at its second level.*

Proof. Let $A \subseteq \{0,1\}^\infty$ be any (standard) coNP problem. Considered as a problem of $\mathbb{C}^\infty$, A is also $\mathrm{coNP}_{\mathbb{C}}$. This problem is therefore in the boolean part of $\mathrm{NP}_{\mathbb{C}}$ if $\mathrm{NP}_{\mathbb{C}} = \mathrm{coNP}_{\mathbb{C}}$. We conclude by Theorem 3 that $\mathrm{coNP} \subseteq \mathrm{AM}$ if $\mathrm{NP}_{\mathbb{C}} = \mathrm{coNP}_{\mathbb{C}}$. This is known to imply $\Sigma^2 = \Pi^2$ [4, 1]. □

The evidence that $\mathrm{CODIM}_{\mathbb{C}} \notin \mathrm{NP}_{\mathbb{C}}$ is almost as strong.

Theorem 5 *If* $\mathrm{CODIM}_{\mathbb{C}} \in \mathrm{NP}_{\mathbb{C}}$ *then (assuming the generalized Riemann hypothesis) the standard polynomial hierarchy collapses at its second level.*

For the proof, we need to introduce several problems of independent interest. An instance of $\mathrm{ISO}_{\mathbb{C}}$ consists of a variety V defined by a system of polynomial equations as in (3). The instance is positive if V has an isolated point.

If the f_i's are now in $\mathbb{Z}[X_1, \ldots, X_n]$ instead of $\mathbb{C}[X_1, \ldots, X_n]$ (and have their coefficients given in bits), we obtain the boolean problem ISO.

An instance of $\mathrm{H_2N}_{\mathbb{C}}$ consists of a system of s homogeneous polynomial equations $f_1 = 0, \ldots, f_s = 0$ in $n+1$ variables $x_1, \ldots, x_{n+1}$. The instance is positive if the f_i's have a non-trivial common zero in $\mathbb{C}^n$.

By restricting again to polynomials with integer coefficients, we obtain the boolean problem $\mathrm{H_2N}$.

Theorem 6 $\mathrm{H_2N}$ *is* NP*-hard and* ISO *is* coNP*-hard.*

Proof. The coNP-hardness of ISO follows immediately from the NP-hardness of $\mathrm{H_2N}$. Indeed, a variety defined by a system of homogeneous polynomials has an isolated point (namely, the origin) if and only if these polynomials do not have a non-trivial common zero (i.e., a common zero different from the origin).

It remains to show that $\mathrm{H_2N}$ is NP-hard. This is done by a reduction from the NP-complete problem BOOLSYS. An instance of this problem is a system of equations in n boolean variables $X_1, \ldots, X_n$. Each equation is of the form $X_i = True$, $X_i = \neg X_j$, or $X_i = X_j \vee X_k$. An instance is positive if it has a satisfying assignment.

Let BS be an instance of BOOLSYS. We shall construct an instance HS of $\mathrm{H_2N}$ in $n+1$ variables $x_1, \ldots, x_{n+1}$ such that BS is satisfiable if and only if HS has a non-trivial solution. There are two group of equations in HS. The first group is made of the n equations $x_i^2 = x_{n+1}^2$ $(1 \leq i \leq n)$. Each equation in the second group is associated to an equation in BS in the following manner. For each equation in BS of the form $X_i = True$ the equation $x_i = -x_{n+1}$ is in HS. To an equation of the form $X_i = \neg X_j$ we associate the equation $x_i = -x_j$, and finally to an equation of the form $X_i = X_j \vee X_k$ we associate the equation

$$4x_i x_{n+1} = (x_j + x_k)^2 + 2x_{n+1}(x_j + x_k) - 4x_{n+1}^2.$$

From a system of s boolean equations in n variables we therefore obtain a system of $s + n$ homogeneous equations in $n+1$ variables. Assume that BS has a satisfying assignment $(X_1, \ldots, X_n)$. It is straightforward to check that for any $x_{n+1} \neq 0$, if we set $x_i = -x_{n+1}$ when X_i is true and $x_i = x_{n+1}$ when X_i is false, $(x_1, \ldots, x_{n+1})$ is a non-trivial solution of HS.

Conversely, assume now that HS has a non-trivial solution $(x_1, \ldots, x_{n+1})$. From the equations in the first group we see that x_{n+1} must be non-zero, and that each x_i must be equal to $-x_{n+1}$ or to x_{n+1}. Set $X_i = True$ if $x_i = -x_{n+1}$, and $X_i = False$ if $x_i = x_{n+1}$. It is again straightforward to check that $(X_1, \ldots, X_n)$ is a solution of BS. Since HS can be constructed from BS in polynomial time, we have shown that $\mathrm{H_2N}$ is NP-hard. □

The above proof shows that if we consider only systems of polynomial equations of degree at most 2, the corresponding restrictions of $\mathrm{H_2N}$ and ISO remain NP-hard and coNP-hard. It turns out that the first part of Theorem 6 can be generalized to arbitrary fields. More precisely, for any field K (of any characteristic) we can consider the problem $\mathrm{H_2N}(K)$: decide whether a systems of homogeneous equations in n variables (with integer coefficients given in bits) has a solution in K^n.

Theorem 7 $\mathrm{H_2N}(K)$ *is* NP*-hard for every field* K*.*

Proof. One can see that the proof of Theorem 6 is valid for any field of characteristic different from two. Let us therefore assume that K is of characteristic two. In this case, we have to do a variation on the proof of Theorem 6. The n equations of the form $x_i^2 = x_{n+1}^2$ in HS are replaced by $x_i^2 = x_i x_{n+1}$. An equation in BS of the form $X_i = True$ is "simulated" by $x_i = x_{n+1}$ in HS. $X_i = \neg X_j$ is simulated by $x_i = x_j + x_{n+1}$, and finally $X_i = X_j \vee X_k$ is simulated by:

$$x_i^2 = x_j x_k + x_{n+1}(x_j + x_k).$$

Assume that BS has a satisfying assignment $(X_1, \ldots, X_n)$. It is straightforward to check that for any $x_{n+1} \neq 0$, if we set $x_i = x_{n+1}$ when X_i is true and $x_i = 0$ when X_i is false, $(x_1, \ldots, x_{n+1})$ is a non-trivial solution of HS.

Conversely, assume now that HS has a non-trivial solution $(x_1, \ldots, x_{n+1})$. From the first n equations in HS we see that x_{n+1} must be non-zero, and that each x_i must be equal to 0 or to x_{n+1}. Set $X_i = True$ if $x_i = x_{n+1}$, and $X_i = False$ if $x_i = 0$. It is again straightforward to check that $(X_1, \ldots, X_n)$ is a solution of BS. Since HS can be constructed from BS in polynomial time, we have shown that $\mathrm{H_2N}(K)$ is NP-hard. □

Proof of Theorem 5. If $\mathrm{CODIM}_{\mathbb{C}} \in \mathrm{NP}_{\mathbb{C}}$ then $\mathrm{ISO} \in \mathrm{NP}_{\mathbb{C}}$ as well since this problem is just the restriction of $\mathrm{CODIM}_{\mathbb{C}}$ obtained by setting $d = n$. If $\mathrm{CODIM}_{\mathbb{C}} \in \mathrm{NP}_{\mathbb{C}}$, ISO is therefore in the boolean part of $\mathrm{NP}_{\mathbb{C}}$. Since ISO is coNP-hard, we conclude as in the proof of Proposition 3 that $\mathrm{coNP} \subseteq \mathrm{AM}$, and the polynomial hierarchy collapses (under GRH). □

The same (or simpler) arguments show that by restricting $\mathrm{CODIM}_{\mathbb{C}}$ to polynomials with integer coefficients given in bits, we obtain a problem which is neither in NP nor coNP, unless NP = coNP.

While $\mathrm{CODIM}_{\mathbb{C}}$ does not seem to lie in the lower levels of the complex polynomial hierarchy, it is not known whether it belongs to that hierarchy at all. Membership to $\mathrm{PH}_{\mathbb{C}}$ is in fact open for $\mathrm{ISO}_{\mathbb{C}}$, and it is also unknown whether the boolean problem ISO belongs to the standard polynomial hierarchy. Finally, it is not known whether $\mathrm{H_2N}_{\mathbb{C}}$ is $\mathrm{NP}_{\mathbb{C}}$-complete.

6 Local Dimensions for Constructible Sets

The goal of this section it to prove the following result.

Theorem 8 *For any fixed integer $d \geq 0$ the following problem is $\mathrm{NP}_{\mathbb{C}}$-complete: given a constructible set $X \subseteq \mathbb{C}^n$, decide whether there exists a point $x_0 \in X$ such that $\dim_{x_0} X \leq n - d$.*

Proof. $\mathrm{NP}_{\mathbb{C}}$ hardness is already known from Theorem 2. Here is a $\mathrm{NP}_{\mathbb{C}}$ algorithm for this problem: guess $x_0 \in \mathbb{C}^n$, verify that $x_0 \in X$ and that $\dim_{x_0} X \leq n - d$. By Theorem 9 below, the verification can indeed be performed in polynomial time. $\square$

It is not difficult to construct examples of constructible sets for which the $\mathrm{NP}_{\mathbb{C}}$ algorithm of Theorem 2 fails. As in Corollary 2, it follows from Theorem 8 that for systems with integer coefficients given in bits, the codimension problem for constructible sets is in AM for any fixed d.

The sequel is devoted to the proof of Theorem 9. Let $Y \subseteq \mathbb{C}^d$ be a constructible set defined by polynomial (in)equations with coefficients in a finitely generated field $K \subseteq \mathbb{C}$. We will use the following characterization of dimension: $\dim Y$ is the largest transcendence degree over K of any sequence $y = (y_1, \ldots, y_d)$ such that $y \in Y$.

Theorem 9 *For every integer $d \geq 0$, the following problem is in $\mathrm{P}_{\mathbb{C}}$:*
Given a constructible set $X \subseteq \mathbb{C}^n$ and a point $x_0 \in \mathbb{C}^n$, decide whether $\dim_{x_0} X \leq n - d$.

The proof relies on the following fact.

Theorem 10 *Let x_0 be a point of $\mathbb{C}^n$ and let $X \subseteq \mathbb{C}^n$ be a constructible set. The two following properties are equivalent.*

(i) *For a generic d-dimensional linear space E, x_0 is isolated in $X \cap (x_0 + E)$.*

(ii) $\dim_{x_0} X \leq n - d$.

The proof of Theorem 10 breaks naturally into two parts. We may assume without loss of generality that x_0 is the origin of $\mathbb{C}^n$.

Proposition 5 *Let Y be a constructible subset of $\mathbb{C}^n$. If* $\dim Y \leq n - d$ *and $d \leq p \leq n$, then* $\dim\, Y \cap E \leq p - d$ *for E in a dense set of p-dimensional linear spaces (in particular, $Y \cap E$ is finite for E in a dense set of d-dimensional linear spaces).*

Proof. There is nothing to prove if Y is finite. Let us therefore assume that $\dim Y \geq 1$, and let K be the subfield of $\mathbb{C}$ generated by the parameters of Y. It suffices to show that if A is a $(n-p) \times n$ matrix with coefficients that are algebraically independent over K, $\dim\,(Y \cap \{Ax = 0\}) \leq p - d$. This follows from the fact that if $a_1, \ldots, a_n$ are algebraically independent over K,

$$\dim(Y \cap \{a_1x_1 + \cdots + a_nx_n = 0\}) < \dim Y.$$

This fact is a direct consequence of the characterization of dimension in terms of transcendence degree and of Lemma 1 below. □

Lemma 1 *Assume that $a_1x_1+\cdots+a_nx_n = 0$ where the a_i's are algebraically independent over K, and x has transcendence degree $r > 0$ over K. Then $x = (x_1, \ldots, x_n)$ has transcendence degree at most $r - 1$ over $K(a)$.*

Proof. Assume for instance that $x_1, \ldots, x_r$ is a transcendence base of $K(x)$ over K. As the a_i's are not algebraically independent over $K(x)$ (because $x \neq 0$), they are not algebraically independent over $K(x_1, \ldots, x_r)$ either. Hence $x_1, \ldots, x_r$ are not algebraically independent over $K(a)$, and $\mathrm{tr.deg}_{K(a)}K(x) = \mathrm{tr.deg}_{K(a)}K(x_1, \ldots, x_r) < r$. □

Proof of Theorem 10. As mentioned previously, we assume that $x_0 = 0$. If $\dim_{x_0} X \leq n - d$ there exists a Zariski-open set O containing x_0 such that $\dim X \cap O \leq n - d$. Applying Proposition 5 to $Y = X \cap O$, we see that $X \cap O \cap E$ is finite for E in a dense set of d-dimensional linear spaces. For such an E, x_0 is isolated in $X \cap O \cap E$ and this point is therefore isolated in $X \cap E$. This shows that (ii) implies (i).

Conversely, assume now that $\dim_{x_0} X \geq n - d + 1$. Then there exists an irreducible variety V and a strict closed subset $W \subset V$ such that $x_0 \in V$, $V \setminus W \subseteq X$ and $\dim V \geq n - d + 1$. Let E be a generic d-dimensional linear space. By the dimension theorem, x_0 lies on an irreducible component V' of $V \cap E$ of dimension at least $\dim V + d - n$. Using now the genericity of E, we see from Proposition 5 that $\dim\, W \cap E \leq \dim W + d - n < \dim V'$. Since $V' \setminus (W \cap E) \subseteq X \cap E$, we conclude that for every Zariski open set O containing x_0, $\dim(X \cap E) \cap O \geq \dim V' \geq 1$, and in particular x_0 is not isolated in $X \cap E$. □

We are now ready for the proof of Theorem 9.

Proof. We will in fact describe a $\mathrm{BPP}_{\mathbb{C}}$ algorithm deciding whether $\dim_{x_0} X \leq n - d$. By Proposition 1, this probabilistic algorithm can be converted into a deterministic algorithm.

The $\mathrm{BPP}_{\mathbb{C}}$ algorithm is as follows: we take random vectors $v_1, \ldots, v_d \in \mathbb{C}^n$ and apply Theorem 10 to $E = \mathrm{Vect}(v_1, \ldots, v_d)$. A system of (in)equations for $X \cap (x_0 + E)$ in d new variables $\lambda_1, \ldots, \lambda_d$ is obtained by performing the substitution $x = x_0 + \sum_{i=1}^{d} \lambda_i v_i$ in the systems of the form (1) defining X. This takes polynomial time since d is fixed. By Corollary 1, deciding whether x_0 is isolated in $X \cap (x_0 + E)$ also takes polynomial time for the same reason. $\square$

Acknowledgment

A significant part of this work was carried out when the author was visiting the Mathematical Sciences Research Institute. Research at MSRI is supported in part by NSF grant DMS-9701755.

References

[1] L. Babai and S. Moran. Arthur-Merlin games: A randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36:254–276, 1988.

[2] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer-Verlag, 1998.

[3] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bulletin of the American Mathematical Society*, 21(1):1–46, July 1989.

[4] R. Boppana, J. Håstad, and S. Zachos. Does co-NP have short interactive proofs? *Information Processing Letters*, 25:127–132, 1987.

[5] O. Chapuis and P. Koiran. Saturation and stability in the theory of computation over the reals. Technical Report 1997/3, Institut Girard Desargues, Université Claude Bernard Lyon I, 1997. To appear in *Annals of Pure and Applied Logic*.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] J. Heintz. Definability and fast quantifier elimination over algebraically closed fields. *Theoretical Computer Science*, 24:239–277, 1983.

[12] P. Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *Journal of Complexity*, 12(4):273–286, 1996. Long version: DIMACS report 96-27.

[13] P. Koiran. Elimination of parameters in the polynomial hierarchy. LIP Research Report 97-37, Ecole Normale Supérieure de Lyon, 1997. To appear in *Theoretical Computer Science.*

[14] 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.

[15] P. Koiran. Elimination of parameters in the polynomial hierarchy. LIP Research Report 98-15, Ecole Normale Supérieure de Lyon, 1998. To appear in *Theoretical Computer Science.*

[16] J. Kollár. Sharp effective Nullstellensatz. *Journal of the AMS*, 1:963–975, 1988.

[17] B. Poizat. *Les Petits Cailloux.* Nur Al-Mantiq Wal-Ma'rifah **3**. Aléas, Lyon, 1995.

[18] A. J. Sommese and C. W. Wampler. Numerical algebraic geometry. In J. Renegar, M. Shub, and S. Smale, editors, *The Mathematics of Numerical Analysis (Park City, Utah, 1995)*, pages 749–763. American Mathematical Society, 1996.