# Randomized and Deterministic Algorithms for the Dimension of Algebraic Varieties*

Pascal Koiran
Laboratoire de l'Informatique du Parallélisme
Ecole Normale Supérieure de Lyon
69364 Lyon Cedex 07, France
koiran@lip.ens-lyon.fr

## Abstract

*We prove old and new results on the complexity of computing the dimension of algebraic varieties. In particular, we show that this problem is NP-complete in the Blum-Shub-Smale model of computation over $\mathbb{C}$, that it admits a $s^{O(1)}D^{O(n)}$ deterministic algorithm, and that for systems with integer coefficients it is in the Arthur-Merlin class under the Generalized Riemann Hypothesis. The first two results are based on a general derandomization argument.*

## 1 Introduction

We wish to compute the dimension of an algebraic variety $V \subseteq \mathbb{C}^n$ defined by a system of algebraic equations

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

where $f_i \in \mathbb{C}[X_1, \ldots, X_n]$. This can be formalized as a decision problem $\mathrm{DIM}_\mathbb{C}$. An instance of $\mathrm{DIM}_\mathbb{C}$ is a system of this form together with an integer $d \leq n$. An instance is accepted if the variety defined by the system has dimension at least $d$. We also consider for each fixed value of $d$ the restriction $\mathrm{DIM}_\mathbb{C}^d$ of $\mathrm{DIM}_\mathbb{C}$. For instance, $\mathrm{DIM}_\mathbb{C}^0$ is the problem of deciding whether a variety has dimension $\geq 0$, i.e., is nonempty. This problem has sometimes been called Hilbert's Nullstellensatz ($\mathrm{HN}_\mathbb{C}$). We also consider systems with integer coefficients (in the standard Turing machine model) since we can give further complexity bounds in that case. The corresponding problems are denoted DIM, $\mathrm{DIM}^d$ and HN.

We show that there is a simple polynomial-time randomized reduction from $\mathrm{DIM}_\mathbb{C}$ to $\mathrm{HN}_\mathbb{C}$. It has been shown in [16] that under the Generalized Riemann Hypothesis (GRH), HN is in the Arthur-Merlin class (AM). This complexity class is included in the second level ($\Pi_2$) of the polynomial hierarchy. It follows from this result and from the randomized reduction that DIM $\in$ AM as well.

Without GRH it is only known that HN $\in$ PSPACE, and that $\mathrm{HN}_\mathbb{C}$ can be solved in parallel polynomial time. It follows from this randomized reduction that the same bounds apply to DIM and $\mathrm{DIM}_\mathbb{C}$. This is not a new result: see [7, 11, 12], and also [19] where special attention is paid to uniformity issues. Another early reference for that problem (with less emphasis on complexity issues) is [18]. The PSPACE algorithm described in section 4.3 seems to be simpler than previously published algorithms.

In [8] and [12], "polynomial time" means polynomial in the input size and in $D^n$, where $D$ is an upper bound on the degree of the $f_i$'s. In fact, the dimension cannot be computed in polynomial time in the usual sense, even if we use a dense representation for the polynomials. To make this point clear, we give a (very simple) NP-hardness proof in section 1.3.

Using a general derandomization argument, we convert the randomized reduction to $\mathrm{HN}_\mathbb{C}$ into a deterministic reduction, showing that $\mathrm{DIM}_\mathbb{C}$ is NP-complete in the Blum-Shub-Smale model of computation over $\mathbb{C}$ [3]. This is perhaps only the second genuine example of a $\mathrm{NP}_\mathbb{C}$-complete problem (all other examples known to the author are straightforward variations on $\mathrm{HN}_\mathbb{C}$, the canonical $\mathrm{NP}_\mathbb{C}$-complete problem). This yields a deterministic algorithm for $\mathrm{DIM}_\mathbb{C}$ with the same sequential complexity as the non-uniform algorithm of [12], i.e., $s^{O(1)}D^{O(n)}$. A similar result is established in [8], albeit for projective varieties only (the author claims that his result also extends to affine varieties). Also the model of computation is different: Chistov's algorithm is not algebraic in the sense that

*This work was supported by the ESPRIT Neurocolt Working Group No. 8556.

the coefficients of input polynomials must be given as a sequence of bits[1].

### 1.1 Outline of the randomized algorithm

Many previous algorithms are based on an effective version of the Noether normalization lemma. We use a different geometric idea (see section 2). Avoiding Noether normalization results in a simpler algorithm, especially for the PSPACE bound. For the reduction to HN, we pick a "random" matrix $A$ and check whether the transformed variety $AV$ has a dense projection in $\mathbb{C}^d$. This is a weaker condition than in Noether Normalization. It is sometimes pointed out in the literature that generic linear transformations can blow up a system's size. This is certainly true, but for the problem under consideration there are at least two simple ways of getting around this difficulty (see section 4).

To check density in $\mathbb{C}^d$, we pick a generic point in $\mathbb{R}^d$ and accept if there exists a point of $AV$ "above" $x$. This can be checked by solving an instance of HN in dimension $n-d$. Here "generic" means that the set of bad choices is nowhere dense (and has Lebesgue measure 0). This procedure can thus be formalized as a probabilistic algorithm that draws random elements from $\mathbb{R}$. In fact we work with ordinary probabilistic algorithms (random elements are from $\{0,1\}$). Any algebraic algorithm that draws random elements from $\mathbb{R}$ can be efficiently converted into an ordinary probabilistic algorithm [14]. Here we use special features of the geometry of this problem (and a result from [14]) to obtain better bounds.

### 1.2 Notations

Let $S$ be a system of the form (1), where the $f_i$'s have degree $d_i \leq D$. For the DIM problem, the size of a system is the bit size of a representation of $S$ in a suitable binary encoding scheme. As usual, for $\mathrm{DIM}_{\mathbb{C}}$ the size of each complex coefficient is defined to be 1.

In this paper we use a sparse representation. This means that we do not charge for monomials with a coefficient equal to 0. A polynomial of degree $D$ in $n$ variables can have up to $\binom{n+D}{D}$ coefficients. Hence there can be a big (exponential) gap between the sizes of dense and sparse encodings. In fact this issue is not that important because one can always assume that the $f_i$'s are of degree $d_i \leq 2$. Indeed, the general case of DIM (or $\mathrm{DIM}_{\mathbb{C}}$) is polynomial-time many-one reducible to this special case: one just has to introduce new variables that help represent monomials of high degree (by "repeated squaring"). Let $S'$ be the system obtained from $S$ by this procedure. The polynomials in $S'$ are polynomials of degree at most 2 in $x \in \mathbb{C}^n$ and new variables $x_{n+1}, \ldots, x_{n+k}$. Let us illustrate this on a random example: starting from

$$\begin{cases} x^5y^4 + x + z^2 = 0 \\ x^2 - y^3 + 2xyz = 0 \end{cases}$$

we obtain

$$\begin{cases} r = x^2; s = r^2; t = sx; u = y^2; v = u^2; w = xy \\ tv + x + z^2 = 0 \\ x^2 - uy + 2wz = 0. \end{cases}$$

Let $V \subseteq \mathbb{C}^n$ be the variety defined by $S$, and $V' \subseteq \mathbb{C}^{n+k}$ the variety defined by $S'$. These two varieties have the same dimension since the projection $\pi_n : \mathbb{C}^{n+k} \to \mathbb{C}^n$ satisfies:

1. $\pi_n(V') = V$;
2. each point of $V$ has a unique preimage in $V'$.

Since $S'$ can be constructed from $S$ in polynomial time, the computation of $\dim V$ can be reduced to the computation of $\dim V'$.

### 1.3 NP-hardness

**Proposition 1.1** *For every $d \geq 0$, $\mathrm{DIM}^d_{\mathbb{C}}$ is $\mathrm{NP}_{\mathbb{C}}$-hard and $\mathrm{DIM}^d$ is NP-hard.*

*Proof.* $\mathrm{DIM}^0_{\mathbb{C}}$ is the canonical $\mathrm{NP}_{\mathbb{C}}$-complete problem. To show that $\mathrm{DIM}^d_{\mathbb{C}}$ is $\mathrm{NP}_{\mathbb{C}}$-hard for $d \geq 1$, we exhibit a (trivial) reduction from $\mathrm{DIM}^0_{\mathbb{C}}$ to $\mathrm{DIM}^d_{\mathbb{C}}$. The reduction is as follows: to decide whether $V \subseteq \mathbb{C}^n$ is nonempty, we ask whether $V' = V \times \mathbb{C}^d$ has dimension at least $d$ ($V' \subseteq \mathbb{C}^{n+d}$ is defined by the same system of equations as $V$; the $d$ additional variables $x_{n+1}, \ldots, x_{n+d}$ do not appear in this system). If $V$ is empty, $V'$ is also empty; and if $V$ is nonempty, $V'$ has dimension $d + \dim V$.

Since $\mathrm{DIM}^0$ is NP-hard, the same reduction shows that $\mathrm{DIM}^d$ is NP-hard as well. $\square$

It is clear from the proof (or from section 1.2) that this result still holds even if we restrict our attention to polynomials of degree 2 and if we use dense representations.

[1] The field of coefficients is represented as an algebraic extension of a transcendental extension of $\mathbb{Q}$, and the generators of this transcendental extension are simply represented by new indeterminates. In this way he still manages to allow arbitrary complex coefficients.

### 1.4 Definable Sets

A basic quasi-algebraic set of $\mathbb{C}^n$ is defined by a system of polynomial equalities and inequalities of the form

$$P_1(x) = 0, \ldots, P_k(x) = 0, Q_1(x) \neq 0, \ldots, Q_l(x) \neq 0$$

where $P_1, \ldots, P_k, Q_1, \ldots, Q_l$ are in $\mathbb{C}[X_1, \ldots, X_n]$. A quasi-algebraic set (or *constructible*) set is a finite union of basic quasi-algebraic sets. By quantifier elimination, a set is quasi-algebraic if and only if it is definable in the first-order theory of $(\mathbb{C}, +, .)$. The following result from [10] gives an effective version of quantifier elimination.

**Theorem 1.2** *Let $K$ be an algebraically closed field and $\Phi$ a prenex formula in the first-order theory of $K$. Let $r$ be the number of quantifier blocks, $n$ the total number of variables, and $\sigma(\Phi)$ the total degree of $\Phi$, defined as:*

$$\sigma(\Phi) = 2 + \sum_{i=1}^{s} \deg\ F_i$$

*where $F_1, \ldots, F_s$ are the polynomials occurring in $\Phi$. $\Phi$ is equivalent to a quantifier-free formula $\Psi$ in which all polynomials have degree at most*

$$2^{n^{O(r)}(\log \sigma(\Phi))^{O(1)}}.$$

*The number of polynomials occurring in $\Psi$ is $O(\sigma(\Phi)^{n^{O(r)}})$.*

*Moreover, when $K$ is of characteristic 0 and $\Phi$ is a formula in which all constants are integers of bit-size at most $L$, the constants in $\psi$ are integers of bit size at most $L.2^{n^{O(r)}(\log \sigma(\Phi))^{O(1)}}$.*

## 2 Normal Position

Let $I \subseteq \{1, \ldots, n\}$ be a set of indices. $\pi_I : \mathbb{C}^n \to \mathbb{C}^{|I|}$ denotes the projection on the $|I|$-dimensional subspace defined by the system of equations $\{x_i = 0;\ i \notin I\}$. It is well known (see e.g. Corollary 4 in section 9.5 of [9]) that for any algebraic variety $V \subseteq \mathbb{C}^n$ of dimension $d$,

1. for $k \leq d$ there exists a set $I$ of $k$ indices such that $\pi_I(V)$ is dense in $\mathbb{C}^k$;

2. for $k > d$ there does not exist a set of $k$ indices with this property.

We say that $V$ is in normal position with respect to the set of variables $\{X_i;\ i \in I\}$ if $\pi_I(V)$ is dense in $\mathbb{C}^{|I|}$ (this terminology may not be quite standard). We say that $V$ is in normal position if it is in normal position with respect to $\{X_1, X_2, \ldots, X_d\}$, and write $\pi_d$ for $\pi_{\{1,2,\ldots,d\}}$.

It is well known that applying a generic linear transformation to $V$ yields a variety of dimension $d$ in normal position. We need to precise the exact meaning of "generic" in this context.

If $A$ is a $n \times n$ matrix, $AV$ denotes the image of $V$ by the linear transformation $x \mapsto Ax$.

**Theorem 2.1** *Let $V \subseteq \mathbb{C}^n$ be a variety of dimension $d$. Let $S_V \subseteq \mathbb{C}^{n^2}$ be the set of matrices $A \in \mathcal{M}_n(\mathbb{C})$ such that:*

1. *$A$ is invertible;*

2. *$AV$ is a variety of dimension $d$ in normal position.*

*$S_V$ contains a set of the form $P_V(A) \cdot \det A \neq 0$ where $P_V \in \mathbb{C}[X_1, \ldots, X_{n^2}]$ is a multilinear polynomial of degree at most $d$.*

$A$ is invertible iff $\det A \neq 0$, and in this case $AV$ is a variety of the same dimension. In order to show that normal position follows from the additional assumption $P_V \neq 0$, we first study a special case.

**Lemma 2.2** *Theorem 2.1 holds when $V$ is an affine subspace.*

*Proof.*
Let $\{v_1, \ldots, v_d\}$ be a basis of $V$. $\{Av_1, \ldots, Av_d\}$ is a basis of $AV$ hence $\{\pi_d(Av_1), \ldots, \pi_d(Av_d)\}$ generates $\pi_d(AV)$. Thus $\pi_d(AV) = \mathbb{C}^d$ if

$$\det(\pi_d(Av_1), \ldots, \pi_d(Av_d)) \neq 0. \qquad (2)$$

This is a multilinear condition of degree at most $d$ in the coefficients of $A$. $\square$

*Proof of Theorem 2.1.* By decomposing $V$ in irreducible components if necessary, we may assume that $V$ is irreducible. Let $x_0 \in V$ be a smooth point of $V$. The tangent space $T$ to $V$ in $x_0$ has dimension $d$. Let us apply Lemma 2.2 to $T$: we claim that one can take $P_V = P_T$. Indeed, let $A$ be a matrix in $S_T$. $AT$ is the tangent space to $AV$ in $Ax_0$. By definition of $S_T$, $\pi_d(AT) = \mathbb{C}^d$ and therefore by the implicit function theorem (Corollary 1.26 in [21]), $\pi_d(AV)$ contains an open set. Hence $\pi_d(AV)$ is dense in $\mathbb{C}^d$. $\square$

Of course dim$AV$ < dim$V$ is possible if $A$ is not invertible (take for instance $V = \{(x_1, x_2);\ x_2 = 0\}$ and $A : (x_1, x_2) \mapsto (x_2, x_2)$).

**Remark 2.3** If $V$ is given by (1) the change of variables $x = A^{-1}y$ yields a system of equations for $AV$. This requires a matrix inversion. Alternatively, one could perform the change of variables $x = Ay$. Then no matrix inversion is required but the coefficients of $A$ must now avoid the zero set of a polynomial of degree $d(n-1)$, instead of degree $d$ only in Theorem 2.1.

## 3 Connected Components

If the projection of an algebraic variety is dense in $\mathbb{C}^l$ then "most" points with integer coordinates belong to the projection. Theorem 3.9 provides an effective version of this statement.

In this section we need to go back and forth between real and complex space. If $z = (x_1 + iy_1, \ldots, x_n + iy_n) \in \mathbb{C}^n$, $\hat{z} = (x_1, y_1, x_2, y_2, \ldots, x_n, y_n) \in \mathbb{R}^{2n}$ denotes the "realification" of $z$. And for $V \subseteq \mathbb{C}^n$, $\hat{V} = \{\hat{x};\ x \in V\}$. If $V$ is defined by a system of $s$ polynomial equations of degree bounded by $D$, $\hat{V}$ is defined by a system of $2s$ equations with the same degree bound.

As in the complex case, $\pi_k : \mathbb{R}^m \to \mathbb{R}^k$ denotes projection on the first $k$ components (usually, $m = 2n$).

The number of connected components of a set $U \subseteq \mathbb{R}^m$ is denoted $B_0(U)$. The following bound is Theorem 4.4.1 from [1] (see also [4]).

**Theorem 3.1** *Let $P \in \mathbb{R}[X_1, \ldots, X_m]$ be a polynomial of degree $D$. The zero set of $P$ has at most $D^{m-1}(D+2)$ connected components.*

A similar bound for systems of algebraic equations immediately follows. Note that the number of equations does not appear in that bound.

**Corollary 3.2** *Let $W \subseteq \mathbb{R}^m$ be defined by a system*

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

*where $f_i \in \mathbb{R}[X_1, \ldots, X_m]$ is a polynomial of degree at most $D$: $B_0(W) \leq (2D)^{m-1}(2D+2)$.*

*Proof.* Apply Theorem 3.1 to $P = \sum_{i=1}^{s} f_i^2$. □

In section 5 we will need a further bound.

**Definition 3.3** *Fix $s$ polynomials $f_1, \ldots, f_s \in \mathbb{R}[X_1, \ldots, X_m]$. A* sign condition *$\epsilon$ is an element of $\{-1, 0, 1\}^s$. A point $x \in \mathbb{R}^m$ satisfies $\epsilon$ if $f_i(x) < 0$ when $\epsilon_i = -1$, $f_i(x) = 0$ when $\epsilon_i = 0$, and $f_i(x) > 0$ when $\epsilon_i = 1$. The sign condition is* consistent *if it is satisfied by some $x \in \mathbb{R}^m$. A* cell *is a connected component of the set of points satisfying a sign condition.*

By definition, the cells form a partition of $\mathbb{R}^m$. They are connected, and the $f_i$'s have constant signs on each cell (and they are maximal with this property).

**Theorem 3.4** *Let $f_1, \ldots, f_s \in \mathbb{R}[X_1, \ldots, X_m]$ be $s$ polynomials of degree at most $D$. They define at most $(sD+1)(2sD+1)^{m+1}(4sD+1)^m$ cells.*

*Proof.* There are at most $(2sD+1)(4sD+1)^m$ consistent sign conditions [20]. By [1] (after correction of a typo in Proposition 4.4.5), the set of points satisfying a given sign condition has at most $(sD+1)(2sD+1)^m$ connected components. Taking the product of these two quantities gives the desired bound. □

This result can be somewhat improved by using Warren's bounds [24].

**Corollary 3.5** *Let $F(u)$ (with $u \in \mathbb{R}^m$) be a quantifier-free formula involving $s$ atomic predicates of degree at most $D$. The set $S$ of $u \in \mathbb{R}^m$ satisfying $F$ has at most $(sD+1)(2sD+1)^{m+1}(4sD+1)^m$ connected components.*

*Proof.* Each cell defined by the $s$ atomic predicates is either included in a unique connected component of $S$, or in a unique connected component of its complement. Hence the number of cells is an upper bound on the number of connected of $S$ (and of its complement). □

In order to work with real rather than complex sample points, we will use the following easy lemma.

**Lemma 3.6** *If a quasi-algebraic set $E \subseteq \mathbb{C}^n$ is dense in $\mathbb{C}^n$ then $E \cap \mathbb{R}^n$ is dense in $\mathbb{R}^n$, otherwise $E \cap \mathbb{R}^n$ has Lebesgue measure 0.*

*Proof.* If $E$ is dense in $\mathbb{C}^n$ it contains a set of the form $P \neq 0$ where $P \in \mathbb{C}[X_1, \ldots, X_n]$ is a nonconstant polynomial. Write $P = Q + iR$ with $Q$ and $R$ in $\mathbb{R}[X_1, \ldots, X_n]$. For $x \in \mathbb{R}^n$, $P(x) \neq 0$ iff $Q(x) \neq 0$ or $R(x) \neq 0$. Either $P$ or $Q$ must be nonconstant, and the complement of the zero set of that polynomial is dense in $\mathbb{R}^n$.

If $E$ is not dense in $\mathbb{C}^n$ it is included in a set of the form $P = 0$ where $P \in \mathbb{C}[X_1, \ldots, X_n]$ is a nonconstant polynomial. By the argument above this is equivalent for $x \in \mathbb{R}^n$ to $Q(x) = 0$ and $R(x) = 0$, where $Q$ and $R$ are the real and imaginary parts of $P$. □

For $W \subseteq \mathbb{R}^m$, $\mu_h(W)$ denotes the proportion of points with integer coordinates smaller than $h$ that lie in $W$, i.e.,

$$\mu_h(W) = |W \cap [h]^n|/h^n$$

where $[h] = \{0, 1, \ldots, h-1\}$.

We need a result which was established in [14] (with slightly different notations).

**Theorem 3.7** *Let $E \subseteq [0,h]^m$ be a measurable set. Let $\kappa(E)$ be the maximum number of connected components of an intersection $E \cap \Delta$ where $\Delta$ is an axis-parallel line.*

*If $\kappa(E)$ is finite, $|\mu(E \cap [0,h]^m)/h^m - \mu_h(E)| \leq m\kappa(E)/h$.*

**Theorem 3.8** *Let $W \subseteq \mathbb{R}^m$ be defined by a system of the form (3). The image of $W$ by the projection $\pi_k : \mathbb{R}^m \to \mathbb{R}^k$ satisfies: $\kappa(\pi_k(W)) \leq (2D)^{m-k}(2D+2)$.*

*Proof.* We need to bound $B_0(U \cap \Delta)$ where $U = \pi_k(W)$ and $\Delta$ is an axis-parallel line. Assume for instance that $\{x_1 = a_1, \ldots, x_{k-1} = a_{k-1}\}$ is an equation of $\Delta$ (i.e., $\Delta$ is parallel to the last axis). $U \cap \Delta$ is the projection on $\Delta$ of a variety $W' \subseteq \mathbb{R}^m$. A system of equations for $W'$ can be obtained by adding the equations $x_1 = a_1, \ldots, x_{k-1} = a_{k-1}$ to (3). $B_0(U \cap \Delta) \leq B_0(W')$ since projections cannot increase $B_0$. Moreover, $B_0(W') = B_0(W'')$ where $W'' \subseteq \mathbb{R}^{m-k+1}$; a system of equations for $W''$ can be obtained by making the substitutions $x_1 = a_1, \ldots, x_{k-1} = a_{k-1}$ in (3). Hence $B_0(W'') \leq (2D)^{m-k}(2D+2)$ by Theorem 3.2. □

**Theorem 3.9** *Let $V \subseteq \mathbb{C}^n$ be defined by a system of degree-$D$ equations, and $V_l = \pi_l(V) \cap \mathbb{R}^l$.*

*If $\pi_l(V)$ is dense in $\mathbb{C}^l$ then $V_l$ is dense in $\mathbb{R}^l$ and for any $h \geq 1$, $\mu_h(V_l) \geq 1 - C/h$ where $C = l(2D)^{2n-2l}(2D+2)$.*

*If $V$ is not dense in $\mathbb{C}^l$ then $\mu(V_l) = 0$ and $\mu_h(V_l) \leq C/h$.*

*Proof.* Let $W_l = \pi_{2l}(\hat{V}) \cap (\mathbb{R} \times \{0\})^l$. Observe that $\kappa(V_l) = \kappa(W_l)$ since the points of $W_l$ are obtained from the points of $V_l$ by interleaving $l$ '0' components. Moreover $\kappa(W_l) \leq \kappa(\pi_{2l}(\hat{V}))$ and by Theorem 3.8, $\kappa(\pi_{2l}(\hat{V})) \leq (2D)^{2n-2l}(2D+2)$. By Lemma 3.6, $\mu(V_l \cap [0,h]^l) = h^l$ if $\pi_l(V)$ is dense in $\mathbb{C}^l$, and $\mu(V_l \cap [0,h]^l) = 0$ otherwise. Hence the result follows from Theorem 3.7 applied to $E = V_l$. □

We conclude this section with a similar result for the set $S_V$ of "good" matrices defined in Theorem 2.1. As in Theorem 3.9 we prefer to work with real rather than complex coefficients, so we deal with $R_V = S_V \cap \mathbb{R}^{n^2}$ instead of $S_V$ proper.

**Theorem 3.10** *Let $V \subseteq \mathbb{C}^n$ be a variety of dimension $d \geq 1$: $\mu_h(R_V) \geq 1 - 2n^2/h$.*

*Proof.* By Theorem 2.1 it is enough to show that $\mu_h(R'_V) \leq 2n^2/h$, where $R'_V$ is the set of real matrices such that $P_V . \det A = 0$. This set has measure 0 since $P_V \not\equiv 0$. Moreover, $R'_V$ is included in the union of the zero sets of two multilinear polynomials. The first such polynomial is $\det A$, and the second one is obtained by separating real and imaginary parts in (2). Thus it remains to show that $\mu_h(Z(P)) \leq n^2/h$ for the zero set of any nonzero multilinear polynomial $P \in \mathbb{R}[X_1, \ldots, X_{n^2}]$. This follows directly from Theorem 3.7 since $\kappa(Z(P)) \leq 1$. □

**Remark 3.11** Theorem 3.7 is a generalization of Schwarz's bound for testing polynomial identities [23]. He gave the same bound for the special case $E = Z(P)$ where $P$ is nonzero polynomial of degree $d$, with $\kappa(E)$ replaced by its worst case upper bound $d$. Instead of Theorem 3.7, one could use his bound together with an "efficient" quantifier elimination result in the proof of Theorem 3.9 (this would presumably give worse results). Schwarz's bound could also be applied more directly in Theorem 3.10 (yielding also a slightly worse result).

# 4 Randomized Reduction

It is sometimes claimed in the literature that generic linear transformations do not preserve sparseness. Indeed, after the change of variables $x = A^{-1}y$, a monomial of the form $x_1^{a_1} \cdots x_n^{a_n}$ in (1) will be replaced by a sum of $n^{a_1+\cdots+a_n} \leq n^D$ monomial in the $y$ variables. However, as pointed out in section 1.2, we can (and will) assume that $D = 2$. Therefore we can compute a system of equations for $AV$ in polynomial time (a more practical solution to that problem is presented in section 4.2). If $A$ turns out to be non-invertible the algorithm halts and rejects $V$ (it is deemed to be of dimension $< d$). In practice one would continue drawing random matrices until an invertible matrix is found.

The precision that should be used for the random elements can be estimated by Theorems 3.9 and 3.10. Assume first that $V$ has dimension at least $d$. The algorithm can fail to accept $V$ only if:

1. $A$ is not in $R_V$, or

2. $A$ is in $R_V$ but the random point $x \in [h]^d$ is not in $\pi_d(AV)$.

By Theorem 3.10 the probability of 1. is at most $2n^2/h$. Therefore we need to use only $\log h = 4 + 2\log n$ bits for the entries of $A$ to make this probability smaller than, say, 1/8.

If $A$ is in $R_V$ then by definition $\pi_d(AV)$ is dense in $\mathbb{C}^d$. Hence by Theorem 3.9 the probability of 2. is at most $6d.4^{2n-2d}/h$. Therefore it suffices to use

$$\log h = 4 + \log 3d + 2(2n - 2d) \tag{4}$$

bits for the components of $x$ to make this probability smaller than 1/8.

These bounds also apply when $V$ has dimension less than $d$. For any invertible matrix $A$, $AV$ also has dimension less than $d$ therefore $\pi_d(AV)$ is not dense in $\mathbb{C}^d$. Hence by Theorem 3.9 the probability of picking a point $x \in \pi_d(AV)$ is also bounded by $6d.4^{2n-2d}/h$.

### 4.1 Conditional Result

This reduction works for systems with arbitrary complex coefficients. For systems with integer coefficients, it follows from the result HN $\in$ AM [16] that DIM $\in$ AM as well.

**Theorem 4.1** *Under the Generalized Riemann Hypothesis,* DIM $\in$ AM.

There are three stages of randomization in the corresponding AM algorithm: the two stages described above (choice of a random matrix and of a random point) plus the randomization stage of the AM algorithm for HN [16]. These random stages are followed by the nondeterministic stage of that algorithm.

Note that this AM algorithm for DIM has two-sided error: it could fail to accept a positive instance due the choice of a bad matrix or a bad point; and it could fail to reject a negative instance due to the choice of a bad point (there are no bad matrices for negative instances) or due to a bad random choice in the AM algorithm for HN. In contrast, that algorithm has one-sided error: positive instances of HN (satisfiable systems) are always correctly classified. One can argue that this difference between HN and DIM is only superficial since an AM algorithm with two-sided error can always be converted into an AM algorithm with one-sided error ([25], Theorem 2). In fact, we will see in Theorem 5.8 of section 5 that there is a deterministic reduction of DIM to HN. This gives directly an AM algorithm with one-sided error for DIM.

### 4.2 Lazy Linear Transformations

Up to now we have used the assumption $D \leq 2$ to preserve sparseness under the linear transformation $V \mapsto AV$. There is another simple solution to that problem. Instead of performing this linear transformation explicitly we just *pretend* to perform it. That is, we consider the variety $\hat{V} \subseteq \mathbb{C}^{2n}$ defined by the system

$$\begin{cases} f_i(x) = 0;\ i = 1, \ldots, s \\ y = Ax. \end{cases} \tag{5}$$

It is clear that $\pi_d(AV) = \hat{\pi}_d(\hat{V})$ where $\hat{\pi}_d : \mathbb{C}^{2n} \to \mathbb{C}^d$ denotes projection on the variables $y_1, \ldots, y_d$. Therefore in order to find out whether a given point $(y_1, \ldots, y_d)$ is in $\pi_d(AV)$ we can substitute its components in (5) and check whether the resulting system ($2n$ equations in $2n - d$ variables) is satisfiable. In fact, the last $n-d$ equations can be dropped from this system since they are automatically satisfied (from the relation $y = Ax$) if a solution exists for the $x$ variables. This yields a system of $s + d$ equations in $x_1, \ldots, x_n$.

This "lazy" solution seems to be quite practical since no additional variable is introduced, and the sparsity of the system is preserved (we just add $d$ linear equations). Note that this method can be interpreted as follows: a variety has dimension at least $d$ if it has a nonempty intersection with a generic affine subspace of dimension $n - d$. A similar idea is used in [8]: a variety has dimension at most $d$ if it has a finite intersection with a generic affine subspace of dimension $n - d$.

### 4.3 Space Complexity

Without GRH we only know that HN $\in$ PSPACE. Since the reduction described above can be implemented in polynomial space we can still conclude that DIM $\in$ PSPACE. In fact there is no need for a linear transformation in a PSPACE algorithm: we can use directly the characterization of dimension given at the beginning of section 2. That is, we enumerate the $\binom{n}{d}$ sets of $d$ indices. This requires only $O(n)$ space. For each such set we check whether $\pi_I(V)$ is dense in $\mathbb{C}^d$. To do this we enumerate the $h^d$ points of $[h]^d$ and check whether a majority of them is in $\pi_I(V)$. By (4) this second enumeration procedure requires $O(dn)$ space. This yields the following result.

**Theorem 4.2** DIM $\in$ PSPACE.

The above algorithm is quite simple but by no means optimal. The best bounds are polynomial in $n$ but only polylogarithmic in the other parameters (those are bounds on the work space only; the input space is not counted). Here we are polynomial in $n$ (this is arguably the most important parameter) but cannot be polylogarithmic in the other parameters with the present technique. For instance, just copying a coefficient of the input system requires space $L$, and this is definitely not $(\log L)^{O(1)}$! The solution to this problem is by now well known: first one must design an efficient parallel algorithm, and then convert it into a space-efficient algorithm using the equivalence between parallel time and sequential space discovered by Borodin [5]. This strategy could be carried out with our present algorithm. We will not go into the details since they can be found in many recent papers, for instance [19]. That paper gives a $O(n^4 \log^2(LsD))$ space bound for both HN and DIM (and also for Noether Normalization).

For $\mathrm{DIM}_{\mathbb{C}}$, Theorem 4.2 would translate into a polynomial depth bound for uniform arithmetic circuits. In terms of sequential complexity, our enumeration procedure implies a uniform bound of roughly $s^{O(1)}D^{O(n^2)}$ for $\mathrm{DIM}_{\mathbb{C}}$ (a similar bound holds for DIM, but bit size must be taken into account). We will see in section 5 that this bound can be reduced to $s^{O(1)}D^{O(n)}$.

## 5 $\mathrm{NP}_{\mathbb{C}}$-Completeness

We already know that $\mathrm{DIM}_{\mathbb{C}}$ is $\mathrm{NP}_{\mathbb{C}}$-hard. To prove $\mathrm{NP}_{\mathbb{C}}$-completeness, we need to exhibit a deterministic reduction to $\mathrm{HN}_{\mathbb{C}}$. It will be based on the randomized reduction of section 4 (as implemented in section 4.2).

The main tool is a "derandomization" result of independent interest. First we need to introduce a notation: given a formula $F(u)$ where $u \in \mathbb{C}^k$, $\exists^* u F(u)$ means that the set of $u$'s such that $F(u)$ holds contains an open set (or equivalently contains an open dense set). It is known (and not difficult to prove) that this new quantifier can be eliminated. Therefore sets defined by first-order formulas in this extended language are ordinary quasi-algebraic sets. As ordinary quantifiers, $\exists^*$ is commutative, i.e.,

$$\exists^* u \exists^* v\, F(u,v) \;\equiv\; \exists^* v \exists^* u\, F(u,v) \;\equiv\; \exists^*(u,v)\, F(u,v).$$

One could also define a $\forall^*$ quantifier as:

$$\forall^* u\; F(u) \;\equiv\; \neg \exists^* u\, \neg F(u)$$

but this would be redundant since this double negation is equivalent to $\exists^* u\, F(u)$. (Note however that over the reals, one can similarly define two distinct quantifiers $\exists^*$ and $\forall^*$.)

Another important remark is that if (and only if) $\exists^* u\; F(u)$ holds, $F(u)$ holds for any $u \in \mathbb{C}^k$ of transcendence degree $k$ over the parameters of $F$.

**Theorem 5.1** *Let $F(u,v)$ be a first-order formula where $u \in \mathbb{C}^p$ and $v \in \mathbb{C}^k$. The set $W(F)$ of sequences $(v_1, \ldots, v_{2p+1}) \in \mathbb{C}^{k(2p+1)}$ satisfying:*

$$\forall u\; [\exists^* v F(u,v) \Leftrightarrow |\{i;\; F(u,v_i)\}| \geq p+1] \qquad (6)$$

*is dense in $\mathbb{C}^{k(2p+1)}$.*

This means that to decide whether $F(u,v)$ holds for "most" $v$'s, one just has to check whether it holds for a majority of $v_1, \ldots, v_{2p+1}$. Moreover, the same $2p+1$ test points can be used for any choice of $u$ and "most" tuples of $2p+1$ points are good for that purpose.

The proof given below relies on transcendence degree arguments, and was suggested by Bruno Poizat (personal communication). In model theory there is abstract version of arguments of this kind, see e.g. [22] (a sequence of algebraically independent complex numbers is an example of an "indiscernible" sequence). It is also possible to use the dimension of definable sets. These two proofs are essentially equivalent, but the first one is much more concise.

*Proof of Theorem 5.1.* Let $K$ be the field extension of $\mathbb{Q}$ generated by the parameters of $F$. We will show that if the components of $w \in \mathbb{C}^{k(2p+1)}$ are algebraically independent over $K$, then $w \in W(F)$ (this will prove the theorem since $\mathbb{C}$ has infinite transcendence degree). Let $w = (v_1, \ldots, v_{2p+1})$ be such a sequence, and fix any $u \in \mathbb{C}^p$.

Assume for instance that $\exists^* v F(u,v)$ holds: we need to show that $|\{i;\; F(u,v_i)\}| \geq p+1$. Let $K'$ be the field extension of $K$ generated by the components of $u$. As pointed out before Theorem 5.1, $F(u,v_i)$ holds if the components of $v_i$ are algebraically independent over $K'$. Hence we just have to show that there are at least $p+1$ such $v_i$'s. Let $K''$ be the field extension of $K'$ generated by the components of $w$: $\mathrm{tr.deg}_{K'} K'' \geq k(2p+1) - p$ since $\mathrm{tr.deg}_K K'' = \mathrm{tr.deg}_{K'} K'' + \mathrm{tr.deg}_K K'$ (this is e.g. the corollary of Theorem 4 in section V.14.3 of [6]), $\mathrm{tr.deg}_K K' \leq p$ and $\mathrm{tr.deg}_K K'' \geq k(2p+1)$ by definition of $w$. Let $B$ be a transcendence base of $K''$ over $K$ made up of components of $w$. $B$ has at least $k(2p+1)-p$ elements, and can therefore omit some components of at most $p$ $v_i$'s. The other $p+1$ $v_i$'s have all their components in $B$, and are therefore algebraically independent over $K'$ as needed.

If $\exists^* v F(u,v)$ does not hold then $\exists^* v \neg F(u,v)$ holds and applying the argument above to $\neg F$ shows that $|\{i;\; \neg F(u,v_i)\}| \geq p+1$. $\square$

The example $F(u,v) \equiv [(v-u_1)(v-u_2)\ldots(v-u_p) \neq 0]$ shows that $2p+1$ cannot be replaced by $2p$ in this theorem. However, for certain formulas one can get away with fewer test points in the following sense.

**Theorem 5.2** *Let $F(u,v)$ be a first-order formula such that for any $u \in \mathbb{C}^p$, if $\exists^* v F(u,v)$ does not hold then $F(u,v)$ does not hold for any $v \in \mathbb{C}^k$. The set $G'(F)$ of sequences $(v_1, \ldots, v_{p+1}) \in \mathbb{C}^{k(p+1)}$ satisfying:*

$$\forall u \ [\exists^* v F(u,v) \Leftrightarrow |\{i;\ F(u,v_i)\}| \geq 1] \qquad (7)$$

*is dense in $\mathbb{C}^{k(p+1)}$.*

*Proof.* Let $K$ be as in the proof of Theorem 5.1. We claim that if the components of $w \in \mathbb{C}^{k(p+1)}$ are algebraically independent over $K$, then $w \in G'(F)$. Indeed, one can show as in Theorem 5.1 that for such a $w$ and any $u \in \mathbb{C}^k$, there must exist at least one $v_i$ with components that are algebraically independent over $K(u_1, \ldots, u_k)$. Then $\exists^* v F(u,v)$ implies $F(u, v_i)$. Conversely, if $F(u,v_i)$ holds for some $i$ then by the hypothesis on $F$, $\exists^* v F(u,v)$ must hold as well. $\square$

The hypothesis in this theorem is satisfied in particular by formulas of the form $F(u,v) \equiv [P(u,v) \neq 0]$, where $P$ is a polynomial. Such formulas have been considered in the study of "correct test sequences" [13] and in the Witness Theorem [2]. The same example shows that the $p+1$ bound cannot be improved in general (there is a similar remark in [13]).

We will see in Theorem 5.6 that it is possible to construct explicitly a sequence in $W(F)$. Before that, we show that $W(F)$ contains a sequence of points with "small" integer coordinates. The proof relies only on a connected component argument. First, note that $W(F)$ is an equivalence class of the equivalence relation $\sim$ on $\mathbb{C}^{k(2p+1)}$ defined by: $v \sim w$ iff

$$\forall u \in \mathbb{C}^p \quad \begin{array}{l} [|\{i;\ F(u,v_i)\}| \geq p+1 \Leftrightarrow \\ |\{i;\ F(u,w_i)\}| \geq p+1]. \end{array} \qquad (8)$$

**Theorem 5.3** *Let $F(u,v)$ be a quantifier-free formula involving $s$ polynomials of degree at most $D$ (with $u \in \mathbb{C}^p$ and $v \in \mathbb{C}^k$). There exists a sequence in $W(F)$ with integer coordinates bounded by $k(2p+1)(2sD+1)(4sD+1)^{2p+2}(8sD+1)^{2p+1}$.*

*Proof.* Since $W(F)$ is dense in $\mathbb{C}^{k(2p+1)}$ (by Theorem 5.1), $R(F) = W(F) \cap \mathbb{R}^{k(2p+1)}$ is dense in $\mathbb{R}^{k(2p+1)}$. As in the proof of Theorem 3.9, we need an upper bound on $\kappa(R(F))$. Fix a sequence $w \in R(F)$. Then $v \in \mathbb{R}^{k(2p+1)}$ is in $R(F)$ if it satisfies the following formula of the first-order theory of the reals:

$$\forall u \in \mathbb{R}^{2p} \quad \begin{array}{l} [|\{i;\ \hat{F}(u,v_i)\}| \geq p+1 \ \Leftrightarrow \\ |\{i;\ \hat{F}(u,w_i)\}| \geq p+1]. \end{array}$$

Formula $\hat{F}$ is obtained from $F$ by separating real and imaginary parts; it involves at most $2s$ atomic predicates of degree at most $D$.

We want to bound $B_0(R(F) \cap \Delta)$, where $\Delta$ is an axis-parallel line. Let $R'(F)$ be the complement of $R(F)$ in $\mathbb{R}^{k(2p+1)}$: $B_0(R(F) \cap \Delta) \leq 1 + B_0(R'(F) \cap \Delta)$. $R'(F) \cap \Delta$ is the projection of a semi-algebraic set $E \subseteq \mathbb{R}^{2p+k(2p+1)}$ defined by

$$\begin{array}{l} \neg[|\{i;\ \hat{F}(u,v_i)\}| \geq p+1 \Leftrightarrow \\ |\{i;\ \hat{F}(u,w_i)\}| \geq p+1] \end{array} \qquad (9)$$

where all the components $v_{ij}$ of the $v_i$'s except one (depending on the direction of $\Delta$) are constant. Since projections do not increase $B_0$, $B_0(R'(F) \cap \Delta) \leq B_0(E)$. Moreover, $B_0(E) = B_0(E')$ where $E' \subset \mathbb{R}^{2p+1}$; a formula defining $E'$ can be obtained from (9) by replacing the constant $v_{ij}$'s by their values. Hence $B_0(E') \leq (2sD+1)(4sD+1)^{2p+2}(8sD+1)^{2p+1}$ by Corollary 3.5, and this is also an upper bound on $\kappa(R(F))$. It follows from Theorem 3.7 that $\mu_h(R(F)) > 0$ if $h > k(2p+1)\kappa(R(F))$. This implies the existence of a point in $R(F)$ with integer coordinates bounded by $k(2p+1)\kappa(R(F))$. $\square$

**Lemma 5.4** *Let $H(w)$ be a quantifier-free first-order formula where $w \in \mathbb{C}^n$. Assume that the polynomials in $H$ are of degree at most $D$, with integer coefficients bounded by $M$ in absolute value. Let $(\alpha_1, \ldots, \alpha_n)$ be any sequence of integers satisfying $\alpha_1 \geq M+1$ and $\alpha_j \geq 1 + M(D+1)^{j-1}\alpha_{j-1}^D$ for $j \geq 2$. Then $H(\alpha_1, \ldots, \alpha_n)$ holds if and only if $\exists^* w H(w)$ holds.*

*Proof.* We only need to prove the "if" part since the converse will follow if $H$ is replaced by $\neg H$. Let us thus assume that $\exists^* w H(w)$ holds. The subset of $\mathbb{C}^n$ defined by $H$ is a finite union of basic quasi-algebraic sets (obtained by putting $H$ in disjunctive normal form), and one of them must be dense. Such a set $S$ is of the form $P_1(w) \neq 0, \ldots, P_m(w) \neq 0$ where the $P_i$'s are non-zero polynomials of degree at most $D$, with integer coefficients bounded by $M$ in absolute value. Then the $\alpha$ defined in the statement of the theorem satisfies $P_i(\alpha) \neq 0$ for any $i = 1, \ldots, m$ (this is not hard to prove, see e.g. [15]). This implies $\alpha \in S$, hence $H(\alpha)$ holds. $\square$

Note that the sequence in this lemma can be constructed in $O(\log\log M + n \log D)$ arithmetic operations (starting from the integer 1).

**Lemma 5.5** *Let $F(u,v)$ be a quantifier-free formula where $u \in \mathbb{C}^p$ and $v \in \mathbb{C}^k$, with integer coefficients of bit size at most $L$. Let $\Sigma$ be its total degree. One* *can construct in* $\log L + (kp \log \Sigma)^{O(1)}$ *arithmetic operations a sequence* $(v_1, \ldots, v_{2p+1}) \in W(F)$ *with integer coordinates. Moreover, this sequence depends only on* $L$, $k$, $p$ *and* $\Sigma$.

*Proof.* $W(F)$ is defined by (8), where $w$ is any fixed point in $W(F)$. The total number of variables in this formula is $p + k(2p+1)$, its total degree is upper bounded by $2(2p+1)\Sigma$, and it has a single block of quantifiers. In order to have a good bound on the size of its coefficients, let us use the point $w \in W(F)$ given by Theorem 5.3. The result then follows from Lemma 5.4, after eliminating quantifiers in (8) by Theorem 1.2. □

A generalization to quantified formulas follows easily.

**Theorem 5.6** *Let* $F(u, v)$ *be a prenex formula with* $r$ *blocks of quantifiers, and integer coefficients of bit size at most* $L$. *Let* $\Sigma$ *be its total degree, and* $m$ *the total number of variables (thus if* $u \in \mathbb{C}^p$ *and* $v \in \mathbb{C}^k$, *there are* $m-p-k$ *quantified variables). One can construct in* $\log L + (m \log \Sigma)^{O(r)}$ *arithmetic operations a sequence* $(v_1, \ldots, v_{2p+1}) \in W(F)$ *with integer coordinates. Moreover, this sequence depends only on* $L$, $m$, $r$ *and* $\Sigma$.

*Proof.* Eliminate quantifiers in $F$ with Theorem 1.2 and then apply Lemma 5.5. □

**Theorem 5.7** $\mathrm{DIM}_{\mathbb{C}}$ *is* $\mathrm{NP}_{\mathbb{C}}$*-complete.*

*Proof.* Let us start for instance from the algorithm of section 4.2: a variety $V$ has dimension at least $d$ if its intersection with a generic affine subspace $H$ of dimension $n-d$ is nonempty. We want to derandomize it using Theorem 5.6. For this we consider a formula $F(u, v)$ where $u \in \mathbb{C}^p$ stands for the coefficients of (1) and $v$ stands for the coefficients of the $d$ equations defining $H$. The formula is satisfied if $H \cap V \neq \emptyset$. By Theorem 5.6 we can construct deterministically $2p+1$ affine subspaces $H_1, \ldots, H_{2p+1}$ such that $\dim V \geq d$ iff a majority of the $H_i$'s have a nonempty intersection with $V$. Therefore a polynomial-size certificate that $\dim V \geq d$ consists of a list of $p+1$ indices $i_1, \ldots, i_{p+1}$ and points $x_1, \ldots, x_{p+1} \in \mathbb{C}^n$ such that $x_j \in V \cap H_{i_j}$ for $j = 1, \ldots, p+1$. □

It seems that this NP-completeness proof can be adapted to the real case. The derandomization argument fails in positive characteristic, but it should be possible to obtain a completeness result for non-uniform reductions (see [15] for similar results).

$\mathrm{HN}_{\mathbb{C}}$ can be solved in sequential time $s^{O(1)} D^{O(n)}$ by a uniform algorithm[2] in the sense of [3]. The proof of Theorem 5.7 implies the same bound for $\mathrm{DIM}_{\mathbb{C}}$ (just solve the $2p+1$ systems independently and take a majority vote). Of course, if we are willing to use a randomized algorithm this bound follows from section 4.

For systems with integer coefficients, the reduction to HN can also be performed in polynomial time in the standard (Turing machine) model of computation.

**Theorem 5.8** DIM *is polynomial-time many-one reducible to* HN.

*Proof.* In this case we have to construct only a single affine subspace $H$ (apply Theorem 5.6 with $p = 0$). The coefficients of the equations defining $H$ cannot be computed explicitly since they have exponential binary length. However they can be *represented* by introducing new variables, in the spirit of section 1.2. □

Conversely, we have seen in the proof of Proposition 1.1 that HN is reducible to DIM. These two problems are therefore polynomially equivalent. The same remark applies to $\mathrm{HN}_{\mathbb{C}}$ and $\mathrm{DIM}_{\mathbb{C}}$.

## Acknowledgements

Thanks are due to Christian Michaux for discussions on the representation of algebraic equations, and to Bruno Poizat for his proof of Theorem 5.1.

## References

[1] R. Benedetti and J.-J. Risler. *Real algebraic and semi-algebraic sets.* Hermann, Paris, 1990.

[2] L. Blum, F. Cucker, M. Shub, and S. Smale. Algebraic settings for the problem "P≠NP?". In J. Renegar, M. Shub, and S. Smale, editors, *The Mathematics of Numerical Analysis*, volume 32 of *Lectures in Applied Mathematics*, pages 125–144. American Mathematical Society, 1996.

[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.

[2] I have not been able to find an appropriate reference in the litterature. As mentioned in the introduction, Chistov's algorithm is not algebraic. There are *randomized* algebraic algorithms for $\mathrm{HN}_{\mathbb{C}}$ [17] and $\mathrm{DIM}_{\mathbb{C}}$ [12]. It should be possible to derandomize these algorithms using Theorem 5.6.

[4] J. Bochnak, M. Coste, and M.-F. Roy. *Géométrie Algébrique Réelle*. Springer-Verlag, 1987.

[5] A. Borodin. On relating time and space to size and depth. *SIAM Journal on Computing*, 6:733–744, 1977.

[6] N. Bourbaki. *Algèbre (Chapitres 4 à 7)*. Masson, Paris, 1981.

[7] L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. In *Proc. 6th Intern. Conf. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, LNCS 357, pages 131–151. Springer, 1989.

[8] A. Chistov. Polynomial-time computation of the dimension of algebraic varieties in zero-characteristic. *Journal of Symbolic Computation*, 22:1–25, 1996.

[9] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer, 1992.

[10] N. Fichtas, A. Galligo, and J. Morgenstern. Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields. *Journal of Pure and Applied Algebra*, 67:1–14, 1990.

[11] 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.

[12] 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.

[13] J. Heintz and C.-P. Schnorr. Testing polynomials which are easy to compute. In *Logic and Algorithmic (an International Symposium held in honour of Ernst Specker)*, pages 237–254. Monographie $n^o$ 30 de L'Enseignement Mathématique, 1982. Preliminary version in *Proc. 12th ACM Symposium on Theory of Computing*, pages 262-272, 1980.

[14] P. Koiran. Approximating the volume of definable sets. In *Proc. 36th IEEE Symposium on Foundations of Computer Science*, pages 134–141, 1995.

[15] P. Koiran. Elimination of constants from machines over algebraically closed fields. Technical Report 96-24, DIMACS (http://dimacs.rutgers.edu/), 1996. To appear in *J. Complexity*.

[16] 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://dimacs.rutgers.edu/).

[17] T. Krick and L. M. Pardo. A computational method for Diophantine approximation. In L. Gonzalez-Vega and T Recio, editors, *Algorithms in Algebraic Geometry and Applications (Proc. MEGA'94)*, Progress in Mathematics 143. Birkhauser, 1996. Preliminary version: Une Approche Informatique pour l'Approximation Diophantienne. *Compte-Rendus de l'Académie des Sciences*, Série I, 318(5):407-412, 1994.

[18] A. Logar. A computational proof of the Noether normalisation lemma. In *Proc. 6th Intern. Conf. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, LNCS 357, pages 260–273. Springer, 1989.

[19] G. Matera and J. Torres. The space complexity of elimination theory: Upper bounds. In F. Cucker and M. Shub, editors, *Foundations of Computational Mathematics (Selected Papers of a Conference Held at IMPA in Rio de Janeiro)*, pages 267–276, 1997.

[20] F. Meyer auf der Heide. Simulating probabilistic by deterministic algebraic computation trees. *Theoretical Computer Science*, 41:325–330, 1985.

[21] D. Mumford. *Algebraic Geometry I: Complex Projective Varieties*. Springer, 1976.

[22] B. Poizat. Théories instables. *Journal of Symbolic Logic*, 46:513–522, 1981.

[23] J. T. Schwarz. Fast probabilistic algorithms for verification of polynomials identities. *Journal of the ACM*, 27:701–717, 1980.

[24] H. Warren. Lower bounds for approximation by nonlinear manifolds. *Transactions of the AMS*, 133:167–178, 1968.

[25] S. Zachos. Probabilistic quantifiers, adversaries, and complexity classes: an overview. In *Proc. 1st Structure in Complexity Theory Conference*, volume 223 of *Lecture Notes in Computer Science*. Springer-Verlag, 1986.