Computing the Dimension of a Polynomial Ideal

Anna Bernasconi, Ernst W. Mayr, Michal Mnuk and Martin Raab
Institut für Informatik
Technische Universität München
80290 Munich, Germany

January 9, 2002

Abstract

Following ideas from [Hei83, DFGS91, MT97] and applying the techniques proposed in [May89, KM96, Küh98], we present a deterministic algorithm for computing the dimension of a polynomial ideal requiring polynomial working space.

1 Introduction

The problem of computing the dimension of an ideal has been investigated in a number of papers, see for instance [KW88, DFGS91, MT97, Koi97, Küh98]. In particular, in [MT97] a deterministic algorithm for computing the dimension of a polynomial ideal requiring polynomial working space is presented. This algorithm is based on ideas from [DFGS91] which in turn relies on results from [Hei83]. In this paper we review these results with the aim of providing a concise self-contained exposition of this topic.

The structure of the presented algorithm is as follows: First we show how to test in polynomial space whether a subset of indeterminates is independent modulo an ideal. Then, using this test as a subroutine, we will compute the dimension of the ideal by enumerating all subsets of indeterminates and testing their independence.

The method of testing whether a subset of indeterminates is independent turns upon the fact that the corresponding elimination ideal either contains only the zero polynomial (if the subset of indeterminates is independent) or it contains at least one nonzero polynomial of total degree which is single exponential in the number of indeterminates, as noticed in [DFGS91]. (The notions of independence modulo an ideal, ideal dimension and elimination ideals are made precise in Section 2.)

Following techniques from [May89, KM96, Küh98], this single exponential degree bound can then be exploited for reducing the problem of deciding whether some indeterminates are independent to the problem of deciding whether a certain homogeneous linear system (of exponential size) has a non trivial solution. The latter is known to be solvable by a parallel algorithm using polynomial number of processors and running in time polylogarithmic in the size of the system. The Parallel Computation Thesis [FW78] then implies the existence of a sequential algorithm which uses space polylogarithmic in the size of the input (thus polynomial space for the system under study).

2 Notations and Some Fundamental Concepts

2.1 Polynomials and Ideals

Let $X = \{x_1, \ldots, x_n\}$ be a finite set of indeterminates. By $k[X]$ we denote the (commutative) ring of polynomials in $x_1, \ldots, x_n$ with coefficients in the field k.

For polynomials $f_1, \ldots, f_s \in k[X]$, let $(f_1, \ldots, f_s) \subseteq k[X]$ denote the *ideal generated by* $\{f_1, \ldots, f_s\}$, i.e.,

$$(f_1, \ldots, f_s) = \{ \sum_{1 \leq i \leq s} p_i f_i \; ; \; p_i \in k[X]\}.$$

If $I = (f_1, \ldots, f_s)$, the set $\{f_1, \ldots, f_s\}$ is called a *basis* of I.

Given an ideal I, we denote with $V(I)$ the *variety* defined by I in the n-dimensional affine space $\mathbb{A}^n$ over the algebraic closure $\overline{k}$ of the field k:

$$V(I) = \{(a_1, \ldots, a_n) \in \overline{k}^{\,n} \; ; \; f(a_1, \ldots, a_n) = 0 \; \text{ for all } f \in I\} \, .$$

Finally, given a subset X of the affine space $\mathbb{A}^n$, we denote with $\overline{X}$ its *Zariski closure*, i.e., the smallest variety containing it.

Remark 2.1. *Let $I = (f_1, \ldots, f_s) \subset k[X]$. By definition, a polynomial g belongs to I if and only if we can write*

$$g = \sum_{i=1}^{s} g_i f_i, \tag{1}$$

for some polynomials g_i. If the degrees of the g_i are fixed and we consider the coefficients of the g_i's as unknowns, we get a system of linear equations in these unknowns. Thus the solvability of (1) in some field extension of k (e.g., in its closure) implies solvability in the ground field k within the same degree bound for the g_i.

2.2 Elimination Ideals

Definition 2.1 (Elimination ideal).
Let $I \subseteq k[X]$ be an ideal and let $Y \subseteq X$ a subset of indeterminates. Then $I \cap k[Y]$, which is an ideal in $k[Y]$, is called an elimination ideal *of I.*

An elimination ideal with respect to some subset of the indeterminates corresponds to the projection of its variety into the coordinate subspace corresponding to this subset of the indeterminates:

Theorem 1 (Closure Theorem).
Let I be an ideal in the polynomial ring $k[X]$, $Y = \{x_{i_1}, \ldots, x_{i_\ell}\}$ a subset of the indeterminates $\{x_1, \ldots, x_n\}$, and let $\pi_Y(V(I))$ denote the projection of the variety $V(I)$ into the coordinate subspace corresponding to Y. Then the Zariski closure of $\pi_Y(V(I))$ is equal to the variety defined by the elimination ideal $I \cap k[Y]$ in the ℓ-dimensional affine space $\mathbb{A}^\ell$ over $\overline{k}$:

$$\overline{\pi_Y(V(I))} = V(I \cap k[Y]) \,.$$

Proof. See e.g. Chapters 3 and 4 of [CLO92]. ☐

2.3 The Dimension of an Ideal

Definition 2.2 (Independent set of indeterminates).
For any polynomial ideal $I \subseteq k[X]$, a subset $Y \subseteq X$ of indeterminates is called independent modulo I *if $I \cap k[Y] = (0)$. Otherwise, Y is called* dependent modulo I.

Definition 2.3 (Dimension of a polynomial ideal). *Let I be a polynomial ideal in $k[X]$. The* affine dimension *of I in $k[X]$, denoted by* $\dim(I)$, *is defined to be the cardinality of a largest subset of X which is independent modulo I. If there is no independent subset at all (which only happens for $I = k[X]$), then the affine dimension of I is defined to be -1.*

2.4 The Noether Normalization Lemma

Definition 2.4 (Integral indeterminates).
Let I be a polynomial ideal in $k[X]$ and $Y \subseteq X$. An indeterminate x_j is called integral *over $k[Y]$* mod I *if there exists a polynomial*

$$p \in I \cap k[Y, x_j] \setminus (0)$$

monic *in x_j, i.e. such that* $\deg_{x_j}(p) = \deg(p) > 0$.

Definition 2.5 (Noether normal position).
Let I be a polynomial ideal in $k[X]$ and let $r = \dim(I)$. We say that I is in Noether normal position *if the following conditions hold:*

(a) $x_1, x_2, \ldots, x_r$ *are independent modulo I,*

(b) $x_{r+1}, \ldots, x_n$ *are integral over $k[x_1, \ldots, x_r]$* mod I.

Lemma 2.1 (Noether Normalization Lemma).
An ideal I in a polynomial ring $k[X]$ over an infinite field k can be transformed by a suitable linear change of coordinates

$$x_i' = \sum_{j=1}^{n} a_{ij} x_j \,, \qquad 1 \le i \le n \,, \qquad a_{ij} \in k$$

in such a way that I is in Noether normal position with respect to the new indeterminates $x'_1, \ldots, x'_n$.

Geometrically, this theorem assures the existence of a finite map φ of $V(I)$ onto $\mathbb{A}^r$ (i.e. a map where $\varphi^{-1}(x)$ is finite for every $x \in \Im\varphi$).

2.5 Degree of a Variety

Definition 2.6 (Degree of an Irreducible Variety).
Let V be an irreducible subvariety of $\mathbb{A}^n$ with $\dim V = r$. *The* degree *of V is defined as the maximal cardinality of a finite set which is obtained by intersecting V with a linear affine subspace of dimension $n - r$:*

$$\deg V = \sup\{\, |E \cap V| \quad ; \quad E \text{ an } (n-r) \text{ dimensional affine subspace of } \mathbb{A}^n \text{ such that } E \cap V \text{ is finite}\}\,.$$

The notion of degree can be extended to reducible varieties as follows:

Definition 2.7 (Degree of a Reducible Variety).
Let V be a variety of $\mathbb{A}^n$ and $\mathcal{C}$ the set of its irreducible components. Then

$$\deg V = \sum_{C \in \mathcal{C}} \deg C\,.$$

It can be verified that $\deg \mathbb{A}^n = 1$, and that the degree of any hypersurface of $\mathbb{A}^n$ equals the total degree of its defining polynomial.

This notion of degree satisfies the following inequality (see [Hei83] for more details):

Theorem 2 (Bézout's Inequality).
Let $V, W \subset \mathbb{A}^n$ be two algebraic varieties. Then

$$\deg(V \cap W) \leq \deg V \cdot \deg W\,.$$

Proposition 1 (Upper Degree Bound).
Let $f_1, f_2, \ldots, f_s$ be polynomials in $k[X]$, let d be the maximal degree of the f_i's and let I be the ideal generated by $f_1, \ldots, f_s$. Then the degree of the affine variety defined by I is bounded by d^μ, where $\mu = \min\{s, n\}$.

Proof. If $s \leq n$, then $\deg V(I) \leq d^s$ as a consequence of the Bézout's inequality:

$$\begin{aligned} \deg V(I) &= \deg\ V(f_1) \cap V(f_2) \cap \ldots \cap V(f_s) \\ &\leq \prod_{i=1}^{s} \deg V(f_i) = \prod_{i=1}^{s} \deg(f_i) \leq d^s\,. \end{aligned}$$

Otherwise, if $s > n$, we can consider the ideal J generated by n generic linear combinations of the polynomials $f_1, \ldots, f_s$. Since $V(J)$ contains all irreducible components of $V(I)$, and possibly some new extraneous ones, it follows that

$$\deg V(I) \leq \deg V(J) \leq d^n\,.$$

□

In the remaining part of this section we prove that the degree of the image of an affine variety under a linear mapping cannot exceed the degree of the variety itself.

We denote by $\mathbb{P}^n$ the *projective space* of dimension n.

Lemma 2.2.
Let $\varphi : \mathbb{P}^n \to \mathbb{P}^m$ be a linear map and $V \subseteq \mathbb{P}^n$ a closed set. Then

$$\deg \varphi(V) \leq \deg V.$$

Proof. Let F be a linear subspace of $\mathbb{P}^m$ given by linear homogeneous polynomials $l_1, \ldots, l_s$ such that $|\varphi(V) \cap F| = \deg \varphi(V)$. We set $E := \varphi^{-1}(F)$ and distinguish two cases depending on whether the intersection $W := V \cap E$ is finite or not:

Case 1. If W is finite, then it is clear from definition that $\deg V$ is not smaller than $|W| = \deg \varphi(V)$.

Case 2. If W is infinite, i.e. $\dim W \geq 1$, then we can find a hyperplane E' in $\mathbb{P}^n$ defined by one linear homogeneous polynomial l' which does not contain W. Then

$$\varphi(\varphi^{-1}(F) \cap E') = \varphi(V) \cap F \text{ and } \dim(V \cap E') = \dim V - 1.$$

Hence we may replace V by $V \cap E'$ in the assertion of the lemma. Continuing this argument we finally arrive at Case 1.

□

Corollary 2.1. *Let $V \subseteq \mathbb{A}^n$ be a closed set and $\varphi : \mathbb{A}^n \to \mathbb{A}^m$ a linear map. Then*

$$\deg \overline{\varphi(V)} \leq \deg V.$$

Proof. Let W be the closure of V in $\mathbb{P}^n$. We consider $\mathbb{A}^n$ and $\mathbb{A}^m$ as open subspaces of $\mathbb{P}^n$ and $\mathbb{P}^m$, resp., and extend φ to a mapping $\psi : \mathbb{P}^n \to \mathbb{P}^m$ such that $\psi|_{\mathbb{A}^n} = \varphi$. Then

$$\deg \overline{\varphi(V)} = \deg \psi(W) \cap \mathbb{A}^m \leq \deg \psi(W) \leq \deg W = \deg V,$$

where $\deg W$ and $\deg \psi(W)$ are computed in $\mathbb{P}^n$ and $\mathbb{P}^m$, resp. Since $\dim W = \dim V$, the last equality follows from the fact that for any finite set there is a projective change of coordinates of $\mathbb{P}^n$ such that no point of the set lies on the line at infinity. □

3 Degree Bound for Polynomials in an Elimination Ideal

We will make use of the following result.

Theorem 3 (Brownawell's Upper Degree Bound).
Let $f, f_1, \ldots, f_s \in k[X]$ have degrees at most D, let $\mu = \min\{s, n\}$, and assume that f vanishes on all the common zeros of $f_1, \ldots, f_s$ (in the algebraic closure of k). Then one can find s polynomials $p_1, \ldots, p_s \in k[X]$ and a positive integer e satisfying

$$f^e = \sum_{i=1}^{s} p_i f_i ,$$

with

$$\begin{aligned} &e \leq (\mu+1)(n+2)(D+1)^{\mu+1} , \\ &\deg(p_i f_i) \leq (\mu+1)(n+2)(D+1)^{\mu+2} . \end{aligned}$$

This degree bound can be improved if $\deg(f_i) \geq 3$ (for all $1 \leq i \leq s$) as follows:

$$\begin{aligned} &e \leq d^{\mu} , \\ &\deg(p_i f_i) \leq d^{\mu} (\deg(f) + 1) , \end{aligned}$$

where d denotes the maximal degree of the generators $f_1, \ldots, f_s$.

For proofs of these and similar exponential degree bounds, see [Bro87], [Kol88], and [BY90].

Following ideas from [Hei83] and [DFGS91], we now provide a single exponential bound for the degree of a polynomial in an elimination ideal.

Theorem 4 (Main).
Given an ideal $I = (f_1, \ldots, f_s)$ in the polynomial ring $k[X]$ over an infinite field k, $X = \{x_1, \ldots, x_n\}$. Let d be the maximal degree of generators f_i and let $Y = \{x_{i_1}, \ldots, x_{i_\ell}\} \subseteq X$ be a subset of indeterminates. If the set Y is dependent modulo I, then there exists a non zero polynomial $g \in I \cap k[Y]$, $g \neq 0$, such that

$$g = \sum_{i=1}^{s} g_i f_i \tag{2}$$

with $g_i \in k[X]$ and

$$\deg(g_i f_i) \leq (\mu+1)(n+2)(d^{\mu}+1)^{\mu+2} , \tag{3}$$

where $\mu = \min\{s, n\}$.

Proof: Let $V(I)$ be the variety defined by I in the n-dimensional affine space $\mathbb{A}^n$ over $\overline{k}$, and let $\pi_Y(V(I))$ denote its projection into the coordinate subspace corresponding to the set of indeterminates Y. From Theorem 1 it follows that the Zariski closure of the set $\pi_Y(V(I))$ is equal to the variety defined by the elimination ideal $I \cap k[Y]$, i.e.,

$$\overline{\pi_Y(V(I))} = V(I \cap k[Y]) .$$

Since Y is dependent modulo I, $I \cap k[Y] \neq (0)$, and this implies that $V(I \cap k[Y]) \neq \mathbb{A}^{\varrho}$, where $\varrho = |Y|$.

Let $r = \dim I \cap k[Y]$, $r \leq \dim I$. From the Noether Normalization Lemma (see Lemma 2.1) it follows that there exists a linear map $\varphi \equiv (\varphi_1, \ldots, \varphi_\varrho)$,

$$\varphi : \mathbb{A}^{\varrho} \to \mathbb{A}^{\varrho} ,$$

such that the ideal $I \cap k[Y]$ is in Noether normal position with respect to the new indeterminates $y_1, \ldots, y_\varrho$ given by

$$y_j = \varphi_j(x_{i_1}, \ldots, x_{i_\varrho}) = \sum_{q=1}^{\varrho} a_{jq}\, x_{i_q}, \quad a_{jq} \in k, \quad j = 1, \ldots, \varrho .$$

Precisely, we have:

1. $y_1, y_2, \ldots, y_r$ are independent modulo $I \cap k[Y]$,
2. $y_{r+1}, \ldots, y_\varrho$ are integral over $k[y_1, \ldots, y_r]$ mod I.

Let W denote the Zariski closure of the image of the variety $V(I \cap k[Y])$ under the map φ, i.e.,

$$W = \overline{\varphi(V(I \cap k[Y]))} ,$$

and consider the projection $\pi(W)$ of W into the coordinate subspace corresponding to the first $r+1$ indeterminates $y_1, \ldots, y_{r+1}$. From the fact that the indeterminates $y_1, \ldots, y_r$ are independent and y_{r+1} is integral over $k[y_1, \ldots, y_r]$ mod I it follows that

$$\dim \overline{\pi(W)} = r .$$

Thus, since $\overline{\pi(W)} \subseteq \mathbb{A}^{r+1}$, it must be a hypersurface in $\mathbb{A}^{r+1}$.

Let $h \in \overline{k}[y_1, \ldots, y_{r+1}]$ be the defining polynomial of $\overline{\pi(W)}$. Proposition 1 and Corollary 2.1 imply

$$\deg h = \deg \overline{\pi(W)} = \deg \overline{\pi(\varphi(\pi_Y(V(I))))} \leq \deg V(I) \leq d^{\mu} .$$

We now consider the polynomial $f \in \overline{k}[Y]$ defined as

$$f = h \circ \pi \circ \varphi .$$

Since π and φ are linear, $\deg f = \deg h$. Moreover, f vanishes on $V(I \cap k[Y])$ and, if considered as an element of $\overline{k}[X]$, it vanishes on $V(I)$. In fact, we may regard f being defined over a simple algebraic extension $k(\alpha)$ of k generated by its coefficients. Then

$$f = \sum_{i=0}^{l} \alpha^i f^{(i)},$$

where $f^{(i)}$'s are polynomials in $k[X]$. If f vanishes at some $x \in k$, then all $f^{(i)}$'s must vanish there too, and vice versa. Thus w.l.o.g. we may assume the coefficients of f to lie in k.

Applying Theorem 3 we can conclude that Equation (2) has a polynomial solution in $\overline{k}[X]$ the overall degree of which is bouded by (3). The solvability in $k[X]$ within the same degree bounds follows from Remark 2.1.

Remark 3.1. *An example shows that the upper bound proved in the theorem is rather tight. Möller and Mora ([MM84]) constructed an example showing that the lower bound for the degree of polynomials in an elimination ideal is single exponential. We recall here a non-homogeneous version of this example.*

Let I be the ideal in the polynomial ring $\mathbb{Q}[X]$ generated by polynomials:

$$\begin{aligned} f_1 &= x_n^d , \\ f_i &= x_i - x_{i-1}^d , \qquad i = 2, \ldots, n . \end{aligned}$$

Then

$$I \cap \mathbb{Q}[x_1] = (x_1^{d^n}) .$$

4 Computing the Dimension in Polynomial Space

In what follows we assume that we are considering ideals in the polynomial ring $\mathbb{Q}[X]$. By exploiting the exponential degree bound of Theorem 4 we shall now develop an algorithm that computes the dimension of an ideal $I = (f_1, \ldots, f_s) \subseteq \mathbb{Q}[X]$ using work space bounded by a polynomially growing function in the size of the problem instance. By the *size* we mean the number of bits used for writing down the problem specification – that is the s generators of the ideal I, and, in the test for independence, a subset Y of indeterminates. A polynomial is written down in the sparse representation using distinct characters for the indeterminates, arabic base ten notation for exponents and coefficients. The input polynomials are separated by some delimiter of unit size.

By the work space required by an algorithm we mean the maximal number of bits used for keeping any data, like intermediate results, during the execution of the algorithm. Here we count only those data that the algorithm will read again at some later time; in particular any part of the final result that is output and no longer needed for performing the remainder of the computation is not regarded to require work space.

4.1 Reducing the Independence Test to a Homogeneous Linear System

We first consider the problem of testing whether a given subset of indeterminates $Y \subseteq \{x_1, \ldots, x_n\}$ is independent modulo I.

From Theorem 4 it follows that we can reduce the problem of deciding whether $I \cap \mathbb{Q}[Y] \neq (0)$ to the problem of deciding whether the homogeneous linear system

$$g - \sum_{i=1}^{s} g_i f_i = 0 \tag{4}$$

has a non trivial solution, for $g \in \mathbb{Q}[Y]$, $g_i \in \mathbb{Q}[X]$, and

$$\deg(g_i f_i) \le (\mu + 1)(n + 2)(1 + d^\mu)^{\mu+2} ,$$

for all $i = 1, \dots, s$, where $\mu = \min\{s, n\}$. The unknowns of the system are the coefficients of the polynomials $g \in \mathbb{Q}[Y]$ and $g_i \in \mathbb{Q}[X]$.

Precisely, let T be the set of power products in the indeterminates $x_1, x_2, \dots, x_n$, i.e.

$$T = \{x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n} \; ; \; (t_1, t_2, \dots, t_n) \in \mathbb{N}\} ,$$

and let $D = (\mu + 1)(n + 2)(1 + d^\mu)^{\mu+2}$. Expanding all polynomials in (4) to sums of monomials we get

$$\sum_{\substack{t \in T \\ \deg(t) \le D}} g_t t - \sum_{i=1}^{s} \sum_{\substack{t \in T \\ \deg(t) \le D}} \left(\sum_{\substack{u,v \in T \\ uv = t}} f_{i_u} g_{i_v} \right) t = 0 , \tag{5}$$

where we assume all coefficients g_t of power products t containing indeterminates from the set $X \setminus Y$ to be zero. Analogously, we assume all coefficients f_{i_t} of those power products t that do not occur in f_i to be zero.

Comparing the coefficients in the polynomial Equation (5), we get for every term t involved an equation in $\mathbb{Q}$ of the form

$$g_t - \sum_{i=1}^{s} \sum_{\substack{u,v \in T \\ uv = t}} f_{i_u} g_{i_v} = 0. \tag{6}$$

Note that the system (6) contains

$$\binom{D + \varrho - 1}{\varrho - 1} \le (D + 1)^{\varrho - 1}$$

equations, $\varrho = |Y|$ – as many as the number of terms in Y of degree less or equal D. We can write all these equations as a single matrix equation by forming a vector $\mathbf{g}$ of all coefficients of unknown polynomials g and g_i, and a matrix F whose entries are the coefficients f_{i_t} of the generating polynomials f_i (the same coefficient may occur quite often in this matrix), some 1's and a lot of 0's. The matrix equation is then

$$F\,\mathbf{g} = 0 . \tag{7}$$

The number of equations (the number of rows of F) is bounded by $(D + 1)^n$ while the number of columns of F (the number of unknowns in the vector $\mathbf{g}$) turns out to be bounded by $(D + 1)^\varrho + s(D + 1)^n$. We can assume now that F has been padded with zero rows to make it square. The size of this matrix is therefore bounded by $(D + 1)^\varrho + s(D + 1)^n$.

For the calculation of F we have to determine the places in F where the coefficients of the generating polynomials f_i go. The entry in the matrix F in the row corresponding to a term t depending only on the indeterminates in Y and the column corresponding to the unknown g_u is one if and only if $u = t$ and zero otherwise. The entry in F in the row corresponding to a term t and the column corresponding to the unknown g_{i_u} is the coefficient f_{i_v}, $v = \frac{t}{u}$, if t is divisible by u and zero otherwise. Thus, the required coefficient is determined by computing the place where to look it up in the table containing the coefficients of the f_i. The space required for that is the space needed for the division of a term by another one; such a division is merely a subtraction of the corresponding exponents vectors. Hence, the space requirement is essentially that for writing down two terms. The degrees of the terms involved are bounded by D, so the space needed is at most $2n(\log D + 1)$.

The space for writing down the entire matrix is far too large. Therefore we do not build the matrix in advance but compute each entry only when it is required in the computation.

4.2 Space Efficient Rank Computations

So far, we have transformed our problem of testing whether a subset of indeterminates is independent into the problem of determining whether a non trivial solution of the homogeneous linear system (7) exists. This can be done by a rank computation. In fact, if we denote with M the submatrix of F defined by the columns corresponding to the unknowns g_t, and with N the submatrix defined by the remaining columns, then, since M has maximum rank, the system (7) has a non trivial solution if and only if

$$\operatorname{rank} F = \operatorname{rank}(M|N) < \operatorname{rank} M + \operatorname{rank} N.$$

In [Csa76] and [IMR80] $O(\log^2 n)$ parallel time algorithms for computing the rank of an $n \times n$ complex matrix using $O(n^4)$ processors were developed. However, these algorithms presume that the whole matrix input data is present in memory before the computation starts. Unfortunately, for the problem at hand we can make no such assumption. Therefore, we simply start the parallel rank algorithm and generate an entry of F only when it is required. After it has been fed into the algorithm the storage will be freed again. As proved in [May89], the bookkeeping and recomputation overhead caused by this approach alters neither the parallel time $O(\log^2 n)$ nor the space requirements.

By the Parallel Computation Thesis ([FW78]) we can perform the same computation sequentially using no more space than the square of the time required by the parallel algorithm. In our case, since the order of the matrix F is bounded by $(D+1)^\ell + s(D+1)^n$, we obtain the following result:

Proposition 2. *Let I be an ideal in the polynomial ring $\mathbb{Q}[X]$ and let Y be a subset of indeterminates. Then there is an algorithm which tests the independence of Y modulo I in sequential space amounting to $O(\log^4(sD^n))$, where $D = (\mu+1)(n+2)(1+d^\mu)^{\mu+2}$ and $\mu = \min\{s, n\}$.*

Let us now analyze in more details the space requirement of the method described. We are given an ideal $I \subseteq \mathbb{Q}[X]$ and a subset Y of indeterminates. Let *size* be the number of bits needed to write down this input. Here we assume that I is given by a collection $f_1, f_2, \ldots, f_s$ of polynomials where the degrees are bounded by d and numerators and denominators of coefficients are bounded by K. Then d and K are bounded by 2^{size}, and n and s are bounded by *size*. The bound D on the degree of a non zero polynomial $g \in I \cap \mathbb{Q}[Y]$, is

$$D = (\mu + 1)(n + 2)(1 + d^{\mu})^{\mu+2} \in 2^{O(size^3)}$$

and hence the order of the matrix F does not exceed $2^{O(size^4)}$. Thus, the following theorem holds:

Theorem 5. *Let I be an ideal in the polynomial ring $\mathbb{Q}[X]$ and let Y be a subset of indeterminates. Then there is a sequential algorithm which tests the independence of Y modulo I in space polynomial in the size of the problem instance.*

If the subset Y of indeterminates is dependent, then, using similar ideas, we can also determine a representation for a polynomial g in the elimination ideal $I \cap \mathbb{Q}[Y]$. Again, using the sequential version of parallel methods for solving linear systems of equations (based on computing the determinant and Cramer's method) [Pan87] we obtain a sequential algorithm running in space polynomial in the input size.

Theorem 6. *Given an ideal $I \subset \mathbb{Q}[X]$ and a subset of indeterminates $Y \subseteq \{x_1, \ldots, x_n\}$, if $I \cap \mathbb{Q}[Y] \neq (0)$, then a polynomial g in the elimination ideal $I \cap \mathbb{Q}[Y]$ can be computed within polynomial space.*

4.3 Computing the Dimension

Using Definition 2.3, the dimension of an ideal $I \subseteq kX$ can be computed as a cardinality of a maximal independent set of variables. This can be done by enumerating all subsets Y of X from small to large ones and testing for each Y whether $I \cap k[Y] \neq (0)$. If the test succeeds, the cardinality of Y is the dimension of the ideal I. As we have shown in the previous section, all these computations require polynomial space. Moreover, determining not only one but *all* independent subsets of indeterminates can be done within the same space bound. Summarizing all results, we obtain:

Theorem 7. *The dimension of a polynomial ideal $I \subset \mathbb{Q}[X]$ can be computed in the space which is polynomial in the size of the input.*

5 Conclusions

References

[Bro87] W. Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *Ann. of Math.*, 126:577–591, 1987.

[BY90] Carlos Berenstein and Alain Yger. Bounds for the degrees in the division problem. *Michigan Math. J.*, 37(1):25–43, 1990.

[CLO92] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*. Springer-Verlag, New York, 1992.

[Csa76] L. Csanky. Fast Parallel Matrix Inversion Algorithms. *SIAM J. Comput.*, 5:718–723, 1976.

[DFGS91] Alicia Dickenstein, Noaï Fitchas, Marc Giusti, and Carmen Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Appl. Math.*, 33:73–94, 1991.

[Eis94] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1994.

[FW78] S. Fortune and J. Wyllie. Parallelism in random access machines. In *Proceedings of the 10th Ann. ACM Symposium on Theory of Computing (San Diego, CA)*, pages 114–118, New York, 1978. ACM, ACM Press.

[Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comput. Sci.*, 24(3):239–277, 1983. see also Corrigendum in Theor. Comput. Sci. 39, 343.

[IMR80] O. Ibarra, S. Moran, and L.E. Rosier. A note on the parallel complexity of computing the rank of order n matrices. *Inf. Process. Lett.*, 11:162, December 1980.

[KM96] Klaus Kühnle and Ernst W. Mayr. Exponential space computation of Gröbner bases. In Y.N. Lakshman, editor, *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation, ISSAC'96 (Zurich, Switzerland, July 24-26, 1996)*, pages 63–71, New York, 1996. ACM Press.

[Koi97] Pascal Koiran. Randomized and deterministic algorithms for the dimension of algebraic varieties. In *38th Annual Symposium on Foundations of Computer Science*, pages 36–45, Miami Beach, Florida, 20–22 October 1997.

[Kol88] J. Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1:963–975, 1988.

[Küh98] Klaus Kühnle. *Space Optimal Computation of Normal Forms of Polynomials*. Ph.D. Thesis, Institut für Informatik, Technische Universität München, March 1998.

[KW88] Heintz Kredel and Volker Weispfenning. Computing dimension and independent sets for polynomial ideals. *J. Symb. Comput.*, 6:231–247, 1988.

[Log89] Alessandro Logar. A computational proof of the Noether's Normalization Lemma. In T. Mora, editor, *Proceedings of the 6th International Conference AAECC-6 (Roma, Italia, 1988)*, volume 357 of *Lecture Notes in Computer Science*, pages 259–273. Springer-Verlag, 1989.

[May89] Ernst W. Mayr. Membership in polynomial ideals over $\mathbb{Q}$ is exponential space complete. In B. Monien and R. Cori, editors, *Proceedings of the 6th Annual Symposium on Theoretical Aspects of Computer Science (Paderborn, FRG, February 1989)*, volume 349 of *Lecture Notes in Computer Science*, pages 400–406. GI, afcet, Springer-Verlag, 1989.

[MM84] H.M. Möller and F. Mora. Upper and lower bounds for the degree of Groebner bases. In John Fitch, editor, *Proceedings of the 3rd International Symposium on Symbolic and Algebraic Computation EUROSAM 84 (Cambridge, England, July 9-11, 1984)*, volume 174 of *Lecture Notes in Computer Science*, pages 172–183. Springer-Verlag, 1984.

[MT97] Guillermo Matera and Jose Maria Turull 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.

[Pan87] V. Pan. Complexity of parallel matrix computations. *Theor. Comput. Sci.*, 54(1):65–85, 1987.

[Sha94] Igor R. Shafarevich. *Basic algebraic geometry 1. Varieties in projective space*. Springer-Verlag, Berlin-Heidelberg-New York, 1994.