Discrete Applied Mathematics 33 (1991) 73-94
North-Holland

The membership problem for unmixed polynomial ideals is solvable in single exponential time

Alicia Dickenstein

Dipartamento de Matemática, Universidad de Buenos Aires, Buenos Aires 1636, Argentina

Noaï Fitchas*

Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Instituto Argentino de Matemática, Viamonte 1636, 1055 Buenos Aires, Argentina

Marc Giusti

Centre de Mathématiques, École Polytechnique, Palaiseau, Paris, France

Carmen Sessa

Dipartamento de Matemática, Universidad de Buenos Aires, Buenos Aires 1636, Argentina

Received 1 August 1989
Revised 20 December 1989

Abstract

Dickenstein, A., N. Fitchas, M. Giusti and C. Sessa, The membership problem for unmixed polynomial ideals is solvable in single exponential time, Discrete Applied Mathematics 33 (1991) 73-94.

Deciding membership for polynomial ideals represents a classical problem of computational commutative algebra which is exponential space hard. This means that the usual algorithms for the membership problem which are based on linear algebra techniques have doubly exponential sequential worst case complexity.

We show that the membership problem has single exponential sequential and polynomial parallel complexity for unmixed ideals. More specific complexity results are given for the special cases of zero-dimensional and complete intersection ideals.

Introduction

Let k be a field and $R := k[X_1, \ldots, X_n]$ the polynomial ring in n indeterminates $X_1, \ldots, X_n$ over k.

* Working group at the Instituto Argentino de Matemática, Consejo Nacional de Investigaciones Científicas y Téchnicas (CONICET), Viamonte 1636, 1055 Buenas Aires, Argentina (mailing address). Its members are: L. Caniglia, S. Danon, J. Heintz, T. Krick and P. Solernó.

We are considering the following problems from a complexity theoretical point of view:

(0.1) *Membership problem* (MP): For given $f_1, \ldots, f_s, f$ in R, decide whether f belongs to $(f_1, \ldots, f_s)$.

(0.2) *Representation problem* (RP): For given $f_1, \ldots, f_s, f$ in R, decide whether f belongs to $(f_1, \ldots, f_s)$, and if so, compute a representation $f = \sum_{1 \le \mu \le s} a_\mu f_\mu$ with $a_\mu \in R$ for $1 \le \mu \le s$.

It is known that (MP) for arbitrary $f_1, \ldots, f_s, f$ is exponential space complete and that (RP) may involve polynomials a_μ, $1 \le \mu \le s$, of degree doubly exponential in n [27].

Obviously a solution for (RP) implies a solution for (MP) but not vice versa.

In this paper we solve (MP) for unmixed ideals and (RP) for both zero-dimensional and complete intersection ideals with tight complexity bounds in sequential and in parallel. We show that in these cases (MP) and (RP) are solvable in single exponential sequential and polynomial parallel time. The algorithmic complexity of (MP) and (RP) is measured in the following parameters:

$$d := \max_{1 \le \mu \le s} (\deg(f_\mu), 3), \quad \deg(f) \quad \text{and} \quad n.$$

Our main theorem can be stated as follows: *Let $(f_1, \ldots, f_s)$ be an unmixed ideal, then it can be decided in sequential time $s^7(\max(\deg(f), d^{n^2}))^{O(n^2)}$ and parallel time $O(n^4 \log^2 s \max(\deg(f), d^{n^2}))$ whether f belongs to $(f_1, \ldots, f_s)$.*

The most interesting examples of unmixed ideals are the zero-dimensional ideals and the complete intersection ideals, $f_1, \ldots, f_s$ being a regular sequence. In these cases we resolve both (MP) and (RP) in a satisfactory way. We have the following results:

(i) Let $(f_1, \ldots, f_s)$ be a zero-dimensional ideal. Then for any compatible monomial order a Gröbner (standard) basis of $(f_1, \ldots, f_s)$ can be computed in sequential time $s^7 d^{O(n^2)}$ and parallel time $O(n^4 \log^2 sd)$.

(This specifies results of [9]. See also [24] and [19] for corresponding results concerning homogeneous ideals.)

This implies that (RP) and (MP) can be resolved in sequential time $s^7(d^n + \deg(f))^{O(n)}$ and parallel time $O(n^2 \log^2 s(d^n + \deg(f)))$ for zero-dimensional ideals.

(ii) Let $f_1, \ldots, f_s$ be a regular sequence in R. Then (RP) and (MP) can be solved in sequential time $(d^n + \deg(f))^{O(n)}$ and parallel time $O(n^2 \log^2 (d^n + \deg(f)))$.

While this work was done, by analytical methods Berenstein and Yger [2] obtained similar results for fields k with characteristic char $k = 0$.

We shall use an affine version of Noether's normalization lemma. For k sufficiently large we describe an algorithm which finds a k-linear transformation of the indeterminates $X_1, \ldots, X_n$ into new indeterminates $X'_1, \ldots, X'_n$ such that for $r := \dim_{\mathrm{Krull}} R/(f_1, \ldots, f_s)$ the following holds:

(i) $k[X'_1, \ldots, X'_r] \cap (f_1, \ldots, f_s) = (0)$,

(ii) $k[X'_1, \ldots, X'_r] \hookrightarrow R/(f_1, \ldots, f_s)$ is an integral extension.

The sequential complexity of this normalization algorithm is $s^7 d^{O(n^2)}$ and its parallel complexity is $O(n^4 \log^2 sd)$ (compare also [22,26,12]).

In particular $r := \dim_{\mathrm{Krull}} R/(f_1, \dots, f_s)$ can be computed within these complexity bounds. (Observe that r is also the dimension of the algebraic variety of zeroes of $f_1, \dots, f_s$ in an algebraic closure of k.) This is up to now the most precise complexity result concerning the computation of the dimension of affine algebraic varieties (compare [11] and [9]).

A homogeneous version of an effective Noether normalization lemma has been given in [18] and is used there to calculate the dimension of projective varieties in single exponential time.

In this paper we will freely use notions and facts from commutative algebra, classical algebraic geometry, and Gröbner (standard) basis theory. We refer the reader to [1,30,20,8,15,25,7]. (The algorithmic notion of Gröbner basis of polynomial ideals was introduced in [5,6].)

Our proofs and algorithmic bounds are based on recent progress concerning effective versions of affine Hilbert Nullstellensätze in fields of arbitrary characteristic [9,10,21,14,29]. First effective Nullstellensätze were proved by Lazard [23] (projective case) and by Brownawell [4] (affine case for fields of characteristic char $k=0$).

1. Noether's normalization lemma from a complexity point of view

In this section we describe an algorithm which solves the problem of finding a "Noether position" for an (arbitrary) ideal I of the polynomial ring $k[X_1, \dots, X_n]$ in n indeterminates $X_1, \dots, X_n$ over a field k. (For a Gröbner basis approach to this algorithm see [22,26].)

The *input* of the algorithm is:

-A set $\{f_1, \dots, f_s\}$ of generators of I in $k[X_1, \dots, X_n]$ with

$$\max_{1 \le \mu \le s} (\deg(f_\mu)) \le d$$

(where s and d are arbitrary but previously fixed integer numbers).

-A field extension $k \subseteq k'$ such that

$$\#(k') > d^n (d^n + 1).$$

The *output* of the algorithm is:

-A set $\{X_1', \dots, X_n'\}$ of k'-linear forms in $k'[X_1, \dots, X_n]$ (variable transformation).

-An integer $0 \le r \le n$ (dimension).

-A set $\{b_{\mu j}: 1 \le \mu \le s,\ r+1 \le j \le n\}$ of polynomials in $k'[X_1, \dots, X_n]$ (generating integral dependence relations).

The properties of the *output* data are the following:

-$k'[X_1', \dots, X_n'] = k'[X_1, \dots, X_n]$.

-The canonical morphism

$$k'[X'_1,\dots,X'_r] \hookrightarrow k'[X_1,\dots,X_n] \to k'[X_1,\dots,X_n]/I\otimes k'$$

is a monomorphism.

-$k'[X_1,\dots,X_n]/I\otimes k'$ is integral over $k'[X'_1,\dots,X'_r]$ (with respect to the monomorphism just mentioned).

-The degree of $b_{\mu j} f_\mu$ is at most $d^n(d^{n-r}+1)$ (for $\mu=1,\dots,s$ and $j=r+1,\dots,n$). The polynomial $g_j := \sum_{1\le\nu\le s} b_{\nu j} f_\nu$ involves only the variables $X'_1,\dots,X'_r,X'_j$ and is "monic" in X'_j, i.e., $\deg_{X'_j}(g_j)=\deg(g_j)>0$. (Thus $g_j=0$ (mod $I\otimes k'$) is an integral dependence equation for X'_j (mod $I\otimes k'$) over $k'[X'_1,\dots,X'_r]$.)

The algorithm can be realized by an arithmetical network with inputs from k and outputs from k' which has size (sequential complexity) $s^7 d^{O(n)}$ and depth (parallel complexity) $O(n^4 \log^2 sd)$. (For the notion of arithmetical network used here see [16].)

Size and depth of this arithmetical network can be interpreted as sequential and parallel complexities of our algorithm. Therefore we shall speak in the future only about "sequential" and "parallel" complexities having in mind the concept of an arithmetical network.

1.1. Notations. Let k be an arbitrary field and $R:=k[X_1,\dots,X_n]$ be the polynomial ring in $n>1$ indeterminates $X_1,\dots,X_n$ over k. We denote by $\bar{k}$ an algebraically closed field such that $k\subseteq\bar{k}$.

From now on let polynomials $f_1,\dots,f_s\in R$ be given with

$$d:=\max_{1\le\mu\le s}(\deg(f_\mu),3).$$

Let $I:=(f_1,\dots,f_s)$ be the ideal of R generated by $f_1,\dots,f_s$. Finally, let k' be a fixed subfield of $\bar{k}$ such that k is contained in k' and $\#(k')>d^n(d^n+1)$.

1.2. Definition. Let $Z_1,\dots,Z_r$ be k-linear forms in R. We say that $\{Z_1,\dots,Z_r\}$ is a *system of independent variables* (with respect to I) if the two following conditions are satisfied:

$$I\cap k[Z_1,\dots,Z_r]=(0), \tag{1}$$

$$\dim_{\mathrm{Krull}}(R/I)=r=\dim_{\mathrm{Krull}} k[Z_1,\dots,Z_r]. \tag{2}$$

1.3. Remark. The condition (1) is equivalent to

The canonical morphism $k[Z_1,\dots,Z_r]\hookrightarrow R\to R/I$ is a monomorphism. (3)

1.4. Definition. Let $\{Z_1,\dots,Z_r\}$ be a system of independent variables with respect to I and let Y be a k-linear form in R. We say that Y is a *dependent variable* with respect to $\{Z_1,\dots,Z_r\}$ and I, if there exists a polynomial $g\in k[Z_1,\dots,Z_r,T]$, T being a new indeterminate, such that $g \neq 0$ and $g(Z_1, \dots, Z_r, Y) \in I$. If g is monic in T and $g(Z_1, \dots, Z_r, Y) \in I$ then Y is called *integral* with respect to $\{Z_1, \dots, Z_r\}$ and I.

1.5. Remark. Let $r := \dim_{\mathrm{Krull}}(R/I)$. Then

$$r = \max\{t \in \mathbb{N}_0 : \exists i_1, \dots, i_t \in [1, \dots, n] \text{ such that } I \cap k[X_{i_1}, \dots, X_{i_t}] = (0)\}.$$

Taking into account Remark 1.5, we see that the problem of finding a system of r independent variables can be reduced to (n/r) many zero-intersection tests. By Proposition 1.7 below we see that such tests require only linear algebra over k (see Remark 1.8).

1.6. Remark. Let f be a polynomial of R belonging to rad(I), the radical of I. Then there exists a representation

$$f^{d^n} = \sum_{1 \leq \mu \leq s} b_\mu f_\mu \tag{4}$$

with $b_\mu \in R$ and $\deg(b_\mu f_\mu) \leq d^n(\deg(f) + 1)$.

Proof. Let $F, F_1, \dots, F_s$ be the homogenizations of $f, f_1, \dots, f_s$ in $k[X_0, \dots, X_n]$. The hypothesis $f \in \mathrm{rad}(I)$ implies that

$$X_0 F \in \mathrm{rad}(F_1, \dots, F_s).$$

From [14, Théorème 10], one obtains that $(X_0F)^{d^n} \in (F_1, \dots, F_s)$. Thus, there exist homogeneous polynomials $B_1, \dots, B_s \in k[X_0, \dots, X_n]$ such that

$$(X_0F)^{d^n} = \sum_{1 \leq \mu \leq s} B_\mu F_\mu$$

and such that $\deg(B_\mu F_\mu) = d^n(\deg(f) + 1)$. Putting $X_0 = 1$, (4) follows. □

1.7. Proposition. *Let* $\{i_1, \dots, i_r\} \subseteq [1, \dots, n]$. *Write* $Y_l := X_{i_l}$ $(1 \leq l \leq r)$. *Let* $V \in A^n$ *be the zero set of* $(f_1, \dots, f_s)$ *in the n-dimensional affine space* A^n *over* $\bar{k}$. *Then the following conditions are equivalent*

(a) $I \cap k[Y_1, \dots, Y_r] \neq (0)$;

(b) $\exists g \in k[Y_1, \dots, Y_r]$ *such that* $g \neq 0$ *and* $g = \sum_{1 \leq \mu \leq s} b_\mu f_\mu$ *with* $b_\mu \in R$,

$$\deg(b_\mu f_\mu) \leq d^n(\deg(V) + 1)$$

where $\deg(V)$ *is the degree of* V *defined by* $\deg(V) := \sum_j \deg(W_j)$ *if* $V = \bigcup_j W_j$ *is the irreducible decomposition of* V *in* A^n *(see* [20, *Remark* 2]).

Proof. Assume that (a) holds. Let A^r be the r-affine space over $\bar{k}$. We consider the (linear) projection map

$$\pi : A^n \to A^n,$$

$$\xi \mapsto (Y_1(\xi), \dots, Y_r(\xi)).$$

The hypothesis (a) implies that $\overline{\pi(V)}\neq A^r$, $\overline{\pi(V)}$ being the Zariski closure of $\pi(V)$ in A^r. From [20, Remark 4], one concludes that there exists $f\in\bar{k}[A^r]$ such that $f\neq 0$, $\deg(f)\leq\deg(V)$ and f vanishes on $\pi(V)$. By Remark 1.6, there exists a representation

$$f(Y_1,\dots,Y_r)^{d^n}=\sum_{1\leq\mu\leq s} b_\mu f_\mu \tag{$*$}$$

with $b_\mu\in\bar{k}[X_1,\dots,X_n]$, $\deg(b_\mu f_\mu)\leq d^n(\deg(V)+1)$. This shows that (b) has a solution with coefficients in $\bar{k}$.

For $\mu=1,\dots,s$ let R_μ be the k-linear subspace of R generated by all monomials M in $X_1,\dots,X_n$ with $\deg(M)\leq d^n(\deg(V)+1)-\deg(f_\mu)$. We consider the k-linear monomorphism

$$\begin{aligned}\Phi: R_1\times\cdots\times R_s&\to R\\ (b_1,\dots,b_s)&\mapsto\sum_{1\leq\mu\leq s} b_\mu f_\mu.\end{aligned}$$

Now ($*$) implies that $(\operatorname{im}\Phi\cap k[Y_1,\dots,Y_r])\otimes_k\bar{k}\neq(0)$. Hence $\operatorname{im}\Phi\cap k[Y_1,\dots,Y_r]\neq(0)$ and (b) follows. □

1.8. Remark. First note that $\deg(V)\leq d^n$ as a consequence of the Bezout inequality (see e.g. [20, Theorem 1 and Corollary 1]). The equivalence of conditions (a) and (b) implies that we can effectively test whether $I\cap k[Y_1,\dots,Y_r]\neq(0)$ holds. In fact, taking into account the degree bounds in (b) and the estimate $\deg(V)\leq d^n$, by comparison of coefficients one reduces the problem of deciding whether $I\cap k[Y_1,\dots,Y_r]\neq(0)$ to the problem of deciding whether some homogeneous linear equation system of size $sd^{n^2}\times sd^{n^2}$ has a nontrivial solution. This can be done by the algorithms of [28] and [3] in sequential time $s^7d^{O(n^2)}$ and parallel time $O(n^4\log^2 sd)$. Repeating this test 2^n times for all subsets of $\{X_1,\dots,X_n\}$, within the same complexity order one finds a system of independent variables with respect to I.

In particular, we obtain the following important

1.9. Corollary (compare [11,9,18]). *Let k be a field with algebraic closure $\bar{k}$ and let $f_1,\dots,f_s\in k[X_1,\dots,X_n]$ be n-variate polynomials with $d:=\max_{1\leq\mu\leq s}(\deg(f_\mu),3)$. Let $I:=(f_1,\dots,f_s)$ and $V:=\{\xi\in\bar{k}^n: f_1(\xi)=0,\dots,f_s(\xi)=0\}$. Denote the dimension of the algebraic variety V by* $\dim(V)$.

Then $\dim_{\mathrm{Krull}}(k[X_1,\dots,X_n]/I)=\dim(V)$ *can be computed in sequential time $s^7d^{O(n^2)}$ and in parallel time* $O(n^4\log^2 sd)$.

Let us consider a system $\{Z_1,\dots,Z_r\}$ of independent variables with respect to I. Let $Y\in R$ be a k-linear form. By Remark 1.5 Y is a dependent variable with respect to $\{Z_1,\dots,Z_r\}$. We ask whether Y is integral with respect to $\{Z_1,\dots,Z_r\}$. By Proposition 1.11 below we see that this question can be decided with a test which requires only linear algebra over k.

We need the following

1.10. Lemma. *Let $W \subset A^n$ be an irreducible and closed subvariety of the n-dimensional affine space A^n over $\bar{k}$. Denote by $\bar{k}[A^n]$ the coordinate ring of A^n. Let $p \subseteq \bar{k}[A^n]$ be the prime ideal consisting of all $f \in \bar{k}[A^n]$ vanishing on W. Suppose that $\{Z_1', \dots, Z_t'\}$ is a system of independent variables with respect to p.*

Then, if a $\bar{k}$-linear form $Y \in \bar{k}[A^n]$ is integral with respect to $\{Z_1', \dots, Z_r'\}$, there exists a polynomial $g \in \bar{k}[Z_1', \dots, Z_t', T]$, T being a new indeterminate, such that

(a) *g is monic in T;*

(b) *$g(Z_1', \dots, Z_t', Y)$ vanishes on W and*

(c) $\deg(g) \le \deg(W)$.

Proof. Let y denote the image of Y in $\bar{k}[W] = \bar{k}[A^n]/p$. The hypothesis on Y implies that y is integral over $\bar{k}[Z_1', \dots, Z_t']$ with respect to the canonical monomorphism $\bar{k}[Z_1', \dots, Z_t'] \hookrightarrow \bar{k}[W]$. Let $g \in \bar{k}(Z_1', \dots, Z_t')[T]$ be the minimal polynomial of y over $\bar{k}(Z_1', \dots, Z_t')$. Since $\bar{k}[Z_1', \dots, Z_t']$ is integrally closed, we see that $g \in \bar{k}[Z_1', \dots, Z_t', T]$. Moreover g satisfies (a) and (b). In order to verify (c) for this minimal polynomial g, we consider the (linear) projection map

$$\pi : A^n \to A^{t+1},$$

$$\xi \mapsto (Z_1'(\xi), \dots, Z_t'(\xi), Y(\xi)).$$

The hypothesis on Y implies that the restriction

$$\pi_W : W \to \overline{\pi(W)}$$

is a finite morphism. Thus $\pi(W) = \overline{\pi(W)}$ is a hypersurface of A^{t+1} defined by a polynomial $h \in \bar{k}[Z_1', \dots, Z_t', T]$, with $\deg(h) = \deg(\pi(W)) \le \deg(W)$ [20, Lemma 2]. Therefore $h(Z_1', \dots, Z_t', y) = 0$. It follows that g divides h. Hence $\deg(g) \le \deg(h) \le \deg(W)$. □

1.11. Proposition. *Let A^n be the n-dimensional affine space over $\bar{k}$ and let $V \subseteq A^n$ be the zero set of $I \otimes \bar{k}$, i.e.,*

$$V = \{\xi \in \bar{k}^n : f_1(\xi) = 0, \dots, f_s(\xi) = 0\}.$$

Let $\{Z_1, \dots, Z_r\}$ be a system of independent variables with respect to I. Assume that a given k-linear form $Y \in R$ is integral with respect to $\{Z_1, \dots, Z_r\}$ and I. Then there exists a polynomial $g \in k[Z_1, \dots, Z_r, T]$ such that

(a) *g is monic in T;*

(b) $\deg(g) \le d^n(\deg(V) + 1)$;

(c) *there exists a representation*

$$g(Z_1, \dots, Z_r, Y) = \sum_{1 \le \mu \le s} b_\mu f_\mu$$

with $b_\mu \in R$ such that $\deg(b_\mu f_\mu) \le d^n(\deg(V) + 1)$ *for all* $1 \le \mu \le s$.

Proof. Let $W_1, \dots, W_m$ be the irreducible components of V. Fix $1 \le j \le m$. We put $W := W_j$ and we denote by p the prime ideal of all $f \in \bar{k}[A^n]$ vanishing on W.

Let y denote the image of Y in $\bar{k}[V]$ and y' its image in $\bar{k}[W]$. We consider the following commutative diagram of canonical morphisms:

$$\begin{array}{ccc}
\bar{k}[V] & \longrightarrow & \bar{k}[W] \\
\uparrow & & \uparrow \\
\bar{k}[Z_1,\dots,Z_r] & \longrightarrow & \bar{k}[Z_1,\dots,Z_r]/p^c \\
 & & \uparrow \\
 & & \bar{k}[Z_1',\dots,Z_t']
\end{array}$$

where $p^c := p \cap \bar{k}[Z_1,\dots,Z_r]$ and where $Z_1',\dots,Z_t'$ are $\bar{k}$-linear combinations of $Z_1,\dots,Z_r$ such that $p \cap \bar{k}[Z_1',\dots,Z_t'], = (0)$ and such that $\bar{k}[Z_1,\dots,Z_r]/p^c$ is integral over $\bar{k}[Z_1',\dots,Z_t']$ (such $Z_1',\dots,Z_t'$ exist by Noether's normalization lemma).

Since $t = \dim(W)$, it follows that $\{Z_1',\dots,Z_t'\}$ is a system of independent variables with respect to p.

The hypothesis on Y implies that y is integral over $\bar{k}[Z_1,\dots,Z_r]$. Therefore y' is integral over $\bar{k}[Z_1,\dots,Z_r]/p^c$ and, a fortiori, over $\bar{k}[Z_1',\dots,Z_t']$. Lemma 1.10 implies that there exists a polynomial $g \in \bar{k}[Z_1',\dots,Z_t', T]$ such that

-g is monic in T,

-$g(Z_1',\dots,Z_t', Y)$ vanishes on W,

-$\deg(g) \leq \deg(W)$.

Writing $Z_1',\dots,Z_t'$ as $\bar{k}$-linear combinations of $Z_1,\dots,Z_r$, we obtain a polynomial $g_j \in \bar{k}[Z_1,\dots,Z_r, T]$ such that

-g_j is monic in T,

-$g_j(Z_1,\dots,Z_r, Y)$ vanishes on W,

-$\deg(g_j) \leq \deg(W)$.

Now put $f := \prod_{1 \leq j \leq m} g_j \in \bar{k}[Z_1,\dots,Z_r, T]$. This polynomial f verifies:

-f is monic in T,

-$f(Z_1,\dots,Z_r, Y)$ vanishes on V,

-$\deg(f) \leq \deg(V)$.

By Remark 1.6 there exists a representation

$$f(Z_1,\dots,Z_r, Y)^{d^n} = \sum_{1 \leq \mu \leq s} b_\mu f_\mu \qquad (**)$$

with $b_\mu \in \bar{k}[X_1,\dots,X_n]$, $\deg(b_\mu f_\mu) \leq d^n(\deg(V)+1)$ for all $1 \leq \mu \leq s$. As in Proposition 1.7 a linear algebra argument completes the proof. □

As in Remark 1.8 the existence of a polynomial g satisfying Proposition 1.11 (a)-(c) can be tested in sequential time $s^7 d^{O(n^2)}$ and in parallel time $O(n^4 \log^2 sd)$.

Taking into account Remark 1.5, Propositions 1.7 and 1.11, we see that we are in position to choose algorithmically a new order of $X_1,\dots,X_n$ such that:

(i) $\{X_1, \ldots, X_r\}$ is a system of independent variables with respect to I;

(ii) $X_{r+1}, \ldots, X_p$ are integral variables with respect to $\{X_1, \ldots, X_r\}$ and I;

(iii) $X_{p+1}, \ldots, X_n$ are dependent (but not integral) variables with respect to $\{X_1, \ldots, X_r\}$ and I.

The next step is to perform a changement of $X_1, \ldots, X_r$ in such a way that the new variables satisfy (i) and (ii) with $p = n$. (Then, we call $X_1, \ldots, X_r$ to be in "Noether position".)

Proposition 1.12 below will be useful in order to obtain complexity bounds.

1.12. Proposition. *Assume that $\{X_1, \ldots, X_r\}$ is a system of independent variables with respect to I. Then, given a k-linear form $Y \in R$, there exists a polynomial $g \in k[X_1, \ldots, X_r, T]$, T being a new indeterminate, such that*

(a) $g \neq 0$, $\deg(g) \leq d^n(\deg(V)+1)$;

(b) $g(X_1, \ldots, X_r, Y) = \sum_{1 \leq \mu \leq s} b_\mu f_\mu$ *with* $b_\mu \in R$ *and* $\deg(b_\mu f_\mu) \leq d^n(\deg(V)+1)$ *for all* $1 \leq \mu \leq s$.

Proof. Consider the (linear) projection map

$$\pi : A^n \to A^{r+1},$$
$$\xi \mapsto (X_1(\xi), \ldots, X_r(\xi), Y(\xi)).$$

The hypothesis implies that $\overline{\pi(V)} \neq A^{r+1}$. By [20, Remark 4], there exists a polynomial $f \in \bar{k}[X_1, \ldots, X_r, T]$ with $\deg(f) \leq \deg(\overline{\pi(V)}) \leq \deg(V)$ such that $f(X_1, \ldots, X_r, Y)$ vanishes on V. Applying Remark 1.6, we obtain a representation

$$f(X_1, \ldots, X_r, Y)^{d^n} = \sum_{1 \leq \mu \leq s} b_\mu f_\mu$$

with $b_\mu \in \bar{k}[X_1, \ldots, X_n]$, $\deg(b_\mu f_\mu) \leq d^n(\deg(V)+1)$. As in Proposition 1.7 a linear algebra argument completes the proof. □

Similarly to Remark 1.8 one reduces the problem of finding a polynomial g satisfying Proposition 1.12 (a) and (b) to the problem of solving a linear equation system. Using [28] and [3], this can be done in sequential time $s^7 d^{O(n^2)}$ and in parallel time $O(n^4 \log^2 sd)$.

1.13. Algorithm (compare [24] and [26]). Here we sketch the algorithm mentioned in the beginning of this section.

Input: $f_1, \ldots, f_s$; $\Lambda \subseteq k'$ such that $\#(\Lambda) > d^n(d^n+1)$
Output: $X_1', \ldots, X_n'$; r; $b_{\mu j}$ $(1 \leq \mu \leq s,\ r+1 \leq j \leq n)$

(1) **find** $\{i_1, \ldots, i_r\} \subseteq [1, \ldots, n]$ such that $\{X_{i_1}, \ldots, X_{i_r}\}$ is a system of independent variables (see Remark 1.8)

(2) **rename** $X_1, \ldots, X_n$ in such a way that $X_1 := X_{i_1}, \ldots, X_r := X_{i_r}$

(3) **find** all integral variables among $X_{r+1}, \ldots, X_n$ (see Proposition 1.11)

(4) **rename** $X_1, \dots, X_n$ in such a way that the integral variables found in (3) are $X_{r+1}, \dots, X_p$

(5) **for** $p+1 \le j \le n$

  find $g_j \in k[X_1, \dots, X_r, T]$ verifying the conditions of Proposition 1.12 for $Y = X_j$

  find $G_j :=$ maximal degree of homogeneous part of g_j

  find $(\lambda_1, \dots, \lambda_r) \in \Lambda^r : G_j(\lambda_1, \dots, \lambda_r, 1) \neq 0$

  put $X_i := X_i + \lambda_i X_j$ $(1 \le i \le r)$

2. The membership problem in the case of an unmixed ideal

In this section we describe an algorithm which solves the membership problem (MP) in the case of an unmixed ideal. This algorithm has simply exponential sequential and parallel complexity. Let the notations be the same as in Notations 1.1.

The ideal I is called *unmixed* if

$$\dim_{\mathrm{Krull}}(R/p) = \dim_{\mathrm{Krull}}(R/I)$$

for all associated primes p of the R-module R/I. Here $\dim_{\mathrm{Krull}}(R/p)$ and $\dim_{\mathrm{Krull}}(R/I)$ denote the Krull dimensions of the rings R/p and R/I.

2.1. Remark. If I is unmixed, then for any field extension $k \subseteq L$, $I \otimes_k L$ is unmixed too.

2.2. Theorem. *Assume that I is unmixed. Let $r := \dim_{\mathrm{Krull}}(R/I)$ and let $\{X_1, \dots, X_r\}$ be a system of independent variables with respect to $I \otimes_k k'$ such that $(R/I) \otimes k'$ is integral over $k'[X_1, \dots, X_r]$ with respect to the canonical morphism (Remark 1.3 (3)). Let f be given in R. Let $B := 1 + \max\{\deg(f), d + (n-r+1)d^n(d^{n-r}+1)\}$.*

Then the following conditions are equivalent:

(a) $f \in I$;

(b) $\exists h \in k'[X_1, \dots, X_r]$ *and* $p_1, \dots, p_s \in R \otimes k'$ *such that*

- $hf = \sum_{1 \le \mu \le s} p_\mu f_\mu$,
- $h \neq 0$,
- $\deg(h) \le dB^{2(n-r)}$,
- $\deg(p_\mu f_\mu) \le B + dB^{2(n-r)}$.

Proof. (b) $\Rightarrow$ (a) Let $h \in k'[X_1, \dots, X_r]$ be such that $h \neq 0$ and $hf \in I \otimes k'$. Let $I \otimes k' = q_1 \cap \cdots \cap q_t$ be an irredundant primary decomposition of $I \otimes k'$.

Let $p_j := \mathrm{rad}(q_j)$ be the radical ideal of q_j $(1 \le j \le t)$. Thus $\{p_1, \dots, p_t\}$ is the set of associated primes of the $R \otimes k'$ module $(R/I) \otimes k'$. Therefore $\dim_{\mathrm{Krull}}((R \otimes k')/p_j) = r$ for $j = 1, \dots, t$. Fix $1 \le j \le t$. Since $(R/I) \otimes k'$ is integral over $k'[X_1, \dots, X_r]$, we see that $(R \otimes k')/p_j$ is integral over $k'[X_1, \dots, X_r]$ too. Therefore $p_j \cap k'[X_1, \dots, X_r] = (0)$. Hence $h \notin p_j$. Since $hf \in q_j$, we conclude that $f \in q_j$. Thus $f \in I \otimes k'$ and, a fortiori, $f \in I$.

(a) ⇒ (b) Let $Y_{r+1},\dots,Y_n$ be k'-linear forms in $R\otimes k'$ such that $R\otimes k'=k'[X_1,\dots,X_r,Y_{r+1},\dots,Y_n]$.

The hypothesis that $(R/I)\otimes k'$ is integral over $k'[X_1,\dots,X_r]$ implies that $Y_{r+1},\dots,Y_n$ are integral variables with respect to $\{X_1,\dots,X_r\}$ (Definition 1.4).

Let $r+1\le j\le n$. By Proposition 1.11 applied to $Y=Y_j$, there exists a polynomial $g_j\in k'[X_1,\dots,X_r,Y_j]$, g_j monic in Y_j and such that

$$g_j=\sum_{1\le\mu\le s} b_{\mu j}f_\mu \tag{5}$$

for certain polynomials $b_{1j},\dots,b_{sj}\in R\otimes k'$ with $\deg(b_{\mu j}f_\mu)\le d^n(\deg(V)+1)$ for $\mu=1,\dots,s$.

Let $K:=k'(X_1,\dots,X_r)$ be the fraction field of $k'[X_1,\dots,X_r]$. The hypothesis $f\in I$ means that there exists a representation

$$f=\sum_{1\le\mu\le s} a_\mu f_\mu,\quad a_\mu\in R\ (1\le\mu\le s). \tag{6}$$

Fix a diagonal order in the set of monomials in $Y_{r+1},\dots,Y_n$. Then $\{g_{r+1},\dots,g_n\}$ is a (Gröbner) standard basis of $(g_{r+1},\dots,g_n)K[Y_{r+1},\dots,Y_n]$ with respect to this order.

By Hironaka division in $K[Y_{r+1},\dots,Y_n]$ we obtain representations

$$a_\mu=\sum_{r+1\le j\le n} c_{\mu j}g_j+\tilde a_\mu\quad(1\le\mu\le s) \tag{7}$$

where $c_{\mu j},\tilde a_\mu\in K[Y_{r+1},\dots,Y_n]$ and $\deg_Y(\tilde a_\mu)<(n-r)d^n(\deg(V)+1)$. Here $\deg_Y$ denotes the total degree in $Y_{r+1},\dots,Y_n$.

Replacing (7) in (6) we see that

$$f=g+\sum_{1\le\mu\le s}\tilde a_\mu f_\mu \tag{8}$$

with $g\in(g_{r+1},\dots,g_n)K[Y_{r+1},\dots,Y_n]$. It follows that

$$\deg_Y(g)\le B_0,$$

where $B_0:=\max\{\deg(f), d+(n-r)d^n(\deg(V)+1)\}$.

Since $\{g_{r+1},\dots,g_n\}$ is a standard basis of $(g_{r+1},\dots,g_n)K[Y_{r+1},\dots,Y_n]$, g has a representation

$$g=\sum_{r+1\le j\le n} v_j g_j \tag{9}$$

with $v_j\in K[Y_{r+1},\dots,Y_n]$, $\deg_Y(v_jg_j)\le\deg_Y(g)$.

From (5), (9) and (8) we conclude that

$$f=\sum_{1\le\mu\le s} c_\mu f_\mu \tag{10}$$

where $c_\mu:=\sum_{r+1\le j\le n} v_jb_{\mu j}+\tilde a_\mu\in K[Y_{r+1},\dots,Y_n]$ and $\deg_Y(c_\mu f_\mu)\le B_1:=B_0+d^n(\deg(V)+1)$.

Put $C:=k'[X_1,\dots,X_r]$. For $\mu=1,\dots,s$ let F_μ be the C-submodule of $R\otimes k'$ freely generated by all monomials M in $Y_{r+1},\dots,Y_n$ with $\deg_Y(M)\le B_1+\deg_Y(f_\mu)$. Similarly, let F be the C-submodule of $R\otimes k'$ freely generated by all monomials M in $Y_{r+1},\dots,Y_n$ with $\deg_Y(M)\le B_1$.

We consider the C-linear map

$$\Phi: F_1\oplus\cdots\oplus F_s\oplus C\to F,$$
$$(p_1,\dots,p_s,h)\mapsto\sum_{1\le\mu\le s}p_\mu f_\mu-hf.$$

Let

$$q:=\operatorname{rank}(F)=\binom{n-r+B_1}{n-r}$$

and

$$m:=\operatorname{rank}(F_1\oplus\cdots\oplus F_s\oplus C)=\sum_{1\le\mu\le s}\binom{n-r+B_1-\deg_Y(f_\mu)}{n-r}+1.$$

We consider $M\in C^{q\times m}$, the matrix of Φ with respect to the canonical bases just introduced.

By [20, Lemma 7], there exists an upper-triangular matrix $\bar{M}\in C^{q\times m}$ with the following properties:

-All entries of $\bar{M}$ have degree bounded by $d\cdot\min\{q,m\}$;

-all $z\in C^m$ satisfy

$$M^{t}z=0\quad\text{iff}\quad\bar{M}^{t}z=0$$

(^{t}z is the column vector obtained by transposing the row vector z.)

Each c_μ of (10) has the form $c_\mu=p_\mu/h$ for certain $p_\mu\in R\otimes k'$ with $\deg_Y(p_\mu f_\mu)\le B_1$ and certain $h\in C$, $h\ne0$. Therefore $(p_1,\dots,p_s,h)\in\ker(\Phi)$.

By taking coordinates with respect to the monomial bases considered, we conclude that there exists $z=(a_1,\dots,a_{m-1},h)\in C^m$ such that

$$\begin{aligned}&\bar{M}^{t}z=0,\\&h\ne0.\end{aligned}\tag{***}$$

Therefore no row of $\bar{M}$ is of the form $(0,\dots,0,c)$ with $c\ne0$.

Taking this into account, we may assume without loss of generality that the vector $z=(a_1,\dots,a_{m-1},h)$ of (***) satisfies:

$$\max(\deg a_1,\dots,\deg a_{m-1},\deg h)\le d\cdot\min(q^2,m^2),$$
$$M^{t}z=0.$$

This shows that there exists $(p_1,\dots,p_s,h)\in\ker(\Phi)$ with $h\ne0$, $\deg(h)\le d\cdot\min(q^2,m^2)\le d\cdot B^{2(n-r)}$ and $\deg(p_\mu f_\mu)\le B_1+d\cdot\min(q^2m^2)\le B+d\cdot B^{2(n-r)}$. (Take into account that $\deg(V)\le d^{n-r}$ by Bezout's inequality, [20, Theorem 1].) $\square$

Let I be unmixed and let $f\in R$. Theorem 2.2 implies that the question whether f

belongs to I can be decided in sequential time $s^7 B^{O(n^2)}$ and parallel time $O(n^4 \log^2(sB))$, where

$$B := 1 + \max(\deg(f), d + (n-r+1)d^n(d^{n-r}+1)) = O(\max(\deg(f), d^{n^2})).$$

To see this, we apply Algorithm 1.13 in order to obtain coordinates $X_1, \ldots, X_r$ which satisfy the hypothesis of Theorem 2.2. Then we translate condition (b) into a homogeneous linear system over k'. Using the algorithm of [28] and [3], we check whether this system has a solution corresponding to the condition $h \neq 0$ in (b). This can be done within the asserted time bounds.

Using arithmetical networks with entries from k and elements from k' as constant operations [16] we obtain

2.3. Corollary. *Let k be a field and let $f, f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ be n-variate polynomials with $d := \max_{1 \leq \mu \leq s} \deg(f_\mu)$. Assume that $I = (f_1, \ldots, f_s)$ is unmixed.*

Then the problem of deciding whether f belongs to I is solvable in sequential time $s^7 \max(\deg(f), d^{n^2})^{O(n^2)}$ and in parallel time $O(n^4 \log^2(s \cdot \max(\deg(f), d^{n^2}))$.

3. The representation problem in the zero-dimensional case

Throughout this section we will assume the following:

For the polynomials $f_1, \ldots, f_s$ of Notations 1.1 the Krull dimension of the quotient ring $k[X_1, \ldots, X_n]/(f_1, \ldots, f_s)$ is less than or equal to zero (i.e., we suppose $\# V < \infty$). (11)

This is a particular case of unmixed ideals studied in Section 2. From Theorem 2.2 we obtain that any polynomial f belonging to $(f_1, \ldots, f_s)$ has a representation

$$f = \sum_{1 \leq \mu \leq s} a_\mu f_\mu$$

with single exponential bounds for the degrees of the coefficients $a_1, \ldots, a_s$. This circumstance allows us to give a parallelizable algorithm for the computation of Gröbner bases with respect to any compatible order. Our algorithm requires only linear algebra techniques over k. Moreover, we will show how any usual Gröbner basis algorithm can be changed into another one involving only computations with polynomials of "small" degree (see [9,8,2,13,17]; compare also [23,24,19] for the case of homogeneous ideals).

3.1. Notations. Let any compatible order of the monomials in $k[X_1, \ldots, X_n]$ be given.

For $f \in k[X_1, \ldots, X_n]$, $f \neq 0$, we denote by $\mathrm{Head}(f)$ the maximum monomial occurring in f. If $\mathrm{Head}(f) = \lambda X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, for some $\lambda \in k$ and some $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$, we write $\mathrm{Exp}(f) := (\alpha_1, \ldots, \alpha_n)$ and $\mathrm{Lc}(f) := \lambda$. ($\mathbb{N}_0$ denotes the set of natural integers, 0 included.)

$\mathrm{Exp}(f)$ is called the exponent and $\mathrm{Lc}(f)$ is called the leading coefficient of f. For a pair (f,f') of nonzero polynomials let $\mathrm{Head}(f,f') := \mathrm{lcm}(\mathrm{Head}(f), \mathrm{Head}(f'))$ be the lowest common multiple of $\mathrm{Head}(f)$ and $\mathrm{Head}(f')$, with leading coefficient equal to $\mathrm{Lc}(f)\mathrm{Lc}(f')$.

For the monomials ψ and ψ' given by

$$\psi \cdot \mathrm{Head}(f) = \psi' \cdot \mathrm{Head}(f') = \mathrm{Head}(f,f')$$

let $\deg(f,f') := \max\{\deg(\psi \cdot f), \deg(\psi' \cdot f')\}$ and $S(f,f') := \psi \cdot f - \psi' \cdot f'$. We call $S(f,f')$ the S-polynomial of f and f'.

3.2. Lemma. *Let $\mathscr{F} = \{f_1^0, \ldots, f_s^0\}$ be a set of polynomials generating an ideal $I \subseteq k[X_1, \ldots, X_n]$. Let $h \in I$ and $D \in \mathbb{N}_0$ be such that there exists a representation*

$$h = \sum_{1 \le \mu \le s} p_\mu f_\mu^0 \tag{12}$$

with $p_\mu \in k[X_1, \ldots, X_n]$ and $\deg(p_\mu f_\mu^0) \le D$ for $\mu = 1, \ldots, s$. Let $S^0(\mathscr{F}) := \mathscr{F}$ and, for $k > 0$, let $S^k(\mathscr{F})$ be the set obtained from $S^{k-1}(\mathscr{F})$ as follows:

$$S^k(\mathscr{F}) := S^{k-1}(\mathscr{F}) \cup \{S(f,f') \colon f,f' \in S^{k-1}(\mathscr{F}) \quad \textit{and} \quad \deg(f,f') \le D\}.$$

Then there exists $N \in \mathbb{N}_0$ and $f \in S^N(\mathscr{F})$ such that

$$\mathrm{Exp}(h) \in \mathrm{Exp}(f) + \mathbb{N}_0^n.$$

Proof. Our rather technical and indirect proof follows the ideas of [15,25] (see also [5,6]). Thus we will suppose that for all $k \ge 0$ and all $f \in S^k(\mathscr{F})$:

$$\mathrm{Exp}(h) \notin \mathrm{Exp}(f) + \mathbb{N}_0^n. \tag{13}$$

We consider all representation families $\mathscr{R} = (\phi_i f_i)_{i \in I}$ such that
- I is a finite set of indices;
- for all $i \in I$, ϕ_i is a monomial and $f_i \in S^k(\mathscr{F})$ for some $k \in \mathbb{N}_0$;
- $h = \sum_{i \in I} \phi_i f_i$.

For each representation family $\mathscr{R} = (\phi_i f_i)_{i \in I}$ we introduce the following notations

$$\mathrm{Head}(\mathscr{R}) := \max_{i \in I} (\mathrm{Head}(\phi_i f_i)),$$

$$J(\mathscr{R}) := \{i \in I \colon \mathrm{Head}(\phi_i f_i) = \mathrm{Head}(\mathscr{R})\},$$

$$\tau(\mathscr{R}) := \# J(\mathscr{R}),$$

$$\deg(\mathscr{R}) := \max_{j \in J(\mathscr{R})} \{\deg(\phi_j f_j)\}.$$

From (12) we see that the set of representation families $\mathscr{R}$ with $\deg(\mathscr{R}) \le D$ is not empty. Thus there exists a representation $\mathscr{R}_0 = (\phi_i f_i)_{i \in I_0}$ having the following properties:

(i) $\deg(\mathscr{R}_0) = \min_{\text{all } \mathscr{R}}(\deg(\mathscr{R})) \le D$,

(ii) $\mathrm{Head}(\mathscr{R}_0)=\min\{\mathrm{Head}(\mathscr{R})\colon \deg(\mathscr{R})=\deg(\mathscr{R}_0)\}$,

(iii) $\tau(\mathscr{R}_0)=\min\{\tau(\mathscr{R})\colon \deg(\mathscr{R})=\deg(\mathscr{R}_0)$ and $\mathrm{Head}(\mathscr{R})=\mathrm{Head}(\mathscr{R}_0)\}$.

Claim. $\tau(\mathscr{R}_0)\geq 2$.

Proof. If $\tau(\mathscr{R}_0)<2$, then $J(\mathscr{R}_0)=\{i_0\}$ for some $i_0\in I_0$. Therefore $\mathrm{Head}(h)=\mathrm{Head}(\sum_{i\in I_0}\phi_i f_i)=\mathrm{Head}(\phi_{i_0}f_{i_0})$. Hence $\mathrm{Exp}(h)\in\mathrm{Exp}(f_{i_0})+\mathbb{N}_0^n$. This contradicts (13).

From our claim, we conclude that there exist, at least, two different indices $l,k\in J(\mathscr{R}_0)$. Let $\theta:=\gcd(\phi_l,\phi_k)$ be the monic greatest common divisor of ϕ_l and ϕ_k. Let ψ and ψ' be the monomials verifying

$$\theta\psi=\phi_l \quad\text{and}\quad \theta\psi'=\phi_k.$$

Let $a:=\mathrm{Lc}(\phi_l f_l)$ and $b:=\mathrm{Lc}(\phi_k f_k)$.

Thus, for some $\lambda\in k$,

$$\psi\mathrm{Head}(f_l)=ab^{-1}\psi'\mathrm{Head}(f_k)=\lambda\mathrm{Head}(f_l,f_k),$$

whence

$$\lambda S(f_l,f_k)=\psi f_l-ab^{-1}\psi' f_k$$

and

$$\phi_l f_l-ab^{-1}\phi_k f_k=\lambda\theta S(f_l,f_k).$$

Moreover,

$$\deg(\psi f_l)\leq\deg(\theta\psi f_l)=\deg(\phi_l f_l)\leq\deg(\mathscr{R}_0)$$

and

$$\deg(\psi' f_k)\leq\deg(\theta\psi' f_k)=\deg(\phi_k f_k)\leq\deg(\mathscr{R}_0).$$

Thus $f_k,f_l\in S^N(\mathscr{F})$ implies $S(f_k,f_l)\in S^{N+1}(\mathscr{F})$. Therefore we obtain a new representation family $\mathscr{R}_0'$: the one induced by the equality

$$h=\sum_{j\in J(\mathscr{R}_0)-\{l,k\}}\phi_j f_j+(1+ab^{-1})\phi_k f_k+\sum_{i\in I_0-J(\mathscr{R}_0)}\phi_i f_i+\lambda\theta S(f_k,f_l).$$

Since $\mathrm{Head}(\lambda\theta S(f_k,f_l))<\mathrm{Head}(\phi_l f_l)=\mathrm{Head}(\mathscr{R}_0)$, we conclude that $\deg(\mathscr{R}_0')\leq\deg(\mathscr{R}_0)$, $\mathrm{Head}(\mathscr{R}_0')\leq\mathrm{Head}(\mathscr{R}_0)$ and $J(\mathscr{R}_0')\subseteq J(\mathscr{R}_0)-\{l\}$. This contradicts (i), (ii) or (iii). □

We conserve Notations 1.1.

3.3. Theorem. *Let be given a compatible order of the monomials in $k[X_1,\dots,X_n]$. Then the following is true:*

(i) *Any reduced Gröbner basis of I with respect to the given order contains at most d^{n^2} many polynomials. Moreover the reduced Gröbner basis of I verifies that all of its polynomials have total degree bounded by nd^n.*

(ii) *Let $\mathscr{H}=\{h_1,\dots,h_t\}$ be the reduced Gröbner basis of I. For each $1\leq j\leq t$ there exists a representation*

$$h_j = \sum_{1 \le \mu \le s} p_{\mu j} f_\mu$$

with $p_{\mu j} \in R$ *and* $\deg(p_{\mu j} f_\mu) \le nd^{2n} + d^n + d$.

(iii) *The stair* $E(I) := \{\mathrm{Exp}(f) : f \in I, f \ne 0\}$ *and the reduced Gröbner basis of* I *can be computed in sequential time*: $s^7 d^{O(n^2)}$, *parallel time*: $O(n^4 \log^2 sd)$.

(iv) *The output of the following algorithm is the reduced Gröbner basis of* I:

```
Input: f_1, ..., f_s
B := {(i,j): 1 ≤ i < j ≤ s}
t := s
while B ≠ ∅ do
  choose (i,j) ∈ B
  if deg(f_i, f_j) ≤ nd^{2n} + d^n + d
    then t := t + 1
         B := B ∪ {(i,t): 1 ≤ i ≤ t − 1}
         f_t := S(f_i, f_j)
  B := B − {(i,j)}
end
```

Proof. We follow the general lines of the proof of [9, Theorem 20]. First observe that $\dim_k(R/I) \le d^n$ (see [9, Theorem 17], for an elementary proof of this well-known fact). Thus, for each $1 \le j \le n$, there exists $g_j \in k[X_j]$ such that

$$g_j \in I \quad \text{and} \quad \deg(g_j) \le d^n.$$

By Remark 1.6 we obtain a representation

$$g_j^{d^n} = \sum_{1 \le \mu \le s} b_{\mu j} f_\mu$$

with $\deg(b_{\mu j} f_\mu) \le d^n(\deg(g_j) + 1)$.

Fix an additional auxiliary diagonal order in the set of monomials of R. Then $\{g_1^{d^n}, \dots, g_n^{d^n}\}$ is a Gröbner basis of $(g_1^{d^n}, \dots, g_n^{d^n})$ with respect to this auxiliary diagonal order.

(i) Let $\mathscr{H} = \{h_1, \dots, h_t\}$ be the Gröbner basis of I with respect to the given order. We see that, for each $1 \le j \le n$, there exists an element in $\mathscr{H}$, say h_j, such that $\mathrm{Head}(h_j)$ divides $\mathrm{Head}(g_j)$. Thus $\mathrm{Head}(h_j) = X_j^{D_j}$ for some $D_j \le d^n$. Now the hypothesis that $\mathscr{H}$ is reduced implies that for each $h \in \mathscr{H}$ and for each $1 \le j \le n$, $\deg_{X_j}(h) \le D_j \le d^n$. Now it is clear that $t \le d^{n^2}$.

Since $\mathscr{H}$ is reduced and $g_1, \dots, g_n$ are in I, Hironaka division of $h \in \mathscr{H}$ by $g_1, \dots, g_n$ leaves h unchanged, if h is different from $g_1, \dots, g_n$. Therefore the degree of the monomials appearing in h is bounded by nd^n.

(ii) Let $h := h_k$, $1 \le k \le t$. Write $h = \sum_{1 \le \mu \le s} a_\mu f_\mu$ with $a_1, \dots, a_s \in R$. We divide $a_1, \dots, a_s$ by $\{g_1^{d^n}, \dots, g_n^{d^n}\}$ with respect to the auxiliary order. Thus

$$a_\mu = \sum_{1 \le j \le n} c_{\mu j} g_j^{d^n} + \tilde{a}_\mu$$

with $\deg(\tilde{a}_\mu) \le nd^{2n}$. Therefore

$$h = \sum_{1\le\mu\le s}\left(\sum_{1\le j\le n} c_{\mu j} g_j^{d^n} + \tilde{a}_\mu\right) f_\mu.$$

Let $g := \sum_{1\le\mu\le s}\sum_{1\le j\le n} c_{\mu j} g_j^{d^n} f_\mu$.

From $g \in (g_1^{d^n}, \dots, g_n^{d^n})$ and $\deg(g) \le nd^{2n} + d$ we conclude by Hironaka division with respect to the auxiliary order that there exists a representation

$$g = \sum_{1\le j\le n} b_j g_j^{d^n} \quad \text{with } \deg(b_j g_j^{d^n}) \le nd^{2n} + d.$$

Therefore

$$h = \sum_{1\le\mu\le s}\left(\sum_{1\le j\le n} b_j b_{\mu j} + \tilde{a}_\mu\right) f_\mu.$$

It is easy to see that $\deg((\sum_{1\le j\le n} b_j b_{\mu j} + \tilde{a}_\mu) f_\mu) \le nd^{2n} + d^n + d$. This implies assertion (ii).

(iii) Immediate from (i) and (ii).

(iv) Immediate from (ii) and Lemma 3.2. □

From Theorem 3.3 one deduces easily

3.4. Corollary. *Let k be a field and let $f, f_1, \dots, f_s \in k[X_1, \dots, X_n]$ be n-variate polynomials with $d := \max_{1\le\mu\le s}(\deg(f_\mu))$. Assume that $I = (f_1, \dots, f_s)$ has dimension less than or equal to zero (i.e., $\dim_{\mathrm{Krull}} k[X_1, \dots, X_n]/I \le 0$).*

If $f \in I$, then a representation $f = \sum_{1\le\mu\le s} a_\mu f_\mu$ can be found with $\deg(a_\mu f_\mu) \le nd^{2n} + d^n + d + \deg(f)$ in sequential time $s^7(\deg(f) + d^n)^{O(n)}$ and in parallel time $O(n^2 \log^2 s(\deg(f) + d^n))$.

Within the same time bounds it can be decided whether f belongs to I.

4. The membership problem in the case of a complete intersection ideal

In this section we describe an efficient test for the membership problem (MP) in the case of a complete intersection ideal. This gives another algorithmic solution of (MP), different from the one described in Section 2. Let us assume the following

> The polynomials $f_1, \dots, f_s$ from Notations 1.1 form a not empty complete intersection in A^n, i.e., $V := \{\xi \in A^n\colon f_1(\xi) = 0, \dots, f_s(\xi) = 0\}$ is not empty and has pure dimension $n - s$. (14)

(Here A^n denotes the n-affine space over the algebraic closure $\bar{k}$ of k.)

Let the notations be the same as in Sections 1 and 2. Using the tools developed in Section 1, we are going to construct a set $\{X_1', \dots, X_n'\}$ of k'-linear forms in $R \otimes k'$ and polynomials $h, g_1, \dots, g_s \in R \otimes k'$ with the following properties:

(i) $k'[X_1', \dots, X_n'] = k'[X_1, \dots, X_n]$.

(ii) For each extension field $k' \subseteq L$ and for each polynomial $f \in L[X_1', \dots, X_n']$, $f \in I \otimes L$ if and only if $hf \in (g_1, \dots, g_s) L[X_1', \dots, X_n']$.

(iii) The polynomials $g_1, \dots, g_s$ form a Gröbner basis of $(g_1, \dots, g_s)$ with respect to the diagonal order induced by $X'_n > \cdots > X'_1$. (Thus the condition $hf \in (g_1, \dots, g_s)$ is easy to check.)

(iv) $\deg(h) \leq s(\deg(V)+1)d^n$.

(v) For each $1 \leq j \leq s$, $g_j \in k'[X'_1, \dots, X'_{n-s}, X'_{n-s+j}]$ and $\deg_{X'_{n-s+j}}(g_j) = \deg(g_j) \leq (\deg(V)+1)d^n$.

(Thus condition (iii) follows from condition (v).)

4.1. Theorem (see also [12]). *Let $\{X'_1, \dots, X'_n\}$ and $\{b_{\mu j}: 1 \leq \mu, j \leq s\}$ be the output data of the algorithm of Section* 1, *applied to the sequence $f_1, \dots, f_s$. For each $1 \leq j \leq s$ let $g_j := \sum_{1 \leq \mu \leq s} b_{\mu j} f_\mu$.*

Then $\{X'_1, \dots, X'_n\}$ satisfies condition (i) *above and the polynomials $h := \det(b_{\mu j})$ and $g_1, \dots, g_s$ satisfy conditions* (ii), (iii), (iv) *and* (v).

Proof. The properties of the output data of the algorithm of Section 1, imply that conditions (i), (iv) and (v) are satisfied. As we have observed already, condition (iii) is a consequence of condition (v). Another consequence of condition (v) is that $g_1, \dots, g_s$ is a regular sequence in $k'[X'_1, \dots, X'_n]$. Therefore condition (ii) follows from Lemma 4.2 below. □

4.2. Lemma. *Let R be a Noetherian commutative ring. Let $f_1, \dots, f_s$ and $g_1, \dots, g_s$ be two regular sequences in R. Assume that there exists a matrix $B \in R^{s \times s}$ transforming the vector $[f_1, \dots, f_s]$ into $[g_1, \dots, g_s]$, i.e., assume that a matrix equation*

$$[g_1, \dots, g_s] = [f_1, \dots, f_s]B \tag{15}$$

holds for some $B \in R^{s \times s}$.

Then, for each $f \in R$, the following statements are equivalent:

(i) $f \in (f_1, \dots, f_s)R$;

(ii) $(\det B) f \in (g_1, \dots, g_s)R$.

Proof. (i) ⇒ (ii) Let $f \in R$ be such that there exist $a_1, \dots, a_s \in R$ with $f = a_1 f_1 + \cdots + a_s f_s$. Thus $f = [f_1, \dots, f_s] \cdot {}^t[a_1, \dots, a_s]$, where ${}^t[a_1, \dots, a_s]$ is the column vector obtained by transposing the row vector $[a_1, \dots, a_s]$. Let $\mathrm{adj}(B) \in R^{s \times s}$ be the adjoint matrix of B. From (15) we obtain that

$$[g_1, \dots, g_s]\mathrm{adj}(B) = (\det B)[f_1, \dots, f_s].$$

Therefore

$$[g_1, \dots, g_s]\mathrm{adj}(B)^t[a_1, \dots, a_s] = (\det B) f.$$

This implies (ii).

(ii) ⇒ (i) The proof proceeds by induction on s.

Case $s=1$. In this case $B \in R$, $g_1 = f_1 B$ and $\det B = B$. Let $f \in R$ be such that $Bf = g_1 a$ for some $a \in R$. Multiplying by f_1, we obtain $g_1 f = g_1 f_1 a$. Since g_1 is regular in R, this implies $f = f_1 a$.

Case $s>1$. Let $f\in R$ be such that $(\det B)f\in(g_1,\dots,g_s)R$. The hypothesis that $f_1,\dots,f_s$ and $g_1,\dots,g_s$ are regular sequences implies that each associated prime ideal of $(f_1,\dots,f_s)R$ is a minimal prime over both ideals $(f_1,\dots,f_s)R$ and $(g_1,\dots,g_s)R$.

Thus, in order to show that $f\in(f_1,\dots,f_s)R$, it is sufficient to consider the case in which R is a local ring with maximal ideal $\mathrm{rad}(f_1,\dots,f_s)=\mathrm{rad}(g_1,\dots,g_s)$. In this case, there exist $N\in\mathbb{N}$ and a matrix $C\in R^{s\times s}$ such that

$$[f_1^N,\dots,f_s^N]=[g_1,\dots,g_s]C.$$

Therefore $[f_1^N,\dots,f_s^N]=[f_1,\dots,f_s]BC$. Since we already know that (i) $\Rightarrow$ (ii), we conclude that $(\det BC)f\in(f_1^N,\dots,f_s^N)R$. Hence the proof can be reduced to the case in which $g_1=f_1^N,\dots,g_s=f_s^N$. In this case the assumption (15) has the form

$$[f_1^N,\dots,f_s^N]=[f_1,\dots,f_s]B. \tag{16}$$

Let $c_1,\dots,c_s$ be the cofactors of B along its last row. Thus, if B_0 is the $(s-1)\times(s-1)$ matrix obtained by removing the last row and the last column from B, we see that $c_s=\det B_0$.

Let $\bar{R}:=R/f_sR$. For any element $a\in R$ denote by $\bar{a}$ the residual class of a in $\bar{R}$. Let $\bar{B}_0$ be the image of B_0 in $\bar{R}^{(s-1)\times(s-1)}$. One verifies immediately

$$[\bar{f}_1^N,\dots,\bar{f}_{s-1}^N]=[\bar{f}_1,\dots,\bar{f}_{s-1}]\bar{B}_0. \tag{17}$$

Now we show that $(\det\bar{B}_0)\bar{f}\in(\bar{f}_1^N,\dots,\bar{f}_{s-1}^N)$.

Since $B^{t}[c_1,\dots,c_s]={}^{t}[0,\dots,0,\det B]$, equation (16) implies that $c_1f_1^N+\cdots+c_sf_s^N=(\det b)f_s$. Therefore $(\det B-c_sf_s^{N-1})f_s\in(f_1^N,\dots,f_{s-1}^N)$. Hence $c_sff_s^{N-1}\in(f_1^N,\dots,f_s^N)$. Thus there exist $a_1,\dots,a_s\in R$ such that $(c_sf-a_sf_s)f_s^{N-1}=a_1f_1^N+\cdots+a_{s-1}f_{s-1}^N$. The regularity of $f_1^N,\dots,f_{s-1}^N,f_s$ implies that $c_sf-a_sf_s\in(f_1^N,\dots,f_{s-1}^N)$, i.e., $\bar{c}_s\bar{f}\in(\bar{f}_1^N,\dots,\bar{f}_{s-1}^N)$. This finishes the proof of $(\det\bar{B}_0)\bar{f}\in(\bar{f}_1^N,\dots,\bar{f}_{s-1}^N)$.

From the inductive hypothesis we conclude now that $\bar{f}\in(\bar{f}_1,\dots,\bar{f}_{s-1})$, whence $f\in(f_1,\dots,f_s)$. □

4.3. Corollary. *Let k be a field and $f_1,\dots,f_s\in k[X_1,\dots,X_n]$ be n-variate polynomials which form a complete intersection in A^n. Let $I:=(f_1,\dots,f_s)$ and let $f\in k[X_1,\dots,X_n]$.*

Then it can be decided in sequential time $(d^n+\deg(f))^{O(n)}$ and in parallel time $O(n^2\log^2(d^n+\deg(f))$ whether f belongs to I.

Proof. Apply the algorithm described in Section 1 to the sequence $f_1,\dots,f_s$. Compute $h,g_1,\dots,g_s$ of Theorem 4.1. For deciding whether f belongs to I test whether hf belongs to $(g_1,\dots,g_s)$ using (parallelizable) Hironaka division. The complexity bounds are immediate. □

5. The representation problem in the case of a complete intersection ideal

In this section we shall assume that the complete intersection condition (14) of

Section 4 holds. We are going to describe an algorithmic solution of the representation problem (RP) for this case. Our algorithm has simply exponential sequential and polynomial parallel complexity. This yields, in particular, a new algorithmic solution of (MP) different from the one described in Section 4. It is also parallelizable and requires only linear algebra techniques over k.

In the sequel we shall use the same notations as before.

5.1. Theorem (compare [8,2]). *Let $f \in R$ be given. Then the following conditions are equivalent:*

(i) $f \in I$;

(ii) *there exist* $a_1, \ldots, a_s \in R$ *such that* $f = \sum_{1 \le \mu \le s} a_\mu f_\mu$ *and* $\deg(a_\mu f_\mu) \le d^s + \deg(f)$ *for* $1 \le \mu \le s$.

Proof (Sketch). (i) $\Rightarrow$ (ii) The proof is essentially the same as the proof of [14, Théorème 1]. Thus we shall point out only the (slight) modifications one has to apply. We shall also adopt the notations introduced in the proof of Théorème 1 (loc.cit.). From the five steps ("étapes") which subdivide the proof of Théorème 1 (loc.cit.) we need only the second, the third and the fourth. The first step ("1ère étape") is obsolete since our polynomials $f_1, \ldots, f_s$ form a regular sequence.

Let $F \in k[X_0, \ldots, X_n]$ be the homogenization of f and let $G_1, \ldots, G_s \in k[X_0, \ldots, X_n]$ be the homogenizations of $f_1, \ldots, f_s$. As in the proof of Théorème 1 (loc.cit.), for $1 \le i \le s$ let B_i be the intersection of the primary ideals belonging to $(G_1, \ldots, G_i)$ whose radical doesn't contain X_0. The condition $f \in I$ implies $X_0^N F \in (G_1, \ldots, G_s)$ for some $N \in \mathbb{N}_0$. Thus $F \in B_s$.

The second and third step ("2ème" and "3ème étape") of the proof of Théorème 1 (loc.cit.) remain unchanged.

The fourth step ("4ème étape") must be modified as follows:

For $1 \le i \le s$ let $l_i, c_i, b_i, d_i \in \mathbb{N}_0$ be defined as in the proof of Théorème 1 (loc.cit.). In the same way as it is done there, inductively one constructs a sequence $R_s, R_{s-1}, \ldots, R_1$ of homogeneous polynomials such that, for $i = s, s-1, \ldots, 1$:

(a) $R_i \in B_i$,

(b) $\deg(R_i) = d_i + \deg(F)$,

(c) $R_i - X_0^{d_i} F \in (G_{i+1}, \ldots, G_s)$.

(Note that for $i = s$ (c) implies that R_s must be equal to F.)

For $i = 1$ one obtains that

$$R_1 - X_0^{d_1} F \in (G_2, \ldots, G_s).$$

Since $R_1 \in B_1 = (G_1)$, it follows that $X_0^{d_1} F \in (G_1, \ldots, G_s)$. Taking into account that $d_1 \le d^s$, one finishes the proof representing $X_0^d F$ as a homogeneous linear combination of $(G_1, \ldots, G_s)$ and specializing X_0 to 1. $\square$

For a more detailed proof we refer the reader to [8].

From Theorem 5.1 one deduces easily

5.2. Corollary. *Let k be a field and let $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ be n-variate polynomials with $d := \max_{1 \le \mu \le s} (\deg(f_\mu))$. Assume that $f_1, \ldots, f_s$ is a regular sequence in $k[X_1, \ldots, X_n]$.*

If $f \in (f_1, \ldots, f_s)$, then a representation $f = \sum_{1 \le \mu \le s} a_\mu f_\mu$ with $a_\mu \in k[X_1, \ldots, X_n]$ and $\deg(a_\mu f_\mu) \le d^s + \deg(f)$ for $1 \le \mu \le s$ can be found in sequential time $(dn + \deg(f))^{O(n)}$ and parallel time $O(n^2 \log^2(d^n + \deg(f))$.

Remark. The reader should observe that Corollary 5.2 does *not* imply that the construction of a Gröbner basis for *any* complete intersection ideal and *any* monomial order can be done in single exponential space (and time). In fact, one easily derives a counterexample from Mayr–Meyer's ideal (see [27]).

Acknowledgement

The authors L. Caniglia and J. Heintz from the working group Noaï Fitchas wish to express their gratitude to T. Mora, L. Robbiano from the University of Genova and to A. Logar from the University of Trieste for many fruitful discussions during their stay at the University of Genova in December 1988. They also thank the Dipartimento di Matematica of the University of Genova for its hospitality during this stay.

References

[1] M.F. Atiyah and I.G. McDonald, Introduction to Commutative Algebra (Addison-Wesley, Reading, MA, 1969).

[2] C.A. Berenstein and A. Yger, Bounds for the degrees in the division problem, Manuscript, University of Maryland (1988).

[3] S.J. Berkowitz, On computing the determinant in small parallel time using a small number of processors, Inform. Process. Lett. 18 (1984) 147–150.

[4] D. Brownawell, Bounds for the degree in the Nullstellensatz, Ann. of math. (2), 126 (1987) 577–591.

[5] B. Buchberger, An algorithm for finding a basis for the residue class ring of a zero dimensional polynomial ideal, Ph.D. Thesis, University of Innsbruck (1965) (in German).

[6] B. Buchberger, Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, Aequationes math. 4 (1970) 374–383.

[7] B. Buchberger, Gröbner-Bases: An algorithmic method in polynomial ideal theory, in: N.K. Bose, ed., Multidimensional System Theory (Reidel, Dordrecht, 1985) 184–232.

[8] L. Caniglia, Complejidad de algoritmos en Geometría Computacional, Ph.D. Thesis, Universidad de Buenos Aires (1989).

[9] L. Caniglia, A. Galligo and J. Heintz, Some new effectivity bounds in computational geometry, in: T. Mora, ed., AAECC-6, Proceedings 6th International Conference, Rome, 1988, Lecture Notes in Computer Science 357 (Springer, Berlin, 1989) 131–151.

[10] L. Caniglia, A. Galligo and J. Heintz, Borne simple exponentielle pour les degrés dans le théorèmes des zéros sur un corps de caractéristique quelconque, C.R. Acad. Sci. Paris Sér. I 307 (1988) 255–258.

[11] A.L. Chistov and D.Yu. Grigor'ev, Subexponential time solving systems of algebraic equations, LOMI Preprints E-9-83, E-10-83, Leningrad (1983).

[12] A. Dickenstein and C. Sessa, An effective residual criterion for the membership problem in $\mathbf{C}[z_1, \ldots, z_n]$, Manuscript (1988).

[13] J.C. Fangère, P. Gianni, D. Lazard and T. Mora, Efficient computation of zero dimensional Gröbner bases by change of ardering, J. Symbolic Comput., to appear.

[14] N. Fitchas and A. Galligo, Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel, Math. Nachr., to appear.

[15] A. Galligo, Algorithmes de construction de bases standards, Preprint, University of Nice (1985).

[16] J. von zur Gathen, Parallel arithmetic computations. A survey, in: Proceedings 13th Symposium MFCS 1986, Lecture Notes in Computer Science 233 (Springer, Berlin, 1986) 93–112.

[17] P. Gianni and T. Mora, Algebraic solution of polynomial equations using Groebner Bases, in: L. Huguet and A. Poli, eds., AAECC-5, Proceedings 5th International Conference, Menorca, 1987, Lecture Notes in Computer Science 356 (Springer, Berlin, 1989) 247–257.

[18] M. Giusti, Combinatorial dimension theory of algebraic varieties, J. Symbolic Comput. 6 (1988) 249–265.

[19] M. Giusti, Complexity of standard bases in projective dimension zero, in: J. Davenport, ed., EUROCAL '87, Leipzig, Lecture Notes in Computer Science 378 (Springer, Berlin, 1989) 333–335.

[20] J. Heintz, Definability and fast quantifier elimination over algebraically closed fields, Theoret. Comput. Sci. 24 (1983) 239–277; also: Kybernet. Sb., Novaja Ser. Vyp. 22 (1985) 113–158 (in Russian).

[21] J. Kollár, Sharp effective Nullstellensatz, J. Amer. Math. Soc. 1 (1988) 963–975.

[22] H. Kredel and V. Weispfenning, Computing dimension and independent sets of polynomial ideals, J. Symbolic Comput. 6 (1988) 231–247.

[23] D. Lazard, Algèbre linéaire sur $K[X_1, \ldots, X_n]$ et élimination, Bull. Soc. Math. France 105 (1977) 165–190.

[24] D. Lazard, Résolution des systèmes d'équations algébriques, Theoret. Comput. Sci. 15 (1981) 77–110.

[25] M. Lejeune-Jalabert, Effectivité de Calculs Polynomiaux, Cours de D.E.A., Institut Fourier, Université de Grenoble I (1985).

[26] A. Logar, A computational proof of the Noether's Normalization Lemma, in: T. Mora, ed., AAECC-6, Proceedings 6th International Conference, Rome, 1988, Lecture Notes in Computer Science 357 (Springer, Berlin, 1989) 259–273.

[27] E. Mayr and A. Meyer, The complexity of the word problem for commutative semigroups and polynomial ideals, Adv. in Math. 46 (1982) 305–329.

[28] K. Mulmuley, A fast parallel algorithm to compute the rank of a matrix over an arbitrary field, in: Proceedings 18th Annual ACM Symposium Theory of Computing (1986) 338–339.

[29] P. Philippon, Théorème des zéros effectif d'après J. Kollár, Séminaire I.H.P. (1988).

[30] I.R. Shafarevich, Algebraic Geometry (Springer, Berlin, 1974).