Intrinsic Complexity for Constructing Zero-Dimensional Gröbner Bases

Amir Hashemi[1,2(✉)], Joos Heintz[3], Luis M. Pardo[4], and Pablo Solernó[5]

[1] Department of Mathematical Sciences, Isfahan University of Technology, 84156-83111 Isfahan, Iran
amir.hashemi@iut.ac.ir
[2] School of Mathematics, Institute for Research in Fundamental Sciences (IPM), 19395-5746 Tehran, Iran
[3] Departamento de Computación and ICC, UBA-CONICET, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina
joos@dc.uba.ar
[4] Depto. de Matemáticas, Estadística y Computación. Facultad de Ciencias, Universidad de Cantabria, Avda. Los Castros s/n, 39071 Santander, Spain
luis.m.pardo@gmail.com
[5] Departamento de Matemática and IMAS, UBA-CONICET, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina
psolerno@dm.uba.ar

Abstract. In this paper, we give a thorough revision of Lakshman's paper by fixing some serious flaws in his approach. Furthermore, following this analysis, an intrinsic complexity bound for the construction of zero-dimensional Gröbner bases is given. Our complexity bound is in terms of the degree of the input ideal as well as the degrees of its generators. Finally, as an application of the presented method, we exhibit and analyze a (Monte Carlo) probabilistic algorithm to compute the degree of an equidimensional ideal.

1 Introduction

Gröbner bases, introduced by Bruno Buchberger in 1965 in his Ph.D. thesis [5] are a powerful tool for constructive problems in polynomial ideal theory. Using the linear algebra method proposed by Lazard [21] to compute Gröbner bases and by having the maximum degree of the intermediate polynomials during the Gröbner basis computation, we are able to give the complexity of this computation. In 1982, Mayr and Meyer [26] proved that, in the worst case, the maximum degree of a reduced Gröbner basis of an ideal may be double exponential in terms of the maximum degree of a generating set of the ideal. However, for the class of zero-dimensional ideals this upper bound becomes single exponential.

Let us recall some of the existing results on the complexity of computing zero-dimensional Gröbner bases. Let R be the polynomial ring $K[x_1, \ldots, x_n]$ and

F. Boulier et al. (Eds.): CASC 2020, LNCS 12291, pp. 245–265, 2020.
https://doi.org/10.1007/978-3-030-60026-6_14

$I \subset R$ a zero-dimensional ideal generated by polynomials of degree at most d. Let us fix a monomial ordering on R. Lazard in [22] showed that if the projective dimension of I is zero then the complexity of computing a Gröbner basis for I is $d^{O(n)}$. Then, Dickenstein et al. in [7] proved the complexity bound $d^{O(n^2)}$ for this problem. Lazard and Lakshman in [20] described a probabilistic algorithm to compute in time $d^{O(n)}$ Gröbner bases of the radical of I as well as of all the irreducible components of $\sqrt{I}$. Finally, based on this algorithm, Lakshman in [19] showed that the reduced Gröbner basis of I and reduced Gröbner bases for all primary components of I can be constructed in a time polynomial in d^n. Unfortunately, the approach presented in [19] has serious flaws which are investigated in this paper. In principle, there are several errors in [19] (as in Lemmata 1, 4 and 5), but the main doubt lies on the statement of [19, Theorem 2]. After fixing these flaws (by a thorough revision of the paper), based on Lakshman's method, we give new upper bounds for the complexity of computing reduced Gröbner bases for I and of the primary components of I. Our bound depends on the maximum degree of a generating set of I, the degree of I and degrees of the primary components of I. Finally, as an application of this approach, we present a probabilistic method to compute the degree of an equi-dimensional ideal and analyze its complexity.

The article is organized as follows. In the next section, we review the basic definitions and notations which will be used throughout. In Sect. 3, we revise the paper [19] in order to fix its flaws and improve its results. In the last section, we illustrate an application of the results obtained in Sect. 3 for computing the degree of an equidimensional ideal.

2 Preliminaries

In this section, we introduce basic notations and preliminaries (related to the Gröbner bases and degree of an ideal) needed in the subsequent sections. Let K be an infinite field, $X = X_1, \ldots, X_n$ be a sequence of variables and $R = K[X]$ be the polynomial ring over K. We consider polynomials $f_1, \ldots, f_k \in R$ and the ideal $\mathfrak{a} = (f_1, \ldots, f_k)$ generated by them (if the f_i's are homogeneous then we will stress it). Furthermore, the dimension of the ideal $\mathfrak{a}$, denoted by $\dim(\mathfrak{a})$, is the (Krull) dimension of the corresponding factor ring $A = R/\mathfrak{a}$.

We denote by $\mathscr{M}(X) = \{X_1^{\alpha_1} \cdots X_n^{\alpha_n} \mid (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}$ the set of all monomials in R. Let us fix a monomial ordering $\prec$ on $\mathscr{M}(X)$ with $X_1 \prec \cdots \prec X_n$. The *leading monomial* of a non-zero polynomial $f \in R$, denoted by $\mathrm{LM}(f)$, is the greatest monomial w.r.t. $\prec$ appearing in f and its coefficient is the leading coefficient of f, denoted by $\mathrm{LC}(f)$. The leading term of f is the product $\mathrm{LT}(f) = \mathrm{LC}(f)\mathrm{LM}(f)$. We denote by $t(f)$ the set of all monomials appearing in f. We denote by $\sharp t(f)$ the number of terms appearing in f. For a finite set F we write $\sharp t(F) = \max\{\sharp t(f) \mid f \in F\}$.

For every finite set F, we denote by $\mathrm{LM}(F)$ the set $\{\mathrm{LM}(f) \mid f \in F\}$. The *leading monomial monoid* of an ideal $\mathfrak{a} \subset R$ w.r.t. $\prec$ is defined as

$$\mathrm{LM}(\mathfrak{a}) = \{\mathrm{LM}(f) \mid 0 \neq f \in \mathfrak{a}\}.$$

For every non-zero polynomial $f \in R$, we denote by $\langle \mathrm{LM} \rangle(f)$ the set of all $\mathrm{LM}(f)X^\alpha$ with $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. We denote by $\langle \mathrm{LM} \rangle(F)$ the set monomials in the following class:

$$\langle \mathrm{LM} \rangle(F) = \bigcup_{f \in F} \langle \mathrm{LM} \rangle(f) = \bigcup_{f \in F} \mathrm{LM}(f) \cdot \mathscr{M}(X).$$

Recall that a finite subset $G \subset \mathfrak{a}$ is called a *Gröbner basis* for $\mathfrak{a}$ w.r.t. $\prec$ if $\mathrm{LM}(\mathfrak{a}) = \langle \mathrm{LM} \rangle(G)$. A Gröbner basis G is *minimal* if all leading coefficients of all polynomials in G are equal to 1 and that for all $f \in G$ we have $\mathrm{LM}(f) \notin \langle \mathrm{LM} \rangle(G \setminus \{f\})$. Computing a minimal Gröbner basis from a given Gröbner basis does not increase significantly the complexity of the computation. Finally, recall that a *reduced* Gröbner basis G of an ideal $\mathfrak{a}$ is a minimal Gröbner basis such that for every $f \in G$ no term of f lies in $\langle \mathrm{LM} \rangle(G \setminus \{f\})$.

A key ingredient of the computation of Gröbner bases is Hironaka's multivariate division algorithm, also called computation of a normal form (remainder) w.r.t. a finite set of polynomials (see [6, Theorem 3, page 64], and more precisely, Exercise 11, page 69). Let $F \subset R$ be a finite set of polynomials and $f \in R$. We will denote by $\mathrm{NF}(f, F)$ a remainder of the multi-variate division of f by F. Another relevant ingredient in the computation of Gröbner bases is the *S-polynomial*. For two non-zero polynomials $f, g \in R$, their S-polynomial is defined to be

$$S(f, g) = \frac{M}{\mathrm{LT}(f)} f - \frac{M}{\mathrm{LT}(g)} g, \tag{1}$$

where M is the least common multiple of $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$. In addition, $S(f, g, F)$ stands for a remainder of the Hironaka division of $S(f, g)$ by F. We also denote by $S(f, 0, F)$ a normal form of f w.r.t. F. *Buchberger's criterion* asserts that a finite set F is a Gröbner basis if and only if $S(f, g, F) = 0$ for all $f, g \in F$.

The *normal set* of an ideal $\mathfrak{a}$ w.r.t. $\prec$ is the set of all monomials not in $\mathrm{LM}(\mathfrak{a})$. For every finite subset $F \subset R$, we also denote by $N(F)$ the monomials not in $\langle \mathrm{LM} \rangle(F)$. Recall that an ideal $\mathfrak{a} \subset R$ is zero-dimensional if and only if $N(\mathfrak{a})$ is finite. Moreover, given a zero-dimensional ideal $\mathfrak{a} \subset R$ the residue classes $\{f + \mathfrak{a} \mid f \in N(\mathfrak{a})\}$ forms a basis for A as a K-vector space. Hence, if $\mathfrak{a}$ is zero-dimensional, we obviously have $\dim_K(R/\mathfrak{a}) = \sharp N(\mathfrak{a})$. For more details, we refer the reader to [6].

Let E be an $\mathbb{N}$-graded R-module. Given any $s \in \mathbb{N}$, we denote by E_s the union of $\{0\}$ and the set of the elements of E of degree s. Recall that the *Hilbert function* of $\mathfrak{a}$ is defined by $\mathrm{HF}_\mathfrak{a}(s) = \dim_K(R_s/\mathfrak{a}_s)$. From a certain degree, this function of s is equal to a (unique) polynomial in s, called the *Hilbert polynomial*, and is denoted by $\mathrm{HP}_\mathfrak{a}$. The *Hilbert series* of $\mathfrak{a}$ is the following power series

$$\mathrm{HS}_\mathfrak{a}(t) = \sum_{s=0}^{\infty} \mathrm{HF}_\mathfrak{a}(s) t^s.$$

By the Hilbert-Serre theorem, we know that the Hilbert series of $\mathfrak{a}$ may be written as $p(t)/(1-t)^r$ where $r = \dim(\mathfrak{a})$ and $p(1) \neq 0$. Let us recall the definitions of the degree of a homogeneous ideal, see e.g. [36, page 43] and [4].

Definition 1. *Suppose that* $\mathfrak{a}$ *is a homogeneous ideal with* $r = \dim(\mathfrak{a})$. *If* $r > 0$, *the (homogeneous)* degree *of* $\mathfrak{a}$, *denoted by* $\deg(\mathfrak{a})$, *is* $(r-1)!$ *times the leading coefficient of the Hilbert polynomial of* $\mathfrak{a}$. *If* $r = 0$, *the degree of* $\mathfrak{a}$ *is the sum of the coefficients of* $\mathrm{HS}_{\mathfrak{a}}(t)$.

By [18, page 173], we have $\deg(\mathfrak{a}) = p(1)$ and in consequence since $\mathfrak{a}$ and $\mathrm{LM}(\mathfrak{a})$ share the same Hilbert function, $\deg(\mathfrak{a}) = \deg(\langle \mathrm{LM} \rangle(\mathfrak{a}))$. Now, let us turn our attention to the relation between the degrees of an ideal and its primary components. Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. The *length* of $\mathfrak{q}$, denoted by $\ell(\mathfrak{q})$, is the maximum length ℓ of a chain $\mathfrak{q} = \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_\ell = \mathfrak{p}$ of primary ideals. Note that ℓ is the length of the Artinian local ring $(R/\mathfrak{q})_{\mathfrak{p}}$. With these notations, we have $\deg(\mathfrak{q}) = \ell \deg(\mathfrak{p})$. The degree of a homogeneous ideal $\mathfrak{a}$ equals to the sum of the degrees of its primary components of dimension $\dim(\mathfrak{a})$. Let $\mathfrak{m} \subset R$ be a maximal ideal and $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal. Then, $\deg(\mathfrak{q}) = \dim_K(R/\mathfrak{q})$. If $\mathfrak{a} \subset R$ is a zero-dimensional ideal then we have

$$\deg(\mathfrak{a}) = \sum_{i=1}^{m} \deg(\mathfrak{q}_i),$$

where $\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i$ is the irredundant primary decomposition of $\mathfrak{a}$. We conclude this section, by defining the degree of a non-necessarily homogeneous zero-dimensional ideal $\mathfrak{a} \subset R$. Let ${}^hR$ be the ring $K[X_0, X_1, \ldots, X_n]$ where X_0 is a new variable. For any polynomial $f \in R$, we define its *homogenization* to be ${}^hf = X_0^{\deg(f)} f(X_1/X_0, \ldots, X_n/X_0) \in {}^hR$. Furthermore, we define ${}^h\mathfrak{a} = ({}^hf \mid f \in \mathfrak{a}) \subset {}^hR$. It is clear that $\dim({}^h\mathfrak{a}) = 1$. Then, we define $\deg(\mathfrak{a})$ to be $\deg({}^h\mathfrak{a})$. If $\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i$ is the irredundant primary decomposition of a zero-dimensional ideal $\mathfrak{a}$ then ${}^h\mathfrak{q}_1 \cap \cdots \cap {}^h\mathfrak{q}_m$ is an irredundant primary decomposition of ${}^h\mathfrak{a} \subset {}^hR$ and $\dim({}^h\mathfrak{q}_i) = 1$ for each i. In addition, since homogenization of a primary (resp. prime) ideal remains primary (resp. prime) ideal, we conclude that the length of a primary ideal remains stable after homogenization, see e.g. [38, Chapter VII, Theorem 17]. These arguments yield $\deg(\mathfrak{a}) = \sum_{i=1}^{m} \deg(\mathfrak{q}_i) = \sum_{i=1}^{m} \ell_i \deg(\mathfrak{p}_i)$ where $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary and $\ell_i = \ell(\mathfrak{q}_i)$. Finally, if $\ell(\mathfrak{a})$ stands for $\max\{\ell_1, \ldots, \ell_m\}$ then we have trivially, $\max\{\ell(\mathfrak{a}), m\} \leq \deg(\mathfrak{a})$.

3 A Thorough Revision of Lakshman's Paper

In this section, we make a thorough revision of the paper [19] by Lakshman with special focus on fixing its serious flaws. In addition, using this approach we will present intrinsic complexity bounds for computing Gröbner bases of a zero-dimensional ideal and for all its primary components.

Indeed, there are some flaws in the intermediate statements leading to [19, Theorem 2]. Firstly, in Lemma 1, Lakshman claims that some sequence of ideals is increasing, which is obviously wrong since it is, in fact, a decreasing sequence of ideals. This error may be fixed without any effort. Secondly,

Lemmata 4 and 5 are directly false since he assumes that the index of a primary zero-dimensional ideal agrees with its length and this is not always true (see Corollary 10 below for an obvious counterexample). Lakshman's bound in Lemma 4 must be replaced by what we exhibit in Lemma 15 below. This modifies [19, Lemma 5] making it doubtful and somehow misleading. Not only because of this confusion between index and length, but also because [19] omits a lot of relevant material to bound the arithmetic complexity of the algorithm. The correction of Lemma 5 in [19] now becomes Lemma 16 and none of the bounds we have found agrees with the bounds exhibited by Lakshman in his paper.

Next, [19, Lemma 6] contains the main flaw. The author assumes that the number of field operations required to compute a normal form w.r.t. a finite set F only depends on the number of polynomials in F and the number of non-zero terms involved. As far as we know, no proof of this fact is known. This was the reason to introduce the function $\mathscr{T}_S$ in Definition 5. In addition, this forces us to make a thorough revision of his Lemma 6 and leads to Theorem 17 which summarizes our study of the complexity of Lakshman's algorithm. Finally, [19, Theorems 2 and 3] can be replaced by Corollaries 18 and 22, respectively.

3.1 Complexity of Converting Gröbner Bases

In this subsection, we give the complexity of converting a given Gröbner basis of a zero-dimensional ideal into the reduced Gröbner basis for the same ideal with respect to the same monomial order (see Corollary 7). We first fix a monomial order $\prec$ on R. For a polynomial $f \in R$, we denote by $\deg_{X_i}(f)$ the degree of f w.r.t. the variable X_i.

Lemma 2. *Let $\mathfrak{a} \subset R$ be a zero-dimensional ideal and $F \subset \mathfrak{a}$ be a finite set of generators of $\mathfrak{a}$ (although not necessarily a Gröbner basis for $\mathfrak{a}$). Assume that $N(F)$ is a finite set. Then, for all $S \subseteq \{1, \ldots, n\}$, such that $\sharp S \leq n-1$, there is some $f \in F$ such that $\deg_{X_i}(\mathrm{LM}(f)) = 0$ for all $i \in S$.*

Proof. Let $\mathscr{M}_S(X) = \{\prod_{k \notin S} X_k^{\alpha_k} \mid \alpha_k \in \mathbb{N}\}$. Since $\sharp S \leq n-1$ then $\mathscr{M}_S(X)$ is infinite and it is not completely included in $N(F)$, because $N(F)$ is a finite set. Thus, there must be some $m = \prod_{k \notin S} X_k^{\alpha_k} \in \mathscr{M}_S(X)$ such that $m \notin N(F)$. Thus

$$m \in \bigcup_{f \in F} \langle \mathrm{LM} \rangle (f),$$

which implies that exists some $f \in F$ such that $\mathrm{LM}(f)$ divides m. Hence, for any $i \in S$, no non-zero power of X_i may divide $\mathrm{LM}(f)$ and, thus $\deg_{X_i}(\mathrm{LM}(f)) = 0$ for all $i \in S$. □

This lemma implies the following result.

Lemma 3. *With the same hypothesis as in Lemma 2, for every monomial $m \in N(F)$ and for each $1 \leq i \leq n$ we have $\deg_{X_i}(m) < \max\{\deg_{X_i}(f) \mid f \in F\}$.*

Proof. Let $m = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in N(F)$ and $d_i = \max\{\deg_{X_i}(\mathrm{LM}(f)) \mid f \in F\}$ for each i. Consider the sets $T = \{k \in \{1, \ldots, n\} \mid d_k \leq \alpha_k\}$ and $S = \{1, \ldots, n\} \setminus T$. Reasoning by reductio ad absurdum assume that $T \neq \emptyset$. Thus, $\sharp S \leq n - 1$ and from Lemma 3, there is $f \in F$ with $\deg_{X_i}(\mathrm{LM}(f)) = 0$, $\forall i \in S$. Thus, we conclude that $\mathrm{LM}(f)$ has the form $\prod_{k \in T} X_k^{\beta_k}$. Then, as d_k is maximal, $\beta_k \leq d_k$, for all $k \in T$ and, hence, $\mathrm{LM}(f) = \prod_{k \in T} X_k^{\beta_k} \mid \prod_{k \in T} X_k^{d_k}$. On the other hand $\prod_{k \in T} X_k^{d_k} \mid m$ which implies that $\mathrm{LM}(f)$ divides m, leading to a contradiction. It follows that $T = \emptyset$ and this yields the claim. □

Next, let us consider $\mathfrak{a} \subset R$ an arbitrary zero-dimensional ideal and let $G = \{f_1, \ldots, f_s\}$ be a minimal Gröbner basis of $\mathfrak{a}$ w.r.t. $\prec$. As G is minimal, we may assume that

$$\mathrm{LM}(f_s) \prec \cdots \prec \mathrm{LM}(f_1). \tag{2}$$

Now, we transform the elements in G as follows. Let $h_i = f_i - \mathrm{LT}(f_i)$ for $1 \leq i \leq s$. Due to (2), every monomial in h_i is strictly smaller than any leading monomial of f_k for all k satisfying $1 \leq k \leq i$. Let $\widetilde{h_i} = \mathrm{NF}(h_i, \{f_{i+1}, \ldots, f_s\})$ and $\widetilde{f_i} = \mathrm{LT}(f_i) + \widetilde{h_i}$. We have the following statement.

Lemma 4. *With these notations and assumptions, we have:*

i) $\mathrm{LM}(\widetilde{f_i}) = \mathrm{LM}(f_i)$ *and* $\widetilde{G} = \{\widetilde{f_1}, \ldots, \widetilde{f_s}\}$ *is the reduced Gröbner basis of* $\mathfrak{a}$.
ii) Any monomial in $t(\widetilde{h_i})$ *lies in* $N(\mathfrak{a})$ *and* $\sharp t(\widetilde{h_i}) \leq \sharp N(\mathfrak{a})$.
iii) The number of non-zero terms of every element of $\widetilde{G}$ *is at most* $\sharp N(\mathfrak{a}) + 1$.

Proof. The results are folklore from the theory of Gröbner bases, see e.g. [6]. □

Definition 5. *Let* $\mathscr{T}_S(n, t, k, D)$ *be an upper bound over the number of arithmetic operations of elements in the field* K *required to compute* $S(f, g, F)$ *where*

i) F *generates a zero-dimensional ideal,* $\sharp F \leq k$ *and* $N(F)$ *is finite,*
ii) the number of non-zero terms of any polynomial in $\{f, g\} \cup F$ *is at most* t,
iii) the maximum of the degrees of the polynomials in $\{f, g\} \cup F$ *is at most* D.

Note that $\mathscr{T}_S(n, t, k, D)$ is assumed to be also a bound for the number of arithmetic operations required to compute a normal form $\mathrm{NF}(f, F) = S(f, 0, F)$, provided that f and F satisfy the required conditions.

Remark 6. The bound $\mathscr{T}_S(n, t, k, D)$ is known to be finite, as we have

$$\mathscr{T}_S(n, t, k, D) \in O\left(nt \log(D) \left(tk \binom{D+n}{n}\right)^{\omega}\right)$$

where $\omega < 2.373$ is the exponent of the complexity of matrix multiplication, see [23]. Other bounds under different assumptions can be found in the literature. It is worth noting that van der Hoeven in [34] by using the concepts of *relaxed power series* and *fast sparse polynomial arithmetic* described a fast algorithm for sparse reduction of a polynomial w.r.t. an autoreduced set of polynomials.

Corollary 7. *Let $\mathfrak{a}$ be a zero-dimensional ideal. The computation of the reduced Gröbner basis G_{red} from a Gröbner basis G of $\mathfrak{a}$ can be done in a number of arithmetic operations in K which is bounded by the following quantity:*

$$O\left(\sharp G\left(n\sharp t(G)+\mathscr{T}_S\left(n,\sharp t(G),\sharp G,D\right)\right)\right)$$

where D is is an upper bound for the degrees of the polynomials in G.

Proof. To compute the reduced Gröbner basis, we first compute a minimal Gröbner basis $G_{\min}$ from G. In doing so, let us sort $G=\{f_1,\ldots,f_s\}$ and remove all f_i with $\mathrm{LM}(f_i)=\mathrm{LM}(f_{i-1})$ to obtain a subset $G_1=\{g_1,\ldots,g_r\}\subseteq G$ such that the $\mathrm{LM}(g_r)\prec\cdots\prec\mathrm{LM}(g_1)$. Then, we eliminate from G_1 all those g_i's such that $\mathrm{LM}(g_i)$ is divisible by some $\mathrm{LM}(g_k)$ with $k>i$. The final result is a minimal Gröbner basis $G_{\min}$. This can be done, obviously in a time linear in n, $\sharp G$ and $\sharp t(G)$ (note that checking the divisibility of two monomials needs n comparisons, and we consider each comparison as a field operation). Now, taking $G_{\min}$ we proceed as explained above to get a reduced Gröbner basis. The total operations performed by this procedure depends polynomially on the number of elements in $G_{\min}$ and the cost of performing the corresponding reductions. But, each normal form computation is performed in a number of field operations bounded by $\mathscr{T}_S\left(n,\sharp t(G),\sharp(G),D\right)$, thus proving the corollary. □

3.2 Complexity of Computing the Primary Decomposition

In this subsection, we present the complexity of computing a Gröbner basis for a primary component of a zero-dimensional ideal under suitable assumptions of genericity (see Corollary 18). Then, we apply this result to prove our main result about the complexity of computing reduced Gröbner bases for zero-dimensional ideals (see Corollary 22). Let us first define the index of a primary ideal.

Definition 8. *Let $\mathfrak{p}\subset R$ be a prime ideal and $\mathfrak{q}$ a $\mathfrak{p}$-primary ideal. We define the index of $\mathfrak{q}$ as the minimum positive integer $\mathrm{Ind}(\mathfrak{q})=\rho$ such that $\mathfrak{p}^\rho\subseteq\mathfrak{q}$.*

Observe that in any Noetherian ring (in particular, in R) the index of a primary ideal is always well-defined. We then fix a zero-dimensional ideal $\mathfrak{a}\subset R$. Recall that $\mathfrak{a}$ is zero-dimensional if and only if every associated prime of $\mathfrak{a}$ is maximal in R. The following classical statement may be seen in [35].

Lemma 9. *Let $\mathfrak{a}$ be a zero-dimensional ideal as above. Let $\mathfrak{p}\subset R$ be an associated prime of $\mathfrak{a}$ and $\mathfrak{q}$ a $\mathfrak{p}$-primary ideal occurring in a minimal primary decomposition of $\mathfrak{a}$. Let ρ be the index of $\mathfrak{q}$. Then, the following properties hold:*

i) if $\sigma<\rho$ then $\dim_K(R/(\mathfrak{a}+\mathfrak{p}^{\sigma-1}))<\dim_K(R/(\mathfrak{a}+\mathfrak{p}^\sigma))$,
ii) if $\sigma\geq\rho$ then $\mathfrak{q}=\mathfrak{a}+\mathfrak{p}^\rho=\mathfrak{a}+\mathfrak{p}^\sigma$.

Namely, the index of a $\mathfrak{p}$-primary ideal $\mathfrak{q}$ occurring in a minimal primary decomposition of a zero-dimensional ideal $\mathfrak{a}$ is the minimal positive integer ρ such that $\mathfrak{a}+\mathfrak{p}^\rho=\mathfrak{a}+\mathfrak{p}^{\rho+1}$ and, in this case, $\mathfrak{q}=\mathfrak{a}+\mathfrak{p}^\rho$. This is the key ingredient of the Lakshman algorithm in [19].

Corollary 10. *With these notations, let* $\mathfrak{a} \subset R$ *be a zero-dimensional ideal,* $\mathfrak{q}$ *an isolated* $\mathfrak{p}$*-primary component of* $\mathfrak{a}$*. Then,*

i) $\mathrm{Ind}(\mathfrak{q}) \leq \ell(\mathfrak{q})$*, see also [4, Lemma 1]. In particular,* $\mathrm{Ind}(\mathfrak{q})\deg(\mathfrak{p}) \leq \deg(\mathfrak{q})$.
ii) $\ell(\mathfrak{q})$ *is an upper bound for the minimal positive integer* $\rho \in \mathbb{N}$ *such that*

$$\mathfrak{a} + \mathfrak{p}^{\rho} = \mathfrak{a} + \mathfrak{p}^{\rho+1}.$$

Proof. Let $\rho = \mathrm{Ind}(\mathfrak{q})$ be the index of $\mathfrak{q}$. Then, according to Claim i) of Lemma 9, for every $\sigma < \rho$, the ideal $\mathfrak{a} + \mathfrak{p}^{\sigma}$ satisfies $\mathfrak{p} = \sqrt{\mathfrak{q}} = \sqrt{\mathfrak{a} + \mathfrak{p}^{\rho}} \subseteq \sqrt{\mathfrak{a} + \mathfrak{p}^{\sigma}} \subseteq \mathfrak{p}$. Hence, $\sqrt{\mathfrak{a} + \mathfrak{p}^{\sigma}} = \mathfrak{p}$ for every $\sigma < \rho$. Thus, $\mathfrak{a} + \mathfrak{p}^{\sigma}$ is a $\mathfrak{p}$-primary ideal. Claim i) of Lemma 9 implies that the following is a chain of $\mathfrak{p}$-primary ideals with strict inclusions:

$$\mathfrak{q} = \mathfrak{a} + \mathfrak{p}^{\rho} \subsetneq \mathfrak{a} + \mathfrak{p}^{\rho-1} \subsetneq \cdots \subsetneq \mathfrak{a} + \mathfrak{p}^{2} \subsetneq \mathfrak{a} + \mathfrak{p} = \mathfrak{p}$$

and, hence, $\mathrm{Ind}(\mathfrak{q}) \leq \ell(\mathfrak{q})$ as claimed. Since $\deg(\mathfrak{q}) = \ell(q)\deg(\mathfrak{p})$, it follows that $\mathrm{Ind}(\mathfrak{q})\deg(\mathfrak{p}) \leq \deg(\mathfrak{q})$.

Finally, Claim ii) of the statement immediately follows from Claim ii) of Lemma 9. □

Example 11. This example shows that the equality $\mathrm{Ind}(\mathfrak{q}) = \ell(\mathfrak{q})$ in Claim i) of Corollary 10 does not hold in general: let $R = K[x_1, x_2]$, $\mathfrak{p} = (x_1, x_2)$ and $\mathfrak{q}$ the $\mathfrak{p}$-primary ideal given by $\mathfrak{q} = \mathfrak{p}^4$. We can see easily that $\deg(\mathfrak{p}) = 1$ and $\mathrm{Ind}(\mathfrak{q}) = \rho = 4$. It is obvious that a basis of $R/\mathfrak{q}$ as a K-vector space is determined by all the monomials of degree at most 3, hence yielding $\ell(\mathfrak{q}) = 10 > \mathrm{Ind}(\mathfrak{q}) = 4$.

Now, we recall Lakshman's main algorithm to compute a Gröbner basis of an isolated primary component $\mathfrak{q}$ of a zero-dimensional ideal $\mathfrak{a}$, provided that we are given a finite set of generators of $\mathfrak{a}$ and the reduced Gröbner basis of the corresponding associated prime $\mathfrak{p}$.

Algorithm 1. PrimaryComponent

Input: A finite generating set F of a zero-dimensional ideal $\mathfrak{a}$ and the reduced Gröbner basis G of the associated prime $\mathfrak{p}$ of $\mathfrak{a}$
Output: The reduced Gröbner basis of the $\mathfrak{p}$-primary component $\mathfrak{q}$ of $\mathfrak{a}$

```
C := F
B := G                                  ▷ The reduced Gröbner basis of a + p = p.
while B ≠ C do
    C := B                  ▷ B is the reduced Gröbner basis of some a + p^σ, for σ < Ind(q).
    B := The reduced Gröbner basis of the ideal generated by F ∪ B · G
                            ▷ B becomes the reduced Gröbner basis of a + p · (a + p^σ) = a + p^(σ+1).
end while
return (B)
```

Lemma 12. *Algorithm 1 computes the reduced Gröbner basis of the isolated primary component* $\mathfrak{q}$*. The number of reduced Gröbner basis calculations (i.e. the number of times the procedure enters in the* **while***-loop) is at most* $\mathrm{Ind}(\mathfrak{q}) \leq \ell(\mathfrak{q})$.

Proof. Both claims are obvious in view of Corollary 10. □

The complexity analysis then depends on the complexity of computing the reduced Gröbner basis inside each **while**-loop. Let $\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i$ be an irredundant primary decomposition of a zero-dimensional ideal $\mathfrak{a}$ where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary for each i. From now on, we assume that the variables $X_1, \ldots, X_n$ are in generic position w.r.t. $\sqrt{\mathfrak{a}} = \cap_{i=1}^{m} \mathfrak{p}_i$. More precisely, we assume that there are $h_1, \ldots, h_n \in K[X_1]$ such that

$$\sqrt{\mathfrak{a}} = (X_n - h_n(X_1), \ldots, X_2 - h_2(X_1), h_1(X_1))$$

where $\deg(h_i) \leq \deg(h_1) - 1$ for each $2 \leq i \leq n$, and $\deg(h_1) = \deg(\sqrt{\mathfrak{a}}) = \sum_{i=1}^{m} \deg(\mathfrak{p}_i)$. We refer to this property as $\sqrt{\mathfrak{a}}$ being in *normal* X_1*-position*. This may be achieved by a generic linear change of coordinates to transform $\sqrt{\mathfrak{a}}$ into this position, see e.g. [13]. Now, let $\mathfrak{q}$ be a $\mathfrak{p}$-primary component of $\mathfrak{a}$. The generic change of variables is also well suited for each of its associated primes and, hence, we may assume that

$$\mathfrak{p} = (X_n - g_n(X_1), \ldots, X_2 - g_2(X_1), g_1(X_1)), \tag{3}$$

where $\deg(g_i) \leq \deg(\mathfrak{p}) - 1$ for each $2 \leq i \leq n$, and $\deg(g_1) = \deg(\mathfrak{p})$. Observe that g_1 is some irreducible factor of h_1 in $K[X_1]$ and for $2 \leq i \leq n$, we have $g_i = \mathrm{rem}(h_i, g_1)$ is the remainder of the division of h_i by g_1, see [1, Proposition 8.69] for more details. According to the comments introduced in Algorithm 1, the procedure computes reduced Gröbner bases of all $\mathfrak{p}$-primary ideals $\mathfrak{h}_i = \mathfrak{a} + \mathfrak{p}^i$ where $1 \leq i \leq \mathrm{Ind}(\mathfrak{q}) \leq \ell(\mathfrak{q})$. Let us also denote by B_i the reduced Gröbner basis of $\mathfrak{h}_i$ computed in the course of Algorithm 1. The following statement was proved in [19, Lemma 2].

Lemma 13. *With the same notations as above, let B_i be the reduced Gröbner basis of $\mathfrak{h}_i$ computed by Algorithm 1. Let $\delta = \deg(\mathfrak{p})$ be the degree of the prime ideal $\mathfrak{p}$ associated to $\mathfrak{a}$. Then, all leading monomials in B_i are of the form $(X_1^{\delta})^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ with $i_j \geq 0$.*

Let $m \in R$ be a monomial which belongs to the normal set $N(\mathfrak{h}_i) = \mathscr{M}(X) \setminus \mathrm{LM}(\mathfrak{h}_i)$ of some intermediate primary ideal $\mathfrak{h}_i$ computed by Algorithm 1. Define the *class* m of all monomials associated to m w.r.t. $\mathfrak{h}_i$ as:

$$\mathrm{Cl}_{\mathfrak{h}_i}(m) = \{m, X_1 m, \ldots, X_1^{\delta-1} m\}.$$

The following lemma resumes the main properties of these classes.

Lemma 14. *Let $m = (X_1^{\delta})^{j_1} X_2^{j_2} \cdots X_n^{j_n}$ and $m' = (X_1^{\delta})^{j'_1} X_2^{j'_2} \cdots X_n^{j'_n}$ be two monomials. Then, the following statements hold.*

i) If $m \in N(\mathfrak{h}_i)$ then $\mathrm{Cl}_{\mathfrak{h}_i}(m) \subseteq N(\mathfrak{h}_i)$.
ii) Given $m, m' \in N(\mathfrak{h}_i)$ as above, we have:

$$\mathrm{Cl}_{\mathfrak{h}_i}(m) \cap \mathrm{Cl}_{\mathfrak{h}_i}(m') \neq \emptyset \Longleftrightarrow \mathrm{Cl}_{\mathfrak{h}_i}(m) = \mathrm{Cl}_{\mathfrak{h}_i}(m') \Longleftrightarrow m = m'.$$

iii) The number of classes of equivalence $\mathrm{Cl}_{\mathfrak{h}_i}(m)$ *is at most* $\ell = \ell(\mathfrak{q})$.

In particular, the set of classes $\mathrm{Cl}_{\mathfrak{h}_i}(m)$ *defines a partition of* $N(\mathfrak{h}_i)$. *Namely, there is a finite set of monomials* $m_1, \ldots, m_L \in N(\mathfrak{h}_i)$ *of the form*

$$m_r = (X_1^{\delta})^{j_{r,1}} n_r, \tag{4}$$

where $n_r \in K[X_2, \ldots, X_n]$ *are monomials such that*

$$N(\mathfrak{h}_i) = \bigcup_{r=1}^{L} \mathrm{Cl}_{\mathfrak{h}_i}(m_r) \tag{5}$$

is a disjoint decomposition of $N(\mathfrak{h}_i)$ *with* $L \leq \ell(\mathfrak{q})$.

Proof. As B_i is the reduced Gröbner basis of $\mathfrak{h}_i$, then by Lemma 13 we may assume that $\mathrm{LM}(B_i)$ has the form

$$\mathrm{LM}(B_i) = \{(X_1^{\delta})^{i_1} u_1, \ldots, (X_1^{\delta})^{i_t} u_t\},$$

where $t \in \mathbb{N}$ and $u_k \in K[X_2, \ldots, X_n]$ are monomials. Consequently, we have:

$$\mathrm{LM}(\mathfrak{h}_i) = \bigcup_{k=1}^{t} (X_1^{\delta})^{i_k} u_k \cdot \{X_1^{\mu_1} \cdots X_n^{\mu_n} \mid (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n\}.$$

Now, to prove Claim i), assume in contrary that for some $0 \leq r \leq \delta - 1$, we have $X_1^r m \in \mathrm{Cl}_{\mathfrak{h}_i}(m) \cap \mathrm{LM}(\mathfrak{h}_i)$. Then, there exist some k and some $a \in \mathbb{N}$ with

$$X_1^{\delta j_1 + r} = X_1^{\delta i_k + a} \text{ and } u_k \mid X_2^{j_2} \cdots X_n^{j_n}.$$

Thus, we must have $i_k \leq j_1$ and in turn $(X_1^{\delta})^{i_k} u_k \mid (X_1^{\delta})^{j_1} X_2^{j_2} \cdots X_n^{j_n} \in N(\mathfrak{h}_i)$ which is impossible and this proves Claim i).

As for Claim ii), assume that there exist r, r' with $0 \leq r, r' \leq \delta - 1$ such that:

$$X_1^r m = X_1^{r'} m' \in \mathrm{Cl}_{\mathfrak{h}_i}(m) \cap \mathrm{Cl}_{\mathfrak{h}_i}(m') \neq \emptyset.$$

Assume that $r' \geq r$, then we have $m = X_1^{r'-r} m' \in \mathrm{Cl}_{\mathfrak{h}_i}(m')$. It follows that $\delta j_1 = \delta j_1' + (r' - r)$ which implies $\delta \mid r' - r$, and $0 \leq r' - r < \delta$. Thus $r = r'$ and, hence, $m = m'$, proving Claim ii).

Assume $m_1, \ldots, m_L$ is a sequence of monomials with $\bigcup_{k=1}^{L} \mathrm{Cl}_{\mathfrak{h}_i}(m_k) \subseteq N(\mathfrak{h}_i)$ where the union is a disjoint union of sets of cardinality δ. Hence, we have

$$\sharp \bigcup_{k=1}^{L} \mathrm{Cl}_{\mathfrak{h}_i}(m_k) = \sum_{k=1}^{L} \sharp \mathrm{Cl}_{\mathfrak{h}_i}(m_k) = L\delta \leq \sharp N(\mathfrak{h}_i) = \deg(\mathfrak{h}_i) \leq \deg(\mathfrak{q}) = \ell(\mathfrak{q}) \deg(\mathfrak{p})$$

and so, $L \leq \ell(\mathfrak{q})$, because $\delta = \deg(\mathfrak{p})$ and this shows Claim iii). Finally, let $u = X_1^{t_1} X_2^{t_2} \cdots X_n^{t_n} \in N(\mathfrak{h}_i)$. Let $i_1, r \in \mathbb{N}$ be the quotient and the remainder of the Euclidean division of t_1 by δ. Let us define $v = (X_1^{\delta})^{i_1} X_2^{t_2} \cdots X_n^{t_n}$. Thus, we have $u = X_1^r v \in \mathrm{Cl}_{\mathfrak{h}_i}(v)$: if $v \in \mathrm{LM}(\mathfrak{h}_i)$, then $u \in \mathrm{LM}(\mathfrak{h}_i)$ which is impossible; hence $v \in N(\mathfrak{h}_i)$ and therefore $u \in \mathrm{Cl}_{\mathfrak{h}_i}(v)$. □

The following lemma is the corrected version of [19, Lemma 4] in which we replace the index of a primary component by its length.

Lemma 15. *With the same notations as above, let G be the reduced Gröbner basis of $\mathfrak{p}$ w.r.t $\prec$. Let B_i be the reduced Gröbner basis for $\mathfrak{h}_i$ w.r.t $\prec$ computed by Algorithm 1. Then, $\sharp\mathrm{LM}(G \cdot B_i) \leq n^2\ell$ and $\sharp N(G \cdot B_i) \leq (n+1)\ell\delta$.*

Proof. Let $m_1, \ldots, m_L \in N(\mathfrak{h}_i)$ be the monomials described in Equality (5). By Claim i) of Lemma 14, for all r and for all k with $0 \leq k \leq \delta - 1$, we have $X_1^k m_r \in N(\mathfrak{h}_i)$. Let $m = (X_1^\delta)^{i_1} X_2^{i_2} \cdots X_n^{i_n} \in \mathrm{LM}(B_i)$ with $i_k \geq 0$. Two cases may happen: if $i_1 \geq 1$, then $m/X_1^\delta = (X_1^\delta)^{i_1 - 1} X_2^{i_2} \cdots X_n^{i_n} \in N(\mathfrak{q}_i)$. Then, there would exist r and k with $0 \leq k \leq \delta - 1$, such that $m/X_1^\delta = X_1^k m_r$. According to Equality (4) of Lemma 14, $m_r = (X_1^\delta)^{j_{r,1}} n_r$, where $n_r \in K[X_2, \ldots, X_n]$. Then,

$$(X_1^\delta)^{i_1} X_2^{i_2} \cdots X_n^{i_n} = m = X_1^k X_1^\delta m_r = X_1^k (X_1^\delta)^{j_{r,1}+1} n_r.$$

We conclude that $k = 0$ and, hence, $m/X_1^\delta = m_r$. Otherwise, if $i_1 = 0$, then $m = X_2^{i_2} \cdots X_n^{i_n} \in \mathrm{LM}(B_i)$ is not a constant. Thus, there exist some k with $2 \leq k \leq n$, such that $M/X_k = X_2^{i_2} \cdots X_k^{i_k - 1} \cdots X_n^{i_n} \in N(\mathfrak{h}_i)$. The same argument used in the case $i_1 \geq 1$ applies to conclude that there must be some r with $1 \leq r \leq L$, such that $m/X_k = m_r$. In conclusion, we have proved the inclusion:

$$\mathrm{LM}(B_i) \subseteq \{X_1^\delta m_r \ : \ 1 \leq r \leq L\} \bigcup \left(\bigcup_{k=2}^{n} \{X_k m_r \ : \ 1 \leq r \leq L\} \right). \tag{6}$$

According to Lemma 14, we conclude that $\sharp\mathrm{LM}(B_i) \leq nL \leq n\ell$. Moreover, as B_i is reduced, then $\sharp B_i = \sharp\mathrm{LM}(B_i) \leq n\ell$. From Equality (3) we know that the Gröbner basis G of $\mathfrak{p}$ has n elements. This yields $\sharp\mathrm{LM}(G \cdot B_i) \leq n^2\ell$.

Let us now study the bound for $\sharp N(G \cdot B_i)$. We have obviously $N(\mathfrak{h}_i) = N(B_i) \subseteq N(G \cdot B_i)$. Next, let us prove that the following inclusion holds:

$$N(G \cdot B_i) \setminus N(\mathfrak{h}_i) \subseteq \bigcup_{t=0}^{\delta - 1} \{X_1^t u \mid u \in \mathrm{LM}(B_i)\}. \tag{7}$$

Let $m \in N(G \cdot B_i)$ be a monomial not in $N(\mathfrak{h}_i)$. Then, $m \notin \mathrm{LM}(G \cdot B_i)$ and $m \in \mathrm{LM}(\mathfrak{h}_i) = \mathrm{LM}(B_i)$. Thus, there exists $f \in B_i$ such that $u = \mathrm{LM}(f)$ and $m = X_1^{t_1} \cdots X_n^{t_n} u$. We claim that $t_1 < \delta$ and $t_2 = \cdots = t_n = 0$. If $t_1 \geq \delta$, then

$$m = X_1^{t_1 - \delta} X_2^{t_2} \cdots X_n^{t_n} \left(X_1^\delta u\right) = X_1^{t_1 - \delta} X_2^{t_2} \cdots X_n^{t_n} \left(\mathrm{LM}(g_1)\mathrm{LM}(f)\right) \in \mathrm{LM}(G \cdot B_i)$$

which contradicts $m \notin \mathrm{LM}(G \cdot B_i)$. Similarly, if $t_k \geq 1$ for some k then

$$m = X_1^{t_1} \cdots X_k^{t_k - 1} \cdots X_n^{t_n} \left(X_k u\right) \in \mathrm{LM}(G \cdot B_i),$$

which is also impossible because of the same reason. In conclusion, if m is a monomial in $N(G \cdot B_i) \setminus N(\mathfrak{h}_i)$ there exists $u \in \mathrm{LM}(B_i)$ and t, $0 \leq t \leq \delta - 1$,

such that $m = X_1^t u$. This proves the inclusion (7). Finally, we just count the cardinalities of these sets to conclude

$$\sharp N(G \cdot B_i) \leq \sharp N(\mathfrak{h}_i) + \delta \sharp \mathrm{LM}(B_i) \leq L\delta + \delta n L \leq (n+1)\delta\ell.$$

□

Assume that $\mathfrak{a}$ is a zero-dimensional ideal generated by $F = \{f_1, \ldots, f_k\}$ with $\deg(f_i) \leq d$. As in Equality (3), assume that $G = \{X_n - g_n(X_1), \ldots, X_2 - g_2(X_1), g_1(X_1)\}$ generates $\mathfrak{p}$. Let B_i be the reduced Gröbner basis of $\mathfrak{h}_i = \mathfrak{a} + \mathfrak{p}^i$ and B_{i+1} the reduced Gröbner basis for $\mathfrak{h}_{i+1} = \mathfrak{a} + \mathfrak{p} \cdot \mathfrak{h}_i = \mathfrak{a} + \mathfrak{p}^{i+1}$ computed by Algorithm 2 from $F \cup G \cdot B_i$. Note that this algorithm is a variant of Buchberger's algorithm applied to our situation. In the next lemma, we bound the size of B_{i+1} and the total number of S-polynomials to construct it, cf. [19, Lemma 5].

Algorithm 2. BUCHBERGER

Input: A finite set $F \cup G \cdot B_i$
Output: A Gröbner basis B_{i+1} for $\mathfrak{h}_{i+1}$

```
F̃ := {NF(f_j, G · B_i) | j = 1, ..., k}
T := F̃ ∪ G · B_i
P := {{f, g} | f ≠ g, f, g ∈ T}
while P ≠ ∅ do
    select {f, g} from P
    r := S(f, g, T)
    if r = 0 then
        P := P \ {{f, g}}
    else
        T := T ∪ {r}
        P := P ∪ {{r, h} | h ∈ T, h ≠ r}
    end if
end while
B := The reduced form of T, by performing an autoreduction
return (B)
```

Lemma 16. *With the above notations, the following statements hold.*

i) $\sharp B_{i+1} \leq k + (n+1)^2 \deg(\mathfrak{q})$.
ii) $\sharp N(\mathfrak{h}_{i+1}) = \sharp N(B_{i+1}) \leq \deg(\mathfrak{q})$.
iii) The total number of treated S-polynomials to compute B_{i+1} is at most

$$\left(k + (n+1)^2 \deg(\mathfrak{q})\right)^3.$$

iv) For every $S(f, g, H)$ constructed in the course of the algorithm, we have:

$$\max\left(\{\deg_{X_1}(f), \deg_{X_1}(g)\} \cup \{\deg_{X_1}(h) \mid h \in H\}\right) \leq \max\{d, \deg(\mathfrak{q})\},$$

and for all k, $2 \leq k \leq n$,

$$\max\left(\{\deg_{X_k}(f), \deg_{X_k}(g)\} \cup \{\deg_{X_k}(h) \mid h \in H\}\right) \leq \max\{d, \ell(\mathfrak{q})\}.$$

Proof. To bound the size of B_{i+1}, let us first count the number of S-polynomials leading to a non-zero normal form computed in this algorithm. Let $\mathscr{R}$ be this number. For this, we shall need to introduce some subindices to determine the size of the intermediate sets computed in the course of this algorithm. We initialize with $T_0 := T$ and $P_0 := P$. In addition, one step is one iteration of the algorithm leading to a non-zero normal form. Thus, $T_{\mathscr{R}}$ is a Gröbner basis of the ideal $\mathfrak{h}_{i+1}$. Whereas the sequence T_s is an increasing sequence, P_{s+1} does not necessarily contain P_s, since some of the elements of P_s may have been removed.

An upper bound for the number of the treated S-polynomials is given by

$$\sharp \bigcup_{s=0}^{\mathscr{R}} P_j + k + \sharp T_{\mathscr{R}} \leq (\mathscr{R}+1) \max\{\sharp P_s \mid 0 \leq s \leq \mathscr{R}\} + k + \sharp T_{\mathscr{R}}. \tag{8}$$

Note that, in the above bound, we considered the fact that the computation of $\widetilde{F}$ from F requires k additional S-polynomials. Here we took also into account the last step of the algorithm to compute the reduced Gröbner basis B. For this purpose, the number of S-polynomials that we need to perform is at most $\sharp T_{\mathscr{R}}$. Now, one observes that for each s we have

$$\begin{cases} \sharp T_{s+1} = \sharp T_s + 1, \\ \sharp P_{s+1} \leq \sharp P_s + \sharp T_s. \end{cases} \tag{9}$$

Let us denote by $\mathscr{S}_0$ the cardinality of the initial set T_0. According to (6) we have $\sharp B_i = \sharp \mathrm{LM}(B_i) \leq n\ell$. As G contains only n polynomials, we obtain

$$\begin{cases} \mathscr{S}_0 = \sharp T_0 = \sharp(F \cup G \cdot B_i) \leq \sharp F + \sharp(G \cdot B_i) \leq k + n^2\ell, \\ \sharp P_0 = \binom{\mathscr{S}_0}{2}. \end{cases} \tag{10}$$

Next, observe that $T_s \supseteq F \cup G \cdot B_i \supseteq G \cdot B_i$ and if $r = S(f, g, T_s) \neq 0$, the leading monomial of r belongs to the normal set $N(T_s)$, which satisfies $N(T_s) \subseteq N(G \cdot B_i)$. Thus, according to Lemma 15, we conclude that

$$\mathscr{R} \leq \sharp N(G \cdot B_i) \leq (n+1)\ell\delta = (n+1)\deg(\mathfrak{q})$$

and in turn $\sharp B_{i+1} \leq \sharp T_{\mathscr{R}} \leq k + n^2\ell + (n+1)\ell\delta \leq k + (n+1)^2 \deg(\mathfrak{q})$, proving the first claim. We notice that $\mathfrak{h}_{i+1} \subset \mathfrak{q}$ and therefore $N(\mathfrak{h}_{i+1}) \subset N(\mathfrak{q})$. This implies that $\sharp N(\mathfrak{h}_{i+1}) \leq \sharp N(\mathfrak{q}) = \deg(\mathfrak{q})$ and the second claim now easily follows. To prove Claim iii), proceeding by induction and using (9) we can show that for all s with $0 \leq s \leq \mathscr{R}$, it holds

$$\sharp P_s \leq \binom{\mathscr{S}_0}{2} + s\mathscr{S}_0 + \sum_{t=1}^{s} t. \tag{11}$$

It follows that for all s, we have

$$\sharp P_s \leq \binom{\mathscr{S}_0}{2} + \mathscr{R}\mathscr{S}_0 + \sum_{t=1}^{\mathscr{R}} t \leq \frac{1}{2}\left(\mathscr{S}_0^2 + \mathscr{R}^2\right) + \mathscr{R}\mathscr{S}_0 = \frac{1}{2}\left(\mathscr{S}_0 + \mathscr{R}\right)^2$$

and hence

$$\sharp P_s \leq \frac{1}{2}\left(k + n^2\ell + (n+1)\deg(\mathfrak{q})\right)^2 \leq \frac{1}{2}\left(k + (n+1)^2\deg(\mathfrak{q})\right)^2.$$

Thus, according to Inequality (8), the total number of S-polynomials calculated by our version of Buchberger's algorithm is bounded by

$$(\mathscr{R}+1)\max\{\sharp P_s \mid 0 \leq s \leq \mathscr{R}\} + k + \sharp T_{\mathscr{R}} \leq \left(k + (n+1)^2\deg(\mathfrak{q})\right)^3.$$

In order to prove Claim iv), we proceed by induction on i. For every finite set Q and for all k, $1 \leq k \leq n$, we denote by $\delta_k(Q) = \max\{\deg_{X_k}(h) \mid h \in Q\}$. As $B_1 = \{X_n - g_n(X_1), \ldots, X_2 - g_2(X_1), g_1(X_1)\}$, we then conclude that

$$\delta_1(B_1) = \max\{\deg_{X_1}(h) \mid h \in B_1\} = \deg(\mathfrak{p}) = \delta$$

and, for all k with $2 \leq k \leq n$, $\delta_k(B_1) = \max\{\deg_{X_k}(h) \mid h \in B_1\} = 1$. Hence the first step of the induction holds. Now observe that B_{i+1} is computed from F and $G \cdot B_i$ using a sequence of intermediate sets of polynomials $T_0, T_1, \ldots, T_{\mathscr{R}}$. Every polynomial f in T_0 satisfies one of the following two conditions:

– If $f \in G \cdot B_i$, for any k with $2 \leq k \leq n$, we have

$$\deg_{X_1}(f) \leq \delta + \delta_1(B_i), \qquad \deg_{X_k}(f) \leq 1 + \delta_k(B_i). \tag{12}$$

– If $f \in \widetilde{F}$ then f is a sum of non-zero terms in $N(G \cdot B_i)$, then, from Lemma 3 we conclude that for all k with $1 \leq k \leq n$, it holds

$$\deg_{X_k}(f) \leq \max\{\deg_{X_k}(h) \mid h \in G \cdot B_i\},$$

and the degree bounds of (12) also apply to $\deg_{X_1}(f)$ and $\deg_{X_k}(f)$.

We know that $T_{j+1} = T_j \cup \{S(f, g, T_j)\}$ for some polynomials $f, g \in T_j$. However, as $G \cdot B_i \subseteq T_j$, we conclude $N(T_j) \subseteq N(G \cdot B_i)$. Hence, every polynomial added to T_j to build up T_{j+1} is a linear combination of monomials in $N(G \cdot B_i)$. Applying once more Lemma 3, we conclude that, for all k with $2 \leq k \leq n$ it holds

$$\begin{aligned} \delta_1(T_{j+1}) &\leq \delta + \delta_1(B_i), \\ \delta_k(T_{j+1}) &\leq 1 + \delta_k(B_i). \end{aligned} \tag{13}$$

The reduced Gröbner basis B_{i+1} is obtained from $T_{\mathscr{R}}$ by applying some computations of normal forms of polynomials whose degrees are bounded by those of $T_{\mathscr{R}}$. All in all, for all k with $2 \leq k \leq n$ we immediately see that

$$\begin{aligned} \delta_1(B_{i+1}) &\leq \delta + \delta_1(B_i) \leq (i+1)\delta_1(B_1) = (i+1)\delta, \\ \delta_k(B_{i+1}) &\leq 1 + \delta_k(B_i) \leq i + 1. \end{aligned}$$

Finally, we note that the reduced Gröbner basis of $\mathfrak{q}$ is obtained by the sequence of intermediate reduced Gröbner bases $B_1, \ldots, B_L$ with $L = \ell$. We then conclude that for all i and k, we have $\delta_1(B_i) \leq \ell\delta = \ell(\mathfrak{q})\deg(\mathfrak{p}) = \deg(\mathfrak{q})$ and

$\delta_k(B_i) \leq \ell = \ell(\mathfrak{q})$. Taking into account that we have considered some preliminary computations of normal forms to obtain $\widetilde{F}$ from F and that polynomials in F have total degrees at most d, we get $\delta_1(B_L) \leq \max\{d, \deg(\mathfrak{q})\}$ and $\delta_k(B_L) \leq \max\{d, \ell(\mathfrak{q})\}$. The same bounds apply for every term $S(f, g, H)$ involved in the computation of S-polynomials along this process. □

Our first partial complexity estimate is the content of the following result, cf. the corollary on page 231 of [19].

Theorem 17. *Let $\mathfrak{q}$ be a zero-dimensional ideal such that $\sqrt{\mathfrak{a}}$ is in normal X_1-position. The number of field operations required by Algorithm 1 is at most*

$$O\left(\ell(\mathfrak{q})\left(k + (n+1)^2 \deg(\mathfrak{q})\right)^3\right) \times \mathscr{T}_S(n, \tau, \sharp\Theta, D)$$

where $\mathscr{T}_S$ is the function that measures the number of arithmetic operations required to compute an S-polynomial with the following parameters:

- $\tau := \max\{\sharp t(F), (n+1)(\deg(\mathfrak{q})+1)^2\}$ *being an upper bound for the number of non-zero terms involved,*
- $\sharp\Theta := k + (n+1)^2 \deg(\mathfrak{q})$ *being an upper bound for the maximum cardinalities of the sets of polynomials involved,*
- $D := \max\{2d, \deg(\mathfrak{q}) + (n-1)\ell(\mathfrak{q})\}$ *being an upper bound for the maximum of the degrees of the polynomials involved.*

Proof. From Lemma 12, we know that the number of times that Algorithm 1 enters the **while**-loop is at most $\ell(\mathfrak{q}) \leq \deg(\mathfrak{q})$. On the other hand, as already mentioned, to compute the reduced Gröbner basis for $\mathfrak{q}$, we shall compute the intermediate reduced Gröbner bases $B_1, \ldots, B_L$ with $L = \ell(\mathfrak{q})$ by starting from the reduced Gröbner basis $B_0 := G$ for $\mathfrak{p}$. Thus, it suffices to prove that the claimed bound without $\ell(\mathfrak{q})$ holds for the number of arithmetic operations to construct B_{i+1} from B_i for each i. For this purpose, by Lemma 16, the number of computations of S-polynomials and normal forms is bounded by

$$O\left(\left(k + (n+1)^2 \deg(\mathfrak{q})\right)^3\right). \tag{14}$$

In addition, at each step, we shall need to compare whether B_i and B_{i+1} are equal, before doing anything. As both of them are reduced Gröbner basis, we just have to compare them element-by-element. This can be done in time

$$O(\sharp B_i \sharp B_{i+1} \max\{\sharp t(B_i), \sharp t(B_{i+1})\}).$$

Observe that in Lemma 16, it was shown that for each i, $\sharp B_{i+1} \leq k + (n+1)^2 \deg(\mathfrak{q})$. Moreover, in Lemma 15, we have proved that $\sharp t(B_{i+1}) \leq (n+1)\deg(\mathfrak{q})$. These arguments confirm the upper bound (14) for the number of operations required in Algorithm 1.

To complete the proof, it is enough to show that the number of arithmetic operations in the field K to calculate an S-polynomial is bounded by

$\mathscr{T}_S(n, \tau, \sharp\Theta, D)$. Following Definition 5, we first prove that the number of non-zero terms in any involved polynomial is at most $\max\{\sharp t(F), (n+1)(\deg(\mathfrak{q})+1)^2\}$. Remark that to compute the Gröbner basis B_{i+1} using Algorithm 2, we construct an increasing sequence of sets of generators of $\mathfrak{h}_{i+1}$, say $T_0 \subset T_1 \subset \cdots \subset T_{\mathscr{R}}$. We want to bound the maximum number of terms occurring in any of the T_s's. As B_i is a reduced Gröbner basis of $\mathfrak{h}_i$, from Lemmata 4 and 16, the maximum number of non-zero terms of any polynomial in B_i is bounded by $\sharp(N(B_i)) + 1 \leq \deg(\mathfrak{q}) + 1$. Now, we consider an arbitrary polynomial $h \in G \cdot B_i$ that generates the ideal $\mathfrak{p}\mathfrak{h}_i$. The number of terms in h is bounded by

$$\sharp t(G \cdot B_i) \leq \sharp t(G) \times \sharp t(B_i) \leq (\delta + 1)(\sharp N(B_i) + 1) \leq (\deg(\mathfrak{p}) + 1)\,(\deg(\mathfrak{q}) + 1)\,.$$

Recall that in Algorithm 2 we defined $T_0 := \widetilde{F} \cup G \cdot B_i$. Every term of $\widetilde{f_j}$ belongs to $N(G \cdot B_i)$ and, hence, from Lemma 15 we have

$$\sharp t(\widetilde{F}) \leq \sharp N(G \cdot B_i) \leq (n+1)\deg(\mathfrak{q}).$$

We conclude that the number of terms of any polynomial in T_0 is at most

$$\max\{\sharp N(G \cdot B_i), (\deg(\mathfrak{p}) + 1)(\deg(\mathfrak{q}) + 1)\} \leq (n+1)(\deg(\mathfrak{q}) + 1)^2.$$

It can be shown similarly, by induction and using the fact that $T_0 \subseteq T_s$ and $G \cdot B_i \subseteq T_s$ for all s, that the same bound holds for T_s as well. Thus, by considering the polynomials in F, the number of non-zero terms involved in the algorithm is bounded by $\max\{\sharp t(F), (n+1)(\deg(\mathfrak{q}) + 1)^2\}$. Moreover, in Lemma 16, we proved that $k+(n+1)^2 \deg(\mathfrak{q})$ is an upper bound for the maximum cardinalities of the sets of polynomials. Finally, from Claim iv) of Lemma 16, we conclude that the maximum degree of $S(f, g, H)$ constructed in the Algorithm 2 is at most $\max\{2d, \deg(\mathfrak{q}) + (n-1)\ell(\mathfrak{q})\}$ and this finishes the proof. □

Corollary 18. *Let $\mathfrak{a}$ be a zero-dimensional ideal such that $\sqrt{\mathfrak{a}}$ is in normal X_1-position and K a field with efficient factorization of univariate polynomials. Assume that the radical $\sqrt{a}$ is given by the Kronecker description of the form $\sqrt{\mathfrak{a}} = (X_n - g_n(X_1), X_{n-1} - g_{n-1}(X_1), \ldots, X_2 - g_2(X_1), g_1(X_1))$ where $g_1, \ldots, g_n \in K[X_1]$ with $\deg(g_i) < \deg(g_1)$, for all i, $2 \leq i \leq n$. Then, we can compute the reduced Gröbner bases for all isolated primary components of $\mathfrak{a}$ in a number of field operations which is bounded by $PFC(\mathfrak{a}) + Q(\mathfrak{a})$ where*

- *the quantity $PFC(\mathfrak{a})$ is the Polynomial Factorization Cost, i.e. the number of arithmetic operations required in K to factorize a univariate polynomial over K of total degree bounded by the degree of $\mathfrak{a}$ and coefficients of bit length bounded by the logarithmic height of $V(\mathfrak{a})$ viewed as an arithmetic variety.*
- *$Q(\mathfrak{a})$ is $O\left(\ell(\mathfrak{a})\deg(\sqrt{\mathfrak{a}})\left((n+1)^2\deg(\mathfrak{a}) + k\right)^3\right) \times \mathscr{T}_S(n, \tau, \sharp\Theta, D)$.*

Proof. From Theorem 17, we know that the reduced Gröbner basis of the primary component $\mathfrak{q}$ can be computed in a number of arithmetic operations in K bounded by

$$O\left(\ell(\mathfrak{q})\left((n+1)^2\deg(\mathfrak{q}) + k\right)^3\right) \times \mathscr{T}_S(n, \tau, \sharp\Theta, D).$$

On the other hand, the number of primary components of $\mathfrak{a}$ is bounded by the number of associated primes of $\mathfrak{a}$ and this number is at most $\deg(\sqrt{\mathfrak{a}})$. □

Remark 19. The quantity $PFC(\mathfrak{a})$ aims to capture the complexity of factoring a univariate polynomial which can be obtained as the instantiation of an elimination polynomial related to $\mathfrak{a}$.

In the case K is a number field, since the old times of LLL, Trager's method and Landau-Miller norm method approach, we know that $PFC(\mathfrak{a})$ is bounded by a polynomial in the degree of the field extension $[K:\mathbb{Q}]$, $\deg(\mathfrak{a})$ and the logarithmic height of $V(\mathfrak{a})$. In our conditions, the less precise quantity could be the logarithmic height of $V(\mathfrak{a})$. Bézout Inequality (see [17,36]) and the Arithmetic Bézout Inequality (see e.g., [3,25,27,29–32], or the references in [12,28]) imply the following upper bounds for $\deg(\mathfrak{a})$ and the logarithmic height of $V(\mathfrak{a})$:

$$\deg(\mathfrak{a}) \leq d^{n-\dim(\mathfrak{a})}, \quad \mathrm{ht}(V(\mathfrak{a})) \leq O(d^{n-\dim(\mathfrak{a})}(h + n\log(d)))$$

where $\mathrm{ht}(V(\mathfrak{a}))$ is equal to $\mathrm{ht}(\mathfrak{a})$ and h is a bound for the bit length of coefficients of the f_i's. Hence, in this case $PFC(\mathfrak{a})$ is bounded by a polynomial in $[K:\mathbb{Q}], d^{n-\dim(\mathfrak{a})}, n$ and h Note that in the case $K=\mathbb{Q}$, in [2, Corollary 5.3] an algorithm is presented for factoring a polynomial $f \in \mathbb{Q}[X]$ within the bit complexity $O(r^8 + r^6p^2)$ where $r = \deg(f)$ and $p = \log(||f||_2)$. Hence, in this case and under our hypothesis, $PFC(\mathfrak{a})$ is bounded by a quantity which is a polynomial of order:

$$PFC(\mathfrak{a}) \leq \left(d^{n-\dim(\mathfrak{a})}nh\right)^{O(1)}.$$

Remark 20. The same type of statement holds for a perfect field with an efficient univariate factorization algorithm. In the case of finite fields we have to add the phrase "with enough elements", in order to have efficient probabilistic non-zero polynomial identity tests (as those in [16,33,39]), for polynomials with degrees bounded by $\deg(\mathfrak{a})$. Note that in the case K is a finite field, as it is known in the literature of the topic, the number of arithmetic operations in the ground field K of deterministic factorization of univariate polynomials (and, hence, $PFC(\mathfrak{a})$) is bounded by a polynomial in $\deg(\mathfrak{a})$ and in the characteristic of the field. If we admit probabilistic algorithms, the quantity $PFC(\mathfrak{a})$ would be bounded by a polynomial in $\deg(\mathfrak{a}) \leq d^{n-\dim(\mathfrak{a})}$ and the logarithm of the field cardinality. See the survey [37] for more detailed references.

Remark 21. From the estimation of $\mathscr{T}_S(n,\tau,\sharp\Theta,D)$ in Remark 6, it holds $Q(\mathfrak{a}) \leq k^3 d^{O(n^2)}$. Our insistence to exhibit an accurate bound for $Q(\mathfrak{a})$ comes from our interest to analyze whether $Q(\mathfrak{a})$ can be of order $\left(d^{n-\dim(\mathfrak{a})}\right)^{O(1)} = d^{O(n)}$. From our study, we conclude that this bound can be achieved provided that there exist methods to compute S-polynomials faster than those cited in Remark 6.

Corollary 22. *The same bound presented in Corollary 18 holds for the number of arithmetic operations in K to compute the reduced Gröbner basis for $\mathfrak{a}$.*

Proof. In [19, page 232], it has been shown that by computing the reduced Gröbner bases of the primary components of $\mathfrak{a}$ and by applying a variant of the FGLM algorithm [11] one is able to construct the reduced Gröbner basis for $\mathfrak{a}$. Note that, in this variant of the FGLM algorithm, we shall consider the vectors of size at most $\deg(\mathfrak{a})$ and therefore the FGLM cost would be $O(n \deg(\mathfrak{a})^3) \leq Q(\mathfrak{a})$, see [11, Proposition 4.1]. □

4 Complexity of Computing the Degree of an Ideal

In this section, we give an algorithm to compute the degree of an ideal. Then, after stating some required preliminaries, we provide the complexity analysis of this algorithm (see Theorem 23).

Let K be an algebraically closed field with efficient factorization of univariate polynomials. Let $\mathfrak{a} = (f_1, \ldots, f_k) \subset K[X]$ be an equidimensional[1] ideal of dimension r. In [15], it has been shown that one is able to choose generic linear polynomials $\ell_1, \ldots, \ell_r$ so that the ideal $\mathfrak{a} + (\ell_1, \ldots, \ell_r)$ is zero-dimensional and the sum of the degrees of all primary components of this ideal is defined to be the degree of $\mathfrak{a}$. On the other hand, in [13], it has been shown that by a generic linear change of coordinates $\sqrt{\mathfrak{a}}$ is transformed to normal X_1-position. Thus, we may choose generic linear polynomials $\ell_1, \ldots, \ell_n$ such that $\mathfrak{b} = \mathfrak{a} + (\ell_1, \ldots, \ell_n)$ is zero-dimensional and $\sqrt{\mathfrak{b}}$ is in normal X_1-position. Based on the results presented in Section 3 we give the next probabilistic algorithm to compute $\deg(\mathfrak{a})$.

Algorithm 3. DEGREE

Input: A finite generating set F of an equidimensional $\mathfrak{a}$ of dimension r
Output: $\deg(\mathfrak{a})$

choose generic linear polynomials $\ell_1, \ldots, \ell_n \in K[X_1, \ldots, X_n]$
compute a Kronecker description of $V(\sqrt{\mathfrak{b}})$ where $\mathfrak{b} = \mathfrak{a} + (\ell_1, \ldots, \ell_n)$
factor the univariate minimal equation of the chosen primitive element of the residue ring $K[V(\mathfrak{b})] := K[X_1, \ldots, X_n]/\sqrt{\mathfrak{b}}$.
compute a Kronecker description of each of the associated prime $\mathfrak{p}$ of $\mathfrak{b}$.
compute $\deg(\mathfrak{q})$, for every primary component $\mathfrak{q}$ of $\mathfrak{b}$.
return $\sum_{\mathfrak{q}} \deg(\mathfrak{q})$ where $\mathfrak{q}$ is a primary component of the ideal $\mathfrak{b}$

It is worth noting that different approaches have been developed in literature to compute primary components of a zero-dimensional ideal generated by $g_1, \ldots, g_s$. For example, we can point out the method of *Kronecker solver* introduced by Giusti et al. [14] (see also [8,10,24]). In this approach, we shall require several assumptions: g_i for $1 < i \leq n$ forms a non-zero divisor in $K[X]/(g_1, \ldots, g_{i-1})$. In addition, we shall perform a linear change of variables

[1] That is all isolated primes of $\mathfrak{a}$ share the same dimension. Note that, in general, an equidimensional is not unmixed. A proper ideal is said to be unmixed if its dimension is equal to the dimension of every associated prime of the ideal.

so that the 12 conditions mentioned in [10, page 127] are satisfied. Under these assumptions, an efficient method, without the use of Gröbner bases, is given to compute Kronecker representations for all the primary components of the ideal. Now, let K be of characteristic zero, d_i denote the degree of g_i so that $d_1 \geq \cdots \geq d_s$ and let $d = d_1 \cdots d_n$. Then, in [9] an algorithm has been proposed for these computations within the arithmetic complexity $\tilde{\mathcal{O}}(d^{11} + (L + ns)d^6)$ where $g_1, \ldots, g_s$ are given by a straight-line program of size L. As a consequence of Corollary 22, we obtain the main result of this section.

Theorem 23. *Algorithm 3 is a (Monte Carlo) probabilistic algorithm such that for every input equidimensional ideal $\mathfrak{a} \subset R$, given by a system of generators $F = \{f_1, \ldots, f_k\}$ of degree at most d and coefficients of bit length at most h, outputs the degree* $\deg(\mathfrak{a})$. *The total number of arithmetic field operations performed by this algorithm is bounded by the sum of two quantities depending on the input ideal $Kron(\mathfrak{a}) + PFC(\mathfrak{a}) + Q(\mathfrak{a})$ where $Kron(\mathfrak{a})$ denotes the number of arithmetic operations in K to compute the Kronecker description for $\sqrt{\mathfrak{a}}$.*

Acknowledgments. The research was partially supported by the following Iranian, Argentinian and Spanish Grants:
- IPM Grant No. 98550413 (Amir Hashemi)
- UBACyT 20020170100309BA and PICT-2014-3260 (Joos Heintz)
- Spanish Grant MTM2014-55262-P (Luis M. Pardo)

References

1. Becker, T., Weispfenning, V.: Gröbner Bases: A Computational Approach to Commutative Algebra. In cooperation with Heinz Kredel. Springer, New York (1993). https://doi.org/10.1007/978-1-4612-0913-3
2. Belabas, K., van Hoeij, M., Klüners, J., Steel, A.: Factoring polynomials over global fields. J. Théor. Nombres Bordx. **21**(1), 15–39 (2009)
3. Bost, J.B., Gillet, H., Soulé, C.: Un analogue arithmétique du théorème de Bézout. C. R. Acad. Sci. Paris Sér. I **312**(11), 845–848 (1991)
4. Brownawell, W.D., Masser, D.W.: Multiplicity estimates for analytic functions. II. Duke Math. J. **47**, 273–295 (1980)
5. Buchberger, B.: Bruno Buchberger's PhD thesis 1965: an algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. Translation from the German. J. Symb. Comput. **41**(3–4), 475–511 (2006). https://doi.org/10.1016/j.jsc.2005.09.007
6. Cox, D.A., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra, 4th edn. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-16721-3
7. Dickenstein, A., Fitchas, N., Giusti, M., Sessa, C.: The membership problem for unmixed polynomial ideals is solvable in single exponential time. Discrete Appl. Math. **33**(1–3), 73–94 (1991)
8. Durvye, C.: Algorithmes pour la décomposition primaire des idéaux polynomiaux de dimension nulle donnés en évaluation. Ph.D. thesis, University of Versailles-St Quentin en Yvelines (2008)

9. Durvye, C.: Evaluation techniques for zero-dimensional primary decomposition. J. Symb. Comput. **44**(9), 1089–1113 (2009)
10. Durvye, C., Lecerf, G.: A concise proof of the Kronecker polynomial system solver from scratch. Expo. Math. **26**(2), 101–139 (2008)
11. Faugère, J.C., Gianni, P., Lazard, D., Mora, T.: Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symb. Comput. **16**(4), 329–344 (1993)
12. Fernández, M., Pardo, L.M.: An arithmetic Poisson formula for the multi-variate resultant. J. Complexity **29**(5), 323–350 (2013)
13. Gianni, P., Mora, T.: Algebrric solution of systems of polynomirl equations using Groebher bases. In: Huguet, L., Poli, A. (eds.) AAECC 1987. LNCS, vol. 356, pp. 247–257. Springer, Heidelberg (1989). https://doi.org/10.1007/3-540-51082-6_83
14. Giusti, M., Lecerf, G., Salvy, B.: A Gröbner free alternative for polynomial system solving. J. Complexity **17**(1), 154–211 (2001)
15. Hashemi, A., Heintz, J., Pardo, L.M., Solernó, P.: On Bézout inequalities for non-homogeneous polynomial ideals. arXiv:1701.04341 (2017)
16. Heintz, J., Schnorr, C.P.: Testing polynomials which are easy to compute. In: International Symposium on Logic and Algorithmic, Zürich 1980, Monographs of L'Enseignement Mathematique, vol. 30, pp. 237–254 (1982)
17. Heintz, J.: Definability and fast quantifier elimination in algebraically closed fields. Theor. Comput. Sci. **24**, 239–277 (1983)
18. Kemper, G.: A Course in Commutative Algebra, vol. 256. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-03545-6
19. Lakshman, Y.N.: A single exponential bound on the complexity of computing Gröbner bases of zero dimensional ideals. In: Mora, T., Traverso, C. (eds.) Effective Methods in Algebraic Geometry. Progress in Mathematics, vol. 94, pp. 227–234. Birkhäuser, Boston (1991). https://doi.org/10.1007/978-1-4612-0441-1_15
20. Lakshman, Y.N., Lazard, D.: On the complexity of zero-dimensional algebraic systems. In: Mora, T., Traverso, C. (eds.) Effective Methods in Algebraic Geometry. Progress in Mathematics, vol. 94, pp. 217–225. Birkhäuser, Boston (1991)
21. Lazard, D.: Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In: van Hulzen, J.A. (ed.) EUROCAL 1983. LNCS, vol. 162, pp. 146–156. Springer, Heidelberg (1983). https://doi.org/10.1007/3-540-12868-9_99
22. Lazard, D.: Résolution des systèmes d'équations algébriques. Theor. Comput. Sci. **15**, 77–110 (1981). https://doi.org/10.1016/0304-3975(81)90064-5
23. Le Gall, F.: Powers of tensors and fast matrix multiplication. In: Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation, ISSAC 2014, pp. 296–303. Association for Computing Machinery (ACM), New York (2014)
24. Lecerf, G.: Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. J. Complexity **19**(4), 564–596 (2003)
25. Lelong, P.: Mesure de Mahler et calcul de constantes universelles pour les polynômes de n variables. Math. Ann. **299**(4), 673–695 (1994)
26. Mayr, E.W., Meyer, A.R.: The complexity of the word problems for commutative semigroups and polynomial ideals. Adv. Math. **46**, 305–329 (1982). https://doi.org/10.1016/0001-8708(82)90048-2
27. McKinnon, D.: An arithmetic analogue of Bezout's theorem. Compos. Math. **126**(2), 147–155 (2001)
28. Pardo, L.M., Pardo, M.: On the zeta Mahler measure function of the Jacobian determinant, condition numbers and the height of the generic discriminant. Appl. Algebra Eng. Commun. Comput. **27**(4), 303–358 (2016). https://doi.org/10.1007/s00200-016-0284-9

29. Philippon, P.: Critères pour l'indépendance algébrique. Publ. Math. Inst. Hautes Étud. Sci. **64**, 5–52 (1986)
30. Philippon, P.: Sur des hauteurs alternatives. I. (On alternative heights. I). Math. Ann. **289**(2), 255–283 (1991)
31. Philippon, P.: Sur des hauteurs alternatives. II. (On alternative heights. II). Ann. Inst. Fourier **44**(4), 1043–1065 (1994)
32. Philippon, P.: Sur des hauteurs alternatives. III. J. Math. Pures Appl. (9) **74**(4), 345–365 (1995)
33. Schwartz, J.T.: Fast probabilistic algorithms for verification of polynomial identities. J. Assoc. Comput. Mach. **27**, 701–717 (1980)
34. Hoeven, J.: On the complexity of multivariate polynomial division. In: Kotsireas, I.S., Martínez-Moro, E. (eds.) ACA 2015. SPMS, vol. 198, pp. 447–458. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56932-1_28
35. Van der Waerden, B.L.: Algebra. Volume II. Based in part on lectures by. E. Artin and E. Noether. Transl. from the German 5th ed. by John R. Schulenberger. Springer, New York (1991)
36. Vogel, W.: Lectures on results on Bezout's theorem. Notes by D. P. Patil. Lectures on Mathematics and Physics. Mathematics, 74. Tata Institute of Fundamental Research. Springer, Berlin, ix, 132 p. (1984)
37. von zur Gathen, J., Panario, D.: Factoring polynomials over finite fields: a survey. J. Symb. Comput. **31**(1–2), 3–17 (2001)
38. Zariski, O., Samuel, P.: Commutative algebra. Vol. II. The University Series in Higher Mathematics. Princeton, N.J.-Toronto-London-New York: D. Van Nostrand Company, Inc. x, 414 p. (1960)
39. Zippel, R.: Interpolating polynomials from their values. J. Symb. Comput. **9**(3), 375–403 (1990)