# A Single Exponential Time Algorithm for Homogeneous Regular Sequence Tests

Amir Hashemi[a], Benyamin M.-Alizadeh[a], Hossein Parnian[a], Werner M. Seiler[b]

[a]*Department of Mathematical Sciences, Isfahan University of Technology, Isfahan 84156-83111, Iran*
[b]*Institut für Mathematik, Universität Kassel, 34109 Kassel, Germany*

**Abstract**

Assume that we are given a sequence $F$ of $k$ homogeneous polynomials in $n$ variables of degree at most $d$ and the ideal $\mathcal{I}$ generated by this sequence. The aim of this paper is to present a new and effective method to determine, within the arithmetic complexity $d^{O(n)}$, whether $F$ is regular. This algorithm has been implemented in Maple and its efficiency (compared to the classical approaches for regular sequence test) is evaluated via a set of benchmark polynomials. Furthermore, we show that, if $F$ is regular then we can transform $\mathcal{I}$ into Nœther position and at the same time compute a reduced Gröbner basis for the transformed ideal within the arithmetic complexity $d^{O(n^2)}$. Finally, under the same assumption, we establish the new upper bound $2(d^k/2)^{2^{n-k-1}}$ for the maximum degree of the elements of any reduced Gröbner basis of $\mathcal{I}$ in the case that $n > k$.

*Keywords:* Homogeneous polynomials, Polynomial ideals, Gröbner bases, $F_5$ algorithm, Regular sequences, Hilbert series, Complexity analysis, Degree upper bounds.
*2010 MSC:* 13P10, 68W30

## 1. Introduction

The notion of *Gröbner bases* as well as the first algorithm for their construction were introduced by Buchberger in 1965 in his Ph.D. thesis (Buchberger, 1965, 2006). In 1979, he improved this algorithm by applying two criteria (known as Buchberger's criteria) to remove some of the superfluous reductions, (Buchberger, 1979). Later on, (Gebauer and Möller, 1988) described an efficient algorithm to install these criteria on Buchberger's algorithm. Since then, several improvements have been proposed to speed-up the computation of Gröbner bases. In particular, in 2002, Faugère described his famous $F_5$ algorithm (Faugère, 2002) based on an incremental and signature-based structure to compute Gröbner bases. Finally, (Gao et al., 2016) proposed the so-called GVW algorithm; a new signature-based algorithm to compute simultaneously Gröbner bases for an ideal and its syzygy module.

*Email addresses:* Amir.Hashemi@iut.ac.ir (Amir Hashemi), Benyamin.M.Alizadeh@gmail.com (Benyamin M.-Alizadeh), Hossein.Parnian@alumni.iut.ac.ir (Hossein Parnian), Seiler@mathematik.uni-kassel.de (Werner M. Seiler)
*URL:* http://amirhashemi.iut.ac.ir (Amir Hashemi), http://www.mathematik.uni-kassel.de/~seiler (Werner M. Seiler)

Let $\mathcal{P} = \mathcal{K}[x_1, \ldots, x_n]$ be the polynomial ring over a infinite field $\mathcal{K}$ and $F := f_1, \ldots, f_k$ a sequence of homogeneous polynomials of degree at most $d$. Furthermore, assume that $\mathcal{I}$ is the ideal generated by $F$. Our main goal in this paper is to describe an effective method to test whether $F$ is *regular*. One of the interesting applications of Gröbner bases is to provide such tests in different manners. For example, for every $i$, to determine if the coset of $f_i$ is a non-zero divisor in $\mathcal{P}/\langle f_1, \ldots, f_{i-1}\rangle$, one can compute the reduced Gröbner basis (with respect to a fix term ordering) for the quotient ideal $\langle f_1, \ldots, f_{i-1}\rangle : f_i$ and check if it is equal to that of $\langle f_1, \ldots, f_{i-1}\rangle$. As an alternative approach, from the Gröbner basis of $\mathcal{I}$, one can derive Krull dimension of the ideal (using the Hilbert polynomial or the Hilbert series of the ideal) and this dimension simply determines whether $F$ is regular. Finally, (Faugère, 2002) proved that $F$ forms a regular sequence if running the $F_5$ algorithm on $F$ produces no reduction to zero. However, we shall note that in all these approaches one needs to compute at least a (full) Gröbner basis for $\mathcal{I}$. On the other hand, by an example due to (Mayr and Meyer, 1982) we know that, in the worst-case, the complexity of Gröbner bases computation is doubly exponential in the number of variables. Thus, the complexity of testing whether $F$ is regular remains doubly exponential in the number of variables.

In this paper, we give a new approach to test, within the arithmetic complexity[1] $d^{O(n)}$, if $F$ is regular or not. We have implemented this algorithm in Maple and its efficiency is compared with the $F_5$ algorithm via a set of benchmark polynomials. Furthermore, as an application of this study, we show that, within the complexity $d^{O(n^2)}$, we are able to transform an ideal $\mathcal{I}$ into Nœther position (we show that for a general sequence $F$, this complexity becomes $(kd^n)^{O(n)}$). As a byproduct, in the case that $F$ is a regular sequence, a reduced Gröbner basis for the transformed ideal is also returned. Finally, we investigate degree upper bounds for the reduced Gröbner basis of an ideal generated by a regular sequence. Dubé (1990) by applying a constructive combinatorial argument proved the degree bound $2(d^2/2 + d)^{2^{n-2}}$ for every reduced Gröbner basis of $\mathcal{I}$. Mayr and Ritscher (2013) improved this bound to the dimension-dependent upper bound $2(1/2(d^{n-D} + d))^{2^{D-1}}$ where $D$ stands for the Krull dimension of $\mathcal{I}$, see also (Hashemi and Seiler, 2017). We show that, in the case that $F$ is a regular sequence and $n > k$, the upper bound $2(d^k/2)^{2^{n-k-1}}$ holds true for the maximum degree of the elements of any reduced Gröbner basis of $\mathcal{I}$ (whenever $n = k$ then the bound $nd - n + 1$ is valid). This shows that in the special case when $F$ is a regular sequence, the second term in the Mayr-Ritscher bound can be dropped.

The structure of the paper is as follows. Section 2 reviews the basic notations and terminologies used throughout the paper. In Section 3, we study the maximum degree of the elements in the (reduced) Gröbner basis of an ideal generated by a regular sequence in generic position. Section 4 is devoted to present the underlying details of the $F_5$ algorithm (Faugère, 2002) to compute Gröbner bases. For the sake of simplicity, we review the matrix variant of this algorithm from (Bardet et al., 2015). This algorithm is applied in Section 5 to provide an effective method to test whether a given sequence of homogeneous polynomials is regular. We show also that with the complexity $d^{O(n^2)}$ we are able to transform an ideal generated by a regular sequence to Nœther position and construct a reduced Gröbner basis for the new ideal. In Section 6, we give a new degree upper bound for the Gröbner basis of an ideal generated by a regular sequence. The last section contains a conclusion along with a discussion of possible future research.

[1] In this paper, from the arithmetic complexity we mean the total number of all involved elementary operations such as comparison, addition and multiplication over the base field. Moreover, we assume that the cost of a single operation is one.

## 2. Preliminaries

Throughout this article, we use the following notations. Let $\mathcal{K}$ be an infinite field and $\mathcal{P} = \mathcal{K}[x_1, \ldots, x_n]$ the polynomial ring over $\mathcal{K}$. We consider a sequence $F = f_1, \ldots, f_k$ of non-zero *homogeneous* polynomials in $\mathcal{P}$ and the ideal $\mathcal{I} = \langle f_1, \ldots, f_k \rangle$ generated by this sequence. We assume that $f_i$ has the total degree $d_i$ and that the numbering is such that $d_1 \geq d_2 \geq \cdots \geq d_k > 0$. We also set $d = d_1$. Furthermore, we denote by $\mathcal{R}$ the factor ring $\mathcal{P}/\mathcal{I}$ and by $D := \dim(\mathcal{I})$ its Krull dimension. Any element of this ring is given by $[f] := f + \mathcal{I}$ where $f \in \mathcal{P}$. For us, a *term* is a power product $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ of the variables $x_1, \ldots, x_n$ where $\alpha = (\alpha_1, \ldots, \alpha_n)$. We use throughout the paper the degree reverse lexicographic (drl) term ordering with $x_n \prec \cdots \prec x_1$. We write $x^\alpha \prec_{drl} x^\beta$ when we have either $\deg(x^\alpha) < \deg(x^\beta)$ or they share the same degree and the right-most non-zero element of $\beta - \alpha$ is negative. The *leading term* of a polynomial $f \in \mathcal{P}$, denoted by $\mathrm{LT}(f)$, is the greatest term (with respect to $\prec$) appearing in $f$. The coefficient of $\mathrm{LT}(f)$ in $f$ is called the *leading coefficient* of $f$ and is denoted by $\mathrm{LC}(f)$. The product $\mathrm{LM}(f) := \mathrm{LC}(f).\mathrm{LT}(f)$ is the *leading monomial* of $f$. The *leading term ideal* of $\mathcal{I}$ is defined as $\mathrm{LT}(\mathcal{I}) = \langle \mathrm{LT}(f) \mid 0 \neq f \in \mathcal{I} \rangle$. For the finite set $G \subset \mathcal{P}$, $\mathrm{LT}(G)$ denotes the set $\{\mathrm{LT}(g) \mid g \in G\}$. A finite subset $G \subset \mathcal{I}$ is called a *Gröbner basis* for $\mathcal{I}$ with respect to $\prec$, if $\mathrm{LT}(\mathcal{I}) = \langle \mathrm{LT}(G) \rangle$. We refer to (Cox et al., 2007; Becker and Weispfenning, 1993) for more details on the theory of Gröbner bases.

Given a graded $\mathcal{P}$-module $A$ and a positive integer $s$, we denote by $A_s$ the set of all homogeneous elements of $A$ of degree $s$. Recall that the *Hilbert function* of $\mathcal{I}$ is defined by $\mathrm{HF}_\mathcal{I}(s) := \dim_\mathcal{K}(\mathcal{R}_s)$; the dimension of $\mathcal{R}_s$ as a $\mathcal{K}$-linear space. From a certain degree on, $\mathrm{HF}_\mathcal{I}(s)$ is equal to a (unique) polynomial in $s$, called *the Hilbert polynomial* of $\mathcal{I}$, and denoted by $\mathrm{HP}_\mathcal{I}$. The *Hilbert regularity* of $\mathcal{I}$ is $\mathrm{hilb}(\mathcal{I}) := \min\{m \mid \forall s \geq m,\ \mathrm{HF}_\mathcal{I}(s) = \mathrm{HP}_\mathcal{I}(s)\}$.

The *Hilbert series* of $\mathcal{I}$ is the power series $\mathrm{HS}_\mathcal{I}(t) := \sum_{s=0}^{\infty} \mathrm{HF}_\mathcal{I}(s) t^s$. From Hilbert–Serre theorem, it is known that this series can be written of the form $p(t)/(1-t)^D$ where $p(t)$ is a univariate polynomial with $p(1) \neq 0$ and $D = \dim(\mathcal{I})$, see (Fröberg, 1997, Theorem 7, page 130) and (Kemper, 2011, Chapter 11).

**Proposition 1.** *With these notations,* $\mathrm{hilb}(\mathcal{I}) = \max\{0, \deg(p) - D + 1\}$.

We refer to (Bruns and Herzog, 1993, Proposition 4.1.12) for the proof of this result and to (Cox et al., 2007) for more details on this topic. From Macaulay's theorem, it is known that the Hilbert function of $\mathcal{I}$ is the same as that of $\mathrm{LT}(\mathcal{I})$ and this allows us to derive an effective method to compute the Hilbert series of $\mathcal{I}$ using Gröbner bases, see (Bigatti et al., 1993) and (Greuel and Pfister, 2007, Algorithm 5.2.4). Let us now deal with regular sequences.

**Definition 2.** *The sequence $F$ is called* regular *if for any $i = 2, \ldots, k$, $[f_i]$ is a non-zero divisor in $\mathcal{P}/\langle f_1, \ldots, f_{i-1} \rangle$.*

Because of the natural grading of $\mathcal{P}$, we do not need the additional assumption $\langle F \rangle \neq \mathcal{P}$ usually made in the definition of a regular sequence over arbitrary rings. An ideal generated by a regular sequence is called a *complete intersection*. Let us continue with the definition of Cohen-Macaulay rings. The *depth* of $\mathcal{I}$, denoted by $\mathrm{depth}(\mathcal{I})$, is the length of any maximal regular sequence in $\mathcal{R}$, see (Eisenbud, 1995, page 425). Furthermore, as in was shown in (Seiler, 2010, Proposition 5.2.7), under the assumption that $\mathcal{K}$ is infinite, $\mathrm{depth}(\mathcal{I})$ is equal to the maximal integer $\lambda$ such that there exists a regular sequence of linear (homogeneous) forms $[y_1], \ldots, [y_\lambda]$ in $\mathcal{R}$. For example, for $\mathcal{I} = \langle x_1^2, x_1x_2 \rangle \subset \mathcal{P} = \mathcal{K}[x_1, x_2]$ every linear form $ax_1 + bx_2$ for $a, b \in \mathcal{K}$ is zero divisor in $\mathcal{R}$ and therefore $\mathrm{depth}(\mathcal{I}) = 0$.

**Definition 3.** *The ring $\mathcal{R}$ is called* Cohen-Macaulay *if* $\dim(\mathcal{I}) = \operatorname{depth}(\mathcal{I})$.

For example, one sees readily that the quotient ring $\mathcal{K}[x_1, x_2]/\langle x_2^2\rangle$ is Cohen-Macaulay, whereas $\mathcal{K}[x_1, x_2]/\langle x_1^2, x_1x_2\rangle$ is not Cohen-Macaulay. A proper ideal is said to be *unmixed* if its dimension is equal to the dimension of every associated prime of the ideal (in some references like (Greuel and Pfister, 2007, Definition 4.1.1), this property is referred to as *equidimensional ideal*). For example, the ideal $\langle x_1^2, x_1x_2\rangle = \langle x_1\rangle \cap \langle x_1^2, x_2\rangle$ is not unmixed.

The next theorem, which gives different characterizations for being a regular sequence, is useful throughout the paper. The assertions of this theorem are mostly well-known, however for the convenience of the reader, the proofs are given. To state this theorem, we need one additional definition. For a sequence $F = (f_1, \dots, f_k) \in \mathcal{P}^k$ of homogeneous polynomials, the (first) *module of syzygies* of $F$ is defined to be

$$\operatorname{Syz}(F) = \operatorname{Syz}(f_1, \dots, f_k) = \left\{(g_1, \dots, g_k) \in \mathcal{P}^k \mid \sum_{i=1}^{k} g_i f_i = 0\right\}.$$

If $\{\mathbf{e}_1, \dots, \mathbf{e}_k\}$ is the standard basis of $\mathcal{P}^k$, then for each $i \neq j$, the syzygy element $-f_j\mathbf{e}_i + f_i\mathbf{e}_j \in \operatorname{Syz}(F)$ is called the *principal syzygy* corresponding to $f_i$ and $f_j$ and is denoted by $\pi_{i,j}$. Furthermore, $\operatorname{PSyz}(F)$ stands for the $\mathcal{P}$-module generated by all $\pi_{i,j}$'s.

**Theorem 4.** *With the above notations, let $\mathcal{I} = \langle F\rangle$. The following statements hold true.*

(1) *$F$ being regular is equivalent to the condition that $f_i$ does not belong to any associated prime of $\langle f_1, \dots, f_{i-1}\rangle$.*

(2) *$F$ is a regular sequence iff* $\operatorname{HS}_{\mathcal{I}}(t) = \prod_{i=1}^{k}(1 - t^{d_i})/(1 - t^n)$.

(3) *$F$ is a regular sequence iff* $\dim(\mathcal{I}) = n - k$.

(4) *Any permutation of a regular sequence is a regular sequence as well.*

(5) *Any regular sequence remains regular after performing an invertible linear change of variables.*

(6) *If $F$ is a regular sequence then $\mathcal{I}$ is unmixed and in turn $\mathcal{R}$ is Cohen-Macaulay.*

(7) *$F$ is a regular sequence iff we have* $\operatorname{Syz}(F) = \operatorname{PSyz}(F)$.

*Proof.* (1) follows from (Greuel and Pfister, 2007, Exercise 4.1.13). For the proof of the second item, we refer to (Kreuzer and Robbiano, 2005, Corollary 5.2.17), see also (Fröberg, 1997, Exercise 7, page 137) and (Lejeune-Jalabert, 1984).

To prove the third item, assume that $F$ is a regular sequence. Then, by (2), the Hilbert series of $\mathcal{I}$ can be written as $p(t)/(1 - t)^{n-k}$ where $p$ is a univariate polynomial with $p(1) \neq 0$ and this implies that $\dim(\mathcal{I}) = n - k$. Conversely, let $\sum_{i=1}^{\ell} p_i f_i = 0$ for some $\ell = 2, \dots, k$ be a relation between the $f_i$'s where each $p_i$ is a homogeneous polynomial. We shall prove that $p_\ell \in \langle f_1, \dots, f_{\ell-1}\rangle$. Let $\mathcal{M}$ be the unique maximal homogeneous ideal of $\mathcal{P}$ and $\mathcal{P}_{\mathcal{M}}$ the localization of $\mathcal{P}$ at $\mathcal{M}$ (for more details see e.g. (Matsumura, 1986)). Since $\mathcal{I}\mathcal{P}_{\mathcal{M}}$ is an ideal generated by $k$ elements and of dimension $n - k$ then $f_1, \dots, f_k$ is a regular sequence in $\mathcal{P}_{\mathfrak{m}}$ by (Matsumura, 1986, Theorem 17.4). Thus there exist $\beta, \alpha_1, \dots, \alpha_{\ell-1} \in \mathcal{P}$ and $\beta \notin \mathcal{M}$ (which are not necessarily homogeneous) such that $\beta p_\ell = \sum_{i=1}^{\ell-1} \alpha_i f_i$. Let $\alpha_i'$ be the homogeneous part of $\alpha_i$

of degree $\deg(p_\ell) - \deg(f_i)$ and $\beta' \in \mathcal{K} \setminus \{0\}$ be the homogeneous part of degree 0 of $\beta$. Then we have $p_\ell = \sum_{i=1}^{\ell-1} \alpha'_i/\beta' f_i$ which implies that $p_\ell \in \langle f_1, \dots, f_{\ell-1}\rangle$.

Item (4) is a consequence of (2). To show (5), let $F$ be a regular sequence. We recall that any invertible linear change of variables is a $\mathcal{K}$-linear automorphism of $\mathcal{P}$ which preserves the degree of a polynomial. Thus, the dimension over $\mathcal{K}$ of $\mathcal{I}_s$ for each $s$ as a $\mathcal{K}$-vector space remains invariant and in turn the Hilbert function and the Hilbert series of $\mathcal{I}$ do not change. The assertion now results from (2).

Let us deal with the item (6). Since $F$ is a regular sequence then by (2) we have $\dim(\mathcal{I}) = n - k$. Thus, by the unmixedness theorem proved in (Macaulay, 1916) (see also (Bruns and Herzog, 1993, Theorem 2.1.6)) we know that $\mathcal{I}$ is unmixed. Thus, from Nœther's Normalization Lemma (Heintz, 1983, Lemma 1) it follows that $\mathcal{R}$ is Cohen-Macaulay.

To prove the last item, suppose that $F$ is a regular. We prove the assertion by induction on $k$. For $k = 2$, assume that $(s_1, s_2) \in \mathrm{Syz}(f_1, f_2)$. Then, $s_1 f_1 = -s_2 f_2$. Using the fact that $f_1, f_2$ is regular, $s_2 \in \langle f_1\rangle$ and we can write it as $s_2 = g_1 f_1$. So, $s_1 f_1 = -g_1 f_1 f_2$ and in consequence $s_1 = -g_1 f_2$. It follows that $(s_1, s_2) = g_1.(-f_2, f_1)$ and this shows the basis step. To prove the inductive step, suppose that the assertion holds true for all $m < k$ and we want to prove it for $k$. Let $(s_1, \dots, s_k) \in \mathrm{Syz}(f_1, \dots, f_k)$. Thus, we have $s_k f_k = -\sum_{i=1}^{k-1} s_i f_i \in \langle f_1, \dots, f_{k-1}\rangle$. From hypothesis, $f_1, \dots, f_k$ is a regular sequence and so $s_k \in \langle f_1, \dots, f_{k-1}\rangle$. Therefore, there are $g_1, \dots, g_{k-1} \in \mathcal{P}$ such that $s_k = \sum_{i=1}^{k-1} g_i f_i$. In this situation, we can write

$$\sum_{i=1}^{k-1} s_i f_i + s_k f_k = \sum_{i=1}^{k-1} s_i f_i + \sum_{i=1}^{k-1} g_i f_i f_k = 0,$$

which implies that $s' := (g_1 f_k + s_1, \dots, g_{k-1} f_k + s_{k-1}) \in \mathrm{Syz}(f_1, \dots, f_{k-1})$. However, from induction hypothesis, we know that $s' \in \mathrm{PSyz}(f_1, \dots, f_{k-1})$. Let $s'' := (g_1 f_k + s_1, \dots, g_{k-1} f_k + s_{k-1}, 0) + g_1 \pi_{1,k} + \dots + g_{k-1}\pi_{k-1,k}$. It is easy to observe that $s = s''$ and $s'' \in \mathrm{PSyz}(f_1, \dots, f_k)$ and this proves that $\mathrm{Syz}(f_1, \dots, f_k) = \mathrm{PSyz}(f_1, \dots, f_k)$.

Conversely, suppose that $\mathrm{Syz}(F) = \mathrm{PSyz}(F)$. We prove by induction on $k$ that $f_1, \dots, f_k$ is a regular sequence. Suppose that $\mathrm{Syz}(f_1, f_2) = \mathrm{PSyz}(f_1, f_2)$, and for some $h_2 \in \mathcal{P}$, $h_2 f_2 \in \langle f_1\rangle$. Thus, there exists $h_1 \in \mathcal{P}$ such that $h_1 f_1 = h_2 f_2$ and so $(h_1, -h_2) \in \mathrm{PSyz}(f_1, f_2) = \langle \pi_{1,2}\rangle$. This yields that for a polynomial $h_3 \in \mathcal{P}$, $(h_1, -h_2) = h_3(-f_1, f_2)$ which in particular proves that $h_1 = -h_3 f_1 \in \langle f_1\rangle$ and so $f_1, f_2$ forms a regular sequence. Now, suppose that the assertion holds true for $f_1, \dots, f_i$ for each $i > 1$ and we prove it for $f_1, \dots, f_{i+1}$. Let for some $h_j$'s in $\mathcal{P}$, we have $h_{i+1} f_{i+1} = \sum_{j=1}^{i} h_j f_j \in \langle f_1, \dots, f_i\rangle$. This implies that

$$s := (h_1, \dots, h_i, -h_{i+1}) \in \mathrm{Syz}(f_1, \dots, f_{i+1}) = \mathrm{PSyz}(f_1, \dots, f_{i+1}).$$

Therefore, $s = \sum_{\ell=1}^{i} \sum_{m=\ell+1}^{i+1} p_{\ell,m}\pi_{\ell,m}$, is a representation in terms of principal syzygies for $s$ where $p_{\ell,m} \in \mathcal{P}$ for all $\ell, m$. Henceforth, the last component of $s$ is equal to

$$h_{i+1} = -\sum_{j=1}^{i} p_{j,i+1} f_j \in \langle f_1, \dots, f_i\rangle,$$

and this finishes the proof. □

## 3. Regular sequences in generic position

Some parts of the materials presented in this section have been already published in (Hashemi and Seiler, 2020, Section 3), however, for the sake of completeness, we report them here again.

These results are taken from the French course notes (Lejeune-Jalabert, 1984), where Lejeune-Jalabert studied the maximum degree of the elements in the reduced Gröbner basis of a zero-dimensional ideal. In particular, in this section, we are concerned with the maximum degree of a complete intersection ideal in generic position. For this, let us give some further definitions and notations by keeping the notations of the previous section. The maximum degree of the elements of the reduced Gröbner basis of an ideal $\mathcal{I}$ with respect to $\prec$ is denoted by $\deg(\mathcal{I}, \prec)$.

The notion of genericity that we consider in this section is Nœther position. A homogeneous ideal $\mathcal{I} \subset \mathcal{P}$ is in *Nœther position* if the ring extension $\mathcal{K}[x_{n-D+1}, \dots, x_n] \hookrightarrow \mathcal{R}$ is integral, i.e. $[x_i]$ for any $i = 1, \dots, n-D$ is a root of a polynomial $X^s + [g_1]X^{s-1} + \cdots + [g_s] = [0]$ where $s$ is an integer and $g_1, \dots, g_s \in \mathcal{K}[x_{n-D+1}, \dots, x_n]$, see e.g. (Eisenbud, 1995; Bermejo and Gimenez, 2001) for more details. As a simple example, one sees that the ideal $\langle x_2^2 - x_1 \rangle \subset \mathcal{K}[x_1, x_2]$ is in Nœther position which is not the case for the ideal $\langle x_1 x_2 \rangle \subset \mathcal{K}[x_1, x_2]$.

**Lemma 5.** *Suppose that $f_1, \dots, f_k$ is a regular sequence and $\mathcal{I}$ is in Nœther position. Then, $f_1, \dots, f_k, x_{k+1}, \dots, x_n$ forms a regular sequence.*

*Proof.* Since $\mathcal{I}$ is in Nœther position then, from (Bermejo and Gimenez, 2001, Lemma 4.1), it follows that $\dim(\mathcal{I} + \langle x_{k+1}, \dots, x_n \rangle) = 0$. Thus the assertion follows from Theorem 4. □

**Proposition 6.** *If $f_1, \dots, f_k$ is a regular sequence then* $\mathrm{hilb}(\mathcal{I}) = \max\{0, d_1 + \cdots + d_k - n + 1\}$.

*Proof.* This equality was proved in (Lejeune-Jalabert, 1984, Remarque 3.2.2, page 104), however, we give here a simpler proof for it. By the second item of Theorem 4, we know that

$$\mathrm{HS}_{\mathcal{I}}(t) = \prod_{i=1}^{k}(1 - t^{d_i})/(1-t)^n = (1 + \cdots + t^{d_1 - 1}) \cdots (1 + \cdots + t^{d_k - 1})/(1-t)^{n-k}$$

and the claim follows by using Proposition 1. □

Now, we state the main result of this section. Compared to the notes of Lejeune-Jalabert, we provide here a novel proof based on Gröbner bases.

**Theorem 7.** *(Lejeune-Jalabert, 1984, Corollary 3.5, page 107) Suppose that $f_1, \dots, f_k$ is a regular sequence and $\mathcal{I}$ is in Nœther position. Then* $\deg(\mathcal{I}, \prec) \leq d_1 + \cdots + d_k - k + 1$.

*Proof.* From Lemma 5, we know that $f_1, \dots, f_k, x_{k+1}, \dots, x_n$ is a regular sequence. Let $\mathcal{J}$ be the ideal generated by this sequence. By the proof of Proposition 6, we have $\mathrm{hilb}(\mathcal{J}) = d_1 + \cdots + d_k - k + 1$. On the other hand, from Theorem 4, it follows that $\mathcal{J}$ is a zero-dimensional ideal and in turn $\mathrm{hilb}(\mathcal{J})$ is the maximum degree of the elements of the Gröbner basis of $\mathcal{J}$. We show that the maximum degree of the elements of the reduced Gröbner basis $G$ of $\mathcal{I}$ is equal to that of $\mathcal{J}$. For this, we claim that for each $g \in G$, the leading term of $g$ does not contain any of the variables $x_{k+1}, \dots, x_n$.

We argue by reductio ad absurdum. Suppose, by contradiction, that there exists $g \in G$ so that $x_s \mid \mathrm{LT}(g)$ and $k < s \leq n$. Since $\mathcal{I}$ is a homogeneous and $G$ is a reduced Gröbner basis then $G$ contains only homogeneous polynomials. Without loss of generality, we may assume that $x_s$ is the smallest variable with respect to $\prec$ so that $x_s \mid \mathrm{LT}(g)$. From definition of $\prec$, we can write $g$ as $x_s A + B$ where $A \in \mathcal{K}[x_1, \dots, x_s] \setminus \langle x_{s+1}, \dots, x_n \rangle$ and $B \in \langle x_{s+1}, \dots, x_n \rangle \subset \mathcal{P}$. It follows that $x_s A \in \mathcal{I} + \langle x_{s+1}, \dots, x_n \rangle$, and in consequence $A \in \mathcal{I} + \langle x_{s+1}, \dots, x_n \rangle$ because from Lemma 5, $x_{k+1}, \dots, x_n$ is a regular sequence in the ring $\mathcal{P}/(\mathcal{I} + \langle x_{s+1}, \dots, x_n \rangle)$ and from

Theorem 4, any permutation of this sequence remains regular. Therefore we can deduce that there exists $C \in \langle x_{s+1}, \dots, x_n \rangle$ so that $A + C \in \mathcal{I}$. It follows that there exists $g' \in G$ with $\mathrm{LT}(g') \mid \mathrm{LT}(A) = \mathrm{LT}(A + C)$ which contradicts the minimality of $G$; ending the proof. □

**Corollary 8.** *If $f_1, \dots, f_n$ is a regular sequence then* $\deg(\mathcal{I}, \prec) \leq d_1 + \cdots + d_n - n + 1$.

**Remark 9.** *In the rest of the paper, we refer to $d_1 + \cdots + d_k - k + 1$ as the* Macaulay bound *and denote it throughout by $M$.*

## 4. The $\mathrm{F}_5$ algorithm

In this section, we review the theory behind the $\mathrm{F}_5$ algorithm to compute Gröbner bases, as the pioneer work to design an incremental and signature-based algorithm for the calculation of Gröbner bases, see (Faugère, 2002; Eder and Faugère, 2017) for more details. For the sake of simplicity, Bardet et al. (2015) presented the *matrix-$F_5$ algorithm*; a variant of this algorithm using matrix structure to compute truncated Gröbner bases. Since in the rest of this paper, we are mainly interested in computing such bases using the $\mathrm{F}_5$ structure, we will review the general idea of the matrix-$\mathrm{F}_5$ algorithm from (Bardet et al., 2015).

Below, we recall first some essential notions and definitions that we require in this section. Following the notations of the previous section and given an integer $L$, the matrix-$\mathrm{F}_5$ algorithm runs degree-by-degree up to degree $L$. Thus, the output of this algorithm is indeed an $L$-truncated Gröbner basis:

**Definition 10.** *Let $L$ be a positive integer. The finite set $G \subset \mathcal{I}$ is called an* $L$-truncated Gröbner basis *for $\mathcal{I}$ if every term of degree $\leq L$ in* $\mathrm{LT}(\mathcal{I})$ *belongs to* $\mathrm{LT}(G)$.

Moreover, to be able to use the $\mathrm{F}_5$ criterion, the matrix-$\mathrm{F}_5$ algorithm benefits from an incremental structure, i.e. at each degree $\ell$, it computes $\ell$-truncated Gröbner bases for the ideals $\langle f_1 \rangle, \langle f_1, f_2 \rangle, \dots, \langle f_1, \dots, f_k \rangle$, successively. Indeed at each step, the Gröbner basis of the previous step is used to remove useless reductions. It is worth noting that due to the conditions that we have forced on the $d_i$'s (which is used in the next section) and for a better performance of the $\mathrm{F}_5$ algorithm, it is better to apply this algorithm on the sequence $f_k, \dots, f_1$. However, for simplicity, we keep the fixed order of the $f_i$'s. An interesting idea proposed by Lazard (1983) to compute truncated Gröbner bases is the use of linear algebra techniques on Macaulay matrices. The origin of these kind of matrices is traced back to the works of Macaulay (1903). The *Macaulay matrix* associated to the ideal $\langle f_1, \dots, f_i \rangle$ at the given degree $\ell$, denoted by $\mathcal{M}_{\ell,i}$, has its columns indexed by all terms of degree $\ell$ sorted decreasingly according to $\prec$. Moreover, for each $j \leq i$ and each term $m$ of degree $\ell - d_j$, if any, we add one row whose entries are the coefficients of $mf_j$ written in the appropriate columns. Indeed, this matrix is associated to the $\mathcal{K}$-linear map which sends $(h_1, \dots, h_i)$ to $f := h_1 f_1 + \cdots + h_i f_i$ where $f$ is a homogeneous polynomial of degree $\ell$ and for each $j$, if $h_j$ is non-zero, it is a homogeneous polynomial of degree $\ell - d_j$. To apply the $\mathrm{F}_5$ structure, we need to label each row with a *signature* of the form $(u_r, j_r)$ where $u_r$ is a term and $j_r \in \{1, \dots, i\}$. The general form of this version of the Macaulay matrix is written as follows:

$$\mathcal{M}_{\ell,i} = \begin{array}{c} \\ (u_1, j_1) \\ (u_2, j_2) \\ \vdots \\ (u_t, j_t) \end{array} \begin{array}{c} \begin{array}{cccc} m_1 & m_2 & \dots & m_s \end{array} \\ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1s} \\ a_{21} & a_{22} & \dots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t1} & a_{t2} & \dots & a_{ts} \end{pmatrix} \end{array}.$$

Signatures are used to order the polynomials (to control the division of polynomials) in order to apply the $F_5$ criterion. To order the signatures, we write $(u_r, j_r) < (u_e, j_e)$ whenever $j_r < j_e$ or $j_r = j_e$ and $u_r \prec u_e$. The signature $(u_r, j_r)$ associated to the $r$-th row shows that the corresponding polynomial $a_{r1}m_1 + \cdots + a_{rs}m_s$ is presented as the sum of $u_r f_{j_r}$ with some smaller polynomials. Once the Macaulay matrix is produced, we perform *valid* Gaussian elimination operations on $\mathcal{M}_{\ell,i}$ to reduce the rows by respecting the signatures. More clearly, given two rows $R_r$ and $R_s$ with signatures $(u_r, j_r)$ and $(u_e, j_e)$ respectively and given $\lambda \in \mathcal{K}$, the row $R_r$ can be substituted by $R_r + \lambda R_t$ only if $(u_e, j_e)$ is smaller than $(u_r, j_r)$. Let $\tilde{\mathcal{M}}_{\ell,i}$ denote the result of performing valid Gaussian elimination operations on $\mathcal{M}_{\ell,i}$. The efficiency of the matrix-$F_5$ algorithm comes from applying the well-known $F_5$ criterion to detect the reductions to zero (Bardet et al., 2015, Proposition 8). Due to this criterion, in the construction of $\mathcal{M}_{\ell,i}$ if we find a row whose signature is of the form $(m, i)$ and $m$ is divisible by the leading term of an already computed row with the signature $(m', j)$ so that $j < i$ then that row is superfluous.

**Theorem 11** ($F_5$ criterion)**.** *Keeping the above notations, any row in $\mathcal{M}_{\ell,i}$ with the signature $(m, i)$ such that $m$ is the leading monomial of a polynomial constructed in $\tilde{\mathcal{M}}_{\ell-d_i,i-1}$ linearly depends on the other rows of $\mathcal{M}_{\ell,i}$ and in turn can be removed.*

Assume that we have already computed $\tilde{\mathcal{M}}_{\ell,i}$ for any $\ell < L$ and any $i < k$. Then, to construct an $L$-truncated Gröbner basis for $\mathcal{I}$, we first produce $\mathcal{M}_{\ell,i+1}$. In this process, if the $F_5$ criterion is applicable then we use it to remove useless rows. Once we compute $\tilde{\mathcal{M}}_{\ell,1}, \ldots, \tilde{\mathcal{M}}_{\ell,k}$ then we go for the next degree and continue to reach an $L$-truncated Gröbner basis for $\mathcal{I}$. Finally, it is worth noting that for an enough large value of $L$, an $L$-truncated Gröbner basis for $\mathcal{I}$ remains a Gröbner basis for the ideal. However, if we do not know in advance this value of $L$, then using Buchberger's first criterion, we must continue to find a value for $L$ such that applying the matrix-$F_5$ algorithm on $\langle f_1, \ldots, f_k\rangle$ from degree $L$ up to $2L$ does not give rise to any new leading terms.

## 5. An effective regular sequence test

In this section, we apply the matrix-$F_5$ algorithm to detect whether a given sequence of homogeneous polynomials is regular. Moreover, we study the complexity of transforming an ideal (resp. generated by a regular sequence) to Nœther position (resp. and computing a reduced Gröbner basis for the new ideal). To do so, we first investigate some properties of the matrix-$F_5$ algorithm whenever the input polynomials form a regular sequence. The following key lemma was already given in (Faugère, 2002) (see also (Bardet et al., 2015, Theorem 9)), but without a complete proof which we provide here for the convenience of the reader.

**Lemma 12.** *Let $L = \deg(\mathcal{I}, \prec)$. No reduction to zero will occur during the execution the matrix-$F_5$ algorithm to compute a(n $L$-truncated) Gröbner basis for $\mathcal{I}$ iff $f_1, \ldots, f_k$ is a regular sequence.*

*Proof.* By reductio ad absurdum, assume that $\sum_{i=1}^{j} h_i f_i = 0$ is a reduction to zero with the signature $(\mathrm{LT}(h_j), j)$ occurred in the course of the algorithm to compute a Gröbner basis at the $j$-th step. Thus, from assumption we have $h_j = \sum_{\ell=1}^{j-1} p_\ell f_\ell \in \langle f_1, \ldots, f_{j-1}\rangle$ for $p_\ell \in \mathcal{P}$. Consequently, $\mathrm{LT}(h_j)$ is divisible by the leading term of some polynomial in a Gröbner basis of $j-1$-th step. Thus, it would be detected by the $F_5$ criterion (see Theorem 11), leading to a contradiction. Hence, no reduction to zero will be appeared during the execution of the matrix-$F_5$ algorithm. For an alternative proof, see (Bardet et al., 2015, Theorem 9).

To prove the converse result, let $f_1, \dots, f_k$ be the input of the matrix-$F_5$ algorithm and no reduction to zero occurs during the execution of this algorithm. We show that this sequence is regular. Suppose that $hf_i \in \langle f_1, \dots, f_{i-1} \rangle$ where $h \in \mathcal{P}$ and $Grob_{i-1} = \{g_1, \dots, g_\ell\}$ is a Gröbner basis of $\langle f_1, \dots, f_{i-1} \rangle$. Furthermore, assume that $h$ is not reducible by $Grob_{i-1}$ and $h$ has the minimal leading term w.r.t $\prec$ among all the polynomials having these properties. In this situation, there exist $h_1, \dots, h_\ell$ such that $hf_i - \sum_{j=1}^{i-1} h_j g_j = 0$. However, this expression exhibits a linear dependency in the matrix $\mathcal{M}_{\ell,i}$ where $\ell = \deg(hf_i)$ and this leads to a reduction to zero in the $i$-the step. This contradiction ends the proof. □

**Example 13.** *In this example, we show that the method presented in Lemma 12 is not in general effective to test whether a given sequence of polynomials is regular. For example, let us consider the ideal* $\mathcal{I} = \langle x_1^2x_4 - 11x_5^2x_4 + 10x_2^2x_4 + 10x_3^2x_4 + 10x_5^3, 10x_1^2x_3 - 11x_5^2x_3 + 10x_2^2x_3 + 10x_3x_4^2 + 10x_5^3, 10x_1x_2^{20} - 11x_5^{20}x_1 + 10x_5^{18}x_1x_3^2 + 10x_5^{18}x_1x_4^2 + 10x_5^{21}, 10x_1^2x_2 - 11x_5^2x_2 + 10x_2x_3^2 + 10x_2x_4^2 + 10x_5^3 \rangle$ *and the drl ordering with* $x_5 \prec x_4 \prec x_3 \prec x_2 \prec x_1$*. Then, the matrix-*$F_5$ *algorithm needs to continue up to degree* 39 *to compute a Gröbner basis for this ideal and to be sure that the generating set of* $\mathcal{I}$ *is a regular sequence. Below, we will show that we can check this property in a lower degree.*

The next corollary is helpful in the proof of the main result of this section.

**Corollary 14.** *Assume that we are applying the matrix* $F_5$ *algorithm to compute a Gröbner basis for* $\mathcal{I} = \langle f_1, \dots, f_k \rangle$*. Then, at the* $i$*−th step of this computation, a reduction to zero at degree* $\ell$ *happens iff there exists a polynomial* $h \notin \langle f_1, \dots, f_{i-1} \rangle$ *of degree* $\ell - d_i$ *such that* $hf_i \in \langle f_1, \dots, f_{i-1} \rangle$*.*

*Proof.* The proof is a straightforward consequence of the proof of Lemma 12. □

Let us state the main result of this paper.

**Theorem 15.** *Let consider the sequence* $F = f_1, \dots, f_k$ *with* $d_i = \deg(f_i)$ *for each* $i$ *and* $d := d_1 \geq \cdots \geq d_k$*. Then,* $F$ *is regular iff there exists no reduction to zero up to the degree* $M := d_1 + \cdots + d_k - k + 1$ *during the execution of the matrix-*$F_5$ *algorithm to compute an* $M$*-truncated Gröbner basis for* $\mathcal{I}$*. Moreover, if* $d \geq 2$*, the arithmetic complexity of this test is* $d^{O(n)}$

*Proof.* From Nœther normalization lemma (Kemper, 2011, Remark 8.20) and using the fact that $\mathcal{K}$ is infinite, there exists a linear and invertible transformation $\varphi$ such that $\varphi(\mathcal{I})$ is in Nœther position. Note that $\varphi$ transforms a homogeneous polynomial into a homogeneous polynomial of the same degree. Furthermore, from Theorem 4, it follows that $F$ is regular iff $\varphi(F) := \varphi(f_1), \dots, \varphi(f_k)$ is a regular sequence. Finally, from Theorem 7, we know that $\deg(\varphi(\mathcal{I}), \prec) \leq M$.

Suppose that $F$ is not a regular sequence. So $\varphi(F)$ is not regular too. Now, using the latter inequality, assume that we compute a full Gröbner basis or equivalently an $M$-truncated Gröbner basis of $\varphi(\mathcal{I})$ by applying the matrix-$F_5$ algorithm. According to Lemma 12 and Corollary 14, there exist an index $i$ and $\ell \leq M$ so that a zero reduction corresponding to the relation $h_1\varphi(f_1) + \cdots + h_i\varphi(f_i) = 0$ occurs where $h_i \notin \langle \varphi(f_1), \dots, \varphi(f_{i-1}) \rangle$ and $\deg(h_i f_i) = \ell$. However, applying $\varphi^{-1}$ on these relations results that $\varphi^{-1}(h_1)f_1 + \cdots + \varphi^{-1}(h_i)f_i = 0$ and $\varphi^{-1}(h_i) \notin \langle f_1, \dots, f_{i-1} \rangle$. Therefore, from Corollary 14 it yields that a reduction to zero at degree $\ell$ appears during the execution of the matrix-$F_5$ algorithm on $f_1, \dots, f_k$. Since all used implications hold true in both directions, the converse holds true as well.

To prove the complexity bound, applying the first result, we shall need to construct an $M$-truncated Gröbner basis of $\mathcal{I}$ by using the matrix-$F_5$ algorithm. For this, we need to construct

$\mathcal{M}_{\ell,i}$ for each $\ell \leq M$ and $i = 2, \dots, k$. Let us discuss the size of $\mathcal{M}_{M,k}$ which has the biggest size among all the constructed matrices. This matrix has $\sum_{i=1}^{k} \binom{n+M-d_i-1}{n-1}$ rows and $\binom{n+M-1}{n-1}$ columns. From (Hashemi and Lazard, 2011, Lemma 3.2), we know that $\binom{n+M-1}{n-1} \leq (ed)^{n-1}$ where $e = 2.71828\cdots$ is the usual Euler number. If $k > n$ then, $F$ is not regular. Thus, we will assume that $k \leq n$. It is easily seen that the number of rows is at most $n(ed)^{n-1}$. On the other hand, from $d \geq 2$ we have $n < d^n$. All these arguments along with the fact that the cost of performing Gaussian elimination on an $N \times N$ matrix is $N^\omega$ with $\omega < 2.3728639$ (see (Alman and Williams, 2021; Le Gall, 2014)) proves the assertion. □

As a consequence of the proof of this theorem, we show that, we are able to transform a complete intersection ideal into Nœther position and at the same time compute a reduced Gröbner basis for the new ideal with the arithmetic complexity $d^{O(n^2)}$.

**Proposition 16.** *Let us consider the regular sequence $F = f_1, \dots, f_k$ with $d_i = \deg(f_i)$ for each $i$ and $2 \leq d := d_1 \geq \cdots \geq d_k$. Then, transforming the ideal $\mathcal{I}$ into Nœther position as well as constructing the reduced Gröbner basis with respect to $\prec$ for the new ideal can be performed in $d^{O(n^2)}$.*

*Proof.* This proof follows essentially the same steps as the proof of (Giusti, 1988, Theorem 5.6.3) which goes back to Lazard (Lazard, 1977, Algorithm 7.2). For this purpose, for a fixed integer $1 \leq i \leq n$, consider the (parametric) linear change $\varphi_i$ of variables which sends $x_j$ for each $j > i$ to $x_j + a_{ij}x_i$. Thus, we obtain polynomials $\varphi_i(F_i) := \varphi_i(f_1), \dots, \varphi_i(f_i)$ and in turn the ideal $\varphi_i(\mathcal{I}_i) \subset \mathcal{K}[a_{i(i+1)}, \dots, a_{in}][x_1, \dots, x_n]$ generated by these homogeneous polynomials. As already mentioned, Nœther normalisation lemma (Kemper, 2011, Theorem 8.19) shows that there exists $a_{ij}$'s in $\mathcal{K}$ such that $\varphi_i(\mathcal{I}_i)$ is in Nœther position. Our aim is to determine, for each $i$, the values for the $a_{ij}$'s such that $\varphi_i(\mathcal{I}_i)$ is in Nœther position and simultaneously to find the reduced Gröbner basis for $\varphi_i(\mathcal{I}_i)$.

For $i = 1$, consider the map $\varphi_1$ by sending $x_j$ for each $j > 1$ to $x_j + a_{1j}x_1$. Then, $\varphi_1(f_1)$ is a polynomial with the leading term $x_1^{d_1}$ whose coefficient is a polynomial in $\mathcal{K}[a_{12}, \dots, a_{1n}]$ of degree $d_1$. From (Giusti, 1988, Proposition 5.3.5), it follows that given a polynomial $f$ in $n$ variables of degree $\delta$, one needs to perform $\delta^{O(n)}$ operations to get a point $(a_1, \dots, a_n) \in \mathcal{K}^n$ such that $f(a_1, \dots, a_n) \neq 0$. This shows that the number of operations to find $a_{12}, \dots, a_{1n}$ such that $\varphi_1(\mathcal{I}_1)$ is in Nœther position is $d^{O(n)} \leq d^{O(n^2)}$ (note that this complexity includes also the cost of all intermediate operations such as the distribution of polynomials).

Now, without loss of generality, assume that the ideal $\mathcal{I}_{i-1} = \langle f_1, \dots, f_{i-1} \rangle$ is in Nœther position. Let $\varphi_i$ be the linear transformation which maps $x_j$ for each $j > i$ to $x_j + a_{ij}x_i$. Let us consider the classical Macaulay matrix[2] $Mac_i$ of degree $M_i := d_1 + \cdots + d_i - i + 1$ by using $\varphi_i(f_1), \dots, \varphi_i(f_i)$. The entries of this matrix lie in the ring $\mathcal{K}[a_{i(i+1)}, \dots, a_{in}]$ and the degree of each entry in terms of these parameters is at most $M_i$. Performing elementary row operations on $Mac_i$ over this ring transforms it to row echelon form. Let us refer to this new matrix as $\tilde{Mac}_i$. Since $Mac_i$ is of size $d^{O(n)} \times d^{O(n)}$ (see the proof of Theorem 15), then it is not hard to see that each entry of $\tilde{Mac}_i$ is a quotient of polynomials which have degree at most $d^{O(n)}$. Hence, the number of field operations to find the point $(a_{i(i+1)}, \dots, a_{in})$ such that the values of all pivots of $\tilde{Mac}_i$ at this point are all non-zero is $d^{O(n^2)}$. By replacing the values of the $a_{ij}$'s in $\varphi_i$, we get the map $\varphi_i$, which transforms $\mathcal{I}_i$ into Nœther position. By Theorem 7, we know that $\deg(\varphi_i(\mathcal{I}_i), \prec) \leq M_i$.

[2]From this we mean, we do not use the signature structure and in addition we do not remove any rows.

Therefore, replacing the values of the $a_{ij}$'s in $\tilde{Mac}_i$ gives the reduced Gröbner basis for $\varphi_i(\mathcal{I}_i)$ with respect to $\prec$. These arguments show that the whole number of field operations to transform $\mathcal{I}_i$ into Nœther position is $d^{O(n^2)}$. Since, $k \leq n$ and $n \leq d^n$ the claim is finally established. □

Below, we show that a similar complexity holds in the case that $F$ is not regular. For this purpose, we need a classical result in commutative algebra which states that if $F$ is not a regular sequence then by a combination of the $f_i$'s, we may assume that $F$ contains the longest possible regular sequence inside the ideal $\mathcal{I}$.

**Lemma 17.** *((Lejeune-Jalabert, 1984, Prop. 4.1, page 108)) There exist homogeneous polynomials $g_1, \dots, g_{n-D} \in \mathcal{P}$ such that the following conditions hold:*

(1) $\deg(g_i) = d_i$ *for each i,*

(2) $g_i \equiv \lambda_i f_i \mod \langle f_{i+1}, \dots, f_k \rangle$ *for some* $0 \neq \lambda_i \in \mathcal{K}$ *for* $i = 1, \dots, n-D$,

(3) $g_1, \dots, g_{n-D}$ *is regular sequence in* $\mathcal{P}$.

**Theorem 18.** *Keeping the notations of Proposition 16, assume that F is not necessarily regular. Then, transforming the ideal $\mathcal{I}$ into Nœther position has the complexity of $(kd^n)^{O(n)}$.*

*Proof.* Using Lemma 17, assume that $g_1, \dots, g_{n-D}$ is a regular sequence inside the ideal $\mathcal{I}$. It is clear to see that the $\mathcal{K}$-linear space generated by homogeneous polynomials of degree $M$ in $\langle g_1, \dots, g_{n-D} \rangle$ is a subset of the space generated by polynomials of degree $M$ generated by $F$. On the other hand, if the map $\varphi$ transforms $\langle g_1, \dots, g_{n-D} \rangle$ into Nœther position then it transforms $\mathcal{I}$ into this position as well. From the proof of Proposition 16, we conclude that working on the $\mathcal{K}$-linear space generated by $F$ at degree $M$ produces the desired map to transform $\mathcal{I}$ into Nœther position. For this purpose, it is equivalent to consider the classical Macaulay matrix of $F$ at this degree. Below, we need the number of rows and columns of this matrix which are $(kd^n)^{O(1)}$ and $d^{O(n)}$, respectively.

Let $\varphi_1$ be the linear transformation which sends $x_j$ for each $j > 1$ to $x_j + a_{1j}x_1$. Let $Mac_1$ be the Macaulay matrix at degree $M$ of $\varphi_1(f_1), \dots, \varphi_1(f_k)$. The entries of $Mac_1$ lies in $\mathcal{K}[a_{12}, \dots, a_{1n}]$ and have degree at most $M$. From the proofs of Theorem 15 and Proposition 16, we conclude that the size of this matrix is $k(ed)^{n-1} \times (ed)^{n-1}$ which can be interpreted as $(kd^n)^{O(1)} \times d^{O(n)}$. By means of a finite sequence of elementary row operations, let us transform $Mac_1$ in row echelon form and $\tilde{Mac}_1$ be the new matrix. Note that we do not need to complete this process and it suffices to find a new matrix such that there exists a row whose pivot is a pure power of $x_1$. The entries of $\tilde{Mac}_1$ have degree at most $(kd^n)^{O(1)}$. It follows that the number of field operations to find the point $(a_{12}, \dots, a_{1n})$ such that the value of the desired pivot of $\tilde{Mac}_1$ at this point is non-zero is $(kd^n)^{O(n)}$ (this complexity includes the cost of performing the elementary row operations). Therefore, within this complexity, we are able to find the map $\varphi_1$ such that a pure power of $x_1$ appears in $\varphi_1(\mathcal{I})$. By repeating this process for $i = 2, \dots, n-D$ (note that in the $i$-th step, we perform the map $\varphi_i$ on $\varphi_{i-1} \circ \cdots \circ \varphi_1(F)$ we get the complexity $(n-D)(kd^n)^{O(n)} = (kd^n)^{O(n)}$. This yields the map $\varphi_{n-D} \circ \cdots \circ \varphi_1$ which transforms $\mathcal{I}$ into Nœther position. □

**Remark 19.** *We shall note that the complexity $(nkd)^{O(n^2)} = (kd)^{O(n^2)}$ has been proved in (Giusti, 1988, Theorem 5.6.3). We think that our proof of Theorem 18 is simpler than the one given in that paper. Furthermore, in (Giusti and Heintz, 1993) (see also (Giusti et al., 2000, Theorem 3)), a randomised algorithm has been described which transforms the ideal $\mathcal{I}$ into Nœther position within the complexity of $(kd^n)^{O(1)}$.*

**Remark 20.** *The aim of this paper is not to discuss the efficiency of the proposed algorithm to transform ideals into Nœther position. In this paper, we only consider the complexity issue related to this problem. In the proof of this theorem, we do not need to take into account the complexity of finding* $g_1, \ldots, g_{n-D}$ *by applying Lemma 17. Studying this complexity will be the subject of another work.*

We have implemented the matrix-$F_5$ algorithm to apply Theorem 15 to test whether or not a given sequence of polynomials is regular. However, since in this algorithm, we need to construct all the intermediate matrices degree-by-degree then it is not efficient enough in practice. Then, we implemented the classical $F_5$ algorithm (Faugère, 2002) to detect whether a given sequence of polynomials is regular. For this purpose, it is enough to restrict the degree of the computation by the Macaulay bound $M$ for each step of the computation. In the sequel, we use this variant of the $F_5$ algorithm and refer to it as $F_5$M. To show the efficiency of this approach in practice, we have implemented a prototype version of both $F_5$ and $F_5$M algorithms in Maple 17. The source code of these algorithms as well as the used examples are available at `http://amirhashemi.iut.ac.ir`.

All the experiments were made on an Intel(R) Core(TM) i7-2620M, 2.70 GHz, 4GB RAM and 64 bits running under Windows operating system. All computations have been done over the field $\mathbb{Q}$. The results are shown in the following table where the first column shows the the name of the instance (see the appendix). The "Time" and "Memory" columns indicate, respectively, the CPU time in seconds and the amount of used memory in gigabytes of the computation.

Remark that for each regular sequence $f_1, \ldots, f_k$ with $\deg(\langle f_1, \ldots, f_k\rangle, \prec) > M$, the $F_5$M is more efficient than the $F_5$ algorithm (note that all the selected examples in the appendix are regular sequences satisfying this property and they have been chosen randomly). In addition, we note that in the case that $f_1, \ldots, f_k$ is not regular both algorithms share the same efficiency as well.

| **Sequence** | **$F_5$** | | **$F_5$M** | |
|---|---|---|---|---|
| | **Time** | **Memory** | **Time** | **Memory** |
| Seq. 1. | 2.2 | 0.12 | 0.66 | 0.04 |
| Seq. 2. | 24 | 1.7 | 0.33 | 0.03 |
| Seq. 3. | 28 | 1.8 | 1 | 0.07 |
| Seq. 4. | 33 | 7.6 | 0.73 | 0.33 |
| Seq. 5. | 37.2 | 2.3 | 5.1 | 0.25 |
| Seq. 6. | 54.3 | 2.92 | 5.1 | 0.25 |
| Seq. 7. | 56.3 | 4.4 | 0.27 | 0.02 |
| Seq. 8. | 80 | 4.6 | 3 | 0.19 |
| Seq. 9. | 122 | 7.1 | 9 | 0.5 |
| Seq. 10. | 718.92 | 31.81 | 6.2 | 0.33 |

Table 1: Comparison of the $F_5$ and $F_5$M algorithms.

## 6. New degree upper bounds

In this section we study the degree upper bounds for the Gröbner basis of an ideal generated by a regular sequence. Our new bound is obtained by analysing the methods presented in (Dubé,

1990) and (Mayr and Ritscher, 2013) in the special case that the given ideal is generated by a regular sequence. For this, we first recall some basic definitions from (Dubé, 1990). If $G$ is a Gröbner basis for $\mathcal{I}$ then we let $N_{\mathcal{I}} = \{\mathrm{NF}_G(f) \mid f \in \mathcal{P}\}$.

**Definition 21.**
- *For a homogeneous polynomial $h$ and the subset $u \subseteq \{x_1, \dots . x_n\}$, the set $C(h,u) = \{gh \mid g \in \mathcal{K}[u]\}$ is called the* cone *generated by $h$ and $u$.*
- *A set $P = \{C(h_1,u_1), \dots, C(h_t,u_t)\}$ of cones is called a* cone decomposition *for $T \subset \mathcal{P}$ if every polynomial in $T$ can be* uniquely *written as the sum of the elements of $C(h_i,u_i)$'s.*

**Example 22.** *For example, the set $\{C(x_1x_2,\{x_1,x_2,x_3\}), C(x_2x_3,\{x_2,x_3\})\}$ is a cone decomposition for the ideal $\mathcal{I} = \langle x_1x_2, x_2x_3\rangle \subset \mathcal{K}[x_1,x_2,x_3]$.*

For a cone decomposition $P$, the notion $P^+$ refers to $\{C(h,u) \in P \mid u \neq \emptyset\}$.

**Definition 23.** *Let $k$ be a non-negative integer and $P$ a cone decomposition for the set $T \subset \mathcal{P}$. Then, $P$ is called $k$-*exact *if the following conditions hold:*

1. *there is no cone $C(h,u) \in P^+$ with $\deg(h) < k$,*
2. *for each $C(g,v) \in P^+$ and $k \leq d \leq \deg(g)$, there exists $C(h,u) \in P^+$ with $\deg(h) = d$ and $|u| \geq |v|$,*
3. *for each $d$, there exists at most one $C(h,u) \in P^+$ with $\deg(h) = d$.*

**Example 24.** *Let us consider the ideal $\mathcal{I} = \langle x_1^3, x_1x_2x_3, x_1^2x_2\rangle \subset \mathcal{K}[x_1,x_2,x_3]$. Then, cone decomposition $\{C(1,\{x_2,x_3\}), C(x_1,\{x_3\}), C(x_1x_2^2,\{x_2\}), C(x_1x_2,\{\}), C(x_1^2,\{x_3\})\}$ is a $0$-exact decomposition for $N_{\mathcal{I}}$.*

**Definition 25.** *Let $P$ be a $k$-exact cone decomposition. For each $i = 0,\dots,n+1$, the $i$-th* Macaulay constant *of $P$ is defined to be*

$$b_i = \min\{d \geq k \mid \forall C(h,u) \in P; |u| \geq i \Longrightarrow \deg(h) < d\}.$$

We note as a simple observation that $b_0 \geq b_1 \geq \cdots \geq b_{n+1} = k$. It was shown in (Hashemi et al., 2022, Proposition 3.2) that if we fix the Macaulay constant $b_{n+1} := d$, then the other Macaulay constants remain unique. In Example 24, the Macaulay constants for the given cone decomposition are $b_0 = 4, b_1 = 4, b_2 = 1, b_3 = 0$ and $b_4 = 0$. (Dubé, 1990) by applying some combinatorial arguments to bound the Macaulay constants of any cone decomposition of $N_{\mathcal{I}}$, found a degree upper bound for any reduced Gröbner basis of $\mathcal{I}$.

(Mayr and Ritscher, 2013) provided a deeper analysis of the method due to Dubé to give a dimension-depending upper bound for Gröbner bases. Let us quickly recall some results from their paper. Furthermore, let $\mathcal{I}$ be generated by the homogeneous polynomials $f_1,\dots,f_k \in \mathcal{P}$ with $\deg(f_1) \geq \cdots \geq \deg(f_k)$ and $D = \dim(\mathcal{I})$. One of the main topics discussed in (Mayr and Ritscher, 2013) is to embed a homogeneous regular sequence $g_1,\dots,g_{n-D}$ in $\mathcal{I}$ such that $\deg(g_i) = \deg(f_i)$ for $1 \leq i \leq n-D$. Schmid in (Schmid, 1995, Lemma 2.2) (see also (Mayr and Ritscher, 2013, Lemma 9)) proved that by a generic linear combination of the $f_i$'s one can always find such a regular sequence. In addition, Mayr and Ritscher in (Mayr and Ritscher, 2013, Lemma 21) proved the following auxiliary decomposition

$$\mathcal{I} = \langle g_1,\dots,g_{n-D}\rangle \oplus \bigoplus_{i=1}^{k} f_i \cdot N_{\mathcal{J}_{i-1}:f_i} \qquad (1)$$

where $\mathcal{J}_i = \langle g_1, \dots, g_{n-D}, f_1, \dots, f_i \rangle$. Then they used this decomposition (Mayr and Ritscher, 2013, Lemma 22) to show that any 0-exact cone decomposition $Q$ for $N_{\mathcal{I}}$ can be extended to a $\deg(f_1)$-exact cone decomposition $P$ for $N_{\mathcal{J}}$ where $\mathcal{J} = \langle g_1, \dots, g_{n-D} \rangle$ such that $\deg(Q) \leq \deg(P)$. Finally, they proved a dimension-depending upper bound for the Macaulay constant $a_0 = \deg(P) + 1$ of $P$ which remains an upper bound for the maximum degree of the polynomials in any reduced Gröbner basis of $\mathcal{I}$. In the case that $f_1, \dots, f_k$ forms already a regular sequence, we do not need to embed a regular sequence in the ideal $\mathcal{I}$ and this may entail to a slightly sharper upper bound, see the next theorem.

**Theorem 26.** *Let $\mathcal{I} \subset \mathcal{P}$ be the ideal generated by the homogeneous regular sequence $f_1, \dots, f_k$ of degrees $d_1, \dots, d_k$ with $d_1 \cdots d_k \geq 2$. Then, the maximum degree of the polynomials in any reduced Gröbner basis G of $\mathcal{I}$ is bounded above by $2\big(d_1 \cdots d_k/2\big)^{2^{n-k-1}}$ whenever $n-k \geq 1$. In the case that $k = n$, the upper bound becomes $d_1 + \cdots + d_n - n + 1$.*

*Proof.* By the above notations, since $\mathcal{I}$ is generated by a regular sequence then there is no need to construct $\mathcal{J}_i$'s and this provides the first improvement. Thus, instead of considering a $d$-exact cone decomposition with $d = \max\{d_1, \dots, d_k\}$ we can consider a 0-exact cone decomposition $P$. Suppose that $n - k \geq 1$ and $b_0, \dots, b_{n+1}$ are the Macaulay constants of $N_{\mathcal{I}}$ corresponding to $P$. Using (Hashemi et al., 2022, Lemma 3.5), we conclude that $b_i = 0$ for $i = n - k + 1, \dots, n + 1$. Now, we proceed by induction to show that $b_{s-1} \leq b_s^2/2$ for each $2 \leq s \leq n - k$. For the basis of the induction, we show that $b_{n-k-1} \leq b_{n-k}^2/2$. By applying (Hashemi et al., 2022, Theorem 4.5), we have $b_{n-k} = d_1 \cdots d_k$ and $b_{n-k-1} = b_{n-k}^2/2 - b_{n-k}[d_1 + \cdots + d_k - (k+1)]/2$. Since $d_i \in \mathbb{N}$ for every $i$ and $d_1 \cdots d_k \geq 2$ then $d_1 + \cdots + d_k - (k+1) \geq 0$ and in turn $b_{n-k-1} \leq b_{n-k}^2/2$. To prove the induction step, we have $b_1 \geq \cdots \geq b_{n-k} \geq 2$ and therefore we are able to follow the proof of (Mayr and Ritscher, 2013, Lemma 31) to get $b_{s-1} \leq b_s^2/2$ for any $2 \leq s \leq n - k$ (note that the proof of the induction basis was missing in (Mayr and Ritscher, 2013) and we gave it here for the sake of completeness). It follows that $b_1 \leq 2(b_{n-k}/2)^{2^{n-k-1}}$. On the other hand, from (Dubé, 1990, Lemma 7.2.), the maximum degree of the elements of $G$ is at most $b_0$. Furthermore, since $\mathcal{I}$ is generated by a regular sequence then it was shown in (Hashemi et al., 2022, Lemma 4.4.) that $b_0 = b_1$. These arguments show that $b_0 = b_1 \leq 2(b_{n-k}/2)^{2^{n-k-1}}$ is an upper bound for the maximum degree of the elements of $G$. In the case that $k = n$, from Corollary 8, the desired upper bound becomes $d_1 + \cdots + d_n - n + 1$. ☐

## 7. Conclusion

In this paper, by applying the structure and properties of the (matrix-)$F_5$ algorithm, we presented an effective method to test whether a sequence of homogeneous polynomials is regular. Furthermore, we gave a sharper degree upper bound for the maximum degree of the elements of any reduced Gröbner basis of an ideal generated by a homogeneous regular sequence. Now, an interesting question that may arise is how we can give a similar complexity bound to test whether a sequence of not necessarily homogeneous polynomials is regular. The first idea that comes to mind is to homogenize the given sequence and apply then the method described in this paper. However, this does not work in general. As a simple counterexample, let $f_1 = x_1^3x_2 - x_3^3, f_2 = x_1^2x_2^2 - x_4^3$ and $f_3 = x_1x_2^3 - x_5^3$ be a sequence of non-homogeneous polynomials in $\mathbb{Q}[x_1, x_2, x_3, x_4, x_5]$. It can be easily seen that this sequence is regular. Let $f_1^h = x_1^3x_2 - x_3^3h, f_2^h = x_1^2x_2^2 - x_4^3h$ and $f_3^h = x_1x_2^3 - x_5^3h$, be the homogenization of the $f_i$'s with respect to the new variable $h$. Since $\langle f_1^h, f_2^h, f_3^h \rangle$ has dimension 4 in $\mathbb{Q}[x_1, x_2, x_3, x_4, x_5, h]$, then $f_1^h, f_2^h, f_3^h$ is not regular (see Theorem 4). So, as a future work, we intend to provide an effective method to test whether a given sequence of affine polynomials is regular or not.

Another direction of research is to improve the complexity bound presented in Proposition 16. Using the approach described in (Hashemi et al., 2018) and linear algebra techniques, we believe that we are able to establish the complexity $d^{O(n)}$ to transform a given homogeneous ideal into Nœther position and compute a reduced Gröbner basis for the new ideal in the case that the given ideal is complete intersection, see (Giusti and Heintz, 1993). Furthermore, we will investigate to extend this study to other notions of genericity in order to provide an effective method to compute Pommaret bases.

## Appendix

$$
\begin{aligned}
\text{Sequence 1} \quad &= \quad -x_1^5x_2^5x_5^2 + x_2x_4^4x_5^7 - x_3x_5^{11},\\
&\quad\;\; x_1^2x_2^3x_3 - x_1^3x_4^3 - x_1x_3^5 + x_2^2x_3^3x_4 + x_2^2x_3x_4^3,\\
&\quad\;\; -x_1^3 + x_1x_2^2 + x_1x_3^2\\
\text{Sequence 2} \quad &= \quad x_1^5x_4^5 - x_1^4x_4^3x_5^3 - x_1^2x_2x_3^2x_4^4x_5 + x_1^2x_2x_5^7 + x_1^2x_4^5x_5^3 - x_2^2x_4^6x_5^2,\\
&\quad\;\; x_1x_3^3 + x_1x_2^2x_4 + x_1x_2x_4^2 + x_2x_3^3 - x_4^4,\\
&\quad\;\; x_1^3 - x_1^2x_2 + x_1^2x_3 + x_1x_2^2 - x_1x_3^2 - x_2^3 + x_2^2x_3\\
\text{Sequence 3} \quad &= \quad -x_2^7x_3^3 - x_1^4x_3^3x_4^3 - x_1^3x_4^5x_5^2 + x_1x_2x_3^4x_4^2x_5^2 - x_1x_2x_3^3x_4^5 + x_1x_3^8x_4\\
&\quad\;\; -x_2^3x_3^2x_4^2x_5^3 - x_2x_3^2x_4^3x_5^4 - x_3^3x_4^7,\\
&\quad\;\; x_2^2x_3^2 + x_1^2x_2x_4 + x_2x_3^3 - x_2x_3^2x_4 + x_2x_4^3 + x_3x_4^3 + x_4^4,\\
&\quad\;\; -x_2^3 - x_1^2x_3 - x_1x_2x_3 + 2x_1x_3^2 - x_2^2x_3 + 2x_2x_3^2\\
\text{Sequence 4} \quad &= \quad -x_1x_2x_4^9x_5 - x_1^9x_4x_5^2 + x_2^4x_4^6x_5^2,\\
&\quad\;\; -x_1^4x_2^2 - x_1x_2x_3^4 - x_2^3x_3^2x_4,\\
&\quad\;\; -x_1^3 - x_1x_2x_3 - x_3^3\\
\text{Sequence 5} \quad &= \quad x_1^4x_3^7x_4 + x_1^6x_2x_3^2x_4x_5^2 + x_3^4x_4x_5^7,\\
&\quad\;\; x_2x_3^5 - x_1^4x_2x_4 + x_1^4x_4^2 - x_1^2x_2^2x_3x_4 + x_1x_2^4x_4 - x_2^4x_4^2 + x_2^3x_4^3,\\
&\quad\;\; x_1^3 - x_1x_2x_3 - x_1x_3^2 - x_2^2x_3\\
\text{Sequence 6} \quad &= \quad -x_1^4x_2^3x_3^2x_4 + x_1^8x_4x_5 - x_1^5x_2^4x_5 + x_1^2x_2^6x_5^2 - x_1^2x_2^4x_3x_4^2x_5 - x_1^2x_2^2x_3^4x_5^2,\\
&\quad\;\; x_1^2x_2^2 + x_1^3x_4 + x_1^2x_2x_3 - x_1x_2^3 + x_1x_3^3 + x_1x_3x_4^2 - x_1x_4^3 + x_2^2x_4^2 + x_3x_4^3,\\
&\quad\;\; -x_1^3 + 2x_1^2x_2 + x_1x_2^2 - x_2^3 - x_2^2x_3\\
\text{Sequence 7} \quad &= \quad -x_2^2x_3^7x_4^2x_5 + x_1^6x_3x_5^5 + x_1^5x_2x_4^2x_5^4 - x_1^3x_3x_4^2x_5^6 + x_1x_2^7x_5^4,\\
&\quad\;\; x_3^6 - x_1^3x_3^2x_4 - x_1^2x_2x_4^3 + x_2^4x_3x_4 + x_2^3x_3^2x_4 - x_4^6,\\
&\quad\;\; -x_1^3 + x_1^2x_2 - 2x_1x_2^2 - x_1x_3^2
\end{aligned}
$$

$$
\begin{aligned}
\text{Sequence 8} \quad &= \quad x_1^2x_2^4x_3^3x_4 - x_1^5x_2x_4^3x_5 - x_1^4x_2^2x_3^2x_4x_5 + x_1^2x_2^2x_3x_4^4x_5 + x_1x_3^4x_4^5 - x_1x_3x_5^8 \\
&\quad +x_2^6x_5^4 + x_2^2x_4^3x_5^5, \\
&\quad -x_1^2x_2^2 + x_1^2x_2x_4 + x_1x_2x_3^2 - x_1x_2x_4^2 - x_1x_3x_4^2 - x_1x_4^3 - x_2^3x_3 - x_2x_3^2x_4 + x_3^4, \\
&\quad -x_1^3 + x_2x_3^2 \\
\text{Sequence 9} \quad &= \quad x_1^5x_2^4x_4 + x_1^3x_2x_3x_4x_5^4 - x_1^2x_2^6x_3x_4 + x_1^2x_2^5x_4^3 - x_1^2x_2^2x_5^6 + x_2x_3^4x_4^2x_5^3, \\
&\quad -x_1^3x_3 + x_1x_2^2x_4 + x_2^3x_3 + x_2x_3^2x_4 + x_4^4, \\
&\quad 2x_1^3 - x_1^2x_2 + x_1^2x_3 + x_1x_2^2 - x_1x_2x_3 + x_2^3 \\
\text{Sequence 10} \quad &= \quad -x_1^3x_2^6x_3x_4x_5 - x_1^6x_2x_5^5 - x_2^6x_3x_4^2x_5^3 - x_4^2x_5^{10}, \\
&\quad x_1x_2^4x_3 - x_1^3x_3^2x_4 + x_1^2x_3x_4^3 + x_1x_2^3x_4^2 - x_1x_4^5, \\
&\quad x_1^3 - x_1^2x_2 - x_1x_2x_3 - x_2x_3^2
\end{aligned}
$$

## References


Alman, J., Williams, V.V., 2021. A refined laser method and faster matrix multiplication, in: Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA), pp. 522–539.

Bardet, M., Faugère, J.C., Salvy, B., 2015. On the complexity of the $F_5$ Gröbner basis algorithm. J. Symb. Comput. 70, 49–70.

Becker, T., Weispfenning, V., 1993. Gröbner bases: a computational approach to commutative algebra. In cooperation with Heinz Kredel. New York: Springer-Verlag.

Bermejo, I., Gimenez, P., 2001. Computing the Castelnuovo-Mumford regularity of some subschemes of $\mathbb{P}_K^n$ using quotients of monomial ideals. J. Pure Appl. Algebra 164, 23–33.

Bigatti, A.M., Conti, P., Robbiano, L., Traverso, C., 1993. A "divide and conquer" algorithm for Hilbert-Poincaré series, multiplicity and dimension of monomial ideals, in: Proceedings of AAECC'79.. Berlin: Springer-Verlag, pp. 76–88.

Bruns, W., Herzog, J., 1993. Cohen-Macaulay rings. volume 39. Cambridge: Cambridge University Press.

Buchberger, B., 1965. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. thesis. Universität Innsbruck.

Buchberger, B., 1979. A criterion for detecting unnecessary reductions in the construction of Gröbner-bases. Symbolic and algebraic computation, EUROSAM'79, int. Symp., Lect. Notes Comput. Sci. 72. 3–21.

Buchberger, B., 2006. 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, 475–511.

Cox, D., Little, J., O'Shea, D., 2007. Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. 3rd ed., New York, NY: Springer.

Dubé, T.W., 1990. The structure of polynomial ideals and Gröbner bases. SIAM J. Comput. 19, 750–773.

Eder, C., Faugère, J.C., 2017. A survey on signature-based algorithms for computing Gröbner bases. J. Symb. Comput. 80, 719–784.

Eisenbud, D., 1995. Commutative algebra. With a view toward algebraic geometry. Berlin: Springer-Verlag.

Faugère, J.C., 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero ($F_5$)., in: Proceedings of ISSAC'02. New York, NY: ACM Press, pp. 75–83.

Fröberg, R., 1997. An introduction to Gröbner bases. Chichester: John Wiley & Sons.

Gao, S., Volny, F.I., Wang, M., 2016. A new framework for computing Gröbner bases. Math. Comput. 85, 449–465.

Gebauer, R., Möller, H.M., 1988. On an installation of Buchberger's algorithm. J. Symb. Comput. 6, 275–286.

Giusti, M., 1988. Combinatorial dimension theory of algebraic varieties. J. Symb. Comput. 6, 249–265. doi:10.1016/S0747-7171(88)80046-4.

Giusti, M., Hägele, K., Lecerf, G., Marchand, J., Salvy, B., 2000. The Projective Noether Maple Package: Computing the dimension of a projective variety. J. Symb. Comput. 30, 291–307.

Giusti, M., Heintz, J., 1993. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial, in: Computational algebraic geometry and commutative algebra. Proceedings of a conference held at Cortina, Italy, June 17-21, 1991. Cambridge: Cambridge University Press, pp. 216–256.

Greuel, G.M., Pfister, G., 2007. A Singular introduction to commutative algebra. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann. 2nd extended ed., Berlin: Springer.

Hashemi, A., Lazard, D., 2011. Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving. Int. J. Algebra Comput. 21, 703–713.

Hashemi, A., Parnian, H., Seiler, W.M., 2022. Computation of Macaulay constants and degree bounds for Gröbner bases. J. Symb. Comput. 111, 44–60.
Hashemi, A., Schweinfurter, M., Seiler, W.M., 2018. Deterministic genericity for polynomial ideals. J. Symb. Comput. 86, 20–50.
Hashemi, A., Seiler, W.M., 2017. Dimension-dependent upper bounds for Gröbner bases., in: Proceedings of ISSAC'17,. New York, NY: ACM Press, pp. 189–196.
Hashemi, A., Seiler, W.M., 2020. Dimension and depth dependent upper bounds in polynomial ideal theory. J. Symb. Comput. 98, 47–64.
Heintz, J., 1983. Definability and fast quantifier elimination in algebraically closed fields. Theor. Comput. Sci. 24, 239–277.
Kemper, G., 2011. A course in commutative algebra. volume 256. Heidelberg: Springer.
Kreuzer, M., Robbiano, L., 2005. Computational commutative algebra. II. Berlin: Springer.
Lazard, D., 1977. Algèbre linéaire sur $K[X_1, \dots, X_n]$ et élimination. Bull. Soc. Math. Fr. 105, 165–190.
Lazard, D., 1983. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. Computer algebra, EUROCAL'83, Lect. Notes Comput. Sci. 162, 146–156.
Le Gall, F., 2014. Powers of tensors and fast matrix multiplication, in: Proceedings of ISSAC'14.. New York, NY: ACM Press, pp. 296–303.
Lejeune-Jalabert, M., 1984. Effectivité de calculs polynomiaux. Cours de D.E.A, Institute Fourier, Grenoble. .
Macaulay, F.S., 1903. Some formulae in eliminations. Proc. Lond. Math. Soc. 35, 3–27. doi:10.1112/plms/s1-35.1.3.
Macaulay, F.S., 1916. The algebraic theory of modular systems. Cambridge: University press, XIV u. 112 S. 8° (1916).
Matsumura, H., 1986. Commutative ring theory. Transl. from the Japanese by M. Reid.
Mayr, E.W., Meyer, A.R., 1982. The complexity of the word problems for commutative semigroups and polynomial ideals. Adv. Math. 46, 305–329.
Mayr, E.W., Ritscher, S., 2013. Dimension-dependent bounds for Gröbner bases of polynomial ideals. J. Symb. Comput. 49, 78–94.
Schmid, J., 1995. On the affine Bezout inequality. Manuscr. Math. 88, 225–232.
Seiler, W.M., 2010. Involution. The formal theory of differential equations and its applications in computer algebra. Berlin: Springer.