Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra

Alessio Caminata[1] and Elisa Gorla[2(✉)]

[1] Dipartimento di Matematica, Università degli Studi di Genova, via Dodecaneso 35, 16146 Genova, Italy
caminata@dima.unige.it

[2] Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, 2000 Neuchâtel, Switzerland
elisa.gorla@unine.ch

Abstract. The complexity of computing the solutions of a system of multivariate polynomial equations by means of Gröbner bases computations is upper bounded by a function of the solving degree. In this paper, we discuss how to rigorously estimate the solving degree of a system, focusing on systems arising within public-key cryptography. In particular, we show that it is upper bounded by, and often equal to, the Castelnuovo-Mumford regularity of the ideal generated by the homogenization of the equations of the system, or by the equations themselves in case they are homogeneous. We discuss the underlying commutative algebra and clarify under which assumptions the commonly used results hold. In particular, we discuss the assumption of being in generic coordinates (often required for bounds obtained following this type of approach) and prove that systems that contain the field equations or their fake Weil descent are in generic coordinates. We also compare the notion of solving degree with that of degree of regularity, which is commonly used in the literature. We complement the paper with some examples of bounds obtained following the strategy that we describe.

Keywords: Gröbner basis · Solving degree · Degree of regularity · Castelnuovo-Mumford regularity · Generic coordinates · Multivariate cryptography · Post-quantum cryptography

Introduction

Polynomial system solving plays an important role in many areas of mathematics. In this paper, we discuss how to solve a system of multivariate polynomial equations by means of Gröbner bases techniques and estimate the complexity of polynomial system solving. Our motivation comes from public-key cryptography, where the computational problem of solving polynomial systems of equations plays a major role.

J. C. Bajard and A. Topuzoğlu (Eds.): WAIFI 2020, LNCS 12542, pp. 3–36, 2021.
https://doi.org/10.1007/978-3-030-68869-1_1

In multivariate cryptography, the security relies on the computational hardness of finding the solutions of a system of polynomial equations over a finite field. One can use similar strategies in order to produce public-key encryption schemes and digital signature algorithms, whose security relies on this problem. For signature schemes, e.g., the public key takes the form of a polynomial map

$$\begin{aligned} \mathcal{P} : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^r \\ (a_1, \ldots, a_n) &\longmapsto (f_1(a_1, \ldots, a_n), \ldots, f_r(a_1, \ldots, a_n)) \end{aligned}$$

where $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \ldots, x_n]$ are multivariate polynomials with coefficients in a finite field $\mathbb{F}_q$. The secret key allows Alice to easily invert the system $\mathcal{P}$. In order to sign the hash b of a message, Alice computes $a \in \mathcal{P}^{-1}(b)$ and sends it to Bob. Bob can readily verify the validity of the signature by checking whether $\mathcal{P}(a) = b$. An illegitimate user Eve who wants to produce a valid signature without knowing Alice's secret key is faced with the problem of solving the polynomial system of r equations in n variables

$$\begin{cases} f_1(x_1, \ldots, x_n) = b_1 \\ \qquad\qquad \vdots \\ f_r(x_1, \ldots, x_n) = b_r \end{cases}$$

Even without knowing Alice's secret key, Eve may be able to exploit the structure of $\mathcal{P}$ in order to solve the system. Such an approach is largely used and the adopted strategies vary significantly from one cryptographic scheme to another. Moreover a direct attack is always possible, i.e., Eve may try to solve the system by computing a Gröbner basis of it. Therefore, being able to estimate the computational complexity of solving a multivariate polynomial system gives an upper bound of the security of the corresponding cryptographic scheme, and is therefore highly relevant. In this context, the complexity of solving a polynomial system is typically large enough to make the computation unfeasible, since being able to compute a solution would enable the attacker to forge a digital signature or to decrypt an encrypted message. We emphasize that the security of multivariate cryptographic schemes is a theme of high current interest. For example, the National Institute of Standards (NIST) is in the process of selecting post-quantum cryptographic schemes for standardization. Three digital signature algorithms were selected as finalists in Round 3 by NIST in July 2020 [NIST], one of which is a multivariate scheme.

Multivariate polynomial systems also appear in connection with the Discrete Logarithm Problem (DLP) on an elliptic or hyperelliptic curve. An index calculus algorithm for solving the DLP on an abelian variety was proposed in [Gau09]. The relation-collection phase of the algorithm relies on Gröbner bases computations to solve a large number of polynomial systems. These systems usually do not have any solutions, but, whenever they have one, they produce a decomposition of a point of the abelian variety over the chosen factor base. In contrast with polynomial systems arising within multivariate cryptography, it is feasible to solve the polynomial systems arising within index calculus algorithms.

Nevertheless, it is important to be able to accurately estimate the complexity of solving them. In fact, the complexity of solving these systems has a direct impact on the complexity of the corresponding index calculus algorithm to solve the DLP.

Estimating the complexity of solving multivariate polynomial systems is relevant within public-key cryptography. In this context, we usually wish to compute the solutions over a finite field of a system of multivariate polynomial equations. Typically, the systems have one, or few, or no solutions, not only over the chosen finite field, but also over its algebraic closure. Moreover, the equations are usually not homogeneous. The degrees of the equations are often small for systems coming from multivariate cryptography, but they can be large for systems arising within index calculus algorithms. Similarly, the number of equations and of variables can vary. Therefore, in this paper we concentrate on finite fields and on non homogeneous systems, which have a finite number of solutions over the algebraic closure. We however do not make assumptions on the number of variables, the number of equations and their degrees.

This paper is devoted to an in-depth discussion of how to estimate the complexity of computing a Gröbner basis for a system of multivariate polynomial equations. As said before, our focus is on finite fields and on systems that have a finite number of solutions over the algebraic closure. At the same time, we try to keep the discussion more general, whenever possible. We often concentrate on systems which are not homogeneous, not only because this is the relevant case for cryptographic applications, but also because it is the most difficult case to treat.

After recalling in Sect. 1 the commutative algebras preliminaries that will be needed throughout the paper, in Sect. 2 we discuss in detail the relation between computing Gröbner bases and solving polynomial systems. This connection is often taken for granted within the cryptographic community, as are the necessary technical assumptions. In Sect. 2 we discuss in detail what these technical assumptions are and what can be done when they are not satisfied. We also show in Theorem 3 that, under the usual assumptions, solving a polynomial system of equations is polynomial-time-equivalent to computing a Gröbner basis of it. We conclude with Subsect. 2.1, where we discuss the feasibility of adding the field equations to a system.

Section 3 is the core of the paper. After establishing the setup that we will be adopting, we prove some results on Gröbner bases and homogenization/dehomogenization. They allow us to compare, in Theorem 7, the solving degree of a system, the solving degree of its homogenization, and the solving degree of the homogenization of the ideal generated by its equations. Combining these results with a classical theorem by Bayer and Stillman [BS87], we obtain Theorem 9 and Theorem 10, where we show that the Castelnuovo-Mumford regularity upper bounds the solving degree of a system, and recover Macaulay's Bound in Corollary 2. These results hold under the assumption that the homogenized system of equations is in generic coordinates, an assumption that is often overlooked in the cryptographic literature and that we discuss in Sect. 1.

In Theorem 11 we prove that any system that contains the field equations or their fake Weil descent is in generic coordinates.

In Sect. 4 we discuss the relation between solving degree and degree of regularity. The latter concept is commonly used in the cryptographic literature and often used as a proxy for the solving degree. In Sect. 4 we discuss the limitations of this approach. In particular, Example 11 and Example 12 are examples of systems coming from index calculus for which, respectively, the degree of regularity is strictly smaller than the solving degree and the degree of regularity is not defined.

Finally, Sect. 5 is meant as an example of how the results from Sect. 3, in combination with known commutative algebra results, easily provide estimates for the solving degree. In particular, Theorem 13 and Theorem 14 give bounds for the solving degree of polynomial systems coming from the MinRank Problem.

1 Preliminaries

In this section we introduce the basic notations and terminology from commutative algebra that we need in the rest of the paper. All the definitions and the proofs of the results that we quote here are extensively covered in the books [KR00, KR05, KR16, CLO07].

1.1 Polynomial Rings and Term Orders

We work in a polynomial ring $R = k[x_1, \dots, x_n]$ in n variables over a field k. An element $f \in R$ is a polynomial, and may be written as a finite sum $f = \sum_\nu a_\nu x^\nu$, where $\nu \in \mathbb{N}^n$, $a_\nu \in k$, and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$. A polynomial of the form $a_\nu x^\nu$ is called a monomial of degree $|\nu| = \nu_1 + \cdots + \nu_n$. In particular, every polynomial f is a sum of monomials. The degree of f, denoted by $\deg(f)$, is the maximum of the degrees of the monomials appearing in f. If all these monomials have the same degree, say d, then f is *homogeneous* of degree d. A monomial $a_\nu x^\nu$ with $a_\nu = 1$ is *monic*. A monic monomial is also called a *term*.

Notation. Given a system of polynomials $\mathcal{F} = \{f_1, \dots, f_r\} \subseteq R$ we denote by $(\mathcal{F}) = (f_1, \dots, f_r)$ the ideal that they generate, that is $(f_1, \dots, f_r) = \{\sum_{i=1}^r p_i f_i : p_i \in R\}$.

The list $\mathcal{F} = \{f_1, \dots, f_r\}$ is called a system of generators of the ideal $I = (\mathcal{F})$. $\mathcal{F}$ is a *minimal system of generators* for I if the ideal generated by any non-empty proper subset of $\mathcal{F}$ is strictly contained in I. If the polynomials $f_1, \dots, f_r$ are homogeneous, then we say that the system $\mathcal{F}$and the ideal I are *homogeneous*.

Remark 1. Let I be an ideal of R minimally generated by homogeneous polynomials $f_1, \dots, f_r$. Then every homogeneous minimal system of generators of I consists of r polynomials of the same degrees as $f_1, \dots, f_r$.

For any degree $d \in \mathbb{Z}_+$, denote by R_d the d-th homogeneous component of R. R_d is generated as a k-vector space by the monomials of R of degree d. If $I \subseteq R$ is homogeneous, we let $I_d = I \cap R_d$ be the k-vector space of homogenous polynomials of degree d in I.

We denote by $\mathbb{T}$ the set of terms of R. A *term order* on R is a total order τ on the set $\mathbb{T}$, which satisfies the following additional properties:

1. $m \leq_\tau n$ implies $p \cdot m \leq_\tau p \cdot n$ for all $p, m, n \in \mathbb{T}$;
2. $1 \leq_\tau m$ for all $m \in \mathbb{T}$.

If in addition $m <_\tau n$ whenever $\deg(m) < \deg(n)$, we say that the term order τ is *degree-compatible*.

Example 1 (Lexicographic order). Let x^α and x^β be two terms in R. We say that $x^\alpha >_{LEX} x^\beta$ if the leftmost non-zero entry in the vector $\alpha - \beta \in \mathbb{Z}^n$ is positive. This term order is called *lexicographic* and it is not degree-compatible. We denote it by LEX.

Example 2 (Degree reverse lexicographic order). Let x^α and x^β be two terms in R. We say that $x^\alpha >_{DRL} x^\beta$ if $|\alpha| > |\beta|$, or $|\alpha| = |\beta|$ and the rightmost non-zero entry in $\alpha - \beta \in \mathbb{Z}^n$ is negative. This term order is called *degree reverse lexicographic* (DRL for short) and it is degree-compatible.

Let $f = \sum_{i \in \mathcal{I}} a_i m_i \in R \setminus \{0\}$ be a polynomial, where $a_i \in k \setminus \{0\}$, and $m_i \in \mathbb{T}$ are distinct terms. We fix a term order τ on R. The *initial term* or *leading term* of f with respect to τ is the largest term appearing in f, that is $\mathrm{in}_\tau(f) = m_j$, where $m_j > m_i$ for all $i \in \mathcal{I} \setminus \{j\}$. The *support* of f is $\mathrm{supp}(f) = \{m_i : \ i \in \mathcal{I}\}$. Given an ideal I of R, the *initial ideal* of I is

$$\mathrm{in}_\tau(I) = (\mathrm{in}_\tau(f) : \ f \in I \setminus \{0\}).$$

Definition 1. *Let I be an ideal of R. A set of polynomials $\mathcal{G} \subseteq I$ is a* Gröbner basis *of I with respect to τ if $\mathrm{in}_\tau(I) = (\mathrm{in}_\tau(g) : \ g \in \mathcal{G})$. A Gröbner basis is* reduced *if $m \notin (\mathrm{in}_\tau(h) : \ h \in \mathcal{G} \setminus \{g\})$ for all $g \in \mathcal{G}$ and $m \in \mathrm{supp}(g)$.*

Sometimes we will need to consider a field extension. At the level of the ideal, this corresponds to looking at the ideal generated by the equations in a polynomial ring over the desired field extension.

Definition 2. *Let $I = (f_1, \ldots, f_r) \subseteq R = k[x_1, \ldots, x_n]$, let $K \supseteq k$ be a field extension. We denote by $IK[x_1, \ldots, x_n]$ the* extension *of I to $K[x_1, \ldots, x_n]$, i.e., the ideal of $K[x_1, \ldots, x_n]$ generated by $f_1, \ldots, f_r$. In symbols, $IK[x_1, \ldots, x_n] = (f_1, \ldots, f_r) \subseteq K[x_1, \ldots, x_n]$.*

1.2 Zero Loci of Ideals

We are mostly interested in ideals, whose zero locus is finite.

Definition 3. *The* affine zero locus *of an ideal* $I = (f_1, \ldots, f_r) \subseteq R$ *over the algebraic closure* $\bar{k}$ *of* k *is*

$$\mathcal{Z}(I) = \{P \in \bar{k}^n : \ f(P) = 0 \ \text{ for all } f \in I\} = \{P \in \bar{k}^n : \ f_1(P) = \ldots = f_r(P) = 0\}.$$

We also denote it by $\mathcal{Z}(f_1, \ldots, f_r)$.

Definition 4. *The* projective zero locus *of a homogeneous ideal* $I = (f_1, \ldots, f_r) \subseteq R$ *over the algebraic closure* $\bar{k}$ *of* k *is*

$$\begin{aligned}\mathcal{Z}_+(I) &= \{P \in \mathbb{P}(\bar{k})^n : \ f(P) = 0 \ \text{ for all } f \in I\} \\ &= \{P \in \mathbb{P}(\bar{k})^n : \ f_1(P) = \ldots = f_r(P) = 0\}.\end{aligned}$$

We also denote it by $\mathcal{Z}_+(f_1, \ldots, f_r)$.

Remark 2. The following are equivalent for a homogeneous ideal $I \subseteq R$:

$$|\mathcal{Z}(I)| < \infty \Leftrightarrow \mathcal{Z}(I) = \{(0, \ldots, 0)\} \Leftrightarrow \mathcal{Z}_+(I) = \emptyset.$$

These conditions are equivalent to the fact that the *Krull dimension* of R/I is zero. This is in turn equivalent to R/I being a finite dimensional k-vector space.

In Definition 3 and Definition 4 it is important to look at the zero locus of I or $\mathcal{F}$ over the algebraic closure of the base field. For cryptographic applications, often the base field k is a finite field. In this case the condition that the zero locus is finite over k is trivially satisfied by any ideal or system of equations.

1.3 Infinite Fields and the Zariski Topology

Let k be a field. The *Zariski topology* on the affine space k^n is the set of complements of solution sets of systems of polynomial equations over R, that is $\{k^n \setminus \mathcal{Z}(f_1, \ldots, f_r) \mid f_1, \ldots, f_r \in R\}$. If k is an algebraically closed field, or at least an infinite field, then every non-empty open set in the Zariski topology is dense, i.e., its closure is equal to the entire space. A non-empty open subset of k^n is often called a *generic set* and a property which holds on a non-empty open set is *generic*. Intuitively, a generic set is almost the whole space and a generic property holds almost everywhere in k^n.

If k is a finite field, on the other side, the Zariski topology is the discrete topology on k^n. In other words, any subset of k^n is both open and closed, and the algebraic-geometric intuition of genericity fails. In particular, one can no longer say that a non-empty open subset of k^n is almost the whole space, as the closure of any subset of k^n is the subset itself. Therefore, as genericity loses its meaning over a finite field, we always will need to assume that the ground field is infinite when dealing with generic sets or properties.

1.4 Generic Changes of Coordinates

Fix a term order τ on $R = k[x_1, \ldots, x_n]$. We denote by $\mathrm{GL}(n, k)$ the general linear group of $n \times n$ invertible matrices with entries in k. This group acts on R via linear changes of coordinates. Namely, a matrix $g = (g_{i,j}) \in \mathrm{GL}(n, k)$ acts on the variable x_j as $g(x_j) = \sum_{i=1}^{n} g_{i,j} x_i$. We refer to g also as a *linear change of coordinates*. We observe that $\mathrm{GL}(n, k) \subseteq k^{n^2}$ is an open subset with respect to the Zariski topology.

It is easy to find examples of $g \in \mathrm{GL}(n, k)$ such that $\mathrm{in}_\tau(gI) \neq \mathrm{in}_\tau(I)$, that is, initial ideals are not independent of coordinate changes. However, a famous theorem by Galligo states that, applying a generic change of coordinates to an ideal I, the initial ideal stays the same.

Theorem 1. [Gal74] *Assume that k is infinite. Let I be a homogeneous ideal of R, then there exist a non-empty Zariski-open set $U \subseteq \mathrm{GL}(n, k)$ and a monomial ideal J such that $\mathrm{in}_\tau(gI) = J$ for all $g \in U$.*

This motivates the following definition.

Definition 5. *Let k be an infinite field. An ideal $I \subseteq R$ is* in generic coordinates *if $1 \in U$, i.e., if*

$$\mathrm{in}_\tau(gI) = \mathrm{in}_\tau(I)$$

for all $g \in U$.

Let k be any field and let $K \supseteq k$ with K infinite. I is in generic coordinates over K *if $IK[x_1, \ldots, x_n] \subseteq K[x_1, \ldots, x_n]$ is in generic coordinates.*

Notice that, over an infinite field k, gI is by definition in generic coordinates for any ideal I and $g \in U$, that is, for any ideal I and for a generic g. Informally, any homogeneous ideal can be put in generic coordinates by applying a random change of coordinates to it. If k is finite, it suffices to apply to I a random change of coordinates over a field extension of sufficiently large cardinality.

1.5 Homogeneous Ideals Associated to a System

Let $R = k[x_1, \ldots, x_n]$ and let $S = R[t]$. Given a polynomial $f \in R$, we denote by $f^h \in S$ the homogenization of f with respect to the new variable t. For $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R$, we let $\mathcal{F}^h \subseteq S$ denote the system obtained from $\mathcal{F}$ by homogenizing each f_i with respect to t, that is $\mathcal{F}^h = \{f_1^h, \ldots, f_r^h\}$.

For an ideal $I \subseteq R$, the *homogenization* of I with respect to t, or simply the homogenization of I, is the ideal

$$I^h = (f^h : \ f \in I) \subseteq S.$$

If $I = (\mathcal{F}) \subseteq R$, then I^h is a homogeneous ideal of S which contains $(\mathcal{F}^h)$. It is easy to produce examples where the containment is strict.

Remark 3. Let $\mathcal{G}$ be a Gröbner basis of I with respect to a degree-compatible term order on R. It can be shown that $\mathcal{G}^h = \{g^h : g \in \mathcal{G}\}$ is a Gröbner basis of I^h with respect to a suitable term order on S, see e.g. [KR05, Section 4.3]. In particular $I^h = (g^h : g \in \mathcal{G})$, hence the degrees of a minimal system of generators of I^h are usually different from those of a minimal system of generators of I. Instead, the degrees of a minimal system of generators of $(\mathcal{F}^h)$ coincide with the degrees of $f_1, \ldots, f_r$.

The *dehomogenization map* ϕ is the standard projection on the quotient $\phi : S \to R \cong S/(t-1)$. For any system of equations $\mathcal{F} \subseteq R$ generating an ideal $I = (\mathcal{F})$ we have $\phi(I^h) = (\phi(\mathcal{F}^h)) = I$. Notice that one also has $\phi((\mathcal{F}^h)) = (\phi(\mathcal{F}^h)) = I$.

For a polynomial $f \in R$, we denote by f^{top} its homogeneous part of highest degree. For a system of equations $\mathcal{F} = \{f_1, \ldots, f_r\}$ we denote by

$$\mathcal{F}^{\text{top}} = \{f_1^{\text{top}}, \ldots, f_r^{\text{top}}\}.$$

Both the ideal $(\mathcal{F}^h)$ and the ideal $(\mathcal{F}^{\text{top}})$ depend on $\mathcal{F}$, and not only on the ideal $I = (\mathcal{F})$.

2 The Importance of Being *LEX*

The main goal of this section is clarifying the relation between solving a system of polynomial equations $\mathcal{F}$ and computing a Gröbner basis of the ideal I generated by the system. In the cryptographic literature it is often stated that, thanks to the Shape Lemma, the problem of finding the solutions of $\mathcal{F}$ can be reduced to that of computing a lexicographic Gröbner basis of I. This statement is however not rigorous, since the Shape Lemma only holds under certain assumptions, which are not always verified for cryptographic systems.

We start by stating the assumptions under which the Shape Lemma holds and showing that, when they are satisfied, the problem of solving the system $\mathcal{F}$ is polynomial-time-equivalent to that of computing a lexicographic Gröbner basis of I. Then we discuss what can be done in the case when the assumptions of the Shape Lemma are not satisfied. We come to the conclusion that, in all situations, one can easily compute the solutions of $\mathcal{F}$ from a lexicographic Gröbner basis of I. We stress that we are not stating that directly computing the reduced lexicographic Gröbner basis is the most efficient way to solve a system (see also Sect. 3). We conclude the section with a brief discussion of when it is feasible to add the field equations to a system $\mathcal{F}$ and how that affects the computation of a Gröbner basis of it.

Throughout the section we focus on systems of equations which have a finite number of solutions over the algebraic closure of the field of definition, since systems that arise in public key cryptography are usually of this kind. Moreover, we always assume that our systems have at least one solution. In fact, if the system has no solutions, the corresponding ideal is equal to the polynomial ring, that is the reduced Gröbner basis with respect to any term order is equal to

{1}. In this case, therefore, computing the reduced lexicographic Gröbner basis allows us to decide that the system has no solutions, without any additional work.

We start by recalling the Shape Lemma.

Theorem 2 (Shape Lemma – [KR00], Theorem 3.7.25). *Let k be a field and let $f_1, \ldots, f_r \in R$ be such that the corresponding ideal $I = (f_1, \ldots, f_r)$ is radical, in normal x_n-position, and $|\mathcal{Z}(I)| = d < \infty$. The reduced lexicographic Gröbner basis of I is of the form*

$$\{g_n(x_n), x_{n-1} - g_{n-1}(x_n), \ldots, x_1 - g_1(x_n)\},$$

where $g_1, \ldots, g_n$ are univariate polynomials in x_n and $\deg(g_1), \ldots, \deg(g_{n-1}) < \deg(g_n) = d$.

The Shape Lemma assumes that the ideal I is radical and in normal x_n-position. An ideal I is *radical* if $f^\ell \in I$ for some $\ell > 0$ implies $f \in I$. This assumption is not always verified for ideals generated by systems arising in cryptography. Later in the section, we will show how one can use a more general version of the Shape Lemma in order to overcome this problem.

Being in *normal x_n-position* means that any two distinct zeros $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n) \in \mathcal{Z}(I)$ satisfy $a_n \neq b_n$. Notice that every ideal I with finite affine zero locus can be brought into normal x_n-position by a suitable linear change of coordinates, passing to a field extension if needed (see [KR00, Proposition 3.7.22]). A field extension may indeed be needed, as the next example shows.

Example 3. Let $\mathcal{F} = \{x_1^2 + x_1, x_1x_2, x_2^2 + x_2\} \subseteq R = \mathbb{F}_2[x_1, x_2]$. Then $I = (x_1^2 + x_1, x_1x_2, x_2^2 + x_2)$ is a radical ideal and $\mathcal{Z}(I) = \{(0,0), (0,1), (1,0)\}$. We claim that I cannot be brought in normal x_2-position by a linear change of coordinates over $\mathbb{F}_2$. In fact, a linear change of coordinates over $\mathbb{F}_2$ sends x_2 to either x_1, x_2, $x_1 + x_2$, $x_1 + 1$, $x_2 + 1$, or $x_1 + x_2 + 1$. However, all these linear forms take the same value on at least two of the elements of $\mathcal{Z}(I)$.

Finally, the Shape Lemma assumes that $|\mathcal{Z}(I)| < \infty$. If k is a finite field, then one can add the field equations to I and obtain an ideal J which is radical and such that $\mathcal{Z}(J) = \mathcal{Z}(I) \cap k^n$, in particular $|\mathcal{Z}(J)| < \infty$. This is however not always advantageous or even feasible, as we discuss in Sect. 2.1.

Whenever the assumptions of the Shape Lemma are satisfied, computing the solutions of a system of equations has the same complexity as computing the reduced lexicographic Gröbner basis of the ideal generated by the system.

Theorem 3. *Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R$ be a polynomial system such that the corresponding ideal $I = (f_1, \ldots, f_r)$ is radical and in normal x_n-position. Assume that $|\mathcal{Z}(I)| = d < \infty$ and $\mathcal{Z}(I) \subseteq \mathbb{F}_q^n$. Consider the LEX order. The set of solutions of $\mathcal{F}$ can be computed from the reduced Gröbner basis of I probabilistically in time polynomial in $\log q, n$ and d. Conversely, the reduced Gröbner basis of I can be computed from the set of solutions of $\mathcal{F}$ deterministically in time polynomial in $\log q, n$ and d.*

Proof. By the Shape Lemma, the reduced lexicographic Gröbner basis of I has the form:

$$\{g_n(x_n), x_{n-1} - g_{n-1}(x_n), \ldots, x_1 - g_1(x_n)\}, \tag{1}$$

where $g_i(x_n)$ are polynomials in the variable x_n only, and $\deg(g_j) < \deg(g_n) = d$ for $1 \leq j < n$.

If we know the reduced lexicographic Gröbner basis of I, then we can factor the polynomial $g_n(x_n)$ to find its roots. Each root α of $g_n(x_n)$ corresponds to a solution $(g_1(\alpha), \ldots, g_{n-1}(\alpha), \alpha)$ of $f_1 = \ldots = f_r = 0$. Notice that the only operation required, apart from the arithmetic over $\mathbb{F}_q$, is factoring univariate polynomials, which can be done in probabilistic polynomial time over a finite field.

Vice versa, assume that we know $\mathcal{Z}(I) = \{P_1, \ldots, P_d\} \subseteq \mathbb{F}_q^n$ of $\mathcal{F}$. Write $P_i = (a_{i,1}, \ldots, a_{i,n})$ for $i = 1, \ldots, d$. We wish to compute the reduced lexicographic Gröbner basis of I, knowing that it is of the form (1). Since the roots of g_n are exactly $a_{1,n}, \ldots, a_{d,n}$ we can compute $g_n(x_n) = \prod_{i=1}^{d}(x_n - a_{i,n})$. Now fix $j \in \{1, \ldots, n-1\}$. Since $g_j(a_{i,n}) = a_{i,j}$ for $i = 1, \ldots, d$ and $\deg(g_j) < d$, we can compute $g_j(x_n)$ by using Lagrange interpolation:

$$g_j(x_n) = \sum_{i=1}^{d} \left(\prod_{\substack{1 \leq \lambda \leq d \\ \lambda \neq i}} \frac{x_n - a_{\lambda,n}}{a_{i,n} - a_{\lambda,n}} \right) a_{i,j}.$$

□

We now discuss the situation in which the assumptions of the Shape Lemma do not hold. In particular, we consider the case when I is not radical. Some authors state that, since $I + (x_1^q - x_1, \ldots, x_n^q - x_n) \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ is always radical, up to adding the field equations one may assume without loss of generality that I is radical. However, adding the field equations to the system is not always computationally feasible, even in the case of systems coming from cryptography. Therefore, being able to deal with the situation when the ideal I is not radical is relevant for cryptographic applications. We discuss this issue in more detail in Sect. 2.1.

Before continuing our discussion, we give an example of system coming from multivariate cryptography for which the corresponding ideal is not radical, adding the field equations to the system is not feasible, and one ends up with a reduced lexicographic Gröbner basis which does not have the shape predicted by the Shape Lemma. Indeed, this was the case for most of the instances of the ABC cryptosystem [TDTD13, TXPD15] that we computed. Since the field sizes proposed in [TXPD15] for achieving 80-bits security are 2^8, 2^{16}, and 2^{32}, adding the field equations to the system is not feasible. In our next example we disregard the linear transformations used in the ABC cryptosystem to disguise the private key, since they do not affect the property of the system to generate a radical ideal.

Example 4. We consider $R = \mathbb{F}_2[x_1, x_2, x_3, x_4]$ with the *LEX* term order and a toy instance of an ABC cryptosystem with

$$A = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix},\ B = \begin{pmatrix} x_1 + x_2 + x_3 & x_1 + x_2 \\ x_1 + x_3 + x_4 & x_3 \end{pmatrix},\ C = \begin{pmatrix} x_1 + x_2 + x_3 + x_4 & x_1 + x_4 \\ x_1 + x_4 & x_1 \end{pmatrix}.$$

We let $p_1, \ldots, p_8$ be the entries of the matrices AB and AC. We take a random plaintext $b = (0, 1, 1, 0) \in \mathbb{F}_2^4$ and we evaluate the polynomials $p_1, \ldots, p_8$ at b to obtain the ciphertext $a = (1, 1, 0, 1, 0, 0, 0, 0) \in \mathbb{F}_2^8$. We then consider the system $\mathcal{F} = \{p_i - a_i : i = 1, \ldots, 8\}$ and the corresponding ideal $I = (\mathcal{F}) \subseteq R$. The ideal I is not radical as $(x_3 + 1)^2 \in I$, but $x_3 + 1 \notin I$. A computation with MAGMA shows that the reduced lexicographic Gröbner basis of I is $\{x_1, x_2 + x_3, x_3^2 + 1, x_4\}$.

We now discuss how one can efficiently compute the solutions of a polynomial system from its lexicographic Gröbner basis, without assuming that the ideal generated by the equations is radical. We stress that we always assume that the system has finitely many solutions over the algebraic closure. The next result will be central to our discussion, as we will use it as a substitute of the Shape Lemma.

Theorem 4 (Elimination Theorem – [CLO07], Chap. 3.1, Theorem 2). *Let $I \subseteq R$ be an ideal and let $\mathcal{G}$ be a lexicographic Gröbner basis of I. Then for every $1 \leq \ell \leq n - 1$ the set $\mathcal{G} \cap k[x_{\ell+1}, \ldots, x_n]$ is a Gröbner basis of $I \cap k[x_{\ell+1}, \ldots, x_n]$ with respect to the LEX order on $k[x_{\ell+1}, \ldots, x_n]$.*

In the next result we use Theorem 4 to prove that one can easily compute the solutions of $\mathcal{F}$ from the reduced lexicographic Gröbner basis of I.

Theorem 5. *Let I be a proper ideal of $R = k[x_1, \ldots, x_n]$ with finite affine zero locus. The reduced lexicographic Gröbner basis of I has the form*

$$\begin{aligned} &p_{n,1}(x_n), \\ &p_{n-1,1}(x_{n-1}, x_n), \ldots, p_{n-1,t_{n-1}}(x_{n-1}, x_n), \\ &p_{n-2,1}(x_{n-2}, x_{n-1}, x_n), \ldots, p_{n-2,t_{n-2}}(x_{n-2}, x_{n-1}, x_n), \\ &\ldots \\ &p_{1,1}(x_1, \ldots, x_n), \ldots, p_{1,t_1}(x_1, \ldots, x_n), \end{aligned}$$

where $p_{i,t_j} \in k[x_i, \ldots, x_n]$ for every index $i \in \{1, \ldots, n\}, j \in \{1, \ldots, t_i\}$ and $t_1, \ldots, t_{n-1} \geq 1$. Moreover, for any $1 \leq \ell \leq n$, let $a = (a_{\ell+1}, \ldots, a_n) \in k^{n-\ell}$ be a solution of the equations

$$\begin{aligned} &p_{n,1}(x_n), \\ &p_{n-1,1}(x_{n-1}, x_n), \ldots, p_{n-1,t_{n-1}}(x_{n-1}, x_n), \\ &\ldots \\ &p_{\ell+1,1}(x_{\ell+1}, \ldots, x_n), \ldots, p_{\ell+1,t_{\ell+1}}(x_{\ell+1}, \ldots, x_n), \end{aligned}$$

and let

$$p_\ell(x_\ell) = \gcd\{p_{\ell,1}(x_\ell, a_{\ell+1}, \ldots, a_n), \ldots, p_{\ell,t_\ell}(x_\ell, a_{\ell+1}, \ldots, a_n)\}.$$

Then $p_\ell(x_\ell) \notin k$.

Proof. Let $\mathcal{G}$ be the reduced lexicographic Gröbner basis of I. The set $\mathcal{G} \cap k[x_\ell, \dots, x_n]$ is of the form

$$\mathcal{G} \cap k[x_\ell, \dots, x_n] = \{p_{i,j}(x_i, \dots, x_n) \mid \ell \leq i \leq n, 1 \leq j \leq t_i\}$$

for some $t_1, \dots, t_n \geq 0$. Moreover, for any $1 \leq \ell \leq n$ such that $p_\ell(x_\ell) \neq 0$, one has $t_\ell \geq 1$. Hence it suffices to show that $p_\ell(x_\ell) \notin k$ for $1 \leq \ell \leq n$.

We prove the claim by descending induction on $\ell \leq n$. Let $\ell = n$, then $\mathcal{G} \cap k[x_n]$ is the reduced lexicographic Gröbner basis of $I \cap k[x_n]$ by Theorem 4. Let $p_{n,1}(x_n)$ be a monic generator of $I \cap k[x_n]$, then $\mathcal{G} \cap k[x_n] = \{p_{n,1}(x_n)\}$ and $t_n = 1$. Since the affine zero locus of I is finite, $p_{n,1}(x_n) \neq 0$. Moreover, $p_n(x_n) = p_{n,1}(x_n) \notin k \setminus \{0\}$, since $\emptyset \neq \mathcal{Z}(I) \subseteq \mathcal{Z}(p_n)$.

We suppose now that the claim holds up to $\ell+1$ and we prove that $p_\ell(x_\ell) \notin k$. By Theorem 4, $\mathcal{G} \cap k[x_\ell, \dots, x_n]$ is the reduced lexicographic Gröbner basis of $I \cap k[x_\ell, \dots, x_n]$, in particular

$$I \cap k[x_\ell, \dots, x_n] = (p_{i,j} \mid \ell \leq i \leq n, 1 \leq j \leq t_i).$$

Let $a \in \mathcal{Z}(I \cap k[x_{\ell+1}, \dots, x_n]) \cap k^{n-\ell}$ and define

$$I(\ell, a) = (p_{\ell,1}(x_\ell, a_{\ell+1}, \dots, a_n), \dots, p_{\ell,t_\ell}(x_\ell, a_{\ell+1}, \dots, a_n)) = (p_\ell(x_\ell)).$$

By [CLO07, Chapter 3.2, Theorem 3] and since $\mathcal{Z}(I)$ is a finite set, one has that

$$\mathcal{Z}(I \cap k[x_\ell, \dots, x_n]) = \pi_{n-\ell+1}(\mathcal{Z}(I)),$$

where $\pi_i : k^n \to k^i$ is the projection on the last i coordinates. In particular, $\mathcal{Z}(I \cap k[x_\ell, \dots, x_n])$ is finite. If $p_\ell(x_\ell)$ is the zero polynomial, then $\mathcal{Z}(I(\ell, a)) = \bar{k}$ and

$$\{(a_\ell, a_{\ell+1}, \dots, a_n) \mid a_\ell \in \bar{k}\} \subseteq \mathcal{Z}(I \cap k[x_\ell, \dots, x_n]),$$

contradicting the finiteness of $\mathcal{Z}(I \cap k[x_\ell, \dots, x_n])$. If instead $p_\ell(x_\ell) \in k \setminus \{0\}$, then $\mathcal{Z}(I(\ell, a)) = \emptyset$. However, $a = (a_{\ell+1}, \dots, a_n) \in \mathcal{Z}(I \cap k[x_{\ell+1}, \dots, x_n]) = \pi_{n-\ell}(\mathcal{Z}(I))$, where equality holds by [CLO07, Chapter 3.2, Theorem 3]. So there exist $a_1, \dots, a_\ell \in \bar{k}$ such that $(a_1, \dots, a_n) \in \mathcal{Z}(I)$. Therefore, $\pi_{n-\ell+1}(a_1, \dots, a_n) = (a_\ell, \dots, a_n) \in \mathcal{Z}(I \cap k[x_\ell, \dots, x_n])$, that is $a_\ell \in \mathcal{Z}(I(\ell, a)) = \emptyset$, a contradiction. □

We use the previous result to build an algorithm which computes the affine zero locus of an ideal I from its reduced lexicographic Gröbner basis. We adopt the notation of Theorem 5.

Corollary 1. *Let $I \subseteq R = k[x_1, \dots, x_n]$ be an ideal with finite affine zero locus $\mathcal{Z}(I)$. Then $\mathcal{Z}(I)$ can be computed as follows:*

1. *Compute the reduced lexicographic Gröbner basis $\mathcal{G}$ of I to obtain the monic polynomial $p_n \in k[x_n]$ such that $(p_n) = I \cap k[x_n]$.*
2. *If $p_n = 1$, then $\mathcal{Z}(I) = \emptyset$. Else, factor p_n.*

3. For every root α of p_n compute

$$p_{n-1}(x_{n-1}) = \gcd\{p_{n-1,1}(x_{n-1}, \alpha), \ldots, p_{n-1,t_{n-1}}(x_{n-1}, \alpha)\}.$$

4. Factor p_{n-1}.
5. For every root β of p_{n-1} compute

$$p_{n-2}(x_{n-2}) = \gcd\{p_{n-2,1}(x_{n-2}, \beta, \alpha), \ldots, p_{n-2,t_{n-2}}(x_{n-2}, \beta, \alpha)\}.$$

6. Proceed similarly, until all the elements of $\mathcal{Z}(I)$ are found.

Notice that the computation is even more efficient under the assumption that the system $\mathcal{F}$, or equivalently the ideal I, has only one zero over the algebraic closure. This is often the case for polynomial systems coming from multivariate cryptosystems, where we usually require that for each ciphertext b there is a unique plaintext a such that $f_i(a) = b$ for every $i = 1, \ldots r$.

In such a situation, one does not need to factor any univariate polynomial, since each one of them has exactly one solution, which, for a monic polynomial of degree d, can be computed by multiplying the coefficient of x^{d-1} by $(-1)^{d-1}d^{-1}$.

Remark 4. Assume that k is either a finite field or has characteristic zero. If I admits only one solution $(a_1, \ldots, a_n) \in \bar{k}^n$, then in fact $(a_1, \ldots, a_n) \in k^n$. This is true even if the solution has multiplicity higher than one. In fact, $g_n(x_n) = (x_n - a_n)^d \in k[x_n]$, hence $da_n \in k$. If k has characteristic zero, then $a_n \in k$. Else, let p be the characteristic of k and write $d = p^\ell e$ where $p \nmid e$. Then $g_n(x_n) = \left(x_n^{p^\ell} - a_n^{p^\ell}\right)^e \in k[x_n]$, so $ea_n^{p^\ell} \in k$. This implies $a_n^{p^\ell} \in k$, hence $a_n \in k$, since k is a finite field. One proceeds similarly to prove that $a_i \in k$ for all i.

Remark 5. By [CLO07, Chapter 3.2, Theorem 3] and since $\mathcal{Z}(I)$ is a finite set, one has that

$$\mathcal{Z}(I \cap k[x_\ell, \ldots, x_n]) = \pi_{n-\ell+1}(\mathcal{Z}(I))$$

for $1 \leq \ell \leq n$, where $\pi_i : k^n \to k^i$ is the projection on the last i coordinates. This implies that each path from the roots to the leaves in the tree-shaped computation of Corollary 1 produces a solution. In particular, Corollary 1 does not perform useless computations.

2.1 Adding the Field Equations to a System

Let $\mathcal{Q} = \{x_1^q - x_1, \ldots, x_n^q - x_n\}$ be the system consisting of the field equations relative to $\mathbb{F}_q$. Clearly, for any system of equations $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R = \mathbb{F}_q[x_1, \ldots, x_n]$ one has

$$\mathcal{Z}(\mathcal{F} \cup \mathcal{Q}) = \mathcal{Z}(\mathcal{F}) \cap \mathbb{F}_q^n.$$

The systems $\mathcal{F}$ and $\mathcal{F} \cup \mathcal{Q}$, however, often have different algebraic properties. It is easy to show that the ideal generated by $\mathcal{F} \cup \mathcal{Q}$ is always radical, while the ideal generated by $\mathcal{F}$ may not be. The structure of the reduced Gröbner bases of the ideals generated by the two systems and the degrees of the elements

appearing in them are often different as well. As a consequence, adding the field equations to a system often affects the complexity of computing a Gröbner basis.

Therefore, passing from $\mathcal{F}$ to $\mathcal{F} \cup \mathcal{Q}$ may or may not provide an advantage. It typically provides an advantage for fields of small size, since the equations of $\mathcal{Q}$ have low degree and adding them to $\mathcal{F}$ makes the ideal radical, a necessary hypothesis for the Shape Lemma (Theorem 2) to apply. Over fields of large size, however, adding the field equations may make the computation of a Gröbner basis practically infeasible. This is due to the fact that we are adding to the system equations of large degree, which are involved in the computation of a Gröbner basis, therefore increasing the degree of the computation. In the next example, we show that the solving degree may increase when passing from $\mathcal{F}$ to $\mathcal{F} \cup \mathcal{Q}$ (see Definition 6 for the definition of solving degree).

Example 5. Let $\mathcal{F} = \{x_3^2 - x_2, x_2^3 - x_1\} \subseteq \mathbb{F}_5[x_1, x_2, x_3]$ and let $I = (\mathcal{F})$. The affine zero locus of I over $\overline{\mathbb{F}}_5$ is infinite. If we add the field equations $\mathcal{Q} = \{x_1^5 - x_1, x_2^5 - x_2, x_3^5 - x_3\}$ of $\mathbb{F}_5$ to $\mathcal{F}$, we obtain the ideal $J = (\mathcal{F} \cup \mathcal{Q})$, which has $\mathcal{Z}(J) = \{(0,0,0), (1,1,1), (4,4,2), (4,4,3), (1,1,4)\}$. The elements of $\mathcal{F}$ are a Gröbner basis of I with respect to the LEX order, while the reduced Gröbner basis of J with respect to the same order also contains $x_3^5 - x_3$. In particular, the Gröbner basis of J contains a polynomial of higher degree and one can easily verify that

$$\text{solv. deg}(\mathcal{F} \cup \mathcal{Q}) = 5 > 3 = \text{solv. deg}(\mathcal{F}).$$

Even if we restrict our attention to polynomial systems arising in public-key cryptography, one may not always assume that the field equations can be added to the system. An example coming from multivariate cryptography was given in Example 4. Another example are systems coming from the relation-collection phase of index calculus on elliptic or hyperelliptic curves, since the field size is very large (e.g., the field size required for 80-bit security is at least $q \sim 2^{160}$ for an elliptic curve and $q \sim 2^{80}$ for a hyperelliptic curve of genus two). In such a situation, adding equations of degree q to the system would make it unmanageable.

3 Solving Degree of Polynomial Systems

In Sect. 2 we discussed how one can compute the solutions of a polynomial system, starting from a lexicographic Gröbner basis of the ideal that it generates. In this section, we address the problem of estimating the complexity of computing a lexicographic Gröbner basis. In practice, one observes that computing a Gröbner basis with respect to LEX is usually slower than with respect to any other term order. On the other hand, computing a Gröbner basis with respect to DRL is often faster than with respect to any other term order. Therefore, computing a degree reverse lexicographic Gröbner basis and converting it to a lexicographic Gröbner basis using FGLM or a similar algorithm is usually more efficient than computing a lexicographic Gröbner basis directly. For this reason, in this section we discuss the complexity of computing a Gröbner basis of an

ideal I in a polynomial ring $R = k[x_1, \ldots, x_n]$ over a field k with respect to the DRL order. We refer the reader to [FGLM93] for a description of the FGLM algorithm and an estimate of its complexity.

3.1 Macaulay Matrices and Solving Degree

We have two main classes of algorithms for computing Gröbner bases: *Buchberger's Algorithm* and *linear algebra based algorithms*, which transform the problem of computing a Gröbner basis into one or more instances of Gaussian elimination. Examples of linear algebra based algorithms are: F_4 [Fau99], F_5 [Fau02], the XL *Algorithm* [CKPS00], and *MutantXL* [DBMMW08]. Buchberger's Algorithm is older, and its complexity has been extensively studied. Linear algebra based algorithms are often faster in practice and have contributed to breaking many cryptographic challenges. However, their complexity is less understood, especially when the input consists of polynomials which are not homogeneous.

In this section, we discuss the complexity of linear algebra based algorithms, which is dominated by Gaussian elimination on the *Macaulay matrices*. First we describe them for homogeneous systems, following [BFS15, p. 54]. Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R$ be a system of homogeneous polynomials and fix a term order. The *homogeneous Macaulay matrix* M_d of $\mathcal{F}$ has columns indexed by the terms of R_d sorted, from left to right, according to the chosen order. The rows of M_d are indexed by the polynomials $m_{i,j} f_j$, where $m_{i,j} \in R$ is a term such that $\deg(m_{i,j} f_j) = d$. Then the entry (i, j) of M_d is the coefficient of the monomial of column j in the polynomial corresponding to the i-th row.

Now let $f_1, \ldots, f_r$ be any polynomials (not necessarily homogeneous). For any degree $d \in \mathbb{Z}_+$ the *Macaulay matrix* $M_{\leq d}$ of $\mathcal{F}$ has columns indexed by the terms of R of degree $\leq d$, sorted in decreasing order from left to right. The rows of $M_{\leq d}$ are indexed by the polynomials $m_{i,j} f_j$, where $m_{i,j}$ is a term in R such that $\deg(m_{i,j} f_j) \leq d$. The entries of $M_{\leq d}$ are defined as in the homogeneous case. Notice that, if $f_1, \ldots, f_r$ are homogeneous, the Macaulay matrix $M_{\leq d}$ is just a block matrix, whose blocks are the homogeneous Macaulay matrices $M_d, \ldots, M_0$ associated to the same equations. This is the reason for using homogeneous Macaulay matrices in the case that $f_1, \ldots, f_r$ are homogeneous.

The size of the Macaulay matrices $M_{\leq d}$ and M_d, hence the computational complexity of computing their reduced row echelon forms, depends on the degree d. Therefore, following [DS13], we introduce the next definition.

Definition 6. *Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R$ and let τ be a term order on R. The* solving degree *of $\mathcal{F}$ is the least degree d such that Gaussian elimination on the Macaulay matrix $M_{\leq d}$ produces a Gröbner basis of $\mathcal{F}$ with respect to τ. We denote it by* $\mathrm{solv.deg}_\tau(\mathcal{F})$. *When the term order is clear from the context, we omit the subscript τ.*

If $\mathcal{F}$ is homogeneous, we consider the homogeneous Macaulay matrix M_d and let the solving degree *of $\mathcal{F}$ be the least degree d such that Gaussian elimination on $M_0, \ldots, M_d$ produces a Gröbner basis of $\mathcal{F}$ with respect to τ.*

Some algorithms perform Gaussian elimination on the Macaulay matrix for increasing values of d. An algorithm of this kind has a termination criterion, which allows to decide whether a Gröbner basis has been found and the algorithm can be stopped. For example, F_5 uses the so-called signatures for this purpose. Other algorithms perform Gaussian elimination on just one Macaulay matrix, for a large enough value of d. For such an algorithm, a sharp bound on the solving degree provides a good estimate for the value of d to be chosen. In both cases, the solving degree produces a bound on the complexity of computing the desired Gröbner basis. In particular, one may choose to artificially stop a Gröbner basis computation in the degree corresponding to the solving degree. For this reason, we use the solving degree to measure the complexity of Gröbner bases computations and we do not discuss termination criteria.

Remark 6. If $\mathcal{F}$ is not homogeneous, then Gaussian elimination on $M_{\leq d}$ may produce a row that corresponds to a polynomial f such that $\deg(f) < d$ and $\mathrm{in}(f)$ was not the leading term of any row of $M_{\leq d}$ before performing Gaussian elimination. If this is the case, then some variants of the algorithms add to $M_{\leq d}$ the rows corresponding to the polynomials mf, where m is a monomial and $\deg(mf) \leq d$. Then they proceed to compute the reduced row echelon form of this larger matrix. If no Gröbner basis is produced in degree $\leq d$, then they proceed by adding to this matrix the appropriate multiples of its rows in the next degree and continue as before. This potentially has the effect of enlarging the span of the rows of $M_{\leq d}$, for all d. Introducing this variation may therefore reduce the computational cost of computing a Gröbner basis with respect to a given term order, since we might be able to obtain a Gröbner basis in a smaller degree than the solving degree, as defined in Definition 6. Throughout the paper, we consider the situation when *no extra rows are inserted*. Notice that the solving degree is an upper bound on the degree in which the algorithms adopting this variation terminate.

Definition 7. *Let $I \subseteq R$ be an ideal and let τ be a term order on R. We denote by* $\mathrm{max.GB.deg}_\tau(I)$ *the maximum degree of a polynomial appearing in the reduced τ Gröbner basis of I. If $I = (\mathcal{F})$, we sometimes write* $\mathrm{max.GB.deg}_\tau(\mathcal{F})$ *in place of* $\mathrm{max.GB.deg}_\tau(I)$.

It is clear that

$$\mathrm{max.GB.deg}_\tau(\mathcal{F}) \leq \mathrm{solv.deg}_\tau(\mathcal{F}),$$

for any system of polynomials $\mathcal{F}$ and any term order τ. Equality does not hold in general, as we show in Example 8.

Remark 7. Assume that $\mathcal{F} = \{f_1, \ldots, f_r\}$ is homogeneous. Gaussian elimination on M_d exclusively produces rows that correspond to polynomials of degree d. Therefore

$$\mathrm{solv.deg}_\tau(\mathcal{F}) = \mathrm{max.GB.deg}_\tau(\mathcal{F})$$

for any τ.

Notice moreover that the solving degree of a system $\mathcal{F}$ may be strictly smaller than the largest degree of an equation of $\mathcal{F}$. This may happen, e.g., when $\mathcal{F}$ contains redundant equations.

Example 6. Let $\mathcal{F} = \{x^2 + x, xy, y^2 + y, x^2y + x^2 + x\} \subseteq \mathbb{F}_2[x, y]$. The reduced DRL Gröbner basis of $I = (\mathcal{F})$ is $\{x^2 + x, xy, y^2 + y\}$ and $\text{solv.deg}_{DRL}\, \mathcal{F} = 2$.

3.2 Homogenization of Ideals and Extensions of Term Order

We consider a polynomial ring $R = k[x_1, \ldots, x_n]$ and its extension $S = R[t]$ with respect to a new variable t. We compare term orders on R and S.

Definition 8. *Let σ be a term order on R, let τ be a term order on $S = R[t]$, and let $\phi : S \to R$ be the dehomogenization map. We say that τ ϕ-*extends *σ, or that τ is a ϕ-*extension *of σ, if $\phi(\text{in}_\tau(f)) = \text{in}_\sigma(\phi(f))$ for every homogeneous $f \in S$.*

The next theorem relates Gröbner basis and dehomogenization.

Theorem 6. *Let σ be a term order on R, and let τ be a ϕ-extension of σ on S. Let I be an ideal in R, let J be a homogeneous ideal in S such that $\phi(J) = I$. The following hold:*

1. $\text{in}_\sigma(I) = \phi(\text{in}_\tau(J))$;
2. *if $\{g_1, \ldots, g_s\}$ is a homogeneous τ Gröbner basis of J, then $\{\phi(g_1), \ldots, \phi(g_s)\}$ is a σ Gröbner basis of I.*

Proof. We prove *(1)*. Notice that $\text{in}_\tau(J) = (\text{in}_\tau(f) : \ f \in J, \ f \text{ homogeneous})$, because J is a homogeneous ideal. Then we have

$$\begin{aligned}\phi(\text{in}_\tau(J)) &= (\phi(\text{in}_\tau(f)) : \ f \in J, \ f \text{ homogeneous}) \\ &= (\text{in}_\sigma(\phi(f)) : \ f \in J, \ f \text{ homogeneous}) .\end{aligned}$$

To conclude the proof of *(1)*, it suffices to show that

$$\{\phi(f) : \ f \in J, \ f \text{ homogeneous}\} = I.$$

The inclusion from left to right follows from the assumption that $\phi(J) = I$. To prove the other inclusion, we fix a system of generators $f_1, \ldots, f_r$ of I and consider $f = \sum_{i=1}^r p_i f_i \in I$, with $p_i \in R$. Let $h_i \in J$ be homogeneous such that $\phi(h_i) = f_i$ for all i and define $\tilde{p} = \sum_{i=1}^r t^{\alpha_i} p_i^h h_i$. The polynomial $\tilde{p}$ belongs to J and it is homogeneous for a suitable choice of the α_i's. Since $\phi(\tilde{p}) = \sum_{i=1}^r \phi(t^{\alpha_i} p_i^h h_i) = \sum_{i=1}^r p_i f_i = f$, the inclusion follows.

To prove *(2)*, observe that

$$\phi(\text{in}_\tau(J)) = (\phi(\text{in}_\tau(g_i)) : \ i = 1, \ldots, s) = (\text{in}_\sigma(\phi(g_i)) \ i = 1, \ldots, s) ,$$

since ϕ is a homomorphism and τ ϕ-extends σ. This shows that $\{\phi(g_1), \ldots, \phi(g_s)\}$ is a Gröbner basis of $\phi(\text{in}_\tau(J))$ with respect to σ, which is equal to $\text{in}_\sigma(I)$ by *(1)*. □

There is a natural way to ϕ-extend a term order σ on R to a term order $\bar{\sigma}$ on S.

Definition 9. *Let m, n be terms in R, let σ be a term order on R. Define a term order $\bar{\sigma}$ on S via: $t^\alpha m >_{\bar{\sigma}} t^\beta n$ if and only if ($m >_\sigma n$) or ($m = n$ and $\alpha > \beta$).*

Lemma 1. *$\bar{\sigma}$ is a term order on S which ϕ-extends σ.*

Proof. First we prove that $\bar{\sigma}$ is a term order. The fact that $1 <_\sigma m$ for every term $m \in R$ implies $1 <_{\bar{\sigma}} m$. We have also $1 = t^0 <_{\bar{\sigma}} t$.

Now, let $t^\alpha m >_{\bar{\sigma}} t^\beta n$, with m, n terms in R, and $\alpha, \beta \in \mathbb{N}$. We show that $>_{\bar{\sigma}}$ respects multiplication by terms. We have two possibilities: *1)* $m >_\sigma n$ or *2)* $m = n$ and $\alpha > \beta$. If *1)* holds, then we have $x_i m >_\sigma x_i n$ for every $i = 1, \ldots, n$ since σ is a term order, which implies $x_i t^\alpha m >_{\bar{\sigma}} x_i t^\beta n$. Clearly $t^{\alpha+1} m >_{\bar{\sigma}} t^{\beta+1} n$. If *2)* holds, then $x_i m = x_i n$ for every $i = 1, \ldots, n$, therefore $x_i t^\alpha m >_{\bar{\sigma}} x_i t^\beta n$ since $\alpha > \beta$. Moreover we have $t^{\alpha+1} m >_{\bar{\sigma}} t^{\beta+1} n$, because $m = n$ and $\alpha + 1 > \beta + 1$.

Now we prove that $\bar{\sigma}$ ϕ-extends σ, that is $\phi(\mathrm{in}_{\bar{\sigma}}(f)) = \mathrm{in}_\sigma(\phi(f))$ for every $f \in S$ homogeneous. Let $f = \sum_{i=1}^d a_i t^{\alpha_i} m_i$ be a homogeneous polynomial, with $m_i \in R$ distinct terms, $\alpha_i \in \mathbb{N}$, and $a_i \in k \setminus \{0\}$. Then $\phi(f) = \sum_{i=0}^d a_i m_i$ and $\deg m_i = \deg f - \alpha_i$. If there is any cancellation in the sum defining $\phi(f)$, then the monomials cancelling have the same degree, then they have already been cancelled in f. Hence, there is no cancellation in $\phi(f)$. Without loss of generality, let $m_1 = \mathrm{in}_\sigma(\phi(f))$, that is $m_1 >_\sigma m_i$ for every $i = 2, \ldots, d$. Then $t^{\alpha_1} m_1 = \mathrm{in}_{\bar{\sigma}}(f)$, and $\phi(\mathrm{in}_{\bar{\sigma}}(f)) = m_1 = \mathrm{in}_\sigma(\phi(f))$. □

Example 7. The equality $\phi(\mathrm{in}_{\bar{\sigma}}(f)) = \mathrm{in}_\sigma(\phi(f))$ does not necessarily hold for f not homogeneous. For example consider $f = tx - x + ty \in S = k[x, y, t]$, and let $\sigma = LEX$. Then $\mathrm{in}_{\bar{\sigma}}(f) = tx$, $\phi(f) = y$, and $\mathrm{in}_\sigma(\phi(f)) = y \neq x = \phi(\mathrm{in}_{\bar{\sigma}}(f))$.

The next Lemma gives an important example of ϕ-extension of a term order.

Lemma 2. *Fix the DRL order on R and extend it to the DRL order on S by letting t be the smallest variable. Then the DRL order on S ϕ-extends the DRL order on R.*

Proof. Let $f = \sum_{i=1}^d a_i t^{\alpha_i} m_i$ be a homogeneous polynomial, with distinct terms $m_i \in R$, $\alpha_i \in \mathbb{N}$, and $a_i \in k \setminus \{0\}$. Then $\phi(f) = \sum_{i=0}^d a_i m_i$ and $\deg m_i = \deg f - \alpha_i$. As in the proof of Lemma 1 there is no cancellation in $\phi(f)$.

Without loss of generality, let $\mathrm{in}_{DRL}(\phi(f)) = m_1$, that is $m_1 >_{DRL} m_i$ for all $i = 2, \ldots, d$. For each $i \in \{2, \ldots, d\}$ we have two possibilities: either $\deg m_1 > \deg m_i$ or $\deg m_1 = \deg m_i$. If $\deg m_1 > \deg m_i$ then we have $\alpha_1 < \alpha_i$, since $\deg m_j + \alpha_j = \deg f$ for every j. This implies $t^{\alpha_1} m_1 >_{DRL} t^{\alpha_i} m_i$. If $\deg m_1 = \deg m_i$ then we have $\alpha_1 = \alpha_i$, and $t^{\alpha_1} m_1 >_{DRL} t^{\alpha_i} m_i$ follows from $m_1 >_{DRL} m_i$. Therefore we have $\mathrm{in}_{DRL}(f) = t^{\alpha_1} m_1$, and $\phi(\mathrm{in}_{DRL}(f)) = m_1 = \mathrm{in}_{DRL}(\phi(f))$. □

Remark 8. Fix the DRL order on R. The DRL order on S is different from the order $\overline{DRL}$ obtained by applying Definition 9. For example, let $R = k[x, y]$ with $x > y$, $S = R[t]$, and consider the monomials t^3x and ty^2. We have $t^3x <_{\overline{DRL}} ty^2$ because $x <_{DRL} y^2$ in R. In particular, $\overline{DRL}$ is not degree-compatible, while DRL is. Notice however that the two orders coincide on pairs of terms of the same degree.

3.3 Solving Degree and Homogenization

Let $R = k[x_1, \ldots, x_n]$ with the DRL order and let $S = R[t]$ with the DRL order with t as smallest variable. Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R$, let $I = (\mathcal{F}) \subseteq R$, let $I^h \subseteq S$ be the homogenization of I with respect to t, and let $(\mathcal{F}^h) \subseteq S$ be the ideal generated by $\mathcal{F}^h = \{f_1^h, \ldots, f_r^h\}$. The goal of this section is comparing the solving degrees of $\mathcal{F}$, $\mathcal{F}^h$, and I^h with respect to the chosen term orders. We start with a preliminary result on Gröbner bases and homogenization.

Proposition 1. *Let $R = k[x_1, \ldots, x_n]$ and let $S = R[t]$. Fix the DRL term order on R and extend it to the DRL term order on S by letting t be the smallest variable. Let I be an ideal of R with Gröbner basis $\{g_1, \ldots, g_s\}$. Then $\{g_1^h, \ldots, g_s^h\}$ is a Gröbner basis of I^h.*

Proof. First we show that $g_1^h, \ldots, g_s^h$ generate I^h. Clearly we have $g_1^h, \ldots, g_s^h \in I^h$. For the other inclusion, consider $f \in I$ of degree d with standard representation $f = \sum_{i=1}^{s} f_i g_i$ for some $f_i \in R$, that is $\mathrm{in}(f) \geq \mathrm{in}(f_i g_i)$ for all $i = 1, \ldots, s$.

Since $\mathrm{in}(f) \geq \mathrm{in}(f_i g_i)$ and DRL is degree-compatible, we have $d \geq \deg f_i + \deg g_i$. Therefore we can write

$$f^h = \sum_{i=1}^{s} t^{d-\deg f_i - \deg g_i} f_i^h g_i^h, \tag{2}$$

which shows that $f^h \in (g_1^h, \ldots, g_s^h)$.

To prove that $\{g_1^h, \ldots, g_s^h\}$ is a Gröbner basis, it is enough to show that (2) is a standard representation for f^h, i.e., $\mathrm{in}(f^h) \geq \mathrm{in}(t^{d-\deg f_i - \deg g_i} f_i^h g_i^h)$ for all $i = 1, \ldots, s$. We observe that $\mathrm{in}(f^h) = \mathrm{in}(f)$ does not contain the variable t and we distinguish two cases.

1. If $d - \deg f_i - \deg g_i > 0$, then a power of t appears in $t^{d-\deg f_i - \deg g_i} f_i^h g_i^h$, and in its initial term as well. It follows that $\mathrm{in}(f^h) \geq \mathrm{in}(t^{d-\deg f_i - \deg g_i} f_i^h g_i^h)$ since t is the smallest variable in the DRL term order of S.
2. If $d - \deg f_i - \deg g_i = 0$, then no power of t appears in $\mathrm{in}(f_i^h g_i^h)$. Therefore we have $\mathrm{in}(f_i^h g_i^h) = \mathrm{in}(f_i g_i) \leq \mathrm{in}(f) = \mathrm{in}(f^h)$. □

The next result relates the solving degrees of $\mathcal{F}$ and $\mathcal{F}^h$. It also clarifies why the largest degree of an element in a reduced Gröbner basis of $\mathcal{F}$ may be smaller than its solving degree.

Theorem 7. *Let $\mathcal{F} = \{f_1, \dots, f_r\} \subseteq R = k[x_1, \dots, x_n]$ and consider the system $\mathcal{F}^h = \{f_1^h, \dots, f_r^h\} \subseteq S = R[t]$ obtained from $\mathcal{F}$ by homogenizing $f_1, \dots, f_r$ with respect to t. Let $I^h \subseteq S$ be the homogenization of $I = (\mathcal{F}) \subseteq R$ with respect to t. Consider the term order DRL on R and S, with t as smallest variable. Then*

$$\begin{aligned} &\max.\,\mathrm{GB}.\deg(\mathcal{F}^h) = \mathrm{solv}.\deg(\mathcal{F}^h) = \mathrm{solv}.\deg(\mathcal{F}) \\ \geq &\max.\,\mathrm{GB}.\deg(\mathcal{F}) = \max.\,\mathrm{GB}.\deg(I^h) = \mathrm{solv}.\deg(I^h). \end{aligned}$$

Proof. We claim that the Macaulay matrix $M_{\leq d}$ of $\mathcal{F}$ with respect to DRL is equal to the homogeneous Macaulay matrix M_d of $\mathcal{F}^h$ with respect to DRL, for every $d \geq 1$. In fact, the monomials of S of degree d are exactly the homogenizations of the monomials of R of degree $\leq d$. Similarly, if $m_{i,j} f_j^h$ is the index of a row of M_d, i.e., $\deg(m_{i,j} f_j^h) = d$, then $\phi(m_{i,j} f_j^h) = \phi(m_{i,j}) f_j$ has degree $\leq d$, hence it is the index of a row of $M_{\leq d}$. Conversely, every index $m_{i,j} f_j^h$ of a row of M_d, can be obtained from an index of a row of $M_{\leq d}$ by homogenizing and multiplying by an appropriate power of t. In a nutshell, the statement on the columns follows from the fact that $I_{\leq d} = \phi\left((\mathcal{F}^h)_d\right)$. One also needs to check that the order on the columns of M_d and $M_{\leq d}$ is the same. We consider $M_{\leq d}$. Since DRL is degree-compatible, the columns are ordered in non-increasing degree order from left to right. The columns of the same degree $j \in \{1, \dots, d\}$ are then ordered according to DRL. Similarly, since t is the smallest variable in the DRL order on S, the columns of M_d are ordered in increasing order (from left to right) of powers of t, which is equivalent to decreasing order of the degree of the variables $x_1, \dots, x_n$. Then, the columns with the same power of t are ordered according to DRL on the variables $x_1, \dots, x_n$. This proves that the matrices $M_{\leq d}$ and M_d coincide.

Let $I = (\mathcal{F})$ and $J = (\mathcal{F}^h)$. Since the matrices $M_{\leq d}$ and M_d coincide and since the dehomogenization of a Gröbner basis of $\mathcal{F}^h$ produces a Gröbner basis of $\mathcal{F}$ by Theorem 6, one has

$$\mathrm{solv}.\deg_{DRL}(\mathcal{F}) \leq \mathrm{solv}.\deg_{DRL}(\mathcal{F}^h).$$

To check that they are equal, for each minimal generator m of $\mathrm{in}(I)$, we consider the least degree d for which a polynomial f with $\mathrm{in}(f) = m$ appears among the rows of the reduced row echelon form of $M_{\leq d}$. Since $M_d = M_{\leq d}$, the polynomial $t^{d-\deg(f)} f^h$ appears among the rows of the reduced row echelon form of M_d. We claim that no polynomial g with $\mathrm{in}(g) \mid t^{d-\deg(f)} m = \mathrm{in}(t^{d-\deg(f)} f^h)$ appears as a row of the reduced row echelon form of M_e for some $e < d$. In fact, if this were the case then, by Theorem 6, the dehomogenization of $\mathrm{in}(g)$ would be equal to m and appear as a row of M_e. This contradicts the assumption that d is the least degree for which a polynomial with leading term m appears among the rows of the reduced row echelon form of $M_{\leq d}$. This shows that the least degree d in which the leading terms of the rows of the reduced row echelon form of the matrix $M_{\leq d}$ generate the initial ideal of I is the same as the the least degree e in which the leading terms of the rows of the reduced row echelon form of the matrix M_e generate $\mathrm{in}(J)_e$. Therefore

$$\mathrm{solv}.\deg_{DRL}(\mathcal{F}) = \mathrm{solv}.\deg_{DRL}(\mathcal{F}^h).$$

The equality $\max.\,\mathrm{GB}.\,\deg(\mathcal{F}) = \max.\,\mathrm{GB}.\,\deg(I^h)$ follows from the following two facts:

- By Lemma 2 and Theorem 6 the dehomogenization of a DRL Gröbner basis of I^h produces a DRL Gröbner basis of I.
- The homogenization of a DRL Gröbner basis of I produces a DRL Gröbner basis of I^h by Proposition 1.

In particular, no leading term of an element of the reduced Gröbner basis of I^h is divisible by t, so dehomogenization does not decrease the degrees of the elements of the Gröbner basis.

Finally, the two equalities

$$\max.\,\mathrm{GB}.\,\deg(\mathcal{F}^h) = \mathrm{solv}.\,\deg(\mathcal{F}^h) \text{ and } \max.\,\mathrm{GB}.\,\deg(I^h) = \mathrm{solv}.\,\deg(I^h)$$

follow from Remark 7. □

Remark 9. Theorem 7 clarifies why, when the system $\mathcal{F}$ is not homogeneous, the largest degree of an element in a reduced Gröbner basis may be strictly smaller than the solving degree. This is due to the difference between the ideals $(\mathcal{F}^h)$ and I^h, and more specifically between $\max.\,\mathrm{GB}.\,\deg(\mathcal{F}^h)$ and $\max.\,\mathrm{GB}.\,\deg(I^h)$.

The following is an example where $\mathrm{solv}.\,\deg(\mathcal{F}) > \max.\,\mathrm{GB}.\,\deg(\mathcal{F})$. See also Example 11 for a cryptographic example.

Example 8. Let $R = k[x, y]$ and let $S = R[t] = k[x, y, t]$, both with the *DRL* order. We consider the system $\mathcal{F} = \{f_1, f_2\} \subseteq R$ with $f_1 = x^2 - 1$, $f_2 = xy + x$, and let $I = (\mathcal{F})$. Then $\mathcal{F}^h = \{f_1^h, f_2^h\} = \{x^2 - t^2, xy + xt\}$, and $I^h = (x^2 - t^2, y + t)$. Writing the Macaulay matrices of $\mathcal{F}$, $\mathcal{F}^h$, and $\{x^2 - t^2, y + t\}$ and doing Gaussian elimination, one sees that $\mathrm{solv}.\,\deg(\mathcal{F}) = \mathrm{solv}.\,\deg(\mathcal{F}^h) = 3$. By computing Gröbner bases, one can check that $\max.\,\mathrm{GB}.\,\deg(\mathcal{F}^h) = 3$ and $\max.\,\mathrm{GB}.\,\deg(\mathcal{F}) = \max.\,\mathrm{GB}.\,\deg(I^h) = 2$.

3.4 Solving Degree and Castelnuovo-Mumford Regularity

In what follows, we compare the solving degree of a homogeneous ideal with a classical invariant from commutative algebra: the *Castelnuovo-Mumford regularity*. We recall the definition of this invariant and its basic properties before illustrating the link with the solving degree.

Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring in n variables over a field k and let I be a homogeneous ideal of R. For any integer j we recall that R_j denotes the k-vector space of homogeneous elements of R of degree j.

Choose a minimal system of generators $f_1, \ldots, f_{\beta_0}$ of I. We recall that, since I is homogeneous, the number β_0 and the degrees $d_i = \deg f_i$ are uniquely determined. We fix an epimorphism $\varphi : R^{\beta_0} \to I$ sending the canonical basis $\{e_1, \ldots, e_{\beta_0}\}$ of the free module R^{β_0} to $\{f_1, \ldots, f_{\beta_0}\}$. The map φ is in general not homogeneous of degree 0, so we introduce degree shifts on R: For any integer d, we denote by $R(-d)$ the R-module R, whose j-th homogeneous component is

$R(-d)_j = R_{-d+j}$. For example, the variables $x_1, \ldots, x_n$ have degree 2 in $R(-1)$, and degree 0 in $R(1)$. The map

$$\varphi : \bigoplus_{j=1}^{\beta_0} R(-d_j) \to I$$

is homogeneous of degree 0, that is $\deg(\varphi(f)) = \deg f$ for every f.

Now consider the submodule $\ker \varphi \subseteq \bigoplus_{j=1}^{\beta_0} R(-d_j)$. It is again finitely generated and graded, and is called (first) syzygy module of I. We choose a minimal system of generators of $\ker \varphi$ and we continue similarly defining an epimorphism from a free R-module (with appropriate shifts) to $\ker \varphi$ and so on.

Hilbert's Syzygy Theorem guarantees that this procedure terminates after a finite number of steps. Thus, we obtain a *minimal graded free resolution* of I:

$$0 \to F_p \to \cdots \to F_1 \to F_0 \xrightarrow{\varphi} I \to 0,$$

where the F_i are free R-modules of the form

$$F_i = \bigoplus_{j=0}^{\beta_i} R(-d_{i,j})$$

for appropriate shifts $d_{i,j} \in \mathbb{Z}$. By regrouping the shifts, we may write the free R-modules of the minimal free resolution of I as

$$F_i = \bigoplus_{j \in \mathbb{Z}} R(-j)^{\beta_{i,j}}.$$

The numbers $\beta_{i,j} = \beta_{i,j}(I)$ are the *(graded) Betti numbers* of I.

Definition 10. *The* Castelnuovo-Mumford regularity *of I is*

$$\operatorname{reg}(I) = \max\{j - i : \ \beta_{i,j}(I) \neq 0\}.$$

If $\mathcal{F}$ is a homogeneous system of generators of I, we set also $\operatorname{reg}(\mathcal{F}) = \operatorname{reg}(I)$.

Example 9. We consider the ideal $I = (x^2, xy, xz, y^3)$ in $R = k[x, y, z]$. A minimal free resolution of I is given by

$$0 \to R(-4) \xrightarrow{\varphi_2} R(-3)^3 \oplus R(-4) \xrightarrow{\varphi_1} R(-2)^3 \oplus R(-3) \xrightarrow{\varphi_0} I \to 0,$$

with R-linear maps given by the following matrices

$$\varphi_0 = (x^2, xy, xz, y^3), \ \varphi_1 = \begin{pmatrix} -y & -z & 0 & 0 \\ x & 0 & -z & -y^2 \\ 0 & x & y & 0 \\ 0 & 0 & 0 & x \end{pmatrix}, \ \varphi_2 = \begin{pmatrix} z \\ -y \\ x \\ 0 \end{pmatrix}.$$

So the non-zero Betti numbers of I are $\beta_{0,2} = 3$, $\beta_{0,3} = 1$, $\beta_{1,3} = 3$, $\beta_{1,4} = 1$, $\beta_{2,4} = 1$, and the Castelnuovo-Mumford regularity is $\operatorname{reg}(I) = 3$.

For more on regularity and its properties, the interested reader may consult [Eis94, Chapter 20] or [Cha07]. In the sequel we only mention the facts that are relevant for our purposes.

Remark 10. In many texts in commutative algebra or algebraic geometry it is assumed that the field k is algebraically closed or infinite. However, the definition of regularity makes perfect sense over a finite field. The construction of a minimal free resolution that we illustrated can be carried out over a finite field. Moreover, it shows that the Castelnuovo-Mumford regularity is preserved under field extensions. In particular, if I is an ideal in a polynomial ring $R = \mathbb{F}_q[x_1, \ldots, x_n]$ over a finite field $\mathbb{F}_q$ and J is its extension to the polynomial ring $S = \overline{\mathbb{F}}_q[x_1, \ldots, x_n]$ over the algebraic closure of $\mathbb{F}_q$, then $\mathrm{reg}_R(I) = \mathrm{reg}_S(J)$.

The next theorem is due to Bayer and Stillman. It relates the regularity of a homogeneous ideal to the regularity of its DRL initial ideal. Combined with our Theorem 7, it will allow us to bound the solving degree of any system.

Theorem 8 ([BS87], Theorem 2.4 and Proposition 2.9). *Let J be a homogeneous ideal in $k[x_1, \ldots, x_n]$. Assume that J is in generic coordinates over $\overline{k}$, then*

$$\mathrm{reg}(J) = \mathrm{reg}(\mathrm{in}_{DRL}(J)).$$

Remark 11. Let J be a homogeneous ideal in generic coordinates. If k has characteristic zero, then we have $\mathrm{reg}(\mathrm{in}_{DRL}(J)) = \mathrm{max.\,GB.\,deg}_{DRL}(J)$, as shown in [BS87]. If k has positive characteristic, one still has that $\mathrm{max.\,GB.\,deg}_{DRL}(J) \leq \mathrm{reg}(\mathrm{in}_{DRL}(J))$ and the inequality is often an equality. In fact this was the case in all the examples that we computed while working on this paper. Nevertheless, in positive characteristic one can find examples of ideals J in generic coordinates for which the inequality is strict. E.g. $J = (x^p, y^p) \subseteq \overline{\mathbb{F}}_p[x, y]$ is in generic coordinates, $\mathrm{max.\,GB.\,deg}_{DRL}(J) = p$, and $\mathrm{reg}(J) = 2p - 1$.

Combining Theorem 7 and Theorem 8, one obtains bounds on the solving degree. Our bounds assume that the ideal generated by the (homogenized) system is in generic coordinates. Notice that this assumption is likely to be satisfied for systems of equations coming from multivariate cryptography, at least over a field of sufficiently large cardinality. In fact, multivariate schemes are often constructed by applying a generic change of coordinates (and a generic linear transformation) to the set of polynomials which constitutes the private key.

For the sake of clarity, we give a homogeneous and a non-homogeneous version of the result. Since the proofs are very similar, and in fact more complicated in the non-homogeneous case, we only give the proof in the latter case.

Theorem 9. *Let $\mathcal{F} \subseteq R$ be a system of homogeneous polynomials and assume that $(\mathcal{F})$ is in generic coordinates over $\overline{k}$. Then*

$$\mathrm{solv.\,deg}_{DRL}(\mathcal{F}) \leq \mathrm{reg}(\mathcal{F}).$$

The following result allows us to bound the complexity of computing a Gröbner basis of a system of equations by establishing a connection with the Castelnuovo-Mumford regularity of the homogenization of the system.

Theorem 10. *Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R$ be a system of polynomials, which is not homogeneous. Let $\mathcal{F}^h = \{f_1^h, \ldots, f_r^h\} \subseteq S = R[t]$ and assume that the ideal $(\mathcal{F}^h)$ is in generic coordinates over $\overline{k}$. Then*

$$\operatorname{solv.deg}_{DRL}(\mathcal{F}) \leq \operatorname{reg}(\mathcal{F}^h).$$

Proof. For a homogeneous ideal J in R or S, $\operatorname{max.GB.deg}_{DRL}(J)$ and $\operatorname{reg}(J)$ are invariant under field extension. So we may extend all ideals to the algebraic closure $\overline{k}$ of k. By Theorem 7 and Theorem 8 we have the chain of equalities and inequalities

$$\begin{aligned}\operatorname{solv.deg}_{DRL}(\mathcal{F}) &= \operatorname{solv.deg}_{DRL}(\mathcal{F}^h)\\ &= \operatorname{max.GB.deg}_{DRL}(\mathcal{F}^h) \leq \operatorname{reg}(\operatorname{in}_{DRL}(\mathcal{F}^h)) = \operatorname{reg}(\mathcal{F}^h).\end{aligned}$$

□

Remark 12. The upper bound in Theorem 9 and Theorem 10 is often an equality, since $\operatorname{max.GB.deg}_{DRL}(\mathcal{F}^h) = \operatorname{reg}(\operatorname{in}_{DRL}(\mathcal{F}^h))$ if k has characteristic zero and often even if it has positive characteristic (see Remark 11).

By combining Theorem 10 and classical results on the Castelnuovo-Mumford regularity (see e.g. [Cha07, Theorem 12.4]), one immediately obtains the following bound on the solving degree of systems which have finitely many solutions over $\overline{k}$. The bound is linear in both the number of variables and the degrees of the polynomials of the system.

Corollary 2 (Macaulay bound – [Laz83], Theorem 2). *Consider a system of equations $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R$ with $d_i = \deg f_i$ and $d_1 \geq d_2 \geq \cdots \geq d_r$. Set $\ell = \min\{n+1, r\}$. Assume that $|\mathcal{Z}_+(\mathcal{F}^h)| < \infty$ and that $(\mathcal{F}^h)$ is in generic coordinates over $\overline{k}$. Then*

$$\operatorname{solv.deg}_{DRL}(\mathcal{F}) \leq d_1 + \ldots + d_\ell - \ell + 1$$

and equality holds if $f_1, \ldots, f_r$ are a regular sequence. In particular, if $r > n$ and $d = d_1$, then

$$\operatorname{solv.deg}_{DRL}(\mathcal{F}) \leq (n+1)(d-1) + 1.$$

The condition that $(\mathcal{F}^h)$ is in generic coordinates is not always easy to verify. Nevertheless, if we add the field equations, or their fake Weil descent, to the generators of the ideal, then we can prove that the homogenized system is in generic coordinates.

Theorem 11. *Let $p > 0$ be a prime and let $q = p^e$, $e \geq 1$. Let k be a field of characteristic p and let $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq k[x_1, \ldots, x_n]$ be a system of polynomial equations. Set $d_i = \deg f_i$ with $d_1 \geq d_2 \geq \cdots \geq d_r$ and $\ell = \min\{n+1, r\}$. Assume that one of the following holds:*

(i) $x_i^q - x_i \in \mathcal{F}$ *for* $i = 1, \ldots, n$, *or*
(ii) $x_1^q - x_2, \ldots, x_{n-1}^q - x_n, x_n^q - x_1 \in \mathcal{F}$.

Then the ideal $(\mathcal{F}^h) = (f_1^h, \ldots, f_r^h)$ *is in generic coordinates over* $\bar{k}$. *In particular*

$$\text{solv. deg}_{DRL}(\mathcal{F}) \leq d_1 + \ldots + d_\ell - \ell + 1$$

and equality holds if $f_1, \ldots, f_r$ *are a regular sequence. Moreover, if* $r > n$ *and* $d = d_1$, *then*

$$\text{solv. deg}_{DRL}(\mathcal{F}) \leq (n+1)(d-1) + 1.$$

Proof. According to [BS87, Theorem 2.4 and Definition 1.5], $J = (\mathcal{F}^h)$ is in generic coordinates over $\bar{k}$ if and only if t is not a zero divisor on the quotient $\bar{k}[x_1, \ldots, x_n, t]/J^{\text{sat}}$, where J^{sat} is the saturation of J with respect to the irrelevant maximal ideal $(x_1, \ldots, x_n, t)$. Substituting $t = 0$ in the equations of J one obtains the equations $x_1 = \ldots = x_n = 0$. Therefore the projective zero locus of J does not contain any point with $t = 0$. This means that $t \nmid 0$ modulo J^{sat}, hence proving that J is in generic coordinates. The second part of the statement then follows from Corollary 2. □

Remark 13. From the proof of Theorem 11 one sees that a system is in generic coordinates whenever it contains equations of the form $x_i^{d_i} + p_i(x_1, \ldots, x_n)$ with $\deg(p_i) < d_i$, for $i = 1, \ldots, n$.

We may use the results established in this section to obtain bounds on the solving degree of the ABC encryption scheme. We assume that the systems have finite affine zero loci, which was the case for all the instances of the ABC cryptosystem that we computed.

Example 10. The system associated to the ABC cryptosystems [TDTD13, TXPD15] consists of $2n$ quadratic equations in n variables. Therefore by assuming that the system is in generic coordinates, or, if the ground field is $\mathbb{F}_2$, simply by adding the field equations to the system we obtain

$$\text{solv. deg}(\mathcal{F}) \leq n + 2.$$

4 Solving Degree and Degree(s) of Regularity

In recent years, different invariants for measuring the complexity of solving a polynomial system of equations were introduced. In particular, the notion of *degree of regularity* gained importance and is widely used nowadays. In this section we discuss how the degree of regularity is related with the Castelnuovo-Mumford regularity.

In the literature we found several definitions of degree of regularity. However, they are mostly variations of the following two concepts:

1. the degree of regularity by Bardet, Faugère, and Salvy [Bar04, BFS04, BFS15];
2. the degree of regularity by Dubois and Gama, later studied by Ding, Schmidt, and Yang [DG10, DS13, DY13].

In this section we recall both definitions of degree of regularity and compare them with the Castelnuovo-Mumford regularity.

4.1 The Degree of Regularity by Bardet, Faugère, and Salvy

To the best of our knowledge, the degree of regularity appeared first in a paper by Bardet, Faugère, and Salvy [BFS04] and in Bardet's Ph.D. thesis [Bar04]. However, the idea of measuring the complexity of computing the Gröbner basis of a homogeneous ideal using its index of regularity can be traced back to Lazard's seminal work [Laz83]. Before giving the definition, we recall some concepts from commutative algebra.

Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring over a field k, let I be a homogeneous ideal of R, and let $A = R/I$. For an integer $d \geq 0$, we recall that A_d denotes the homogeneous part of degree d of A. The function $HF_A(-) : \mathbb{N} \to \mathbb{N}$, $HF_A(d) = \dim_k A_d$ is called *Hilbert function* of A. It is well known that for large d, the Hilbert function of A is a polynomial in d called *Hilbert polynomial* and denoted by $HP_A(d)$. The generating series of HF_A is called *Hilbert series* of A. We denote it by $HS_A(z) = \sum_{d \in \mathbb{N}} HF_A(d) z^d$. A classical theorem by Hilbert and Serre says that the Hilbert series of A is a rational function, and more precisely has the form

$$HS_A(z) = \frac{h_A(z)}{(1-z)^\ell} \tag{3}$$

where $h_A(z)$ is a polynomial such that $h_A(1) \neq 0$, called *h-polynomial* of A.

Definition 11. *The* index of regularity *of I is the smallest integer $i_{\mathrm{reg}}(I) \geq 0$ such that $HF_{R/I}(d) = HP_{R/I}(d)$ for all $d \geq i_{\mathrm{reg}}(I)$. If $\mathcal{F}$ is a system of generators for I, we set also $i_{\mathrm{reg}}(\mathcal{F}) = i_{\mathrm{reg}}(I)$.*

The index of regularity can be read off the Hilbert series of the ideal, as shown in the next theorem.

Theorem 12 ([BH98], Proposition 4.1.12). *Let $I \subseteq R$ be a homogeneous ideal with Hilbert series as in (3) and let $\delta = \deg h_A$. Then $i_{\mathrm{reg}}(I) = \delta - \ell + 1$.*

Let $I \subseteq R$ be a homogeneous ideal. Applying the Grothendieck-Serre's Formula [BH98, Theorem 4.4.3] to R/I one obtains

$$i_{\mathrm{reg}}(I) \leq \mathrm{reg}(I). \tag{4}$$

Moreover, if I is homogeneous and $I_d = R_d$ for $d \gg 0$, then $i_{\mathrm{reg}}(I) = \mathrm{reg}(I)$ by [Eis05, Corollary 4.15].

Definition 12. *Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R$ be a system of equations and let $(\mathcal{F}^{\mathrm{top}}) = (f_1^{\mathrm{top}}, \ldots, f_r^{\mathrm{top}})$ be the ideal of R generated by the homogeneous part of highest degree of $\mathcal{F}$. Assume that $(\mathcal{F}^{\mathrm{top}})_d = R_d$ for $d \gg 0$. The* degree of regularity *of $\mathcal{F}$ is*

$$d_{\mathrm{reg}}(\mathcal{F}) = i_{\mathrm{reg}}(\mathcal{F}^{\mathrm{top}}).$$

Remark 14. If $(\mathcal{F}^{\mathrm{top}})_d = R_d$ for $d \gg 0$, then $|\mathcal{Z}(\mathcal{F})| < \infty$. The converse, however, does not hold in general. See Example 12 for an example where $\mathcal{F}$ has finitely many solutions over $\bar{k}$, but $(\mathcal{F}^{\mathrm{top}})_d \neq R_d$ for all d.

The following is an easy consequence of the definitions.

Proposition 2. *Let $\mathcal{F} \subseteq R$ be a system of equations. Assume that $(\mathcal{F}^{\text{top}})_d = R_d$ for $d \gg 0$. Then*

$$d_{\text{reg}}(\mathcal{F}) = \text{reg}(\mathcal{F}^{\text{top}}).$$

If in addition $\mathcal{F}$ is homogeneous, then $\mathcal{F}^{\text{top}} = \mathcal{F}$ and

$$d_{\text{reg}}(\mathcal{F}) = \text{reg}(\mathcal{F}).$$

In the context of multivariate cryptosystems however, it is almost never the case that $\mathcal{F}$ is homogeneous and $(\mathcal{F})_d = R_d$ for $d \gg 0$. In fact, this is equivalent to saying that $\mathcal{Z}(I) = \{(0, \ldots, 0)\}$ by Remark 2.

For a system $\mathcal{F}$ such that $I = (\mathcal{F})$ has finite affine zero locus, we may interpret the condition $(\mathcal{F}^{\text{top}})_d = R_d$ for $d \gg 0$ as a *genericity* assumption. This assumption guarantees that the degree of regularity gives an upper bound on the maximum degree of a polynomial in a Gröbner basis of I, with respect to any degree-compatible term order.

Remark 15. Let τ be a degree-compatible term order and assume that $(\mathcal{F}^{\text{top}})_d = R_d$ for $d \gg 0$. Let $I = (\mathcal{F})$ and $J = (\mathcal{F}^{\text{top}})$. Then $HP_{R/J}(z) = 0$, hence $J_d = \text{in}_\tau(J)_d = R_d$ for $d \geq d_{\text{reg}}(\mathcal{F})$. The inclusion $\text{in}_\tau(J)_d \subseteq \text{in}_\tau(I)_d$ holds for any d, since τ is degree-compatible. So we obtain $\text{in}_\tau(I)_d = R_d$ for $d \geq d_{\text{reg}}(\mathcal{F})$. This implies that every element of the reduced Gröbner basis of I has degree at most $d_{\text{reg}}(\mathcal{F})$, that is

$$\text{max. GB. deg}_\tau(\mathcal{F}) \leq d_{\text{reg}}(\mathcal{F}). \tag{5}$$

Notice however that (5) does not yield a bound on the solving degree of $\mathcal{F}$, as we show in the next example.

Example 11. We consider the polynomial systems $\mathcal{F}$ obtained in [BG18] (see also [Bia17, Chapter 5]) for collecting relations for index calculus following the approach outlined by Gaudry in [Gau09]. For $n = 3$, they consist of three non-homogeneous equations f_1, f_2, f_3 of degree 3 in two variables. Computing 150'000 randomly generated examples of cryptographic size (3 different q's, 5 elliptic curves for each q, 10'000 random points per curve), we found that $(\mathcal{F}^{\text{top}})_d = R_d$ for $d \gg 0$ and

$$\text{solv. deg}_{DRL}(\mathcal{F}) = \text{reg}(\mathcal{F}^h) = 5 > 4 = d_{\text{reg}}(\mathcal{F}) = i_{\text{reg}}(\mathcal{F}^{\text{top}}).$$

The computations were performed by G. Bianco with MAGMA [BCP97].

Notice moreover that there are systems $\mathcal{F}$ for which $|\mathcal{Z}(\mathcal{F})| < \infty$ and $(\mathcal{F}^{\text{top}})_d \neq R_d$ for all $d \geq 0$. Definition 12 and inequality (5) do not apply to such systems. This can happen also for polynomial systems arising in cryptography.

When this happens, one may be tempted to consider $i_{\text{reg}}(\mathcal{F}^{\text{top}})$ anyway, and use it to bound the solving degree of $\mathcal{F}$. Unfortunately this approach fails since

$i_{\mathrm{reg}}(\mathcal{F}^{\mathrm{top}})$ and $\mathrm{solv.deg}(\mathcal{F})$ might be far apart, as the next examples shows. On the other hand, the Castelnuovo-Mumford regularity of $\mathcal{F}^h$ still allows us to correctly bound the solving degree of $\mathcal{F}$.

Example 12. We consider the polynomial systems obtained in [GM15] for collecting relations for index calculus following the approach outlined by Gaudry in [Gau09]. For $n = 3$, they consist of three non-homogeneous equations f_1, f_2, f_3 in two variables, of degrees 7,7, and 8. Let $\mathcal{F} = \{f_1, f_2, f_3\}$, $\mathcal{F}^h = \{f_1^h, f_2^h, f_3^h\}$, and $\mathcal{F}^{\mathrm{top}} = \{f_1^{\mathrm{top}}, f_2^{\mathrm{top}}, f_3^{\mathrm{top}}\}$. For 150'000 randomly generated examples of cryptographic size (as in Example 11) we found that $\mathrm{solv.deg}_{DRL}(\mathcal{F}) = \mathrm{reg}(\mathcal{F}^h) = 15$, $(\mathcal{F}^{\mathrm{top}})_d \neq R_d$ for all $d \geq 0$, and $i_{\mathrm{reg}}(\mathcal{F}^{\mathrm{top}}) = 8$. The computations were performed by G. Bianco with MAGMA [BCP97].

Finally, given a polynomial system $\mathcal{F} = \{f_1, \ldots, f_r\}$ there is a simple relation between the ideals $(\mathcal{F}^{\mathrm{top}}) \subseteq R$ and $(\mathcal{F}^h) \subseteq S$, namely

$$(\mathcal{F}^{\mathrm{top}})S + (t) = (\mathcal{F}^h) + (t). \tag{6}$$

Here $(\mathcal{F}^{\mathrm{top}})S$ denotes the extension of $(\mathcal{F}^{\mathrm{top}})$ to S, i.e., the ideal of S generated by $\mathcal{F}^{\mathrm{top}}$. Since $\mathcal{F}^{\mathrm{top}} \subseteq R$, $t \nmid 0$ modulo $(\mathcal{F}^{\mathrm{top}})S$. If $t \nmid 0$ modulo $(\mathcal{F}^h)$, then $(\mathcal{F}^h) = (\mathcal{F})^h$ is the homogenization of $(\mathcal{F})$ and $\mathrm{reg}(\mathcal{F}^h) = \mathrm{reg}(\mathcal{F}^{\mathrm{top}})$. Therefore, if $t \nmid 0$ modulo $\mathcal{F}^h$ and $(\mathcal{F}^{\mathrm{top}})_d = R_d$ for $d \gg 0$, then

$$d_{\mathrm{reg}}(\mathcal{F}) = \mathrm{reg}(\mathcal{F}^h)$$

by Proposition 2. However, one expects that in most cases $t \mid 0$ modulo $(\mathcal{F}^h)$. In fact, $(\mathcal{F}^h) = (\mathcal{F})^h$ only in very special cases, namely when $f_1, \ldots, f_r$ are a Macaulay basis of $(\mathcal{F})$ with respect to the standard grading (see [KR05, Theorem 4.3.19]). Therefore (6) usually does not allow us to compare the regularity and the index of regularity of $\mathcal{F}^h$ and $\mathcal{F}^{\mathrm{top}}$. See also [BDDGMT20, Section 4.1] for a more detailed discussion.

4.2 The Degree of Regularity by Ding and Schmidt

The second notion of degree of regularity is more recent. To the extent of our knowledge it has been introduced by Dubois and Gama [DG10], and later has been used by several authors such as Ding, Schmidt, and Yang [DS13,DY13]. The definition we present here is taken from [DS13], and differs slightly from the original one of Dubois and Gama.

Let $\mathbb{F}_q$ and let $B = \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$. Let $f_1, \ldots, f_r \in B$ be homogeneous polynomials of degree 2. We fix a B-module homomorphism φ sending the canonical basis $e_1, \ldots, e_r$ of B^r to $\{f_1, \ldots, f_r\}$, that is for every $(b_1, \ldots, b_r) \in B^r$ we have $\varphi(b_1, \ldots, b_r) = \sum_{i=1}^r b_i f_i$. We denote by $\mathrm{Syz}(f_1, \ldots, f_r)$ the first syzygy module of $f_1, \ldots, f_r$, that is the kernel of φ. An element of $\mathrm{Syz}(f_1, \ldots, f_r)$ is a syzygy of $f_1, \ldots, f_r$. In other words, it is a vector of polynomials $(b_1, \ldots, b_r) \in B^r$ such that $\sum_{i=1}^r b_i f_i = 0$.

An example of syzygy is given by the Koszul syzygies $f_i e_j - f_j e_i$, where $i \neq j$ or by the syzygies coming by the quotient structure of B, that is $f_i^{q-1} e_i$.

Here e_i denotes the i-th element of the canonical basis of B. These syzygies are called *trivial syzygies*, because they are always present and do not depend on the structure of $f_1, \ldots, f_r$, but rather on the ring structure of B. We define the module $\mathrm{Triv}(f_1, \ldots, f_r)$ of trivial syzygies of $f_1, \ldots, f_r$ as the submodule of $\mathrm{Syz}(f_1, \ldots, f_r)$ generated by $\{f_i e_j - f_j e_i : 1 \leq i < j \leq r\} \cup \{f_i^{q-1} e_i : 1 \leq i \leq r\}$.

For any $d \in \mathbb{N}$ we define the vector space $\mathrm{Syz}(\mathcal{F})_d = \mathrm{Syz}(\mathcal{F}) \cap B_d^r$ of syzygies of degree d. We define the vector subspace of trivial syzygies of degree d as $\mathrm{Triv}(\mathcal{F})_d = \mathrm{Triv}(\mathcal{F}) \cap B_d^r$. Clearly, we have $\mathrm{Triv}(\mathcal{F})_d \subseteq \mathrm{Syz}(\mathcal{F})_d$.

Definition 13. *Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq B$ be a system of polynomials of degree 2. The* degree of regularity *of $\mathcal{F}$ is*

$$\delta_{\mathrm{reg}}(\mathcal{F}) = \min\{d \geq 2 : \ \mathrm{Syz}(\mathcal{F}^{\mathrm{top}})_{d-2} / \mathrm{Triv}(\mathcal{F}^{\mathrm{top}})_{d-2} \neq 0\}.$$

Remark 16. Dubois and Gama [DG10] work in the ring $\mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q - x_1, \ldots, x_n^q - x_n)$ and not in $B = \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$.

The degree of regularity is the first degree where we have a linear combination of multiples of $f_1, \ldots, f_r$ which produces a non-trivial cancellation of their top degree parts. For this reason, some authors refer to it as *first fall degree*.

One may wonder whether the degree of regularity by Ding and Schmidt is close to the solving degree of a polynomial system of quadratic equations. Ding and Schmidt showed that this is not always the case. In fact, it is easy to produce examples, the so-called degenerate systems, for which the degree of regularity and the solving degree are far apart. For a detailed exposition on this problem and several examples we refer the reader to their paper [DS13].

We are not aware of any results relating $\delta_{\mathrm{reg}}(\mathcal{F})$ (Definition 13) and $d_{\mathrm{reg}}(\mathcal{F})$ (Definition 12). Despite the fact that they share the name, we do not see an immediate connection. A comparison between these two invariants is beyond the scope of this paper.

5 Solving Degree of Ideals of Minors and the MinRank Problem

The goal of this section is giving an example of how the results from Sect. 3, in combination with known commutative algebra results, allow us to prove estimates for the solving degree in a simple and synthetic way. We consider polynomial systems coming from the MinRank Problem. For more bounds on the complexity of the MinRank Problem, see [CG20].

The MinRank Problem can be stated as follows. Given an integer $t \geq 1$ and a set $\{M_1, \ldots, M_n\}$ of $s \times s$ matrices with entries in a field k, find a non-zero tuple $\lambda = (\lambda_1, \ldots, \lambda_n) \in k^n$ such that

$$\mathrm{rank}\left(\sum_{i=1}^{n} \lambda_i M_i\right) \leq t - 1. \tag{7}$$

This problem finds several applications in multivariate cryptography and in other areas of cryptography as well. For example, Goubin and Courtois [GC00] solved a MinRank Problem to attack Stepwise Triangular Systems, and Kipnis and Shamir [KS99] solved an instance of MinRank in their cryptanalysis of the HFE cryptosystem.

Consider the matrix $M = \sum_{i=1}^{n} x_i M_i$, whose entries are homogeneous linear forms in R. Condition (7) is equivalent to requiring that the minors of size $t \times t$ of M vanish. Therefore, every solution of the MinRank Problem corresponds to a non-zero point in the zero locus in k^n of the ideal $I_t(M)$ of t-minors of M. A similar algebraic formulation can be given for the Generalized MinRank Problem, which finds applications within coding theory, non-linear computational geometry, real geometry, and optimization. We refer the interested reader to [FSS13] for a discussion of the applications of the Generalized MinRank Problem and a list of references.

Problem 1 (Generalized MinRank Problem). Given a field k, an $r \times s$ matrix M whose entries are polynomials in $R = k[x_1, \ldots, x_n]$, and an integer $1 \leq t \leq \min\{r, s\}$, find a point in $k^n \setminus \{(0, \ldots, 0)\}$ at which the evaluation of M has rank at most $t - 1$.

The Generalized MinRank Problem can be solved by computing the zero locus of the ideal of t-minors $I_t(M)$. The minors of size $t \times t$ of the matrix M form an algebraic system of multivariate polynomials, which one can attempt to solve by computing a Gröbner basis. This motivates our interest in estimating the solving degree of this system for large classes of matrices.

Ideals of minors of a matrix with entries in a polynomial ring are called *determinantal ideals* and have been extensively studied in commutative algebra and algebraic geometry. Using Theorem 9, we can take advantage of the literature on the regularity of determinantal ideals to give bounds on the solving degree of systems of minors of certain large classes of matrices. For simplicity, we focus on homogeneous matrices.

Definition 14. *Let M be an $r \times s$ matrix with $r \leq s$, whose entries are elements of R. The matrix M is* homogeneous *if both its entries and its 2-minors are homogeneous polynomials.*

It is easy to see that the minors of any size of a homogeneous matrix are homogeneous polynomials. Moreover, observe that a matrix whose entries are homogeneous polynomials of the same degree is a homogeneous matrix, but there are homogeneous matrices whose entries have different degrees. After possibly exchanging some rows and columns, we may assume without loss of generality that the degrees of the entries of a homogeneous matrix increase from left to right and from top to bottom. With this notation, we can compute the solving degree of our first family of systems of minors. We refer the reader to [Eis94] for the definition of height of an ideal.

Theorem 13. *Let $M = (f_{ij})$ be an $r \times s$ homogeneous matrix with $r \leq s$, whose entries are elements of R, $n \geq s - r + 1$. Let $\mathcal{F}$ be the polynomial system of the*

minors of size r of M and assume that $\operatorname{height}(I_r(M)) = s - r + 1$. *Then the solving degree of $\mathcal{F}$ is upper bounded by*

$$\operatorname{solv.deg}(\mathcal{F}) \leq \deg(f_{1,1}) + \ldots + \deg(f_{m,m}) + \deg(f_{m,m+1}) + \ldots + \deg(f_{m,n}) - s + r.$$

If $\deg(f_{i,j}) = 1$ *for all* i, j, *then* $\operatorname{solv.deg}(\mathcal{F}) = r$.

Proof. Since the matrix M is homogeneous, the system of minors $\mathcal{F}$ consists of homogeneous polynomials. The regularity of the corresponding ideal $I_r(M) = (\mathcal{F})$ is

$$\operatorname{reg}(I_r(M)) = \deg(f_{1,1}) + \ldots + \deg(f_{r,r}) + \deg(f_{r,r+1}) + \ldots + \deg(f_{r,s}) - s + r.$$

The formula can be found in [BCG04, Proposition 2.4] and is derived from a classical result of Eagon and Northcott [EN62]. The bound on the solving degree now follows from Theorem 9. In particular, if $\deg(f_{i,j}) = 1$ for all i, j, then $\operatorname{solv.deg}(\mathcal{F}) \leq r$. Since $I_r(M)$ is generated in degree r, then $\operatorname{solv.deg}(\mathcal{F}) = r$. □

Notice that the assumption on the height is satisfied by a matrix M whose entries are generic homogeneous polynomials of fixed degrees. If $n = s - r + 1$, then $I_r(M)_d = R_d$ for $d \gg 0$, hence $d_{\mathrm{reg}}(\mathcal{F}) = \operatorname{reg}(\mathcal{F})$, where $\mathcal{F}$ is the set of maximal minors of M. Therefore, Theorem 13 recovers the results of [FSS10, FSS13] for $n = s - r + 1$ and $t = r$, and extends them to homogeneous matrices whose entries do not necessarily have the same degree.

We now restrict to systems of maximal minors of matrices of linear forms. The MinRank Problem associated to this class of matrices is a slight generalization of the classical MinRank Problem of (7). From the previous result it follows that, if the height of the ideal of maximal minors is as large as possible, then the solving degree of the corresponding system is as small as possible, namely r. We now give different assumptions which allows us to obtain the same estimate on the solving degree, for ideals of maximal minors whose height is not maximal. We are also able to bound the solving degree of the system of 2-minors.

Let R have a standard $\mathbb{Z}^v$-graded structure, i.e., the degree of every indeterminate of R is an element of the canonical basis $\{e_1, \ldots, e_v\}$ of $\mathbb{Z}^v$.

Definition 15. *Let $M = (f_{i,j})$ be an $r \times s$ matrix with entries in R, $r \leq s$. We say that M is* column-graded *if $s \leq v$, and $f_{i,j} = 0$ or it is homogeneous of degree $\deg(f_{i,j}) = e_j \in \mathbb{Z}^v$ for every i, j. We say that M is* row-graded *if $r \leq v$, and $f_{i,j} = 0$ or it is homogeneous of degree $\deg(f_{i,j}) = e_i \in \mathbb{Z}^v$ for every i, j.*

Informally, a matrix is row-graded if the entries of each row are homogeneous linear forms in a different set of variables. Similarly for a column-graded matrix.

Theorem 14. *Let M be an $r \times s$ row-graded or column-graded matrix with entries in R . Assume that $r \leq s$ and $I_r(M) \neq 0$. Then:*

- *if $\mathcal{F}$ is the system of maximal minors of M then* $\operatorname{solv.deg}(\mathcal{F}) = r$,

– *if* $\mathcal{F}$ *is the system of* 2*-minors of* M *then* $\operatorname{solv.deg}(\mathcal{F}) \leq s$ *in the column-graded case, and* $\operatorname{solv.deg}(\mathcal{F}) \leq r$ *in the row-graded case.*

Proof. It is shown in [CDG15, CDG20] that $\operatorname{reg}(I_r(M)) = r$, $\operatorname{reg}(I_2(M)) \leq s$ in the column-graded case, and $\operatorname{reg}(I_2(M)) \leq r$ in the row-graded case. The bounds on the solving degree now follow from Theorem 9. □

Acknowledgements. The authors are grateful to Albrecht Petzoldt for help with MAGMA computations, to Wouter Castryck for pointing out some typos in an earlier version of this paper, and to Marc Chardin, Teo Mora, Christophe Petit, and Pierre-Jean Spaenlehauer for useful discussions on the material of this paper. This work was made possible thanks to funding from Armasuisse.

References

[Bar04] Bardet, M.: Étude des systémes algébriques surdéterminés. Applications aux codes correcteurs et á la cryptographie, Ph.D. thesis, Université Paris 6 (2004)

[BFS04] Bardet, M., Faugère, J.-C., Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: ICPPSS International Conference on Polynomial System Solving (2004)

[BFS15] Bardet, M., Faugère, J.-C., Salvy, B.: On the complexity of the F_5 Gröbner basis algorithm. J. Symb. Comput. **70**, 49–70 (2015)

[BS87] Bayer, D., Stillman, M.: A criterion for detecting m-regularity. Invent. Math. **87**(1), 1–11 (1987). https://doi.org/10.1007/BF01389151

[Bia17] Bianco, G.: Trace-zero subgroups of elliptic and twisted Edwards curves: a study for cryptographic applications, Ph.D. thesis (2017). https://doi.org/10.35662/unine-thesis-2631

[BG18] Bianco, G., Gorla, E.: Index calculus in trace-zero subgroups and generalized summation polynomials, preprint (2018)

[BDDGMT20] Bigdeli, M., De Negri, E., Dizdarevic, M.M., Gorla, E., Minko, R., Tsakou, S.: Semi-regular sequences and other random systems of equations, preprint (2020)

[BCP97] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997)

[BH98] Bruns, W., Herzog, J.: Cohen-Macaulay rings. Revised ed. Cambridge Studies in Advanced Mathematics, vol. 39. Cambridge University Press, Cambridge (1998)

[BCG04] Budur, N., Casanellas, M., Gorla, E.: Hilbert functions of irreducible arithmetically Gorenstein schemes. J. Algebra **272**(1), 292–310 (2004)

[CG20] Caminata, A., Gorla, E.: The complexity of MinRank. In: Cojocaru, A., Ionica, S., Lorenzo Garcia, E. (eds.) Women in Numbers Europe III: Research Directions in Number Theory. Springer (to appear)

[Cha07] Chardin, M.: Some results and questions on Castelnuovo-Mumford regularity. In: Syzygies and Hilbert Functions. Lecture Notes in Pure and Applied Mathematics, vol. 254, pp. 1–40 (2007)

[CDG15] Conca, A., De Negri, E., Gorla, E.: Universal Gröbner bases for maximal minors. In: International Mathematics Research Notices, IMRN 2015, no. 11, pp. 3245–3262 (2015)

[CDG20] Conca, A., De Negri, E., Gorla, E.: Universal Gröbner bases and Cartwright-Sturmfels ideals. International Mathematics Research Notices, IMRN 2020, no. 7, pp. 1979–1991 (2020)

[CKPS00] Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 392–407. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_27

[CLO07] Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer, Cham (2015). https://doi.org/10.1007/978-0-387-35651-8

[DBMMW08] Ding, J., Buchmann, J., Mohamed, M.S.E., Moahmed, W.S.A.E., Weinmann, R.-P.: MutantXL. In: Proceedings of the 1st international conference on Symbolic Computation and Cryptography (SCC08), Beijing, China, LMIB, pp. 16–22 (2008)

[DS13] Ding, J., Schmidt, D.: Solving degree and degree of regularity for polynomial systems over a finite fields. In: Fischlin, M., Katzenbeisser, S. (eds.) Number Theory and Cryptography. LNCS, vol. 8260, pp. 34–49. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-42001-6_4

[DY13] Ding, J., Yang, B.-Y.: Degree of regularity for HFEv and HFEv-. In: Gaborit, P. (ed.) PQCrypto 2013. LNCS, vol. 7932, pp. 52–66. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38616-9_4

[DG10] Dubois, V., Gama, N.: The degree of regularity of HFE systems. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 557–576. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17373-8_32

[Eis94] Eisenbud, D.: Commutative Algebra. With a View Toward Algebraic Geometry. Graduate Texts in Mathematics, vol. 150. Springer, New York (1994). https://doi.org/10.1007/978-1-4612-5350-1

[Eis05] Eisenbud, D.: The Geometry of Syzygies A Second Course in Algebraic Geometry and Commutative Algebra. Graduate Texts in Mathematics, vol. 229. Springer, New York (2005). https://doi.org/10.1007/b137572

[EN62] Eagon, J.A., Northcott, D.G.: Ideals defined by matrices and a certain complex associated with them. In: Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, vol. 269, no. 1337, pp. 188–204 (1962)

[Fau99] Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases (F4). J. Pure Appl. Algebra **139**, 61–88 (1999)

[Fau02] Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ISSAC 2002, New York, NY, USA, pp. 75–83 (2002)

[FGLM93] Faugère, J.-C., Gianni, P.M., Lazard, D., Mora, T.: Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symb. Comput. **16**(4), 329–344 (1993)

[FSS10] Faugère, J.-C., El Din, M.S., Spaenlehauer, P.-J.: Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, ISSAC 2010, Munich, Germany, pp. 257–264 (2010)

[FSS13] Faugère, J.-C., Din, M.S.E., Spaenlehauer, P.-J.: On the complexity of the generalized MinRank problem. J. Symb. Comput. **55**, 30–58 (2013)

[Gal74] Galligo, A.: A propos du théorème de préparation de weierstrass. In: Norguet, F. (ed.) Fonctions de Plusieurs Variables Complexes. LNM, vol. 409, pp. 543–579. Springer, Heidelberg (1974). https://doi.org/10.1007/BFb0068121

[Gau09] Gaudry, P.: Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. J. Symb. Comput. **44**(12), 1690–1702 (2009)

[GC00] Goubin, L., Courtois, N.T.: Cryptanalysis of the TTM cryptosystem. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 44–57. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-44448-3_4

[GM15] Gorla, E., Massierer, M.: Index calculus in the trace zero variety. Adv. Math. Commun. **9**(4), 515–539 (2015)

[KS99] Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 19–30. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_2

[KR00] Kreuzer, M., Robbiano, L.: Computational Commutative Algebra 1. Springer, Heidelberg (2000). https://doi.org/10.1007/978-3-540-70628-1

[KR05] Kreuzer, M., Robbiano, L.: Computational Commutative Algebra 2. Springer, Heidelberg (2005). https://doi.org/10.1007/3-540-28296-3

[KR16] Kreuzer, M., Robbiano, L.: Computational Linear and Commutative Algebra. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-319-43601-2

[Laz83] Lazard, D.: Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In: Computer Algebra (London, 1983). Lecture Notes in Computer Science, vol. 162, pp. 146–156. Springer, Berlin (1983)

[NIST] National Institute of Standards, Post-Quantum Cryptography, Round 3 Submissions. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[TDTD13] Tao, C., Diene, A., Tang, S., Ding, J.: Simple matrix scheme for encryption. In: Gaborit, P. (ed.) PQCrypto 2013. LNCS, vol. 7932, pp. 231–242. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38616-9_16

[TXPD15] Tao, C., Xiang, H., Petzoldt, A., Ding, J.: Simple matrix - a multivariate public key cryptosystem (MPKC) for encryption. Finite Fields Appl. **35**, 352–368 (2015)