SOLVING MULTIVARIATE POLYNOMIAL SYSTEMS AND AN INVARIANT FROM COMMUTATIVE ALGEBRA

ALESSIO CAMINATA AND ELISA GORLA

Abstract. The security of several post-quantum cryptosystems is based on the assumption that solving a system of multivariate (quadratic) polynomial equations $p_1 = \cdots = p_r = 0$ over a finite field is hard. Such a system can be solved by computing a lexicographic Gröbner basis of the ideal $(p_1, \dots, p_r)$. The most efficient algorithms for computing Gröbner bases transform the problem into several instances of Gaussian elimination. The computational complexity of these algorithms is not completely understood, especially when the polynomials $p_1, \dots, p_r$ are not homogeneous. In this paper, we prove that this complexity is controlled by the Castelnuovo-Mumford regularity of the ideal $(p_1^h, \dots, p_r^h)$ obtained by homogenizing the input polynomials. This allows us to bound the complexity of solving a system of polynomial equations when the associated ideal is zero-dimensional, a common situation in cryptography. In combination with some theorems in commutative algebra, our results also allow us to bound the complexity of the ABC and cubic simple matrix schemes, as well as some instances of the MinRank Problem.

Introduction

Multivariate (public key) cryptography is one of the main candidates for post-quantum cryptography, that is cryptographic schemes which are expected to resist to attacks run on quantum computers. The public key of a multivariate cryptosystem takes the form of a multivariate polynomial map $\mathcal{P} = (p_1, \dots, p_r)$ over a finite field $\mathbb{F}_q$. Each p_i is a polynomial in n variables with coefficients in $\mathbb{F}_q$, thus the encryption map $\mathcal{P}$ goes from $\mathbb{F}_q^n$ to $\mathbb{F}_q^r$. Usually the polynomials p_i are quadratic, for this reason these systems are also called multivariate quadratic (MQ) cryptosystems. For a given plaintext $x \in \mathbb{F}_q^n$, the user computes $y = \mathcal{P}(x) = (p_1(x), \dots, p_r(x))$ and sends the message $y \in \mathbb{F}_q^r$. An illegitimate user who wants to read the message may try to solve the system of polynomial equations

$$\begin{cases} y_1 - p_1(x) = 0 \\ \vdots \\ y_r - p_r(x) = 0 \end{cases} \tag{1}$$

The security of MQ cryptosystem is thus based on the assumption that solving a system of polynomial (quadratic) equations over a finite field is hard. Actually, solving a generic system of multivariate polynomials p_i is NP-complete, even for degree 2 polynomials over $\mathbb{F}_2$ (see e.g. [GJ79, Appendix A7]). However, in polynomial systems coming from cryptography the polynomials p_i are not truly random, since they must possess a trapdoor in order to allow the legitimate receiver of the message to easily decrypt it. Hence, an illegitimate user may be able to exploit the specific structure of the trapdoor to break a given cryptosystem. Moreover, another attack is possible for every MQ system, namely trying to solve system (1) directly. This kind of attack is sometimes called *algebraic attack*. For this reason, it is important to be able to estimate the difficulty of solving system (1) for different choices of the polynomials $p_1, \dots, p_r$.

2010 *Mathematics Subject Classification.* Primary: 94A60, 13P10, 13P15, 13P25, 68W40.

Key words and phrases. solving degree; degree of regularity; Castelnuovo-Mumford regularity; Gröbner basis; multivariate cryptography; post-quantum cryptography.

This work was supported by Armasuisse.

The elimination properties of lexicographic Gröbner bases ensure that the solutions of a polynomial system of equations can be easily read from a lexicographic Gröbner basis of the corresponding ideal (see Proposition 2.2). Lexicographic Gröbner bases usually have large computational complexity, while Gröbner bases with respect to the graded reverse lexicographic (*DRL*) term order can often be computed more efficiently than for any other term order. Hence a commonly used strategy for computing the zero locus of an ideal is computing a *DRL* Gröbner basis, then converting it to a lexicographic Gröbner basis. The second step is usually performed via the Gröbner walk Algorithm, or the FGLM Algorithm if the ideal is zero-dimensional. The computational complexity of the last two algorithms is well understood and it is often lower than that of the *DRL* Gröbner basis computation. Therefore, in this paper we concentrate on the latter.

One may identify at least two main families of Gröbner bases algorithms: Buchberger's Algorithm and its improvements, and algorithms that transform the problem of computing a Gröbner basis into several instances of Gaussian elimination. Algorithms in the second family are more recent and include F_4, F_5, the XL algorithm, and MutantXL. They are usually faster than the algorithms in the first family, but their computational complexity is less understood.

The complexity of these algorithms is dominated by Gaussian elimination in the *Macaulay matrix* corresponding to the largest degree encountered in the computation. Since the number of rows and columns of a Macaulay matrix depends on the degree considered, the number of variables, the number of polynomials in the system, and their degrees, the computational complexity of Gaussian elimination can be expressed in terms of these invariants. Therefore, in order to estimate the complexity of computing a *DRL* Gröbner basis using the second family of algorithms, it is crucial to be able to determine the highest degree of the polynomials involved in the computation. This degree is called *solving degree* (see Definition 3.1).

In order to design a multivariate cryptosystem that is secure against algebraic attacks, one needs to know how the solving degree depends on the parameters of the system, or at least to have a good estimate for it. Clearly, one would like to be able to estimate the solving degree without computing a Gröbner basis. For this reason, one wishes to better understand the solving degree from both a practical and a theoretical point of view. The most interesting case from the point of view of cryptographic applications, and also the most challenging one, is that when the polynomials $f_1, \ldots, f_r$ are not homogeneous.

Our main result is Theorem 3.23, where we prove that the solving degree of a polynomial system $f_1, \ldots, f_r$ is upper bounded by – and often equal to – the *Castelnuovo-Mumford regularity* of the ideal $\tilde{I} = (f_1^h, \ldots, f_r^h)$, where f_i^h is the homogenization of f_i. We establish this result under the assumption that the ideal $\tilde{I}$ is either zero-dimensional (i.e., that it has finitely many projective solutions) or in generic coordinates (see Definition 1.10). The analogous result for the case of homogeneous equations is shown in Theorem 3.22.

The Castelnuovo-Mumford regularity is an invariant of a homogeneous ideal which can be defined in terms of its minimal graded free resolution (see Definition 3.17). Upper bounds for the Castelnuovo-Mumford regularity of several classes of ideals are known. Our main theorem allows us to convert these bounds into bounds on the solving degree of multivariate polynomial systems. In particular, we obtain an upper bound for the solving degree of any zero-dimensional ideal, which is linear both in the number of variables and in the maximum of the degrees of the equations (see Corollary 3.26).

In addition, in Theorem 3.14 we establish a series of equalities and inequalities relating the solving degree and the largest degree of a polynomial in a reduced Gröbner basis of the ideals $I = (f_1, \ldots, f_r)$, $\tilde{I} = (f_1^h, \ldots, f_r^h)$, and the homogenized ideal $I^h = (f^h \mid f \in I)$. This in particular clarifies the fact that the solving degree of I is in general larger than the largest degree of a polynomial in a reduced Gröbner basis of I, and relates this phenomenon to the well-known fact that in general the homogenized ideal I^h strictly contains the ideal $\tilde{I}$.

We also provide a comparison with the main current approaches for estimating the complexity of computing Gröbner bases. In particular, we compare the invariant that we propose with the two main notions of degree of regularity currently in use. In particular, we provide examples of systems coming from cryptographic applications such that the solving degree is strictly larger than the degree of regularity (see Example 4.7) or the degree of regularity is not defined (see Example 4.8).

Finally, we give examples of how one can use our techniques to bound the solving degree of specific systems coming from cryptographic applications: Examples 3.27 and 3.28 provide the first provable upper bounds on the solving degree of the ABC and cubic simple matrix cryptosystems. In Section 5 we apply our techniques to some systems of equations related to the MinRank Problem. We are able to prove some known results on the solving degree of such systems and to extend them in some cases. The strength of our approach lies in the fact that, while previous estimates of similar nature were obtained with lengthy and complicated computations, our approach yields simple and very short proofs.

The structure of the paper is the following. In Section 1 we recall the basic definitions and results on Gröbner bases that we need in the rest of the paper. In Section 2 we discuss the connection between lexicographic Gröbner bases and solving polynomial systems of equations. Section 3 contains the main result of the paper. Here we prove that the computational complexity of solving a system of polynomial equations with F_4, F_5, XL, or MutantXL is controlled by the Castelnuovo-Mumford regularity of a homogeneous ideal associated to the system. We also show that the Macaulay bound is an immediate consequence of our approach. In Section 4 we investigate the relation between the Castelnuovo-Mumford regularity of an ideal and its degree of regularity. Section 5 contains an application of our results to 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 can be found with expanded details in the books [KR00], [KR05], [KR16], and [CLO07].

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*.

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

Remark 1.1. Let I be a homogeneous ideal of R minimally generated by $f_1, \dots, f_r$, then every homogeneous minimal system of generators of I consists of r polynomials of the same degrees as $f_1, \dots, f_r$.

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

(1) $m \leq n$ implies $p \cdot m \leq p \cdot n$ for all $p, m, n \in \mathbb{T}$;

(2) $1 \leq m$ for all $m \in \mathbb{T}$.

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

Example 1.2 (Lexicographic term order)**.** Let x^α and x^β be two terms in $k[x_1,\dots,x_n]$. We say that $x^\alpha >_{LEX} x^\beta$ if the leftmost nonzero 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 1.3 (Graded reverse lexicographic term order)**.** Let x^α and x^β be two terms in $k[x_1,\dots,x_n]$. We say that $x^\alpha >_{DRL} x^\beta$ if $|\alpha|>|\beta|$, or $|\alpha|=|\beta|$ and the rightmost nonzero entry in $\alpha-\beta\in\mathbb{Z}^n$ is negative. This term order is called graded reverse lexicographic (*DRL* for short) and it is degree compatible.

Let $f=\sum_{i\in\mathcal{I}}a_im_i$ be a polynomial of R, where $a_i\in k\setminus\{0\}$, and $m_i\in\mathbb{T}$ are distinct terms. We fix a term order $\leq$ on R. The *initial term* or *leading term* of f with respect to $\leq$ is the largest term appearing in f, that is $\mathrm{in}_\leq(f)=m_j$, 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

$$\mathrm{in}_\leq(I)=(\mathrm{in}_\leq(f):\ f\in I).$$

Definition 1.4. Let I be an ideal of R, a set of polynomials $\mathcal{G}\subseteq I$ is a *Gröbner basis* of I with respect to $\leq$ if $\mathrm{in}_\leq(I)=(\mathrm{in}_\leq(g):\ g\in\mathcal{G})$. A Gröbner basis is *reduced* if $m\notin(\mathrm{in}_\leq(h):\ h\in\mathcal{G}\setminus\{g\})$ for all $g\in\mathcal{G}$ and $m\in\mathrm{supp}(g)$.

Notice that a Gröbner basis of I is also a system of generators of I, although often not a minimal one.

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

1.1. **Zero-dimensional ideals.**

In this paper we are mostly interested in ideals whose zero locus is finite.

Definition 1.6. An inhomogeneous ideal I of $k[x_1,\dots,x_n]$ is *zero-dimensional* if the affine zero locus

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

of I over the algebraic closure $\bar{k}$ of k is finite.

Equivalently, I is zero-dimensional if the *Krull dimension* of R/I is zero. This is in turn equivalent to R/I being a finite dimensional k-vector space.

The affine zero locus of a homogeneous ideal is finite if and only if $\mathcal{Z}(I)=\{(0,\dots,0)\}$. This motivates the following definition.

Definition 1.7. A homogeneous ideal I of $k[x_0,\dots,x_n]$ is *zero-dimensional* if the projective zero locus

$$\mathcal{Z}_+(I)=\{P\in\mathbb{P}(\bar{k})^n:\ f(P)=0\ \text{ for all } f\in I\}$$

of I over the algebraic closure $\bar{k}$ of k is finite.

In Definition 1.6 and Definition 1.7 it is important to look at the zero locus of I 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 of I is finite over k is trivially satisfied by any ideal. This clearly does not imply that every ideal defined over a finite field is zero-dimensional.

However, for any $I=(f_1,\dots,f_r)\subset R=\mathbb{F}_q[x_1,\dots,x_n]$ there is a canonical way to construct an ideal J which has the same zero locus of I over $\mathbb{F}_q$ and is zero-dimensional. This is done by adding the field equations of $\mathbb{F}_q$ to I. Namely, $J = (f_1, \dots, f_r, x_1^q - x_1, \dots, x_n^q - x_n)$ is zero-dimensional and has the same zero locus as I. Notice however that, even if I and J have the same zero locus over $\mathbb{F}_q$, they often have different algebraic properties. For example, in most cases J has a minimal generator of degree q and this may affect the complexity of computing a Gröbner basis. Therefore, depending on the size q of the finite field, passing from I to J may or may not provide an advantage. Even more, for large values of q adding the field equations may not be computationally feasible. In the next example, we show that the solving degree may increase when passing from I to J.

Example 1.8. Let $I = (x_1^2 - x_2, x_2^3 - x_3)$ be an ideal in $\mathbb{F}_5[x_1, x_2, x_3]$. The ideal I is not zero-dimensional, actually it has infinitely many solutions over the algebraic closure $\overline{\mathbb{F}}_5$. Its zero locus is a curve in the three-dimensional affine space over $\overline{\mathbb{F}}_5$. If we add the field equations of $\mathbb{F}_5$ to I, we obtain a zero-dimensional ideal $J = (x_1^2 - x_2, x_2^3 - x_3, x_1^5 - x_1, x_2^5 - x_2, x_3^5 - x_3)$ which has the same solutions of I over $\mathbb{F}_5$, namely the five points $(0,0,0)$, $(1,1,1)$, $(2,4,4)$, $(3,4,4)$, $(4,1,1)$. Notice that the generators of I are a Gröbner basis with respect to the LEX order with $x_3 > x_2 > x_1$, while the reduced Gröbner basis of J with respect to the same order also contains $x_1^5 - x_1$. In particular, the Gröbner basis of J contains a polynomial of higher degree and $\operatorname{solv.deg}(J) = 5$, while $\operatorname{solv.deg}(I) = 3$ (see Definition 3.1 for the definition of solving degree).

1.2. **Generic changes of coordinates.** Throughout this section, we assume that the ground field k is infinite and we fix a term order $\leq$ on the polynomial ring $R = k[x_1, \dots, x_n]$.

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 the polynomial ring 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 $\mathrm{GL}(n,k)$ is an algebraic group equipped with the Zariski topology.

Theorem 1.9. ([Gal74]) *Let I be a homogeneous ideal of R, then there exist a nonempty Zariski open set $U \subseteq \mathrm{GL}(n,k)$ and a monomial ideal J such that $\mathrm{in}_\leq(gI) = J$ for all $g \in U$.*

Definition 1.10 (generic coordinates). An ideal $I \subseteq R$ is *in generic coordinates* if $1 \in U$, i.e., if

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

for all $g \in U$. Let $L \supseteq k$ be a field extension. I is *in generic coordinates over L* if $IL[x_1, \dots, x_n] \subseteq L[x_1, \dots, x_n]$ is in generic coordinates.

Notice that gI is in generic coordinates for any ideal I and a generic $g \in \mathrm{GL}(n,k)$. In other words, any ideal can be put in generic coordinates by applying a generic change of coordinates to it.

1.3. **Homogeneous ideals associated to an ideal.** Let $R = k[x_1, \dots, x_n]$ be a polynomial ring in n variables over a field k, 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 any ideal $I = (f_1, \dots, f_r) \subseteq R$, we denote by $\tilde{I}$ the homogeneous ideal of S generated by the homogenizations of the f_i's, that is

$$\tilde{I} = (f_1^h, \dots, f_r^h).$$

The notation $\tilde{I}$ is compact, but may be misleading, since the ideal $\tilde{I}$ actually depends on the choice of the generators $f_1, \dots, f_r$ and not only on the ideal I.

The *homogenization of I with respect to t* or simply the homogenization of I is the ideal

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

Notice that I^h is a homogeneous ideal of S which contains $\tilde{I}$. Moreover I^h only depends on I, and not on the choice of generators of I.

Remark 1.11. 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 $\tilde{I}$ coincide with the degrees of $f_1, \dots, f_r$.

The *dehomogenization map* ϕ is the standard projection on the quotient $\phi : S \to R \cong S/(t-1)$. For any ideal, $I \subseteq R$ we have $\phi(I^h) = \phi(\tilde{I}) = I$.

For a polynomial $f \in R$, we denote by f^{top} its homogeneous part of highest degree. For an ideal $I = (f_1, \dots, f_r)$ we denote by

$$I^{\text{top}} = (f_1^{\text{top}}, \dots, f_r^{\text{top}}).$$

As for the ideal $\tilde{I}$, the ideal I^{top} depends on the choice of the generators $f_1, \dots, f_r$ and not only on I. We use the notation I^{top}, hoping that no confusion arises.

2. The importance of being *LEX*

The main link between the theory of Gröbner basis and solving polynomial systems is provided by the *LEX* term order. It is often stated that a Gröbner basis of an ideal I with respect to a *LEX* term order allows one to efficiently find the solutions of I. To the extent of our knowledge, this is only proved under the assumption that I is radical. In this section, we prove that this also holds in the case when I is not radical.

Most authors use the Shape Lemma (cf. [KR00, Theorem 3.7.25]) to justify the claim that one can easily compute the solutions of I from a lexicographic Gröbner basis of it. The Shape Lemma however requires that the ideal I is radical and in normal x_n-position. Being in normal x_n-position means that any two distinct zeros $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \bar{k}$ satisfy $a_n \neq b_n$. Notice that every zero-dimensional ideal I 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]).

On the other hand, the radicality hypothesis is not always fulfilled. Some authors say that one may assume without loss of generality that the ideal is radical up to adding the field equations, since $I + (x_1^q - x_1, \dots, x_n^q - x_n) \subset \mathbb{F}_q[x_1, \dots, x_n]$ is radical for any I. As we already observed however, adding the field equations to I is not always computationally feasible, even if one restricts to systems coming from cryptography. One 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.

One can also find examples of polynomial systems coming from cryptosystems, whose lexicographic Gröbner basis does not have the shape predicted by the Shape Lemma. For example, all the instances that we computed of the ABC and cubic simple matrix cryptosystems (see [TDTD13, TXPD15]) give rise to ideals that are not radical. Notice that the field sizes proposed in [DPW14, TXPD15] for achieving 80-bits security are 2^8, 2^{16}, and 2^{32}, which are too large in order to add the field equations to the polynomial system. Therefore, being able to deal with the situation when the ideal I is not radical is relevant for cryptographic applications.

Example 2.1. We consider $R = \mathbb{F}_2[x_1, x_2, x_3, x_4]$ with the *LEX* term order $(x_1 > x_2 > x_3 > x_4)$ and the ideal I coming from a toy instance of an ABC cryptosystem (cf. [TDTD13, TXPD15]) with

$$A = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}, \; B = \begin{pmatrix} x_1 + x_2 + x_3 + x_4 & x_1 + x_2 + x_4 \\ x_3 & x_1 + x_2 + x_4 \end{pmatrix}, \; C = \begin{pmatrix} x_4 & x_3 + x_4 \\ x_1 + x_4 & 0 \end{pmatrix}.$$

The ideal I is generated by the polynomials of degree 2 which are the entries of the matrices AB and AC. It is a homogeneous non-radical ideal of R. A computation with MAGMA shows that the reduced lexicographic Gröbner basis of I does not have the form of the Shape Lemma, namely it is

$$\begin{aligned}
&p_{4,1} = x_4^3,\\
&p_{3,1} = x_3x_4^2,\ p_{3,2} = x_3^2 + x_3x_4,\\
&p_{2,1} = x_2x_4 + x_3x_4,\ p_{2,2} = x_2x_3 + x_4^2,\ p_{2,3} = x_2^2 + x_4^2,\\
&p_{1,1} = x_1x_4 + x_3x_4 + x_4^2,\ p_{1,2} = x_1x_3 + x_3x_4 + x_4^2,\ p_{1,3} = x_1x_2 + x_4^2,\ p_{1,4} = x_1^2.
\end{aligned}$$

In order to show how one can efficiently compute the solutions of a polynomial system from its lexicographic Gröbner basis, we will use the next result. We refer to [CLO07, Chapter 3, Theorem 2] and the following discussion for a proof.

Proposition 2.2. *Let I be a zero-dimensional inhomogeneous ideal of $R = k[x_1, \dots, x_n]$ and let $\mathcal{G}$ be the reduced Gröbner basis of I with respect to LEX with $x_1 > x_2 > \cdots > x_n$. Then $\mathcal{G}$ consists of polynomials of the form:*

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

where $p_{i,t_j} \in k[x_i, \dots, x_n]$ for every $i \in \{1, \dots, n\}$, $j \in \{1, \dots, t_i\}$ and $t_1, \dots, t_{n-1} \geq 1$.

Notice that Proposition 2.2 alone does not substitute the Shape Lemma. In fact, one can compute the solutions of $p_{n,1}(x_n) = 0$, but Proposition 2.2 does not guarantee that one of the polynomials $p_{n-1,1}(x_{n-1}, a), \dots, p_{n-1,t_{n-1}}(x_{n-1}, a)$ is not identically zero, where a is a root of $p_{n,1}$. Therefore, one is not sure that the reduced LEX Gröbner basis will produce a polynomial in x_{n-1} only, when evaluated at $x_n = a$. In this section, we prove that this is generically the case and use this result to build an algorithm which computes all the solutions of a zero-dimensional ideal I from its lexicographic Gröbner basis.

In the sequel, we fix the *LEX* term order with $x_1 > \cdots > x_n$ on $R = k[x_1, \dots, x_n]$, and the induced *LEX* term order with $x_1 > \cdots > x_{n-1}$ on $k[x_1, \dots, x_{n-1}]$.

Lemma 2.3. *Assume that k is infinite. Fix the LEX term order with $x_1 > \cdots > x_n$ on R, and the induced LEX term order with $x_1 > \cdots > x_{n-1}$ on $k[x_1, \dots, x_{n-1}]$. Let $f \in R$, then*

$$(\mathrm{in}_{\leq} f)(x_1, \dots, x_{n-1}, a) = \mathrm{in}_{\leq}(f(x_1, \dots, x_{n-1}, a))$$

for a generic $a \in k$.

Proof. We have $x_1^{\alpha_1} \cdots x_n^{\alpha_n} >_{LEX} x_1^{\beta_1} \cdots x_n^{\beta_n}$ if and only if $x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} >_{LEX} x_1^{\beta_1} \cdots x_{n-1}^{\beta_{n-1}}$ OR $x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} = x_1^{\beta_1} \cdots x_{n-1}^{\beta_{n-1}}$ and $\alpha_n > \beta_n$. So for $m = \mathrm{in}(f)$ we have $m(x_1, \dots, x_{n-1}, a) \geq \ell(x_1, \dots, x_{n-1}, a)$ for every ℓ in the support of f. Hence, as long as $m(x_1, \dots, x_{n-1}, a)$ belongs to the support of $f(x_1, \dots, x_{n-1}, a)$ (i.e. if it does not cancel with other terms when we put $x_n = a$), then $m(x_1, \dots, x_{n-1}, a) = \mathrm{in}(f(x_1, \dots, x_{n-1}, a))$. Since the previous condition is verified for a generic a, the claim follows. □

Remark 2.4. The conclusion of Lemma 2.3 also holds for any fixed $a \in k$, under the assumption that $f \in R$ is generic.

Example 2.5. Notice that there may be more than one monomial in f which specializes to $\mathrm{in}(f(x_1,\dots,x_{n-1},a))$ and not just $\mathrm{in}(f)$. For example consider $k[x_1,x_2,x_3]$ with $x_1 > x_2 > x_3$ and $f = \underline{x_1x_2x_3^2} - \underline{x_1x_2x_3} + \underline{x_1x_2} + x_2^2x_3 + x_3^5$. Then all three underlined monomials specialize to cx_1x_2 for some $c \in k$, which is the leading term of $f(x_1,x_2,a)$ for any a s.t. $a^2 - a + 1 \neq 0$.

In the next theorem, the ideal I is not necessarily zero-dimensional.

Theorem 2.6. *Assume that k is infinite. Let I be an ideal of R, and let $\mathcal{G}$ be a lexicographic Gröbner basis of I with respect to $x_1 > \cdots > x_n$. Then for a generic $a \in k$, $\mathcal{G}(a) = \{g(x_1,\dots,x_{n-1},a) : g \in \mathcal{G}\}$ is a lexicographic Gröbner basis of the ideal $I(a) = \{f(x_1,\dots,x_{n-1},a) : f \in I\}$ with respect to $x_1 > \cdots > x_{n-1}$.*

Proof. Let $\mathcal{G}'$ be a lexicographic Gröbner basis of $I(a)$ with respect to $x_1 > \cdots > x_{n-1}$. Let $\mathcal{H}$ be a set of elements of I which specializes to $\mathcal{G}'$, i.e. $\mathcal{H}(a) = \mathcal{G}'$. Then by construction $\mathcal{G} \cup \mathcal{H}$ is a lexicographic Gröbner basis of I, and $\mathcal{G}(a) \cup \mathcal{G}'$ is a lexicographic Gröbner basis of $I(a)$. Hence, we obtain

$$\begin{aligned}(\mathrm{in}(I))(a) &= \Big(\mathrm{in}(f)(x_1,\dots,x_{n-1},a) : f \in \mathcal{G} \cup \mathcal{H}\Big)\\ &= \Big(\mathrm{in}(f(x_1,\dots,x_{n-1},a)) : f \in \mathcal{G} \cup \mathcal{H}\Big)\\ &= \Big(\mathrm{in}(p) : p \in \mathcal{G}(a) \cup \mathcal{G}'\Big)\\ &= \mathrm{in}(I(a)),\end{aligned}$$

where the second equality follows from Lemma 2.3 for a generic $a \in k$, since both $\mathcal{G}$ and $\mathcal{H}$ may be chosen finite.

On the other hand, again by Lemma 2.3 we have $\mathrm{in}(I)(a) = \Big(\mathrm{in}(f)(x_1,\dots,x_{n-1},a) : f \in \mathcal{G}\Big) = \Big(\mathrm{in}(f(x_1,\dots,x_{n-1},a)) : f \in \mathcal{G}\Big) = \Big(\mathrm{in}(p) : p \in \mathcal{G}(a)\Big)$ for $a \in k$ generic. It follows that $\mathrm{in}(I(a)) = (\mathrm{in}(I))(a) = \Big(\mathrm{in}(p) : p \in \mathcal{G}(a)\Big)$, thus $\mathcal{G}(a)$ is a lexicographic Gröbner basis of $I(a)$. □

We can use Theorem 2.6 to write down a procedure which *generically* allows us to compute the solutions of a zero-dimensional ideal I with just one Gröbner basis computation.

Corollary 2.7. *Let $I \subseteq R = k[x_1,\dots,x_n]$ be a zero-dimensional inhomogeneous ideal with zero locus $\mathcal{Z}(I) = \{P_1,\dots,P_d\}$. Then the solutions can be computed as follows:*

1. *Compute the reduced lexicographic Gröbner basis $\mathcal{G}$ of I with respect to $x_1 > \cdots > x_n$ to obtain the monic polynomial $g_n \in k[x_n]$ such that $(g_n) = I \cap k[x_n]$.*
2. *Factor g_n.*
3. *For every root α of g_n compute $\mathcal{G}(\alpha)$ and reduce it to find (generically!) the reduced lexicographic Gröbner basis of $I(\alpha)$.*
4. *This Gröbner basis contains a polynomial $g_{n-1} \in k[x_{n-1}]$ such that $(g_{n-1}) = I(\alpha) \cap k[x_{n-1}]$.*
5. *Factor g_{n-1}. For every root β of g_{n-1} compute $\mathcal{G}(\alpha)(\beta)$.*
6. *Proceed as before until $P_1,\dots,P_d$ are found.*

We stress that we are not suggesting to compute the reduced LEX Gröbner basis directly. As we already mentioned, computing a DRL Gröbner basis of I then converting it to a LEX Gröbner basis using FGLM or a similar algorithm is usually more efficient than computing a LEX Gröbner basis directly.

The computation may be further improved under the assumption that the ideal I has only one zero over the algebraic closure, namely $\mathcal{Z}(I) = \{P \in \bar{k}^n : f(P) = 0 \text{ for all } f \in I\} = \{(a_1,\dots,a_n)\}$. This is often the case for a polynomial system coming from a cryptographic scheme, where we usually require that for each ciphertext y there is a unique plaintext x such that $p_i(x) = y$ for every $i = 1,\dots m$. For example, we tested this assumption on several instances of the ABC cryptosystem and found that it was almost always satisfied.

Corollary 2.8. *Let $I \subseteq R = k[x_1, \ldots, x_n]$ be a zero-dimensional inhomogeneous ideal which admits only one solution in $\bar{k}^n$, i.e. $\mathcal{Z}(I) = \{(a_1, \ldots, a_n)\}$. Then the solution can be computed as follows:*

(1) Compute the reduced lexicographic Gröbner basis $\mathcal{G}$ of I with respect to $x_1 > \cdots > x_n$ to obtain the monic polynomial $g_n \in k[x_n]$ such that $(g_n) = I \cap k[x_n]$.
(2) g_n is of the form $g_n(x_n) = (x_n - a_n)^d$. Compute a_n from it.
(3) Compute $\mathcal{G}(a_n)$ and reduce it to find (generically!) the reduced lexicographic Gröbner basis of $I(a_n)$.
(4) This Gröbner basis contains a polynomial $g_{n-1} \in k[x_{n-1}]$ such that $(g_{n-1}) = I(a_n) \cap k[x_{n-1}] = I \cap k[x_{n-1}]$.
(5) Compute the only root a_{n-1} of g_{n-1}, compute $\mathcal{G}(a_n)(a_{n-1})$.
(6) Proceed until $(a_1, \ldots, a_n)$ is found.

As for Corollary 2.7, the previous procedure *generically* allows us to compute the solution $(a_1, \ldots, a_n)$ of the system with just one Gröbner basis computation.

Remark 2.9. 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.

We conclude the section with a result that shows that finding a lexicographic Gröbner basis of a zero-dimensional radical ideal over a finite field is essentially equivalent to solving the corresponding polynomial system.

Theorem 2.10. *Let k be a finite field and let $f_1, \ldots, f_r \in R = k[x_1, \ldots, x_n]$ be inhomogeneous polynomials such that the corresponding ideal $I = (f_1, \ldots, f_r)$ is zero-dimensional, radical, in normal x_n-position, and its zero locus $\mathcal{Z}(I)$ is contained in k^n. Then, computing a lexicographic Gröbner basis of I is polynomial time equivalent to solving the system $f_1 = \cdots = f_r = 0$.*

Proof. If we know a lexicographic Gröbner basis of I, then we can use the procedure of Corollary 2.7 to find the solutions of the corresponding system. Notice that the only operation required, apart from the arithmetic over the field, is factoring univariate polynomials, which can be done in polynomial time over a finite field.

Viceversa, assume that the system $f_1 = \cdots = f_r = 0$ has the solutions $P_1, \ldots, P_d \in k^n$ with $P_i = (a_{i,1}, \ldots, a_{i,n})$ for $i = 1, \ldots, d$. Then, by the Shape Lemma we know that the reduced lexicographic Gröbner basis of I will have the following form:

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

where $g_i(x_n)$ are polynomials in the variable x_n only, and the lexicographic order is intended with x_n as smallest variable. Now, since the roots of g_n are exactly $a_{1,n}, \ldots, a_{d,n}$ we can compute $g_n(x_n) = \prod_{i=1}^d (x_n - a_{i,n})$. Similarly, for each $j \in \{1, \ldots, n-1\}$ we know that if x_n is replaced by a root of $g_n(x_n)$ then the roots of $x_j - g_j(x_n)$ are $a_{1,j}, \ldots, a_{d,j}$. Therefore, we can compute $g_j(x_n)$ by using interpolation with Lagrange polynomials

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

□

3. Solving degree of inhomogeneous ideals

In this section we discuss the complexity of computing a Gröbner basis of an ideal I in a polynomial ring $R = k[x_1, \dots, x_n]$ over a field k. In practice one observes that computing a Gröbner basis with respect to *DRL* is usually faster than with respect to any other term order. On the other side, computing a Gröbner basis with respect to *LEX* is usually slower than with respect to any other term order. For this reason, we focus on *DRL*. However, we state our results in greater generality whenever possible.

We have two main classes of algorithms for computing a Gröbner basis: Buchberger's Algorithm and its improvements, and algorithms which transform the problem of computing a Gröbner basis into several instances of Gaussian elimination, such as F_4 [Fau99], F_5 [Fau02], the *XL* Algorithm [CKPS00], and MutantXL [DBMMW08]. Buchberger's Algorithm is older, and its computational complexity has been extensively studied. The other class of algorithms is often faster in practice, and has contributed to breaking many cryptographic challenges. However, their computational complexity is less understood, especially when the input is given by inhomogeneous polynomials. In this section we focus on the second family of algorithms.

The computational complexity of the above algorithms is dominated by Gaussian elimination on the *Macaulay matrices*. First we describe them for homogeneous ideals, following [BFS14, p. 54].

Let $\{f_1, \dots, f_r\}$ be a system of homogeneous polynomials, defining an ideal I in the polynomial ring R. We fix a term order on R. For any degree $d \in \mathbb{Z}_+$, denote by R_d the d-th homogeneous component of R. The *Macaulay matrix* $\widetilde{M}_d$ of I has columns indexed by the terms of R_d sorted, from left to right, by decreasing monomial order. The rows of $\widetilde{M}_d$ are indexed by the polynomials $m_{i,j}f_j$, where $m_{i,j}$ is a term in R such that $\deg m_{i,j}f_j = d$. Then the entry (r, s) of $\widetilde{M}_d$ is the coefficient of the monomial of the column s in the polynomial corresponding to the r-th row.

When the polynomials $f_1, \dots, f_r$ are not homogeneous, let I be the ideal that they generate. For any degree $d \in \mathbb{Z}_+$ the *(inhomogeneous) Macaulay matrix* M_d of I has columns indexed by the terms of R of degree $\leq d$ sorted, from left to right, by decreasing monomial order. The rows of M_d are indexed by 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_d are defined as in the homogeneous case.

Typically, the algorithms perform Gaussian elimination on the Macaulay matrix for increasing values of d, until a Gröbner basis is found. The size of the Macaulay matrices M_d and $\widetilde{M}_d$, hence the computational complexity of computing their reduced row echelon form, is determined by the degree d. Therefore, following [DS13] we introduce the next definition.

Definition 3.1. Let $I \subseteq R$ be an ideal and let τ be a term order on R, the *solving degree* of I is the highest degree of the polynomials involved in the computation of a τ Gröbner basis of I. We denote it by $\operatorname{solv.deg}_\tau(I)$. When the term order is clear from the context, we omit the subscript τ.

Remark 3.2. Notice that, if I is not homogeneous, then a row r that corresponds to a polynomial of degree $e < d$ may be produced while doing Gaussian elimination on M_d. If this is the case, then some variants of the algorithms add to M_d the rows mr where m runs over the monomials of $\deg(m) \leq d - e$ and proceed to compute the reduced row echelon form of this larger matrix. This may have the effect of reducing the solving degree with respect to a given ideal and term order. Therefore the solving degree also depends on the version of the algorithm adopted. Throughout the paper, we consider the situation when the extra rows are inserted, since this approach is usually the most efficient.

Notice also that, if I is homogeneous, then the solving degree is the smallest degree such that Gaussian elimination on $\widetilde{M}_d$ yields a Gröbner basis of I with respect to the chosen term order.

The solving degree of I is strongly related to the largest degree of a polynomial appearing in the Gröbner basis.

Definition 3.3. Let $I \subseteq R$ be an ideal and let τ be a term order on R. We denote by $\max.\mathrm{GB}.\deg_\tau(I)$ the maximum degree of a polynomial appearing in the reduced τ Gröbner basis of I.

It is clear that

$$\max.\mathrm{GB}.\deg_\tau(I) \leq \mathrm{solv}.\deg_\tau(I),$$

for any ideal I and any term order τ. Equality does not hold in general, as we show in Example 3.16.

Remark 3.4. If I is a homogeneous ideal, then $\max.\mathrm{GB}.\deg_\tau(I) = \mathrm{solv}.\deg_\tau(I)$ for any τ. In fact, all the polynomials that we obtain during the computation of a Gröbner basis are homogeneous. In particular, any nonzero linear combination of polynomials of degree $d > 0$ has also degree d.

If the ideal I is not homogeneous, it is natural to associate a homogeneous ideal to I. We do this in the next subsection.

3.1. **Homogenization of ideals and extensions of term order.** We now find relations between the Gröbner bases of I, $\tilde{I}$, and I^h.

Definition 3.5. Let σ be a term order on R, and let τ be a term order on $S = R[t]$. We say that τ *ϕ-extends* σ, or that τ is a *ϕ-extension* of σ, if $\phi(\mathrm{in}_\tau(f)) = \mathrm{in}_\sigma(\phi(f))$ for every $f \in S$ homogeneous.

Theorem 3.6. *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) $\mathrm{in}_\sigma(I) = \phi(\mathrm{in}_\tau(J))$;
(2) if $\{g_1, \dots, g_s\}$ is a homogeneous τ Gröbner basis of J, then $\{\phi(g_1), \dots, \phi(g_s)\}$ is a σ Gröbner basis of I.

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

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

To conclude, 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 $f_1, \dots, f_r$ 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

$$\phi(\mathrm{in}_\tau(J)) = \big(\phi(\mathrm{in}_\tau(g_i)) : i = 1, \dots, s\big) = \big(\mathrm{in}_\sigma(\phi(g_i))\ i = 1, \dots, s\big),$$

since ϕ is a homomorphism and τ ϕ-extends σ. This shows that $\{\phi(g_1), \dots, \phi(g_s)\}$ is a Gröbner basis of $\phi(\mathrm{in}_\tau(J))$ with respect to σ, which is equal to $\mathrm{in}_\sigma(I)$ 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 3.7. Let m, n be terms in R, we say that $t^\alpha m >_{\bar{\sigma}} t^\beta n$ if and only if $(m >_\sigma n)$ OR $(m = n$ and $\alpha > \beta)$.

Lemma 3.8. *$\bar{\sigma}$ 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 $1 <_{\bar{\sigma}} t$, since $0 < 1$.

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 $i = 1, \dots, n$ 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 $i = 1, \dots, n$, 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 $a_i \in k^*$. 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 $i = 2, \dots, d$. 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 3.9. The equality $\phi(\mathrm{in}_{\bar{\sigma}}(f)) = \mathrm{in}_\sigma(\phi(f))$ is not necessarily true if f is not homogeneous. For example consider $f = tx - x + ty \in S = k[x, y, t]$, and let $\sigma = LEX$ with $x > y$. Then $\mathrm{in}_{\bar{\sigma}}(f) = tx$, $\phi(f) = y$, and $\mathrm{in}_\sigma(\phi(f)) = y \neq x = \phi(\mathrm{in}_{\bar{\sigma}}(f))$.

Another important example of ϕ-extension of a term order is the following.

Example 3.10. Fix a *DRL* order on R and consider the *DRL* order on S with t the smallest variable. In other words, for m, n terms in R we have $t^\alpha m >_{DRL} t^\beta n$ if and only if ($\deg m + \alpha > \deg n + \beta$) OR ($\deg m + \alpha = \deg n + \beta$ and $\alpha < \beta$) OR ($\deg m + \alpha = \deg n + \beta$ and $\alpha = \beta$ and $m >_{DRL} n$).

Lemma 3.11. *Fix a DRL order on R and extend it to a 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 $m_i \in R$ distinct terms, $\alpha_i \in \mathbb{N}$, and $a_i \in k^*$. 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 3.8 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 $i = 2, \dots, d$. For each $i \in \{2, \dots, d\}$ 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 3.12. Fix a *DRL* order on R. The *DRL* order on S defined in Example 3.10 is different from the order $\overline{DRL}$ obtained by applying Definition 3.7. For example, let $R = k[x, y]$ with $x > y$, $S = R[t]$, and consider the monomials $t^3 x$ and ty^2. We have $t^3 x <_{\overline{DRL}} ty^2$ 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.

3.2. **Solving degree of I and solving degree of $\tilde{I}$.**

Let $R = k[x_1, \dots, x_n]$ with the *DRL* order and let $S = R[t]$ with the *DRL* order with t as smallest variable, as defined in Example 3.10. Let $I \subseteq R$ be an inhomogeneous ideal. Let I^h be the homogenization of I with respect to t and let $\tilde{I} = (f_1^h, \dots, f_r^h) \subseteq S$ be the ideal obtained by homogenizing the generators $f_1, \dots, f_r$ of I with respect to t. The goal of this section is comparing the solving degree of I, $\tilde{I}$, and I^h with respect to the chosen term orders.

We start with a preliminary result on Gröbner bases and homogenization.

Proposition 3.13. *Let $R = k[x_1, \ldots, x_n]$ and let $S = R[t]$. Fix a DRL term order on R and extend it to a 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 positive 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 positive power of t will appear 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 results allow us to compare the solving degrees of I and $\tilde{I}$. It also clarifies why for an inhomogeneous ideal the largest degree in an element in a reduced Gröbner basis may be smaller than the solving degree of the ideal.

Theorem 3.14. *Let $I = (f_1, \ldots, f_r) \subseteq R = k[x_1, \ldots, x_n]$. Let I^h be the homogenization of I with respect to t and let $\tilde{I} = (f_1^h, \ldots, f_r^h) \subseteq S = k[x_1, \ldots, x_n, t]$ be the ideal obtained by homogenizing the generators $f_1, \ldots, f_r$ of I with respect to t. Consider the term order DRL on R and S, with t as smallest variable. Then*

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

Proof. We claim that the Macaulay matrix M_d of I with respect to *DRL* is equal to the Macaulay matrix $\widetilde{M}_d$ of $\tilde{I}$ 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 $\widetilde{M}_d$, 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_d. Conversely, every index $m_{i,j} f_j^h$ of a row of $\widetilde{M}_d$, can be obtained from an index of a row of M_d by homogenizing and multiplying by an appropriate power of t. In a nutshell, the statement on the columns follows from the fact that $I_{\leq d} = \phi(\tilde{I}_d)$.

The only thing that needs to be checked is that the order on the columns of $\widetilde{M}_d$ and M_d is the same. We consider M_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 $j \in \{1, \ldots, d\}$ are then ordered following *DRL* on the variables $x_1, \ldots, x_n$. Similarly, since t is the smallest variable in the *DRL* order on S, the columns of $\widetilde{M}_d$ 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 $x_1, \ldots, x_n$. Then, the columns with the same power of t are ordered following *DRL* on the variables $x_1, \ldots, x_n$. This proves that the matrices M_d and $\widetilde{M}_d$ coincide.

The inequality $\mathrm{solv.deg}_{DRL}(I) \leq \mathrm{solv.deg}_{DRL}(\tilde{I})$ now follows from Remark 3.2, where we observed that in the inhomogeneous case the algorithm may terminate in lower degree. The equalities $\mathrm{max.GB.deg}(\tilde{I}) = \mathrm{solv.deg}(\tilde{I})$ and $\mathrm{max.GB.deg}(I^h) = \mathrm{solv.deg}(I^h)$ follow from Remark 3.4, since the ideals are homogeneous. Finally, the equality $\mathrm{max.GB.deg}(I) = \mathrm{max.GB.deg}(I^h)$ follows from the following two facts:

- By Lemma 3.11 and Theorem 3.6 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 3.13

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. □

Remark 3.15. Notice that the strategy of adding extra rows when a degree drop occurs during Gaussian elimination mentioned in Remark 3.2 essentially corresponds to anticipating a part of the computation that would take place in the following degrees. This makes the algorithm terminate earlier, if the polynomials in the Gröbner basis that should have been produced in a larger degree happen to be exactly those whose computation is anticipated to an earlier degree. Unfortunately, it is in general unclear when this may be the case. E.g., in all the examples that we computed for this paper we found $\mathrm{solv.deg}_{DRL}(I) = \mathrm{solv.deg}_{DRL}(\tilde{I})$.

We observed in Remark 3.4 that the inequality $\mathrm{solv.deg}(I) \geq \mathrm{max.GB.deg}(I)$ becomes an equality if I is homogeneous. However it may be strict in general, as the following example shows. See also Example 4.7 for a cryptographic example.

Example 3.16. Let $R = k[x, y]$ with DRL term order $x > y$, and let $S = R[t]$ with DRL term order $x > y > t$. We consider the ideal $I = (f_1, f_2) \subseteq R$ with $f_1 = x^2 - 1$, and $f_2 = xy + x$. Then, we have $\tilde{I} = (f_1^h, f_2^h) = (x^2 - t^2, xy + xt)$, and $I^h = (x^2 - t^2, y + t)$. Writing the Macaulay matrices of I, $\tilde{I}$, and I^h and doing Gaussian elimination one sees that $\mathrm{solv.deg}(I) = \mathrm{solv.deg}(\tilde{I}) = 3$, but $\mathrm{solv.deg}(I^h) = 2$. By computing Gröbner bases, one can also check that $\mathrm{max.GB.deg}(\tilde{I}) = 3$ and $\mathrm{max.GB.deg}(I) = \mathrm{max.GB.deg}(I^h) = 2$.

3.3. **Solving degree and Castelnuovo-Mumford regularity.** In this section, we link the solving degree of a homogeneous ideal with a classic 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 denote by R_j the k-vector space of homogeneous elements of R of degree j. We 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 the following shifts on the polynomial ring 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 $R(1)$.

We consider the map

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

defined as before. With this shifted grading on the domain, the map φ 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 $d_{i,j} \in \mathbb{Z}$. The numbers β_i are the *(global) Betti numbers* of I and denoted by $\beta_i(I)$, and the number $\operatorname{pd}(I) = p$ is the projective dimension of I. Hilbert's Syzygy Theorem tells us that $\operatorname{pd}(I) \leq n$.

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 $\beta_{i,j}$ are called *(graded) Betti numbers* of I and denoted by $\beta_{i,j}(I)$.

Definition 3.17 (Castelnuovo-Mumford regularity)**.** The *Castelnuovo-Mumford regularity* of I is

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

Example 3.18. 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 $\operatorname{reg}(I) = 3$.

The Castelnuovo-Mumford regularity is an invariant of an ideal which gives a measure of how complicated that ideal is in terms of its minimal free resolution. It has been studied (although not precisely defined) by Castelnuovo, when he studied what is now called Castelnuovo's base-point free pencil trick. A rigorous definition was given by Mumford for sheaves, and by Kleiman for ideals and modules.

There are other equivalent definitions of Castelnuovo-Mumford regularity in commutative algebra, using for example local cohomology or Ext modules. To read more on regularity and its properties the interested reader may consult the book of Eisenbud [Eis94, Chapter 20] or the survey paper of Chardin [Cha07]. In the sequel we only mention the properties and facts that are relevant for our purposes.

Remark 3.19. In the references we gave and in many texts in commutative algebra or algebraic geometry, it is often assumed that the field k is algebraically closed or infinite. However, the definition of regularity makes perfect sense over a finite field as well. 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 $\operatorname{reg}_R(I) = \operatorname{reg}_S(J)$.

In the next theorem, we collect two results due to Bayer and Stillman, and Chardin, respectively. They relate the regularity of a homogeneous ideal to the regularity of its *DRL* initial ideal, under some assumptions. Combined with our Theorem 3.14, they will allow us to bound the solving degree of inhomogeneous ideals.

Theorem 3.20 ([BS87], Theorem 2.4 and Proposition 2.9, [Cha03])**.** *Let k be an infinite field, and let $J \subseteq k[x_1, \ldots, x_n]$ be a homogeneous ideal. Assume that J is either zero-dimensional or in generic coordinates over $\overline{k}$, then*

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

Remark 3.21. If k has characteristic zero and J is a homogeneous ideal in generic coordinates, then $\operatorname{reg}(\operatorname{in}_{DRL}(J))$ is equal to the largest degree of a minimal generator of $\operatorname{in}_{DRL}(J)$ as shown in [BS87]. In positive characteristic, one still has that the degree of the minimal generators of $\operatorname{in}_{DRL}(J)$ is upper bounded by $\operatorname{reg}(\operatorname{in}_{DRL}(J))$. However, the bound is often met even in positive characteristic, i.e. it is often the case that $\operatorname{in}_{DRL}(J)$ has a minimal generator of degree $\operatorname{reg}(\operatorname{in}_{DRL}(J))$. In fact this is the case in all the examples that we compute in this paper. Nevertheless, there are examples of ideals J for which $\operatorname{in}_{DRL}(J)$ has no minimal generator of degree $\operatorname{reg}(\operatorname{in}_{DRL}(J))$. E.g., $J = (x^p, y^p) \subseteq \mathbb{F}_p[x, y]$ has $\operatorname{in}_{DRL}(J) = J$ and $\operatorname{reg}(J) = 2p - 1$.

Combining Theorem 3.14 and Theorem 3.20, one obtains bounds on the solving degree. For the sake of clarity, we give a homogeneous and an inhomogeneous version of the result. Since the proofs are very similar, we only give the proof in the inhomogeneous case.

Theorem 3.22. *Let $I \subseteq k[x_1, \ldots, x_n]$ be a homogeneous ideal and assume that I is either zero-dimensional or in generic coordinates over $\overline{k}$. Then*

$$\operatorname{solv.deg}_{DRL}(I) \leq \operatorname{reg}(I).$$

The following is the main result of this paper. It allows us to bound the complexity of computing a Gröbner basis of a system of inhomogeneous equations by establishing a connection with the Castelnuovo-Mumford regularity of a suitable ideal.

Theorem 3.23. *Let $I = (f_1, \ldots, f_r) \subseteq R = k[x_1, \ldots, x_n]$ be an inhomogeneous ideal. Let $\tilde{I} = (f_1^h, \ldots, f_r^h) \subseteq S = R[t]$ and assume that $\tilde{I}$ is either zero-dimensional or in generic coordinates over $\overline{k}$. Then*

$$\operatorname{solv.deg}_{DRL}(I) \leq \operatorname{reg}(\tilde{I}).$$

Proof. For any 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.

We have the chain of equalities and inequalities

$$\operatorname{solv.deg}_{DRL}(I) \leq \operatorname{solv.deg}_{DRL}(\tilde{I}) = \operatorname{max.GB.deg}_{DRL}(\tilde{I}) \leq \operatorname{reg}(\operatorname{in}_{DRL}(\tilde{I})) = \operatorname{reg}(\tilde{I})$$

where the first inequality follows from Theorem 3.14 and the first equality from Remark 3.4. The last equality follows from Theorem 3.20. □

Remark 3.24. The upper bound in Theorem 3.23 is often an equality, since generically $\operatorname{solv.deg}_{DRL}(I) = \operatorname{solv.deg}_{DRL}(\tilde{I})$ as already observed in Remark 3.15. Moreover, we have $\operatorname{max.GB.deg}_{DRL}(\tilde{I}) = \operatorname{reg}(\operatorname{in}_{DRL}(\tilde{I}))$ if k has characteristic zero and often even in positive characteristic as observed in Remark 3.21.

Remark 3.25. Theorem 3.22 and Theorem 3.23 assume that the ideal is either in generic coordinates or zero-dimensional. Notice that both assumptions are likely to be satisfied for systems of equations coming from cryptographic systems. More precisely, the assumption that the ideal is in generic coordinates is usually satisfied for multivariate cryptosystems, since they 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. In addition, most systems of equations coming from cryptography are overdetermined, i.e. the number of polynomials r is greater than the number of variables n. Therefore, under a *genericity* assumption, the corresponding ideal is zero-dimensional.

By combining Theorem 3.23 and classical results on the Castelnuovo-Mumford regularity (see e.g. [CP99, Theorem A]), one immediately obtains the following bound on the solving degree of zero-dimensional ideals, which is linear in both the number of variables and the degree of the minimal generators of the ideal.

Corollary 3.26. *[Macaulay bound] Let k be a field, and let $I = (f_1, \dots, f_r)$ be an ideal of $k[x_1, \dots, x_n]$ with $d_i = \deg f_i$. Assume that $\tilde{I} = (f_1^h, \dots, f_r^h)$ is zero-dimensional, then*

$$\text{solv.}\deg_{DRL}(I) \leq d_1 + \dots + d_r - r + 1$$

and equality holds if $f_1, \dots, f_r$ are a regular sequence. In particular, if $d = \max\{d_1, \dots, d_r\}$ then

$$\text{solv.}\deg_{DRL}(I) \leq (n+1)(d-1) + 1.$$

Notice that the Macaulay bound was shown by Lazard in [Laz83] for the maximum degree of an element of a reduced Gröbner basis of I. Our result is in fact slightly stronger, since we prove the same inequality for the solving degree, which may be strictly larger.

We may use this result to obtain bounds on the solving degree of the ABC and cubic simple matrix encryption schemes. We assume that the systems are zero-dimensional, which was the case for all the instances of the ABC cryptosystem and cubic simple matrix encryption scheme that we computed.

Example 3.27 (ABC cryptosystem [TDTD13, TXPD15])**.** The system associated to the ABC cryptosystems consists of $2n$ quadratic equations in n variables and

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

Example 3.28 (Cubic simple matrix encryption scheme [DPW14])**.** The system associated to the cubic simple matrix encryption scheme consists of $2n$ cubic equations in n variables and

$$\text{solv.}\deg(I) \leq 2n + 3.$$

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. The goal of this section is explaining how the degree of regularity is related with the Castelnuovo-Mumford regularity and the solving degree introduced in the previous sections.

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 Faugère et al. [Bar04, BFS04, BFS14];
(2) the degree of regularity by Ding et al. [DS13, DY13].

We briefly recall both definitions, and compare them with the Castelnuovo-Mumford regularity.

4.1. **The degree of regularity by Faugère.** To the best of our knowledge, the degree of regularity appeared first in a paper by Bardet, Faugère, and Salvy in [BFS04], and in Bardet's Ph.D. thesis [Bar04]. However, the idea of measuring the complexity of a polynomial system with the index of regularity of the corresponding ideal can be traced back to Lazard's seminal work [Laz83]. The definition of degree of regularity was given first for homogeneous polynomial systems, and then extended to inhomogeneous polynomials. Before giving the definition, we recall some concepts from commutative algebra.

Let $R = k[x_1, \dots, x_n]$ be a polynomial ring over a field k, let I be a homogeneous ideal of R, and let $A = R/I$. For a natural number d, we denote by A_d the homogeneous part of degree d of A, where we fix $A_d = 0$ for any negative integer d. The function $HF_A(-) : \mathbb{Z} \to \mathbb{N}$, $HF_A(d) = \dim_k A_d$ 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 4.1. The *index of regularity* of I is the smallest integer $i_{\text{reg}}(I)$ such that $HF_A(d) = HP_A(d)$ for all $d \geq i_{\text{reg}}(I)$.

The index of regularity can be read off the Hilbert series of the ideal, as shown in the following theorem (cf. [BH98, Proposition 4.1.12]).

Theorem 4.2. *Let $I \subseteq R$ be a homogeneous ideal with Hilbert series as in* (3) *and let $\delta = \deg h_A$. Then $i_{\text{reg}}(I) = \delta - \ell + 1$.*

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

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

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

Definition 4.3 (degree of regularity by Faugère)**.** Let I be an ideal of R such that $I_d^{\text{top}} = R_d$ for $d \gg 0$. The *degree of regularity* of I is

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

If $f_1, \dots, f_r \in R$, then the degree of regularity of $f_1, \dots, f_r$ is the degree of regularity of the ideal $I = (f_1, \dots, f_r)$.

Remark 4.4. If $I_d^{\text{top}} = R_d$ for $d \gg 0$, then I is zero-dimensional. The converse, however, does not hold in general. See Example 4.8 for an example where I is zero-dimensional, but $I_d^{\text{top}} \neq R_d$ for all d.

The following is an easy consequence of the definitions.

Proposition 4.5. *Let I be an ideal of R such that $I_d^{\text{top}} = R_d$ for $d \gg 0$. Then*

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

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

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

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

For an inhomogeneous, zero-dimensional ideal I, we may interpret the condition $I_d^{\text{top}} = R_d$ 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 4.6. Let $\leq$ be a degree compatible term order and assume that $I_d^{\text{top}} = R_d$ for $d \gg 0$. In particular $HP_{R/I^{\text{top}}}(z) = 0$, hence $I_d^{\text{top}} = \text{in}_{\leq}(I^{\text{top}})_d = R_d$ for $d \geq d_{\text{reg}}^F(I)$. The inclusion $\text{in}_{\leq}(I^{\text{top}})_d \subseteq \text{in}_{\leq}(I)_d$ holds for any d, since $\leq$ is degree compatible. So we obtain $\text{in}_{\leq}(I)_d = R_d$ for $d \geq d_{\text{reg}}^F(I)$. This implies that every element of the reduced Gröbner basis of I has degree at most $d_{\text{reg}}^F(I)$, that is

$$\max.\text{GB}.\deg_{\leq}(I) \leq d_{\text{reg}}^F(I). \tag{5}$$

Notice however that (5) does not yield a bound on the solving degree of I, as we show in the next example.

Example 4.7. The polynomial systems obtained in [BG17] for collecting relations for index calculus following the approach outlined by Gaudry in [Gau09] for $n = 3$ consist of three inhomogeneous equations f_1, f_2, f_3 of degree 3 in two variables. Let $I = (f_1, f_2, f_3)$. For 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 $I_d^{\text{top}} = R_d$ for $d \gg 0$ and

$$\text{solv.}\deg_{DRL}(I) = \text{reg}(\tilde{I}) = 5 > 4 = d_{\text{reg}}^F(I) = i_{\text{reg}}(I^{\text{top}}).$$

The computations were performed by G. Bianco with MAGMA.

Notice moreover that there are inhomogeneous, zero-dimensional ideals I for which $I_d^{\text{top}} \neq R_d$ for all $d \geq 0$. Definition 4.3 and inequality (5) do not apply to such ideals. Unfortunately, this can happen also for polynomial systems coming from cryptographic problems. When this happens, one may be tempted to consider $i_{\text{reg}}(I^{\text{top}})$ anyway, and use it to bound the solving degree of I. Unfortunately this approach fails since $i_{\text{reg}}(I^{\text{top}})$ and $\text{solv.}\deg(I)$ might be far apart, as the next example shows. On the other side, the Castelnuovo-Mumford regularity of $\tilde{I}$ still allows us to correctly bound the solving degree of I.

Example 4.8. The polynomial systems obtained in [GM15] for collecting relations for index calculus following the approach outlined by Gaudry in [Gau09] for $n = 3$ consist of three inhomogeneous equations f_1, f_2, f_3 in two variables, of degrees 7,7,and 8. Let $I = (f_1, f_2, f_3)$. For 150'000 randomly generated examples of cryptographic size (as in Example 4.7) we found that $\text{solv.}\deg_{DRL}(I) = \text{reg}(\tilde{I}) = 15$, $I_d^{\text{top}} \neq R_d$ for all $d \geq 0$, and $i_{\text{reg}}(I^{\text{top}}) = 8$. The computations were performed by G. Bianco with MAGMA.

Finally, there is a simple relation between $I^{\text{top}} \subseteq R$ and $\tilde{I} \subseteq S$, namely

$$I^{\text{top}}S + (t) = \tilde{I} + (t). \tag{6}$$

Here $I^{\text{top}}S$ denotes the extension of I^{top} to S, i.e., the ideal of S generated by a system of generators of I^{top}. Since $I^{\text{top}} \subseteq R$, $t \nmid 0$ modulo $I^{\text{top}}S$. If $t \nmid 0$ modulo $\tilde{I}$, then $\tilde{I} = I^h$ is the homogenization of I and $\text{reg}(\tilde{I}) = \text{reg}(I^{\text{top}})$. Therefore, if $t \nmid 0$ modulo $\tilde{I}$ and $I_d^{\text{top}} = R_d$ for $d \gg 0$, then

$$d_{\text{reg}}^F(I) = \text{reg}(\tilde{I})$$

by Proposition 4.5. However, one expects that in most cases $t \mid 0$ modulo $\tilde{I}$. In fact, $\tilde{I} = I^h$ only in very special cases, namely when $f_1, \ldots, f_r$ are a Macaulay basis of I 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 $\tilde{I}$ and I^{top}.

4.2. **The degree of regularity by Ding.** 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, Yang, and Schmidt [DS13, DY13]. This degree of regularity can be read immediately from an instance of the algorithm F_4 which is implemented in MAGMA, as we explain in Remark 4.11. The definition we present here is taken from [DS13], and differs slightly from the original one of Dubois and Gama.

Let $\mathbb{F}_q$ be a finite field. We work in the graded quotient ring $B = \mathbb{F}_q[x_1, \dots, x_n]/(x_1^q, \dots, x_n^q)$. Let $f_1, \dots, f_r \in B$ be homogeneous polynomials of degree 2. We fix a B-module homomorphism φ sending the canonical basis $e_1, \dots, e_r$ of B^r to $\{f_1, \dots, f_r\}$, that is for every $(b_1, \dots, b_r) \in B^r$ we have $\varphi(b_1, \dots, b_r) = \sum_{i=1}^r b_i f_i$. We denote by $\mathrm{Syz}(f_1, \dots, f_r)$ the first syzygy module of $f_1, \dots, f_r$, that is the kernel of φ. An element of $\mathrm{Syz}(f_1, \dots, f_r)$ is called a *syzygy* of $f_1, \dots, f_r$. In other words, a syzygy of $f_1, \dots, f_r$ is a list of polynomials $(b_1, \dots, b_r) \in B^r$ 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 particular structure of $f_1, \dots, f_r$, but rather on the ring structure of B. We define the module $\mathrm{Triv}(f_1, \dots, f_r)$ of trivial syzygies of $f_1, \dots, f_r$ as the submodule of $\mathrm{Syz}(f_1, \dots, f_r)$ generated by $\{f_i e_j - f_j e_i : 1 \leq i < j \leq r\}$ and $\{f_i^{q-1} e_i : 1 \leq i \leq r\}$.

Following notations from the previous sections, if I is the ideal generated by $f_1, \dots, f_r$ we denote by $\mathrm{Syz}(I)$ and $\mathrm{Triv}(I)$ the modules of syzygies and trivial syzygies of $f_1, \dots, f_r$. For any $d \in \mathbb{N}$ we define the vector space $\mathrm{Syz}(I)_d = \mathrm{Syz}(I) \cap B_d^r$ of syzygies of degree d. Similarly, we define also the vector subspace of trivial syzygies of degree d $\mathrm{Triv}(I)_d = \mathrm{Triv}(I) \cap B_d^r$. Clearly, we have $\mathrm{Triv}(I)_d \subseteq \mathrm{Syz}(I)_d$.

Definition 4.9 (degree of regularity by Ding)**.** The *degree of regularity* of the homogeneous quadratic polynomials $f_1, \dots, f_r$ generating a homogeneous ideal I is

$$d_{\mathrm{reg}}^D(I) = \min\{d \in \mathbb{N} : \mathrm{Syz}(I)_{d-2}/\,\mathrm{Triv}(I)_{d-2} \neq 0\}.$$

Let $f_1, \dots, f_r \in B$ be inhomogeneous polynomials of degree 2 generating an inhomogeneous ideal I, then

$$d_{\mathrm{reg}}^D(I) = d_{\mathrm{reg}}^D(I^{\mathrm{top}}).$$

Remark 4.10. Dubois and Gama [DG10] work in the ring $\mathbb{F}_q[x_1, \dots, x_n](x_1^q - x_1, \dots, x_n^q - x_n)$ and not in $B = \mathbb{F}_q[x_1, \dots, x_n]/(x_1^q, \dots, x_n^q)$.

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

Ding and Schmidt [DS13] pointed out the following.

Remark 4.11. In the MAGMA implementation of F_4, the algorithm goes thorough different steps. At each step, a Gaussian elimination of a Macaulay matrix $\widetilde{M}_d$ with polynomials of a given degree d is performed. We call this degree d the *step degree*. In the first steps of the algorithm, the step degree is increasing. The degree of regularity is the first step degree at which the step degree does not increase. On the other hand, the solving degree is the highest step degree reached during the computation.

Many authors believe that the degree of regularity by Ding and the solving degree of a polynomial system of quadratic equations must be close. However, Ding and Schmidt showed that this is not always the case. In fact, it is easy to produce examples (the so-called degenerate systems) where 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].

Concerning the relation between the degree of regularity by Ding (Definition 4.9) and the degree of regularity by Faugère (Definition 4.3), we are not aware of any result in this direction. Despite the fact that they share the same name, we do not see a connection following immediately from their definitions. Anyway, 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 Section 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.

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 (at least) a nonzero n-tuple $\lambda = (\lambda_1, \ldots, \lambda_n) \in k^n$ such that

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

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.

The condition on the rank of (7) is equivalent to requiring that the minors of size $t \times t$ of the matrix with linear entries $M = \sum_{i=1}^{n} x_i M_i$ vanish. In particular, every solution of the MinRank Problem corresponds to a 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.

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 $1 \leq t \leq \min\{r, s\}$ compute the set of points in k^n at which the evaluation of M has rank at most $t-1$, that is 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 $I_t(M)$ for large classes of matrices.

Ideals of minors of a matrix with entries in a polynomial ring are called *determinantal ideals* and have been largely studied in commutative algebra and algebraic geometry. Using Theorem 3.22, we can take advantage of the literature on the regularity of determinantal ideals to give bounds on the solving degree of certain large classes of determinantal ideals. For simplicity, we focus on homogeneous determinantal ideals.

Definition 5.1. Let M be an $r \times s$ matrix with $r \leq s$, whose entries are elements of $R = k[x_1, \ldots, x_n]$. 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 determinantal ideals.

Theorem 5.2. *Let $M = (f_{ij})$ be an $r \times s$ homogeneous matrix with $r \leq s$, whose entries are elements of $R = k[x_1, \dots, x_n]$, $n \geq s - r + 1$. Assume that* $\operatorname{height} I_r(M) = s - r + 1$. *Then the solving degree of the corresponding MinRank Problem is*

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

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

Proof. The regularity of $I_r(M)$ 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 3.22. In particular, if $\deg(f_{i,j}) = 1$ for all i, j, then $\operatorname{solv.deg} I_r(M) \leq r$. Since $I_r(M)$ is generated in degree r, then $\operatorname{solv.deg} I_r(M) = r$. □

Notice that in particular 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 $d^F_{\mathrm{reg}}(I_r(M)) = \operatorname{reg}(I_r(M))$. Therefore, Theorem 5.2 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 all have the same degree.

Notice also that $\operatorname{solv.deg} I_r(M) = r$ implies that a Gröbner basis can be computed from the set of maximal minors via Gaussian elimination.

We now restrict to ideals of maximal minors of matrices of linear forms. The MinRank Problem associated to this class of matrices is 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 $I_r(M)$ is 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 $I_2(M)$.

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 $\{e_1, \dots, e_v\}$ of $\mathbb{Z}^v$. For $v = 1$, this is just the standard $\mathbb{Z}$-grading.

Definition 5.3. 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 $\deg f_{i,j} = e_j \in \mathbb{Z}^v$ for every i, j. We say that M is *row-graded* if $r \leq v$, and $f_{i,j} = 0$ or $\deg f_{i,j} = e_i \in \mathbb{Z}^v$ for every i, j.

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

Theorem 5.4. *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:*

- $\operatorname{solv.deg} I_r(M) = r$,
- $\operatorname{solv.deg} I_2(M) \leq s$ *in the column-graded case, and* $\operatorname{solv.deg} I_2(M) \leq r$ *in the row-graded case.*

Proof. It is shown in [CDG15, CDG16] 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 3.22. □

Acknowledgements

The authors are grateful to Albrecht Petzoldt for help with MAGMA computations, to Wouter Castryck for pointing out mistakes 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. The authors wish to thank the anonymous referees whose comments helped to improve this article. The work in this paper was made possible by funding from Armasuisse.

References

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

[BFS04] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, *On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations*, ICPPSS International Conference on Polynomial System Solving, 2004.

[BFS14] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, *On the complexity of the F_5 Gröbner basis algorithm*, J. Symbolic Comput., vol. 70, pp. 49–70, 2015.

[BS87] David Bayer, Michael Stillman, *A criterion for detecting m-regularity*, Invent. Math. vol. 87, n. 1, pp. 1–11, 1987.

[BG17] Giulia Bianco, Elisa Gorla, *Index calculus in trace-zero subgroups and generalized summation polynomials*, preprint 2018.

[BCP97] Wieb Bosma, John Cannon, Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., vol. 24, pp. 235–265, 1997.

[BH98] Winfried Bruns, Jürgen Herzog, *Cohen-Macaulay rings. Revised edition*, Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, 1998.

[BCG04] Nero Budur, Marta Casanellas, Elisa Gorla, *Hilbert functions of irreducible arithmetically Gorenstein schemes*, Journal of Algebra, vol. 272, n. 1, pp. 292–310, 2004.

[Cha03] Marc Chardin, *Bounds for Castelnuovo-Mumford Regularity in Terms of Degrees of Defining Equations*, Commutative Algebra, Singularities and Computer Algebra, NATO Science Series, vol. 115, pp. 67–73 Springer, 2003.

[Cha07] Marc Chardin, *Some results and questions on Castelnuovo-Mumford regularity*, Syzygies and Hilbert Functions. Lecture Notes in Pure and Appl. Math., vol. 254, pp. 1–40, 2007.

[CP99] Marc Chardin and Patrice Philippon, *Régularité et interpolation*, J. Algebraic Geom. vol. 8, no. 3, 471–481, 1999.

[CDG15] Aldo Conca, Emanuela De Negri, Elisa Gorla, *Universal Gröbner bases for maximal minors*, International Mathematics Research Notices, vol. 11, pp. 3245–3262, 2015.

[CDG16] Aldo Conca, Emanuela De Negri, Elisa Gorla, *Universal Gröbner bases and Cartwright-Sturmfels ideals*, to appear in International Mathematics Research Notices.

[CKPS00] Nicolas Courtois, Alexander Klimov, Jacques Patarin, Adi Shamir, *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, in Proceedings of International Conference on the Theory and Application of Cryptographic Techniques(EUROCRYPT), vol. 1807, Lecture Notes in Computer Science, pp. 392–407, Springer Bruges, Belgium, 2000.

[CLO07] David Cox, John Little, Donal O'Shea, *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra. Third Edition*, Springer, 2007.

[DBMMW08] Jintai Ding, Johannes Buchmann, Mohamed S.E. Mohamed, Wael S.A.E. Moahmed, Ralf-Philipp Weinmann, *MutantXL*, Proceedings of the 1st international conference on Symbolic Computation and Cryptography (SCC08), Beijing, China, LMIB pp. 16–22, 2008.

[DPW14] Jintai Ding, Albrecht Petzoldt, Lih-chung Wang, *The Cubic Simple Matrix Encryption Scheme*, Proceedings of 6th International Workshop, PQCrypto 2014, Waterloo ON, Canada, October 1–3, 2014, Lecture Notes in Computer Science, vol. 8772, pp. 76–87, 2014.

[DS13] Jintai Ding, Dieter Schmidt, *Solving degree and degree of regularity for polynomial systems over finite fields*, Number theory and cryptography, pp. 34–49, Lecture Notes in Comput. Sci., 8260, Springer, Heidelberg, 2013.

[DY13] Jintai Ding, Bo-Yin Yang, *Degree of regularity for HFEv and HFEv-*, Proceedings of 5th International Workshop, PQCrypto 2013, Limoges, France, June 4–7, 2013, Lecture Notes in Computer Science, vol. 7932, pp. 52–66, 2013.

[DG10] Vivien Dubois, Nicolas Gama, *The Degree of Regularity of HFE Systems*, Abe, M. (ed.) ASIACRYPT 2010, LNCS, vol. 6477, pp. 557–576, Springer, Heidelberg, 2010.

[Eis94] David Eisenbud, *Commutative algebra. With a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1994.

[Eis05] David Eisenbud, *The Geometry of Syzygies. A Second Course in Algebraic Geometry and Commutative Algebra*, Graduate Texts in Mathematics, vol. 229, Springer-Verlag, New York, 2005.

[EN62] John A. Eagon and Douglas G. Northcott, *Ideals Defined by Matrices and a Certain Complex Associated with Them*, Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, vol. 269, n. 1337, pp. 188–204 , 1962.

[Fau99] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases (F4)*, Journal of Pure and Applied Algebra, vol. 139, pp. 61–88, 1999.

[Fau02] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ISSAC '02, pp. 75–83, New York, NY, USA, 2002.

[FSS10] Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer, *Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology*, Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, ISSAC '10, pp. 257–264, Munich, Germany, 2010.

[FSS13] Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer, *On the Complexity of the Generalized MinRank Problem*, Journal of Symbolic Computation, vol. 55, pp. 30–58, 2013.

[Gal74] André Galligo, *A propos du théorème de préparation de Weierstrass*, Fonctions des Plusieurs Variables Complexes, Lecture Notes in Mathematics, vol. 409, Springer-Verlag, pp. 543–579, 1974.

[GJ79] Michael R. Garey, David S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W.H. Freeman and Company, 1979.

[Gau09] Pierrick Gaudry, *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, Journal of Symbolic Computation, vol. 44, no.12, pp.1690–1702, 2009.

[GC00] Louis Goubin, Nicolas T. Courtois, *Cryptanalysis of the TTM Cryptosystem*, Advances in Cryptology, Proceedings of ASIACRYPT 2000, Lecture Notes in Computer Science, vol. 1976, Springer-Verlag, pp. 44–57, 2000.

[GM15] Elisa Gorla, Maike Massierer, *Index calculus in the trace zero variety*, Advances in Mathematics of Communications, vol. 9, no. 4, pp. 515–539, 2015.

[KS99] Aviad Kipnis, Adi Shamir, *Cryptanalysis of the HFE public key cryptosystem*, Advances in Cryptology, Proceedings of Crypto '99, LNCS no. 1666, Springer-Verlag, pp. 19–30, 1999.

[KR00] Martin Kreuzer, Lorenzo Robbiano, *Computational Commutative Algebra 1*, Springer, 2000.

[KR05] Martin Kreuzer, Lorenzo Robbiano, *Computational Commutative Algebra 2*, Springer, 2005.

[KR16] Martin Kreuzer, Lorenzo Robbiano, *Computational Linear and Commutative Algebra*, Springer, 2016.

[Laz83] Daniel Lazard, *Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations*, Computer algebra (London, 1983), pp. 146–156, Lecture Notes in Comput. Sci., vol. 162, Springer, Berlin, 1983.

[TDTD13] Chengdong Tao, Adama Diene, Shaohua Tang, Jintai Ding, *Simple matrix scheme for encryption*, Gaborit, P. (ed.) PQ Crypto 2013. LNCS, vol. 7932, pp. 231–242, Springer, Heidelberg, 2013.

[TXPD15] Chengdong Tao, Hong Xiang, Albrecht Petzoldt, Jintai Ding, *Simple Matrix – A Multivariate Public Key Cryptosystem (MPKC) for Encryption*, Finite Fields and Their Applications, vol. 35, pp. 352–368, 2015.

Alessio Caminata, Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, CH-2000 Neuchâtel, Switzerland

Current address: Institut de Matemàtica, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain

E-mail address: `caminata@ub.edu`

Elisa Gorla, Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, CH-2000 Neuchâtel, Switzerland
E-mail address: elisa.gorla@unine.ch