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 $p_1 = \cdots = p_m = 0$ over a finite field is hard. Such a system can be solved by computing a lexicographic Gröbner basis of the ideal $(p_1, \ldots, p_m)$. The most efficient algorithms for computing Gröbner bases, such as F_4 and F_5, transform the problem into several instances of Gaussian elimination. The computational complexity of these algorithms is not completely understood, especially when the polynomials $p_1, \ldots, p_m$ are non-homogeneous. In this paper, we prove that this complexity is bounded by a function of the Castelnuovo-Mumford regularity of the ideal $(p_1^h, \ldots, p_m^h)$ 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. More precisely, we show that the degree of the polynomials involved in the computation a Gröbner basis of a zero-dimensional ideal grows at most linearly in the number of variables. In combination with some theorems in commutative algebra, our results also allow us to bound the complexity of 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 $\mathcal{P} := (p_1, \ldots, p_m)$ 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 $\mathbb{F}_q^m$. 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 $y = \mathcal{P}(x) = (p_1(x), \ldots, p_m(x))$ and sends the message $y \in \mathbb{F}_q^m$. An illegitimate user who wants to read the message may try to solve the system of polynomial equations

$$\begin{cases} y_1 - p_1(x) = 0 \\ \cdots \\ y_m - p_m(x) = 0 \end{cases} \tag{1}$$

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, a direct attack is possible for every MQ system, namely trying to solve the system (1). This kind of attack is sometimes called *algebraic attack*. For this reason, it is important to be able

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

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

Alessio Caminata was supported by Armasuisse.

to estimate the difficulty of solving the system (1) for different choices of the polynomials $p_1, \ldots, p_m$.

It is a common assumption that an estimate on the complexity of computing a Gröbner basis of the ideal $I = (y_1 - p_1, \ldots, y_m - p_m)$ yields an estimate on the difficulty of solving the polynomial system (1). Although it is true that we can solve the system (1) *by computing some Gröbner basis*, the situation is more complicated than this, and several steps should be taken into account. The goal of this paper is clarifying these steps and giving an estimate of the complexity of solving a system of polynomial equations over a finite field by means of Gröbner bases algorithms.

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). Thus, computing a lexicographic Gröbner basis is an efficient strategy to solve a system of polynomial equations. Unfortunately lexicographic Gröbner bases are usually slow to compute, while Gröbner bases with respect to other monomial orders can often be obtained faster. In particular, experiments indicate that the graded reverse lexicographic term order (*DRL*) usually makes the computation of a Gröbner basis much faster than any other term order. Therefore, a commonly used strategy for computing the zero-locus of an ideal I is:

(1) computing a *DRL*-Gröbner basis of I, then
(2) converting the *DRL*-Gröbner basis into 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 these algorithms is well understood and depends on the (geometric) degree of the ideal I. It is in general lower than the complexity of step (1), although in special cases step (2) may take more time than step (1). Nevertheless, in this paper we concentrate on step (1).

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, and the XL algorithm. They appear to be 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 on 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 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.

In their survey chapter on multivariate cryptography in [BBD09], Ding and Yang write "*From the theoretical point of view, to answer these problems, the foundation again lies in modern algebraic geometry*". We also believe that the answer may be found in algebraic geometry and commutative algebra, the branches of mathematics that study the solutions of polynomial equations. In particular, taking another look at the solving degree and other important concepts in multivariate cryptography from the point of view of commutative algebra and algebraic geometry may provide further insight. The main result of this paper is a step in this direction. Namely, in Theorem 3.25 we prove that, under a genericity assumption, the solving degree of a polynomial system $f_1, \ldots, f_m$ is upper bounded by – and often equal to –

the *Castelnuovo-Mumford regularity* of the ideal $(f_1^h, \dots, f_m^h)$, where f_i^h is the homogenization of f_i.

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. Using Theorem 3.25, we can 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 (Corollary 3.26). Zero-dimensional ideals appear often in cryptography, since any system of equations that has only a finite number of solutions over the algebraic closure generates a zero-dimensional ideals. Our bound on the solving degree of a zero-dimensional ideal is linear both in the number of variables and in the maximum d of the degrees of the equations, in stark contrast with the bound for the solving degree of an arbitrary system, which is doubly exponential in d (see Theorem 3.21). In Section 5 we derive upper bounds for the solving degree of several classes of determinantal ideals, which are related to the MinRank Problem.

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 is controlled by the Castelnuovo-Mumford regularity of a homogeneous ideal associated to the system. This yields a bound on the solving degree of any zero-dimensional ideal, which is linear in the maximum of the degrees of the equations and in the number of variables. In Section 4 we investigate the relation between the Castelnuovo-Mumford regularity of an ideal and its degree of regularity, a notion that was previously introduced by other authors to study the computational complexity of finding the zero-locus of the ideal. 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], 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 $f = \sum_{i \in \mathcal{I}} a_i m_i$ 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.

1.1. **Zero-dimensional ideals.**

In this paper we are mostly interested in zero-dimensional ideals.

Definition 1.5. An ideal I of $k[x_1, \dots, x_n]$ is *zero-dimensional* if the 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.

In Definition 1.5 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 does not imply that every ideal defined over a finite field is zero-dimensional.

Remark 1.6. The definition of zero-dimensional ideal refers to the dimension of the *affine* zero-locus, also for homogeneous ideals. For example, the homogeneous ideal $I = (x_0 - x_1, x_0 - x_2) \subseteq \mathbb{C}[x_0, x_1, x_2]$ corresponds to the point $[1 : 1 : 1]$ in the projective plane $\mathbb{P}^2_{\mathbb{C}}$. However, the affine zero-locus of I is the line of equation $x_0 = x_1 = x_2$ in the affine space $\mathbb{A}^3_{\mathbb{C}}$. Hence the zero-locus of I is infinite and I is not zero-dimensional.

Notice in particular that for any zero-dimensional homogeneous ideal I we have

$$\mathcal{Z}(I) = \{(0, \dots, 0)\}.$$

Given an ideal I in a polynomial ring $R = \mathbb{F}_q[x_1, \dots, x_q]$ over a finite field $\mathbb{F}_q$, 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, if $I = (f_1, \dots, f_r)$ then $J := (f_1, \dots, f_r, x_1^q - x_1, \dots, x_n^q - x_n)$ 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 have different algebraic properties in general. For example, in most cases J has a minimal generator of degree q and this may affect the computation of a Gröbner basis of it.

Example 1.7. 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 $\overline{\mathbb{F}}_5$. It corresponds to 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 I and J have different algebraic properties: The generators of I are a Gröbner basis with respect to the LEX order with $x_3 > x_2 > x_1$, while a 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 $\operatorname{solv.deg}(I) = 3$.

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

We denote by $\mathrm{GL}(n, k)$ the general linear group of $n \times n$ invertible matrices with entries in k. This group acts on 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 1.8. *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 $g \in U$.*

The homogeneous ideal J of the previous theorem is the *generic initial ideal* of I and is denoted by $\mathrm{gin}_\leq(I)$. It is an invariant of the ideal (and of the term order) which encodes many properties of I. For example, we will see in Section 3 that the Castelnuovo-Mumford regularity of I can be read from $\mathrm{gin}_\leq(I)$ for $\leq$ the graded reverse lexicographic term order.

Definition 1.9 (generic coordinates)**.** An ideal $I \subseteq R$ is *in generic coordinates* if $1 \in U$, i.e., if $\mathrm{gin}_\leq(I) = \mathrm{in}_\leq(I)$.

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 $R := k[x_1, \ldots, x_n]$ 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 $I = (f_1, \ldots, f_r) \subseteq R$, we denote by $\tilde{I}$ the homogeneous ideal of S generated by the homogenizations of the f_i's, that is

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

The notation $\tilde{I}$ is compact, but may be misleading, since the ideal $\tilde{I}$ actually depends on the choice of the generators $f_1, \ldots, f_r$ 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 1.10. 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 $f_1, \ldots, f_r$.

The *dehomogenization map* ϕ is the ring homomorphism given by $\phi : S \to R \cong S/(t-1)$. 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. Similarly, 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 $\tilde{I}$, also the ideal I^{top} depends on the polynomials $f_1, \dots, f_r$ 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 ordering. It is well known that a Gröbner basis of an ideal I with respect to a *LEX* term order allows one to efficiently find the solutions of I.

Most authors invoke the Shape Lemma (see Theorem 2.8) to justify this claim. However, the Shape Lemma only applies to radical ideals, and many polynomial systems coming from cryptographic schemes generate ideals which are not radical. In fact, it is easy to find examples of polynomial systems coming from cryptosystems, whose *LEX*-Gröbner basis does not have the shape predicted by the Shape Lemma, e.g., all instances that we computed of the ABC cryptosystem (see [TDTD13, TXPD15]). In this section, we discuss how to justify this claim by using the Elimination Theorem (cf. [CLO07, Ch. 3]), a result which applies to all zero-dimensional ideals.

Throughout this section, we fix $R := k[x_1, \dots, x_n]$ a polynomial ring in n variables over a field k. For an ideal I of R and an integer $\ell \in \{0, \dots, n-1\}$ we denote by $R_{[\ell]} := k[x_{\ell+1}, \dots, x_n]$ and by $I_{[\ell]} := I \cap R_{[\ell]}$ the ℓ-th elimination ideal of I.

Theorem 2.1 (Elimination Theorem). *Let I be an ideal of R and let $\mathcal{G}$ be a Gröbner basis of I with respect to the LEX order with $x_1 > x_2 > \cdots > x_n$. Then for every $\ell \in \{0, \dots, n-1\}$ $\mathcal{G}_{[\ell]} := \mathcal{G} \cap R_{[\ell]}$ is a Gröbner basis of the ℓ-th elimination ideal $I_{[\ell]}$.*

We can use this theorem to characterize the shape of a *LEX*-Gröbner basis of a zero-dimensional ideal. For a proof, see [CLO07, Chapter 3, Theorem 2] and the following discussion.

Proposition 2.2. *Let I be a zero-dimensional ideal of R and let $\mathcal{G}$ be a Gröbner basis of I with respect to the LEX order 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 $p_{i,t_j} \in R_{[i-1]}$ for every $i \in \{1, \dots, n\}$, $j \in \{1, \dots, t_i\}$ and $t_1, \dots, t_{n-1} \geq 1$.

We may use Proposition 2.2 to build an algorithm which finds all the solutions of a zero-dimensional ideal I from its *LEX*-Gröbner basis. Before that, we need some preliminary results. In the sequel, we 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 $k[x_1, \dots, x_{n-1}]$.

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*

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

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 $m = \text{in}(f)$ 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 $m(x_1,\dots,x_{n-1},a) = \text{in}(f(x_1,\dots,x_{n-1},a))$. 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 $\text{in}(f(x_1,\dots,x_{n-1},a))$ and not just $\text{in}(f)$. 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 $f(x_1,x_2,a)$.

In the following 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 LEX-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 LEX-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 *LEX*-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 *LEX*-Gröbner basis of I, and $\mathcal{G}(a) \cup \mathcal{G}'$ is a *LEX*-Gröbner basis of $I(a)$. Hence, we obtain

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

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 $\text{in}(I)(a) = \Big(\text{in}(f)(x_1,\dots,x_{n-1},a) : f \in \mathcal{G}\Big) = \Big(\text{in}(f(x_1,\dots,x_{n-1},a)) : f \in \mathcal{G}\Big) = \Big(\text{in}(p) : p \in \mathcal{G}(a)\Big)$ for $a \in k$ generic. It follows that $\text{in}(I(a)) = (\text{in}(I))(a) = \Big(\text{in}(p) : p \in \mathcal{G}(a)\Big)$, thus $\mathcal{G}(a)$ is a *LEX*-Gröbner basis of $I(a)$. □

We can use Theorem 2.6 to write down a procedure which *generically* allows us to compute the solutions $P_1,\dots,P_r$ of a zero-dimensional ideal I with just one Gröbner basis computation, namely the *LEX*-Gröbner basis of I.

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

1. *Compute a reduced LEX-basis 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!) a reduced LEX-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 $P_1,\dots,P_r$ are found.*

Under stronger assumptions on the zero-dimensional ideal I, then a *LEX*-Gröbner basis of I has an even simpler form than that provided by Proposition 2.2. This is the well-known Shape Lemma (cf. [KR00, Theorem 3.7.25]).

Theorem 2.8 (Shape Lemma). *Let k be a perfect field, let $I \subseteq k[x_1, \dots, x_n]$ be a zero-dimensional radical ideal in normal x_n-position, let $g_n \in k[x_n]$ be the monic generator of the elimination ideal $I \cap k[x_n]$, and let $d = \deg g_n$. Then the following facts hold:*

1. *The reduced Gröbner basis of the ideal I with respect to a LEX order where x_n is the smallest variable is of the form $\{x_1 - g_1, \cdots, x_{n-1} - g_{n-1}, g_n\}$, where $g_1, \dots, g_{n-1} \in k[x_n]$.*
2. *The polynomial g_n has d distinct roots $a_1, \dots, a_d \in \bar{k}$, and the set of zeros of I is*
$$\mathcal{Z}(I) = \{(g_1(a_i), \dots, g_{n-1}(a_i), a_i) : i = 1, \dots, d\}.$$

Two important assumptions are made on the ideal I in Theorem 2.8: I is in normal x_n-position and I is radical. 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 $a_n \neq b_n$. This is not a restrictive condition, since 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 necessary. There exist non-radical ideals, whose LEX-Gröbner basis is not in the form of the Shape Lemma, as we show in Example 2.9. Ideals which admit a LEX-basis of the form of Theorem 2.8 have a *Shape Basis*. The Shape Lemma says that a zero-dimensional radical ideal *in generic coordinates* has a Shape Basis.

Example 2.9. 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, zero-dimensional, non-radical ideal of R. A computation with MAGMA shows that the reduced *LEX*-Gröbner basis of I is
$$\begin{aligned}
&p_{4,1} = x_4^3,\\
&p_{3,1} = x_3x_4^2,\ p_{3,2} = x_3^2 + x_3x_4,\\
&p_{2,1} = x_2x_4 + x_3x_4,\ p_{2,2} = x_2x_3 + x_4^2,\ p_{2,3} = x_2^2 + x_4^2,\\
&p_{1,1} = x_1x_4 + x_3x_4 + x_4^2,\ p_{1,2} = x_1x_3 + x_3x_4 + x_4^2,\ p_{1,3} = x_1x_2 + x_4^2,\ p_{1,4} = x_1^2.
\end{aligned}$$
This basis has the form predicted by Proposition 2.2, but it is not a Shape Basis.

As in Example 2.9, many ideals coming from cryptosystems are not radical, and they do not admit a Shape Basis. In this case, we see two possible solutions:

1. use the procedure from Corollary 2.7, which works also for non-radical ideals;
2. compute the radical $\sqrt{I}$, which has the same solutions of I over the algebraic closure $\bar{k}$, and then apply the Shape Lemma.

The radical of I can be found as in the following remark (cf. [KR00, Corollary 3.7.26]).

Remark 2.10. Let $I \subseteq R$ be a zero-dimensional ideal. For every $i = 1, \dots, n$ let $g_i \in k[x_i]$ be the monic generator of the elimination ideal $I \cap k[x_i]$. Then the radical of I is $\sqrt{I} = I + (g_1, \dots, g_n)$.

Although theoretically correct, the procedure of Remark 2.10 is computationally inefficient, since it involves the computation of several elimination ideals. In fact, in order to find the monic generator $g_i \in k[x_i]$, one usually computes a Gröbner basis with respect to a *LEX* order where x_i is the smallest variable.

For these reasons, in general the procedure of Corollary 2.7 is more efficient than computing the radical.

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

1. *Compute a reduced LEX-basis 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!) a reduced LEX-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 as before until $(a_1, \dots, a_n)$ is found.*

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

3. Solving degree of non-homogeneous 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 a *DRL* term order is usually much faster than with repect to any other term order. *LEX* term orders appear to be particularly slow. For this reason, we focus mainly on *DRL* term orders. 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], and the *XL* Algorithm [CKPS00]. 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 non-homogeneous polynomials. In this section we focus on the second family of algorithms.

It is a common assumption that in these algorithms the computational complexity is dominated by Gaussian elimination on the *Macaulay matrices*. First, we describe them for homogeneous ideals, as they are presented in [BFS14, p. 54].

Let $\{f_1, \dots, f_r\}$ be a system of homogeneous polynomials, defining an ideal I in a 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.

The size of the Macaulay matrices which appear in the algorithm is determined by the degree of the polynomials involved in the computation. 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.

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

Definition 3.2. Let $I \subseteq R$ be an ideal and let τ be a term order on R. We denote by $\operatorname{max.GB.deg}_\tau(I)$ the maximum degree of a polynomial appearing in a reduced τ-Gröbner basis of I.

It is clear that

$$\operatorname{max.GB.deg}_\tau(I) \leq \operatorname{solv.deg}_\tau(I),$$

for any ideal I and any term order τ. Equality does not hold in general, as we show in Example 3.15.

Remark 3.3. If I is a homogeneous ideal, then $\operatorname{max.GB.deg}_\tau(I) = \operatorname{solv.deg}_\tau(I)$. 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.

Since $\operatorname{solv.deg}_\tau(I)$ is the highest degree of the polynomials involved in the computation of a τ-Gröbner basis for I, we can bound the computational complexity as follows.

Proposition 3.4. *Let $f_1, \dots, f_r$ be a system of homogeneous polynomials in $R = k[x_1, \dots, x_n]$, defining an ideal I. Let d_i be the degree of f_i, let $s = \operatorname{solv.deg}_\tau(I)$. Let $m = \sum_{i=1}^r \binom{n+s-d_i-1}{s-d_i}$. The number of operations in k required to compute a τ-Gröbner basis of I is*

$$O\left(\binom{n+s-1}{s} m^{\omega-1}\right) \text{ if } m \leq \tbinom{n+s-1}{s} \quad \text{and} \quad O\left(m\binom{n+s-1}{s}^{\omega-1}\right) \text{ if } m \geq \tbinom{n+s-1}{s}$$

where ω is the exponent of matrix multiplication.

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

3.1. **Homogenization of ideals and extensions of term ordering.**

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 $\phi(\operatorname{in}_\tau(f)) = \operatorname{in}_\sigma(\phi(f))$ 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) $\operatorname{in}_\sigma(I) = \phi(\operatorname{in}_\tau(J))$*;*
(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 $\operatorname{in}_\tau(J) = (\operatorname{in}_\tau(f) : f \in J,\ f \text{ homogeneous})$, because J is a homogeneous ideal. Then we have

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

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

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

since ϕ is a homomorphism and τ ϕ-extends σ. This shows that $\{\phi(g_1), \ldots, \phi(g_s)\}$ is a σ-Gröbner basis of $\phi(\mathrm{in}_\tau(J))$, 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 $i = 1, \ldots, n$ since σ is a term order, which implies $x_i t^\alpha m >_{\bar{\sigma}} x_i t^\beta n$. Clearly $t^{\alpha+1} m >_{\bar{\sigma}} t^{\beta+1} n$.

If *2)* holds, then $x_i m = x_i n$ for every $i = 1, \ldots, n$, therefore $x_i t^\alpha m >_{\bar{\sigma}} x_i t^\beta n$ since $\alpha > \beta$. Moreover we have $t^{\alpha+1} m >_{\bar{\sigma}} t^{\beta+1} n$, because $m = n$ and $\alpha + 1 > \beta + 1$.

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

Example 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. We fix a graded reverse lexicographic (*DRL*) term order on R, and we consider the graded reverse lexicographic term (*DRL*) order on S with t the smallest variable, that is 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 term order on R and extend it to a DRL term 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, we may assume that there is no cancellation in $\phi(f)$.

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

Therefore we have $\mathrm{in}_{DRL}(f) = t^{\alpha_1} m_1$, and $\phi(\mathrm{in}_{DRL}(f)) = m_1 = \mathrm{in}_{DRL}(\phi(f))$. □

Example 3.12. The term order DRL on S is different from the term order $\overline{DRL}$ obtained from the DRL order on R by applying Definition 3.7. For example, let $R = k[x, y]$, $S = R[t]$, and consider the monomials t^3x and ty^2. We have $t^3x <_{\overline{DRL}} ty^2$ because $x <_{DRL} y^2$ in R. On the other hand, $t^3x >_{DRL} ty^2$ because $\deg(t^3x) = 4 > 3 = \deg(ty^2)$. 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 $\tilde{I}$.

From now on, we consider $R = k[x_1, \dots, x_n]$ with term order DRL, and $S = R[t]$ with term order DRL with t as smallest variable as defined in Example 3.10. Let $I \subseteq R$ be an ideal.

In order to understand the relation between the solving degrees of I and of $\tilde{I}$, we look at the Macaulay matrix $\widetilde{M}_d$ of $\tilde{I}$ and the Macaulay matrix M_d of I.

Theorem 3.13. *For every $d \geq 1$, 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.*

Proof. 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 $I_{\leq d} = \tilde{I}_d$.

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 $j \in \{1, \dots, d\}$ are then ordered following DRL on the variables $x_1, \dots, x_n$. 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 $x_1, \dots, x_n$. Then, the columns with the same power of t are ordered following DRL on the variables $x_1, \dots, x_n$ □

Corollary 3.14. *We have* $\mathrm{solv.deg}_{DRL}(I) = \mathrm{solv.deg}_{DRL}(\tilde{I})$.

We collect the equalities from Remark 3.3 and Corollary 3.14 in the following chain. All term orders are DRL, they coincide on R, and t is the smallest variable of S.

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

The first equality in the second line 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 [KR05, Proposition 4.3.21].

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

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

Example 3.15. 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

$\operatorname{solv.deg}(I^h) = 2$. By computing Gröbner bases, one can also check that $\max.\mathrm{GB}.\deg(\tilde{I}) = 3$ and $\max.\mathrm{GB}.\deg(I) = \max.\mathrm{GB}.\deg(I^h) = 2$.

From Proposition 3.4 and Corollary 3.14 we obtain the following.

Proposition 3.16. *Let $f_1, \dots, f_r$ be a system of non-homogeneous polynomials in $R = k[x_1, \dots, x_n]$, defining an ideal I. Let d_i be the degree of f_i, let $s = \operatorname{solv.deg}_{DRL}(I)$. Let $m = \sum_{i=1}^{r} \binom{n+s-d_i}{s-d_i}$. The number of operations in k required to compute a DRL-Gröbner basis of I is*

$$O\left(\binom{n+s}{s} m^{\omega-1}\right) \text{ if } m \leq \binom{n+s}{s} \quad \text{and} \quad O\left(m \binom{n+s}{s}^{\omega-1}\right) \text{ if } m \geq \binom{n+s}{s}$$

where ω is the exponent of matrix multiplication.

3.3. Solving degree and Castelnuovo-Mumford regularity.

A well-known result of Bayer and Stillman (Theorem 3.23) allows us to link the solving degree of I 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 $R := k[x_1, \dots, x_n]$ 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 $f_1, \dots, f_{\beta_0}$ 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 $\{e_1, \dots, e_{\beta_0}\}$ of the free module R^{β_0} to $\{f_1, \dots, f_{\beta_0}\}$.

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 $x_1, \dots, x_n$ 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

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

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 3.18. 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 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 $\operatorname{reg}_R(I) = \operatorname{reg}_S(J)$.

Example 3.19. 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 $\operatorname{reg}(I) = 3$.

In general, one computes the regularity of an ideal by computing a Gröbner basis of it. However, there are formulas for the regularity of many classes of ideals. The simplest case is that of a regular sequence.

Example 3.20. Let $I = (f_1, \ldots, f_r) \subseteq R = k[x_1, \ldots, x_n]$ and assume that $f_1, \ldots, f_r$ are a homogeneous regular sequence. Let $d_i = \deg f_i$ for all i. Then

$$\operatorname{reg}(I) = d_1 + \ldots + d_r - r + 1.$$

In particular, if $r = n$ and $d_1 = \ldots = d_n = d$, then I is zero-dimensional and

$$\operatorname{reg}(I) = n(d-1) + 1.$$

Even when no exact formula is known, one can bound the regularity of an ideal I in terms of the number of variables n and the maximum degree d of a minimal generator of I. The bound in the next theorem applies to any homogeneous ideal.

Theorem 3.21. *([Giu84, Gal79, CS07]) Let $I \subseteq R := k[x_1, \ldots, x_n]$ be a homogeneous ideal generated in degree $\leq d$. Then:*

$$\operatorname{reg}(I) \leq (2d)^{2^{n-2}}.$$

This result was proved by Giusti [Giu84] and Galligo [Gal79] in characteristic zero, and then extended to any characteristic by Caviglia and Sbarra [CS07]. Moreover, Mayr and Meyer [MM82] proved that for each $n > 1$ there is an ideal $I_n \subseteq \mathbb{C}[x_1, \ldots, x_n]$ generated in degree at most 4 such that $\operatorname{reg}(I_n) \geq 2^{2^{\frac{n-2}{10}}}$. Hence the bound can be regarded as sharp. On the other hand, the bound is quite large compared to the regularity of most systems. So, while this general bound cannot be significantly improved, one expects that tighter bounds can be given for special families of systems.

For example, if one restricts to zero-dimensional ideals, one obtains the following bound, which is linear in both the number of variables and the degree of the minimal generators of the ideal (cf. [Cha07, Theorem 9.4]).

Theorem 3.22. *Let $J \subseteq R$ be a homogeneous ideal. Assume that J is generated in degree at most d, and that its projective zero-locus over the algebraic closure consists of a finite number of points. Then*

$$\operatorname{reg}(J) \leq n(d-1) + 1.$$

The next result is due to Bayer and Stillman ([BS87, Theorem 2.4 and Proposition 2.9]). It allows us to use the Castelnuovo-Mumford regularity to bound the computational complexity of computing a Gröbner basis.

Theorem 3.23 (Bayer-Stillman)**.** *Let k be an infinite field, and let J be a homogeneous ideal in a polynomial ring $k[x_1, \ldots, x_n]$ over k. Then*

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

Hence, if J is in generic coordinates, then

$$\operatorname{reg}(J) \geq \operatorname{max.GB.deg}_{DRL}(J) = \operatorname{solv.deg}(J).$$

If k has characteristic zero, then the Castelnuovo-Mumford regularity of $\operatorname{gin}_{DRL}(J)$ is equal to the maximum degree of a polynomial in a minimal system of generators for $\operatorname{gin}_{DRL}(J)$. Hence, if J is in generic coordinates and k has characteristics zero, then

$$\operatorname{reg}(J) = \operatorname{max.GB.deg}_{DRL}(J) = \operatorname{solv.deg}(J).$$

Notice that the inequality in the theorem is often an equality even in positive characteristics, in fact this is the case in all the examples that we compute in this paper. Nevertheless, it is possible to find examples in positive characteristics where the equality does not hold.

The next corollary follows easily from Theorem 3.23 and Remark 3.3.

Corollary 3.24. *Let k be a field, let $R := k[x_1, \ldots, x_n]$, and let $I := (f_1, \ldots, f_r)$ be a homogeneous ideal of R. Assume that I is in generic coordinates in $\overline{k}[x_1, \ldots, x_n]$, then*

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

and equality holds if k has characteristics zero.

More interestingly, we can use Bayer and Stillman's result to obtain the following.

Theorem 3.25. *Let k be a field, let $R := k[x_1, \ldots, x_n]$, and let $I := (f_1, \ldots, f_r)$ be an ideal of R. Assume that $\tilde{I} := (f_1^h, \ldots, f_r^h)$ is in generic coordinates in $\overline{k}[x_1, \ldots, x_n, t]$, then*

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

and equality holds if k has characteristics zero.

Proof. By Corollary 3.14 we have $\operatorname{solv.deg}_{DRL}(I) = \operatorname{solv.deg}_{DRL}(\tilde{I}) = \operatorname{max.GB.deg}_{DRL}(\tilde{I})$. A Gröbner basis of $\tilde{I}$ is invariant by field extension, so $\operatorname{max.GB.deg}_{DRL}(\tilde{I})$ is the same if we consider the extension of $\tilde{I}$ to $\overline{k}[x_1,\ldots,x_n,t]$. The ideal $\tilde{I}$ is in generic coordinates in $\overline{k}[x_1,\ldots,x_n,t]$, hence $\operatorname{max.GB.deg}_{DRL}(\tilde{I}) \leq \operatorname{reg}(\tilde{I})$ by Theorem 3.23. Since the regularity of $\tilde{I}$ is invariant by field extensions, the claim is proved. □

The previous theorem tells us that the Castelnuovo-Mumford regularity of the homogeneous ideal $\tilde{I}$ bounds the solving degree of $\tilde{I}$, hence the solving degree of I. Therefore, a bound on the regularity of $\tilde{I}$ produces a bound the complexity of computing a Gröbner basis of I. Notice that 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.

We apply this strategy to two important settings. We give an upper bound for the solving degree of any zero-dimensional ideal, which is linear both in the degree of the generators and in the number of variables. Then, in Section 5 we estimate the solving degree of some determinantal ideals, which are related to MinRank Problems.

The bound on the solving degree of zero-dimensional ideals follows immediately by combining Theorem 3.25 and Theorem 3.22.

Corollary 3.26. *Let k be a field, let $R := k[x_1,\ldots,x_n]$, let $S := R[t]$ and let $I := (f_1,\ldots,f_r)$ be an ideal of R generated in degree at most d. Assume that $\tilde{I} := (f_1^h,\ldots,f_r^h)$ is in generic coordinates and its projective zero-locus over $\overline{k}$ consists of a finite number of points, then*

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

Corollary 3.26 is particularly relevant for cryptographic applications. In fact many systems of equations coming from multivariate quadratic cryptoschemes 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 and satisfies the hypothesis of Corollary 3.26.

Example 3.27 (ABC cryptosystem [TDTD13, TXPD15])**.** The system associated to the ABC cryptosystems consists of $2n$ quadratic equations in n variables, so one expects that the ideal I associated to such a system is generically zero-dimensional. For all instances of the ABC cryptosystem that we computed, the corresponding ideal is indeed zero-dimensional. Hence one obtains

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

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, so one expects that the ideal I associated to such a system is generically zero-dimensional. For all instances of the cubic simple matrix encryption scheme that we computed, the corresponding ideal is indeed zero-dimensional. Hence one obtains

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

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

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

4.1. **The degree of regularity of 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 non-homogeneous 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. The function $HF_A(-) : \mathbb{N} \to \mathbb{N}$, $HF_A(d) := \dim_k A_d$ is called *Hilbert function* of A. It is well known that for large d, the Hilbert function of A is a polynomial in d called *Hilbert polynomial* and denoted by $HP_A(d)$. The generating series of HF_A is called *Hilbert series* of A. We denote it by $HS_A(z) := \sum_{d\in\mathbb{N}} HF_A(d)z^d$. A classical theorem by Hilbert and Serre says that the Hilbert series of A is a rational function, and more precisely has the form

$$HS_A(z) = \frac{h_A(z)}{(1-z)^\ell} \tag{2}$$

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 easily 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* (2) *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

$$i_{\text{reg}}(I) \leq \text{reg}(I). \tag{3}$$

If I is a homogeneous zero-dimensional ideal, then its index of regularity and Castelnuovo-Mumford regularity coincide (cf. [Eis05, Corollary 4.15]), that is

$$i_{\text{reg}}(I) = \text{reg}(I).$$

Definition 4.3 (degree of regularity of 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 both I and I^{top} are zero-dimensional ideals. In fact, $I_d^{\text{top}} = R_d$ for $d \gg 0$ if and only if I^{top} is a zero-dimensional ideal. Moreover, if I^{top} is zero-dimensional then I is, while the converse does not hold in general. See Example 4.8 for an example where I is zero-dimensional, but I^{top} is not.

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*

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

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

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

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 I is zero-dimensional and $\mathcal{Z}(I) = \{(0,\dots,0)\}$, as discussed in Remark 1.6.

For a non-homogeneous, 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 a reduced Gröbner basis of I has degree at most $d_{\text{reg}}^F(I)$, that is

$$\max.\text{GB}.\deg_{\leq}(I) \leq d_{\text{reg}}^F(I). \tag{4}$$

Notice however that (4) 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^{top} is zero-dimensional and

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

The computations were performed by G. Bianco with MAGMA.

Notice moreover that there are non-homogeneous, zero-dimensional ideals I for which $I_d^{\text{top}} \neq R_d$ for all $d \geq 0$. Definition 4.3 and (4) 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 $\text{solv.}\deg_{DRL}(I) = \operatorname{reg}(\tilde{I}) = 15$, I^{top} is not zero-dimensional, 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

$$I^{\text{top}}S + (t) = \tilde{I} + (t). \tag{5}$$

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 $\operatorname{reg}(\tilde{I}) = \operatorname{reg}(I^{\text{top}})$. Therefore, if $t \nmid 0$ modulo $\tilde{I}$ and $I^{\text{top}}_d = R_d$ for $d \gg 0$, then

$$d^F_{\text{reg}}(I) = \operatorname{reg}(\tilde{I})$$

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 $f_1, \dots, f_r$ are a Macaulay basis of I with respect to the standard grading (see [KR05, Theorem 4.3.19]). Therefore (5) 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 of 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 differ 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 $\operatorname{Syz}(f_1, \dots, f_r)$ the first syzygy module of $f_1, \dots, f_r$, that is the kernel of φ. An element of $\operatorname{Syz}(f_1, \dots, f_r)$ 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 $\operatorname{Triv}(f_1, \dots, f_r)$ of trivial syzygies of $f_1, \dots, f_r$ as the submodule of $\operatorname{Syz}(f_1, \dots, f_r)$ 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 $\operatorname{Syz}(I)$ and $\operatorname{Triv}(I)$ the modules of syzygies and trivial syzygies of $f_1, \dots, f_r$. For any $d \in \mathbb{N}$ we define the vector space $\operatorname{Syz}(I)_d := \operatorname{Syz}(I) \cap B^r_d$ of syzygies of degree d. Similarly, we define also the vector subspace of trivial syzygies of degree d $\operatorname{Triv}(I)_d := \operatorname{Triv}(I) \cap B^r_d$. Clearly, we have $\operatorname{Triv}(I)_d \subseteq \operatorname{Syz}(I)_d$.

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

$$d^D_{\text{reg}}(I) := \min\{d \in \mathbb{N} : \operatorname{Syz}(I)_{d-2} / \operatorname{Triv}(I)_{d-2} \neq 0\}.$$

Let $f_1, \dots, f_r \in B$ be non-homogeneous polynomials of degree 2 generating a non-homogeneous ideal I, then

$$d^D_{\text{reg}}(I) := d^D_{\text{reg}}(I^{\text{top}}).$$

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 of 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 of Ding (Definition 4.9) and the degree of regularity of 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 MinRank Problem can be stated as follows. Given an integer $r \geq 1$ and a set $\{M_1, \ldots, M_m\}$ of $n \times n$ matrices with entries in a field k, find (at least) a nonzero m-tuple $\lambda = (\lambda_1, \ldots, \lambda_m) \in k^m$ such that

$$\operatorname{rank}\left(\sum_{i=1}^{m} \lambda_i M_i\right) \leq r - 1. \tag{6}$$

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 (6) is equivalent to requiring that the minors of size $r \times r$ of the matrix $M = \sum_{i=1}^{m} \lambda_i M_i$ vanish. In particular, every solution λ of the MinRank Problem corresponds to a point in the zero-locus in k^m of the ideal $I_r(M)$ of r-minors of M. This algebraic interpretation leads to the following generalization of the MinRank Problem.

Generalized MinRank Problem. Given a field k, a $n \times m$ matrix M whose entries are polynomials in $R = k[x_1, \ldots, x_s]$, and an integer $1 \leq r \leq \min\{m, n\}$ compute the set of points in k^s at which the evaluation of M has rank at most r, that is the zero-locus of the ideal of r-minors $I_r(M)$.

Minors of size $r \times r$ of the matrix M form an algebraic system of multivariate polynomials. So one can attempt to solve it using the strategy illustrated in the previous sections. Namely, one can compute a *DRL*-Gröbner basis of $I_r(M)$ using an algorithm such as F_4/F_5 and then convert it to a *LEX*-Gröbner basis using a Gröbner walk, or FGLM if the ideal is zero-dimensional.

Since the security of several multivariate cryptosystems relies on the difficulty of solving the MinRank Problem, it is important to understand the computational complexity of finding a solution to the system associated to $I_r(M)$. In particular, it is important to give theoretical estimates for the solving degree of $I_r(M)$ for large classes of matrices M.

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. In particular, some bounds on the Castelnuovo-Mumford regularity for determinantal ideals are known. Using Theorem 3.25, we can take advantage of the literature on the regularity of determinantal ideals to give bounds on the solving degree of two large classes of determinantal ideals. We focus on homogeneous determinantal ideals in this section. Analogous results in the non-homogeneous setting can be obtained applying the arguments developed in Section 3.

The first case we consider concerns ideals of maximal minors of matrices of linear forms. The MinRank Problem associated to this class of matrices is the classical MinRank Problem of (6).

Theorem 5.1 (Bruns-Conca-Varbaro, [BCV15]). *Let M be an $m \times n$ matrix with $m \leq n$ whose entries are linear forms in a polynomial ring over a field k. Assume that*

$$\text{height}\, I_m(M) \geq n - m + 1 \quad \textit{and} \quad \text{height}\, I_r(M) \geq \min\{(m+1-r)(n-m)+1, \text{height}\, I_1(M)\}, \tag{7}$$

for every $r = 2, \ldots, m-1$. Then we have $\text{reg}\, I_m(M) = m$.

The conditions on the heights of the determinantal ideals are satisfied for a generic matrix. In particular, they are satisfied if all the ideals $I_r(M)$ are zero-dimensional, a common situation in cryptography.

Corollary 5.2. *Let M be an $m \times n$ matrix with $m \leq n$ whose entries are linear forms in a polynomial ring over a field k such that conditions* (7) *hold. Then the solving degree of the corresponding MinRank Problem is* $\text{solv.deg}\, I_m(M) \leq m$.

For the next class of determinantal ideals, we assume that the polynomial ring R has a standard $\mathbb{Z}^v$-graded structure. By this we mean that the degree of every indeterminate of R is an element of the canonical basis $\{e_1, \ldots, e_v\}$ of $\mathbb{Z}^v$. For $v = 1$, this is just the standard $\mathbb{Z}$-grading. Let $M = (m_{i,j})$ be a $m \times n$ matrix with entries in R, and assume without loss of generality that $m \leq n$. We say that M is *column-graded* if $n \leq v$ and $m_{i,j} = 0$ or $\deg m_{i,j} = e_j \in \mathbb{Z}^v$ for every i, j. We say that M is *row-graded* if $m \leq v$ and $m_{i,j} = 0$ or $\deg m_{i,j} = e_i \in \mathbb{Z}^v$ 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 5.3 (Conca-De Negri-Gorla, [CDG16]). *Let M be a $m \times n$ row-graded or column-graded matrix with entries in a polynomial ring over a field and assume $m \leq n$. Then:*

1. *the ideal of maximal minors $I_m(M)$ is radical and has* $\text{reg}\, I_m(M) = m$;
2. *the ideal of* 2*-minors $I_2(M)$ is radical and has* $\text{reg}\, I_2(M) \leq n$ *in the column-graded case, and* $\text{reg}\, I_2(M) \leq m$ *in the row-graded case.*

Corollary 5.4. *Let $m \leq n$ be two integers and let M be a $m \times n$ row-graded or column-graded matrix with entries in a polynomial ring over a field. Then the solving degree of the corresponding MinRank Problems are:*

1. $\text{solv.deg}\, I_m(M) \leq m$;
2. $\text{solv.deg}\, I_2(M) \leq n$ *in the column-graded case, and* $\text{solv.deg}\, I_2(M) \leq m$ *in the row-graded case.*

Notice that $\text{solv.deg}\, I_m(M) = m$ implies that a Gröbner basis can be computed from the set of maximal minors via Gaussian elimination.

In addition, the following stronger result is shown in [CDG15, CDG16]. A *universal Gröbner basis* of I is a set of polynomials that are a Gröbner basis of I with respect to any term order.

Theorem 5.5 (Conca-De Negri-Gorla, [CDG15, CDG16]). *Let M be a $m \times n$ matrix with entries in a polynomial ring over a field and assume $m \leq n$.*

1. *If M is column-graded, then its maximal minors are a universal Gröbner basis of $I_m(M)$.*
2. *If M is row-graded, then $I_m(M)$ has a universal Gröbner basis which consists of linear combinations of the maximal minors of M.*

Acknowledgements

The authors are grateful to A. Petzoldt for help with MAGMA computations. 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 ála 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.

[BBD09] Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, *Post-Quantum Cryptography*, Springer Verlag, 2009

[BG17] Giulia Bianco, Elisa Gorla, *Index calculus in trace-zero subgroups and generalized summation polynomials*, preprint 2017.

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

[BCV15] Winfried Bruns, Aldo Conca, Matteo Varbaro, *Maximal minors and linear powers*, J. reine angew. Math., vol. 702, pp. 41–53, 2015.

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

[CS07] Giulio Caviglia, Enrico Sbarra, *Characteristic-free bounds for the Castelnuovo-Mumford regularity*, Compositio Mathematica, vol. 141, pp.1365–1373, 2005.

[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.

[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*, preprint ArXiv:1608.08942.

[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.

[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.

[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.

[FGLM93] Jean-Charles Faugère, Patrizia M. Gianni, Daniel Lazard, Teo Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, Journal of Symbolic Computation, vol. 16, n. 4, pp. 329–344, 1993.

[Gal79] André Galligo, *Theoreme de division et stabilite en geometrie analytique locale*, Ann. Inst. Fourier (Grenoble), vol. 29, n. 2, pp. 107–184, 1979.

[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.

[Giu84] Marc Giusti, *Some effectivity problems in polynomial ideal theory*, (EUROSAM 84), Lecture Notes in Computer Science, vol. 204, Springer-Verlag, pp. 159–171, 1984.

[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.

[M2] Daniel R. Grayson, Michael E. Stillman, *Macaulay2, a software system for research in algebraic geometry*, Available at http://www.math.uiuc.edu/Macaulay2/

[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.

[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.

[MM82] Ernst W. Mayr, Albert R. Meyer, *The complexity of the word problem for commutative semigroups and polynomial ideals*, Advances in Math., vol. 46, pp. 305–329, 1982.

[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
E-mail address: alessio.caminata@unine.ch

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