SOLVING DEGREE, LAST FALL DEGREE, AND RELATED INVARIANTS

ALESSIO CAMINATA AND ELISA GORLA

ABSTRACT. In this paper we study and relate several invariants connected to the solving degree of a polynomial system. This provides a rigorous framework for estimating the complexity of solving a system of polynomial equations via Gröbner bases methods. Our main results include a connection between the solving degree and the last fall degree and one between the degree of regularity and the Castelnuovo–Mumford regularity.

INTRODUCTION

As computational problems can often be modelled via polynomial equations, several security estimates in cryptography depend on the complexity of polynomial system solving. Within public key cryptography, polynomial system solving plays a crucial role in index-calculus on Abelian varieties [12] as well as in multivariate cryptography [7]. The relation-collection phase of index calculus algorithms on elliptic and hyperelliptic curves relies on the ability to solve multivariate polynomial systems over a finite field. Being able to accurately predict the complexity of solving these systems has an impact on the balancing of complexities between the relation-collection and the linear-algebra phase, and consequently on the complexity of the whole algorithm. Multivariate cryptography is one of the current proposals for post-quantum cryptography and it offers short digital signatures which are believed to be quantum-resistant. Forging a signature requires finding a solution to a system of multivariate polynomial equations. Therefore, security estimates in multivariate cryptography rely on estimates for the complexity of solving certain polynomial systems.

The solutions of a system of polynomial equations over a finite field can be computed in polynomial time from a lexicographic Gröbner basis of the system. Nowadays, the most efficient algorithms to compute Gröbner bases belong to the family of linear-algebra-based algorithms, including F4/F5 and the family of XL Algorithms [10, 11, 5, 6]. The complexity of these algorithms is bounded from above by a known function of the solving degree. Therefore, an estimate on the solving degree of a system of equations directly translates into an upper bound on the complexity of solving the system.

Computer experiments are often used to provide an indication on how the solving degree scales with the parameters of the system. In multivariate cryptography, however, the complexity of solving the polynomial system is huge by design and there is a large

gap between the size of the parameters for which we can compute the solving degree experimentally and the proposed system parameters. Because of this large gap, the security estimates obtained from the experimental results by extrapolation have limited reliability. In such a scenario, proven security estimate become essential.

Unfortunately however, finding the solving degree of a system without computing its Gröbner basis is often hard. This motivated the introduction of several algebraic invariants related to the solving degree. The main ones are the first [9, 8] and last fall degrees [15], the degree of regularity [2, 1], and the Castelnuovo–Mumford regularity [4]. These invariants are routinely used within the cryptographic community in order to estimate the solving degree. Relating them with the solving degree and with each other is therefore essential for producing accurate and provable security estimates.

Several connections between these invariants, both heuristic and proven, are known. In [4] we have shown that, under suitable assumptions, the Castelnuovo–Mumford regularity of the homogenization of a system is an upper bound for its solving degree. In [14] the authors outlined an algorithm to compute the solution of a polynomial system and provided an upper bound on its complexity in terms of its last fall degree. Later in [13] it was shown that the last fall degree is a lower bound for the solving degree. Only recently in [18, 19] it was shown that, under suitable assumptions, the solving degree is bounded from above by twice the degree of regularity. Finally, while the first fall degree is widely used as a proxy for the solving degree, their relation is only heuristic. Several authors in fact assume that the solving degree and the first fall degree are not far apart. This is usually referred to as *first fall degree assumption*. The intuition behind this assumption is that, once some degree falls appear, new polynomials are added to the computation and this makes the computation terminate soon after. There are examples for which this assumption does not hold, see e.g. [8], however many authors believe that it is satisfied with high probability, see e.g. [16].

In this paper, we explore the relations between these invariants. We compare two equivalent definitions for the last fall degree and provide a new one, which we prove being equivalent to the previous ones.

Our main theorem, Theorem 3.1, shows that, for any degree-compatible term order, the solving degree of a system is the maximum between its last fall degree and the largest degree of an element in a reduced Gröbner basis of the system. This provides a proof for the intuitive fact that the two key ingredients in determining the solving degree of a system are the degrees of the elements in its reduced Gröbner basis and the degree falls. Notice that, while it is clear that these two ingredients play a role in determining the solving degree, until now it was not known that these are the only two relevant factors. We also look at the first fall degree and show by means of examples that it may be arbitrarily larger or smaller than either of the other invariants.

Another main result, Theorem 5.3, relates the degree of regularity of a system with the Castelnuovo–Mumford regularity of its homogenization. While for a homogeneous system the degree of regularity, the Castelnuovo–Mumford regularity, and the solving degree of the system often coincide, the relation between these invariants is much more complicated for a non-homogeneous system. If the system is not homogeneous, both the

degree of regularity and the Castelnuovo–Mumford regularity are algebraic invariants of associated homogeneous systems. Their relation, however, depends on a number of factors and was until now unclear. In this paper, we show that the degree or regularity is smaller than or equal than the Castelnuovo–Mumford regularity. This is consistent with the known fact that the solving degree is bounded from above by the Castelnuovo–Mumford regularity [4] and by twice the degree of regularity [18, 19].

The paper is structured as follows. In Section 1 we introduce all the invariants that we discuss in the paper. In Section 2 we compare two equivalent definitions of last fall degree. In Definition 2.6 we formalize the concept of degree falls and in Theorem 2.8 we prove that the last fall degree is the largest degree in which a degree fall occurs. Finally, in Theorem 2.9 we show that, for any degree-compatible term order, the last fall degree is equal to the largest degree of an element in a Gröbner basis, for which a degree fall occurs. Section 3 contains the main result of this paper. In Theorem 3.1 we prove that the solving degree of a system is the maximum between its last fall degree and the degrees of the elements in its reduced Gröbner basis, under the assumption that the term order is degree-compatible. Section 4 focuses on the first fall degree. We show by means of examples that the difference between the first fall degree and any other of the invariants that we have mentioned can be either positive or negative and arbitrarily large in absolute value.

Finally, in Section 5 we discuss the relation between the degree of regularity and the Castelnuovo–Mumford regularity. In Theorem 5.3 we show that the degree of regularity of a system is smaller than or equal to the Castelnuovo–Mumford regularity of its homogenization.

1. Preliminaries

Throughout the paper, we let k be a field and denote by $R = k[x_1, \ldots, x_n]$ the polynomial ring in n variables with coefficients in k. We let $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R$ be a system of polynomial equations and let $(\mathcal{F}) = (f_1, \ldots, f_r) \subseteq R$ be the ideal generated by the equations of $\mathcal{F}$. For $f \in R$, let f^{top} denote the homogeneous component of f of largest degree, i.e., if $f = \sum_{a_1, \ldots, a_n \geq 0} \alpha_{a_1, \ldots, a_n} x_1^{a_1} \cdots x_n^{a_n}$ with $\alpha_{a_1, \ldots, a_n} \in k$, then

$$f^{\mathrm{top}} = \sum_{a_1 + \ldots + a_n = \deg(f)} \alpha_{a_1, \ldots, a_n} x_1^{a_1} \cdots x_n^{a_n}.$$

We denote by $\mathcal{F}^{\mathrm{top}}$ the system $\{f_1^{\mathrm{top}}, \ldots, f_r^{\mathrm{top}}\} \subseteq R$. Let t be a new variable and denote by f^h the homogenization of a polynomial f with respect to t. Let $\mathcal{F}^h$ be the system $\{f_1^h, \ldots, f_r^h\} \subseteq R[t]$.

For an $i \in \mathbb{N}$, we denote by R_i the k-vector space generated by the monomials of degree i of R. For an ideal $I \subseteq R$, let $I_i = I \cap R_i$. Denote by $R_{\leq i} = \sum_{j \leq i} R_j$ and by $I_{\leq i} = I \cap R_{\leq i}$.

In this paper we study several invariants, which are used to estimate the complexity of solving a polynomial system via Gröbner bases methods. The main such invariants is

the solving degree, which by definition measures the complexity of computing a Gröbner basis using a linear algebra algorithm that follows the strategy proposed by Lazard in [17]. We now briefly recall what such an algorithm does.

Fix a term order σ on R and a degree $d \geq 1$. Let

$$\mathcal{M}_{\leq d} = \{a \in \{0, \ldots, d\}^n \mid a_1 + \ldots + a_n \leq d\}.$$

The elements of $\mathcal{M}_{\leq d}$ correspond to the monomials in $R_{\leq d}$ via

$$a = (a_1, \ldots, a_n) \longleftrightarrow x_1^{a_1} \cdots x_n^{a_n}.$$

Build a matrix M whose columns are indexed by the elements of $\mathcal{M}_{\leq d}$ in decreasing order from left to right with respect to σ. The rows correspond to polynomials of the form uf where $u \in R$ is a monomial, $f \in \mathcal{F}$, and $\deg(uf) \leq d$. Notice that this includes the possibility that $u = 1$. In order to associate a row $\ell(g)$ to a polynomial g, write

$$g = \sum_{a = (a_1, \ldots, a_n) \in \mathcal{M}_{\leq d}} \alpha_a x_1^{a_1} \cdots x_n^{a_n},$$

then $\ell(g)_a = \alpha_a$. The matrix M is called **Macaulay matrix** of $\mathcal{F}$ in degree d.

Perform Gaussian elimination on M to obtain a matrix in reduced row echelon form (RREF). Any row $\ell = (\ell_a \mid a \in \mathcal{M}_{\leq d})$ in the RREF of M corresponds to a polynomial

$$f_\ell = \sum_{a \in \mathcal{M}_{\leq d}} \ell_a x_1^{a_1} \cdots x_n^{a_n}.$$

If $\deg(f_\ell) < d$, we add new rows to M corresponding to the polynomials uf_ℓ where u is a monomial, $\deg(uf_\ell) \leq d$ and $uf_\ell \notin \mathrm{rowsp}(M)$. Here $\mathrm{rowsp}(M)$ denotes the rowspace of M. Repeat the computation of the RREF and the operation of adding new rows, until there are no new rows to add. Denote by M_d the matrix in RREF computed via this algorithm.

It is clear that $\mathrm{rowsp}(M_d) \subseteq (\mathcal{F})_{\leq d}$. For a given d, one may have $\mathrm{rowsp}(M_d) \neq (\mathcal{F})_{\leq d}$. However, it is well-known that $\mathrm{rowsp}(M_d)$ contains a Gröbner basis of $\mathcal{F}$ with respect to σ for $d \gg 0$. For any such d, one also has that $\mathrm{rowsp}(M_d) = (\mathcal{F})_{\leq d}$.

Definition 1.1. Let $\mathcal{F} \subseteq R$ be a polynomial system. The **solving degree** of $\mathcal{F}$ with respect to a term order σ is the least d such that $\mathrm{rowsp}(M_d)$ contains a Gröbner basis of $(\mathcal{F})$ with respect to σ. We denote it by $\mathrm{sd}_\sigma(\mathcal{F})$.

Definition 1.2. Let $\mathcal{F} \subseteq R$ be a polynomial system and let σ be a term order. We denote by $\max.\mathrm{GB}.\deg_\sigma(\mathcal{F})$ the largest degree of an element of a reduced Gröbner basis of $(\mathcal{F})$ with respect to σ.

Since computing the solving degree without computing a Gröbner basis is hard, several authors have introduced other invariants which they use to estimate the solving degree. The main ones are the first and the last fall degree, the degree of regularity, and the Castelnuovo–Mumford regularity.

The **first fall degree** was introduced by Dubois and Gama in [9]. Here we use a modified definition from [8]. We consider a finite field $\mathbb{F}_q$ and we work over $B =$

$\mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$. Let $f_1, \ldots, f_r \in B$ be homogeneous polynomials. If $f_1, \ldots, f_r$ are not homogeneous, use $f_1^{\text{top}}, \ldots, f_r^{\text{top}}$ instead of $f_1, \ldots, f_r$. We define a B-module homomorphism φ by letting $\varphi(b_1, \ldots, b_r) = \sum_{i=1}^r b_i f_i$ for any $(b_1, \ldots, b_r) \in B^r$. We denote by $\text{Syz}(f_1, \ldots, f_r)$ the syzygy module of $f_1, \ldots, f_r$, that is, the kernel of φ. An element of $\text{Syz}(f_1, \ldots, f_r)$ is called a syzygy of $f_1, \ldots, f_r$. In other words, a syzygy is a vector $(b_1, \ldots, b_r) \in B^r$ such that $\sum_{i=1}^r b_i f_i = 0$. The degree of the syzygy $(b_1, \ldots, b_r)$ is

$$\deg(b_1, \ldots, b_r) = \max\{\deg(b_i) + \deg(f_i) \mid 1 \leq i \leq r\}.$$

For any $d \in \mathbb{N}$ we define the vector space $\text{Syz}(\mathcal{F})_d$ of homogeneous syzygies of degree d, i.e., syzygies $(b_1, \ldots, b_r)$ such that $\deg(b_i) + \deg(f_i) = d$ for all $1 \leq i \leq r$.

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 from the quotient structure of B, that is $f_i^{q-1} e_i$. Here e_i denotes the i-th element of the canonical basis of B. These syzygies are called **trivial syzygies**, because they are always present and do not depend on the structure of $f_1, \ldots, f_r$, but rather on the ring structure of B. We define the module $\text{Triv}(f_1, \ldots, f_r)$ of trivial syzygies of $f_1, \ldots, f_r$ as the submodule of $\text{Syz}(f_1, \ldots, f_r)$ generated by

$$\{f_i e_j - f_j e_i : \ 1 \leq i < j \leq r\} \cup \{f_i^{q-1} e_i : \ 1 \leq i \leq r\}.$$

We define the vector subspace of trivial syzygies of degree d as $\text{Triv}(\mathcal{F})_d = \text{Triv}(\mathcal{F}) \cap \text{Syz}(\mathcal{F})_d$.

Definition 1.3. Let $\mathcal{F} \subseteq B$ be a polynomial system. The **first fall degree** of $\mathcal{F}$ is

$$d_{\text{ff}}(\mathcal{F}) = \min\{d \in \mathbb{N} : \ \text{Syz}(\mathcal{F}^{\text{top}})_d / \text{Triv}(\mathcal{F}^{\text{top}})_d \neq 0\}.$$

The definition of **Castelnuovo–Mumford regularity** is the most technical and it requires concepts from commutative algebra that we have not defined here. Therefore, we refer the reader to [4, Section 3.4] for the definition of Castelnuovo–Mumford regularity and a discussion of its relation with the solving degree.

The **degree of regularity** was introduced by Bardet, Faugère, and Salvy in [1, 2]. Let I be a homogeneous ideal of $R = k[x_1, \ldots, x_n]$, we recall that for an integer $d \geq 0$ we denote by $I_d = I \cap R_d$ the k-vector space of homogeneous polynomials of degree d of I. The function $\text{HF}_I(-) : \mathbb{N} \to \mathbb{N}$, $\text{HF}_I(d) = \dim_k I_d$ is called Hilbert function of I. It is well-known that, for large d, the Hilbert function of I is a polynomial in d called Hilbert polynomial and denoted by $\text{HP}_I(d)$. The index of regularity of I is the smallest integer $i_{\text{reg}}(I) \geq 0$ such that $\text{HF}_I(d) = \text{HP}_I(d)$ for all $d \geq i_{\text{reg}}(I)$. If $\mathcal{F}$ is a system of generators for I, we set $i_{\text{reg}}(\mathcal{F}) = i_{\text{reg}}(I)$.

Definition 1.4. Let $\mathcal{F} \subseteq R$ be a polynomial system. The **degree of regularity** of $\mathcal{F}$ is

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

Notice that, if $(\mathcal{F}^{\text{top}})_d = R_d$ for $d \gg 0$, then

$$d_{\text{reg}}(\mathcal{F}) = \min\{d \geq 0 \mid \text{HF}_{(\mathcal{F}^{\text{top}})}(d) = \text{HF}_R(d)\} = \min\{d \geq 0 \mid (\mathcal{F}^{\text{top}})_d = R_d\}.$$

The **last fall degree** was introduced by Huang, Kosters, and Yeo in [15]. In [14, Proposition 2.3 and Proposition 2.8] the authors outline a linear-algebra-based algorithm

which computes the solutions of a non-homogeneous polynomial system $\mathcal{F}$ and show that its complexity is controlled by the last fall degree of the system $\mathcal{F}$.

Definition 1.5. Let $\mathcal{F} \subseteq R$ be a polynomial system. Let $i \in \mathbb{N}$ and let $V_{\mathcal{F},i}$ be the smallest k-vector space such that:

- $\mathcal{F} \cap R_{\leq i} \subseteq V_{\mathcal{F},i}$,
- if $f \in V_{\mathcal{F},i}$ and $g \in R_{\leq i-\deg(f)}$, then $fg \in V_{\mathcal{F},i}$.

We set also $V_{\mathcal{F},\infty} = (\mathcal{F})$ and $V_{\mathcal{F},-1} = \emptyset$.

The **last fall degree** of $\mathcal{F}$ is

$$d_{\mathcal{F}} = \min\{d \in \mathbb{N} \cup \{\infty\} \mid f \in V_{\mathcal{F},\max\{d,\deg(f)\}} \text{ for all } f \in (\mathcal{F})\}.$$

A direct consequence of the existence of a Gröbner basis for $(\mathcal{F})$ is that the last fall degree is an integer, i.e. $d_{\mathcal{F}} \in \mathbb{N}$, see also [14, Proposition 2.6 i].

These concepts also allow us to show that the rowspace of a Macaulay matrix after applying the algorithm described at the beginning of this section does not depend on the choice of the term order, provided that it is degree-compatible. In fact, it follows from Definition 1.5 that

$$V_{\mathcal{F},d} \supseteq \mathrm{rowsp}(M_d)$$

for all d. In the proof of [14, Proposition 2.3] it is stated that, if σ is degree-compatible, then

$$(1) \hspace{4cm} V_{\mathcal{F},d} = \mathrm{rowsp}(M_d)$$

for all $d \in \mathbb{Z}_{\geq 0}$. A proof of (1) is given in [13, Theorem 1].

Corollary 1.6. $\mathrm{rowsp}(M_d)$ *does not depend on the choice of σ, if σ is degree-compatible.*

The next example shows that, in general, equality (1) and Corollary 1.6 do not hold for a term order which is not degree-compatible.

Example 1.7. Let $d \geq 3$ be an integer. Let $\mathcal{F} = \{x - y^{d-1}, x - y^d\}$ and let σ be the lexicographic order on $k[x,y]$ with $x > y$. Let

$$f = xy - x = y(x - y^{d-1}) - (x - y^d) \in V_{\mathcal{F},d}.$$

By the definition of last fall degree, one also has that $xf \in V_{\mathcal{F},d}$. The rows of the matrix M_d correspond to the polynomials $x - y^{d-1}, x(x - y^{d-1}), y(x - y^{d-1})$, and $x - y^d$. All the rows of the RREF of M_d correspond to polynomials of degree d, therefore

$$\mathrm{rowsp}(M_d) = \langle x - y^{d-1}, x(x - y^{d-1}), y(x - y^{d-1}), x - y^d \rangle.$$

In particular, $xf \notin \mathrm{rowsp}(M_d)$ since it contains the monomial $x^2 y$ in its support.

2. Equivalent definitions for the last fall degree

In this section, we explore some properties of the last fall degree and use them to give different definitions for this and compare them to each other. We start by observing that, by Definition 1.5, one has

$$V_{\mathcal{F},d} = (\mathcal{F})_{\leq d}$$

for any polynomial system $\mathcal{F} \subseteq R$ and any $d \geq d_{\mathcal{F}}$.

Proposition 2.1. *One has*

$$V_{\mathcal{F},d_{\mathcal{F}}-1} \neq (\mathcal{F})_{\leq d_{\mathcal{F}}-1}.$$

In particular

$$d_{\mathcal{F}} = \min\{d \mid V_{\mathcal{F},e} = (\mathcal{F})_{\leq e} \text{ for all } e \geq d\}.$$

Proof. By Definition 1.5 there exists $f \in (\mathcal{F})$ such that $f \notin V_{\mathcal{F},\max\{d_{\mathcal{F}}-1,\deg(f)\}}$. If $\deg(f) \geq d_{\mathcal{F}}$, then $f \in V_{\mathcal{F},\deg(f)}$ by Definition 1.5. This contradicts the assumption that $f \notin V_{\mathcal{F},\max\{d_{\mathcal{F}}-1,\deg(f)\}} = V_{\mathcal{F},\deg(f)}$. Therefore $\deg(f) \leq d_{\mathcal{F}} - 1$. Then $f \in (\mathcal{F})_{\leq d_{\mathcal{F}}-1}$ and $f \notin V_{\mathcal{F},d_{\mathcal{F}}-1}$, in particular $V_{\mathcal{F},d_{\mathcal{F}}-1} \neq (\mathcal{F})_{\leq d_{\mathcal{F}}-1}$. $\square$

Remark 2.2. The same polynomial f as in the proof of Proposition 2.1 satisfies $f \notin V_{\mathcal{F},d}$ for any $d \leq d_{\mathcal{F}} - 1$, since $V_{\mathcal{F},d} \subseteq V_{\mathcal{F},d_{\mathcal{F}}-1}$. Therefore, for any $\deg(f) \leq d \leq d_{\mathcal{F}} - 1$ one has

$$V_{\mathcal{F},d} \neq (\mathcal{F})_{\leq d}.$$

Notice that the definition of last fall degree from Proposition 2.1 is not computationally more efficient than Definition 1.5. In fact, the standard way of computing $(\mathcal{F})_{\leq d}$ is by computing a (part of a) Gröbner basis of $\mathcal{F}$.

We now discuss another equivalent definition of last fall degree, coming from [14]. In [14, Proposition 2.6] it is shown that

$$d_{\mathcal{F}} = \min\{d \in \mathbb{N} \mid V_{\mathcal{F},e} = V_{\mathcal{F},e+1} \cap R_{\leq e} \text{ for all } e \geq d\}.$$

We now study the set of d's such that $V_{\mathcal{F},d} = V_{\mathcal{F},d+1} \cap R_{\leq d}$.

Proposition 2.3. *Let $d \in \mathbb{N}$. If $V_{\mathcal{F},d} = (\mathcal{F})_{\leq d}$, then $V_{\mathcal{F},d} = V_{\mathcal{F},d+1} \cap R_{\leq d}$. In other words,*

$$(2) \qquad \{d \in \mathbb{N} \mid V_{\mathcal{F},d} = (\mathcal{F})_{\leq d}\} \subseteq \{d \in \mathbb{N} \mid V_{\mathcal{F},d} = V_{\mathcal{F},d+1} \cap R_{\leq d}\}.$$

Proof. If $V_{\mathcal{F},d} = (\mathcal{F})_{\leq d}$, then

$$V_{\mathcal{F},d} = (\mathcal{F}) \cap R_{\leq d} = ((\mathcal{F}) \cap R_{\leq d+1}) \cap R_{\leq d} \supseteq V_{\mathcal{F},d+1} \cap R_{\leq d} \supseteq V_{\mathcal{F},d}$$

where the last inclusion holds for all d by Definition 1.5. $\square$

Since the equality $V_{\mathcal{F},d} = V_{\mathcal{F},d+1} \cap R_{\leq d}$ can be checked for any given d by checking whether $\mathrm{rowsp}(M_{d+1}) \cap R_{\leq d} = \mathrm{rowsp}(M_d)$, one may think that the definition from [14, Proposition 2.6] is more computationally friendly than that from Proposition 2.1. Unfortunately, one cannot hope to compute $d_{\mathcal{F}}$ by progressively increasing the value of d until one finds a d for which $V_{\mathcal{F},d} = V_{\mathcal{F},d+1} \cap R_{\leq d}$. In fact, in Example 2.4 we show that there are values of d for which $V_{\mathcal{F},d-1} = V_{\mathcal{F},d} \cap R_{\leq d-1}$ but $V_{\mathcal{F},d} \neq V_{\mathcal{F},d+1} \cap R_{\leq d}$.

Notice moreover that, while the definition from Proposition 2.1 and that from [14, Proposition 2.6] are equivalent, the inclusion in (2) may be strict. Even if $[d_{\mathcal{F}}, +\infty)$ is the largest right-unbounded interval contained in either of the sets from (2), each of the two sets can contain smaller values of $d \in \mathbb{N}$. The next example shows that this can indeed occur.

Example 2.4. Let $\mathcal{F} = \{x^2 - x, xy - 1, w^6 - w, w^5 z^5 - 1\} \subseteq R = k[w, x, y, z]$ with char $k = 0$ or char $k \gg 0$. It is easy to check that $(\mathcal{F}) = (x - 1, y - 1, w^5 - 1, z^5 - 1)$. Since $\mathcal{F}$ contains no elements of degree 0 or 1, then

$$V_{\mathcal{F},0} = V_{\mathcal{F},1} = 0.$$

Moreover

$$V_{\mathcal{F},2} = \langle x^2 - x, xy - 1 \rangle,$$

since the Macaulay matrix associated to $\mathcal{F}$ in degree 2 with respect to a degree-compatible term order is in RREF and contains only rows of degree 2. By repeatedly performing Gaussian elimination and adding rows whenever the matrix contains new rows of degree smaller than 3, one can check that $x - 1, y - 1 \in V_{\mathcal{F},3}$, hence

$$V_{\mathcal{F},3} \supseteq (x - 1)R_{\leq 2} + (y - 1)R_{\leq 2} = (\mathcal{F})_{\leq 3}.$$

Therefore

$$V_{\mathcal{F},d} = V_{\mathcal{F},d+1} \cap R_{\leq d}$$

for $d = 0, 1$, but

$$x - 1, y - 1 \in (V_{\mathcal{F},3} \cap R_{\leq 2}) \setminus V_{\mathcal{F},2}.$$

Since $(\mathcal{F})_{\leq 4} = (x - 1, y - 1)_{\leq 4}$, then

$$V_{\mathcal{F},3} = V_{\mathcal{F},4} \cap R_{\leq 3}.$$

One can also check that $V_{\mathcal{F},5} = V_{\mathcal{F},4} \cdot R_{\leq 1}$, hence

$$V_{\mathcal{F},4} = V_{\mathcal{F},5} \cap R_{\leq 4}.$$

Notice moreover that, for $0 \leq d \leq 5$ one has

$$V_{\mathcal{F},d} = (\mathcal{F})_{\leq d} \text{ if and only if } d \neq 1, 2, 5.$$

Now $V_{\mathcal{F},6} = V_{\mathcal{F},5} + \langle w^6 - w \rangle$ and $V_{\mathcal{F},d} = V_{\mathcal{F},6} \cdot R_{\leq d-6}$ for $6 \leq d \leq 9$. Finally, $V_{\mathcal{F},10} = V_{\mathcal{F},9} + \langle w^5 z^5 - 1 \rangle$. Therefore

$$V_{\mathcal{F},d} = V_{\mathcal{F},d+1} \cap R_{\leq d}$$

for $5 \leq d \leq 9$. Moreover, one can check that $w^5 - 1 \notin V_{\mathcal{F},d}$ for $d \leq 10$, hence

$$V_{\mathcal{F},d} \neq (\mathcal{F})_{\leq d} \text{ for } 6 \leq d \leq 10.$$

One can verify by direct computation that $w^5 - 1, z^5 - 1 \in V_{\mathcal{F}_{11}}$. Therefore

$$V_{\mathcal{F},10} \neq V_{\mathcal{F},11} \cap R_{\leq 10}.$$

Moreover,

$$V_{\mathcal{F},d} = (\mathcal{F})_{\leq d} \text{ for } d \geq 11,$$

therefore also

$$V_{\mathcal{F},d} = V_{\mathcal{F},d+1} \cap R_{\leq d} \text{ for } d \geq 11.$$

In fact, this shows that $d_{\mathcal{F}} = 11$. In the next table, we summarize for which values of d each equality holds.

d	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$V_{\mathcal{F},d} = V_{\mathcal{F},d+1} \cap R_{\leq d}$	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	...
$V_{\mathcal{F},d} = (\mathcal{F})_{\leq d}$	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	...

2.1. **Degree falls and last fall degree.** In this subsection, we give a mathematical formulation for the notion of degree falls. This allows us to prove that the last fall degree is the largest degree in which a degree fall occurs. This is also the largest degree for which a degree fall occurs for an element of a Gröbner basis. We start by defining degree falls.

Definition 2.5. Let $\mathcal{F} \subseteq R$ be a polynomial system. For any $f \in (\mathcal{F})$ let

$$d_f = \min\{d \in \mathbb{N} : f \in V_{\mathcal{F},d}\}.$$

We always have that $d_f \geq \deg(f)$.

Definition 2.6. If $d_f > \deg(f)$, then we say that f has a **degree fall** in degree d_f. We say that $\mathcal{F}$ has a **degree fall** if there is an $f \in (\mathcal{F})$ such that f has a degree fall. Else we say that $\mathcal{F}$ has **no degree falls**.

For example, a homogeneous system has no degree falls. Moreover, its last fall degree is zero. More in general, one can prove the following.

Lemma 2.7. *Let $\mathcal{F} \subseteq R$ be a polynomial system. Then $\mathcal{F}$ has no degree falls if and only if $d_{\mathcal{F}} = 0$.*

Proof. If $d_{\mathcal{F}} = 0$, then for all $f \in (\mathcal{F})$ we have $f \in V_{\mathcal{F},\deg(f)}$. Therefore $\mathcal{F}$ has no degree falls. Conversely, assume that $\mathcal{F}$ has no degree falls. Let σ be a degree-compatible term order and let $\{g_1, \ldots, g_s\}$ be a Gröbner basis of $(\mathcal{F})$ with respect to σ. Let $f \in (\mathcal{F})$. Since σ is degree-compatible, f can be written as

$$f = \sum_{i=1}^{s} h_i g_i$$

for some $h_i \in R$ with $\deg(h_i g_i) \leq \deg(f)$. For any g_i such that $h_i \neq 0$, we have the following: Since $g_i \in V_{\mathcal{F},\deg(g_i)} \subseteq V_{\mathcal{F},\deg(f)}$ and $h_i \in R_{\leq \deg(f)-\deg(g_i)}$, then $h_i g_i \in V_{\mathcal{F},\deg(f)}$. It follows that $f \in V_{\mathcal{F},\deg(f)}$, hence $d_{\mathcal{F}} = 0$. $\square$

We now can prove that the last fall degree is the largest degree in which a degree fall occurs.

Theorem 2.8. *Let $\mathcal{F} \subseteq R$ be a polynomial system. If $\mathcal{F}$ has a degree fall, then*

$$d_{\mathcal{F}} = \max\{d_f : f \in (\mathcal{F}), d_f > \deg(f)\}.$$

Proof. Let $f \in \mathcal{F}$. If $d_f > \deg(f)$, then $f \notin V_{\mathcal{F},d}$ for any $d < d_f$. In particular, $d_{\mathcal{F}} > d_f - 1$ by the definition of last fall degree. This implies that

$$d_{\mathcal{F}} \geq \sup\{d_f : f \in (\mathcal{F}), d_f > \deg(f)\}.$$

Notice that, by the finiteness of the last fall degree, the supremum of the set $\{d_f :\ f \in (\mathcal{F}), d_f > \deg(f)\}$ is in fact a maximum.

We now prove the reverse inequality. Let $\mu = \max\{d_f :\ f \in (\mathcal{F}), d_f > \deg(f)\}$ and fix $f \in (\mathcal{F})$. If $d_f > \deg(f)$ we have $f \in V_{\mathcal{F},d_f} \subseteq V_{\mathcal{F},\mu}$ and $\mu = \max\{\mu, \deg(f)\}$ since $\mu \geq d_f > \deg(f)$. If $d_f = \deg(f)$, then $f \in V_{\mathcal{F},\deg(f)} \subseteq V_{\mathcal{F},\max\{\mu,\deg(f)\}}$. Therefore, for all $f \in (\mathcal{F})$, $f \in V_{\mathcal{F},\max\{\mu,\deg(f)\}}$, so $\mu \in \{d \in \mathbb{N} \cup \{\infty\} \mid f \in V_{\mathcal{F},\max\{d,\deg(f)\}} \text{ for all } f \in (\mathcal{F})\}$. It follows that $d_{\mathcal{F}} \leq \mu$. $\qquad\square$

It is worth noticing that the last fall degree is the largest degree of a degree fall occuring for an element of a Gröbner basis of $\mathcal{F}$ with respect to a degree-compatible term order.

Theorem 2.9. *Let $\mathcal{F} \subseteq R$ be a polynomial system, and let $\{g_1, \dots, g_s\}$ be a Gröbner basis of $\mathcal{F}$ with respect to a degree compatible term order. If $\mathcal{F}$ has a degree fall, then*
$$d_{\mathcal{F}} = \max\{d_{g_i} :\ \deg(g_i) < d_{g_i}\}.$$

Proof. Up to reordering, we may assume without loss of generality that $\{g_1, \dots, g_t\}$ are a minimal Gröbner basis of $\mathcal{F}$ for some $t \leq s$. Let $\delta_{\mathcal{F}} = \max\{d_{g_i} : d_{g_i} > \deg(g_i), 1 \leq i \leq t\}$. Then
$$d_{\mathcal{F}} = \max\{d_f :\ f \in (\mathcal{F}), d_f > \deg(f)\}$$
$$\geq \max\{d_{g_i} : d_{g_i} > \deg(g_i), 1 \leq i \leq s\} \geq \delta_{\mathcal{F}},$$
where the first equality follows from Theorem 2.8. Therefore, it suffices to show that the statement holds for $\{g_1, \dots, g_t\}$ a minimal Gröbner basis.

To prove the reverse inequality, let $f \in (\mathcal{F})$ and write
$$f = \sum_{i \in J} h_i g_i$$
with $J \subseteq \{1, \dots, t\}$, $\deg(h_i) \leq \deg(f) - \deg(g_i)$ and $h_i \neq 0$ for all $i \in J$. Fix $i \in J$ and let $u_i = \max\{\deg(f), d_{g_i}\}$. Then $g_i \in V_{\mathcal{F},d_{g_i}} \subseteq V_{\mathcal{F},u_i}$ and $h_i \in R_{\leq \deg(f)-\deg(g_i)} \subseteq R_{\leq u_i - \deg(g_i)}$. It follows that $h_i g_i \in V_{\mathcal{F},u_i}$. Therefore $f \in V_{\mathcal{F},\max\{\deg(f),d_{g_i}:i\in J\}}$. Notice that if $i \in J$ and $\deg(g_i) = d_{g_i}$, then $d_{g_i} \leq \deg(f)$. Therefore
$$\max\{\deg(f), d_{g_i} :\ i \in J\} \leq \max\{\deg(f), \delta_{\mathcal{F}}\} \ \text{ and } \ f \in V_{\mathcal{F},\max\{\deg(f),\delta_{\mathcal{F}}\}}.$$
This shows that $d_{\mathcal{F}} \leq \delta_{\mathcal{F}}$. $\qquad\square$

Remark 2.10. Theorem 2.9 implies that the largest degree of a degree fall occuring for an element of a Gröbner basis of $\mathcal{F}$ with respect to a degree-compatible term order σ is independent of the choice of σ and of the Gröbner basis.

3. Solving degree and last fall degree

It is clear by definition that the solving degree of a system with respect to a fixed term order is bounded from below by the largest degree of an element of a Gröbner basis with respect to that term order. In addition, in [13, Theorem 1] it was proved that the solving degree with respect to a degree-compatible term order is bounded from below by

the last fall degree. The next theorem clarifies the relation between the last fall degree and the solving degree, by providing a direct comparison. From a computational point of view, the theorem allows us to split estimates for the solving degree in two parts: an estimate on the degrees of the elements in a reduced Gröbner basis and an estimate on the last fall degree. Notice that, while the degrees of the elements in a Gröbner basis depend on the choice of the order and on the system of coordinates, the last fall degree does not.

Theorem 3.1. *Let $\mathcal{F} \subseteq R$ be a polynomial system. Let σ be a degree-compatible term order. Then*

$$\mathrm{sd}_\sigma(\mathcal{F}) = \max\{d_\mathcal{F}, \max.\,\mathrm{GB.\,deg}_\sigma(\mathcal{F})\}.$$

Proof. If $\mathcal{F}$ is homogeneous, then $d_\mathcal{F} = 0$. The thesis follows from observing that $\mathrm{sd}_\sigma(\mathcal{F}) = \max.\,\mathrm{GB.\,deg}_\sigma(\mathcal{F})$, whenever $\mathcal{F}$ is homogeneous.

Suppose now that $\mathcal{F}$ is not homogeneous. The inequality $\mathrm{sd}_\sigma(\mathcal{F}) \geq d_\mathcal{F}$ follows from [13, Theorem 1]. From the definition of solving degree, $\mathrm{sd}_\sigma(\mathcal{F}) \geq \max.\,\mathrm{GB.\,deg}_\sigma(\mathcal{F})$. Therefore, it suffices to show that $\mathrm{sd}_\sigma(\mathcal{F}) \leq \max\{d_\mathcal{F}, \max.\,\mathrm{GB.\,deg}_\sigma(\mathcal{F})\}$. Let $\mathrm{rowsp}(M_d)$ be the vector space generated by the rows of the matrix obtained from the Macaulay matrix M in degree d after applying the algorithm described in Section 1. By [13, Theorem 1], $\mathrm{rowsp}(M_d) = V_{\mathcal{F},d}$ for every $d \in \mathbb{N}$.

Let $D = \max\{d_\mathcal{F}, \max.\,\mathrm{GB.\,deg}_\sigma(\mathcal{F})\}$. Then

$$\mathrm{rowsp}(M_D) = V_{\mathcal{F},D} = (\mathcal{F}) \cap R_{\leq D},$$

where the second equality follows from the definition of last fall degree, since $D \geq d_\mathcal{F}$. Let g be an element of the reduced Gröbner basis of $\mathcal{F}$ with respect to σ. Then $g \in \mathrm{rowsp}(M_D)$, therefore g is a linear combination of the rows of the matrix M_D obtained from the Macaulay matrix in degree D after applying the algorithm from Section 1. Since M_D is in reduced row-echelon form, the leading terms of the rows of M_D are pairwise distinct.

We claim that, up to scalar multiples, g is a row of M_D. In fact, if g is a combination of more than one row, since M_D is in reduced row-echelon form, then g contains in its support one or more monomials that appear as leading term of a row of M_D, beyond its leading term. However this is impossible, since g is an element of a reduced Gröbner basis and each row of M_D corresponds to an element of $(\mathcal{F})$, hence its leading term is divisible by a leading term of an elements of the reduced Gröbner basis. Hence a scalar multiple of g appears among the rows of M_D, so $\mathrm{sd}_\sigma(\mathcal{F}) \leq D$. $\square$

Remark 3.2. Notice that while $\mathrm{sd}_\sigma(\mathcal{F})$ and $\max.\,\mathrm{GB.\,deg}_\sigma(\mathcal{F})$ depend in general on the term order σ and on the system of coordinates, the last fall degree of $\mathcal{F}$ does not depend on either of them.

The next example shows that the conclusion of Theorem 3.1 is in general false for term orders which are not degree-compatible.

Example 3.3 ([13], Example 2)**.** Let $d \geq 2$ be an integer. Let $\mathcal{F} = \{x_0 - x_0 x_2^{d-1}, x_1 - x_2^d\}$ and let σ be the lexicographic order on $k[x_0, x_1, x_2]$ with $x_0 > x_1 > x_2$. The elements of

$\mathcal{F}$ are a Gröbner basis of the ideal that they generate and $\mathrm{sd}_\sigma(\mathcal{F}) = d$. Let

$$f = x_0x_2 - x_0x_1 = x_2(x_0 - x_0x_2^{d-1}) - x_0(x_1 - x_2^d) \in V_{\mathcal{F},d+1}.$$

Since $f \notin V_{\mathcal{F},d} = \langle x_0 - x_0x_2^{d-1}, x_1 - x_2^d \rangle$, then $d_{\mathcal{F}} \geq d + 1$. Therefore

$$\mathrm{sd}_\sigma(\mathcal{F}) = d < \max\{d_{\mathcal{F}}, \max. \mathrm{GB}. \deg_\sigma(\mathcal{F})\}.$$

4. How does the first fall degree relate to the other invariants?

The first fall degree is used by many authors as an estimate for the solving degree. While this is justified by a heuristic argument, this does not always provide a reliable estimate. In fact, it is easy to produce examples where the first fall degree and the solving degree are far apart, see [8]. In this section, we explore further the relation of the first fall degree with the other algebraic invariants related to the solving degree. We provide examples that show that the following are possible:

- $d_{\mathrm{ff}}(\mathcal{F}) > \mathrm{sd}(\mathcal{F})$ or $d_{\mathrm{ff}}(\mathcal{F}) < \mathrm{sd}(\mathcal{F})$,
- $d_{\mathrm{ff}}(\mathcal{F}) < d_{\mathcal{F}}$ or $d_{\mathrm{ff}}(\mathcal{F}) > d_{\mathcal{F}}$,
- $d_{\mathrm{ff}}(\mathcal{F}) > d_{\mathrm{reg}}(\mathcal{F})$ or $d_{\mathrm{ff}}(\mathcal{F}) < d_{\mathrm{reg}}(\mathcal{F})$,
- $d_{\mathrm{ff}}(\mathcal{F}) > \mathrm{reg}(\mathcal{F}^h)$ or $d_{\mathrm{ff}}(\mathcal{F}) < \mathrm{reg}(\mathcal{F}^h)$,

In addition, our examples show that the difference between the first fall degree and each of the other invariants can be positive or negative and arbitrarily large in absolute value.

Example 4.1. Let $q > 3$ be odd. Fix any degree-compatible term order. Then $\mathcal{F} = \{x_1x_2 + x_2, x_2^2 - 1, x_1^{q-1} - 1\} \subseteq \mathbb{F}_q[x_1, x_2]$ has Gröbner basis $\{x_1 + 1, x_2^2 - 1\}$. One can compute

$$\mathcal{F}^{\mathrm{top}} = \{x_1x_2, x_2^2, x_1^{q-1}\},$$

with non-trivial syzygies $(x_2, -x_1, 0), (x_1^{q-2}, 0, -x_2), (0, x_2^{q-2}, 0), (0, 0, x_1)$. Since $\mathcal{F}^{\mathrm{top}}$ has no syzygies in degree smaller than 3, then $d_{\mathrm{ff}}(\mathcal{F})$. One can show by direct computation that $\mathrm{sd}(\mathcal{F}) = 3$. Then $d_{\mathcal{F}} = 3$ by Theorem 3.1.

Let x_0 be the homogenizing variable and consider $S = \mathbb{F}_q[x_0, x_1, x_2]$. The regularity of $\mathcal{F}^h$ can be obtained from its minimal free resolution

$$0 \to S(-q-2) \to \begin{matrix} S(-q-1) \\ \oplus \\ S(-q) \\ \oplus \\ S(-4) \end{matrix} \to \begin{matrix} S(-q+1) \\ \oplus \\ S(-2)^2 \end{matrix} \to (\mathcal{F}^h) \to 0$$

where $\{x_1x_2 + x_2x_0, x_2^2 - x_0^2, x_1^{q-1} - x_0^{q-1}, x_1x_0^2 + x_0^3\}$ is a Gröbner basis with respect to the degree reverse lexicographic term order with $x_1 > x_2 > x_0$. A minimal system of generators of the first syzygy module of $x_1^{q-1} - x_0^{q-1}, x_1x_2 + x_2x_0, x_2^2 - x_0^2$ is

$$\left\{ \left(x_2, \sum_{j=0}^{q-3} (-1)^{j+1}x_0^jx_1^{q-2-j}, 0 \right), (-x_2^2 + x_0^2, 0, x_1^{q-1} - x_0^{q-1}), (0, -x_2^2 + x_0^2, x_1x_2 + x_2x_0) \right\}$$

and the second syzygy module is $\langle (-x_2^2 + x_0^2, -x_2, \sum_{j=0}^{q-3}(-1)^{j+1}x_0^j x_1^{q-2-j}) \rangle$. Therefore we have shown that

$$d_{\mathrm{ff}}(\mathcal{F}) = \mathrm{sd}(\mathcal{F}) = d_{\mathcal{F}} = 3 < q - 1 = d_{\mathrm{reg}}(\mathcal{F}) < q = \mathrm{reg}(\mathcal{F}^h).$$

Example 4.2. Let $q > 3$ be odd. Fix any degree-compatible term order. Then $\mathcal{F} = \{x_1 x_2 + x_2, x_2^2 - 1, x_3^{q-1} - 1\} \subseteq \mathbb{F}_q[x_1, x_2, x_3]$ has Gröbner basis $\{x_1 + 1, x_2^2 - 1, x_3^{q-1} - 1\}$. One can compute

$$\mathcal{F}^{\mathrm{top}} = \{x_1 x_2, x_2^2, x_3^{q-1}\},$$

with non-trivial syzygies $(x_2, -x_1, 0), (0, x_2^{q-2}, 0), (0, 0, x_3)$. Since $\mathcal{F}^{\mathrm{top}}$ has no syzygies in degree smaller than 3, then $d_{\mathrm{top}}(\mathcal{F}) = 3$. The Macaulay matrix of $\mathcal{F}$ in degree 2 is already in RREF, therefore $x_1 + 1 \notin V_{\mathcal{F},2}$. Hence there is a degree fall in degree 3, as $x_1 + 1 = x_2(x_1 x_2 + x_2) - (1 + x_1)(x_2^2 - 1) \in V_{\mathcal{F},3}$. Since $\{x_1 + 1, x_2^2 - 1, x_3^{q-1} - 1\}$ are a Gröbner basis of $(\mathcal{F})$, then this is the only degree fall. It follows from Theorem 2.8 that $d_{\mathcal{F}} = 3$. Moreover, the solving degree is $q - 1$ by Theorem 3.1.

Let x_0 be the homogenizing variable and consider the degree reverse lexicographic order on $S = \mathbb{F}_q[x_0, x_1, x_2, x_3]$ with $x_3 > x_1 > x_0 > x_2$. The three polynomials in $\mathcal{F}^h$ have pairwise coprime leading terms, hence they are a regular sequence and $\mathrm{reg}(\mathcal{F}^h) = q + 1$. The degree of regularity of $\mathcal{F}$ can be computed directly from the Hilbert series of $\mathcal{F}^{\mathrm{top}}$. Therefore we have

$$d_{\mathrm{ff}}(\mathcal{F}) = d_{\mathcal{F}} = 3 < q - 1 = \mathrm{sd}(\mathcal{F}) < q = d_{\mathrm{reg}}(\mathcal{F}) < q + 1 = \mathrm{reg}(\mathcal{F}^h).$$

Example 4.3. Let $q \geq 3$ be a prime power, let $\mathcal{F} = \{(x_1 + x_2)^2, x_1 x_2 + x_3^2 + x_4\} \subseteq R = \mathbb{F}_q[x_1, \ldots, x_4]$. Since $(x_1 + x_2)^2, x_1 x_2 - x_3^2$ are a regular sequence, $\mathcal{F}^{\mathrm{top}}$ has only trivial syzygies in R. Therefore, every non-trivial syzygy of $\mathcal{F}^{\mathrm{top}}$ in $B = R/(x_1^q, \ldots, x_4^q)$ has degree at least q. Since $((x_1 + x_2)^{q-2}, 0)$ is a non-trivial syzygy of degree q of $\mathcal{F}^{\mathrm{top}}$ in B, then $d_{\mathrm{ff}}(\mathcal{F}) = q$.

The elements g_1, g_2 of $\mathcal{F}$ are a Gröbner basis with respect to DRL with $x_3 > x_1, x_2, x_4$, since their leading terms are a regular sequence. Therefore, any $f \in (\mathcal{F})$ can be written as $f = h_1 g_1 + h_2 g_2$ for some $h_1, h_2 \in R$ with $\deg(h_1 g_1), \deg(h_2 g_2) \leq \deg(f)$. It follows that $f \in V_{\mathcal{F}, \deg(f)}$ for every $f \in (\mathcal{F})$, hence $d_{\mathcal{F}} = 0$ by Lemma 2.7. Since $\max. \mathrm{GB}. \deg(\mathcal{F}) = 2$, then $\mathrm{sd}(\mathcal{F}) = 2$ by Theorem 3.1.

The degree of regularity of $\mathcal{F}$ may be computed by observing that $x_0 \nmid 0$ modulo $(\mathcal{F}^h)$, where x_0 is the homogenizing variable. Hence $d_{\mathrm{reg}}(\mathcal{F}) = \mathrm{reg}(\mathcal{F}^h) = 3$, since $\mathcal{F}^{\mathrm{top}}$ is a regular sequence. Therefore

$$d_{\mathcal{F}} = 0 < 2 = \mathrm{sd}(\mathcal{F}) < \mathrm{reg}(\mathcal{F}^h) = d_{\mathrm{reg}}(\mathcal{F}) = 3 < q = d_{\mathrm{ff}}(\mathcal{F}).$$

Example 4.4. Let $\mathcal{F} = \{x^2 - x, xy - 1, w^q - w, w^{q-1}z^{q-1} - 1\} \subseteq R = \mathbb{F}_q[w, x, y, z]$, $q \neq 2$. It is easy to check that $\{x - 1, y - 1, w^{q-1} - 1, z^{q-1} - 1\}$ is a Gröbner basis of $(\mathcal{F})$ with respect to any term order. The element $(y, -x, 0, 0)$ is a non-trivial syzygy of $\mathcal{F}^{\mathrm{top}} = \{x^2, xy, w^q, w^{q-1}z^{q-1}\}$ of degree 3. Since $\mathcal{F}^{\mathrm{top}}$ has no syzygy in degree smaller than 3, then $d_{\mathrm{ff}}(\mathcal{F}) = 3$.

One can verify by direct computation that $w^{q-1} - 1, z^{q-1} - 1 \in V_{\mathcal{F}, 2q-1} \setminus V_{\mathcal{F}, 2q-2}$, see also Example 2.4. Therefore $\mathrm{sd}(\mathcal{F}) = 2q - 1$, hence also $d_{\mathcal{F}} = 2q - 1$ by Theorem 3.1.

Hence we have
$$d_{\mathrm{ff}}(\mathcal{F}) = 3 < 2q - 1 = \mathrm{sd}(\mathcal{F}) = d_{\mathcal{F}}.$$

5. Degree of regularity and Castelnuovo–Mumford regularity

Both the degree of regularity and the Castelnuovo–Mumford regularity provide upper bounds on the solving degree of a system of polynomial equations. The main result of this section is an inequality between the degree of regularity and the Castelnuovo–Mumford regularity.

The following relation between the solving degree of a system $\mathcal{F}$ of polynomial equations and the Castelnuovo–Mumford regularity of the system $\mathcal{F}^h$ obtained from $\mathcal{F}$ by homogenizing its equations with respect to a new variable was proved in [4]. In case $\mathcal{F}$ is homogeneous, then $\mathcal{F}^h = \mathcal{F}$.

Theorem 5.1 ([4], Theorem 9, Theorem 10, and Theorem 11). *Let $\mathcal{F} \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial system which contains the field equations. Then*
$$\mathrm{sd}(\mathcal{F}) \leq \mathrm{reg}(\mathcal{F}^h).$$

The next result was proved by Semaev and Tenti. To the extent of our knowledge, this is the first proven upper bound for the solving degree of a system in terms of its degree of regularity. Notice however that the solving degree considered by Semaev and Tenti may be different from the one considered in this paper, as Semaev and Tenti work in the quotient ring $\mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q - x_1, \ldots, x_n^q - x_n)$. For more details see the doctoral thesis of Tenti [19], in particular the discussion above [18, Theorem 2.1] and [19, Corollary 3.67].

Theorem 5.2 ([18], Theorem 2.1). *Let $\mathcal{F} = \{f_1, \ldots, f_r, x_1^q - x_1, \ldots, x_n^q - x_n\} \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial system. If $d_{\mathrm{reg}}(\mathcal{F}) \geq \max\{q, \deg(f_1), \ldots, \deg(f_r)\}$, then*
$$\mathrm{sd}(\mathcal{F}) \leq 2d_{\mathrm{reg}}(\mathcal{F}) - 2.$$

Because of Theorem 5.1 and Theorem 5.2, both the degree of regularity of $\mathcal{F}$ and the Castelnuovo–Mumford regularity of $\mathcal{F}^h$ produce estimates for the solving degree of $\mathcal{F}$. Hence it is interesting to relate these invariants to each other.

Theorem 5.3. *Let $\mathcal{F} \subseteq R = k[x_1, \ldots, x_n]$ be a polynomial system. One has*
$$d_{\mathrm{reg}}(\mathcal{F}) \leq \mathrm{reg}(\mathcal{F}^h).$$

Proof. Since $d_{\mathrm{reg}}(\mathcal{F}) \leq \mathrm{reg}_R(\mathcal{F}^{\mathrm{top}})$ for any $\mathcal{F}$ by [4, (4) pg. 26], it suffices to show that $\mathrm{reg}_R(\mathcal{F}^{\mathrm{top}}) \leq \mathrm{reg}_S(\mathcal{F}^h)$. Write $(\mathcal{F}^h) = J + tH$ where $t \nmid 0$ modulo J. Then $(\mathcal{F}^h) : t = J + H$ and $S/(\mathcal{F}^h) + (t) = S/(\mathcal{F}^{\mathrm{top}}) + (t) \cong R/(\mathcal{F}^{\mathrm{top}})$. Therefore
$$\mathrm{reg}_R(\mathcal{F}^{\mathrm{top}}) = \mathrm{reg}_S((\mathcal{F}^{\mathrm{top}}) + (t)).$$
Moreover, one has the short exact sequence
$$0 \to S/J + H(-1) \to S/(\mathcal{F}^h) \to S/(\mathcal{F}^{\mathrm{top}}) + (t) \to 0.$$

By the Mapping Cone Construction one has that

$$(3) \qquad \operatorname{reg}_S((\mathcal{F}^{\mathrm{top}}) + (t)) \leq \max\{\operatorname{reg}_S(\mathcal{F}^h), \operatorname{reg}_S(J + H)\}.$$

Moreover, by [3, Theorem 3.1]

$$\operatorname{reg}_S(\mathcal{F}^h) \in \{\operatorname{reg}_S((\mathcal{F}^{\mathrm{top}}) + (t)), \operatorname{reg}_S(H + J) + 1\}.$$

If $\operatorname{reg}_S(\mathcal{F}^h) = \operatorname{reg}_S(H+J)+1$, then by (3) $\operatorname{reg}_S((\mathcal{F}^{\mathrm{top}})+(t)) \leq \operatorname{reg}_S(H+J)+1 = \operatorname{reg}_S(\mathcal{F}^h)$.
If $\operatorname{reg}_S(\mathcal{F}^h) \neq \operatorname{reg}_S(H + J) + 1$, then by (3) $\operatorname{reg}_S((\mathcal{F}^{\mathrm{top}}) + (t)) = \operatorname{reg}_S(\mathcal{F}^h)$. □

The first inequality in the next corollary was already observed in [19, Section 3.3.2].

Corollary 5.4. *Assume that $\mathcal{F}$ contains the field equations and that $d_{\mathrm{ff}}(\mathcal{F}) \neq +\infty$. Then*

$$d_{\mathrm{ff}}(\mathcal{F}) \leq d_{\mathrm{reg}}(\mathcal{F}) + 1 \leq \operatorname{reg}(\mathcal{F}^h) + 1.$$

Proof. The first fall degree is the minimum degree of a syzygy of $\mathcal{F}^{\mathrm{top}}$ which does not belong to the submodule of trivial syzygies. Therefore, it is a minimal generator of the syzygy module of $\mathcal{F}^{\mathrm{top}}$. This proves that $d_{\mathrm{ff}}(\mathcal{F}) \leq \operatorname{reg}(\mathcal{F}^{\mathrm{top}})+1$. Moreover, $\operatorname{reg}(\mathcal{F}^{\mathrm{top}})+1 \leq \operatorname{reg}(\mathcal{F}^h) + 1$ by the previous theorem. □

REFERENCES

1. M. Bardet, *Étude des systémes algébriques surdéterminés. Applications aux codes correcteurs et á la cryptographie*, Ph.D. thesis, Université Paris 6, 2004.
2. M. Bardet, J.-C. Faugère, B. Salvy, *On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations*, ICPPSS International Conference on Polynomial System Solving, 2004.
3. G. Caviglia, H.T. Hà, J. Herzog, M. Kummini, N. Terai, N.V. Trung, *Depth and regularity modulo a principal ideal*, J. Algebr. Comb. **49** (2019), 1–20.
4. A. Caminata, E. Gorla, *Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra*, Arithmetic of finite fields, 3–36, Lecture Notes in Comput. Sci., 12542, Springer, Cham, 2021.
5. N. Courtois, A. Klimov, J. Patarin, A. Shamir, *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, Proceedings of International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT), vol. 1807, Lecture Notes in Computer Science, 392–407, Springer Bruges, Belgium, 2000.
6. J. Ding, J. Buchmann, M. Mohamed, W. Moahmed, R.P. Weinmann, *MutantXL*, Proceedings of the 1st international conference on Symbolic Computation and Cryptography (SCC08), Beijing, China, LMIB, 16–22, 2008.
7. J. Ding, A. Petzold, D. Schmidt, *Multivariate Public Key Cryptosystems*, Adv. Information Security, Springer New York, NY, 2020.
8. J. Ding, D. Schmidt, *Solving degree and degree of regularity for polynomial systems over finite fields*, Number theory and cryptography, 34–49, Lecture Notes in Comput. Sci., 8260, Springer, Heidelberg, 2013.
9. V. Dubois, N. Gama, *The degree of regularity of HFE systems*, International Conference on the Theory and Application of Cryptology and Information Security, Springer, Berlin, Heidelberg, 2010.
10. J.C. Faugère, *A new efficient algorithm for computing Gröbner bases (F4)*, J. Pure Appl. Algebra **139** (1999), 61–88.
11. J.C. 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, 75–83, New York, NY, USA, 2002.
12. P. Gaudry, *Index calculus for Abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, J. Symbolic Comput. **44** (2009), 1690–1702.

13. E. Gorla, D. Müller, and C. Petit, *Stronger bounds on the cost of computing Gröbner bases for HFE systems*, J. Symbolic Comput. **109** (2022), 386–398.
14. M.-D. A. Huang, M. Kosters, Y. Yang, S. L. Yeo, *On the last fall degree of zero-dimensional Weil descent systems*, J. Symbolic Comput. **87** (2018), 207–226.
15. M.-D. A. Huang, M. Kosters, S. L. Yeo, *Last fall degree, HFE, and Weil descent attacks on ECDLP*, Advances in Cryptology – CRYPTO 2015, Springer-Verlag, 581–600, 2015.
16. Y.-J. Huang, C. Petit, N. Shinohara, T. Takagi, *On Generalized First Fall Degree Assumptions*, `https://eprint.iacr.org/2015/358`.
17. D. Lazard, *Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations*, Computer algebra (London, 1983), 146–156, Lecture Notes in Comput. Sci., vol. 162, Springer, Berlin, 1983.
18. I. Semaev, A. Tenti, *Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Gröbner bases*, J. Algebra **565** (2021), 651–674.
19. A. Tenti, *Sufficiently overdetermined random polynomial systems behave like semiregular ones*, PhD Thesis, University of Bergen (2019), available at `https://hdl.handle.net/1956/21158`.

Alessio Caminata, Dipartimento di Matematica, Università degli Studi di Genova, via Dodecaneso 35, 16146 Genova, Italy

Email address: `caminata@dima.unige.it`

Elisa Gorla, Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, 2000 Neuchâtel, Switzerland

Email address: `elisa.gorla@unine.ch`