The solving degrees for computing Gröbner bases of affine semi-regular polynomial sequences

Momonari Kudo* Kazuhiro Yokoyama†

July 5, 2024

Abstract

Determining the complexity of computing Gröbner bases is an important problem both in theory and in practice, and for that the solving degree plays a key role. In this paper, we study the solving degrees of affine semi-regular sequences and their homogenized sequences. Some of our results are considered to give mathematically rigorous proofs of the correctness of methods for computing Gröbner bases of the ideal generated by an affine semi-regular sequence. This paper is a sequel of the authors' previous work [30] and gives additional results on the solving degrees and important behaviors of Gröbner basis computation.

We also define the *generalized* degree of regularity for a sequence of homogeneous polynomials. For the homogenization of an affine semi-regular sequence, we relate its generalized degree of regularity with its maximal Gröbner basis degree (i.e., the solving degree of the homogenized sequence). The definition of a *generalized* (cryptographic) semi-regular sequence is also given, and it derives a new cryptographic assumption to estimate the security of cryptosystems. From our experimental observation, we raise a conjecture and some questions related to this generalized semi-regularity. These definitions and our results provide a theoretical formulation of (somehow heuristic) discussions done so far in the cryptographic community.

1 Introduction

Let K be a field, and let $\overline{K}$ denote its algebraic closure. We denote by $\mathbb{A}_K^n$ (resp. $\mathbb{P}_K^n$) the n-dimensional affine (resp. projective) space over K. Let $R = K[x_1, \ldots, x_n]$ be the polynomial ring in n variables over K. For a given monomial ordering $\prec$ on the set of monomials in R, let $\mathrm{LM}(f)$ denote the leading monomial of $f \in R \smallsetminus \{0\}$ with respect to it. For a non-empty subset $F \subset R \smallsetminus \{0\}$, put $\mathrm{LM}(F) := \{\mathrm{LM}(f) : f \in F\}$. A set F (resp. a sequence $\boldsymbol{F}$) of polynomials in R is said to be homogeneous if the elements of F (resp. $\boldsymbol{F}$) are all homogeneous, and otherwise F is said to be affine. We denote by $\langle F \rangle_R$ (or $\langle F \rangle$ simply) the ideal generated by a non-empty subset F of R. For a polynomial f in $R \smallsetminus \{0\}$, let f^{top} denote its maximal total degree part which we call the *top part* of f, and let f^h denote its homogenization in $R' = R[y]$ by an extra variable y, see Subsection A.2 below for details. For a sequence $\boldsymbol{F} = (f_1, \ldots, f_m) \in (R \smallsetminus \{0\})^m$, we also set $\boldsymbol{F}^{\mathrm{top}} := (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ and $\boldsymbol{F}^h := (f_1^h, \ldots, f_m^h)$. For a finitely generated graded R-(or

*Fukuoka Institute of Technology, 3-30-1 Wajiro-higashi, Higashi-ku, Fukuoka, 811-0295 Japan, m-kudo@fit.ac.jp
†Rikkyo University, 3-34-1 Nishi-Ikebukuro, Toshima-ku, Tokyo, 171-8501 Japan, kazuhiro@rikkyo.ac.jp

R'-)module M, we also denote by HF_M and HS_M its Hilbert function and its Hilbert–Poincaré series, respectively.

A *Gröbner basis* of an ideal I in R is defined as a special kind of generating set for I, and it gives a computational tool to determine many properties of I. A typical application of computing Gröbner bases is solving the multivariate polynomial (MP) problem: Given a sequence $\boldsymbol{F} = (f_1, \ldots, f_m)$ of m polynomials $f_1, \ldots, f_m$ in $R \smallsetminus \{0\}$, find $(a_1, \ldots, a_n) \in K^n$ such that $f_i(a_1, \ldots, a_n) = 0$ for all i with $1 \leq i \leq m$. A particular case where $f_1, \ldots, f_m$ are all quadratic is called the MQ problem, and its hardness is applied to constructing public-key cryptosystems that are expected to be quantum resistant. Therefore, analyzing the complexity of computing Gröbner bases is one of the most important problems both in theory and in practice.

An algorithm for computing Gröbner bases was proposed first by Buchberger [6], and so far a number of its improvements such as the F_4 [18] and F_5 [19] algorithms have been proposed. In determining the complexity of computing Gröbner bases, as we will see in the first paragraph of Subsection 2.2 below, one of the most important cases is the case where the input system is zero-dimensional and where the monomial ordering is graded (i.e., degree-compatible), and we focus on that case in the rest of this paper. Namely, we suppose that the input sequence $\boldsymbol{F} = (f_1, \ldots, f_m)$ admits a finite number of zeros in $\mathbb{A}^n_{\overline{K}}$ (resp. $\mathbb{P}^{n-1}_{\overline{K}}$) if $\boldsymbol{F}$ is affine (resp. homogeneous), and we consider a monomial ordering $\prec$ on R that compares monomials first by their total degrees, e.g., a degree reverse lexicographical (DRL) ordering. Then, the complexity of the Gröbner basis computation for $F = \{f_1, \ldots, f_m\}$ is estimated as a function of the *solving degree(s)*: To the authors' best knowledge, there are three (in fact four) kinds of definitions of solving degree, and they will be *rigorously* described in Subsection 2.2 below. In the first definition, the solving degree is defined as the highest degree of the polynomials involved during the Gröbner basis computation. Since this solving degree depends on an algorithm $\mathcal{A}$ that one adopts, we denote it by $\mathrm{sd}^{\mathcal{A}}_{\prec}(F)$. On the other hand, in the second and the third definitions, which were originally provided in a series of Gorla et al.'s studies (cf. [8], [4], [24], [9], [23]), we can see that the solving degrees do not depend on an algorithm, but only on F and $\prec$. The solving degree in the second (resp. third) definition is defined by using Macaulay matrices (resp. those with mutants), and it is denoted by $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$ (resp. $\mathrm{sd}^{\mathrm{mut}}_{\prec}(F)$) in this paper, where the subscripts "mac" and "mut" stand for Macaulay matrices and mutants respectively. Note that, when F is homogeneous, these three solving degrees coincide with one another (for $\mathcal{A}$ with suitable setting) and we call them the solving degree simply; they are equal to the maximal Gröbner basis degree $\mathrm{max.GB.deg}_{\prec}(F)$ of F with respect to $\prec$. In this case, we can apply a well-known bound [31, Theorem 2] by Lazard. In the following, we mainly treat with the case where F is affine.

In their celebrated works (cf. [8], [4], [24], [9], [23]), Gorla et al. have studied well the relations between the solving degrees $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$ and $\mathrm{sd}^{\mathrm{mut}}_{\prec}(F)$ and other invariants such as the *degree of regularity* and the *Castelnuovo–Mumford regularity*. Their results provide a mathematically rigorous framework for estimating the complexity of computing Gröbner bases. In particular, Caminata-Gorla [8] proved the following upper-bound on $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$ by using Lazard's bound:

- ([8, Theorem 11]) When $K = \mathbb{F}_q$, the solving degree $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$ for a DRL ordering $\prec$ can be upper-bounded by the Macaulay bound $d_1 + \cdots + d_\ell - \ell + 1$ with $d_1 \geq d_2 \geq \cdots \geq d_m$ and $\ell = \min\{n+1, \ell\}$, if F contains the field equations $x_i^q - x_i$ for all $1 \leq i \leq n$.

As for upper-bounds on the solving degrees $\mathrm{sd}^{\mathcal{A}}_{\prec}(F)$ and $\mathrm{sd}^{\mathrm{mut}}_{\prec}(F)$, we know the following:

- Semaev-Tenti [40] (see also Tenti's PhD thesis [41]) constructed a Buchberger-like algorithm $\mathcal{A}$ for the case $K = \mathbb{F}_q$ such that $\mathrm{sd}^{\mathcal{A}}_{\prec}(F) \leq 2D - 2$ with $D := d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ for a DRL ordering $\prec$, assuming that $\{x_i^q - x_i : 1 \leq i \leq n\} \subset F$ and $\max\{q, \deg(f_1), \ldots, \deg(f_m)\} \leq D$. Here $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ is the degree of regularity for F^{top}, i.e., the smallest integer d with $R_d = \langle F^{\mathrm{top}} \rangle_d$, where R_d denotes the homogeneous part (component) of degree d and where we set $I_d = I \cap R_d$ for a homogeneous ideal I of R.

- Caminata-Gorla proved in [9, Theorem 3.1] that $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F) = \max\{d_F, \mathrm{max.GB.deg}_{\prec}(F)\}$ for any graded monomial ordering $\prec$, where d_F denotes the *last fall degree* of F defined in [9, Definition 1.5] (originally in [27], [26]). Recently, Salizzoni [39] also proved $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F) \leq D+1$, in the case where $\max\{\deg(f_1), \ldots, \deg(f_m)\} \leq D < \infty$.

In this paper, by a mathematically rigorous way following Gorla et al.'s works, we study the solving degrees and related Gröbner bases of *affine semi-regular* polynomial sequences, where a sequence $\boldsymbol{F} = (f_1, \ldots, f_m) \in (R \smallsetminus K)^m$ of (not necessarily homogeneous) polynomials is said to be affine semi-regular (resp. affine cryptographic semi-regular) if $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ is semi-regular (resp. cryptographic semi-regular), see Definitions 2.1.3, 2.1.10, and 2.1.13 for details. Note that homogeneous semi-regular sequences are conjectured by Pardue [36, Conjecture B] to be generic sequences of polynomials (see e.g., [36] for the definition of genericness), and affine (cryptographic) semi-regular sequences are often appearing in the construction of multivariate public key cryptosystems. As a sequel of the authors' previous work [30], we investigate further results on the solving degrees and on behaviors of the computation of Gröbner bases.

As the first main result in this paper, we revisit the result in our previous paper [30] with some additional remarks, which shall give an explicit characterization (Theorem 1 below) of the Hilbert function and the Hilbert-Poincaré series associated to the homogenization F^h. This characterization is useful to analyze the Gröbner basis computation for both F and F^h.

Theorem 1 (Theorem 3.1.1, Remark 3.1.2, Remark 3.1.3 and Corollary 3.1.5)**.** *With notation as above, assume that $\boldsymbol{F}$ is affine cryptographic semi-regular, and put $D := d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$. Then, we have the following:*

(1) For each d with $d < D$, we have $\mathrm{HF}_{R'/\langle F^h \rangle}(d) = \mathrm{HF}_{R/\langle F^{\mathrm{top}} \rangle}(d) + \mathrm{HF}_{R'/\langle F^h \rangle}(d-1)$, and hence $\mathrm{HF}_{R'/\langle F^h \rangle}(d) = \sum_{i=0}^{d} \mathrm{HF}_{R/\langle F^{\mathrm{top}} \rangle}(i)$.

(2) The Hilbert function $\mathrm{HF}_{R'/\langle F^h \rangle}$ is unimodal and its highest value is attained at $d = D-1$. In more detail, the multiplication map by y from $(R'/\langle F^h \rangle)_{d-1}$ to $(R'/\langle F^h \rangle)_d$ is injective for $d < D$ and surjective for $d \geq D$.

(3) There exists d_0 such that $\mathrm{HF}_{R'/\langle F^h \rangle}(d_0) = \mathrm{HF}_{R'/\langle F^h \rangle}(d)$ for all d with $d \geq d_0$, namely the number of projective zeros for F^h is finite at most. Here, d_0 gives an upper-bound on the solving degree of F^h (or equivalently the maximal degree of the Gröbner basis of $\langle F^h \rangle$).

(4) $\mathrm{HS}_{R'/\langle F^h \rangle}(z) \equiv \prod_{i=1}^{m} (1 - z^{d_i})/(1-z)^{n+1} \pmod{z^D}$, so that F^h is D-regular, equivalently $\mathrm{syz}(F^h)_{<D} = \mathrm{tsyz}(F^h)_{<D}$. Here we denote by $\mathrm{syz}(F^h)$ and $\mathrm{tsyz}(F^h)$ the module of syzygies of F^h and that of trivial syzygies of F^h, respectively (see Appendix A.1 for the definition of $\mathrm{syz}(F^h)$ and $\mathrm{tsyz}(F^h)$).

As for (3) of Theorem 1, it follows from the proof of Lazard's bound [31, Theorem 2] that $\mathrm{max.GB.deg}_{\prec^h}(F^h) \leq d_0$ for a DRL ordering $\prec$ (we give an explicit proof for this in Lemma 2.2.2 below), where $\prec^h$ is the homogenization of $\prec$. As in [8, Theorem 11] recalled above, we can apply Lazard's bound to obtaining $d_0 \leq d_1 + \cdots + d_\ell - \ell + 1$ with $d_i = \deg(f_i)$ and $\ell = \min\{n+1, \ell\}$, assuming $d_1 \geq \cdots \geq d_m$ in *descending* order. As an additional result in this paper, we also obtain the following upper-bound on the solving degree of F^h:

Theorem 2 (Theorem 3.2.3 and Proposition 3.2.5)**.** *(1) Suppose that that $d_1 \leq d_2 \leq \cdots \leq d_m$ (in ascending order) and $m > n$. If $\boldsymbol{F}^{\mathrm{top}}$ satisfies a stronger condition that it is semi-regular, then the solving degree of F^h is upper-bounded by $d_1 + d_2 + \cdots + d_n + d_m - n$. Moreover, if $d_m \leq D$, the solving degree of F^h is upper-bounded by $d_1 + d_2 + \cdots + d_n + d_{n+1} - n$.*

(2) Let S_0 be the saturation exponent *of $(\langle F^h\rangle : \langle y^\infty\rangle)$, that is, the minimum integer s such that $(\langle F^h\rangle : \langle y^s\rangle) = (\langle F^h\rangle : \langle y^\infty\rangle)$. Then the solving degree of F^h is upper-bounded by $D + s_0$.*

Based on Theorem 1, we can explore the computations of reduced Gröbner bases of $\langle F\rangle$, $\langle F^h\rangle$, and $\langle F^{\mathrm{top}}\rangle$ in Section 4 below, dividing the cases into the degree less than D or not. More precisely, denoting by G, G_{hom}, and G_{top} the reduced Gröbner bases of $\langle F\rangle$, $\langle F^h\rangle$, and $\langle F^{\mathrm{top}}\rangle$ respectively, where their monomial orderings are DRL $\prec$ or its extension $\prec^h$, we revisit [30, Section 5] and obtain more precise results:

Theorem 3 (Section 4; cf. [30, Section 5])**.** *With notation as above, assume that $\boldsymbol{F}$ is affine cryptographic semi-regular, and that $D := d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle) < \infty$.*

(1) $\mathrm{LM}(G_{\mathrm{hom}})_d = \mathrm{LM}(G_{\mathrm{top}})_d$ for each degree $d < D$. This implies that the Gröbner basis computation process for $\langle F^h\rangle$ corresponds to that for $\langle F\rangle$, for each degree less than D.

(2) $\langle \mathrm{LM}((G_{\mathrm{hom}})_{\leq D})\rangle_{R[y]} \cap R_D = R_D$. Moreover, for each element g in $(G_{\mathrm{hom}})_D$ with $g^{\mathrm{top}} := g(x_1,\ldots,x_n,0) \neq 0$, the top-part g^{top} consists of one term, that is, $g^{\mathrm{top}} = \mathrm{LT}(g)$.

(3) There is a strong correspondence between the computation of G_{hom} and that of G at early stages, namely, at the step degrees not greater than D.

(4) If $D \geq \max\{\deg(f) : f \in F\}$, then the maximal Gröbner basis degree with respect to a DRL ordering $\prec$ is upper-bounded by D. Moreover, there exists a Buchberger-like algorithm $\mathcal{A}$ whose solving degree $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ is upper-bounded by $2D-1$, and by $2D-2$ in the strict sense (see (I) in Subsection 2.2 for details on the definition of the terminology 'strict sense').

Note that (2) and the first half of (4) hold not necessarily assuming the affine cryptographic semi-regularity of $\boldsymbol{F}$.

In particular, we rigorously prove some existing results, which are often used for analyzing the complexity of computing Gröbner bases, and moreover extend them to our case.

Furthermore, based on Lemma 2.2.2 below, for homogeneous ideals of projective dimension 0, we naturally extend the notion of degree of regularity: We shall define the *generalized* degree of regularity $\widetilde{d}_{\mathrm{reg}}(I)$ of such a homogeneous ideal I, as the index of regularity (or called the Hilbert regularity) $i_{\mathrm{reg}}(I)$ of I. The generalized degree of regularity on $\langle F^h\rangle$ plays a very important role on the computation of Gröbner bases for such ideals, see Subsections 2.3 and 4.3. The following proposition summarizes theoretical results on this generalized degree of regularity:

Proposition 1 (Proposition 2.3.4)**.** *With notation as above, assume that $R/\langle F^{\mathrm{top}}\rangle$ is Artinian, and that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular. Then we have the following:*

1. $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle) \geq d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle) - 1$.
2. $\mathrm{max.GB.deg}_{\prec^h}(F^h) \leq \max\{d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle), \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)\}$ *for any graded monomial ordering $\prec$.*

Moreover, the equality holds in the second inequality if $\langle \mathrm{LM}(\langle F^h\rangle)\rangle$ is weakly reverse lexicographic.

Here, a weakly reverse lexicographic ideal is a monomial ideal J such that if x^α is one of the minimal generators of J then every monomial of the same degree which preceeds x^α must belong to J as well (see [36, Section 4] for the original definition).

Finally, in Subsection 4.3, we give some observation on the behavior of Gröbner basis computation based on our experiments, from which we arrive at a conjecture on the Hilbert–Poincaré series for affine polynomial sequences without constant terms. For this conjecture, we also generalize the notion of cryptographic semi-regular in Subsection 2.3.

Notation

- $R = K[x_1, \ldots, x_n]$: The polynomial ring of n variables over a field K.
- $\deg(f)$: The total degree of $f \in R$.
- f^{top}: The maximal total degree part of $f \in R$, namely, f^{top} is the sum of all terms of f whose total degree equals to $\deg(f)$.
- f^h: The homogenization of $f \in R \smallsetminus \{0\}$ by an extra variable y, say $f^h := y^{\deg(f)} f(x_1/y, \ldots, x_n/y)$.
- HF_M: The Hilbert function of a finitely generated graded R-module $M = \bigoplus_{d\in\mathbb{Z}} M_d$, say $\mathrm{HF}_M(d) = \dim_K M_d$ for each $d \in \mathbb{Z}_{\geq 0}$.
- HS_M: The Hilbert–Poincaré series of a finitely generated graded R-module $M = \bigoplus_{d\in\mathbb{Z}} M_d$, say $\mathrm{HS}_M(z) = \sum_{d=0}^{\infty} \mathrm{HF}_M(d) z^d \in \mathbb{Z}[\![z]\!]$.
- $K_\bullet(f_1, \ldots, f_m)$: The Koszul complex on a sequence $(f_1, \ldots, f_m)$ of homogeneous polynomials in R.
- $H_i(K_\bullet(f_1, \ldots, f_m))$: The i-th homology group of the Koszul complex $K_\bullet(f_1, \ldots, f_m)$.

As for the definition of Koszul complex and homogenization, see Appendix A for details.

2 Preliminaries

In this section, we recall definitions of semi-regular sequences and solving degrees, and collect some known facts related to them.

2.1 Semi-regular sequences

We first review the notion of semi-regular sequence defined by Pardue [36].

Definition 2.1.1 (Semi-regular sequences, [36, Definition 1])**.** Let I be a homogeneous ideal of R. A degree-d homogeneous element $f \in R$ is said to be *semi-regular* on I if the multiplication map $(R/I)_{t-d} \longrightarrow (R/I)_d$; $g \longmapsto gf$ is injective or surjective, for every t with $t \geq d$. A sequence $(f_1, \ldots, f_m) \in (R \smallsetminus \{0\})^m$ of homogeneous polynomials is said to be *semi-regular* on I if f_i is semi-regular on $I + \langle f_1, \ldots, f_{i-1}\rangle_R$, for every i with $1 \leq i \leq m$.

Throughout the rest of this subsection, let $f_1, \ldots, f_m \in R \smallsetminus K$ be homogeneous elements of degree $d_1, \ldots, d_m$ respectively, unless otherwise noted, and put $I = \langle f_1, \ldots, f_m\rangle_R$, $I^{(0)} := \{0\}$, and $A^{(0)} := R/I^{(0)} = R$. For each i with $1 \leq i \leq m$, we also set $I^{(i)} := \langle f_1, \ldots, f_i\rangle_R$ and $A^{(i)} := R/I^{(i)}$. The degree-d homogeneous part $A_d^{(i)}$ of each $A^{(i)}$ is given by $A_d^{(i)} = R_d/I_d^{(i)}$, where $I_d^{(i)} = I^{(i)} \cap R_d$. We denote by ψ_{f_i} the multiplication map

$$A^{(i-1)} \ni g \longmapsto gf_i \in A^{(i-1)},$$

which is a graded homomorphism of degree d_i. For every t with $t \geq d_i$, the restriction map

$$\psi_{f_i}|_{A_{t-d_i}^{(i-1)}} : A_{t-d_i}^{(i-1)} \longrightarrow A_t^{(i-1)}$$

is a K-linear map.

The semi-regularity is characterized by equivalent conditions in Proposition 2.1.2 below. In particular, the fourth condition enables us to compute the Hilbert–Poincaré series of each $A^{(i)}$.

Proposition 2.1.2 (cf. [36, Proposition 1])**.** *With notation as above, the following are equivalent:*

1. *The sequence $(f_1, \ldots, f_m)$ is semi-regular.*
2. *For each $1 \le i \le m$ and for each $t \ge d_i$, the multiplication map $\psi_{f_i}|_{A_{t-d_i}^{(i-1)}}$ is injective or surjective, namely $\dim_K A_t^{(i)} = \max\{0, \dim_K A_t^{(i-1)} - \dim_K A_{t-d_i}^{(i-1)}\}$.*
3. *For each i with $1 \le i \le m$, we have $\mathrm{HS}_{A^{(i)}}(z) = [\mathrm{HS}_{A^{(i-1)}}(z)(1 - z^{d_i})]$, where $[\cdot]$ means truncating a formal power series over $\mathbb{Z}$ after the last consecutive positive coefficient.*
4. *For each i with $1 \le i \le m$, we have $\mathrm{HS}_{A^{(i)}}(z) = \left[\frac{\prod_{j=1}^{i}(1-z^{d_j})}{(1-z)^n}\right]$.*

When K is an infinite field, Pardue also conjectured in [36, Conjecture B] that generic polynomial sequences are semi-regular.

We next review the notion of *cryptographic semi-regular* sequence, which is defined by a condition weaker than one for semi-regular sequence. The notion of cryptographic semi-regular sequence is introduced first by Bardet et al. (e.g., [2], [3]) motivated to analyze the complexity of computing Gröbner bases. Diem [14] also formulated cryptographic semi-regular sequences, in terms of commutative and homological algebra. The terminology "cryptographic" was named by Bigdeli et al. in their recent work [4], in order to distinguish such a sequence from a semi-regular one defined by Pardue (see Definition 2.1.1).

Definition 2.1.3 ([2, Definition 3]; see also [14, Definition 1])**.** Let $f_1, \ldots, f_m \in R$ be homogeneous polynomials of positive degrees $d_1, \ldots, d_m$ respectively, and put $I = \langle f_1, \ldots, f_m \rangle_R$. For each integer d with $d \ge \max\{d_i : 1 \le i \le m\}$, we say that a sequence $(f_1, \ldots, f_m)$ is *d-regular* if it satisfies the following condition:

- For each i with $1 \le i \le m$, if a homogeneous polynomial $g \in R$ satisfies $g f_i \in \langle f_1, \ldots, f_{i-1} \rangle_R$ and $\deg(g f_i) < d$, then we have $g \in \langle f_1, \ldots, f_{i-1} \rangle_R$. In other word, the multiplication map $A_{t-d_i}^{(i-1)} \longrightarrow A_t^{(i-1)}$; $g \mapsto g f_i$ is injective for every t with $d_i \le t < d$.

Diem [14] determined the (truncated) Hilbert series of d-regular sequences as in the following proposition:

Theorem 2.1.4 (cf. [14, Theorem 1])**.** *With the same notation as in Definition 2.1.3, the following are equivalent for each d with $d \ge \max\{d_i : 1 \le i \le m\}$:*

1. *The sequence $(f_1, \ldots, f_m)$ is d-regular. Namely, for each (i, t) with $1 \le i \le m$ and $d_i \le t < d$, the equality $\dim_K A_t^{(i)} = \dim_K A_t^{(i-1)} - \dim_K A_{t-d_i}^{(i-1)}$ holds.*
2. *We have*
$$\mathrm{HS}_{A^{(m)}}(z) \equiv \frac{\prod_{j=1}^{m}(1 - z^{d_j})}{(1-z)^n} \pmod{z^d}. \tag{2.1.1}$$
3. *$H_1(K_\bullet(f_1, \ldots, f_m))_{\le d-1} = 0$.*

Proposition 2.1.5 ([14, Proposition 2 (a)])**.** *With the same notation as in Definition 2.1.3, let D and i be natural numbers. Assume that $H_i(K(f_1, \ldots, f_m))_{\le D} = 0$. Then, for each j with $1 \le j < m$, we have $H_i(K(f_1, \ldots, f_j))_{\le D} = 0$.*

Definition 2.1.6. A finitely generated graded R-module M is said to be *Artinian* if there exists a sufficiently large $D \in \mathbb{Z}$ such that $M_d = 0$ for all $d \ge D$.

Definition 2.1.7 ([2, Definition 4], [3, Definition 4])**.** For a homogeneous ideal I of R, we define its *degree of regularity* $d_{\mathrm{reg}}(I)$ as follows: If the finitely generated graded R-module R/I is Artinian, we set $d_{\mathrm{reg}}(I) := \min\{d : R_d = I_d\}$, and otherwise we set $d_{\mathrm{reg}}(I) := \infty$.

As for an upper-bound on the degree of regularity, we refer to [23, Theorem 21]. An elementary but important fact that relates $d_{\mathrm{reg}}(I)$ and $\mathrm{max.GB.deg}_{\prec}(I)$ is the following (the proof is straightforward, but write it here for the readers' convenience):

Lemma 2.1.8. *For any homogeneous ideal I of R and any graded ordering $\prec$ on the set of monomials in R, we have* $\mathrm{max.GB.deg}_{\prec}(I) \leq d_{\mathrm{reg}}(I)$.

Proof. The case $d_{\mathrm{reg}}(I) = \infty$ is trivial, so we consider the case where $d_{\mathrm{reg}}(I) < \infty$, namely R/I is Artinian. Let G be the reduced Gröbner basis of I with respect to $\prec$, and let g be an arbitrary element in G. Put $D := d_{\mathrm{reg}}(I)$ and take an arbitrary monomial M in R_D. Then, it follows from $R_D = I_D$ that M is divisible by $\mathrm{LM}(g)$ for some $g \in G$. Since $\prec$ is graded, we have $\deg(g) = \deg \mathrm{LM}(g) \leq \deg M = D$, as desired. $\square$

Remark 2.1.9. In Definition 2.1.7, since R/I is Noetherian, it is Artinian if and only if it is of finite length. In this case, the degree of regularity $d_{\mathrm{reg}}(I)$ is equal to the *Castelnuovo-Mumford regularity* $\mathrm{reg}(I)$ of I (see e.g., [16, §20.5] for the definition), whence $d_{\mathrm{reg}}(I) = \mathrm{reg}(I) = \mathrm{reg}(R/I)+1$.

Definition 2.1.10 ([2, Definition 5], [3, Definition 5]; see also [14, Section 2])**.** A sequence $(f_1, \ldots, f_m) \in (R \smallsetminus K)^m$ of homogeneous polynomials is said to be *cryptographic semi-regular* if it is $d_{\mathrm{reg}}(I)$-regular, where we set $I = \langle f_1, \ldots, f_m \rangle_R$.

The cryptographic semi-regularity is characterized by equivalent conditions in Proposition 2.1.11 below.

Proposition 2.1.11 ([14, Proposition 1 (d)]; see also [3, Proposition 6])**.** *With the same notation as in Definition 2.1.3, we put $D = d_{\mathrm{reg}}(I)$. Then, the following are equivalent:*

1. $(f_1, \ldots, f_m) \in (R \smallsetminus K)^m$ *is cryptographic semi-regular.*
2. *We have*
$$\mathrm{HS}_{R/I}(z) = \left[\frac{\prod_{j=1}^{m} (1 - z^{d_j})}{(1 - z)^n} \right]. \tag{2.1.2}$$
3. $H_1(K_\bullet(f_1, \ldots, f_m))_{\leq D-1} = 0$.

Remark 2.1.12. By the definition of degree of regularity, if $(f_1, \ldots, f_m)$ is cryptographic semi-regular, then $d_{\mathrm{reg}}(I)$ coincides with $\deg(\mathrm{HS}_{R/I}(z)) + 1$, where we set $I = \langle f_1, \ldots, f_m \rangle_R$.

In 1985, Fröberg had already conjectured in [21] that, when K is an infinite field, a generic sequence of homogeneous polynomials $f_1, \ldots, f_m \in R$ of degrees $d_1, \ldots, d_m$ generates an ideal I with the Hilbert–Poincaré series of the form (2.1.2), namely $(f_1, \ldots, f_m)$ is cryptographic semi-regular. It can be proved (cf. [36]) that Fröberg's conjecture is equivalent to Pardue's one [36, Conjecture B]. We also note that Moreno-Socías conjecture [35] is stronger than the above two conjectures, see [36, Theorem 2] for a proof.

It follows from the fourth condition of Proposition 2.1.2 together with the second condition of Proposition 2.1.11 that the semi-regularity implies the cryptographic semi-regularity. Note that, when $m \leq n$, both 'semi-regular' and 'cryptographic semi-regular' are equivalent to 'regular'.

Finally, we define an affine semi-regular sequence.

Definition 2.1.13 (Affine semi-regular sequences)**.** A sequence $\boldsymbol{F} = (f_1, \ldots, f_m) \in (R \smallsetminus K)^m$ of not necessarily homogeneous polynomials $f_1, \ldots, f_m$ is said to be semi-regular (resp. cryptographic semi-regular) if $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ is semi-regular (resp. cryptographic semi-regular). In this case, we call F an *affine semi-regular (resp. affine cryptographic semi-regular)* sequence.

2.2 Solving degrees of Gröbner basis computation

In general, determining precisely the complexity of computing a Gröbner basis is very difficult; in the worst-case, the complexity is doubly exponential in the number of variables, see e.g., [10], [33], [37] for surveys. However, it is experimentally well-known that a Gröbner basis with respect to a graded monomial ordering, in particular degree reverse lexicographical (DRL) ordering, can be computed quite more efficiently than ones with respect to other orderings in general. Moreover, in the case where the input set $F = \{f_1, \ldots, f_m\}$ of polynomials generate a zero-dimensional inhomogeneous ideal, once a Gröbner basis G with respect to an efficient monomial ordering $\prec$ is computed, a Gröbner basis G' with respect to any other ordering $\prec'$ can be computed easily by the FGLM basis conversion [20]. Even when F is homogeneous, one can efficiently convert G to G' by Gröbner walk [12] (or Hilbert driven [42] if both $\prec$ and $\prec'$ are graded). From this, we focus on the case where the monomial ordering is graded, and if necessary we also assume that the ideal generated by the input polynomials is zero-dimensional.

Definitions of solving degrees In the case where the chosen monomial ordering is graded, the complexity of computing a Gröbner basis is often estimated with the so-called *solving degree*. To the best of the authors' knowledge, there are three (in fact four) kinds of definitions of solving degree, and we here review them. The first definition is explicitly provided first by Ding and Schmidt in [15], and it depends on algorithms or their implementations:

(I) As the first definition, we define the solving degree of an algorithm to compute a Gröbner basis as the highest degree of the polynomials involved during the execution of the algorithm, see [15, p. 36]. For example, applying Buchberger's algorithm or its variants such as F_4 with the normal strategy, we collect critical S-pairs with the lowest degree and then reduce the corresponding S-polynomials in each iteration of the main loop of reductions. The lowest degree of each iteration is called the *step degree*. Then the solving degree is defined as the highest step degree. Instead, we may adopt the highest degree of S-polynomials appearing in the whole computation as in [41] and [40] by Semaeve-Tenti, and in this case we use the terminology "the solving degree *in the strict sense*".

(I)' Their is a variant of the above first definition, where the solving degree is defined as a value depending not only on an algorithm but also on its implementation. More precisely, in [15, Section 2.1], the authors use the term solving degree for the step degree at which it takes the most amount of time among all iterations. In the cryptographic literature, the term solving degree often means this solving degree. Although this solving degree is estimated based on experiments, it is practically a quite important ingredient for analyzing the security of multivariate cryptosystems. The degree of regularity $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ can be often used as a proxy for this solving degree.

We do not consider the solving degree in (I)', since this paper focuses on theoretical aspects on computing Gröbner bases, but not on aspects in practical implementation. For a graded monomial ordering $\prec$ on R and an input set F of non-zero polynomials in R, we denote by $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ the solving degree in (I) of an algorithm $\mathcal{A}$ to compute a Gröbner basis of F with respect to $\prec$.

On the other hand, Caminata and Gorla [8] defined the solving degree of an input system, so that it does not depend on an algorithm, by using *Macaulay matrices*. Here, a Macaulay matrix is defined as follows: For a (fixed) graded monomial ordering $\prec$ and a finite sequence $H = (h_1, \ldots, h_k) \in (R \smallsetminus \{0\})^k$ with $d := \max\{\deg(h_i) : 1 \leq i \leq k\}$, writing each h_i as $h_i = \sum_{j=1}^{\ell} c_{i,j} t_j$, where $\mathcal{T}_{\leq d} = \{t_1, \ldots, t_{\ell-1}, t_\ell = 1\}$ is the set of monomials in R of degree $\leq d$ with $t_1 \succ \cdots \succ t_\ell$, the Macaulay matrix of H, denoted by $\mathrm{Mac}_{\prec}(H)$ is defined to be the $k \times \ell$ matrix $(a_{i,j})_{i,j}$ over K (we let $\mathrm{Mac}_{\prec}(H)$ be the 1×1 zero-matrix if H is empty). Moreover, for each non-negative integer d, *the degree-d Macaulay matrix of* F, denoted by $M_{\leq d}(F)$ when $\prec$ is fixed, is defined as $M_{\leq d}(F) := \mathrm{Mac}_{\prec}(\mathcal{S}_{\leq d}(F))$, where $\mathcal{S}_{\leq d}(F)$ is a sequence of the multiples tf for $f \in F$ with $\deg(f) \leq d$ and $t \in \mathcal{T}_{\leq d-\deg(f)}$. Namely, the rows of $M_{\leq d}(F)$ correspond to tf's above, and the columns are indexed by the monomials of degree at most d in descending order with respect to $\prec$. Note that the order of elements in $\mathcal{S}_{\leq d}(F)$ can be arbitrary.

(II) We define the solving degree of F with respect to a fixed (graded) monomial ordering as the lowest degree d at which the reduced row echelon form (RREF) of $M_{\leq d}(F)$ produces a Gröbner basis of F.

Note that the computation of the RREF of $M_{\leq d}(F)$ corresponds to the standard XL algorithm [11], which is based on an idea of Lazard [31].

The third definition is given in Gorla et al.'s works (cf. [4], [24], [9], [23]), see also [39]. More precisely, for each non-negative integer $d \in \mathbb{Z}_{\geq 0}$, let $V_{F,d}$ be the smallest K-vector space such that $\{f \in F : \deg(f) \leq d\} \subset V_{F,d}$ and $\{tf : f \in V_{F,d},\ t \in \mathcal{T}_{\leq d-\deg(f)}\} \subset V_{F,d}$, where $\mathcal{T}_{\leq d}$ denotes the set of all monomials in R of degree at most d. Then the third definition is as follows:

(III) The solving degree of F is defined as the smallest d for which $V_{F,d}$ contains a Gröbner basis of F with respect to a fixed monomial ordering.

We can also describe the solving degree in (III) with Macaulay matrices. Specifically, we consider to compute a Gröbner basis of F by the following *mutant strategy*:

- Initialize d as $d = \max\{\deg(f) : f \in F\}$. Compute the RREF of $M_{\leq d}(F)$. If the RREF contains a polynomial f with $\deg(f) < d$ whose leading monomial is not equal to that of any row of $M_{\leq d}(F)$, add to the RREF the new rows corresponding to tf for all $t \in \mathcal{T}_{\leq d-\deg(f)}$ such that tf does not belong to the linear space spanned by the rows of the RREF. Repeat the computation of the RREF and the operation of adding new rows, until there are no new rows to add. If the resulting matrix produces a Gröbner basis of F, then we stop, and otherwise we proceed to the next degree, $d+1$.

This strategy computes a basis of $V_{F,d}$ for each d, and therefore the smallest d for which the mutant strategy terminates is equal to the solving degree of F in terms of (III), see [24, Theorem 1]. As in [23], we refer to the algorithms such as Mutant-XL [7] and MXL2 [34] that employ this strategy as *mutant algorithms*. In the following, we denote the solving degree in (II) and that in (III) respectively by $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ and $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$. By definitions, it is clear that $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F) \leq \mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ for any graded monomial oredering $\prec$, and the equality holds if the elements in F are all homogeneous.

In a series of their celebrated works (cf. [8], [4], [24], [9], [23]), Gorla et al. provided a mathematical formulation for the relations between the solving degrees $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ and $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ and algebraic invariants coming from F, such as the maximal Gröbner basis degree, the degree of regularity, the Castelnuovo–Mumford regularity, the first and last degrees, and so on. Here, the *maximal Gröbner basis degree* of the ideal $\langle F\rangle_R$ is the maximal degree of elements in the reduced Gröbner basis of $\langle F\rangle_R$ with respect to a fixed monomial ordering $\prec$, and is denoted by $\mathrm{max.GB.deg}_{\prec}(F)$. For any graded monomial oredering $\prec$, it is straightforward that

$$\mathrm{max.GB.deg}_{\prec}(F) \leq \mathrm{sd}_{\prec}^{\mathrm{mut}}(F) \leq \mathrm{sd}_{\prec}^{\mathrm{mac}}(F). \tag{2.2.1}$$

Upper bounds on solving degree If F consists of homogeneous elements, then one has $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F) = \mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$, and moreover these solving degrees are equal to $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ if the algorithm $\mathcal{A}$ incrementally computes the reduced d-Gröbner basis for each d in increasing the degree d. For example, Buchberger algorithm, F_4, F_5, matrix-F_5, and Hilbert driven algorithm are the cases. Furthermore, the equalities in (2.2.1) hold, and hence we can use a bound on $\mathrm{max.GB.deg}_{\prec}(F)$. Since we are now considering the zero-dimensional case, we can apply Lazard's upper-bound below.

In the non-homogeneous case, i.e., F contains at least one non-homogeneous element, the euqalities in (2.2.1) do not hold in general, and it is not so easy to estimate any of the solving degrees. A straightforward way of bounding the solving degrees in the non-homogeneous case is to apply the *homogenization* as follows. We set $\prec$ as the DRL ordering on R with $x_n \prec \cdots \prec x_1$, and fix it throughout the rest of this subsection. Let y be an extra variable for homogenization as in Subsection A.2, and $\prec^h$ the homogenization of $\prec$, so that $y \prec x_i$ for any i with $1 \leq i \leq n$. Then, we have

$$\max.\mathrm{GB.deg}_{\prec}(F) \leq \mathrm{sd}_{\prec}^{\mathrm{mac}}(F) = \mathrm{sd}_{\prec^h}^{\mathrm{mac}}(F^h) = \max.\mathrm{GB.deg}_{\prec^h}(F^h),$$

see [8] for a proof. Here, we also recall Lazard's bound for the maximal Gröbner basis degree of $\langle F^h \rangle_{R'}$ with $R' = R[y]$:

Theorem 2.2.1 (Lazard; [31, Theorem 2], [32, Théorèm 3.3])**.** *With notation as above, we assume that the number of projective zeros of F^h is finite (and therefore $m \geq n$), and that $f_1^h = \cdots = f_m^h = 0$ has no non-trivial solution over the algebraic closure $\overline{K}$ with $y = 0$, i.e., F^{top} has no solution in $\overline{K}^n$ other than $(0, \ldots, 0)$. Then, supposing also that $d_1 \geq \cdots \geq d_m$, we have*

$$\max.\mathrm{GB.deg}_{\prec^h}(F^h) \leq d_1 + \cdots + d_\ell - \ell + 1 \tag{2.2.2}$$

with $\ell := \min\{m, n+1\}$.

One of the most essential parts for the proof of Theorem 2.2.1 is an argument stated in the following lemma (we here write a proof for readers' convenience):

Lemma 2.2.2. *With notation as above, let d_0 be a positive integer satisfying the following two properties:*

1. *The multiplication-by-y map $(R'/\langle F^h \rangle)_{d_0-1} \longrightarrow (R'/\langle F^h \rangle)_{d_0}$ is surjective.*
2. *For any $d \in \mathbb{Z}$ with $d \geq d_0$, the multiplication-by-y map $(R'/\langle F^h \rangle)_d \longrightarrow (R'/\langle F^h \rangle)_{d+1}$ is injective.*

Then we have $\max.\mathrm{GB.deg}_{\prec^h}(F^h) \leq d_0$.

Proof. Let G be a Gröbner basis of $\langle F^h \rangle$ with respect to $\prec^h$. Clearly, we may suppose that each element of G is homogeneous. It suffices to prove that $G_{\leq d_0} := \{g \in G : \deg(g) \leq d_0\}$ is a Gröbner basis of $\langle F^h \rangle$ with respect to $\prec^h$. Indeed, the maximal degree of the reduced Gröbner basis of $\langle F^h \rangle$ with respect to $\prec^h$ is not greater than that of any Gröbner basis of $\langle F^h \rangle$ with respect to $\prec^h$.

Let $f \in \langle F^h \rangle$, and $d := \deg(f)$. We show that there exists $g \in G_{\leq d_0}$ with $\mathrm{LM}(g) \mid \mathrm{LM}(f)$, by the induction on d. It suffices to consider the case where f is homogeneous, since $\langle F^h \rangle$ is homogeneous. The case where $d \leq d_0$ is clear, and so we assume $d > d_0$.

First, if $\mathrm{LM}(f) \in R = K[x_1, \ldots, x_n]$ (namely $y \nmid \mathrm{LM}(f)$), we choose an arbitrary monomial $t \in R$ of degree d_0 with $t \mid \mathrm{LM}(f)$. Since the multiplication map $(R'/\langle F^h \rangle)_{d_0-1} \longrightarrow (R'/\langle F^h \rangle)_{d_0}$ by y is surjective, there exists a homogeneous polynomial $h \in (R')_{d_0-1}$ such that $h_1 := t - yh \in \langle F^h \rangle$. Here, h_1 is homogeneous of degree d_0, and $y \nmid t$, whence $\mathrm{LM}(h_1) = t$. Therefore, we have $\mathrm{LT}(g) \mid t$ for some $g \in G$. Since $\deg(t) = d_0$, we also obtain $\deg(g) \leq d_0$, so that $g \in G_{\leq d_0}$.

Next, assume that $y \mid \mathrm{LM}(f)$. In this case, it follows from the definition of $\prec^h$ that any other term in f is also divisible by y, so that $f \in \langle y \rangle$. Hence, we can write $f = yf_1$ for some homogeneous $f_1 \in R'$. By $d - 1 \geq d_0$, the multiplication map $(R'/\langle F^h \rangle)_{d-1} \longrightarrow (R'/\langle F^h \rangle)_d$ by y is injective, so that $f_1 \in \langle F^h \rangle_{d-1}$. By the induction hypothesis, there exists $g \in G_{\leq d_0}$ such that $\mathrm{LM}(g) \mid \mathrm{LM}(f_1)$. Since $\mathrm{LM}(f) = y\mathrm{LM}(f_1)$, we obtain $\mathrm{LM}(g) \mid \mathrm{LM}(f)$. We have proved that $G_{\leq d_0}$ is a Gröbner basis of $\langle F^h \rangle$ with respect to $\prec^h$. ∎

Lazard proved that we can take $d_1 + \cdots + d_\ell - \ell + 1$ in Theorem 2.2.1 as d_0 in Lemma 2.2.2. Lazard's bound given in (2.2.2) is also referred to as the *Macaulay bound*, and it provides an upper-bound for the solving degree of F with respect to a DRL ordering.

As for the maximal Gröbner basis degree of $\langle F \rangle$, if $\langle F^{\mathrm{top}} \rangle$ is Aritinian, we have

$$\mathrm{max.GB.deg}_{\prec'}(F) \leq d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) \tag{2.2.3}$$

for any graded monomial ordering $\prec'$ on R, see [8, Remark 15] or Lemma 4.2.4 below for a proof. Both $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ and $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ are greater than or equal to $\mathrm{max.GB.deg}_{\prec}(F)$, whereas it is pointed out in [4], [8], and [9] by explicit examples that *any* of the degree of regularity and the first fall degree does *not* produce an estimate for the solving degrees in general, even when F is an affine (cryptographic) semi-regular sequence. Caminata-Gorla proved in [9] that the solving degree $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ is nothing but the *last fall degree* if it is greater than the maximal Gröbner basis degree:

Theorem 2.2.3 ([9, Theorem 3.1]). *With notation as above, for any degree-compatible monomial ordering $\prec'$ on R, we have the following equality:*

$$\mathrm{sd}_{\prec'}^{\mathrm{mut}}(F) = \max\{d_F, \mathrm{max.GB.deg}_{\prec'}(F)\},$$

where d_F denotes the last fall degree of F defined in [9, Definition 1.5] (originally in [27], [26]).

By this theorem, if $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) < d_F$, the degree of regularity is no longer an upper-bound on the solving degrees $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ and $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$. Recently, Salizzoni [39] proved the following theorem:

Theorem 2.2.4 ([39, Theorem 1.1]). *With notation as above, we also set $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$, and assume that $D \geq \max\{\deg(f) : f \in F\}$. Then, for any graded monomial ordering $\prec'$ on R, we have $\mathrm{sd}_{\prec'}^{\mathrm{mut}}(F) \leq D+1$. Moreover, a Gröbner basis of F can be find in $O((n+1)^{4(d+1)})$ operations in K.*

On the other hand, Semaev and Tenti proved that the solving degree $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ for some algorithm $\mathcal{A}$ is linear in the degree of regularity, if K is a (small) finite field, and if the input system contains polynomials related to the *field equations*, say $x_i^q - x_i$ for $1 \leq i \leq n$:

Theorem 2.2.5 ([40, Theorem 2.1], [41, Theorem 3.65 & Corollary 3.67]). *With notation as above, assume that $K = \mathbb{F}_q$, and that F contains $x_i^q - x_i$ for all $1 \leq i \leq n$. If $D \geq \max\{\deg(f) : f \in F\}$ and $D \geq q$, then there exists a Buchberger-like algorithm $\mathcal{A}$ to compute the reduced Gröbner basis of F with S-polynomials such that*

$$\mathrm{sd}_{\prec}^{\mathcal{A}}(F) \leq 2D - 1. \tag{2.2.4}$$

and

$$\mathrm{sd}_{\prec}^{\mathcal{A}}(F) \leq 2D - 2. \tag{2.2.5}$$

in the strict sense (see the definition (I) of the solving degree for details). Furthermore, the complexity of the algorithm $\mathcal{A}$ is

$$O(L_q(n, D)^2 L_q(n, D-1)^2 L_q(n, 2D-2))$$

operations in K, where $L_q(n, d)$ denotes the number of monomials in $\mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^q, \ldots, x_n^q \rangle$ of degree $\leq d$.

In Subsection 4.2 below, we will prove the same inequality as in (2.2.4), in the case where F not necessarily contains a field equation but is cryptographic semi-regular.

2.3 Extension of the notion of degree of regularity

In this subsection, we shall extend the notion of degree of regularity of a homogeneous ideal I of R. Let $\prec$ be a graded ordering on the monomials of R. Recall from Definition 2.1.7 that we set $d_{\mathrm{reg}}(I) = \infty$ if R/I is not Artinian, but this is not feasible to analyzing the Gröbner basis computation of F^h unless a system defined by F^h has no non-trivial root over an algebraic closure. For the feasibility, we here give an alternative definition for degree of regularity, which is viewed as a generalization of the original definition (Definition 2.1.7):

Definition 2.3.1. For a homogeneous ideal I of R, we define its *generalized degree of regularity* $\widetilde{d}_{\mathrm{reg}}(I)$ as follows: If there exists an integer d_0 such that $\dim_K(R/I)_d = \dim_K(R/I)_{d_0}$ for any d with $d \geq d_0$, we set $\widetilde{d}_{\mathrm{reg}}(I) := \min\{d_0 : \dim_K(R/I)_d = \dim_K(R/I)_{d_0} \text{ for any } d \text{ with } d \geq d_0\}$, and otherwise we set $\widetilde{d}_{\mathrm{reg}}(I) := \infty$.

Remark 2.3.2. For a homogeneous ideal I in R, its generalized degree of regularity $\widetilde{d}_{\mathrm{reg}}(I)$ is nothing but *the index of regularity* $i_{\mathrm{reg}}(I)$, if I has finite number of roots over an algebraic closure. Here, the index of regularity of I is defined as follows: Denoting by $\mathrm{HP}_{R/I}$ the Hilbert polynomial of R/I, we define the index of regularity of I as the smallest non-negative integer $i_{\mathrm{reg}}(I)$ such that $\mathrm{HF}_{R/I}(d) = \mathrm{HP}_{R/I}(d)$ for all d with $d \geq i_{\mathrm{reg}}(I)$. If I has finite number of roots over an algebraic closure, then $\mathrm{HP}_{R/I}$ is a constant, and $\tilde{d}_{\mathrm{reg}}(I) < \infty$, so that $\tilde{d}_{\mathrm{reg}}(I) = i_{\mathrm{reg}}(I)$.

Note that the degree of regularity $d_{\mathrm{reg}}(I)$ is also equal to $i_{\mathrm{reg}}(I)$ if R/I is Artinian, but these are distinguished in the literature. Following this, we distinguish $\widetilde{d}_{\mathrm{reg}}(I)$ and $i_{\mathrm{reg}}(I)$.

The existence of d_0 in Definition 2.3.1 is equivalent to that the number of projective zeros of I is finite at most. Note also that, in Definition 2.3.1, we have $\widetilde{d}_{\mathrm{reg}}(I) = d_{\mathrm{reg}}(I) < \infty$ if R/I is Artinian, and otherwise $\widetilde{d}_{\mathrm{reg}}(I) < d_{\mathrm{reg}}(I)$ or $\widetilde{d}_{\mathrm{reg}}(I) = d_{\mathrm{reg}}(I) = \infty$. We also extend the cryptographic semi-regularity (Definition 2.1.10) of a sequence of homogeneous polynomials, as follows:

Definition 2.3.3. A sequence $(f_1, \ldots, f_m) \in (R \smallsetminus K)^m$ of homogeneous polynomials is said to be *generalized cryptographic semi-regular* if it is $\widetilde{d}_{\mathrm{reg}}(I)$-regular, where we set $I = \langle f_1, \ldots, f_m \rangle_R$.

A sequence $\boldsymbol{F} = (f_1, \ldots, f_m) \in (R \smallsetminus K)^m$ of not necessarily homogeneous polynomials $f_1, \ldots, f_m$ is said to be generalized cryptographic semi-regular if $\boldsymbol{F}^h = (f_1^h, \ldots, f_m^h)$ is generalized cryptographic semi-regular. In this case, we call $\boldsymbol{F}$ an *affine generalized cryptographic semi-regular* sequence.

Here, we relate the solving degree of F^h (namely the maximal Gröbner basis degree of F^h) with our generalized degree of regularity, under some assumptions.

Proposition 2.3.4. *Let $\boldsymbol{F} = (f_1, \ldots, f_m) \in (R \smallsetminus K)^m$ be a sequence of not necessarily homogeneous polynomials. We set $F = \{f_1, \ldots, f_m\}$. Assume that $R/\langle F^{\mathrm{top}} \rangle$ is Artinian, and that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular. Then we have the following:*

1. $\widetilde{d}_{\mathrm{reg}}(\langle F^h \rangle) \geq d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) - 1$.
2. $\mathrm{max.GB.deg}_{\prec^h}(F^h) \leq \max\{d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle), \widetilde{d}_{\mathrm{reg}}(\langle F^h \rangle)\}$ *for any graded monomial ordering* $\prec$.

Moreover, the equality holds in the second inequality if $\prec$ is a DRL ordering and if $\langle \mathrm{LM}(\langle F^h \rangle) \rangle$ is weakly reverse lexicographic. Here, a weakly reverse lexicographic ideal is a monomial ideal J such that if x^α is one of the minimal generators of J then every monomial of the same degree which preceeds x^α must belong to J as well (see [36, Section 4] for the original definition).

Proof. Put $D := \widetilde{d}_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ and $D' := \widetilde{d}_{\mathrm{reg}}(\langle F^h \rangle)$. By the proof of Theorem 3.1.1 below, we have the following exact sequence:

$$H_1(K_\bullet \otimes_{R'} R)_d \longrightarrow H_0(K_\bullet)_{d-1} \xrightarrow{\times y} H_0(K_\bullet)_d \longrightarrow H_0(K_\bullet \otimes_{R'} R)_d \longrightarrow 0$$

for each d, where $K_\bullet$ denotes the Koszul complex on $\boldsymbol{F}^h$. Here we have $H_1(K_\bullet \otimes_{R'} R)_d = 0$ and $H_0(K_\bullet \otimes_{R'} R)_d \neq 0$ for $d \leq D-1$, whence $\dim_K(R'/\langle F^h\rangle)_{d-1} < \dim_K(R'/\langle F^h\rangle)_d$ for any such d. Therefore, the first argument to be proved holds. On the other hand, it follows from the definition of d_{reg} that $H_0(K_\bullet \otimes_{R'} R)_d = 0$ for any d with $d \geq D$. Thus, for such any d, the multiplication-by-y map $H_0(K_\bullet)_{d-1} \longrightarrow H_0(K_\bullet)_d$ is surjective, and it is bijective if and only if $\dim_K(R'/\langle F^h\rangle)_{d-1} = \dim_K(R'/\langle F^h\rangle)_d$. If $D' \geq D$, for any d with $d \geq D'$, the multiplication-by-y map $H_0(K_\bullet)_d \longrightarrow H_0(K_\bullet)_{d+1}$ is bijective, since $d+1 \geq D'+1 \geq D$. By this together with the surjectivity of $H_0(K_\bullet)_{D'-1} \longrightarrow H_0(K_\bullet)_{D'}$, it follows from Lemma 2.2.2 that $\mathrm{max.GB.deg}_{\prec^h}(F^h)$ is upper-bounded by $D' = \max\{D, D'\}$. Also if $D' = D-1$, for any d with $d \geq D'$, the multiplication-by-y map $H_0(K_\bullet)_d \longrightarrow H_0(K_\bullet)_{d+1}$ is bijective, since $d+1 \geq D'+1 = D$. However, $H_0(K_\bullet)_{D'-1} \longrightarrow H_0(K_\bullet)_{D'}$ is injective but *not* surjective, we cannot apply Lemma 2.2.2 for $d_0 = D'$, but apply it for $d_0 = D'+1 = D$. Hence, $\mathrm{max.GB.deg}_{\prec^h}(F^h)$ is upper-bounded by $D'+1 = D = \max\{D, D'\}$, as desired.

Assume that $\langle \mathrm{LM}(\langle F^h\rangle)\rangle$ is a weakly reverse lexicographic ideal. First we consider the case where $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle) \geq d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$, so that $\max\{d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle), \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)\} = \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)$. We put $d := \mathrm{max.GB.deg}_{\prec^h}(F^h)$, and let $\{t_1, \ldots, t_r\}$ be a standard monomial basis of $R'_d/\langle F^h\rangle_d$, that is,

$$\{t \in R'_d : t \text{ is a monomial and } t \notin \langle \mathrm{LM}(\langle F^h\rangle)\rangle\}.$$

For $s \geq 1$, we prove that $\{t_1 y^s, \ldots, t_r y^s\}$ is a basis of $R'_{d+s}/\langle F^h\rangle_{d+s}$, from which we have $\dim_K R'_d/\langle F^h\rangle_d = \dim_K R'_{d+s}/\langle F^h\rangle_{d+s}$ for any positive integer s, so that $d \geq \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)$ and therefore $d = \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)$.

By Remark 3.1.2 and Lemma 2.3.6 below, the multiplication-by-y^s map from $R'_d/\langle F^h\rangle_d$ to $R'_{d+s}/\langle F^h\rangle_{d+s}$ is surjective. Therefore $B_s := \{t_1 y^s, \ldots, t_r y^s\}$ generates $R'_{d+s}/\langle F^h\rangle_{d+s}$. Suppose to contrary that B_s is not a basis. In this case, there exists an i such that $t_i y^s$ is divisible by $\mathrm{LM}(g)$ for some $g \in G_{\mathrm{hom}}$, but t_i is not divisible by $\mathrm{LM}(g)$, where G_{hom} is the reduced Gröbner basis of $\langle F^h\rangle$ with respect to $\prec^h$. Therefore, we can write $t_i y^s = s_i u_i y^s$ with $s_i u_i = t_i$ and $u_i y^{s'} = \mathrm{LM}(g)$ for some $s' \leq s$. (We note that $\deg s_i = d - \deg u_i \geq \deg \mathrm{LM}(g) - \deg u_i = s'$ and $u_i = \mathrm{GCD}(t_i, \mathrm{LM}(g))$.) Note that $s' \geq 1$ since otherwise t_i is divisible by $\mathrm{LM}(g)$.

Take an arbitrary monomial s'_i such that $\deg s'_i = s'$ and s'_i divides s_i. Then, by the weakly reverse lexicographicness, as $\mathrm{LM}(g) = u_i y^{s'} \preceq u_i s'_i$, the monomial $s'_i u_i$ should belong to $\langle \mathrm{LM}(G_{\mathrm{hom}})\rangle$. Moreover, since $s'_i u_i$ divides $t_i = s_i u_i$, the monomial $t_i = s_i u_i$ also belongs to $\langle \mathrm{LM}(G_{\mathrm{hom}})\rangle$, which is a contradiction.

Finally, we consider the remaining case, namely we have $d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle) > \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)$, so that $\max\{d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle), \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)\} = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$. In this case, it follows from Lemma 2.3.6 below that $d \geq d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$, whence $d = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$. □

Remark 2.3.5. In the proof of Proposition 2.3.4, the case where $D' \geq D$ (i.e., $D' > D-1$) means that

$$\cdots < \mathrm{HF}_{A'}(D-2) < \mathrm{HF}_{A'}(D-1) \geq \mathrm{HF}_{A'}(D) \geq \cdots \geq \mathrm{HF}_{A'}(D') = \mathrm{HF}_{A'}(D'+1) = \cdots$$

with $A' := R'/\langle F^h\rangle$, and the case where $D' = D-1$ (i.e., $D'+1 = D$) means that

$$\cdots < \mathrm{HF}_{A'}(D-2) < \mathrm{HF}_{A'}(D-1) = \mathrm{HF}_{A'}(D) = \cdots.$$

Lemma 2.3.6. *Let $\boldsymbol{F} = (f_1, \ldots, f_m) \in (R \smallsetminus K)^m$ be a sequence of not necessarily homogeneous polynomials. We set $F = \{f_1, \ldots, f_m\}$, and assume that $R/\langle F^{\mathrm{top}}\rangle$ is Artinian and that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular. We also suppose that $\prec$ is a DRL ordering and that $\langle \mathrm{LM}(\langle F^h\rangle)\rangle$ is weakly reverse lexicographic. Then we have* $\mathrm{max.GB.deg}_{\prec^h}(F^h) \geq d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$ *and* $\mathrm{max.GB.deg}_{\prec}(F^{\mathrm{top}}) = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$.

Proof. Put $d := \max.\mathrm{GB.deg}_{\prec^h}(F^h)$ and assume for a contradiction that $d < D := d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$. By Lemma 4.1.4 below, we have $\mathrm{LM}(G_{\mathrm{hom}}) = \mathrm{LM}(G_{\mathrm{top}})_{\leq d} \subset R$. Then $\langle \mathrm{LM}(G_{\mathrm{hom}})\rangle_R$ contains $\mathrm{LM}(G_{\mathrm{top}})$. This can be shown as follows: For any $t \in \mathrm{LM}(G_{\mathrm{top}})$, there are polynomials $a_1, \ldots, a_m$ in R such that $t = \mathrm{LM}(\sum_{i=1}^m a_i f_i^{\mathrm{top}})$. In this case, it can be easily checked that $t = \mathrm{LM}(\sum_{i=1}^m a_i f_i^h)$, and thus t is divisible by some element of $\mathrm{LM}(G_{\mathrm{hom}})$.

Thus, as $R/\langle F^{\mathrm{top}}\rangle = R/\langle G_{\mathrm{top}}\rangle$ is Artinian, it follows from $\langle \mathrm{LM}(G_{\mathrm{hom}})\rangle_R \supset \mathrm{LM}(G_{\mathrm{top}})$ that there is an element g in G_{hom} with $\mathrm{LM}(g) = x_n^{d'}$ for some $d' \leq d$. Then, for any monomial $t \in R_{d'}$, as $t \succeq x_n^{d'}$, it belongs to $\langle \mathrm{LM}(\langle F^h\rangle)\rangle_{R'} (= \langle \mathrm{LM}(G_{\mathrm{hom}})\rangle_{R'} = \langle \mathrm{LM}(G_{\mathrm{top}})_{\leq d}\rangle_{R'})$ by its weakly reverse lexicographicness. This implies that t also belongs to $\langle \mathrm{LM}(G_{\mathrm{top}})\rangle_R$, and hence $R_d/\langle F^{\mathrm{top}}\rangle_d = 0$. Thus, we have $d \geq d' \geq d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$, a contradiction.

By the same argument as above, we can show that $\max.\mathrm{GB.deg}_{\prec}(F^{\mathrm{top}}) = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$ as follows. Recall from Lemma 2.1.8 that $\max.\mathrm{GB.deg}_{\prec}(F^{\mathrm{top}}) \leq d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$. Thus, we assume to the contrary that $d := \max.\mathrm{GB.deg}_{\prec}(F^{\mathrm{top}}) < D := d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$. Then, it follows from Lemma 4.1.4 below that $\mathrm{LM}(G_{\mathrm{top}}) = \mathrm{LM}(G_{\mathrm{hom}})_{\leq d}$ and the ideal $\langle \mathrm{LM}(G_{\mathrm{top}})\rangle_R$ has the *weak reverse lexicographicness up to d*. Since there is an element g in G_{top} with $\mathrm{LM}(g) = x_n^{d'}$ for some $d' \leq d$, any monomial in $R_{d'}$ belongs to $\langle \mathrm{LM}(G_{\mathrm{top}})\rangle$ and so $R_{d'}/\langle F^{\mathrm{top}}\rangle_{d'} = 0$, which implies $d \geq d' \geq D$, a contradiction. □

Remark 2.3.7. In Lemma 2.3.6, when $R/\langle F^{\mathrm{top}}\rangle$ is Artinian, we can easily prove the equality $\max.\mathrm{GB.deg}_{\prec}(F^{\mathrm{top}}) = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$ if $\langle \mathrm{LM}(\langle F^{\mathrm{top}}\rangle)\rangle$ is weakly reverse lexicographic, not assuming that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular nor that $\langle \mathrm{LM}(\langle F^h\rangle)\rangle$ is weakly reverse lexicographic.

3 Proofs of Theorems 1 and 2

In this section, we shall prove Theorems 1 and 2 stated in Section 1. As in the previous section, let K be a field, and $R = K[X] = K[x_1, \ldots, x_n]$ denote the polynomial ring of n variables over K. We denote by R_d the homogeneous part of degree d, that is, the set of homogeneous polynomials of degree d and 0. As in Theorems 1 and 2, let $F = \{f_1, \ldots, f_m\}$ be a set of not necessarily homogeneous polynomials in R of positive degrees $d_1, \ldots, d_m$, and put $\boldsymbol{F} = (f_1, \ldots, f_m)$. Recall Definition 2.1.10 for the definition of cryptographic semi-regular sequences.

3.1 Bounded regularity of homogenized sequences

Here we revisit the main results in [30, Section 4]. For the readability, we remain the proofs. Also, as additional remarks, we explicitly give an important property of the Hilbert-Poincaré series of $R'/\langle F^h\rangle$ with $R' = R[y]$, and also give an alternative proof for [30, Theoem 7] (Theorem 3.1.1 below).

The Hilbert-Poincaré series associated to a (homogeneous) cryptographic semi-regular sequence is given by (2.1.2). On the other hand, the Hilbert-Poincaré series associated to the homogenizaton F^h cannot be computed without knowing its Gröbner basis in general, but we shall prove that it can be computed up to the degree $d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle) - 1$ if $\boldsymbol{F}$ is affine cryptographic semi-regular, namely $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ is cryptographic semi-regular.

Theorem 3.1.1 (Theorem 1 (1); [30, Theoem 7])**.** *Let $R' = R[y]$, and let $\boldsymbol{F} = (f_1, \ldots, f_m)$ be a sequence of not necessarily homogeneous polynomials in R of positive degrees. Assume that $\boldsymbol{F}$ is affine cryptographic semi-regular. Then, for each d with $d < D := d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$, we have*

$$\mathrm{HF}_{R'/\langle F^h\rangle}(d) = \mathrm{HF}_{R/\langle F^{\mathrm{top}}\rangle}(d) + \mathrm{HF}_{R'/\langle F^h\rangle}(d-1), \tag{3.1.1}$$

and hence

$$\mathrm{HF}_{R'/\langle F^h\rangle}(d) = \mathrm{HF}_{R/\langle F^{\mathrm{top}}\rangle}(d) + \cdots + \mathrm{HF}_{R/\langle F^{\mathrm{top}}\rangle}(0), \tag{3.1.2}$$

whence we can compute the value $\mathrm{HF}_{R'/\langle F^h\rangle}(d)$ *from the formula* (2.1.2).

Proof. Let $K_\bullet = K_\bullet(f_1^h, \ldots, f_m^h)$ be the Koszul complex on $(f_1^h, \ldots, f_m^h)$, which is given by (A.1.1). By tensoring $K_\bullet$ with $R'/\langle y\rangle_{R'} \cong K[x_1, \ldots, x_n] = R$ over R', we obtain the following exact sequence of chain complexes:

$$0 \longrightarrow K_\bullet \xrightarrow{\times y} K_\bullet \xrightarrow{\pi_\bullet} K_\bullet \otimes_{R'} R \longrightarrow 0,$$

where $\times y$ is a graded homomorphism of degree 1 multiplying each entry of a vector with y, and where π_i is a canonical homomorphism sending $v \in K_i$ to $v_i \otimes 1 \in K_i \otimes_{R'} R$. Note that there is an isomorphism

$$K_i \otimes_{R'} R \cong \bigoplus_{1\le j_1<\cdots<j_i\le m} R(-d_{j_1\cdots j_i})\mathbf{e}_{j_1\cdots j_i},$$

via which we can interpret $\pi_i : K_i \to K_i \otimes_{R'} R$ as a homomorphism that projects each entry of a vector in K_i modulo y. In particular, we have

$$\begin{aligned} K_0 \otimes_{R'} R &= R'/\langle f_1^h, \ldots, f_m^h\rangle_{R'} \otimes_{R'} R'/\langle y\rangle_{R'} \\ &\cong R'/\langle f_1^h, \ldots, f_m^h, y\rangle_{R'} \\ &\cong R/\langle f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}\rangle_R \end{aligned}$$

for $i = 0$. This means that the chain complex $K_\bullet \otimes_{R'} R$ gives rise to the Kosuzul complex on $(f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$. We induce a long exact sequence of homology groups. In particular, for each degree d, we have the following long exact sequence:

$$\begin{tikzcd} H_{i+1}(K_\bullet)_{d-1} \arrow[r, "\times y"] & H_{i+1}(K_\bullet)_d \arrow[r, "\pi_{i+1}"] & H_{i+1}(K_\bullet \otimes_{R'} R)_d \arrow[dll, "\delta_{i+1}"'] \\ H_i(K_\bullet)_{d-1} \arrow[r, "\times y"'] & H_i(K_\bullet)_d \arrow[r, "\pi_i"'] & H_i(K_\bullet \otimes_{R'} R)_d, \end{tikzcd}$$

where δ_{i+1} is a connecting homomorphism produced by the Snake lemma. For $i = 0$, we have the following exact sequence:

$$H_1(K_\bullet \otimes_{R'} R)_d \longrightarrow H_0(K_\bullet)_{d-1} \xrightarrow{\times y} H_0(K_\bullet)_d \longrightarrow H_0(K_\bullet \otimes_{R'} R)_d \longrightarrow 0.$$

From our assumption that F^{top} is cryptographic semi-regular, it follows from Proposition 2.1.11 that $H_1(K_\bullet \otimes_{R'} R)_{\le D-1} = 0$ for $D := d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$. Therefore, if $d \le D-1$, we have an exact sequence

$$0 \longrightarrow H_0(K_\bullet)_{d-1} \xrightarrow{\times y} H_0(K_\bullet)_d \longrightarrow H_0(K_\bullet \otimes_{R'} R)_d \longrightarrow 0$$

of K-linear spaces, so that

$$\dim_K H_0(K_\bullet)_d = \dim_K H_0(K_\bullet \otimes_{R'} R)_d + \dim_K H_0(K_\bullet)_{d-1} \tag{3.1.3}$$

by the dimension theorem. Since $H_0(K_\bullet) = R'/\langle F^h\rangle$ and $H_0(K_\bullet \otimes_{R'} R) = R/\langle F^{\mathrm{top}}\rangle$, we have the equality (3.1.1), as desired. $\square$

Remark 3.1.2 (Theorem 1 (2), (3); [30, Remark 6])**.** Note that, in the proof of Theorem 3.1.1, the multiplication map $H_0(K_\bullet)_{d-1} \to H_0(K_\bullet)_d$ by y is injective for all $d < D$, whence $\mathrm{HF}_{R'/\langle F^h\rangle}(d)$ is monotonically increasing for $d < D$. On the other hand, since $H_0(K_\bullet \otimes_{R'} R)_d = (R/\langle F^{\mathrm{top}}\rangle)_d = 0$ for all $d \geq D$ by the definition of the degree of regularity, the multiplication map $H_0(K_\bullet)_{d-1} \to H_0(K_\bullet)_d$ by y is surjective for all $d \geq D$, whence $\mathrm{HF}_{R'/\langle F^h\rangle}(d)$ is monotonically decreasing for $d \geq D-1$. By this together with [10, Theorem 3.3.4], the homogeneous ideal $\langle F^h\rangle$ is zero-dimensional or trivial, i.e., there are at most a finite number of projective zeros of F^h (and thus there are at most a finite number of affine zeros of F).

Remark 3.1.3. We note that, for each $d \geq D$, the condition $\dim_K H_0(K_\bullet)_{d-1} = \dim_K H_0(K_\bullet)_d$ is equivalent to that the multiplication map $H_0(K_\bullet)_{d-1} \to H_0(K_\bullet)_d$ by y is injective (and thus bijective). By this together with Lemma 2.2.2, letting d_0 be the smallest number with $d_0 \geq D$ such that $\dim_K H_0(K_\bullet)_{d_0} = \dim_K H_0(K_\bullet)_{d_0+1}$, the maximal Gröbner basis degree of $\langle F^h\rangle$ is upper-bounded by d_0.

Remark 3.1.4. We have another proof of Theorem 1 (1), (2) by using the following exact sequence:

$$0 \longrightarrow R'/(\langle F^h\rangle : y)(-1) \xrightarrow{\times y} R'/\langle F^h\rangle \longrightarrow R'/(\langle F^h\rangle + \langle y\rangle) \longrightarrow 0.$$

Then, as an easy consequence, for $d \in \mathbb{N}$, we have

$$\mathrm{HF}_{R'/\langle F^h\rangle}(d) = \mathrm{HF}_{R'/(\langle F^h\rangle + \langle y\rangle)}(d) + \mathrm{HF}_{R'/(\langle F^h\rangle : \langle y\rangle)}(d-1),$$

see [25, Lemmas 5.2.1 and 5.2.2]. Note that $\mathrm{HF}_{R'/(\langle F^h\rangle + \langle y\rangle)}(d) = \mathrm{HF}_{R/\langle F^{\mathrm{top}}\rangle}(d)$ for any positive integer d. On the other hand, for $d < D$, *any degree-fall does not occur*, that is, if $yf \in \langle F^h\rangle_d$ with $f \in R'$ then $f \in \langle F^h\rangle_{d-1}$. This can be shown by *some semantic argument* (see Remark 4.1.3) or also rigidly by the injectiveness of the multiplication map of y in (3.1.3). Thus, we also have $\langle f \in R[y] : fy \in \langle F^h\rangle\rangle_{d-1} = \langle F^h\rangle_{d-1}$, so that

$$\dim_K(R'/(\langle F^h\rangle : \langle y\rangle))_{d-1} = \dim_K(R'/\langle F^h\rangle)_{d-1},$$

namely $\mathrm{HF}_{R'/(\langle F^h\rangle : \langle y\rangle)}(d-1) = \mathrm{HF}_{R'/\langle F^h\rangle}(d-1)$, and hence we have (3.1.1) for $d < D$. For $d \geq D$, since $(R/\langle F^{\mathrm{top}}\rangle)_d = 0$ by the definition of D, we have

$$\dim_K(R'/\langle F^h\rangle)_d = \mathrm{HF}_{R'/\langle F^h\rangle}(d) = \mathrm{HF}_{R'/(\langle F^h\rangle : \langle y\rangle)}(d-1) = \dim_K(R'/(\langle F^h\rangle : \langle y\rangle))_{d-1}. \quad (3.1.4)$$

Now we consider the following multiplication map by y:

$$\times y : (R'/\langle F^h\rangle)_{d-1} \longrightarrow (R'/\langle F^h\rangle)_d \ ; \ g \mapsto yg.$$

Since $\mathrm{Ker}(\times y) = (\langle F^h\rangle : \langle y\rangle)_{d-1}/\langle F^h\rangle_{d-1}$, we have

$$\begin{aligned}
\dim_K R'_d/\langle F^h\rangle_d &\geq \dim_K(\mathrm{Im}(\times y)) \\
&= \dim_K(R'/\langle F^h\rangle)_{d-1} - \dim_K(((\langle F^h\rangle : \langle y\rangle)/\langle F^h\rangle)_{d-1} \\
&= \dim_K R'_{d-1} - \dim_K(\langle F^h\rangle : \langle y\rangle)_{d-1} \\
&= \dim_K(R'/(\langle F^h\rangle : \langle y\rangle))_{d-1}. \qquad (3.1.5)
\end{aligned}$$

Since the both ends of (3.1.4) and (3.1.5) coincide, we have $\mathrm{Im}(\times y) = (R'/\langle F^h\rangle)_d$, that is, the multiplication map by y is surjective.

The Hilbert-Poincaré series of $R'/\langle F^h\rangle$ satisfies the following equality (3.1.6):

Corollary 3.1.5 (Theorem 1 (3); [30, Corollary 1])**.** *Let $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$. Then we have*

$$\mathrm{HS}_{R'/\langle F^h\rangle}(z) \equiv \frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^{n+1}} \pmod{z^D}. \tag{3.1.6}$$

Therefore, by Theorem 2.1.4 ([14, Theorem 1]), the sequence $\boldsymbol{F}^h$ is D-regular. Here, we note that $D = \deg(\mathrm{HS}_{R/\langle F^{\mathrm{top}}\rangle}) + 1 = \deg\left(\left[\frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n}\right]\right) + 1$.

3.2 Solving degree for homogenized sequences

Here we assume that $\boldsymbol{F}^{\mathrm{top}}$ is semi-regular and that all degrees $d_i = \deg(f_i)$ are smaller or equal to the degree of regularity $d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$. Then, any n-subsequence of $\boldsymbol{F}^{\mathrm{top}}$ is regular. Under this assumption, we can give a detailed discussion on the solving degree of F^h. From now on, we assume that $m \geq n$, and set $\boldsymbol{F}_k := (f_1, \ldots, f_{n+k})$ and $D_k := d_{\mathrm{reg}}(\langle F_k^{\mathrm{top}}\rangle)$ for each $k \geq 0$. As $\boldsymbol{F}_0^{\mathrm{top}}$ is regular and $\boldsymbol{F}_1^{\mathrm{top}}$ is semi-regular, we have $D_0 = d_1 + \cdots + d_n - n + 1$ and $D_1 = \lfloor \frac{d_1 + \cdots + d_{n+1} - n - 1}{2} \rfloor + 1$, see [4, Theorem 4.1]. Thus, by setting $d_1 \leq d_2 \leq \cdots \leq d_m$, we can minimize the values D_0 and D_1.

Remark 3.2.1. Our estimations on the solving degree below require that $\boldsymbol{F}_1^{\mathrm{top}}$ is semi-regular. Thus, even when $\boldsymbol{F}^{\mathrm{top}}$ is not semi-regular, if there is an $(n+1)$-subset which is semi-regular, we may assume that $\boldsymbol{F}_1^{\mathrm{top}}$ is semi-regular and apply our arguments below.

We denote by $K_\bullet^{(j,\mathrm{top})}$ the Koszul complex on $(f_1^{\mathrm{top}}, \ldots, f_j^{\mathrm{top}})$, and let

$$K_\bullet^{(j-1,\mathrm{top})}(-d_j) \xrightarrow{\times f_j^{\mathrm{top}}} K_\bullet^{(j-1,\mathrm{top})}$$

be a graded homomorphism of degree d_j multiplying each entry of a vector with f_j^{top}. (This kind of complex is also used in [14].) Regarding $K_\bullet^{(j,\mathrm{top})}$ as the mapping cone of the above $\times f_j^{\mathrm{top}}$, we obtain the following short exact sequence of complexes

$$0 \longrightarrow K_\bullet^{(j-1,\mathrm{top})} \longrightarrow K_\bullet^{(j,\mathrm{top})} \longrightarrow K_\bullet^{(j-1,\mathrm{top})}[-1](-d_j) \longrightarrow 0,$$

where $K_\bullet^{(j-1,\mathrm{top})}[-1]$ is a shifted complex defined by $K_\bullet^{(j-1,\mathrm{top})}[-1]_i = K_{i-1}^{(j-1,\mathrm{top})}$, and where $K_i^{(j,\mathrm{top})} \cong K_i^{(j-1,\mathrm{top})} \oplus K_{i-1}^{(j-1,\mathrm{top})}(-d_j)$, for example

$$K_1^{(j,\mathrm{top})} = \bigoplus_{s=1}^{j} R(-d_s) \cong \left(\bigoplus_{s=1}^{j-1} R(-d_s)\right) \oplus R(-d_j) = K_1^{(j-1,\mathrm{top})} \oplus K_0^{(j-1,\mathrm{top})}(-d_j).$$

Note also that $K_\bullet^{(j-1,\mathrm{top})} \longrightarrow K_\bullet^{(j,\mathrm{top})}$ and $K_\bullet^{(j,\mathrm{top})} \longrightarrow K_\bullet^{(j-1,\mathrm{top})}[-1](-d_j)$ are the canonical inclusion and projection respectively. Then we deduce the following exact sequence from the Snake lemma:

$$\begin{tikzcd}
H_{i+1}(K_\bullet^{(j-1,\mathrm{top})}) \arrow[r] & H_{i+1}(K_\bullet^{(j,\mathrm{top})}) \arrow[r] & H_i(K_\bullet^{(j-1,\mathrm{top})})(-d_j) \arrow[dll, "\delta_i"'] \\
H_i(K_\bullet^{(j-1,\mathrm{top})}) \arrow[r] & H_i(K_\bullet^{(j,\mathrm{top})}) \arrow[r] & H_{i-1}(K_\bullet^{(j-1,\mathrm{top})})(-d_j),
\end{tikzcd}$$

where δ_i denotes a connecting homomorphism. Note that δ_i coincides with the multiplication map by f_j^{top} on

$$H_i(K_\bullet^{(j-1,\mathrm{top})}(-d_j)) \longrightarrow H_i(K_\bullet^{(j-1,\mathrm{top})})$$

induced from that on $K_\bullet^{(j-1,\mathrm{top})}(-d_j) \longrightarrow K_\bullet^{(j-1,\mathrm{top})}$ (this is also derived from general facts in homological algebra). Since $H_{-1}(K_\bullet^{(j-1,\mathrm{top})}) = 0$, we can rewrite the above long exact sequence as

$$\begin{tikzcd} H_{i+1}(K_\bullet^{(j-1,\mathrm{top})})(-d_j) \arrow[r, "\times f_j^{\mathrm{top}}"] & H_{i+1}(K_\bullet^{(j-1,\mathrm{top})}) \arrow[r] & H_{i+1}(K_\bullet^{(j,\mathrm{top})}) \arrow[dll] \\ H_i(K_\bullet^{(j-1,\mathrm{top})})(-d_j) \arrow[r, "\times f_j^{\mathrm{top}}"'] & H_i(K_\bullet^{(j-1,\mathrm{top})}) \arrow[r] & H_i(K_\bullet^{(j,\mathrm{top})}). \end{tikzcd}$$

In particular, for $i = 0$ and for each degree d, we have the following exact sequence:

$$\begin{tikzcd} H_1(K_\bullet^{(j-1,\mathrm{top})})_{d-d_j} \arrow[r, "\times f_j^{\mathrm{top}}"] & H_1(K_\bullet^{(j-1,\mathrm{top})})_d \arrow[r] & H_1(K_\bullet^{(j,\mathrm{top})})_d \arrow[dll] \\ H_0(K_\bullet^{(j-1,\mathrm{top})})_{d-d_j} \arrow[r, "\times f_j^{\mathrm{top}}"'] & H_0(K_\bullet^{(j-1,\mathrm{top})})_d \arrow[r] & H_0(K_\bullet^{(j,\mathrm{top})})_d. \end{tikzcd}$$

Now consider $H_1(K_\bullet^{(m,\mathrm{top})})$ for $m \geq n+1$. Here we remark that $H_i(K_\bullet^{(n,\mathrm{top})}) = 0$ for all i with $i \geq 1$, since the sequence $\boldsymbol{F}_0^{\mathrm{top}} = (f_1^{\mathrm{top}}, \ldots, f_n^{\mathrm{top}})$ is regular by our assumption.

Proposition 3.2.2. *Suppose that $d_1 \leq d_2 \leq \cdots \leq d_m$ and $m > n$. If $\boldsymbol{F}^{\mathrm{top}}$ is semi-regular, then $H_1(K_\bullet^{(m,\mathrm{top})})_d = 0$ for any d with $d \geq D_0 + d_m$. Moreover, if $d_m \leq D_1$, then $H_1(K_\bullet^{(m,\mathrm{top})})_d = 0$ for any d with $d \geq D_0 + d_{n+1}$.*

Proof. First consider the case where $m = n+1$. For $d \geq D_0 + d_{n+1}$, as $d - d_{n+1} \geq D_0$, we have $H_0(K_\bullet^{(n,\mathrm{top})})_{d-d_{n+1}} = 0$. Therefore, for any d with $d \geq D_0 + d_{n+1}$, we obtain an exact sequence

$$0 = H_1(K_\bullet^{(n,\mathrm{top})}))_d \longrightarrow H_1(K_\bullet^{(n+1,\mathrm{top})})_d \longrightarrow H_0(K_\bullet^{(n,\mathrm{top})})_{d-d_{n+1}} = 0,$$

so that $H_1(K_\bullet^{(n+1,\mathrm{top})})_d = 0$.

Next we consider the case where $m \geq n+1$ and we show that $H_1(K_\bullet^{(m,\mathrm{top})})_d = 0$ for $d \geq D_0 + d_m$ by the induction on m. So we assume that $H_1(K_\bullet^{(m,\mathrm{top})})_d = 0$ for $d \geq D_0 + d_m$. Then, for $d \geq D_0 + d_{m+1} \geq D_0 + d_m$, we have an exact sequence

$$0 = H_1(K_\bullet^{(m,\mathrm{top})})_d \longrightarrow H_1(K_\bullet^{(m+1,\mathrm{top})})_d \longrightarrow H_0(K_\bullet^{(m,\mathrm{top})})_{d-d_{m+1}}. \tag{3.2.1}$$

It follows from $H_0(K_\bullet^{(n,\mathrm{top})})_{d'} = 0$ for $d' \geq D_0$ that $H_0(K_\bullet^{(m,\mathrm{top})})_{d'} = 0$ by $F_{m-n}^{\mathrm{top}} \supset F_0^{\mathrm{top}}$. Therefore, we also have $H_0(K_\bullet^{(m,\mathrm{top})})_{d-d_{m+1}} = 0$ by $d - d_{m+1} \geq D_0$, whence $H_1(K_\bullet^{(m+1,\mathrm{top})})_d = 0$.

Finally we consider the case where $d_m \leq D_1$ and show $H_1(K_\bullet^{(m,\mathrm{top})})_d = 0$ for $d \geq D_0 + d_{n+1}$ by the induction on m in a similar manner as above. So we assume that $H_1(K_\bullet^{(m,\mathrm{top})})_d = 0$ for $d \geq D_0 + d_{n+1}$. Then, we consider the sequence (3.2.1) for $d \geq D_0 + d_{n+1}$ again. Thus it suffices to show that $H_0(K_\bullet^{(m,\mathrm{top})})_{d-d_{m+1}} = 0$.

Using $D_1 = \left\lfloor \frac{d_1+\cdots+d_{n+1}-n-1}{2} \right\rfloor + 1 \geq d_{m+1}$, we have

$$\begin{aligned} d - d_{m+1} &\geq D_0 + d_{n+1} - d_{m+1} \\ &\geq (d_1 + \cdots + d_{n+1} - n - 1) + 2 - \left(\left\lfloor \frac{d_1 + \cdots + d_{n+1} - n - 1}{2} \right\rfloor + 1 \right) \\ &\geq \left\lfloor \frac{d_1 + \cdots + d_{n+1} - n - 1}{2} \right\rfloor + 1 = D_1. \end{aligned}$$

Thus, it follows that $H_0(K_\bullet^{(n+1,\mathrm{top})})_{d-d_{m+1}} = 0$. Since one has $\langle F_{m-n}^{\mathrm{top}} \rangle \supset \langle F_1^{\mathrm{top}} \rangle$, the condition $H_0(K_\bullet^{(n+1,\mathrm{top})})_{d-d_{m+1}} = 0$ implies $H_0(K_\bullet^{(m,\mathrm{top})})_{d-d_{m+1}} = 0$, as desired. □

Theorem 3.2.3 (Theorem 2)**.** *Suppose that that $d_1 \leq d_2 \leq \cdots \leq d_m$ and $m > n$. If $\boldsymbol{F}^{\mathrm{top}}$ is semi-regular, then the generalized degree of regularity of $\langle F^h \rangle$ is upper-bounded by $d_1+d_2+\cdots+d_n+d_m-n$ and so the solving degree of F^h. Moreover, if $d_m \leq D_1$, the generalized degree of regularity of $\langle F^h \rangle$ is upper-bounded by $d_1 + \cdots + d_n + d_{n+1} - n$ and so the solving degree of F^h.*

Proof. We recall the long exact sequence of homology groups derived from the following exact sequence considered in the proof of Theorem 3.1.1:

$$0 \longrightarrow K_\bullet(F^h) \xrightarrow{\times y} K_\bullet(F^h) \xrightarrow{\pi_\bullet} K_\bullet(F^{\mathrm{top}}) \longrightarrow 0.$$

For $i = 0$ and $d \in \mathbb{N}$, we have the following exact sequence:

$$H_1(K_\bullet(F^{\mathrm{top}}))_d \longrightarrow H_0(K_\bullet(F^h))_{d-1} \xrightarrow{\times y} H_0(K_\bullet(F^h))_d \longrightarrow H_0(K_\bullet(F^{\mathrm{top}}))_d \longrightarrow 0.$$

Then, for $d \geq D_0 + d_m$ (or $d \geq D_0 + d_{n+1}$ if $d_m \leq D_1$), it follows from Proposition 3.2.2 that $H_1(K_\bullet(F^{\mathrm{top}}))_d = 0$. Moreover, $H_0(K_\bullet(F^{\mathrm{top}}))_d = 0$ also holds, since $d > D_0 \geq D$. Therefore, we have an exact sequence

$$0 \longrightarrow H_0(K_\bullet(F^h))_{d-1} \xrightarrow{\times y} H_0(K_\bullet(F^h))_d \longrightarrow 0,$$

and, by letting $A = R'/\langle F^h \rangle$, we have

$$A_{d-1} = H_0(K_\bullet(F^h))_{d-1} \cong H_0(K_\bullet(F^h))_d = A_d$$

for any $d \geq D_0 + d_m$ (or $d \geq D_0 + d_{n+1}$ if $d_m \leq D_1$). Moreover, the multiplication map by y from A_{d-1} to A_d is a bijection. Thus, the generalized degree of regularity of $\langle F^h \rangle$ is bounded by $D_0 + d_m - 1$ (or $D_0 + d_{n+1} - 1$ if $d_m \leq D_1$). Then, by Proposition 2.3.4, it bounds the solving degree (= $\max.\mathrm{GB}.\deg_{\prec^h}(F^h)$). □

Remark 3.2.4. The bound in Theorem 3.2.3 looks the same as Lazard's bound (Theorem 2.2.1). However, in our bound, except d_m, the degrees $d_1, \ldots, d_n$ are set in ascending order, while in Lazard's bound they are set in descending order. We note that, when $d_1 = \cdots = d_m$, these two bounds coincide with one another.

Finally in this subsection, under the assumption that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, we show that the generalized degree of regularity of $\langle F^h \rangle$ (and thus solving degree of F^h) can be bounded by D plus *the saturation exponent*, say S_0 here, that is, the minimal integer k such that $\langle F \rangle^h = (\langle F^h \rangle : y^\infty) = (\langle F^h \rangle : y^k)$. See [25, p. 81] for the definition of saturation exponent.

Proposition 3.2.5. *The generalized degree of regularity $\langle F^h \rangle$ and the solving degree of F^h are both bounded by $D + S_0$.*

Proof. Consider the following exact sequence:

$$0 \longrightarrow R'/\langle F\rangle^h(-S_0) \xrightarrow{\times y^{S_0}} R'/\langle F^h\rangle \longrightarrow R'/(\langle F^h\rangle + \langle y^{S_0}\rangle) \longrightarrow 0,$$

where $R'/(\langle F^h\rangle : \langle y^{S_0}\rangle) = R'/\langle F\rangle^h$. Then, we have

$$\mathrm{HS}_{R'/\langle F^h\rangle}(z) = \mathrm{HS}_{R'/(\langle F^h\rangle+\langle y^{S_0}\rangle)}(z) + z^{S_0}\mathrm{HS}_{R'/\langle F\rangle^h}(z).$$

First, we show $\mathrm{HF}_{R'/(\langle F^h\rangle+\langle y^{S_0}\rangle)}(d) = 0$ for $d \geq D + S_0$, by which we have $\mathrm{HF}_{R'/\langle F^h\rangle}(d) = \mathrm{HF}_{R'/\langle F\rangle^h}(d - S_0)$. Suppose for a contradiction that $(R'/(\langle F^h\rangle + \langle y^{S_0}\rangle))_d \neq 0$. Then, it follows from *Macaulay's basis theorem* (cf. [28, Theorem 1.5.7]) that

$$LB_d := \{t \in R'_d : t \text{ is a monomial and } t \notin \langle \mathrm{LM}(\langle F^h\rangle + \langle y^{S_0}\rangle)\rangle\}$$

is a non-empty basis for the K-vector space $(R'/(\langle F^h\rangle + \langle y^{S_0}\rangle))_d$. For any element T in LB_d, if T is divisible by y^{S_0}, then T belongs to $(\langle F^h\rangle + \langle y^{S_0}\rangle)_d$, which is a contradiction. Otherwise, the degree of the X-part of T is not smaller than D. Since $\mathrm{LM}(\langle F^h\rangle)$ contains any monomial in X of degree D by Lemma 4.1.4, it also contains T. Therefore $T \in \mathrm{LM}(\langle F^h\rangle + \langle y^{S_0}\rangle))$, which is a contradiction.

Next we show that $\mathrm{HF}_{R'/\langle F\rangle^h}(d)$ becomes constant for $d \geq D$, which implies that $\mathrm{HF}_{R'/\langle F^h\rangle}(d)$ becomes constant for $d \geq D+S_0$. Then, the generalized degree of regularity of $\langle F^h\rangle$ is bounded by $D+S_0$, and by Proposition 2.3.4, it follows that the solving degree of F^h is bounded by $D+S_0$.

Let G be the reduced Gröbner basis of $\langle F\rangle$ with respect to $\prec$. Then G^h is a Gröbner basis of $\langle F\rangle^h$. By Lemma 4.2.4 below, we have $\max.\mathrm{GB.deg}(F) \leq D$ and thus, any element of G^h is of degree not greater than D. Then, let $\{t_1, \ldots, t_r\}$ be the standard monomial basis of $R/\langle F\rangle$ as a K-vector space, that is, $\{t_1, \ldots, t_r\} = \{t : \mathrm{LM}(g) \nmid t \text{ for any } g \in G\}$ with $r := \dim_K R/\langle F\rangle$.

Again by Macaulay's basis theorem, as a basis of the K-linear space $(R'/\langle F\rangle^h)_d$, we can take $LB'_d = \{t \in R'_d : t \text{ is a monomial and } \mathrm{LM}(g) \nmid t \text{ for any } g \in G^h\}$, which is equal to $\{t_1 y^{k_1}, \ldots, t_r y^{k_r}\}$ for $d \geq D$, where $\deg(t_i y^{k_i}) = d$ for $1 \leq i \leq r$. Thus, for $d \geq D$, it follows that $\dim_K(R'/\langle F\rangle^h)_d$ is equal to the constant r. □

4 Behaviors of Gröbner bases computation

Here we show certain correspondences in the Gröbner basis computations among inputs F^h, F^{top}, and F. First we revisit the correspondence among the computation of the Gröbner basis of F^h and that of F^{top} given in [30, Section 5.1]. Then, we explicitly give an important correspondence between the computation of the Gröbner basis of F^h and that of F, which brings an upper-bound (Lemma 4.2.4 below) on the solving degree of F related to Samaev-Tenti's bound [40].

Here we use the same notation as in the previous section, and unless otherwise noted, assume that $\boldsymbol{F}$ is cryptographic semi-regular. Let G, G_{hom}, and G_{top} be the reduced Gröbner bases of $\langle F\rangle$, $\langle F^h\rangle$, and $\langle F^{\mathrm{top}}\rangle$, respectively, where their monomial orderings are DRL $\prec$ or its extension $\prec^h$. Also we let $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$, and assume $D < \infty$. Moreover, we extend the notion of *top part* to a homogeneous polynomial h in $R' = R[y]$ as follows. We call $h|_{y=0}$ the *top part* of h and denote it by h^{top}. Thus, if h^{top} is not zero, it coincides with the top part $(h|_{y=1})^{\mathrm{top}}$ of the dehomogenization $h|_{y=1}$ of h. We remark that $g^{\mathrm{top}} = (g^h)^{\mathrm{top}}$ for a polynomial g in R.

4.1 Correspondence between G_{hom} and G_{top}

Here we revisit the results in [30, Section 5.1].

Corollary 4.1.1 ([30, Corollary 2]). *With notation as above, assume that $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ is affine cryptographic semi-regular. Put $\overline{I} := \langle F^{\mathrm{top}} \rangle_R$ and $\tilde{I} := \langle F^h \rangle_{R'}$. Then, we have $(\langle \mathrm{LM}(\tilde{I}) \rangle_{R'})_d = (\langle \mathrm{LM}(\overline{I}) \rangle_{R'})_d$ for each d with $d < D := d_{\mathrm{reg}}(\overline{I})$.*

Since $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular and since $\boldsymbol{F}^h$ is D-regular by Corollary 3.1.5, we obtain $H_1(K_\bullet(F^{\mathrm{top}}))_{<D} = H_1(K_\bullet(F^h))_{<D} = 0$. Moreover, as $H_1(K_\bullet(F^h)) = \mathrm{syz}(F^h)/\mathrm{tsyz}(F^h)$ and $H_1(K_\bullet(F^{\mathrm{top}})) = \mathrm{syz}(F^{\mathrm{top}})/\mathrm{tsyz}(F^h)$ (see (A.1.2)), we have the following corollary, where tsyz denotes the module of trivial syzygies (see Definition A.1.1).

Corollary 4.1.2 ([14, Theorem 1]). *With notation as above, we have $\mathrm{syz}(F^{\mathrm{top}})_{<D} = \mathrm{tsyz}(F^{\mathrm{top}})_{<D}$ and $\mathrm{syz}(F^h)_{<D} = \mathrm{tsyz}(F^h)_{<D}$.*

Remark 4.1.3. Corollary 4.1.2 implies that, in the Gröbner basis computation G_{hom} with respect to a graded ordering $\prec^h$, if an S-polynomial $S(g_1, g_2) = t_1 g_1 - t_2 g_2$ of degree less than D is reduced to 0, it comes from some trivial syzyzy, that is, $\sum_{i=1}^m (t_1 a_i^{(1)} - t_2 a_i^{(2)} - b_i)\mathbf{e}_i$ belongs to $\mathrm{tsyz}(F^h)_{<D}$, where $g_1 = \sum_{i=1}^m a_i^{(1)} f_i^h$, $g_2 = \sum_{i=1}^m a_i^{(2)} f_i^h$, and $S(g_1, g_2) = \sum_{i=1}^m b_i f_i^h$ is obtained by Σ-reduction in the F_5 algorithm (or its variant such as the matrix-F_5 algorithm) with the *Schreyer ordering*. Thus, since the F_5 algorithm (or its variant) automatically discards an S-polynomial whose signature is the LM of some trivial syzygy, we can avoid unnecessary S-polynomials. See [17] for the F_5 algorithm and its variant, and also for the syzygy criterion.

In addition to the above facts, as mentioned (somehow implicitly) in [1, Section 3.5] and [3], when we compute a Gröbner basis of $\langle F^h \rangle$ for the degree less than D by the F_5 algorithm with respect to $\prec^h$, for each computed non-zero polynomial g from an S-polynomial, say $S(g_1, g_2)$, of degree less than D, its signature does not come from any trivial syzygy and so the reductions of $S(g_1, g_2)$ are done only at its top part. This implies that any degree-fall does not occur at each step degree less than D. This can be rigidly shown by using the injectiveness of the multiplication map by y shown in Remark 3.1.2.

Now we recall that the Gröbner basis computation process of $\langle F^h \rangle$ corresponds exactly to that of $\langle F^{\mathrm{top}} \rangle$ at each step degree less than D. (We also discuss similar correspondences among the Gröbner basis computation of $\langle F^h \rangle$ and that of $\langle F \rangle$ in the next subsection.) Especially, the following lemma holds.

Lemma 4.1.4 ([30, Lemma 2]). *With notation as above, assume that $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ is affine cryptographic semi-regular. For each degree $d < D$, we have*

$$\mathrm{LM}(G_{\mathrm{hom}})_d = \mathrm{LM}(G_{\mathrm{top}})_d. \tag{4.1.1}$$

We also note that the argument and the proof of Lemma 4.1.4 can be considered as a corrected version of [38, Theorem 4].

Next we consider $(G_{\mathrm{hom}})_D$. The following lemma holds, not assuming that $\boldsymbol{F}$ is affine cryptographic semi-regular:

Lemma 4.1.5 ([30, Lemma 3]). *Assume that $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) < \infty$ (the assumption that $\boldsymbol{F}$ is affine cryptographic semi-regular is not necessary). Then, for each monomial M in X of degree D, there is an element g in $(G_{\mathrm{hom}})_{\leq D}$ such that $\mathrm{LM}(g)$ divides M. Therefore,*

$$\langle \mathrm{LM}((G_{\mathrm{hom}})_{\leq D}) \rangle_{R'} \cap R_D = R_D. \tag{4.1.2}$$

Moreover, for each element g in $(G_{\mathrm{hom}})_D$ with $g^{\mathrm{top}} \neq 0$, the top-part g^{top} consists of one term, that is, $g^{\mathrm{top}} = \mathrm{LT}(g)$, where LT denotes the leading term of g. (We recall $\mathrm{LT}(g) = \mathrm{LC}(g)\mathrm{LM}(g)$.)

Remark 4.1.6. If we apply a signature-based algorithm such as the F_5 algorithm or its variant to compute the Gröbner basis of $\langle F^h \rangle$, its Σ-Gröbner basis is a Gröbner basis, but is not always *reduced* in the sense of ordinary Gröbner basis, in general. In this case, we have to compute so called *inter-reduction* among elements of the Σ-Gröbner basis to obtain the reduced Gröbner basis.

4.2 Correspondence between the computations of G_{hom} and G

In this subsection, we show that, at early stages, there is a strong correspondence between the computation of G_{hom} and that of G, from which we shall extend the upper bound on solving degree given in [40, Theorem 2.1] to our case.

Remark 4.2.1. In [40], polynomial ideals over $R = \mathbb{F}_q[x_1, \ldots, x_n]$ are considered. Under the condition where the generating set F contains the field equations $x_i^q - x_i$ for $1 \leq i \leq n$, recall from Theorem 2.2.5 ([41, Theorem 6.5 & Corollary 3.67]) that the solving degree $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ in the strict sense (see the definition (I) of Subsection 2.2 for the definition) with respect to a Buchberger-like algorithm $\mathcal{A}$ for $\langle F \rangle$ is upper-bounded by $2D - 2$, where $D = d_{\deg}(\langle F^{\mathrm{top}} \rangle)$. In the proofs of [41, Theorem 6.5 & Corollary 3.67], the property $\langle F^{\mathrm{top}} \rangle_D = R_D$ was essentially used for obtaining the upper-bound. As the property also holds in our case, we may apply their arguments. Also in [4, Section 3.2], the case where F^h is cryptographic semi-regular is considered. The results on the solving degree and the maximal degree of the Gröbner basis are heavily related to our results in this subsection.

Here we examine how two computations look like each other in early stages when we use the normal selection strategy on the choice of S-polynomials with respect to the monomial ordering $\prec^h$. Here we denote by $\mathcal{G}_{\mathrm{hom}}$ the set of intermediate polynomials during the computation of G_{hom}, and denote by $\mathcal{G}$ that of G, namely, $\mathcal{G}$ and $\mathcal{G}_{\mathrm{hom}}$ may not be reduced and G and G_{hom} are obtained by applying so-called "inter-reduction" to $\mathcal{G}$ and $\mathcal{G}_{\mathrm{hom}}$, respectively.

Phase 1: Before degree fall in the computation of G: The computation of $\mathcal{G}$ can simulate faithfully that of $\mathcal{G}_{\mathrm{hom}}$ until the degree of computed polynomials becomes $D-1$. Here, we call this stage an *early stage* and denote by $\mathcal{G}^{(e)}$ and $\mathcal{G}_{\mathrm{hom}}^{(e)}$ the set of all elements in $\mathcal{G}$ and that in $\mathcal{G}_{\mathrm{hom}}$ computed in an early stage, respectively.

In this process, we can make the following correspondence among $\mathcal{G}^{(e)}$ and that of $\mathcal{G}_{\mathrm{hom}}^{(e)}$ by *carefully choosing S-polynomials and their reducers*:

$$\mathcal{G}_{\mathrm{hom}}^{(e)} \ni g \longleftrightarrow g^{\mathrm{deh}} \in \mathcal{G}^{(e)}.$$

We can show it by induction on the degree. Consider a step where two polynomial g_1 and g_2 in $\mathcal{G}_{\mathrm{hom}}^{(e)}$ are chosen such that its S-polynomial $S(g_1, g_2) = t_1 g_1 - t_2 g_2$ is of degree $d < D$, where t_1 and t_2 are terms (monomials with non-zero coefficients), $\deg(t_1 g_1) = \deg(t_2 g_2) = d$ and $\mathrm{LCM}(\mathrm{LM}(g_1), \mathrm{LM}(g_2)) = \mathrm{LM}(t_1 g_1) = \mathrm{LM}(t_2 g_2)$. From $S(g_1, g_2)$, we obtain a new element $g_3 \neq 0$ by using some $h_1, \ldots, h_t$ in $\mathcal{G}_{\mathrm{hom}}^{(e)}$ as reducers, where $h_1, \ldots, h_t$ are already produced before the computation of $S(g_1, g_2)$. That is, g_3 can be written as

$$g_3 = t_1 g_1 - t_2 g_2 - \sum_{i=1}^{t} b_i h_i$$

for some $b_1, \ldots, b_t$ in R such that $\mathrm{LM}(b_i h_i) \preceq \mathrm{LM}(S(g_1, g_2))$ for every i. Simultaneously, for the counter part in $\mathcal{G}^{(e)}$, two polynomial g_1^{deh} and g_2^{deh} are chosen by induction. Then we can make the obtained new element from the S-polynomial $S(g_1^{\mathrm{deh}}, g_2^{\mathrm{deh}})$ equal to g_3^{deh}. Indeed, as there is no degree-fall for $< D$ by Lemma 4.1.4 (since F^{top} is cryptographic semi-regular), we have $\mathrm{LM}(S(g_1,g_2)) = \mathrm{LM}(S(g_1^{\mathrm{deh}},g_2^{\mathrm{deh}}))$, whence the condition $\mathrm{LM}(b_ih_i) \preceq^h \mathrm{LM}(S(g_1,g_2))$ is equivalent to $\mathrm{LM}(b_i^{\mathrm{deh}}h_i^{\mathrm{deh}}) \preceq \mathrm{LM}(S(g_1^{\mathrm{deh}},g_2^{\mathrm{deh}}))$. Since $h_1^{\mathrm{deh}},\dots,h_t^{\mathrm{deh}}$ are already computed before the computation of $S(g_1^{\mathrm{deh}},g_2^{\mathrm{deh}})$ by induction, the following expression

$$g_3^{\mathrm{deh}} = t_1g_1^{\mathrm{deh}} - t_2g_2^{\mathrm{deh}} - \sum_{i=1}^t b_i^{\mathrm{deh}}h_i^{\mathrm{deh}}$$

matches to the reduction process of $S(g_1^{\mathrm{deh}},g_2^{\mathrm{deh}})$. (It can be easily checked by our induction hypothesis that g_3^{deh} cannot be reduced by any element in $\mathcal{G}^{(e)}$ already computed before the computation of $S(g_1^{\mathrm{deh}},g_2^{\mathrm{deh}})$.) Here we note that, since we use the *normal selection strategy*, each pair (g_1,g_2) is chosen simply by checking $\mathrm{LCM}(\mathrm{LM}(g_1),\mathrm{LM}(g_2))$. Moreover, also by synchronizing the choice of reducers, the computation of reduction of $S(g_1^{\mathrm{deh}},g_2^{\mathrm{deh}})$ can be synchronized faithfully with that of g_3 in $G_{\mathrm{hom}}^{(e)}$ at this early stage.

Conversely, we can make the computation of $\mathcal{G}_{\mathrm{hom}}^{(e)}$ to match with that of $\mathcal{G}^{(e)}$ at an early stage in the same manner. Thus, we have $\mathrm{LM}(\mathcal{G}^{(e)}) = \mathrm{LM}(\mathcal{G}_{\mathrm{hom}}^{(e)})$ in this case. Of course, the reduction computation for each S-polynomial depends on the choice of reducers, and some elements might be not synchronized faithfully in actual computation. However, the set $\mathrm{LM}(\mathcal{G}_{\mathrm{hom}}^{(e)})$ is automatically minimal, that is, it has no element g in $\mathcal{G}_{\mathrm{hom}}^{(e)}$ such that $\mathrm{LM}(g)$ is divisible by $\mathrm{LM}(g')$ for some its another element g' in $\mathcal{G}_{\mathrm{hom}}^{(e)}$. Thus, $\mathrm{LM}(\mathcal{G}_{\mathrm{hom}}^{(e)})$ coincides with $\mathrm{LM}((G_{\mathrm{hom}})_{<D})$, that is, it does not depend on the process for the computation of G_{hom}. Hence, we have the following:

Lemma 4.2.2. *$LM(\mathcal{G}^{(e)})$ coincides with $LM(\mathcal{G}_{\mathrm{hom}}^{(e)}) = \mathrm{LM}((G_{\mathrm{hom}})_{<D})$.*

Phase 2: At the step degree D: Next we investigate the computation of G_{hom} at the step degree D. In this phase, there might occur some *degree fall*, from which the computation process would become very complicated. Thus, to simply our investigation, we also assume to use the *sugar strategy* for the computation of G, by which the computational behaviour becomes very close to that for G_{hom}. See [13] for details on the sugar strategy.

After the computation at the step degree $D-1$, we enter the computation at step degree D. In this phase, pairs of degree D in $\mathcal{G}_{\mathrm{hom}}^{(e)}$ are chosen. Simultaneously, corresponding pairs in $\mathcal{G}_{\mathrm{hom}}$ of degree D are chosen. (Here we continue to synchronize the computation of $\mathcal{G}^{(e)}$ and that of $\mathcal{G}_{\mathrm{hom}}^{(e)}$ as in Phase 1.) Thus, we extend the notations $\mathcal{G}_{\mathrm{hom}}^{(e)}$ and $\mathcal{G}^{(e)}$ to the step degree D. Let $\mathcal{G}_{\mathrm{hom}}^{(e),D}$ be the set of all elements obtained at the step degree D, each of which is computed from an S-polynomial (g_1,g_2) such that g_1 and g_2 belong to $\mathcal{G}_{\mathrm{hom}}^{(e)}$ and $S(g_1,g_2)$ is of degree D. Similarly we let $\mathcal{G}^{(e),D}$ be the set of all elements in $\mathcal{G}$ obtained at the step degree D. We note that no element in $\mathcal{G}_{\mathrm{hom}}^{(e),D}$ is used for constructing an S-polynomial at this phase, and so for $\mathcal{G}^{(e),D}$.

Let (g_1,g_2) be a pair in $\mathcal{G}_{\mathrm{hom}}^{(e)}$ such that its S-polynomial $S(g_1,g_2)$ is reduced to g_3 and $\mathrm{LM}(g_3)$ is not divisible by y. Consider the step where (g_1,g_2) is chosen, and simultaneously, its corresponding pair $(g_1^{\mathrm{deh}},g_2^{\mathrm{deh}})$ is also chosen. Let g' be an element computed from the corresponding S-polynomial $S(g_1^{\mathrm{deh}},g_2^{\mathrm{deh}})$. Then g_3 is obtained from $S(g_1,g_2) = t_1g_1 - t_2g_2$ as

$$g_3 = t_1g_1 - t_2g_2 - \sum_{i=1}^t b_ih_i$$

by reducers $h_1,\dots,h_t$ in $\mathcal{G}_{\mathrm{hom}}^{(e)}$. Simultaneously, $S(g_1^{\mathrm{deh}},g_2^{\mathrm{deh}})$ can be also reduced to g_3^{deh} by reducers $h_1^{\mathrm{deh}},\dots,h_t^{\mathrm{deh}}$;

$$g_3^{\mathrm{deh}} = t_1g_1^{\mathrm{deh}} - t_2g_2^{\mathrm{deh}} - \sum_{i=1}^t b_i^{\mathrm{deh}}h_i^{\mathrm{deh}}.$$

If g_3^{deh} is not reducible by any element in $\mathcal{G}^{(e)} \cup \mathcal{G}^{(e),D}$ already computed before the computation of $S(g_1^{\mathrm{deh}}, g_2^{\mathrm{deh}})$, then $\mathrm{LM}(g_3^{\mathrm{deh}}) = \mathrm{LM}(g')$. So, there is still a correspondence, and $\langle \mathrm{LM}(\mathcal{G}^{(e)} \cup \mathcal{G}^{(e),D}) \rangle$ contains $\mathrm{LM}(g_3^{\mathrm{deh}})$. Otherwise, $\mathrm{LM}(g_3^{\mathrm{deh}})$ is divisible by $\mathrm{LM}(g'')$ for some g'' already computed elements in $\mathcal{G}^{(e)} \cup \mathcal{G}^{(e),D}$ at the step degree D. This implies that $\langle \mathrm{LM}(\mathcal{G}^{(e)} \cup \mathcal{G}^{(e),D}) \rangle$ contains $\mathrm{LM}(g_3^{\mathrm{deh}})$, which holds for any pair (g_1, g_2) generated at the step degree D. Hence, $\langle \mathrm{LM}(\mathcal{G}^{(e)} \cup \mathcal{G}^{(e),D}) \rangle$ includes $\mathrm{LM}((G_{\mathrm{hom}})_{\leq D}) \cap R_D$. Therefore, $\langle \mathrm{LM}(\mathcal{G}^{(e)} \cup \mathcal{G}^{(e),D}) \rangle$ contains all monomials of degree D in X, since $\langle \mathrm{LM}((G_{\mathrm{hom}})_{\leq D}) \rangle_{R'} \cap R_D = R_D$ by Lemma 4.1.5. Thus, we have the following lemma.

Lemma 4.2.3. $\langle \mathrm{LM}(\mathcal{G}^{(e)} \cup \mathcal{G}^{(e),D}) \rangle$ *contains all monomials in X of degree $\geq D$.*

Solving degree of F as the highest step degree: Here we show an upper-bound on the highest step degree appeared in the computation of G with respect to the DRL ordering by a Buchberger-like algorithm $\mathcal{A}$ based on S-polynomials with the normal strategy and the sugar strategy. We note that, in [30, Lemma 4.2.4], we restart the computation of the Gröbner basis of F from $H = \{g|_{y=1} : g \in (G_{\mathrm{hom}})_{\leq D}\}$. However, here we do not need $(G_{\mathrm{hom}})_{\leq D}$. We refer to [8, Remark 15] for another proof of $\mathrm{max.GB.deg}_{\prec}(F) \leq D$.

Lemma 4.2.4 (cf. [30, Lemma 4])**.** *Assume that $D \geq \max\{\deg(f) : f \in F\}$, and that $\prec$ is a DRL ordering on the set of monomials in R. Then, it follows that* $\mathrm{max.GB.deg}_{\prec}(F) \leq D$*. Moreover, there exists a Buchberger-like algorithm $\mathcal{A}$ with normal strategy such that*

$$\mathrm{sd}_{\prec}^{\mathcal{A}}(F) \leq 2D - 1,$$

and

$$\mathrm{sd}_{\prec}^{\mathcal{A}}(F) \leq 2D - 2.$$

in the strict sense (see (I) in Subsection 2.2 for details on the definition of these solving degrees). Namely, the maximal degree of S-polynomials generated during the execution of $\mathcal{A}$ is bounded by $2D - 2$.

Remark 4.2.5. We refer to [8, Remark 15] for another proof of $\mathrm{max.GB.deg}_{\prec}(F) \leq D$. We also note that, if $D = d_{\mathrm{reg}}(F^{\mathrm{top}}) < \infty$, Lemma 4.2.3 and Lemma 4.2.4 hold without the assumption that F^{top} is cryptographic semi-regular.

Remark 4.2.6 (cf. [30, Section 5.2])**.** As to the computation of G_{hom}, we have a result similar to Lemma 4.2.4. Since $\langle \mathrm{LM}(G_{\mathrm{hom}})_{\leq D} \rangle$ contains all monomials in X of degree D, for any polynomial g generated in the middle of the computation of G_{hom} the degree of the X-part of $\mathrm{LM}(g)$ is less than D. Because g is reduced by $(G_{\mathrm{hom}})_{\leq D}$. Thus, letting $\mathcal{U}$ be the set of all polynomials generated during the computation of G_{hom}, we have

$$\{\text{The } X\text{-part of } \mathrm{LM}(g) : g \in \mathcal{U}\} \subset \{x_1^{e_1} \cdots x_n^{e_n} : e_1 + \cdots + e_n \leq D\}.$$

As different $g, g' \in \mathcal{U}$ can not have the same X-part in their leading terms, the size $\#\mathcal{U}$ is upper-bounded by the number of monomials in X of degree not greater than D, that is $\binom{n+D}{n}$. By using the F_5 algorithm or its efficient variant, under an assumption that every unnecessary S-polynomial can be avoided, the number of computed S-polynomials during the computation of G_{hom} coincides with the number $\#\mathcal{U}$ and is upper-bounded by $\binom{n+D}{n}$.

We review a simple example shown in [30, Example 1] and examine the correspondences discussed in this and the previous subsections.

Example 4.2.7. We give a simple example. Let $p = 73$, $K = \mathbb{F}_p$, and

$$\begin{aligned}
f_1 &= x_1^2 + 3x_1x_2 + x_2^2 - 2x_1x_3 - 2x_2x_3 + x_3^2 - x_1 - 2x_2 + x_3,\\
f_2 &= 4x_1^2 + 3x_1x_2 + 4x_1x_3 + x_3^2 - 2x_1 - x_2 + 2x_3,\\
f_3 &= 3x_1^2 + 9x_2^2 - 6x_2x_3 + x_3^2 - x_1 + x_2 - x_3,\\
f_4 &= x_1^2 - 6x_1x_2 + 9x_2^2 + 2x_1x_3 - 6x_2x_3 + 2x_3^2 - 2x_1 + x_2.
\end{aligned}$$

Then, $d_1 = d_2 = d_3 = d_4 = 2$. As their top parts (maximal total degree parts) are

$$\begin{aligned}
f_1^{\rm top} &= x_1^2 + 3x_1x_2 + x_2^2 - 2x_1x_3 - 2x_2x_3 + x_3^2,\\
f_2^{\rm top} &= 4x_1^2 + 3x_1x_2 + 4x_1x_3 + x_3^2,\\
f_3^{\rm top} &= 3x_1^2 + 9x_2^2 - 6x_2x_3 + x_3^2,\\
f_4^{\rm top} &= x_1^2 - 6x_1x_2 + 9x_2^2 + 2x_1x_3 - 6x_3x_2 + 2x_3^2,
\end{aligned}$$

one can verify that $\boldsymbol{F}^{\rm top}$ is cryptographic semi-regular (and furthermore, $\boldsymbol{F}^{\rm top}$ is semi-regular). Then its degree of regularity is equal to 3. Indeed, the reduced Gröbner basis $G_{\rm top}$ of the ideal $\langle F^{\rm top}\rangle$ with respect to the DRL ordering $x_1 \succ x_2 \succ x_3$ is

$$\{\underline{x_2x_3^2},\ \underline{x_3^3},\ \underline{x_1^2} + 68x_2x_3 + 55x_3^2,\ \underline{x_1x_2} + 27x_2x_3 + 29x_3^2,\ \underline{x_2^2} + x_2x_3 + 71x_3^2,\ \underline{x_1x_3} + 3x_2x_3 + 33x_3^2\}.$$

Then its leading monomials are $x_2x_3^2, x_3^3, x_1^2, x_1x_2, x_2^2, x_1x_3$ and its Hilbert-Poincaré series satisfies

$$\mathrm{HS}_{R/\langle F^{\rm top}\rangle}(z) = 2z^2 + 3z + 1 = \left(\frac{(1-z^2)^4}{(1-z)^3} \bmod z^3\right),$$

whence the degree of regularity of $\langle F^{\rm top}\rangle$ is 3.

On the other hand, the reduced Gröbner basis $G_{\rm hom}$ of the ideal $\langle F^h\rangle$ with respect to the DRL ordering $x_1 \succ x_2 \succ x_3 \succ y$ is

$$\begin{aligned}
&\{\underline{x_1y^3},\ \underline{x_2y^3},\ \underline{x_3y^3},\ \underline{x_2x_3^2} + 60x_1y^2 + 22x_2y^2 + 39x_3y^2,\\
&\underline{x_3^3} + 72x_1y^2 + 14x_2y^2 + 56x_3y^2,\ \underline{x_2x_3y} + 16x_1y^2 + 55x_2y^2 + 38x_3y^2,\\
&\underline{x_3^2y} + 72x_1y^2 + 66x_2y^2 + 70x_3y^2,\ \underline{x_1^2} + 68x_2x_3 + 55x_3^2 + 72x_1y + 40x_2y + 14x_3y,\\
&\underline{x_1x_2} + 27x_2x_3 + 29x_3^2 + 20x_1y + 37x_2y + 12x_3y,\\
&\underline{x_2^2} + x_2x_3 + 71x_3^2 + 57x_1y + 3x_2y + 52x_3y,\\
&\underline{x_1x_3} + 3x_2x_3 + 33x_3^2 + 22x_1y + 5x_2y + 14x_3y\}
\end{aligned}$$

and its leading monomials are $x_1y^3, x_2y^3, x_3y^3, x_2x_3^2, x_3^3, x_2x_3y, x_3^2y, x_1^2, x_1x_2, x_2^2, x_1x_3$. Then the Hilbert-Poincaré series of $R'/\langle F^h\rangle$ satisfies

$$\left(\mathrm{HS}_{R'/\langle F^h\rangle}(z) \bmod z^3\right) = \left(6z^2 + 4z + 1 \bmod z^3\right) = \left(\frac{(1-z^2)^4}{(1-z)^4} \bmod z^3\right).$$

We note that $\mathrm{HF}_{R'/\langle F^h\rangle}(3) = 4$ and $\mathrm{HF}_{R'/\langle F^h\rangle}(4) = 1$. We can also examine the *correspondence* $\mathrm{LM}(G_{\rm hom})_{<D} = \mathrm{LM}(G_{\rm top})_{<D}$ and, for $g \in G_{\rm hom}$, if $\mathrm{LM}(g)$ is divided by y, then $\deg(g) \geq D = 3$. Thus, any *degree-fall* cannot occur at degree less than $3 = D$.

Finally, we examine the correspondence between $\mathcal{G}^{(e)} \cup \mathcal{G}^{(e),D}$ and $(G_{\rm hom})_{\leq D}$. The reduced Gröbner basis of $\langle F\rangle$ with respect to $\prec$ is $\{x, y, z\}$ and we can examine that $\mathrm{LM}(\mathcal{G}^{(e)})$ coincides with $\mathrm{LM}(G_{\mathrm{hom}})_{<3}$. Because we have the following $\mathcal{G}$ without inter-reduction (see the paragraph just after Remark 4.2.1 for the definition of $\mathcal{G}$);

$$\begin{aligned}
&\{\underline{x_1^2} + 3x_1x_2 + x_2^2 + 71x_1x_3 + 71x_2x_3 + x_3^2 + 72x_1 + 71x_2 + x_3,\\
&\underline{x_1x_2} + 41x_2^2 + 23x_1x_3 + 64x_2x_3 + 49x_3^2 + 16x_1 + 56x_2 + 57x_3,\\
&\underline{x_2^2} + 14x_1x_3 + 43x_2x_3 + 22x_3^2 + 29x_3,\ \underline{x_1x_3} + 3x_2x_3 + 33x_3^2 + 22x_1 + 5x_2 + 14x_3,\\
&\underline{x_2x_3^2} + 41x_3^3 + 5x_2x_3 + 35x_3^2 + 64x_1 + 42x_2 + 11x_3,\ \underline{x_3^3} + 35x_3^2 + 37x_1 + 61x_2 + 24x_3,\\
&\underline{x_3x_2} + 13x_3^2 + 3x_1 + 37x_2 + 72x_3,\ \underline{x_3^2} + 72x_1 + 66x_2 + 70x_3,\\
&\underline{x_1} + 61x_2 + 51x_3,\ \underline{x_2} + 70x_3,\ \underline{x_3}\},
\end{aligned}$$

and $\mathrm{LM}(\mathcal{G}^{(e)}) = \{x_1^2, x_1x_2, x_2^2, x_1x_3\}$. Moreover, $\mathrm{LM}(G_{\mathrm{hom}})_D$ coincides with $\mathrm{LM}(\mathcal{G}^{(e),D})$, as it is $\{x_2x_3^2, x_3^3, x_2x_3, x_3^2\}$. We note that we have removed f_2, f_3, f_4 from $\mathcal{G}$ as they have the same LM as f_1. Interestingly, in this case, we can see that the whole $\mathrm{LM}(\mathcal{G})$ corresponds to $\mathrm{LM}(G_{\mathrm{hom}})$.

4.3 Experimental observation and a variant of Fröberg's conjecture

In this subsection, we observe actual behavior of Gröbner basis computation from a part of our experimental results. For experiments, we used Magma V2.25-3 [5]. In particular, the built-in functions `Dimension`, `HilbertSeries`, and `GroebnerBasis` were applied. In our experiments, given n, m, $(d_1, \ldots, d_m)$, and an odd prime q with $n < m$ and $d_i \geq 2$ (for the case where $n = m$, see Remark 4.3.3 below), we generate inhomogeneous polynomials $f_1, \ldots, f_m$ in $R = \mathbb{F}_q[x_1, \ldots, x_n]$ of degrees $d_1, \ldots, d_m$ whose constant terms are all zero (as in Example 4.2.7), where coefficients are chosen uniformly at random. Note that, for any sequence $\boldsymbol{F} = (f_1, \ldots, f_m)$ generated in this way, the homogenization F^h with $F = \{f_1, \ldots, f_m\}$ always has a non-trivial root $(0, \ldots, 0, 1)$: Any sequence of m polynomials (in R) that has at least one root is transformed by a linear coordinate change into a polynomial sequence $(f_1, \ldots, f_m) \in R^m$ such that each f_i has no constant term. Moreover, $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ is expected to be cryptographic semi-regular (in fact, semi-regular) with high probability. Therefore, our setting causes no loss of generality.

As an experimental result, we heuristically find an upper-bound

$$\deg\left(\left[\frac{\prod_{i=1}^{m}(1 - z^{d_i})}{(1 - z)^{n+1}}\right]\right) + 1 \tag{4.3.1}$$

on the maximal Gröbner basis degree $\mathrm{max.GB.deg}_{\prec^h}(F^h)$, which is sharper than our upper-bound provided in Theorem 2 (1). This sharper bound comes from a property that $\boldsymbol{F}^h$ is generalized cryptographic semi-regular (i.e., D'-regular), where we set $D' := \widetilde{d}_{\mathrm{reg}}(F^h)$: We confirmed in our experiments that $\boldsymbol{F}^h$ satisfies this property in most cases. Here we use the following lemma (the proof is straightfoward):

Lemma 4.3.1. *Let $\boldsymbol{F} = (f_1, \ldots, f_m) \in (R \smallsetminus K)^m$ be a sequence of not necessarily homogeneous polynomial. Assume that $n < m$. Then we have the following:*

1. *If F^h has at least one solution and if $\boldsymbol{F}^h$ is D'-regular (and thus $D' < \infty$), then D' is upper-bounded by (4.3.1).*
2. *If $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, then $D := d_{\mathrm{reg}}(F^{\mathrm{top}})$ is also upper-bounded by (4.3.1) (this also holds even if $n = m$).*

Supposing both the assumptions in this lemma, we have

$$\max.\mathrm{GB.deg}_{\prec^h}(F^h) \leq \max\{D, D'\} \leq \deg\left(\left[\frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^{n+1}}\right]\right) + 1$$

by Proposition 2.3.4. We compare exact values for several bounds, for $n = 9$ and 10 with some conditions on m and $(d_1, \ldots, d_m)$ in Tables 1 and 2, where we set $D := d_{\mathrm{reg}}(F^{\mathrm{top}})$ for the case where $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular.

Table 1: Exact values for several upper-bounds on $\max.\mathrm{GB.deg}_{\prec^h}(F^h)$ (which is equal to the solving degree of F^h in this case) in the case where $n \in \{9, 10\}$, $n+1 \leq m \leq 2n$, and $d_1 = \cdots = \cdots = d_m = 2$. The first table is for the case $n = 9$, and the second one is for the case $n = 10$.

The number m ($> n = 9$) of polynomials	10	11	12	13	14	15	16	17	18
Lazard's bound (Theorem 2.2.1)	11	11	11	11	11	11	11	11	11
Our bound in Theorem 2 (1)	11	11	11	11	11	11	11	11	11
Heuristic bound (4.3.1) (Conjecture 4.3.4)	11	6	6	5	5	4	4	4	4
D for semi-regular F^{top}	6	5	5	4	4	4	4	4	4
$2D-1$ (Theorem 3 (4))	11	9	9	7	7	7	7	7	7

The number m ($> n = 10$) of polynomials	11	12	13	14	15	16	17	18	19	20
Lazard's bound (Theorem 2.2.1)	12	12	12	12	12	12	12	12	12	12
Our bound in Theorem 2 (1)	12	12	12	12	12	12	12	12	12	12
Heuristic bound (4.3.1) (Conjecture 4.3.4)	12	7	6	5	5	5	5	4	4	4
D for semi-regular $\boldsymbol{F}^{\mathrm{top}}$	6	6	5	5	4	4	4	4	4	4
$2D-1$ (Theorem 3 (4))	11	11	9	9	7	7	7	7	7	7

Table 2: Exact values for several upper-bounds on $\max.\mathrm{GB.deg}_{\prec^h}(F^h)$ (which is equal to the solving degree of F^h in this case) in the case where $n \in \{9, 10\}$, $n+1 \leq m \leq 2n$, $d_1 = \cdots = d_n = 3$, and $d_{n+1} = \cdots = d_m = 2$. The first table is for the case $n = 9$, and the second one is for the case $n = 10$.

The number m ($> n = 9$) of polynomials	10	11	12	13	14	15	16	17	18
Lazard's bound (Theorem 2.2.1)	20	20	20	20	20	20	20	20	20
Our bound in Theorem 2 (1)	20	19	18	17	16	15	14	13	12
Heuristic bound (4.3.1) (Conjecture 4.3.4)	20	11	9	8	7	7	6	6	5
D for semi-regular F^{top}	10	9	8	7	6	6	6	5	5
$2D-1$ (Theorem 3 (4))	19	17	15	13	11	11	9	9	9

The number m ($> n = 10$) of polynomials	11	12	13	14	15	16	17	18	19	20
Lazard's bound (Theorem 2.2.1)	22	22	22	22	22	22	22	22	22	22
Our bound in Theorem 2 (1)	22	21	20	19	18	17	16	15	14	13
Heuristic bound (4.3.1) (Conjecture 4.3.4)	22	12	10	9	8	7	7	6	6	6
D for semi-regular $\boldsymbol{F}^{\mathrm{top}}$	11	10	9	8	7	6	6	6	5	5
$2D-1$ (Theorem 3 (4))	21	19	17	15	13	11	11	11	9	9

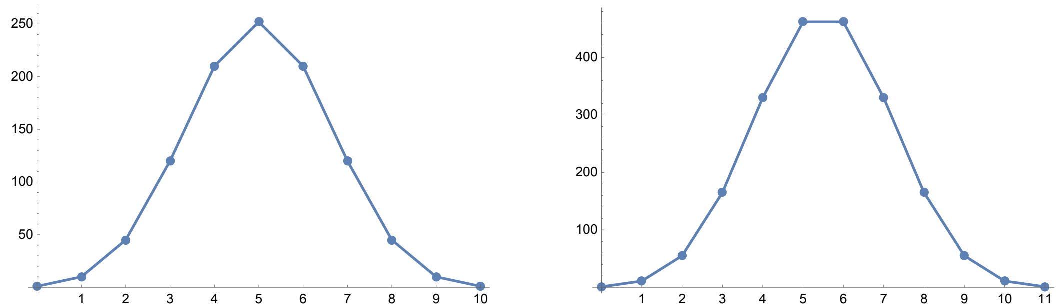

Figure 1: The values of coefficients in $(1+z)^{n+1}$ for $(n,m) = (9,10)$ (the left figure) and $(n,m) = (10,11)$ (the right figure). The horizontal axis indicates the degree i of z^i, and the vertical axis indicates the value of the coefficient of z^i. Note that $D = (n+3)/2$ for an odd n and $D = (n+2)/2$ for even n, and thus $D-1 = 5$ for $n \in \{9, 10\}$. See Remark 4.3.2 for a description.

Remark 4.3.2. Note that, if $m = n+1$, then it follows from $\frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^{n+1}} = \prod_{i=1}^{n+1}(1+z+\cdots+z^{d_i-1})$ that the bound (4.3.1) is equal to $\sum_{j=1}^{n+1}(d_j-1)+1$, which is equal to Lazard's bound. As a more particular case, if $d_i = 2$ for all i, then it is equal to $n+2$. On the other hand, recall from [4, Theorem 4.1] that $D = \lfloor (n+1)/2 \rfloor + 1$, and thus $2D-1$ is equal to $n+2$ if n is odd and to $n+1$ if n is even. More precisely, assuming the D'-regularity of F^h, we have

$$\mathrm{HS}_{R'/\langle F^h \rangle}(z) \equiv (1+z)^{n+1} \pmod{z^{D'}},$$

where $(1+z)^{n+1} = \sum_{i=0}^{n+1}\binom{n+1}{i} z^i$. In the expansion of $(1+z)^{n+1}$, the coefficient of $z^{(n+1)/2}$ is (resp. the coefficients of $z^{n/2}$ and $z^{(n+2)/2}$ are) maximal among the non-zero coefficients for an odd (resp. even) n, see Figure 1 for some specific n. In particular, if n is even, then we have $D = n/2+1$ and $\dim_K(R'/\langle F^h \rangle)_{D-1} = \dim_K(R'/\langle F^h \rangle)_D$, which means that multiplication by-y map $(R'/\langle F^h \rangle)_{D-1} \longrightarrow (R'/\langle F^h \rangle)_D$ is bijective. Thus, in the Gröbner basis computation of F, there is no degree fall at degree D (in fact, up to D, see Subsections 4.1 and 4.2).

Remark 4.3.3. If $m = n$, then it follows from $\frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^{n}} = \prod_{i=1}^{n}(1+z+\cdots+z^{d_i-1})$ that $D = \sum_{j=1}^{n}(d_j-1)+1$, and we have

$$\frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^{n+1}} = \frac{\prod_{i=1}^n (1-z^{d_i})}{(1-z)^{n}} \cdot (1+z+z^2+\cdots),$$

whose degree-d coefficients are equal to a constant for $d \geq D-1$. In this case, the D'-regularity of F^h implies that $D' \leq D$, whence $D' \in \{D-1, D\}$ and $\mathrm{max.GB.deg}_{\prec^h}(F^h) \leq D$ by Proposition 2.3.4. Note that the equality $\mathrm{max.GB.deg}_{\prec^h}(F^h) = D$ holds if $\prec$ is a DRL ordering and if $\langle \mathrm{LM}(F^h) \rangle$ is a weakly reverse lexicographic ideal.

Based on our experiments, we here raise the following conjecture:

Conjecture 4.3.4. Let K be an infinite field, and let $R = K[x_1, \ldots, x_n]$. Let $d_1, \ldots, d_m$ are integers larger than 1, and let $f_1, \ldots, f_m$ be polynomials in R of degrees $d_1, \ldots, d_m$ such that each f_i has no constant term. Then, for given K, n, m, and $(d_1, \ldots, d_m)$, the property that $\boldsymbol{F}^h = (f_1^h, \ldots, f_m^h)$ is generalized cryptographic semi-regular (i.e., D'-regular) is *generic*, where $D' = \widetilde{d}_{\mathrm{reg}}(F^h)$ is the generalized degree of regularity of $\boldsymbol{F}^h$ defined in Definition 2.3.1.

Conjecture 4.3.4 can be viewed as Fröberg's conjecture [21]: A generic sequence of *homogeneous* polynomials is D-regular, where D is the degree of regularity of the sequence.

As a consequence of Conjecture 4.3.4, if F is generated in the way described in the beginning of this subsection, we may expect the following properties:

1. As we described as above, the solving degree $\mathrm{sd}^{\mathrm{mac}}_{\prec^h}(F^h)$ (which is equal to the solving degree $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$ if $\prec$ is a DRL order, see Subsection 2.2) is also upper-bounded by D', which can be quite smaller than $2D-1$.

2. It follows from Theorem 2.1.4 that $\mathrm{HS}_{A'}(z) \equiv \frac{\prod_{j=1}^{m}(1-z^{d_j})}{(1-z)^n} \pmod{z^{D'}}$ for $A' = R'/\langle F^h \rangle$ with $R' = K[x_1, \ldots, x_n, y]$. Hence, by the definition of D', the Hilbert series of A' is computed as follows:
$$\mathrm{HS}_{A'}(z) = \left(\frac{\prod_{j=1}^{m}(1-z^{d_j})}{(1-z)^n} \bmod z^{D'} \right) + \sum_{d=D'}^{\infty} N_{F^h} z^d, \tag{4.3.2}$$
where N_{F^h} is the number of projective roots of F^h counted with multiplicity. This implies that the Hilbert driven algorithm can be effectively applied to the Gröbner basis computation of F^h, from which a Gröbner basis of F is easily obtained.

3. As to the shape of the Hilbert function $\mathrm{HF}_{A'}(z)$ of A', its unimodality and symmetry (up to degree D') can be easily examined by the formula (4.3.2).

Here, we also raise interesting questions:

Question 4.3.5. 1. Does Fröberg's conjecture imply Conjecture 4.3.4? (Or, does the converse hold?)

2. If $R/\langle F^{\mathrm{top}} \rangle$ is Artinian and if $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, does one of the following conditions hold generically?
   (A) $\boldsymbol{F}^h$ is generalized cryptographic semi-regular (i.e., D'-regular).
   (B) $\langle \mathrm{LM}(\boldsymbol{F}^h) \rangle$ is a weakly reverse lexicographic ideal. (Cf. Moreno-Socías conjecture [35].)

3. Are the conditions (A) and (B) are equivalent to each other?

We refer to [36] for several conjectures equivalent to Fröberg's conjecture. It is one of our future works to give answers to these questions.

Final remark for security analysis in cryptography The assumption that $\boldsymbol{F}^h$ is generalized cryptographic semi-regular (i.e., D'-regular) could be useful to estimate the security of multivariate cryptosystems (or algebraic attacks based on Gröbner basis computation), see e.g., [22, Subsection 2.3], where the authors of [22] assume that the bound (4.3.1) gives a degree bound of the XL algorithm [11]. In fact, the bound (4.3.1) has been sometimes used in the cryptographic community *without* assuming the D'-regularity of $\boldsymbol{F}^h$, see [22, Subsection 2.3] (in particular [22, Remark 1]) for details. Supposing the D'-regularity of the homogenization of a target polynomial system, one could give a mathematically rigid explanation about the complexity of computing the Gröbner basis of the system.

Acknowledgement

The contents of this paper will be presented at Effective Methods in Algebraic Geometry (MEGA 2024). The authors thank the anonymous referees assigned by the organization of this conference for their comments and suggestions. The authors are grateful to Yuta Kambe and Shuhei Nakamura for helpful comments. They are also thankful to Masayuki Noro for providing computational tools for our computational experiments. This work was supported by JSPS Grant-in-Aid for Young Scientists 20K14301 and 23K12949, JSPS Grant-in-Aid for Scientific Research (C) 21K03377, and JST CREST Grant Number JPMJCR2113.

References

[1] M. Bardet: Étude des systémes algébriques surdéterminés. Applications aux codes correcteurs et á la cryptographie. PhD thesis, Université Paris IV, 2004.

[2] M. Bardet, J.-C. Faugére, and B. Salvy: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations (extended abstract). In: Proceedings of the International Conference on Polynomial System Solving, 71–74, 2004.

[3] M. Bardet, J.-C. Faugére, B. Salvy, and B.-Y. Yang: Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In: Proceedings of Eighth International Symposium on Effective Methods in Algebraic Geometry (MEGA 2005), 2005.

[4] M. Bigdeli, E. De Negri, M. M. Dizdarevic, E. Gorla, R. Minko, and S. Tsakou: Semi-Regular Sequences and Other Random Systems of Equations. In: Women in Numbers Europe III, **24**, pp. 75–114, Springer, 2021.

[5] W. Bosma, J. Cannon, and C. Playoust: The Magma algebra system I: The user language. Journal of Symbolic Computation, **24**(3-4), 235-–265, 1997.

[6] B. Buchberger: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Innsbruck: Univ. Innsbruck, Mathematisches Institut (Diss.), 1965.

[7] J. A. Buchmann, J. Ding, M. S. E. Mohamed, and W. S. A. E. Mohamed: MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis. In H. Handschuh, S. Lucks, B. Preneel, and P. Rogaway (eds), Symmetric Cryptography, Dagstuhl Seminar Proceedings, **9031**, pp. 1–7, Dagstuhl, Germany, 2009.

[8] A. Caminata and E. Gorla: Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra. In: Arithmetic of Finite Fields (Proc. of WAIFI 2020), LNCS, **12542**, pp. 3–36, Springer, 2021.

[9] A. Caminata and E. Gorla: Solving degree, last fall degree, and related invariants. J. Symb. Comp., **114**, 322–335 (2023).

[10] J. G. Capaverde: Gröbner bases: Degree bounds and generic ideals. PhD thesis, Clemson University, 2014.

[11] N. Courtois, A. Klimov, J. Patarin, and A. Shamir: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. EUROCRYPT 2000, LNCS, **1807**, pp. 392–407, Springer, 2000.

[12] S. Collart, M. Kalkbrener, and D. Mall: Coverting bases with the Groebner walk. J. Symb. Comp., **24**, Issues 3–4, 465–469, 1997.

[13] D. A. Cox, J. Little, and D. O'Shea. Ideals, Varieties, and Algorithms (Fourth Edition). Undergraduate Texts in Mathematics, Springer, NY, 2010.

[14] C. Diem: Bounded regularity. Journal of Algebra, **423**, 1143–1160, 2015.

[15] J. Ding and D. Schmidt: Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields. In: M. Fischlin and S. Katzenbeisser (eds), Number Theory and Cryptography, LNCS, **8260**, pp. 34–49, Springer, Berlin, Heidelberg.

[16] D. Eisenbud: Commutative Algebra: With a View Toward Algebraic Geometry. GTM, **150**, Springer, 1995.

[17] C. Eder and J.-C., Faugère: A survey on signature-based algorithms for computing Gröbner bases. Journal of Symbolic Computation **80** (2017), 719–784.

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

[19] J.-C., Faugère: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of ISSAC 2002, ACM Press, (2002), pp. 75–82.

[20] J.-C., Faugère, P. Gianni, D. Lazard, and T. Mora: Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. J. Symb. Comp., **16** (4), 329–344, 1993.

[21] R. Fröberg: An inequality for Hilbert series of graded algebras. Math. Scand., **56** (1985), 117–144.

[22] H. Furue and M. Kudo: Polynomial XL: A Variant of the XL Algorithm Using Macaulay Matrices over Polynomial Rings. Post-Quantum Cryptography, PQCrypto 2024, Lecture Notes in Computer Science, **14772**, pp. 109–143, Springer, Cham, 2024.

[23] G. Gaggero and E. Gorla: The complexity of solving a random polynomial system. arxiv:2309.03855.

[24] E. Gorla, D. Mueller, and C. Petit: Stronger bounds on the cost of computing Gröbner bases for HFE systems. J. Symb. Comp., **109**, 386–398, 2022.

[25] G.-M. Greuerl and G. Pfister: A Sinular Introduction to Commutative Algebra. 2nd Edition, Springer, 2007.

[26] M.-D. A. Huang, M. Kosters, Y. Yang, and S. L. Yeo: On the last fall degree of zero-dimensional Weil descent systems. J. Symb. Comp., **87** (2018), 207–226.

[27] M.-D. A. Huang, M. Kosters, and S. L. Yeo: Last fall degree, HFE, and Weil descent attacks on ECDLP. In: Advances in Cryptology — CRYPTO 2015, LNCS, **9215**, 581–600, Springer, Berlin, Heidelberg, 2015.

[28] M. Kreuzer and L. Robbiano: Computational Commutative Algebra 1. Springer, 2000.

[29] M. Kreuzer and L. Robbiano: Computational Commutative Algebra 2. Springer, 2003.

[30] M. Kudo and K. Yokoyama: On Hilbert-Poincaré series of affine semi-regular polynomial sequences and related Gröbner bases. In: T. Takagi et al. (eds), Mathematical Foundations for Post-Quantum Cryptography, Mathematics for Industry, 26 pages, Springer, to appear (arXiv:2401.07768).

[31] D. Lazard: Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In: Computer algebra (London, 1983), LNCS, **162**, pp. 146–156, Springer, Berlin, 1983.

[32] D. Lazard: Résolution des systèmes d'équations algébriques. Theoretical Computer Science, **15**, Issue 1, 77–110, 1981.

[33] E. W. Mayr and S. Ritscher: Dimension-dependent bounds for Gröbner bases of polynomial ideals. J. Symb. Comp., **49** (2013), 78–94.

[34] M. S. E. Mohamed, W. S. A. E. Mohamed, J. Ding, and J. A. Buchmann: MXL2: Solving polynomial equations over GF(2) using an improved mutant strategy. In J. A. Buchmann and J. Ding (eds.), Post-Quantum Cryptography, pp. 203—215, Springer Berlin Heidelberg, 2008.

[35] G. Moreno-Socías: Autour de la fonction de Hilbert-Samuel (escaliers d'idéaux polynomiaux), Thèse, École Polytechnique, 1991.

[36] K. Pardue: Generic sequences of polynomials. Journal of Algebra, **324.4**, 579–590, 2010.

[37] S. Ritscher: Degree Bounds and Complexity of Gröbner Bases of Important Classes of Polynomial Ideals. PhD thessis, Technische Universität München Institut für Mathematik, 2012.

[38] Y. Sakata and T. Takagi: An Efficient Algorithm for Solving the MQ Problem using Hilbert Series, Cryptology ePrint Archive, 2023/1650.

[39] F. Salizzoni: An upper bound for the solving degree in terms of the degree of regularity. arXiv:2304.13485.

[40] I. Semaev and A. Tenti: Probabilistic analysis on Macaulay matrices over finite fields and complexity constructing Gröbner bases. Journal of Algebra, **565**, 651–674, 2021.

[41] 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

[42] C. Traverso: Hilbert functions and the Buchberger algorithm. J. Symb. Comp., **22.4** (1996), 355–376.

A Koszul complex and homogenization

A.1 Koszul complex

Let $f_1, \ldots, f_m \in R$ be homogeneous polynomials of positive degrees $d_1, \ldots, d_m$ respectively, and put $d_{j_1 \cdots j_i} := \sum_{k=1}^{i} d_{j_k}$. For each $0 \leq i \leq m$, we define a free R-module of rank $\binom{m}{i}$

$$K_i(f_1, \ldots, f_m) := \begin{cases} \displaystyle\bigoplus_{1 \leq j_1 < \cdots < j_i \leq m} R(-d_{j_1 \cdots j_i})\mathbf{e}_{j_1 \cdots j_i} & (i \geq 1) \\ R & (i = 0), \end{cases}$$

where $\mathbf{e}_{j_1 \cdots j_i}$ is a standard basis. We also define a graded homomorphism

$$\varphi_i : K_i(f_1, \ldots, f_m) \longrightarrow K_{i-1}(f_1, \ldots, f_m)$$

of degree 0 by

$$\varphi_i(\mathbf{e}_{j_1 \cdots j_i}) := \sum_{k=1}^{i} (-1)^{k-1} f_{j_k} \mathbf{e}_{j_1 \cdots \hat{j_k} \cdots j_i}.$$

Here, $\hat{j_k}$ means to omit j_k. For example, we have $\mathbf{e}_{1\hat{2}3} = \mathbf{e}_{13}$. To simplify the notation, we set $K_i := K_i(f_1, \ldots, f_m)$. Then,

$$K_\bullet : 0 \to K_m \xrightarrow{\varphi_m} \cdots \xrightarrow{\varphi_3} K_2 \xrightarrow{\varphi_2} K_1 \xrightarrow{\varphi_1} K_0 \to 0 \tag{A.1.1}$$

is a complex of graded free R-modules, and we call it the *Koszul complex* on $(f_1, \ldots, f_m)$. The i-th homology group of $K_\bullet$ is given by

$$H_i(K_\bullet) = \mathrm{Ker}(\varphi_i)/\mathrm{Im}(\varphi_{i+1}).$$

In particular, we have

$$H_0(K_\bullet) = R/\langle f_1, \ldots, f_m \rangle_R.$$

We also note that $H_m(K_\bullet) = 0$, since φ_m is clearly injective by definition. The kernel and the image of a graded homomorphism are both graded submodules in general, so that $\mathrm{Ker}(\varphi_i)$ and $\mathrm{Im}(\varphi_{i+1})$ are graded R-modules, and so is the quotient module $H_i(K_\bullet)$ (and each homogeneous part is finite-dimensional K-vector space). In the following, we denote by $H_i(K_\bullet)_d$ the degree-d homogeneous part of $H_i(K_\bullet)$.

Note that $\mathrm{Ker}(\varphi_1) = \mathrm{syz}(f_1, \ldots, f_m)$ (the right hand side is the module of syzygies), and that $\mathrm{Im}(\varphi_2) \subset K_1 = \bigoplus_{j=1}^m R(-d_j)\mathbf{e}_j$ is generated by

$$\{\mathbf{t}_{i,j} := f_i\mathbf{e}_j - f_j\mathbf{e}_i : 1 \leq i < j \leq m\}.$$

Hence, putting

$$\mathrm{tsyz}(f_1, \ldots, f_m) := \langle \mathbf{t}_{i,j} : 1 \leq i < j \leq m\rangle_R,$$

we have

$$H_1(K_\bullet) = \mathrm{syz}(f_1, \ldots, f_m)/\mathrm{tsyz}(f_1, \ldots, f_m). \tag{A.1.2}$$

Definition A.1.1 (Trivial syzygies)**.** With notation as above, we call each generator $\mathbf{t}_{i,j}$ (or each element of $\mathrm{tsyz}(f_1, \ldots, f_m)$) a *trivial syzygy* for $(f_1, \ldots, f_m)$. We also call $\mathrm{tsyz}(f_1, \ldots, f_m)$ the *module of trivial syzygies.*

A.2 Homogenization of polynomials and monomial orders

We here recall the notion of homogenization; see [29, Chapter 4] for details. Let $R = K[x_1, \ldots, x_n]$ be the polynomial ring of n variables over a field K, and $\mathcal{T}$ the set of all monomials in $x_1, \ldots, x_n$. Put $R' = R[y]$ for an extra variable y.

(1) For a non-homogeneous and non-zero polynomial $f = \sum_{t\in\mathcal{T}} c_t t$ in R with $c_t \in K$, its *homogenization* f^h is defined, by introducing an extra variable y, as

$$f^h = \sum_{t\in\mathcal{T}} c_t t y^{\deg(f)-\deg(t)} \in R' = R[y].$$

Thus f^h is a homogeneous polynomial in R' with total degree $d = \deg(f)$. Also for a set F (or a sequence $F = (f_1, \ldots, f_m) \in R^m$) of non-zero polynomials, its *homogenization* F^h (or F^h) is defined as $F^h = \{f^h \mid f \in F\}$ (or $F^h = (f_1^h, \ldots, f_m^h) \in (R')^m$).

(2) Conversely, for a homogeneous polynomial h in R', its *dehomogenization* h^{deh} is defined by substituting y with 1, that is, $h^{\mathrm{deh}} = h(x_1, \ldots, x_n, 1)$ (it is also denoted by $h|_{y=1}$). For a set H of homogeneous polynomials in R', its *dehomogenization* H^{deh} (or $H|_{y=1}$) is defined as $H^{\mathrm{deh}} = \{h^{\mathrm{deh}} : h \in H\}$. We also apply the dehomogenization to sequences of polynomials.

(3) For an ideal I of R, its homogenization I^h, as an ideal, is defined as $\langle I^h\rangle_{R'}$. We remark that, for a set F of polynomials in R, we have $\langle F^h\rangle_{R'} \subset I^h$ with $I = \langle F\rangle_R$, and the equality does not hold in general.

(4) For a homogeneous ideal J in R', its dehomogenization J^{deh}, as a set, is an ideal of R. We note that if a homogeneous ideal J is generated by H, then $J^{\mathrm{deh}} = \langle H^{\mathrm{deh}}\rangle_R$ and for an ideal I of R, we have $(I^h)^{\mathrm{deh}} = I$.

(5) For a monomial ordering $\prec$ on the set of *monomials* $\mathcal{T}$ in X, its *homogenization* $\prec_h$ on the set of *monomials* $\mathcal{T}^h$ in $x_1, \ldots, x_n, y$ is defined as follows: For two monomials $X^\alpha y^a$ and $X^\beta y^b$ in $\mathcal{T}^h$, we say $X^\alpha y^a \prec_h X^\beta y^b$ if and only if one of the following holds:
   (i) $a + |\alpha| < b + |\beta|$, or
   (ii) $a + |\alpha| = b + |\beta|$ and $X^\alpha \prec X^\beta$,

where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ and $|\alpha| = \alpha_1 + \cdots + \alpha_n$, and where X^α denotes $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Here, for a monomial $X^\alpha y^a$, we call X^α and y^a *the X-part* and *the y-part*, respectively. If a monomial ordering $\prec$ is *graded*, that is, it first compares the total degrees, the restriction $\prec_h |_{\mathcal{T}}$ of $\prec_h$ on $\mathcal{T}$ coincides with $\prec$.

It is well-known that, for a Gröbner basis H of $\langle F^h \rangle$ with respect to $\prec^h$, its dehomogenization $H^{\mathrm{deh}} = \{h^{\mathrm{deh}} : h \in H\}$ is also a Gröbner basis of $\langle F \rangle$ with respect to $\prec$ if $\prec$ is graded. Moreover, we have $\langle F \rangle^h = (\langle F^h \rangle : \langle y \rangle^\infty) = (\langle F^h \rangle : \langle y^k \rangle)$ for some integer k, where $(\langle F^h \rangle : \langle y^k \rangle)$ is the ideal quotient of $\langle F^h \rangle$ by $\langle y^k \rangle$, namely $\{f \in R' : f \langle y^k \rangle \subset \langle F^h \rangle\}$ see [29, Corollary 4.3.8].