On Hilbert-Poincaré series of affine semi-regular polynomial sequences and related Gröbner bases

Momonari Kudo and
Kazuhiro Yokoyama

Abstract Gröbner bases are nowadays central tools for solving various problems in commutative algebra and algebraic geometry. A typical use of Gröbner bases is the multivariate polynomial system solving, which enables us to construct algebraic attacks against post-quantum cryptographic protocols. Therefore, the determination of the complexity of computing Gröbner bases is very important both in theory and in practice: One of the most important cases is the case where input polynomials compose an (overdetermined) affine semi-regular sequence. The first part of this paper aims to present a survey on Gröbner basis computation and its complexity. In the second part, we shall give an explicit formula on the (truncated) Hilbert-Poincaré series associated to the homogenization of an affine semi-regular sequence. Based on the formula, we also study (reduced) Gröbner bases of the ideals generated by an affine semi-regular sequence and its homogenization. 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.

1 Introduction

Let K be a field, and $R = K[x_1, \dots, x_n]$ the polynomial ring in n variables over K. For a polynomial f in R, let f^{top} denote its maximal total degree part which is called the *top part* of f here, and let f^h denote its homogenization in $R' = R[y]$ by an extra variable y, see Subsection 3.1.1 below for details. 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 finitely generated

Momonari Kudo
Fukuoka Institute of Technology, 3-30-1 Wajiro-higashi, Higashi-ku, Fukuoka, 811-0295 Japan
e-mail: m-kudo@fit.ac.jp

Kazuhiro Yokoyama
Rikkyo University, 3-34-1 Nishi-Ikebukuro, Toshima-ku, Tokyo, 171-8501 Japan
e-mail: kazuhiro@rikkyo.ac.jp

graded R-(or 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 the ideal I. A typical application of computing Gröbner bases is solving the multivariate polynomial (MP) problem: Given m polynomials $f_1, \ldots, f_m$ in R, 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 polynomials are all quadratic is called the MQ problem, and its hardness is applied to constructing public-key cryptosystems and digital signature schemes 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 [19] and F_5 [20] algorithms have been proposed, see Subsection 3.1 below for a summary. In general, it is very difficult to determine the complexity of computing Gröbner bases, but in some cases, we can estimate it with several algebraic invariants such as the solving degree, the degree of regularity, the Castelnuovo–Mumford regularity, and the first and last fall degrees; we refer to [8] for the relations between these invariants.

The first part of this paper aims to survey Gröbner basis computation, and to review its complexity in the case where input polynomials generate a zero-dimensional ideal. For this, in Section 2, we first recall foundations in commutative algebra such as Koszul complex, Hilbert-Poincaré series, and semi-regular sequence, which are useful ingredients to estimate the complexity of computing Gröbner bases. Then, we overview existing Gröbner basis algorithms in Subsection 3.1. Subsequently, it will be described in Subsection 3.2 how to estimate the complexity of computing the reduced Gröbner basis of a zero-dimensional ideal, with the notion of homogenization.

In the second part, we focus on *affine semi-regular* polynomial sequences, where a sequence $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ of (not necessarily homogeneous) polynomials is said to be affine (cryptographic) semi-regular if $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ is (cryptographic) semi-regular, see Definitions 4, 7, and 8 for details. Note that homogeneous semi-regular sequences are conjectured by Pardue [32, Conjecture B] to be generic sequences of polynomials, and affine (cryptographic) semi-regular sequences are often appearing in the construction of multivariate public key cryptosystems and digital signature schemes. In Section 4 below, we relate the Hilbert-Poincaré series of $R'/\langle \boldsymbol{F}^h \rangle$ with that of $R/\langle \boldsymbol{F}^{\mathrm{top}} \rangle$. As a corollary, we obtain an explicit formula of the truncation at degree $D-1$ of the Hilbert-Poincaré series of $R'/\langle \boldsymbol{F}^h \rangle$, where D is the degree of regularity for $\langle \boldsymbol{F}^{\mathrm{top}} \rangle$. The following theorem summarizes these results:

Theorem 1 (Theorem 7, Corollaries 1 and 2) *With notation as above, assume that $\boldsymbol{F}$ is affine cryptographic semi-regular. Then $\mathrm{HF}_{R'/\langle \boldsymbol{F}^h \rangle}(d) = \sum_{i=0}^{d} \mathrm{HF}_{R/\langle \boldsymbol{F}^{\mathrm{top}} \rangle}(i)$ and $(\langle \mathrm{LM}(\langle \boldsymbol{F}^h \rangle) \rangle_{R'})_d = (\langle \mathrm{LM}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle) \rangle_{R'})_d$ for each d with $d < D$, where we use a DRL ordering on the set of monomials in R and its homogenization on that in R'. Hence, we also obtain $\mathrm{HS}_{R'/\langle \boldsymbol{F}^h \rangle}(z) \equiv \prod_{i=1}^{m}(1-z^{d_i})/(1-z)^{n+1} \pmod{z^D}$, so that $\boldsymbol{F}^h$ is D-regular (see Definition 4 for the definition of d-regularity).*

As an application of this theorem, we explore reduced Gröbner bases of $\langle \boldsymbol{F} \rangle$, $\langle \boldsymbol{F}^h \rangle$, and $\langle \boldsymbol{F}^{\mathrm{top}} \rangle$ in Section 5 below, dividing the cases into the degree less than D or not. 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.

2 Preliminaries

In this section, we recall definitions of Koszul complex, Hilbert–Poincaré series, and semi-regular polynomial sequences, and collect some known facts related to them. Throughout this section, let $R = K[X] = K[x_1, \ldots, x_n]$ be the polynomial ring of n variables $X = (x_1, \ldots, x_n)$ over a field K. As a notion, for a polynomial f in R, we denote its total degree by $\deg(f)$. As R is a graded ring with respect to total degree, for a polynomial f, its maximal total degree part, denoted by f^{top}, is defined as its graded component of $\deg(f)$, that is, the sum of all terms of f whose total degree equals to $\deg(f)$.

2.1 Koszul complex and its homology

Let $f_1, \ldots, f_m \in R$ be homogeneous polynomials of degrees $d_1, \ldots, d_m$, 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,

$$K_\bullet : 0 \to K_m \xrightarrow{\varphi_m} \cdots \xrightarrow{\varphi_3} K_2 \xrightarrow{\varphi_2} K_1 \xrightarrow{\varphi_1} K_0 \to 0 \tag{1}$$

is a complex, 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

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

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 $H_i(K_\bullet)$. 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

$$H_1(K_\bullet) = \mathrm{syz}(f_1, \ldots, f_m)/\mathrm{tsyz}(f_1, \ldots, f_m). \tag{2}$$

Definition 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*.

We also note that $H_m(K_\bullet) = 0$, since φ_m is clearly injective by definition.

Remark 1 When $K = \mathbb{F}_q$, a vector of the form $f_i^{q-1}\mathbf{e}_i$ is also referred to as a trivial syzygy, in the context of Ding-Schmidt's definition for *first fall degree* [16] (see [7, Section 4.2] or [30, Section 3.2] for reviews). More concretely, putting $B := R/\langle x_1^q, \ldots, x_n^q \rangle_R$ and $\overline{f}_i := f_i \bmod \langle x_1^q, \ldots, x_n^q \rangle$, we define the Koszul complex on $(\overline{f}_1, \ldots, \overline{f}_m) \in B^m$ similarly to that on $(f_1, \ldots, f_m) \in R^m$, and denote it by $\overline{K}_\bullet = \overline{K}_\bullet(\overline{f}_1, \ldots, \overline{f}_m)$. Then, the vectors $\overline{f}_i\mathbf{e}_j - \overline{f}_j\mathbf{e}_i$ and $\overline{f}_i^{q-1}\mathbf{e}_i$ in B^m for $1 \leq i < j \leq m$ are syzygies for $(\overline{f}_1, \ldots, \overline{f}_m)$. Each $\overline{f}_i\mathbf{e}_j - \overline{f}_j\mathbf{e}_i$ is called a Koszul syzygy, and the Koszul syzygies together with $\overline{f}_i^{q-1}\mathbf{e}_i$'s are referred to as trivial syzygies for $(\overline{f}_1, \ldots, \overline{f}_m)$. The *first fall degree* $d_{\mathrm{ff}}(f_1, \ldots, f_m)$ is defined as the minimal integer d with $\mathrm{syz}(\overline{f}_1, \ldots, \overline{f}_m)_d \supsetneq \mathrm{tsyz}^{+}(\overline{f}_1, \ldots, \overline{f}_m)_d$ in $(B_{d-d_i})^m$, where $\mathrm{tsyz}^{+}(\overline{f}_1, \ldots, \overline{f}_m)$ denotes the submodule in B^m generated by the trivial syzygies for $(\overline{f}_1, \ldots, \overline{f}_m)$.

Note that, for each i, a homomorphism $H_i(K_\bullet) \longrightarrow H_i(\overline{K}_\bullet)$ is canonically induced by taking modulo $\langle x_1^q, \ldots, x_n^q \rangle_R$. In particular, we have the following composite K-linear map:

$$\eta_d : H_1(K_\bullet)_d \to H_1(\overline{K}_\bullet)_d \to \mathrm{syz}(\overline{f}_1, \ldots, \overline{f}_m)_d/\mathrm{tsyz}^{+}(\overline{f}_1, \ldots, \overline{f}_m)_d.$$

for each d. Putting $d = d_{\mathrm{ff}}(f_1, \ldots, f_m)$ and letting D to be the minimal integer with $H_1(K_\bullet)_D \neq 0$, it is straightforward to verify the following:

- If $q > D$, then η_D is injective, and $\mathrm{syz}(\overline{f}_1, \ldots, \overline{f}_m)_D \supsetneq \mathrm{tsyz}^+(\overline{f}_1, \ldots, \overline{f}_m)_D$, whence $D \geq d$.
- If $q > d$, then η_d is surjective. In this case, $H_1(K)_d \neq 0$, so that $D \leq d$.

See [30, Lemmas 4.2 and 4.3] for a proof. Therefore, we have $d = D$ for sufficiently large any q.

2.2 Hilbert–Poincaré series and semi-regular sequences

Definition 2 (Hilbert–Poincaré series) For a finitely generated graded R-module M, we define the *Hilbert function* HF_M of M, given by

$$\mathrm{HF}_M(d) = \dim_K M_d$$

for each $d \in \mathbb{Z}_{\geq 0}$. The *Hilbert–Poincaré series* HS_M of M is defined as the formal power series

$$\mathrm{HS}_M(z) = \sum_{d=0}^{\infty} \mathrm{HF}_M(d) z^d \in \mathbb{Z}[\![z]\!].$$

Theorem 2 (cf. [4, Chapter 10]) *Let I be a homogeneous ideal of R generated by a set $G \subset R$ of homogeneous elements of degree not greater than a non-negative integer d. Let $\mathrm{LM}(f)$ denote the leading monomial of $f \in R \smallsetminus \{0\}$ with respect to a graded ordering $\prec$ on the set of monomials in R. For a non-empty subset $F \subset R \smallsetminus \{0\}$, put $\mathrm{LM}(F) := \{\mathrm{LM}(f) : f \in F\}$. Then, the following are equivalent:*

1. $\langle \mathrm{LM}(G) \rangle_{\leq d} = \langle \mathrm{LM}(I) \rangle_{\leq d}$.
2. *Every $f \in I_{\leq d}$ is reduced to zero modulo G.*
3. *For every pair of $f, g \in G$ with $\deg(\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))) \leq d$, the S-polynomial $S(f, g)$ is reduced to zero modulo G.*

In this case, G is called a d-Gröbner basis of I with respect to $\prec$.

We also review the notion of semi-regular sequence defined by Pardue [32].

Definition 3 (Semi-regular sequences, [32, 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 $(R/I)_{t-d} \longrightarrow (R/I)_d$; $g \mapsto gf$ is injective or surjective, for every t with $t \geq d$. A sequence $(f_1, \ldots, f_m) \in R^m$ 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 $f_1, \ldots, f_m \in R$ be homogeneous elements of degree $d_1, \ldots, d_m$, respectively, and put $I = \langle f_1, \ldots, f_m \rangle_R$. Furthermore, put $I^{(0)} := \{0\}$ 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

$$A^{(i-1)} \longrightarrow A^{(i-1)} \ ; \ g \mapsto gf_i,$$

which is a graded homomorphism of degree d_i. For every $t \geq d_i$, 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. On the other hand, as for the surjective homomorphism

$$\phi_{i-1} : A^{(i-1)} \longrightarrow A^{(i)} \ ; \ f + I^{(i-1)} \mapsto f + I^{(i)},$$

it is straightforward to see that for each t with $0 \leq t \leq d_i - 1$, the restriction map

$$\phi_{i-1}|_{A_t^{(i-1)}} : A_t^{(i-1)} \longrightarrow A_t^{(i)}$$

is an isomorphism of K-linear spaces, whence

$$\dim_K A_t^{(i-1)} = \dim_K A_t^{(i)} \quad (0 \leq t \leq d_i - 1).$$

Lemma 1 *With notation as above, for each $1 \leq i \leq m$ and for each $t \geq d_i$, we have the following equalities:*

$$\dim_K A_t^{(i)} = \dim_K A_t^{(i-1)} - \dim_K \mathrm{Im}\left(A_{t-d_i}^{(i-1)} \xrightarrow{\times f_i} A_t^{(i-1)}\right), \tag{3}$$

$$\dim_K \mathrm{Im}\left(A_{t-d_i}^{(i-1)} \xrightarrow{\times f_i} A_t^{(i-1)}\right) = \dim_K A_{t-d_i}^{(i-1)} - \dim_K (0 : f_i)_{t-d_i}, \tag{4}$$

where we set $(0 : f_i) = \{g \in A^{(i-1)} : gf_i = 0\}$. Hence,

- *The multiplication map $A_{t-d_i}^{(i-1)} \xrightarrow{\times f_i} A_t^{(i-1)}$ is injective if and only if*

$$\dim_K A_t^{(i)} = \dim_K A_t^{(i-1)} - \dim_K A_{t-d_i}^{(i-1)}. \tag{5}$$

  In this case, one has $\dim_K A_{t-d_i}^{(i-1)} \leq \dim_K A_t^{(i-1)}$.
- *The multiplication map $A_{t-d_i}^{(i-1)} \xrightarrow{\times f_i} A_t^{(i-1)}$ is surjective if and only if*

$$\dim_K A_t^{(i)} = 0. \tag{6}$$

  In this case, one has $\dim_K A_{t-d_i}^{(i-1)} \geq \dim_K A_t^{(i-1)}$.

Proof. Let i and t be integers such that $1 \leq i \leq m$ and $t \geq d_i$. Since we have $(0 : f_i)_{t-d_i} = \{g \in A_{t-d_i}^{(i-1)} : gf_i = 0\}$, the sequence

$$0 \longrightarrow (0 : f_i)_{t-d_i} \longrightarrow A_{t-d_i}^{(i-1)} \xrightarrow{\times f_i} A_t^{(i-1)} \longrightarrow A_t^{(i)} \longrightarrow 0$$

of K-linear maps is exact, where $(0 : f_i)_{t-d_i} \longrightarrow A_{t-d_i}^{(i-1)}$ is an inclusion map. The exactness of this sequence implies the desired equalities (3) and (4). □

The semi-regularity is characterized by equivalent conditions in Proposition 1 below. In particular, the fourth condition enables us to compute the Hilbert–Poincaré series of each $A^{(i)}$ easily.

Proposition 1 (cf. [32, Proposition 1]) *With notation as above, the following are equivalent:*

1. *The sequence $(f_1, \ldots, f_m) \in R^m$ is semi-regular.*
2. *For each $1 \leq i \leq m$ and for each $t \geq d_i$, we have (5) or (6), 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 $1 \leq i \leq m$, 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 $1 \leq i \leq m$, 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 [32, Conjecture B] that generic polynomial sequences are semi-regular.

2.3 Cryptographic semi-regular sequences

We here review the notion of *cryptographic semi-regular* sequence, which is defined by a condition weaker than one for semi-regular sequences. 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 [5], in order to distinguish such a sequence from a semi-regular one defined by Pardue (see Definition 3 in the previous subsection).

Definition 4 ([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 $I = \langle f_1, \ldots, f_m \rangle_R$. The notations $I^{(i)}$ and $A^{(i)}$ are also the same as in the previous subsection. For each integer d with $d \geq \max\{d_i : 1 \leq i \leq m\}$, we call a sequence $(f_1, \ldots, f_m) \in R^m$ of homogeneous polynomials *d-regular* if it satisfies the following condition:

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

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

Theorem 3 (cf. [14, Theorem 1]) *With the same notation as in Definition 4, the following are equivalent for each d with $d \geq \max\{d_i : 1 \leq i \leq m\}$:*

1. *The sequence $(f_1, \ldots, f_m) \in R^m$ is d-regular. Namely, for each (i, t) with $1 \leq i \leq m$ and $d_i \leq t < d$, the equality (5) holds.*
2. *We have*
$$\mathrm{HS}_{A^{(m)}}(z) \equiv \frac{\prod_{j=1}^{m}(1 - z^{d_j})}{(1 - z)^n} \pmod{z^d}.$$
3. *$H_1(K_\bullet(f_1, \ldots, f_m))_{\leq d-1} = 0$.*

Proposition 2 ([14, Proposition 2 (a)]) *With the same notation as in Definition 4, let D and i be natural numbers. Assume that $H_i(K(f_1, \ldots, f_m))_{\leq D} = 0$. Then, for each j with $1 \leq j < m$, we have $H_i(K(f_1, \ldots, f_j))_{\leq D} = 0$.*

Definition 5 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 $d \geq D$.

Definition 6 ([2, Definition 4], [3, Definition 5]) 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].

Remark 2 In Definition 6, 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., [17, §20.5] for the definition), whence $d_{\mathrm{reg}}(I) = \mathrm{reg}(I) = \mathrm{reg}(R/I) + 1$.

Definition 7 ([2, Definition 5], [3, Definition 5]; see also [15, Section 2]) A sequence $(f_1, \ldots, f_m) \in R^m$ 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 3 below. In particular, the second condition enables us to compute the Hilbert–Poincaré series of $A^{(i)}$ easily.

Proposition 3 ([14, Proposition 1 (d)]; see also [3, Proposition 6]) *With the same notation as in Definition 4, we put $D = d_{\mathrm{reg}}(I)$. Then, the following are equivalent:*

1. *$(f_1, \ldots, f_m) \in R^m$ is cryptographic semi-regular.*

2. *We have*

$$\mathrm{HS}_{R/I}(z) = \left[\frac{\prod_{j=1}^{m}(1 - z^{d_j})}{(1 - z)^n} \right]. \tag{7}$$

3. $H_1(K_\bullet(f_1, \dots, f_m))_{\le D-1} = 0.$

Remark 3 By the definition of *degree of regularity*, if $(f_1, \dots, f_m) \in R^m$ is cryptographic semi-regular, $d_{\mathrm{reg}}(I)$ coincides with $\deg(\mathrm{HS}_{R/I}(z)) + 1$, where we set $I = \langle f_1, \dots, f_m \rangle$.

In 1985, Fröberg already conjectured in [22] that, when K is an infinite field, a generic sequence of homogeneous polynomials $f_1, \dots, f_m \in R$ of degrees $d_1, \dots, d_m$ generates an ideal I with the Hilbert-Poincaré series of the form (7), namely $(f_1, \dots, f_m)$ is cryptographic semi-regular. It can be proved (cf. [32]) that Fröberg's conjecture is equivalent to Pardue's one [32, Conjecture B] introduced in Subsection 2.2. We also note that Moreno-Socías conjecture [29] is stronger than the above two conjectures, see [32, Theorem 2] for a proof.

It follows from the fourth condition of Proposition 1 together with the second condition of Proposition 3 that the semi-regularity implies the cryptographic semi-regularity.

Definition 8 (Affine semi-regular sequences) A sequence $\boldsymbol{F} = (f_1, \dots, f_m) \in R^m$ of not necessarily homogeneous polynomials $f_1, \dots, f_m$ is said to be semi-regular (resp. cryptographic semi-regular) if $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, \dots, f_m^{\mathrm{top}})$ is semi-regular (resp. cryptographic semi-regular). In this case, we call $\boldsymbol{F}$ an *affine semi-regular (resp. affine cryptographic semi-regular)* sequence.

Remark 4 For an affine cryptographic semi-regular sequence $\boldsymbol{F} = (f_1, \dots, f_m) \in R^m$ with $K = \mathbb{F}_q$, it follows from Proposition 3 that $d_{\mathrm{reg}}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle) \le d_{\mathrm{ff}}(f_1^{\mathrm{top}}, \dots, f_m^{\mathrm{top}})$ for $q \gg 0$, where $d_{\mathrm{ff}}(f_1^{\mathrm{top}}, \dots, f_m^{\mathrm{top}})$ is the first fall degree defined in Remark 1.

3 Quick review on the computation of Gröbner basis

In this section, we first review previous studies on the computation of Gröbner bases for polynomial ideals.

3.1 Overview of existing Gröbner basis algorithms

Since Buchberger [6] discovered the notion of Gröbner basis and a fundamental algorithm for computing them, many efforts have been done for improving the efficiency of Gröbner basis computation based on Buchberger's algorithm. In his algorithm, S-polynomials play an important role for Gröbner basis computation and give a famous termination criterion called Buchberger's criterion, that is, for a given ideal I of a polynomial ring over a field, its finite generating subset G is a Gröbner basis of I with respect to a monomial ordering if and only if the S-polynomial $S(g, g')$ for any distinct pair $g, g' \in G$ is reduced to 0 modulo G. For details on Buchberger's algorithm and monomial orderings, see e.g., [4].

In the below, we list effective improvements for algorithms which are, at the same time, very useful to analyze the complexity of Gröbner basis computation. Here we note that the choice of a monomial ordering is also very crucial for the efficiency of Gröber basis computation, but we here do not discuss about its choice. (In general, the degree reverse lexicographical (DRL) ordering[1] is considered as the most efficient ordering for the computation.)

(1) **Related to S-polynomial:**

(1-1) **Strategy for selecting S-polynomial:** It is considered to be very effective to apply the *normal strategy*, where we choose a pair (g, g') for which the least common multiple (LCM) of the leading monomials $\mathrm{LM}(g)$ and $\mathrm{LM}(g')$ with respect to the fixed ordering $\prec$ as smaller as possible. (See [4, Chapter 5.5].) The strategy is very suited for a homogeneous ideal with a *graded*[2] ordering such as DRL, as we can utilize the graded structure of a homogeneous ideal. Also, the *sugar strategy* is designed for a non-homogeneous ideal generated by F to make the computational behavior very close to that for the ideal generated by the *homogenization* F^h. See Subsection 3.1.1 below for some details on homogenization. (See also [12, Chapter 2.10].)
(1-2) **Avoiding unnecessary S-polynomial computation:** In Buchberger's algorithm, we add a polynomial to a generating set G which is computed from an S-polynomial by possible reduction of elements in G. Since the cost of the construction of S-polynomials and their reduction dominate the whole computation, S-polynomials which are reduced to 0 are very harmful for the efficiency. Thus, it is highly desired to avoid such unnecessary S-polynomials as many as possible.

(A) **Based on simple rules:** At earlier stages, there are easily computable rules, called Buchberger's criterion and Gebauer-Möller's one. Those are using the relation of the LMs of a pair and those of a triple, see [4, Chapter 5.5]. Then, in 2002, Faugére [20] introduced the notion of *signature* and proposed his F_5 algorithm based on a general rule among signatures. We call algorithms using signatures including variants of F_5 *signature-based algorithms (SBA)*. See a survey [18] and Subsection 3.1.2 below for details.
(B) **Using invariants of polynomial ideal:** For a homogeneous ideal I of a polynomial ring R, when its Hilbert function $\mathrm{HF}_{R/I}(z)$ is known before the computation, we can utilize the value $\mathrm{HF}_{R/I}(d)$ for each $d \in \mathbb{N}$ (cf. [37]). Because, by the value $\mathrm{HF}_{R/I}(d)$, we can check whether we can stop the computation of S-polynomials of degree d or not. We call an algorithm using Hilbert functions a *Hilbert driven* (Buchberger's) algorithm. See [37], [12, Chapter 10.2] or [13, Section 3.5].

[1] This ordering is also called the graded reverse lexicographical (grevlex) ordering.

[2] We also call a graded ordering a *degree-compatible* ordering.

(2) **Efficient computation of S-polynomial reduction:** Since the computation of S-polynomial reduction is a dominant step in the whole Gröbner basis computation, its efficiency heavily affects the total efficiency. As the reduction for a polynomial by elements of G is sequentially applied, we can transform the whole reduction to a Gaussian elimination of a matrix. This approach was suggested in form of Macaulay matrices by Lazard [27] and the first efficient algorithm was given by Faugére [19], which is called the F_4 algorithm. Of course, we can combine the F_4 and F_5 algorithms effectively, which is called the *matrix-F_5 algorithm*.

(3) **Solving coefficient growth:** For a polynomial ideal over the rational number field $\mathbb{Q}$, the computation may be suffered by certain growth of coefficients in polynomials appearing during Gröbner basis computation. To resolve this problem, several modular methods were proposed. As a typical one, we can use Chinese remainder algorithm (CRA), where we first compute the reduced Gröbner bases G_p over several finite fields $\mathbb{F}_p$ and then recover the reduced Gröbner basis from G_p's by CRA. See [31] for details about choosing primes p.

Remark 5 For several public key cryptosystems based on polynomial ideals over finite fields or the elliptic curve discrete logarithm problem, estimating the cost of finding zeros of polynomial ideals is important to analyze the security of those systems, where the computation of their Gröbner bases is a fundamental tool. In this situation, the F_5 algorithm and matrix-F_5 algorithm as its efficient variant with an efficient DRL ordering are considered, as not only those can attain efficient computation but also they are suited for estimating the computational complexity.

In the following, we introduce the notion of *homogenization* and an algorithm for Gröbner basis computation based on signatures (F_5 or its variants), which will be used for our study in Section 5 below.

3.1.1 Homogenization of polynomials and monomial orderings

We begin with recalling the notion of homogenization. (See [24, Chapter 4] for details.) Let K be a field, $X = \{x_1, \ldots, x_n\}$ a set of variables, and $\mathcal{T}$ the set of all monomials in X. [3]

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

$$f^h = \sum_{t\in\mathcal{T}} c_t t y^{\deg(f)-\deg(t)}.$$

Thus f^h is a homogeneous polynomial in $X \cup \{y\}$ over K with total degree $d = \deg(f)$. Also for a set F (or a sequence $\boldsymbol{F} = (f_1, \ldots, f_m) \in K[X]^m$) of polynomials, its *homogenization* F^h (or $\boldsymbol{F}^h$) is defined as $F^h = \{f^h \mid f \in F\}$ (or $\boldsymbol{F}^h = (f_1^h, \ldots, f_m^h) \in K[X \cup \{y\}]^m$). We also write X^h for $X \cup \{y\}$.

[3] As the symbol m is used for the size of a generating set, we use $\mathcal{T}$ instead of $\mathcal{M}$.

(2) Conversely, for a homogeneous polynomial h in $K[X\cup\{y\}]$, its *dehomogenization* h^{deh} is defined by substituting y with 1, that is, $h^{\mathrm{deh}} = h(X,1)$. (It is also denoted by $h|_{y=1}$.) For a set H of homogeneous polynomials in $K[X\cup\{y\}]$, its *dehomogenization* H^{deh} (or $H|_{y=1}$) is defined as $H^{\mathrm{deh}} = \{h^{\mathrm{deh}} \mid h \in H\}$. We also apply the dehomogenization to sequences of polynomials.
(3) For an ideal I of $K[X]$, its homogenization I^h, as an ideal, is defined as $\langle I^h\rangle_{K[X\cup\{y\}]}$. We remark that, for a set F of polynomials in $K[X]$, we have $\langle F^h\rangle_{K[X^h]} \subset I^h$ with $I = \langle F\rangle_{K[X]}$, and the equality does not hold in general.
(4) For a homogeneous ideal J in $K[X\cup\{y\}]$, its dehomogenization J^{deh}, as a set, is an ideal of $K[X]$. We note that if a homogeneous ideal J is generated by H, then $J^{\mathrm{deh}} = \langle H^{\mathrm{deh}}\rangle_{K[X]}$ and for an ideal I of $K[X]$, we have $(I^h)^{\mathrm{deh}} = I$.
(5) For a monomial (term) ordering $\prec$ on the set of *monomials* $\mathcal{T}$ in X, its *homogenization* $\prec_h$ on the set of *monomials* $\mathcal{T}^h$ in $X\cup\{y\}$ 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 its *X-part* and its $\{y\}$-part (or y-part simply), respectively. If a monomial ordering $\prec$ is *graded*, 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 $\{h^{\mathrm{deh}} \mid h \in H\}$ is also a Gröbner basis of $\langle F\rangle$ with respect to $\prec$.

3.1.2 Signature and F_5 algorithm

Here we briefly outline the F_5 algorithm, which is an improvement of Buchberger's algorithm. For details, see a survey [18]. Let $F = \{f_1,\ldots,f_m\} \subset R = K[X]$ be a given generating set. For each polynomial h constructed during the Gröbner basis computation of $\langle F\rangle$, the F_5 algorithm attaches a *special label called a signature* as follows: Since h belongs to $\langle F\rangle$, it can be written as

$$h = a_1f_1 + a_2f_2 + \cdots + a_mf_m \tag{8}$$

for some $a_1,\ldots,a_m \in R$. Then, we assign h to $a_1\mathbf{e}_1+\cdots+a_m\mathbf{e}_m \in R^m$ and we call its leading monomial $t\mathbf{e}_i$ with respect to a monomial (module) ordering in R^m *the signature* of h. As the expression (8) is not unique, in order to determine the signature, we construct the expression procedurally or use the uniquely determined residue in $R^m/\mathrm{syz}(f_1,\ldots,f_m)$ by a module Gröbner basis of $\mathrm{syz}(f_1,\ldots,f_m)$. (For the latter case, we call it the *minimal* signature.) Here we denote the signature of h by $\mathrm{sig}(h)$. Anyway, in the F_5 algorithm, we can meet the both by carefully choosing S-polynomials and by applying restricted reduction steps (called Σ-reductions) for S-polynomials without any change of the signature. (So, we need not compute a module Gröbner basis of $\mathrm{syz}(f_1,\ldots,f_m)$.) We note that for the S-polynomial $S(h_1,h_2) = c_1t_1h_1 - c_2t_2h_2$ with $c_1,c_2 \in K$ and $t_1,t_2 \in \mathcal{T}$, the signature $\mathrm{sig}(S(h_1,h_2))$ is determined as the largest one between $\mathrm{sig}(c_1t_1h_1)$ and $\mathrm{sig}(c_2t_2h_2)$. Then, we have the following criteria, which are very useful to avoid the computation of unnecessary S-polynomials. (The latter one is called the *syzygy criterion*.)

Proposition 4 (cf. [12], [18]) *In the F_5 algorithm, we need not compute an S-polynomial if some S-polynomial of the same signature was already proceeded, since both are reduced to the same polynomial. Moreover, we need not compute an S-polynomial of signature s if there is a signature s' such that s' divides s and some S-polynomial with the signature s' is reduced to* 0*.*

3.2 Complexity of the Gröbner basis computation

In general, determining the complexity of computing a Gröbner basis is very hard; in the worst-case, the complexity is doubly exponential in the number of variables, see e.g., [10], [28], [33] for surveys. It is well-known that a Gröbner basis with respect to a graded monomial ordering (in particular, DRL ordering) can be computed quite more efficiently than ones with respect to other orderings in general. Moreover, in the case where the input polynomials generate a zero-dimensional ideal, once a Gröbner basis with respect to an efficient monomial ordering is computed, one with respect to any other ordering can be computed easily by the FGLM basis conversion algorithm [21]. 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.

A typical way to estimate the complexity of computing a Gröbner basis for a sequence $\boldsymbol{F}$ of polynomials is to count the number of S-polynomials that are reduced during the Gröbner basis computation. In the case where the chosen monomial ordering is graded, the most efficient strategy to compute Gröbner bases is the normal strategy, on which we proceed *degree by degree*, namely increase the degree of critical pairs defining S-polynomials, as in the F_4 and F_5 algorithms. For an algorithm adopting this strategy, several S-polynomials are dealt with consecutively at the same degree, which is called the *step degree*. The highest step degree at which an intermediate ideal basis contains a minimal Gröbner basis is called the *solving degree* of the algorithm, and it is denoted by $\mathrm{sd}_{\prec}^{\mathrm{hsd}}(\boldsymbol{F})$. Determining (or finding a tight bound for) the solving degree is difficult without computing any Gröbner basis. Once it is specified, we may estimate the complexity of the algorithm, as in [36].

On the other hand, for a linear algebra-based algorithm, such as an F_4-family including the (matrix-)F_5 algorithm and the XL family (cf. [11]), that follows Lazard's strategy [26] to reduces S-polynomials by the Gaussian elimination on Macaulay matrices, Caminata-Gorla [7] defined *another solving degree* in a different manner. Specifically, it is defined as the lowest degree d at which the reduced row echelon form (RREF) of the Macaulay matrix $M_{\leq d}(\boldsymbol{F})$ produces a Gröbner basis, see [7] for details. In this case, the complexity is estimated to be $O(N^{\omega})$ with $N = \binom{n+d}{n}$, where ω is the *matrix multiplication exponent* with $2 \leq \omega < 3$. For a given polynomial sequence $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ and a graded monomial ordering $\prec$, we denote by $\mathrm{sd}_{\prec}^{\mathrm{mac}}(\boldsymbol{F})$ this solving degree. In a series of works (cf. [7], [5], [8]) by Gorla et al., they provided a mathematical formulation for the relation between the solving degree $\mathrm{sd}_{\prec}^{\mathrm{mac}}(\boldsymbol{F})$ (or $\mathrm{sd}_{\prec}^{\mathrm{mut}}(\boldsymbol{F})$ described below) and algebraic invariants coming from $\boldsymbol{F}$, such as the maximal Gröbner basis degree, the degree of regularity, the Castelnuovo–Mumford regularity, the first and last fall degrees, and so on. Here, the *maximal Gröbner basis degree* of the ideal $\langle \boldsymbol{F} \rangle_R$ is the maximal degree of elements in the reduced Gröbner basis of $\langle \boldsymbol{F} \rangle_R$ with respect to a fixed monomial ordering $\prec$, and is denoted by $\mathrm{max.GB.deg}_{\prec}(\boldsymbol{F})$.

In the following, we recall some of Caminata et al.'s results. 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 the previous subsection, 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

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

see [7] for a proof. Here, we also recall Lazard's bound for the maximal Gröbner basis degree of $\langle \boldsymbol{F}^h \rangle_{R'}$ with $R' = R[y]$:

Theorem 4 (Lazard; [26, Theorem 2]) *With notation as above, we assume that the number of projective zeros of $\boldsymbol{F}^h$ 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., $\boldsymbol{F}^{\mathrm{top}}$ has no solution in $\overline{K}^n$ other than $(0, \ldots, 0)$. Then, supposing also that $d_1 \geq \cdots \geq d_m$ and putting $\ell := \min\{m, n+1\}$, we have*

$$\mathrm{max.GB.deg}_{\prec^h}(\boldsymbol{F}^h) \leq d_1 + \cdots + d_\ell - \ell + 1 \tag{9}$$

Lazard's bound given in (9) is also referred to as the *Macaulay bound*, and it provides an upper-bound for the solving degree of $\boldsymbol{F}$ with respect to a DRL ordering.

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

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

for any graded ordering $\prec'$ on R, see [7, Remark 15] or Lemma 4 below for a proof. Both $d_{\mathrm{reg}}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle)$ and $\mathrm{sd}_{\prec}^{\mathrm{mac}}(\boldsymbol{F})$ are greater than or equal to $\mathrm{max.GB.deg}_{\prec}(\boldsymbol{F})$, whereas the degree of regularity (or the first fall degree) used in the cryptographic literature as a proxy (or a heuristic upper-bound) for the solving degree. However, it is pointed out in [5], [7], and [8] by explicit examples that *any* of the degree of regularity and the first fall degree does *not* produce an estimate for the solving degree in general, even when $\boldsymbol{F}$ is an affine (cryptographic) semi-regular sequence. In [8], Caminata-Gorla provided yet another solving degree, denoted by $\mathrm{sd}_{\prec'}^{\mathrm{mut}}(\boldsymbol{F})$, with respect to algorithms based on the *mutant strategy* (see [9] for details), and they proved that it is nothing but the *last fall degree* if it is greater than the maximal Gröbner basis degree:

Theorem 5 ([8, Theorem 3.1]) *With notation as above, for any graded monomial ordering $\prec'$ on R, we have the following inequality:*

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

where $d_{\boldsymbol{F}}$ denotes the last fall degree of $\boldsymbol{F}$ defined in [8, Definition 1.5].

By this theorem, if $d_{\mathrm{reg}}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle) < d_{\boldsymbol{F}}$, the degree of regularity is no longer an upper-bound on the solving degree.

On the other hand, Semaev and Tenti claimed (see Tenti's thesis [36] for a proof) that the solving degree $\mathrm{sd}_{<}^{\mathrm{hsd}}(\boldsymbol{F})$ (in terms of the highest step degree) is linear in the degree of regularity, if K is a (large) 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 6 ([35, Theorem 2.1], [36, Corollary 3.67]) *With notation as above, assume that $K = \mathbb{F}_q$, and that $\boldsymbol{F}$ contains $x_i^q - x_i$ for $1 \leq i \leq n$. Put $D = d_{\mathrm{reg}}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle)$. If $D \geq \max\{\deg(f) : f \in \boldsymbol{F}\}$ and $D \geq q$, then we have*

$$\mathrm{sd}_{<}^{\mathrm{hsd}}(\boldsymbol{F}) \leq 2D - 2. \tag{10}$$

In Subsection 5.2 below, we will prove a similar inequality (10) for the case where $\boldsymbol{F}$ not necessarily contains a field equation but is cryptographic semi-regular.

4 Hilbert-Poincaré series of affine semi-regular sequence

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. Recall Definition 7 for the definition of cryptographic semi-regular sequences.

The Hilbert-Poincaré series associated to a (homogeneous) cryptographic semi-regular sequence is given by (7). On the other hand, the Hilbert-Poincaré series associated to the homogenization $\boldsymbol{F}^h$ of $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ not necessarily homogeneous polynomials cannot be computed without knowing its Gröbner basis in general, but we shall prove that it can be computed up to the degree $d_{\mathrm{reg}}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle)$ if $\boldsymbol{F}$ is affine cryptographic semi-regular, namely $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular.

Theorem 7 *Let $R = K[x_1, \ldots, x_n]$ and $R' = R[y]$, and let $\boldsymbol{F} = (f_1, \ldots, f_m)$ be a sequence of not necessarily homogeneous polynomials in R. Assume that $\boldsymbol{F}$ is affine cryptographic semi-regular. Then, for each d with $d < D := d_{\mathrm{reg}}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle)$, we have*

$$\mathrm{HF}_{R'/\langle \boldsymbol{F}^h \rangle}(d) = \mathrm{HF}_{R/\langle \boldsymbol{F}^{\mathrm{top}} \rangle}(d) + \mathrm{HF}_{R'/\langle \boldsymbol{F}^h \rangle}(d-1), \tag{11}$$

and hence

$$\mathrm{HF}_{R'/\langle \boldsymbol{F}^h \rangle}(d) = \mathrm{HF}_{R/\langle \boldsymbol{F}^{\mathrm{top}} \rangle}(d) + \cdots + \mathrm{HF}_{R/\langle \boldsymbol{F}^{\mathrm{top}} \rangle}(0), \tag{12}$$

whence we can compute the value $\mathrm{HF}_{R'/\langle \boldsymbol{F}^h \rangle}(d)$ from the formula (7).

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 (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

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

for $i = 0$. This means that the chain complex $K_\bullet \otimes_{R'} R$ gives rise to the Koszul complex on $(f_1^{\mathrm{top}}, \dots, f_m^{\mathrm{top}})$. 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 the 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 $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, it follows from Proposition 3 that $H_1(K_\bullet \otimes_{R'} R)_{\le D-1} = 0$ for $D := d_{\mathrm{reg}}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle)$. 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

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

by the dimension theorem. Since $H_0(K_\bullet) = R'/\langle \boldsymbol{F}^h \rangle$ and $H_0(K_\bullet \otimes_{R'} R) \cong R/\langle \boldsymbol{F}^{\mathrm{top}} \rangle$, we have the equality (11), as desired. $\square$

Remark 6 With notation as in Theorem 7, assume that $D < \infty$ (and thus $m \ge n$). In the proof of Theorem 7, 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 $d < D-1$. 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 $\langle \boldsymbol{F}^h\rangle$ 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 $\boldsymbol{F}$).

By Theorem 4, it can be proved that the Hilbert-Poincaré series of $R'/\langle \boldsymbol{F}^h\rangle$ satisfies the following equality (13), which may correspond to [3, Proposition 6]:

Corollary 1 *Let $D = d_{\mathrm{reg}}(\langle \boldsymbol{F}^{\mathrm{top}}\rangle)$. Then we have*

$$\mathrm{HS}_{R'/\langle \boldsymbol{F}^h\rangle}(z) \equiv \frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^{n+1}} \pmod{z^D}. \tag{13}$$

Therefore, by Theorem 3 ([14, Theorem 1]), $\boldsymbol{F}^h$ is D-regular. Here, we note that $D = \deg(\mathrm{HS}_{R/\langle \boldsymbol{F}^{\mathrm{top}}\rangle}) + 1 = \deg\left(\left[\frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^n}\right]\right) + 1$.

Proof. Let $\mathrm{HS}'(z) = \frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^{n+1}} \bmod z^D$ and let $\mathrm{HF}'(d)$ denote the coefficient of $\mathrm{HS}'(z)$ of degree d for $d < D$. First we remark that, as $\boldsymbol{F}^{\mathrm{top}}$ is a cryptographic semi-regular sequence, the Hilbert-Poincaré series of $R/\langle \boldsymbol{F}^{\mathrm{top}}\rangle$ satisfies the following:

$$\mathrm{HS}_{R/\langle \boldsymbol{F}^{\mathrm{top}}\rangle}(d) = \left[\frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^n}\right] = \frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^n} \bmod z^D,$$

since $\mathrm{HF}_{R/\langle \boldsymbol{F}^{\mathrm{top}}\rangle}(d) = 0$ for $d \geq D$. Then we have

$$\begin{aligned}\mathrm{HS}'(z) \bmod z^D &= \frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^{n+1}} \bmod z^D \\ &= \frac{\prod_{i=1}^m (1-z^{d_i})}{(1-z)^n} \times (1+z+\cdots+z^{D-1}) \bmod z^D \\ &= \mathrm{HS}_{R/\langle \boldsymbol{F}^{\mathrm{top}}\rangle}(z) \cdot (1+z+\cdots+z^{D-1}) \bmod z^D.\end{aligned}$$

Therefore, for $d < D$, the equation (12) gives

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

which implies the desired equality (13). ◻

To prove the following corollary, we use a fact that, for a homogeneous ideal I in R, the equality $\sum_{i=0}^d \dim_K I_i = \dim_K (IR')_d$ holds for each $d \geq 0$. Also we take a graded ordering $\prec$ (preferably a DRL ordering) on monomials in X and its homogenization on monomials in $X \cup \{y\}$.

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

Proof. We prove $(\langle \mathrm{LM}(\tilde{I}) \rangle_{R'})_d \subset (\langle \mathrm{LM}(\overline{I}) \rangle_{R'})_d$ by the induction on d. The case where $d = 0$ is clear from Theorem 7, and so we assume $d > 0$. Any element in $(\langle \mathrm{LM}(\tilde{I}) \rangle_{R'})_d$ is represented as a finite sum of elements in R' of the form $g \cdot \mathrm{LM}(h)$ with $g \in R'$, $h \in \tilde{I}$, and $\deg(gh) = d$. Hence, we can also write each $g \cdot \mathrm{LM}(h)$ as a K-linear combination of elements of the form $\mathrm{LM}(th)$ for a monomial t in R' of degree $\deg(g)$, where th is an element in $\tilde{I}$ of degree d. Therefore, it suffices for showing "$\subset$" to prove that $\mathrm{LM}(f) \in (\langle \mathrm{LM}(\overline{I}) \rangle_{R'})_d$ for any $f \in \tilde{I}$ with $\deg(f) = d$. We may assume that f is homogeneous. It is straightforward that $f|_{y=0} \in \overline{I}_{\leq d}$. If $\mathrm{LM}(f) \in R = K[x_1, \ldots, x_n]$, then we have $\mathrm{LM}(f) = \mathrm{LM}(f|_{y=0}) \in \mathrm{LM}(\overline{I})$. Thus, we may also assume that $y \mid \mathrm{LM}(f)$. In this case, it follows from the definition of the DRL ordering that any other term in f is also divisible by y, so that $f \in \langle y \rangle_{R'}$. Thus, we can write $f = yh$ for some $h \in R'$, where h is homogeneous of degree $d - 1$. As in the proof of Theorem 7, the multiplication map

$$(R'/\tilde{I})_{d'-1} \longrightarrow (R'/\tilde{I})_{d'} \ ; \ h' \bmod \tilde{I} \mapsto yh' \bmod \tilde{I}$$

is injective for any $d' < d_{\mathrm{reg}}(\overline{I})$, since F is cryptographic semi-regular. Therefore, it follows from $f \in \tilde{I}_d$ that $h \in \tilde{I}_{d-1}$, whence $f = yh \in y\tilde{I}_{d-1}$. By the induction hypothesis, there exists $g \in \overline{I}$ such that $\mathrm{LM}(g) \mid \mathrm{LM}(h)$, whence $\mathrm{LM}(f) \in (\langle \mathrm{LM}(\overline{I}) \rangle_{R'})_d$.

Here, it follows from Theorem 7 that

$$\begin{aligned} \dim_K (R')_d - \dim_K \tilde{I}_d &= \sum_{i=0}^{d} \left(\dim_K R_i - \dim_K \overline{I}_i \right) = \sum_{i=0}^{d} \dim_K R_i - \sum_{i=0}^{d} \dim_K \overline{I}_i \\ &= \dim_K (R')_d - \dim_K (\overline{I} R')_d, \end{aligned}$$

and thus $\dim_K \tilde{I}_d = \dim_K (\overline{I} R')_d$. Hence, it follows from $\langle \mathrm{LM}(\overline{I}) \rangle_{R'} = \langle \mathrm{LM}(\overline{I} R') \rangle_{R'}$ that

$$\dim_K (\langle \mathrm{LM}(\tilde{I}) \rangle_{R'})_d = \dim_K (\langle \mathrm{LM}(\overline{I}) \rangle_{R'})_d,$$

whence $(\langle \mathrm{LM}(\tilde{I}) \rangle_{R'})_d = (\langle \mathrm{LM}(\overline{I}) \rangle_{R'})_d$, as desired. □

Example 1 We give a simple example. Let $p = 73$, $K = \mathbb{F}_p$, and

$$\begin{aligned} f_1 &= x_1^2 + (3x_2 - 2x_3 - 1)x_1 + x_2^2 + (-2x_3 - 2)x_2 + x_3^2 + x_3, \\ f_2 &= 4x_1^2 + (3x_2 + 4x_3 - 2)x_1 - x_2 + x_3^2 + 2x_3, \\ f_3 &= 3x_1^2 - x_1 + 9x_2^2 + (-6x_3 + 1)x_2 + x_3^2 - x_3, \\ f_4 &= x_1^2 + (-6x_2 + 2x_3 - 2)x_1 + 9x_2^2 + (-6x_3 + 1)x_2 + 2x_3^2. \end{aligned}$$

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

$$\begin{aligned}
f_1^{\mathrm{top}} &= x_1^2 + (3x_2 - 2x_3)x_1 + x_2^2 - 2x_3x_2 + x_3^2,\\
f_2^{\mathrm{top}} &= 4x_1^2 + (3x_2 + 4x_3)x_1 + x_3^2,\\
f_3^{\mathrm{top}} &= 3x_1^2 + 9x_2^2 - 6x_3x_2 + x_3^2,\\
f_4^{\mathrm{top}} &= x_1^2 + (-6x_2 + 2x_3)x_1 + 9x_2^2 - 6x_3x_2 + 2x_3^2,
\end{aligned}$$

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

$$\{x_3^2x_2, x_3^3, x_1^2{+}68x_3x_2{+}55x_3^2, x_2x_1{+}27x_3x_2{+}29x_3^2, x_2^2{+}x_3x_2{+}71x_3^2, x_3x_1{+}3x_3x_2{+}33x_3^2\}.$$

Then its leading monomials are $x_3^3, x_3^2x_2, x_1^2, x_1x_2, x_2^2, x_3x_1$ and its Hilbert-Poincaré series satisfies

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

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

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

$$\begin{aligned}
&\{y^3x_1, y^3x_2, y^3x_3, 60y^2x_1 + (x_3^2 + 22y^2)x_2 + 39y^2x_3,\\
&72y^2x_1 + 14y^2x_2 + x_3^3 + 56y^2x_3, 16y^2x_1 + (yx_3 + 55y^2)x_2 + 38y^2x_3,\\
&72y^2x_1 + 66y^2x_2 + yx_3^2 + 70y^2x_3, x_1^2 + 72yx_1 + (68x_3 + 40y)x_2 + 55x_3^2 + 14yx_3,\\
&(x_2 + 20y)x_1 + (27x_3 + 37y)x_2 + 29x_3^2 + 12yx_3,\\
&57yx_1 + x_2^2 + (x_3 + 3y)x_2 + 71x_3^2 + 52yx_3,\\
&(x_3 + 22y)x_1 + (3x_3 + 5y)x_2 + 33x_3^2 + 14yx_3\}
\end{aligned}$$

and its leading monomials are y^3x_1, y^3x_2, y^3x_3, $x_3^2x_2$, x_3^3, yx_2x_3, yx_3^2, x_1^2, x_1x_2, x_2^2, and x_1x_3. Then the Hilbert-Poincaré series of $R'/\langle \boldsymbol{F}^h \rangle$ satisfies

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

We note that $\mathrm{HF}_{R'/\langle \boldsymbol{F}^h \rangle}(3) = 4$ and $\mathrm{HF}_{R'/\langle \boldsymbol{F}^h \rangle}(4) = 1$. We can also examine $\mathrm{LM}(G_{\mathrm{hom}})_{d<D} = \mathrm{LM}(G_{\mathrm{top}})_{d<D}$ and, for $g \in G_{\mathrm{hom}}$, if $\mathrm{LM}(g)$ is divided by y, then $\deg(g) \geq D = 3$. Thus, at the degree 3, there occurs a *degree-fall*. See [8, Sebsection 2.1] for details. Also, the reduced Gröbner basis of $\langle \boldsymbol{F} \rangle$ with respect to $\prec$ is $\{x, y, z\}$ and we can examine that the dehomogenization of G_{hom} is also a Gröbner basis of $\langle \boldsymbol{F} \rangle$.

5 Application to Gröbner bases computation

We use the same notation as in the previous section, and assume that $\boldsymbol{F}$ is cryptographic semi-regular such that $D := d_{\mathrm{reg}}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle) < \infty$. Here we apply results in the previous section to the computation of Gröbner bases of the ideals $\langle \boldsymbol{F} \rangle$ and $\langle \boldsymbol{F}^h \rangle$. Let G, G_{hom}, and G_{top} be the reduced Gröbner bases of $\langle \boldsymbol{F} \rangle$, $\langle \boldsymbol{F}^h \rangle$, and $\langle \boldsymbol{F}^{\mathrm{top}} \rangle$, respectively, where their monomial orderings are DRL $\prec$ or its extension $\prec^h$.

As to the computation of G, in special settings on $\boldsymbol{F}$ such as $\boldsymbol{F}$ containing field equations or $\boldsymbol{F}$ appearing in a multivariate polynomial cryptosystem, methods using the value D or those of the Hilbert function for degrees less than D were proposed. (See [35, 34].) Our results in the section can be considered as a *certain extension* and to *give exact mathematical proofs* for the correctness of the methods.

Here, we extend the notion of *top part* to a homogeneous polynomial h in $R' = R[y]$. 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.

5.1 Gröbner basis elements of degree less than D

Here we show relations between $(G_{\mathrm{hom}})_{<D}$ and $(G_{\mathrm{top}})_{<D}$ with proofs, which are useful for the computations of G_{hom} and G.

Since $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular and $\boldsymbol{F}^h$ is D-regular by Corollary 1, $H_1(K_\bullet(\boldsymbol{F}^{\mathrm{top}}))_{<D} = H_1(K_\bullet(\boldsymbol{F}^h))_{<D} = 0$. As $H_1(K_\bullet(\boldsymbol{F}^h)) = \mathrm{syz}(\boldsymbol{F}^h)/\mathrm{tsyz}(\boldsymbol{F}^h)$ and $H_1(K_\bullet(\boldsymbol{F}^{\mathrm{top}})) = \mathrm{syz}(\boldsymbol{F}^{\mathrm{top}})/\mathrm{tsyz}(\boldsymbol{F}^h)$ (see (2)), we have the following corollary, where $\mathrm{tsyz}(\boldsymbol{F}^h)$ denotes the module of trivial syzygies (see Definition 1).

Corollary 3 ([14, Theorem 1]) *It follows that* $\mathrm{syz}(\boldsymbol{F}^{\mathrm{top}})_{<D} = \mathrm{tsyz}(\boldsymbol{F}^{\mathrm{top}})_{<D}$ *and* $\mathrm{syz}(\boldsymbol{F}^h)_{<D} = \mathrm{tsyz}(\boldsymbol{F}^h)_{<D}$.

This 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 syzygy, that is, $\sum_{i=1}^m (t_1 a_i^{(1)} - t_2 a_i^{(2)} - b_i)\mathbf{e}_i$ belongs to $\mathrm{tsyz}(\boldsymbol{F}^h)_{<D}$, 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 such as the matrix-F_5 algorithm) with the *Schreyer ordering* automatically discards an S-polynomial whose signature is the LM of some trivial syzygy, we can avoid unnecessary S-polynomials. See Subsection 3.1.2 for a brief outline of the F_5 algorithm and the syzygy criterion (Proposition 4).

In addition to the above facts, as mentioned (somehow implicitly) in [1, Section 3.5] and [3], when we compute a Gröbner basis of $\langle \boldsymbol{F}^h \rangle$ 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 the Gröbner basis computation process of $\langle \boldsymbol{F}^h \rangle$ corresponds exactly to that of $\langle \boldsymbol{F} \rangle$ for each degree less than D, see [25] for details. Especially, the following lemma holds. Here we give a *concrete and easy* proof using Corollary 2. We also note that the argument and the proof of Lemma 2 can be considered as corrected versions for those of [34, Theorem 4].

Lemma 2 *For each degree $d < D$, we have*

$$\mathrm{LM}(G_{\mathrm{hom}})_d = \mathrm{LM}(G_{\mathrm{top}})_d. \tag{14}$$

Proof. We can prove the equality (14) by the induction on d. Assume that the equality (14) holds for $d < D - 1$.

Consider any $t \in \mathrm{LM}(G_{\mathrm{hom}})_{d+1}$. Then, there is a polynomial $g \in G_{\mathrm{hom}}$ such that $\mathrm{LM}(g) = t$. By Corollary 2, for $d + 1 < D$, we have

$$(\langle \mathrm{LM}(\langle \boldsymbol{F}^h \rangle)\rangle_{R'})_{d+1} = (\langle \mathrm{LM}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle_R)\rangle_{R'})_{d+1}$$

and $\mathrm{LM}(g)$ is divided by $\mathrm{LM}(g')$ for some $g' \in G_{\mathrm{top}}$. Since G_{hom} is reduced, $\mathrm{LM}(g)$ is not divisible by any monomial in $\mathrm{LM}(G_{\mathrm{hom}})_{\leq d} = \mathrm{LM}(G_{\mathrm{top}})_{\leq d}$, so that $\deg(g') = d + 1$. Then we have $\mathrm{LM}(g) = \mathrm{LM}(g')$, and so $\mathrm{LM}(G_{\mathrm{hom}})_{d+1} \subset \mathrm{LM}(G_{\mathrm{top}})_{d+1}$.

By the same argument, $\mathrm{LM}(G_{\mathrm{hom}})_{d+1} \supset \mathrm{LM}(G_{\mathrm{top}})_{d+1}$ can be shown. We note that for each $t \in \mathrm{LM}(G_{\mathrm{top}})_{d+1}$, there is a polynomial $g \in (G_{\mathrm{top}})_{d+1} \subset \langle \boldsymbol{F}^{\mathrm{top}} \rangle_{d+1}$ such that $t = \mathrm{LM}(g)$. In this case, there are homogeneous polynomials $a_1, \ldots, a_m$ such that $g = \sum_{i=1}^m a_i f_i^{\mathrm{top}}$. Then $g' = \sum_{i=1}^m a_i f_i^h$ in $\langle \boldsymbol{F}^h \rangle_{d+1}$ has t as its LM. □

Next we consider $(G_{\mathrm{hom}})_D$.

Lemma 3 *For each monomial t in X of degree D, there is an element g in $(G_{\mathrm{hom}})_{\leq D}$ such that $\mathrm{LM}(g)$ divides t. Therefore,*

$$\langle \mathrm{LM}((G_{\mathrm{hom}})_{\leq D})\rangle_{R'} \cap R_D = R_D. \tag{15}$$

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 $\mathrm{LT}(g) = \mathrm{LC}(g)\mathrm{LM}(g)$.)

Proof. Since $\langle \boldsymbol{F}^{\mathrm{top}} \rangle_D = R_D$, for each monomial t in X of degree D, there are homogeneous $a_1, \ldots, a_m \in R$ with $t = \sum_{i=1}^m a_i f_i^{\mathrm{top}}$. Now consider $h = \sum_{i=1}^m a_i f_i^h$, which belongs to $\langle \boldsymbol{F}^h \rangle$. Then, as $f_i^h = f_i^{\mathrm{top}} + y h_i$ for some h_i in R', we have

$$h = \sum_{i=1}^m a_i (f_i^{\mathrm{top}} + y h_i) = \sum_{i=1}^m a_i f_i^{\mathrm{top}} + y \sum_{i=1}^m a_i h_i = t + y \sum_{i=1}^m a_i h_i$$

and $\mathrm{LM}(h) = t$. As G_{hom} is the reduced Gröbner basis of $\langle \boldsymbol{F}^h \rangle$, there is some g in $(G_{\mathrm{hom}})_{\leq D}$ whose LM divides $\mathrm{LM}(h)$, as desired.

Next we prove the second assertion. Let $g_1, \ldots, g_k$ be all elements of $(G_{\mathrm{hom}})_D$ which have non-zero top parts, and set $\mathrm{LM}(g_1) \prec \cdots \prec \mathrm{LM}(g_k)$. We show that

$g_i^{\mathrm{top}} = \mathrm{LT}(g_i)$ for all i. Suppose, to the contrary, that our claim does not hold for some g_i. Then, g_i^{top} can be written as $= \mathrm{LT}(g_i)+T_2+\cdots+T_s$ for some terms $T_2, \ldots, T_s$ in R_D. Since $\mathrm{LM}(T_j) \prec \mathrm{LM}(g_i)$ for $2 \leq j \leq s$, it follows from equality (15) that each $\mathrm{LM}(T_j)$ is equal to $\mathrm{LM}(g_\ell)$ for some $\ell < i$ or is divisible by $\mathrm{LM}(g')$ for some $g' \in (G_{\mathrm{hom}})_{<D}$. This contradicts to the fact that G_{hom} is reduced. □

Remark 7 If we apply a signature-based algorithm such as the F_5 algorithm or its variant to compute the Gröbner basis of $\langle \boldsymbol{F}^h \rangle$, 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 for obtaining the reduced Gröbner basis.

5.2 Gröbner basis elements of degree not less than D

In this subsection, we shall extend the upper bound on solving degree given in [35, Theorem 2.1] to our case.

Remark 8 In [35], polynomial ideals over $\mathbb{F}_q[X]$ are considered. Under the condition where the generating sequence $\boldsymbol{F}$ contains the field equations $x_i^q - x_i$ for $1 \leq i \leq n$, recall from Theorem 6 ([36, Theorem 6.5 & Corollary 3.67]) that the solving degree $\mathrm{sd}_{\prec}^{\mathrm{hsd}}(\boldsymbol{F})$ with respect to a Buchberger-like algorithm for $\langle \boldsymbol{F} \rangle$ is upper-bounded by $2D-2$, where $D = d_{\mathrm{deg}}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle)$. In the proofs of [36, Theorem 6.5 & Corollary 3.67], the property $\langle \boldsymbol{F}^{\mathrm{top}} \rangle_D = R_D$ was essentially used for obtaining the upper-bound. As the property also holds in our case, we may apply their arguments. Also in [5, Section 3.2], the case where $\boldsymbol{F}^h$ 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 result in this subsection.

Now we show an upper-bound on the solving degree of $\boldsymbol{F}$ by using the set $H := \{g|_{y=1} : g \in (G_{\mathrm{hom}})_{\leq D}\}$, that is, at the pre-process of the computation of G, we first compute $H = (G_{\mathrm{hom}})_{\geq D}$, and at the latter process, we continue the computation from H. We remark that, when we use the normal selection strategy on the choice of S-polynomials, the Gröbner basis computation of $\langle \boldsymbol{F} \rangle$ proceeds along with the graded structure of R in its early stages, By Lemma 2 it simulates faithfully that of $\langle \boldsymbol{F}^{\mathrm{top}} \rangle$ until the degree of computed polynomials becomes $D-1$, that is, it produces $\{g|_{y=1} : g \in (G_{\mathrm{hom}})_{<D}\}$. Also, by Lemma 3, it may also produce $\{g|_{y=1} : g \in (G_{\mathrm{hom}})_D,\ g^{\mathrm{top}} \neq 0\}$ by carefully choosing S-polynomials, see [25] for details. We also note that the F_5 algorithm actually uses the normal strategy.

Lemma 4 *If $D \geq \max\{\deg(f) : f \in \boldsymbol{F}\}$, then the maximal Gröbner basis degree and the solving degree $\mathrm{sd}_{\prec}^{\mathrm{hsd}}(\boldsymbol{F})$ (see Subsection 3.2 for the definition of $\mathrm{sd}_{\prec}^{\mathrm{hsd}}(\boldsymbol{F})$) are bounded as follows:*

$$\mathrm{max.GB.deg}_{\prec}(\boldsymbol{F}) \leq D \text{ and } \mathrm{sd}_{\prec}^{\mathrm{hsd}}(\boldsymbol{F}) \leq 2D-2.$$

Proof. Recall from Lemma 3 that $\langle \mathrm{LM}(H)\rangle$ contains all monomials in X of degree D. We continue the Gröbner basis computation from H. In this *latter process*, all polynomials generated from S-polynomials are reduced by elements of H. Therefore, their LM's are reduced with respect to any monomial (in X) of degree D and thus, their degrees are not more than $D-1$. Thus, the maximal Gröbner basis degree is upper-bounded by D, and the degree of S-polynomials dealt in the whole computation is upper-bounded by $2D$.

Next we show that we can avoid any S-polynomial of degree $2D$ or $2D-1$.

- If an S-polynomial $S(g_1, g_2)$ has its degree $2D$, then we have $\deg(g_1) = \deg(g_2) = D$ and $\gcd(\mathrm{LM}(g_1), \mathrm{LM}(g_2)) = 1$. Then, Buchberger's criterion predicts that $S(g_1, g_2)$ is always reduced to 0.
- If an S-polynomial $S(g_1, g_2)$ has its degree $2D-1$, then one has $\deg(g_1) = \deg(g_2) = D$, $\deg(g_1) = D, \deg(g_2) = D-1$ or $\deg(g_1) = D-1, \deg(g_2) = D$. For the case where $\deg(g_1) = D, \deg(g_2) = D-1$ or $\deg(g_1) = D-1, \deg(g_2) = D$, we have $\gcd(\mathrm{LM}(g_1), \mathrm{LM}(g_2)) = 1$, and hence $S(g_1, g_2)$ is always reduced to 0 by Buchberger's criterion.

  Finally, we consider the remaining case where $\deg(g_1) = \deg(g_2) = D$. In this case, g_1 and g_2 should belong to H and recall from Lemma 3 that both of $(g_1)^{\mathrm{top}}$ and $(g_2)^{\mathrm{top}}$ are single terms. Then $S(g_1, g_2)$ cancels the top parts of $t_1 g_1$ and $t_2 g_2$, where $S(g_1, g_2) = t_1 g_1 - t_2 g_2$ for some terms t_1 and t_2. Thus, the degree of $S(g_1, g_2)$ is less than $2D-1$.

$\square$

Remark 9 We refer to [7, Remark 15] for another proof of $\mathrm{max.GB.deg}_{<}(\boldsymbol{F}) \le D$. We also note that, if $D = d_{\mathrm{reg}}(\boldsymbol{F}^{\mathrm{top}})$ is finite, Lemma 3 and Lemma 4 hold without the assumption that $\boldsymbol{F}^{\mathbf{top}}$ is cryptographic semi-regular.

As to the computation of G_{hom}, we have a result similar to Lemma 4. Since $\langle \mathrm{LM}(G_{\mathrm{hom}})_{\le D}\rangle$ 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 $(G_{\mathrm{hom}})_{\le D}$. Thus, letting $\mathcal{U}$ be the set of all polynomials generated during the computation of G_{hom}, we have

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

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 $\binom{n+D}{n}$.

Example 2 When $m = n+1$ and $d_1 = \cdots = d_m = 2$, the Hilbert-Poincáre series of $R/\langle \boldsymbol{F}^{\mathrm{top}}\rangle$ is $\left[\frac{(1-z^2)^{n+1}}{(1-z)^n}\right]$. Since $\frac{(1-z^2)^n}{(1-z)^n} = (1+z)^n = \sum_{i=0}^n \binom{n}{i} z^i$, we have

$$\frac{(1-z^2)^{n+1}}{(1-z)^n} = (1+z)^n(1-z^2) = 1 + nz + \sum_{i=2}^{n}\left(\binom{n}{i} - \binom{n}{i-2}\right) z^i - nz^{n+1} - z^{n+2},$$

so that $D = d_{\mathrm{reg}}(\langle \boldsymbol{F}^{\mathrm{top}} \rangle) = \min\left\{ i : \binom{n}{i} - \binom{n}{i-2} \leq 0 \right\} = \lfloor (n+1)/2 \rfloor + 1$, see [5, Theorem 4.1]. In this case, it follows from

$$2D - 2 = 2(\lfloor (n+1)/2 \rfloor + 1) - 2 = \begin{cases} n+1 & (n\text{: odd}), \\ n & (n\text{: even}) \end{cases}$$

that $\mathrm{sd}_{\prec}^{\mathrm{hsd}}(\boldsymbol{F}) \leq n+1$ in Lemma 4; see [5, Theorem 4.2, Therorem 4.7] for the bound in the case where $\boldsymbol{F}^h$ is a generic sequence.

We note that, in the homogeneous case, the solving degree $\mathrm{sd}_{\prec_h}^{\mathrm{hsd}}(\boldsymbol{F}^h)$ is equal to the maximal Gröbner basis degree of $\boldsymbol{F}^h$ (for an appropriate setting in the algorithm one adopts), so that we can apply Lazard's bound, see Theorem 4. It also follows (see [25] for details) that the solving degree $\mathrm{sd}_{\prec}^{\mathrm{hsd}}(\boldsymbol{F})$ can be upper-bounded by $\mathrm{max.GB.deg}_{\prec^h}(\boldsymbol{F}^h) = \mathrm{sd}_{\prec_h}^{\mathrm{hsd}}(\boldsymbol{F}^h)$, and we can apply Theorem 4, as our case satisfies its conditions. Then, for the case where $m = n+1$ and $d_1 = \cdots = d_{n+1} = 2$, Lazard's bound gives the bound $n+2$ for $\mathrm{max.GB.deg}_{\prec^h}(\boldsymbol{F}^h) = \mathrm{sd}_{\prec_h}^{\mathrm{hsd}}(\boldsymbol{F}^h) \geq \mathrm{sd}_{\prec}^{\mathrm{hsd}}(\boldsymbol{F})$.

Acknowledgements The authors thank the anonymous referee for helpful comments. The authors are also grateful to Yuta Kambe and Shuhei Nakamura for helpful comments. 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. 20
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. 7, 8
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 MEGA 2005: Eighth International Symposium on Effective Methods in Algebraic Geometry, 2005. 7, 8, 17, 20
4. T. Becker and V. Weispfenning: Gröbner Bases: A Computational Approach to Commutative Algebra. GTM, **141**, Springer, NY, 1993. 5, 10
5. 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**, Springer (2021). 7, 13, 14, 22, 24
6. B. Buchberger: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Innsbruck: Univ. Innsbruck, Mathematisches Institut (Diss.) (1965). 2, 9
7. A. Caminata and E. Gorla: Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra. WAIFI 2020: 3–36. 4, 13, 14, 23
8. A. Caminata and E. Gorla: Solving degree, last fall degree, and related invariants. Journal of Symbolic Computation, **114**, 322–335 (2023). 2, 13, 14, 15, 19
9. A. Caminata and E. Gorla: The complexity of solving a random polynomial system. arXiv:2309.03855, 2023. 14
10. J. G. Capaverde: Gröbner bases: Degree bounds and generic ideals. Ph.D thesis, Clemson University, 2014. 13, 17
11. N. Courtois, A. Klimov, J. Patarin, and A. Shamir: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. EUROCRYPT 2000, LNCS, **1807**, Springer, 2000. 13
12. D. A. Cox, J. Little, and D. O'Shea. Ideals, Varieties, and Algorithms (Fourth Edition). Undergraduate Texts in Mathematics, Springer, NY, 2010. 10, 13

13. W. Decker and C. Lossen: Computing in Algebraic Geometry: A Quick Start using SINGULAR. Algorithms and Computation in Mathematics, **16**, Springer, 2006. 10
14. C. Diem: Bounded regularity. Journal of Algebra, Volume **423**, 2015, pp. 1143–1160. 7, 8, 17, 20
15. C. Diem: The XL-algorithm and a Conjecture from Commutative Algebra. Asiacrypt'04, LNCS, **3329**, pp. 323–337. 8
16. J. Ding and D. Schmidt: Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields. In: M. Fischlin, S. Katzenbeisser (eds), Number Theory and Cryptography, Lecture Notes in Computer Science, **8260**, Springer, Berlin, Heidelberg. 4
17. D. Eisenbud: Commutative Algebra: With a View Toward Algebraic Geometry. GTM, vol. **150**, Springer (1995). 8
18. C. Eder and J.-C., Faugère: A survey on signature-based algorithms for computing Gröbner bases. Journal of Symbolic Computation **80** (2017), 719–784. 10, 12, 13
19. J.-C., Faugère: A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra, **139** (1999), 61–88. 2, 11
20. J.-C., Faugère: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). Proceedings of ISSAC 2002, ACM Press, (2002), pp.75–82. 2, 10
21. J.-C., Faugère, P. Gianni, D. Lazard, and T. Mora: Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. Journal of Symbolic Computation, **16** (4), pp. 329–344 (1993) 13
22. R. Fröberg: An inequality for Hilbert series of graded algebras. Math. Scand., **56** (1985), 117–144. 9
23. G. Gaggero and E. Gorla: The complexity of solving a random polynomial system. arxiv: 2309.03855, 2023. 8
24. M. Kreuzer and L. Robbiano: Computational Commutative Algebra 2. Springer, 2005. 11
25. M. Kudo and K. Yokoyama: The solving degree for computing Gröbner bases of affine semi-regular polynomial sequences, in preparation. 21, 22, 24
26. D. Lazard: Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. Computer algebra (London, 1983), pp. 146–156, Lecture Notes in Computer Science, vol. **162**, Springer, Berlin, 1983. 13, 14
27. D. Lazard: Résolution des systèmes d'équations algébriques. Theoretical Computer Science, Volume **15**, Issue 1, pp. 77–110, 1981. 11
28. E. W. Mayr and S. Ritscher: Dimension-dependent bounds for Gröbner bases of polynomial ideals. Journal of Symbolic Computation, Vol. **49** (2013), pp. 78–94. 13
29. G. Moreno-Socías: Autour de la fonction de Hilbert-Samuel (escaliers d'idéaux polynomiaux), Thèse, École Polytechnique, 1991. 9
30. S. Nakamura: Formal Power Series on Algebraic Cryptanalysis, arxiv: 2007.14729, 2023. 4, 5
31. M. Noro and K. Yokoyama. Usage of modular techniques for efficient Computation of ideal operations. Mathematics in Computer Science, **12**, 1–32, 2018. 11
32. K. Pardue: Generic sequences of polynomials. Journal of Algebra, **324.4**, pp. 579–590, 2010. 2, 5, 7, 9
33. S. Ritscher: Degree Bounds and Complexity of Gröbner Bases of Important Classes of Polynomial Ideals. Ph.D thessis, Technische Universität München Institut für Mathematik, 2012. 13
34. Y. Sakata and T. Takagi: An Efficient Algorithm for Solving the MQ Problem using Hilbert Series, Cryptology ePrint Archive, 2023/1650. 20, 21
35. 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. 15, 20, 22
36. 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 13, 15, 22
37. C. Traverso: Hilbert functions and the Buchberger algorithm. Journal of Symbolic Computation **22.4** (1996): 355–376. 10