Degree bounds and synchronization in Gröbner basis computations for affine semi-regular systems

Momonari Kudo* Kazuhiro Yokoyama†

September 1, 2026

Abstract

Determining the complexity of computing Gröbner bases is an important problem in both theory and practice, and solving degrees provide a central measure of this complexity. We study solving degrees and Gröbner basis computations for affine polynomial systems, with particular emphasis on semi-regular sequences.

We first derive two upper bounds for the maximum Gröbner basis degree of the homogenized system. One is based on a regular initial subsequence of the highest-degree homogeneous parts. When these parts form a semi-regular sequence in nondecreasing degree order, the bound involves the n smallest input degrees together with the largest one. The other bound is expressed in terms of the saturation exponent with respect to the homogenizing variable. Both are obtained by bounding the degree from which the Hilbert function of the quotient ring associated with the homogenized system is constant.

We then compare the Buchberger-like Gröbner basis computations for an affine system, its homogenization, and its highest-degree homogeneous parts. The first degree fall is characterized by failure of injectivity of multiplication by the homogenizing variable. Before that point, choices of S-pairs and reducers in any computation can be matched in the others, and reduction sequences, remainders, intermediate bases, and leading monomials correspond under specialization. Cryptographic semi-regularity guarantees this correspondence until the step degree first reaches the degree of regularity. At that degree, affine reduction steps that preserve the sugar degree lift to homogeneous ones, yielding upper bounds on the algorithmic solving degree for a computation starting directly from the affine input.

1 Introduction

Computing Gröbner bases is a fundamental task in computational commutative algebra and in solving polynomial systems. Since Buchberger's original algorithm [8], several major improvements, including the F_4 [21] and F_5 [22] algorithms, have been developed. A central problem in both theory and practice is to estimate the complexity of these computations. When the ideal generated by the input is zero-dimensional and a graded monomial ordering is used, particularly a degree reverse lexicographic (DRL) ordering, this complexity is commonly studied through various notions of *solving degree*, which we review in Section 2.1. For homogeneous systems, degree growth

*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

can often be controlled by invariants of the generated ideal. For affine systems, homogenization makes homogeneous methods available but leaves two distinct problems: bounding degree growth in the homogenized computation and transferring homogeneous information to a computation starting directly from the affine input. These are the two problems addressed in this paper.

Let K be a field, and let $R = K[x_1, \dots, x_n]$ be the polynomial ring in n variables over K. Throughout, we fix a DRL ordering $\prec$ on R. For a polynomial $f \in R \setminus \{0\}$, let f^{top} denote its homogeneous component of highest total degree, and let f^h denote its homogenization in $R' = R[y]$ with respect to an extra variable y. We denote by $\prec^h$ the homogenization of $\prec$ on R', with y as the smallest variable. Note that $\prec^h$ is also a DRL ordering. Let $\boldsymbol{F} = (f_1, \dots, f_m)$ be a sequence of polynomials in $R \setminus \{0\}$, and put $F = \{f_1, \dots, f_m\}$ and $d_i = \deg(f_i)$, where deg denotes total degree. We write $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, \dots, f_m^{\mathrm{top}})$ and $\boldsymbol{F}^h = (f_1^h, \dots, f_m^h)$, and use F^{top} and F^h for the corresponding sets. For a subset H of R or R', we denote by $\langle H \rangle$ the ideal generated by H. For a sequence $\boldsymbol{H} = (h_1, \dots, h_r)$, we also write $\langle \boldsymbol{H} \rangle := \langle h_1, \dots, h_r \rangle$. We write $d_{\mathrm{reg}}(I)$ for the degree of regularity of a homogeneous ideal I, and $\mathrm{max.GB.deg}_{\prec'}(I)$ for the maximum total degree of the elements in the reduced Gröbner basis of an ideal I with respect to a monomial ordering $\prec'$; precise definitions are recalled in Section 2. When $I = \langle H \rangle$, we also write $\mathrm{max.GB.deg}_{\prec'}(H)$ for $\mathrm{max.GB.deg}_{\prec'}(I)$.

A general algebraic framework for studying solving degrees was developed by Caminata, Gorla, and their collaborators, who established rigorous relations among several notions of solving degree, the maximum Gröbner basis degree, and invariants from commutative algebra; see [10, 28, 11]. A complementary line of research uses semi-regularity in the sense of Pardue [46] and the weaker notion of cryptographic semi-regularity as tractable models for overdetermined polynomial systems. The foundational work of Bardet, Faugère, Salvy, and Yang described the Hilbert series and obtained asymptotic estimates for the degree of regularity under cryptographic semi-regularity; see [1, 2, 4]. These estimates have played an important role in complexity analyses in multivariate cryptography. Further work clarified the hypotheses under which such estimates give rigorous bounds for particular notions of solving degree and particular Gröbner basis algorithms; see [6, 26].

The degree of regularity of F^{top} alone does not determine the degree growth in the computation for F^h, while relations among the final Gröbner bases do not determine the intermediate S-pairs and reductions in a computation starting from F. In our previous work [39], we studied the Hilbert–Poincaré series of $R'/\langle F^h \rangle$ and compared the Gröbner bases of $\langle F \rangle$, $\langle F^h \rangle$, and $\langle F^{\mathrm{top}} \rangle$. Building on those results, we address the two issues above by deriving new upper bounds for $\mathrm{max.GB.deg}_{\prec^h}(F^h)$ and by comparing, step by step, the Buchberger-like computations for F, F^h, and F^{top}.

Degree bounds Our first group of results concerns degree growth in the homogenized system. For homogeneous input, $\mathrm{max.GB.deg}_{\prec^h}(F^h)$ coincides with the two notions of solving degree reviewed in Section 2.1 that do not depend on a particular execution, and the relations in Section 2.2 transfer a bound for this quantity to the corresponding solving degrees of F. Lazard's classical bound provides a natural benchmark: In the overdetermined case, its formula involves the $n+1$ largest input degrees. Our first bound instead exploits a regular initial subsequence of $\boldsymbol{F}^{\mathrm{top}}$, while the second reflects saturation with respect to the homogenizing variable y. The results are summarized as follows.

Theorem 1 (Theorem 3.1.3 and Proposition 3.2.1)**.** *Let $\boldsymbol{F} = (f_1, \dots, f_m)$ be a sequence of non-constant polynomials in R, and put $d_i = \deg(f_i)$.*

(1) Assume that $m > n$, that $1 \le d_{n+1} \le \cdots \le d_m$, and that $(f_1^{\mathrm{top}}, \dots, f_n^{\mathrm{top}})$ is a regular sequence. Then

$$\mathrm{max.GB.deg}_{\prec^h}(F^h) \le d_1 + \cdots + d_n + d_m - n.$$

If, in addition,

$$\max\left\{d_m,\, d_{\mathrm{reg}}\left(\langle f_1^{\mathrm{top}},\dots,f_{n+1}^{\mathrm{top}}\rangle\right)\right\} \le \left\lfloor \frac{d_1+\cdots+d_{n+1}-n-1}{2} \right\rfloor + 1,$$

then

$$\max.\mathrm{GB}.\deg_{\prec^h}(F^h) \le d_1+\cdots+d_n+d_{n+1}-n.$$

(2) *Put* $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$*, and let* s *be the least positive integer such that* $(\langle F^h\rangle : y^s) = (\langle F^h\rangle : y^\infty)$*, where* $(I : y^\infty) := \bigcup_{k\ge 1}(I : y^k)$ *denotes the saturation of* I *with respect to* y*. Then* $\max.\mathrm{GB}.\deg_{\prec^h}(F^h) \le D + s - 1$.

The hypothesis in Theorem 1 (1) on regularity is generic: for fixed degrees over an infinite field, a generic choice of $f_1^{\mathrm{top}},\dots,f_n^{\mathrm{top}}$ forms a regular sequence. If $\boldsymbol{F}^{\mathrm{top}}$ is semi-regular, then its first n elements form a regular sequence, and Theorem 1 (1) applies after permuting only $f_{n+1},\dots,f_m$ so that $d_{n+1} \le \cdots \le d_m$. In particular, if the generators are indexed in nondecreasing degree order and $\boldsymbol{F}^{\mathrm{top}}$ is semi-regular in this order, the first bound involves the n smallest input degrees together with the largest one, whereas Lazard's bound involves the $n+1$ largest input degrees. Under the additional numerical condition in the theorem, d_m is replaced by d_{n+1}, the $(n+1)$-st smallest input degree in this setting. The second bound is system-dependent in a different sense. Since $\langle F\rangle^h = (\langle F^h\rangle : y^\infty)$, the exponent s measures the y-torsion separating the ideal generated by the homogenized input from the homogenization of the affine ideal. If $\langle F^h\rangle$ is already saturated with respect to y, then $s = 1$ and the bound reduces to $\max.\mathrm{GB}.\deg_{\prec^h}(F^h) \le D$. Thus this estimate complements the degree-based bounds above and connects the first group of results with the y-torsion governing degree falls below.

Both bounds are obtained by first estimating $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)$, defined in Section 2.3 as the least degree from which the Hilbert function of $R'/\langle F^h\rangle$ is constant. For Theorem 1 (1), this estimate follows from the vanishing of the first Koszul homology. For Theorem 1 (2), in the nontrivial case $D < \infty$, it follows from an exact sequence associated with saturation by powers of y. Together with a bound for $d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$, Hashemi's result converts these estimates into the stated bounds on the maximum Gröbner basis degree.

Degree falls and specialization Our second group of results concerns the Gröbner basis computation process itself. The systems F^{top}, F^h, and F are related by the specializations $y = 0$ and $y = 1$. The basic relation between an affine system and its highest-degree homogeneous parts before degree falls is familiar in the study of semi-regular systems and is implicit in several complexity analyses based on the degree of regularity, especially for matrix-F_5 type algorithms; see, e.g., [1, 2, 4, 3]. Our contribution is to make this relation explicit at the level of individual steps of a Buchberger-like computation and determine how long the choices and the resulting polynomials can be made to correspond under specialization. Here the step degree is the degree of the S-pair selected under the normal selection strategy; see Section 2.1.

We also use this comparison to revisit earlier upper bounds on algorithmic solving degrees. Tenti [50] and Semaev–Tenti [49] obtained such bounds over finite fields under assumptions involving the field equations. In our previous work [39], analogous bounds over arbitrary fields were obtained by restarting the computation after dehomogenizing a partial Gröbner basis of the homogenized system. The comparison developed here shows that this restart is unnecessary. The main consequences are summarized as follows.

Theorem 2. *With notation as above, assume that* $\boldsymbol{F}^{\mathrm{top}}$ *is cryptographic semi-regular, and put* $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle) \in \mathbb{Z}_{>0} \cup \{\infty\}$.

(1) *If $D < \infty$, then, before the step degree first reaches D, corresponding S-pairs can be selected in the three Gröbner basis computations for $\langle F^{\mathrm{top}} \rangle$, $\langle F^h \rangle$, and $\langle F \rangle$. After a reduction sequence is chosen in any one of them, corresponding sequences can be constructed in the other two; reduction steps that specialize to the identity at $y = 0$ are omitted. The resulting remainders, intermediate bases, and leading monomials correspond under the specializations $y = 0$ and $y = 1$. If $D = \infty$, the same statements hold through every finite step degree. In particular, no degree fall occurs in the indicated part of the affine computation.*

(2) *Assume in addition that $D < \infty$. At the first stage at which the step degree reaches D, we carry out the affine computation using the sugar strategy and the reduction convention introduced in Definition 4.4.2. For every selected affine S-pair of sugar degree D, the part of its reduction sequence that preserves the sugar degree lifts to a reduction sequence for the corresponding homogeneous S-pair. Consequently, the leading monomials obtained by the end of sugar degree D generate a monomial ideal containing every monomial of R of degree D.*

If $D \geq \max\{\deg(f) : f \in F\}$, then the algorithmic solving degree of the resulting Buchberger-like computation is at most $2D - 1$. If, after sugar degree D, the sugar strategy is stopped and the polynomials obtained up to that degree are inter-reduced before the computation is continued, then the solving degree in the strict sense is at most $2D - 2$.

Theorem 2 (1) allows an S-pair or a reduction sequence to be chosen first in any one of the three computations; corresponding choices can then be made in the other two. In particular, this correspondence is realized by the deterministic choices described in Remark 4.2.5. The mechanism behind the correspondence is the multiplication-by-y map on $R'/\langle F^h \rangle$. We define the y-injectivity threshold d_{inj} as the first positive degree in which this map is not injective and prove that it is exactly the first step degree at which a degree fall occurs in the affine computation. If $d_{\mathrm{inj}} = \infty$, no degree fall occurs. Cryptographic semi-regularity implies $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) \leq d_{\mathrm{inj}}$, but the converse does not hold; see Section A.2. Thus cryptographic semi-regularity is a sufficient condition for the correspondence below D, whereas injectivity of multiplication by y is the underlying condition. When the step degree first reaches D, a full correspondence of reduction sequences may fail. Theorem 2 (2) shows that the reduction steps preserving the sugar degree still lift from the affine computation to the homogeneous one. This is enough to control all monomials of R of degree D and to apply the argument of [39, Lemma 4] directly to the computation starting from F. The same construction can more generally be carried out at any finite threshold below which multiplication by y is injective, in particular at d_{inj} when it is finite.

Beyond the numerical bounds, Theorem 2 transfers degree-by-degree information from the homogeneous computations to a computation performed directly on the affine input. Before the first degree fall, leading monomials, intermediate bases, and reduction outcomes may be analyzed on the homogeneous side without replacing F by a dehomogenized partial Gröbner basis. Because the governing condition is injectivity of multiplication by y, rather than semi-regularity itself, the same argument applies to systems outside the cryptographic semi-regular class whenever that injectivity can be established; see Section A.2. The theorem also permits arbitrary matched choices of S-pairs and reduction sequences within the stated setting, while Remark 4.2.5 gives one deterministic realization.

2 Preliminaries and auxiliary results

In this section, we review several notions of solving degree and collect known degree bounds relevant to this paper. In Section 2.3, we use the stabilization index of the Hilbert function, which agrees with the classical Hilbert regularity when finite, as a generalized degree of regularity. We then

relate this invariant to the maximum Gröbner basis degree and record a specialization property of Koszul homology that will also be used later. We recall below the notions of semi-regularity, cryptographic semi-regularity, and their affine variants; see also [39, Section 2.1], where concise descriptions and characterizations in terms of Hilbert series are given.

Notations and Terminology We continue to use the notation from Section 1. In particular, let $R = K[x_1, \dots, x_n]$ denote the polynomial ring in n variables over a field K, let F be a finite subset of $R \setminus \{0\}$, and let $\prec$ be the fixed DRL ordering on R. Unless otherwise stated, we follow [29] for terminology and notation related to Gröbner bases. For example, the total degree of a polynomial f is denoted by $\deg(f)$. For a monomial ordering $\prec$, we denote by $\mathrm{LM}_\prec(f)$ (and $\mathrm{LT}_\prec(f)$) the leading monomial (and term) of a nonzero polynomial f with respect to $\prec$. For a set H of nonzero polynomials, we put $\mathrm{LM}_\prec(H) := \{\mathrm{LM}_\prec(h) : h \in H\}$. For an integer d, we also put $H_d := \{h \in H : \deg(h) = d\}$ and $H_{<d} := \{h \in H : \deg(h) < d\}$, and define $H_{\le d}$ similarly. When $d = \infty$, we use the convention $H_{<d} = H$. For a set $H \subset R' = R[y]$ and $a \in K$, we write $H|_{y=a} := \{h|_{y=a} : h \in H\}$; specialization of a sequence is understood componentwise. For an ideal $I \subset R$, its homogenization in R' is denoted by I^h.

For the definition of homogenization, see [37, Chapter 2] or [39, Section 3.1.1]. For convenience, we recall the homogenization ordering $\prec^h$ on $R' = R[y]$ associated with $\prec$. The ordering $\prec^h$ is a monomial ordering on $R' = R[y]$ defined as follows: For two monomials $t_1 = X_1 y^a$ and $t_2 = X_2 y^b$, where X_1 and X_2 are monomials in R, we set $t_1 \prec^h t_2$ if and only if (i) $\deg(t_1) = \deg(X_1) + a < \deg(t_2) = \deg(X_2) + b$, or (ii) $\deg(t_1) = \deg(t_2)$ and $X_1 \prec X_2$. It is obvious that if $\prec$ is graded, then $\prec^h$ is also graded. Moreover, if $\prec$ is the DRL ordering with $x_n \prec \cdots \prec x_1$, then $\prec^h$ is also the DRL ordering with $y \prec x_n \prec \cdots \prec x_1$.

For a graded K-algebra A and an integer d, we denote by A_d its homogeneous component of degree d. For a non-negative integer d, we also put $R_{\le d} := \bigoplus_{j=0}^{d} R_j$. For a finitely generated standard graded K-algebra $A = \bigoplus_{d \ge 0} A_d$, we denote its Hilbert function, Hilbert series, and Hilbert polynomial by HF_A, $\mathrm{HS}_A(z)$, and HP_A, respectively, where $\mathrm{HF}_A(d) = \dim_K A_d$ and $\mathrm{HS}_A(z) = \sum_{d \ge 0} \mathrm{HF}_A(d) z^d$.

For a commutative ring A, we denote by $\dim(A)$ its Krull dimension; see [19, Section 10.2]. For an ideal I of a polynomial ring S, we say that I is *zero-dimensional* if $\dim(S/I) = 0$; see also [15, Chapter IX]. Recall that, for a homogeneous ideal I in a standard graded polynomial ring S, the degree of regularity $d_{\mathrm{reg}}(I)$ is defined as the smallest non-negative integer d such that $I_d = S_d$, with the convention $d_{\mathrm{reg}}(I) = \infty$ if no such integer exists. If $d_{\mathrm{reg}}(I)$ is finite, then it coincides with the Castelnuovo–Mumford regularity of I as a graded module, denoted by $\mathrm{reg}(I)$; see [19, Section 20.5] for a definition.

For a positive integer d, a homogeneous sequence $\boldsymbol{H} = (h_1, \dots, h_m) \in R_{d_1} \times \cdots \times R_{d_m}$ is said to be *d-regular* if $\mathrm{HS}_{R/\langle \boldsymbol{H} \rangle}(z) \equiv \frac{\prod_{j=1}^{m} (1 - z^{d_j})}{(1-z)^n} \pmod{z^d}$. We use this definition for every positive integer d, thereby extending its usual range $d \ge \max\{d_1, \dots, d_m\}$. The sequence $\boldsymbol{H}$ is said to be *cryptographic semi-regular* if it is $d_{\mathrm{reg}}(\langle \boldsymbol{H} \rangle)$-regular; when $d_{\mathrm{reg}}(\langle \boldsymbol{H} \rangle) = \infty$, this means that $\boldsymbol{H}$ is d-regular for every positive integer d. For $1 \le i \le m$, put $\boldsymbol{H}^{(i)} = (h_1, \dots, h_i)$. We say that $\boldsymbol{H}$ is *semi-regular* if every initial subsequence $\boldsymbol{H}^{(i)}$ is cryptographic semi-regular. By [39, Propositions 1 and 3], this is equivalent to semi-regularity in the sense of Pardue [46]. In particular, if $m \le n$, then regularity, semi-regularity, and cryptographic semi-regularity are equivalent. A sequence $\boldsymbol{F}$ of not necessarily homogeneous polynomials is said to be *affine semi-regular* (resp. *affine cryptographic semi-regular*) if $\boldsymbol{F}^{\mathrm{top}}$ is semi-regular (resp. cryptographic semi-regular).

For a graded module M and an integer a, the notation $M(-a)$ denotes the internal degree shift defined by $M(-a)_d = M_{d-a}$. If $C_\bullet$ is a complex of graded modules, then $C_\bullet(-a)$ denotes the complex obtained by applying this shift termwise: $(C_\bullet(-a))_i = C_i(-a)$. Thus $(-a)$ changes only

the internal grading and does not change the homological indices.

For a finite homogeneous sequence $\boldsymbol{H} = (h_1, \ldots, h_m)$ in a standard graded polynomial ring S, we denote by $K_\bullet(\boldsymbol{H})$ its Koszul complex, regarded as a complex of graded free S-modules, with the grading convention of [29, Definition 7.6.6]. Its boundary maps preserve the internal degree. We denote its i-th homology by $H_i(K_\bullet(\boldsymbol{H}))$ and write $H_i(K_\bullet(\boldsymbol{H}))_d$ for its homogeneous component of internal degree d. The ambient polynomial ring will be specified whenever it is not clear from the context. For $d \geq \max\{d_1, \ldots, d_m\}$, Diem showed in [16, Theorem 1] that $\boldsymbol{H}$ is d-regular if and only if $H_1(K_\bullet(\boldsymbol{H}))_t = 0$ for every $t < d$. The same equivalence remains valid for every positive integer d under the convention above. Indeed, deleting from $\boldsymbol{H}$ all elements of degree at least d changes neither the Hilbert-series congruence modulo z^d nor the Koszul complex in internal degrees below d.

2.1 Solving degrees of Gröbner basis computation

For Buchberger's algorithm and its variants with the normal selection strategy (see [15, Section II.10]), S-pairs are selected according to the least common multiples of their leading monomials. For an S-pair $\boldsymbol{s} = (g_1, g_2)$, we put $\delta_\prec(\boldsymbol{s}) := \deg(\mathrm{lcm}(\mathrm{LM}_\prec(g_1), \mathrm{LM}_\prec(g_2)))$ and call it the *degree of the S-pair*. The corresponding S-polynomial is

$$S(g_1, g_2) = \frac{\mathrm{lcm}(\mathrm{LM}_\prec(g_1), \mathrm{LM}_\prec(g_2))}{\mathrm{LT}_\prec(g_1)} g_1 - \frac{\mathrm{lcm}(\mathrm{LM}_\prec(g_1), \mathrm{LM}_\prec(g_2))}{\mathrm{LT}_\prec(g_2)} g_2. \tag{2.1.1}$$

The two multiples on the right-hand side of (2.1.1) have total degree $\delta_\prec(\boldsymbol{s})$.

At each stage, the normal selection strategy processes an available S-pair whose least common multiple is minimal with respect to $\prec$. Since $\prec$ is graded, the selected pair has minimum degree among all available S-pairs. We call the degree of the selected S-pair the *step degree*. For homogeneous input, the sequence of step degrees is nondecreasing. For inhomogeneous input, however, it may decrease after a reduction produces a polynomial of degree smaller than the degree of the selected S-pair. The normal selection strategy is thus naturally adapted to computations with graded monomial orderings.

Degree growth is one of the main parameters used to estimate the complexity of Gröbner basis computation with respect to a graded monomial ordering. The term *solving degree* is used in the literature for several closely related, but not identical, degree parameters. In this paper, we distinguish a solving degree attached to a particular execution from two others that do not depend on the choice of an execution.

Ding and Schmidt [18] call a computationally dominant step a *solving step*, and call the highest degree of the polynomials involved in such a step the *solving degree*. For the theoretical degree bounds considered in this paper, we use the following closely related global formulation.

Definition 2.1.1 (Solving degree I (algorithmic solving degree); cf. [18, p. 36])**.** Let $\mathcal{A}$ be a Gröbner basis algorithm applied to an input set F with respect to a graded monomial ordering $\prec$. The *algorithmic solving degree* of $\mathcal{A}$ on F is the highest total degree of the polynomials involved during the entire execution of $\mathcal{A}$. We denote it by $\mathrm{sd}_\prec^{\mathcal{A}}(F)$.

For the Buchberger-like algorithm considered in this paper, the algorithmic solving degree is the maximum of the highest step degree and the largest input degree. Indeed, the input polynomials and the two multiples used to form each selected S-polynomial are regarded as polynomials involved in the computation. The two multiples associated with an S-pair $\boldsymbol{s}$ have degree $\delta_\prec(\boldsymbol{s})$, and reductions with respect to a graded monomial ordering do not increase total degree. In particular, if the highest step degree is at least $\max\{\deg(f) : f \in F\}$, then $\mathrm{sd}_\prec^{\mathcal{A}}(F)$ is equal to the highest step degree.

Note that an S-pair discarded by a criterion (cf. [15, p. 116]) before its S-polynomial is formed is not regarded as processed. Accordingly, neither the degree of such a pair nor the corresponding multiples contributes to $\mathrm{sd}^{\mathcal{A}}_{\prec}(F)$.

Remark 2.1.2. The original notion of Ding and Schmidt is operational: A solving step is selected according to running time or memory consumption. It may therefore depend not only on the algorithm but also on its implementation and on the chosen cost measure.

Definition 2.1.1, by contrast, records the maximum degree reached during the whole computation. It therefore gives an upper bound for the operational solving degree of Ding and Schmidt, and the two agree whenever a computationally dominant step occurs at the maximum degree reached.

Remark 2.1.3 (Solving degree in the strict sense)**.** For a selected S-pair $\boldsymbol{s} = (g_1, g_2)$, the leading terms of the two multiples in (2.1.1) cancel, and hence one has $\deg(S(g_1, g_2)) \leq \delta_{\prec}(\boldsymbol{s})$. Following the convention used in [50, 49], we call the highest degree of the nonzero S-polynomials appearing during the computation the *solving degree in the strict sense*. Thus the strict solving degree records the actual degrees after the leading-term cancellations, rather than the degrees assigned to the selected S-pairs. In particular, if $g_i^{\mathrm{top}} = \mathrm{LT}_{\prec}(g_i)$ for $i = 1, 2$ and $S(g_1, g_2) \neq 0$, then $\deg(S(g_1, g_2)) < \delta_{\prec}(\boldsymbol{s})$.

We next recall two notions of solving degree that do not depend on a particular execution. The first, due to Caminata and Gorla [10], is formulated in terms of Macaulay matrices. For a fixed graded monomial ordering $\prec$ and a non-negative integer d, let $M_{\leq d}(F)$ denote the degree-d Macaulay matrix associated with F and $\prec$ in the sense of [10, Section 3].

Definition 2.1.4 (Solving degree II [10])**.** The solving degree of F with respect to $\prec$ is defined as the smallest non-negative integer d such that the reduced row echelon form of the degree-d Macaulay matrix $M_{\leq d}(F)$ yields a Gröbner basis of F with respect to $\prec$. We denote this degree by $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$.

The computation of the reduced row echelon form of $M_{\leq d}(F)$ corresponds to the standard XL algorithm [13], which is based on an idea of Lazard [40].

The third definition is related to the last fall degree. For each non-negative integer d, let $V_{F,d}$ be the smallest K-vector subspace of R such that $F \cap R_{\leq d} \subset V_{F,d}$ and such that, whenever $f \in V_{F,d}$ and $g \in R$ satisfy $\deg(gf) \leq d$, one has $gf \in V_{F,d}$; see [35, Definition 1], [34, Definition 2.1], and [11, Definition 1.5].

Definition 2.1.5 (Solving degree III)**.** The solving degree of F with respect to the fixed graded monomial ordering $\prec$ is defined as the smallest non-negative integer d such that the vector space $V_{F,d}$ contains a Gröbner basis of F with respect to $\prec$. We denote this degree by $\mathrm{sd}^{\mathrm{mut}}_{\prec}(F)$.

The solving degree in Definition 2.1.5 can be interpreted in terms of Macaulay matrices equipped with the so-called mutant strategy; this strategy computes a basis of $V_{F,d}$ for each d, and hence terminates precisely at the degree described in Definition 2.1.5; see [28, Theorem 1]. Algorithms employing this strategy, such as MutantXL [9] and MXL2 [45], are often called *mutant algorithms*; see also [11, 26, 48]. For this reason, we use the notation $\mathrm{sd}^{\mathrm{mut}}_{\prec}(F)$, where "mut" stands for the mutant strategy.

The two notions above correspond, respectively, to the solving degrees $\mathrm{solvdeg}^s$ and $\mathrm{solvdeg}^m$ for standard and mutant algorithms in [26]. We use the superscripts mac and mut to indicate the definition using Macaulay matrices and the mutant strategy, respectively.

We next recall the notion of the maximum Gröbner basis degree, a purely algebraic invariant of the ideal that will be compared with the solving degrees.

Definition 2.1.6 (Maximum Gröbner basis degree)**.** Let S be either R or R', let $I \subset S$ be an ideal, and let $\prec'$ be a monomial ordering on S. The *maximum Gröbner basis degree* of I with

respect to $\prec'$, denoted by $\max.\mathrm{GB}.\deg_{\prec'}(I)$, is defined as the maximum of the total degrees of the elements in the reduced Gröbner basis of I with respect to $\prec'$. If $I = \langle H \rangle$, we sometimes write $\max.\mathrm{GB}.\deg_{\prec'}(H)$ instead of $\max.\mathrm{GB}.\deg_{\prec'}(I)$.

Remark 2.1.7. In a series of works (cf. [10, 6, 28, 11, 26]), Gorla et al. established precise relations between the solving degrees $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ and $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ and several algebraic invariants associated with F. For any graded monomial ordering $\prec$, one has

$$\max.\mathrm{GB}.\deg_{\prec}(F) \leq \mathrm{sd}_{\prec}^{\mathrm{mut}}(F) \leq \mathrm{sd}_{\prec}^{\mathrm{mac}}(F). \tag{2.1.2}$$

Moreover, if all elements of F are homogeneous, then all three quantities coincide.

Remark 2.1.8 (On graded monomial orderings)**.** In practice, Gröbner bases with respect to graded orderings, especially DRL, can often be computed substantially faster than bases with respect to nongraded orderings such as the lexicographical ordering. DRL is also central to the theoretical analysis used in this paper, since the relevant degree bounds, homogenization results, and comparisons with regularity are formulated for graded or DRL orderings. For zero-dimensional ideals, a Gröbner basis can subsequently be converted to another ordering by the FGLM algorithm [23]; more generally, one may use the Gröbner walk [14]. For these practical and theoretical reasons, we work primarily with graded orderings and, when needed, zero-dimensional ideals.

2.2 Known bounds on solving degrees and maximum Gröbner basis degrees

Here we consider a polynomial set $F = \{f_1, \ldots, f_m\} \subset R \setminus \{0\}$, where $R = K[x_1, \ldots, x_n]$, and a graded monomial ordering $\prec$.

If F consists of homogeneous polynomials, then all three quantities in (2.1.2) coincide, whence any upper bound on $\max.\mathrm{GB}.\deg_{\prec}(F)$ also bounds both of these solving degrees. For example, $\max.\mathrm{GB}.\deg_{\prec}(F)$ can be bounded in terms of the Castelnuovo–Mumford regularity $\mathrm{reg}(\langle F \rangle)$ (cf. [5, Corollary 2.5] and [31, Proposition 4.15]), under additional assumptions such as $\prec$ being a DRL ordering and $\langle F \rangle$ being in strong Noether position (see Remark 2.2.1 below). The algorithmic solving degree $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$, however, depends on the particular execution, including the pair-discarding criteria and the stopping rule. For the Buchberger-like computations used in our algorithmic results, the precise computational setting is specified at the beginning of Section 4.

Remark 2.2.1. Several results relate the maximum Gröbner basis degree to the Castelnuovo–Mumford regularity of a homogeneous ideal. Throughout this remark, we assume that $\prec$ is the DRL ordering with $x_n \prec \cdots \prec x_1$.

Bayer and Stillman [5] showed that, if a homogeneous ideal I is given in generic coordinates, then $\max.\mathrm{GB}.\deg_{\prec}(I) \leq \mathrm{reg}(I)$. Hashemi later obtained related statements under structural assumptions on I. In particular:

(1) By [31, Theorem 4.17], if I is in *strong Noether position* (SNP), then

$$\max.\mathrm{GB}.\deg_{\prec}(I) \leq \mathrm{reg}(I) = \overline{\mathrm{hilb}}(I), \tag{2.2.1}$$

where $\overline{\mathrm{hilb}}(I) = \max\{\mathrm{hilb}(\mathrm{sec}(I, j)) \mid 0 \leq j \leq \dim(R/I)\}$ is the *stabilized Hilbert regularity* introduced in [31]. See [31] for the definition of the sections $\mathrm{sec}(I, j)$ and Remark 2.3.2 below for the definition of the Hilbert regularity $\mathrm{hilb}(-)$.

(2) By [30, Theorem 4.1], if I is in *quasi stable position* (QSP) in the sense of [30], then

$$\max.\mathrm{GB}.\deg_{\prec}(I) = \mathrm{reg}(I). \tag{2.2.2}$$

We stress that the terminology is not uniform. It follows from [30, Lemma 3.1] and [33, Definition 3.1 and Proposition 3.2(v)] that every ideal in QSP in the sense of [30] is in quasi-stable position in the sense of [33].

The converse does not hold. Indeed, for $2 \leq i \leq n$ and $d \geq 2$, the ideal $J_{i,d} := \langle x_1^d, \ldots, x_i^d \rangle$ is quasi-stable in the sense of [33], as is readily checked from [33, Definition 3.1(i)]. On the other hand, its minimal monomial generators form its reduced Gröbner basis, while $J_{i,d}$ is a complete intersection; hence $\mathrm{max.GB.deg}_{\prec}(J_{i,d}) = d < i(d-1)+1 = \mathrm{reg}(J_{i,d})$. Therefore $J_{i,d}$ is not in QSP in the sense of [30], since QSP would imply equality by (2.2.2). The special case $J_{2,2} \subset \mathbb{Q}[x_1, x_2]$ is explicitly noted in [30, p. 1171]. Thus the QSP condition of [30] is strictly stronger than quasi-stable position in the sense of [33].

Finally, a homogeneous ideal is in quasi-stable position in the sense of [33] if and only if it is in strong Noether position in the sense of [31]; see [33, Definition 3.1 and Proposition 3.2(v)] and [31, Definition 2.4, Theorem 2.19, and Corollary 2.20].

In the remainder of this subsection, we consider the inhomogeneous case, i.e., F contains at least one inhomogeneous polynomial. In this case, the three quantities in (2.1.2) need not coincide, and it becomes difficult to estimate the solving degrees without knowing a Gröbner basis of $\langle F \rangle$.

A straightforward way to bound the solving degrees in the inhomogeneous case is via homogenization. For the rest of this subsection, we fix a DRL ordering $\prec$ on R, and denote by $\prec^h$ its homogenization on $R' = R[y]$. Then, we have

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

where $F^h = \{f_1^h, \ldots, f_m^h\}$. The inequality $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F) \leq \mathrm{sd}_{\prec^h}^{\mathrm{mac}}(F^h)$ follows from the proof of [10, Theorem 7], while the other inequalities and equality follow from Remark 2.1.7. We note that, without additional assumptions such as zero-dimensionality, the maximum Gröbner basis degree (and hence the solving degree) can grow doubly exponentially in the number of variables (see, e.g., Mayr–Ritscher [43]). The bounds discussed below are therefore meaningful only under additional structural hypotheses.

For a zero-dimensional affine ideal satisfying some hypotheses below, Lazard's classical bound applies to $\mathrm{max.GB.deg}_{\prec^h}(F^h)$.

Theorem 2.2.2 (Lazard's bound; [40, Theorem 2], [41, 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 $d_1 \geq \cdots \geq d_m$, where $d_i := \deg(f_i)$ for $1 \leq i \leq m$, we have*

$$\mathrm{max.GB.deg}_{\prec^h}(F^h) \leq d_1 + \cdots + d_\ell - \ell + 1 \tag{2.2.3}$$

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

For a detailed exposition of Lazard's argument and related degree bounds, see also [12]. One of the key ingredients in the proof of Theorem 2.2.2 is the following lemma.

Lemma 2.2.3 (cf. [40]). *Let I be a homogeneous ideal of $R' = R[y]$, and let d_0 be a positive integer satisfying the following two properties:*

(1) The multiplication-by-y map $(R'/I)_{d_0-1} \longrightarrow (R'/I)_{d_0}$ is surjective.

(2) For any integer $d \geq d_0$, the multiplication-by-y map $(R'/I)_d \longrightarrow (R'/I)_{d+1}$ is injective.

Then $\mathrm{max.GB.deg}_{\prec'}(I) \leq d_0$, where $\prec'$ is the homogenization (with respect to y) of any graded monomial ordering on R.

Lazard showed that one can take $d_0 = d_1 + \cdots + d_\ell - \ell + 1$ in Lemma 2.2.3 to obtain Theorem 2.2.2, where we take $I = \langle F^h \rangle$ and $\prec' = \prec^h$ respectively. The bound in (2.2.3), often referred to as the *Macaulay bound*, yields an upper bound for $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$ via homogenization, and hence also for $\mathrm{sd}^{\mathrm{mut}}_{\prec}(F)$. Whether the same bound applies to an algorithmic solving degree or not depends on the computational setting. The Buchberger-like setting used for our algorithmic results is specified in Section 4.

Bounds via the top homogeneous system For the maximum Gröbner basis degree of $\langle F \rangle$, if $R/\langle F^{\mathrm{top}} \rangle$ is Artinian, where $F^{\mathrm{top}} = \{f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}\}$, then one has

$$\mathrm{max.GB.deg}_{\prec'}(F) \leq d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) \tag{2.2.4}$$

for any graded monomial ordering $\prec'$ on R; see [10, Remark 15] or [39, Lemma 4] for a proof. When $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) < \infty$, it coincides with the Castelnuovo–Mumford regularity $\mathrm{reg}(\langle F^{\mathrm{top}} \rangle)$ of the homogeneous ideal $\langle F^{\mathrm{top}} \rangle$.

Remark 2.2.4. Note that both $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ and $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$ are always greater than or equal to $\mathrm{max.GB.deg}_{\prec}(F)$. In the cryptographic literature, the degree of regularity $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ (or related quantities such as the first fall degree) is often used as a proxy or heuristic upper bound for the solving degree, motivated by the inequality (2.2.4) and by its good predictive behavior in many structured instances. On the other hand, it is pointed out in [6, 10, 11] by explicit examples that the degree of regularity does *not* control the solving degrees in general: Even when $\boldsymbol{F} = (f_1, \ldots, f_m)$ is an affine (cryptographic) semi-regular sequence (that is, $\boldsymbol{F}^{\mathrm{top}}$ is (cryptographic) semi-regular), the quantities $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$ and $\mathrm{sd}^{\mathrm{mut}}_{\prec}(F)$ can be strictly larger than $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$.

As for $\mathrm{sd}^{\mathrm{mut}}_{\prec'}(F)$, Caminata and Gorla proved in [11] that it coincides with the *last fall degree* d_F, introduced by Huang, Kosters, and Yeo [35, Definition 2] (see also [34, Definition 2.5]) whenever $d_F > \mathrm{max.GB.deg}_{\prec'}(F)$. In particular, if $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) < d_F$ and $d_F > \mathrm{max.GB.deg}_{\prec'}(F)$, then $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) < \mathrm{sd}^{\mathrm{mut}}_{\prec'}(F)$. Hence $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ cannot provide an upper bound for $\mathrm{sd}^{\mathrm{mut}}_{\prec'}(F)$.

Nevertheless, a refined bound is available for the mutant strategy. Recently, Salizzoni [48, Theorem 1.1] proved that

$$\mathrm{sd}^{\mathrm{mut}}_{\prec'}(F) \leq d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) + 1,$$

under the assumption that $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) \geq \max\{\deg(f) : f \in F\}$. Thus, although $d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ alone does not bound the solving degrees in general, it still yields an upper bound for $\mathrm{sd}^{\mathrm{mut}}_{\prec'}(F)$ up to an additive constant of one.

Bounds for Buchberger-like algorithms with special settings In the case where $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ is finite, one can derive upper bounds on $\mathrm{sd}^{\mathcal{A}}_{\prec}(F)$ for certain Buchberger-like algorithms based on S-polynomial computation (including variants based on sub-Macaulay matrix computation). These algorithms proceed in two phases: The computation is first carried out up to a fixed degree bound and then continued using the intermediate polynomials obtained so far. Semaev and Tenti [49] considered the case where $K = \mathbb{F}_q$ and F contains the field equations $x_i^q - x_i$ for all $1 \leq i \leq n$. In the first phase of their algorithm, a generating set B of $\langle F \rangle$ is constructed by row-echelon form computation of sub-Macaulay matrices so that every monomial of degree at least D is divisible by the leading monomial $\mathrm{LM}_{\prec}(g)$ for some $g \in B$. The second phase then applies a Buchberger-like algorithm starting from B as its input set.

Theorem 2.2.5 ([49, Theorem 2.1], [50, 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 $D := d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) \geq \max\{\deg(f) : f \in F\}$, then there exists a Buchberger-like algorithm $\mathcal{A}$ (with two phases) to compute the reduced Gröbner basis of F (based on S-polynomials) such that $\mathrm{sd}^{\mathcal{A}}_{\prec}(F) \leq 2D-1$. Furthermore, in the strict sense of Remark 2.1.3, $\mathrm{sd}^{\mathcal{A}}_{\prec}(F) \leq 2D - 2$.*

Independently of Semaev and Tenti's work, analogous bounds over arbitrary fields and without assuming field equations were also obtained in our previous work [39, Lemma 4]. The argument in [39] was formulated under the additional assumption that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular and considered another Buchberger-like algorithm with two phases. In Section 4.4 below, we revisit this result and show that similar bounds remain valid for Buchberger-like algorithms using the sugar strategy together with the reduction convention introduced in Definition 4.4.2 below; see Lemma 4.4.10.

2.3 Hilbert regularity as a generalized degree of regularity

Recall that $d_{\mathrm{reg}}(I) = \infty$ whenever the quotient by a homogeneous ideal I is not Artinian. In particular, this occurs for $\langle F^h \rangle$ when F^h has a nontrivial projective zero over the algebraic closure $\overline{K}$. If F^h has only finitely many projective zeros—equivalently, if $R'/\langle F^h \rangle$ has Krull dimension at most one—then the Hilbert function of $R'/\langle F^h \rangle$ is eventually constant. We use its stabilization index as a replacement for d_{reg} in the degree bounds below.

Definition 2.3.1 (Generalized degree of regularity)**.** Let S be a standard graded polynomial ring over K, and let $I \subset S$ be a homogeneous ideal. We define the *generalized degree of regularity* of I by

$$\widetilde{d}_{\mathrm{reg}}(I) := \inf \{ d_0 \in \mathbb{Z}_{\geq 0} \mid \dim_K(S/I)_d = \dim_K(S/I)_{d_0} \text{ for all } d \geq d_0 \},$$

with the convention that $\inf \emptyset = \infty$.

Remark 2.3.2. The *index of regularity*, also called the *Hilbert regularity* and often denoted by $\mathrm{hilb}(I)$, is the smallest integer $i \geq 0$ such that $\mathrm{HF}_{S/I}(d) = \mathrm{HP}_{S/I}(d)$ for all $d \geq i$.

Since the Hilbert function agrees with the Hilbert polynomial in all sufficiently large degrees, $\widetilde{d}_{\mathrm{reg}}(I) < \infty$ if and only if $\mathrm{HP}_{S/I}$ is constant, and in this case $\widetilde{d}_{\mathrm{reg}}(I) = \mathrm{hilb}(I)$. In particular, if S/I is Artinian, then $\mathrm{HP}_{S/I} = 0$ and $\widetilde{d}_{\mathrm{reg}}(I) = d_{\mathrm{reg}}(I) = \mathrm{hilb}(I)$. If S/I is not Artinian, then $d_{\mathrm{reg}}(I) = \infty$, whereas $\widetilde{d}_{\mathrm{reg}}(I)$ may still be finite. For instance, for $I = \langle y \rangle \subset K[x, y]$, one has $d_{\mathrm{reg}}(I) = \infty$ but $\widetilde{d}_{\mathrm{reg}}(I) = 0$.

This identification allows us to apply bounds involving Hilbert regularity due to Hashemi and collaborators to the maximum Gröbner basis degree; see Proposition 2.3.4 below.

We record the following standard specialization property of Koszul homology. It makes explicit the homological identification underlying the tensor-product argument in the proof of [39, Theorem 7].

Lemma 2.3.3. *Let $\boldsymbol{H} = (h_1, \ldots, h_m)$ be a sequence of homogeneous polynomials in $R' = R[y]$, and put $\boldsymbol{H}' = (h_1, \ldots, h_m, y)$. Then, for every $i \geq 0$, specialization at $y = 0$ induces a degree-preserving isomorphism of graded K-vector spaces $H_i\big(K_\bullet(\boldsymbol{H}')\big) \cong H_i\big(K_\bullet(\boldsymbol{H}|_{y=0})\big)$, where the Koszul complex on the left is taken over R' and that on the right is taken over R.*

Proof. Put $C_\bullet := K_\bullet(\boldsymbol{H})$ and $C'_\bullet := K_\bullet(\boldsymbol{H}')$, where both Koszul complexes are taken over R', and let $\partial_i : C_i \longrightarrow C_{i-1}$ and $\partial'_i : C'_i \longrightarrow C'_{i-1}$ denote their boundary maps. Regarding $C'_\bullet$ as the mapping cone of $C_\bullet(-1) \xrightarrow{\times y} C_\bullet$, we write $C'_i = C_i \oplus C_{i-1}(-1)$ and choose the signs so that

$$\partial'_i(u, v) = \big(\partial_i(u) + yv, -\partial_{i-1}(v)\big).$$

For every i, put $\overline{C}_i := C_i/yC_i$. Since $\partial_i(yC_i) \subseteq yC_{i-1}$, the boundary maps of $C_\bullet$ induce maps $\overline{\partial}_i : \overline{C}_i \longrightarrow \overline{C}_{i-1}$, and hence the graded modules $\overline{C}_i$ form a complex $\overline{C}_\bullet$. Define $\Phi_i : C'_i \longrightarrow \overline{C}_i$ by $\Phi_i(u, v) = u \bmod yC_i$. Then the maps Φ_i are surjective and form a morphism of complexes, because

$$\Phi_{i-1}\big(\partial'_i(u, v)\big) = \partial_i(u) + yv \bmod yC_{i-1} = \partial_i(u) \bmod yC_{i-1} = \overline{\partial}_i\big(\Phi_i(u, v)\big).$$

We next show that the kernel complex of Φ, denoted by $\ker(\Phi_\bullet)$, has zero homology. Since each C_i is a free R'-module, multiplication by y on C_i is injective. Thus every element of $\ker(\Phi_i)$ can be written uniquely as (yu, v) with $u \in C_i(-1)$ and $v \in C_{i-1}(-1)$. Let

$$\psi_i : C_i(-1) \oplus C_{i-1}(-1) \longrightarrow \ker(\Phi_i) \ ; \ (u, v) \longmapsto (yu, v).$$

On $C_i(-1) \oplus C_{i-1}(-1)$, let

$$\delta_i(u, v) = \big(\partial_i(u) + v, -\partial_{i-1}(v)\big),$$

which is the boundary map of the mapping cone of the identity map on $C_\bullet(-1)$. A direct computation gives $\partial'_i \circ \psi_i = \psi_{i-1} \circ \delta_i$. Hence the maps ψ_i define an isomorphism of complexes between the mapping cone of the identity map on $C_\bullet(-1)$ and $\ker(\Phi_\bullet)$. If $\delta_i(u, v) = 0$, then $\partial_i(u) + v = 0$, and hence $v = -\partial_i(u)$. Therefore, $(u, v) = \big(u, -\partial_i(u)\big) = \delta_{i+1}(0, u)$. Thus every cycle is a boundary, and consequently $H_i(\ker(\Phi_\bullet)) = 0$ for every i.

Therefore, the long exact sequence in homology associated with the short exact sequence of complexes $0 \longrightarrow \ker(\Phi_\bullet) \longrightarrow C'_\bullet \xrightarrow{\Phi} \overline{C}_\bullet \longrightarrow 0$ gives degree-preserving isomorphisms $H_i(C'_\bullet) \cong H_i(\overline{C}_\bullet)$ for every i.

Finally, reduction modulo y replaces each h_j by $h_j|_{y=0}$, and therefore gives an isomorphism of graded complexes $\overline{C}_\bullet \cong K_\bullet(\boldsymbol{H}|_{y=0})$, where the latter Koszul complex is taken over R. The assertion follows. □

The following proposition provides an upper bound on the maximum Gröbner basis degree, and hence on the Macaulay and mutant solving degrees, of a homogeneous system H. It will later be applied to F^h.

Proposition 2.3.4. *Let $H = \{h_1, \dots, h_m\}$ be a set of homogeneous polynomials in $R' \setminus K$ with $R' = R[y]$, and put $\boldsymbol{H} := (h_1, \dots, h_m) \in (R' \setminus K)^m$. Assume that $R/\langle H|_{y=0}\rangle$ is Artinian. Then we have the following:*

(1) Assume that no element of H is divisible by y, and that $\boldsymbol{H}|_{y=0}$ is cryptographic semi-regular. Then $\widetilde{d}_{\mathrm{reg}}(\langle H\rangle_{R'}) \geq d_{\mathrm{reg}}(\langle H|_{y=0}\rangle_R) - 1$.

(2) For any DRL ordering $\prec'$ on R' such that y is the least among the variables, one has $\max.\mathrm{GB.deg}_{\prec'}(H) \leq \max\{d_{\mathrm{reg}}(\langle H|_{y=0}\rangle_R), \widetilde{d}_{\mathrm{reg}}(\langle H\rangle_{R'})\}$. This inequality is an equality if the monomial ideal $\langle \mathrm{LM}_{\prec'}(\langle H\rangle)\rangle$ is weakly reverse lexicographic; see [46, Section 4] for the definition of a weakly reverse lexicographic monomial ideal.

Proof. Put $D := d_{\mathrm{reg}}(\langle H|_{y=0}\rangle_R)$ and $D' := \widetilde{d}_{\mathrm{reg}}(\langle H\rangle_{R'})$. Let $K_\bullet$ and $K'_\bullet$ denote the Koszul complexes on $(h_1, \dots, h_m)$ and $(h_1, \dots, h_m, y)$ over R', respectively. Regarding $K'_\bullet$ as the mapping cone of $K_\bullet(-1) \xrightarrow{\times y} K_\bullet$, we obtain the exact sequence

$$H_1(K'_\bullet)_d \longrightarrow H_0(K_\bullet)_{d-1} \xrightarrow{\times y} H_0(K_\bullet)_d \longrightarrow H_0(K'_\bullet)_d \longrightarrow 0 \tag{2.3.1}$$

for each d.

We first prove (1). Assume that no element of H is divisible by y, and that $\boldsymbol{H}|_{y=0}$ is cryptographic semi-regular. By Lemma 2.3.3, for every i and every d one has $H_i(K'_\bullet)_d \cong H_i\big(K_\bullet(\boldsymbol{H}|_{y=0})\big)_d$. Hence, for every $d < D$, it follows from the definition of d_{reg} that $H_0(K'_\bullet)_d \cong (R/\langle H|_{y=0}\rangle)_d \neq 0$. Moreover, the cryptographic semi-regularity of $\boldsymbol{H}|_{y=0}$ and [16, Theorem 1] give $H_1(K'_\bullet)_d = 0$ for every $d < D$. Hence exactness of (2.3.1) implies $\dim_K(R'/\langle H\rangle)_{d-1} < \dim_K(R'/\langle H\rangle)_d$ for every $d < D$. Therefore, we have $D' \geq D - 1$, which proves (1).

We next prove (2). Again by the definition of d_{reg}, we have $H_0(K'_\bullet)_d = 0$ for all $d \geq D$. Thus, for such d, exactness of (2.3.1) shows that multiplication by y induces a surjection $H_0(K_\bullet)_{d-1} \twoheadrightarrow$

$H_0(K_\bullet)_d$, and therefore $\dim_K(R'/\langle H\rangle)_{d-1} \geq \dim_K(R'/\langle H\rangle)_d$ holds. Thus, the non-negative integral sequence $(\dim_K(R'/\langle H\rangle)_d)_{d\geq D}$ is weakly decreasing, from which we have $D' < \infty$, equivalently the Krull dimension of $R'/\langle H\rangle$ is at most one. Moreover, the homogeneous ideal $\langle H\rangle$ is in Noether position. Indeed, if $\dim(R'/\langle H\rangle) = 1$, then $R'/(\langle H\rangle + \langle y\rangle)$ is Artinian, so that $R'/\langle H\rangle$ is finite over $K[y]$. If $\dim(R'/\langle H\rangle) = 0$, Noether position is automatic.

Since $\dim(R'/\langle H\rangle) \leq 1$, Noether position is equivalent to quasi-stable position in the sense of [33]; see [32, the paragraph following Proposition 5.7]. By Remark 2.2.1, quasi-stable position in this sense is equivalent to strong Noether position. Hence $\langle H\rangle$ is in strong Noether position, and (2.2.1) gives $\mathrm{max.GB.deg}_{\prec'}(H) \leq \mathrm{reg}(\langle H\rangle) = \overline{\mathrm{hilb}}(\langle H\rangle)$. If $\dim(R'/\langle H\rangle) = 1$, then $\mathrm{sec}(\langle H\rangle, 0) = \langle H\rangle$ and $\mathrm{sec}(\langle H\rangle, 1) = \langle H\rangle + \langle y\rangle$, so that $\overline{\mathrm{hilb}}(\langle H\rangle) = \max\{D', D\}$ by Remark 2.3.2. If $\dim(R'/\langle H\rangle) = 0$, then $\overline{\mathrm{hilb}}(\langle H\rangle) = D'$. Moreover, $R'/(\langle H\rangle + \langle y\rangle)$ is a graded quotient of $R'/\langle H\rangle$ and is isomorphic to $R/\langle H|_{y=0}\rangle$; hence $D \leq D'$. Thus $\overline{\mathrm{hilb}}(\langle H\rangle) = \max\{D, D'\}$ in either case, proving (2).

The equality under the weakly reverse lexicographic assumption is proved by applying general structural facts as follows: Assume that the initial ideal $J := \langle \mathrm{LM}_{\prec'}(\langle H\rangle)\rangle$ is weakly reverse lexicographic. Then it follows directly from the definition of weakly reverse lexicographic ideals that J is strongly stable; see also [33, Definition 3.1 (iii)] for the definition of a strongly stable ideal. In particular, J satisfies the QSP criterion in [30, Corollary 3.1], and hence $\langle H\rangle$ is in QSP in the sense of [30]. Therefore (2.2.2) gives $\mathrm{max.GB.deg}_{\prec'}(H) = \mathrm{reg}(\langle H\rangle)$. Since the preceding argument shows that $\mathrm{reg}(\langle H\rangle) = \max\{D, D'\}$, equality holds in (2). □

Remark 2.3.5. Although Proposition 2.3.4 is stated for homogeneous systems $H \subset R[y]$, it applies in particular to any affine polynomial system $F \subset R$ via homogenization. Indeed, taking $H = F^h$, one has $H|_{y=0} = F^{\mathrm{top}}$. Hence the assumptions of the proposition reduce to conditions on the top homogeneous system F^{top}. The resulting bound controls $\mathrm{max.GB.deg}_{\prec^h}(F^h)$ and hence, via homogenization, $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$. By (2.1.2), it also bounds $\mathrm{sd}^{\mathrm{mut}}_{\prec}(F)$.

3 New bounds on maximum Gröbner basis degree

In this section, we prove new upper bounds on the maximum Gröbner basis degree, using the notation introduced in Sections 1 and 2. Throughout, $R = K[x_1, \ldots, x_n]$ is equipped with the fixed DRL ordering $\prec$, and $\prec^h$ denotes its homogenization on $R' = R[y]$. For a sequence $\boldsymbol{F} = (f_1, \ldots, f_m)$ of non-constant polynomials in R, we put $d_j = \deg(f_j)$, $\boldsymbol{F}^{(k)} = (f_1, \ldots, f_k)$, and $F^{(k)} = \{f_1, \ldots, f_k\}$ for $k \leq m$, and retain the notation F, F^{top}, and $\boldsymbol{F}^h$ from Section 1.

3.1 New bounds under a regularity assumption

Throughout the rest of this paper, for positive integers n and $d_1, \ldots, d_m$ with $m \geq n$, we set

$$D^{(n;d_1,\ldots,d_m)} := \deg\left(\left[\frac{\prod_{j=1}^m (1-z^{d_j})}{(1-z)^n}\right]\right) + 1, \tag{3.1.1}$$

where $[\cdot]$ means truncating a formal power series in z over $\mathbb{Z}$ after the last consecutive positive coefficient. Note that $D^{(n;d_1,\ldots,d_m)}$ does not depend on the order of $d_1, \ldots, d_m$, and $D^{(n+1;d_1,\ldots,d_m,1)} = D^{(n;d_1,\ldots,d_m)}$ for any $(n; d_1, \ldots, d_m)$. It is known (see [44, Lemma 2.5]) that

$$D^{(n;d_1,\ldots,d_n)} = d_1 + \cdots + d_n - n + 1,\ D^{(n;d_1,\ldots,d_{n+1})} = \left\lfloor \frac{d_1 + \cdots + d_{n+1} - n - 1}{2} \right\rfloor + 1.$$

Lemma 3.1.1. *Let $h_1, \dots, h_m$ be non-constant homogeneous polynomials in R of degrees $d_1, \dots, d_m$. Put $\boldsymbol{H} = (h_1, \dots, h_m)$ and $H = \{h_1, \dots, h_m\}$. Assume that $m > n$ and $1 \le d_{n+1} \le \cdots \le d_m$ and that $\boldsymbol{H}^{(n)} = (h_1, \dots, h_n)$ forms a regular sequence in R. Then $H_1(K_\bullet(\boldsymbol{H}))_d = 0$ for all $d \ge D^{(n;d_1,\dots,d_n)} + d_m$. Moreover, if $\max\{d_m, d_{\mathrm{reg}}(\langle H^{(n+1)}\rangle)\} \le D^{(n;d_1,\dots,d_{n+1})}$ with $H^{(n+1)} = \{h_1, \dots, h_{n+1}\}$, then $H_1(K_\bullet(\boldsymbol{H}))_d = 0$ for all $d \ge D^{(n;d_1,\dots,d_n)} + d_{n+1}$.*

Proof. For each $2 \le j \le m$, we regard $K_\bullet(\boldsymbol{H}^{(j)})$ as the mapping cone of

$$K_\bullet(\boldsymbol{H}^{(j-1)})(-d_j) \xrightarrow{\times h_j} K_\bullet(\boldsymbol{H}^{(j-1)}),$$

as in [16]. This yields a long exact sequence of graded K-vector spaces; in particular, taking $j = m$ we obtain

$$H_1(K_\bullet(\boldsymbol{H}^{(m-1)}))_d \longrightarrow H_1(K_\bullet(\boldsymbol{H}))_d \longrightarrow H_0(K_\bullet(\boldsymbol{H}^{(m-1)}))_{d-d_m}. \tag{3.1.2}$$

We prove the assertions by induction on m.

Case $m = n+1$. Since $\boldsymbol{H}^{(n)}$ is regular, we have $H_1(K_\bullet(\boldsymbol{H}^{(n)}))_d = 0$ for all d and $d_{\mathrm{reg}}(\langle H^{(n)}\rangle) = D^{(n;d_1,\dots,d_n)}$. Thus, it follows that $H_0(K_\bullet(\boldsymbol{H}^{(n)}))_\ell = (R/\langle H^{(n)}\rangle)_\ell = 0$ for all $\ell \ge D^{(n;d_1,\dots,d_n)}$. Considering the sequence (3.1.2) for $m = n+1$, we obtain $H_1(K_\bullet(\boldsymbol{H}^{(n+1)}))_d = 0$ for all $d \ge D^{(n;d_1,\dots,d_n)} + d_{n+1}$, which proves the first assertion for $m = n+1$ (and implies the second assertion in this case).

Induction step for the first assertion. Assume now that $m > n+1$ and that the first assertion holds for $m-1$. Let $d \ge D^{(n;d_1,\dots,d_n)} + d_m$. Since $d_m \ge d_{m-1}$, we have $d \ge D^{(n;d_1,\dots,d_n)} + d_{m-1}$, and thus $H_1(K_\bullet(\boldsymbol{H}^{(m-1)}))_d = 0$ by the induction hypothesis. It remains to show $H_0(K_\bullet(\boldsymbol{H}^{(m-1)}))_{d-d_m} = 0$. Note that $\langle H^{(n)}\rangle \subset \langle H^{(m-1)}\rangle$, hence $d_{\mathrm{reg}}(\langle H^{(m-1)}\rangle) \le d_{\mathrm{reg}}(\langle H^{(n)}\rangle) = D^{(n;d_1,\dots,d_n)}$. Since $d - d_m \ge D^{(n;d_1,\dots,d_n)}$, we have $H_0(K_\bullet(\boldsymbol{H}^{(m-1)}))_{d-d_m} = (R/\langle H^{(m-1)}\rangle)_{d-d_m} = 0$. Therefore, the sequence (3.1.2) implies $H_1(K_\bullet(\boldsymbol{H}))_d = 0$.

Induction step for the second assertion. Assume $\max\{d_m, d_{\mathrm{reg}}(\langle H^{(n+1)}\rangle)\} \le D^{(n;d_1,\dots,d_{n+1})}$. We argue again by induction on m. Let $m > n+1$ and $d \ge D^{(n;d_1,\dots,d_n)} + d_{n+1}$. Since $d_{m-1} \le d_m$, the additional hypothesis is inherited by $\boldsymbol{H}^{(m-1)}$: $\max\{d_{m-1}, d_{\mathrm{reg}}(\langle H^{(n+1)}\rangle)\} \le D^{(n;d_1,\dots,d_{n+1})}$. Hence the induction hypothesis gives $H_1(K_\bullet(\boldsymbol{H}^{(m-1)}))_d = 0$, so it suffices to show $H_0(K_\bullet(\boldsymbol{H}^{(m-1)}))_{d-d_m} = 0$. By $d_m \le D^{(n;d_1,\dots,d_{n+1})}$, we have

$$\begin{aligned} d - d_m &\ge D^{(n;d_1,\dots,d_n)} + d_{n+1} - d_m \ge D^{(n;d_1,\dots,d_n)} + d_{n+1} - D^{(n;d_1,\dots,d_{n+1})} \\ &= (d_1 + \cdots + d_{n+1} - n - 1) + 2 - \left(\left\lfloor \frac{d_1 + \cdots + d_{n+1} - n - 1}{2} \right\rfloor + 1 \right) \\ &\ge \left\lfloor \frac{d_1 + \cdots + d_{n+1} - n - 1}{2} \right\rfloor + 1 = D^{(n;d_1,\dots,d_{n+1})} \ge d_{\mathrm{reg}}(\langle H^{(n+1)}\rangle). \end{aligned}$$

Since $\langle H^{(n+1)}\rangle \subset \langle H^{(m-1)}\rangle$, we also have $d_{\mathrm{reg}}(\langle H^{(m-1)}\rangle) \le d_{\mathrm{reg}}(\langle H^{(n+1)}\rangle)$, and therefore $H_0(K_\bullet(\boldsymbol{H}^{(m-1)}))_{d-d_m} = (R/\langle H^{(m-1)}\rangle)_{d-d_m} = 0$, as desired. □

Proposition 3.1.2. *Let $\boldsymbol{F} = (f_1, \dots, f_m)$ be a sequence of non-constant polynomials in R with $m > n$ and $1 \le d_{n+1} \le \cdots \le d_m$. Assume that $(\boldsymbol{F}^{\mathrm{top}})^{(n)}$ forms a regular sequence in R. Then we have $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle) \le D^{(n;d_1,\dots,d_n)} + d_m - 1$. Moreover, if $\max\{d_m, d_{\mathrm{reg}}(\langle (F^{\mathrm{top}})^{(n+1)}\rangle)\} \le D^{(n;d_1,\dots,d_{n+1})}$, then $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle) \le D^{(n;d_1,\dots,d_n)} + d_{n+1} - 1 = D^{(n+1;d_1,\dots,d_{n+1})}$.*

Proof. Let $\boldsymbol{F}' = (f_1^h, \dots, f_m^h, y)$. Regarding the Koszul complex $K_\bullet(\boldsymbol{F}')$ as the mapping cone of $K_\bullet(\boldsymbol{F}^h)(-1) \xrightarrow{\times y} K_\bullet(\boldsymbol{F}^h)$, we obtain a long exact sequence of graded K-vector spaces

$$\begin{array}{ccccccc} \cdots \longrightarrow & H_1(K_\bullet(\boldsymbol{F}^h))_{d-1} & \xrightarrow{\times y} & H_1(K_\bullet(\boldsymbol{F}^h))_d & \longrightarrow & H_1(K_\bullet(\boldsymbol{F}'))_d & \\ & \searrow & & & & & \\ & H_0(K_\bullet(\boldsymbol{F}^h))_{d-1} & \xrightarrow[\times y]{} & H_0(K_\bullet(\boldsymbol{F}^h))_d & \longrightarrow & H_0(K_\bullet(\boldsymbol{F}'))_d & \longrightarrow 0. \end{array} \tag{3.1.3}$$

We first show that $H_1(K_\bullet(\boldsymbol{F}'))_d = 0$ for all $d \geq \hat{d}$, where $\hat{d} = D^{(n;d_1,\dots,d_n)} + d_m$ in the first assertion and $\hat{d} = D^{(n;d_1,\dots,d_n)} + d_{n+1}$ in the second one. Here we put $\boldsymbol{H} = (f_1^h, \dots, f_n^h, y, f_{n+1}^h, \dots, f_m^h)$. Recall that, for each k with $1 \leq k \leq m$, the specialization $y \mapsto 0$ induces a natural isomorphism of graded K-algebras

$$R'/\langle f_1^h, \dots, f_k^h, y\rangle \cong R/\langle f_1^{\mathrm{top}}, \dots, f_k^{\mathrm{top}}\rangle. \tag{3.1.4}$$

In particular, the corresponding Hilbert series coincide. Since $(\boldsymbol{F}^{\mathrm{top}})^{(n)}$ is a regular sequence, the Hilbert-series characterization of regular sequences [1, Proposition 1.7.4] gives

$$\mathrm{HS}_{R'/\langle \boldsymbol{H}^{(n+1)}\rangle} = \mathrm{HS}_{R/\langle (\boldsymbol{F}^{\mathrm{top}})^{(n)}\rangle} = \frac{\prod_{j=1}^n (1-z^{d_j})}{(1-z)^n} = \frac{\prod_{j=1}^n (1-z^{d_j})(1-z)}{(1-z)^{n+1}},$$

where $\boldsymbol{H}^{(n+1)} = (f_1^h, \dots, f_n^h, y)$. Therefore, the sequence $\boldsymbol{H}^{(n+1)}$ is also regular in R'. Moreover, we have $d_{\mathrm{reg}}(\langle f_1^h, \dots, f_n^h, y, f_{n+1}^h\rangle) = d_{\mathrm{reg}}(\langle (F^{\mathrm{top}})^{(n+1)}\rangle)$. In addition, it follows immediately from the definition of $D^{(n;d_1,\dots,d_m)}$ (see (3.1.1)) that $D^{(n+1;d_1,\dots,d_n,1)} = D^{(n;d_1,\dots,d_n)}$ and $D^{(n+1;d_1,\dots,d_n,1,d_{n+1})} = D^{(n;d_1,\dots,d_{n+1})}$. Hence Lemma 3.1.1, applied to the homogeneous sequence $\boldsymbol{H}$ in R' with $m+1 > n+1$, gives $H_1(K_\bullet(\boldsymbol{H}))_d = 0$ for all $d \geq \hat{d}$, in each of the first and second assertions. Since the Koszul complex is unchanged up to the usual sign isomorphism under a permutation of the sequence, we have $H_1(K_\bullet(\boldsymbol{F}'))_d \cong H_1(K_\bullet(\boldsymbol{H}))_d = 0$ for all $d \geq \hat{d}$.

Next, by (3.1.4) with $k = m$, one has $H_0(K_\bullet(\boldsymbol{F}'))_d \cong (R/\langle F^{\mathrm{top}}\rangle)_d$. Since $d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle) \leq d_{\mathrm{reg}}(\langle (F^{\mathrm{top}})^{(n)}\rangle) = D^{(n;d_1,\dots,d_n)}$, this vector space vanishes for every $d \geq D^{(n;d_1,\dots,d_n)}$, and hence for every $d \geq \hat{d}$.

Since $H_1(K_\bullet(\boldsymbol{F}'))_d = H_0(K_\bullet(\boldsymbol{F}'))_d = 0$ for every $d \geq \hat{d}$, exactness of (3.1.3) shows that multiplication by y induces an isomorphism

$$H_0(K_\bullet(\boldsymbol{F}^h))_{d-1} \xrightarrow{\sim} H_0(K_\bullet(\boldsymbol{F}^h))_d$$

for every $d \geq \hat{d}$. Therefore the Hilbert function of $R'/\langle F^h\rangle$ is constant from degree $\hat{d}-1$ onward, and hence $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle) \leq \hat{d} - 1$. □

We can combine Proposition 3.1.2 and Proposition 2.3.4 to obtain the following bound.

Theorem 3.1.3. *Let $\boldsymbol{F} = (f_1, \dots, f_m)$ be a sequence of non-constant polynomials in R with $m > n$ and $1 \leq d_{n+1} \leq \cdots \leq d_m$. Assume that $(\boldsymbol{F}^{\mathrm{top}})^{(n)}$ forms a regular sequence in R. Then, for any DRL ordering $\prec$ on R (and its homogenization $\prec^h$ on R'), we have*

$$\max.\mathrm{GB.deg}_{\prec^h}(F^h) \leq D^{(n;d_1,\dots,d_n)} + d_m - 1 = d_1 + \cdots + d_n + d_m - n.$$

Moreover, if $\max\{d_m, d_{\mathrm{reg}}(\langle (\boldsymbol{F}^{\mathrm{top}})^{(n+1)}\rangle)\} \leq D^{(n;d_1,\dots,d_{n+1})}$, then

$$\max.\mathrm{GB.deg}_{\prec^h}(F^h) \leq D^{(n;d_1,\dots,d_n)} + d_{n+1} - 1 = d_1 + \cdots + d_n + d_{n+1} - n.$$

Proof. Set $\hat{d} := D^{(n;d_1,\ldots,d_n)} + d_m$ (or $\hat{d} := D^{(n;d_1,\ldots,d_n)} + d_{n+1}$ under the additional assumption). By Proposition 3.1.2, we have $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle) \leq \hat{d} - 1$. Moreover, since $(\boldsymbol{F}^{\mathrm{top}})^{(n)}$ is regular, it follows that $d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle) \leq D^{(n;d_1,\ldots,d_n)} \leq \hat{d}-1$. Hence $\max\{\, d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle),\ \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)\,\} \leq \hat{d}-1$. Applying Proposition 2.3.4 (2) with $H = F^h$ and $\boldsymbol{H} = \boldsymbol{F}^h$ yields the stated bound on $\mathrm{max.GB.deg}_{\prec^h}(F^h)$. □

Remark 3.1.4. Assume that K is an infinite field and fix positive integers $d_1 \leq \cdots \leq d_m$. Then the regularity assumption in Theorem 3.1.3 is generic with respect to the choice of the highest-degree homogeneous parts. Indeed, the set of regular sequences is a nonempty Zariski-open subset $U \subset R_{d_1} \times \cdots \times R_{d_n}$. Hence, the inverse image of U under the natural projection $\pi : R_{d_1} \times \cdots \times R_{d_m} \longrightarrow R_{d_1} \times \cdots \times R_{d_n}$ is again nonempty Zariski-open. Thus, for a generic sequence of homogeneous polynomials of the prescribed degrees, the first n elements form a regular sequence.

Corollary 3.1.5. *Let $\boldsymbol{F} = (f_1, \ldots, f_m)$ be a sequence of non-constant polynomials in R with $m > n$, and assume that $\boldsymbol{F}^{\mathrm{top}}$ is semi-regular. After permuting only the generators $f_{n+1}, \ldots, f_m$, we may assume that $d_{n+1} \leq \cdots \leq d_m$. Under this ordering, the first bound in Theorem 3.1.3 applies. The second bound applies whenever its additional numerical hypothesis is satisfied.*

Proof. The characterization of semi-regularity recalled in Section 2 shows that $(f_1^{\mathrm{top}}, \ldots, f_n^{\mathrm{top}})$ is regular. The result follows from Theorem 3.1.3. □

Remark 3.1.6. Suppose, in addition, that the generators are indexed in nondecreasing degree order, $d_1 \leq \cdots \leq d_m$, and that $\boldsymbol{F}^{\mathrm{top}}$ is semi-regular in this order. Then the regular initial subsequence $(f_1^{\mathrm{top}}, \ldots, f_n^{\mathrm{top}})$ consists of the n generators of smallest degrees, and the first bound in Theorem 3.1.3 involves the n smallest input degrees together with the largest one. This should be compared with Lazard's bound (Theorem 2.2.2), which is formulated after arranging the input degrees in nonincreasing order. When $d_1 = \cdots = d_m$, the two bounds coincide.

Since semi-regularity need not be preserved under an arbitrary permutation (see [46, p. 582]), the nondecreasing degree ordering is an additional assumption on the chosen order of the sequence.

3.2 New bound using saturation exponent

In this subsection, we consider a set F of non-constant polynomials in R with $F \neq F^h$, and derive an upper bound on $\mathrm{max.GB.deg}_{\prec^h}(F^h)$ in terms of the saturation exponent with respect to y. We use the following positive convention: s denotes the least positive integer such that $\langle F\rangle^h = (\langle F^h\rangle : y^\infty) = (\langle F^h\rangle : y^s)$. Thus $s = 1$ when $\langle F^h\rangle$ is already saturated with respect to y. See [29, p. 81] for the definition of saturation exponent. Here, for a monomial $t = x_1^{\alpha_1}\cdots x_n^{\alpha_n} y^k$ of R', we call $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ its X-part.

Proposition 3.2.1. *With notation as above, put $D := d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$. Then, $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle) \leq D+s-1$. Moreover, $\mathrm{max.GB.deg}_{\prec^h}(F^h) \leq D+s-1$. Consequently, the same bound applies to the Macaulay and mutant solving degrees of the homogeneous system F^h.*

Proof. If $D = \infty$, both assertions are immediate. Hence assume that $D < \infty$. Consider the following exact sequence:

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

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

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

First, we show $\mathrm{HF}_{R'/(\langle F^h\rangle+\langle y^s\rangle)}(d)=0$ for $d\geq D+s-1$, so that $\mathrm{HF}_{R'/\langle F^h\rangle}(d)=\mathrm{HF}_{R'/\langle F\rangle^h}(d-s)$. Let t be any monomial in R'_d. If $y^s\mid t$, then $t\in(\langle F^h\rangle+\langle y^s\rangle)_d$. Otherwise, the exponent of y in t is at most $s-1$, and hence the degree of the X-part of t is at least $d-(s-1)\geq D$. Since $D<\infty$, recall from [39, Lemma 3] that $\langle \mathrm{LM}_{\prec^h}(\langle F^h\rangle)\rangle$ contains any monomial of R of degree D, and thus it also contains t. Hence we have $t\in\langle \mathrm{LM}_{\prec^h}(\langle F^h\rangle+\langle y^s\rangle)\rangle$ in either case. This implies that any element in R'_d is reduced to 0 modulo a Gröbner basis of $\langle F^h\rangle+\langle y^s\rangle$ with respect to $\prec^h$, so that $R'_d/(\langle F^h\rangle+\langle y^s\rangle)_d=0$.

Next we show that $\mathrm{HF}_{R'/\langle F\rangle^h}(d)$ becomes constant for $d\geq D-1$, which implies that $\mathrm{HF}_{R'/\langle F^h\rangle}(d)$ becomes constant for $d\geq D+s-1$. Let G be the reduced Gröbner basis of $\langle F\rangle$ with respect to $\prec$. Then G^h is a Gröbner basis of $\langle F\rangle^h$ with respect to $\prec^h$. By [10, Remark 15] (see also [39, Remark 9]), we have $\mathrm{max.GB.deg}_{\prec}(F)\leq D$, and thus any element of G^h is of total degree not greater than D. Since $R/\langle F^{\mathrm{top}}\rangle$ is Artinian, the affine ideal $\langle F\rangle$ is zero-dimensional (see [39, Remark 6]), and hence $R/\langle F\rangle$ is finite-dimensional over K. Let $\{t_1,\ldots,t_r\}$ be the standard monomial basis of $R/\langle F\rangle$ as a K-vector space, that is,

$$\{t_1,\ldots,t_r\}=\{t\in R : t \text{ is a monomial such that } \mathrm{LM}_{\prec}(g)\nmid t \text{ for any } g\in G\}$$

with $r:=\dim_K R/\langle F\rangle<\infty$. It follows from [39, Lemma 3] that any monomial of R_D is divisible by $\mathrm{LM}_{\prec}(g)$ for some $g\in G$. This implies that the degree of each t_i is smaller than D. By Macaulay's basis theorem (cf. [36, Theorem 1.5.7]), as a basis of the K-vector space $(R'/\langle F\rangle^h)_d$, we can take

$$LB'_d=\{t\in R'_d : t \text{ is a monomial such that } \mathrm{LM}_{\prec^h}(g)\nmid t \text{ for any } g\in G^h\}.$$

For each d with $d\geq D-1$, it is clear that $LB'_d\supset\{t_1y^{k_1},\ldots,t_ry^{k_r}\}$ with $\deg(t_i)+k_i=d$, and we claim that the equality holds. Indeed, for every $t\in LB'_d$, it follows from $\mathrm{LM}_{\prec}(G)=\mathrm{LM}_{\prec^h}(G^h)$ that $\mathrm{LM}_{\prec}(g)\nmid t$ for any $g\in G$. Therefore, the X-part of t coincides with some t_i. Thus, for $d\geq D-1$, it follows that $\dim_K(R'/\langle F\rangle^h)_d$ is equal to the constant r.

Consequently, the Hilbert function of $R'/\langle F^h\rangle$ is constant from degree $D+s-1$ onward. Hence $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)\leq D+s-1$, which proves the first assertion. Since $s\geq 1$, one has $D\leq D+s-1$. Therefore Proposition 2.3.4 (2), together with the first inequality, gives $\mathrm{max.GB.deg}_{\prec^h}(F^h)\leq D+s-1$. □

Example 3.2.2. In Appendix A below, we consider the case where $n=3$, $m=4$, $d_1=d_2=d_3=d_4=2$ and $R=\mathbb{F}_{73}[x_1,x_2,x_3]$, where F has one affine zero $(0,0,0)$ with multiplicity 1. In this example, $D=d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)=3$, the saturation exponent s is 3, $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)=4$ and $\mathrm{max.GB.deg}_{\prec^h}(F^h)=4$. Thus, as $D+s-1=5$, the gap between $D+s-1$ and $\widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)$ is 1. Their Hilbert series are as follows:

$$\begin{aligned}\mathrm{HS}_{R'/\langle F^h\rangle} &= 1+4z+6z^2+4z^3+z^4+z^5+\cdots,\\ \mathrm{HS}_{R'/(\langle F^h\rangle+\langle y^3\rangle)} &= 1+4z+6z^2+3z^3,\\ \mathrm{HS}_{R'/\langle F\rangle^h} &= 1+z+z^2+\cdots.\end{aligned}$$

These Hilbert series also verify the identity $\mathrm{HS}_{R'/\langle F^h\rangle}=\mathrm{HS}_{R'/(\langle F^h\rangle+\langle y^3\rangle)}+z^3\mathrm{HS}_{R'/\langle F\rangle^h}$.

4 Correspondence and degree falls in Gröbner basis computations

We continue to use the notation introduced in Sections 2 and 3. In this section, we compare the Gröbner basis computations for $\boldsymbol{F}^{\mathrm{top}}$, $\boldsymbol{F}^h$, and $\boldsymbol{F}$. The basic degree-by-degree relation between

these computations is already implicit in complexity analyses based on semi-regularity. Here we need a more explicit description because the bounds obtained at the end of this section concern the solving degree of the particular Buchberger-like computation considered here and depend on the selection and reduction processes.

We therefore consider the Buchberger-like computations specified below and examine when pair selection, reduction, and insertion of remainders commute with specialization. The computations are *synchronized* before the first *degree fall*, while the first degree fall marks the point at which full synchronization may break. We characterize this point in terms of the injectivity of multiplication by the homogenizing variable y. The three systems are naturally related via specialization: F is obtained from F^h by setting $y = 1$, whereas F^{top} is obtained by setting $y = 0$. Examples illustrating the correspondence are given in Appendix A.

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 the monomial orderings are DRL $\prec$ on R and its homogenization $\prec^h$ on $R' = R[y]$. It is well-known that a Gröbner basis of $\langle F^h\rangle$ yields a Gröbner basis of $\langle F\rangle$ after dehomogenization by setting $y = 1$.

Computational setting Throughout this section, we consider a Buchberger-like Gröbner basis computation that repeatedly selects a single S-pair, forms the corresponding S-polynomial, and reduces it by the current intermediate basis; in particular, we do not consider matrix-based simultaneous reductions such as those used in the F_4 algorithm. When comparing the computations for F^h and F^{top}, the input generators are kept indexed by i when S-pairs are formed; thus generators with different indices are not identified even if $f_i^{\mathrm{top}} = f_j^{\mathrm{top}}$.

We use the normal selection strategy (see the first paragraph of Section 2.1), except in Section 4.4, where the choices of S-pairs and reducers are described separately. Whenever a nonzero remainder is inserted into the current basis, all new S-pairs involving it are generated. We may use any criterion for discarding unnecessary S-pairs which can be examined only by leading monomials; for example, Buchberger's product criterion. Thus an S-pair whose leading monomials are relatively prime is discarded before its S-polynomial is formed. A discarded S-pair is not regarded as processed; its degree is not counted as a step degree, and the corresponding multiples do not contribute to the algorithmic solving degree. We do not prescribe how ties among S-pairs are resolved or in which order reducers are chosen. Proposition 4.2.3 shows that, under its hypothesis, corresponding S-pairs can be selected in either computation and that, after a reduction sequence is chosen in either computation, a corresponding sequence can be constructed in the other; when $a = 0$, reduction steps that specialize to the identity are omitted.

For either of the pairs $(R, \prec)$ and $(R', \prec^h)$, we use the standard notion of polynomial reduction. Let A denote either R or R' and $\prec_A$ the corresponding monomial ordering. A nonzero polynomial $g \in A$ is said to be reducible by a nonzero polynomial $h \in A$ if g has a term ct with monomial t and non-zero constant c such that t is divisible by $\mathrm{LM}_{\prec_A}(h)$. In this case, a one-step reduction of g by h replaces g by $g' = g - c\,\frac{t}{\mathrm{LT}_{\prec_A}(h)}\,h$, by which the term ct is eliminated. Here we write $g \underset{h}{\longrightarrow} g'$. For a set H of nonzero polynomials in A, we say that g is *reducible by* H if it is reducible by some $h \in H$. A reduction sequence of g by H means a sequence $g = r_0 \to r_1 \to \cdots \to r_k$ such that each r_{i+1} is obtained from r_i by a one-step reduction by some element of H. If r_k is not reducible by H, then we call r_k a *remainder* of g (on division) by H and write $g \xrightarrow[H]{*} r_k$.

We denote by $\mathcal{G}_{\mathrm{hom}}$ and $\mathcal{G}$ the sets of all polynomials that occur as elements of the current intermediate basis during the computations of G_{hom} and G, respectively, and similarly define $\mathcal{G}_{\mathrm{top}}$ for G_{top}. Thus each of these sets consists of the original input generators together with all nonzero polynomials inserted into the current basis during the corresponding computation. These sets need not be reduced; after termination, their inter-reductions give G_{hom}, G, and G_{top}, respectively.

Leading monomials of intermediate bases For homogeneous input, the step degrees are nondecreasing under the normal selection strategy, and every nonzero remainder is reduced by the current basis before being inserted. Hence the leading monomial of every such remainder is minimal with respect to divisibility when it is inserted and remains minimal thereafter. Consequently, the only possible nonminimal monomials in $\mathrm{LM}_{\prec^h}(\mathcal{G}_{\mathrm{hom}})$ and $\mathrm{LM}_{\prec}(\mathcal{G}_{\mathrm{top}})$ are those contributed by the original input generators. After removing from these sets the input leading monomials that are properly divisible by another monomial in the same set, the remaining sets are precisely $\mathrm{LM}_{\prec^h}(G_{\mathrm{hom}})$ and $\mathrm{LM}_{\prec}(G_{\mathrm{top}})$, respectively.

For the affine computation, the leading monomial of every nonzero remainder likewise remains minimal with respect to divisibility until the first degree fall. Indeed, during this period every nonzero remainder has total degree equal to its step degree, and hence the step degrees are nondecreasing.

4.1 Degree falls and y-injectivity

We introduce three conditions relating the injectivity of multiplication by y to the absence of y-divisible leading monomials in the homogeneous computation. These conditions will later be used to control degree falls in the affine computation. Let $\mathcal{B}$ be the minimal generating set of the monomial ideal $\langle \mathrm{LM}_{\prec^h}(\langle F^h \rangle)\rangle$, so that $\mathcal{B} = \mathrm{LM}_{\prec^h}(G_{\mathrm{hom}})$. Consider the following conditions for a fixed positive integer d:

(A) The following multiplication-by-y map is injective:

$$(R'/\langle F^h\rangle)_{d-1} \longrightarrow (R'/\langle F^h\rangle)_d \ ; \ h + \langle F^h\rangle \longmapsto yh + \langle F^h\rangle, \tag{4.1.1}$$

where $R' = R[y]$.

(B) No monomial in $\mathcal{B}_d := \mathcal{B} \cap R'_d$ is divisible by y.

(C) In a Buchberger-like computation with the normal selection strategy for $\langle F^h\rangle$, every nonzero remainder obtained at step degree d (see the beginning of Section 2.1) has leading monomial not divisible by y.

Lemma 4.1.1. *For each positive integer d, the condition* (A) *implies condition* (B)*, and the conditions* (B) *and* (C) *are equivalent.*

Conversely, if the condition (B) *holds for every degree $d < d_0$, then the condition* (A) *also holds for every degree $d < d_0$.*

Proof. (A) $\Longrightarrow$ (B): Suppose that $\mathrm{LM}_{\prec^h}(g)$ were divisible by y for some $g \in (G_{\mathrm{hom}})_d$. Since y is the smallest variable for the DRL ordering $\prec^h$, this implies that g itself is divisible by y, say $g = yh$ with $h \in R[y]_{d-1}$. As $g \in \langle F^h\rangle$, the injectivity condition implies that $h \in \langle F^h\rangle_{d-1}$. Hence $\mathrm{LM}_{\prec^h}(h)$ is divisible by $\mathrm{LM}_{\prec^h}(g_1)$ for some $g_1 \in (G_{\mathrm{hom}})_{\leq d-1}$, and so is $\mathrm{LM}_{\prec^h}(g) = y\,\mathrm{LM}_{\prec^h}(h)$. This contradicts the minimality of $\mathcal{B}$.

(B) $\Longleftrightarrow$ (C): By the observation on leading monomials above for homogeneous input, the elements of $\mathcal{B}_d$ not arising from the input generators are precisely the leading monomials of the nonzero remainders obtained at step degree d. On the other hand, $\mathrm{LM}_{\prec^h}(f_i^h) = \mathrm{LM}_{\prec}(f_i) \in R$ for every input generator f_i, so none of the input contributions is divisible by y. Therefore, (B) and (C) are equivalent.

To prove the last statement, assume that $yh \in \langle F^h\rangle_d$ with $h \in R[y]_{d-1}$. Let r be a remainder of h by $(G_{\mathrm{hom}})_{\leq d-1}$, so that $yr \in \langle F^h\rangle_d$. Suppose $r \neq 0$. Then the monomial $\mathrm{LM}_{\prec^h}(yr) = y\,\mathrm{LM}_{\prec^h}(r)$ belongs to $\langle \mathrm{LM}_{\prec^h}(\langle F^h\rangle)\rangle$, whence it is divisible by some element $t \in \mathcal{B}$. Since the condition (B) holds for every degree $< d_0$ and $\deg(t) \leq d < d_0$, we have $y \nmid t$. Therefore, the monomial t satisfies

$t \mid \mathrm{LM}_{\prec^h}(r)$ and $\deg(t) \leq d-1$, contradicting the fact that r is a remainder by $(G_{\mathrm{hom}})_{\leq d-1}$. Thus $r = 0$, and hence $h \in \langle F^h \rangle_{d-1}$. □

For later use, we package the degree-wise conditions above into the following cumulative condition:

Condition 4.1.2 (Injectivity condition below d_0)**.** Let d_0 be a positive integer. For every $d < d_0$, the conditions (A), (B), and (C) hold.

We define the *y-injectivity threshold* d_{inj} by

$$d_{\mathrm{inj}} := \inf\{d \in \mathbb{Z}_{\geq 1} \mid (R'/\langle F^h \rangle)_{d-1} \xrightarrow{\times y} (R'/\langle F^h \rangle)_d \text{ is not injective}\} \tag{4.1.2}$$

where $\inf \emptyset = \infty$. Equivalently, Lemma 4.1.1 shows that d_{inj} is the supremum of the positive integers d_0 for which Condition 4.1.2 holds.

Relation with saturation and semi-regularity Put $I = \langle F^h \rangle$. For every positive integer d, the kernel of (4.1.1) is $((I : y)/I)_{d-1}$. Thus, if $(I : y) \neq I$, then $d_{\mathrm{inj}} - 1$ is the least integer ℓ such that $(I : y)_\ell \neq I_\ell$, and otherwise $d_{\mathrm{inj}} = \infty$.

A criterion of Bayer–Stillman [5, Lemma 1.6], in the form recalled in [30, Lemma 2.1], shows that a linear form ℓ is *generic* for a homogeneous ideal I if and only if $(I : \ell)_d = I_d$ for all sufficiently large d. Moreover, when ℓ is generic for I, the *satiety* $\mathrm{sat}(I)$ is equivalently the least positive integer m such that $(I : \ell)_d = I_d$ for every $d \geq m$.

If $R/\langle F^{\mathrm{top}} \rangle$ is Artinian, then the homogenizing variable y is generic for I. Indeed, the same argument as in the proof of [10, Theorem 11] applies, since $R'/(I + \langle y \rangle) \cong R/\langle F^{\mathrm{top}} \rangle$ is Artinian, so there is no projective zero of I on $y = 0$. In particular, if $d_{\mathrm{inj}} < \infty$, then $d_{\mathrm{inj}} \leq \mathrm{sat}(I)$.

The saturation exponent s used in Section 3.2 measures a different aspect of the same y-torsion phenomenon: It is the least positive integer such that $y^s\big((I : y^\infty)/I\big) = 0$, or equivalently, such that $y^s g \in I$ for every $g \in (I : y^\infty)$.

Lemma 4.1.3. *With notation as above, assume that $R/\langle F^{\mathrm{top}} \rangle$ is Artinian, and let $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$.*

(1) If $d_{\mathrm{inj}} < \infty$, then $d_{\mathrm{inj}} \leq \mathrm{sat}(I) \leq \widetilde{d}_{\mathrm{reg}}(I) \leq D + s - 1$.

(2) If $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, then $D \leq d_{\mathrm{inj}}$. Consequently, if in addition $d_{\mathrm{inj}} < \infty$, then $D \leq d_{\mathrm{inj}} \leq \mathrm{sat}(I) \leq \widetilde{d}_{\mathrm{reg}}(I) \leq D + s - 1$.

Proof. (1) The first inequality follows from the preceding discussion. Since $R'/(I+\langle y \rangle)$ is Artinian, one has $\dim(R'/I) \leq 1$, and hence $\widetilde{d}_{\mathrm{reg}}(I) = \mathrm{hilb}(I)$ by Remark 2.3.2. Thus it follows from [31, Lemma 5.6] that $\mathrm{sat}(I) \leq \widetilde{d}_{\mathrm{reg}}(I)$. The last inequality follows from Proposition 3.2.1.

(2) If $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, then $H_1(K_\bullet(\boldsymbol{F}^{\mathrm{top}}))_d = 0$ for every $d < D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$. By Lemma 2.3.3, the same holds for $H_1(K_\bullet(\boldsymbol{F}'))_d$, where $\boldsymbol{F}' := (f_1^h, \ldots, f_m^h, y)$. Thus the exact sequence (3.1.3) gives the condition (A) for every $d < D$, while Lemma 4.1.1 gives (B) and (C). Consequently, $D \leq d_{\mathrm{inj}}$. □

The converse of Lemma 4.1.3 (2) does not hold. Indeed, the condition $D \leq d_{\mathrm{inj}}$, equivalently Condition 4.1.2 with $d_0 = D$, does not imply cryptographic semi-regularity of $\boldsymbol{F}^{\mathrm{top}}$; see Section A.2 in Appendix A. Thus Condition 4.1.2 with $d_0 = D$ is strictly weaker than cryptographic semi-regularity.

Relation to degree falls We next introduce the notions of a *degree fall* and the *early stage*, which will later be related to the homogeneous conditions above.

Definition 4.1.4 (Degree fall and early stage)**.** Let d be a positive integer. In a Buchberger-like Gröbner basis computation, we say that a *degree fall occurs at step degree* d if a nonzero remainder obtained at step degree d has total degree strictly smaller than d. Under the normal selection strategy, we call the part of the computation preceding the first degree fall the *early stage*. If no degree fall occurs, the whole computation is regarded as the early stage.

For homogeneous input, every nonzero remainder obtained at step degree d is homogeneous of degree d. Hence no degree fall occurs, and the whole computation is the early stage. For arbitrary input, under the normal selection strategy, the step degree is nondecreasing during the early stage.

Lemma 4.1.1 is formulated purely on the homogeneous side. Its significance for the specialized computations will become clear in the next subsection, where we show that the computation for F^h can be synchronized with that for $F^h|_{y=a}$ throughout the early stage. In particular, taking $a = 1$ gives the corresponding synchronization between the computations for F^h and F.

As will be proved in Corollary 4.2.6 below, if $d_{\mathrm{inj}} < \infty$, then d_{inj} is precisely the first step degree at which a degree fall occurs in the chosen Buchberger-like computation for $\langle F \rangle$. If $d_{\mathrm{inj}} = \infty$, then no degree fall occurs. Thus d_{inj} gives a homogeneous characterization of the first degree fall in the affine computation.

Remark 4.1.5 (Comparison with the first fall degree)**.** Following [39, Remark 1], we define the first fall degree in terms of Koszul homology by $d_{\mathrm{ff}} := \inf\left\{ d \in \mathbb{Z}_{\geq 0} \;\middle|\; H_1(K_\bullet(\boldsymbol{F}^{\mathrm{top}}))_d \neq 0 \right\}$ with $\inf \emptyset = \infty$; cf. [11, Definition 1.3]. Then $d_{\mathrm{ff}} \leq d_{\mathrm{inj}}$. Indeed, Lemma 2.3.3 gives $H_1(K_\bullet(\boldsymbol{F}'))_d \cong H_1(K_\bullet(\boldsymbol{F}^{\mathrm{top}}))_d$, which vanishes for every $d < d_{\mathrm{ff}}$, and hence the relevant part of (3.1.3) shows that (4.1.1) is injective. In particular, if $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, then $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) \leq d_{\mathrm{ff}} \leq d_{\mathrm{inj}}$.

4.2 Synchronization among Gröbner basis computations via specialization

In this subsection, we establish a general correspondence principle between Buchberger-like Gröbner basis computations under specialization. This principle provides a unified framework to compare the three computations associated with F^h, F, and F^{top}, and will be applied in the subsequent analysis of the three computations. For $a \in K$, we consider the specialization map $R' = R[y] \longrightarrow R\ ;\ f \longmapsto f^{(a)} := f|_{y=a}$ and compare Buchberger-like Gröbner basis computations for $\langle F^h \rangle \subset R'$ and for its specialization $\langle F^h|_{y=a} \rangle \subset R$ under the normal selection strategy. The key observation is the following: As long as all polynomials actually used in the computation—both for forming S-pairs and as reducers—have leading monomials not divisible by y, the formation and reduction of S-polynomials are compatible with specialization.

We begin with the following easy lemma:

Lemma 4.2.1. *Let $g, h \in R'$ be homogeneous, and assume that $y \nmid \mathrm{LM}_{\prec^h}(h)$. If $g^{(a)}$ admits a one-step reduction by $h^{(a)}$, then there is a corresponding one-step reduction of g by h. Conversely, if g admits a one-step reduction by h, then there is a corresponding one-step reduction of $g^{(a)}$ by $h^{(a)}$ for $a \neq 0$. For $a = 0$, if the monomial of the term of g eliminated by h is not divisible by y, then there is a corresponding one-step reduction of $g^{(a)}$ by $h^{(a)}$, and otherwise, $g^{(a)} \to g^{(a)}$ corresponds, which may be called a* trivial reduction.

Proof. Let

$$g^{(a)} \xrightarrow[h^{(a)}]{} r' := g^{(a)} - c\,\frac{u}{\mathrm{LT}_{\prec}(h^{(a)})}\,h^{(a)}$$

be a one-step reduction in R which eliminates the term cu with a monomial u and a non-zero constant c in $g^{(a)}$. Thus, u is divisible by $\mathrm{LM}_{\prec}(h^{(a)})$. Since g is homogeneous, it follows that $t = u\,y^{\deg(g)-\deg(u)}$ is a monomial of g. By the y-freeness of $\mathrm{LM}_{\prec^h}(h)$, we have $\mathrm{LM}_{\prec^h}(h) = \mathrm{LM}_{\prec}(h^{(a)})$, so that $\mathrm{LM}_{\prec^h}(h) \mid t$. We note that for $a = 0$, $\deg(u)$ should be equal to $\deg(g)$. Hence g admits the one-step reduction in R';

$$g \xrightarrow[h]{} r := g - c' \frac{t}{\mathrm{LT}_{\prec^h}(h)}\, h,$$

where we set $c' = c/a^{\deg(g)-\deg(u)}$ if $a \neq 0$, and $c' = c$ if $a = 0$. In either case, r is a homogeneous polynomial with $r^{(a)} = r'$.

The converse can be shown in the same manner as above: Let g admit the following one-step reduction which eliminates the term ct in g with monomial t and coefficient c;

$$g \xrightarrow[h]{} r := g - c \frac{t}{\mathrm{LT}_{\prec^h}(h)}\, h, \tag{4.2.1}$$

where $c \in K^\times$ and t is a monomial in R'. The assumption $y \nmid \mathrm{LM}_{\prec^h}(h)$ implies $\mathrm{LT}_{\prec^h}(h) = \mathrm{LT}_{\prec^h}(h)^{(a)} = \mathrm{LT}_{\prec}(h^{(a)})$, which divides the X-part of t. Thus, applying the substitution map at $y = a$ to the sequence (4.2.1), we have

$$g^{(a)} \xrightarrow[h^{(a)}]{} r' := g^{(a)} - c \frac{t^{(a)}}{\mathrm{LT}_{\prec}(h^{(a)})}\, h^{(a)} \tag{4.2.2}$$

with $\mathrm{LT}_{\prec}(h^{(a)}) \mid t^{(a)}$. When $a \neq 0$, the above step (4.2.2) is a one-step reduction which eliminates the term $ct^{(a)}$ in $g^{(a)}$. When $a = 0$, if $t^{(a)} \neq 0$, that is, t is not divisible by y, the above step (4.2.2) is also a one-step reduction. In the case where $a = 0$ and $t^{(a)} = 0$, $g^{(a)} = r'$ holds in the above step (4.2.2). □

Definition 4.2.2 (Current intermediate bases)**.** For an S-pair $\boldsymbol{s}$ appearing in the computation for $\langle F^h \rangle$, we denote by $\mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s})}$ and $\mathcal{G}_{\mathrm{hom}}^{(\preceq \boldsymbol{s})}$ the current intermediate bases just before and just after $\boldsymbol{s}$ is processed, respectively. For an S-pair $\boldsymbol{u}$ appearing in the computation for $\langle F^h|_{y=a} \rangle$, the notation $\mathcal{G}_{(y=a)}^{(\prec \boldsymbol{u})}$ and $\mathcal{G}_{(y=a)}^{(\preceq \boldsymbol{u})}$ is defined in the same way.

Proposition 4.2.3. *Let $a \in K$. Suppose that, immediately before the next S-pair is selected, the current intermediate bases in the computations for $\langle F^h \rangle$ and $\langle F^h|_{y=a} \rangle$ correspond under $g \mapsto g^{(a)} := g|_{y=a}$, and that their S-pairs that have neither been processed nor discarded correspond as well. For $a = 0$, the input generators are distinguished by their indices as specified in the computational setting. Let $\boldsymbol{s} = (g_1, g_2)$ be one of these S-pairs in the homogeneous computation, and put $\boldsymbol{s}^{(a)} = (g_1^{(a)}, g_2^{(a)})$. Assume that every polynomial in $\mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s})}$ has leading monomial not divisible by y. Then the following hold.*

(1) The least common multiples of the leading monomials of $\boldsymbol{s}$ and $\boldsymbol{s}^{(a)}$ agree. Hence, $\boldsymbol{s}$ can be selected under the normal selection strategy if and only if $\boldsymbol{s}^{(a)}$ can be selected. Thus, after either pair is selected in one computation, the other pair can be selected in the other computation.

(2) Suppose that a chosen reduction sequence in the homogeneous computation is $S(g_1, g_2) = r_0 \xrightarrow[h_0]{} \cdots \xrightarrow[h_{k-1}]{} r_k$, where r_k is a remainder by $\mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s})}$. After specialization, and after omitting trivial steps when $a = 0$, this gives a reduction sequence of $S(g_1^{(a)}, g_2^{(a)})$ whose remainder is $r_k^{(a)}$.

(3) *Conversely, suppose that a chosen reduction sequence of* $S(g_1^{(a)}, g_2^{(a)})$ *in the specialized computation has remainder* r'*. This sequence can be lifted to a homogeneous reduction sequence. If* $a \neq 0$*, the lifted sequence ends in a homogeneous remainder* r *satisfying* $r^{(a)} = r'$*. If* $a = 0$*, it reaches a homogeneous polynomial* $\widetilde{r}$ *with* $\widetilde{r}^{(0)} = r'$*; further reductions of terms whose monomials are divisible by* y*, if necessary, yield a homogeneous remainder* r *with* $r^{(0)} = r'$*.*

If the homogeneous remainder is zero, or if its specialization is nonzero, the current intermediate bases after the corresponding pairs are processed satisfy $\mathcal{G}_{(y=a)}^{(\preceq \boldsymbol{s}^{(a)})} = \mathcal{G}_{\mathrm{hom}}^{(\preceq \boldsymbol{s})}|_{y=a}$*. If, in addition, the leading monomial of every new nonzero homogeneous remainder is not divisible by* y*, then the S-pairs that have neither been processed nor discarded also correspond after this step.*

Proof. For (1), let US be the set of all S-pairs that have neither been processed nor discarded immediately before $\boldsymbol{s}$ is selected in the homogeneous computation; in particular, $\boldsymbol{s} \in US$. By the hypothesis on the current computations, $US^{(a)} := (\boldsymbol{u}^{(a)})_{\boldsymbol{u} \in US}$ is precisely the family of S-pairs that have neither been processed nor discarded in the specialized computation, with the input indices retained when $a = 0$. For every S-pair $\boldsymbol{u} = (h_1, h_2) \in US$, our assumption gives $y \nmid \mathrm{LM}_{\prec^h}(h_i)$ for $i = 1, 2$. Thus we have $\mathrm{LT}_{\prec^h}(h_i)^{(a)} = \mathrm{LT}_{\prec}(h_i^{(a)})$ and $\mathrm{LM}_{\prec^h}(h_i) = \mathrm{LM}_{\prec}(h_i^{(a)})$, and hence

$$\mathrm{lcm}\big(\mathrm{LM}_{\prec^h}(h_1), \mathrm{LM}_{\prec^h}(h_2)\big) = \mathrm{lcm}\big(\mathrm{LM}_{\prec}(h_1^{(a)}), \mathrm{LM}_{\prec}(h_2^{(a)})\big).$$

Suppose first that $\boldsymbol{s} = (g_1, g_2)$ is selected in the homogeneous computation. As the normal selection strategy is used, for every $\boldsymbol{u} = (h_1, h_2) \in US$ we have

$$\mathrm{lcm}\big(\mathrm{LM}_{\prec^h}(g_1), \mathrm{LM}_{\prec^h}(g_2)\big) \preceq^h \mathrm{lcm}\big(\mathrm{LM}_{\prec^h}(h_1), \mathrm{LM}_{\prec^h}(h_2)\big).$$

Since all these leading monomials and least common multiples belong to R, the restriction of $\prec^h$ to them agrees with $\prec$. Therefore, the corresponding inequality holds in the specialized computation, and $\boldsymbol{s}^{(a)}$ is among the S-pairs that may be selected under the normal selection strategy. The converse follows by the same argument. Thus, after either $\boldsymbol{s}$ or $\boldsymbol{s}^{(a)}$ is selected in one computation, its counterpart may be selected in the other. Moreover, $S(g_1, g_2)^{(a)} = S(g_1^{(a)}, g_2^{(a)})$.

For (2), assume that the following reduction sequence is chosen:

$$S(g_1, g_2) = r_0 \xrightarrow[h_0]{} \cdots \xrightarrow[h_{k-1}]{} r_k \tag{4.2.3}$$

with remainder r_k by $\mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s})}$, where each reducer $h_i \in \mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s})}$ is homogeneous and satisfies $y \nmid \mathrm{LM}_{\prec^h}(h_i)$. Applying Lemma 4.2.1 successively to each step in (4.2.3), specialization at $y = a$ yields

$$S(g_1^{(a)}, g_2^{(a)}) = r_0^{(a)} \xrightarrow[h_0^{(a)}]{} \cdots \xrightarrow[h_{k-1}^{(a)}]{} r_k^{(a)}. \tag{4.2.4}$$

For $a \neq 0$, (4.2.4) is a reduction sequence. If $a = 0$, removing the trivial reductions from (4.2.4) gives a reduction sequence whose final polynomial is still $r_k^{(a)}$.

Next we show that $r_k^{(a)}$ is a remainder by $\mathcal{G}_{(y=a)}^{(\prec \boldsymbol{s}^{(a)})}$. If $r_k^{(a)}$ were reducible by some $h' \in \mathcal{G}_{(y=a)}^{(\prec \boldsymbol{s}^{(a)})}$, then the assumed correspondence between the current intermediate bases would give an element $h \in \mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s})}$ such that $h^{(a)} = h'$. By Lemma 4.2.1, r_k would then be reducible by h, contrary to the fact that r_k is a remainder. Thus $r_k^{(a)}$ is a remainder, proving (2).

For (3), let

$$S(g_1^{(a)}, g_2^{(a)}) = r_0' \xrightarrow[h_0^{(a)}]{} \cdots \xrightarrow[h_{\ell-1}^{(a)}]{} r_\ell' \tag{4.2.5}$$

be a chosen reduction sequence in the specialized computation with remainder r'_ℓ, where each h_i is a corresponding element of $\mathcal{G}_{\mathrm{hom}}^{(\prec_{\boldsymbol{s}})}$. Applying Lemma 4.2.1 successively to the one-step reductions in (4.2.5), we obtain a homogeneous reduction sequence

$$S(g_1, g_2) = \widetilde{r}_0 \longrightarrow \widetilde{r}_1 \longrightarrow \cdots \longrightarrow \widetilde{r}_\ell, \tag{4.2.6}$$

where $\widetilde{r}_i^{(a)} = r'_i$ for every i. If $a \neq 0$, in the same manner as in (2), it can be shown that $\widetilde{r}_\ell$ is a remainder. If $a = 0$, the polynomial $\widetilde{r}_\ell$ need not be a remainder. Any term of $\widetilde{r}_\ell$ that is still reducible must, however, have a monomial divisible by y; otherwise the corresponding one-step reduction would remain nontrivial after specialization and would contradict the fact that r'_ℓ is a remainder. Reducing only such y-divisible terms eventually yields a homogeneous remainder r. Since each of these additional reductions specializes to the identity at $y = 0$, we still have $r^{(0)} = \widetilde{r}_\ell^{(0)} = r'_\ell$.

Finally, if the homogeneous remainder is zero, neither computation inserts a new polynomial. If its specialization is nonzero, the two computations insert corresponding remainders, and hence their current intermediate bases continue to correspond. If, moreover, every new nonzero homogeneous remainder has leading monomial not divisible by y, then specialization preserves its leading monomial and does not annihilate it. The newly generated S-pairs therefore correspond, and Buchberger's product criterion gives the same decision for them because relative primality of their leading monomials is preserved. Together with the assumed correspondence for the previously available S-pairs, this proves the last assertion. □

We now derive degree-wise consequences of Proposition 4.2.3. For $a \in K$ and for $d_0 \in \mathbb{Z}_{>0}$, let $\mathcal{G}_{\mathrm{early},(\mathrm{y}=\mathrm{a})}^{(<d_0)}$ (resp. $\mathcal{G}_{\mathrm{hom}}^{(<d_0)}$) denote the set of intermediate polynomials appearing in the early stage of the Gröbner basis computation for $\langle F^h|_{y=a}\rangle$ (resp. $\langle F^h\rangle$) up to step degree less than d_0. Supposing that the condition (B) in Section 4.1 holds for every degree $d < d_0$, any intermediate polynomial obtained up to step degree less than d_0 has no leading monomial divisible by y. Hence specialization at any $a \in K$, including $a = 0$, preserves all intermediate polynomials in the early stage. This yields the following degree-wise correspondence, where d_{inj} is defined as in (4.1.2):

Corollary 4.2.4. *Let d_0 be a positive integer satisfying Condition 4.1.2, equivalently $d_0 \leq d_{\mathrm{inj}}$, and let $a \in K$. Then, through all step degrees less than d_0, corresponding S-pairs can be selected in the computations for $\langle F^h\rangle$ and $\langle F^h|_{y=a}\rangle$. After a reduction sequence is chosen in either computation, a corresponding sequence can be constructed in the other as in Proposition 4.2.3. Moreover, for these choices, one has $\mathcal{G}_{\mathrm{early},(\mathrm{y}=\mathrm{a})}^{(<d_0)} = \{\, g^{(a)} : g \in \mathcal{G}_{\mathrm{hom}}^{(<d_0)} \,\}$ and $\mathrm{LM}_{\prec}(\mathcal{G}_{\mathrm{early},(\mathrm{y}=\mathrm{a})}^{(<d_0)}) = \mathrm{LM}_{\prec^h}(\mathcal{G}_{\mathrm{hom}}^{(<d_0)})$. After removing from the two sets of leading monomials above the nonminimal monomials contributed by the input generators, the resulting sets are both precisely $\{\mathrm{LM}_{\prec^h}(g) : g \in G_{\mathrm{hom}},\ \deg(g) < d_0\}$.*

Proof. By Lemma 4.1.1, condition (C) holds at every degree $d < d_0$. Starting with the input generators, we apply Proposition 4.2.3 successively to the S-pairs of step degree less than d_0. Its hypotheses hold initially, with the input indices retained when $a = 0$, and its last assertion shows that they remain valid after each step, because every new nonzero homogeneous remainder has leading monomial not divisible by y. Hence corresponding S-pairs and reduction sequences can be chosen through all step degrees less than d_0, and the intermediate polynomials correspond under specialization. Their degrees are also preserved, so no degree fall occurs in this range and the specialized polynomials belong to the early stage. Since all leading monomials involved are not divisible by y, specialization preserves them, which gives the equality of the sets of leading monomials. The last assertion follows from the observation on leading monomials of intermediate bases at the beginning of this section. □

Remark 4.2.5. The choices in Corollary 4.2.4 may also be made deterministically. Keep the input generators in their index order and order every later basis element by the time at which it is inserted. Among the S-pairs allowed by the normal selection strategy, choose the pair whose ordered pair of basis indices is lexicographically smallest; see [27] for the practical efficiency of such a strategy. In each reduction, eliminate the largest reducible term and, among the reducers whose leading monomial divides that term, use the first one in the current basis. Assign the same indices to corresponding polynomials under specialization.

With these choices, the two executions in Corollary 4.2.4 correspond until the first degree fall, after reductions that specialize to the identity at $y = 0$ are omitted. Indeed, leading monomials and insertion order are preserved. Moreover, since y is the smallest variable, a term not divisible by y precedes every term of the same total degree that is divisible by y. Thus the same nontrivial term and reducer are selected on both sides; any remaining reduction of a y-divisible term specializes to the identity. At step degree D, the same index order may be used together with the priority prescribed in Definition 4.4.2 below.

In particular, for $a = 0$ and $d_0 \leq d_{\mathrm{inj}}$, we have $\mathcal{G}_{\mathrm{top}}^{(<d_0)} = \mathcal{G}_{(y=0)}^{(<d_0)} = \mathcal{G}_{\mathrm{early},(y=0)}^{(<d_0)}$. We next turn to $a = 1$, where the threshold d_{inj} admits the following computational interpretation.

Corollary 4.2.6. *If $d_{\mathrm{inj}} < \infty$, then the first degree fall in the Buchberger-like computation for $\langle F \rangle$ occurs at step degree d_{inj}. If $d_{\mathrm{inj}} = \infty$, no degree fall occurs. Equivalently, for every positive integer d_0, Condition 4.1.2 with this d_0 holds if and only if no degree fall occurs at any step degree less than d_0 in the affine computation.*

Proof. By Corollary 4.2.4 and Lemma 4.1.1, no degree fall occurs at any step degree $d < d_{\mathrm{inj}}$. Suppose now that $d_{\mathrm{inj}} < \infty$. It also follows from the definition of d_{inj} and Lemma 4.1.1 that the condition (C) first fails at $d = d_{\mathrm{inj}}$. Otherwise condition (B) would hold for every $d < d_{\mathrm{inj}} + 1$, and the converse part of Lemma 4.1.1 would imply condition (A) at $d = d_{\mathrm{inj}}$, a contradiction.

Choose the first nonzero homogeneous remainder r at step degree d_{inj} with $y \mid \mathrm{LM}_{\prec^h}(r)$. All polynomials used before this remainder is produced have leading monomials not divisible by y, so Proposition 4.2.3 applies up to this point. Thus $r^{(1)}$ is the corresponding nonzero remainder in the computation for F. Since r is homogeneous and $y \mid \mathrm{LM}_{\prec^h}(r)$, one has $y \mid r$, whence $\deg(r^{(1)}) < d_{\mathrm{inj}}$ with $r^{(1)} \neq 0$. Hence a degree fall occurs at step degree d_{inj}.

If $d_{\mathrm{inj}} = \infty$, the first part applies at every finite step degree, as desired. □

Thus the injectivity condition gives the exact condition governing the absence of degree falls below a prescribed threshold.

4.3 Consequences at step degrees below $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$

We apply the correspondence principle established in Section 4.2 to analyze the Gröbner basis computations at step degrees below $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ *under the assumption that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular.* In these steps, no degree fall occurs and the injectivity condition holds, see Condition 4.1.2. We write $\mathcal{G}_{\mathrm{early}}^{(<D)}$ for the sets of intermediate polynomials obtained up to step degree $< D$ in the early stage of $\langle F \rangle$, and also write $\mathcal{G}_{\mathrm{hom}}^{(<D)}$ and $\mathcal{G}_{\mathrm{top}}^{(<D)}$ for the sets of intermediate polynomials obtained up to step degree $< D$ in the computations $\langle F^h \rangle$ and $\langle F^{\mathrm{top}} \rangle$, respectively. When $D = \infty$, the superscript $(< D)$ refers to all intermediate polynomials occurring in the corresponding computation.

Corollary 4.3.1. *Assume that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, and let $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$. If $D < \infty$, then, before the step degree first reaches D, corresponding S-pairs and reduction sequences can be chosen in the three computations for $\langle F^h \rangle$, $\langle F \rangle$, and $\langle F^{\mathrm{top}} \rangle$ so that they correspond under*

specialization, after trivial reductions at $y = 0$ are omitted. If $D = \infty$, the same conclusion holds through every finite step degree. At each step in this range, every polynomial used for forming S-pairs or as a reducer has leading monomial not divisible by y. Moreover, for these choices, one has $\mathcal{G}_{\mathrm{early}}^{(<D)} = (\mathcal{G}_{\mathrm{hom}}^{(<D)})|_{y=1}$, $\mathcal{G}_{\mathrm{top}}^{(<D)} = (\mathcal{G}_{\mathrm{hom}}^{(<D)})|_{y=0}$, and $\mathrm{LM}_{\prec}(\mathcal{G}_{\mathrm{early}}^{(<D)}) = \mathrm{LM}_{\prec^h}(\mathcal{G}_{\mathrm{hom}}^{(<D)}) = \mathrm{LM}_{\prec}(\mathcal{G}_{\mathrm{top}}^{(<D)})$.

Proof. The cryptographic semi-regularity of $\boldsymbol{F}^{\mathrm{top}}$ implies that Condition 4.1.2 holds in every degree $d < D$. If $D < \infty$, Corollary 4.2.4 applies with $d_0 = D$. If $D = \infty$, it applies with every finite positive integer d_0. Thus the stated choices and the correspondence of intermediate polynomials follow. □

Thus, throughout the range specified in Corollary 4.3.1, the affine computation and the computation for F^{top} are obtained from the homogeneous computation by specialization at $y = 1$ and $y = 0$, respectively.

Proposition 4.3.2. *With notation as above, $(G_{\mathrm{top}})_{<D} = (G_{\mathrm{hom}})_{<D}\big|_{y=0}$.*

Proof. Since $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, the condition (C) of Section 4.1 holds for each step degree $d < D$. Hence every element of $\mathcal{G}_{\mathrm{hom}}^{(<D)}$ is homogeneous and has leading monomial not divisible by y. It also follows from Corollary 4.3.1 that $\mathcal{G}_{\mathrm{top}}^{(<D)} = (\mathcal{G}_{\mathrm{hom}}^{(<D)})|_{y=0}$. If $D < \infty$, all S-pairs of step degree less than D have been processed; if $D = \infty$, the computations have terminated. Therefore, the inter-reductions of $\mathcal{G}_{\mathrm{hom}}^{(<D)}$ and $\mathcal{G}_{\mathrm{top}}^{(<D)}$ give $(G_{\mathrm{hom}})_{<D}$ and $(G_{\mathrm{top}})_{<D}$, respectively. Let $g \in \mathcal{G}_{\mathrm{hom}}^{(<D)}$, and consider a reduction sequence of g by $\mathcal{G}_{\mathrm{hom}}^{(<D)} \setminus \{g\}$. By the same argument as in the proof of Proposition 4.2.3 (using the corresponding reduction sequences under specialization), we obtain the corresponding reduction sequence of $g|_{y=0}$ by $\mathcal{G}_{\mathrm{top}}^{(<D)} \setminus \{g|_{y=0}\}$. Hence the remainder of g by $\mathcal{G}_{\mathrm{hom}}^{(<D)} \setminus \{g\}$ is specialized to the remainder of $g|_{y=0}$ by $\mathcal{G}_{\mathrm{top}}^{(<D)} \setminus \{g|_{y=0}\}$. Applying this argument to all elements, we conclude that the inter-reduction of $\mathcal{G}_{\mathrm{hom}}^{(<D)}$ is specialized to that of $\mathcal{G}_{\mathrm{top}}^{(<D)}$, so that $(G_{\mathrm{top}})_{<D} = (G_{\mathrm{hom}})_{<D}\big|_{y=0}$. □

Remark 4.3.3. The above argument shows that the correspondence between the computations of $\langle F^h \rangle$ and $\langle F^{\mathrm{top}} \rangle$ up to degree less than D depends only on the injectivity condition (Condition 4.1.2). In particular, the equality $\mathrm{LM}_{\prec^h}(\mathcal{G}_{\mathrm{hom}}^{(<D)}) = \mathrm{LM}_{\prec}(\mathcal{G}_{\mathrm{top}}^{(<D)})$ implies $\mathrm{LM}_{\prec^h}(G_{\mathrm{hom}})_{<D} = \mathrm{LM}_{\prec}(G_{\mathrm{top}})_{<D}$. This yields an alternative computation-theoretic proof of [39, Lemma 2], based on tracking the computation process. In contrast to the original proof in [39], which relies on Hilbert function arguments and semi-regularity, the above proof requires only Condition 4.1.2 with $d_0 = D$.

4.4 Synchronization among Gröbner basis computations at step degree D

Throughout this subsection, we assume that $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) < \infty$ and that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular. At the first stage at which the step degree reaches D, degree falls may occur, so Proposition 4.2.3 no longer ensures that an entire affine reduction sequence corresponds to a homogeneous one. We therefore begin with the affine computation and introduce below the choices of S-pairs and reducers used in this subsection. We will show that an initial part of each affine reduction lifts to the homogeneous computation. We denote by $\mathcal{G}_{\mathrm{hom}}^{(D)}$ the set of intermediate polynomials obtained at step degree D in the homogeneous computation.

First we recall the *sugar strategy*, which is an extension of the normal selection strategy devised for improving the practicality of the computation, and *redefine* the step degree by using the *sugar degree*. This change does not affect $\mathcal{G}_{\mathrm{early}}^{(<D)}$, see Remark 4.4.3 below. By this definition, the

(redefined) step degrees form a nondecreasing sequence throughout the computation of $\langle F \rangle$, as in the homogeneous computation of $\langle F^h \rangle$.

Definition 4.4.1 (Sugar strategy [27])**.** For each polynomial g appearing as an *intermediate polynomial* in the computation of $\mathcal{G}$, its *sugar degree*, denoted by $\mathrm{sdeg}(g)$ here, is defined in a recursive manner as follows:

(1) For each f_i, we set $\mathrm{sdeg}(f_i) = \deg(f_i)$.

(2) For a polynomial g, a monomial t, and a non-zero constant c, we set $\mathrm{sdeg}(ctg) = \mathrm{sdeg}(g) + \deg(t)$.

(3) For polynomials g and h, we set $\mathrm{sdeg}(g+h) = \max\{\mathrm{sdeg}(g), \mathrm{sdeg}(h)\}$.

Thus, for each one-step reduction $r \underset{h}{\longrightarrow} r' = r - cth$, where $c \in K^\times$ and t is a monomial, we have $\mathrm{sdeg}(r') = \max\{\mathrm{sdeg}(r), \mathrm{sdeg}(h) + \deg(t)\}$. For each S-pair (g_1, g_2) appearing in the computation of $\mathcal{G}$, we define its sugar degree by $\mathrm{sdeg}(S(g_1, g_2))$, namely $\max\{\mathrm{sdeg}(t_1 g_1), \mathrm{sdeg}(t_2 g_2)\}$, where $S(g_1, g_2) = t_1 g_1 - t_2 g_2$ with $t_i = \mathrm{lcm}(\mathrm{LM}_\prec(g_1), \mathrm{LM}_\prec(g_2))/\mathrm{LT}_\prec(g_i)$. The *sugar strategy* selects S-pairs in order of lowest sugar degree, where the tie-breaking is done by the normal selection strategy. A "sugar degree" can be considered as a "phantom degree", where each polynomial g in R with sugar degree s may be associated to a homogeneous polynomial in R' with degree s.

We use the sugar strategy for the affine computation throughout this subsection. We denote by $\mathcal{G}^{(<D)}$ and $\mathcal{G}^{(D)}$ the sets of intermediate polynomials obtained while S-pairs of sugar degree less than D and equal to D are processed, respectively. We denote by $\mathcal{G}_{\mathrm{hom}}^{(D)}$ the set of intermediate polynomials obtained at step degree D in the homogeneous computation. Remark 4.4.3 below shows that $\mathcal{G}^{(<D)} = \mathcal{G}_{\mathrm{early}}^{(<D)}$.

The following definition specifies the intermediate polynomial retained for use in later reductions. This convention is related to the *saccharine strategy* introduced in [27] in the context of the *double sugar strategy*, in which every reduction preserves the sugar degree.

Definition 4.4.2. For each S-polynomial $S(g_1, g_2)$, by prioritizing reducers which do not change the sugar degree as far as possible, the following reduction sequence is computed:

$$S(g_1, g_2) = r_0 \underset{h_0}{\longrightarrow} r_1 \underset{h_1}{\longrightarrow} \cdots \underset{h_{k-1}}{\longrightarrow} r_k \underset{h_k}{\longrightarrow} r_{k+1} \longrightarrow \cdots \longrightarrow r_\ell, \tag{4.4.1}$$

where $\mathrm{sdeg}(r_0) = \cdots = \mathrm{sdeg}(r_k)$, and, if $k < \ell$, $\mathrm{sdeg}(r_k) < \mathrm{sdeg}(r_{k+1})$. Note that r_ℓ is the computed remainder by the *current* basis $\mathcal{G}^{(\prec \boldsymbol{s})} := \mathcal{G}_{(y=1)}^{(\prec \boldsymbol{s})}$ with $\boldsymbol{s} = (g_1, g_2)$. Then, we define $r_{\mathrm{sgr}}(g_1, g_2)$ by r_k and $r_{\mathrm{fin}}(g_1, g_2)$ by r_ℓ. Of course, the sequence (4.4.1) may stop at k, that is, $r_{\mathrm{fin}}(g_1, g_2) = r_{\mathrm{sgr}}(g_1, g_2)$. We may apply the double sugar strategy, where we always stop the reduction at $r_{\mathrm{sgr}}(g_1, g_2)$.

After the reduction of the selected S-polynomial has been completed, each nonzero $r_{\mathrm{sgr}}(g_1, g_2)$ is retained in the current basis, as is the nonzero final remainder if it is different from $r_{\mathrm{sgr}}(g_1, g_2)$. The corresponding new S-pairs are generated before the next S-pair is selected. This rule is used only while S-pairs of sugar degree D are processed. After all such pairs have been processed, the computation continues from the current basis, and no $r_{\mathrm{sgr}}(g_1, g_2)$ distinct from the final remainder is retained.

Using this choice of reducers, we now show that, for each affine S-pair selected at sugar degree D, the reduction steps from its S-polynomial to $r_{\mathrm{sgr}}(g_1, g_2)$ lift to homogeneous reduction steps.

Remark 4.4.3. For any $g \in \mathcal{G}_{\mathrm{early}}^{(<D)}$, it can be shown inductively that $\mathrm{sdeg}(g) = \deg(g)$ holds by using the correspondence between $\mathcal{G}_{\mathrm{early}}^{(<D)}$ and $\mathcal{G}_{\mathrm{hom}}^{(<D)}$. Indeed, each $g \in \mathcal{G}_{\mathrm{early}}^{(<D)}$ is not a degree fall element and its counterpart $g^h \in \mathcal{G}_{\mathrm{hom}}^{(<D)}$ is not divisible by y, see Proposition 4.2.3. Thus, for each

S-pair at step degree less than D, its sugar degree coincides with its degree. Consequently, before the step degree first reaches D, the sugar strategy makes the same choices of S-pairs as the normal selection strategy, and every reduction preserves the sugar degree. In particular, $r_{\mathrm{sgr}} = r_{\mathrm{fin}}$ at such step degrees. Also, for our *revised* step degree, $\mathcal{G}_{\mathrm{early}}^{(<D)} = \mathcal{G}^{(<D)}$ holds. Moreover, Lemma 4.4.5 shows that every S-pair of sugar degree D has S-pair degree D.

Remark 4.4.4. The preceding reduction convention is particularly simple for signature-based algorithms [20], including F_5-type algorithms. For a Schreyer ordering (see [29, p. 161]) satisfying $t_i \boldsymbol{e}_i \prec t_j \boldsymbol{e}_j$ whenever $\deg(t_i f_i) < \deg(t_j f_j)$, where each basis element $\boldsymbol{e}_i$ of a free R-module of rank m corresponds to f_i, the sugar degree agrees with the total degree of the signature, and any one-step reduction does not change such degree. Hence $r_{\mathrm{fin}}(g_1, g_2)$ always coincides with $r_{\mathrm{sgr}}(g_1, g_2)$.

Now we consider the process of the Gröbner basis computation for F at step degree D with the sugar strategy. In this process, a pair (g_1, g_2) is chosen such that g_1 and g_2 are already computed *intermediate polynomials* and $\mathrm{sdeg}(S(g_1, g_2)) = D$. Writing $S(g_1, g_2) = c_1 t_1 g_1 - c_2 t_2 g_2$ for some monomials t_1, t_2 and non-zero constants c_1, c_2, we have $\max\{\mathrm{sdeg}(t_1 g_1), \mathrm{sdeg}(t_2 g_2)\} = D$. Here $\mathrm{sdeg}(g_i) \leq D$ for $i = 1, 2$; otherwise $\max\{\mathrm{sdeg}(t_1 g_1), \mathrm{sdeg}(t_2 g_2)\} > D$. Put $F_D := \{f_i \in F \mid \deg(f_i) = D\}$.

Lemma 4.4.5. *For each S-pair (g_1, g_2) of sugar degree D, we have $\mathrm{sdeg}(g_i) = \deg(g_i) < D$ or $g_i \in F_D$ for $i = 1, 2$, so that the degree of (g_1, g_2) is also D.*

Proof. Without loss of generality, we may assume $\mathrm{sdeg}(g_1) \geq \mathrm{sdeg}(g_2)$. If $\mathrm{sdeg}(g_1) < D$, then $\mathrm{sdeg}(g_2) < D$ and $\mathrm{sdeg}(g_i) = \deg(g_i)$ by Remark 4.4.3. Suppose, to the contrary, that $\mathrm{sdeg}(g_1) = D$ holds for some $g_1 \notin F$. (In this case, $t_1 = 1$ and g_1 is computed from some S-polynomial.) If $\mathrm{sdeg}(g_2) < D$, then g_2 should belong to $\mathcal{G}_{\mathrm{early}}^{(<D)}$ and is computed before g_1. Otherwise, that is, $\mathrm{sdeg}(g_2) = D$, we may set the pair (g_1, g_2) so that g_2 is computed before g_1. (We note that all polynomials of degree D in F are always computed before g_1.) In either case, we may assume that g_2 is computed before g_1. Then g_1 is reducible by g_2, and a one-step reduction gives a nonzero scalar multiple of $S(g_1, g_2)$, still of sugar degree D. Since g_2 had already been computed when g_1 was obtained, this is impossible: r_{fin} is reduced, while r_{sgr} admits no further reduction preserving the sugar degree. □

Conversely, if the degree of S-pair (g_1, g_2) with $g_i \in \mathcal{G}^{(<D)} \cup F_D$ is D, then clearly the sugar degree of (g_1, g_2) is also D.

Therefore, it follows from Lemma 4.4.5 that

$$\begin{aligned}\mathsf{Spairs}_D :=& \{(g_1, g_2) \mid \mathrm{sdeg}(S(g_1, g_2)) = D,\ g_1, g_2 \in \mathcal{G}^{(<D)} \cup F_D\} \\ =& \{(g_1, g_2) \mid \text{the degree of } (g_1, g_2) \text{ is } D,\ g_1, g_2 \in \mathcal{G}^{(<D)} \cup F_D\}.\end{aligned}$$

By Corollary 4.3.1, we have $(\mathcal{G}^{(<D)})^h = \mathcal{G}_{\mathrm{hom}}^{(<D)}$, and hence

$$\begin{aligned}\mathsf{Spairs}_D^h :=& \{(g_1^h, g_2^h) \mid (g_1, g_2) \in \mathsf{Spairs}_D\} \\ =& \{(g_1', g_2') \mid \deg(S(g_1', g_2')) = D,\ g_1', g_2' \in \mathcal{G}_{\mathrm{hom}}^{(<D)} \cup F_D^h\}.\end{aligned}$$

When a pair $\boldsymbol{s} = (g_1, g_2) \in \mathsf{Spairs}_D$ is selected in the affine computation, we process the corresponding pair $\boldsymbol{s}^h := (g_1^h, g_2^h) \in \mathsf{Spairs}_D^h$ in the homogeneous computation.

Remark 4.4.6. In the computation of $\mathcal{G}_{\mathrm{hom}}$, for each S-pair (g_1', g_2') chosen at the step degree D, we have $\deg(g_i') < D$ or $g_i' \in F_D^h$ for $i = 1, 2$. This can be shown in the same manner as Lemma 4.4.5.

Lemma 4.4.7. *With notation as above, we have the following:*

(1) For $i < k$, to each one-step reduction

$$r_i \xrightarrow[h_i]{} r_{i+1} := r_i - c_i t_i h_i \tag{4.4.2}$$

in the sequence (4.4.1), where $c_i \in K^\times$ and t_i is a monomial in R, the following one-step reduction corresponds:

$$r_i^* \xrightarrow[h_i^*]{} r_{i+1}^* = r_i^* - c_i t_i h_i^* y^{\delta_i}, \tag{4.4.3}$$

where $r_i^* = y^{a_i} r_i^h$ for $a_i = D - \deg(r_i)$, $r_{i+1}^* = y^{a_{i+1}} r_{i+1}^h$ for $a_{i+1} = D - \deg(r_{i+1})$, $h_i^* = y^{b_i} h_i^h$ for $b_i = \operatorname{sdeg}(h_i) - \deg(h_i)$ and $\delta_i = D - \deg(t_i) - \operatorname{sdeg}(h_i)$. Note that, as the reduction (4.4.2) does not change the sugar degree for $i < k$, we have $\delta_i = D - \deg(t_i) - \operatorname{sdeg}(h_i) \geq 0$.

(2) The part of the affine reduction sequence (4.4.1) from $S(g_1, g_2)$ to $r_k = r_{\mathrm{sgr}}(g_1, g_2)$ lifts to the homogeneous reduction sequence

$$S(g_1^h, g_2^h) = r_0^* \xrightarrow[h_0^*]{} r_1^* \xrightarrow[h_1^*]{} \cdots \xrightarrow[h_{k-1}^*]{} r_k^*.$$

Then $r_k^* = r_{\mathrm{sgr}}(g_1, g_2)^*$ is the computed remainder by the current *basis $\mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s}^h)}$, where $\boldsymbol{s} = (g_1, g_2)$. In particular, $h_0^*, \ldots, h_{k-1}^*$ belong to $\mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s}^h)}$.*

Therefore, together with the obvious correspondence $f_i^h \leftrightarrow f_i$ for $f_i \in F_D$, (1) and (2) give a one-to-one correspondence between $\mathcal{G}_{\mathrm{hom}}^{(D)}$ and $\widehat{\mathcal{G}}^{(D)} := \{g \in \mathcal{G}^{(D)} : \operatorname{sdeg}(g) = D\}$, the set of all intermediate polynomials in $\mathcal{G}^{(D)}$ with sugar degree D.

Proof. (1) First we consider r_i^h and $c_i t_i h_i^h$, which are the homogenizations of r_i and $c_i t_i h_i$, respectively. Then, by adjusting the degrees by powers of y, we have $r_{i+1}^h y^{\epsilon_i} = r_i^h - c_i t_i y^{\deg(r_i) - \deg(t_i) - \deg(h_i)} h_i^h$ for $\epsilon_i = \deg(r_i) - \deg(r_{i+1})$. Multiplying both sides by $y^{D - \deg(r_i)}$, we have

$$\begin{aligned} r_{i+1}^* (= y^{D-\deg(r_{i+1})} r_{i+1}^h) &= y^{D-\deg(r_i)+\epsilon_i} r_{i+1}^h \\ &= r_i^* - c_i t_i h_i^h y^{D-\deg(t_i)-\deg(h_i)} \\ &= r_i^* - c_i t_i h_i^* y^{D-\deg(t_i)-\deg(h_i)-(\operatorname{sdeg}(h_i)-\deg(h_i))} \\ &= r_i^* - c_i t_i h_i^* y^{D-\deg(t_i)-\operatorname{sdeg}(h_i)}. \end{aligned}$$

The one-step reduction (4.4.2) eliminates the term $c_i t_i \operatorname{LT}_\prec(h_i)$ of r_i, and r_i^* has a term $c_i t_i \operatorname{LT}_\prec(h_i) y^{D-\deg(t_i)-\deg(h_i)}$. As $\operatorname{LT}_{\prec^h}(h_i^*) = \operatorname{LT}_\prec(h_i) y^{\operatorname{sdeg}(h_i)-\deg(h_i)}$, we have $c_i t_i \operatorname{LT}_\prec(h_i) y^{D-\deg(t_i)-\deg(h_i)} = c_i t_i \operatorname{LT}_\prec(h_i^*) y^{D-\deg(t_i)-\operatorname{sdeg}(h_i)}$. This implies that (4.4.3) gives a one-step reduction of r_i^* by h_i^*, as desired.

(2) We prove the assertion by induction on the selection order in Spairs_D. First we show that every h_i^* belongs to $\mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s}^h)}$.

If $\operatorname{sdeg}(h_i) < D$, then h_i belongs to $\mathcal{G}^{(<D)}$ $(= \mathcal{G}_{\mathrm{early}}^{(<D)})$. By the correspondence between $\mathcal{G}^{(<D)}$ and $\mathcal{G}_{\mathrm{hom}}^{(<D)}$, we have $\operatorname{sdeg}(h_i) = \deg(h_i)$ and $h_i^* = h_i^h \in \mathcal{G}_{\mathrm{hom}}^{(<D)} \subset \mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s}^h)}$ (see Remark 4.4.3).

If $\operatorname{sdeg}(h_i) = D$, then h_i belongs to F, or we can write $h_i = r_{\mathrm{sgr}}(g_3, g_4)$, which is obtained from $S(g_3, g_4)$ for some (g_3, g_4) selected beforehand from Spairs_D. If $h_i \in F$, it is obvious that $h_i^* = h_i^h \in \mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s}^h)}$. Thus, suppose that h_i is obtained from $S(g_3, g_4)$. Since the lemma holds for $S(g_3, g_4)$ by the induction hypothesis, the affine reduction sequence from $S(g_3, g_4)$ to $h_i = r_{\mathrm{sgr}}(g_3, g_4)$ lifts to the corresponding homogeneous reduction sequence ending in h_i^*. Thus, h_i^* belongs to $\mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s}^h)}$.

Next we show that the reduction sequence from $S(g_1^h, g_2^h)$ stops at r_k^*. Assume, to the contrary, that r_k^* is reduced to $\hat{r}$ by some element $\hat{h}$ in $\mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s}^h)}$. That is, we have a one-step reduction

$$\hat{r} = r_k^* - ct\hat{h} \tag{4.4.4}$$

for some monomial $t \in R'$ and $c \in K^\times$ and $\deg(t)+\deg(\hat{h}) = \deg(r_k^*) = D$. Then the specialization of (4.4.4) gives the following one-step reduction:

$$\hat{r}^{(1)} = r_k - ct^{(1)}\hat{h}^{(1)}. \tag{4.4.5}$$

As $\hat{h}$ belongs to $\mathcal{G}_{\mathrm{hom}}^{(\prec \boldsymbol{s}^h)}$, the polynomial $\hat{h}^{(1)}$ belongs to $\mathcal{G}^{(<D)} \cup \widehat{\mathcal{G}}^{(D)}$ and $\mathrm{sdeg}(\hat{h}^{(1)}) = \deg(\hat{h})$ by the correspondence between $\mathcal{G}_{\mathrm{early}}^{(<D)}$ and $\mathcal{G}_{\mathrm{hom}}^{(<D)}$ and by the induction argument on the correspondence between $\widehat{\mathcal{G}}^{(D)}$ and $\mathcal{G}_{\mathrm{hom}}^{(D)}$. Then,

$$\mathrm{sdeg}(ct^{(1)}\hat{h}^{(1)}) = \deg(t^{(1)}) + \mathrm{sdeg}(\hat{h}^{(1)}) \le \deg(t) + \deg(\hat{h}) = D,$$

which implies that the reduction (4.4.5) keeps the sugar degree D. This contradicts the definition of $r_k = r_{\mathrm{sgr}}(g_1, g_2)$. □

Consequence at (redefined) step degree D As a natural consequence of the correspondence in Lemma 4.4.7, we have the following lemma.

Lemma 4.4.8. *The monomial ideal $\langle \mathrm{LM}_\prec(\mathcal{G}^{(\le D)})\rangle$ contains all monomials of R of degree at least D, where $\mathcal{G}^{(\le D)} := \mathcal{G}^{(<D)} \cup \mathcal{G}^{(D)}$.*

Proof. It suffices to show that every monomial in R_D belongs to $\langle \mathrm{LM}_\prec(\mathcal{G}^{(\le D)})\rangle$. Let t be a monomial in R_D. Then, it follows from [39, Lemma 3] that $\langle \mathrm{LM}_{\prec^h}((G_{\mathrm{hom}})_{\le D})\rangle_{R'} \cap R_D = R_D$, whence $t' \mid t$ for some monomial $t' \in \mathrm{LM}_{\prec^h}((G_{\mathrm{hom}})_{\le D})$. If $\deg(t') < D$, the monomial t' belongs to $\mathrm{LM}_{\prec^h}((G_{\mathrm{hom}})_{<D})$, where $\mathrm{LM}_{\prec^h}((G_{\mathrm{hom}})_{<D}) \subset \mathrm{LM}_{\prec^h}(\mathcal{G}_{\mathrm{hom}}^{(<D)}) = \mathrm{LM}_\prec(\mathcal{G}^{(<D)})$ by Corollary 4.3.1. Otherwise, namely if $\deg(t') = D$, then $t = t' \in \mathrm{LM}_{\prec^h}(G_{\mathrm{hom}})_D \subset \mathrm{LM}_{\prec^h}(\mathcal{G}_{\mathrm{hom}}^{(D)})$.

It remains to show $\mathrm{LM}_{\prec^h}(\mathcal{G}_{\mathrm{hom}}^{(D)}) \cap R_D \subset \langle \mathrm{LM}_\prec(\mathcal{G}^{(\le D)})\rangle$. Let $q \in \mathcal{G}_{\mathrm{hom}}^{(D)}$ satisfy $\mathrm{LM}_{\prec^h}(q) \in R_D$. If $q \in F_D^h$, then $q = f_i^h$ for some $f_i \in F_D$. Since $\mathrm{LM}_{\prec^h}(f_i^h) = \mathrm{LM}_\prec(f_i)$ and $f_i \in \mathcal{G}^{(D)}$, the assertion follows. Otherwise, by Lemma 4.4.7, we have $q = r_{\mathrm{sgr}}(g_1, g_2)^*$ for some $(g_1, g_2) \in \mathsf{Spairs}_D$. Since

$$r_{\mathrm{sgr}}(g_1, g_2)^* = y^{D-\deg(r_{\mathrm{sgr}}(g_1,g_2))} r_{\mathrm{sgr}}(g_1, g_2)^h$$

and $\mathrm{LM}_{\prec^h}(q)$ is not divisible by y, we must have $\deg(r_{\mathrm{sgr}}(g_1, g_2)) = D$. Hence $q = r_{\mathrm{sgr}}(g_1, g_2)^h$ and $\mathrm{LM}_{\prec^h}(q) = \mathrm{LM}_\prec(r_{\mathrm{sgr}}(g_1, g_2))$, where $r_{\mathrm{sgr}}(g_1, g_2) \in \mathcal{G}^{(D)}$. This proves the desired inclusion. □

Remark 4.4.9. The construction above is not tied to the degree of regularity. More generally, let T be a positive integer such that Condition 4.1.2 holds in every degree $d < T$. Suppose that, when the sugar degree first reaches T, the reduction convention of Definition 4.4.2 is used while the S-pairs of sugar degree T are processed. Then the proofs of Lemmas 4.4.5 and 4.4.7 remain valid with T in place of D. Indeed, below T no degree fall occurs, so the sugar degree agrees with the ordinary degree, the sugar strategy selects the same pairs as the normal selection strategy, and every reduction preserves the sugar degree. After all S-pairs of sugar degree T have been processed, the computation may be continued by Buchberger's algorithm, with only final remainders inserted into the current basis.

In particular, if $d_{\mathrm{inj}} < \infty$, one may take $T = d_{\mathrm{inj}}$. If $d_{\mathrm{inj}} = \infty$, the preceding agreement holds at every finite step degree and no additional reduction convention is needed. If, moreover, $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, then $D \le d_{\mathrm{inj}}$ and $\mathcal{G}^{(\le D)} \subseteq \mathcal{G}^{(\le d_{\mathrm{inj}})}$. Here $\mathcal{G}^{(\le T)}$ refers to the computation in which the convention of Definition 4.4.2 is applied while S-pairs of sugar degree T are processed. Consequently, Lemma 4.4.8 implies that $\langle \mathrm{LM}_\prec(\mathcal{G}^{(\le d_{\mathrm{inj}})})\rangle$ contains every monomial of R of degree at least d_{inj}.

Solving degree of F as the highest S-pair degree Finally, Lemma 4.4.8 allows us to apply the bound of [39, Lemma 4] on the highest S-pair degree (equivalently, the highest original step degree) directly to the present computation, without restarting it.

Lemma 4.4.10 (cf. [39, Lemma 4])**.** *With notation as above, assume that $D \geq \max\{\deg(f) : f \in F\}$ and that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular. Let $\mathcal{A}$ be a Buchberger-like algorithm satisfying the computational setting above, including Buchberger's product criterion, the sugar strategy, and the reduction convention of Definition 4.4.2. Then $\mathrm{sd}_{\prec}^{\mathcal{A}}(F) \leq 2D-1$. If the sugar strategy is stopped after sugar degree D and $\mathcal{G}^{(\leq D)}$ is inter-reduced before the computation is continued, then the solving degree in the strict sense is at most $2D-2$.*

Proof. After all S-pairs of sugar degree D have been processed, Lemma 4.4.8 shows that the current set $H := \mathcal{G}^{(\leq D)}$ satisfies $\langle \mathrm{LM}_{\prec}(H)\rangle_D = R_D$. This is precisely the property used in the proof of [39, Lemma 4]. Hence that proof applies to the present computation without restarting it and yields $\mathrm{sd}_{\prec}^{\mathcal{A}}(F) \leq 2D-1$. After the stated inter-reduction of H, the second part of the same argument gives the strict bound $2D-2$. □

Acknowledgement

Many of the contents of this paper were 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 26K06753, JSPS Grant-in-Aid for Scientific Research (B) 25K00140, and JST CREST Grant Number JPMJCR2113, and JST K Program Grant Number JPMJKP24U2, Japan.

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. Faugère, 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. Faugère, and B. Salvy: On the complexity of the F_5 Gröbner basis algorithm. J. Symb. Comp., **70**, 49–70, 2015.

[4] M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. Yang: Asymptotic behavior 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.

[5] D. Bayer and M. Stillman: A criterion for detecting m-regularity. Invent. Math., **87** (1), 1–11, 1987.

[6] 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.

[7] W. Bosma, J. Cannon, and C. Playoust: The Magma algebra system I: The user language. J. Symb. Comp., **24**(3-4), 235–265, 1997.

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

[9] 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.

[10] 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; corrected version available as arXiv:1706.06319v7.

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

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

[13] 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.

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

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

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

[17] C. Diem: The XL-algorithm and a Conjecture from Commutative Algebra. Asiacrypt'04, LNCS, **3329**, pp. 323–337, 2004.

[18] 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, 2013.

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

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

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

[22] 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.

[23] 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.

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

[25] 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.

[26] G. Gaggero and E. Gorla: The complexity of solving a system of equations of the same degree. arxiv:2309.03855v4, 2026.

[27] A. Giovini, T. Mora, G. Niesi, L. Robbiano, and C. Traverso: "One sugar cube, please" or selection strategies in the Buchberger algorithm. ISSAC '91: Proceedings of the 1991 international symposium on Symbolic and algebraic computation, pp. 49–54, ACM Press, 1991.

[28] 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.

[29] G.-M. Greuel and G. Pfister: A Singular Introduction to Commutative Algebra. 2nd Edition, Springer, 2007.

[30] A. Hashemi: Efficient computation of Castelnuovo–Mumford regularity. Mathematics of Computation, **81**, 1163–1177, 2012.

[31] A. Hashemi: Strong Noether Position and Stabilized Regularities. Communications in Algebra, **38**, 515–533, 2010.

[32] A. Hashemi and W. M. Seiler: Dimension and depth dependent upper bounds in polynomial ideal theory. J. Symb. Comp., **98**, 47–64, 2020.

[33] A. Hashemi, M. Schweinfurter, and W. M. Seiler: Deterministic genericity for polynomial ideals. J. Symb. Comp., **86**, 20–50, 2018.

[34] 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.

[35] 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.

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

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

[38] M. Kudo and K. Yokoyama: Generalization of semi-regular sequences: Maximal Gröbner basis degree, variants of genericness, and related conjectures. arXiv:2410.23211v2, 2025.

[39] 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 40, 205–231, Springer, Singapore, 2026.

[40] 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.

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

[42] G. McGuire and D. O'Hara: On the termination of the general XL algorithm and ordinary multinomials. J. Symb. Comp., **104**, 90–104, 2021.

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

[44] J. Migliore and R. Mirò-Roig: On the minimal free resolution of n+1 general forms, Transactions of the American Mathematical Society, **355**, 1–36, 2003.

[45] 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.

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

[47] Risa/Asir developing team: Risa/asir — A computer algebra system for polynomial computations, 2026. https://www.math.kobe-u.ac.jp/Asir

[48] F. Salizzoni: An upper bound for the solving degree in terms of the degree of regularity. Transactions on Mathematical Cryptology, **5**(1), 1–7, 2025.

[49] 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.

[50] 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

Appendix A Examples for Section 4

We use the same notation as in Section 4. We give two examples illustrating the results of that section. The first revisits [39, Example 1] and illustrates the correspondence among the three Gröbner basis computations in the cryptographic semi-regular case, including the behavior at step degree D. The second shows that Condition 4.1.2 with $d_0 = D$ may hold even when $\boldsymbol{F}^{\mathrm{top}}$ is not cryptographic semi-regular.

The reduced Gröbner bases in the first example were computed with Risa/Asir [47]. For the affine computation below, we also give a direct Buchberger computation in order to make the intermediate steps explicit.

A.1 A cryptographic semi-regular example

Let $p = 73$, $K = \mathbb{F}_p$, and

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

with $n = 3$ and $m = 4$. Then, $d_1 = d_2 = d_3 = d_4 = 2$. The highest-degree homogeneous parts are

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

One verifies that $\boldsymbol{F}^{\mathrm{top}}$ is semi-regular, and hence cryptographic semi-regular. Moreover, $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle) = 3$. For ease of comparison with the stepwise computation below, we list the elements of the Gröbner bases in increasing order of total degree. Indeed, the reduced Gröbner basis G_{top} of the ideal $\langle F^{\mathrm{top}}\rangle$ with respect to the DRL ordering $x_1 \succ x_2 \succ x_3$ is

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

Therefore, we have $\mathrm{LM}_{\prec}(G_{\mathrm{top}}) = \{x_1^2, x_1x_2, x_2^2, x_1x_3, x_2x_3^2, x_3^3\}$, from which the Hilbert-Poincaré series of $R/\langle F^{\mathrm{top}}\rangle$ is computed as

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

whence $D = 3$.

On the other hand, the reduced Gröbner basis G_{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

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

and thus

$$\mathrm{LM}_{\prec^h}(G_{\mathrm{hom}}) = \{x_1^2, x_1x_2, x_2^2, x_1x_3, x_2x_3^2, x_3^3, x_2x_3y, x_3^2y, x_1y^3, x_2y^3, x_3y^3\}.$$

Then the Hilbert-Poincaré series of $R'/\langle F^h\rangle$ satisfies

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

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* $\mathrm{LM}_{\prec^h}(G_{\mathrm{hom}})_{<D} = \mathrm{LM}_{\prec}(G_{\mathrm{top}})_{<D}$. Moreover, no element of $\mathrm{LM}_{\prec^h}(G_{\mathrm{hom}})$ of degree less than D is divisible by y. Thus Condition 4.1.2 holds with $d_0 = D$, and Corollary 4.2.6 shows that no degree fall occurs at any step degree less than D.

We next examine the affine computation more closely, step degree by step degree. As in Section 4.4, we use the sugar degree as the step degree in the following computation. No interreduction is performed during the computation.

Step degree 2 Since $\mathrm{LM}_{\prec}(f_i) = x_1^2$ for $1 \le i \le 4$, all six S-pairs among the input generators have sugar degree 2. In the direct Buchberger computation considered here, these pairs are processed at step degree 2. Put $g_1 := f_1$. In the execution considered here, the pairs (f_1, f_2), (f_1, f_3), and (f_1, f_4) are processed first, and their monic nonzero remainders are, respectively,

$$\begin{aligned}
g_2 &= \underline{x_1x_2} + 41x_2^2 + 23x_1x_3 + 64x_2x_3 + 49x_3^2 + 16x_1 + 56x_2 + 57x_3,\\
g_3 &= \underline{x_2^2} + 14x_1x_3 + 43x_2x_3 + 22x_3^2 + 29x_3,\\
g_4 &= \underline{x_1x_3} + 3x_2x_3 + 33x_3^2 + 22x_1 + 5x_2 + 14x_3.
\end{aligned}$$

The remaining three S-pairs among f_2, f_3, f_4 reduce to zero after g_2, g_3, g_4 have been inserted. Indeed, one has $S(f_2, f_3) = 19g_2 + 21g_3$, $S(f_2, f_4) = 25g_2 + 61g_3 + 30g_4$, and $S(f_3, f_4) = 6g_2 + 40g_3 + 30g_4$. Moreover, every new S-pair involving one of g_2, g_3, g_4 has sugar degree at least 3. Hence no further nonzero remainder is obtained at step degree 2. In particular,

$$\mathrm{LM}_{\prec}(\mathcal{G}^{(<D)}) = \{x_1^2, x_1x_2, x_2^2, x_1x_3\} = \mathrm{LM}_{\prec^h}(G_{\mathrm{hom}})_{<D}.$$

Step degree $D = 3$ At this point, we have $\mathrm{LM}_\prec(g_1) = x_1^2$, $\mathrm{LM}_\prec(g_2) = x_1x_2$, $\mathrm{LM}_\prec(g_3) = x_2^2$, and $\mathrm{LM}_\prec(g_4) = x_1x_3$. The four nonzero remainders inserted at step degree 3 are obtained, in this order, from the S-pairs (g_2, g_4), (g_1, g_4), (g_2, g_3), and (g_1, g_2). The corresponding least common multiples are $x_1x_2x_3 \prec x_1^2x_3 \prec x_1x_2^2 \prec x_1^2x_2$, in accordance with the normal selection strategy used to break ties among S-pairs of the same sugar degree. The resulting monic remainders are

$$\begin{aligned} g_5 &= \underline{x_2x_3^2} + 41x_3^3 + 5x_2x_3 + 35x_3^2 + 64x_1 + 42x_2 + 11x_3, \\ g_6 &= \underline{x_3^3} + 35x_3^2 + 37x_1 + 61x_2 + 24x_3, \\ g_7 &= \underline{x_2x_3} + 13x_3^2 + 3x_1 + 37x_2 + 72x_3, \\ g_8 &= \underline{x_3^2} + 72x_1 + 66x_2 + 70x_3. \end{aligned}$$

In a direct Buchberger computation, all other S-pairs of sugar degree 3 reduce to zero. Moreover, these zero reductions can be carried out without increasing the sugar degree, and every new S-pair involving one of g_5, g_6, g_7, g_8 has sugar degree at least 4. Thus g_5, g_6, g_7, g_8 are precisely the nonzero elements inserted at step degree $D = 3$.

All four polynomials have sugar degree D. Since the sugar degree cannot decrease along a reduction sequence, the reductions producing g_5, g_6, g_7, g_8 never increase the sugar degree. Together with the preceding observation on the zero reductions, this shows that the modified computation of Section 4.4 produces no additional intermediate polynomial at step degree D. Hence $\mathcal{G}^{(D)} = \widehat{\mathcal{G}}^{(D)} = \{g_5, g_6, g_7, g_8\}$.

Among them, g_7 and g_8 have total degree 2, and hence are degree-fall elements. After homogenizing them to sugar degree D, their leading monomials are x_2x_3y and x_3^2y, respectively. Consequently,

$$\mathrm{LM}_\prec(\mathcal{G}^{(D)}) = \mathrm{LM}_{\prec^h}(G_{\mathrm{hom}})_D\big|_{y=1} = \{x_2x_3^2, x_3^3, x_2x_3, x_3^2\}.$$

Note that the degree-fall element g_7 is actually used as a reducer in the computation of g_8. More precisely, the reduction of $S(g_1, g_2)$ contains the step $67x_2x_3 + 65x_3^2 + 58x_1 + 18x_2 + 15x_3 \xrightarrow[g_7]{} 70x_3^2 + 3x_1 + 21x_2 + 9x_3$, whose monic form is g_8. Since $\mathrm{sdeg}(g_7) = D$ and it is used without a monomial multiplier, this reduction preserves the sugar degree. Thus the use of g_7 is consistent with the reduction convention of Definition 4.4.2. This explicitly illustrates the reduction convention used in Lemma 4.4.7.

Step degree 4 Continuing the computation yields the following three nonzero remainders of sugar degree 4:

$$g_9 = \underline{x_1} + 61x_2 + 51x_3, \qquad g_{10} = \underline{x_2} + 70x_3, \qquad g_{11} = \underline{x_3}.$$

The remaining S-pairs of sugar degree 4 reduce to zero, so these are the only nonzero remainders inserted at this step degree. The degree-4 homogenizations of g_9, g_{10}, g_{11} inter-reduce to $\{x_1y^3, x_2y^3, x_3y^3\}$, which is the degree-4 part of G_{hom}. This additional correspondence at step degree 4 is not asserted in general; the general synchronization result of Section 4.4 is needed only through step degree D.

After inter-reduction, the reduced Gröbner basis of $\langle F \rangle$ is therefore $G = \{x_1, x_2, x_3\}$. This also agrees with the inter-reduction of $G_{\mathrm{hom}}|_{y=1}$.

A.2 An example beyond cryptographic semi-regularity

The preceding example illustrates the correspondence under cryptographic semi-regularity. We conclude with an example showing that the injectivity condition governing this correspondence is strictly weaker than cryptographic semi-regularity.

Let K be an arbitrary field, let $R = K[x_1, x_2, x_3]$ with the DRL ordering $x_1 \succ x_2 \succ x_3$, and set

$$f_1 = x_1^3 + x_2, \quad f_2 = x_2^3, \quad f_3 = x_3^3, \quad f_4 = x_2^3 + x_2x_3^2, \quad f_5 = x_1x_2x_3$$

with $d_1 = \cdots = d_5 = 3$. The highest-degree homogeneous parts are

$$f_1^{\mathrm{top}} = x_1^3, \quad f_2^{\mathrm{top}} = x_2^3, \quad f_3^{\mathrm{top}} = x_3^3, \quad f_4^{\mathrm{top}} = x_2^3 + x_2x_3^2, \quad f_5^{\mathrm{top}} = x_1x_2x_3.$$

Then $\langle F^{\mathrm{top}} \rangle = \langle x_1^3, x_2^3, x_3^3, x_2x_3^2, x_1x_2x_3 \rangle$. Indeed, the monomial $x_1^2x_3^2$ does not belong to this ideal, whereas every monomial of degree 5 does. Therefore we obtain $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle) = 5$.

On the other hand, $x_3f_2^{\mathrm{top}} + x_2f_3^{\mathrm{top}} - x_3f_4^{\mathrm{top}} = 0$ gives a nonzero class in $H_1(K_\bullet(\boldsymbol{F}^{\mathrm{top}}))_4$. Indeed, the corresponding Koszul cycle is $(0, x_3, x_2, -x_3, 0)$, whereas the degree-4 part of the second Koszul module is zero, since all five generators have degree 3. Thus $H_1(K_\bullet(\boldsymbol{F}^{\mathrm{top}}))_4 \neq 0$. Since $4 < D$, the sequence $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, f_2^{\mathrm{top}}, f_3^{\mathrm{top}}, f_4^{\mathrm{top}}, f_5^{\mathrm{top}})$ is not cryptographic semi-regular.

The homogenizations are $f_1^h = x_1^3 + x_2y^2$ and $f_i^h = f_i$ for $2 \leq i \leq 5$. With respect to the DRL ordering $x_1 \succ x_2 \succ x_3 \succ y$, the reduced Gröbner basis G_{hom} of $\langle F^h \rangle$ is

$$\{\underline{x_1^3 + x_2y^2}, \underline{x_2^3}, \underline{x_3^3}, \underline{x_1x_2x_3}, \underline{x_2x_3^2}, \underline{x_2^2x_3y^2}\}.$$

Thus the first minimal leading monomial divisible by y is $x_2^2x_3y^2$, of degree 5. By Lemma 4.1.1, we obtain $d_{\mathrm{inj}} = 5 = D$. Therefore Condition 4.1.2 holds with $d_0 = D$, although $\boldsymbol{F}^{\mathrm{top}}$ is not cryptographic semi-regular.

For completeness, the corresponding degree fall can also be seen directly. First, $S(f_2^h, f_4^h) = -x_2x_3^2$, so its monic remainder $g := x_2x_3^2$ is inserted at step degree 3. The only new S-pairs of sugar degree 4 are those of g with f_3 and f_5, and both reduce to zero:

$$S(g, f_3) = x_3g - x_2f_3 = 0, \qquad S(g, f_5) = x_1g - x_3f_5 = 0.$$

Thus no further nonzero remainder is inserted before step degree 5. At step degree 5, we have

$$S(f_1^h, f_5^h) = x_2x_3f_1^h - x_1^2f_5^h = x_2^2x_3y^2.$$

Correspondingly, in the affine computation,

$$S(f_1, f_5) = x_2x_3f_1 - x_1^2f_5 = x_2^2x_3.$$

The leading monomials of the current intermediate basis are

$$\begin{aligned} &\mathrm{LM}_\prec(f_1) = x_1^3, \qquad \mathrm{LM}_\prec(f_2) = \mathrm{LM}_\prec(f_4) = x_2^3, \\ &\mathrm{LM}_\prec(f_3) = x_3^3, \qquad \mathrm{LM}_\prec(f_5) = x_1x_2x_3, \qquad \mathrm{LM}_\prec(g) = x_2x_3^2, \end{aligned}$$

none of which divides $x_2^2x_3$. Hence $S(f_1, f_5)$ is already reduced with respect to the current intermediate basis, and its nonzero remainder is $x_2^2x_3$ itself. Since $\deg(x_2^2x_3) = 3 < 5$, a degree fall occurs at step degree $5 = d_{\mathrm{inj}}$, in agreement with Corollary 4.2.6.

Appendix B Generalized cryptographic semi-regularity

As in the main body of this paper, let $R = K[x_1, \ldots, x_n]$ be the polynomial ring in n variables over a field K, and let $\boldsymbol{F} = (f_1, \ldots, f_m)$ be a sequence of inhomogeneous polynomials of degrees $d_1, \ldots, d_m$. Put $F = \{f_1, \ldots, f_m\}$ and $R' = R[y]$.

B.1 Motivation and definition

The following discussion was motivated by exploratory computations over finite fields. We first consider the overdetermined case $m > n$; the case $m = n$ will be discussed separately in Remark B.2.2 below.

We constructed systems having at least one prescribed affine zero as follows. We chose a point $\boldsymbol{a} = (a_1, \ldots, a_n) \in K^n$, generated polynomials $g_1, \ldots, g_m \in R$ of degrees $d_1, \ldots, d_m$ by choosing their coefficients at random, and set $f_j = g_j - g_j(\boldsymbol{a})$ for $1 \leq j \leq m$. Then $\boldsymbol{a}$ is a common zero of F, while $f_j^{\mathrm{top}} = g_j^{\mathrm{top}}$ for $1 \leq j \leq m$. We considered those instances for which F has only finitely many zeros over the algebraic closure $\overline{K}$.

The computations were performed with Magma V2.25-3 [7], using in particular the built-in functions `Dimension`, `HilbertSeries`, and `GroebnerBasis`. They were intended to explore the behavior described below and to motivate the following definition, rather than to provide a statistical study of its frequency.

This construction also gives a natural explanation for the two properties that repeatedly appeared in our computations. Since the prescribed affine zero affects only the lower-degree parts of the input polynomials, the highest-degree homogeneous parts $\boldsymbol{F}^{\mathrm{top}}$ have the same distribution as those of the randomly generated polynomials $g_1, \ldots, g_m$. Thus it is natural to compare their behavior with the usual cryptographic semi-regularity expected for random homogeneous systems.

On the other hand, the homogenized system $\boldsymbol{F}^h$ always has the projective zero $(a_1 : \cdots : a_n : 1)$. Moreover, when $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, it follows from $m > n$ that $R/\langle F^{\mathrm{top}} \rangle$ is Artinian, and hence F^h has no projective zero with $y = 0$. Thus, for the instances considered above satisfying the property (1) below, F^h has finitely many projective zeros. It is then natural to ask whether the Hilbert function initially has the same behavior as that predicted for a homogeneous system with the given degree pattern and subsequently stabilizes at the number of projective zeros counted with multiplicity.

Put $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}} \rangle)$ and $D' = \widetilde{d}_{\mathrm{reg}}(\langle F^h \rangle)$. The following two properties were repeatedly observed:

(1) $\boldsymbol{F}^{\mathrm{top}}$ is D-regular, i.e., cryptographic semi-regular;

(2) $\boldsymbol{F}^h$ is D'-regular.

The property (1) is the usual cryptographic semi-regularity condition. Over an infinite field, Fröberg's conjecture [24] predicts the corresponding Hilbert series for generic homogeneous polynomials of prescribed degrees. We do not claim that the property (2) holds generically.

For these instances, we have $D' < \infty$, and the property (2) can be written as

$$\mathrm{HS}_{R'/\langle F^h \rangle}(z) = \left(\frac{\prod_{j=1}^{m} (1 - z^{d_j})}{(1-z)^{n+1}} \bmod z^{D'} \right) + \sum_{d=D'}^{\infty} N_{F^h} z^d,$$

where N_{F^h} is the number of projective zeros of F^h, counted with multiplicity. This motivates the following extension of cryptographic semi-regularity.

Definition B.1.1. A homogeneous polynomial sequence $\boldsymbol{H} = (h_1, \ldots, h_m)$ is said to be *generalized cryptographic semi-regular* if it is $\widetilde{d}_{\mathrm{reg}}(\langle \boldsymbol{H} \rangle)$-regular when $\widetilde{d}_{\mathrm{reg}}(\langle \boldsymbol{H} \rangle) < \infty$. When $\widetilde{d}_{\mathrm{reg}}(\langle \boldsymbol{H} \rangle) = \infty$, this means that $\boldsymbol{H}$ is d-regular for every positive integer d.

Every cryptographic semi-regular sequence is generalized cryptographic semi-regular. In particular, the property (2) above says that $\boldsymbol{F}^h$ is generalized cryptographic semi-regular. We include the consequence below because it directly sharpens the degree bounds established in Section 3; a systematic study of generalized cryptographic semi-regularity and further consequences is undertaken in [38].

B.2 A refined bound under generalized cryptographic semi-regularity

We next record a consequence of generalized cryptographic semi-regularity for the degree bounds considered in this paper. For positive integers $n, d_1, \ldots, d_m$, recall the notation $D^{(n;d_1,\ldots,d_m)}$ from (3.1.1).

Proposition B.2.1. *Assume that $m > n$, that $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, and that $\boldsymbol{F}^h$ is generalized cryptographic semi-regular. Put $D = d_{\mathrm{reg}}(\langle F^{\mathrm{top}}\rangle)$ and $D' = \widetilde{d}_{\mathrm{reg}}(\langle F^h\rangle)$. Then $D = D^{(n;d_1,\ldots,d_m)}$ and*

$$\max.\mathrm{GB.deg}_{\prec^h}(F^h) \leq \max\{D, D'\} \leq D^{(n+1;d_1,\ldots,d_m)} \tag{B.2.1}$$

Consequently,

$$\mathrm{sd}^{\mathrm{mut}}_{\prec}(F) \leq \mathrm{sd}^{\mathrm{mac}}_{\prec}(F) \leq \mathrm{sd}^{\mathrm{mac}}_{\prec^h}(F^h) = \max.\mathrm{GB.deg}_{\prec^h}(F^h) \leq D^{(n+1;d_1,\ldots,d_m)}.$$

Proof. Since $m > n$ and $\boldsymbol{F}^{\mathrm{top}}$ is cryptographic semi-regular, we have $D < \infty$ and $D = D^{(n;d_1,\ldots,d_m)}$. Moreover, $R/\langle F^{\mathrm{top}}\rangle$ is Artinian, and the proof of Proposition 2.3.4 shows that $D' < \infty$. Since $\boldsymbol{F}^h$ is generalized cryptographic semi-regular, it is D'-regular. By the definition of $D^{(n+1;d_1,\ldots,d_m)}$, the coefficient of degree $D^{(n+1;d_1,\ldots,d_m)}$ in $\frac{\prod_{j=1}^{m}(1-z^{d_j})}{(1-z)^{n+1}}$ is nonpositive. If $D' > D^{(n+1;d_1,\ldots,d_m)}$, then D'-regularity would identify this coefficient with the corresponding value of the Hilbert function. A negative value is impossible, while a zero value would force the Hilbert function to vanish in all subsequent degrees, and hence it would stabilize no later than $D^{(n+1;d_1,\ldots,d_m)}$, contrary to the definition of D'. Hence $D' \leq D^{(n+1;d_1,\ldots,d_m)}$. Moreover, we have $D = D^{(n;d_1,\ldots,d_m)} \leq D^{(n+1;d_1,\ldots,d_m)}$, where the inequality follows directly from the definition. Proposition 2.3.4 (2) therefore yields (B.2.1). The assertions on the solving degrees now follow from the relations recalled in Section 2.2. □

Consequently, the arithmetic complexity over K of computing a Gröbner basis of $\langle F^h\rangle$, and hence of $\langle F\rangle$ via homogenization, is bounded by

$$O\left(m\binom{n + D^{(n+1;d_1,\ldots,d_m)}}{D^{(n+1;d_1,\ldots,d_m)}}^{\omega}\right), \tag{B.2.2}$$

where ω denotes the exponent of matrix multiplication over K; see [38, Theorem 1.1 (2) and Remark 3].

Remark B.2.2. When $m = n$, cryptographic semi-regularity of $\boldsymbol{F}^{\mathrm{top}}$ already implies that $\boldsymbol{F}^h$ is generalized cryptographic semi-regular and that $D' = D - 1$; see [38, Lemma 3.1.1]. Consequently, $\max.\mathrm{GB.deg}_{\prec^h}(F^h) \leq D$. Moreover, equality $\max.\mathrm{GB.deg}_{\prec^h}(F^h) = D$ holds if the initial ideal $\langle \mathrm{LM}_{\prec^h}(\langle F^h\rangle)\rangle$ is weakly reverse lexicographic; see Proposition 2.3.4 and [38, Theorem 1.2].

The bound in (B.2.1) can be substantially smaller than the first bound in Theorem 3.1.3 when the system is sufficiently overdetermined. For example, in the quadratic case with $n = 9$ and $m = 18$, we have $D = D^{(9;2,\ldots,2)} = D^{(10;2,\ldots,2)} = 4$, whereas the first bound in Theorem 3.1.3 is 11.

The degree $D^{(n+1;d_1,\ldots,d_m)}$ also appears in analyses of algebraic attacks. For example, [25, Section 2.3] uses $D^{(n+1;d_1,\ldots,d_m)}$ as a degree bound for the XL algorithm [13]. As discussed in [25, Section 2.3, in particular Remark 1], this degree has also appeared in the cryptographic literature without an explicit regularity assumption on $\boldsymbol{F}^h$. Generalized cryptographic semi-regularity gives a sufficient condition under which this degree bound, and consequently the arithmetic-complexity estimate (B.2.2), is rigorously justified.