New efficient algorithms for computing Gröbner bases of saturation ideals (F4SAT) and colon ideals (Sparse-FGLM-colon)

Jérémy Berthomieu, Christian Eder, Mohab Safey El Din

New efficient algorithms for computing Gröbner bases of saturation ideals (F_4SAT) and colon ideals (Sparse-FGLM-colon)

Jérémy Berthomieu[1], Christian Eder[2], and Mohab Safey El Din[1]

[1]Sorbonne Université, CNRS, LIP6, F-75005, Paris, France
[2]Technische Universität Kaiserslautern, Kaiserslautern, Germany

February 1, 2022

Abstract

This paper is concerned with linear algebra based methods for solving exactly polynomial systems through so-called Gröbner bases, which allow one to compute modulo the polynomial ideal generated by the input equations. This is a topical issue in non-linear algebra and more broadly in computational mathematics because of its numerous applications in engineering and computing sciences. Such applications often require geometric computing features such as representing the closure of the set difference of two solution sets to given polynomial systems. Algebraically, this boils down to computing Gröbner bases of colon and/or saturation polynomial ideals. In this paper, we describe and analyze new Gröbner bases algorithms for this task and present implementations which are more efficient by several orders of magnitude than the state-of-the-art software.

1 Introduction

Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ and φ be polynomials in the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ where $\mathbb{K}$ is a field. Further, we denote by $I = \langle \boldsymbol{f} \rangle = \langle f_1, \ldots, f_s \rangle$ the polynomial ideal generated by $f_1, \ldots, f_s$ and by $V(I) \subset \overline{\mathbb{K}}^n$ the algebraic set associated to I (where $\overline{\mathbb{K}}$ is an algebraic closure of $\mathbb{K}$).

We consider the following computational problem: compute a Gröbner basis associated to the colon (resp. saturated) ideal of I by φ, i.e.

$$I : \langle \varphi \rangle = \{h \mid h\varphi \in I\} \quad \text{(resp.} \quad I : \langle \varphi \rangle^\infty = \{h \mid \exists k \in \mathbb{N}\ h\varphi^k \in I\}).$$

By e.g. [11, Chap. 4], the algebraic set $V(I : \langle \varphi \rangle^\infty) \subset \overline{\mathbb{K}}^n$ is the Zariski closure of the set difference $V(I) \setminus V(\varphi)$ and there exists $N \in \mathbb{N}$ such that $I : \langle \varphi^N \rangle = I : \langle \varphi^{N+1} \rangle = \cdots = I : \langle \varphi \rangle^\infty$.

Computing algebraic representations of saturated ideals arises in many applications ranging from experimental mathematics to engineering sciences (see e.g. [7, 21, 29]) since some natural algebraic modelings come with parasite solutions which one excludes through some saturation process. For instance, modeling that some $p \times q$ matrix with polynomial entries has rank r through the simultaneous vanishing of its $(r+1)$-minors will include those points at which the matrix has rank less than r.

In the paper, we design new efficient algorithms for computing *Gröbner bases* of such ideals, given as input $\boldsymbol{f} = (f_1, \ldots, f_s)$, φ and some admissible monomial ordering $\prec$ over the monomials in $\mathbb{K}[x_1, \ldots, x_n]$.

Recall that Gröbner bases are finite generating sets of polynomial ideals capturing their combinatorial and algebraic properties. They allow to compute *modulo* the ideal they generate, hence to decide the membership of a polynomial to the ideal under consideration. Gröbner bases algorithms are a classical and versatile tool for polynomial system solving, non-linear algebra and geometry, implemented in most of computer algebra systems.

Prior results. The first algorithm for computing Gröbner bases is introduced by Buchberger in [9]. It is based on the so-called Buchberger's criterion which provides an effective way to decide whether a given polynomial sequence is already a Gröbner basis of the ideal it generates. Modern algorithms such as Faugère's F_4 [14] and F_5 [15] (see also [13]) algorithms actually use the connection of Gröbner basis theories with Macaulay's constructions for the multivariate resultant (see e.g. [25]) by considering the finite-dimensional vector spaces

$$E_d(\boldsymbol{f}) = \{h_1 f_1 + \cdots + h_s f_s \mid \deg(h_i f_i) \leq d \text{ for all } 1 \leq i \leq s\}$$

for which a basis with appropriate properties w.r.t. the given monomial ordering is computed through the row echelonization of some Macaulay-like matrix. The way these linear algebra constructions are generated at each degree $d, d+1, \ldots$ (and so on) plus a termination criterion is done via a connection to the Gröbner basis theory and Buchberger's criterion in F_4. The F_5 algorithm poses a module theoretic view of Gröbner basis calculations which allows one to generate Macaulay-like matrices of maximal rank under some genericity assumptions as well as a module theoretic transposition of the notion of critical pairs through the notion of *signature* to handle termination issues in this context. These two algorithms have been used to solve many difficult applications and challenges of polynomial system solving (see e.g. [17, 18, 32]). Such algorithms are usually run with so-called total degree monomial orderings, i.e. those orderings which filter monomials first w.r.t. their total degrees.

When I has dimension zero (i.e. $V(I)$ is a non-empty finite set) this linear algebra view of Gröbner basis computations is often used in change of ordering algorithms since the quotient ring $\mathbb{K}[x_1, \ldots, x_n]/I$ is a finite-dimensional vector space. Based on this, the so-called FGLM algorithm [16] reduces change of ordering algorithms to kernel computations. Under some extra assumptions, the so-called Sparse-FGLM algorithm [19, 20] makes the connection with relation reconstructions.

Despite these developments, computing saturations of polynomial ideals is currently done using the above Gröbner basis algorithms *as a black box*.

Using Rabinowitsch trick [30] and [11, Chap. 4, Sec. 4, Th. 14, (ii)], the saturated ideal $I : \langle\varphi\rangle^\infty$ equals $(I + \langle 1 - t\varphi\rangle) \cap \mathbb{K}[x_1, \ldots, x_n]$. Thus, computing a Gröbner basis of $I + \langle 1 - t\varphi\rangle$ for a monomial ordering eliminating t and keeping all polynomials not involving t yields a Gröbner basis of $I : \langle\varphi\rangle^\infty$, see also [11, Chap. 3, Sec. 1, Th. 2 and Ex. 6].

Moreover, if I is homogeneous, i.e. it is spanned by a set of homogeneous polynomials, Bayer's algorithm [1] allows us to compute $I : \langle x_n\rangle^\infty$. If it is not, then one can still recover a Gröbner basis of $I : \langle x_n\rangle^\infty$ using the algorithm below, still called Bayer's algorithm:

1. Homogenize the input polynomials $f_1, \ldots, f_s$ with a new variable x_0 yielding homogeneous polynomials $\boldsymbol{f}^{\mathrm{h}} = (f_1^{\mathrm{h}}, \ldots, f_s^{\mathrm{h}})$;
2. compute a Gröbner basis G^{h} for $\boldsymbol{f}^{\mathrm{h}}$ and a total degree monomial ordering (called graded reverse lexicographical ordering) where x_n is smaller than the other variables $x_0, x_1, \ldots, x_{n-1}$;
3. factor out from all polynomials in G^{h} the highest possible power of x_n;
4. set x_0 to 1 in these obtained polynomials and return the result.

When $\varphi \neq x_n$, one just introduces a slack variable x_{n+1} and computes the saturation of $I + \langle x_{n+1} - \varphi\rangle$ w.r.t. x_{n+1}.

The above two approaches constitute the state-of-the-art algorithms for computing saturations of ideals. Note that they do not take advantage of intermediate data obtained during the Gröbner basis computations since these are used as black boxes.

Main results. In this paper, we propose new algorithms which actually compute "on the fly" Gröbner bases of saturated ideals through the linear algebra approaches we sketched above. We design two families of efficient algorithms which are the counterparts of the F_4 and the FGLM algorithms. We also present (publicly available) implementations of these algorithms which are more efficient than the state-of-the-art software in computer algebra systems by several orders of magnitude.

The first algorithm, named F_4SAT, is a modification of the F_4 algorithm to discover on the fly polynomials in $I : \langle\varphi\rangle^\infty$. The core idea is as follows. Recall that, on input $\boldsymbol{f} = (f_1, \ldots, f_s)$ and φ in $\mathbb{K}[x_1, \ldots, x_n]$ and a given total degree monomial ordering $\prec$, the F_4 algorithm roughly computes bases G_d of the finite-dimensional vector spaces E_d, we introduced above, using G_d to generate a generating family for E_{d+1} (using the notion of critical pairs, see [14]) and so on. Termination is ensured using Buchberger's criterion.

We show that, during this process, one can search for polynomials h of maximum prescribed degree δ in the colon ideal $I : \langle\varphi\rangle$ such that $h\varphi \in E_d$ using *(i)* the computation of *normal forms* of $m.\varphi$ where m lies in a set of well-chosen monomials; and *(ii)* the computation of the kernel of some matrix which is built from the above normal forms.

This algorithmic strategy allows us to discover on the fly new polynomials in the colon ideal $I : \langle\varphi\rangle$ which are then taken into account early in the whole computation. Repeating this, with (maybe incomplete) generating sets of $I : \langle\varphi\rangle$ allows us to discover polynomials in $(I : \langle\varphi\rangle) : \langle\varphi\rangle = I : \langle\varphi^2\rangle$ and so on.

We prove how to complete such a computation and how the above prescribed degree δ can be chosen to ensure correctness of the algorithm.

When the ideal $I : \langle\varphi\rangle^{\infty}$ is known to be zero-dimensional in advance, one can adapt FGLM-like algorithms, assuming we have precomputed a Gröbner basis for I w.r.t. some monomial ordering, to compute a Gröbner basis for $I : \langle\varphi\rangle^{\infty}$ w.r.t. a so-called lexicographical ordering (yielding a triangular basis). Here the main difficulty to overcome is that since *we do not assume that I is zero-dimensional*, the vector space $\mathbb{K}[x_1, \dots, x_n]/I$ is of infinite dimension. We demonstrate how the change of ordering can still be realized through linear algebra techniques which borrow from FGLM the construction of matrices representing multiplication operators in the quotient ring from which one can extract the lexicographical Gröbner basis. We show how to use algebraic properties to reduce the size of such matrices and state the complexity of our approach when only the matrix representing the multiplication by the last variable is needed. All in all, this new algorithm reduces the change of ordering in this context to the computation of minimal relations satisfied by sequences of scalars computed from the aforementioned matrices as well as Hankel linear system solving.

Next, we present our implementation, which we wrote using the `C` programming language and which is available in the MSOLVE library [3, 4]. We compare it against implementations based on the Rabinowitsch trick using Gröbner basis engine in MSOLVE (which is one of the fastest open source implementations), the one in MAPLE (which is one of the fastest in commercial computer algebra systems), and the leading software for algebra and geometry SINGULAR. We carefully analyze the practical behaviors of the new algorithms in this paper. Our experiments show that on many examples the new algorithms are faster, often by several orders of magnitude, than the state-of-the-art software alternatives.

Structure of the paper. Section 2 is devoted to fix some notation we use about Gröbner bases and recall the basics of F_4 and FGLM algorithms needed to describe our new algorithms. Section 3 describes the F_4SAT algorithm, and its correctness and termination proofs. Section 4 focuses on the FGLM variant for saturation. Finally, Section 5 presents our implementations and compares it with the state-of-the-art software.

2 Preliminaries

2.1 Gröbner bases

We recall some basic definitions and properties of Gröbner bases. We refer to [11, Chap. 2, 3 and 5] for more details.

Throughout this paper, let $\mathbb{K}$ be a field and $0 \in \mathbb{N}$. We denote by $\mathbb{K}[\boldsymbol{x}] \coloneqq \mathbb{K}[x_1, \dots, x_n]$ the polynomial ring in n variables $x_1, \dots, x_n$ with coefficients in $\mathbb{K}$. A polynomial $f \in \mathbb{K}[\boldsymbol{x}]$ is defined as $f = \sum_{\boldsymbol{s}\in\mathbb{N}^n} f_{\boldsymbol{s}}\boldsymbol{x}^{\boldsymbol{s}}$ such that $f_{\boldsymbol{s}} = 0$ for all but finitely many $\boldsymbol{s} \in \mathbb{N}^n$. For $f \neq 0$ we define its support $\operatorname{supp} f = \{\boldsymbol{s} \in \mathbb{N}^n \mid f_{\boldsymbol{s}} \neq 0\}$. Otherwise, by convention, $\operatorname{supp} 0 = \{\boldsymbol{0}\}$.

A monomial ordering $\prec$ on $\mathbb{K}[\boldsymbol{x}]$ is a total order on the set of monomials such that for all monomials m, m' and s, if $m \preceq m'$, then $ms \preceq m's$. Furthermore, the monomial orders in this paper are assumed to be well-orderings, i.e. for all monomials m we have that $1 \preceq m$.

Fix a monomial ordering $\prec$. Given a polynomial $f \in \mathbb{K}[\boldsymbol{x}]$, we define its *leading monomial*, denoted by $\text{LM}_\prec(f)$, the largest monomial in f for $\prec$. The *leading coefficient* of f, $\text{LC}_\prec(f)$, is the coefficient of $\text{LM}_\prec(f)$ and the *leading term* of f, $\text{LT}_\prec(f)$ is $\text{LC}_\prec(f)\,\text{LM}_\prec(f)$. For a set $G \subseteq \mathbb{K}[\boldsymbol{x}]$, we let $\text{LM}_\prec(G) = \{\text{LM}_\prec(f) \mid f \in G\}$. For an ideal $I \subset \mathbb{K}[\boldsymbol{x}]$ we define $\text{LM}_\prec(I)$ as the ideal generated by leading monomials of all elements of I. We recall briefly the definition of a Gröbner basis and of its associated staircase.

Definition 2.1. *A set of monomials S is a* staircase *if for two monomials μ_1 and μ_2 such that $\mu_1\mu_2 \in S$, we have $\mu_1 \in S$ and $\mu_2 \in S$.*

Definition 2.2 ([11, Chap. 2, Sec. 5, Def. 5 and Sec. 7, Def. 4])**.** *Let I be a nonzero ideal of $\mathbb{K}[\boldsymbol{x}]$ and let $\prec$ be a monomial ordering. A set $\mathcal{G} \subseteq I$ is a* Gröbner basis *of I for $\prec$ if for all $f \in I$, there exists $g \in \mathcal{G}$ such that $\text{LM}_\prec(g) \mid \text{LM}_\prec(f)$ or, equivalently, if $\langle \text{LM}_\prec(\mathcal{G})\rangle = \text{LM}_\prec(I)$. It is* reduced *if for any $g \in \mathcal{G}$, g is monic, i.e. $\text{LC}_\prec(g) = 1$, and for any $g' \in \mathcal{G} \setminus \{g\}$ and any monomial $m \in \operatorname{supp} g'$, $\text{LM}_\prec(g) \nmid m$.*

The staircase *associated to $\mathcal{G}$ is the set of monomials* Staircase($\mathcal{G}$) *which are not divisible by any $\text{LM}_\prec(g)$ for $g \in \mathcal{G}$, i.e. the complement of $\text{LM}_\prec(I)$ in the set of monomials.*

Once a monomial ordering $\prec$ is chosen, a monomial basis of the quotient algebra $\mathbb{K}[\boldsymbol{x}]/I$ can be canonically set: it is the set of monomials that are not leading monomials of polynomials in I w.r.t. $\prec$. In other words, this is Staircase($\mathcal{G}$), where $\mathcal{G}$ is a Gröbner basis of I for $\prec$, see [11, Chap. 5, Sec. 3, Prop. 1]. Furthermore, if $\mathbb{K}[\boldsymbol{x}]/I$ is a finite-dimensional $\mathbb{K}$-vector space, then I is said to be *zero-dimensional* of *degree* $\dim_\mathbb{K} \mathbb{K}[\boldsymbol{x}]/I$, otherwise it is *positive-dimensional*.

In this paper, we mainly deal with the lexicographic (LEX, $\prec_{\text{LEX}}$) and degree reverse lexicographic (DRL, $\prec_{\text{DRL}}$) orderings with the convention that $x_n \prec \cdots \prec x_2 \prec x_1$. They are defined as below:

LEX: $\boldsymbol{x}^{\boldsymbol{i}} \prec_{\text{LEX}} \boldsymbol{x}^{\boldsymbol{j}}$ if, and only if, there exists $1 \leq p \leq n$ such that for all $q < p$, $i_q = j_q$ and $i_p < j_p$, see [11, Chap. 2, Sec. 2, Def. 3];

DRL: $\boldsymbol{x}^{\boldsymbol{i}} \prec_{\text{DRL}} \boldsymbol{x}^{\boldsymbol{j}}$ if, and only if, $i_1 + \cdots + i_n < j_1 + \cdots + j_n$ or both $i_1 + \cdots + i_n = j_1 + \cdots + j_n$ and there exists $2 \leq p \leq n$ such that for all $q > p$, $i_q = j_q$ and $i_p > j_p$, see [11, Chap. 2, Sec. 2, Def. 6]. Observe that it is a total degree monomial ordering.

An important property of Gröbner bases is that given a polynomial $f \in \mathbb{K}[\boldsymbol{x}]$ and $\mathcal{G} = \{g_1, \ldots, g_r\}$ a Gröbner basis of an ideal of $\mathbb{K}[\boldsymbol{x}]$ for $\prec$, there exist polynomials $h_0, h_1, \ldots, h_r$, with h_0 unique, such that $f = g_1h_1 + \cdots + g_rh_r + h_0$ and $\text{LM}_\prec(h_0)$ is not divisible by $\text{LM}_\prec(g_1), \ldots, \text{LM}_\prec(g_r)$. This polynomial h_0 is called the *normal form of f with respect to $\mathcal{G}$ for $\prec$* and will be denoted by $\text{NF}\,(f, \mathcal{G}, \prec)$.

Definition 2.3 ([11, Chap. 9, Sec. 3])**.** *Let I be an ideal of $\mathbb{K}[\boldsymbol{x}]$ spanned by homogeneous polynomials. Let $\mathbb{K}[\boldsymbol{x}]_d$ (resp. I_d) be the subset of homogeneous polynomials of degree d, together with the zero polynomial, of $\mathbb{K}[\boldsymbol{x}]$ (resp. I).*

The Hilbert series $\mathrm{HS}_{\mathbb{K}[\boldsymbol{x}]/I}$ of $\mathbb{K}[\boldsymbol{x}]/I$ *is the generating series of the sequence* $\dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{x}]_d/I_d$*, i.e.*

$$\mathrm{HS}_{\mathbb{K}[\boldsymbol{x}]/I} = \sum_{d\geq 0} \dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{x}]_d/I_d \, t^d.$$

2.2 Gröbner basis algorithms

Buchberger developed the theory of Gröbner bases and designed a first algorithm to compute them in [9]. Since then, many efficient Gröbner basis algorithms were developed. Here, we focus on Faugère's F_4 algorithm [14].

2.2.1 The F_4 algorithm

In [9], Buchberger's algorithm introduced the concept of *critical pairs* for computing Gröbner bases. For two polynomials f_1 and f_2 in a set of generators of an ideal, the critical pair (f_1, f_2) leads to a normal form computation of the *S-polynomial*

$$\mathrm{sp}_{\prec}(f_1, f_2) = \frac{\mathrm{LCM}(\mathrm{LM}_{\prec}(f_1), \mathrm{LM}_{\prec}(f_2))}{\mathrm{LT}_{\prec}(f_1)} f_1 - \frac{\mathrm{LCM}(\mathrm{LM}_{\prec}(f_1), \mathrm{LM}_{\prec}(f_2))}{\mathrm{LT}_{\prec}(f_2)} f_2$$

w.r.t. the current intermediate basis. The *degree* of such a critical pair is $\deg \mathrm{LCM}(\mathrm{LM}_{\prec}(f_1), \mathrm{LM}_{\prec}(f_2))$. Notice that this bounds from above $\deg \mathrm{sp}_{\prec}(f_1, f_2)$.

In Algorithm 2.1 we state the pseudocode of Faugère's F_4 algorithm, highlighting (in red) the main differences to Buchberger's algorithm.

Input: A list of polynomials $f_1, \dots, f_s$ spanning an ideal $I \subseteq \mathbb{K}[\boldsymbol{x}]$ and a total degree monomial ordering $\prec$.
Output: A Gröbner basis $\mathcal{G}$ of I for $\prec$.

$\mathcal{G} \coloneqq \{f_1, \dots, f_s\}$.
$P \coloneqq \{(f_i, f_j) \mid 1 \leq i < j \leq s\}$.
While $P \neq \emptyset$ **do**
    Choose a subset L of P.
    $P \coloneqq P \setminus L$.
    $L \coloneqq \mathrm{SymbolicPreprocessing}(L, \mathcal{G})$.
    $L \coloneqq \mathrm{LinearAlgebra}(L)$.
    For $h \in L$ *with* $\mathrm{LM}_{\prec}(h) \notin \langle \mathrm{LM}_{\prec}(\mathcal{G}) \rangle$ **do**
        $P \coloneqq P \cup \{(g, h) \mid g \in \mathcal{G}\}$.
        $\mathcal{G} \coloneqq \mathcal{G} \cup \{h\}$.
Return $\mathcal{G}$.

Algorithm 2.1: Faugère's F_4

Observe that the termination of the F_4 algorithm only relies on Buchberger's first criterion: $\mathcal{G} = \{g_1, \dots, g_t\}$ is a Gröbner basis of an ideal I for $\prec$ if for all $1 \leq i, j \leq s$, $\mathrm{NF}(\mathrm{sp}_{\prec}(g_i, g_j), \mathcal{G}, \prec) = 0$, see [11, Chap. 2, Sec. 6, Th. 6].

We detail the differences to Buchberger's algorithm.

1. One can choose several critical pairs at a time, stored in a subset $L \subseteq P$. The so-called *degree strategy* chooses L to be the set of *all* critical pairs of minimal degree for a total degree monomial ordering, typically $\prec_{\text{DRL}}$.
2. For all terms of all the generators of the S-polynomials, one searches in the current intermediate Gröbner basis $\mathcal{G}$ for possible reducers. One adds those to L and again search for all of their terms for reducers in $\mathcal{G}$. This is the SymbolicPreprocessing function.
3. Once all reduction data is collected from the last step, one generates a Macaulay-like matrix with columns corresponding to the monomials appearing in L (sorted by $\prec$) and rows corresponding to the coefficients of each polynomial in L. Gaussian Elimination is then applied to reduce now all chosen S-polynomials at once. This is the LinearAlgebra function.
4. Finally, one adds those polynomials associated to rows in the updated matrix to $\mathcal{G}$ whose leading monomials are not already in $\text{LM}_\prec(\mathcal{G})$.

In order to optimize the algorithm one can now apply Buchberger's product and chain criteria, see [10, 23]. Thus many useless critical pairs are removed before even being added to P and fewer zero rows are computed during the linear algebra part of F_4. Still, in general, there are many zero reductions left.

Different selection strategies yield different behavior of the algorithm. The degree strategy allows one to compute *truncated Gröbner bases* of ideals in case of early terminations.

Definition 2.4. *Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[\boldsymbol{x}]$ and $\prec$ be a monomial ordering. Let μ be a monomial and F_μ be the $\mathbb{K}$-vector subspace of $\langle f_1, \ldots, f_s \rangle$ defined as*

$$F_\mu = \left\{ \sum_{i=1}^{s} h_i f_i \,\middle|\, \forall\, 1 \leq i \leq s, \text{LT}_\prec(h_i f_i) \preceq \mu \right\}.$$

Then, $\mathcal{G} \subset F_\mu$ is a μ-truncated Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ for $\prec$ if for all $p \in F_\mu$, there exists $g \in \mathcal{G}$ such that $\text{LM}_\prec(g) \mid \text{LM}_\prec(p)$ and $p - \frac{\text{LT}_\prec(p)}{\text{LT}_\prec(g)} g$ is in F_μ.

Observe that taking a triangular basis of F_μ ordered increasingly w.r.t. $\prec$ naturally yields a μ-truncated Gröbner basis thereof.

Proposition 2.5. *Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[\boldsymbol{x}]$ and $\prec$ be a monomial ordering. Let μ be a monomial and F_μ be the $\mathbb{K}$-vector subspace of $\langle f_1, \ldots, f_s \rangle$*

$$F_\mu = \left\{ \sum_{i=1}^{s} h_i f_i \,\middle|\, \forall\, 1 \leq i \leq s, \text{LM}_\prec(h_i f_i) \preceq \mu \right\}.$$

A subset $\mathcal{G} = \{g_1, \ldots, g_t\} \subset F_\mu$ is a μ-truncated Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ for $\prec$ if, and only if,

$$F_\mu \subseteq G_\mu = \left\{ \sum_{j=1}^{t} h_j g_j \,\middle|\, \forall\, 1 \leq j \leq t, \text{LM}_\prec(h_j g_j) \preceq \mu \right\}.$$

and for all $(g_i, g_j) \in \mathcal{G}^2$ with $i \neq j$, if $\text{LCM}(\text{LM}_\prec(g_i), \text{LM}_\prec(g_j)) \preceq \mu$, then

$$\text{NF}\left(\text{sp}_\prec\left(g_i, g_j\right), \mathcal{G}, \prec\right) = 0.$$

Proof. This proof follows the proof of [11, Chap. 2, Sec. 6, Th. 6].

If $\mathcal{G}$ is a μ-truncated Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ for $\prec$, then observe that both F_μ and G_μ only contain polynomials with leading monomial less or equal to μ for $\prec$. Let $p \in F_\mu$, then there exists $g \in \mathcal{G}$ such that $\mathrm{LM}_\prec(g) \mid \mathrm{LM}_\prec(p)$, $\mathrm{LM}_\prec(g)$ is maximal and $p - \frac{\mathrm{LT}_\prec(p)}{\mathrm{LT}_\prec(g)} g$ is in F_μ. Thus, $p = hg + q$ with $\mathrm{LM}_\prec(q) \prec \mathrm{LM}_\prec(p) \preceq \mu$, $\mathrm{LM}_\prec(hg) = \mathrm{LM}_\prec(p) \preceq \mu$ and $q \in F_\mu$. Repeating this division process on q shows that $p \in G_\mu$. As a consequence p reduces to 0 w.r.t. G and $\prec$.

Now, let g_i and g_j be in G and $i \neq j$. Let $m = \mathrm{LCM}(\mathrm{LM}_\prec(g_i), \mathrm{LM}_\prec(g_j))$, then $\mathrm{sp}_\prec(g_i, g_j) = \frac{m}{\mathrm{LT}_\prec(g_i)} g_i - \frac{m}{\mathrm{LT}_\prec(g_j)} g_j$. Furthermore, if $m \preceq \mu$, then $\mathrm{LM}_\prec\left(\frac{m}{\mathrm{LT}_\prec(g_i)} g_i\right) = m \preceq \mu$, and likewise for g_j. Hence, $\mathrm{sp}_\prec(g_i, g_j) \in G_\mu$ and its normal form w.r.t. G and $\prec$ is 0.

For the converse, assume that G_μ contains F_μ and that for all $(g_i, g_j) \in \mathcal{G}^2$ with $i \neq j$, if $\mathrm{LCM}(\mathrm{LM}_\prec(g_i), \mathrm{LM}_\prec(g_j)) \preceq \mu$, then $\mathrm{NF}(\mathrm{sp}_\prec(g_i, g_j), \mathcal{G}, \prec) = 0$.

Let $p \in F_\mu$, since $F_\mu \subseteq G_\mu$, there exist $h_1, \ldots, h_t$ such that $\mathrm{LM}_\prec(h_i g_i) \preceq \mu$ for all $1 \leq i \leq t$ and $p = h_1 g_1 + \cdots + h_t g_t$. Let $m = \max_{1 \leq i \leq t} \mathrm{LM}_\prec(h_i g_i) \preceq \mu$, then observe that $\mathrm{LM}_\prec(p) \preceq m \preceq \mu$. Assume that among all the possible such writings of p, the polynomials $h_1, \ldots, h_t$ are chosen so that m is minimal for $\prec$. Such a minimal monomial exists by the well-ordering property of $\prec$.

Now, if $\mathrm{LM}_\prec(p) = m = \mathrm{LM}_\prec(h_i g_i) = \mathrm{LM}_\prec(h_i) \, \mathrm{LM}_\prec(g_i)$ for some $1 \leq i \leq t$, then $\mathrm{LM}_\prec(g_i)$ divides $\mathrm{LM}_\prec(f)$, hence $\mathrm{LM}_\prec(p) \in \mathrm{LM}_\prec(\mathcal{G})$.

Otherwise, $\mathrm{LM}_\prec(p) \prec m$. We will use the fact that if the critical pair (g_i, g_j) satisfies $\mathrm{LCM}(\mathrm{LM}_\prec(g_i), \mathrm{LM}_\prec(g_j)) \preceq \mu$ implies $\mathrm{NF}(\mathrm{sp}_\prec(g_i, g_j), \mathcal{G}, \prec) = 0$ to build a new expression of p that decreases m.

Let us write

$$p = \sum_{\substack{1 \leq i \leq t \\ \mathrm{LM}_\prec(h_i g_i) = m}} h_i g_i + \sum_{\substack{1 \leq i \leq t \\ \mathrm{LM}_\prec(h_i g_i) \prec m}} h_i g_i,$$

Then,

$$p = \sum_{\substack{1 \leq i \leq t \\ \mathrm{LM}_\prec(h_i g_i) = m}} \mathrm{LM}_\prec(h_i) g_i + \sum_{\substack{1 \leq i \leq t \\ \mathrm{LM}_\prec(h_i g_i) = m}} (h_i - \mathrm{LM}_\prec(h_i)) g_i + \sum_{\substack{1 \leq i \leq t \\ \mathrm{LM}_\prec(h_i g_i) \prec m}} h_i g_i,$$

Since the second and third sums only involve monomials smaller than m for $\prec$, then the leading monomial of the first one is also smaller than m for $\prec$. Observe, on the one hand, that

$$s_{i,j} = \mathrm{sp}_\prec(g_i \, \mathrm{LM}_\prec(h_i), g_j \, \mathrm{LM}_\prec(h_j)) = \mathrm{sp}_\prec(g_i, g_j) \frac{m}{\mathrm{LM}_\prec(g_i) \, \mathrm{LM}_\prec(g_j)}.$$

Now, on the other hand, $\mathrm{LM}_\prec(g_i \, \mathrm{LM}_\prec(h_i)) = \mathrm{LM}_\prec(g_j \, \mathrm{LM}_\prec(h_j)) = m$, hence their lcm is m. Therefore, $\mathrm{LCM}(\mathrm{LM}_\prec(g_i), \mathrm{LM}_\prec(g_j)) \preceq m \preceq \mu$. By [11, Chap. 2, Sec. 6, Lemma 5], the first sum in the latter expression of p is a linear combination of the $s_{i,j}$'s and $\mathrm{LM}_\prec(s_{i,j}) \prec m$ for all $1 \leq i < j \leq t$.

Consider, one of these polynomials $s_{i,j}$. Since $\mathrm{LCM}(\mathrm{LM}_\prec(g_i), \mathrm{LM}_\prec(g_j)) \preceq \mu$, then we know that the critical pair (g_i, g_j) is such that $\mathrm{NF}(\mathrm{sp}_\prec(g_i, g_j), \mathcal{G}, \prec) = 0$, hence

$\mathrm{NF}(s_{i,j}, \mathcal{G}, \prec) = 0$ and there exist $A_1, \dots, A_t \in \mathbb{K}[\boldsymbol{x}]$ such that

$$s_{i,j} = A_1 g_1 + \cdots + A_t g_t,$$

and for all $1 \leq i \leq t$, $\mathrm{LM}_\prec(A_i g_i) \preceq \mathrm{LM}_\prec(s_{i,j}) \prec m$.

Doing this for all the polynomials $s_{i,j}$, we show that the first sum of the latter expression of p can be replaced by $B_1 g_1 + \cdots + B_t g_t$, where for all $1 \leq i \leq t$, $\mathrm{LM}_\prec(B_i g_i) \prec m$. This contradicts the minimality of m for this property, hence $\mathrm{LM}_\prec(p) = m$ and $\mathrm{LM}_\prec(p) \in \mathrm{LM}_\prec(\mathcal{G})$. By Definition 2.4, $\mathcal{G}$ is a μ-truncated Gröbner basis of $\langle f_1, \dots, f_s \rangle$ for $\prec$. □

Remark 2.6. *1. If $\prec$ is a total degree monomial ordering, then for $d \in \mathbb{N}$, we can also define a d-*truncated Gröbner basis *as a μ-truncated Gröbner basis for μ the largest monomial of degree d for $\prec$.*

2. If $\mathcal{G} = \{g_1, \dots, g_t\}$ is a μ-truncated Gröbner basis of $\langle f_1, \dots, f_s \rangle$ for $\prec$ and

$$\mu \succeq \max_{1 \leq i < j \leq t} \mathrm{LCM}(\mathrm{LM}_\prec(g_i), \mathrm{LM}_\prec(g_j)),$$

then $\mathcal{G}$ is a Gröbner basis of $\langle f_1, \dots, f_s \rangle$ for $\prec$. Indeed, it spans the ideal and by Proposition 2.5, all the S-polynomials reduce to 0 w.r.t. $\mathcal{G}$ and $\prec$. Hence, by Buchberger's first criterion [11, Chap. 2, Sec. 6, Th. 6], it is a Gröbner basis of $\langle f_1, \dots, f_s \rangle$ for $\prec$.

3. Definition 2.4 depends greatly on the set of generators of the ideal. Consider $f_1 = x^n$, $f_2 = (y-1)^n$ and $f_3 = xy - y - 1$ for $n \in \mathbb{N} \setminus \{0, 1\}$. By Proposition 2.5, $\mathcal{G} = \{f_1, f_2, f_3\}$ is a n-truncated Gröbner basis of $\langle f_1, f_2, f_3 \rangle$ for $\prec_{\mathrm{DRL}}$. Yet, this ideal is $\langle 1 \rangle$ hence $\{1\}$ is a n-truncated Gröbner basis of $\langle 1 \rangle$ for all $n \in \mathbb{N}$.

Lemma 2.7. *Let $f_1, \dots, f_s \in \mathbb{K}[\boldsymbol{x}]$ be the input polynomials of the* F_4 *algorithm. Let $d \in \mathbb{N}$. Assume that the* F_4 *algorithm uses the degree selection strategy and that, on line 4, L consists in all the critical pairs of degree d.*

If no new polynomial is added to $\mathcal{G}$ on line 10, then $\mathcal{G}$ is a d-truncated Gröbner basis of $\langle f_1, \dots, f_s \rangle$.

Proof. By the degree selection strategy, only critical pairs of degree at least d exist. Since no new polynomial is added at the end of the turn, this means that all S-polynomials coming from critical pairs of degree d reduce to 0 w.r.t. $\mathcal{G}$ and $\prec$. Furthermore, $\mathcal{G}$ contains $f_1, \dots, f_s$, thus, by Proposition 2.5, $\mathcal{G}$ is a d-truncated Gröbner basis of $\langle f_1, \dots, f_s \rangle$ for $\prec$. □

2.2.2 The Sparse-FGLM algorithm

In this subsection, the input Gröbner basis, $\mathcal{G}_{\mathrm{DRL}}$ is the reduced Gröbner basis of a zero-dimensional I of degree D for $\prec_{\mathrm{DRL}}$. The output is the reduced Gröbner basis, $\mathcal{G}_{\mathrm{LEX}}$, of I for $\prec_{\mathrm{LEX}}$. In [19] and [20, Algorithm 3], using [28], the authors observe that the map

$$\begin{aligned} \mathbb{K}[\boldsymbol{x}]/I &\to \mathbb{K}[\boldsymbol{x}]/I \\ f &\mapsto \mathrm{NF}(x_n f, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}}) \end{aligned}$$

given in the basis $S_{\text{DRL}} = \text{Staircase}(\mathcal{G}_{\text{DRL}})$ is represented by a matrix, M_{x_n}, with a special structure given in the following two lemmas.

Lemma 2.8. *Let I be a zero-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$ of degree D, $\mathcal{G}_{\text{DRL}}$ be its reduced Gröbner basis for $\prec_{\text{DRL}}$ and $S_{\text{DRL}} = \{\sigma_0, \ldots, \sigma_{D-1}\}$ be its associated staircase. Let M_{x_n} be the matrix of the linear map $f \in \mathbb{K}[\boldsymbol{x}]/I \mapsto \text{NF}(x_n f, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}) \in \mathbb{K}[\boldsymbol{x}]/I$.*

Then, one can build the matrix $M_{x_n} = (m_{i,j})_{0\le i,j<N}$ with the following procedure:

- *if $x_n\sigma_j = \sigma_k$, then $m_{k,j} = 1$ and for all $0 \le i < D$, $i \ne k$, $m_{i,j} = 0$;*
- *otherwise for all $0 \le i < D$, $m_{i,j}$ is the coefficient of σ_i in $\text{NF}(x_n\sigma_j, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}})$.*

Proof. By construction, the matrix M_{x_n} has its jth column which is the vector of coefficients of $\text{NF}(x_n\sigma_j, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}})$ in the basis S_{DRL}.

The former case is immediate.

The latter case is obtained by linearity. □

Lemma 2.9 ([19, 20] using [28])**.** *Let $f_1, \ldots, f_n$ be generic polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ of degrees at most d. Let $\mathcal{G}_{\text{DRL}}$ be the reduced Gröbner basis of $\langle f_1, \ldots, f_n\rangle$ for $\prec_{\text{DRL}}$. Then, the latter case of Lemma 2.8 only happens if there exists $g \in \mathcal{G}_{\text{DRL}}$ such that $\text{LM}_{\prec_{\text{DRL}}}(g) = x_n\sigma_j$. As a consequence, one has $\text{NF}(x_n\sigma_j, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}) = x_n\sigma_j - g$.*

Proof. By the genericity assumption on $f_1, \ldots, f_n$, the ideal $\langle f_1, \ldots, f_n\rangle$ is complete intersection and zero-dimensional. Then, in [28], a description of S_{DRL} is given in that case: if $\sigma \in S_{\text{DRL}}$, then either $x_n\sigma \in S_{\text{DRL}}$ or $x_n\sigma \in \text{LM}_{\prec_{\text{DRL}}}(\mathcal{G}_{\text{DRL}})$, i.e. there exists $g \in \mathcal{G}_{\text{DRL}}$ such that $\text{LM}_{\prec_{\text{DRL}}}(g) = x_n\sigma$. □

Following, we can use Wiedemann algorithm [33] on M_{x_n} to recover its minimal polynomial. Furthermore, whenever the reduced Gröbner basis $\mathcal{G}_{\text{LEX}}$ for $\prec_{\text{LEX}}$ is in *shape position*, i.e. there exist $g_n, g_{n-1}, \ldots, g_1 \in \mathbb{K}[x_n]$ such that

$$\mathcal{G}_{\text{LEX}} = \{g_n(x_n), x_{n-1} - g_{n-1}(x_n), \ldots, x_1 - g_1(x_n)\},$$

and for all $1 \le k \le n-1$, $\deg g_k < \deg g_n$, then $g_1, \ldots, g_{n-1}$ can be computed by solving Hankel systems of size D. This can be done using the following two algorithms, Algorithm 2.2 and 2.3.

Proposition 2.10. *Let $M \in \mathbb{K}^{D\times D}$ be a matrix with s nonzero coefficients, $\boldsymbol{r} \in \mathbb{K}^D$ be a row-vector and $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{n-1} \in \mathbb{K}^D$ be n column-vectors. Then, Algorithm 2.2 is correct and computes the sequences $(\boldsymbol{r}M\mathbf{c}_0)_{0\le i<2D}$ and $(\boldsymbol{r}M\mathbf{c}_k)_{0\le i<D}$ for $1 \le k \le n-1$ in $O(sD + nD^2)$ operations in $\mathbb{K}$.*

Furthermore, if the vectors $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{n-1}$ are vectors of the canonical basis, then this complexity drops to $O((s+n)D)$.

Proof. The termination and the correctness of the algorithm are immediate. It remains to prove its complexity.

Each vector matrix product $\boldsymbol{r}M$ accounts for $O(s)$ operations in $\mathbb{K}$, hence computing them all requires $O(sD)$ operations.

Then, we need to perform the scalar products $\boldsymbol{r}\mathbf{c}_k$ for $0 \le k \le n-1$ at each step. Each one needs $O(D)$ operations. Hence a total of $O(nD^2)$ operations.

Input: A matrix $M \in \mathbb{K}^{D\times D}$, a row-vector $\boldsymbol{r} \in \mathbb{K}^D$ and n column-vectors $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{n-1} \in \mathbb{K}^D$

Output: $(\boldsymbol{r}M\mathbf{c}_0)_{0\le i<2D}, (\boldsymbol{r}M\mathbf{c}_1)_{0\le i<D}, \ldots, (\boldsymbol{r}M\mathbf{c}_{n-1})_{0\le i<D}$, with $\mathbf{1} = (1,0,\ldots,0)^{\mathrm{T}}$.

$w_0^{(0)} \coloneqq \boldsymbol{r}\mathbf{c}_0, w_0^{(1)} \coloneqq \boldsymbol{r}\mathbf{c}_1, \ldots, w_0^{(n-1)} \coloneqq \boldsymbol{r}\mathbf{c}_{n-1}$.

For i **from** 1 **to** $D-1$ **do**

- $\boldsymbol{r} \coloneqq \boldsymbol{r}M$.
- $w_i^{(0)} \coloneqq \boldsymbol{r}\mathbf{c}_0, w_i^{(1)} \coloneqq \boldsymbol{r}\mathbf{c}_1, \ldots, w_i^{(n-1)} \coloneqq \boldsymbol{r}\mathbf{c}_{n-1}$.

For i **from** D **to** $2D-1$ **do**

- $\boldsymbol{r} \coloneqq \boldsymbol{r}M$.
- $w_i^{(0)} \coloneqq \boldsymbol{r}\mathbf{c}_0$

Return $(w_i^{(0)})_{0\le i<2D}, (w_i^{(1)})_{0\le i<D}, \ldots, (w_i^{(n-1)})_{0\le i<D}$

Algorithm 2.2: Sequences for Sparse-FGLM

Observe that if $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{n-1}$ are vectors of the canonical basis, then these scalar products need, each, $O(1)$ operations, hence a total of $O(nD)$ operations. This concludes the proof. □

Input: Sequences $(w_i^{(0)})_{0\le i<2D-1}$ and $(w_i^{(k)})_{0\le i<D}$ for $1 \le k \le n-1$ with coefficients in $\mathbb{K}$.

Output: $\gamma_{0,k}, \ldots, \gamma_{D-1,k}$ for $1 \le k \le n-1$ such that for all $0 \le i < D$,
$w_i^{(k)} = \gamma_{D-1,k} w_{D-1+i}^{(0)} + \cdots + \gamma_{0,k} w_i^{(0)}$.

For k **from** 1 **to** $n-1$ **do**

- Solve the Hankel linear system

$$\begin{pmatrix} w_0^{(0)} & w_1^{(1)} & \cdots & w_{D-1}^{(0)} \\ w_1^{(0)} & w_2^{(1)} & \cdots & w_D^{(0)} \\ \vdots & \vdots & & \vdots \\ w_{D-1}^{(0)} & w_D^{(1)} & \cdots & w_{2D-2}^{(0)} \end{pmatrix} \begin{pmatrix} \gamma_{0,k} \\ \gamma_{1,k} \\ \vdots \\ \gamma_{D-1,k} \end{pmatrix} = \begin{pmatrix} w_0^{(k)} \\ w_1^{(k)} \\ \vdots \\ w_{D-1}^{(k)} \end{pmatrix}.$$

Return $\gamma_{i,k}$ for $0 \le i < D$ and $1 \le k \le n-1$.

Algorithm 2.3: Hankel system solving for Sparse-FGLM

Proposition 2.11. *Let $(w_i^{(0)})_{0\le i<2D-1}(w_i^{(1)})_{0\le i<D}, \ldots, (w_i^{(n-1)})_{0\le i<D}$ be sequences such that $(w_i^{(0)})_{0\le i<2D-1}$ is linear recurrent of order D, then Algorithm 2.3 is correct and computes, for all $1 \le k \le n-1$, $\gamma_{0,k}, \ldots, \gamma_{D-1,k}$ such that*

$$\forall\, 0 \le i < D,\ w_i^{(k)} = \gamma_{D-1,k} w_{D-1+i}^{(0)} + \cdots + \gamma_{0,k} w_i^{(0)}$$

in $O(\mathsf{M}(D)(n + \log D))$ operations, where $\mathsf{M}(D)$ denote a cost function for multiplying univariate polynomials of degree D with coefficients in $\mathbb{K}$.

Proof. The termination of the algorithm is immediate. Since $(w_i^{(0)})_{0\le i<2D-1}$ is linear recurrent of order D, then the Hankel matrix on line 2 is invertible, see [8] or for instance the proof of [5, Th. 3.2], thus the algorithm is correct.

Concerning the complexity, using [8], we can compute a representation of this inverse in $O(\mathsf{M}(D)\log D)$ operations in $\mathbb{K}$. Then, multiplying this representation of this inverse with the right-hand side member of the equality requires $O(\mathsf{M}(D))$ operations in $\mathbb{K}$. Hence a total of $O(\mathsf{M}(D)(n+\log D))$ operations in $\mathbb{K}$. □

We are now in a position to present the Sparse-FGLM algorithm in the shape position case.

Input: The reduced Gröbner basis $\mathcal{G}_{\text{DRL}}$ of a zero-dimensional ideal I for $\prec_{\text{DRL}}$ and its associated staircase S_{DRL} of size D.
Output: The reduced Gröbner basis of I for $\prec_{\text{LEX}}$, if it is in shape position.

Build the matrix M as in Lemma 2.8.
Pick $\boldsymbol{r}\in\mathbb{K}^D$ a row-vector at random.
$\mathbf{1} \coloneqq (1,0,\dots,0)^{\mathrm{T}}$. // the column-vector of coefficients of $\mathrm{NF}\,(1,\mathcal{G}_{\text{DRL}},\prec_{\text{DRL}})$
For k **from** 1 **to** $n-1$ **do**
  Build $\mathbf{c}_k$ the column-vector of coefficients of $\mathrm{NF}\,(x_k,\mathcal{G}_{\text{DRL}},\prec_{\text{DRL}})$.
Compute $(w_i^{(0)})_{0\le i<2D},(w_i^{(1)})_{0\le i<D},\dots,(w_i^{(n-1)})_{0\le i<D})$ with Algorithm 2.2 called on $M,\boldsymbol{r},\mathbf{1},\mathbf{c}_1,\dots,\mathbf{c}_{n-1}$.
$g_n \coloneqq$ Berlekamp–Massey$(w_0^{(0)},\dots,w_{2D-1}^{(0)})$.
If $\deg g_n < D$ **then Return** "Not in shape position or bad vector".
Compute $g_1 \coloneqq \gamma_{D-1,1}x_n^{D-1}+\dots+\gamma_{0,1},\dots,g_{n-1}\coloneqq\gamma_{D-1,n-1}x_n^{D-1}+\dots+\gamma_{0,n-1}$ with Algorithm 2.3 called on $(w_i^{(0)})_{0\le i<2D-1},(w_i^{(1)})_{0\le i<D},\dots,(w_i^{(n-1)})_{0\le i<D})$.
Return $\{g_n(x_n),x_{n-1}-g_{n-1}(x_n),\dots,x_1-g_1(x_n)\}$.

Algorithm 2.4: Sparse-FGLM

Theorem 2.12. *Let I be a zero-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$ of degree D, $\mathcal{G}_{\text{DRL}}$ be its reduced Gröbner basis for $\prec_{\text{DRL}}$ and S_{DRL} be its associated staircase. Let M_{x_n} be the matrix of the map $f\in\mathbb{K}[\boldsymbol{x}]/I\mapsto \mathrm{NF}\,(x_nf,\mathcal{G}_{\text{DRL}},\prec_{\text{DRL}})\in\mathbb{K}[\boldsymbol{x}]/I$ in the monomial basis S_{DRL}.*

Let us assume that there are t monomials σ in S_{DRL} such that $x_n\sigma\in\mathrm{LT}_{\prec_{\text{DRL}}}(I)$ and that $x_1,\dots,x_{n-1}\in S_{\text{DRL}}$, that M_{x_n} is known and that the reduced Gröbner basis $\mathcal{G}_{\text{LEX}}$ of I for $\prec_{\text{LEX}}$ is in shape position. Then, one can compute $\mathcal{G}_{\text{LEX}}$ in $O(tD^2+n\mathsf{M}(D))$ operations, where $\mathsf{M}(D)$ denote a cost function for multiplying univariate polynomials of degree D with coefficients in $\mathbb{K}$.

Proof. Taking the column-vector $\mathbf{1}=(1,0,\dots,0)^{\mathrm{T}}$ so that for all $i\in\mathbb{N}$, $M_{x_n}^i\mathbf{1}$ is the vector of coefficients in S_{DRL} of $\mathrm{NF}\left(x_n^i,\mathcal{G}_{\text{DRL}},\prec_{\text{DRL}}\right)$, we can pick at random a row-vector $\boldsymbol{r}$ to compute the sequence $\boldsymbol{w}^{(0)}=(w_i^{(0)})_{0\le i<2D}=\left(\boldsymbol{r}M_{x_n}^i\mathbf{1}\right)_{0\le i<2D}$. Generically, the linear recurrence relation of minimal order satisfied by this sequence

$$\forall\, i\in\mathbb{N},\ w_{i+d}^{(0)}+c_{d-1}w_{i+d-1}^{(0)}+\dots+c_0w_i^{(0)}=0,$$

is such that $g_n = x_n^d + c_{d-1}x_n^{d-1} + \cdots + x_0$ is the minimal polynomial of M_{x_n}.

Let us assume that $\mathcal{G}_{\text{LEX}}$ is in shape position, then there exist $\gamma_{0,k}, \ldots, \gamma_{D-1,k}^{D-1}$ in $\mathbb{K}$ such that $x_k - \gamma_{D-1,k}^{D-1} x_n^{D-1} - \cdots - \gamma_{0,k} = 0$ in $\mathbb{K}[\boldsymbol{x}]/I$. Since $M_{x_n}^d \mathbf{c}_k$ is the vector of coefficients of $\text{NF}\left(x_n^d x_k, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)$, by multiplying on the left $M_{x_n}^d \mathbf{c}_k$ by $\boldsymbol{r} M_{x_n}^i$ for all $0 \leq d \leq D-1$, we obtain

$$\forall\, 0 \leq i < D,\ w_i^{(k)} = \gamma_{D-1,k} w_{D-1+i}^{(0)} + \cdots + \gamma_{0,k} w_i^{(0)}.$$

Hence the algorithm is correct and terminates. Observe that if $\deg g_n < D$, then $\mathcal{G}_{\text{LEX}}$ is not in shape position and the algorithm is still correct to return the error message.

It remains to prove the complexity statement. By assumption, $x_1, \ldots, x_{n-1} \in S_{\text{DRL}}$, hence $1 \in S_{\text{DRL}}$ and $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{n-1}$ are vectors of the canonical basis. Moreover, there are t monomials σ in S_{DRL} such that $x_n\sigma \in \text{LT}_{\prec_{\text{DRL}}}(I)$, hence M_{x_n} has at most $tD + (D-t) = O(tD)$ nonzero coefficients. Observe that among these t monomials, there must be a pure power of each x_k, for $1 \leq k \leq n-1$, which is not 1, hence $t > n$. Therefore, by Proposition 2.10, the call to Algorithm 2.2 requires $O(tD^2 + nD) = O(tD^2)$ operations.

Now, using fast variants [8] of the Berlekamp–Massey algorithm [2, 27], one recover the minimal linear recurrence relation in $O(\mathsf{M}(D)\log D)$ operations. Finally, by Proposition 2.11, we can compute $g_1, \ldots, g_n$ in $O(\mathsf{M}(D)(n + \log D))$ operations.

All in all, we have a complexity in $O(tD^2 + n\mathsf{M}(D))$ operations in $\mathbb{K}$. □

Note that the Berlekamp–Massey algorithm and its faster variants return a factor of g_n, so if the computed polynomial has degree D, i.e. it is the characteristic polynomial of M_{x_n}, then it is also its minimal polynomial. Furthermore, based on a deterministic variant of Wiedemann's algorithm, one can also provide a deterministic variant of this algorithm to recover g_n [20, Algorithm 4].

Remark 2.13. *In [6, 22], the authors consider the case where an ideal J is not in shape position but its radical $\sqrt{J}$ is. Let us recall that $\sqrt{J} = \left\{f \in \mathbb{K}[\boldsymbol{x}] \,\middle|\, \exists k \in \mathbb{N}, f^k \in J\right\}$, see [11, Chap. 4, Sec. 2, Def. 4]. In that case, the lexicographic Gröbner basis of $\sqrt{J}$ can be computed in a similar fashion, it suffices to replace the call to Algorithm 2.3 on line 9 by a call to [22, Algorithm 2].*

3 The $\mathbf{F_4}$SAT algorithm for saturated ideals

This section is devoted to the design of an algorithm which on input $f_1, \ldots, f_s$ and φ in $\mathbb{K}[\boldsymbol{x}]$ computes a Gröbner basis of $I : \langle\varphi\rangle^\infty$ for a total degree monomial ordering $\prec$, typically $\prec_{\text{DRL}}$, where $I = \langle f_1, \ldots, f_s\rangle$. As explained earlier, this algorithm modifies the F_4 algorithm [14] to discover on the fly polynomials in $I : \langle\varphi\rangle^\infty$ as early as possible during the computation. The use of the $\prec_{\text{DRL}}$ ordering allows us to obtain these polynomials of lowest possible degree early in the computation.

3.1 Description of the $\mathbf{F_4}$SAT algorithm

From Lemma 2.7, after the first step of the F_4 algorithm in degree d, if no new polynomial of degree at most d is discovered, then the current Gröbner basis $\mathcal{G}$ is a d-truncated

Gröbner basis of I for $\prec$. Therefore, we have a partial information on the staircase of I, and thus of $I : \langle\varphi\rangle^\infty$, for $\prec$ since we know monomials that are outside of this staircase. The F_4SAT algorithm searches for polynomials in $I : \langle\varphi\rangle^\infty$ whose supports are entirely included in the given staircase using the fact that $(I : \langle\varphi\rangle^\infty) : \langle\varphi\rangle = I : \langle\varphi\rangle^\infty$. If new polynomials are found, they are added to $\mathcal{G}$ and the necessary critical pairs are added to the set of pairs to handle. Then, we resume the F_4 algorithm.

The search of new polynomials is done through linear algebra computations. From a d-truncated Gröbner basis of an ideal J, we compute $\mathrm{NF}(\sigma\varphi, \mathcal{G}, \prec)$ for all monomials σ in the associated staircase S_d of degree at most d. Then, we search for vanishing linear combinations thereof. Indeed, if

$$\mathrm{NF}(s\varphi, \mathcal{G}, \prec) - \sum_{\substack{\sigma\in S_d\\ \sigma\prec s}} c_\sigma \,\mathrm{NF}(\sigma\varphi, \mathcal{G}, \prec) = 0,$$

then $\left(s - \sum_{\sigma\in S_d, \sigma\prec s} c_\sigma \sigma\right)\varphi \in J$. This yields Algorithm 3.1.

Input: A list of polynomials $f_1, \ldots, f_s$ spanning an ideal $I \subseteq \mathbb{K}[\boldsymbol{x}]$, a polynomial $\varphi \in \mathbb{K}[\boldsymbol{x}]$ and a total degree monomial ordering $\prec$.

Output: A Gröbner basis $\mathcal{G}$ of $I : \langle\varphi\rangle^\infty$ for $\prec$.

$\mathcal{G} \coloneqq \{f_1, \ldots, f_s\}$
$P \coloneqq \{(f_i, f_j) \mid 1 \leq i < j \leq s\}$
While $P \neq \emptyset$ **do**
  Choose a subset L of P.
  $P \coloneqq P \setminus L$.
  $L \coloneqq \mathrm{SymbolicPreprocessing}(L, \mathcal{G})$.
  $L \coloneqq \mathrm{LinearAlgebra}(L)$.
  For $h \in L$ *with* $\mathrm{LM}_\prec(h) \notin \langle \mathrm{LM}_\prec(\mathcal{G})\rangle$ **do**
    $P \coloneqq \{(g, h) | g \in \mathcal{G}\}$.
    $\mathcal{G} \coloneqq \mathcal{G} \cup \{h\}$.
  If $\mathcal{G}$ *was augmented* **then** // New information on $\langle \mathrm{LM}_\prec(I : \langle\varphi\rangle^\infty)\rangle$
    For $\sigma \notin \mathrm{LM}_\prec(\mathcal{G})$ *and* $\deg \sigma \leq \max_{g\in\mathcal{G}\cup\{\varphi\}} \deg g$ **do**
      $q_\sigma \coloneqq \mathrm{NF}(\sigma\varphi, \mathcal{G}, \prec)$.
    Build the matrix M whose rows are given by polynomials q_σ and columns by each monomials in their support in decreasing order.
    Compute a lower triangular basis B of the left-kernel of M.
    For each $b \in B$ **do**
      $h \coloneqq \sum_{\sigma\notin\langle \mathrm{LM}_\prec(\mathcal{G})\rangle} b_\sigma \sigma$, whose vector of coefficients is b, to $\mathcal{G}$.
      $P \coloneqq \{(g, h) \mid g \in \mathcal{G}\}$.
      $\mathcal{G} \coloneqq \mathcal{G} \cup \{h\}$.
Return $\mathcal{G}$.

Algorithm 3.1: F_4SAT

Theorem 3.1. *Let $f_1, \dots, f_s$ be a generating family of an ideal $I \subseteq \mathbb{K}[\boldsymbol{x}]$, $\varphi \in \mathbb{K}[\boldsymbol{x}]$ be a polynomial and $\prec$ be a total degree monomial ordering. Then, Algorithm 3.1 terminates and returns a Gröbner basis of $I : \langle\varphi\rangle^\infty$ for $\prec$.*

3.2 Proof of termination and correctness

Lemma 3.2. *Let I and J be two ideals of $\mathbb{K}[\boldsymbol{x}]$ such that $I \subseteq J$ and $\mathcal{G}$ and $\mathcal{H}$ be their respective reduced Gröbner bases for a common monomial order $\prec$. Let S and T be the associated staircases to $\mathcal{G}$ and $\mathcal{H}$. Then, $T \subseteq S$. Furthermore, there exist $h_1, \dots, h_r$, such that for all i, $\operatorname{supp} h_i \subseteq S$ and $J = I + \langle h_1, \dots, h_r\rangle$.*

Proof. Let $\mathcal{G} = \{g_1, \dots, g_t\}$. By definition of a Gröbner basis, for all $f \in I$, there exists $1 \le i \le r$ such that $\textsc{lm}_\prec(g_i) \mid \textsc{lm}_\prec(f)$. Since $I \subseteq J$, then $f \in J$ and there also exists $h \in \mathcal{H}$ such that $\textsc{lm}_\prec(h) \mid \textsc{lm}_\prec(f)$, hence $\textsc{lm}_\prec(I) \subseteq \textsc{lm}_\prec(J)$. By definition, S (resp. T) is the complement of $\textsc{lm}_\prec(I)$ (resp. $\textsc{lm}_\prec(J)$) in the set of monomials, hence $T \subseteq S$.

Since $I \subseteq J$, there exist $f_1, \dots, f_r$ such that $J = I + \langle f_1, \dots, f_r\rangle$. Thus, $J = \langle g_1, \dots, g_t, f_1, \dots, f_r\rangle$. By the definition of $\mathcal{G}$ being a Gröbner basis of I for $\prec$, for all $1 \le j \le r$, we have $f_j = q_{j,1}g_1 + \cdots + q_{j,t}g_t + \mathrm{NF}(f_j, \mathcal{G}, \prec) \in J$. Since $\mathrm{NF}(f_j, \mathcal{G}, \prec)$ has no monomial divisible by $\textsc{lm}_\prec(g)$, for $g \in \mathcal{G}$, its support is a subset of S. Thus, taking $h_j = \mathrm{NF}(f_j, \mathcal{G}, \prec)$, we have $\operatorname{supp} h_j \in S$ and $J = I + \langle h_1, \dots, h_r\rangle$. □

We will apply Lemma 3.2 with $J = I : \langle\varphi\rangle$, thus, by definition of $I : \langle\varphi\rangle$, we also know that for all $1 \le j \le r$, $h_j\varphi$ is in I. Moreover, h_j is a polynomial whose support is in S, thus it can be written as $h_j = s - \sum_{\sigma\in S, \sigma\prec s} c_\sigma\sigma$, with $s \in S$ and c_σ's in $\mathbb{K}$. Since $h_j\varphi \in I$, we know that

$$\mathrm{NF}(h_j\varphi, \mathcal{G}, \prec) = 0 \quad \text{and} \quad \mathrm{NF}(s\varphi, \mathcal{G}, \prec) = \sum_{\substack{\sigma\in S\\ \sigma\prec s}} c_\sigma \,\mathrm{NF}(\sigma\varphi, \mathcal{G}, \prec).$$

From Lemma 3.2, we deduce a superset of the support of the polynomials in the reduced Gröbner basis of $I : \langle\varphi\rangle^\infty$ for $\prec$ from the staircase S of I for $\prec$. Yet, if S is not finite, it is not clear up to which degree we need to search for polynomials in $I : \langle\varphi\rangle^\infty$. This is given by the following results.

Lemma 3.3. *Let $\prec$ be a total degree monomial ordering. Let $\{g_1, \dots, g_r\}$ be a Gröbner basis of an ideal $I \subseteq \mathbb{K}[\boldsymbol{x}]$, for $\prec$. Then, no polynomial in the reduced Gröbner basis of $I : \langle x_n\rangle^\infty$ for $\prec$ has a degree which is larger than $\max_{1\le i\le r} \deg g_i$.*

Proof. By [11, Chap. 8, Sec. 4, Proof of Th. 4], homogenezing $g_1, \dots, g_r$ with variable x_0 yields a homogeneous Gröbner basis $\{g_1^{\mathrm{h}}, \dots, g_r^{\mathrm{h}}\}$ for $\prec$ with $x_0 \prec x_n \prec \cdots \prec x_1$ of the homogeneous ideal $I^{\mathrm{h}} = \langle f^{\mathrm{h}} \mid f \in I\rangle$. Thus, the Hilbert series $\mathrm{HS}_{\mathbb{K}[x_0,\boldsymbol{x}]/I^{\mathrm{h}}}(t)$ of $\mathbb{K}[x_0, \boldsymbol{x}]/I^{\mathrm{h}}$ equals the Hilbert series $\mathrm{HS}_{\mathbb{K}[x_0,\boldsymbol{x}]/I}(t)$ of $\mathbb{K}[x_0, \boldsymbol{x}]/I$ divided by $1 - t$:

$$\mathrm{HS}_{\mathbb{K}[x_0,\boldsymbol{x}]/I^{\mathrm{h}}}(t) = \frac{\mathrm{HS}_{\mathbb{K}[x_0,\boldsymbol{x}]/I}(t)}{1-t} = \mathrm{HS}_{\mathbb{K}[x_0,\boldsymbol{x}]/I}(t) \sum_{i\ge 0} t^i.$$

Let $\prec_2$ be a total degree monomial ordering such that $x_n \prec_2 \cdots \prec_2 x_1 \prec_2 x_0$ and let $\mathcal{G}_2 = \{\tilde{g}_1^{\mathrm{h}}, \dots, \tilde{g}_s^{\mathrm{h}}\}$ be a Gröbner basis of I^{h} for $\prec_2$. By [11, Chap. 10, Sec. 2, Prop. 8], the Hilbert series of the quotient ring $\mathbb{K}[x_0, \boldsymbol{x}]/I^{\mathrm{h}}$ only depends on I^{h} and not on the chosen total degree monomial ordering. From $\mathrm{HS}_{\mathbb{K}[x_0,\boldsymbol{x}]/I^{\mathrm{h}}}(t)$, we deduce

$$\max_{1\leq i\leq r} \deg g_i = \max_{1\leq i\leq r} \deg g_i^{\mathrm{h}} = \max_{1\leq j\leq s} \deg \tilde{g}_j^{\mathrm{h}}.$$

Finally, using Bayer's algorithm [1, p. 120], we can compute a Gröbner basis of $I^{\mathrm{h}} : \langle x_n\rangle^\infty$ for $\prec_2$ from $\mathcal{G}_2$ as follows: for each $g \in \mathcal{G}_2$, find the largest integer k such that x_n^k divides g and take $\frac{g}{x_n^k}$. Then, we can obtain a Gröbner basis of $I : \langle x_n\rangle^\infty$ for $\prec_2$ by dehomogenizing the resulting polynomials, i.e. by setting x_0 to 1. Thus no polynomial in this Gröbner basis has degree larger than $\max_{1\leq j\leq s} \deg \tilde{g}_j^{\mathrm{h}} = \max_{1\leq i\leq r} \deg g_i$. □

Theorem 3.4. *Let $\prec$ be a total degree monomial ordering. Let $\mathcal{G} = \{g_1, \ldots, g_r\}$ be a Gröbner basis of an ideal $I \subseteq \mathbb{K}[\boldsymbol{x}]$ for $\prec$. Let $\varphi \in \mathbb{K}[\boldsymbol{x}]$.*

Then, no polynomial in the reduced Gröbner basis of $I : \langle\varphi\rangle^\infty$ has a degree which is larger than $\max_{1\leq i\leq r} \deg g_i$ *and* $\deg \mathrm{NF}(\varphi, \mathcal{G}, \prec)$.

Proof. By the definition of a Gröbner basis, there exist polynomials $q_1, \ldots, q_r$ such that $\varphi = q_1 g_1 + \cdots + q_r g_r + \psi$ and $\psi = \mathrm{NF}(\varphi, \mathcal{G}, \prec)$. Then, a polynomial h is in $I : \langle\varphi\rangle$ if, and only if, $h\varphi$ is in I. Thus, this is equivalent to requiring that $h\psi$ is in I. In other words, $I : \langle\varphi\rangle = I : \langle\psi\rangle$ and $I : \langle\varphi\rangle^\infty = I : \langle\psi\rangle^\infty$.

Now, let us denote $g_{r+1} = x_{n+1}^d - \psi$, where x_{n+1} is a new indeterminate and $d = \deg\psi$. Then, its leading monomial for $\prec$ with $x_n \prec \cdots \prec x_1 \prec x_{n+1}$ is x_{n+1}^d. Since $g_1, \ldots, g_r$ do not involve x_{n+1}, their leading monomials are exactly the same as those for $\prec$ with $x_n \prec \cdots \prec x_1$. By Buchberger's second criterion [11, Chap. 2, Sec. 9, Prop. 4], adding g_{r+1} to $\mathcal{G}$ does not create new critical pairs. Since $\mathcal{G}$ is already a Gröbner basis of I for $\prec$ with $x_n \prec \cdots \prec x_1$, by Buchberger's first criterion [11, Chap. 2, Sec. 6, Th. 6], $\mathcal{H} = \{g_1, \ldots, g_r, g_{r+1}\}$ is also a Gröbner basis of $J = I + \langle x_{n+1}^d - \psi\rangle$ for $\prec$ with $x_n \prec \cdots \prec x_1 \prec x_{n+1}$.

Furthermore, saturating I by ψ is equivalent to saturating J by ψ (resp. x_{n+1}^d, resp. x_{n+1}) and then eliminating x_{n+1}. Finally, using Lemma 3.3 on the ideal J, the Gröbner basis $\mathcal{H}$, and the monomial ordering $\prec$ with $x_n \prec \cdots \prec x_1 \prec x_{n+1}$, we deduce that no polynomial in the Gröbner basis of $J : \langle x_{n+1}\rangle^\infty$ has degree larger than $\max_{1\leq i\leq r+1} \deg g_i$. □

We are now in a position to prove Theorem 3.1.

Proof. of Theorem 3.1 At the first round of the while loop, $\mathcal{G}$ contains a generating family of $I \subseteq I : \langle\varphi\rangle^\infty$.

Let us assume that at each round of the while loop, $\mathcal{G}$ starts by containing a generating family of an ideal $J \subseteq I : \langle\varphi\rangle^\infty$. Then, at the end of the round, it contains a generating family of an ideal K with $J \subseteq K \subseteq J : \langle\varphi\rangle$. Since $J \subseteq I : \langle\varphi\rangle^\infty$, then $K \subseteq J : \langle\varphi\rangle \subseteq (I : \langle\varphi\rangle^\infty) : \langle\varphi\rangle = I : \langle\varphi\rangle^\infty$.

Thus, by recurrence and the fact that $\mathbb{K}[\boldsymbol{x}]$ is Noetherian, this sequence of ideals must stabilize to an ideal that is included in $I : \langle\varphi\rangle^\infty$ so that the loop terminates. Furthermore, by Buchberger's first criterion [11, Chap. 2, Sec. 6, Th. 6], the output family is a Gröbner basis for $\prec$ of the ideal it spans.

By the correctness of the F_4 algorithm, the F_4SAT algorithm computes a Gröbner basis for $\prec$ of an ideal J containing I. Moreover, by Theorem 3.4, we know that if $\mathcal{G}$ is a Gröbner basis, then the given bound is enough to retrieve a Gröbner basis of $\langle\mathcal{G}\rangle : \langle\varphi\rangle^\infty$ and thus of $\langle\mathcal{G}\rangle : \langle\varphi\rangle$. Furthermore, at each round of the loop, $\mathcal{G}$ is a d-truncated Gröbner basis for some d and the algorithm adds polynomials h of degree at most d such that φh is the ideal spanned by the current set $\mathcal{G}$. Therefore, the algorithm can only terminates if J is saturated by φ, that is $J : \langle\varphi\rangle = J$.

Since $I : \langle\varphi\rangle^\infty$ is the smallest ideal containing I and saturated by φ, we conclude that $J = I : \langle\varphi\rangle^\infty$. □

3.3 Practical optimization

As we shall see in Section 5, the most expensive step of F_4SAT is the last saturation step, that is checking on line 15 that no new polynomial in the saturated ideal can be formed thanks to the monomials in the discovered staircase of the computed Gröbner basis $\mathcal{G}$. To bypass this, whenever we detect that $I : \langle\varphi\rangle^\infty$ is zero-dimensional, we rely on the following trick to determine if we have computed a Gröbner basis of $I : \langle\varphi\rangle^\infty$: From the geometric point of view, the variety defined by $I : \langle\varphi\rangle^\infty$ is the Zariski closure of the variety defined by I to which the variety defined by φ is removed. If this resulting variety is a finite set of points, then none of them can lie on the hypersurface defined by φ. Thus the intersection of this set of points and this hypersurface is empty. Algebraically, this means that $(I : \langle\varphi\rangle^\infty) + \langle\varphi\rangle = \langle 1\rangle$. Hence, we add φ to $\mathcal{G}$ and run the F_4 algorithm. If the output is indeed 1, then the saturation has already been computed.

Furthermore, the search of new polynomials in the saturated ideal need not be performed as soon as possible. As an optimization, we can decide to perform it after a given number of steps of the F_4 algorithm, so that the new information on the staircase increases the probability to find new polynomials in the saturated ideal. Furthermore, if we target specifically small degree polynomials, we can require to only compute the q_σ for small degree σ's compared to the degrees of th polynomials in $\mathcal{G}$ on line 13. Then, when no new polynomials are found and the set of critical pairs is empty, we can compute all the q_σ to ensure the correctness of the algorithm and the output.

When the base field is the field of rational numbers, a practical efficient implementation of the F_4SAT algorithm requires a multi-modular approach. Like for the F_4 algorithm, we can use a tracing algorithm [3] where we *learn* from the first modular steps and *apply* optimal computations in the following modular steps.

In contrast to F_4 we cannot learn all information needed for optimal runs of F_4SAT in the first modular run: Observe that on line 13, the normal form q_σ can be computed iteratively to increase the usage of already pre-reduced data from lower degrees: If q_σ was computed in a previous turn, we reduce it w.r.t. to the new $\mathcal{G}$ and $\prec$. Though, modulo the first prime p_1, we cannot learn how these iterative reductions are performed, since there might be useless saturation steps. Since these are skipped in the following modular steps, we cannot predict, during the computation modulo p_1, the normal form computations modulo other primes. However, these reductions can be learnt from the computations modulo p_2, the second modular step. Here we know exactly when we apply useful saturation steps, thus the normal form computations and its information stabilizes. This might also have an impact on the overall F_4 computation, thus we can only learn when to apply useful saturation steps modulo p_1. Only in the second modular step can we learn all the information for the complete computation.

The *tracing* of F_4SAT can now be described by three main steps:

1. In the *first* modular computation *learn*
   (a) when to apply a useful saturation step and
   (b) which F_4 matrices give new information for the basis.

   Since we cannot learn anything further for the F_4 computation we can apply probabilistic linear algebra to accelerate this step.

2. In the second modular computation *learn*
   (a) all polynomial data that is needed in the F_4 matrices to generate the non-zero information w.r.t. each corresponding matrix and
   (b) all polynomial data needed to apply the normal form computations in the useful saturation steps.

   In order to learn this data we have to apply exact linear algebra.

3. For all *successive* modular computations we can just *apply* the learnt data, no need of handling critical pairs or symbolic preprocessing. There will be no reductions to zero, all computational steps will be useful from now on.

In Section 5, the first learning phase, modulo p_1, is denoted by *learn 1*, the second one, modulo p_2, is denoted by *learn 2*. The apply phase, modulo $p_3, \ldots$, is denoted by *apply*.

4 Change of ordering algorithm for colon ideals

In this section, let I be an ideal of $\mathbb{K}[\boldsymbol{x}]$, let $\mathcal{G}_{\text{DRL}}$ be its reduced Gröbner basis for $\prec_{\text{DRL}}$ and S_{DRL} be its associated staircase and let φ be a polynomial. We assume that the colon ideal $I : \langle \varphi \rangle$ is zero-dimensional, thus $\varphi \notin I$, and that its lexicographic reduced Gröbner basis $\mathcal{H}_{\text{LEX}}$ is in *shape position*: There exist $h_1, \ldots, h_n \in \mathbb{K}[x_n]$, with $\deg h_k < \deg h_n$ for $1 \le k \le n-1$, such that

$$\mathcal{H}_{\text{LEX}} = \{h_n(x_n), x_{n-1} - h_{n-1}(x_n), \ldots, x_1 - h_1(x_n)\}\,.$$

We design a new algorithm to compute $\mathcal{H}_{\text{LEX}}$ from $\mathcal{G}_{\text{DRL}}$, even when I is positive-dimensional. Our approach is to build a matrix $\widetilde{M}_{x_n}$ so that applying Wiedemann's algorithm allows us to recover $\mathcal{H}_{\text{LEX}}$, similarly to the Sparse-FGLM algorithm [19, 20].

Firstly, we discuss the situation if I is zero-dimensional (Subsection 4.1). Next, we handle the case when I is positive-dimensional (Subsection 4.2). Subsection 4.3 focuses on the construction of the matrix $\widetilde{M}_{x_n}$, followed by possible optimizations in Subsection 4.4. Finally, in Subsection 4.5, we discuss how to handle the situation if the assumption that $\mathcal{H}_{\text{LEX}}$ is in shape position is dropped.

4.1 The case where I is zero-dimensional ideal

Let I be zero-dimensional of degree D. Thus, $I : \langle\varphi\rangle$ is also zero-dimensional, of degree $D' \leq D$. Let S_{DRL} be the staircase of I associated to $\mathcal{G}_{\text{DRL}}$ and let $\boldsymbol{\varphi}$ be the vector of coefficients of $\operatorname{NF}(\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}})$ in the basis given by S_{DRL}. Further, let M_{x_n} be the matrix of the map $f \in \mathbb{K}[\boldsymbol{x}]/I \mapsto \operatorname{NF}(x_n f, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}) \in \mathbb{K}[\boldsymbol{x}]/I$ in the basis S_{DRL}.

Lemma 4.1. *Let I be a zero-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$ of degree D, $\mathcal{G}_{\text{DRL}}$ be its reduced Gröbner basis for $\prec_{\text{DRL}}$ and S_{DRL} be the associated staircase. Let $\varphi \in \mathbb{K}[\boldsymbol{x}]\backslash I$ be such that $I : \langle\varphi\rangle$ is in shape position and let $\mathcal{H}_{\text{LEX}} = \{h_n(x_n), x_{n-1} - h_{n-1}(x_n), \ldots, x_1 - h_1(x_n)\}$ be the reduced Gröbner basis of $I : \langle\varphi\rangle$ for $\prec_{\text{LEX}}$, with $\deg h_n = D'$.*

Let M_{x_n} be the matrix of the map $f \in \mathbb{K}[\boldsymbol{x}]/I \mapsto \operatorname{NF}(x_n f, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}) \in \mathbb{K}[\boldsymbol{x}]/I$ in the basis S_{DRL} and $\boldsymbol{\varphi}$ be the vector of coefficients of φ in the basis S_{DRL}.

Then, for all $i \in \mathbb{N}$, $M_{x_n}^i \boldsymbol{\varphi}$ is the vector of coefficients of $\operatorname{NF}\left(x_n^i \varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)$.

Furthermore, let $\boldsymbol{r} \in \overline{\mathbb{K}}^D$ be a row-vector and $\boldsymbol{w} = (w_i)_{i\in\mathbb{N}} = (\boldsymbol{r} M_{x_n}^i \boldsymbol{\varphi})_{i\in\mathbb{N}}$. Let $d \in \mathbb{N}$ be minimal such that there exist $c_0, \ldots, c_{d-1} \in \mathbb{K}$ such that

$$\forall i \in \mathbb{N}, \quad w_{i+d} + c_{d-1} w_{i+d-1} + \cdots + c_0 w_i = 0.$$

Then, the polynomial $x_n^d + c_{d-1} x_n^{d-1} + \cdots + c_0$ divides h_n. Furthermore, if $\boldsymbol{r}$ is generic in $\overline{\mathbb{K}}^D$, then $d = D'$ and $h_n = x_n^d + c_{d-1} x_n^{d-1} + \cdots + c_0$.

Proof. Since $\boldsymbol{\varphi}$ is the vector of coefficients of φ in $\mathbb{K}[x_n]/I$, then by construction of M_{x_n}, $M_{x_n}\boldsymbol{\varphi}$ is the vector of coefficients of $\operatorname{NF}(x_n\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}})$ in $\mathbb{K}[x_n]/I$. By recurrence, we obtain the first statement.

Now, since $\mathbb{K}[\boldsymbol{x}]/I$ is finite-dimensional, there exists a smallest integer b such that $\boldsymbol{\varphi}, M_{x_n}\boldsymbol{\varphi}, \ldots, M_{x_n}^b \boldsymbol{\varphi}$ are not linearly independent. We let $a_0, \ldots, a_{b-1} \in \mathbb{K}$ such that

$$M_{x_n}^b \boldsymbol{\varphi} + a_{b-1} M_{x_n}^{b-1} + \cdots + a_0 \boldsymbol{\varphi} = 0.$$

Thus, $\operatorname{NF}\left(\left(x_n^b + a_{b-1} x_n^{b-1} + \cdots + a_0\right)\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right) = 0$ and the polynomial $(x_n^b + a_{b-1} x_n^{b-1} + \cdots + a_0)\varphi$ is in I. Hence, $\left(x_n^b + a_{b-1} x_n^{b-1} + \cdots + a_0\right) \in I : \langle\varphi\rangle$.

By the minimality of b, this ensures that $h_n = x_n^b + a_{b-1} x_n^{b-1} + \cdots + a_0$.

Now, multiplying the vector equality above by $\boldsymbol{r} M_{x_n}^i$ on the left yields

$$\forall\, i \in \mathbb{N},\ w_{i+b} + a_{b-1} w_{i+b-1} + \cdots + a_0 w_i = 0.$$

Thus, $\boldsymbol{w}$ is linearly recurrent of order at most b and $d \leq b$. Since linear recurrences are in one-to-one correspondence with polynomials, these polynomials define an ideal of $\mathbb{K}[x_n]$ spanned by $x_n^d + c_{d-1} x_n^{d-1} + \cdots + c_0$ that contains h_n. Hence the former divides the latter.

Following the proof of Wiedemann's algorithm [33], it suffices to take $\boldsymbol{r}$ outside finitely many vector subspaces of $\bar{\mathbb{K}}^D$ to recover the minimal polynomial of M_{x_n} instead of a proper factor thereof. Thus, for $\boldsymbol{r}$ generic, we actually compute h_n. □

Lemma 4.2. *Let I be a zero-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$ of degree D, $\mathcal{G}_{\text{DRL}}$ be its reduced Gröbner basis for $\prec_{\text{DRL}}$ and S_{DRL} be the associated staircase. Let $\varphi \in \mathbb{K}[\boldsymbol{x}]\backslash I$ be such that*

$I : \langle\varphi\rangle$ is in shape position and let $\mathcal{H}_{\text{LEX}} = \{h_n(x_n), x_{n-1} - h_{n-1}(x_n), \ldots, x_1 - h_1(x_n)\}$ be the reduced Gröbner basis of $I : \langle\varphi\rangle$ for $\prec_{\text{LEX}}$.

Let M_{x_n} be the matrix of the map $f \in \mathbb{K}[\boldsymbol{x}]/I \mapsto \operatorname{NF}(x_n f, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}) \in \mathbb{K}[\boldsymbol{x}]/I$ in the basis S_{DRL} and $\boldsymbol{\varphi}$ be the vector of coefficients of φ in the basis S_{DRL}.

Let $\boldsymbol{r} \in \overline{\mathbb{K}}^D$ be a generic row-vector and $\boldsymbol{w} = (w_i)_{i\in\mathbb{N}} = (\boldsymbol{r}M_{x_n}^i\boldsymbol{\varphi})_{i\in\mathbb{N}}$. Let $d \in \mathbb{N}$ be minimal such that there exist $c_0, \ldots, c_{d-1} \in \mathbb{K}$ such that

$$\forall i \in \mathbb{N}, \quad w_{i+d} + c_{d-1}w_{i+d-1} + \cdots + c_0 w_i = 0,$$

then $d = D'$ and $h_n = x_n^d + c_{d-1}x_n^{d-1} + \cdots + c_0$.

For all $1 \leq k \leq n-1$, let $\boldsymbol{\psi}_k$ be the vector of coefficients of $\operatorname{NF}(x_k\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}})$, then $M_{x_n}^i\boldsymbol{\psi}_k$ is the vector of coefficients of $\operatorname{NF}\left(x_n^i x_k\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)$ and there exist unique $\gamma_{0,k}, \ldots, \gamma_{D'-1,k} \in \mathbb{K}$ such that

$$\begin{pmatrix} w_0 & w_1 & \cdots & w_{D'-1} \\ w_1 & w_2 & \cdots & w_{D'} \\ \vdots & \vdots & & \vdots \\ w_{D'-1} & w_{D'} & \cdots & w_{2D'-2} \end{pmatrix} \begin{pmatrix} \gamma_{0,k} \\ \gamma_{1,k} \\ \vdots \\ \gamma_{D'-1,k} \end{pmatrix} = \begin{pmatrix} \boldsymbol{r}M_{x_n}^0\boldsymbol{\psi}_k \\ \boldsymbol{r}M_{x_n}^1\boldsymbol{\psi}_k \\ \vdots \\ \boldsymbol{r}M_{x_n}^{D'-1}\boldsymbol{\psi}_k \end{pmatrix},$$

and $h_k = \gamma_{D'-1,k}x_n^{D'-1} + \cdots + \gamma_{0,k}$.

Proof. The proof of the first statement is a direct consequence of the definition of M_{x_n}.

Now, since $\boldsymbol{r}$ is generic, then by Lemma 4.2, $d = D'$ and $\boldsymbol{w}$ does not satisfy any linear recurrence relation of order less than D'. Thus, there is no vector in the kernel of the above Hankel matrix, see [8].

Let $1 \leq k \leq n-1$ and $h_k(x_n) = \alpha_{D'-1,k}x_n^{D'-1} + \cdots + \alpha_{0,k}$, then $(x_k - h_k(x_n))\varphi$ is in I and $\operatorname{NF}((x_k - h_k(x_n))\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}) = 0$, hence

$$\boldsymbol{\psi}_k = \alpha_{D'-1,k}M_{x_n}^{D'-1}\boldsymbol{\varphi} + \cdots + \alpha_{0,k}\boldsymbol{\varphi}.$$

Now, multiplying this equality by $\boldsymbol{r}M_{x_n}^i$ for $0 \leq i \leq D'-1$ shows that $(\alpha_0, \ldots, \alpha_{D'-1})^{\mathrm{T}}$ is a solution of the above linear system. Since the matrix has full rank, the solution is unique and this ends the proof. □

From this, we deduce the following algorithm.

Remark 4.3. *Observe that line 6 of Algorithm 4.1 can lead to a large computational overhead whenever D is much larger than D'. This is the bottleneck of the algorithm.*

Mixing lines 6 and 7 so that the minimal linear recurrence relation is computed online during the computation of the terms $w_i^{(0)}$ ensures that only $O(D')$ of them are computed. Then, we can also compute only $O(D')$ terms $w_i^{(k)}$ for each $1 \leq k \leq n-1$.

Theorem 4.4. *Let I be a zero-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$ of degree D, $\mathcal{G}_{\text{DRL}}$ be its reduced Gröbner basis for $\prec_{\text{DRL}}$ and S_{DRL} be its associated staircase. Let M_{x_n} be the matrix of the map $f \in \mathbb{K}[\boldsymbol{x}]/I \mapsto \operatorname{NF}(x_n f, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}) \in \mathbb{K}[\boldsymbol{x}]/I$ in the monomial basis S_{DRL}. Let φ be a polynomial not in I, so that $I : \langle\varphi\rangle$ is zero-dimensional of degree D'.*

Let us assume that there are t monomials σ in S_{DRL} such that $x_n\sigma \in \operatorname{LT}_{\prec_{\text{DRL}}}(I)$, that M_{x_n} is known and that the reduced Gröbner basis $\mathcal{H}_{\text{LEX}}$ of I for $\prec_{\text{LEX}}$ is in shape position. Then, one can compute $\mathcal{H}_{\text{LEX}}$ by computing n normal forms w.r.t. $\mathcal{G}_{\text{DRL}}$ and $\prec_{\text{DRL}}$ and $O((t+n)DD')$ operations in $\mathbb{K}$.

Input: The reduced Gröbner basis $\mathcal{G}_{\text{DRL}}$ of a zero-dimensional ideal I for $\prec_{\text{DRL}}$, its associated staircase S_{DRL} of size D and a polynomial $\varphi \in \mathbb{K}[\boldsymbol{x}]$.

Output: The reduced Gröbner basis of $I : \langle \varphi \rangle$ for $\prec_{\text{LEX}}$, if it is in shape position.

```
Build the matrix M as in Lemma 2.8.
Pick r ∈ K^D a row-vector at random.
Build φ the column-vector of coefficients of NF(φ, G_DRL, ≺_DRL).
For k from 1 to n − 1 do
  └ Build ψ_k the column-vector of coefficients of NF(x_k φ, G_DRL, ≺_DRL).
Compute (w_i^(0))_{0≤i<2D}, (w_i^(1))_{0≤i<D}, ..., (w_i^(n−1))_{0≤i<D} with Algorithm 2.2 called on
  M, r, φ, ψ_1, ..., ψ_{n−1}.
h_n ← Berlekamp–Massey(w_0^(0), ..., w_{2D−1}^(0)), D' := deg h_n.
If NF(h_n φ, G_DRL, ≺_DRL) ≠ 0 then Return "Bad vector".
Compute h_1 := γ_{D'−1,1} x_n^{N−1} + ··· + γ_{0,1}, ..., h_{n−1} := γ_{D'−1,n−1} x_n^{N−1} + ··· + γ_{0,n−1} with
  Algorithm 2.3 called on (w_i^(0))_{0≤i<2D'−1}, (w_i^(1))_{0≤i<D'}, ..., (w_i^(n−1))_{0≤i<D'}.
For k from 1 to n − 1 do
  └ If NF((x_k − h_k(x_n))φ, G_DRL, ≺_DRL) ≠ 0 then Return "Not in shape position".
Return {h_n(x_n), x_{n−1} − h_{n−1}(x_n), ..., x_1 − h_1(x_n)}.
```

Algorithm 4.1: Sparse-FGLM for colon ideals

Proof. The proof follows the proof of Theorem 2.12.

Taking the column-vector $\boldsymbol{\varphi}$ so that for all $i \in \mathbb{N}$, $M_{x_n}^i \boldsymbol{\varphi}$ is the vector of coefficients in S_{DRL} of $\text{NF}\left(x_n^i, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)$, we can pick at random a row-vector $\boldsymbol{r}$ to compute the sequence $\boldsymbol{w} = (w_i^{(0)})_{0 \le i < 2D} = \left(\boldsymbol{r} M_{x_n}^i \mathbf{1}\right)_{0 \le i < 2D}$. Generically, the linear recurrence relation of minimal order satisfied by this sequence

$$\forall\, i \in \mathbb{N},\ w_{i+d}^{(0)} + c_{d-1} w_{i+d-1}^{(0)} + \cdots + c_0 w_i^{(0)} = 0,$$

is such that $h_n = x_n^d + c_{d-1} x_n^{d-1} + \cdots + x_0$ is the minimal polynomial of x_n in the quotient algebra $\mathbb{K}[\boldsymbol{x}]/(I : \langle \varphi \rangle)$, hence $d = D'$.

Let us assume that $\mathcal{H}_{\text{LEX}}$ is in shape position, then there exist $\gamma_{0,k}, \ldots, \gamma_{D'-1,k}$ in $\mathbb{K}$ such that $x_k - \gamma_{D'-1,k} x_n^{D'-1} - \cdots - \gamma_{0,k} = 0$ in $\mathbb{K}[\boldsymbol{x}]/(I : \langle \varphi \rangle)$. Since $M_{x_n}^j \mathbf{c}_k$ is the vector of coefficients of $\text{NF}\left(x_n^j x_k, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)$, by multiplying on the left $M_{x_n}^j \mathbf{c}_k$ by $\boldsymbol{r} M_{x_n}^i$ for all $0 \le j \le D' - 1$, we obtain

$$\forall\, 0 \le i < D,\ w_i^{(k)} = \gamma_{D'-1,k} w_{D'-1+i}^{(0)} + \cdots + \gamma_{0,k} w_i^{(0)}.$$

Hence the algorithm is correct and terminates. Observe that if $h_n \varphi$ is not in I, then h_n is not correctly computed and the algorithm correctly returns an error message. Likewise, if $\mathcal{H}_{\text{LEX}}$ is not in shape position, one of the computed polynomial $x_k - h_k(x_n)$ is not in $I : \langle \varphi \rangle$, hence multiplied by φ, it is not in I and the algorithm correctly returns an error message.

By assumption, there are t monomials σ in S_{DRL} such that $x_n \sigma \in \text{LT}_{\prec_{\text{DRL}}}(I)$, hence M_{x_n} has at most $tD + (D - t) = O(tD)$ nonzero coefficients. Therefore, by Proposition 2.10, the call to Algorithm 2.2 requires $O((t+n)D^2)$ operations.

Now, using fast variants [8] of the Berlekamp–Massey algorithm [2, 27], one recover the minimal linear recurrence relation in $O(\mathsf{M}(D)\log D)$ operations. Finally, by Proposition 2.11, we can compute $h_1,\dots,h_n$ in $O(\mathsf{M}(D)(n+\log D))$ operations.

All in all, we have a complexity in $O((t+n)D^2)$ operations in $\mathbb{K}$.

Using the modification of Remark 4.3, we can only compute $O(D')$ sequence terms $w_i^{(k)}$ for $0\leq k\leq n-1$ in $O((t+n)DD')$ operations. As a trade-off, the minimal recurrence relation is computed in $O(D'^2)$ operations but this is not the bottleneck. □

4.2 The case where I is positive-dimensional ideal

Now, let I be positive-dimensional, i.e. $\mathbb{K}[\boldsymbol{x}]/I$ is an infinite-dimensional vector space. Still, we assume that $I:\langle\varphi\rangle$ is zero-dimensional and in shape position with $\mathcal{H}_{\text{LEX}}=\{h_n(x_n),x_{n-1}-h_{n-1}(x_n),\dots,x_1-h_1(x_n)\}$ such that $\deg h_n=D'$.

To compute the polynomials $h_n,h_{n-1},\dots,h_1\in\mathbb{K}[x_n]$, we shall show that we can rely on linear algebra routines in a finite-dimensional vector subspace of $\mathbb{K}[\boldsymbol{x}]/I$. We start by defining such a vector subspace by giving a monomial basis thereof.

Lemma 4.5. *Let $\prec$ be a monomial ordering and I be an ideal of $\mathbb{K}[\boldsymbol{x}]$. Let $\mathcal{G}$ be the reduced Gröbner basis of I for $\prec$ and S be its associated staircase. Let $\varphi\in\mathbb{K}[\boldsymbol{x}]\setminus I$ be a polynomial and $1\leq k\leq n$ such that $J=(I:\langle\varphi\rangle)\cap\mathbb{K}[x_k,\dots,x_n]$ is zero-dimensional with staircase T for another monomial ordering $\prec_2$.*

Then, the set

$$\Sigma=\left\{\sigma\in S\;\middle|\;\exists s\in\bigcup_{\tau\in T}\operatorname{supp}\operatorname{NF}(\tau\varphi,\mathcal{G},\prec),\sigma\mid s\right\},$$

is a finite subset of S, which is a staircase as well, and is such that for all $(i_k,\dots,i_n)\in\mathbb{N}^{n-k+1}$, $\operatorname{supp}\operatorname{NF}\left(x_k^{i_k}\cdots x_n^{i_n}\varphi,\mathcal{G},\prec\right)\subseteq\Sigma$.

Proof. Since T is finite, then $\bigcup_{\tau\in T}\operatorname{supp}\operatorname{NF}(\tau\varphi,\mathcal{G},\prec)$ is a finite set of monomials. Since a monomial admits finitely many divisors, then Σ is finite.

Let t be a monomial not in T, then for each $\tau\in T$ such that $\tau\prec_2 t$, there exists $c_\tau\in\mathbb{K}$ such that $h=t-\sum_{\substack{\tau\in T\\ \tau\prec_2 t}}c_\tau\tau\in J$, that is $\operatorname{NF}(h\varphi,\mathcal{G},\prec)=0$. Then, by linearity

$$\operatorname{NF}(t\varphi,\mathcal{G},\prec)=\sum_{\tau\in T}c_\tau\operatorname{NF}(\tau\varphi,\mathcal{G},\prec),$$

and $\operatorname{supp}\operatorname{NF}(t\varphi,\mathcal{G},\prec)\subseteq\Sigma$. □

Remark 4.6. *By our assumptions, we can take $T=\left\{1,x_n,\dots,x_n^{D'-1}\right\}$ for $\prec_{\text{LEX}}$ so that*

$$\Sigma=\left\{\sigma\in S\;\middle|\;\exists s\in\bigcup_{i=0}^{D'-1}\operatorname{supp}\operatorname{NF}\left(x_n^i\varphi,\mathcal{G}_{\text{DRL}},\prec_{\text{DRL}}\right),\sigma\mid s\right\}.$$

Proposition 4.7. *Let I be a positive-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$, $\mathcal{G}_{\text{DRL}}$ be its reduced Gröbner basis for $\prec_{\text{DRL}}$ and S_{DRL} be its associated staircase. Let $\varphi \in \mathbb{K}[\boldsymbol{x}] \setminus I$ such that $I : \langle\varphi\rangle$ is zero-dimensional and in shape position. Let $\mathcal{H}_{\text{LEX}} = \{h_n(x_n), x_{n-1} - h_{n-1}(x_n), \dots, x_1 - h_1(x_n)\}$ be the reduced Gröbner basis of $I : \langle\varphi\rangle$ for $\prec_{\text{LEX}}$, with $\deg h_n = D'$.*

Let $\Sigma = \left\{\sigma \in S_{\text{DRL}} \,\middle|\, \exists s \in \bigcup_{i=0}^{D'-1} \operatorname{supp} \operatorname{NF}\left(x_n^i \varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right), \sigma \mid s\right\}$.

Then, there exist unique $c_0, \dots, c_{D'-1} \in \mathbb{K}$ and, for all $1 \leq k \leq n-1$, unique $\gamma_{0,k}, \dots, \gamma_{D'-1,k} \in \mathbb{K}$ such that

$$\begin{aligned}\operatorname{NF}\left(x_n^{D'}\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right) &= -c_{D'-1} \operatorname{NF}\left(x_n^{D'-1}\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right) \\ &\quad - \cdots - c_0 \operatorname{NF}\left(\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right), \\ \operatorname{NF}\left(x_k\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right) &= \gamma_{D'-1,k} \operatorname{NF}\left(x_n^{D'-1}\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right) \\ &\quad + \cdots + \gamma_{0,k} \operatorname{NF}\left(\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right),\end{aligned}$$

and all these vectors lie in the vector space spanned by Σ.

Furthermore, $h_n = x_n^{D'} + c_{D'-1}x_n^{D'-1} + \cdots + c_0$ and for all $1 \leq k \leq n-1$, we have $h_k = \gamma_{D'-1,k}x_n^{D'-1} + \cdots + \gamma_{0,k}$.

Proof. By assumption, $\mathcal{H}_{\text{LEX}}$ is in shape position, hence $T_{\text{LEX}} = \left\{1, x_n, \dots, x_n^{D'-1}\right\}$ is a monomial basis of $\mathbb{K}[\boldsymbol{x}]/(I : \langle\varphi\rangle)$. Thus, there exist unique $c_0, \dots, c_{D'-1} \in \mathbb{K}$ and for all $1 \leq k \leq D'-1$, unique $\gamma_{0,k}, \dots, \gamma_{D'-1,k}$ such that $h_n = x_n^{D'} + c_{D'-1}x_n^{D'-1} + \cdots + c_0$ and for all $1 \leq k \leq n-1$, $h_k = \gamma_{D'-1,k}x_n^{D'-1} + \cdots + \gamma_{0,k}$.

Now, multiplying h_n and $x_k - h_k$ by φ makes these polynomials lie in I. Hence the equality on the normal forms. Now, they all have their support in Σ, hence they lie in the vector space spanned by Σ. □

As a consequence, we can compute $h_n, h_{n-1}, \dots, h_1$ by means of Gaussian elimination in the vector space spanned by Σ.

Remark 4.8. *Observe that whenever $\operatorname{supp} \varphi$ is much larger than $\bigcup_{g \in \mathcal{G}_{\text{DRL}}} \operatorname{supp} g$, its support might already be large enough to define Σ, or a subset Σ' thereof such that the vector space it spans allows us to recover $h_n, h_{n-1}, \dots, h_1$ by Gaussian elimination. Furthermore, testing effectively the correctness of the computed polynomials can be done via multiplying $h_n(x_n)$ (resp. $x_k - h_k(x_n)$ for $1 \leq k \leq n-1$) by φ and checking if its normal form w.r.t. $\mathcal{G}_{\text{DRL}}$ and $\prec_{\text{DRL}}$ is 0.*

Otherwise, Σ' was too small. We can enlarge it by adding the missing monomials of $\operatorname{supp} \operatorname{NF}\left(x_n\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)$ and their divisors, iterating this process further.

4.3 Building the multiplication matrix

Let W be the vector subspace of $\mathbb{K}[\boldsymbol{x}]/I$ whose monomial basis is Σ. The goal is to build a matrix $\tilde{M}_{x_n}$ of a linear map from W to itself allowing us to compute $h_n, h_{n-1}, \dots, h_1$. The image of the map $f \in W \mapsto \operatorname{NF}\left(x_n f, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right) \in \mathbb{K}[\boldsymbol{x}]/I$ need not be in W. Thus we compose it with the projection π_W onto W, which discards any monomial of $\operatorname{supp} \operatorname{NF}\left(x_n f, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right) \subseteq S_{\text{DRL}}$ not in Σ.

Lemma 4.9. *Let I be a positive-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$, $\mathcal{G}_{\mathrm{DRL}}$ be its reduced Gröbner basis for $\prec_{\mathrm{DRL}}$ and S_{DRL} be its associated staircase. Let $\varphi \in \mathbb{K}[\boldsymbol{x}] \setminus I$ such that $I : \langle\varphi\rangle$ is zero-dimensional and in shape position. Let $\mathcal{H}_{\mathrm{LEX}} = \{h_n(x_n), x_{n-1} - h_{n-1}(x_n), \ldots, x_1 - h_1(x_n)\}$ be the reduced Gröbner basis of $I : \langle\varphi\rangle$ for $\prec_{\mathrm{LEX}}$, with $\deg h_n = D'$.*

Let $\Sigma = \left\{\sigma \in S_{\mathrm{DRL}} \,\middle|\, \exists s \in \bigcup_{i=0}^{D'-1} \operatorname{supp} \mathrm{NF}\left(x_n^i \varphi, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}}\right), \sigma \mid s\right\} \subset S_{\mathrm{DRL}}$ be a finite staircase and W be the vector subspace of $\mathbb{K}[\boldsymbol{x}]/I$ it spans.

Let $\tilde{M}_{x_n}$ be the matrix of the linear map $f \in W \mapsto \pi_W\big(\mathrm{NF}(x_n f, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}})\big) \in W$.

Assuming $\Sigma = \{\sigma_0, \ldots, \sigma_{N-1}\}$ with for all $0 \le i < N-1$, $\sigma_i \prec_{\mathrm{DRL}} \sigma_{i+1}$, one can build the matrix $\tilde{M}_{x_n} = (\tilde{m}_{i,j})_{0 \le i,j < N}$ with the following procedure:

- *if $x_n\sigma_j = \sigma_k$, then $\tilde{m}_{k,j} = 1$ and for all $0 \le i < N$, $i \ne k$, $\tilde{m}_{i,j} = 0$;*
- *if $x_n\sigma_j \in S_{\mathrm{DRL}} \setminus \Sigma$, then for all $0 \le i < N$, $\tilde{m}_{i,j} = 0$;*
- *otherwise for all $0 \le i < N$, $\tilde{m}_{i,j}$ is the coefficient of σ_i in $\mathrm{NF}(x_n\sigma_j, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}})$.*

Proof. By construction, the matrix $\tilde{M}_{x_n}$ has its jth column which is the vector of coefficients of the projection of $\mathrm{NF}(x_n\sigma_j, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}})$ onto W in the basis Σ.

The first case is immediate.

Observe that in the second case, $x_n\sigma_j \in S_{\mathrm{DRL}}$, hence it is its own normal form w.r.t. $\mathcal{G}_{\mathrm{DRL}}$ and $\prec_{\mathrm{DRL}}$. Yet, since it is not in Σ, its projection is 0.

The last case is obtained by linear combination of the first two. □

Remark 4.10. *While the first two cases of Lemma 4.9 require no computation whatsoever, a priori, the last one needs a normal form computation.*

Since $\mathcal{G}_{\mathrm{DRL}}$ is a reduced Gröbner basis, if $x_n\sigma_j = \mathrm{LT}_{\prec_{\mathrm{DRL}}}(g)$ for some $g \in \mathcal{G}_{\mathrm{DRL}}$, then $\mathrm{NF}(x_n\sigma_j, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}}) = x_n\sigma_j - g$. Therefore, only the case $x_n\sigma_j \in \mathrm{LT}_{\prec_{\mathrm{DRL}}}(I) \setminus \mathrm{LT}_{\prec_{\mathrm{DRL}}}(\mathcal{G}_{\mathrm{DRL}})$ requires a nontrivial normal form computation.

Proposition 4.11. *Let I be a positive-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$, $\mathcal{G}_{\mathrm{DRL}}$ be its reduced Gröbner basis for $\prec_{\mathrm{DRL}}$ and S_{DRL} be the associated staircase. Let $\varphi \in \mathbb{K}[\boldsymbol{x}] \setminus I$, $\mathcal{H}_{\mathrm{LEX}} = \{h_n(x_n), x_{n-1} - h_{n-1}(x_n), \ldots, x_1 - h_1(x_n)\}$ be the reduced Gröbner basis of $I : \langle\varphi\rangle$, with $\deg h_n = D'$.*

Let $\Sigma = \left\{\sigma \in S_{\mathrm{DRL}} \,\middle|\, \exists s \in \bigcup_{i=0}^{D'-1} \operatorname{supp} \mathrm{NF}\left(x_n^i \varphi, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}}\right), \sigma \mid s\right\}$ be of size D and W be the vector subspace of $\mathbb{K}[\boldsymbol{x}]/I$ spanned by Σ.

Let $\tilde{M}_{x_n}$ be the matrix of the map $f \in W \mapsto \pi_W(\mathrm{NF}(x_n f, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}})) \in W$ in the basis Σ and $\boldsymbol{\varphi}$ be the vector of coefficients of φ in the basis Σ.

Let $\boldsymbol{r} \in \overline{\mathbb{K}}^D$ be a row-vector and $\boldsymbol{w} = (w_i)_{i\in\mathbb{N}} = (\boldsymbol{r}\tilde{M}_{x_n}^i \boldsymbol{\varphi})_{i\in\mathbb{N}}$. Let $d \in \mathbb{N}$ be minimal such that there exist $c_0, \ldots, c_{d-1} \in \mathbb{K}$ such that

$$\forall i \in \mathbb{N}, \quad w_{i+d} + c_{d-1}w_{i+d-1} + \cdots + c_0 w_i = 0.$$

Then, the polynomial $x_n^d + c_{d-1}x_n^{d-1} + \cdots + c_0$ divides h_n. Furthermore, if $\boldsymbol{r}$ is generic in $\overline{\mathbb{K}}^D$, then $d = D'$ and $h_n = x_n^d + c_{d-1}x_n^{d-1} + \cdots + c_0$.

In addition, for all $1 \le k \le n-1$, let $\boldsymbol{\psi}_k$ be the vector of coefficients of $\pi_W(\mathrm{NF}(x_k\varphi, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}}))$. Then, for all $1 \le k \le n-1$, there exist unique $\gamma_{0,k}, \ldots,$

$\gamma_{D'-1,k} \in \mathbb{K}$ *such that*

$$\begin{pmatrix} w_0 & w_1 & \cdots & w_{D'-1} \\ w_1 & w_2 & \cdots & w_{D'} \\ \vdots & \vdots & & \vdots \\ w_{D'-1} & w_{D'} & \cdots & w_{2D'-2} \end{pmatrix} \begin{pmatrix} \gamma_{0,k} \\ \gamma_{1,k} \\ \vdots \\ \gamma_{D'-1,k} \end{pmatrix} = \begin{pmatrix} \boldsymbol{r}\tilde{M}_{x_n}^{0}\boldsymbol{\psi}_k \\ \boldsymbol{r}\tilde{M}_{x_n}^{1}\boldsymbol{\psi}_k \\ \vdots \\ \boldsymbol{r}\tilde{M}_{x_n}^{D'-1}\boldsymbol{\psi}_k \end{pmatrix},$$

and $h_k = \gamma_{D'-1,k} x_n^{D'-1} + \cdots + \gamma_{0,k}$.

Proof. The proof is similar to the proofs of Lemma 4.1 and 4.2.

For the first statement, by Proposition 4.7 and the definition of $\tilde{M}_{x_n}$, there exists a smallest integer b such that $\boldsymbol{\varphi}, \tilde{M}_{x_n}\boldsymbol{\varphi}, \ldots, \tilde{M}_{x_n}^{b}\boldsymbol{\varphi}$ are not linearly independent. We let $a_0, \ldots, a_{b-1} \in \mathbb{K}$ such that

$$\tilde{M}_{x_n}^{b}\boldsymbol{\varphi} + a_{b-1}\tilde{M}_{x_n}^{b-1} + \cdots + a_0\boldsymbol{\varphi} = 0.$$

Thus, $\pi_W\left(\mathrm{NF}\left(\left(x_n^b + a_{b-1}x_n^{b-1} + \cdots + a_0\right)\varphi, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}}\right)\right) = 0$. Since the support of this normal form is included in Σ, the normal form actually lies in W. Hence, we conclude that the polynomial $(x_n^b + a_{b-1}x_n^{b-1} + \cdots + a_0)\varphi$ is in I and thus that $x_n^b + a_{b-1}x_n^{b-1} + \cdots + a_0$ is in $I : \langle\varphi\rangle$.

By minimality of b, this ensures that $h_n = x_n^b + a_{b-1}x_n^{b-1} + \cdots + a_0$.

Now, multiplying the vector equality above by $\boldsymbol{r}\tilde{M}_{x_n}^{i}$ on the left yields

$$\forall\, i \in \mathbb{N},\ w_{i+b} + a_{b-1}w_{i+b-1} + \cdots + a_0 w_i = 0.$$

Thus, $\boldsymbol{w}$ is linearly recurrent of order at most b and $d \le b$. Since linear recurrences are in one-to-one correspondence with polynomials, these polynomials define an ideal of $\mathbb{K}[x_n]$ spanned by $x_n^d + c_{d-1}x_n^{d-1} + \cdots + c_0$ that contains h_n. Hence the former divides the latter.

For the second statement, since $d = D'$, then $\boldsymbol{w}$ does not satisfy any linear recurrence relation of order less than D'. Thus, there is no vector in the kernel of the above Hankel matrix, see [8].

Let $1 \le k \le n-1$ and $h_k(x_n) = \alpha_{D'-1,k}x_n^{D'-1} + \cdots + \alpha_{0,k}$, then $(x_k - h_k(x_n))\varphi$ is in I and $\mathrm{NF}\left((x_k - h_k(x_n))\,\varphi, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}}\right) = 0$. Projecting onto W, we have

$$\boldsymbol{\psi}_k = \alpha_{D'-1,k}\tilde{M}_{x_n}^{D'-1}\boldsymbol{\varphi} + \cdots + \alpha_{0,k}\boldsymbol{\varphi}.$$

Now, multiplying this equality by $\boldsymbol{r}\tilde{M}_{x_n}^{i}$ for $0 \le i \le D'-1$ shows that $(\alpha_0, \ldots, \alpha_{D'-1})^{\mathrm{T}}$ is a solution of the above linear system. Since the matrix has full rank, the solution is unique and this ends the proof. ☐

We obtain the following Algorithm 4.2, the so-called Sparse-FGLM-colon algorithm.

Observe that Remark 4.3 applies also to Algorithm 4.2.

Theorem 4.12. *Let I be a positive-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$, let $\mathcal{G}_{\mathrm{DRL}}$ be its reduced Gröbner basis for $\prec_{\mathrm{DRL}}$ and S_{DRL} be the associated staircase. Let $\varphi \in \mathbb{K}[\boldsymbol{x}] \setminus I$ such that $I : \langle\varphi\rangle$ is zero-dimensional of degree D' and in shape position.*

Input: The reduced Gröbner basis $\mathcal{G}_{\text{DRL}}$ of a generic ideal for $\prec_{\text{DRL}}$, a polynomial $\varphi \in \mathbb{K}[\boldsymbol{x}]$, and a finite staircase Σ of size N containing $\operatorname{supp} \operatorname{NF}\left(x_n^k \varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)$ for all $k \in \mathbb{N}$.

Output: The reduced Gröbner basis of $I : \langle \varphi \rangle$ for $\prec_{\text{LEX}}$, if it is in shape position.

1 Build the matrix $\tilde{M}$ as in Lemma 4.9.

2 Pick $\boldsymbol{r} \in \mathbb{K}^N$ a row-vector at random.

3 Build $\boldsymbol{\varphi}$ the column-vector of coefficients of φ restricted to Σ.

4 **For** k **from** 1 **to** $n-1$ **do**

5 $\quad$ Build $\boldsymbol{\psi}_k$ the column-vector of coefficients of $\operatorname{NF}(x_k \varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}})$ restricted to Σ.

6 Compute $(w_i^{(0)})_{0 \le i < 2N}, (w_i^{(1)})_{0 \le i < N}, \ldots, (w_i^{(n-1)})_{0 \le i < N})$ with Algorithm 2.2 called on $\tilde{M}, \boldsymbol{r}, \boldsymbol{\varphi}, \boldsymbol{\psi}_1, \ldots, \boldsymbol{\psi}_{n-1}$.

7 $h_n \leftarrow$ Berlekamp–Massey$(w_0^{(0)}, \ldots, w_{2D-1}^{(0)})$, $D' \coloneqq \deg h_n$.

8 **If** $\operatorname{NF}(h_n \varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}) \neq 0$ **then Return** "Bad vector".

9 Compute $h_1 \coloneqq \gamma_{D'-1,1} x_n^{N-1} + \cdots + \gamma_{0,1}, \ldots, h_{n-1} \coloneqq \gamma_{D'-1,n-1} x_n^{N-1} + \cdots + \gamma_{0,n-1}$ with Algorithm 2.3 called on $(w_i^{(0)})_{0 \le i < 2D'-1}, (w_i^{(1)})_{0 \le i < D'}, \ldots, (w_i^{(n-1)})_{0 \le i < D'})$.

10 **For** k **from** 1 **to** $n-1$ **do**

11 $\quad$ **If** $\operatorname{NF}((x_k - h_k(x_n))\varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}) \neq 0$ **then Return** "Not in shape position".

12 **Return** $\{h_n(x_n), x_{n-1} - h_{n-1}(x_n), \ldots, x_1 - h_1(x_n)\}$.

Algorithm 4.2: SPARSE-FGLM-COLON

Let Σ be a finite staircase of size N containing $\operatorname{supp} \operatorname{NF}\left(x_n^i \varphi, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)$ *for all $i \in \mathbb{N}$.*

Let t be the number of monomials σ in Σ such that $x_n \sigma \in \operatorname{LM}_{\prec_{\text{DRL}}}(\mathcal{G}_{\text{DRL}})$ and let u be the number of monomials σ in Σ such that $x_n \sigma \in \langle \operatorname{LM}_{\prec_{\text{DRL}}}(I) \rangle \setminus \operatorname{LM}_{\prec_{\text{DRL}}}(\mathcal{G}_{\text{DRL}})$.

Then, for a generic choice of vector $\boldsymbol{r} \in \mathbb{K}^N$, Algorithm 4.2 terminates and returns the reduced Gröbner basis of $I : \langle \varphi \rangle$ for $\prec_{\text{LEX}}$. To do so, it requires at most $u + n$ normal form computations w.r.t. $\mathcal{G}_{\text{DRL}}$ and $\prec_{\text{DRL}}$ plus $O\left((t+u+n)ND'\right)$ operations in $\mathbb{K}$.

Proof. The proof follows the proofs of Theorems 2.12 and 4.4.

By the terminations of the normal form computations and the Berlekamp–Massey algorithm, Algorithm 4.2 terminates.

We now prove the correctness of the algorithm. By Corollary 4.11, we know that the polynomial returned by the Berlekamp–Massey algorithm, on line 7 is a divisor of the minimal univariate polynomial of the reduced Gröbner basis of $I : \langle \varphi \rangle$ for $\prec_{\text{LEX}}$. Thus, it suffices to check that, multiplied by φ, it lies in I to ensure that this is the correct polynomial.

By Proposition 4.11 also, we know that if a polynomial $x_k - h_k(x_n)$ is in $I : \langle \varphi \rangle$, then calling Algorithm 2.3 allows us to compute h_k. It suffices then to multiply $x_k - h_k(x_n)$ by φ and to check that it is in I to ensure that $x_k - h_k(x_n)$ is in $I : \langle \varphi \rangle$ and thus that h_k is correct. If it is not, then $I : \langle \varphi \rangle$ is actually not in shape position. This proves the correctness of the algorithm.

Finally, let us prove the complexity of the algorithm. To build the matrix $\tilde{M}$, we need to compute normal forms of monomials $x_n\sigma \notin S_{\text{DRL}}$. By Remark 4.10, the only normal forms which are not free to compute are those of $x_n\sigma \in \text{LT}_{\prec_{\text{DRL}}}(I) \setminus \text{LT}_{\prec_{\text{DRL}}}(\mathcal{G}_{\text{DRL}})$, by assumption, there are u of them. Then, we also need to compute the n normal forms of $\boldsymbol{\varphi}, \boldsymbol{\psi}_1, \ldots, \boldsymbol{\psi}_{n-1}$ w.r.t. $\mathcal{G}_{\text{DRL}}$ and $\prec_{\text{DRL}}$.

By Remark 4.3, it suffices to compute $O(D')$ terms for each sequence $w_i^{(k)}$ for $0 \leq k \leq n-1$ and make a call to the Berlekamp–Massey algorithm in $O((t+u+n)ND')$ operations.

All in all, we have a cost of $u+n$ normal forms computations plus $O((t+u+n)ND')$ operations in $\mathbb{K}$. □

4.4 Reduction of the size of Σ

In many applications, see Section 5, the size of the chosen Σ is much larger than the degree of $I : \langle\varphi\rangle$. This contrasts greatly with the original Sparse-FGLM where, by definition, the size of the staircase S_{DRL} is the degree of the ideal I. Therefore, in order to speed the computation up, one needs to reduce the size of Σ as much as possible. This can be done either before any computation with $\tilde{M}$ or after.

In particular, we shall prove that the zero columns in $\tilde{M}$ will make us remove many monomials in Σ such that after this reduction, $\tilde{M}$ does not have any zero columns left.

Lemma 4.13. *Let I be an ideal of $\mathbb{K}[\boldsymbol{x}]$, $\mathcal{G}_{\text{DRL}}$ be its reduced Gröbner basis for $\prec_{\text{DRL}}$ and S_{DRL} be its associated staircase. Let $\varphi \in \mathbb{K}[\boldsymbol{x}]$ be a polynomial such that $(I : \langle\varphi\rangle)$ is zero-dimensional with staircase $T = \left\{1, x_n, \ldots, x_n^{D'-1}\right\}$ for $\prec_{\text{LEX}}$.*

Let
$$\Sigma = \left\{\sigma \in S_{\text{DRL}} \,\middle|\, \exists s \in \bigcup_{\tau\in T} \operatorname{supp} \text{NF}\left(\tau\varphi, \mathcal{G}, \prec\right), \sigma \mid s\right\} \subset S_{\text{DRL}},$$
and
$$\Sigma' = \Sigma \setminus \left\{\sigma \in \Sigma \,\middle|\, \exists\, i \in \mathbb{N},\ x_n^i\sigma \in S_{\text{DRL}} \setminus \Sigma\right\}.$$
Let W' be the vector subspace of $\mathbb{K}[\boldsymbol{x}]/I$ spanned by Σ'. Let $\tilde{M}'_{x_n}$ be the matrix of the map $f \in W' \mapsto \pi_{W'}\left(\text{NF}\left(x_n\sigma, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)\right) \in W'$ in the basis $\Sigma' = \{\sigma_0, \ldots, \sigma_{N'-1}\}$. Then, $\tilde{M}'_{x_n}$ can be built using the same procedure as in Lemma 4.9.

Furthermore, if its jth column is zero, then $x_n\sigma_j \in \text{LT}_{\prec_{\text{DRL}}}(I)$.

Proof. As $\tilde{M}'_{x_n}$ is defined in a similar fashion as $\tilde{M}_{x_n}$, the procedure of Lemma 4.9 still applies.

By construction of $\tilde{M}'_{x_n}$, the jth column is 0 if, and only if,
$$\pi_{W'}\left(\text{NF}\left(x_n\sigma_j, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)\right) = 0.$$
This can only happen in two cases. Either when $x_n\sigma_j$ is its own normal form and $\pi_{W'}(x_n\sigma_j) = 0$, that is $x_n\sigma_j \in S_{\text{DRL}} \setminus \Sigma'$. Or when $x_n\sigma_j \neq \text{NF}\left(x_n\sigma_j, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)$, that is $x_n\sigma_j \in \text{LT}_{\prec_{\text{DRL}}}(I)$, and then the projection onto W' is 0.

By assumption on Σ', the multiplication of σ_j by x_n cannot reach a monomial in S_{DRL} not in Σ, hence if the projection of its normal form is 0, this means that $x_n\sigma_j$ is not its own normal form, i.e. $x_n\sigma_j \in \text{LT}_{\prec_{\text{DRL}}}(I)$. □

Observe that Σ' need not be a staircase: indeed, 1 may have even been removed.

Proposition 4.14. *Let I be a positive-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$, let $\mathcal{G}_{\mathrm{DRL}}$ be its reduced Gröbner basis for $\prec_{\mathrm{DRL}}$ and S_{DRL} be the associated staircase. Let $\varphi \in \mathbb{K}[\boldsymbol{x}] \setminus I$ such that $I : \langle \varphi \rangle$ is zero-dimensional and in shape position.*

Let

$$\Sigma = \left\{ \sigma \in S_{\mathrm{DRL}} \,\middle|\, \exists s \in \bigcup_{\tau \in T} \operatorname{supp} \mathrm{NF}\left(\tau\varphi, \mathcal{G}, \prec\right), \sigma \mid s \right\} \subset S_{\mathrm{DRL}},$$

and

$$\Sigma' = \Sigma \setminus \left\{ \sigma \in \Sigma \,\middle|\, \exists\, i \in \mathbb{N},\ x_n^i \sigma \in S_{\mathrm{DRL}} \setminus \Sigma \right\}.$$

Let W (resp. W') be the vector subspace of $\mathbb{K}[\boldsymbol{x}]/I$ spanned by Σ (resp. Σ'). Let $\boldsymbol{\varphi}$ (resp. $\boldsymbol{\varphi}'$) be the vector of coefficients of the projection of $\mathrm{NF}\left(\varphi, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}}\right)$ onto W (resp. W').

Let $d \in \mathbb{N}$ be minimal such that there exist $c_0, \ldots, c_{d-1} \in \mathbb{K}$ such that

$$\forall\, i \in \mathbb{N}, \quad \tilde{M}_{x_n}^{i+d} \boldsymbol{\varphi} + c_{d-1} \tilde{M}_{x_n}^{i+d-1} \boldsymbol{\varphi} + \cdots + c_0 \tilde{M}_{x_n}^{i} \boldsymbol{\varphi} = 0.$$

Let $b \in \mathbb{N}$ be minimal such that there exist $a_0, \ldots, a_{b-1} \in \mathbb{K}$ such that

$$\forall\, i \in \mathbb{N}, \quad \tilde{M}_{x_n}^{\prime i+b} \boldsymbol{\varphi}' + a_{b-1} \tilde{M}_{x_n}^{\prime i+b-1} \boldsymbol{\varphi} + \cdots + a_0 \tilde{M}_{x_n}^{\prime i} \boldsymbol{\varphi} = 0.$$

Then, $b = d$ and $a_0 = c_0, \ldots, a_{b-1} = c_{d-1}$.

Proof. By assumption, the sequence $\left(\tilde{M}_{x_n}^{\prime i} \boldsymbol{\varphi}\right)_{i \in \mathbb{N}}$ is linear recurrent of order d. The linear recurrences it satisfies are then in one-to-one correspondence with the ideal $\langle h_n \rangle \in \mathbb{K}[\boldsymbol{x}]$, where $h_n = x_n^d + c_{d-1} x_n^{d-1} + \cdots + c_0$.

Now, there exist a smallest integer β such that there exist unique $\alpha_0, \ldots, \alpha_{\beta-1}$ such that

$$\forall\, i \in \mathbb{N}, \quad \tilde{M}_{x_n}^{i+\beta+1} \boldsymbol{\varphi} + \alpha_{\beta-1} \tilde{M}_{x_n}^{i+\beta-1} \boldsymbol{\varphi} + \cdots + \alpha_0 \tilde{M}_{x_n}^{i+1} \boldsymbol{\varphi} = 0.$$

Hence, the sequence $\left(\tilde{M}_{x_n}^{\prime i+1} \boldsymbol{\varphi}\right)_{i \in \mathbb{N}}$ is linear recurrent of order β. Therefore, $x_n^\beta + \alpha_{\beta-1} + \cdots + \alpha_0$ divides h_n. Furthermore, because of the extra multiplication by $\tilde{M}_{x_n}$ in the definition of this sequence, we know that the ideal of $\mathbb{K}[x_n]$ in one-to-one correspondence with its sets of linear recurrence relation is actually $\langle h_n \rangle : \langle x_n \rangle$. Thus it is spanned by h_n if $x_n \nmid h_n$ and by h_n / x_n otherwise.

Let us denote $\sigma_0 \prec_{\mathrm{DRL}} \cdots \prec_{\mathrm{DRL}} \sigma_{N-1}$ the monomials in Σ. If a monomial $\sigma_j \in \Sigma$ is such that $x_n \sigma_j \in S_{\mathrm{DRL}} \setminus \Sigma$, which implies that the jth column of $\tilde{M}_{x_n}$ is 0, then the coefficients of $\tilde{M}_{x_n}^{\prime i+1} \boldsymbol{\varphi}, \ldots, \tilde{M}_{x_n}^{\prime i+\beta} \boldsymbol{\varphi}$ are all independent from the jth coefficient of $\boldsymbol{\varphi}$. Thus, this coefficient does not appear in the second linear system and $c_0, \ldots, c_{d-1}$ do not depend on it. Hence, we can reduce the linear system by removing σ_j from Σ without changing the linear recurrence relation of smallest order that is satisfied.

Now, if this monomial σ_j is divisible by x_n, then there exists an index $i < j$ such that $\sigma_i = \sigma_j / x_n$. This implies that the ith column of the new matrix is zero. Thus, the previous argument can be repeated to remove σ_i from Σ as well.

By recurrence, at the end of this removal procedure, the set of monomials *is* Σ' and there was no change whatsoever in the linear recurrence relations satisfied by the modified sequence. Hence d is the smallest integer such that there exist unique $c_0, \ldots, c_{d-1} \in \mathbb{K}$ such that

$$\forall\, i \in \mathbb{N}, \quad \tilde{M}'^{i+d}_{x_n} \boldsymbol{\varphi}' + c_{d-1} \tilde{M}'^{i+d-1}_{x_n} \boldsymbol{\varphi} + \cdots + c_0 \tilde{M}'^{i}_{x_n} \boldsymbol{\varphi} = 0,$$

in other words, $b = d$ and $a_0 = c_0, \ldots, a_{b-1} = c_{d-1}$. □

4.5 Non shape position case

Next, we want to lift the assumption that $I : \langle \varphi \rangle$ is in shape position. In the Sparse-FGLM algorithm, this is easy to test, see Subsection 2.2.2: The minimal univariate polynomial in x_n has the same degree as the ideal if, and only, the ideal is in shape position. However, now, we do not know the degree of the polynomial h_n such that $(I : \langle \varphi \rangle) \cap \mathbb{K}[x_n] = \langle h_n \rangle$. Since for a generic choice of $\boldsymbol{r}$, we know that the Sparse-FGLM-colon algorithm computes correctly h_n on line 7, the computation of the normal form at the following line can be skipped. Now, the goal is to avoid computing the normal forms of $(x_k - h_k(x_n))\varphi$ to ensure that $I : \langle \varphi \rangle$ is in shape position using the following lemma.

Lemma 4.15. *Let J be a zero-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$. Let $\lambda \in \bar{\mathbb{K}}$ be generic. Then, for $1 \leq k \leq n$, $J = J : \langle x_k + \lambda \rangle$.*

Proof. Clearly $J \subseteq J : \langle x_k + \lambda \rangle$ so it remains to prove the converse inclusion for generic λ. This is equivalent to proving that the converse inclusion does not hold for only finitely many possible values of λ.

Let us assume that $J : \langle x_k + \lambda \rangle \neq J$ and let $f \in J : \langle x_k + \lambda \rangle$ not in J. Then $g = (x_k + \lambda) f \in J$. Thus, g vanishes on the finitely many points of the variety defined by J. If we assume that J is radical, then f does not vanish on at least one of these points but g does. Since $x_k + \lambda$ is prime in $\mathbb{K}[\boldsymbol{x}]$, this means that $x_k + \lambda$ vanishes on this point. Therefore, one of the points of the variety defined by J has its kth coordinate which is $-\lambda$. Thus, this situation can only occur for finitely many choices of λ.

If now, J is not radical, then the same reasoning applies if one takes the multiplicities into account as well. Hence, only finitely many $\lambda \in \bar{\mathbb{K}}$ are such that $J : \langle x_k + \lambda \rangle \neq J$. □

Remark 4.16. *Thanks to Lemma 4.15 applied to $J = I : \langle \varphi \rangle$, we can check if the polynomial $x_k - h_k(x_n)$ computed by the* Sparse-FGLM-colon *algorithm is correct. We compute $x_k - h'_k(x_n)$ for the ideal $I : \langle x_k + \lambda \rangle$ by*

1. *Building ψ'_k the column-vector of* $\mathrm{NF}\left(x_k^2 \varphi, \mathcal{G}_{\mathrm{DRL}}, \prec_{\mathrm{DRL}}\right)$ *restricted to Σ.*
2. *Computing $\left(w_i^{(0)}\right)_{0 \leq i < 2N}$ and $\left(w_i^{(k)}\right)_{0 \leq i < N}$ with Algorithm 2.2 called on $\boldsymbol{r}$, $\boldsymbol{\psi}_k + \lambda \boldsymbol{\varphi}$ and $\boldsymbol{\psi}'_k + \lambda \boldsymbol{\psi}_k$.*

If $h_k = h'_k$ for generic λ, then $x_k - h_k(x_n)$ is in $I : \langle \varphi \rangle$.

Now let us assume that $I : \langle \varphi \rangle$ is not in shape position but its radical $\sqrt{I : \langle \varphi \rangle}$ is.

Proposition 4.17. *Let I be a positive-dimensional ideal of $\mathbb{K}[\boldsymbol{x}]$, let $\mathcal{G}_{\mathrm{DRL}}$ be its reduced Gröbner basis for $\prec_{\mathrm{DRL}}$ and S_{DRL} be the associated staircase. Let $\varphi \in \mathbb{K}[\boldsymbol{x}] \setminus I$ such that $I : \langle\varphi\rangle$ is zero-dimensional, let $\mathcal{H}_{\mathrm{LEX}}$ be its reduced Gröbner basis for $\prec_{\mathrm{LEX}}$ and let $h_n \in \mathcal{H}_{\mathrm{LEX}} \cap \mathbb{K}[x_n]$.*

If $\sqrt{I : \langle\varphi\rangle}$ is in shape position, then one can compute its reduced Gröbner basis for $\prec_{\mathrm{LEX}}$ calling the Sparse-FGLM-colon *algorithm with the following modifications:*

1. *On line 7, h_n is the squarefree part of the polynomial returned by the Berlekamp–Massey algorithm.*
2. *On line 9, h_k is obtained thanks to [22, Algorithm 2], see also [6].*

Proof. By Lemma 4.1, we already know that we can recover the minimal univariate polynomial in x_n of $I : \langle\varphi\rangle$. Extracting its squarefree part yields the one of $\sqrt{I : \langle\varphi\rangle}$.

Now, Algorithm 2 of [22] called on these sequences yields the polynomials with leading terms $x_1, \ldots, x_{n-1}$ in $\sqrt{J}$ for some ideal J. By construction of these sequences, $J = I : \langle\varphi\rangle$. □

Remark 4.18. *In practice, when an ideal J is not in shape position, it is not easy to check that $\sqrt{J}$ is. Therefore, using Lemma 4.15 is the cornerstone of our probabilistic verification algorithm in* msolve *[3, 4] when J is not in shape position but its radical might be, see [3, Sec. 4.4]. We proceed as in Remark 4.16:*

1. *Compute the polynomials $x_k - g_k(x_n)$ in $\sqrt{J}$ for $1 \leq k \leq n-1$, with $\deg g_k$ minimal.*
2. *Compute the polynomials $x_k - g_k'(x_n)$ in $\sqrt{J : \langle x_k + \lambda\rangle}$ for λ picked at random and $1 \leq k \leq n-1$, with $\deg g_k'$ minimal.*
3. *Check whether $g_k = g_k'$ for $1 \leq k \leq n-1$.*

By Lemma 4.15, for a generic λ, $J = J : \langle x_k + \lambda\rangle$, hence both radical ideals are the same. Furthermore, if they are in shape position, then $g_k = g_k'$ for $1 \leq k \leq n-1$. Therefore, any discrepancy must come from the fact that $\sqrt{J}$ is not *in shape position and the polynomials $x_k - g_k(x_n)$ and $x_k - g_k'(x_n)$ are meaningless.*

5 Implementation and practical experiments

We implemented Algorithms 3.1 and 4.2 in msolve [3, 4], using the `C` programming language. The saturation examples we use come from classical benchmarks of real algebraic geometry when it comes to compute *limits* of critical points of the restriction of a polynomial map to some algebraic set depending on a parameter. This is used, for instance, for computing sample points in singular real algebraic sets [31] or computing their real dimension [24] and boils down to the computation of saturated ideals.

These computations were performed on a computing server with 1.48 TB of memory and an Intel Xeon Gold 6244 @ 3.60GHz processor.

In Tables 1 and 2, we report on timings for computing the Gröbner basis of the saturation $I : \langle\varphi\rangle^\infty$ of an ideal I w.r.t. φ for $\prec_{\mathrm{DRL}}$. In both tables, I is positive-dimensional. However, in Table 1, $I : \langle\varphi\rangle^\infty$ is also positive-dimensional, while in Table 2 it is zero-dimensional.

We optimized the F_4SAT algorithm (Algorithm 3.1), as discussed in Subsection 3.3. In the first phase of learning, we search for new elements in the saturation only if F_4 has added new elements to the basis in three distinct linear algebra steps. Furthermore, on line 13, q_σ is computing if $\deg \sigma$ is at most $2/3$ of the maximal degree in the current basis $\mathcal{G}$, in order to speed intermediate steps of the algorithm up. When the set of critical pairs is empty, all q_σ up to the maximal degree of the basis are taken into account. Columns learn 1 and learn 2 are for the two learning rounds of the tracer while column apply is for the apply phase.

The columns MSOLVE correspond to our implementation of Rabinowitsch trick in MSOLVE, with column prob. using the probabilistic linear algebra while the column learn is for the learning phase of the tracer and the column apply is for the apply phase (see [3]). These last two columns are to be compared with the learn 1 and 2, and the apply phases of F_4SAT. The one related to the probabilistic linear algebra is to be compared to the apply phase of F_4SAT.

We compare our implementations with Maple [26] using probabilistic linear algebra and SINGULAR [12].

In both tables, examples SOS mean that we consider a polynomial f which the sum of p squares of polynomials of degree d in n variables. In Table 1, $I = \left\langle \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_{n-1}} \right\rangle$ and $\varphi = \frac{\partial f}{\partial x_n}$. In Table 2, $I = \left\langle f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_{n-1}} \right\rangle$ and $\varphi = \frac{\partial f}{\partial x_n}$.

In general, F_4SAT is the most efficient attempt to compute the saturations (sometimes with a speed-up close to 10), MSOLVE's F_4 with elimination order is in general a bit faster than Maple on the probabilistic linear algebra. When applying the tracing approach we can see that sometimes the search for the correct steps to search for new elements in the saturation in F_4SAT has a bigger impact (i.e. learn 1 is slower than learn 2). In other cases, the exact linear algebra applied in learn 2 to trace the full computation is the bottleneck (i.e. learn 2 is slower than learn 1). Nevertheless, the application phase of F_4SAT is in general the fastest implementation, often by an order of magnitude. This suggests that F_4SAT provides a very efficient method for computing saturations of ideals over $\mathbb{Q}$ using the multi-modular tracer approach. The few examples where F_4SAT is slower than MSOLVE's F_4 or Maple are identified by the fact that F_4SAT finds saturation elements a bit later than the Rabinowitsch trick-based implementations. Clearly, one could test for saturation elements more often in learn 1, but this would have a bigger impact on the running time. A future plan is to apply a more dynamic and adaptable strategy of when to search for saturation elements.

In Table 3, we compare Algorithm 4.2 for computing a Gröbner basis of the zero-dimensional colon ideal $I : \langle \varphi \rangle = I : \langle \varphi \rangle^\infty$ for $\prec_{\text{LEX}}$ with MAPLE [26] using the `Groebner:-Basis` command followed by the `Groebner:-FGLM` command. As in Table 2, $I = \left\langle f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_{n-1}} \right\rangle$ and $\varphi = \left(\frac{\partial f}{\partial x_n}\right)^M$ for M large enough, with f the sum of p squares of polynomials of degree d in n variables. The columns $\#\,\Sigma$ and $\#\,\Sigma'$ correspond to the size of the set Σ before and after reductions as defined in Lemma 4.5, Remark 4.8 and Proposition 4.14, while column D' gives the degree of the saturated ideal. Whether it is between $\#\,\Sigma$ and $\#\,\Sigma'$ or between $\#\,\Sigma'$ and D', we can observe ratios going up to around 5. Therefore, it is clear that the algorithm would not be as efficient if one were to work with Σ directly. Still, it would be even more beneficial to reduce further the

Sys-SOS	F_4SAT (learn1)	(learn2)	(apply)	MSOLVE (prob.)	MSOLVE (learn)	(apply)	Maple (prob.)	Singular
d3-n6-p2	1.31	0.,41	0.31	0.77	2.40	0.40	1.12	52.2
d3-n6-p3	43.7	5.55	1.84	25.2	142	16.6	35.4	2,902
d3-n6-p4	533	53.1	19.7	171	882	126	223	39,501
d3-n6-p5	1,863	184	104	276	1,145	183	394	42,854
d4-n6-p2	972	107	77	253	1,176	191	394	28,043
d4-n6-p3	31,101	1,316	596	7,444	43,803	6,336	8,817	–
d2-n7-p6	5.13	1.82	0.77	3.01	15.3	1.84	4.95	443
d3-n7-p2	13.4	3.61	2.23	9.59	54.1	5.29	12.5	872
d3-n7-p3	1,263	164	32.4	533	3,647	406	984	–
d3-n7-p4	22,296	2,235	469	6,605	47,286	5,348	10,001	–
d3-n7-p5	126,006	137,724	2,881	29,740	204,718	22,925	33,635	–
d2-n8-p5	11.7	8.37	1.79	15.1	99.9	7.92	20.4	3,972
d2-n8-p6	95.7	63.7	10.5	54.3	387	33.8	63.1	15,950
d2-n8-p7	265	79.6	22.2	81.9	556	47.2	122	15,125
d3-n8-p2	228	276	18.1	98.3	787	71.7	135	15,252
d3-n8-p3	25,593	3,716	471	11,050	107,744	8,984	13,705	–

Table 1: Timings in seconds, Gröbner basis for $\prec_{\text{DRL}}$, positive-to-positive-dimensional case

Examples	F_4SAT (learn 1)	(learn 2)	(apply)	MSOLVE (prob.)	MSOLVE (learn)	(apply)	Maple (prob.)	Singular
Steiner	115	134	67.2	204	614	153	239	3,642
d3-n6-p3	82.4	127	56.7	51.5	191	32.6	67.4	8,226
d3-n6-p4	1,592	1,776	810	2,123	5,284	1,720	3,585	–
d3-n6-p5	9,646	7,032	3,321	7,485	16,711	6,466	7,226	–
d4-n6-p2	720	1,581	536	120	520	60.6	135	24,532
d4-n6-p3	45,749	38,657	18,123	40,646	190,009	35,835	38,466	–
d2-n7-p6	18.9	41.85	10.8	31.8	101	19.5	41.4	1,773
d3-n7-p2	28.2	45.2	23.9	5.02	11.6	2.63	8.09	961
d3-n7-p3	1,462	2,688	937	953	5,851	875	1,108	–
d3-n7-p4	48,907	65,035	22,844	40,383	248,889	34,670	39,729	–
d2-n8-p4	2.68	5.04	1.89	3.55	10.1	2.02	4.12	500
d2-n8-p5	47.7	171.9	37.1	62.9	270	45.3	48.8	8,333
d2-n8-p6	287	820	169	420	1,599	301	350	54,567
d2-n8-p7	1,018	1,841	442	907	3,198	683	871	–
d3-n8-p2	300	585	266	32.4	105	20.4	50.7	9,812
d3-n8-p3	18,152	42,436	11,285	15,502	71,595	8,478	15,182	–

Table 2: Timings in seconds, Gröbner basis for $\prec_{\text{DRL}}$, positive-to-zero-dimensional case

size of Σ' to be as close as possible to D'.

The column F_4 gives the proportion of time to compute the Gröbner basis $\mathcal{G}_{\text{DRL}}$ of I for $\prec_{\text{DRL}}$ using the F_4 algorithm in MSOLVE, the column Sat. order corresponds to the time for computing iteratively $\text{NF}\left(\left(\frac{\partial f}{\partial x_n}\right)^M, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}}\right)$ with M large enough. The column Matrix corresponds to the proportion of time to compute all the normal forms $\text{NF}(x_n\sigma, \mathcal{G}_{\text{DRL}}, \prec_{\text{DRL}})$ for σ in Σ' and $x_n\sigma \in \langle \text{LM}_{\prec}(\mathcal{G}_{\text{DRL}})\rangle$ as in Lemma 4.9. The FGLM column gives the proportion of time to perform the SPARSE-FGLM algorithm with this matrix. Finally, the total column gives the total time to perform all these computations in seconds, resulting in the computation of the saturation of I w.r.t. φ. Likewise the columns MAPLE give the time for MAPLE in seconds using Rabinowitsch trick [30]. The column `Basis` computes the Gröbner basis for $\prec_{\text{DRL}}$ of $I + \left\langle 1 - t\frac{\partial f}{\partial x_n}\right\rangle$ while the column `FGLM` computes the Gröbner basis of the same ideal for $\prec_{\text{LEX}}$ with $x_n \prec_{\text{LEX}} \cdots \prec_{\text{LEX}} x_1 \prec_{\text{LEX}} t$.

We can notice that the SPARSE-FGLM-COLON algorithm approach is most efficient when either the change of ordering step is the most time-consuming or when the ratios between $\#\,\Sigma$, $\#\,\Sigma'$ and D' are the smallest. In the former case, the algorithm benefits from the regularity of the computation of the reduced Gröbner basis of I for $\prec_{\text{DRL}}$ compared to the one of $I + \langle 1 - t\varphi\rangle$ in the Rabinowitsch trick approach. In the latter case, when Σ or Σ' are large compared to D', the overhead in the linear algebra part becomes overwhelming. Clearly, in a multi-modular approach, one would want to consider an even smaller subset of Σ' to perform the computations, once D' is known. All in all, we can see speed-ups that are significant and sometimes higher than 10.

	sizes			msolve					Maple Groebner		
	$\#\,\Sigma$	$\#\,\Sigma'$	D'	F_4	Sat. order	Mat.	FGLM	Total	Basis	FGLM	Total
d2-n8-p5	5746	2636	1516	60%	20%	7%	13%	21	96%	4%	56
d2-n8-p6	7901	5100	3756	35%	9%	6%	50%	140	88%	12%	350
d2-n8-p7	8841	7340	6444	33%	9%	6%	52%	320	79%	21%	890
d2-n9-p5	11748	4548	2308	56%	14%	8%	22%	150	68%	32%	410
d2-n9-p6	18829	10372	6788	40%	7%	8%	45%	1200	91%	9%	3200
d2-n9-p7	24332	17540	13956	33%	5%	7%	55%	4400	83%	17%	12000
d2-n10-p4	9724	1996	652	67%	27%	5%	1%	42	99%	1%	68
d2-n10-p5	22408	7372	3340	52%	11%	9%	28%	900	97%	3%	1200
d2-n10-p6	40946	19468	11404	42%	7%	9%	42%	9900	92%	8%	17000
d3-n5-p3	3034	1320	672	39%	33%	9%	19%	1.1	97%	3%	4
d3-n5-p4	3750	2616	1968	27%	27%	11%	35%	4.3	95%	5%	43
d3-n6-p3	10773	3792	1632	60%	11%	8%	21%	50	96%	4%	77
d3-n6-p4	16271	9192	5952	37%	5%	6%	52%	500	89%	11%	1300
d3-n6-p5	18897	14862	12432	12%	5%	6%	77%	1200	82%	18%	5600
d3-n7-p3	35117	10320	3840	52%	9%	8%	31%	1300	95%	5%	1100
d3-n7-p4	62104	29760	16800	19%	4%	11%	66%	12000	91%	9%	31000
d4-n5-p3	15881	7560	4104	41%	6%	5%	48%	200	94%	6%	620
d4-n5-p4	19274	14088	11016	32%	4%	4%	60%	1000	86%	14%	4700
d4-n6-p2	41189	8424	1944	74%	5%	9%	12%	590	97%	3%	224
d4-n6-p3	81068	32184	14904	16%	3%	12%	69%	11000	92%	8%	27000
d5-n4-p3	7235	4540	3040	13%	24%	11%	52%	9	93%	7%	180
d5-n5-p3	54787	27360	15360	8%	4%	7%	81%	5100	92%	8%	22000

Table 3: Timings in seconds, Gröbner basis for $\prec_{\text{LEX}}$, positive-to-zero-dimensional case.

References

[1] D. A. Bayer. *The Division Algorithm and the Hilbert Scheme*. PhD thesis, Harvard University, USA, 1982. AAI8222588.

[2] E. Berlekamp. Nonbinary BCH decoding. *IEEE Trans. Inform. Theory*, 14(2):242–242, 1968.

[3] J. Berthomieu, Ch. Eder, and M. Safey El Din. Msolve: A library for solving polynomial systems. In *Proceedings of the 46th International Symposium on Symbolic and Algebraic Computation*, ISSAC '21, pages 51–58, New York, NY, USA, 2021. Association for Computing Machinery.

[4] J. Berthomieu, Ch. Eder, and M. Safey El Din. msolve: A library for solving polynomial systems, 2021. `https://msolve.lip6.fr/`.

[5] J. Berthomieu and M. Safey El Din. Guessing Gröbner bases of structured ideals of relations of sequences. *J. Symbolic Comput.*, 111:1–26, 2022.

[6] A. Bostan, B. Salvy, and É. Schost. Fast Algorithms for Zero-Dimensional Polynomial Systems Using Duality. *Appl. Algebra Eng. Commun. Comput.*, 14(4):239–272, 2003.

[7] P. Breiding, B. Sturmfels, and S. Timme. 3264 conics in a second. *Notices of the American Mathematical Society*, 67(1):30–37, 2020.

[8] R. P. Brent, F. G. Gustavson, and D. Y. Yun. Fast solution of Toeplitz systems of equations and computation of Padé approximants. *Journal of Algorithms*, 1(3):259–295, 1980.

[9] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, University of Innsbruck, 1965.

[10] B. Buchberger. A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases. In *EUROSAM '79, An International Symposium on Symbolic and Algebraic Manipulation*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21, Berlin, 1979. Springer.

[11] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics. Springer, New York, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[12] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. Singular 4-1-2 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`, 2019.

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

[14] J.-Ch. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1):61–88, 1999.

[15] J.-Ch.. Faugère. A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

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

[17] J.-Ch. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (hfe) cryptosystems using gröbner bases. In D. Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, pages 44–60, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[18] J.-Ch. Faugère, A. Joux, L. Perret, and J. Treger. Cryptanalysis of the hidden matrix cryptosystem. In M. Abdalla and P. S. L. M. Barreto, editors, *Progress in Cryptology – LATINCRYPT 2010*, pages 241–254, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[19] J.-Ch. Faugère and C. Mou. Fast Algorithm for Change of Ordering of Zero-dimensional Gröbner Bases with Sparse Multiplication Matrices. In *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, ISSAC '11, pages 115–122, New York, NY, USA, 2011. ACM.

[20] J.-Ch. Faugère and C. Mou. Sparse FGLM algorithms. *Journal of Symbolic Computation*, 80(3):538–569, 2017.

[21] J. García Fontán, A. Nayak, S. Briot, and M. Safey El Din. Singularity Analysis for the Perspective-Four and Five-Line Problems. *International Journal of Computer Vision*, 2022.

[22] S. G. Hyun, V. Neiger, H. Rahkooy, and É. Schost. Block-Krylov techniques in the context of sparse-FGLM algorithms. *Journal of Symbolic Computation*, 98:163–191, 2020. Special Issue on Symb. and Alg. Comp.: ISSAC 2017.

[23] C. Kollreider and B. Buchberger. An improved algorithmic construction of Gröbner-bases for polynomial ideals. *SIGSAM Bull.*, 12:27–36, 1978.

[24] P. Lairez and M. Safey El Din. Computing the dimension of real algebraic sets. In *Proceedings of the 46th International Symposium on Symbolic and Algebraic Computation*, ISSAC '21, pages 257–264, New York, NY, USA, 2021. Association for Computing Machinery.

[25] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra (London, 1983)*, volume 162 of *Lecture Notes in Comput. Sci.*, pages 146–156. Springer, Berlin, 1983.

[26] Maplesoft, a division of Waterloo Maple Inc.. Maple.

[27] J. L. Massey. Shift-register synthesis and BCH decoding. *IEEE Trans. Inform. Theory*, IT-15:122–127, 1969.

[28] G. Moreno-Socías. Degrevlex Gröbner bases of generic complete intersections. *Journal of Pure and Applied Algebra*, 180(3):263–283, 2003.

[29] B. Pascual-Escudero, A. Nayak, S. Briot, O. Kermorgant, P. Martinet, M. Safey El Din, and F. Chaumette. Complete Singularity Analysis for the Perspective-Four-Point Problem. *International Journal of Computer Vision*, 129(4):1217–1237, Apr. 2021.

[30] J. Rabinowitsch. Zum Hilbertschen Nullstellensatz. *Mathematische Annalen*, 102:520–520, 1930.

[31] M. Safey El Din. Computing Sampling Points on a Singular Real Hypersurface using Lagrange's System. Research Report RR-5464, INRIA, 2005.

[32] A. K. Steel. Direct solution of the (11, 9, 8)-MinRank problem by the block Wiedemann algorithm in Magma with a Tesla GPU. In *Proceedings of the 2015 International Workshop on Parallel Symbolic Computation, PASCO 2015, July 10-12, 2015*, pages 2–6, Bath, United Kingdom, 2015. ACM.

[33] D. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Trans. Inf. Theory*, 32(1):54–62, 1986.