

Faster change of order algorithm for Gröbner bases under shape and stability assumptions

Jérémy Berthomieu, Vincent Neiger, Mohab Safey El Din

▶ **To cite this version:**

Jérémy Berthomieu, Vincent Neiger, Mohab Safey El Din. Faster change of order algorithm for Gröbner bases under shape and stability assumptions. 2022 International Symposium on Symbolic and Algebraic Computation, Jul 2022, Lille, France. 10.1145/3476446.3535484 . hal-03580736v2

HAL Id: hal-03580736
https://hal.science/hal-03580736v2

Submitted on 16 May 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Faster Change of Order Algorithm for Gröbner Bases Under Shape and Stability Assumptions

Jérémy Berthomieu
Sorbonne Université, CNRS, LIP6
F-75005 Paris, France
jeremy.berthomieu@lip6.fr

Vincent Neiger
Sorbonne Université, CNRS, LIP6
F-75005 Paris, France
vincent.neiger@lip6.fr

Mohab Safey El Din
Sorbonne Université, CNRS, LIP6
F-75005 Paris, France
mohab.safey@lip6.fr

ABSTRACT

Solving zero-dimensional polynomial systems using Gröbner bases is usually done by, first, computing a Gröbner basis for the degree reverse lexicographic order, and next computing the lexicographic Gröbner basis with a change of order algorithm. Currently, the change of order now takes a significant part of the whole solving time for many generic instances.

Like the fastest known change of order algorithms, this work focuses on the situation where the ideal defined by the system satisfies natural properties which can be recovered in generic coordinates. First, the ideal has a *shape* lexicographic Gröbner basis. Second, the set of leading terms with respect to the degree reverse lexicographic order has a *stability* property; in particular, the multiplication matrix can be read on the input Gröbner basis.

The current fastest algorithms rely on the sparsity of this matrix. Actually, this sparsity is a consequence of an algebraic structure, which can be exploited to represent the matrix concisely as a univariate polynomial matrix. We show that the Hermite normal form of that matrix yields the sought lexicographic Gröbner basis, under assumptions which cover the shape position case. Under some mild assumption implying $n \leq t$, the arithmetic complexity of our algorithm is $O^{\sim}(t^{\omega-1}D)$, where n is the number of variables, t is a sparsity indicator of the aforementioned matrix, D is the degree of the zero-dimensional ideal under consideration, and ω is the exponent of matrix multiplication. This improves upon both state-of-the-art complexity bounds $O^{\sim}(tD^2)$ and $O^{\sim}(D^{\omega})$, since $\omega < 3$ and $t \leq D$. Practical experiments, based on the libraries `msolve` and `PML`, confirm the high practical benefit.

CCS CONCEPTS

• **Computing methodologies** → **Algebraic algorithms**; • **Theory of computation** → **Design and analysis of algorithms**.

KEYWORDS

Gröbner basis; polynomial system solving; change of monomial order; polynomial matrix; Hermite normal form.

ACM Reference Format:
Jérémy Berthomieu, Vincent Neiger, and Mohab Safey El Din. 2022. Faster Change of Order Algorithm for Gröbner Bases Under Shape and Stability Assumptions. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation (ISSAC '22), July 4–7, 2022, Villeneuve-d'Ascq, France.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3476446.3535484

The authors are supported by the joint ANR-FWF ANR-19-CE48-0015 ECARP project, the ANR grants ANR-18-CE33-0011 Sesame and ANR-19-CE40-0018 De Rerum Natura projects, grant FA8665-20-1-7029 of the EOARD-AFOSR and the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement N. 813211 (POEMA). We thank the referees for their valuable comments on the paper.

ISSAC '22, July 4–7, 2022, Villeneuve-d'Ascq, France
© 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM. This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation (ISSAC '22), July 4–7, 2022, Villeneuve-d'Ascq, France*, https://doi.org/10.1145/3476446.3535484.

1 INTRODUCTION

Context. A method of choice for solving polynomial systems of dimension zero with coefficients in some field $\mathbb{K}$ consists in computing a Gröbner basis for a degree-refining order (such as the degree reverse lexicographic one) using an algorithm such as Buchberger's, or Faugère's F_4 or F_5 algorithms [9, 13, 14] and next apply a change of order to obtain the lexicographic Gröbner basis, using the FGLM algorithm [16]. We refer to [31, 46] for an exposition on solving polynomial systems through algebraic methods, and some applications.

In this paper, we consider polynomial systems and ideals in $\mathbb{K}[x_1, \ldots, x_{n-1}, y]$ as well as two classical assumptions (which are recalled with more details below). When a zero-dimensional ideal $\mathcal{I}$ under consideration is in *shape position* (see the *shape lemma* in [21, Lem. 1.4], and Eq. (1) below), the leading monomials of its reduced lexicographical Gröbner basis are $x_1, \ldots, x_{n-1}, y^D$ where D is the degree of the ideal. This shape position is important for solving polynomial systems, as it reduces multivariate to univariate solving. The second assumption is a *stability* one which we also describe in detail below. Roughly, a consequence of this assumption is that the matrix encoding the multiplication by y in the quotient ring $\mathbb{K}[x_1, \ldots, x_{n-1}, y]/\mathcal{I}$ can be read on the reduced Gröbner basis of $\mathcal{I}$ for the degree-refining monomial order. Both the shape position and stability property are satisfied generically and, when the base field is large enough and the ideal under consideration is radical, they can be ensured through a generic linear change of coordinates. When these assumptions hold, Sparse-FGLM variant [17, 18] can be applied and is faster than the classical FGLM algorithm for the change of order step.

This paper aims at improving this change of order step, under assumptions similar to the ones of Sparse-FGLM, since despite the progress brought by [17, 18], this step has become the bottleneck of polynomial system solving with Gröbner bases on a wide range of problems (see [8, Tbl. 1]).

Prior results. The original FGLM algorithm [16] uses $O(nD^3)$ operations in $\mathbb{K}$ without any assumption. We refer to [38, Thm. 1.7] for some improvements around this algorithm.

In [15], the authors consider the special case where $\preccurlyeq_1$ is the degree reverse lexicographic order $\preccurlyeq_{\mathrm{drl}}$ and $\preccurlyeq_2$ is the lexicographic one $\preccurlyeq_{\mathrm{lex}}$, with $y \preccurlyeq_{\mathrm{drl}} x_k$ and $y \preccurlyeq_{\mathrm{lex}} x_k$ for $1 \leq k \leq n-1$. They show that the aforementioned multiplication matrix by y can be read on the $\preccurlyeq_{\mathrm{drl}}$-Gröbner basis, under some genericity assumptions and using results from [35]. Assuming additionally the shape position, this multiplication matrix alone suffices to recover the $\preccurlyeq_{\mathrm{lex}}$-Gröbner basis, which is done in time $O^{\tilde{}}(D^\omega)$ [15].

In [17, 18], the authors follow on from the same assumptions: shape and stability. They observe and exploit the sparsity of the multiplication matrix thanks to Wiedemann's approach [48]. Precisely, the matrix has about tD nonzero entries out of D^2, where the parameter t is the number of polynomials in the $\preccurlyeq_{\mathrm{drl}}$-Gröbner basis whose leading monomial is divisible by y. This leads to a complexity estimate of $O(tD^2)$ operations in $\mathbb{K}$, which improves upon $O^{\tilde{}}(D^\omega)$ when t is small compared to D. This provides significant practical benefit for the change of order step of polynomial system solving in many cases [18, Tbl. 2], and this is the approach used by the state-of-the-art change of order implementation in `msolve` [8].

Contributions. We push forward the study of the properties of the multiplication matrix M by y. Let $\mathcal{B}$ be the monomial basis of $\mathbb{K}[x_1, \ldots, x_{n-1}, y]/\mathcal{I}$ obtained from the reduced $\preccurlyeq_{\mathrm{drl}}$-Gröbner basis $\mathcal{G}$ of $\mathcal{I}$. Under the stability position assumption, its columns are either unit vectors (for those $\mu \in \mathcal{B}$ such that $y \cdot \mu \in \mathcal{B}$) or vectors of coefficients of polynomials in $\mathcal{G}$ (for thos $\mu \in \mathcal{B}$ such that $y \cdot \mu$ is a leading monomial of one element in $\mathcal{G}$). The latter ones are usually referred to as a "dense" columns [18, Sec. 5] [44, Sec. 4]. This is a well-known matrix structure in $\mathbb{K}$-linear algebra, called a *shifted form* in [39, 40], and studied in particular in the context of the computation of the characteristic polynomial or the Frobenius normal form of a matrix over $\mathbb{K}$ (see [45, Sec. 9.1] and Section 3.3).

We exploit the algebraic structure itself and relate it to operations in a $\mathbb{K}[y]$-submodule of $\mathcal{I}$. Following a classical construction in [45, Sec. 9.1], instead of the multiplication matrix M which is in $\mathbb{K}^{D\times D}$, we consider a univariate polynomial matrix P in $\mathbb{K}[y]^{t\times t}$ whose average column degree is D/t. This polynomial matrix can be seen as a "compression" of M, or more precisely of the characteristic matrix $yI_D - M$, with smaller matrix dimension but larger degrees.

Our main result is that, if P is known and the lexicographic Gröbner basis satisfies some assumption which covers the shape position case, then this Gröbner basis can be directly retrieved from the Hermite normal form of P (Theorem 4.1). We also prove that the matrix P can be computed for free from some part of a border basis of $\mathcal{I}$ in general (Theorem 5.2) and, as a consequence under the stability assumption, from the input Gröbner basis (Corollary 5.4). Observe that both structural assumptions, of being *stable* and *shape*, are used independently. In particular it is expected that in some situations where the stability assumption is not satisfied, P may still be obtained efficiently, and then its Hermite normal form yields the lexicographic Gröbner basis if $\mathcal{I}$ is in shape position.

The Hermite normal form can be computed deterministically in $O^{\tilde{}}(t^{\omega-1}D)$ operations in $\mathbb{K}$ [32], which dominates the overall complexity of the change of order.

Theorem 1.1. *Let $\mathcal{I} \subset \mathcal{R} = \mathbb{K}[x_1, \ldots, x_{n-1}, y]$ be a zero-dimensional ideal of degree D. Let $\mathcal{G}_{\preccurlyeq_{\mathrm{drl}}}$ (resp. $\mathcal{G}_{\preccurlyeq_{\mathrm{lex}}}$) be the reduced $\preccurlyeq_{\mathrm{drl}}$-(resp. $\preccurlyeq_{\mathrm{lex}}$-)Gröbner basis of $\mathcal{I}$ and $\mathcal{B}$ be the $\preccurlyeq_{\mathrm{drl}}$-monomial basis of $\mathcal{R}/\mathcal{I}$. Assume that $x_1, \ldots, x_{n-1}$ are in $\mathcal{B}$, and that for all monomials $\mu \in \mathcal{B}$, either $y \cdot \mu$ is in $\mathcal{B}$ or it is the $\preccurlyeq_{\mathrm{drl}}$-leading monomial of an element in $\mathcal{G}_{\preccurlyeq_{\mathrm{drl}}}$. Assume that $\mathcal{I}$ is in shape position. Then, one can compute $\mathcal{G}_{\mathrm{lex}}$ using $O^{\tilde{}}(t^{\omega-1}D)$ operations in $\mathbb{K}$, where t is the number of elements of $\mathcal{G}_{\preccurlyeq_{\mathrm{drl}}}$ whose $\preccurlyeq_{\mathrm{drl}}$-leading monomial is divisible by y.*

Compared to the previous $O(tD^2)$, the speed-up factor is of the order of $t^{2-\omega}D$. We give explicit complexity gains for families of polynomial systems for which closed formulas or asymptotic estimates for t and D are known [7, 18].

We study the practical performance of the new approach. For this, we designed an efficient implementation of the Hermite normal form, which follows the approach of [32] but tailored to the matrices P encountered here, which have specific degree shapes. This implementation relies on the Polynomial Matrix Library [28] (PML) and on NTL [43]. We show that it outperforms both the existing change of order algorithm in the current version of `msolve` [8], and an implementation of a block-Wiedemann approach in NTL.

Structure of the paper. Section 2 is devoted to preliminaries and detailed definitions of the shape position and stability assumptions. Section 3 shows how the aforementioned univariate polynomial matrix P can be obtained from a module-theoretic perspective. Section 4 establishes the connexion between the reduced $\preccurlyeq_{\mathrm{lex}}$-Gröbner basis of $\mathcal{I}$ and the Hermite normal form of P. Section 5 shows how to compute P from a Gröbner basis. Finally, in Section 6, we discuss complexity results and report on practical performance.

2 NOTATION AND PRELIMINARIES

Consider the polynomial ring $\mathcal{R} = \mathbb{K}[x_1, \ldots, x_{n-1}, y]$. For a nonzero polynomial $f \in \mathcal{R} \setminus \{0\}$, the *support* of f, denoted by $\mathrm{supp}(f)$, is the collection of all monomials appearing in f, with a nonzero coefficient. For a set of polynomials $S \subset \mathcal{R}$, the ideal generated by S in $\mathcal{R}$ is denoted by $\langle S \rangle$.

Monomial orders, normal forms. For the definition of a *monomial order* $\preccurlyeq$ on $\mathcal{R}$, we refer to [10, Chap. 2, §2]. We recall that $\preccurlyeq$ is a total order on the set of monomials, and we write $\prec$ for the corresponding strict order. Here, monomial orders are such that $y \prec x_{n-1} \prec \cdots \prec x_1$. We will use the *lexicographic* order $\preccurlyeq_{\mathrm{lex}}$, and the *degree reverse lexicographic* order $\preccurlyeq_{\mathrm{drl}}$. We denote by $\mathrm{lt}_{\preccurlyeq}(f)$ the $\preccurlyeq$-leading term of a nonzero polynomial $f \in \mathcal{R}$, and by $\mathrm{lt}_{\preccurlyeq}(S)$ the set of $\preccurlyeq$-leading terms of all nonzero elements of a set $S \subseteq \mathcal{R}$.

For a monomial order $\preccurlyeq$ and an ideal $\mathcal{I} \subset \mathcal{R}$, consider the set $\mathcal{B}$ of monomials in $\mathcal{R}$ that are not in the ideal of leading terms $\langle \mathrm{lt}_{\preccurlyeq}(\mathcal{I}) \rangle$. This set $\mathcal{B}$ is called the *$\preccurlyeq$-monomial basis* of $\mathcal{R}/\mathcal{I}$: it is a basis of $\mathcal{R}/\mathcal{I}$ as a $\mathbb{K}$-vector space [5, Prop. 6.52]. For a polynomial $f \in \mathcal{R}$, the *$\preccurlyeq$-normal form* of f with respect to $\mathcal{I}$, denoted by $\mathrm{nf}_{\preccurlyeq,\mathcal{I}}(f)$, is the unique polynomial whose support is in $\mathcal{B}$ and such that $f - \mathrm{nf}_{\preccurlyeq,\mathcal{I}}(f) \in \mathcal{I}$.

Gröbner bases, shape position. For the notion of (reduced) *$\preccurlyeq$-Gröbner bases* of ideals in $\mathcal{R}$, we refer to [10, Chap. 2]. By definition, for a $\preccurlyeq$-Gröbner basis $\mathcal{G}$ of $\mathcal{I}$, we have $\mathcal{G} \subset \mathcal{I}$ and $\langle \mathrm{lt}_{\preccurlyeq}(\mathcal{G}) \rangle = \langle \mathrm{lt}_{\preccurlyeq}(\mathcal{I}) \rangle$ and the $\preccurlyeq$-monomial basis $\mathcal{B}$ is also the set of monomials that are not multiples of an element in $\mathrm{lt}_{\preccurlyeq}(\mathcal{G})$.

A proper ideal $\mathcal{I} \subset \mathcal{R}$ is *zero-dimensional* [5, Def. 6.46] if and only if $\mathcal{R}/\mathcal{I}$ has finite dimension D as a $\mathbb{K}$-vector space [5, Thm. 6.54]. In that case, following [4], $\mathcal{I}$ is said to be in *shape position* if its reduced $\leqslant_{\text{lex}}$-Gröbner basis has the form

$$\mathcal{G}_{\text{lex}} = \{h(y),\ \ x_{n-1} - g_{n-1}(y),\ \ \ldots,\ \ x_1 - g_1(y)\}, \tag{1}$$

where $g_1, \ldots, g_{n-1}, h$ are in $\mathbb{K}[y]$. By properties of reduced Gröbner bases, this implies $\deg g_i < \deg h$ for $1 \leq i < n$. Then, $\mathcal{R}/\mathcal{I}$ is isomorphic to $\mathbb{K}[y]/\langle h(y)\rangle$ as an $\mathcal{R}$-module (equipping this quotient with the multiplication $x_i \cdot f = g_i(y)f$ for $1 \leq i < n$), and the $\leqslant_{\text{lex}}$-monomial basis is $(1, y, \ldots, y^{D-1})$ for $D = \deg h = \dim_{\mathbb{K}}(\mathcal{R}/\mathcal{I})$.

Stability assumption. This assumption, mentioned in Section 1, concerning the stability of the ideal of $\leqslant_{\text{drl}}$-leading terms of $\mathcal{I}$, is defined as follows.

Definition 2.1. For a set S of monomials in $\mathcal{R}$, the statement $\mathcal{S}(S)$ is: "for any monomial $\mu \in S$ such that y divides μ, the monomial $\frac{x_i}{y}\mu$ belongs to S for all $i \in \{1, \ldots, n-1\}$".

This is directly related to classical notions of stability of sets of monomials and of monomial ideals [26, Sec. 4.2.2, 6.3 and 7.2.2], which arise notably through the Borel-fixedness of generic initial ideals [3, 20]. The next lemma states that when considering the monomials in a monomial ideal, the above statement holds if, and only if, it holds for the minimal generating monomials of that ideal.

Lemma 2.2. *Let $\mathcal{J}$ be a monomial ideal of $\mathcal{R}$, and $\{\mu_1, \ldots, \mu_s\}$ be its minimal generating set. Let S be the set of monomials in $\mathcal{J}$. Then, $\mathcal{S}(S)$ is equivalent to $\mathcal{S}(\mu_1, \ldots, \mu_s)$.*

We do not prove this, as this is a direct consequence of [38, Lem. 2.2]. For our purpose, we are mostly interested in the case $\mathcal{J} = \text{lt}_{\leqslant}(\mathcal{I})$ for some monomial order $\leqslant$ and some ideal $\mathcal{I}$. The above lemma shows that, if $\text{lt}_{\leqslant}(\mathcal{I})$ is known (for example via the $\leqslant$-leading terms of a $\leqslant$-Gröbner basis), then it is straightforward to check whether $\mathcal{S}(\text{lt}_{\leqslant}(\mathcal{I}))$ holds.

Example 2.3. Consider the ideal $\mathcal{I}$ of $\mathbb{F}_{29}[x_1, x_2, y]$ generated by

$$\begin{aligned} x_2^2 + 12x_1y + 26x_2y + 5y^2 + 9x_1 + 6x_2 + 8y + 6, \\ x_1x_2 + 10x_2^2 + 10x_1y + 9y^2 + 2x_1 + 14x_2 + y + 13, \\ x_1^2 + 7x_1x_2 + 27x_2^2 + 15x_1y + 24x_2y + 3y^2 + 4x_1 + 28x_2 + 18y + 26. \end{aligned}$$

Its reduced $\leqslant_{\text{drl}}$-Gröbner basis $\mathcal{G}_{\text{drl}}$ consists of the polynomials

$$\begin{aligned} \boldsymbol{y^4} + 3y^3 + 15x_1y + 23x_2y + 3y^2 + 26x_2 + 22y, \\ \boldsymbol{x_2y^2} + 5x_1y + 28x_2y + 3y^2 + 19x_1 + 15x_2 + 17, \\ \boldsymbol{x_1y^2} + 18y^3 + 24x_1y + 27x_2y + 19y^2 + 2x_1 + 9y + 3, \\ x_2^2 + 12x_1y + 26x_2y + 5y^2 + 9x_1 + 6x_2 + 8y + 6, \\ x_1x_2 + 6x_1y + x_2y + 17y^2 + 28x_1 + 12x_2 + 8y + 11, \\ x_1^2 + x_1y + 10x_2y + 2y^2 + 3x_1 + 16x_2 + 21. \end{aligned}$$

Observe that it has $t = 3$ polynomials whose $\leqslant_{\text{drl}}$-leading terms, in boldface font, are multiples of y. The $\leqslant_{\text{drl}}$-monomial basis $\mathcal{B}$ of $\mathcal{R}/\mathcal{I}$ is the set of monomials not in

$$\langle \text{lt}_{\leqslant_{\text{drl}}}(\mathcal{G}_{\text{drl}})\rangle = \langle y^4, x_2y^2, x_1y^2, x_2^2, x_1x_2, x_1^2\rangle,$$

that is, $\mathcal{B} = (1, y, y^2, y^3, x_2, x_2y, x_1, x_1y)$.

Finally, we verify that the stability property $\mathcal{S}(\text{lt}_{\leqslant_{\text{drl}}}(\mathcal{I}))$ holds. As noted in Lemma 2.2, it is sufficient to check that for each minimal generator μ of $\langle \text{lt}_{\leqslant_{\text{drl}}}(\mathcal{I})\rangle$ such that y divides μ, the monomials $\frac{x_1}{y}\mu$ and $\frac{x_2}{y}\mu$ remain in $\text{lt}_{\leqslant_{\text{drl}}}(\mathcal{I})$. Thus we consider $\mu \in \{x_2y^2, x_1y^2, y^4\}$, and it is easily verified that x_1x_2y, x_2^2y, x_1^2y, x_1x_2y, x_1y^3, x_2y^3 are all in $\text{lt}_{\leqslant_{\text{drl}}}(\mathcal{I})$. □

3 RESTRICTING TO A $\mathbb{K}[y]$-MODULE

The algorithmic approach in this paper makes use of a $\mathbb{K}[y]$-module denoted by $\mathcal{M}_{\mathcal{T},\mathcal{I}}$, which is defined from an ideal $\mathcal{I}$ and a set of monomials $\mathcal{T}$. Using the module addition of $\mathbb{K}[x_1, \ldots, x_{n-1}, y]$, this module is a subset of $\mathcal{I}$, which is sufficient to recover the $\leqslant_{\text{lex}}$-Gröbner basis of $\mathcal{I}$ in the shape position case, and which allows us to benefit from efficient algorithms for matrices over $\mathbb{K}[y]$.

3.1 General definitions and properties

See [11, Chap. 10] for general definitions and properties of modules. Roughly, *free* modules are those which admit a basis, and since $\mathbb{K}[y]$ is commutative, all bases of a free $\mathbb{K}[y]$-module have the same cardinality which is called the *rank* of the module [11, Sec. 10.3].

For modules over a principal ideal domain such as $\mathbb{K}[y]$, we refer to [11, Chap. 12]. In particular, if $\mathcal{N}$ is a free $\mathbb{K}[y]$-module of rank $t \in \mathbb{N}$ and $\mathcal{M}$ is a $\mathbb{K}[y]$-submodule of $\mathcal{N}$, then $\mathcal{M}$ is free and its rank ρ is at most t [11, Sec. 12.1, Thm. 4]. As a result, $\mathcal{M}$ has a basis of cardinality ρ, which can be represented as a matrix in $\mathbb{K}[y]^{\rho\times t}$. This matrix has full row rank, and its rows are the basis elements. Furthermore $\mathcal{M}$ has a unique basis in a specific form, at the core of this work: the *Hermite normal form* [25, 29]. When $\rho = t$, a matrix $P = [p_{ij}] \in \mathbb{K}[y]^{t\times t}$ is in Hermite normal form if:

- P is lower triangular;
- the diagonal entries of P are monic;
- in each column of P, the diagonal entry has degree greater than the other entries, i.e. $\deg(p_{ij}) < \deg(p_{jj})$ for $i \neq j$.

A typical example of ambient module is $\mathcal{N} = \mathbb{K}[y]^t$. Here we will also consider the $\mathbb{K}[y]$-module $\mathcal{N} = \mathcal{R}_{\mathcal{T}} \subset \mathcal{R}$, defined as follows. Let $\mathcal{T} = (\mu_1, \ldots, \mu_t)$ be a list of pairwise distinct monomials in $\mathbb{K}[x_1, \ldots, x_{n-1}]$, and consider the set of monomials

$$\mathcal{T}^* = \{y^e\mu \mid \mu \in \mathcal{T}, e \geq 0\}$$

of y-multiples of a monomial in $\mathcal{T}$. Then we define

$$\mathcal{R}_{\mathcal{T}} = \{f \in \mathcal{R} \mid \text{supp}(f) \in \mathcal{T}^*\}, \tag{2}$$

which is a free $\mathbb{K}[y]$-module of rank t, with basis given by $\mathcal{T}$.

Hereafter, for a finite set of polynomials $S \subset \mathcal{R}$, the $\mathbb{K}[y]$-module generated by S will be denoted by $\langle\!\langle S\rangle\!\rangle$.

Example 3.1. Let $\mathcal{T} = (1, x_{n-1}, \ldots, x_1)$. Then

$$\mathcal{R}_{\mathcal{T}} = \langle\!\langle 1, x_{n-1}, \ldots, x_1\rangle\!\rangle = \mathbb{K}[y] + x_{n-1}\mathbb{K}[y] + \cdots + x_1\mathbb{K}[y]$$

is a $\mathbb{K}[y]$-submodule of $\mathcal{R}$ of rank n. □

3.2 A module associated to the ideal

Consider the $\mathbb{K}[y]$-module $\mathcal{R}_{\mathcal{T}}$ as in Section 2, for some pairwise distinct monomials $\mathcal{T} = (\mu_1, \ldots, \mu_t)$ in $\mathbb{K}[x_1, \ldots, x_{n-1}]$. This module is free of rank t, with basis $\mathcal{T}$. Then, for any ideal $\mathcal{I}$ of $\mathcal{R}$, let

$$\mathcal{M}_{\mathcal{T},\mathcal{I}} = \mathcal{I} \cap \mathcal{R}_{\mathcal{T}}. \tag{3}$$

By construction, we have the inclusion of ideals $\langle \mathcal{M}_{\mathcal{T},\mathcal{I}} \rangle \subseteq \mathcal{I}$.

Example 3.2. Let $\mathcal{T}$ be as in Example 3.1. Then $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ is the set of polynomials in $\mathcal{I}$ which have degree at most 1 in each of the variables $x_{n-1}, \ldots, x_1$, and

- for $\mathcal{I} = \langle x_1^2 \rangle$, $\mathcal{M}_{\mathcal{T},\mathcal{I}} = \{0\}$ and $\langle \mathcal{M}_{\mathcal{T},\mathcal{I}} \rangle \subsetneq \mathcal{I}$;
- for $\mathcal{I} = \langle x_1 - 1 \rangle$, $\mathcal{M}_{\mathcal{T},\mathcal{I}} = (x_1 - 1)\mathbb{K}[y]$ and $\langle \mathcal{M}_{\mathcal{T},\mathcal{I}} \rangle \subsetneq \mathcal{I}$;
- for a zero-dimensional ideal $\mathcal{I}$, if $\mathcal{I}$ is in shape position then $\langle \mathcal{M}_{\mathcal{T},\mathcal{I}} \rangle = \mathcal{I}$ (see Lemma 5.1). □

The case of equality $\langle \mathcal{M}_{\mathcal{T},\mathcal{I}} \rangle = \mathcal{I}$ is of particular interest: it ensures that no information is lost when restricting to polynomials with monomial support in $\mathcal{T}^*$. Our aim is to compute objects related to $\mathcal{I}$, such as its $\preccurlyeq_{\text{lex}}$-Gröbner basis, using only computations in the smaller submodule $\mathcal{M}_{\mathcal{T},\mathcal{I}}$. The motivation behind this idea is that many efficient tools are known for computing with $\mathcal{M}_{\mathcal{T},\mathcal{I}}$, thanks to the matrix representation explained below.

As seen in Section 3.1, as a $\mathbb{K}[y]$-submodule of $\mathcal{R}_{\mathcal{T}}$, $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ is free of rank ρ, with $\rho \leq t$, and any basis of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ is a collection of ρ polynomials $\{P_1, \ldots, P_\rho\} \subset \mathcal{R}_{\mathcal{T}}$. Such a basis can be represented as a matrix

$$P = \begin{bmatrix} P_{11} & \cdots & P_{1t} \\ \vdots & \vdots & \vdots \\ P_{\rho 1} & \cdots & P_{\rho t} \end{bmatrix} \in \mathbb{K}[y]^{\rho \times t} \tag{4}$$

of rank ρ, whose row i is formed by the univariate polynomials $P_{i1}, \ldots, P_{it}$ in $\mathbb{K}[y]$ such that $P_i = P_{i1}\mu_1 + \cdots + P_{it}\mu_t$.

Example 3.3 (following on from Example 2.3). Take $\mathcal{T}$ as the set of monomials in $\mathcal{B}$ which are not multiples of y, that is, $\mathcal{T} = (1, x_2, x_1)$; observe that the cardinality of $\mathcal{T}$ is $t = 3$. As noted in Example 3.1, $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ is then the set of polynomials in $\mathcal{I}$ which have degree at most 1 in x_1 and in x_2. This is the case for 3 polynomials of $\mathcal{G}_{\text{drl}}$:

$$\boldsymbol{y^4} + 3y^3 + 15x_1y + 23x_2y + 3y^2 + 26x_2 + 22y,$$
$$\boldsymbol{x_2y^2} + 5x_1y + 28x_2y + 3y^2 + 19x_1 + 15x_2 + 17,$$
$$\boldsymbol{x_1y^2} + 18y^3 + 24x_1y + 27x_2y + 19y^2 + 2x_1 + 9y + 3.$$

Hence these polynomials are in $\mathcal{M}_{\mathcal{T},\mathcal{I}}$; note they are exactly the polynomials of $\mathcal{G}_{\text{drl}}$ whose $\preccurlyeq_{\text{drl}}$-leading terms are multiples of y. In Section 5 we will prove that, since $\mathcal{S}(\text{lt}_{\preccurlyeq_{\text{drl}}}(\mathcal{I}))$ is satisfied (see Example 2.3), these polynomials form a basis of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$.

Representing these polynomials on the basis $\mathcal{T}$ of $\mathcal{R}_{\mathcal{T}}$, we obtain the following matrix in $\mathbb{F}_{29}[y]^{t\times t}$:

$$P = \begin{bmatrix} y^4 + 3y^3 + 3y^2 + 22y & 23y + 26 & 15y \\ 3y^2 + 17 & y^2 + 28y + 15 & 5y + 19 \\ 18y^3 + 19y^2 + 9y + 3 & 27y & y^2 + 24y + 2 \end{bmatrix}.$$

Note that this matrix is directly read off from $\mathcal{G}_{\text{drl}}$. □

We end this section by showing that if $\mathcal{I}$ is zero-dimensional, then the bases $P \in \mathbb{K}[y]^{\rho\times t}$ of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ are square, nonsingular matrices. This is implied by the first item of the following lemma, thanks to the fact that a zero-dimensional ideal contains a univariate polynomial in each variable [5, Lem. 6.50]. For completeness, we also give a partial converse property in the second item.

Lemma 3.4. *With the above notation,*

- *If there exists a nonzero univariate $h \in \mathcal{I} \cap \mathbb{K}[y]$, then $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ has rank $\rho = t$ as a $\mathbb{K}[y]$-module.*
- *If $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ has rank $\rho = t$ as a $\mathbb{K}[y]$-module and $1 \in \mathcal{T}$, then there exists a nonzero univariate $h \in \mathcal{I} \cap \mathbb{K}[y]$.*

Proof. We already observed that $\rho \leq t$. *First item:* assuming the existence of h, the set $g\mathcal{R}_{\mathcal{T}} = \{hf \mid f \in \mathcal{R}_{\mathcal{T}}\}$ is a $\mathbb{K}[y]$-module of rank t, having $h\mathcal{T}$ as a basis. Since $h \in \mathcal{I}$, $h\mathcal{R}_{\mathcal{T}}$ is contained in $\mathcal{M}_{\mathcal{T},\mathcal{I}}$, which implies $t \leq \rho$ as recalled in Section 2. Hence $\rho = t$. *Second item:* assuming $\rho = t$, we define $P \in \mathbb{K}[y]^{t\times t}$ as in Eq. (4), from a basis $\{P_1, \ldots, P_\rho\} \subset \mathcal{R}_{\mathcal{T}}$ of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$. Then, we let $h = \det(P) \in \mathbb{K}[y]$, which is nonzero since P is nonsingular. By assumption, there exists $j \in \{1, \ldots, t\}$ such that $\mu_j = 1$. Then, by Cramer's rule, there are $u_1, \ldots, u_t \in \mathbb{K}[y]$ such that $[u_1 \ \cdots \ u_t]P = [0 \ \cdots \ 0 \ \ h \ \ 0 \ \cdots \ 0]$ with h at the jth position. By construction of P, this means $u_1P_1 + \cdots + u_tP_t = h\mu_j = h$, hence $h \in \mathcal{I}$. □

3.3 Link with the multiplication matrix

In Example 3.3, the basis $P \in \mathbb{K}[y]^{t\times t}$ of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ can be seen as a compact representation of the operator of multiplication by y in $\mathcal{R}/\mathcal{I}$. The more classical representation uses a *multiplication matrix*, which is the matrix of this operator expressed on the $\preccurlyeq$-monomial basis. We have seen that in the case of Examples 2.3 and 3.3, the $\preccurlyeq_{\text{drl}}$-monomial basis is $\mathcal{B} = (1, y, y^2, y^3, x_2, x_2y, x_1, x_1y)$. Then this multiplication matrix is

$$M = \left[\begin{array}{cccc|cc|cc} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 7 & 26 & 26 & 3 & 6 & 0 & 14 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 12 & 0 & 26 & 0 & 14 & 1 & 10 & 24 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 26 & 20 & 10 & 11 & 0 & 2 & 27 & 5 \end{array}\right] \in \mathbb{K}^{D\times D}.$$

The choice of ordering of $\mathcal{B}$ makes the following structure obvious: this matrix has companion blocks on the diagonal, and its other blocks have zeroes everywhere but possibly on the last row. Note how the basis P from Example 3.3 can be built by replacing each block by a single polynomial in $\mathbb{K}[y]$ (recall here $\mathbb{K} = \mathbb{F}_{29}$):

- companion blocks are replaced by their respective characteristic polynomials, for example the first companion block becomes $y^4 - (26y^3 + 26y^2 + 7y) = y^4 + 3y^3 + 3y^2 + 22y$;
- other blocks by are replaced by the opposite of the polynomial given by the last row, for example the block $(3, 1)$ yields $-(11y^3 + 10y^2 + 20y + 26) = 18y^3 + 19y^2 + 9y + 3$.

Both this type of structure for matrices over a field and the corresponding compact representation as univariate polynomial matrices have been studied, in particular concerning questions of matrix similarity. For example, the Frobenius normal form of M corresponds to the Smith normal form of P [45, Thm. 9.1], whereas the shifted Hessenberg form of M corresponds to the Hermite normal form of P [45, Thm. 9.5 and Lem. 9.7]. More recently, such matrix structures were instrumental in the design of fast algorithms for the Frobenius normal form of a matrix over a field [39, 40].

However, to our knowledge, in the context of Gröbner basis change of order, this structure of the multiplication matrix had only been exploited through the sparsity it brings, in order to rely on (block-)Wiedemann techniques [18, 27, 44].

4 RETRIEVING LEXICOGRAPHIC GRÖBNER BASES FROM HERMITE NORMAL FORMS

From a matrix P as in Eq. (4), whose rows in $\mathbb{K}[y]^{1\times t}$ represent a basis of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$, one can compute the reduced Gröbner basis of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ with respect to a chosen monomial order on $\mathbb{K}[y]^{1\times t}$; see [12, Chap. 15] for Gröbner bases of submodules of a free module with basis. Here this ambient free module is $\mathcal{R}_{\mathcal{T}} \simeq \mathbb{K}[y]^{1\times t}$, with $\mathbb{K}[y]$ univariate: specific terminology and computational tools exist. In particular, classical reduced Gröbner bases are the Hermite normal form [25] (corresponding to the position-over-term order [30]), the Popov normal form [42] (corresponding to the term-over-position order [30]), and shifted variants of the latter [6] (corresponding to term-over-position orders with weights [36, Sec. 1.3.4]). The definition of Hermite normal forms was given in Section 2.

However, these Gröbner bases of the submodule $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ do not necessarily correspond to Gröbner bases of the ideal $\mathcal{I}$, even when $\langle \mathcal{M}_{\mathcal{T},\mathcal{I}} \rangle = \mathcal{I}$. The next result states that, under the stability assumption, there is a correspondence between the lexicographic Gröbner basis of $\mathcal{I}$ and the basis of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ in Hermite normal form. (A link of this kind is not new [33, Sec. 5] [47, Sec. 7], yet we were not able to find a statement similar to the next one in the literature.)

Theorem 4.1. *Let $\mathcal{I}$ be a zero-dimensional ideal of $\mathcal{R}$ and let $\mathcal{G}_{\mathrm{lex}}$ be the reduced $\preccurlyeq_{\mathrm{lex}}$-Gröbner basis of $\mathcal{I}$. Let $\mathcal{T} = (\mu_1, \ldots, \mu_t)$ be pairwise distinct monomials in $\mathbb{K}[x_1, \ldots, x_{n-1}]$, sorted increasingly according to $\preccurlyeq_{\mathrm{lex}}$. Define $\mathcal{R}_{\mathcal{T}}$ and $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ as in Eqs. (2) and (3). Let $H \in \mathbb{K}[y]^{t\times t}$ be the basis of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ in Hermite normal form.*

Assuming $\mathcal{G}_{\mathrm{lex}} \subseteq \mathcal{R}_{\mathcal{T}}$, then $\mathcal{G}_{\mathrm{lex}}$ can be read off from the rows of H. Explicitly, let f be an element of $\mathcal{G}_{\mathrm{lex}}$ and let i be the unique integer in $\{1, \ldots, t\}$ such that $\mathrm{lm}_{\preccurlyeq_{\mathrm{lex}}}(f) = y^e\mu_i$ for some $e \geq 0$. Then the ith row of H has the form $[f_1 \ \cdots \ f_i \ 0 \ \cdots \ 0] \in \mathbb{K}[y]^{1\times t}$, with $\deg(f_i) = e$ and $f = f_1\mu_1 + \cdots + f_i\mu_i$.

Proof. In this proof, $\preccurlyeq$ stands for the lexicographic order $\preccurlyeq_{\mathrm{lex}}$.

Let f be an element of $\mathcal{G}_{\mathrm{lex}}$. Since $\mathcal{G}_{\mathrm{lex}} \subseteq \mathcal{R}_{\mathcal{T}}$, every monomial of f belongs to $\mathcal{T}^* = \{y^e\mu_j \mid 1 \leq j \leq t, e \geq 0\}$. In particular, $\mathrm{lm}_{\preccurlyeq}(f) = y^e\mu_i$ for some i in $\{1, \ldots, t\}$ and $e \geq 0$ (and i is unique since the μ_j's are pairwise distinct).

Since $f \in \mathcal{R}_{\mathcal{T}}$, and $\mathcal{T}$ is a basis of $\mathcal{R}_{\mathcal{T}}$ as a $\mathbb{K}[y]$-module, there is a unique $[f_1 \ \cdots \ f_t] \in \mathbb{K}[y]^{1\times t}$ such that $f = f_1\mu_1 + \cdots + f_t\mu_t$.

Let $j \in \{i+1, \ldots, t\}$. We are going to prove $f_j = 0$. Recall that $y \prec x_k$ for $1 \leq k \leq n-1$, and that the monomial μ_j only involves the variables $x_1, \ldots, x_{n-1}$. Besides, $\mathcal{T}$ being sorted increasingly ensures $\mu_i \prec \mu_j$. Hence $y^e\mu_i \prec y^d\mu_j$ for any $d \geq 0$: having $f_j \neq 0$ would contradict $\mathrm{lm}_{\preccurlyeq}(f) = y^e\mu_i$.

Thus $f = f_1\mu_1 + \cdots + f_i\mu_i$, and $\mathrm{lm}_{\preccurlyeq}(f) = y^e\mu_i$ ensures $\deg(f_i) = e$. It remains to show that the ith row of H is equal to $[f_1 \cdots f_i \ 0 \cdots 0]$.

We first show that the ith diagonal entry of H has degree $e = \deg(f_i)$. On the one hand, the ith row of H corresponds to a nonzero polynomial in $\mathcal{I}$ whose $\preccurlyeq$-leading term is $y^d\mu_i$. Then, having $d < e$ would mean that $\mathrm{lt}_{\preccurlyeq}(f)$ is a strict multiple of the $\preccurlyeq$-leading term of some element of $\mathcal{I}$, which contradicts the definition of $\mathcal{G}_{\mathrm{lex}}$. Thus $d \geq e$. On the other hand, f is in $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ and therefore corresponds to a vector in the $\mathbb{K}[y]$-row space of H whose rightmost nonzero entry is at index i. Then, the triangularity of H implies that

$$[f_1 \ \cdots \ f_i \ 0 \ \cdots \ 0] = [\lambda_1 \ \cdots \ \lambda_i \ 0 \ \cdots \ 0]H$$

for some $\lambda_1, \ldots, \lambda_i \in \mathbb{K}[y]$ and $\lambda_i \neq 0$. Using the triangularity again, we obtain $e = \deg(f_i) = \deg(\lambda_i) + d$, hence $d \leq e$. This yields $e = d$.

Let $d_1, \ldots, d_{i-1} \in \mathbb{N}$ be the degrees of the first $i-1$ diagonal entries of H. In this paragraph we show that, to conclude the proof, it is enough to prove $\deg(f_j) < d_j$ for $1 \leq j < i$. Indeed, as seen above, the vector $[f_1 \ \cdots \ f_i \ 0 \ \cdots \ 0]$ is in the $\mathbb{K}[y]$-row space of H, and has rightmost nonzero entry f_i at index i, which has the same degree as the ith diagonal entry of H and is monic by definition of a reduced $\preccurlyeq$-Gröbner basis. Thus, if $\deg(f_j) < d_j$ for $1 \leq j < i$, then this vector must be equal to the ith row of H, by uniqueness of the Hermite normal form: otherwise one could replace the ith row of H by this vector and get a different Hermite normal form for the same $\mathbb{K}[y]$-module.

Let $1 \leq j < i$. We are going to prove $\deg(f_j) < d_j$. The jth row of H yields a polynomial in $\mathcal{I}$ with $\preccurlyeq$-leading term $y^{d_j}\mu_j$, hence $y^{d_j}\mu_j \in \langle \mathrm{lt}_{\preccurlyeq}(\mathcal{I}) \rangle$. At the same time, since $\mathcal{G}_{\mathrm{lex}}$ is reduced, $\mathrm{lt}_{\preccurlyeq}(f) = y^e\mu_i$ is the only monomial appearing in f which is in $\langle \mathrm{lt}_{\preccurlyeq}(\mathcal{I}) \rangle$. In particular, defining $d = \deg(f_j)$, the monomial $y^d\mu_j$ of f is not a multiple of or equal to $y^{d_j}\mu_j$, hence $d < d_j$. □

Example 4.2 (following on from Example 3.3). Computing the Hermite normal form of the basis matrix P from Example 3.3 yields

$$H = \begin{bmatrix} y^8 + 26y^7 + 8y^6 + 17y^5 + 19y^4 + y^3 + 28y^2 + 20y + 18 & 0 & 0 \\ 28y^7 + 23y^6 + 17y^5 + 25y^4 + 24y^3 + 17y^2 + 14y + 4 & 1 & 0 \\ 6y^7 + 13y^6 + 22y^5 + 12y^4 + 28y^3 + 24y^2 + 26y + 14 & 0 & 1 \end{bmatrix}.$$

This is the basis of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ in Hermite normal form; recall that here $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ is the $\mathbb{K}[y]$-submodule of polynomials in $\mathcal{I}$ which have the form $p_1(y) + p_2(y)x_2 + p_3(y)x_1$. This basis gives the $\preccurlyeq_{\mathrm{lex}}$-Gröbner basis of $\mathcal{I}$:

$$y^8 + 26y^7 + 8y^6 + 17y^5 + 19y^4 + y^3 + 28y^2 + 20y + 18,$$
$$x_2 + 28y^7 + 23y^6 + 17y^5 + 25y^4 + 24y^3 + 17y^2 + 14y + 4,$$
$$x_1 + 6y^7 + 13y^6 + 22y^5 + 12y^4 + 28y^3 + 24y^2 + 26y + 14. \quad \square$$

Suppose the basis H of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ in Hermite normal form is known. If $\mathrm{lt}_{\preccurlyeq}(\mathcal{G}_{\mathrm{lex}})$ is known as well, which is the case under the shape position assumption, then Theorem 4.1 indicates precisely which rows of H give the polynomials of $\mathcal{G}_{\mathrm{lex}}$, without any further computation.

Remark 4.3. *Even when $\mathrm{lt}_{\preccurlyeq_{\mathrm{lex}}}(\mathcal{G}_{\mathrm{lex}})$ is unknown, $\mathcal{G}_{\mathrm{lex}}$ is easily found from H. Indeed, H yields polynomials $h_1, \ldots, h_t$ in $\mathcal{M}_{\mathcal{T},\mathcal{I}} \subseteq \mathcal{I}$, and Theorem 4.1 ensures that they include the polynomials of $\mathcal{G}_{\mathrm{lex}}$. Thus $\{h_1, \ldots, h_t\}$ is a $\preccurlyeq_{\mathrm{lex}}$-Gröbner basis of $\mathcal{I}$, and filtering out from it the polynomials which are not in $\mathcal{G}_{\mathrm{lex}}$ is easily done and computationally cheap, by following the classical procedure for transforming a non-minimal Gröbner basis into a minimal one. Explicitly:*

- *let $v_i = \mathrm{lt}_{\preccurlyeq_{\mathrm{lex}}}(h_i)$ for $1 \leq i \leq t$;*
- *find the indices $1 \leq i_1 < \cdots < i_s \leq t$ such that $\{v_{i_1}, \ldots, v_{i_s}\}$ is a minimal generating set of the monomial ideal $\langle v_1, \ldots, v_t \rangle$;*
- *then $\mathcal{G}_{\mathrm{lex}} = \{h_{i_1}, \ldots, h_{i_s}\}$.*

Note that the uniqueness of the indices $i_1, \ldots, i_s$ is ensured by the fact that $v_1, \ldots, v_t$ are pairwise distinct by construction.

5 CONSTRUCTING A BASIS OF THE MODULE FROM A KNOWN GRÖBNER BASIS

There are two missing ingredients in order to use the above framework to compute $\mathcal{G}_{\mathrm{lex}}$. First, the assumptions of Theorem 4.1 must

be satisfied. Second, we need an efficient method to compute the basis H of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ in Hermite normal form; for this, known methods require the knowledge of some basis $P \in \mathbb{K}[y]^{t\times t}$ of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$.

The assumption that $\mathcal{I}$ is zero-dimensional will be guaranteed from our context. The main constraint is therefore the choice of $\mathcal{T}$ in order to ensure that $\mathcal{G}_{\text{lex}} \subset \mathcal{R}_{\mathcal{T}}$ is satisfied. This relates to the more general equality $\langle \mathcal{M}_{\mathcal{T},\mathcal{I}} \rangle = \mathcal{I}$, via the following characterization: $\langle \mathcal{M}_{\mathcal{T},\mathcal{I}} \rangle = \mathcal{I}$ if and only if there exists a generating set of $\mathcal{I}$ formed by polynomials in $\mathcal{R}_{\mathcal{T}}$. Obviously, taking $\mathcal{T}$ large enough ensures $\mathcal{G}_{\text{lex}} \subset \mathcal{R}_{\mathcal{T}}$; yet a larger set $\mathcal{T}$ also means a larger matrix dimension t and thus more expensive computations to find P and deduce H.

Now, focusing on the shape position case as explained in Section 1, all monomials occurring in $\mathcal{G}_{\text{lex}}$ are either in $\{x_{n-1}, \ldots, x_1\}$ or in $\{y^e \mid e \geq 0\}$. Hence the following lemma.

Lemma 5.1. *Using notation from Theorem 4.1, assume the ideal $\mathcal{I}$ is zero-dimensional and in shape position. If $\{1, x_{n-1}, \ldots, x_1\} \subseteq \mathcal{T}$, then $\mathcal{G}_{\text{lex}} \subset \mathcal{R}_{\mathcal{T}}$.*

Therefore, in the shape position case, the condition $\mathcal{G}_{\text{lex}} \subseteq \mathcal{R}_{\mathcal{T}}$ is easily satisfied, and the main missing ingredient is an efficient method for computing P. The next theorem shows that, for any monomial order $\preccurlyeq$, the knowledge of some $\preccurlyeq$-*border basis* of $\mathcal{I}$ [34] directly provides a suitable set $\mathcal{T}$ and a corresponding basis $P \in \mathbb{K}[y]^{t\times t}$ of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$. Furthermore, this matrix P has a particular degree pattern related to the $\preccurlyeq$-monomial basis of $\mathcal{I}$.

In Corollary 5.4 we deduce that, under the stability assumption $\mathcal{S}(\mathrm{lt}_{\preccurlyeq}(\mathcal{I}))$, the knowledge of the reduced $\preccurlyeq$-Gröbner basis of $\mathcal{I}$ is enough to find $\mathcal{T}$ and P. Then, it will only remain to find the Hermite normal form of P, which is the sought basis H: the efficient computation of H from P is discussed in Section 6.1.

Theorem 5.2. *Let $\preccurlyeq$ be a monomial order such that $y \prec x_i$ for $1 \leq i \leq n-1$. Let $\mathcal{I}$ be a zero-dimensional ideal in $\mathcal{R}$ and let $\mathcal{B}$ be the $\preccurlyeq$-monomial basis of $\mathcal{R}/\mathcal{I}$. Let $\mathcal{T} = (\mu_1, \ldots, \mu_t)$ be the monomials in $\mathcal{B}$ which are not divisible by y, i.e. $\mathcal{T} = \mathcal{B} \cap \mathbb{K}[x_1, \ldots, x_{n-1}]$. Then,*

$$\{\mu \in \mathcal{B} \mid y\mu \notin \mathcal{B}\} = \{y^{e_i-1}\mu_i \mid 1 \leq i \leq t\} \tag{5}$$

for some $e_1, \ldots, e_t \in \mathbb{Z}_{>0}$ with $e_1 + \cdots + e_t = \dim_{\mathbb{K}}(\mathcal{R}/\mathcal{I})$, and

$$\mathcal{P} = \{y^{e_i}\mu_i - \mathrm{nf}_{\preccurlyeq,\mathcal{I}}(y^{e_i}\mu_i) \mid 1 \leq i \leq t\}$$

is a basis of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ as a $\mathbb{K}[y]$-module.

Furthermore, representing $\mathcal{P}$ as a matrix $P \in \mathbb{K}[y]^{t\times t}$ whose ith row contains the coefficients of $y^{e_i}\mu_i - \mathrm{nf}_{\preccurlyeq,\mathcal{I}}(y^{e_i}\mu_i)$ on the basis $\mathcal{T}$ of $\mathcal{R}_{\mathcal{T}}$, it holds that $P = \mathrm{diag}(y^{e_1}, \ldots, y^{e_t}) + R$ where $R \in \mathbb{K}[y]^{t\times t}$, with the jth column of R of degree less then e_j for $1 \leq j \leq t$.

Proof. First note that, since $\mathcal{I}$ is zero-dimensional, $\mathcal{B}$ is finite and therefore $\mathcal{T}$ is finite as well. Concerning the identity in Eq. (5) we first observe that, since $\mathcal{B}$ is finite and is the complement of $\mathrm{lt}_{\preccurlyeq}(\mathcal{I})$, for each $i \in \{1, \ldots, t\}$ there is a unique $e \in \mathbb{Z}_{>0}$ such that $y^{e-1}\mu_i \in \mathcal{B}$ and $y^e\mu_i \notin \mathcal{B}$. Conversely, for any $\mu \in \mathcal{B}$ such that $y\mu \notin \mathcal{B}$, the integer $e = 1 + \max\{j \in \mathbb{N} \mid y^j \text{ divides } \mu\}$ satisfies $y^{1-e}\mu \in \mathcal{T}$, hence $\mu = y^{e-1}\mu_i$ for some i. This shows Eq. (5).

Now, concerning $\mathcal{P}$, its elements are in $\mathcal{I}$ by definition of the $\preccurlyeq$-normal form (see Section 2), hence $\mathcal{P} \subseteq \mathcal{M}_{\mathcal{T},\mathcal{I}}$. Furthermore $\mathcal{P}$ has cardinality t, which is the cardinality of $\mathcal{T}$ and therefore the rank of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ (see Lemma 3.4). Thus, to prove that $\mathcal{P}$ is a basis of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ it is sufficient to show that any polynomial f in $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ is a $\mathcal{R}$-linear combination of $\mathcal{P}$, that is, $f \in \langle\!\langle \mathcal{P} \rangle\!\rangle$. Since $f \in \mathcal{M}_{\mathcal{T},\mathcal{I}}$,

$$\begin{aligned} f &\in \mathrm{Span}_{\mathbb{K}}(\{y^e\mu_i \mid 1 \leq i \leq t, e \in \mathbb{N}\}) \\ &= \mathrm{Span}_{\mathbb{K}}(\mathcal{B} \cup \{y^{e_i+k}\mu_i \mid 1 \leq i \leq t, k \in \mathbb{N}\}). \end{aligned}$$

On the other hand, as showed in Lemma 5.3, $y^{e_i+k}\mu_i - b_{i,k} \in \langle\!\langle \mathcal{P} \rangle\!\rangle$ for some $b_{i,k} \in \mathrm{Span}_{\mathbb{K}}(\mathcal{B})$, for all $1 \leq i \leq t$ and $k \in \mathbb{N}$. Altogether, this implies that $f = b + p$, for some $b \in \mathrm{Span}_{\mathbb{K}}(\mathcal{B})$ and $p \in \langle\!\langle \mathcal{P} \rangle\!\rangle$. Since $\langle\!\langle \mathcal{P} \rangle\!\rangle \subseteq \mathcal{M}_{\mathcal{T},\mathcal{I}}$, we have $f - p \in \mathcal{M}_{\mathcal{T},\mathcal{I}} \subseteq \mathcal{I}$ and therefore $b = \mathrm{nf}_{\preccurlyeq,\mathcal{I}}(f) = 0$. Hence $f \in \langle\!\langle \mathcal{P} \rangle\!\rangle$.

Finally, consider the matrix representation P of $\mathcal{P}$. As seen in Section 3.2, the ith row of P is the vector $[p_1 \ \cdots \ p_t] \in \mathbb{K}[y]^{1\times t}$ such that $y^{e_i}\mu_i - \mathrm{nf}_{\preccurlyeq,\mathcal{I}}(y^{e_i}\mu_i) = p_1\mu_1 + \cdots + p_t\mu_t$. Therefore all monomials of $p_1\mu_1 + \cdots + p_t\mu_t - y^{e_i}\mu_i$ are in $\mathcal{B}$. By definition of the e_j's, it follows that $\deg(p_j) < e_j$ for all $j \neq i$, and $\deg(p_i - y^{e_i}) < e_i$. This shows that the jth column of $R = P - \mathrm{diag}(y^{e_1}, \ldots, y^{e_t})$ has degree less than e_j, for $1 \leq j \leq t$. □

Lemma 5.3. *Using notation from Theorem 5.2, for all $k \in \mathbb{N}$ and $i \in \{1, \ldots, t\}$, $y^{e_i+k}\mu_i - b_{i,k} \in \langle\!\langle \mathcal{P} \rangle\!\rangle$, where we have defined $b_{i,k} = \mathrm{nf}_{\preccurlyeq,\mathcal{I}}(y^{e_i+k}\mu_i) \in \mathrm{Span}_{\mathbb{K}}(\mathcal{B})$.*

Proof. We prove this by induction on k, noting that this property holds for $k = 0$ by definition of $\mathcal{P}$. Now, consider $k \in \mathbb{Z}_{>0}$ and suppose the property holds for all integers up to $k-1$. Let $i \in \{1, \ldots, t\}$. By induction hypothesis there exists $p \in \langle\!\langle \mathcal{P} \rangle\!\rangle$ such that $y^{e_i+k-1}\mu_i = b_{i,k-1} + p$. Then $y^{e_i+k}\mu_i = yb_{i,k-1} + yp$, with $yp \in \langle\!\langle \mathcal{P} \rangle\!\rangle$ and therefore $b_{i,k} = \mathrm{nf}_{\preccurlyeq,\mathcal{I}}(y^{e_i+k}\mu_i) = \mathrm{nf}_{\preccurlyeq,\mathcal{I}}(yb_{i,k-1})$.

It remains to prove that $yb_{i,k-1}$ is the sum of an element of $\langle\!\langle \mathcal{P} \rangle\!\rangle$ and one of $\mathrm{Span}_{\mathbb{K}}(\mathcal{B})$ (the latter must then be $b_{i,k}$ by uniqueness). This follows from the facts that

$$yb_{i,k-1} \in \mathrm{Span}_{\mathbb{K}}(y\mathcal{B}) \subseteq \mathrm{Span}_{\mathbb{K}}(\mathcal{B} \cup \{y^{e_j}\mu_j \mid 1 \leq j \leq t\}),$$

and that the elements of $\mathcal{P}$ are $\{y^{e_j}\mu_j - b_{j,0} \mid 1 \leq j \leq t\}$ with $b_{j,0} \in \mathrm{Span}_{\mathbb{K}}(\mathcal{B})$; indeed these imply more precisely that $yb_{i,k-1}$ is the sum of an element of $\mathrm{Span}_{\mathbb{K}}(\mathcal{P})$ and one of $\mathrm{Span}_{\mathbb{K}}(\mathcal{B})$. □

Corollary 5.4. *Using notation from Theorem 5.2, assume further $\mathcal{S}(\mathrm{lt}_{\preccurlyeq}(\mathcal{I}))$, let $\mathcal{G}$ be the reduced $\preccurlyeq$-Gröbner basis of $\mathcal{I}$, and let $f_1, \ldots, f_s$ be the elements of $\mathcal{G}$ whose $\preccurlyeq$-leading term is divisible by y. Then $\{f_1, \ldots, f_s\}$ is a basis of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ as a $\mathbb{K}[y]$-module.*

Proof. It suffices to prove that, thanks to $\mathcal{S}(\mathrm{lt}_{\preccurlyeq}(\mathcal{I}))$, we have

$$\{y^{e_j}\mu_j \mid 1 \leq j \leq t\} = \{\mathrm{lt}_{\preccurlyeq}(f_i) \mid 1 \leq i \leq s\};$$

then $\mathcal{P} = \{f_1, \ldots, f_s\}$ follows (and in particular $s = t$).

To prove this identity, we first observe that for $1 \leq i \leq s$, the monomial $\mathrm{lt}_{\preccurlyeq}(f_i)$ is divisible by y and does not belong to $\mathcal{B}$, whereas $y^{-1}\,\mathrm{lt}_{\preccurlyeq}(f_i)$ belongs to $\mathcal{B}$. Therefore

$$y^{-1}\,\mathrm{lt}_{\preccurlyeq}(f_i) \in \{\mu \in \mathcal{B} \mid y\mu \notin \mathcal{B}\} = \{y^{e_j-1}\mu_j \mid 1 \leq j \leq t\},$$

and $\mathrm{lt}_{\preccurlyeq}(f_i) \in \{y^{e_j}\mu_j \mid 1 \leq j \leq t\}$. Hence $f_i \in \mathcal{P}$.

Conversely, for $1 \leq j \leq t$, we want to prove $y^{e_j}\mu_j = \mathrm{lt}_{\preccurlyeq}(f_i)$ for some $i \in \{1, \ldots, s\}$. By construction, the monomial $y^{e_j}\mu_j$ is in $\mathrm{lt}_{\preccurlyeq}(\mathcal{P}) \subseteq \mathrm{lt}_{\preccurlyeq}(\mathcal{I})$. Thus $y^{e_j}\mu_j$ is divisible by $\mathrm{lt}_{\preccurlyeq}(f)$ for some $f \in \mathcal{G}$. If $\mathrm{lt}_{\preccurlyeq}(f)$ is not divisible by y, then $\mathrm{lt}_{\preccurlyeq}(f)$ is a divisor of μ_j, which is impossible since $\mu_j \in \mathcal{B}$ and $\mathrm{lt}_{\preccurlyeq}(f) \in \mathrm{lt}_{\preccurlyeq}(\mathcal{I})$. It follows that $f = f_i$ for some $i \in \{1, \ldots, s\}$. Thus $y^{e_j}\mu_j = \mu\,\mathrm{lt}_{\preccurlyeq}(f_i)$ for some monomial

μ, which may only involve the variables $x_1, \ldots, x_{n-1}$ since $y^{e_j-1}\mu_j$ is in $\mathcal{B}$ and thus cannot be a multiple of $\mathrm{lt}_\preccurlyeq(f_i)$. If $\mu \neq 1$, there exists $k \in \{1, \ldots, n-1\}$ such that x_k divides μ. By $\mathcal{S}(\mathrm{lt}_\preccurlyeq(\mathcal{I}))$, the monomial $\frac{x_k}{y}\,\mathrm{lt}_\preccurlyeq(f_i)$ is in $\mathrm{lt}_\preccurlyeq(\mathcal{I})$, hence $\frac{\mu}{x_k}\frac{x_k}{y}\,\mathrm{lt}_\preccurlyeq(f_i)$ is in $\mathrm{lt}_\preccurlyeq(\mathcal{I})$ as well. This contradicts the fact that the latter monomial is $y^{-1}\mu\,\mathrm{lt}_\preccurlyeq(f_i) = y^{e_j-1}\mu_j$, which is in $\mathcal{B}$. Thus $\mu = 1$ and we are done. □

6 COMPLEXITY AND PERFORMANCE

6.1 Hermite normal form computation

We assume that the basis $P \in \mathbb{K}[y]^{t\times t}$ from Theorem 5.2 is known, and we review the computation of its Hermite normal form. This subsection ends with a proof of Theorem 1.1.

Reducing to average degree, and general algorithms. By Theorem 5.2, the matrix P has column degrees $(e_1, \ldots, e_t)$, and $D = e_1 + \cdots + e_t$ is the degree $D = \dim_{\mathbb{K}}(\mathcal{R}/\mathcal{I})$. Hence P has average column degree $\frac{D}{t}$. Then, its Hermite normal form H can be found deterministically in $O^{\sim}(t^{\omega-1}D)$ operations in $\mathbb{K}$ [32, Thm. 1].

Besides, it is showed in [32, Sec. 6] that computing H directly reduces to computing the Hermite normal form of a matrix which is built from P and has slightly larger size but with all entries of degree at most $\lceil\frac{D}{t}\rceil$. Since $t \leq D$ here, $\lceil\frac{D}{t}\rceil \in O(\frac{D}{t})$, hence the same cost $O^{\sim}(t^{\omega}\frac{D}{t}) = O^{\sim}(t^{\omega-1}D)$ is obtained by the Las Vegas randomized algorithm in [22, 24]. Observe that, in both cases, the number of logarithmic factors in the cost bound is currently unknown.

Hermite normal form knowing degrees. Assume the ideal is in shape position; further make the mild assumption that $\mathcal{G}_{\mathrm{lex}} \subseteq \mathcal{R}_{\mathcal{T}}$ is satisfied, meaning that the variables $x_1, \ldots, x_{n-1}$ are in $\mathcal{T}$. Order $\mathcal{T}$ so that its first n elements are $(\mu_1, \ldots, \mu_n) = (1, x_{n-1}, \ldots, x_1)$. Then, $\mathcal{G}_{\mathrm{lex}} = \{h(y), x_{n-1} - g_{n-1}(y), \ldots, x_1 - g_1(y)\}$, and

$$H = \begin{bmatrix} h(y) & & & & & & \\ -g_{n-1}(y) & 1 & & & & & \\ \vdots & & \ddots & & & & \\ -g_1(y) & & & 1 & & & \\ -b_{n+1}(y) & & & & 1 & & \\ \vdots & & & & & \ddots & \\ -b_t(y) & & & & & & 1 \end{bmatrix} \tag{6}$$

for some polynomials $b_{n+1}, \ldots, b_t \in \mathbb{K}[y]$ of degree less than $\deg(h)$. Indeed, for the first n rows of H this follows directly from Theorem 4.1, proving also $\deg(h) = D = \deg(\det(H))$. Then, properties of Hermite normal forms imply that the diagonal entries of H are $(h, 1, \ldots, 1)$ and that the remaining rows have the above form.

In particular, we know the degree shape of the sought Hermite normal form. Finding these degrees is the first step of the fastest known Hermite normal form algorithm [32, Sec. 3], which can therefore be omitted: we directly use the second step in [32, Sec. 5]. The advantage is that the latter boils down to one call to a row reduction algorithm, for which the cost bound is known including logarithmic factors: it is $O(t^{\omega}\mathsf{M}(\frac{D}{t})(\log(t)^2 + \log(\frac{D}{t})))$, if one uses the fastest known deterministic algorithm [23, Thm. 18]. Here, $\mathsf{M}(\cdot)$ is a time function for the multiplication of univariate polynomials in $\mathbb{K}[y]$, with usual assumptions recalled for example in [23, Sec. 2].

Observe that one may still follow this approach when it is unknown whether the ideal is in shape position. If the obtained matrix does not have the expected form described in Eq. (6), then the ideal is not in shape position, and one can restart computations using a more general, slower change of order algorithm.

Using a kernel basis to reduce the matrix dimension. For our purpose, we are only interested in the $n\times n$ leading principal submatrix $H_{1..n,1..n}$, which corresponds to $\mathcal{G}_{\mathrm{lex}}$. To compute it from the known P, we can proceed as follows ([32, Lem. 3.1] and [49, Lem. 3.1]):

- compute a left kernel basis $K \in \mathbb{K}[y]^{n\times t}$ of the right $t\times(t-n)$ submatrix $P_{1..t,n+1..t}$ of P, using the algorithm of [50];
- multiply K with the left submatrix: $Q = KP_{1..t,1..n}$, using partial linearization in case of unbalanced degrees [50, Sec. 3.6];
- compute the Hermite normal form of Q, which is $H_{1..n,1..n}$, using [32, Algo. 3].

Our implementation, on which we report in Section 6.3, is based on this approach. The advantage is that this uses a single call to the fast kernel basis algorithm of [50], for which a precise cost estimate is known. After the multiplication, whose cost is also well understood, we are left with the computation of a Hermite normal form of an $n \times n$ matrix. In most interesting instances, this has negligible cost, since $n \ll t$ (see for example Sections 6.2 and 6.3).

Explicitly, the complexity of computing the kernel basis K is $O(t^{\omega}\mathsf{M}(\frac{D}{t})\log(\frac{D}{t}))$ [37, Lem. 2.10], while the multiplication to obtain Q, although possibly involving unbalanced degrees, has a lower complexity [37, Lem. 2.8].

Here again, one does not have to assume that the ideal is in shape position: this can be detected from the degrees in Q, which in fact can be predicted from the degrees in the kernel basis K. In the case where the degrees in K reveal that the ideal is not in shape position, one could switch to another more general method.

Proof of Theorem 1.1. Since $\mathcal{S}(\mathrm{lt}_\preccurlyeq(\mathcal{I}))$ is assumed (via Lemma 2.2), Corollary 5.4 ensures that the set of t elements of $\mathcal{G}_{\mathrm{drl}}$ whose $\preccurlyeq_{\mathrm{drl}}$-leading term is divisible by y forms a basis $P \in \mathbb{K}[y]^{t\times t}$ of $\mathcal{M}_{\mathcal{T},\mathcal{I}}$ as a $\mathbb{K}[y]$-module, where $\mathcal{T}$ is built as in Theorem 5.2.

Besides, since the variables $x_1, \ldots, x_{n-1}$ are in the $\preccurlyeq_{\mathrm{drl}}$-monomial basis $\mathcal{B}$, they belong to $\mathcal{T}$, which implies $\mathcal{G}_{\mathrm{lex}} \subseteq \mathcal{R}_{\mathcal{T}}$ according to Lemma 5.1, since $\mathcal{I}$ is in shape position. Hence Theorem 4.1 states that the Hermite normal form H of P yields the sought lexicographical Gröbner basis. As we have seen above, computing H from P takes $O^{\sim}(t^{\omega-1}D)$ operations in $\mathbb{K}$.

6.2 Extrinsic asymptotics of complexity gains

The estimate $O^{\sim}(t^{\omega-1}D)$ of Theorem 1.1 depends on the sparsity indicator t which is less than the degree D of the ideal. These are intrinsic to the ideal and the monomial order. On several important classes of problems, the asymptotics of t and D can be expressed as a function of the number of variables n, the maximum degree of the input polynomials d and some other extraneous parameters. These results can then be used to make explicit the speed up $t^{2-\omega}D$ we obtain from the complexity $O(tD^2)$ of [17, 18].

These are given in Table 1. For *generic* systems of n polynomials of degree d, [18, Tbl. 2] provides such asymptotics ; we refer to these in the line (rand n, d). In [7, Tbl. 1] asymptotic values of t, D are given for systems defining the critical points of the restriction of a linear map to an algebraic set defined by p generic polynomials by means of the simultaneous vanishing of maximal minors of a

truncated Jacobian matrix. We refer to these in the line (crit n, d, p). More recently, [19, Tbl. 1], provides asymptotic estimates for t, D when considering the $(r+1)$-minors of a polynomial symmetric matrix of size m in $n = \binom{m-r+1}{2}$ variables (symdet n, d, m, r).
For all these systems, the asymptotics of $t^{2-\omega}D$ appear with a positive exponent of quantities greater than 1, showing that the new algorithm is asymptotically faster than Sparse-FGLM. Note that for $2 < \omega < 3$, the complexity gain is exponential in n for most of them, in particular for rand n, d and crit n, d, p.

Table 1: Asymptotics of t, D and the ratio $t^{2-\omega}D$.

system	D	t	speed-up $t^{2-\omega}D$
rand n, d [18, Cor. 5.10]	d^n	$\frac{d^{n-1}}{\sqrt{n}}$	$d^{(n-1)(3-\omega)} n^{\frac{\omega-2}{2}}$
crit $n, 2, p$ [7, Thm. 2]	$2^p\binom{n-1}{p-1}$	$\frac{2^p}{\sqrt{p}}\binom{n-2}{p-1}$	$\left(2^p\binom{n-2}{p-1}\right)^{3-\omega} p^{\frac{\omega-2}{2}}$
crit n, d, p [7, Thm. 2]	$d^n\binom{n-1}{p-1}$	$\frac{d^{n-1}}{\sqrt{n-p}}\binom{n-2}{p-1}$	$\left(d^{n-1}\binom{n-2}{p-1}\right)^{3-\omega}$
symdet $3, d, m, m-2$ [19, Prop. 9]	m^3	$m^2 d$	$\frac{m^{7-2\omega}}{d^{\omega-2}} \geq m^{9-3\omega}$
symdet $6, d, m, m-1$ [19, Prop. 12]	$m^6 d^6$	$m^5 d^5$	$(md)^{16-5\omega}$
symdet $\binom{m}{2}, d, m, 1$ [19, Prop. 14]	$2^m d^{\binom{m}{2}}$	$\frac{2^m}{m} d^{\binom{m}{2}-1}$	$\left(2^m d^{\binom{m}{2}}\right)^{3-\omega} m^{\omega-2}$

6.3 Practical performance

We compare our implementation of the new change of order algorithm with two other algorithms:

- The state-of-the-art implementation of the Sparse-FGLM algorithm [17, 18], provided by `msolve` [8]. This is based on the Wiedemann algorithm, with the core computational task consisting of a series of matrix-vector products.
- A prototype implementation of a block-Wiedemann variant of Sparse-FGLM, whose core computational task consists of a series of matrix-matrix products. For the sake of comparison with our prototype PML/NTL implementation of the new algorithm, this was written with NTL using the linear algebra tools provided by its `Mat<zz_p>` module.

Both implementations exploit the structure of the multiplication matrix of y in $\mathcal{R}/\mathcal{I}$ written on the $\preccurlyeq_{\text{drl}}$-monomial basis, as explained in Section 3.3. In this context, the expected advantage of the block variant comes from the greater efficiency of performing a single matrix-matrix product $M \cdot [v_1 \ \cdots \ v_k]$ versus performing several matrix-vector products Mv_i for $1 \leq i \leq k$.

In our experiments on the block-Wiedemann approach, a block-size k in the range between 64 and 128 appeared as a good compromise. When k is below 64, the benefit from matrix-matrix products remains limited. On the other hand, when k is above 128, although there could still be some gain by further increasing the matrix dimension, this is counter-balanced by the cost of the second step which starts to be non-negligible. This second step is a matrix fraction reconstruction, performed via an approximant basis of a $(2k) \times k$ matrix at order $2D/k$, for which we used PML [28].

Note that, although block-Wiedemann approaches are often used for benefiting from multi-threaded or parallel computations, here only single-threaded performance is considered, and we keep the design of an optimized, multi-threaded implementation of our new change of order algorithm as a future perspective. Indeed, we expect it to also benefit from multi-threading, since the dominant part of its computations consists of multiplication and Gaussian elimination of large-dimension matrices over $\mathbb{K}$.

We summarize our comparison in Table 2. All computations were performed on a single thread on a computer equipped with Intel® Xeon® Gold CPU 6246R v4 @ 3.40GHz and 1.5TB of RAM.

The base field is $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ with a 30-bit prime modulus p. This choice comes from the fact that many application areas require Gröbner bases computations over large fields. This is the case for problems in multivariate cryptography and number theory [1, 2, 41]. Furthermore, large computations over the rationals $\mathbb{K} = \mathbb{Q}$ boil down to solving several instances over $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, through the Chinese Remainder Theorem. We consider the 30-bit prime fields as a base case in this setting, since it allows us both to choose sufficiently many primes for large instances, and to avoid bad primes with higher probability than e.g. 16-bit prime fields. It also seems to be the base case used in computer algebra software like Macaulay2, Maple and Singular and in the state-of-the-art change of order implementation in `msolve` which we compare to.

We observe that our implementation of the new algorithm is always faster than both other implementations, and that the gap is increasing with the size of the instances. For large instances, the speed-up factor is close to 5.

Let us notice that the block-Wiedemann approach also outperforms `msolve` for large sizes, as might be expected, yet only by a very small margin. One explanation can be that NTL does not seem to use `AVX2` vectorization techniques for matrix multiplication over a 30-bit prime field, whereas `msolve` does for its matrix-vector products. Investigating this is a future perspective, and incorporating `AVX2` may lead to further accelerations for the block-Wiedemann approach, but also for the new algorithm which makes an intensive use of the multiplication of matrices over $\mathbb{K}$ when multiplying univariate polynomial matrices.

Let us recall that when computing over the rationals, the common strategy through Chinese Remainder Theorem is to use F_4 with a tracer for the computation of $\mathcal{G}_{\text{drl}}$ modulo each prime: perform a full F_4 algorithm modulo the first prime and *learn* which polynomials are used in the construction of each matrix and remove those that reduce to 0, and those used only in these reductions to 0. This allows one to minimize the computations modulo the subsequent primes. As a practical consequence, FGLM used to be slower than F_4-tracer, but this is not the case anymore, we have reestablished a kind of balance. With the above perspective we expect the change of order step to be consistently faster than the F_4-tracer step. Furthermore, even when computing over a 30-bit prime field, with only F_4 and no tracer, FGLM could take more than 25% of the total time, sometimes even close to 40% (see rand $(4, 7)$ or $(4, 8)$), now it is closer to negligible (often below or close to 10%).

Table 2: Timings in seconds for random square systems in n variables and degree d, over a prime field $\mathbb{Z}/p\mathbb{Z}$ with a 30-bit modulus. `F4` *is the algorithm of [13]. "*`F4`*-tr" is the tracer algorithm after the initial learning phase [8, Sec. 4.3]. "Wied." and "bl-Wied." are the change of order comparison points described in Section 6.3. They use respectively the Wiedemann-based Sparse-FGLM algorithm [18] and a folklore block-Wiedemann variant (see e.g. [27, 44]). "HNF" is the new algorithm, based on Hermite normal form, as described in Section 6.1.*

			Step 1: $\mathcal{G}_{\text{drl}} \approx P$		Step 2: $\mathcal{G}_{\text{lex}} \approx H$		
			`msolve`		`msolve`	NTL	PML
n, d	D	t	`F4`	`F4`-tr	Wied.	bl-Wied.	HNF
11, 2	2048	462	11.6	1.1	1.2	1.7	0.8
12, 2	4096	924	115.9	8.3	6.5	14.5	5.3
13, 2	8192	1716	970	62	103.6	110	34.8
14, 2	16384	3432	7921	460	1011	880	240
15, 2	32768	6435	61381	3193	7844	6691	1665
16, 2	65536	12870	482515	24523	58744	52709	11359
8, 3	6561	1107	122.6	12.8	23.6	44.7	15.1
9, 3	19683	3139	3552.7	361	1302	1163	314
10, 3	59049	8953	95052	8664	34844	29974	6709
6, 4	4096	580	9.9	2.2	4	8.8	3.5
7, 4	16384	2128	876	128	575	545	157
8, 4	65536	8092	57237	6977	36454	33452	7231

REFERENCES

[1] S. Abelard. 2018. *Counting points on hyperelliptic curves in large characteristic: algorithms and complexity.* PhD thesis. Université de Lorraine. https://tel.archives-ouvertes.fr/tel-01876314

[2] S. Abelard, P. Gaudry, and P.-J. Spaenlehauer. 2019. Improved Complexity Bounds for Counting Points on Hyperelliptic Curves. *Foundations of Computational Mathematics* 19, 3 (2019), 591–621. https://doi.org/10.1007/s10208-018-9392-1

[3] D. Bayer and M. Stillman. 1987. A theorem on refining division orders by the reverse lexicographic order. *Duke Mathematical Journal* 55, 2 (1987), 321–328. https://doi.org/10.1215/S0012-7094-87-05517-7

[4] E. Becker, T. Mora, M.G. Marinari, and C. Traverso. 1994. The Shape of the Shape Lemma. In *Proceedings ISSAC 1994*. ACM, 129–133. https://doi.org/10.1145/190347.190382

[5] T. Becker, V. Weispfenning, and H. Kredel. 1993. *Gröbner bases – A computational approach to commutative algebra.* Graduate texts in mathematics, Vol. 141. Springer.

[6] B. Beckermann, G. Labahn, and G. Villard. 2006. Normal forms for general polynomial matrices. *J. Symb. Comput.* 41, 6 (2006), 708–737. https://doi.org/10.1016/j.jsc.2006.02.001

[7] J. Berthomieu, A. Bostan, A. Ferguson, and M. Safey El Din. 2022. Gröbner bases and critical values: The asymptotic combinatorics of determinantal systems. *J. Algebra* 602 (2022), 154–180. https://doi.org/10.1016/j.jalgebra.2022.03.002

[8] J. Berthomieu, C. Eder, and M. Safey El Din. 2021. Msolve: A Library for Solving Polynomial Systems. In *Proceedings ISSAC 2021*. ACM, 51–58. https://doi.org/10/gk8549 https://msolve.lip6.fr/.

[9] B. Buchberger. 1976. A Theoretical Basis for the Reduction of Polynomials to Canonical Forms. *SIGSAM Bull.* 10, 3 (1976), 19–29. https://doi.org/10/d2cskd

[10] D. A. Cox, J. Little, and D. O'Shea. 2007. *Ideals, Varieties, and Algorithms (third edition).* Springer-Verlag New-York. https://doi.org/10.1007/978-0-387-35651-8

[11] D. S. Dummit and R. M. Foote. 2004. *Abstract algebra* (3rd ed.). Wiley.

[12] D. Eisenbud. 1995. *Commutative Algebra: with a View Toward Algebraic Geometry.* Springer. https://doi.org/10.1007/978-1-4612-5350-1

[13] J.-C. Faugère. 1999. A New Efficient Algorithm for Computing Gröbner bases (F4). *J. Pure Appl. Algebra* 139, 1 (1999), 61–88. https://doi.org/10/bpq5dx

[14] J.-C. Faugère. 2002. A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F5). In *Proceedings ISSAC 2002*. ACM, 75–83. https://doi.org/10/bd4nnq

[15] J.-C. Faugère, P. Gaudry, L. Huot, and G. Renault. 2014. Sub-Cubic Change of Ordering for Gröbner Basis: A Probabilistic Approach. In *Proceedings ISSAC 2014*. ACM, 170–177. https://doi.org/10.1145/2608628.2608669

[16] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. 1993. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *J. Symb. Comput.* 16, 4 (1993), 329–344. https://doi.org/10.1006/jsco.1993.1051

[17] J.-C. Faugère and C. Mou. 2011. Fast Algorithm for Change of Ordering of Zero-dimensional Gröbner Bases with Sparse Multiplication Matrices. In *Proceedings ISSAC 2011*. ACM, 115–122. https://doi.org/10/fhhs56

[18] J.-C. Faugère and C. Mou. 2017. Sparse FGLM algorithms. *J. Symb. Comput.* 80, 3 (2017), 538–569. https://doi.org/10/gfz47c

[19] A. Ferguson and H.P. Le. 2022. Finer complexity estimates for the change of ordering of Gröbner bases for generic symmetric determinantal ideals. In *Proceedings ISSAC 2022*. ACM. https://doi.org/10.1145/3476446.3536182

[20] A. Galligo. 1974. À propos du théorème de préparation de Weierstrass. In *Fonctions de Plusieurs Variables Complexes*. Springer Berlin Heidelberg, 543–579. https://doi.org/10.1007/BFb0068121

[21] P. Gianni and T. Mora. 1989. Algebraic solution of systems of polynomial equations using Groebner bases. In *Proceedings AAECC 1987*. Springer, 247–257. https://doi.org/10.1007/3-540-51082-6_83

[22] S. Gupta. 2011. *Hermite forms of polynomial matrices.* Master's thesis. University of Waterloo, Canada.

[23] S. Gupta, S. Sarkar, A. Storjohann, and J. Valeriote. 2012. Triangular x-basis decompositions and derandomization of linear algebra algorithms over $K[x]$. *J. Symb. Comput.* 47, 4 (2012), 422–453. https://doi.org/10.1016/j.jsc.2011.09.006

[24] S. Gupta and A. Storjohann. 2011. Computing Hermite Forms of Polynomial Matrices. In *Proceedings ISSAC 2011*. ACM, 155–162. https://doi.org/10.1145/1993886.1993913

[25] C. Hermite. 1851. Sur l'introduction des variables continues dans la théorie des nombres. *J. Reine Angew. Math.* 41 (1851), 191–216. https://doi.org/10.1515/crll.1851.41.191

[26] J. Herzog and T. Hibi. 2011. *Monomial Ideals.* Springer London. 3–22 pages. https://doi.org/10.1007/978-0-85729-106-6

[27] S. G. Hyun, V. Neiger, H. Rahkooy, and É. Schost. 2020. Block-Krylov techniques in the context of sparse-FGLM algorithms. *J. Symb. Comput.* 98 (2020), 163–191. https://doi.org/10.1016/j.jsc.2019.07.010 Special Issue on Symbolic and Algebraic Computation: ISSAC 2017.

[28] S. G. Hyun, V. Neiger, and É. Schost. 2019. Implementations of Efficient Univariate Polynomial Matrix Algorithms and Application to Bivariate Resultants. In *Proceedings ISSAC 2019*. ACM, 235–242. https://doi.org/10.1145/3326229.3326272 https://github.com/vneiger/pml.

[29] T. Kailath. 1980. *Linear Systems.* Prentice-Hall.

[30] C. Kojima, P. Rapisarda, and K. Takaba. 2007. Canonical forms for polynomial and quadratic differential operators. *Systems & Control Letters* 56, 11 (2007), 678–684. https://doi.org/10.1016/j.sysconle.2007.06.004

[31] M. Kreuzer and L. Robbiano. 2016. *Computational linear and commutative algebra.* Springer.

[32] G. Labahn, V. Neiger, and W. Zhou. 2017. Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix. *J. Complexity* 42 (2017), 44–71. https://doi.org/10.1016/j.jco.2017.03.003

[33] D. Lazard. 1985. Ideal bases and primary decomposition: case of two variables. *J. Symb. Comput.* 1, 3 (1985), 261–270. https://doi.org/10/cr48qn

[34] M. G. Marinari, H. M. Möller, and T. Mora. 1993. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Appl. Algebra Engrg. Comm. Comput.* 4, 2 (1993), 103–145. https://doi.org/10.1007/BF01386834

[35] G. Moreno-Socías. 2003. Degrevlex Gröbner bases of generic complete intersections. *J. Pure Appl. Algebra* 180, 3 (2003), 263–283. https://doi.org/10/fvbj64

[36] V. Neiger. 2016. *Bases of relations in one or several variables: fast algorithms and applications.* PhD thesis. École Normale Supérieure de Lyon. https://tel.archives-ouvertes.fr/tel-01431413

[37] V. Neiger and C. Pernet. 2021. Deterministic computation of the characteristic polynomial in the time of matrix multiplication. *J. Complexity* 67 (2021), 101572. https://doi.org/10.1016/j.jco.2021.101572

[38] V. Neiger and É Schost. 2020. Computing syzygies in finite dimension using fast linear algebra. *J. Complexity* 60 (2020), 101502. https://doi.org/10/ht25

[39] C. Pernet and A. Storjohann. 2007. Faster Algorithms for the Characteristic Polynomial. In *Proceedings ISSAC 2007*. ACM, 307–314. https://doi.org/10/fcdnsm

[40] C. Pernet and A. Storjohann. 2007. Frobenius form in expected matrix multiplication time over sufficiently large fields. Unpublished report. https://cs.uwaterloo.ca/~astorjoh/cpoly.pdf

[41] L. Perret. 2016. *Bases de Gröbner en Cryptographie Post-Quantique.* Habilitation à diriger des recherches. UPMC - Paris 6 Sorbonne Universités. https://tel.archives-ouvertes.fr/tel-01417808

[42] V. M. Popov. 1972. Invariant Description of Linear, Time-Invariant Controllable Systems. *SIAM Journal on Control* 10, 2 (1972), 252–264. https://doi.org/10.1137/0310020

[43] V. Shoup. 2021. NTL: A library for doing number theory, version 11.5.1. https://libntl.org.

[44] A. Steel. 2015. Direct Solution of the (11,9,8)-MinRank Problem by the Block Wiedemann Algorithm in Magma with a Tesla GPU. In *Proceedings PASCO 2015*. ACM, 2–6. https://doi.org/10.1145/2790282.2791392

[45] A. Storjohann. 2000. *Algorithms for Matrix Canonical Forms.* PhD thesis. Swiss Federal Institute of Technology – ETH. https://cs.uwaterloo.ca/~astorjoh/diss2up.pdf

[46] B. Sturmfels. 2002. *Solving systems of polynomial equations.* Number 97. American Mathematical Soc.

[47] G. Villard. 2018. On computing the resultant of generic bivariate polynomials. In *Proceedings ISSAC 2018.* ACM, 391–398. https://doi.org/10.1145/3208976.3209020

[48] D. H. Wiedemann. 1986. Solving sparse linear equations over finite fields. *IEEE Trans. Inf. Theory* 32, 1 (1986), 54–62. https://doi.org/10.1109/TIT.1986.1057137

[49] W. Zhou and G. Labahn. 2013. Computing Column Bases of Polynomial Matrices. In *Proceedings ISSAC 2013.* ACM, 379–386. https://doi.org/10.1145/2465506.2465947

[50] W. Zhou, G. Labahn, and A. Storjohann. 2012. Computing Minimal Nullspace Bases. In *Proceedings ISSAC 2012.* ACM, 366–373. https://doi.org/10.1145/2442829.2442881