Gröbner Basis over Semigroup Algebras: Algorithms and Applications for Sparse Polynomial Systems

Matías Bender, Jean-Charles Faugère, Elias Tsigaridas

Gröbner Basis over Semigroup Algebras: Algorithms and Applications for Sparse Polynomial Systems

Matías R. Bender [1,2] Jean-Charles Faugère [1] Elias Tsigaridas [1]
[1] Sorbonne Université, CNRS, INRIA, Laboratoire d'Informatique de Paris 6, LIP6, Équipe PolSys
F-75005, Paris, France
FirstName.LastName@inria.fr
[2] Technische UniversitÃďt Berlin, Institut fÃijr Mathematik
Berlin 10623, Germany
mbender@math.tu-berlin.de

ABSTRACT

Gröbner bases is one the most powerful tools in algorithmic non-linear algebra. Their computation is an intrinsically hard problem with a complexity at least single exponential in the number of variables. However, in most of the cases, the polynomial systems coming from applications have some kind of structure. We consider sparse systems where the input polynomials have a few non-zero terms.

Our approach to exploit sparsity is to embed the systems in a semigroup algebra and to compute Gröbner bases over this algebra. Up to now, the algorithms that follow this approach benefit from the sparsity only in the case where all the polynomials have the same sparsity structure, that is the same Newton polytope. We introduce the first algorithm that overcomes this restriction. Under regularity assumptions, it performs no redundant computations. Further, we extend this algorithm to compute Gröbner basis in the standard algebra and solve sparse polynomials systems over the torus $(\mathbb{C}^*)^n$. The complexity of the algorithm depends on the Newton polytopes.

CCS CONCEPTS

• **Mathematics of computing → Gröbner bases and other special bases**.

KEYWORDS

Gröbner Basis; Solving Polynomial System; Mixed Sparse System; Sparse Elimination Theory; Toric Variety; Koszul Complex

1 INTRODUCTION

The introduction of the first algorithm to compute Gröbner bases in 1965 established them as a central tool in nonlinear algebra. Computing Gröbner bases is an intrinsically hard problem. For many "interesting" cases related to applications the complexity of the algorithms to compute them is single exponential in the number of variables, but there are instances where the complexity is double exponential; it is an EXPSPACE complete problem [25]. There are many practically efficient algorithms, see [9, 13] and references therein, for which, under genericity assumptions, we can deduce precise complexity estimates [1]. However, the polynomial systems coming from applications, i.e. computer-aided design, robotics, biology, cryptography, and optimization e.g., [33], have some kind of structure. One of the main challenges in Gröbner basis theory is to improve the complexity and the practical performance of the related algorithms by exploiting the structure.

We employ the structure related to the sparsity of the polynomial systems; in other words, we focus on the non-zero terms of the input polynomials. In addition, we consider polynomials having different supports. There are different approaches to benefit from sparsity, e.g., [2, 6, 15, 30]. We follow [15, 30] and we consider Gröbner bases over semigroup algebras. We construct a semigroup algebra related to the Newton polytopes of the input polynomials and compute Gröbner bases for the ideal generated by the original polynomials in this semigroup algebra. Semigroup algebras are related to toric varieties. An affine toric variety is the spectrum of a semigroup algebra [8]. Hence, the variety defined by the polynomials over the semigroup is a subvariety of a toric variety. It is different from the one defined by the polynomials over the original polynomial algebra, but they are related and in many applications the difference is irrelevant, e.g., [12]. We refer to [8] for an introduction to toric varieties and to [32] for their relation with Gröbner basis.

In ISSAC'14, Faugère et al. [15] considered sparse *unmixed systems*, that is, polynomial systems where all the polynomials have the same Newton polytope, and they introduced an algorithm to compute Gröbner bases over the semigroup algebra generated by the Newton polytope. This algorithm is a variant of the MatrixF5 algorithm [1, 13]. They compute Gröbner bases by performing Gaussian elimination on various Macaulay matrices [22] and they avoid computations with rows reducing to zero using the F5 criterion [13]. The efficiency of this approach relies on an incremental construction which, under regularity assumptions, skips all the rows reducing to zero. They exploit the property that, for normal Newton polytopes, *generic* unmixed systems are regular sequences over the corresponding semigroup algebra. Unfortunately, this property is no longer true for *mixed systems*, that is, for systems of polynomials with different Newton polytopes. So, this algorithm fails to predict all rows reducing to zero. Moreover, the degree bound for the maximal degree in [15, Lem. 5.2] misses some assumptions to hold, see App. A. We relax the regularity assumptions of [15] and we introduce an F5-like criterion that, under regularity assumptions, predicts all the rows reducing to zero during Gröbner bases computation.

In this context, we also mention our previous work [2] on computing *sparse Gröbner bases* for mixed sparse polynomial systems. Besides the similarity in the titles, this work and [2] are completely different approaches: we compute different objects (Sparse Gröbner bases [2, Sec. 3] are not Gröbner bases for semigroup algebras), we follow different computational strategies (in [2] we perform the computations polynomial by polynomial, while in this work we proceed degree by degree), and we have no complexity bounds to solve 0-dimensional using [2].

A direct application of Gröbner basis theory is to solve polynomial systems. This is also an intrinsically hard problem [19]. Hence, it is important to exploit the sparsity of the input polynomials to obtain new algorithms for solving with better complexity bounds. The different ways of doing so include homotopy methods e.g., [21, 36], chordal elimination [6], triangular decomposition [27], and various other techniques [20, 28, 34, 35].

Among the symbolic approaches related to toric geometry, the main tool to solve sparse systems is the sparse resultant [17]. The resultant is a central object in elimination theory and there are many different ways of exploiting it to solve sparse systems, see for example [7, Chp. 7.6]. Canny and Emiris [4] and Sturmfels [31] showed how to compute the sparse resultant as the determinant of a square Macaulay matrix (Sylvester-type formula) whose rows are related to mixed subdivisions of some polytopes. Using this matrix, e.g., [11], we can solve square sparse systems. For this, we add one more polynomial to the system and we consider the matrix of the resultant of the new system. Under genericity assumptions, we can recover the multiplication maps of the quotient ring defined by original square system over the ring of Laurent polynomials and we obtain the solutions over $(\mathbb{C} \setminus \{0\})^n$. Recently, Massri [24] dropped the genericity assumptions by considering a bigger matrix.

We build on Massri's work and, under regularity assumptions, we propose an algorithm to solve 0-dimensional square systems with complexity related to the Minkowski sum of the Newton polytopes. Because we work with toric varieties, we compute solutions over $(\mathbb{C} \setminus \{0\})^n$. Our strategy is to reuse part of our algorithm to compute Gröbner bases over semigroup algebras to compute multiplication maps and, via FGLM [14], recover a Gröbner basis over the standard polynomial algebra. As we compute the solutions over $(\mathbb{C} \setminus \{0\})^n$, we do not recover a Gröbner basis for the original ideal, but for its saturation with respect to the product of all the variables. We compute with a matrix that has the same size as the resultant approach [11]. Our approach to solve is more general than the one in [15] as we compute with mixed sparse systems, and because it terminates earlier as we do not compute Gröbner bases but multiplication maps. An overview of our strategy is as follows:

(1) Let $f_1, \dots, f_n \in \mathbb{K}[\boldsymbol{x}]$ be a sparse regular polynomial system with a finite number of solutions over $(\mathbb{C} \setminus \{0\})^n$.
(2) Embed the polynomials to a multigraded semigroup algebra $\mathbb{K}[S_\Delta^h]$ related to the Newton polytopes of $f_1, \dots, f_n$ and to the standard n-simplex (see Def. 2.6).
(3) For each variable x_i:
  - Use the Gröbner basis algorithm (Alg. 2) to construct a square Macaulay matrix related to $(f_1, \dots, f_n, x_i)$ of size equal to the number of integer points in the Minkowski sum of the Newton polytopes of $f_1, \dots, f_n$ and the n-simplex.
  - Split the matrix in four parts and compute a Schur complement, which is the multiplication map of x_i in $\mathbb{K}[\boldsymbol{x}^{\pm 1}]/\langle f_1, \dots, f_n \rangle$.
(4) Use the multiplication maps and FGLM to get a Gröbner basis for $\langle f_1, \dots, f_n \rangle : \langle \prod_i x_i \rangle^\infty$ with respect to any monomial order.

The contributions and consequences of our work include:

- *We present the first generalization of [15] to the mixed case.* We introduce an algorithm to compute Gröbner bases over semigroup algebras associated to mixed polynomial systems. We provide complexity estimates related to the Newton polytopes of the input polynomials.
- *We relate the solving techniques using Sylvester-type formulas in resultant theory with Gröbner bases computations.* The simplest, but not necessarily the most efficient as there are more compact formulas [37], way to compute the resultant is to use a Sylvester-type formula and compute it as the determinant of a Macaulay matrix [7, Chp. 3.4]. Using this matrix we extract multiplication maps and solve polynomial systems [7, Chp. 3.4]. In the standard polynomial algebra, such matrices are at the heart of linear algebra algorithms to compute Gröbner bases because they correspond to the biggest matrix that appears during Gröbner basis computations for regular 0-dimensional systems [22]. However, such a relation was not known for the sparse case. We bring out this relation and we build on it algorithmically.
- *We generalize the F5 criterion to depend on the strands of the Koszul complexes instead of regular sequences.* The exactness of the Koszul complex is closely related to regular sequences [10, Ch. 17] and, geometrically, to complete intersections. Roughly speaking, when we consider generic square systems of equations in the coordinate ring of a "nice" projective variety, the variety that the system defines is closely related to a complete intersection. In this case, the Koszul complex of the system might not be exact in general, but only in some "low" degrees. To extend the optimality of the F5 criterion to these systems, we restrict our computations to the degrees at which the strands of the Koszul complex are exact because, at these degrees, we can predict the algebraic structure of the system and avoid every reduction to zero. These allow us to present an optimal criterion for "nice" mixed sparse systems which are not regular sequences. Moreover, additional information on the exactness of the strands of the Koszul complex and the multigraded Castelnuovo-Mumford regularity [3, 23] results in better degree and complexity bounds; similarly to the case of the multihomogeneous systems [2, Sec. 4].
- *We solve sparse systems by truncating our computation of an intermediate Gröbner basis.* The classical approach for solving 0-dimensional systems using Gröbner bases involves the computation of an intermediate Gröbner basis that we use to deduce multiplication maps and, by using FGLM, to obtain the lexicographical Gröbner basis of the ideal. If the intermediate Gröbner basis is computed with respect to a graded reverse lexicographical order and the input system "behaves well" when we homogenize it, this strategy is in some sense optimal because it is related to the Castelnuovo-Mumford regularity of the homogenized ideal [5, Cor. 3]. However, over semigroup algebras, it might not be always possible to relate the complexity of the intermediate Gröbner basis computation to the Castelnuovo-Mumford regularity of the ideal; this is so because we can not define monomial orders that behave like a graded reverse lexicographical, see [2,

Ex. 2.3]. We overcome this obstacle by truncating the computation of the intermediate Gröbner basis in such a way that the complexity is given by Castelnuovo-Mumford regularity of the ideal.

2 PRELIMINARIES

Let $\mathbb{K} \subset \mathbb{C}$ be a field of characteristic 0, $\boldsymbol{x} := (x_1, \ldots, x_n)$, and $\mathbb{K}[\boldsymbol{x}] := \mathbb{K}[x_1, \ldots, x_n]$. We consider $\mathbf{0} := (0, \ldots, 0)$ and $\mathbf{1} := (1, \ldots, 1)$. For each $r \in \mathbb{N}$, let $\boldsymbol{e_1}, \ldots, \boldsymbol{e_r}$ be the canonical basis of $\mathbb{R}^r$. Given $\boldsymbol{d_1}, \boldsymbol{d_2} \in \mathbb{N}^r$, we say $\boldsymbol{d_1} \geq \boldsymbol{d_2}$ when $\boldsymbol{d_1} - \boldsymbol{d_2} \in \mathbb{N}^r$. We use $[r] = \{1, \ldots, r\}$. Let $\langle f_1, \ldots, f_m \rangle$ be the ideal generated by $f_1, \ldots, f_m$.

2.1 Semigroup algebras

Definition 2.1 (Affine semigroup and semigroup algebra). Following [26], an affine semigroup S is a finitely-generated additive subsemigroup of $\mathbb{Z}^n$, for some $n \in \mathbb{N}$, such that it contains $\mathbf{0} \in \mathbb{Z}^n$. An affine semigroup S is pointed if it does not contain non-zero invertible elements, that is for all $\boldsymbol{\alpha}, \boldsymbol{\beta} \in S \setminus \{\mathbf{0}\}$, $\boldsymbol{\alpha} + \boldsymbol{\beta} \neq \mathbf{0}$ [26, Def 7.8]. The semigroup algebra $\mathbb{K}[S]$ is the $\mathbb{K}$-algebra generated by the monomials $\{\boldsymbol{X}^{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in S\}$ such that $\boldsymbol{X}^{\boldsymbol{\alpha}} \cdot \boldsymbol{X}^{\boldsymbol{\beta}} = \boldsymbol{X}^{\boldsymbol{\alpha}+\boldsymbol{\beta}}$.

Definition 2.2 (Convex set and convex hull). A set $\Delta \subset \mathbb{R}^n$ is convex if every line segment connecting two elements of Δ also lies in Δ; that is, for every $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \Delta$ and $0 \leq \lambda \leq 1$ it holds $\lambda\boldsymbol{\alpha} + (1 - \lambda)\boldsymbol{\beta} \in \Delta$. The convex hull of Δ is the unique minimal, with respect to inclusion, convex set that contains Δ.

Definition 2.3 (Pointed rational polyhedral cones). A cone C is a convex subset of $\mathbb{R}^n$ such that $\mathbf{0} \in C$ and for every $\boldsymbol{\alpha} \in C$ and $\lambda > 0$, $\lambda\,\boldsymbol{\alpha} \in C$. The dimension of a cone is the dimension of the vector space spanned by the cone. A cone is pointed if does not contain any line; that is, if $\mathbf{0} \neq \boldsymbol{\alpha} \in C$, then $-\boldsymbol{\alpha} \notin C$. A ray is a pointed cone of dimension one. A ray is *rational* if it contains a non-zero point of $\mathbb{Z}^n$. A *rational polyhedral cone* is the convex hull of a finite set of rational rays. For a set of points $\Delta \subset \mathbb{R}^n$, let C_Δ be the cone generated by the elements in Δ. If Δ is (the convex hull of) a finite set of integer points, then C_Δ is a rational polyhedral cone.

A rational polyhedral cone C defines the affine semigroup $C \cap \mathbb{Z}^n$, which is pointed if and only if the cone is pointed.

Definition 2.4 (Integer polytopes and Minkowski sum). An integer polytope $\Delta \subset \mathbb{R}^n$ is the convex hull of a finite set of (integer) points in $\mathbb{Z}^n$. The Minkowski sum of two integer polytopes Δ_1 and Δ_2 is $\Delta_1 + \Delta_2 = \{\boldsymbol{\alpha} + \boldsymbol{\beta} : \boldsymbol{\alpha} \in \Delta_1, \boldsymbol{\beta} \in \Delta_2\}$. For each polytope Δ and $k \in \mathbb{N}$, we denote by $k \cdot \Delta$ the Minkowski sum of k copies of Δ.

Definition 2.5 (Laurent polynomials and Newton polytopes). A Laurent polynomial is a finite $\mathbb{K}$-linear combination of monomials $\boldsymbol{X}^{\boldsymbol{\alpha}}$, where $\boldsymbol{\alpha} \in \mathbb{Z}^n$. The Laurent polynomials form a ring, $\mathbb{K}[\mathbb{Z}^n]$, that corresponds to the semigroup algebra of $\mathbb{Z}^n$. For a Laurent polynomial $f = \sum_{\boldsymbol{\alpha} \in \mathbb{Z}^n} c_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$, its Newton polytope is the integer polytope generated by the set of the exponents $\boldsymbol{\alpha}$ of the non-zero coefficients of f; that is, $\mathrm{NP}(f) := \text{Convex Hull}(\{\boldsymbol{\alpha} \in \mathbb{Z}^n, c_{\boldsymbol{\alpha}} \neq 0\})$.

Instead of working over $\mathbb{K}[\mathbb{Z}^n]$, we embed f in a subalgebra related to its Newton polytope, given by $\mathbb{K}[C_{\mathrm{NP}(f)} \cap \mathbb{Z}^n]$. In this way we exploit the sparsity of the (polynomials of the) system.

Definition 2.6 (Semigroup algebra of polytopes). We consider r integer polytopes $\Delta_1, \ldots, \Delta_r \subset \mathbb{R}^n$ such that their Minkowski sum, $\Delta := \sum_{i=1}^r \Delta_i$, has dimension n and $\mathbf{0}$ is its vertex; in particular, $\mathbf{0}$ as a vertex of every Newton polytope Δ_i. We also consider the polytope $\bar{\Delta} := \sum(\Delta_i \times \{\boldsymbol{e_i}\})$, which is the Cayley embedding of $\Delta_1, \ldots, \Delta_r$. In what follows, we work with the semigroup algebras $\mathbb{K}[S_\Delta] := \mathbb{K}[C_\Delta \cap \mathbb{Z}^n]$ and $\mathbb{K}[S_\Delta^h] := \mathbb{K}[C_{\bar{\Delta}} \cap \mathbb{Z}^{n+r}]$. We will write the monomials in $\mathbb{K}[S_\Delta^h]$ as $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d})}$, where $\boldsymbol{\alpha} \in (C_\Delta \cap \mathbb{Z}^n)$ and $\boldsymbol{d} \in \mathbb{N}^r$.

The algebra $\mathbb{K}[S_\Delta^h]$ is $\mathbb{N}^r$-multigraded as follows: for every $\boldsymbol{d} = (d_1, \ldots, d_r) \in \mathbb{N}^r$, $\mathbb{K}[S_\Delta^h]_{\boldsymbol{d}}$ is the $\mathbb{K}$-vector space spanned by the monomials $\{\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d})} : \boldsymbol{\alpha} \in (\sum d_i \cdot \Delta_i) \cap \mathbb{Z}^n\}$. Then, $F \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}}$ is homogeneous and has multidegree $\boldsymbol{d}$, which we denote by $\mathrm{mdeg}(F)$.

We can think of $\mathbb{K}[S_\Delta]$ as the "dehomogenization" of $\mathbb{K}[S_\Delta^h]$.

Definition 2.7 (Dehomogenization morphism). The dehomogenization morphism from $\mathbb{K}[S_\Delta^h]$ to $\mathbb{K}[S_\Delta]$ is the surjective ring homomorphism $\chi : \mathbb{K}[S_\Delta^h] \to \mathbb{K}[S_\Delta]$ that maps the monomials $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d})} \in \mathbb{K}[S_\Delta^h]$ to $\chi(\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d})}) := \boldsymbol{X}^{\boldsymbol{\alpha}} \in \mathbb{K}[S_\Delta]$.

If $\mathcal{L}$ is a set of homogeneous polynomials in $\mathbb{K}[S_\Delta^h]$, then we consider $\chi(\mathcal{L}) = \{\chi(G) : G \in \mathcal{L}\}$.

Observation 2.8. *As $\mathbf{0}$ is a vertex of Δ, there is a monomial $\boldsymbol{X}^{(\mathbf{0},\boldsymbol{e_i})} \in \mathbb{K}[S_\Delta^h]$, for every $i \in [r]$. Hence, given a finite set of monomials $\boldsymbol{X}^{\boldsymbol{\alpha_1}}, \ldots, \boldsymbol{X}^{\boldsymbol{\alpha_k}} \in \mathbb{K}[S_\Delta]$, we can find a multidegree $\boldsymbol{d} \in \mathbb{N}^r$ such that $\boldsymbol{X}^{(\boldsymbol{\alpha_1},\boldsymbol{d})}, \ldots, \boldsymbol{X}^{(\boldsymbol{\alpha_k},\boldsymbol{d})} \in \mathbb{K}[S_\Delta]_{\boldsymbol{d}}$.*

Given a system of polynomials $f_1, \ldots, f_m \in \mathbb{K}[S_\Delta]$, we can find a multidegree $\boldsymbol{d} \in \mathbb{N}^r$ and homogeneous polynomials $F_1, \ldots, F_m \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}}$ so that it holds $\chi(F_i) = f_i$, for every $i \in [m]$.

Moreover, given homogeneous polynomials $F_1, \ldots, F_m \in \mathbb{K}[S_\Delta^h]$ and an affine polynomial $g \in \langle \chi(F_1), \ldots, \chi(F_m) \rangle$, there is an homogeneous polynomial $G \in \langle F_1, \ldots, F_m \rangle$ such that $\chi(G) = g$.

2.2 Gröbner bases

Our definitions follow [15]. Let S be a pointed affine semigroup.

Definition 2.9 (Monomial order). Given a pointed semigroup algebra $\mathbb{K}[S]$, a monomial order for $\mathbb{K}[S]$, say $<$, is a total order for the monomials in $\mathbb{K}[S]$ such that:

- For any $\boldsymbol{\alpha} \in S \setminus \{\mathbf{0}\}$, it holds $\boldsymbol{X}^{\mathbf{0}} < \boldsymbol{X}^{\boldsymbol{\alpha}}$.
- For every $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in S$, if $\boldsymbol{X}^{\boldsymbol{\alpha}} < \boldsymbol{X}^{\boldsymbol{\beta}}$ then $\boldsymbol{X}^{\boldsymbol{\alpha}+\boldsymbol{\gamma}} < \boldsymbol{X}^{\boldsymbol{\beta}+\boldsymbol{\gamma}}$.

Observation 2.10. *Monomial orders always exist for pointed affine semigroups. To construct them, first we embed any pointed affine semigroup of dimension n in a pointed rational cone $C \subset \mathbb{R}^n$. Then, we choose n linearly independent forms $l_1, \ldots, l_n$ from the dual cone of C, which is $\{l : \mathbb{R}^n \to \mathbb{R} \mid \forall \boldsymbol{\alpha} \in \mathbb{C}, l(\boldsymbol{\alpha}) \geq 0\}$. We define the monomial order so that $\boldsymbol{X}^{\boldsymbol{\alpha}} < \boldsymbol{X}^{\boldsymbol{\beta}}$ if and only if there is a $k \leq n$ such that for all $i < k$ it holds $l_i(\boldsymbol{\alpha}) = l_i(\boldsymbol{\beta})$ and $l_k(\boldsymbol{\alpha}) < l_k(\boldsymbol{\beta})$.*

Definition 2.11 (Leading monomial). Given a monomial order $<$ for a pointed affine semigroup algebra $\mathbb{K}[S]$ and a polynomial $f \in \mathbb{K}[S]$, its leading monomial, $\mathrm{LM}_<(f)$ is the biggest monomial of f with respect to the monomial order $<$.

The exponent of the leading monomial of f always corresponds to a vertex of $\mathrm{NP}(f)$.

Definition 2.12 (Gröbner basis). Let $\mathbb{K}[S]$ be a pointed affine semigroup algebra and consider a monomial order $<$ for $\mathbb{K}[S]$. For an ideal $I \subset \mathbb{K}[S]$, a set $G \subset I$ is a Gröbner basis of I if $\{LM_<(g) : g \in G\}$ generates the same ideal as $\{LM_<(f) : f \in I\}$. In other words, if for every $f \in I$, there is $g \in G$ and $\boldsymbol{X}^{\boldsymbol{\alpha}} \in \mathbb{K}[S]$ such that $\mathrm{LM}_<(f) = \boldsymbol{X}^{\boldsymbol{\alpha}}\, \mathrm{LM}_<(g)$.

As S is finitely generated, the algebra $\mathbb{K}[S]$ is a Noetherian ring [18, Thm. 7.7]. Hence, for any monomial order and any ideal, there is always a finite Gröbner basis. We will consider monomial orders for $\mathbb{K}[S^h_\Delta]$ that we can relate to monomial orders in $\mathbb{K}[S_\Delta]$ and $\mathbb{K}[\mathbb{N}^r]$.

Definition 2.13 (Multigraded monomial order). We say that a monomial order $<$ for $\mathbb{K}[S^h_\Delta]$ is multigraded, if there are monomial orders $<_\Delta$ for $\mathbb{K}[S_\Delta]$ and $<_h$ for $\mathbb{K}[\mathbb{N}^r]$ such that, for every $\boldsymbol{X}^{(\boldsymbol{\alpha}_1, \boldsymbol{d}_1)}, \boldsymbol{X}^{(\boldsymbol{\alpha}_2, \boldsymbol{d}_2)} \in \mathbb{K}[S^h_\Delta]$, it holds

$$\boldsymbol{X}^{(\boldsymbol{\alpha}_1, \boldsymbol{d}_1)} < \boldsymbol{X}^{(\boldsymbol{\alpha}_2, \boldsymbol{d}_2)} \iff \begin{cases} \boldsymbol{X}^{\boldsymbol{d}_1} <_h \boldsymbol{X}^{\boldsymbol{d}_2} \text{ or} \\ \boldsymbol{d}_1 = \boldsymbol{d}_2 \text{ and } \boldsymbol{X}^{\boldsymbol{\alpha}_1} <_\Delta \boldsymbol{X}^{\boldsymbol{\alpha}_2} \end{cases}. \quad (1)$$

Multigraded monomial orders are "compatible" with the dehomogenization morphism (Def. 2.7).

Remark 2.14. *In what follows, given a multigraded monomial order $<$ for $\mathbb{K}[S^h_\Delta]$, we also use the same symbol, that is $<$, for the associated monomial order of $\mathbb{K}[S_\Delta]$.*

Lemma 2.15. *Consider a polynomial $f \in \mathbb{K}[S_\Delta]$. Let $<$ be a multigraded monomial order. For any multidegree $\boldsymbol{d}$ and any homogeneous $F \in \mathbb{K}[S^h_\Delta]_{\boldsymbol{d}}$ such that $\chi(F) = f$, it holds $\mathrm{LM}_<(f) = \chi(\mathrm{LM}_<(F))$.*

2.3 Regularity and solutions at infinity

The Bernstein-Kushnirenko-Khovanskii (BKK) theorem bounds the (finite) number of solutions of a square system of sparse Laurent polynomials over the torus $(\mathbb{C}^*)^n$, where $(\mathbb{C}^*)^n := \mathbb{C} \setminus \{0\}$.

Definition 2.16 (Mixed volume). Let $\Delta_1, \dots, \Delta_n \in \mathbb{R}^n$ be integer polytopes. Their mixed volume, $\mathrm{MV}(\Delta_1, \dots, \Delta_n)$, is the alternating sum of the number of integer points of the polytopes obtained by all possible Minkowski sums, that is

$$\mathrm{MV}(\Delta_1 \dots \Delta_n) = (-1)^n + \sum_{k=1}^{n} (-1)^{n-k} \Big(\sum_{\substack{I \subset \{1,\dots,n\} \\ \#I = k}} \# \Big((\Delta_{I_1} + \dots + \Delta_{I_k}) \cap \mathbb{Z}^n \Big) \Big). \quad (2)$$

Theorem 2.17 (BKK bound [7, Thm 7.5.4]). *Let $f_1, \dots, f_n$ be a system of polynomials with Newton polytopes $\Delta_1, \dots, \Delta_n$ having a finite number of solutions over $(\mathbb{C}^*)^n$. The mixed volume $\mathrm{MV}(\Delta_1, \dots, \Delta_n)$ upper bounds the number of solutions of the system over the torus $(\mathbb{C}^*)^n$. If the non-zero coefficients of the polynomials are generic, then the bound is tight.*

Toric varieties relate semigroup algebras with the torus $(\mathbb{C}^*)^n$. A toric variety is an irreducible variety X that contains $(\mathbb{C}^*)^n$ as an open subset such that the action of $(\mathbb{C}^*)^n$ on itself extends to an algebraic action of $(\mathbb{C}^*)^n$ on X [8, Def. 3.1.1]. Semigroup algebras correspond to the coordinate rings of the affine pieces of X.

Given an integer polytope Δ, we can define a projective complete normal irreducible toric variety X associated to it [8, Sec. 2.3]. Likewise, given a polynomial system $(f_1, \dots, f_m)$, we can define a projective toric variety X associated to the Minkowski sum of their Newton polytopes. We can homogenize these polynomials in a way that they belong to the total coordinate ring of X [8, Sec. 5.4]. This homogenization is related to the facets of the polytopes.

To be more precise, given an integer polytope $\Delta \subset \mathbb{R}^n$, we say that an integer polytope Δ_1 is a $\mathbb{N}$-*Minkowski summand* of Δ if there is a $k \in \mathbb{N}$ and another polytope Δ_2 such that $\Delta_1 + \Delta_2 = k \cdot \Delta$ [8, Def. 6.2.11]. Every $\mathbb{N}$-Minkowski summand Δ_1 of Δ defines a torus-invariant basepoint free Cartier divisor D of the projective toric variety X associated to Δ [8, Cor. 6.2.15]. This divisor defines an invertible sheaf $\mathcal{O}_X(D)$ whose global sections form the vector space of polynomials in $\mathbb{K}[\mathbb{Z}^n]$ whose Newton polytopes are contained in Δ_1 [24, Lem. 1]. Therefore, to homogenize $f_1, \dots, f_m$ over X we need to choose polytopes $\Delta_1, \dots, \Delta_m$ such that all of them are $\mathbb{N}$-Minkowski summands of Δ associated to X and $\mathrm{NP}(f_i) \subset \Delta_i$. Hence, for any homogeneous $F \in \mathbb{K}[S^h_\Delta]_{\boldsymbol{d}}$, we can homogenize $\chi(F)$ with respect to the $\mathbb{N}$-Minkowski summand $\sum_i d_i \Delta_i$ of Δ.

We alert the reader that homogeneity in $\mathbb{K}[S^h_\Delta]_{\boldsymbol{d}}$ is different from homogeneity in the total coordinate ring of X, see [8, Sec. 5.4] but they are related through the degree $\boldsymbol{d}$.

Definition 2.18 (Solutions at infinity). Let $(f_1, \dots, f_m)$ be a system of polynomials. Let X be the projective toric variety associated to a polytope Δ such that the Newton polytope of f_i is a $\mathbb{N}$-Minkowski summand of Δ, for all i. We say that the system has no solutions at infinity with respect to X if the homogenized system with respect to their Newton polytopes has no solutions over $X \setminus (\mathbb{C}^*)^n$.

Proposition 2.19 ([24, Thm. 3]). *Consider a system $(f_1, \dots, f_n)$ having finite number of solutions over $(\mathbb{C}^*)^n$. Let X be the projective toric variety associated to the corresponding Newton polytopes. Then, the number of solutions of the homogenized system over X, counting multiplicities, is exactly the BKK bound. When the original system has no solutions at infinity, then the BKK is tight over $(\mathbb{C}^*)^n \subset X$.*

Definition 2.20 (Koszul complex, [10, Sec. 17.2]). For a sequence of homogeneous $F_1, \dots, F_k \in \mathbb{K}[S^h_\Delta]$ of multidegrees $\boldsymbol{d}_1, \dots, \boldsymbol{d}_k$ and a multidegree $\boldsymbol{d} \in \mathbb{N}^r$, we denote by $\mathcal{K}(F_1, \dots, F_k)_{\boldsymbol{d}}$ the strand of the Koszul complex of $F_1, \dots, F_k$ of multidegree $\boldsymbol{d}$, that is,

$$\mathcal{K}(F_1, \dots, F_k)_{\boldsymbol{d}} : 0 \to (\mathcal{K}_k)_{\boldsymbol{d}} \xrightarrow{\delta_k} \dots \xrightarrow{\delta_1} (\mathcal{K}_0)_{\boldsymbol{d}} \to 0,$$

where, for $1 \leq t \leq k$, we have

$$(\mathcal{K}_t)_{\boldsymbol{d}} := \bigoplus_{\substack{I \subset \{1,\dots,k\} \\ \#I = t}} \mathbb{K}[S^h_\Delta]_{(\boldsymbol{d} - \sum_{i \in I} \boldsymbol{d}_i)} \otimes (e_{I_1} \wedge \dots \wedge e_{I_t}).$$

The maps (differentials) act as follows:

$$\delta_t \Big(\sum_{\substack{I \subset \{1,\dots,k\} \\ \#I = t}} g_I \otimes (e_{I_1} \wedge \dots \wedge e_{I_t}) \Big) = \sum_{\substack{I \subset \{1,\dots,k\} \\ \#I = t}} \sum_{i=1}^{t} (-1)^{i-1} F_{I_i}\, g_I \otimes (e_{I_1} \wedge \dots \wedge \widehat{e_{I_i}} \wedge \dots \wedge e_{I_t}). \quad (3)$$

The expression $(e_{I_1} \wedge \dots \wedge \widehat{e_{I_i}} \wedge \dots \wedge e_{I_t})$ denotes that we skip the term e_{I_i} from the wedge product. We denote by $\mathcal{H}_t(F_1, \dots, F_k)_{\boldsymbol{d}}$ the t-th Koszul homology of $\mathcal{K}(F_1, \dots, F_k)_{\boldsymbol{d}}$, that is $\mathcal{H}_t(F_1, \dots, F_k)_{\boldsymbol{d}} := (\ker(\delta_t)/\mathrm{im}(\delta_{t+1}))_{\boldsymbol{d}}$.

The 0-th Koszul homology is $\mathcal{H}_0(F_1, \dots, F_k) \cong (\mathbb{K}[S^h_\Delta]/\langle F_1, \dots, F_k \rangle)$.

Definition 2.21 (Koszul and sparse regularity). A sequence $F_1, \ldots, F_k \in \mathbb{K}[S_\Delta^h]$ is Koszul regular if for every $\boldsymbol{d} \in \mathbb{N}^r$ coordinate-wise greater than or equal to $\boldsymbol{D_k} := \sum_{i=1}^k \boldsymbol{d}_i$, that is, $\boldsymbol{d} \geq \boldsymbol{D_k}$, and for every $t > 0$, the t-th Koszul homology vanishes at degree $\boldsymbol{d}$, that is $\mathcal{H}_t(F_1, \ldots, F_k)_{\boldsymbol{d}} = 0$. We say that the sequence is (sparse) regular if $F_1, \ldots, F_j$ is Koszul regular, for every $j \leq k$.

Observation 2.22. *Note that Koszul regularity does not depend on the order of the polynomials, as (sparse) regularity does.*

3 THE ALGORITHM

To compute Gröbner basis over $\mathbb{K}[S_\Delta]$ we work over $\mathbb{K}[S_\Delta^h]$. We follow the classical approach of Lazard [22] adapted to the semi-group case, see also [15]; we "linearize" the problem by reducing the Gröbner basis computation to a linear algebra problem.

Lemma 3.1. *Consider $F_1, \ldots, F_m \in \mathbb{K}[S_\Delta^h]$ and a multigraded monomial order $<$ for $\mathbb{K}[S_\Delta]$ (Def. 2.13). There is a multidegree $\boldsymbol{d}$ and homogeneous $\{G_1, \ldots, G_t\} \subset \langle F_1, \ldots, F_m \rangle \cap \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}}$ such that $\{\chi(G_1), \ldots, \chi(G_t)\}$ is a Gröbner basis of the ideal $\langle \chi(F_1), \ldots, \chi(F_m) \rangle$ with respect to the associated monomial order $<$ (Rem. 2.14).*

Proof. Let $g_1, \ldots, g_t \in \mathbb{K}[S_\Delta]$ be a Gröbner basis for the ideal $\langle \chi(F_1), \ldots, \chi(F_m) \rangle$ with respect to $<$. By Obs. 2.8, there are polynomials $\bar{G}_1, \ldots, \bar{G}_t \in \langle F_1, \ldots, F_m \rangle$ such that $\chi(\bar{G}_i) = g_i$, for $i \in [t]$. Consider $\boldsymbol{d} \in \mathbb{N}^r$ such that $\boldsymbol{d} \geq \mathrm{mdeg}(\bar{G}_i)$, for $i \in [t]$. It suffices to consider $G_i = \boldsymbol{X}^{(\boldsymbol{0}, \boldsymbol{d} - \mathrm{mdeg}(\bar{G}_i))} \bar{G}_i \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}}$, for $i \in [t]$. □

When we know a multidegree $\boldsymbol{d}$ that satisfies Lem. 3.1, we can compute the Gröbner basis over $\mathbb{K}[S_\Delta]$ using linear algebra.

Definition 3.2 (Macaulay matrix). A Macaulay matrix $\mathcal{M}$ of degree $\boldsymbol{d} \in \mathbb{N}^r$ with respect to a monomial order $<$ is a matrix whose columns are indexed by all monomials $\boldsymbol{X}^{(\boldsymbol{\alpha}, \boldsymbol{d})} \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}}$ and the rows by polynomials in $\mathbb{K}[S_\Delta^h]_{\boldsymbol{d}}$. The indices of the columns are sorted in decreasing order with respect to $<$. The element of $\mathcal{M}$ whose row corresponds to a polynomial F and whose column corresponds to a monomial $\boldsymbol{X}^{(\boldsymbol{\alpha}, \boldsymbol{d})}$ is the coefficient of the monomial $\boldsymbol{X}^{(\boldsymbol{\alpha}, \boldsymbol{d})}$ of F. Let $\mathtt{Rows}(\mathcal{M})$ be the set of non-zero polynomials that index the rows of $\mathcal{M}$ and $\mathrm{LM}_<(\mathtt{Rows}(\mathcal{M}))$ be the set of leading monomials of these polynomials.

Remark 3.3. *As the columns of the Macaulay matrices are sorted in decreasing order with respect to a monomial order, the leading monomial of a polynomial associated to a row corresponds to the index of the column of the first non-zero element in this row.*

Definition 3.4. Given a Macaulay matrix $\mathcal{M}$, let $\widetilde{\mathcal{M}}$ be a new Macaulay matrix corresponding to the row echelon form of $\mathcal{M}$. We can compute $\widetilde{\mathcal{M}}$ by applying Gaussian elimination to $\mathcal{M}$.

Remark 3.5. *When we perform row operations (excluding multiplication by 0) to a Macaulay matrix, we do not change the ideal spanned by the polynomials corresponding to its rows.*

We use Macaulay matrices to compute a basis for the vector space $\langle F_1, \ldots, F_k \rangle_{\boldsymbol{d}} := \langle F_1, \ldots, F_k \rangle \cap \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}}$ by Gaussian elimination.

Lemma 3.6. *Consider homogeneous polynomials $F_1, \ldots, F_k \in \mathbb{K}[S_\Delta^h]$ of multidegrees $\boldsymbol{d_1}, \ldots, \boldsymbol{d_k}$ and a multigraded monomial order $<$. Let*

Algorithm 1 `ComputeGB`

Input: $f_1, \ldots, f_k \in \mathbb{K}[S_\Delta]$, a monomial order $<$.
Output: Gröbner basis for $\langle f_1, \ldots, f_k \rangle$ with respect to $<$.

1: **for all** f_i **do**
2: Choose $F_i \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d_i}}$ of multidegree $\boldsymbol{d_i}$ such that $\chi(F_i) = f_i$.
3: Pick a big enough $\boldsymbol{d} \in \mathbb{N}^r$ that satisfies Lem. 3.1.
4: $\mathcal{M}_{\boldsymbol{d}}^k \leftarrow$ Macaulay matrix of multidegree $\boldsymbol{d}$ with respect to a multigraded monomial order associated to $<$. (This matrix has zero rows)
5: **for all** F_i **do**
6: **for all** $\boldsymbol{X}^{(\boldsymbol{\alpha}, \boldsymbol{d} - \boldsymbol{d_i})} \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d} - \boldsymbol{d_i}}$ **do**
7: Add the polynomial $\boldsymbol{X}^{(\boldsymbol{\alpha}, \boldsymbol{d} - \boldsymbol{d_i})} F_i$ as row to $\mathcal{M}_{\boldsymbol{d}}^k$.
8: $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k \leftarrow \mathtt{GaussianElimination}(\mathcal{M}_{\boldsymbol{d}}^k)$
9: **return** $\chi(\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k))$

$\mathcal{M}_{\boldsymbol{d}}^k$ be the Macaulay matrix whose rows correspond to the polynomials that we obtain by considering the product of every monomial of multidegree $\boldsymbol{d} - \boldsymbol{d_i}$ and every polynomial F_i; that is

$$\mathtt{Rows}(\mathcal{M}_{\boldsymbol{d}}^k) = \left\{ \boldsymbol{X}^{(\boldsymbol{\alpha}, \boldsymbol{d} - \boldsymbol{d_i})} F_i : i \in [k], \boldsymbol{X}^{(\boldsymbol{\alpha}, \boldsymbol{d} - \boldsymbol{d_i})} \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d} - \boldsymbol{d_i}} \right\}. \quad (4)$$

Let $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k$ be the row echelon form of the Macaulay matrix $\mathcal{M}_{\boldsymbol{d}}^k$ (Def. 3.4).

Then, the set of the leading monomials of the polynomials in $\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k)$ with respect to $<$ is the set of all the leading monomials of the ideal $\langle F_1, \ldots, F_k \rangle$ at degree $\boldsymbol{d}$.

Proof. We prove that $\mathrm{LM}_<(\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k)) = \mathrm{LM}_<(\langle F_1, \ldots, F_k \rangle_{\boldsymbol{d}})$. First, we show that $\mathrm{LM}_<(\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k)) \supseteq \mathrm{LM}_<(\langle F_1, \ldots, F_k \rangle_{\boldsymbol{d}})$. Let G be a polynomial in the vector space of polynomials of degree $\boldsymbol{d}$ in $\langle F_1, \ldots, F_k \rangle$. This vector space, $\langle F_1, \ldots, F_k \rangle_{\boldsymbol{d}}$, is isomorphic to the row space of $\mathcal{M}_{\boldsymbol{d}}^k$, which, in turn, is the same as the row space of $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k$, by Rem. 3.5. Hence, there is a vector v in the row space of $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k$ that corresponds to G. Let s be the index of the first non-zero element of v. As $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k$ is in row echelon form and v belongs to its row space, there is a row of $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k$ such that its first non-zero element is also at the s-th position. Let F be the polynomial that corresponds to this row. Finally, the leading monomials of the polynomials F and G are the same, that is $LM_<(G) = LM_<(F)$, by Rem. 3.3.

The other direction is straightforward. □

Theorem 3.7. *Consider the ideal generated by homogeneous polynomials $F_1, \ldots, F_k \in \mathbb{K}[S_\Delta^h]$ of multidegrees $\boldsymbol{d_1}, \ldots, \boldsymbol{d_k}$. Consider a multigraded monomial order $<$ and a multidegree $\boldsymbol{d} \in \mathbb{N}^r$ that satisfy Lem. 3.1. Let $\mathcal{M}_{\boldsymbol{d}}^k$ and $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k$ be the Macaulay matrices of Lem. 3.6.*

Then, the set $\chi(\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k))$, see Def. 2.7, is a Gröbner basis of the ideal $\langle \chi(F_1), \ldots, \chi(F_k) \rangle \subset \mathbb{K}[S_\Delta]$ with respect to $<$.

Proof. Let $R := \mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k)$ be the set of polynomials indexing the rows of $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k$. By Lem. 3.6, for every $G \in \langle F_1, \ldots, F_k \rangle_{\boldsymbol{d}}$ there is a $F \in R$ such that $LM_<(G) = LM_<(F)$. As $<$ is a multigraded order, it holds $LM_<(\chi(G)) = LM_<(\chi(F))$ (Lem. 2.15). As $\boldsymbol{d}$ satisfies Lem. 3.1 for every $h \in \langle \chi(F_1), \ldots, \chi(F_k) \rangle$ there is $G \in \langle F_1, \ldots, F_k \rangle_{\boldsymbol{d}}$ such that $LM_<(\chi(G))$ divides $LM_<(h)$. Hence, there is an $F \in R$ such that $LM_<(\chi(F))$ divides $LM_<(h)$. Therefore, R is a Gröbner basis for $\langle \chi(F_1), \ldots, \chi(F_k) \rangle$. □

As with the MatrixF5 algorithm [9], the correctness of this approach relies on knowing a priori the multidegree $\boldsymbol{d}$ from Lem. 3.1.

Algorithm 2 `ReduceMacaulay`

Input: Homogeneous $F_1, \dots, F_k \in \mathbb{K}[S_\Delta^h]$ of multidegree $\boldsymbol{d}_1, \dots, \boldsymbol{d}_k$, a multidegree $\boldsymbol{d}$, and a monomial order $<$.

Output: The Macaulay matrix of $\langle F_1, \dots, F_k\rangle_{\boldsymbol{d}} \in \mathbb{K}[S_\Delta^h]$ with respect to $<$ in row echelon form.

$\mathcal{M}_{\boldsymbol{d}}^k \leftarrow$ Macaulay matrix with columns indexed by the monomials in $\mathbb{K}[S_\Delta^h]_{\boldsymbol{d}}$ in decreasing order w.r.t. $<$. (This matrix has zero rows)
if $k > 1$ **then**
  $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^{k-1} \leftarrow$ `ReduceMacaulay`$(\{F_1, \dots, F_{k-1}\}, \boldsymbol{d}, <)$
  $\widetilde{\mathcal{M}}_{\boldsymbol{d}-\boldsymbol{d}_k}^{k-1} \leftarrow$ `ReduceMacaulay`$(\{F_1, \dots, F_{k-1}\}, \boldsymbol{d}-\boldsymbol{d}_k, <)$
  for $F \in$ `Rows`$(\widetilde{\mathcal{M}}_{\boldsymbol{d}}^{k-1})$ **do**
    Add the polynomial F as a row to $\mathcal{M}_{\boldsymbol{d}}^k$.
  for $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d}_k)} \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}-\boldsymbol{d}_k} \setminus \mathrm{LM}_<($`Rows`$(\widetilde{\mathcal{M}}_{\boldsymbol{d}-\boldsymbol{d}_k}^{k-1}))$ **do**
    Add the polynomial $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d}_k)} F_k$ as a row to $\mathcal{M}_{\boldsymbol{d}}^k$.
$\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k \leftarrow$ `GaussianElimination`$(\mathcal{M}_{\boldsymbol{d}}^k)$
return $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^k$

3.1 Exploiting the structure of Macaulay matrices (Koszul F5 criterion)

If we consider all the polynomials of the set in Eq. (4), then many of them are linearly dependent. Hence, when we construct the Macaulay matrix of Thm. 3.7 and perform Gaussian elimination, many of the rows reduce to zero; this forces Alg. 1 to perform unnecessary computations. We will extend to F5 criterion [13] in our setting to avoid redundant computations.

Theorem 3.8 (Koszul F5 criterion). *Consider homogeneous polynomials $F_1, \dots, F_k \in \mathbb{K}[S_\Delta^h]$ of multidegrees $\boldsymbol{d_1}, \dots, \boldsymbol{d_k}$ and a multidegree $\boldsymbol{d} \in \mathbb{N}^r$ such that $\boldsymbol{d} \geq \boldsymbol{d_k}$, that is coordinate-wise greater than or equal to $\boldsymbol{d_k}$. Let $\mathcal{M}_{\boldsymbol{d}}^{k-1}$ and $\mathcal{M}_{\boldsymbol{d}-\boldsymbol{d_k}}^{k-1}$ be the Macaulay matrices of degrees $\boldsymbol{d}$ and $\boldsymbol{d}-\boldsymbol{d_k}$, respectively, of the polynomials $F_1, \dots, F_{k-1}$ as in Thm. 3.7, and let $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^{k-1}$ and $\widetilde{\mathcal{M}}_{\boldsymbol{d}-\boldsymbol{d_k}}^{k-1}$ be their row echelon forms.*

For every $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d_k})} \in \mathrm{LM}_<(\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}-\boldsymbol{d_k}}^{k-1}))$, the polynomial $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d_k})} F_k$ is a linear combination of the polynomials

$$\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}}^{k-1}) \cup \left\{ \boldsymbol{X}^{(\boldsymbol{\beta},\boldsymbol{d}-\boldsymbol{d_k})} F_k : \begin{array}{l} \boldsymbol{X}^{(\boldsymbol{\beta},\boldsymbol{d}-\boldsymbol{d_k})} \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}-\boldsymbol{d_k}} \text{ and} \\ \boldsymbol{X}^{(\boldsymbol{\beta},\boldsymbol{d}-\boldsymbol{d_k})} < \boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d_k})} \end{array} \right\}.$$

Proof. If $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d_k})} \in \mathrm{LM}_<(\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}-\boldsymbol{d_k}}^{k-1}))$, then there is $G \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}-\boldsymbol{d_k}}$ such that $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d_k})} + G \in \langle F_1, \dots, F_{k-1}\rangle_{\boldsymbol{d}-\boldsymbol{d_k}}$ and $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d_k})} > \mathrm{LM}_<(G)$. So, there are homogeneous $H_1, \dots, H_{k-1} \in \mathbb{K}[S_\Delta^h]$ such that $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d_k})} + G = \sum_i H_i F_i$. The proof follows by noticing that $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d_k})} F_k = \sum_{i=1}^{k-1} (F_k H_i) F_i - G F_k$. ◻

In the following, $\mathcal{M}_{\boldsymbol{d}}^k$ is not the Macaulay matrix of Lem. 3.6. It contains less rows because of the Koszul F5 criterion. However, both matrices have the same row space, so we use the same name.

Corollary 3.9. *Using the notation of Thm. 3.8, let $\mathcal{M}_{\boldsymbol{d}}^k$ be a Macaulay matrix of degree $\boldsymbol{d}$ w.r.t. the order $<$ whose rows are*

$$\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}}^{k-1}) \cup \left\{ \boldsymbol{X}^{(\boldsymbol{\beta},\boldsymbol{d}-\boldsymbol{d_k})} F_k : \begin{array}{l} \boldsymbol{X}^{(\boldsymbol{\beta},\boldsymbol{d}-\boldsymbol{d_k})} \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}-\boldsymbol{d_k}} \text{ and} \\ \boldsymbol{X}^{(\boldsymbol{\beta},\boldsymbol{d}-\boldsymbol{d_k})} \notin \mathrm{LM}_<(\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}-\boldsymbol{d_k}}^{k-1})) \end{array} \right\}$$

The row space of $\mathcal{M}_{\boldsymbol{d}}^k$ and the Macaulay matrix of Lem. 3.6 are equal.

The correctness of Alg. 2 follows from Thm. 3.8.

Lemma 3.10. *If $\mathcal{H}_1(F_1, \dots, F_k)_{\boldsymbol{d}} = 0$ and there is a syzygy $\sum_i G_i F_i = 0$ such that $G_i \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}-\boldsymbol{d}_i}$, then $G_k \in \langle F_1, \dots, F_{k-1}\rangle_{\boldsymbol{d}-\boldsymbol{d_k}}$.*

Proof. We consider the Koszul complex $\mathcal{K}(F_1, \dots, F_k)$ (Def. 2.20). As $\sum_i G_i F_i = \delta_1(G_1, \dots, G_k)$, the vector of polynomials $(G_1, \dots, G_k)$ belongs to the Kernel of δ_1. As $\mathcal{H}_1(F_1, \dots, F_k)_{\boldsymbol{d}}$ vanishes, the kernel of δ_1 is generated by the image of δ_2. The latter map is

$$(H_{1,2}, \dots, H_{k-1,k}) \mapsto \sum_{1 \leq i < j \leq k} H_{i,j}(F_j \boldsymbol{e}_i - F_i \boldsymbol{e}_j),$$

where $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ is the canonical basis of $\mathbb{R}^k$. Hence, there are homogeneous polynomials $(H_{1,2}, \dots, H_{k-1,k})$ such that

$$(G_1, \dots, G_k) = \sum_{1 \leq i < j \leq k} H_{i,j}(F_j \boldsymbol{e}_i - F_i \boldsymbol{e}_j).$$

Thus, $G_k = \sum_{i=1}^{k-1} H_{i,k} F_i$ and so $G_k \in \langle F_1, \dots, F_{k-1}\rangle_{\boldsymbol{d}-\boldsymbol{d_k}}$. ◻

The next lemma shows that we avoid all redundant computations, that is all the rows reducing to zero during Gaussian elimination.

Lemma 3.11. *If $\mathcal{H}_1(F_1, \dots, F_k)_{\boldsymbol{d}} = 0$, then all the rows of the matrix $\mathcal{M}_{\boldsymbol{d}}^k$ in Alg. 2 are linearly independent.*

Proof. By construction, the rows of $\mathcal{M}_{\boldsymbol{d}}^k$ corresponding to $\widetilde{\mathcal{M}}_{\boldsymbol{d}}^{k-1}$ are linearly independent because the matrix is in row echelon form. Hence, if there are rows that are not linearly independent, then at least one of them corresponds to a polynomial of the form $\boldsymbol{X}^{(\boldsymbol{\alpha},\boldsymbol{d}-\boldsymbol{d_k})} F_k$. The right action of the Macaulay matrix $\mathcal{M}_{\boldsymbol{d}}^k$, that is the linear function defined by its matrix-vector multiplication by right, represents a map equivalent to the map δ_1 from the strand of Koszul complex $\mathcal{K}(F_1, \dots, F_k)_{\boldsymbol{d}}$. Hence, if some of the rows of the matrix are linearly dependent, then there is an element in the kernel of δ_1. That is, there are $G_i \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{d}-\boldsymbol{d}_i}$ such that

- $\sum_{i=1}^{k-1} G_i F_i$ belongs to the linear span of `Rows`$(\widetilde{\mathcal{M}}_{\boldsymbol{d}}^{k-1})$,
- the monomials of G_k do not belong to $\mathrm{LM}_<(\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}-\boldsymbol{d_k}}^{k-1}))$, and
- $\sum_{i=1}^{k} G_i F_i = 0$.

By Lem. 3.10, $G_k \in \langle F_1, \dots, F_{k-1}\rangle_{\boldsymbol{d}-\boldsymbol{d_k}}$. By Lem. 3.6 and Cor. 3.9, the leading monomials of `Rows`$(\widetilde{\mathcal{M}}_{\boldsymbol{d}-\boldsymbol{d_k}}^{k-1})$ and the ideal $\langle F_1, \dots, F_{k-1}\rangle$ at degree $\boldsymbol{d}-\boldsymbol{d_k}$ are the same. Hence, we reach a contradiction because we have assumed that the leading monomial of G_k does not belong to $\mathrm{LM}_<(\mathtt{Rows}(\widetilde{\mathcal{M}}_{\boldsymbol{d}-\boldsymbol{d_k}}^{k-1}))$. ◻

Corollary 3.12. *If $F_1, \dots, F_k$ is a sparse regular polynomial system (Def. 2.21) and $\boldsymbol{d} \in \mathbb{N}^r$ is such that $\boldsymbol{d} \geq (\sum_i \boldsymbol{d}_i)$, then* `ReduceMacaulay`$(F_1, \dots, F$ *) only considers matrices with linearly independent rows and avoids all redundant computations.*

To benefit from the Koszul F5 criterion and compute with smaller matrices during the Gröbner basis computation we should replace Lines 4 – 8 in Alg. 1 by `ReduceMacaulay`$(F_1, \dots, F_k, \boldsymbol{d}, <)$ (Alg. 2).

4 GRÖBNER BASES FOR 0-DIM SYSTEMS

We introduce an algorithm, that takes as input a 0-dimensional ideal I and computes a Gröbner basis for the ideal $\left(I : \langle \prod_j x_j \rangle^\infty\right)$. The latter corresponds to the ideal associated to the intersection of the torus $(\mathbb{C}^*)^n$ with the variety defined by I.

Let $f_1, \dots, f_n \in \mathbb{K}[\boldsymbol{x}]$ be a square 0-dimensional system. First we embed each f_i in $\mathbb{K}[\mathbb{Z}^n]$. We multiply each polynomial by an appropriate monomial, $\boldsymbol{X}^{\boldsymbol{\beta}_i} \in \mathbb{K}[\mathbb{Z}^n]$, so that $\mathbf{0}$ is a vertex of each new polynomial, as well as, a vertex of their Minkowski sum. Let the Newton polytopes be $\Delta_i = \mathrm{NP}(\boldsymbol{X}^{\boldsymbol{\beta}_i} f_i)$, for $1 \leq i \leq n$, Let Δ_0 be the standard n-simplex; it is the Newton polytope of $\mathrm{NP}(1 + \sum_i x_i)$. We consider the algebras $\mathbb{K}[S_\Delta]$ and $\mathbb{K}[S^h_\Delta]$ associated to the polytopes $\Delta_0, \dots, \Delta_n$ and the embedding $\boldsymbol{X}^{\boldsymbol{\beta}_1} f_1, \dots, \boldsymbol{X}^{\boldsymbol{\beta}_1} f_n \in \mathbb{K}[S_\Delta]$. For each i, we consider $F_i \in \mathbb{K}[S^h_\Delta]_{\boldsymbol{e}_i}$ such that $\chi(F_i) = \boldsymbol{X}^{\boldsymbol{\beta}_i} f_i \in \mathbb{K}[S_\Delta]$.

Assumption 4.1. *Using the previous notation, let X be the projective toric variety associated to $\Delta_0 + \cdots + \Delta_n$ (see also the discussion on toric varieties at Sec. 2.3). Assume that the system $(f_1, \dots, f_n)$ has no solutions at infinity with respect to X (Def. 2.18). Further, assume that the system $(f_0, f_1, \dots, f_n)$, where f_0 is generic linear polynomial, has no solutions over $(\mathbb{C}^*)^n$.*

Lemma 4.2 ([24, Thm. 3.a]). *Under Assum. 4.1, for every $\boldsymbol{d} \in \mathbb{N}^{n+1}$ such that $\boldsymbol{d} \geq \sum_{i>0} \boldsymbol{e}_i$, it holds $\mathcal{H}_0(F_1, \dots, F_n)_{\boldsymbol{d}} \cong \mathbb{K}[\mathbb{Z}^n]/\langle f_1, \dots, f_n \rangle$.*

Lemma 4.3 ([24, Thm. 3.c]). *Under Assum. 4.1, for every homogeneous polynomial $F_0 \in \mathbb{K}[S^h_\Delta]_{\boldsymbol{d}_0}$ such that the system $(f_1, \dots, f_n, \chi(F_0))$ has no solutions over $(\mathbb{C}^*)^n$, the system $(F_1, \dots, F_n, F_0)$ is Koszul regular (Def. 2.21) and, for every $\boldsymbol{d} \in \mathbb{N}^{n+1}$ such that $\boldsymbol{d} \geq \sum_i \boldsymbol{e}_i + \boldsymbol{d}_0$, $\langle F_1, \dots, F_n, F_0 \rangle_{\boldsymbol{d}} = \mathbb{K}[S^h_\Delta]_{\boldsymbol{d}}$.*

Proof. The homogenization of system $(f_1, \dots, f_n, \chi(F_0))$ with respect to the toric variety X has no solutions over X (see at Sec. 2.3 the discussion before Def. 2.18). To see this, notice that by Assum. 4.1 the homogenization of the system $(f_1, \dots, f_n)$ with respect to X has no solutions over $X \setminus (\mathbb{C}^*)^n$ (see also Def. 2.18). Moreover, we also assume that there are no solutions over $(\mathbb{C}^*)^n$ of $(f_1, \dots, f_n, \chi(F_0))$.

Now, the proof follows from the argument in the proof of [24, Thm. 3]. This argument is the same as in [17, Prop. 3.4.1], where the stably twisted condition is given by [24, Thm. 1]. □

Corollary 4.4. *For any monomial $\boldsymbol{X}^{(\boldsymbol{\alpha}, D\,\boldsymbol{e}_0)} \in \mathbb{K}[S^h_\Delta]_{D\,\boldsymbol{e}_0}$, the system $(F_1, \dots, F_n, \boldsymbol{X}^{(\boldsymbol{\alpha}, D\,\boldsymbol{e}_0)})$ is Koszul regular. For every $\boldsymbol{d} \in \mathbb{N}^{n+1}$ such that $\boldsymbol{d} \geq \sum_i \boldsymbol{e}_i + D\,\boldsymbol{e}_0$, it holds $\langle F_1 \dots F_n, \boldsymbol{X}^{(\boldsymbol{\alpha}, D\,\boldsymbol{e}_0)} \rangle_{\boldsymbol{d}} = \mathbb{K}[S^h_\Delta]_{\boldsymbol{d}}$.*

Fix a graded monomial order $<$ for $\mathbb{K}[S^h_\Delta]$; $\mathcal{L}$ is the set of monomials that are not leading monomials of $\langle F_1, \dots, F_n \rangle_{\sum_{i \geq 1} \boldsymbol{e}_i}$, that is

$$\mathcal{L} := \left\{ \boldsymbol{X}^{(\boldsymbol{\alpha}, \sum_{i \geq 1} \boldsymbol{e}_i)} \in \mathbb{K}[S^h_\Delta]_{\sum_{i \geq 1} \boldsymbol{e}_i} : \begin{array}{c} \forall G \in \langle F_1, \dots, F_n \rangle_{\sum_{i \geq 1} \boldsymbol{e}_i}, \\ \mathrm{LM}_<(G) \neq \boldsymbol{X}^{(\boldsymbol{\alpha}, \sum_{i \geq 1} \boldsymbol{e}_i)} \end{array} \right\}.$$

We will prove that the dehomogenization of these monomials, $\chi(\mathcal{L})$, forms a monomial basis for $\mathbb{K}[\mathbb{Z}^n]/\langle f_1, \dots, f_n \rangle$.

Lemma 4.5. *The monomials in the set $\chi(\mathcal{L})$ are $\mathbb{K}$-linearly independent in $\mathbb{K}[\mathbb{Z}^n]/\langle f_1, \dots, f_n \rangle$.*

Proof. Assume that the lemma does not hold. Hence, there are $c_1, \dots, c_v \in \mathbb{K}$, not all of them 0, and $g_1, \dots, g_n \in \mathbb{K}[\mathbb{Z}^n]$ such that $\sum_i c_i \chi(\mathcal{L}_i) = \sum_i g_i f_i$. We can clear the denominators, introduced by the g_i's, by choosing a monomial $\boldsymbol{X}^{\boldsymbol{\alpha}} \in \mathbb{K}[\mathbb{N}^n]$ such that, for every i, $\left(\frac{\boldsymbol{X}^{\boldsymbol{\alpha}}}{\boldsymbol{X}^{\boldsymbol{\beta}_i}} g_i \right) \in \mathbb{K}[\mathbb{N}^n]$. Moreover, there is a degree $D \in \mathbb{N}$ and homogeneous polynomials $G_i \in \mathbb{K}[S^h_\Delta]$ of multidegrees $(D\,\boldsymbol{e}_0 + \sum_{j>0} \boldsymbol{e}_j - \boldsymbol{e}_i)$ such that $\chi(G_i) = \left(\frac{\boldsymbol{X}^{\boldsymbol{\alpha}}}{\boldsymbol{X}^{\boldsymbol{\beta}_i}} g_i \right)$ and $\boldsymbol{X}^{(\boldsymbol{\alpha}, D\,\boldsymbol{e}_0)} \sum_i c_i \mathcal{L}_i = \sum_i G_i F_i$. By Lem. 4.3, $(F_1, \dots, F_n, \boldsymbol{X}^{(\boldsymbol{\alpha}, D\,\boldsymbol{e}_0)})$ is Koszul regular and so, by Lem. 3.10, $\sum_i c_i \mathcal{L}_i \in \langle F_1, \dots, F_n \rangle_{\sum_{i>1} \boldsymbol{e}_i}$. So, a monomial in $\mathcal{L}$ is a leading monomial of an element in $\langle F_1, \dots, F_n \rangle_{\sum_{i>1} \boldsymbol{e}_i}$. This is a contradiction as, by construction, there is no monomial in $\mathcal{L}$ which is a leading monomial of a polynomial in $\langle F_1, \dots, F_n \rangle_{\sum_{i>1} \boldsymbol{e}_i}$. □

Corollary 4.6. *The set of monomials $\chi(\mathcal{L})$ is a monomial basis of $\mathbb{K}[\mathbb{Z}^n]/\langle f_1, \dots, f_n \rangle$.*

Proof. By Lem. 4.2, the number of elements in $\mathcal{L}$ and the dimension of $\mathbb{K}[\mathbb{Z}^n]/\langle f_1, \dots, f_n \rangle$ are the same. If we fix a multidegree $\boldsymbol{d} \in \mathbb{N}^r$, then the map χ restricted to $\mathbb{K}[S^h_\Delta]_{\boldsymbol{d}}$ is injective. Hence, the sets $\mathcal{L}$ and $\chi(\mathcal{L})$ have the same number of elements. By Lem. 4.5, the monomials in the set $\chi(\mathcal{L})$ are linearly independent. □

Remark 4.7. *One way to compute the set $\mathcal{L}$ is to compute a basis of the vector space $\langle F_1, \dots, F_n \rangle_{\sum_{i \geq 1} \boldsymbol{e}_i}$ using Alg. 2, that is* $\texttt{ReduceMacaulay}\left((F_1, \dots, F_n), \sum_{i \geq 1} \boldsymbol{e}_i, <\right)$.

For each $F_0 \in \mathbb{K}[S^h_\Delta]_{\boldsymbol{e}_0}$, we will construct a Macaulay matrix for $(F_1, \dots, F_n, F_0)$ at multidegree $\mathbf{1} := \sum_i \boldsymbol{e}_i$, say $\mathcal{M}(F_0)$; from this matrix we will recover the multiplication map of $\chi(F_0)$ in $\mathbb{K}[\boldsymbol{x}]/\langle f_1, \dots, f_n \rangle$. The rows of $\mathcal{M}(F_0)$ are of two kinds:

- the polynomials in $\mathtt{Rows}(\widetilde{\mathcal{M}}^n_{\mathbf{1}})$, where $\widetilde{\mathcal{M}}^n_{\mathbf{1}} = \texttt{ReduceMacaulay}\left((F_1, \dots, F_n), \mathbf{1}, <\right)$,
- the polynomials of the form $m\,F_0$, where $m \in \mathcal{L}$.

Lemma 4.8. *The matrix $\mathcal{M}(F_0)$ is always square. It is full-rank if and only if $(F_1, \dots, F_n, F_0)$ is Koszul regular.*

Proof. According to the Koszul F5 criterion (see Thm. 3.8), the row space spanned by $\mathcal{M}(F_0)$ is the same as the vector space $\langle F_1, \dots, F_n, F_0 \rangle_{\mathbf{1}}$ for any choice of F_0. We can consider an F_0 such that $(F_1, \dots, F_n, F_0)$ is Koszul regular, by Cor. 4.4. Then, the rows of $\mathcal{M}(F_0)$ generate $\mathbb{K}[S^h_\Delta]_{\mathbf{1}}$ and, by Lem. 3.11, the rows of $\mathcal{M}(F_0)$ are linearly independent. Hence, by Lem. 4.3, for this particular F_0, the matrix $\mathcal{M}(F_0)$ is square and full-rank. However, the matrix $\mathcal{M}(F_0)$ is square for any choice of F_0, because its number of rows does not depend on F_0. Nevertheless, it is not full-rank for any choice of F_0. If $\mathcal{M}(F_0)$ is full-rank, then $(F_1, \dots, F_n, F_0)$ is Koszul regular because, by the sparse Nullstellensatz [29, Thm. 2], the homogenization of the system $(f_1, \dots, f_n, \chi(F_0))$ has no solutions over $(\mathbb{C}^*)^n$. Consequently, the proof follows from Lem. 4.3. □

We reorder the columns of $\mathcal{M}(F_0)$ as shown in Eq. (5), such that

- the columns of the submatrix $\left(\frac{M_{1,2}(F_0)}{M_{2,2}(F_0)} \right)$ correspond to monomials of the form $m\,\boldsymbol{X}^{(\mathbf{0}, \boldsymbol{e}_0)}$, where $m \in \mathcal{L}$, and
- the rows of $\left(M_{2,1}(F_0) \mid M_{2,2}(F_0) \right)$ are polynomials of the form $m\,F_0$, where $m \in \mathcal{L}$.

$$\begin{array}{r} \\ \mathtt{Rows}(\widetilde{\mathcal{M}}^n_{\mathbf{1}}) \left\{ \right. \\ F_0 \cdot \mathcal{L} \left\{ \right. \end{array} \begin{array}{c} \hspace{4em} \overbrace{\hspace{4em}}^{\boldsymbol{X}^{(\mathbf{0}, \boldsymbol{e}_0)} \cdot \mathcal{L}} \\ \left[\begin{array}{c||c} M_{1,1}(F_0) & M_{1,2}(F_0) \\ \hline\hline M_{2,1}(F_0) & M_{2,2}(F_0) \end{array} \right] \end{array} \qquad (5)$$

We prove that $M_{1,1}(F_0)$ is invertible and the Schur complement of $M_{2,2}(F_0)$, $M^c_{2,2}(F_0) := (M_{2,2} - M_{2,1}\, M_{1,1}^{-1}\, M_{1,2})(F_0)$, is the multiplication map of $\chi(F_0)$ in the basis $\chi(\mathcal{L})$ of $\mathbb{K}[\mathbb{Z}^n]/\langle f_1,\ldots,f_n\rangle$.

Lemma 4.9. *If $(F_1,\ldots,F_n,\boldsymbol{X}^{(0,\boldsymbol{e}_0)})$ is Koszul regular then, for any $F_0 \in \mathbb{K}[S^h_\Delta]_{\boldsymbol{e}_0}$, the matrix $M_{1,1}(F_0)$ is invertible.*

Proof. By Lem. 4.8, as the system $(F_1,\ldots,F_n,\boldsymbol{X}^{(0,\boldsymbol{e}_0)})$ is Koszul regular, then the matrix $\mathcal{M}(\boldsymbol{X}^{(0,\boldsymbol{e}_0)})$ is invertible. As $M_{2,1}(\boldsymbol{X}^{(0,\boldsymbol{e}_0)})$ is the zero matrix and $M_{2,2}(\boldsymbol{X}^{(0,\boldsymbol{e}_0)})$ is the identity, then $M_{1,1}(\boldsymbol{X}^{(0,\boldsymbol{e}_0)})$ must be invertible. By construction, the matrices $M_{1,1}(F_0)$ and $M_{1,2}(F_0)$ are independent of the choice of F_0. Hence, for any F_0 the matrix $M_{1,1}(F_0)$ is invertible. □

Theorem 4.10. *The multiplication map of $\chi(F_0)$ in the monomial basis $\chi(\mathcal{L})$ of $\mathbb{K}[\mathbb{Z}^n]/\langle f_1,\ldots,f_n\rangle$ is the Schur complement of $M_{2,2}(F_0)$, that is $M^c_{2,2}(F_0) := (M_{2,2} - M_{2,1}\, M_{1,1}^{-1}\, M_{1,2})(F_0)$.*

Proof. Note that for every $F_0 \in \mathbb{K}[S^h_\Delta]_{\boldsymbol{e}_0}$ and each element L_i of $\mathcal{L}$, $L_i F_0 \equiv \boldsymbol{X}^{(0,\boldsymbol{e}_0)} \sum_j (M^c_{2,2}(F_0))_{i,j} L_j$ in $\mathbb{K}[S^h_\Delta]/\langle F_1,\ldots,F_n\rangle$, where $(M^c_{2,2}(F_0)_{i,j}$ is the (i,j) element of the matrix $M^c_{2,2}(F_0))$. Hence, if we dehomogenize this relation we obtain that, $\chi(L_i)\chi(F_0) \equiv \sum_j (M^c_{2,2}(F_0))_{i,j}\chi(L_j)$ in $\mathbb{K}[S_\Delta]/\langle \boldsymbol{X}^{\beta_1} f_1,\ldots,\boldsymbol{X}^{\beta_n} f_n\rangle$. As $\mathbb{K}[S_\Delta] \subset \mathbb{K}[\mathbb{Z}^n]$, the same relation holds in $\mathbb{K}[\mathbb{Z}^n]/\langle f_1,\ldots,f_n\rangle$. By Cor. 4.6, the set $\chi(\mathcal{L})$ is a monomial basis of $\mathbb{K}[\mathbb{Z}^n]/\langle f_1,\ldots,f_n\rangle$. Therefore, $M^c_{2,2}(F_0)$ is the multiplication map of F_0 in $\mathbb{K}[\mathbb{Z}^n]/\langle f_1,\ldots,f_n\rangle$. □

Using the multiplication maps in $\mathbb{K}[\mathbb{Z}^n]/\langle f_1,\ldots,f_n\rangle$ and the FGLM algorithm [14], we can compute a Gröbner basis for $\langle f_1,\ldots,f_n\rangle : \langle \prod_i x_i\rangle^\infty$ over $\mathbb{K}[\boldsymbol{x}]$. The latter is the saturation over $\mathbb{K}[\mathbb{N}^n]$ of the ideal $\langle f_1,\ldots,f_n\rangle$ by the product of all the variables.

Lemma 4.11. *Consider polynomials $f_1,\ldots,f_m \subset \mathbb{K}[\mathbb{N}^n]$ such their ideal over $\mathbb{K}[\mathbb{Z}^n]$, $\langle f_1,\ldots,f_m\rangle_{\mathbb{K}[\mathbb{Z}^n]}$, is 0-dimensional. Let $\langle f_1,\ldots,f_m\rangle_{\mathbb{K}[\mathbb{N}^n]}$ be the ideal generated by $f_1,\ldots,f_m$ over $\mathbb{K}[\mathbb{N}^n]$. Then, the sets $\langle f_1,\ldots,f_m\rangle_{\mathbb{K}[\mathbb{Z}^n]} \cap \mathbb{K}[\mathbb{N}^n]$ and $\langle f_1,\ldots,f_m\rangle_{\mathbb{K}[\mathbb{N}^n]} : \langle \prod_i x_i\rangle^\infty$ are the same. The latter is an ideal over $\mathbb{K}[\mathbb{N}^n]$.*

Proof. Consider $f \in \langle f_1,\ldots,f_m\rangle_{\mathbb{K}[\mathbb{Z}^n]}$. Then there are $g_i \in \mathbb{K}[\mathbb{Z}^n]$ such that $f = \sum_i g_i f_i$. We can clear the denominators introduced by the g_i's by multiplying both sides by a monomial $(\prod_j x_j)^d$, where d is big enough. Then, $(\prod_j x_j)^d f = \sum_i ((\prod_j x_j)^d g_i) f_i$ and $((\prod_j x_j)^d g_i) \in \mathbb{K}[\mathbb{N}^n]$. Thus, $(\prod_j x_j)^d f \in \langle f_1,\ldots,f_m\rangle_{\mathbb{K}[\mathbb{N}^n]}$ and $f \in \langle f_1,\ldots,f_m\rangle_{\mathbb{K}[\mathbb{N}^n]} : \langle \prod_j x_j\rangle^\infty$. The opposite direction is straightforward as $\prod_i x_i$ is a unit in $\mathbb{K}[\mathbb{Z}^n]$. □

Complexity. We estimate the arithmetic complexity of the algorithm in Sec 4; it is polynomial with respect to the Minkowski sum of the polytopes. We omit the cost of computing all the monomials in $\mathbb{K}[S^h_\Delta]_{\boldsymbol{d}}$ and we only consider the complexity to read them. Our purpose is to highlight the dependency on the Newton polytopes. A more detailed analysis might give sharper bounds.

Definition 4.12. For polytopes $\Delta_0,\ldots,\Delta_n$ and for each multidegree $\boldsymbol{d} \in \mathbb{N}^{n+1}$ of $\mathbb{K}[S^h_\Delta]$, let $P(\boldsymbol{d})$ be the number of integer points in the Minkowski sum of the polytopes given by $\boldsymbol{d}$,

$$P(\boldsymbol{d}) = \#\Big(\big(\textstyle\sum_{j=0}^n d_j \Delta_j\big) \cap \mathbb{Z}^n\Big).$$

Note that $P(\boldsymbol{d})$ equals the number of different monomials in $\mathbb{K}[S^h_\Delta]_{\boldsymbol{d}}$.

Lemma 4.13. *Let $F_1,\ldots,F_k \in \mathbb{K}[S^h_\Delta]$ be a (sparse) regular sequence and let $\boldsymbol{d}_i \in \mathbb{N}^{n+1}$ be the multidegree of F_i, for $i \in [k]$. Consider a multigraded monomial order $<$. For every multidegree $\boldsymbol{d} \in \mathbb{N}^{n+1}$ such that $\boldsymbol{d} \geq \sum_i \boldsymbol{d}_i$, the arithmetic complexity of computing* `ReduceMacaulay` *$((F_1,\ldots,F_k),\boldsymbol{d},<)$ is $O(2^{k+1}\,P(\boldsymbol{d})^\omega)$, where ω is the constant of matrix multiplication.*

Proof. By Cor. 3.12, as $F_1,\ldots,F_k \in \mathbb{K}[S^h_\Delta]$ is a (sparse) regular sequence and $\boldsymbol{d} \geq \sum_i \boldsymbol{d}_i$, all the matrices that appear during the computations of `ReduceMacaulay` $((F_1,\ldots,F_k),\boldsymbol{d},<)$ are full-rank and their rows are linearly independent. Hence, their number of rows is at most their number of columns. The number of columns of a Macaulay matrix of multidegree $\boldsymbol{d}$ is $P(\boldsymbol{d})$. Thus, in this case, the complexity of Gaussian elimination is $O(P(\boldsymbol{d})^\omega)$. If $C(k,\boldsymbol{d})$ is the cost of `ReduceMacaulay` $((F_1,\ldots,F_k),\boldsymbol{d},<)$, then we have the following recursive relation

$$C(k,\boldsymbol{d}) = \begin{cases} O(P(\boldsymbol{d})^\omega) & \text{if } k=1,\\ C(k-1,\boldsymbol{d}) + C(k-1,\boldsymbol{d}-\boldsymbol{d}_k) + O(P(\boldsymbol{d})^\omega) & \text{if } k>1.\end{cases}$$

The cost $C(k-1,\boldsymbol{d})$ is greater than $C(k-1,\boldsymbol{d}-\boldsymbol{d}_k)$, as it involves bigger matrices. Hence, we obtain $C(k,\boldsymbol{d}) = O(2^{k+1}P(\boldsymbol{d})^\omega)$. □

Theorem 4.14. *Consider an affine polynomial system $(f_1,\ldots,f_n)$ in $\mathbb{K}[\boldsymbol{x}]$ such that Assum. 4.1 holds and the system $(F_1,\ldots,F_n)$ is (sparse) regular, where $F_i \in \mathbb{K}[S^h_\Delta]_{\boldsymbol{e}_i}$ and $\chi(F_i) = f_i$, for $i \in [n]$. Then, the complexity of computing $\langle f_1,\ldots,f_n\rangle : \langle \prod_i x_i\rangle^\infty$ is*

$$O(2^{n+1}\,P(\boldsymbol{1})^\omega + n\,\mathrm{MV}(\Delta_1,\ldots,\Delta_n)^3).$$

Proof. We need to compute:

- The set `Rows`(`ReduceMacaulay` $((F_1,\ldots,F_n),\sum_{i>1}\boldsymbol{e}_i,<)$) to generate $\mathcal{L}$ (Rem. 4.7). By Lem. 4.13, this costs $O(2^{n+1}\,P(\sum_{i>1}\boldsymbol{e}_i)^\omega)$.
- The set `Rows`(`ReduceMacaulay` $((F_1,\ldots,F_n),\boldsymbol{1},<)$) to generate the matrix $\mathcal{M}(F_0)$ of Lem. 4.8, for any $F_0 \in \mathbb{K}[S^h_\Delta]_{\boldsymbol{e}_0}$. By Lem. 4.13, it costs $O(2^{n+1}\,P(\boldsymbol{1})^\omega)$.
- For each variable x_i, the Schur complement of $\mathcal{M}(F_0)$, for $\chi(F_0) = x_i$. The cost of each Schur complement computation is $O(P(\boldsymbol{1})^\omega)$, and so the cost of this step is $O(n\,P(\boldsymbol{1})^\omega)$.
- The complexity of FGLM depends on the number of solutions, and in this case it is $O(n\,\mathrm{MV}(\Delta_1,\ldots,\Delta_n)^3)$ [14]. □

Note that $\mathrm{MV}(\Delta_1,\ldots,\Delta_n) < P(\boldsymbol{1})$. Hence, to improve the previous bound for lexicographical orders, we can follow [16].

ACKNOWLEDGMENTS

We thank C. D'Andrea, C. Massri, B. Mourrain, P.-J. Spaenlehauer, and B. Teissier for the helpful discussions and references. Partially supported by ANR JCJC GALOP (ANR-17-CE40-0009), the PGMO grant ALMA and the PHC GRAPE. MatÃŋas R. Bender is partially supported by the European Research Council (ERC) under the EuropeanâĂŹs Horizon 2020 researchand innovation programme (grant agreement No 787840).

REFERENCES

[1] M. Bardet, J.-C. Faugère, and B. Salvy. 2015. On the complexity of the F5 GrÃűbner basis algorithm. J. Symbolic Comput. 70 (Sept. 2015), 49–70.
[2] M. R. Bender, J.-C. Faugère, and E. Tsigaridas. 2018. Towards Mixed Gröbner Basis Algorithms: The Multihomogeneous and Sparse Case. In Proc. ACM ISSAC. ACM, 71–78.

[3] N. Botbol and M. Chardin. 2017. Castelnuovo Mumford regularity with respect to multigraded ideals. Journal of Algebra 474 (March 2017), 361–392.

[4] J. Canny and I. Emiris. 1993. An efficient algorithm for the sparse mixed resultant. In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (LNCS), G. Cohen, T. Mora, and O. Moreno (Eds.). Springer, 89–104.

[5] M. Chardin. 2003. Bounds for Castelnuovo-Mumford Regularity in Terms of Degrees of Defining Equations. In Commutative Algebra, Singularities and Computer Algebra, J. Herzog and V. Vuletescu (Eds.). Springer, 67–73.

[6] D. Cifuentes and P. Parrilo. 2016. Exploiting Chordal Structure in Polynomial Ideals: A Gröbner Bases Approach. SIAM J. Discr. Math. 30, 3 (2016), 1534–1570.

[7] D. A. Cox, J. Little, and D. O'Shea. 2005. Using Algebraic Geometry (2 ed.). Springer-Verlag.

[8] D. A. Cox, J. B. Little, and H. K. Schenck. 2011. Toric Varieties. AMS.

[9] C. Eder and J.-C. Faugère. 2017. A survey on signature-based algorithms for computing Gröbner bases. J. Symbolic Comput. 80 (2017), 719 – 784.

[10] D. Eisenbud. 2004. Commutative Algebra: with a View Toward Algebraic Geometry. Springer-Verlag.

[11] I. Z. Emiris. 1996. On the Complexity of Sparse Elimination. Journal of Complexity 12, 2 (June 1996), 134–166.

[12] I. Z. Emiris and B. Mourrain. 1999. Computer Algebra Methods for Studying and Computing Molecular Conformations. Algorithmica 25, 2 (June 1999), 372–402.

[13] J. C. Faugère. 2002. A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F5). In Proc. ACM ISSAC (ISSAC '02). ACM, 75–83.

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

[15] J.-C. Faugère, P.-J. Spaenlehauer, and J. Svartz. 2014. Sparse Gröbner bases: the unmixed case. In Proc. ACM ISSAC. ACM, 178–185.

[16] J.-C. FaugÃĺre, P. Gaudry, L. Huot, and G. Renault. 2013. Polynomial Systems Solving by Fast Linear Algebra. arXiv:1304.6039 [cs] (April 2013). arXiv: 1304.6039.

[17] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. 1994. Discriminants, Resultants, and Multidimensional Determinants. BirkhÃďuser.

[18] R. Gilmer. 1984. Commutative Semigroup Rings. University of Chicago Press.

[19] J. Heintz and J. Morgenstern. 1993. On the Intrinsic Complexity of Elimination Theory. Journal of Complexity 9, 4 (Dec. 1993), 471–498.

[20] M. I. Herrero, G. Jeronimo, and J. Sabia. 2013. Affine solution sets of sparse polynomial systems. J. Symbolic Comput. 51 (2013), 34–54.

[21] B. Huber and B. Sturmfels. 1995. A polyhedral method for solving sparse polynomial systems. Math. Comp. 64, 212 (1995), 1541–1555.

[22] D. Lazard. 1983. GrÃűbner-Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations. In Proc. of the European Computer Algebra Conference (EUROCAL '83). Springer-Verlag, 146–156.

[23] D. Maclagan and G. G. Smith. 2004. Multigraded Castelnuovo-Mumford Regularity. J. Reine Angew. Math. (Crelles Journal) 2004, 571 (Jan. 2004).

[24] C. Massri. 2016. Solving a sparse system using linear algebra. J. Symbolic Comput. 73 (March 2016), 157–174.

[25] E. W. Mayr. 1997. Some Complexity Results for Polynomial Ideals. Journal of Complexity 13, 3 (Sept. 1997), 303–325.

[26] E. Miller and B. Sturmfels. 2005. Combinatorial Commutative Algebra. Springer.

[27] C. Mou and Y. Bai. 2018. On the Chordality of Polynomial Sets in Triangular Decomposition in Top-Down Style. In Proc. ACM ISSAC. ACM, 287–294.

[28] J. M. Rojas. 1999. Solving degenerate sparse polynomial systems faster. J. Symbolic Comput. 28, 1-2 (1999), 155–186.

[29] M. Sombra. 1999. A Sparse Effective Nullstellensatz. Advances in Applied Mathematics 22, 2 (Feb. 1999), 271–295.

[30] B. Sturmfels. 1993. Sparse elimination theory. In Proc. Comp. Algebraic Geom. and Commut. Algebra. CUP, 264–298.

[31] B. Sturmfels. 1994. On the Newton polytope of the resultant. Journal of Algebraic Combinatorics 3, 2 (1994), 207–236.

[32] B. Sturmfels. 1996. GrÃűbner Bases and Convex Polytopes. AMS.

[33] B. Sturmfels. 2002. Solving systems of polynomial equations. Number 97. AMS.

[34] A. Szanto. 2008. Solving over-determined systems by the subresultant method (with an appendix by Marc Chardin). J. Symbolic Comput. 43, 1 (2008), 46–74.

[35] S. Telen, B. Mourrain, and M. Van Barel. 2018. Solving Polynomial Systems via a Stabilized Representation of Quotient Algebras. SIAM J. Matrix Anal. Appl. 39, 3 (Oct. 2018), 1421–1447.

[36] J. Verschelde, P. Verlinden, and R. Cools. 1994. Homotopies Exploiting Newton Polytopes for Solving Sparse Polynomial Systems. SIAM J. Numer. Anal. 31, 3 (June 1994), 915–930.

[37] J. Weyman and A. Zelevinsky. 1994. Multigraded formulae for multigraded resultants. J. Algebr. Geom 3, 4 (1994), 569–597.

A COUNTER-EXAMPLE TO THE COMPLEXITY BOUNDS IN [15]

Let Δ be the standard 2-simplex and consider the regular system given by two polynomials $F_1, F_2 \in \mathbb{K}[S_\Delta^h]_2$ of degree 2,

$$F_1 := X^{((2,0),2)} + X^{((1,1),2)} + X^{((0,2),2)} + X^{((1,0),2)} + X^{((0,1),2)} + X^{((0,0),2)}$$

$$F_2 := X^{((2,0),2)} + 2\,X^{((1,1),2)} + 3\,X^{((0,2),2)} + 4\,X^{((1,0),2)} + 5\,X^{((0,1),2)} + 6\,X^{((0,0),2)}$$

Consider the graded monomial order $<$ given by

$$X^{((x_1,y_1),d_1)} < X^{((x_2,y_2),d_2)} \iff \begin{cases} d_1 < d_2, \text{ or} \\ d_1 = d_2 \text{ and } x_1 < x_2, \text{ or} \\ d_1 = d_2 \text{ and } x_1 = x_2 \text{ and } y_1 < y_2 \end{cases}.$$

In this case, the bound in [15, Lem. 5.2] is 3, meanwhile the maximal degree of an element in the Gröbner basis of (F_1, F_2) with respect to $<$ has degree 4.

B ALGORITHM TO COMPUTE GRÖBNER BASIS OVER THE STANDARD ALGEBRA

Algorithm 3 `compute-0-Dim-GB`

Input: Affine system $f_1, \ldots, f_n \in \mathbb{K}[\boldsymbol{x}]$ and a monomial order $<$ for $\mathbb{K}[\boldsymbol{x}]$, such that it has a finite number of solutions over $(\mathbb{C}^*)^n$ and satisfies Assum. 4.1.

Output: Gröbner basis G for the ideal $\langle f_1, \ldots, f_n \rangle : \langle \prod_i x_i \rangle^\infty$ with respect to the monomial order $<$.

Consider the semigroup algebra $\mathbb{K}[S_\Delta^h]$ related to the polytopes of $f_1, \ldots, f_n$ and the standard n-simplex.
Choose a multigraded monomial order $\prec$ for $\mathbb{K}[S_\Delta^h]$.
For each $i \in [n]$, choose $F_i \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{e}_i}$ such that $\chi(F_i) = f_i$.
$C \leftarrow \mathtt{Rows}(\mathtt{ReduceMacaulay}((F_1, \ldots, F_n), \sum_{i>0} \boldsymbol{e}_i, \prec))$,
$P \leftarrow \mathtt{Rows}(\mathtt{ReduceMacaulay}((F_1, \ldots, F_n), \mathbf{1}, \prec))$,
$\mathcal{L} \leftarrow \left\{ X^{(\boldsymbol{\alpha}, \sum_{i\geq 1} \boldsymbol{e}_i)} \in \mathbb{K}[S_\Delta^h]_{\sum_{i\geq 1} \boldsymbol{e}_i} : X^{(\boldsymbol{\alpha}, \sum_{i\geq 1} \boldsymbol{e}_i)} \notin C \right\}$
for all $x_i \in \mathbb{K}[\boldsymbol{x}]$ **do**
  Choose a monomial $m \in \mathbb{K}[S_\Delta^h]_{\boldsymbol{e}_0}$ such that $\chi(m) = x_i$.
  $\mathcal{M}(m) \leftarrow$ Macaulay matrix of degree $\mathbf{1}$ with respect to $\prec$.
  for all $F \in P$ **do**
    Add F to $\mathcal{M}(m)$
  for all $L_i \in \mathcal{L}$ **do**
    Add $L_i\, m$ to $\mathcal{M}(m)$
  Rearrange $\mathcal{M}(m)$ as $\begin{bmatrix} M_{1,1}(m) & M_{1,2}(m) \\ M_{2,1}(m) & M_{2,2}(m) \end{bmatrix}$ like (5).
  $M_{x_i} \leftarrow (M_{2,2} - M_{2,1}\, M_{1,1}^{-1}\, M_{1,2})(m)$.
Perform FGLM with the multiplication matrices $M_{x_1}, \ldots, M_{x_n}$ with respect to $>$ to obtain Gröbner basis G.
return G.