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

Matías R. Bender  Jean-Charles Faugère  Elias Tsigaridas  
Sorbonne Université, CNRS, INRIA, Laboratoire d’Informatique de Paris 6, LIP6, Équipe Polysys  
F-75005, Paris, France  
FirstName.LastName@inria.fr

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. For example, several problems in computer-aided design, robotics, vision, biology, kinematics, cryptography, and optimization involve 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.

1 INTRODUCTION
The introduction of the first algorithm to compute Gröbner bases in 1965 [4] established them as a central tool in nonlinear algebra. Their applications span most of the spectrum of mathematics and engineering [5]. 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 [33]. There are many practically efficient algorithms, see [11, 16] 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. [14, 19, 42], 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, 8, 18, 20, 39]. We follow [20, 39] 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.

We embed the system in semigroup algebras because in this place they “behave” in a predictable way that we can exploit algorithmically. Semigroup algebras are related to toric varieties. An affine toric variety is the spectrum of a semigroup algebra [10, Thm. 1.1.17]. Hence, the variety defined by the polynomials over the semigroup is a subvariety of a toric variety. This variety 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., [14]. We refer to [10] for an introduction to toric varieties and to [41] for their relation with Gröbner basis.

In ISSAC’14, Faugère et al. [20] 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, 16]. They compute Gröbner basis by performing Gaussian elimination on various Macaulay matrices [30] and they avoid computations with rows reducing to zero using the F5 criterion [16]. 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 during Gaussian elimination. Moreover, the degree bound for the maximal degree in [20, Lem. 5.2] misses some assumptions to hold, see App. A. We relax the regularity assumptions of [20] 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. We emphasize that besides the similarity in the titles, this work and [2] are completely different approaches. First, we compute different objects. Sparse Gröbner bases [2, Sec. 3] are not Gröbner basis for semigroup algebras. Moreover, we follow different computational strategies: in [2] we perform the computations polynomial by polynomial, while in this work we proceed degree by degree. Further, when we use [2] to solve 0-dimensional systems, there are no complexity bounds, let alone bounds depending on the Newton polytopes, for this approach.

A direct application of Gröbner basis theory is to solve polynomial systems. This is also an intrinsically hard problem [26].
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., [28, 44], chordal elimination [8], triangular decomposition [36], and various other techniques [21, 25, 27, 35, 37, 43].

Among the symbolic approaches related to toric geometry, the main tool to solve sparse systems is the sparse resultant [23]. 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 [9, Chp. 7.6]. Canny and Emiris [6] and Sturmfels [40] 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., [13, 15], 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 \((C \setminus \{0\})^n\). Recently, Massri [32] 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 \((C \setminus \{0\})^n\). Our strategy is to reuse part of our algorithm to compute Gröbner bases over semigroup algebras to compute multiplication maps and, via FGLM [17], recover a Gröbner basis over the standard polynomial algebra. As we compute the solutions over \((C \setminus \{0\})^n\), 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 one in Emiris’ resultant approach [13]. Our approach to solve is more general than the one in [20] 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 \(f_1, \ldots, f_n \in \mathbb{K}[x]\) be a sparse regular polynomial system with a finite number of solutions over \((C^*)^n\).
2. Embed the polynomials to a multigraded semigroup algebra \(\mathbb{K}[S_A]\) related to the Newton polytopes of \(f_1, \ldots, f_n\) 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 \((f_1, \ldots, f_n, x_i)\) of size equal to the number of integer points in the Minkowski sum of the Newton polytopes of \(f_1, \ldots, f_n\) and the n-simplex.
   - Split the matrix in four parts and compute a Schur complement, which is the multiplication map of \(x_i\) in \(\mathbb{K}[x^{\mathbb{N}}]/(f_1, \ldots, f_n)\).
4. Use the multiplication maps and FGLM to get a Gröbner basis for \((f_1, \ldots, f_n) : (\Pi_i x_i)^m\) with respect to any monomial order.

The contributions and consequences of our work include:

- We introduce the first effective algorithm to compute Gröbner bases over semigroup algebras associated to mixed polynomial systems. We generalize the work of [20] to the mixed case from which we could provide accurate 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 [46], way to compute the resultant is to use a Sylvester-type formula and compute it as the determinant of a Macaulay matrix [9, Chp. 3.4]. Using this matrix we extract multiplication maps and solve polynomial systems [9, 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 [30]. 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 Koszul complexes instead of regular sequences. The exactness of the Koszul complex is closely related to regular sequences [12, 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. Hence, even if the system is not a regular sequence, by focusing on the degrees at which the strads of the Koszul complex are exact, we can still predict the algebraic structure of the system and perform efficient computations. Using this property we extend the classical F5-like criteria that apply only to regular sequences. Moreover, additional information on the exactness of the strads of the Koszul complex and the multigraded Castelnuovo-Mumford regularity [3, 31] results in better degree and complexity bounds; similarly to the case of the multihomogeneous systems [2, Sec. 4].
- We disrupt the classical strategy to solve 0-dimensional systems using Gröbner basis, by avoiding intermediate Gröbner basis computations. 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 some sense optimal because it is related to the Castelnuovo-Mumford regularity of the homogenized ideal [7, 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 \(K \subset \mathbb{C}\) be a field of characteristic 0, \(x := (x_1, \ldots, x_n)\), and \(\mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]\). We consider \(0 := (0, \ldots, 0)\) and \(1 := (1, \ldots, 1)\). For each \(r \in \mathbb{N}\), let \(e_1, \ldots, e_r\) be the canonical basis of \(\mathbb{R}^r\). Given
\(d_1, d_2 \in \mathbb{N}^n\), we say \(d_1 \preceq d_2\) when \(d_1 - d_2 \in \mathbb{N}^n\). We use \([r] = \{1, \ldots, r\}\). We denote by \((f_1, \ldots, f_m)\) the ideal generated by \(f_1, \ldots, f_m\).

### 2.1 Semigroup algebras

**Definition 2.1 (Affine semigroup and semigroup algebra).** Following [34], an affine semigroup \(S\) is a finitely-generated additive sub-semigroup of \(\mathbb{Z}^n\), for some \(n \in \mathbb{N}\), such that it contains \(0 \in \mathbb{Z}^n\). An affine semigroup \(S\) is pointed if it does not contain non-zero invertible elements, that is, for all \(\alpha, \beta \in S \setminus \{0\}\), \(\alpha + \beta \neq 0\) [34, Def 7.8]. The semigroup algebra \(\mathbb{K}[S]\) is the \(\mathbb{K}\)-algebra generated by the monomials \(\{X^\alpha : \alpha \in S\}\) such that \(X^{\alpha} \cdot X^{\beta} = X^{\alpha+\beta}\).

**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 \(\Delta\) also lies in \(\Delta\); that is, for every \(\alpha, \beta \in \Delta\) and \(0 \leq \lambda \leq 1\) it holds \(\lambda \alpha + (1 - \lambda) \beta \in \Delta\). The convex hull of \(\Delta\) is the unique minimal, with respect to inclusion, convex set that contains \(\Delta\).

**Definition 2.3 (Pointed rational polyhedral cones).** A cone \(C\) is a convex subset of \(\mathbb{R}^n\) such that \(0 \in C\) and for every \(\alpha \in C\) and \(\lambda > 0\), \(\lambda \alpha \in C\). The dimension of a cone \(C\) is the dimension of the vector space spanned by the cone. A cone is pointed if does not contain any line; that is, if \(0 \neq \alpha \in C\), then \(-\alpha \notin C\). 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 \(C_\Delta\) be the cone generated by the elements of \(\Delta\). If \(\Delta\) is (the convex hull of) a finite set of integer points, then \(C_\Delta\) 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 \(\Delta_1\) and \(\Delta_2\) is \(\Delta_1 + \Delta_2 = \{\alpha + \beta : \alpha \in \Delta_1, \beta \in \Delta_2\}\). For each polytope \(\Delta\) and \(k \in \mathbb{N}\), we denote by \(k \cdot \Delta\) the Minkowski sum of \(k\) copies of \(\Delta\).

**Definition 2.5 (Laurent polynomials and Newton polytopes).** A Laurent polynomial is a finite \(\mathbb{K}\)-linear combination of monomials \(X^\alpha\), where \(\alpha \in \mathbb{Z}^n\). 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 \(f = \sum_{\alpha \in \mathbb{Z}^n} c_{\alpha} X^\alpha\), its Newton polytope is the integer polytope generated by the set of the exponents \(\alpha\) of the non-zero coefficients of \(f\); that is, \(\text{NP}(f) := \text{Convex Hull}\{\alpha \in \mathbb{Z}^n : c_{\alpha} \neq 0\}\).

Instead of working over \(\mathbb{K}[\mathbb{Z}^n]\), we embed \(f\) in a subalgebra related to its Newton polytope, given by \(\mathbb{K}[C_{\text{NP}(f)} \cap \mathbb{Z}^n]\). 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 \(0\) is its vertex; in particular, \(0\) as a vertex of every Newton polytope \(\Delta_i\). We also consider the polytope \(\Delta := \sum (\Delta_i \times (e_i))\), 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 \(\mathbb{K}[S^\bullet] := \mathbb{K}[C_\Delta \cap \mathbb{Z}^{n+r}]\). We will write the monomials in \(\mathbb{K}[S^\bullet_\Delta]\) as \(X^{\alpha,d}\), where \(\alpha \in (C_\Delta \cap \mathbb{Z}^n)\) and \(d \in \mathbb{N}^r\).
As $S$ is finitely generated, the algebra $\mathbb{K}[S]$ is a Noetherian ring [24, Thm. 7.7]. Hence, for any monomial order and any ideal, there is always a finite Gröbner basis.

We will consider monomial orders for $\mathbb{K}[S^n]$ that we can relate to monomial orders in $\mathbb{K}[S]$ and $\mathbb{K}[\mathbb{N}^n]$.

**Definition 2.14 (Multigraded monomial order)**. We say that a monomial order $< \in \mathbb{K}[S^n]$ is multigraded, if there are monomial orders $<_A$ for $\mathbb{K}[S]_A$ and $<_\mathbb{N}$ for $\mathbb{K}[\mathbb{N}]$ such that, for every $X^{(\alpha_1, d_1)}, X^{(\alpha_2, d_2)} \in \mathbb{K}[S^n]$, it holds

$$X^{(\alpha_1, d_1)} < X^{(\alpha_2, d_2)} \iff \begin{cases} \alpha_1 <_A \alpha_2 \\ d_1 = d_2 \text{ and } \alpha_1 < \mathbb{N} <_A \alpha_2. \end{cases}$$

(1)

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

**Remark 2.15**. In what follows, given a multigraded monomial order $< \in \mathbb{K}[S^n]$, we also use the same symbol, that is, $<$, for the associated monomial order of $\mathbb{K}[S]_A$.

**Lemma 2.16**. Consider a polynomial $f \in \mathbb{K}[S]$. Let $< \in \mathbb{K}$ be a multigraded monomial order. Then for any multigraded and any homogeneous $F \in \mathbb{K}[S]_A$ such that $\chi(F) = \chi(A)$, it holds $\text{LM}_<(F) = \chi_<(\text{LM}_<(F))$.

**2.3 Regularity and solutions at infinity**

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

**Definition 2.17 (Mixed volume)**. Let $\Delta_1, \ldots, \Delta_n \in \mathbb{R}^n$ be integer polytopes. Their mixed volume, $\text{MV}(\Delta_1, \ldots, \Delta_n)$, is the alternating sum of the number of integer points of the polytopes obtained by all possible Minkowski sums, that is

$$\text{MV}(\Delta_1, \ldots, \Delta_n) = (-1)^{n} + \sum_{k=1}^{n} (-1)^{n-k} \left( \sum_{i \in \{1, \ldots, n\}} \#((\Delta_1 \cup \cdots \cup \Delta_k) \cap \mathbb{Z}^n) \right).$$

(2)

**Theorem 2.18 (BKK bound)** [9, Thm. 7.5.4]. Let $f_1, \ldots, f_k$ be a system of polynomials with Newton polytopes $\Delta_1, \ldots, \Delta_n$ having a finite number of solutions over $(\mathbb{C}^*)^n$. The mixed volume $\text{MV}(\Delta_1, \ldots, \Delta_n)$ 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 $X$ [10, Def. 3.1.1]. Semigroup algebras correspond to the coordinate rings of the affine pieces of $X$.

Given an integer polytope $\Delta$, we can define a projective complete normal irreducible toric variety $X$ associated to it [10, Sec. 2.3]. Likewise, given a polynomial system $(f_1, \ldots, f_m)$, we can define a projective toric variety $X$ associated to the Newton polytopes of their Newton polytopes. We can homogenize these polytopes in a way that they belong to the total coordinate ring of $X$ [10, 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 $\Delta_1$ is a $\mathbb{N}$-Minkowski summand of $\Delta$ if there is a $k \in \mathbb{N}$ and another polytope $\Delta_2$ such that $\Delta_1 + \Delta_2 = k \cdot \Delta$ [10, Def. 6.2.11]. Every $\mathbb{N}$-Minkowski summand $\Delta_1$ of $\Delta$ defines a torus-invariant basepoint free Cartier divisor $D$ of the projective toric variety $X$ associated to $\Delta$ [10, Cor. 6.2.15]. This divisor defines an invertible sheaf $O_X(D)$ whose global sections form the vector space of polynomials in $\mathbb{K}[\mathbb{Z}^n]$ whose Newton polytopes are contained in $\Delta_1$ [32, Lem. 1]. Therefore, to homogenize $f_1, \ldots, f_m$ over $X$ we need to choose polytopes $\Delta_1, \ldots, \Delta_m$ such that all of them are $\mathbb{N}$-Minkowski summands of $\Delta$ associated to and $\text{NP}(f_i) \subset \Delta_i$. Hence, for any homogeneous $F \in \mathbb{K}[S^n]$, we can homogenize $\chi(F)$ with respect to the $\mathbb{N}$-Minkowski summand $\sum_i d_i \Delta_i$ of $\Delta$.

We alert the reader that homogeneity in $\mathbb{K}[S^n]$ is different from homogeneity in the total coordinate ring of $X$, see [10, Sec. 5.4] but they are related through the degree $d$.

**Definition 2.19 (Solutions at infinity)**. Let $(f_1, \ldots, f_m)$ be a system of polynomials. Let $X$ be the projective toric variety associated to a polytope $\Delta$ such that the Newton polytope of $f_i$ is a $\mathbb{N}$-Minkowski summand of $\Delta$, 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 2.20** ([32, Thm. 3]). Consider a system $(f_1, \ldots, f_n)$ 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 $(\mathbb{C}^*)^n$.

**Definition 2.21 (Koszul complex)**. For a sequence of homogeneous polynomials $F_1, \ldots, F_k \in \mathbb{K}[S^n]$ of multidegrees $d_1, \ldots, d_k$ and a multidegree $d \in \mathbb{N}^n$, we denote by $\mathcal{K}(F_1, \ldots, F_k)_d$ the strand of the Koszul complex of $F_1, \ldots, F_k$ of multidegree $d$, that is,

$$\mathcal{K}(F_1, \ldots, F_k)_d : \text{0} \rightarrow (\mathcal{K}_d) \rightarrow \delta \rightarrow \cdots \rightarrow (\mathcal{K}_{d-k}) \rightarrow \text{0},$$

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

$$(\mathcal{K}_d)_t := \bigoplus_{I \subset \{1, \ldots, k\}} (\mathbb{K}[S^n]_d) \otimes (e_{i_1} \wedge \cdots \wedge e_{i_t}).$$

The maps (differentials) act as follows:

$$\delta_1 \left( \sum_{I \subset \{1, \ldots, k\}} g_I \otimes (e_{i_1} \wedge \cdots \wedge e_{i_t}) \right) = \sum_{I \subset \{1, \ldots, k\}} \left( \sum_{i=1}^{t} (-1)^{t-1} F_i g_I \wedge (e_{i_1} \wedge \cdots \wedge \hat{e}_{i_i} \wedge \cdots \wedge e_{i_t}) \right).$$

(3)

The expression $(e_{i_1} \wedge \cdots \wedge \hat{e}_{i_i} \wedge \cdots \wedge e_{i_t})$ denotes that we skip the term $e_{i_i}$ from the wedge product. We denote by $\mathcal{H}(F_1, \ldots, F_k)_d$ the $t$-th Koszul homology of $\mathcal{K}(F_1, \ldots, F_k)_d$, that is

$$\mathcal{H}(F_1, \ldots, F_k)_d := (\ker(\delta_t) / \text{im}(\delta_{t+1}))_d.$$ 

The 0-th Koszul homology is $\mathcal{H}_0(F_1, \ldots, F_k) \equiv (\mathbb{K}[S^n]_d / (F_1, \ldots, F_k))$. By $\mathcal{H}_t(F_1, \ldots, F_k)_d \equiv \mathbb{K}[S^n]_d / (F_1, \ldots, F_k)$.

**Definition 2.22 (Koszul and sparse regularity)**. A sequence $F_1, \ldots, F_k \in \mathbb{K}[S^n]$ is Koszul regular if for every $d \in \mathbb{N}^n$ coordinate-wise greater than or equal to $D_k := \sum_{i=1}^{k} d_i$, that is, $d \geq D_k$, and for every $t > 0$, the $t$-th Koszul homology vanishes at degree $d$, Matías R. Bender, Jean-Charles Faugère, and Elias Tsigaridas
that is $\mathcal{H}_d(F_1, \ldots, F_k)_d = 0$. We say that the sequence is (sparse) regular if $F_1, \ldots, F_k$ is Koszul regular, for every $j \leq k$.

Observation 2.23. Note that Koszul regularity does not depend on the order of the polynomials, as (sparse) regularity does.

Kushnirenko’s proof of the BKK bound [29, Thm. 2] follows from Koszul regularity.

3 THE ALGORITHM

To compute Gröbner basis over $\mathbb{K}[S_A]$ we work over $\mathbb{K}[S_A^h]$. We follow the classical approach of Lazard [30] adapted to the semigroup case, see also [20]; we “linearize” the problem by reducing the Gröbner basis computation to a linear algebra problem.

Lemma 3.1. Consider $F_1, \ldots, F_m \in \mathbb{K}[S_A^h]$ and a multigraded monomial order $<$. For $\mathbb{K}[S_A]^d$, there is a multidegree $d$ and homogeneous $\{G_1, \ldots, G_i \} \subset \{F_1, \ldots, F_m \} \cap \mathbb{K}[S_A^d]$ such that $\{\chi(G_1), \ldots, \chi(G_i)\}$ is a Gröbner basis of the ideal $\langle \chi(F_1), \ldots, \chi(F_m) \rangle$ with respect to the associated monomial order $<$ (Rem. 2.15).

Proof. Let $g_1, \ldots, g_i \in \mathbb{K}[S_A]$ 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 $G_1, \ldots, G_i \in \{F_1, \ldots, F_m \}$ such that $\chi(G_i) = g_i$ for $i \in [t]$. Consider $d = \in \mathbb{N}^r$ such that $d \geq \deg(G_i)$ for $i \in [t]$. It suffices to consider $G_i = X(d_{i_{j_{1}}}^{\alpha_{i_{j_{1}}}} \cdots d_{i_{k}}^{\alpha_{i_{k}}})$ where $G_i \in \mathbb{K}[S_A^d]_d$ for $i \in [t]$.

When we know a multidegree $d$ that satisfies Lem. 3.1, we can compute the Gröbner basis over $\mathbb{K}[S_A]$ using linear algebra. For this task we need to introduce the Macaulay matrix.

Definition 3.2 (Macaulay matrix). A Macaulay matrix $M$ of degree $d \in \mathbb{N}^r$ with respect to a monomial order $<$ is a matrix whose columns are indexed by all monomials $X(d_{1_{1}}^{\alpha_{1_{1}}} \cdots d_{1_{k}}^{\alpha_{1_{k}}}, \ldots, d_{i_{1}}^{\alpha_{i_{1}}} \cdots d_{i_{k}}^{\alpha_{i_{k}}})$ of a finite set of monomials $\chi(h)$ and the rows by polynomials in $\mathbb{K}[S_A^d]$. The indices of the columns are sorted in decreasing order with respect to $<$. The element of $M$ whose row corresponds to a polynomial $F$ and whose column is a monomial $X$ is the element of the monomial $X \chi(h)$ of $F$. Let $\text{Rows}(M)$ be the set of non-zero polynomials that the rows of $M$ and $\text{LM}(\text{Rows}(M))$ 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 $M$, let $\overline{M}$ be a new Macaulay matrix corresponding to the row echelon form of $M$. We can compute $\overline{M}$ by applying Gaussian elimination to $M$.

Remark 3.5. When we perform row operations (excluding multiplication by 0) to a Macaulay matrix, we do not change the order of the rows.

We use Macaulay matrices to compute a basis for the vector space $(F_1, \ldots, F_k)_d := \langle F_1, \ldots, F_k \rangle \cap \mathbb{K}[S_A^d]$ by Gaussian elimination.

Lemma 3.6. Consider homogeneous polynomials $F_1, \ldots, F_k \in \mathbb{K}[S_A^h]$ of multidegrees $d_1, \ldots, d_k$ and a multigraded monomial order $<$. Let $\mathcal{M}^d$ be a Macaulay matrix of multidegree $d$ and monomial order associated to $<$. For all $F_i$ do

1. Choose $F_i \in \mathbb{K}[S_A^d]$ of multidegree $d_i$ such that $\chi(F_i) = f_i$.
2. Pick a big enough $d \in \mathbb{N}^r$ that satisfies Lem. 3.1.
3. $\mathcal{M}^d$ be a Macaulay matrix of multidegree $d$ and monomial order associated to $<$. For all $F_i$ do
4. $\text{Rows}(\mathcal{M}^d_i)$ be the row echelon form of the Macaulay matrix $\mathcal{M}^d_i$ (Def. 3.4).
5. Let $\mathcal{M}^d_i$ be the row echelon form of the Macaulay matrix $\mathcal{M}^d_i$ (Def. 3.4).
6. for all $F_i$ do
7. for all $\chi(a, \ldots, d_i) \in \mathbb{K}[S_A^d]$ do
8. $\chi(\text{Rows}(\mathcal{M}^d_i))$
Algorithm 2 ReduceMacaulay

Input: Homogeneous $F_1, \ldots, F_k \in \mathbb{K}[S^d_1]$ of multidegree $d_1, \ldots, d_k$, a multidegree $d$, and a monomial order $<$

Output: The Macaulay matrix of $(F_1, \ldots, F_k)_d \in \mathbb{K}[S^d_1]$ with respect to $<$ in row echelon form.

1. $M^k_d \leftarrow$ Macaulay matrix with columns indexed by the monomials in $\mathbb{K}[S^d_1]$ in decreasing order w.r.t $<$
2. if $k \geq 1$ then
3. $M^{k-1}_d \leftarrow$ ReduceMacaulay$(F_1, \ldots, F_k-1, d, \ <)$
4. $M^{k-1}_d \leftarrow$ ReduceMacaulay$(F_1, \ldots, F_k-1, d-d_k, \ <)$
5. for $F \in \text{Rows}(M^{k-1}_d)$ do
6. Add the polynomial $F$ as a row to $M^k_d$
7. for $X^{(\alpha,d-d_k)} \in \mathbb{K}[S^d_1]_{d-d_k}$ do $LM_1(\text{Rows}(M^{k-1}_d))$ do
8. Add the polynomial $X^{(\alpha,d-d_k)}F_k$ as a row to $M^k_d$
9. $M^k_d \leftarrow$ GaussianElimination$(M^k_d)$
10. return $M^k_d$

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, 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 [16] in our setting to avoid redundant computations.

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

For every $X^{(\alpha,d-d_k)} \in LM_{n}(\text{Rows}(M^{k-1}_d))$, the polynomial $X^{(\alpha,d-d_k)}F_k$ is a linear combination of the polynomials $\text{Rows}(M^{k-1}_d) \cup \left\{ X^{(\beta,d-d_k)}F_k : X^{(\beta,d-d_k)} \in \mathbb{K}[S^d_1]_{d-d_k} \text{ and } X^{(\alpha,d-d_k)} < X^{(\beta,d-d_k)} \right\}$.

Proof. If $X^{(\alpha,d-d_k)} \in LM_{n}(\text{Rows}(M^{k-1}_d))$, then there is $G \in \mathbb{K}[S^d_1]_{d-d_k}$ such that $X^{(\alpha,d-d_k)} + G \in \{ F_1, \ldots, F_k-1 \}_{d-d_k}$ and $X^{(\alpha,d-d_k)} > LM_{n}(G)$. So, there are homogeneous $H_1, \ldots, H_{k-1} \in \mathbb{K}[S^d_1]$ such that $X^{(\alpha,d-d_k)} + G = \sum_{i=1}^{k-1} H_i F_i$. The proof follows by noticing that $X^{(\alpha,d-d_k)}F_k = \sum_{i=1}^{k-1} (F_iH_i F_i) - G F_k$.

In the following, $M^k_d$ is not the Macaulay matrix of 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 $M^k_d$ be a Macaulay matrix of degree $d$ w.r.t the order $<$ whose rows are

\[
\text{Rows}(M^{k-1}_d) \cup \left\{ X^{(\beta,d-d_k)}F_k : X^{(\beta,d-d_k)} \in \mathbb{K}[S^d_1]_{d-d_k} \text{ and } X^{(\alpha,d-d_k)} < X^{(\beta,d-d_k)} \in LM_{n}(\text{Rows}(M^{k-1}_d)) \right\}
\]

The row space of $M^k_d$ and the Macaulay matrix of Lem. 3.6 are equal.

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

**Lemma 3.10.** If $H_1(F_1, \ldots, F_k)_d = 0$ and there is a syzygy $\sum_i G_i F_i = 0$ such that $G_i \in \mathbb{K}[S^d_1]_{d-d_k}$, then $G_k \in \{ F_1, \ldots, F_k-1 \}_{d-d_k}$.

Proof. We consider the Koszul complex $K(F_1, \ldots, F_k)$ (Def. 2.21). As $\sum_i G_i F_i = \delta_1(G_1, \ldots, G_k)$, the vector of polynomials $(G_1, \ldots, G_k)$ belongs to the Kernel of $\delta_1$. As $H_1(F_1, \ldots, F_k)_d$ vanishes, the kernel of $\delta_1$ is generated by the image of $\delta_2$. The latter map is $(H_1, \ldots, H_{k-1, k}) \mapsto \sum_{1 \leq i < j \leq k} H_{i,j} F_i e_i - F_j e_j$.

where $e_i$ and $e_j$ are canonical basis of $\mathbb{R}^k$. Hence, there are homogeneous polynomials $(H_1, \ldots, H_{k-1, k})$ such that

$$(G_1, \ldots, G_k) = \sum_{1 \leq i < j \leq k} H_{i,j} F_i e_i - F_j e_j.$$ 

Thus, $G_k = \sum_{i=1}^{k-1} H_i F_i$ and so $G_k \in \{ F_1, \ldots, F_k-1 \}_{d-d_k}$.

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 $H_1(F_1, \ldots, F_k)_d = 0$, then all the rows of the matrix $M^k_d$ in Alg. 2 are linearly independent.

Proof. By construction, the rows of $M^k_d$ corresponding to $M^{k-1}_d$ 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 $X^{(\alpha,d-d_k)}F_k$.

The right action of the Macaulay matrix $M^k_d$ represents a map equivalent to the map $\delta_1$ from the strand of Koszul complex $K(F_1, \ldots, F_k)_d$. Hence, if some of the rows of the matrix are linearly dependent, then there is an element in the kernel of $\delta_1$. That is, there are $G_i \in \mathbb{K}[S^d_1]_{d-d_i}$ such that

- $\sum_{i=1}^{k-1} G_i F_i$ belongs to the linear span of $\text{Rows}(M^{k-1}_d)$,
- the monomials of $G_k$ do not belong to $LM_{n}(\text{Rows}(M^{k-1}_d))$, and
- $\sum_{i=1}^{k-1} G_i F_i = 0$.

By Lem. 3.10, $G_k \in \{ F_1, \ldots, F_k-1 \}_{d-d_k}$. By Lem. 3.6 and Cor. 3.9, the leading monomials of $\text{Rows}(M^{k-1}_d)$ and the ideal $(F_1, \ldots, F_k-1)$ at degree $d - d_k$ are the same. Hence, we reach a contradiction because we have assumed that the leading monomial of $G_k$ does not belong to $LM_{n}(\text{Rows}(M^{k-1}_d))$.

**Corollary 3.12.** If $F_1, \ldots, F_k$ is a sparse regular polynomial system (Def. 2.22) and $d \in \mathbb{N}^r$ is such that $d \geq (\sum_i d_i)$, then ReduceMacaulay$(F_1, \ldots, F_k, d, \ <)$ only considers matrices with linearly independent rows and avoids all redundant computations.

To benefit from the Koszul criterion and compute with smaller matrices during the Gröbner basis computation we should use the following algorithm.

Let $f_1, \ldots, f_n \in \mathbb{K}[x]$ be a square 0-dimensional system. First we embed each $f_i \in \mathbb{K}[z^n]$. We multiply each polynomial by an appropriate monomial, $X^{\delta_i} \in \mathbb{K}[z^n]$, so that $0$ is a vertex of each
new polynomial, as well as, a vertex of their Minkowski sum. Let the Newton polytopes be \( \Lambda_i = \text{NP}(X^n f_i) \), for \( 1 \leq i \leq n \), let \( \Delta_0 \) be the standard \( n \)-simplex; it is the Newton polytope of \( \text{NP}(1 + \sum_i x_i) \). We consider the algebras \( \mathbb{K}[S_\Lambda] \) and \( \mathbb{K}[S_\Lambda]^{\text{mon}} \) associated to the polytopes \( \Lambda_0, \ldots, \Lambda_n \) and the embedding \( X^0 f_1, \ldots, X^n f_n \in \mathbb{K}[S_\Lambda] \). For each \( i \), we consider \( F_i \in \mathbb{K}[S_\Lambda]^{\text{mon}} \) such that \( \chi(F_i) = X^d f_i \in \mathbb{K}[S_\Lambda] \).

**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 \( (f_1, \ldots, f_n) \) has no solutions at infinity with respect to \( X \) (Def. 2.19). Further, assume that the system \((f_0, f_1, \ldots, f_n)\), where \( f_0 \) is generic linear polynomial, has no solutions over \( (\mathbb{C}^*)^n \).

**Lemma 4.2** [32, Thm. 3.A]. Under Assum. 4.1, for every \( d \in \mathbb{N}^{n+1} \) such that \( d \geq \sum_{i \geq 0} e_i \), it holds that\( (f_0, f_1, \ldots, f_n) \in \mathbb{K}[S_\Lambda]^{\text{mon}} \) and \( f_0 \) is Koszul regular (Def. 2.22) and, for every \( d \in \mathbb{N}^{n+1} \) such that \( d \geq \sum_{i \geq 0} e_i + d_0 \), \( (f_0, f_1, \ldots, f_n) \in \mathbb{K}[S_\Lambda]^{\text{mon}} \).

**Proof.** The homogenization of system \((f_1, \ldots, f_n, \chi(f_0))\) with respect to the toric variety \( X \) has no solutions over \( X \) (see Sec. 2.3 the discussion before Def. 2.19). To see this, notice that by Assum. 4.1 the homogenization of the system \((f_1, \ldots, f_n, \chi(f_0))\) with respect to \( X \) has no solutions over \( X \setminus (\mathbb{C}^*)^n \) (see also Def. 2.19). Moreover, we also assume that there are no solutions over \( (\mathbb{C}^*)^n \) of \((f_1, \ldots, f_n, \chi(f_0))\).

Now, the proof follows from the argument in the proof of [32, Thm. 3]. This argument is the same as in [25, Prop. 3.4.1], where the stably twisted condition is given by [32, Thm. 1].

**Corollary 4.4.** For any monomial \( X^{\alpha(D_{de})} \in \mathbb{K}[S_\Lambda]^{\text{mon}} \), the system \((f_1, \ldots, f_n, X^{\alpha(D_{de})})\) is Koszul regular. For every \( d \in \mathbb{N}^{n+1} \) such that \( d \geq \sum_{i \geq 0} e_i + d_0 \), it holds that \( (f_0, f_1, \ldots, f_n, X^{\alpha(D_{de})}) \in \mathbb{K}[S_\Lambda]^{\text{mon}} \).

Fix a graded monomial order \( < \) for \( \mathbb{K}[S_\Lambda]^{\text{mon}} \). \( L \) is the set of monomials that are not leading monomials of \((f_1, \ldots, f_n, \sum_{i \geq 0} e_i)\) and \( \mathbb{K}[S_\Lambda]^{\text{mon}} \).

**Lemma 4.5.** The monomials in the set \( \mathcal{L} \) are the \( \mathbb{K} \)-linearly independent in \( \mathbb{K}[S_\Lambda]^{\text{mon}} / \langle f_0, \ldots, f_n \rangle \).
Lemma 4.9. If \((F_1, \ldots, F_n, X^{(0,\mathbf{e_0})})\) is Koszul regular then, for any \(F_0 \in \mathbb{E}[S^d_\Lambda]_{\leq m},\) the matrix \(M_{1,1}(F_0)\) is invertible.

Proof. By Lem. 4.8, as the system \((F_1, \ldots, F_n, X^{(0,\mathbf{e_0})})\) is Koszul regular, then the matrix \(M(X^{(0,\mathbf{e_0})})\) is invertible. As \(M_{2,1}(X^{(0,\mathbf{e_0})})\) is the zero matrix and \(M_{2,2}(X^{(0,\mathbf{e_0})})\) is the identity, then \(M_{1,1}(X^{(0,\mathbf{e_0})})\) must be invertible. By construction, the matrices \(M_{1,1}(F_0)\) and \(M_{2,2}(F_0)\) are independent of the choice of \(F_0\). Hence, for any \(F_0\) the matrix \(M_{1,1}(F_0)\) is invertible.

\[P(d) = \# \left( \big( \sum_{j=0}^n d_j / \Delta_j \big) \cap \mathbb{Z}^n \right)\]

Note that \(P(d)\) equals the number of different monomials in \(\mathbb{E}[S^d_\Lambda]_{d}\).

Lemma 4.13. Let \((F_1, \ldots, F_k, X^{(0,\mathbf{e_0})}) \in \mathbb{E}[S^d_\Lambda]\) be a (sparse) regular sequence and let \(d_i \in \mathbb{N}^{n+1}\) be the multidegree of \(F_i\), for \(i \in [k]\). Consider a multigraded monomial order \(<\). For every multidegree \(d \in \mathbb{N}^{n+1}\) such that \(d \geq \sum_i d_i\), the arithmetic complexity of computing \(\text{ReduceMacauley}\) \(((F_1, \ldots, F_k), d, <)\) is \(O(k^{k+1}P(d)^{\omega_0})\), where \(\omega_0\) is the constant of matrix multiplication.

Proof. By Cor. 3.12, as \((F_1, \ldots, F_k, X^{(0,\mathbf{e_0})}) \in \mathbb{E}[S^d_\Lambda]\) is a (sparse) regular sequence and \(d \geq \sum_i d_i\), all the matrices that appear during the computations of \(\text{ReduceMacauley}\) \(((F_1, \ldots, F_k), d, <)\) 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 \(d\) is \(P(d)\). Thus, in this case, the complexity of Gaussian elimination is \(O(P(d)^{\omega_0})\) [45]. If \(\mathcal{C}(d, \omega_0)\) is cost of \(\text{ReduceMacauley}\) \(((F_1, \ldots, F_k), d, <)\), then we have the following recursive relation

\[\mathcal{C}(d, \omega_0) = \begin{cases} O(P(d)^{\omega_0}) & \text{if } k = 1, \\ \mathcal{C}(k - 1, d, <) + O(k^{k+1}P(d)^{\omega_0}) \end{cases}\]

The cost \(\mathcal{C}(k - 1, d, <)\) is greater than \(\mathcal{C}(k - 1, d - d_k, <)\), as it involves bigger matrices. Hence, we obtain \(\mathcal{C}(d, \omega_0) = O(k^{k+1}P(d)^{\omega_0})\).

Theorem 4.14. Consider an affine polynomial system \((f_1, \ldots, f_n)\) in \(\mathbb{K}[x]\) such that Assum. 4.1 holds and the system \((F_1, \ldots, F_n)\) is (sparse) regular, where \(F_i \in \mathbb{E}[S^d_\Lambda]_{\leq m}\) and \(\chi(F_i) = f_i\), for \(i \in [n]\). Then, the complexity of computing \(\langle f_1, \ldots, f_n \rangle : \langle \Pi_i x_i \rangle^{\omega_0}\) is \(O((\sum_i d_i)^{\omega_0} P(d)^{\omega_0} + n MV(\Delta_1, \ldots, \Delta_n)^{\omega_0})\).

We need to compute:

- The set rows(\(\text{ReduceMacauley}\) \(((F_1, \ldots, F_n), \sum_i e_i, <)\)) to generate \(\mathcal{C}(d)\) (Rem. 4.7). By Lem. 4.13, this costs \(O((\sum_i d_i)^{\omega_0} P(d)^{\omega_0})\).
- The set rows(\(\text{ReduceMacauley}\) \(((F_1, \ldots, F_n), 1, <)\)) to generate the matrix \(M(F_0)\) of Lem. 4.8. By Lem. 4.13, it costs \(O((\sum_i d_i)^{\omega_0} P(d)^{\omega_0})\).
- For each variable \(x_i\), the Schur complement of \(M(F_0)\), for \(\chi(F_0) = x_i\). The cost of each Schur complement computation is \(O(P(d)^{\omega_0})\), and so the cost of this step is \(O(n P(d)^{\omega_0})\).
- The complexity of \(\text{FGLM}\) depends on the number of solutions, and in this case it is \(O(n MV(\Delta_1, \ldots, \Delta_n)^{\omega_0})\).

Note that \(MV(\Delta_1, \ldots, \Delta_n) < P(1)\). Hence, to improve the previous bound for lexicographical orders, we can follow [22].

Acknowledgements: We thank C. D’Andrea, C. Massri, B. Mourrain, P.-J. Spaenlehauer, and B. Teissier for the helpful discussions and references.

REFERENCES
[1] M. Bardet, J.-C. Faugère, and B. Salvy. 2015. On the complexity of the F5 Gröbner 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. Bobb and M. Chardin. 2017. Castelnuovo Mumford regularity with respect to multigraded ideals. Journal of Algebra 474 (March 2017), 361–392.
[4] B. Buchberger. 2006. Bruno Buchberger’s PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. J. Symbolic Comput. 41, 3-4 (March 2006), 475–511.
[5] B. Buchberger and F. Winkler. 1998. Gröbner Bases and Applications. CUP.
Gröbner Basis over Semigroup Algebras

[6] 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.

[7] 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.

[8] J. C. Faugère and P. Paillot. 2016. Exploring chordal structure in polynomial ideals: A Gröbner bases approach. SIAM J. Discrete Math., 30, 3 (2016), 1534–1570.

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

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

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

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

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

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

[15] I. Z. Emiris and A. Rege. 1994. Monomial Bases and Polynomial System Solving. In Proc. ACM ISSAC. ACM, 114–122.

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

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

[18] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. 2011. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity. J. Symbolic Comput., 46, 4 (April 2011), 406–437.

[19] J.-C. Faugère and P.-J. Spaenlehauer. 2010. Algebraic Cryptanalysis of the PKC’09 Algebraic Surface Cryptosystem. In PKC 2010 (Lecture Notes in Computer Science), Phong Q. Nguyen and David Pointcheval (Eds.), Vol. 6056. Springer, Paris, France, 35–52.

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

[21] J.-C. Faugère, P.-J. Spaenlehauer, and J. Svartz. 2016. Computing Small Certificates of Inconsistency of Quadratic Fewnomial Systems. In Proc. ACM ISSAC. ACM, 223–230.

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

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

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

[25] M. Giusti, G. Lecerf, and B. Salvy. 2001. A Gröbner free alternative for polynomial system solving. Journal of Complexity, 17, 1 (2001), 154–211.

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

[27] M. I. Herrero, G. Jeronimo, and J. Sabia. 2013. Affine solution sets of sparse polynomial systems. In Proc. ACM ISSAC. ACM, 223–230.

[28] J. von zur Gathen and J. Gerhard. 2013. Modern Computer Algebra (3rd ed.). CUP.

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

[30] B. Sturmfels. 1996. Gröbner Bases and Convex Polytopes. AMS.

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

[32] 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.

[33] 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.

[34] J. von zur Gathen and J. Gerhard. 2013. Modern computer algebra (3rd ed.). CUP.

[35] B. Sturmfels. 1993. Sparse elimination theory. In Proc. Conf. Computer Algebra. Springer, 158–165.

[36] B. Huber and B. Sturmfels. 1995. A polyhedral method for solving sparse polynomial systems. In Proc. Conf. Computer Algebra. Springer, 89–104.

[37] M. I. Herrero, G. Jeronimo, and J. Sabia. 2013. Affine solution sets of sparse polynomial systems. In Proc. ACM ISSAC. ACM, 223–230.

[38] J. M. Rojas. 1999. Solving degenerate sparse polynomial systems faster. Algorithmica 25, 2 (June 1999), 372–402.

[39] B. Sturmfels. 1993. Sparse elimination theory. In Proc. Conf. Computer Algebra. Springer, 158–165.

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

[41] B. Sturmfels. 1996. Gröbner Bases and Convex Polytopes. AMS.

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

[43] 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.

[44] 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.

[45] J. von zur Gathen and J. Gerhard. 2013. Modern computer algebra (3rd ed.). CUP.

[46] J. Weyman and A. Zelevinsky. 1994. Multigraded formulae for multigraded resultants. J. Algebra Geom, 3, 4 (1994), 569–597.
A COUNTER-EXAMPLE TO THE COMPLEXITY BOUNDS IN [20]

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

\[
F_1 = X^{(1,2,0,2)} + X^{(2,1,2,1)} + X^{(0,2,1,2)} + X^{(0,2,0,1)} + X^{(2,0,1,2)} + X^{(0,0,0,2)}
\]

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

Consider the graded monomial order $<$ given by

\[
X^{(i_1, j_1, k_1, l_1)} < X^{(i_2, j_2, k_2, l_2)} \iff \left\{ \begin{array}{l}
d_1 < d_2, \text{ or} \\
d_1 = d_2 \text{ and } i_1 < i_2, \text{ or} \\
d_1 = d_2 \text{ and } i_1 = i_2 \text{ and } j_1 < j_2
\end{array} \right.
\]

In this case, the bound in [20, 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-8-Dim-GB**

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

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

1. Consider the semigroup algebra $\mathbb{K}[S^h_{\Delta}]$ related to the polytopes of $f_1, \ldots, f_n$ and the standard n-simplex.
2. Choose a multigraded monomial order $<$ for $\mathbb{K}[S^h_{\Delta}]$.
3. For each $i \in [n]$, choose $F_i \in \mathbb{K}[S^h_{\Delta}]$ such that $\chi(F_i) = f_i$.
4. $C \leftarrow \text{Rows}(\text{ReduceMacaulay}((F_1, \ldots, F_n), \{i > 0 \mid e_i, <\}))$.
5. $P \leftarrow \text{Rows}(\text{ReduceMacaulay}((F_1, \ldots, F_n), \{1, <\}))$.
6. $L \leftarrow \{X^{(i \alpha, \sum_{i=1}^n e_i)} \in \mathbb{K}[S^h_{\Delta}] : X^{(i \alpha, \sum_{i=1}^n e_i)} \notin C\}$.
7. for all $x_i \in \mathbb{K}[x]$ do
8. Choose a monomial $m \in \mathbb{K}[S^h_{\Delta}]$ such that $\chi(m) = x_i$.
9. $M(m) \leftarrow \text{Macaulay matrix of degree } 1$ with respect to $<.$
10. for all $P \in P$ do
11. Add $F$ to $M(m)$
12. for all $L \in L$ do
13. Add $L \cdot m$ to $M(m)$
14. Rearrange $M(m)$ as $\left[ M_{1,1}(m) \ M_{1,2}(m) \right] \left[ M_{2,1}(m) \ M_{2,2}(m) \right]$ like (5).
15. $M_{x_i} \leftarrow (M_{2,2} - M_{2,1} \cdot \ M_{1,2}(m))$.
16. Perform FGLM with the multiplication matrices $M_{x_1}, \ldots, M_{x_n}$ with respect to $>$ to obtain Gröbner basis $G$.
17. return $G$. 