Toric Border Basis

Bernard Mourrain, Philippe Trebuchet

TORIC BORDER BASES

BERNARD MOURRAIN
INRIA, ÉQUIPE GALAAD
BP 93, 06902 SOPHIA ANTIPOLIS, FRANCE
BERNARD.MOURRAIN@INRIA.FR

PHILIPPE TRÉBUCHET
SORBONNE UNIVERSITÉS, UPMC, EQUIPE APR. LIP6, UMR 7606,
INRIA, ÉQUIPE OURAGAN
4 PLACE JUSSIEU 75256 PARIS CEDEX PHILIPPE.TREBUCHET@LIP6.FR

Abstract. We extend the theory and the algorithms of Border Bases to systems of Laurent polynomial equations, defining "toric" roots. Instead of introducing new variables and new relations to saturate by the variable inverses, we propose a more efficient approach which works directly with the variables and their inverse. We show that the commutation relations and the inversion relations characterize toric border bases. We explicitly describe the first syzygy module associated to a toric border basis in terms of these relations. Finally, a new border basis algorithm for Laurent polynomials is described and a proof of its termination is given for zero-dimensional toric ideals.

1. Introduction

Polynomial equations appear naturally in many applications, as a way to describe constraints between the unknown variables of a problem. These could be, for instance, geometric constraints between objects (as in robotics, or CAGD) or physical constraints (as in chemistry). In such problems, partial additional information may also be known: the unknown variables are not zero, or real, positive, between 0 and 1, etc.

Finding the solutions by exploiting these constraints and this additional information is thus an important operation, which usually requires dedicated and efficient methods.

An algebraic approach to get (all) the complex solutions of a polynomial system is based on the computation of quotient algebra structures [4, 7]. These structures are described effectively by a set of polynomials which represent the normal forms in the quotient structure and a method to compute the normal form of any polynomial. This family of methods includes, for instance, Gröbner basis [3, 6] or border basis computation [15, 18, 12]. A "fixed-point" strategy is involved in these algorithms: starting with the initial set of equations, so-called S-polynomials or commutation polynomials are computed and reduced. If non-zero remainders are found, the set of equations is updated and the computation is iterated; otherwise, the process is stopped.

An important difference between Gröbner bases and border Bases is that a monomial ordering compatible with monomial multiplication is necessary in the first type of methods. This monomial ordering is used to define the initial ideal associated to the ideal of the equations. The border basis approach extends Gröbner basis methods by removing the monomial ordering constraint, which may induce numerical instability when the coefficients of the polynomials are known approximately [15, 18, 11, 13, 12, 16, 19, 10, 20].

In this paper, we consider systems of polynomial equations defining (complex) solutions with non-zero coordinates. In this case, variables can be inverted and a natural setting for normal form computation is the ring of the Laurent polynomials. The extension of Gröbner basis algorithm to Laurent polynomials is difficult, due to the lack of monomial well-order and the fact that monomial ideals are trivial. A classical way to handle this difficulty is to introduce new variables y_i for the inverse of the initial variables x_i and new relations $x_iy_i-1=0$ and to compute with polynomials in

this extended set of variables. Doubling the number of variables and adding new relations usually significantly reduce the performance of algorithms whose complexity is at least exponential in the number of variables (even doubly exponential in the worst case).

In the context of elimination and resultant theory, the approach of Macaulay [14] for the construction of projective resultant matrices has been extended successfully to toric resultant for Laurent polynomials [9, 1, 8, 21, 2, 5]. By analyzing the support of the Laurent polynomials, resultant matrices of smaller size than for the projective resultant can be constructed. This leads to more efficient algorithms to compute a monomial basis of the quotient algebra and the (toric) roots for a square polynomial system, provided that it is *generic* for its support.

Our motivation is to develop normal form algorithms that can be performed with Laurent polynomials in the same type of complexity bounds than for usual polynomials, using efficient sparse linear algebra on Laurent polynomial spaces.

Contributions. We extend the border basis approach to Laurent polynomials and show that a characterization similar to the criterion for classical border bases [15, 18, 19] applies in this case: namely, the commutation relations (the product of two variables should commute) and the inversion relations (the product of a variable by its inverse should be 1) can be used to check if a set of polynomials is a toric border basis in a given degree. As a new result, this characterization yields an explicit description of the first module of syzygies of a toric border basis, generalizing in a natural way results from [19]. It is an extension of Schreyer Theorem which describes generators of the first syzygy module of a Grobner basis in terms of the reduction of S-polynomials [6][Theorem 15.10]. We also deduce a new algorithm for computing a toric border basis, which requires light modifications of the classical border basis algorithm. We prove its termination in the case of zero-dimensional toric ideals.

Content. The paper is organized as follows. Section 2 describes the normal form criterion for toric border bases. In Section 3, an explicit family of generators of the first syzygy module of a toric border basis is given. In Section 4, we detail the algorithm for computing a border basis for Laurent polynomials and prove its correctness for zero-dimensional ideals, before the concluding Section 5.

Notation. Let $\mathcal{M}$ be the set of Laurent monomials in the variables $x_1, \ldots, x_n$. An element of $\mathcal{M}$ is of the form $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$.

Definition 1.1. *The degree of a monomial* $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots\ x_n^{\alpha_n} \in \mathcal{M}$ *is* $\delta(\mathbf{x}^\alpha) = |\alpha_1| + \cdots + |\alpha_n|$, *which we also denote* $\delta(\alpha)$.

We will use the following notation: $x_{-i} = x_i^{-1}$, $i = 1 \ldots n$, $x_0 = 1$, $[-n, n]^* = \{i \in [-n, n] \mid i \neq 0\}$. We say that a sequence $(i_1, \ldots, i_k), i_j \in [-n, n]^*$ is canonical if $|i_1| \leq |i_2| \leq \cdots \leq |i_k|$ and $\delta(x_{i_1} \cdots x_{i_k}) = k$. It corresponds to a canonical way to write a monomial as a product of variables.

For $m \in \mathcal{M}$, we denote by $((m))$ the cone generated by m, that is, $((m)) = \{m' \in \mathcal{M} \mid m' = m\, m''$ *s.t.* $m'' \in \mathcal{M}, \delta(m') = \delta(m) + \delta(m'')\}$. It corresponds to the set of monomial multiples of m, which are in the same "quadrant" of $\mathbb{Z}^n$.

Let $S = \mathbb{K}[x_1^{\pm}, \ldots, x_n^{\pm}]$ be the ring of Laurent polynomials in the variables $x_1, \ldots, x_n$ with coefficients in a field $\mathbb{K}$, that is the set of finite linear combinations of monomials in $\mathcal{M}$.

For $p = \sum_{\alpha \in A} p_\alpha\, \mathbf{x}^\alpha \in S$ with $p_\alpha \neq 0$, A is the support of p and $\delta(p) = \max_{\alpha \in A} \delta(\alpha)$.

For $F \subset S$, let $\langle F \rangle$ be the $\mathbb{K}$-vector space spanned by F.

For $d \in \mathbb{N}$ and $F \subset S$, let $F_{\leq d}$ (resp. F_d) be the set of polynomials $p \in F$ such that $\delta(p) \leq d$ (resp. $\delta(p) = d$).

For $d \in \mathbb{N}_+ = \mathbb{N} \setminus \{0\}$, let $F_{[\leq d]} = \{m\, f \mid m \in \mathcal{M}, f \in F, \delta(m\, f) \leq d\}$ and $F_{[d]} = F_{[\leq d]} \setminus F_{[\leq d-1]}$.

For $B \subset \mathcal{M}$, we denote $B^\times = B \cup x_1 B \cup \cdots \cup x_n B \cup x_1^{-1} B \cup \cdots \cup x_n^{-1} B$ and call it the prolongation of B. Let $\partial B = B^\times \setminus B$ be the border of B. Let $B^{[0]} = B$ and for $k \in \mathbb{N}_+$, let $B^{[k]} = (B^{[k-1]})^\times$.

A set $B \subset \mathcal{M}$ is *connected to* 1 if $1 \in B$ and $\forall m \in B \setminus \{1\}$, there exists $i \in [-n, n]^*$ and $m' \in B$, such that $m = x_i\, m'$ and $\delta(m') < \delta(m)$.

2. Normal form criterion

In this section, we describe normal form criteria for toric border bases. The purpose of these criteria is to determine when we have a decomposition:

$$S_{\leq d} = \langle B\rangle_{\leq d} \oplus (F)_{\leq d}$$

for a monomial set B connected to 1, a polynomial set F and a degree $d \in \mathbb{N}$. The conditions that we describe extend naturally those known for classical border bases, which are related to the commutation property of multiplication operators.

Hereafter, $B \subset \mathcal{M}$ is a finite set of monomials connected to 1, $V = \langle B\rangle$ and $V^\times = \langle B^\times\rangle$.

Let $\pi : V^\times_{\leq d} \to V_{\leq d}$ be a projection such that $\pi \circ \pi = \pi$ and $\pi_{|V_{\leq d}}$ is the identity map, and which is compatible with the degree δ: $\forall b \in \langle B^+\rangle_{\leq d}$, $\delta(\pi(b)) \leq \delta(b)$.

Let $K = \ker \pi$ be the kernel of π, so that

$$V^\times = V \oplus K.$$

As each monomial of $(\partial B)_{\leq d}$ can be projected by π in $V_{\leq d}$, we can define a rewriting family as follows:

Definition 2.1. *For $B \subset \mathcal{M}$ connected to 1 and a projection $\pi : \langle B^\times\rangle_{\leq d} \to \langle B\rangle_{\leq d}$, the* rewriting family *for π is the set F of polynomials of $\ker \pi$ of the form*

$$f_\alpha = \mathbf{x}^\alpha - b_\alpha, \tag{1}$$

with $b_\alpha = \pi(\mathbf{x}^\alpha) \in \langle B\rangle_{\leq d}$, $\mathbf{x}^\alpha \in (\partial B)_{\leq d}$.

We check that F is a generating set of $K = \ker \pi$. Conversely, a set F of polynomials of the form (1) with $b_\alpha \in \langle B\rangle_{\leq d}$, $\mathbf{x}^\alpha \in (\partial B)_{\leq d}$ and $\langle B^\times\rangle_{\leq d} = \langle F\rangle \oplus \langle B\rangle$ defines a projection from $\langle B^\times\rangle_{\leq d}$ onto $\langle B\rangle_{\leq d}$.

Definition 2.2. *For $F \subset S$ and $B \subset \mathcal{M}$, let $\mathcal{C}_B(F)$ be the set of polynomials in $\langle B^\times\rangle$ which are of the form*

1. *$x_i f$ for some $f \in F$, $i \in [-n, n]^*$ or*
2. *$x_i f - x_j f'$ for $f, f' \in F$, $-1 \leq i < j \leq n$.*

The set of polynomials of type 1 (resp. 2) is denoted $\mathcal{C}^1_B(F)$ (resp. $\mathcal{C}^2_B(F)$). The polynomials in $\mathcal{C}^1_B(F)$ (resp. $\mathcal{C}^2_B(F)$) are called the prolongation (resp. commutation) polynomials of F for B. Let $\mathcal{C}_B(F) = \mathcal{C}^1_B(F) \cup \mathcal{C}^2_B(F)$.

From this definition, we see that $\mathcal{C}(F) \subset \langle F^\times\rangle \cap \langle B^\times\rangle$. Hereafter, the set B will be fixed and we will simply write $\mathcal{C}_B(F) = \mathcal{C}(F)$.

We define the operator of multiplication by x_i associated to π as:

$$\begin{array}{rcl} X_i : \langle B\rangle_{\leq d-1} & \to & \langle B\rangle_{\leq d} \\ b & \mapsto & \pi(x_i b). \end{array}$$

As π is compatible with the degree, the image by X_i of an element of degree $\leq k < d$ is of degree $\leq k + 1$.

For a monomial $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathcal{M}$ of degree $\leq d$, we define $\mathbf{X}^\alpha := X_1^{\alpha_1} \circ \cdots \circ X_n^{\alpha_n}$. It is an operator from $\langle B\rangle_{\leq d-\delta(\alpha)}$ to $\langle B\rangle_{\leq d}$. We extend this construction by linearity and for any $p \in S_{\leq d}$, we define $p(\mathbf{X}) : \langle B\rangle_{\leq d-\delta(p)} \to \langle B\rangle_{\leq d}$.

As B contains 1 which is of degree 0, we can then define

$$\begin{array}{rcl} \sigma : S_{\leq d} & \to & \langle B\rangle_{\leq d} \\ p & \mapsto & p(\mathbf{X})(1). \end{array}$$

Its kernel is denoted $I_{\pi,d}$.

Our objective is to relate properties of commutation and inversion of the operators X_i with the property that σ defines a normal form, that is a projection on $\langle B\rangle_{\leq d}$ along the ideal generated by

F in degree $\leq d$. We also relate it with a property which is easy to test algorithmically, namely the polynomials $\mathcal{C}_B(F)$ reduce to 0 by the rewriting family F.

The techniques used here are very similar to those developed in [15, 18, 19, 20], but they require specific adaptations to the toric case, which we need to detail.

Theorem 2.3. *Let $d \geq 2$, let B be a subset of $\mathcal{M}$ connected to 1, let $\pi : \langle B^\times\rangle_{\leq d} \to \langle B\rangle_{\leq d}$ be a projection and let F be the rewriting family for π. The following conditions are equivalent:*

1. $(X_i \circ X_{-i})_{|\langle B\rangle_{\leq d-2}} = Id$ *for* $1 \leq i \leq n$,
   $(X_i \circ X_j - X_j \circ X_i)_{|\langle B\rangle_{\leq d-2}} = 0$ *for* $1 \leq i < j \leq n$,
2. *the map σ is a projection which defines the exact sequence*
$$0 \to \langle F_{[\leq d]}\rangle \to \mathcal{S}_{\leq d} \xrightarrow{\sigma} \langle B\rangle_{\leq d} \to 0$$
3. $\forall r \in \mathcal{C}_B(F_{\leq d-1})$, $\pi(r) = 0$.

Proof. 1) $\Rightarrow$ 2) : As the operators X_i are commuting and $X_{-i} = X_i^{-1}$ in degree $d-2$, for any monomials m, m' such that $\delta(m) \leq d, \delta(m') \leq d, \delta(m\,m') \leq d$, we have $m(\mathbf{X}) \circ m'(\mathbf{X}) = m'(\mathbf{X}) \circ m(\mathbf{X})$ and $\sigma(m\,m') = m(\mathbf{X})(\sigma(m'))$. The construction of σ is independent of the order in which we compose the operators X_i since they are commuting.

Let us show by induction on $\delta(m)$, that for all monomials $m \in B^\times$, we have $\sigma(m) = \pi(m)$.

The only monomial $m \in \mathcal{M}$ such that $\delta(m) = 0$ is $1 \in B$ and by definition $\sigma(1) = \pi(1) = 1$. The property is true for the degree 0.

Assume that it is true in degree $0 \leq k-1 < d$ and let $m \in B$ with $\delta(m) = k$. As $B^\times$ is connected to 1, there exists $i \in [-n, n]^*$ and $m' \in B$ with $\delta(m') \leq k-1$ such that $m = x_i\,m'$. By induction, we have $\sigma(m') = \pi(m') = m'$, thus
$$\sigma(m) = m(\mathbf{X})(1) = X_i(\sigma(m')) = X_i(m') = \pi(x_i\,m') = \pi(m).$$

This shows, in particular, that $\forall m \in B, \sigma(m) = m$ and that $\sigma \circ \sigma = \sigma$. We deduce that the image of σ is $\langle B\rangle_{\leq d}$ and that the kernel $I_{\pi,d}$ of σ is generated by $p - \sigma(p)$ for $p \in S_{\leq d}$.

We now prove that $\langle F_{[\leq d]}\rangle \subset I_{\pi,d}$. For any $m \in \partial B$, we have $\sigma(m) = \pi(m)$ and $\sigma(\pi(m)) = \pi(m)$ since $\pi(m) \in \langle B\rangle_{\leq d}$. This implies that $\sigma(m - \pi(m)) = 0$. We have shown that the elements $m - \pi(m)$, $m \in \partial B$ are in $I_{\pi,d}$. We deduce that $F \subset I_{\pi,d}$ and thus that $\langle F_{[\leq d]}\rangle \subset I_{\pi,d}$.

In the next step, we prove that $I_{\pi,d} \subset \langle F_{[\leq d]}\rangle$. As $I_{\pi,d}$ is spanned by $p - \sigma(p)$ for $p \in S_{\leq d}$, it is sufficient to prove that for a monomial m with $\delta(m) \leq d$, we have $m - \sigma(m) \in \langle F_{[\leq d]}\rangle$, which we do by induction on $\delta(m)$. The case $\delta(m) = 0$ or $m = 1$ is obvious. For any monomial $m \in \mathcal{M}_{\leq d}$, we can decompose it as $m = x_i m'$ with $i \in [-n, n]^*$ and $\delta(m') < \delta(m)$. By the induction hypothesis, $m' - \sigma(m') \in \langle F_{[\leq d-1]}\rangle$. We deduce that
$$m - \sigma(m) = x_i(m' - \sigma(m')) + x_i\sigma(m') - \pi(x_i\sigma(m'))$$
is in $\langle F_{[\leq d]}\rangle$, since $x_i\sigma(m') - \pi(x_i\sigma(m')) \in \ker\pi = \langle F\rangle$. This proves that $I_{\pi,d} \subset \langle F_{[\leq d]}\rangle$.

This implies that $I_{\pi,d} = \langle F_{[\leq d]}\rangle$ and proves point (2).

2) $\Rightarrow$ 3) : Let $r \in \mathcal{C}(F_{\leq d-1})$ then $r \in \langle (F_{\leq d-1})^\times\rangle \cap \langle B^\times\rangle$. As $\langle (F_{\leq d-1})^\times\rangle \subset \langle F_{[\leq d]}\rangle = \ker\sigma$ we have $\sigma(r) = 0$. But σ coincides with π on $\langle B^\times\rangle$ so that we have $\pi(r) = 0$, which shows that $r \in \ker\pi = \langle F\rangle$.

3) $\Rightarrow$ 1) : Let $m \in B$ of degree $\leq d-2$ and $1 \leq i < j \leq n$. Suppose that $m_1 := x_i m \in \partial B$ and $m_2 := x_j m \in \partial B$. Let $f_1 = m_1 - \pi(m_1), f_2 = m_2 - \pi(m_2) \in F_{\leq d-1}$. As $x_i m_2 = x_j m_1 = x_i x_j m$, we have
$$\begin{aligned}(X_i \circ X_j - X_j \circ X_i)(m) &= \pi(x_i\pi(m_2)) - \pi(x_j\pi(m_1)) \\ &= \pi(x_i(m_2 - f_2) - x_j(m_1 - f_1)) \\ &= \pi(x_j f_1 - x_i f_2).\end{aligned}$$
As $x_j f_1 - x_i f_2 = x_i\pi(m_2) - x_j\pi(m_1) \in \mathcal{C}_B(F_{\leq d-1})$, the hypothesis (3) implies that $\pi(x_j f_1 - x_i f_2) = 0$. A similar argument applies if $x_i m \in B$ or $x_j m \in B$. Consequently, we have $(X_i \circ X_j - X_j \circ X_i)_{|\langle B\rangle_{\leq d-2}} = 0$.

Similarly, we have

$$\begin{aligned} X_{-i} \circ X_i(m) &= \pi(x_{-i}\pi(m_1)) = \pi(x_{-i}(m_1 - f_1)) \\ &= \pi(m - x_{-i}f_1)). \end{aligned}$$

As $m - x_{-i}f_1 \in \langle B^\times \rangle$, we have $x_{-i}f_i \in \langle B^\times \rangle$ and thus $x_{-i}f_1 \in \mathcal{C}_B(F_{\leq d-1})$, which implies that $\pi(x_{-i}f_1) = 0$. We deduce that $\pi(m - x_{-i}f_1) = \pi(m) = m$. A similar argument applies if $x_i m \in B$. This proves that $(X_{-i} \circ X_i)_{|\langle B \rangle_{\leq d-2}} = Id$ and concludes the proof of point (3). □

If one of these (equivalent) conditions is satisfied, we say that F is a *border basis* in degree d for B.

Remark 2.4. *If F is a border basis for B in degree d, then Theorem 2.3 implies that $F_{\leq d'}$ is a border basis for B in degree d' for any $2 \leq d' \leq d$.*

Remark 2.5. *If Theorem 2.3 (2) is satisfied, then any element $p \in S_{\leq d}$ is the sum of $\sigma(p) \in \langle B \rangle_{\leq d}$ and $p - \sigma(p) \in I_{\pi,d} = \langle F_{[\leq d]} \rangle$. Moreover, $p \in \langle B \rangle_{\leq d} \cap \langle F_{[\leq d]} \rangle$ is such that $p = \sigma(p) = 0$. We deduce that*

$$S_{\leq d} = \langle B \rangle_{\leq d} \oplus \langle F_{[\leq d]} \rangle,$$

and σ is the projection on $\langle B \rangle_{\leq d}$ along $\langle F_{[\leq d]} \rangle$. It is also called a normal form on $S_{\leq d}$ modulo $\langle F_{[\leq d]} \rangle$.

3. Syzygies

Let F be a border basis in any degree for a finite set B of monomials, which is connected to 1.

For any monomial $m \in \mathcal{M}$, we define $\delta_B(m)$ as the smallest integer $d \in \mathbb{N}$ such that $m \in B^{[d]}$. If $m \in B$, then $\delta_B(m) = 0$. For any $m_1, m_2 \in \mathcal{M}$, $\delta_B(m_1\, m_2) \leq \delta(m_1)\delta_B(m_2)$.

For any $i \in [-n, n]^*$, let μ_i be the multiplication by x_i in S. We define the map

$$\begin{aligned} \psi_i : \langle B \rangle &\to \langle F \rangle \\ m &\mapsto (\mu_i - X_i)(m) = x_i m - \pi(x_i m) \end{aligned}$$

For a monomial $m \in B$, if $x_i m \in B$ then $\psi_i(m) = 0$, otherwise $\psi_i(m)$ is an element of F. Conversely, for any $f \in F$ of the form $f = \mathbf{x}^\alpha - b_\alpha$ with $\mathbf{x}^\alpha \in \partial B$ and $b_\alpha \in \langle B \rangle$, there exist $m \in B$ and $i \in [-n, n]^*$ such that $\mathbf{x}^\alpha = x_i m$. We deduce that $f = \psi_i(m)$. Therefore, the set of elements $\psi_i(m) \neq 0$ with $m \in B$, $i \in [-n, n]^*$ is F.

Using the relations between elements in F and elements of the form $\psi_i(m)$, we are going now to associate to the set F a basis of a free S module. The purpose of this construction is to describe generators of the syzygies between the elements of F explicitly. We denote by $Y_i, i \in [-n, n]^*$ the canonical basis of the vector space $Y = \mathbb{K}^{2n}$. Let $\mathcal{S}_1$ be the free S-module generated by $Y_i \otimes m$ with $i \in [-n, n]^*$, $m \in B$ and $x_i m \notin B$. The basis of the S module $\mathcal{S}_1$ is also denoted

$$Y_i[m] := Y_i \otimes m.$$

By convention, $Y_i[m] = 0$ if $x_i\, m \in B$ and for any $b = \sum_j \lambda_j m_j \in \langle B \rangle$, $Y_i[b] = Y_i \otimes b = \sum_j \lambda_j Y_i[m_j]$. An element of $\mathcal{S}_1$ is a sum of terms of the form $\lambda\, m_1 Y_i[m_2]$ with $\lambda \in \mathbb{K} \setminus \{0\}$, $m_1 \in \mathcal{M}$, $m_2 \in B$.

We extend the degree δ to $\mathcal{S}_1$ as follows: for any term of the form $m_1 Y_i[m_2]$ with $m_1 \in \mathcal{M}$, $m_2 \in B$, we set $\delta(m_1 Y_i[m_2]) = \delta(m_1)$. For all $r \in \mathcal{S}_1$, $\delta(r)$ is the maximum degree of its non-zero terms.

We define now the map $\partial_1 : \mathcal{S}_1 \to S$ as

$$\begin{aligned} \partial_1 : \mathcal{S}_1 &\to S \\ Y_i[m] &\mapsto \psi_i(m). \end{aligned}$$

The kernel of ∂_1 is the set of syzygies between the elements $\psi_i(m) = f$ of F.

Lemma 3.1. *$\forall m = x_{i_1}\cdots x_{i_k} \in \mathcal{M}$, we have $m = \pi(m) + \partial_1(\Psi_{i_1,\ldots,i_k})$ where*

$$\Psi_{i_1,\ldots,i_k} = \sum_{l=1}^{k} x_{i_1}\cdots x_{i_{l-1}} Y_{i_l}[X_{i_{l+1}} \circ \cdots \circ X_{i_k}(1)]. \tag{2}$$

Proof. We prove the relation by induction on k. For $k = 1$ and $i_1 \in [-n, n]^*$, $m = x_{i_1} = X_{i_1}(1) + \psi_{i_1}(1)$.

Assume that the property is true for $x_{i_2}\cdots x_{i_k} \in \mathcal{M}$. Then, by induction hypothesis,

$$\begin{aligned}
x_{i_1} x_{i_2}\cdots x_{i_k} &= x_{i_1}(x_{i_2}\cdots x_{i_k}) \\
&= x_{i_1}(\pi(x_{i_2}\cdots x_{i_k}) + \partial_1(\Psi_{i_2,\ldots,i_k})) \\
&= x_{i_1} X_{i_2} \circ \cdots \circ X_{i_k}(1) + x_{i_1} \sum_{l=2}^{k} x_{i_2}\cdots x_{i_{l-1}} \psi_{i_l} \circ X_{i_{l+1}} \circ \cdots \circ X_{i_k}(1) \\
&= X_{i_1} \circ X_{i_2} \circ \cdots \circ X_{i_k}(1) \\
&\quad + \psi_{i_1} \circ X_{i_2} \circ \cdots \circ X_{i_k}(1) + \sum_{l=2}^{k} x_{i_1}\cdots x_{i_{l-1}} \psi_{i_l} \circ X_{i_{l+1}} \circ \cdots \circ X_{i_k}(1). \\
&= X_{i_1} \circ X_{i_2} \circ \cdots \circ X_{i_k}(1) + \sum_{l=1}^{k} x_{i_1}\cdots x_{i_{l-1}} \psi_{i_l} \circ X_{i_{l+1}} \circ \cdots \circ X_{i_k}(1). \\
&= \pi(x_{i_1}\cdots x_{i_k}) + \partial_1\Big(\sum_{l=1}^{k} x_{i_1}\cdots x_{i_{l-1}} Y_{i_l}[X_{i_{l+1}} \circ \cdots \circ X_{i_k}(1)]\Big)
\end{aligned}$$

since by Theorem 2.3, $\pi(x_{i_1}\cdots x_{i_k}) = \sigma(x_{i_1}\cdots x_{i_k}) = X_{i_1} \circ X_{i_2} \circ \cdots \circ X_{i_k}(1)$. □

This construction allows us to relate any term of $\mathcal{S}_1$ with an element of the form $\Psi_{i_1,\ldots,i_k}$ as follows:

Lemma 3.2. *For any term $m_1 Y_i[m_2]$ of $\mathcal{S}_1$ with $m_1 \in \mathcal{M}$, $m_2 \in B$, there exists $i_1, \ldots, i_l \in [-n, n]^*$ such that*

$$\Psi_{i_1,\ldots,i_k} = m_1 Y_i[m_2] + r$$

with $\delta(r) < \delta(m_1) = \delta(m_1 Y_i[m_2])$.

Proof. Let $m_1 = x_{i_1}\cdots x_{i_{k_1}}$ with $\delta(m_1) = k_1$ and $m_2 = x_{j_1}\cdots x_{j_{k_2}}$ with $x_{j_l}\cdots x_{j_{k_2}} \in B$ for $1 \le l \le k_2$. As $Y_{j_l}[X_{j_{l+1}} \circ \cdots \circ X_{j_{k_2}}(1)] = Y_{j_l}[x_{j_{l+1}}\cdots x_{j_{k_2}}] = 0$, the expansion (2) of $\Psi_{i_1,\ldots,i_{k_1},i,j_1,\ldots,j_{k_2}}$ yields

$$\Psi_{i_1,\ldots,i_{k_1},i,j_1,\ldots,j_{k_2}} = m_1 Y_i[m_2] + r$$

with

$$r = \sum_{l=1}^{k_1} x_{i_1}\cdots x_{i_{l-1}} Y_{i_l}[X_{i_{l+1}} \circ \cdots \circ X_{i_{k_1}} \circ X_i \circ m_2(X)(1)].$$

The term r is such that $\delta(r) \le k_1 - 1 < \delta(m_1)$, which proves the lemma. □

Lemma 3.3. *$\forall i \neq j \in [-n, n]^*$ and $\forall m \in B$, the element*

$$\phi_{i,j}(m) := x_i Y_j[m] - x_j Y_i[m] - Y_j[X_i(m)] + Y_i[X_j(m)]$$

is in $\ker \partial_1$.

Proof. By definition of ψ_i, we have

$$\begin{aligned}
&\partial_1(x_i Y_j[m] - x_j Y_i[m] - Y_j[X_i(m)] + Y_i[X_j(m)]) \\
&\quad = x_i\psi_j(m) - x_j\psi_i(m) - \psi_j(X_i(m)) + \psi_i(X_j(m)) \\
&\quad = x_i(x_j m - X_j(m)) - x_j(x_i m - X_i(m)) \\
&\qquad -(x_j X_i(m) - X_j(X_i(m))) + (x_i X_j(m) - X_i(X_j(m))) \\
&\quad = X_j(X_i(m)) - X_i(X_j(m)) = 0
\end{aligned}$$

since X_i and X_j commute. □

By linearity, we extend the map $\phi_{i,j}$ to the vector space $\langle B\rangle$ spanned by B, so that $\phi_{i,j}(\sum_k \lambda_k m_k) = \sum_k \lambda_k \phi_{i,j}(m_k)$.

Lemma 3.4. *$\forall i \in [-n,n]^*$ and $\forall m \in B$, the element*

$$\rho_i(m) := x_i Y_{-i}[m] + Y_i[X_{-i}(m)]$$

is in $\ker \partial_1$.

Proof.

$$\begin{aligned}
&\partial_1(x_i Y_{-i}[m] + Y_i[X_{-i}(m)]) \\
&= x_i\, \psi_{-i}(m) + \psi_i(X_{-i}(m)) \\
&= x_i\,(x_{-i}\, m - X_{-i}(m)) + (x_i\, X_{-i}(m) - X_i(X_{-i}(m))) \\
&= m - X_i \circ X_{-i}(m) = 0
\end{aligned}$$

since $X_i \circ X_{-i} = Id$. □

Let $K_1 \subset \mathcal{S}_1$ be the S-module generated by the elements $\rho_i(m)$, $\phi_{i,j}(m)$ for $i \neq j \in [-n,n]^*$ and $m \in B$.

We are going now to describe how a term $m_1 Y_i[m_2]$ with $m_1 \in \mathcal{M}$, $m_2 \in B$ can be transformed modulo K_1.

Lemma 3.5. *$\forall m = x_{i_1}\cdots x_{i_k} = x_{j_1}\cdots x_{j_{k'}} \in \mathcal{M}$,*

$$\Psi_{i_1,\ldots,i_k} - \Psi_{j_1,\ldots,j_{k'}} \in K_1.$$

Proof. By successive permutations of two adjacent indices and contraction of adjacent indices $-i, i$, we can transform any sequence $J = (j_1,\ldots,j_{k'})$ into a canonical sequence $I = (i_1,\ldots,i_k)$. Thus it is enough to prove the property for the permutation of two consecutive indices: $J = (i_1,\ldots,i_l,i_{l+1},\ldots,i_k)$ and for the contraction of two indices $J = (i_1,\ldots,i_l,-j,j,i_{l+1},\ldots,i_k)$. By definition of Ψ and since the operators X_i are commuting, we have

$$\begin{aligned}
&\Psi_{\ldots,i_l,i_{l+1},\ldots} - \Psi_{\ldots,i_{l+1},i_l,\ldots} \\
&= x_{i_1}\cdots x_{i_{l-1}}\big(x_{i_l} Y_{i_{l+1}}[X_{i_{l+2}}\circ X_{i_{l+3}}\cdots\circ X_{i_k}(1)] - x_{i_{l+1}} Y_{i_l}[X_{i_{l+2}}\circ X_{i_{l+3}}\cdots\circ X_{i_k}(1)] \\
&\quad - Y_{i_l}[X_{i_{l+1}}\circ X_{i_{l+2}}\circ X_{i_{l+3}}\cdots\circ X_{i_k}(1)] + Y_{i_{l+1}}[X_{i_l}\circ X_{i_{l+2}}\circ X_{i_{l+3}}\cdots\circ X_{i_k}(1)]\big) \\
&= x_{i_1}\cdots x_{i_{l-1}}\phi_{i,j}(X_{i_{l+2}}\circ X_{i_{l+3}}\cdots\circ X_{i_k}(1))
\end{aligned}$$

which is an element of K_1. Similarly, for $j \in [-n,n]^*$

$$\begin{aligned}
&\Psi_{\ldots,i_l,j,-j,i_{l+1},\ldots} - \Psi_{\ldots,i_l,i_{l+1},\ldots} \\
&= x_{i_1}\cdots x_{i_l}\big(Y_j[X_{-j}\circ X_{i_{l+1}}\circ X_{i_{l+3}}\cdots\circ X_{i_k}(1)] \\
&\quad + x_j Y_{-j}[X_{i_{l+1}}\circ X_{i_{l+3}}\cdots\circ X_{i_k}(1)]\big) \\
&= x_{i_1}\cdots x_{i_{l-1}}\rho_j(X_{i_{l+1}}\circ X_{i_{l+3}}\cdots\circ X_{i_k}(1))
\end{aligned}$$

which is also an element of K_1. □

Theorem 3.6. *The first module of syzygies of F is generated by the elements*

- $\rho_i(m) = x_i Y_{-i}[m] + Y_i[X_{-i}(m)]$,
- $\phi_{i,j}(m) = x_i Y_j[m] - x_j Y_i[m] + Y_i[X_j(m)] - Y_j[X_i(m)]$

for $i \neq j \in [-n,n]^*$ and $m \in B$.

Proof. Let $s \in \ker\partial_1$ be a sum of non-zero terms of the form $\lambda m_1 Y_i[m_2]$ with $\lambda \in \mathbb{K}\setminus\{0\}$, $m_1 \in \mathcal{M}$, $m_2 \in B$.

The monomial $m = m_1 x_i m_2$ can be decomposed in a unique way as $m = m_1' x_{i'} m_2'$ with $\delta_B(m) = \delta(m_1')$ and $m_2' \in B$ and (i', m_1') the smallest possible for the lexicographic ordering.

By Lemma 3.2 and Lemma 3.5, there exist $i_1, \ldots, i_k$, $i'_1, \ldots, i'_{k'} \in [-n, n]^*$ with $m = x_{i_1} \cdots x_{i_k} = x_{i'_1} \cdots x_{i'_{k'}}$ and $r \in \mathcal{S}$ with $\delta(r) < \delta(m_1)$ such that

$$\begin{aligned} m_1 Y_i[m_2] &= m'_1 Y_{i'}[m'_2] + r + \Psi_{i_1,\ldots,i_k} - \Psi_{i'_1,\ldots,i'_{k'}} \\ &\equiv m'_1 Y_{i'}[m'_2] + r \mod K_1. \end{aligned}$$

Applying this relation inductively on the terms of r, any element $m_1 Y_i[m_2]$ can be reduced modulo K_1 to a sum of terms of the form $\lambda m'_1 Y_{i'}[m'_2]$ with $\delta_B(m'_1 x_{i'} m'_2) = \delta(m'_1)$ and (i, m'_1) the smallest possible for the lexicographic ordering.

Thus we can assume that the terms of the decomposition of $s \in \ker \partial_1$ satisfy this property. Hereafter, we call this decomposition a canonical decomposition of s. Suppose that the canonical decomposition s is not zero. Then for any term $(m_1 Y_i[m_2]$ of this canonical decomposition, we have $\partial_1(m_1 Y_i[m_2]) = m_1 x_i m_2 + p$ with $\delta_B(p) < \delta_B(m_1 x_i m_2)$.

Let us consider a term $\lambda\, m_1 Y_i[m_2]$ such that $\delta_B(m_1 x_i\ m_2) = \delta(m_1)$ is maximal. As $s \in \ker \partial_1$, the monomial $\lambda m_1 x_i m_2$ must be cancelled by a monomial $\lambda' m'_1 x_{i'} m'_2$ from the image $\partial_1(m'_1 Y_{i'}[m'_2])$ of a distinct term of the canonical decomposition s.

As there is a unique way to decompose a monomial $m \in \mathcal{M}$ as $m = m_1 x_i m_2$ with $m_1 Y_i[m_2] \neq 0$, $\delta_B(m'_1 x_{i'} m'_2) = \delta(m'_1)$ and (i, m'_1) the smallest possible for the lexicographic ordering, this is not possible. We obtain a contradiction, which shows that the canonical decomposition of s is zero and that $s \in \ker \partial_1$ can be reduced to 0 modulo K_1. In other words, $K_1 = \ker \partial_1$ which proves the theorem. □

4. Algorithm

In this section we describe an algorithm based on the above properties to compute a border basis for a system of Laurent polynomials. For the sake of simplicity, and as they were not needed before, we introduce the following definitions:

Definition 4.1. *The ball $Ball(k)$ of radius k is the set of monomials m of $\mathcal{M}$ such that $\delta(m) \leq k$.*

Definition 4.2. *Let f be a Laurent polynomial. A monomial m of the support of f is said to be* extremal *for f if $\delta(m) = max(\delta(m'),\ m' \in \mathrm{supp}(f))$. In other words an extremal monomial is a monomial of maximal degree.*

We use the preceeding definitions to extend the notion of choice functions introduced in [18] to the context of Laurent polynomials. We recall that in the context of usual polynomials, the choice function generalizes the construction of the leading monomial for a monomial ordering. It is used to the select a monomial of a polynomial in the reduction process.

Definition 4.3. *A choice function γ refining the degree δ is a function such that, given a Laurent polynomial f returns a monomial $\gamma(f)$ of the support of f that is extremal.*

4.1. **Description.** We now describe the complete algorithm for computing a border basis for a Laurent polynomial system. This algorithm follows the same approach as in [20], with adaptations to be done for dealing with the fact that the prolongation operation $\cdot^{\times}$ can lead to degree drops. It is a "fixed-point" method which updates a set of polynomials F and a monomial set B until they stabilize. The update is done so that if a fixed-point is reached, then F is a border basis for the monomial set B.

The monomial set B is represented as a finite union of differences of cones $B = \cup_i \left(((m_i)) \setminus((m_{j_1})) \cdots \setminus((m_{j_{k'_i}}))\right)$. By construction, if $1 \in B$, then B is connected to 1. When a monomial m is removed from B, the corresponding cone $((m))$ is removed from the representation of B, so that B remains connected to 1.

Let us detail how Algorithm 4.1 is running. The procedure $Initialization(\mathcal{F})$ is used to find the initial degree k and the initial relations F_k of degree k and the associated monomial set B.

Algorithm 4.1: Border basis

Input: A set of Laurent polynomials $\mathcal{F} = \{f_1, \dots, f_s\}$ and γ a choice function refining the degree.

Output: A border basis for $I = (f_1, \dots, f_s)$.

- $[k, F_k, B] := Initialization(\mathcal{F})$
- While $not(is\_empty(F_k))$ or $k < \max_{f\in\mathcal{F}} \delta(f)$;

  core loop

  (1) Compute $C^1_{k+1} := \mathcal{C}^1_B(F_k)$ and $A_{k+1} := (B^\times)_{\leq k+1}$.

  (2) If there exists polynomials in C^1_{k+1} of degree $< k$, then
  - Compute the minimal l such that the ball of radius l contains polynomials of C^1_{k+1};
  - Using γ choose leading monomials for the polynomials of $\{f \in C^1_{k+1}, supp(f) \subset Ball(k)\}$;
  - Compute $C^1_l \cup \{f \in C^1_{k+1}, supp(f) \subset Ball(k)\}$
  - Set $k = l$;

  (3) Construct the matrix $M_{k+1} := (C^1_{k+1}|A_{k+1})$.

  (4) Compute $r_{k+1} := \operatorname{rank} M_{k+1}$.

  (5) If $\langle C^1_{k+1}\rangle$ contains polynomials of degree $< k+1$, add them to $\mathcal{F}$ and start a new loop with $k := \min_{p\in C^1_{k+1}} \delta(p)$.

  (6) If $\#(A_{k+1} \setminus B_{k+1}) \neq r_{k+1}$,
  - compute $A'_{k+1} \subset A_{k+1}$ such that $\#A'_{k+1} = r_{k+1} = \operatorname{rank}(F_{k+1} \mid A'_{k+1})$; for instance looking at the monomials indexing the columns of a maximal invertible submatrix of M_{k+1}.
  - compute $B'_{k+1} = A_{k+1} \setminus A'_{k+1}$;
  - add the monomials B'_{k+1} to B;

  (7) Define $\pi_{k+1} : \langle B^\times\rangle_{\leq k+1} \to \langle B\rangle_{\leq k+1}$ as the extension of π_k such that $C^1_{k+1} \subset \ker \pi_{k+1}$ and F_{k+1} as the new polynomials in the ball of radius $k+1$ in the corresponding rewriting family.

  (8) Compute $C^2_{k+1} := \pi_{k+1}(\mathcal{C}^2_B(F_k)) \cup \pi_{k+1}(\mathcal{F}_{k+1})$.

  (9) If $C^2_{k+1} = \{0\}$, then start a new loop with $k := k+1$.

  (10) If $\langle C^2_{k+1}\rangle$ contains polynomials in the ball of radius $< k+1$, add them to $\mathcal{F}$ and start a new loop with $k := \min_{p\in C^2_{k+1}} \delta(p)$.

  (11) Apply γ to $\langle C^2_{k+1}\rangle$, remove the monomial ideal generated by $\gamma(\langle C^2_{k+1}\rangle)$ from B and update $\pi_{k+1} : \langle B^\times\rangle_{\leq k+1} \to \langle B\rangle_{\leq k+1}$ and F_{k+1}, so that $C^2_{k+1} \subset \ker \pi_{k+1}$.

The core of the algorithm is a loop where the set of polynomials F_k and the monomial set B are updated. The variable k of each loop is the degree in which the polynomial operations are performed.

After computing the prolongation polynomials $\mathcal{C}^1(F_k)$ in step 1, the degree k is adjusted in step 2 to the maximal degree of these polynomials.

The coefficient matrix of these polynomials is computed in step 3, and used in step 4 and 5 to determine their rank and the minimal degree of a polynomial in the vector space that they span. The degree k is then adjusted to this minimal degree in a new loop.

Step 6 checks if there is a rank deficiency, that is, if the rank of the prolongation polynomials $\mathcal{C}^1(F_k)$ corresponds to the number of new monomials of ∂B in degree $k+1$. If there is a rank deficiency, the monomial set B is extended by new monomials so that there is no rank deficiency.

Step 7 constructs the projection and the rewriting family in degree $k+1$.

The steps 8, 9 compute the commutation polynomials $\mathcal{C}^2(F_k)$, the polynomial of degree $k+1$ of $\mathcal{F}$ and their remainders by the rewriting family in degree $k+1$.

The steps 10 and 11 checks if there polynomials of degree $< k+1$ in the vector space spanned by these remainders and update the degree and the monomial set B if needed.

As we can see, the degree k can either increase or drop to a lower value (in steps 2, 5 and 10).

The degree k is adjusted so that throughout the algorithm, the leading monomial of the polynomials in F_k is of degree $\leq k$.

The new algorithm does not required a large modification of the border basis algorithm of [20].

4.2. **Correctness.** We now prove that this algorithm stops and produces a border basis of the generators of a zero dimensional ideal, that is, a system of Laurent polynomials $\mathcal{F}$ such that $\dim \mathcal{A} < \infty$ where $\mathcal{A} = S/(\mathcal{F})$. A proof relying on the Noetherianity of monomial ideals (as for Gröbner bases) cannot be employed here since all non-zero monomial ideals of S are equal to (1).

We give here a lemma which is useful in the proof of correctness.

Lemma 4.4. *Let $k \in \mathbb{N}$ then $\ker(\pi_k)^\times \subset \ker \pi_{k+1}$.*

Proof. This comes from the fact that we construct π_{k+1} as a prolongation of π_k in step 7. □

We can now give the proof of termination and correctness of the algorithm. This proof relies heavily on the fact that γ refines the degree. It is new and simpler than the one given in [18].

Theorem 4.5. *If $\mathcal{F}$ is zero dimensionnal, i.e. $\dim S/(\mathcal{F}) < \infty$, then Algorithm 4.1 stops and returns a border basis $\mathcal{F}$ of $\mathcal{F}$ for a monomial set B.*

Proof. Let us first notice that if at anytime in the algorithm, the variable k is equal to 0 then the algorithm stops and returns the polynomial 1, which allows us to define the null projection.

We now remark that the construction of B is not monotonic: B can increase or decrease. However, the monomial set B is extended with new monomials only at step 6. At step 6, the algorithm is operating on polynomials of degree k, performing the prolongation operation $\cdot^x$ on them, checking that no non-zero remainder of degree less than $k+1$ have appeared and applying linear algebra steps. If some monomials are added to B, these monomials are the leading monomials of polynomials of degree $k+1$ and hence they are of degree $k+1$. This means that one cannot add to B a monomial of degree 1, otherwise we would have gone through degree 0. Hence there are finitely many `core loop` turns where $k = 1$.

Let us now prove by induction that for all $d \in \mathbb{N}$ there is finitely many `core loop` turns where $k = d$. This is true for $d = 1$. Let us suppose this is true for some d and prove it for $d+1$. Consider one `core loop` turn *after* the last loop turn where $k = d$ (this last turn exists due to our hypothesis). Then as mentioned in the above paragraph, not going any further with $k = d$, one will never add to B any monomial of degree $d+1$. We now remark that at the `core loop` considered, there are two possibilities:

- k is strictly below d and due to our induction hypothesis one will never reach degree $d+1$ since the degree $d+1$ can only be reached after a step at degree $k = d$,
- k is greater than d. In that case, k can become equal to $d+1$ only in case of a degree drop during subsequent `core loop` turns, and that dropping to degree $d+1$ implies removing from B at least one monomial of degree $d+1$. As there is only finitely many monomials of degree $d+1$, k cannot take infinitely many times the value $d+1$.

In these two cases, k can only be finitely many times equal to $d+1$ which ends our induction.

Let us show now that k is bounded during all the computation.

First remark that the B constructed by this algorithm is connected to 1, hence if in the `core loop` $k = d$, there is at least d monomials in B at that loop turn. Let $D = \dim S/(\mathcal{F}) < \infty$. If at any time k becomes greater than $D+1$ then there exists a polynomial in the ideal I whose support is included in the corresponding monomial set B. Let $p = p_1 f_1 + p_2 f_2 + \cdots + p_s f_s$ be this polynomial. Applying Lemma 4.4 inductively starting from $max(deg(f_i),\ i \in [1,s])$ up to $k' = max(deg(p_i f_i),\ i \in [1,s])$, one has that $p \in \ker(\pi_{k'})$. Hence $k' \geq k$ since π_k is the identity on B. Since $p \in \ker(\pi_{k'})$, there is at least one monomial of the support of p outside B when the `core loop` is ran with $k = k'$. Let m be this monomial, one have $deg(m) \leq D+1$ since B is connected

to 1. Therefore between the initial step when $k > D+1$ and the step when $k = k'$, k must drop to a degree less than $D+1$. Since there is finitely many drops possible below degree $D+1$ there is finitely many moment when $k > D+1$.

We deduce that k remains bounded and for each degree $d \in \mathbb{N}$, there is finitely many steps when $k = d$. This implies that the algorithm eventually stops.

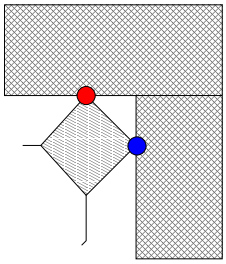
The termination of the algorithm follows from the inductive application of Lemma 4.4.

As the algorithm stops, say with $k = d$, all the monomials of ∂B_d are the leading monomial of an element of the rewriting family F_d. Since the monomial set B_d is not updated during the last loop of the algorithm, the commutation polynomials $\mathcal{C}^1_B(F_d)$, $\mathcal{C}^2_B(F_d)$ project to 0 by π_{d+1}. By Theorem 2.3, we deduce that F_d is a border basis for B_d. □

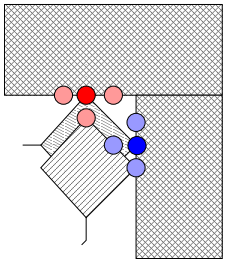
4.3. **Example.** Let us examine the behavior of the previous algorithm on a generic quadratic system of two equations in two variables, that is a system of generic Laurent polynomials which support is the set of integer points A of the convex hull of $(-2,0),(0,-2),(0,2),(2,0) \in \mathbb{Z}^2$.

Suppose that we use a Macaulay-like choice function, i.e., a function that chooses one monomial of highest partial degree.

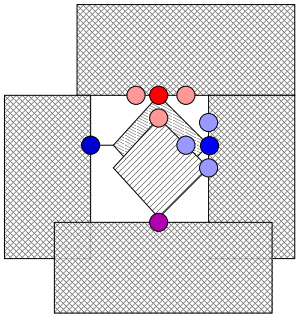
The *Initialization* procedure defines an initial monomial set B to be all the monomials except those of higher partial degree than 2 which graphically looks like:



The prolongation operation $^{\times}$ on this initial configuration produces six new polynomials, obtained by multiplying the equations by all the variables that either follow the border of B or get into it. We have drawn there leading monomials and the Newton polytope of one of them.



According to our test in the core loop, the new polynomial drawn is such that its leading monomial is not among the maximal degree monomials of the support. The other polynomial is also in this situation. So, according to the test done in step 2, two new leading monomials are chosen for these two polynomials and B is update accordingly.



The rest of the computation consists in following the border of this monomial set B in the same way as it is done in the generic polynomial setting [17].

The algorithm ends with a monomial set $B = \{x_1^{\alpha_1} x_2^{\alpha_2} \mid -2 \leq \alpha_1 < 2, -2 \leq \alpha_2 < 2\}$ of size 16, which is the normalized volume of A (i.e. $2 \times Vol(A)$). The corresponding border basis F is a set of 16 polynomials, one for each monomial of ∂B.

What occurs on this example of a generic 2 variate system can be generalized to n variate systems. The following table shows the sizes N of the different linear systems that have to be solved and the associated integer k in the main loop of the algorithm, for solving a system of n generic n variate Laurent polynomials of δ-degree 2 in each variable. For comparison, we give the size M of the matrix to be inverted in the Schur complement computation involved in the sparse resultant approach (see [1]).

n	N	M
2	$2, 6, 6, 2$	39
3	$3, 15, 30, 30, 15, 3$	475
4	$4, 28, 84, 140, 140, 84, 28, 4$	5165
5	$45, 180, 420, 630, 630, 420, 180, 45, 5$	54306
6	$6, 66, 330, 990, 1980, 2772, 2772, 1980, 990, 330, 66, 6$	566461

In this table, we clearly see the improvement of the toric border basis algorithm, compared to the sparse resultant method. Instead of solving one big linear system, the toric border basis computation involves the solution of several much smaller linear systems. This improves both the complexity and the numerical behaviour of the method.

5. Conclusion

Normal form methods provides an effective way to compute the quotient structure of a polynomial ring by an ideal, and thus to solve polynomial equations. The Gröbner basis approach consists in completing a set of rewriting rules on the monomials which is driven by a monomial ordering. Its extension to Laurent polynomials is difficult or expensive.

The border basis approach consists in imposing commutation relations to operators of multiplication, extending the rewriting techniques to a wider class of problems. We show in this paper, that the approach can naturally be extended to Laurent polynomials by imposing inversion and commutation relations to the multiplication operators. The border basis approach provides also a description of the first module of syzygies. This leads to a normal form algorithm for Laurent polynomials, which performs linear algebra operations on monomials with exponents in $\mathbb{Z}^n$.

If the ideal $(\mathcal{F})$ is a zero-dimensional ideal, we have shown the termination of the new algorithm. For ideal of positive dimension, we plan to investigate techniques based on regularity detection as in [20].

In this paper, we have considered Laurent polynomial rings, in which all the variables are invertible. We can check that the approach applies also to rings where only some of the variables are invertible, by considering the inversion relations for these variables and the commutation relations for all the pairs of variables.

This approach can be used to compute the solutions of a polynomial system outside a variety: $g(x_1, \ldots, x_n) \neq 0$. A new invertible variable x_{n+1} and the equation $x_{n+1} - g(x_1, \ldots, x_n) = 0$ can be introduced to compute the solutions of a system outside the hypersurface defined by g. We plan to investigate further applications of this toric border basis approach such as residual intersections and to compare it with saturation techniques for classical polynomial computation. We also plan to provide an implementation of this new algorithm in the package BORDERBASIX[1].

References

[1] J. Canny and I. Emiris. An efficient algorithm for the sparse mixed resultant. In G. Cohen, T. Mora, and O. Moreno, editors, *Proc. Intern. Symp. Applied Algebra, Algebraic Algor. and Error-Corr. Codes (Puerto Rico)*, volume 673 of *Lect. Notes in Comp. Science*, pages 89–104. Springer-Verlag, 1993.

[1] `mathemagix.org/www/borderbasix/doc/html/index.en.html`

[2] J.F. Canny and I.Z. Emiris. A subdivision-based algorithm for the sparse resultant. *J. ACM*, 47(3):417–451, May 2000.
[3] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2nd edition, 1997.
[4] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer-Verlag, New York, 1997.
[5] C. D'Andrea. Macaulay style formulas for sparse resultants. *Trans. Amer. Math. Soc.*, 354:2595–2629, 2002.
[6] D. Eisenbud. *Commutative Algebra with a view toward Algebraic Geometry*, volume 150 of *Graduate Texts in Math.* Berlin, Springer-Verlag, 1994.
[7] M. Elkadi and B. Mourrain. *Introduction à la résolution des systèmes polynomiaux*, volume 59 of *Mathématiques et Applications*. Springer, 2007.
[8] I.Z. Emiris and A. Rege. Monomial bases and polynomial system solving. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC '94, pages 114–122, New York, NY, USA, 1994. ACM.
[9] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Boston, Birkhäuser, 1994.
[10] S. Kaspar. Computing border bases without using a term ordering. *Beiträge zur Algebra und Geometrie / Contributions to Algebra and Geometry*, pages 1–13, 2011.
[11] A. Kehrein and M. Kreuzer. Characterizations of border bases. *J. Pure Appl. Algebra*, 196(2-3):251–270, 2005.
[12] A. Kehrein and M. Kreuzer. Computing border bases. *J. Pure Appl. Algebra*, 205(2):279–295, 2006.
[13] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 2*. Springer, Heidelberg, 2005.
[14] F.S. Macaulay. Some formulae in elimination. *Proc. London Math. Soc.*, 1(33):3–27, 1902.
[15] B. Mourrain. A new criterion for normal form algorithms. In M. Fossorier, H. Imai, Shu Lin, and A. Poli, editors, *Proc. AAECC*, volume 1719 of *LNCS*, pages 430–443. Springer, Berlin, 1999.
[16] B. Mourrain. *Symbolic-Numeric Computation*, chapter Pythagore's Dilemma, Symbolic-Numeric Computation, and the Border Basis Method, pages 223–243. Trends in Mathematics. Birkhäuser, 2007.
[17] B. Mourrain and Ph. Trébuchet. Solving projective complete intersection faster. In C. Traverso, editor, *Proc. Intern. Symp. on Symbolic and Algebraic Computation*, pages 231–238. New-York, ACM Press., 2000.
[18] B. Mourrain and Ph. Trébuchet. Generalised normal forms and polynomial system solving. In M. Kauers, editor, *International Conference on Symbolic and Algebraic Computation*, pages 253–260, Beijing, China, 2005. ACM New York, NY, USA.
[19] B. Mourrain and Ph. Trébuchet. Stable normal forms for polynomial system solving. *Theoretical Computer Science*, 409(2):229–240, 2008.
[20] B. Mourrain and Ph. Trébuchet. Border basis representation of a general quotient algebra. In *International Conference on Symbolic and Algebraic Computation (ISSAC)*, pages 265–272, Grenoble, France, July 2012. ACM Press.
[21] B. Sturmfels. Sparse elimination theory. In D. Eisenbud and L. Robbiano, editors, *Proc. Computat. Algebraic Geom. and Commut. Algebra 1991*, pages 264–298, Cortona, Italy, 1993. Cambridge Univ. Press.