Master Thesis


A polynomial matrix version of Lazard's Gröbner basis algorithm

Robin Kouba

December 14, 2023

Supervisors:
Vincent Neiger, Mohab Safey El Din
PolSys, Lip6

Contents

1 Introduction

Context and Prior results. The resolution of multivariate polynomial systems is a major issue in many domains as cryptography [12] and robotics [13] for example. A geometric algebra approach to this NP-Hard problem is to consider that a system of polynomial equations is associated with an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. A Gröbner basis of an ideal is essentially an equivalent polynomial system that has a triangular structure which makes it much easier to solve . This point of view raises questions such as the unique representation of a polynomial in the quotient ring $\mathbb{K}[x_1, \ldots, x_n]/I$. The notion of Gröbner basis also depends on an ordering on monomials. This allows to define the leading terms of a multivariate polynomial and a division algorithm. The first algorithm to compute Gröbner basis have been introduced by Buchberger in 1965 [4]. His idea was to consider some pairs of polynomials and to consider the reduction of S-polynomials. Later, in 1983, D. Lazard has proposed an algorithm in [15] to compute Gröbner basis using tools of computational linear algebra. The linearization of this problem is made by building a large matrix with entries in $\mathbb{K}$ and computing its echelon form. One of the major result is the Macaulay bound form Lazard [15], it gives an explicit degree D that majorize the size of the Matrix in Lazard's algorithm with a hypothesis that the sequence $(f_1, \ldots, f_s)$ is regular. Another of the hypothesis to use this bound is to work with the grevlex ordering. The original Lazard's algorithm uses $\mathcal{O}\left(\binom{D+n}{n}^{\omega-1} n \binom{D-d+n}{n}\right)$ operations in $\mathbb{K}$ to compute a Gröbner basis where d is the degree of the considered polynomials under the above assumption.

By combining the ideas of those two algorithms, Faugère created the Algorithm F4 in 1998 [9], a new algorithm that performs much better than the previous ones in practice. In 2002, the Algorithm F5 has been proposed by Faugère that cost $\mathcal{O}\left(\binom{D+n-1}{D}^{\omega}\right)$ operations in $\mathbb{K}$ [10] . The advantage of F5 is that the matrices have full rank generically.

The goal of the internship is to create a version of Lazard's algorithm that uses univariate matrices with entries in $\mathbb{K}[x_n]$. Such matrices are smaller as one of the variables is in the matrices.

The Popov's forms of univariate matrices are the generalizations of the row echelon form for matrices with entries in $\mathbb{K}$. For a matrix of degree d in $\mathbb{K}[t]^{r\times c}$, the computation of its Popov form takes $\mathcal{O}^{\sim}(r^{\omega-1}c(d+\mathrm{amp}(s)))$ with s a row vector called the shift which is a parameter of the Popov's form [16, Section 1,Section 5.1]. The price of the computation of Popov's forms is obviously higher than for the row echelon form but the structure of the matrices in $\mathbb{K}[x_n]$ and the distribution of the degree in them offer a lot of ideas for some improvements.

As Lazard's Algorithm use the row echelon form, it is natural to consider

Popov's forms to adapt this algorithm. This idea come from a recent work by Berthomieu, Neiger and Safey El Din on change of order algorithms for Gröbner basis [3]. This work go forward the FGLM Algorithm which change the order of a Gröbner basis by considering a link between the multiplication matrices and univariate matrices that are in a Popov's form.

Contribution. One of the main results of this internship is the following theorem that shows a fundamental relation between Popov's form and Gröbner basis.

Theorem 1. *Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n, t]$, let $\succ_{grlext}$ be the grevlex ordering on the ring $\mathbb{K}[x_1, \ldots, x_n, t]$ and $\succ_{grlex}$ the grevlex ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Let $(g_1, \ldots, g_\ell)$ be a Gröbner basis of $(I, \succ_{grlext})$. Then the representative matrix of G is in s-weak-Popov form.*

The adaptation of Lazard's algorithm is the Algorithm 4 given in Section 4.2 and it uses the s-Popov form with s the shift described in the above theorem. Finally, the number of operations in $\mathbb{K}$ for this new algorithm is discribed in the following theorem.

Theorem 2. *Let $F = (f_1, \ldots, f_\ell)$ be a regular sequence of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ with $\deg(f_i) = d_i$. Suppose $\langle f_1, \ldots, f_\ell \rangle$ is zero dimensional. Write $D = \sum_{i=1}^{\ell}(d_i - 1) + 1$. The number of operations in $\mathbb{K}$ that Algorithm 4 uses is*

$$\mathcal{O}^{\sim}\left(n\binom{D-d+n-1}{n-1}\binom{D+n-1}{n-1}^{\omega-1}(d+D)\right).$$

The ratio between the complexity of the classical Lazard's algorithm above and the new algorithm underneath is nearly $\frac{d^{\omega-1}}{n}$. This improves on the state of art for families of problems of fixed number of variables and increasing degree.

Perspectives. There is still some work on this algorithm to do, we have good reason to think that we could obtain $d^{\omega-1}$ as new ratio for future algorithm. It came from the complexity of s-Popov form when s is zero. With genericity hypothesis, the shift zero could be used thanks to the row echeloned by block structure of the Macaulay matrix. Moreover, there exists some results of complexity that uses the averge degree on columns which could improve the complexity of Algorithm 4 [19].

Structure of the document. Section 2 is devoted to preliminaries on polynomial matrices and Gröbner basis. Section 3 introduces different versions of Lazard's algorithm and its complexity. Section 4 generalizes the algorithm for polynomial matrices by explaining the link between monomial ordering and Popov form.

2 Basic definitions and preliminary results

2.1 Echelon forms of matrices over a field

For this subsection, we refer the reader to [7] for more details. Let $\mathbb{K}$ be a field. The set of matrices over $\mathbb{K}$ with r rows and c columns is written $\mathbb{K}^{r\times c}$.

Definition 2.1. *A matrix $M \in \mathbb{K}^{r\times c}$ is in* row echelon form *if*

1) Each zero row of the matrix is below all the nonzero rows.

2) On each nonzero row, the leftmost nonzero entry is strictly to the right of those of the rows above. Those entries are called pivots *of the matrix M.*

Moreover, the matrix M is in reduced row echelon form *if Items 1) and 2) hold and*

3) In each column that contains a pivot, all entries other than this pivot are zeros.

4) All pivots are equal to 1.

In particular, a nonzero row vector $A = (a_i)_{1\leq i\leq c} \in \mathbb{K}^{1\times c}$ is in row echelon form. There exists $i_0 \in \{1,\dots,c\}$ such that a_{i_0} is the pivot of A.

By Gaussian elimination, every matrix can be row echelonized.

Proposition-Definition 2.2. *Let M be in $\mathbb{K}^{r\times c}$. There exists a matrix A in $\mathbb{K}^{r\times r}$ invertible such that AM is in row echelon form. In that case, we call AM* a row echelon form *of M. If the product AM is in reduced row echelon form, it is* a reduced row echelon form *of M.*

This theorem can be found in [7, Theorem 1.2].

Theorem 2.3. *Let M be in $\mathbb{K}^{r\times c}$. There exists a unique reduced row echelon form of M.*

Proposition 2.4. *Let $M = (m_{i,j})_{1\leq i\leq r, 1\leq j\leq c}$ be in $\mathbb{K}^{r\times c}$ and $A = (a_i)_{1\leq i\leq r}$ be a vector in $\mathbb{K}^{1\times r}$. Suppose that the matrix M is in row echelon form. If the pivot of the vector $B = AM = (b_j)_{1\leq j\leq c}$ is b_{j_0} for some $j_0 \in \{1,\dots,c\}$, then there exists $i_0 \in \{1,\dots,r\}$ such that m_{i_0,j_0} is a pivot of M.*

Proof. For i in $\{1,\dots,r\}$, write $M_i \in \mathbb{K}^{1\times c}$ for the i-th row of the matrix M, so that $AM = \sum_{i=1}^{r} a_i M_i$. Let E_1 be the subset of $\{1,\dots,r\}$ that contains all row indices of pivots of M whose column indices are in $\{1,\dots,j_0-1\}$. Let E_2 be the subset of $\{1,\dots,r\}$ that contains all row indices of pivots of M whose column indices are in $\{j_0,\dots,c\}$. Then we can write :

$$AM = \sum_{i\in E_1} a_i M_i + \sum_{i\in E_2} a_i M_i.$$

By considering the smallest element of E_1, and using the fact that pivot indices in M are increasing, we see that the first sum is zero. By considering the smallest element of E_2 and calling it i_0, we are done. □

2.2 Hermite forms of polynomial matrices

In this subsection, we introduce some notions about polynomial matrices, which are matrices with univariate polynomial entries. Let $\mathbb{K}$ be a field. We write $\mathbb{K}[t]^{r\times c}$ the set of univariate polynomial matrices with r rows and c columns and entries in $\mathbb{K}[t]$. The following definition can be found in [17, Definition 1].

Definition 2.5. *Let M be in $\mathbb{K}[t]^{r\times c}$. The matrix M is said to be in* weak-Hermite form *if*

1) Each zero row of the matrix is below all the nonzero rows.

2) On each nonzero row, the leftmost nonzero entry is strictly to the right of those of the rows above. Those entries are called pivots *of the matrix M.*

Moreover, the matrix M is in reduced row echelon form *if Items 1) and 2) hold and*

3) All other entries on a column that contain a pivot have lower degrees than the pivot.

4) All pivots are monic.

Note that the name "weak-Hermite" does not appear in the literature, this has been chosen to make a parallel with Section 2.3.

Example 2.6. *The matrix $M_1 \in \mathbb{Q}[t]^{3\times 4}$ is in weak-Hermite form:*

$$M_1 = \begin{pmatrix} t+1 & t^2+2t & t^2+1 & 7 \\ 0 & 0 & 2t & 4t \\ 0 & 0 & 0 & t^4-1 \end{pmatrix}$$

but it is not in Hermite form because neither Item 3) nor Item 4) holds. Indeed $\deg(2t) \leq \deg(t^2+1)$ and $2t$ is not monic in the third column.

A square matrix A in $\mathbb{K}[t]^{r\times r}$ is said to be *unimodular* if it is invertible over $\mathbb{K}[t]$ (i.e., A^{-1} has entries in $\mathbb{K}[t]$, or equivalently, $\det(A) \in \mathbb{K}\setminus\{0\}$). It is said to be *nonsingular* if it is invertible over the field of fractions $\mathbb{K}(t)$, or equivalently, if $\det(A) \in \mathbb{K}[t]\setminus\{0\}$.

Proposition-Definition 2.7. *Let M be in $\mathbb{K}[t]^{r\times c}$. There exists a unimodular matrix A in $\mathbb{K}[t]^{r\times r}$ such that AM is in weak-Hermite form. In that case, we call AM* a weak-Hermite form *of M. If AM is in Hermite form, it is* a Hermite form *of M.*

Example 2.8. *Let M be in $\mathbb{Q}[t]^{3\times 4}$ and A be in $\mathbb{Q}[t]^{3\times 3}$:*

$$M = \begin{pmatrix} t+1 & t^2+2t & t^2+1 & 7 \\ 0 & 0 & 2t & 4t \\ t^2+t & t^3+2t^2 & t^3+t & t^4+7t-1 \end{pmatrix} \text{ and } A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -t & 0 & 1 \end{pmatrix}.$$

The matrix M is not in weak-Hermite form but:

$$M_1 = AM = \begin{pmatrix} t+1 & t^2+2t & t^2+1 & 7 \\ 0 & 0 & 2t & 4t \\ 0 & 0 & 0 & t^4-1 \end{pmatrix}$$

is in weak-Hermite form.

The following theorem can be found in [17, Theorem 1].

Theorem 2.9. *Let M be in $\mathbb{K}[t]^{r\times c}$. There exists a unique Hermite form of M.*

Example 2.10. *The matrix M_1 is a weak-Hermite form of M but not the Hermite form of M. We can get the Hermite form as follows :*

$$\begin{aligned} M_2 &= \begin{pmatrix} 1 & -\frac{1}{2}t & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} t+1 & t^2+2t & t^2+1 & 7 \\ 0 & 0 & 2t & 4t \\ 0 & 0 & 0 & t^4-1 \end{pmatrix} \\ &= \begin{pmatrix} t+1 & t^2+2t & 1 & -2t^2+7 \\ 0 & 0 & t & 2t \\ 0 & 0 & 0 & t^4-1 \end{pmatrix}. \end{aligned}$$

The matrix $M_2 \in \mathbb{Q}[t]^{3\times 4}$ is the unique Hermite form of M.

Proposition 2.11. *The rows of a matrix M in $\mathbb{K}[t]^{r\times c}$ generate a $\mathbb{K}[t]$-submodule of $\mathbb{K}[t]^{1\times c}$. If $A \in \mathbb{K}[t]^{r\times r}$ is unimodular, then the rows of AM generates the same $\mathbb{K}[t]$-submodule as those of M.*

Proof. Let $N = AM$, the rows of N are $\mathbb{K}[t]$-linear combinations of rows of M. Then the $\mathbb{K}[t]$-submodule generated by the rows of N is included in the $\mathbb{K}[t]$-submodule generated by the rows of M. We have the other inclusion by the same argument using $A^{-1}N = M$, where $A^{-1} \in \mathbb{K}[t]^{r\times r}$ since the matrix A is unimodular. □

Proposition 2.12. *Let $M = (m_{i,j})_{1\le i\le r, 1\le j\le c}$ be in $\mathbb{K}[t]^{r\times c}$ and $A = (a_j)_{1\le j\le r}$ be in $\mathbb{K}[t]^{1\times r}$. Suppose that M is in weak-Hermite form. If the pivot of the vector $B = AM = (b_j)_{1\le j\le c}$ is b_{j_0} for some $j_0 \in \{1,\dots,c\}$, then there exists $i_0 \in \{1,\dots,r\}$ such that m_{i_0,j_0} is a pivot of M. Moreover, the inequality $\deg(b_{j_0}) \ge \deg(m_{i_0,j_0})$ holds.*

Proof. Using the same arguments as those in the proof of Proposition 2.4, we get

$$AM = \sum_{i\in E_1} a_i M_i + \sum_{i\in E_2} a_i M_i = a_{i_0} M_{i_0} + \sum_{i\in E_2\setminus\{i_0\}} a_i M_i,$$

where E_1 is the subset of $\{1,\dots,r\}$ that contains all row indices of pivots of M whose column indices are in $\{1,\dots,j_0-1\}$, E_2 is the subset of $\{1,\dots,r\}$ that contains all row indices of pivots of M whose column indices are in $\{j_0,\dots,c\}$, and i_0 is the smallest element of E_2. By definition of a pivot we have that for all $i \in E_2\backslash\{i_0\}$, the entry m_{i,j_0} is zero. Then we see that $b_{j_0} = a_{i_0} m_{i_0,j_0}$, hence $\deg(b_{j_0}) = \deg(m_{i_0,j_0}) + \deg(a_{i_0})$. □

2.3 Shifted Popov forms of polynomial matrices

For more details on the notion of Popov's forms, we refer the reader to [16]. Popov's forms are a generalization of Hermite form, in [16, chapter 2] you can see that the Hermite form of a matrix can be seen as a Popov form. The row echelon form is an essential tool for Lazard's algorithm and Popov's forms are a generalization of the row echelon form. We can then establish a relation between Popov's forms and Gröbner basis.

Definition 2.13. *Let $M = (m_{i,j})_{1\le i\le r, 1\le j\le c}$ be in $\mathbb{K}[t]^{r\times c}$. The* row degree *of M is the vector $\mathrm{rdeg}_0(M) = (d_1,\dots,d_r)$ where*

$$d_i = \max_{j\in\{1,\dots,c\}} (\deg(m_{i,j})) \in \mathbb{N}\cup\{-\infty\}.$$

Example 2.14. *Let $M_2 \in \mathbb{Q}[t]^{3\times 4}$ be the Hermite form of M:*

$$M_2 = \begin{pmatrix} t+1 & t^2+2t & 1 & -2t^2+7 \\ 0 & 0 & t & 2t \\ 0 & 0 & 0 & t^4-1 \end{pmatrix}.$$

The row degree of M_2 is the row vector

$$\mathrm{rdeg}_0(M) = (2,1,4).$$

Definition 2.15. *Let M be in $\mathbb{K}[t]^{r\times c}$. A* shift *$s = (s_1,\dots,s_c)$ is an element of $\mathbb{Z}^{1\times c}$. We define $\mathrm{amp}(s) = \max(s_1,\dots,s_c) - \min(s_1,\dots,s_c)$.*

Definition 2.16. *Let $M = (m_{i,j})_{1\le i\le r, 1\le j\le c}$ be in $\mathbb{K}[t]^{r\times c}$ and the shift s in $\mathbb{Z}^{1\times c}$. For $1\le i\le r$, we define $d_i = \max_{j\in\{1,\dots,c\}}(\deg(m_{i,j}) + s_j)$. The* s-row degree *of M is the vector $\mathrm{rdeg}_s(M) = (d_1,\dots,d_r)$.*

Example 2.17. *Let $s = (4,2,0,1)$ be a shift,*

$$M_2 = \begin{pmatrix} t+1 & t^2+2t & 1 & -2t^2+7 \\ 0 & 0 & t & 2t \\ 0 & 0 & 0 & t^4-1 \end{pmatrix} \in \mathbb{Q}[t]^{3\times 4}.$$

The s-row degree of the matrix M_2 is the row vector

$$\mathrm{rdeg}_s(M) = (5,2,5).$$

Definition 2.18. *Let $M = (m_{i,j})_{1\leq i\leq r, 1\leq j\leq c}$ be a matrix in $\mathbb{K}[t]^{r\times c}$ with $a_{i,j}$ the leading coefficient of the polynomial $m_{i,j}$, let $s \in \mathbb{Z}^{1\times c}$ and $\mathrm{rdeg}_s(M) = (d_1, \ldots, d_r)$. The* leading matrix *of M for the shift s is $L = \mathrm{LM}_s(M) = (\ell_{i,j})_{1\leq i\leq r, 1\leq j\leq c}$ with $\ell_{i,j} = 0$ if $\deg(m_{i,j}) + s_j < d_i$ and $\ell_{i,j} = a_{i,j}$ if $\deg(m_{i,j}) + s_j = d_i$. For the polynomial 0, the leading coefficient is 0 by convention.*

Example 2.19. *Let us consider the shift $s = (3, 2, 0, 1)$ and the matrix*

$$M_2 = \begin{pmatrix} t+1 & t^2+2t & 1 & -2t^2+7 \\ 0 & 0 & t & 2t \\ 0 & 0 & 0 & t^4-1 \end{pmatrix}.$$

The s-row degree of M_2 for the shift s is the row vector

$$\mathrm{rdeg}_s(M) = (4, 2, 5).$$

The leading matrix of M for the shift s is the matrix

$$\mathrm{LM}_s(M) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Definition 2.20. *Let M be in $\mathbb{K}[t]^{r\times c}$. If $\mathrm{LM}_s(M)$ is full rank, then the matrix M is said to be* s-reduced.

Definition 2.21. *Let $M = (m_{i,j})_{1\leq i\leq r, 1\leq j\leq c}$ be a matrix in $\mathbb{K}[t]^{r\times c}$, M is said to be in* s-weak-Popov form *if $L = \mathrm{LM}_s(M) = (\ell_{i,j})_{1\leq i\leq r, 1\leq j\leq c}$ is row echelonized. If $\ell_{i,j}$ is a pivot of $\mathrm{LM}_s(M)$, we call the entry $m_{i,j}$ a s-pivot of M.*

Definition 2.22. *The matrix $M = (m_{i,j})_{1\leq i\leq r, 1\leq j\leq c}$ is said to be in* s-Popov form *with $s \in \mathbb{Z}^{1\times c}$ if*

1) *The matrix M is in s-weak-Popov form.*
2) *For each pivot $m_{i,j}$ of M, We have $\deg(m_{i,j}) > \deg(m_{k,j})$ for all indices k in $\{1, \ldots, r\}\backslash\{i\}$.*
3) *All pivots are monic.*

Proposition 2.23. *Let M be in $\mathbb{K}[t]^{r\times c}$ and s in $\mathbb{Z}^{1\times c}$. There exists a matrix A in $\mathbb{K}[t]^{r\times r}$ unimodular such that AM is in s-weak-Popov form. We call AM* a s-weak-Popov form *of M. If AM is in s-Popov form, it is* a s-Popov form *of M.*

The following theorem can be found in [2, page 716 theorem 2.7].

Theorem 2.24. *Let M be in $\mathbb{K}[t]^{r\times c}$ and $s \in \mathbb{Z}^{1\times c}$. There exists a unique s-Popov form of M.*

Lemma 2.25. *Let $M = (m_{i,j})_{1\leq i\leq r, 1\leq j\leq c}$ be a matrix in $\mathbb{K}[t]^{r\times c}$ and $A = (a_i)_{1\leq i\leq r}$ a vector in $\mathbb{K}[t]^{1\times r}$ with $A \neq 0$. Suppose that M is in s-weak-Popov form with s in $\mathbb{Z}^{1\times c}$ and M has no zero row. Write the vector $B = AM = (b_i)_{1\leq i\leq c}$ and $\sigma : \{1,\dots,r\} \to \{1,\dots,c\}$ the application such that the entry $m_{i,\sigma(i)}$ is a s-pivot of M. Let i_0 be the smallest integer of the set*

$$E = \{i \in \{1,\dots,r\} | d_i + \deg(a_i) = \max_{k\in\{1,\dots,r\}}(d_k + \deg(a_k))\}.$$

Then

(i) The equality

$$\deg(b_{\sigma(i_0)}) = \deg(a_{i_0}) + \deg(m_{i_0,\sigma(i_0)}).$$

(ii) The entry $b_{\sigma(i_0)}$ is the s-pivot of the vector AM.

Proof of Item (i). First, as M and A have no zero row, there exists k in $\{1,\dots,r\}$ such that $d_k+\deg(a_k)$ is positive. Then $\max_{k\in\{1,\dots,r\}}(d_k+\deg(a_k))$ is positive. Moreover, $E \neq \emptyset$ so i_0 is well defined. Let us write the s-row degree $\mathrm{rdeg}_s(M) = (d_1,\dots d_r)$. By the definition of a s-pivot, we have the equality $d_i = \deg(m_{i,\sigma(i)}) + s_{\sigma(i)}$ because M is s-weak Popov. As $b_{\sigma(i_0)} = \sum_{i=1}^{r} a_i m_{i,\sigma(i_0)}$, then we need to show that for all indices i in $\{1,\dots,r\}\backslash\{i_0\}$:

$$\deg(a_i) + \deg(m_{i,\sigma(i_0)}) < \deg(a_{i_0}) + \deg(m_{i_0,\sigma(i_0)}).$$

- If $i \in \{i_0+1,\dots,r\}$, then $d_i+\deg(a_i) \leq d_{i_0}+\deg(a_{i_0})$ because $i_0 \in E$ and $s_{\sigma(i_0)}+\deg(m_{i,\sigma(i_0)}) < d_i$ because M is in s-weak-Popov form and $\sigma(i_0) < \sigma(i)$. So we can write:

$$\begin{aligned}\deg(a_i) + \deg(m_{i,\sigma(i_0)}) + s_{\sigma(i_0)} &< \deg(a_i) + d_i \\ &\leq \deg(a_{i_0}) + d_{i_0}.\end{aligned}$$

  As $\deg(a_{i_0}) + d_{i_0} = \deg(a_{i_0}) + \deg(m_{i_0,\sigma(i_0)}) + s_{\sigma(i_0)}$ by the definition of d_{i_0}, then :

$$\deg(a_i) + \deg(m_{i,\sigma(i_0)}) + s_{\sigma(i_0)} < \deg(a_{i_0}) + \deg(m_{i_0,\sigma(i_0)}) + s_{\sigma(i_0)}$$

  which implies that

$$\deg(a_i) + \deg(m_{i,\sigma(i_0)}) < \deg(a_{i_0}) + \deg(m_{i_0,\sigma(i_0)}).$$

- If we have $i \in \{1,\dots,i_0-1\}$, it holds that $\deg(a_i)+d_i < \deg(a_{i_0})+d_{i_0}$ because i is not an element of E as i_0 is the smallest integer of E. By the definition of d_i, it holds that $\deg(m_{i,\sigma(i_0)}) + s_{i_0} \leq d_i$. So we can write:

$$\begin{aligned}\deg(a_i) + \deg(m_{i,\sigma(i_0)}) + s_{\sigma(i_0)} &\leq \deg(a_i) + d_i \\ &< \deg(a_{i_0}) + d_{i_0}.\end{aligned}$$

As $\deg(a_{i_0}) + d_{i_0} = \deg(a_{i_0}) + \deg(m_{i_0,\sigma(i_0)}) + s_{\sigma(i_0)}$, then :

$$\deg(a_i) + \deg(m_{i,\sigma(i_0)}) + s_{\sigma(i_0)} < \deg(a_{i_0}) + \deg(m_{i_0,\sigma(i_0)}) + s_{\sigma(i_0)}$$

which implies that

$$\deg(a_i) + \deg(m_{i,\sigma(i_0)}) < \deg(a_{i_0}) + \deg(m_{i_0,\sigma(i_0)}).$$

We deduce that $\deg(b_{\sigma(i_0)}) = \deg(a_{i_0}) + \deg(m_{i_0,\sigma(i_0)})$.

□

Proof of Item (ii). Let us compare $\deg(b_j) + s_j$ and $\deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}$ for j in $\{1, \ldots, c\}$.

- If j is in $\{\sigma(i_0) + 1, \ldots, c\}$, as $b_j = \sum_{i=1}^{r} a_i m_{i,j}$, then we can write:

$$\begin{aligned}\deg(b_j) + s_j &\leq \max_{i\in\{1,\ldots,r\}} (\deg(m_{i,j}) + \deg(a_i) + s_j) \\ &\leq \max_{i\in\{1,\ldots,r\}} (d_i + \deg(a_i)) \\ &\leq d_{i_0} + \deg(a_{i_0}),\end{aligned}$$

  so it holds that $\deg(b_j) + s_j \leq d_{i_0} + \deg(a_{i_0})$. By Lemma 2.25, the following equalities hold:

$$d_{i_0} + \deg(a_{i_0}) = s_{\sigma(i_0)} + \deg(m_{i_0,\sigma(i_0)}) + \deg(a_{i_0}) = \deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}.$$

  We deduce that $\deg(b_j) + s_j \leq \deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}$.
- If j is in $\{1, \ldots, \sigma(i_0) - 1\}$, we need to show that:

$$\deg(b_j) + s_j < \deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}.$$

  As $b_j = \sum_{i=1}^{r} a_i m_{i,j}$, then we can write

$$\deg(b_j) + s_j \leq \max_{i\in\{1,\ldots,r\}} (\deg(m_{i,j}) + \deg(a_i) + s_j).$$

  We need to show that for all $i \in \{1, \ldots, r\}$:

$$\deg(m_{i,j}) + \deg(a_i) + s_j < \deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}.$$

  First, if $i \in \{1, \ldots, i_0 - 1\}$:

$$\begin{aligned}\deg(m_{i,j}) + \deg(a_i) + s_j &\leq \deg(a_i) + d_i \\ &< \deg(a_{i_0}) + d_{i_0}, \text{ as } i < i_0.\end{aligned}$$

  As $d_{i_0} + \deg(a_{i_0}) = \deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}$, then

$$\deg(m_{i,j}) + \deg(a_i) + s_j < \deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}.$$

If $i \in \{i_0, \ldots, r\}$:

$$\begin{aligned}\deg(m_{i,j}) + \deg(a_i) + s_j &< \deg(a_i) + d_i, \text{ as } j < \sigma(i)\\ &\leq \deg(a_{i_0}) + d_{i_0}.\end{aligned}$$

As $d_{i_0} + \deg(a_{i_0}) = \deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}$, then

$$\deg(m_{i,j}) + \deg(a_i) + s_j < \deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}.$$

As for all $j \in \{\sigma(i_0)+1, \ldots, c\}$, $\deg(b_j) + s_j \leq \deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}$ and for all $j \in \{1, \ldots, \sigma(i_0)-1\}$, $\deg(b_j) + s_j < \deg(b_{\sigma(i_0)}) + s_{\sigma(i_0)}$, then $b_{\sigma(i_0)}$ is the s-pivot of the vector AM.

□

Proposition 2.26. *Let $M = (m_{i,j})_{1\leq i\leq r, 1\leq j\leq c}$ be a matrix in $\mathbb{K}[t]^{r\times c}$ and $A = (a_i)_{1\leq i\leq r}$ be a vector in $\mathbb{K}[t]^{1\times r}$ with $A \neq 0$. Suppose that M is in s-weak-Popov form with s in $\mathbb{Z}^{1\times c}$ and M have no zero row. Write the vector $B = AM = (b_i)_{1\leq i\leq c}$. If b_{j_0} is the s-pivot of B, then there exists $i_0 \in \{1, \ldots, r\}$ such that m_{i_0,j_0} is a s-pivot of M and $\deg(b_{j_0}) \geq \deg(m_{i_0,j_0})$.*

Proof. The first assertion is a restatement of Item (ii) of Lemma 2.25. We have to prove that $\deg(b_{\sigma(i_0)}) \geq \deg(m_{i_0,\sigma(i_0)})$. By Item (i) of Lemma 2.25 we have the equality $\deg(b_{\sigma(i_0)}) = \deg(m_{i_0,\sigma(i_0)}) + \deg(a_{i_0})$. We have already seen that $\max_{k\in\{1,\ldots,r\}}(d_k + \deg(a_k))$ is positive in the beginning of the proof of Item (i) and by hypothesis we have $i_0 \in E$. Then $\deg(a_{i_0})$ is positive.

□

2.4 Admissible monomial orderings

For more details on admissible monomial orderings, we refer the reader to [8, chapter 2]. Let $\mathbb{K}$ be a field and consider the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ be a vector in $\mathbb{N}^n$, the monomial $\prod_{i=1}^n x_i^{\alpha_i}$ is written $\boldsymbol{x}^{\boldsymbol{\alpha}}$ and $|\boldsymbol{\alpha}| = \sum_{i=1}^n \alpha_i$ is its degree.

Definition 2.27. *An* admissible monomial ordering $\succ$ *is a total ordering on the monomials such that*

(i) If $\boldsymbol{x}^{\boldsymbol{\alpha}} \succ \boldsymbol{x}^{\boldsymbol{\beta}}$ then for any $\boldsymbol{\gamma} \in \mathbb{N}^n$ we have $\boldsymbol{x}^{\boldsymbol{\alpha}+\boldsymbol{\gamma}} \succ \boldsymbol{x}^{\boldsymbol{\beta}+\boldsymbol{\gamma}}$.

(ii) Every nonempty subset of $\mathbb{N}^n$ has a smallest element for $\succ$.

For a total order on monomial of $\mathbb{K}[x_1, \ldots, x_n]$ that respects Item (i), Item (ii) is equivalent to the following assertion: for any $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^n$, if $\boldsymbol{x}^{\boldsymbol{\alpha}}$ divides $\boldsymbol{x}^{\boldsymbol{\beta}}$ then $\boldsymbol{x}^{\boldsymbol{\beta}} \succcurlyeq \boldsymbol{x}^{\boldsymbol{\alpha}}$.

Notation 2.28. *For a polynomial p and an admissible monomial ordering $\succ$ we write $\mathrm{lm}_\succ(p), \mathrm{lt}_\succ(p)$ and $\mathrm{lc}_\succ(p)$ the* leading monomial*, term and coefficient of p w.r.t $\succ$.*

Definition 2.29. *An admissible monomial ordering* $\succ$ *on* $\mathbb{K}[x_1, \ldots, x_n]$ *is called* an elimination ordering *in* $\{x_k, \ldots, x_n\}$ *with* $k \in \{1, \ldots, n\}$ *if for all polynomials* f *in* $\mathbb{K}[x_1, \ldots, x_n]$, $\mathrm{lm}_{\succ}(f) \in \mathbb{K}[x_k, \ldots, x_n]$ *implies that* $f \in \mathbb{K}[x_k, \ldots, x_n]$.

Definition 2.30. *Consider two disjoint sets of variables* $\{x_1, \ldots, x_n\}$ *and* $\{y_1, \ldots, y_m\}$ *with admissible monomial orderings* $\succ_x$ *and* $\succ_y$ *on each. We define the admissible monomial ordering* $(\succ_x, \succ_y) = \succ$ *on monomials of* $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ *as follows.*

Let the following exponents $\boldsymbol{\alpha}_x$, $\boldsymbol{\beta}_x$ *be in* $\mathbb{N}^n$ *and* $\boldsymbol{\alpha}_y$, $\boldsymbol{\beta}_y$ *be in* $\mathbb{N}^m$. *Let* $\boldsymbol{x}^{\boldsymbol{\alpha}_x}\boldsymbol{y}^{\boldsymbol{\alpha}_y}$ *and* $\boldsymbol{x}^{\boldsymbol{\beta}_x}\boldsymbol{y}^{\boldsymbol{\beta}_y}$ *be two monomials,* $\boldsymbol{x}^{\boldsymbol{\alpha}_x}\boldsymbol{y}^{\boldsymbol{\alpha}_y} \prec \boldsymbol{x}^{\boldsymbol{\beta}_x}\boldsymbol{y}^{\boldsymbol{\beta}_y}$ *if and only if one of the two assertions that follow is true:*

- $\boldsymbol{x}^{\boldsymbol{\alpha}_x} \prec_x \boldsymbol{x}^{\boldsymbol{\beta}_x}$,
- $\boldsymbol{x}^{\boldsymbol{\alpha}_x} = \boldsymbol{x}^{\boldsymbol{\beta}_x}$ *and* $\boldsymbol{y}^{\boldsymbol{\alpha}_y} \prec_y \boldsymbol{y}^{\boldsymbol{\beta}_y}$.

Moreover, the ordering $\succ$ *is an elimination ordering in the variables* $\{y_1, \ldots, y_m\}$.

Definition 2.31. *An admissible monomial ordering* $\succ$ *on* $\mathbb{K}[x_1, \ldots, x_n]$ *is said to be a* graded ordering *if for all monomials* $\boldsymbol{x}^{\boldsymbol{\alpha}}, \boldsymbol{x}^{\boldsymbol{\beta}}$:

$$\deg(\boldsymbol{x}^{\boldsymbol{\alpha}}) > \deg(\boldsymbol{x}^{\boldsymbol{\beta}}) \text{ implies that } \boldsymbol{x}^{\boldsymbol{\alpha}} \succ \boldsymbol{x}^{\boldsymbol{\beta}}.$$

Definition 2.32. *The* grevlex *ordering or* drl *ordering on* $\mathbb{K}[x_1, \ldots, x_n]$ *is an admissible monomial ordering defined as follows.*
For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *and* $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$, *two monomials* $\boldsymbol{x}^{\boldsymbol{\alpha}}$ *and* $\boldsymbol{x}^{\boldsymbol{\beta}}$, $\boldsymbol{x}^{\boldsymbol{\alpha}} \prec_{grlex} \boldsymbol{x}^{\boldsymbol{\beta}}$ *if and only if one of the following assertions is satisfied:*

- $\deg(\boldsymbol{x}^{\boldsymbol{\beta}}) > \deg(\boldsymbol{x}^{\boldsymbol{\alpha}})$,
- $\deg(\boldsymbol{x}^{\boldsymbol{\beta}}) = \deg(\boldsymbol{x}^{\boldsymbol{\alpha}})$ *and the rightmost nonzero entry of* $\boldsymbol{\beta} - \boldsymbol{\alpha} \in \mathbb{Z}^n$ *is negative.*

Definition 2.33. *The lexicographic ordering on* $\mathbb{K}[x_1, \ldots, x_n]$ *is defined as follows:*
For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *and* $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$, *two monomials* $\boldsymbol{x}^{\boldsymbol{\alpha}}$ *and* $\boldsymbol{x}^{\boldsymbol{\beta}}$, $\boldsymbol{x}^{\boldsymbol{\alpha}} \prec_{lex} \boldsymbol{x}^{\boldsymbol{\beta}}$ *if and only if:*

- *the leftmost nonzero entry of* $\boldsymbol{\beta} - \boldsymbol{\alpha} \in \mathbb{Z}^n$ *is positive.*

Remark 2.34. *On* $\mathbb{K}[t]$ *there exists one admissible monomial ordering. It is the ordering induced by the degree. We write it* $\succ_t$.

2.5 Gröbner basis

Let $\succ$ be an admissible monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Let S be a subset of $\mathbb{K}[x_1, \ldots, x_n]$. We write $\langle \mathrm{lm}_{\succ}(S) \rangle$ the ideal generated by all the leading monomials of polynomials in S. For more details on Gröbner basis we refer the reader to [8, Chapter2], in particular for the following theorem,[8, section 5, theorem 4].

Theorem 2.35. *(Hilbert Basis Theorem). Every ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ has a finite generating set. In other words, there exists some polynomials $g_1, \ldots, g_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that $I = \langle g_1, \ldots, g_s \rangle$.*

Definition 2.36. *Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and $\{g_1, \ldots, g_s\}$ a subset of I. The set $\{g_1, \ldots, g_s\} \subset I$ is a Gröbner basis of $(I, \succ)$ if and only if*

$$\langle \mathrm{lm}_\succ(I) \rangle = \langle \mathrm{lm}_\succ(g_1), \ldots, \mathrm{lm}_\succ(g_s) \rangle.$$

Example 2.37. *The ideal $I = \langle y, xy^2 + x + 1 \rangle$ in $\mathbb{K}[x, y]$ is equal to the ideal $\langle y, x + 1 \rangle$ because*

$$xy^2 + x + 1 = (x + 1) + (yx)y \text{ and } x + 1 = (xy^2 + x + 1) - (yx)y.$$

The set $\{x + 1, y\}$ is a Gröbner basis *of $(I, \succ_{lex})$ because I is not equal to $\mathbb{K}[x, y]$.*

Definition 2.38. *A Gröbner basis G of $(I, \succ)$ in $\mathbb{K}[x_1, \ldots, x_n]$ is* minimal *if :*

1) There are no polynomials f and g in G such that $\mathrm{lm}_\succ(f)$ divides $\mathrm{lm}_\succ(g)$.

Moreover, the minimal Gröbner basis G is reduced *if :*

2) For all $g \in G$, $\mathrm{lc}_\succ(g) = 1$.

3) For all $g \in G$, no monomial of g lies in $\langle \mathrm{lm}_\succ(G \backslash \{g\}) \rangle$.

The following proposition can be found in [5, page 22].

Proposition 2.39. *Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. There exists a unique minimal reduced Gröbner basis of $(I, \succ)$.*

For a ring R and I an ideal of R we define the quotient ring R/I as the equivalent classes of the following equivalent relation on R: $a \sim b$ if and only if $a - b \in I$. The following proposition can be found in [8, chapter 5, section 3, proposition 4].

Proposition 2.40. *Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. The set of monomials $\{\underline{x}^\alpha, \alpha \in \mathbb{N}^n \mid \underline{x}^\alpha \notin \langle \mathrm{lm}_\succ(I) \rangle\}$ is a basis of the $\mathbb{K}$-vector space $\mathbb{K}[x_1, \ldots, x_n]/I$.*

Definition 2.41. *An ideal I of $\mathbb{K}[x_1, \ldots, x_n]$ is said to be* zero-dimensional *if the $\mathbb{K}$-vector space $\mathbb{K}[x_1, \ldots, x_n]/I$ has finite dimension.*

2.6 Homogenization

Definition 2.42. *Let f be a polynomial in $\mathbb{K}[x_1, \ldots, x_n]$. We define the* homogenization *of f the polynomial $f^h = h^{\deg(f)} f(x_1/h, \ldots, x_n/h)$ in the polynomial ring $\mathbb{K}[x_1, \ldots, x_n, h]$. Let g be a polynomial in $\mathbb{K}[x_1, \ldots, x_n, h]$. We define the* dehomogenization *of g the polynomial $g_h = g(x_1, \ldots, x_n, 1)$ in $\mathbb{K}[x_1, \ldots, x_n]$.*

Remark 2.43. *We can see that for a polynomial f in $\mathbb{K}[x_1,\dots,x_n]$ we have $(f^h)_h = f$ but for a polynomial g in $\mathbb{K}[x_1,\dots,x_n,h]$, the equality $(g_h)^h = g$ is not necessarily true. For example for $xh+1 \in \mathbb{K}[x,h]$ we have $((xh+1)_h)^h = x+h$.*

Lemma 2.44. *Let $\succ$ be an admissible monomial ordering on $\mathbb{K}[x_1,\dots,x_n]$. Let I and J be ideals of $\mathbb{K}[x_1,\dots,x_n]$ such that $I \subseteq J$ and $\langle \mathrm{lm}_\succ(I)\rangle = \langle \mathrm{lm}_\succ(J)\rangle$, then $I = J$.*

Proof. Suppose that there exists f in $J\backslash I$. Choose f in $J\backslash I$ with a leading monomial as lower as possible. Then there exists a polynomial g in I which has the same leading monomial. Write the polynomial

$$h = \frac{f}{\mathrm{lc}_\succ(f)} - \frac{g}{\mathrm{lc}_\succ(g)}.$$

We see that h is in J but $\mathrm{lm}_\succ(f) \succ \mathrm{lm}_\succ(h)$ so h must lie in I by our minimality hypothesis we deduce that the polynomials g and h are in I which implies that f is in I which is a contradiction. □

Proposition 2.45. *Let $\succ_x$ be an admissible monomial ordering in the ring $\mathbb{K}[x_1,\dots,x_n]$ and $f_1,\dots,f_s$ be some polynomials of $\mathbb{K}[x_1,\dots,x_n]$. Let us consider the ideals $I = \langle f_1,\dots,f_s\rangle$ and $J = \langle f_1^h,\dots,f_s^h\rangle$. If $\{g_1,\dots,g_\ell\}$ is a Gröbner basis of $(J,\succ)$ where $\succ = (\succ_x,\succ_h)$ on $\mathbb{K}[x_1,\dots,x_n,h]$, then $\{(g_1)_h,\dots,(g_\ell)_h\}$ is a Gröbner basis of $(I,\succ_x)$.*

Proof. Let f be in I. One can write it as $f = \sum_{i=1}^s u_i f_i$ with $u_i \in \mathbb{K}[x_1,\dots,x_n]$ for $i \in \{1,\dots,s\}$. Deduce from the definition that

$$f^h = \sum_{i=1}^s u_i\left(\frac{x_1}{h},\dots,\frac{x_n}{h}\right) f_i\left(\frac{x_1}{h},\dots,\frac{x_n}{h}\right).$$

So there exists $(\beta,\alpha_1,\dots,\alpha_s) \in \mathbb{N}^{s+1}$ such that

$$h^\beta f^h = \sum_{i=1}^s h^{\alpha_i} u_i^h f_i^h.$$

So it means that $h^\beta f^h$ is in J, and there exists $k \in \{1,\dots,\ell\}$ such as $\mathrm{lm}_\succ(g_k)$ divides $\mathrm{lm}_\succ(h^\beta f^h)$. Moreover, by the definition of $\succ$, $\mathrm{lm}_{\succ_x}(f) = \mathrm{lm}_\succ(f^h)/(h^\alpha)$ for some $\alpha \in \mathbb{N}$. Deduce that $\mathrm{lm}_\succ(g_k)$ divides $h^{\alpha+\beta}\,\mathrm{lm}_{\succ_x}(f)$ which implies that $\mathrm{lm}_{\succ_x}((g_k)_h)$ divides $\mathrm{lm}_{\succ_x}(f)$. It means that

$$\mathrm{lm}_{\succ_x}(I) \subseteq \langle \mathrm{lm}_{\succ_x}((g_1)_h),\dots,\mathrm{lm}_{\succ_x}((g_\ell)_h)\rangle$$

Finally, if $g_k = \sum_{i=1}^s v_i(f_i)^h$ for some polynomials $v_i \in \mathbb{K}[x_1,\dots,x_n,h]$ with $i \in \{1,\dots,\ell\}$ then $(g_k)_h = \sum_{i=1}^\ell (v_i)_h f_i$. Deduce that

$$\langle (g_1)_h,\dots,(g_\ell)_h\rangle \subseteq I.$$

Observe that

$$\mathrm{lm}_{\succ_x}(I) = \langle \mathrm{lm}_{\succ_x}((g_1)_h), \ldots, \mathrm{lm}_{\succ_x}((g_\ell)_h)\rangle$$

By Lemma 2.44,

$$\langle (g_1)_h, \ldots, (g_\ell)_h\rangle = I.$$

Then the family of polynomials $\{(g_1)_h, \ldots, (g_\ell)_h\}$ is a Gröbner basis of I. □

The following property is a known is the literature.

Proposition 2.46. *Let $\succ_{grlex}$ be the grevlex ordering in $\mathbb{K}[x_1, \ldots, x_n]$ and $f_1, \ldots, f_s$ be some polynomials of $\mathbb{K}[x_1, \ldots, x_n]$. Consider the ideals $I = \langle f_1, \ldots, f_s\rangle$ and $J = \langle f_1^h, \ldots, f_s^h\rangle \subseteq \mathbb{K}[x_1, \ldots, x_n, h]$. If $\{g_1, \ldots, g_\ell\}$ is a Gröbner basis of $(J, \succ_{grlexh})$ where $\succ_{grlexh}$ is the grevlex ordering on $\mathbb{K}[x_1, \ldots, x_n, h]$, then $\{(g_1)_h, \ldots, (g_\ell)_h\}$ is a Gröbner basis of $(I, \succ_{grlex})$.*

Proof. Let f be in I, we can write it as $f = \sum_{i=1}^{s} u_i f_i$ with $u_i \in \mathbb{K}[x_1, \ldots, x_n]$ for $i \in \{1, \ldots, s\}$. So there exists $(\beta, \alpha_1, \ldots, \alpha_s) \in \mathbb{N}^{s+1}$ such that

$$h^\beta f^h = \sum_{i=1}^{s} h^{\alpha_i} u_i^h f_i^h.$$

So it means that $h^\beta f^h$ is in J, and there exists $k \in \{1, \ldots, \ell\}$ such as $\mathrm{lm}_{\succ_{grlexh}}(g_k)$ divides $\mathrm{lm}_{\succ_{grlexh}}(h^\beta f^h)$. Moreover, by the definition the grevlex ordering we can see that $\mathrm{lm}_{\succ_{grlex}}(f) = \mathrm{lm}_{\succ_{grlexh}}(f^h)$. We deduce by the same argument as in the proof of Proposition 2.45 that $\mathrm{lm}_{\succ_{grlex}}((g_k)_h)$ divides $\mathrm{lm}_{\succ_{grlex}}(f)$. The end of the proof is exactly the same as in Proposition 2.45. □

2.7 Regular sequences

For more details on regular sequences we refer the reader to [6, page 24, subsection 3.4].

Definition 2.47. *Let $F = (f_1, \ldots, f_s) \in \mathbb{K}[x_1, \ldots, x_n]^s$ be a sequence of nonzero homogeneous polynomials. The sequence F is said to be a regular sequence if:*

(∗) *For all $i \in \{2, \cdots, s\}$, f_i does not divide zero in the quotient ring $\mathbb{K}[x_1, \ldots, x_n]/\langle f_1, \ldots, f_{i-1}\rangle$.*

For a sequence $F = (f_1, \ldots, f_s)$ of polynomials which are not homogeneous we define for all $i \in \{1, \ldots, s\}$ the polynomial $(f_i)^H$ by $(f_i)^H(x_1, \ldots, x_n) = (f_i)^h(x_1, \ldots, x_n, 0)$. The sequence F is said to be regular if and only if the sequence $((f_1)^H, \ldots, (f_s)^H)$ is regular in $\mathbb{K}[x_1, \ldots, x_n]$.

Remark 2.48.

- *If a sequence of homogeneous polynomials is regular then the polynomials are pairwise coprime.*
- *By [11, Remark 8,page 20] and [11, definition 19,page 20], we can see that for any regular sequence of homogeneous polynomials* $(f_1, \ldots, f_s) \in \mathbb{K}[x_1, \ldots, x_n]^s$ *such that* $I = \langle f_1, \ldots, f_s \rangle$ *is zero-dimensional we have* $s = n$.

Example 2.49.

- *This is an example of a sequence of homogeneous polynomials that are pairwise coprime but the sequence is not regular:*

$$f_1 = x, f_2 = y, f_3 = x - y \in \mathbb{C}[x, y, z].$$

The sequence (f_1, f_2, f_3) *is not regular because*

$$f_3 = 0 \in \mathbb{C}[x, y, z]/\langle f_1, f_2 \rangle.$$

- *This is an example of a sequence of polynomials that satisfies the property* $(*)$ *but without being homogeneous and there homogenization does not respect* $(*)$ *anymore:*

$$f_1 = x - 1, f_2 = xy^2 - 2, f_3 = x^2 - z \in \mathbb{C}[x, y, z].$$

The sequence (f_1, f_2, f_3) *satisfies the property* $(*)$ *but it is not the case for* $((f_1)^h, (f_2)^h, (f_3)^h)$ *because :*

$$(x^2 - zh)(hy^2 - 2h^2y) \in \langle (f_1)^h, (f_2)^h \rangle$$

and $(hy^2 - 2h^2y) \notin \langle (f_1)^h, (f_2)^h \rangle$.

2.8 Hilbert series

For more details on Hilbert series we refer the reader to [6] chapter 2 section 2. For $n \in \mathbb{N}$ the set $\mathbb{K}[x_1, \ldots, x_n]_d = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid \deg(f) = d \text{ and } f \text{ is homogeneous}\}$ is a $\mathbb{K}$-vector space of dimension $\binom{n+d-1}{d}$. If I is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$, then the set $I_d = I \cap \mathbb{K}[x_1, \ldots, x_n]_d$ is also a K-vector space.

Definition 2.50. *Let* $f_1, \ldots, f_s$ *be homogeneous polynomials of* $\mathbb{K}[x_1, \ldots, x_n]$ *and* $I = \langle f_1, \ldots, f_s \rangle$. *The Hilbert function in degree* $d \in \mathbb{N}$ *of the ideal* I *is defined by:*

$$HF_I(d) = \dim(\mathbb{K}[x_1, \ldots, x_n]_d) - \dim(I_d).$$

Definition 2.51. *Let* $f_1, \ldots, f_s$ *be homogeneous polynomials of* $\mathbb{K}[x_1, \ldots, x_n]$ *and* $I = \langle f_1, \ldots, f_s \rangle$. *The Hilbert series of an ideal* I *of* $\mathbb{K}[x_1, \ldots, x_n]$ *is defined as follows:*

$$HS_I(t) = \sum_{d=0}^{+\infty} HF_I(d) t^d.$$

The following theorem can be found in [1, page 2, theorem 2].

Theorem 2.52. *Let $f_1, \ldots, f_s$ be homogeneous polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ with $\deg(f_i) = d_i$ and $I = \langle f_1, \ldots, f_s \rangle$. The sequence $(f_1, \ldots, f_s)$ is regular if and only if its Hilbert series is given by*

$$HS_I(t) = \frac{\prod_{i=1}^{s}(1 - t^{d_i})}{(1-t)^n}.$$

3 Lazard's algorithm

The original paper of this algorithm is [15]. For a set S of polynomials, the set $\mathrm{Span}_{\mathbb{K}}(S)$ is the $\mathbb{K}$-vector space generated by S. In $\mathbb{K}[x_1, \ldots, x_n]$, the set Mon_d is the set of monomials of degree d and $\mathrm{Mon}_{\leq d}$ is the set of monomials of degree at most d. The set Mon is the set of all monomials of $\mathbb{K}[x_1, \ldots, x_n]$. The support of a polynomial f in $\mathbb{K}[x_1, \ldots, x_n]$ is a finite subset J of $\mathbb{N}^n$ such that $f = \sum_{\boldsymbol{j} \in J} a_{\boldsymbol{j}} \boldsymbol{x}^{\boldsymbol{j}}$ were $a_{\boldsymbol{j}}$ is in $\mathbb{K}\backslash\{0\}$. For a set S, the set $P(S)$ is the set of all subset of S.

3.1 The homogeneous case

Let us explain Lazard's algorithm in the homogeneous case and prove that it computes a Gröbner basis.

Proposition 3.1. *Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ generated by the homogeneous polynomials $f_1, \ldots, f_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ with $\deg(f_i) = d_i$. Let d be in $\mathbb{N}$, we consider the $\mathbb{K}$-vector space $I_d = I \bigcap \mathbb{K}[x_1, \ldots, x_n]_d$ of homogeneous polynomials of degree d in I. Then I_d is equal to the $\mathbb{K}$-vector space $\mathrm{Span}_{\mathbb{K}}(\{f_i m \mid m \in \mathrm{Mon}_{d-d_i}$ and $i \in \{1, \ldots, s\}\})$.*

Proof. Show that $I_d = \mathrm{Span}_{\mathbb{K}}(\{f_i m \mid m \in \mathrm{Mon}_{d-d_i}$ and $i \in \{1, \ldots, s\}\})$:

($\supseteq$) It is obvious that this vector space is in I_d because the polynomials $f_i m$ lies in $\mathbb{K}[x_1, \ldots, x_n]_d$ and in I. Moreover, a $\mathbb{K}$-linear combination of those polynomials stay in I_d .

($\subseteq$) Conversely, let f be in I_d. Then f can be written as $f = \sum_{i=1}^{s} u_i f_i$ with u_i in $\mathbb{K}[x_1, \ldots, x_n]$ for all i in $\{1, \ldots, s\}$. Let i be in $\{1, \ldots, s\}$, we define $J_i \subset \mathbb{N}^n$ as the support of the polynomial f_i and $K_i \subset \mathbb{N}^n$ as the support of the polynomial u_i. We express those polynomials as

$$u_i = \sum_{\boldsymbol{k} \in K_i} b_{i,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} \text{ and } f_i = \sum_{\boldsymbol{j} \in J_i} a_{i,\boldsymbol{j}} \boldsymbol{x}^{\boldsymbol{j}}$$

with $a_{i,\boldsymbol{j}}$ and $b_{i,\boldsymbol{k}}$ in $\mathbb{K}$ for all $\boldsymbol{j}$ in J_i and $\boldsymbol{k}$ in K_i. Then we have

$$f_i u_i = \sum_{\boldsymbol{j}\in J_i, \boldsymbol{k}\in K_i} a_{i,\boldsymbol{j}} b_{i,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{j}+\boldsymbol{k}}$$

which leads to

$$f = \sum_{i=1}^{s} \sum_{\boldsymbol{j}\in J_i, \boldsymbol{k}\in K_i} a_{i,\boldsymbol{j}} b_{i,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{j}+\boldsymbol{k}}.$$

Let i be in $\{1,\dots,s\}$, observe that for all $\boldsymbol{j} \in J_i$, $|\boldsymbol{j}| = d_i$. We define the sets $K_{i,1} = \{\boldsymbol{k} \in K_i \mid |\boldsymbol{k}| = d - d_i\}$ and $K_{i,2} = \{\boldsymbol{k} \in K_i \mid |\boldsymbol{k}| \neq d - d_i\}$. We can see that $K_i = K_{i,1} \sqcup K_{i,2}$. We can write:

$$f = \sum_{i=1}^{s} \sum_{\boldsymbol{j}\in J_i, \boldsymbol{k}\in K_{i,2}} a_{i,\boldsymbol{j}} b_{i,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{j}+\boldsymbol{k}} + \sum_{i=1}^{s} \sum_{\boldsymbol{j}\in J_i, \boldsymbol{k}\in K_{i,1}} a_{i,\boldsymbol{j}} b_{i,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{j}+\boldsymbol{k}}.$$

The first term of the sum has no monomial of degree d while the other term is homogeneous of degree d. As f is homogeneous of degree d then the first term is zero. We define new polynomials $\tilde{u}_i = \sum_{k\in K_{i,1}} b_{i,k} \boldsymbol{x}^{\boldsymbol{k}}$ which are homogeneous of degree $d - d_i$ and $f = \sum_{i=1}^{s} \tilde{u}_i f_i$. Then f is in the vector space generated by the polynomials $f_i m$ where m is in Mon_{d-d_i}. □

The following definition can be found in [14, chapter 2, definition 2.61].

Definition 3.2. ***Macaulay matrix***
Let $F = (f_1,\dots,f_s)$ be a sequence of polynomials in the ring $\mathbb{K}[x_1,\dots,x_n]$ with $\deg(f_i) = d_i$ and $\succ$ be an admissible monomial ordering. Let d be in $\mathbb{N}$. Let $\phi : \mathbb{N} \times \mathbb{K}[x_1,\dots,x_n]^{\mathbb{N}} \to P(\mathrm{Mon}) \times P(\mathrm{Mon})^{\mathbb{N}}$ be a function such that $\phi(d,F) = (A,B)$ where $B = (B_i)_{i\in\mathbb{N}}$. We define the Macaulay matrix for $d \in \mathbb{N}$ as follows.

Each column is indexed by an element of A by decreasing order for $\succ$. Each row is indexed by an element of the set $\{f_i m \mid i \in \{1,\dots,s\}, m \in B_i\}$. For i in $\{1,\dots,s\}$, we write the set $B_i = \{m_{i,1},\dots,m_{i,k_i}\}$. The rows are arranged in decreasing order for the order $\succ_{row}$ defined as follows

$$f_i m_{i,k} \succ_{row} f_{i'} m_{i',k'} \Leftrightarrow i < i' \text{ or } (i = i' \text{ and } m_{i,k} \succ m_{i',k'})$$

for all i and i' in $\{1,\dots,s\}$ and for all k in $\{1,\dots,k_i\}$ and k' in $\{1,\dots,k_{i'}\}$. Let i be in $\{1,\dots,s\}$, j be in $\{1,\dots,\ell\}$ and k be in $\{1,\dots,k_i\}$, the entry c in the row $f_i m_{i,k}$ and in the column m_j in the matrix is the coefficient of m_j in the polynomial $f_i m_{i,k}$.

$$\mathrm{Mac}_{\phi(d,F),\succ} = \begin{array}{r} \\ f_1 \cdot m_{1,k_1} \\ \cdots \\ f_1 \cdot m_{1,1} \\ f_i \cdot m_{i,k_i} \\ \cdots \\ f_i \cdot m_{i,k} \\ \cdots \\ f_i \cdot m_{i,1} \\ f_s \cdot m_{s,k_s} \\ \cdots \\ f_s \cdot m_{s,1} \end{array} \begin{array}{c} m_\ell \succ \cdots \succ m_j \succ \cdots \succ m_1 \\ \left(\begin{array}{ccc} & \vdots & \\ \cdots\cdots\cdots & \boxed{c} & \\ & & \end{array} \right) \end{array}.$$

The idea in Lazard's algorithm is to find elements of I_d that have for leading monomials the leading monomials of I_d. The following proposition claims that those can be found in the row echelon form of the Macaulay matrix of degree d.

Notation 3.3. *Let $f_1, \ldots, f_s$ be polynomials of the ring $\mathbb{K}[x_1, \ldots, x_n]$ with $\deg(f_i) = d_i$. Define $\phi_0(d, F) = (\mathrm{Mon}_d, \mathrm{Mon}_{d-d_1}, \ldots, \mathrm{Mon}_{d-d_s})$.*

Remark 3.4. *Let M be a matrix in $\mathbb{K}^{r\times c}$, in Section 2.1 we saw that there exists a invertible matrix A in $\mathbb{K}^{r\times r}$ such that $M_1 = AM$ is the reduced echelon form of M. Let $F = (f_1, \ldots, f_s)$ be a sequence of homogeneous polynomials and $\succ$ be an admissible monomial ordering. Suppose that $M = \mathrm{Mac}_{\phi_0(d,F),\succ}$. Then the columns of M_1 are also indexed by monomials of Mon_d. The rows of such matrices can be seen as homogeneous polynomials of degree d in $\mathbb{K}[x_1, \ldots, x_n]$.*

Proposition 3.5. *Let $F = (f_1, \ldots, f_s)$ be a sequence of homogeneous polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ be an admissible monomial ordering. Let M be the row echelon form of $\mathrm{Mac}_{\phi_0(d,F),\succ}$. The set $\mathrm{lm}_\succ(I_d)$ is equal to the set of monomials that index a column that contains a pivot in M.*

Proof. By Proposition 3.1, the rows of $\mathrm{Mac}_{\phi_0(d,F),\succ}$ generate the $\mathbb{K}$-vector space I_d. As there exists a square invertible matrix A such that

$$M = A\,\mathrm{Mac}_{\phi_0(d,F),\succ}\,.$$

The rows of the matrix M generate the same $\mathbb{K}$-vector space I_d. By Definition 3.2, it is obvious that a monomial which indexes a column that contains a pivot in M is an element of $\mathrm{lm}_\succ(I_d)$. Moreover, let f be in I_d, then

$$\mathrm{Mac}_{\phi_0(d,(f)),\succ} = \tilde{A}M$$

for a certain row vector $\tilde{A}$ with entries in $\mathbb{K}$. By Proposition 2.4, $\mathrm{Mac}_{\phi_0(d,(f)),\succ}$ has the same pivot as a row of M. That means $\mathrm{lm}_\succ(f)$ is a monomial that index a column that contains a pivot in M. □

Proposition 3.6. *Let $f_1, \ldots, f_s$ be homogeneous polynomials in the ring $\mathbb{K}[x_1, \ldots, x_n]$ with $d = \min_{i\in\{1,\ldots,s\}}(\deg(f_i))$ which generate an ideal $I = \langle f_1, \ldots, f_s\rangle$. Then the equality $\min_{f\in I} \deg(f) = d$ holds.*

Proof. Write

$$f = \sum u_i f_i,$$

observe that the degree of all monomials of f is greater than d.

□

Definition 3.7. *Let $F = \{f_1, \ldots, f_s\}$ be a set of homogeneous polynomials of an ideal I of $\mathbb{K}[x_1, \ldots, x_n]$ and let $\succ$ be an admissible monomial order on $\mathbb{K}[x_1, \ldots, x_n]$. The set F is said to be a d-Gröbner basis of $(I, \succ)$ if for any f in I with $\deg(f) \leq d$ we have*

$$\mathrm{lm}_\succ(f) \in \langle \mathrm{lm}_\succ(f_1), \ldots, \mathrm{lm}_\succ(f_s)\rangle.$$

The following Proposition can be found in [14, Chapter 2, Proposition 2.60]

Proposition 3.8. *Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ be an admissible monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. There exists some d_0 such that for all $d \geq d_0$ in $\mathbb{N}$, if $\{p_1, \ldots, p_\ell\}$ is a d-Gröbner basis of $(I, \succ)$ then it is a Gröbner basis of $(I, \succ)$.*

Proof. Write $\{g_1, \ldots, g_s\}$ the minimal reduced Gröbner basis of $(I, \succ)$. Write $d_0 = \max(\deg(g_1), \ldots, \deg(g_s))$, let $d \geq d_0$ and $\{p_1, \ldots, p_\ell\}$ be a d-Gröbner basis of $(I, \succ)$ and $\tilde{I} = \langle p_1, \ldots, p_\ell\rangle$. As $deg(g_i) \leq d$ then as $\{p_1, \ldots, p_\ell\}$ is a d-Gröbner basis of $(I, \succ)$, $\mathrm{lm}_\succ(g_i) \in \langle \mathrm{lm}_\succ(p_1), \ldots, \mathrm{lm}_\succ(p_\ell)\rangle$, so $\langle \mathrm{lm}_\succ(I)\rangle = \langle \mathrm{lm}_\succ(\{p_1, \ldots, p_\ell\})\rangle$ as $\{g_1, \ldots, g_s\}$ is a Gröbner basis of I. Moreover $\tilde{I} \subseteq I$ which leads to $\langle \mathrm{lm}_\succ(I)\rangle = \langle \mathrm{lm}_\succ(\tilde{I})\rangle$, by Lemma 2.44 we deduce that $I = \tilde{I}$ which means $\{p_1, \ldots, p_\ell\}$ is a Gröbner basis of $(I, \succ)$. □

Remark 3.9. ***Macaulay bound*** *[15, page 154, Theorem 3]*
Let $F = (f_1, \ldots, f_s)$ be a regular sequence of polynomials of degree $d_1, \ldots, d_s$ that generate the ideal I. There exists a formula for such a d_0 that works for the grevlex ordering:

$$D = \left(\sum_{i=1}^{s}(d_i - 1)\right) + 1.$$

It implies that all polynomial from the reduced minimal Gröbner basis of $(I, \succ_{grlex})$ have degree D or less. The $\mathbb{K}[t]$-vector space

$$V = \langle mf_i \mid i \in \{1, \ldots, s\}, m \in \mathrm{Mon}_{\leq D-d_i}\rangle_{\mathbb{K}}$$

contains a Gröbner basis of $(I, \succ_{grlex})$.

Theorem 3.10. ***Macaulay bound*** *[15, page 154, Theorem 3]*
Let $F = (f_1, \ldots, f_s)$ be a regular sequence of homogeneous polynomials of degree $d_1, \ldots, d_s$ that generate the ideal I. Let $\succ$ be a graded ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Suppose I is zero-dimensional, then for all element g of the minimal Gröbner basis of $(I, \succ)$ the inequality:

$$\left(\sum_{i=1}^{s}(d_i - 1)\right) + 1 \geq \deg(g)$$

holds.

Proof. As $(f_1, \ldots, f_s)$ is a regular sequence and I is zero-dimensional, then $s = n$ by Remark 2.48. As $f_1, \ldots, f_s$ are homogeneous and $(f_1, \ldots, f_s)$ is a regular sequence, then

$$HS_I(t) = \frac{\prod_{i=1}^{n}(1 - t^{d_i})}{(1-t)^n}$$

by Theorem 2.52. Observe that $HS_I(t)$ is a polynomial in t:

$$\begin{aligned} HS_I(t) &= \frac{\prod_{i=1}^{n}(1 - t^{d_i})}{(1-t)^n} \\ &= \frac{\prod_{i=1}^{n}(1-t)\sum_{j=0}^{d_i-1} t^j}{(1-t)^n} \\ &= \prod_{i=1}^{n}\sum_{j=0}^{d_i-1} t^j \end{aligned}$$

Observe that the degree of $HS_I(t)$ is $(\sum_{i=1}^{s}(d_i - 1))$. Let us define the integer $D = (\sum_{i=1}^{s}(d_i - 1)) + 1$. By Definition 2.51, for all $d \geq D$ the equality $HF_I(d) = 0$ holds, which means

$$I \cap \mathbb{K}[x_1, \ldots, x_n]_d = \mathbb{K}[x_1, \ldots, x_n]_d.$$

Let g be an element of the minimal Gröbner basis of $(I, \succ)$ and let suppose that $\deg(g) > D$. As $\succ$ is a graded ordering, then $\deg(\mathrm{lm}_\succ(g)) = \deg(g)$. Write $\boldsymbol{x}^{\boldsymbol{\alpha}} = \mathrm{lm}_\succ(g)$, then there exists a monomial $\boldsymbol{x}^{\boldsymbol{\beta}}$ such that:

- $\boldsymbol{x}^{\boldsymbol{\beta}} \neq \boldsymbol{x}^{\boldsymbol{\alpha}}$
- $\boldsymbol{x}^{\boldsymbol{\beta}}$ divides $\boldsymbol{x}^{\boldsymbol{\alpha}}$
- $\deg(\boldsymbol{x}^{\boldsymbol{\beta}}) \geq D$.

As $\deg(\boldsymbol{x}^{\boldsymbol{\beta}}) \geq D$, the monomial $\boldsymbol{x}^{\boldsymbol{\beta}}$ is in I because

$$I \cap \mathbb{K}[x_1, \ldots, x_n]_{\deg(\boldsymbol{x}^{\boldsymbol{\beta}})} = \mathbb{K}[x_1, \ldots, x_n]_{\deg(\boldsymbol{x}^{\boldsymbol{\beta}})}.$$

As the monomial $\boldsymbol{x^\beta}$ is in I, there exists f an element of the minimal Gröbner basis of $(I, \succ)$ such that

$$\mathrm{lm}_\succ(f) \text{ divides } \boldsymbol{x^\beta}$$

which implies that

$$\mathrm{lm}_\succ(f) \text{ divides } \mathrm{lm}_\succ(g).$$

This is a contradiction with the fact that g is an element of the minimal Gröbner basis of $(I, \succ)$. By this contradiction, deduce that $\deg(g) \leq D$.

□

Example 3.11. *If we take $I = \langle x, xh^2 - y^3, yh^2 - z^3\rangle$ for the lexicographic ordering in $\mathbb{K}[x, y, z, h]$, the Macaulay bound is 5 but the minimal reduced Gröbner basis of $(I, \succ_{lex})$ is $\{x, y^3, y^2z^3, yz^6, yh^2 - z^3, z^9\}$. This shows that the Macaulay bound does not apply for the lexicographic ordering.*

Algorithm 1 Homogeneous Lazard's Algorithm

Input: homogeneous polynomials $F = (f_1, \ldots, f_s)$ of $\mathbb{K}[x_1, \ldots, x_n]$ with $\deg(f_i) = d_i$ an admissible monomial ordering $\succ$ and an integer d_{max}.
Output: a d_{max}-Gröbner basis of $(\langle f_1 \ldots f_s\rangle, \succ)$.

1: G = {}
2: $d_{min} = \min_{i\in\{1,\ldots,s\}}(\deg(f_i))$
3: **for** $d = d_{min}$ to d_{max} **do**
4: $M = \mathrm{Mac}_{\phi_0(d,F),\succ}$
5: m_d = column vector that contains all the monomials of degree d in decreasing order for $\succ$.
6: $\widetilde{M}$ = reduced row echelon form of M
7: $I = \widetilde{M} \cdot m_d$
8: $G = G \bigcup \{h \in I \mid \forall g \in G \bigcup I, g \neq h, \mathrm{lm}_\succ(g)$ does not divide $\mathrm{lm}_\succ(h)\}$
9: return G

Proposition 3.12. *The output of Algorithm 1 is a d_{max}-Gröbner basis of $(\langle f_1, \ldots f_s, \rangle, \succ)$.*

Proof. Write G the set of polynomials that the algorithm returns and we write $\tilde{G}$ the set of polynomials which are the nonzero rows of the reduced row echelon forms of all Macaulay matrices from d_{min} to d_{max}. We notice by Step 8 in the algorithm that G is a d_{max}-Gröbner basis of I if and only if $\tilde{G}$ is also one, in fact $\langle\{\mathrm{lm}_<(g), g \in \tilde{G}\}\rangle = \langle\{\mathrm{lm}_<(g), g \in G\}\rangle$. Let us show that $\tilde{G}$ is a d_{max}-Gröbner basis.

Let f be a polynomial I such that $\deg(f) \leq d_{max}$ then by Proposition 3.6

$$f = \sum_{d=d_{min}}^{d_{max}} p_d$$

such that the polynomial $p_d \in \mathbb{K}[x_1, \ldots, x_n]_d$ (the homogeneous part in degree d of f). There exists j such that $\mathrm{lm}_\succ(p_j) = \mathrm{lm}_\succ(f)$. As $f = \sum_{i=1}^{s} u_i f_i$, we notice that $p_j = \sum_{i=1}^{s} \tilde{u}_i f_i$ with the $\tilde{u}_i$ that are homogeneous with degree $j - d_i$. As p_j is in $\mathrm{Span}_{\mathbb{K}}(\{f_i m \mid m \in \mathrm{Mon}_{d-d_i} \text{ and } i \in \{1, \ldots, s\}\})$, by Proposition 3.1 the polynomial p_j is in $I_d = I \bigcap \mathbb{K}[x_1, \ldots, x_n]_d$. As p_j is in I_d, by Proposition 3.5 $\mathrm{lm}_\succ(f) = \mathrm{lm}_\succ(p_j)$ is in the ideal generated by the leading terms of $\tilde{G}$ which means $\tilde{G}$ is a d_{max}-Gröbner-basis of $(\langle f_1 \ldots f_s \rangle, \succ)$. □

3.2 The affine case

In Section 3.1 we saw that if $f_1, \ldots, f_s$ are homogeneous we can find a Gröbner basis with Lazard's algorithm but this is still possible when those polynomials are not homogeneous. By Section 2.6 we can proceed by homogenizing input polynomials $f_1, \ldots, f_s$ hence obtaining $f_1^h, \ldots, f_s^h$. After that we apply the algorithm on $f_1^h, \ldots, f_s^h$ and we obtain a set of polynomials as output. By evaluating this set in 1 on the variable h of homogenization ($g \longrightarrow g_h$) it gives us a Gröbner basis by Proposition 2.46. The following algorithm does not use homogenization.

Notation 3.13. *Let $f_1, \ldots, f_s$ be polynomials of the ring $\mathbb{K}[x_1, \ldots, x_n]$ with $\deg(f_i) = d_i$. Define $\phi_1(d, F) = (\mathrm{Mon}_{\leq d}, \mathrm{Mon}_{d-d_1}, \ldots, \mathrm{Mon}_{d-d_s})$ and $\phi_2(d, F) = (\mathrm{Mon}_{\leq d}, \mathrm{Mon}_{\leq d-d_1}, \ldots, \mathrm{Mon}_{\leq d-d_s})$.*

Algorithm 2 Affine Lazard's Algorithm

Input: $F = (f_1, \dots, f_s)$ polynomials of $\mathbb{K}[x_1, \dots, x_n]$ with $\deg(f_i) = d_i$.
Output: Gröbner basis of $(\langle f_1 \dots f_s \rangle, \succ_{grlex})$.

1: $d_{min} = \min_{i \in \{1,\dots,s\}}(d_i)$
2: $D = \sum_{i=1}^{n}(d_i - 1) + 1$
3: $G = \{\}$
4: $M = \text{Mac}_{\phi_2(d_{min},F),\succ_{grlex}}$
5: $m_{d_{min}}$ = vector column that contain all the monomials of degree d_{min} or less in decreasing order.
6: $\widetilde{M}$ = row echelon form of M
7: $I = \widetilde{M} \times m_{d_{min}}$
8: $G = I$
9: **for** $d = d_{min} + 1$ to D **do**
10: $M = \text{Mac}_{\phi_1(d,F),\succ_{grlex}}$
11: $M = \begin{pmatrix} M & \\ 0 & \tilde{M} \end{pmatrix}$
12: m_d = vector column that contain all the monomials of degree d or less in decreasing order.
13: $\tilde{M}$ = row echelon form of M
14: $I = \tilde{M} \times m_d$
15: $G = G \bigcup \{h \in I \mid \forall g \in G \bigcup I, g \neq h, \text{lm}_{\succ_{grlex}}(g)$ does not divide $\text{lm}_{\succ_{grlex}}(h)\}$
16: return G

Proposition 3.14. *Suppose that $F = ((f_1)^h, \dots, (f_s)^h)$ is a regular sequence and that the ideal $\rangle f_1, \dots, f_s \langle$ is zero-dimensional . The output of Algorithm 2 is a Gröbner basis of the pair $(\langle f_1 \dots f_s \rangle, \succ_{grlex})$.*

Proof. Let a regular sequence $F = (f_1, \dots, f_s)$ be in $\mathbb{K}[x_1, \dots, x_n]$ with $\deg(f_i) = d_i$ and the ideal $I = \langle f_1, \dots, f_s \rangle$. Let $\succ_{grlexh}$ the grevlex ordering on $\mathbb{K}[x_1, \dots, x_n, h]$. Write $\tilde{F} = (f_1^h, \dots, f_s^h)$ and $d_{min} = \min_{i \in \{1,\dots,s\}}(\deg(f_i))$. As f is regular, by Proposition 2.46 and Remark 3.9, we know that if g is an element of the minimal reduced Gröbner basis of I for $\succ_{grlex}$ there exists p in the ring $\mathbb{K}[x_1, \dots, x_n, h]$ such that $p_h = \tilde{g}$ with $\text{lm}_{\succ_{grlex}}(g) = \text{lm}_{\succ_{grlex}}(\tilde{g})$ and there exists $d \in \{d_{min}, \dots, D\}$, with D is the Macaulay bound, such that p is in the vector space generated by the rows of $\text{Mac}_{\phi_0(d,\tilde{F}),\succ_{grlexh}}$. So we can then write $p = \sum_{i=1}^{s} f_i^h u_i$ with $\deg(u_i) = d - d_i$. Then by taking $h = 1$ we have $\tilde{g} = \sum_{i=1}^{s} f_i (u_i)_h$ with $\deg((u_i)_h) \leq d - d_i$, that means $\tilde{g}$ is generated by the rows of $\text{Mac}_{\phi_2(d,F),\succ_{grlex}}$. Then Algorithm 2 gives us a Gröbner basis of $(I, \succ_{grlex})$ as for all g in the minimal Gröbner basis of $(I, \succ_{grlex})$ the output contains $\tilde{g}$ such $\text{lm}_{\succ_{grlex}}(g) = \text{lm}_{\succ_{grlex}}(\tilde{g})$. □

3.3 Complexity

We assume that we are computing a Gröbner basis for the grevlex ordering. Let $F = (f_1, \ldots, f_s)$ be a regular sequence of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ so that means we can use the Macaulay bound. Suppose that F is regular and that $\langle f_1, \ldots, f_s \rangle$ is zero-dimensional. That implies that $s = n$ by [11, page20,definition 19].

Suppose that for all i in $\{1, \ldots, n\}$, $\deg(f_i) = d$ in $\mathbb{N}$. Now write the Macaulay bound:

$$D = 1 - n + \sum_{i=1}^{n} d = 1 + n(d-1).$$

Let us find some information about the size of the last matrix $M = \mathrm{Mac}_{D \leq, \succ_{drl}} F$:

- The number of columns is:

$$\mathrm{Col}(n, d) = \binom{D+n}{D}.$$

- The number of rows is:

$$\mathrm{Row}(n, d) = n\binom{D-d+n}{D-d}.$$

- The rank is lower than the minimum of the two numbers above.

In order to know $\min(\mathrm{Col}(n, d), \mathrm{Row}(n, d))$ and to efficiently bounded the rank, write:

$$R(n, d) = \frac{\mathrm{Row}(n, d)}{\mathrm{Col}(n, d)} = n \prod_{i=0}^{d-1} \frac{D-i}{D+n-i}.$$

Proposition 3.15. *For $n \geq 4$ and $d \geq 2$, $R(n, d) > 1$.*

Proof. Let $d \geq 2$, we will show that $(n \longmapsto R(n, d))$ is increasing on $[4, +\infty[$. We can show it for:

$$\ln(R(n, d)) = \ln(n) + \sum_{i=0}^{d-1} (\ln(n(d-1) + 1 - i) - \ln(nd + 1 - i)).$$

The derivative in n is:

$$\begin{aligned}
&\frac{1}{n} + \sum_{i=0}^{d-1} \frac{d-1}{n(d-1)+1-i} - \frac{d}{nd+1-i} \\
=&\frac{1}{n} + \sum_{i=0}^{d-1} \frac{(d-1)(nd+1-i) - d(n(d-1)+1-i)}{(n(d-1)+1-i)(nd+1-i)} \\
=&\frac{1}{n} + \sum_{i=0}^{d-1} \frac{i-1}{(n(d-1)+1-i)(nd+1-i)}.
\end{aligned}$$

It is easy to see that the only term that is negative is when $i = 0$ but it is less in ultimate value than $\frac{1}{n}$. Then $(n \longmapsto R(n,d))$ is increasing on $[4, +\infty[$.

We know that $R(4,2) = \frac{10}{9} > 1, R(4,3) = \frac{168}{143} > 1, R(4,4) = \frac{143}{119} > 1$, if we prove that $(d \longmapsto R(4,d))$ is increasing on $[4, +\infty[$ we can deduce that $R(4,d) > 1$ for all $d \geq 2$. First we ensure that this function is well defined:

$$\begin{aligned} R(4,d) &= 4\prod_{i=0}^{d-1} \frac{4(d-1)+1-i}{4d+1-i} = 4\prod_{i=0}^{d-1} \frac{4d+1-(i+4)}{4d+1-i} \\ &= 4\left(\prod_{i=0}^{d-1} \frac{1}{4d+1-i}\right)\left(\prod_{i=4}^{d+3} 4d+1-i\right) = 4\prod_{i=0}^{3} \frac{3d+1-i}{4d+1-i}. \end{aligned}$$

As above we look at the derivative in d of $\ln(R(4,d))$:

$$\sum_{i=0}^{3} \frac{3}{3d+1-i} - \frac{4}{4d+1-i} = \sum_{i=0}^{3} \frac{i-1}{(3d+1-i)(4d+1-i)}.$$

We can see that in ultimate value the term $i = 2$ is greater than the term $i = 0$ so this quantity is positive. This concludes the proof. □

Proposition 3.16. *For $n = 2$ or $n = 3$ and $d \geq 2$, $R(n,d) < 1$.*

Proof. If $n = 2$ it is easy to see that $(d \longmapsto R(2,d))$ is a decreasing function on $[2, +\infty[$ with the same method as above. Moreover, $R(2,2) = \frac{3}{5} < 1$.

Let us take $n = 3$, $(d \longmapsto R(3,d))$ is increasing on $[3, +\infty[$ but it seems that $R(3,d) < 1$ for all $d \geq 2$.

$$R(3,d) = 3\prod_{i=0}^{d-1} \frac{3(d-1)+1-i}{3d+1-i} = 3\prod_{i=0}^{2} \frac{2d+1-i}{3d+1-i}.$$

See that $R(3,2) = \frac{6}{7}$, $R(3,3) = \frac{7}{8}$ and $\lim\limits_{d\to+\infty}(R(3,d)) = \frac{8}{9}$, which concludes the proof. □

Proposition 3.17. *Let us take $F = (f_1, \ldots, f_n)$ with $\deg(f_i) = d_i$ and $\widetilde{F} = (\tilde{f}_1, \ldots, \tilde{f}_n)$ with $\deg(\tilde{f}_i) = d$ and $nd = \sum_{i=1}^{n} d_i$. The new function is*

$$R(n,d) = \frac{\sum_{i=1}^{n} \binom{n+D-d_i}{D-d_i}}{\binom{D+n}{D}}.$$

Then for $n \geq 4$ and $d \geq 2$, $R(n,d) > 1$ in that case.

Proof. The Macaulay bounds of F and $\widetilde{F}$ are equal:

$$D = \left(\sum_{i=1}^{n} d_i\right) - n + 1 = nd - n + 1 = \left(\sum_{i=1}^{n} d\right) - n + 1 = \tilde{D}.$$

We want to compare the numbers of lines in those two cases:

$$\text{Row} = \sum_{i=1}^{n} \binom{n + D - d_i}{D - d_i}$$

and

$$\widetilde{\text{Row}} = n\binom{n + D - d}{D - d}.$$

First, $D - d$ is the mean of the $D - d_i$:

$$\frac{1}{n}\sum_{i=1}^{n}(D - d_i) = D - d.$$

Let x be in $\mathbb{N}$, then:

$$\binom{x + n}{x} = \frac{1}{n!}\prod_{i=0}^{n-1}(x + n - i).$$

Observe that the function $f : \mathbb{R}^+ \longrightarrow \mathbb{R}$ defined as:

$$f(x) = \frac{1}{n!}\prod_{i=0}^{n-1}(x + n - i)$$

is convex as it is a polynomial with positive coefficients.
Deduce that the inequality:

$$\frac{1}{n}\sum_{i=0}^{n} f(D - d_i) \geq f(\frac{1}{n}\sum_{i=0}^{n}(D - d_i))$$

which is equivalent to $\text{Row} \geq \widetilde{\text{Row}}$ holds. As the number of column is the same, that concludes the proof. □

The following result can be found in [18, chapter 2]. The exponent ω is the constant of matrices multiplication.

Theorem 3.18. *Let M be a matrix of $\mathbb{K}^{r\times c}$, then it takes*

$$\mathcal{O}(\text{rank}(M)^{\omega-2}rc)$$

operations in $\mathbb{K}$ to obtain its reduced row echelon form.

Let us find the rank of M more precisely. By Proposition 3.5 and the definition of the Hilbert function, the following result holds.

Proposition 3.19. *Let $F = (f_1, \ldots, f_s)$ be a set of homogeneous polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ of degree d_0 and $I = \langle f_1, \ldots, f_s \rangle$. Let d be in $\mathbb{N}$. The following equality holds:*

$$\operatorname{rank}(\operatorname{Mac}_{d,\succ_{grlex}} F) = \binom{n-1+d}{d} - HF_I(d).$$

Let $F = (f_1, \ldots, f_s)$ be a set of polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ of degree d_0 and $I = \langle f_1, \ldots, f_s \rangle$. By applying the homogenization it gives $F^h = (f_1^h, \ldots, f_s^h)$. In order to search the number of operations to compute a Gröbner basis of $(I, \succ_{grlex})$, we compute for the homogenized set of polynomials. It gives us

$$\sum_{d=d_0}^{D} \mathcal{O}\left(\left(\binom{d+n}{d} - HF_I(d)\right)^{\omega-2} \binom{d+n}{d} n \binom{d-d_0+n}{d-d_0}\right)$$

where $D = 1 + n(d_0 - 1)$.

4 Polynomial matrix version of Lazard's algorithm

4.1 The Hermite normal form

This section generalizes Lzard's algorithm by working on $\mathbb{K}[t][x_1, \ldots, x_n] \approx \mathbb{K}[x_1, \ldots, x_n, t]$. As those two rings are isomorphic, the notion of ideal is exactly the same. Let $t^\beta \boldsymbol{x}^{\boldsymbol{\alpha}}$ be a monomial, the x part of this monomial is $\boldsymbol{x}^{\boldsymbol{\alpha}}$. Let f be a polynomial of $\mathbb{K}[t][x_1, \ldots, x_n]$, it can be written $f = \sum_{\boldsymbol{\gamma} \in M} a_{\boldsymbol{\gamma}} \boldsymbol{x}^{\boldsymbol{\gamma}}$ with M a finite subset of $\mathbb{N}^n$ and $a_{\boldsymbol{\gamma}}$ in $\mathbb{K}[t]$ for all γ in M. The set $\operatorname{Mon}_{d,x}$ is the set of monomials in the $x_1, \ldots, x_n$ variables of degree d, Mon_d is the set of monomials in the $x_1, \ldots, x_n, t$ variables of degree d as above. Let $\succ_x$ be an admissible monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Let f be a polynomial of $\mathbb{K}[t][x_1, \ldots, x_n]$, write $\deg_x(f)$ its degree in the $x_1, \ldots, x_n$ variables. The polynomial f is x-homogeneous if all monomials of f have the same degree in the $x_1, \ldots, x_n$ variables. The degree of a coefficient $a_{\boldsymbol{\gamma}}$ it will be written $\deg_t(a)$. For $\succ_x$ an admissible monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$, write $\operatorname{lm}_{\succ_x,x}(f)$ for leading monomial, $\operatorname{lt}_{\succ_x,x}(f)$ for the leading term and $\operatorname{lc}_{\succ_x,x}(f)$ for leading coefficient. For a subset S of $\mathbb{K}[t][x_1, \ldots, x_n]$, the set $\langle S \rangle_{\mathbb{K}[t]}$ is the $\mathbb{K}[t]$-module generated by S.

Example 4.1. *Let $f = 2x_1x_2t^2 - x_1^2t + 4x_1^2$ be a polynomial in $\mathbb{Q}[t][x_1, x_2]$. Let $\succ_{grlex}$ be the grevlex ordering on $\mathbb{Q}[x_1, x_2]$ and $\succ_{grlext}$ the grevlex ordering on $\mathbb{Q}[x_1, x_2, t]$. Then:*

- $\deg(f) = 4$
- $\deg_x(f) = 2$
- $\mathrm{lm}_{\succ_{grlext}}(f) = x_1x_2t^2$
- $\mathrm{lt}_{\succ_{grlext}}(f) = 2x_1x_2t^2$
- $\mathrm{lc}_{\succ_{grlext}}(f) = 2$
- $\mathrm{lm}_{\succ_{grlex},x}(f) = x_1^2$
- $\mathrm{lt}_{\succ_{grlex},x}(f) = (-t+4)x_1^2$
- $\mathrm{lc}_{\succ_{grlex},x}(f) = -t+4$
- $\deg_t(\mathrm{lc}_{\succ_{grlex},x}(f)) = 1$.

For the following proposition, the sets $\mathbb{K}[t][x_1,\ldots,x_n]_d$ and $\mathbb{K}[x_1,\ldots,x_n,t]_d$ are not equal. In fact, $\mathbb{K}[t][x_1,\ldots,x_n]_d$ is the set of x-homogeneous polynomials f in $\mathbb{K}[t][x_1,\ldots,x_n]$ such that $\deg_x(f) = d$.

Proposition 4.2. *Let $f_1,\ldots,f_s$ be x-homogeneous polynomials of the ring $\mathbb{K}[t][x_1,\cdots,x_n]$ with $\deg_x(f_i) = d_i$ and the ideal $I = \langle f_1,\ldots,f_s\rangle$. Consider the $\mathbb{K}][t]$-module $I_d = I\bigcap\mathbb{K}[t][x_1,\ldots,x_n]_d$. This is the set of x-homogeneous polynomials of degree d in I. Then I_d is equal to the $\mathbb{K}[t]$-module $\langle\{f_im_i | m_i \in \mathrm{Mon}_{d-d_i,x}$ and $i \in \{1,\ldots,s\}\}\rangle_{\mathbb{K}[t]}$.*

Proof. It is exactly the same proof that for Proposition 3.1 in Section 3.1 but with coefficients which are polynomials in $\mathbb{K}[t]$. □

Notation 4.3. *Let $f_1,\ldots,f_s$ be polynomials of the ring $\mathbb{K}[t][x_1,\ldots,x_n]$ with $\deg_x(f_i) = d_i$. Define $\phi_3(d,F) = (\mathrm{Mon}_{d,x},\mathrm{Mon}_{d-d_1,x},\ldots,\mathrm{Mon}_{d-d_s,x})$.*

Example 4.4. *Let $F = (x_1t+2x_2, 3x_2^2t^2-4x_1x_2) = (f_1,f_2)$ in $\mathbb{Q}[t][x_1,x_2]$ and $\succ_{grlex}$ be the grevlex ordering on $\mathbb{Q}[x_1,x_2]$, then*

$$\mathrm{Mac}_{\phi_3(3,F),\succ_{grlex}} = \begin{array}{c} \\ x_1^2\cdot f_1 \\ x_1x_2\cdot f_1 \\ x_2^2\cdot f_1 \\ x_1\cdot f_2 \\ x_2\cdot f_2 \end{array} \begin{array}{c} \begin{array}{cccc} x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{array} \\ \begin{pmatrix} t & 2 & 0 & 0 \\ 0 & t & 2 & 0 \\ 0 & 0 & t & 2 \\ 0 & -4 & 3t^2 & 0 \\ 0 & 0 & -4 & 3t^2 \end{pmatrix} \end{array}.$$

Proposition 4.5. *Let f be a x-homogeneous polynomial in the ring $\mathbb{K}[t][x_1,\ldots,x_n]$ with $\deg_x(f) = d$ and $\succ_x$ an admissible monomial ordering on the ring $\mathbb{K}[x_1,\ldots,x_n]$. Consider $\mathrm{Mac}_{\phi_3(d,(f)),\succ_x}$. This is a row vector with entries in $\mathbb{K}[t]$. It is then in weak-Hermite from, write c its pivot and m the monomial in x that indexes the column of the entry c. Then $\mathrm{lm}_{\succ_x,x}(f) = m$ and $\mathrm{lc}_{\succ_x,x}(f) = c$.*

Proof. By Definition 3.2, the monomials that index the columns are ordered with $\succ_x$, then we are done.

□

Proposition 4.6. *Let $F = (f_1, \ldots, f_s)$ a family of x-homogeneous polynomials of $\mathbb{K}[t][x_1, \ldots, x_n]$ with $\deg_x(f_i) = d_i$ and $I = \langle f_1, \ldots, f_n \rangle$. Let us consider I_d for a degree d in $\mathbb{N}$ and $\succ_x$ an admissible monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Let f be a polynomial in I_d and $M = \mathrm{Mac}_{\phi_3(d,F),\succ_x}$. Then there exists a row of the Hermite form of M which represents a polynomial g in I_d such that $\mathrm{lm}_{\succ_x,x}(g)$ is equal to $\mathrm{lm}_{\succ_x,x}(f)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(g)) \leq \deg_t(\mathrm{lc}_{\succ_x,x}(f))$.*

Proof. By Proposition-Definition 2.7, there exists a square unimodular matrix A such that $\widetilde{M} = AM$ is the Hermite form of M. As A is unimodular, by Proposition 2.11, the rows of $\widetilde{M}$ generate the same $\mathbb{K}[t]$-module as the rows of M. By **??**, the rows of M generate I_d. Then the rows of $\widetilde{M}$ generate I_d. Observe that there exists a row vector B which has its entries in $\mathbb{K}[t]$ such that:

$$\mathrm{Mac}_{\phi_3(d,(f)),\succ_x} = B\widetilde{M}.$$

As $\widetilde{M}$ is in Hermite form, by Proposition 2.12 there exists a row of $\widetilde{M}$ such that the column index of its pivot is the same as the one of the pivot of $\mathrm{Mac}_{\mathbb{K}[t],d,\succ_x}\{f\}$. As this row can be seen as a polynomial g in I_d, Proposition 4.5 implies that $\mathrm{lm}_{\succ_x,x}(g)$ is equal to $\mathrm{lm}_{\succ_x,x}(f)$. Moreover, the inequality on the degree in Proposition 2.12 implies that the inequality $\deg_t(\mathrm{lc}_{\succ_x,x}(g)) \leq \deg_t(\mathrm{lc}_{\succ_x,x}(f))$ holds. □

Definition 4.7. *Let $f_1, \ldots, f_s$ be x-homogeneous polynomials of the ring $\mathbb{K}[t][x_1, \cdots, x_n]$ with $\deg_x(f_i) = d_i$ and the ideal $I = \langle f_1, \ldots, f_s \rangle$. The set $F = (f_1, \ldots, f_s)$ is a $\mathbb{K}[t]$-Gröbner basis of $(I, \succ_x)$ if $I = \langle f_1, \ldots, f_s \rangle$ and for all $f \in I$ there exists i in $\{1, \ldots, s\}$ such that $\mathrm{lm}_{\succ_x,x}(f_i)$ divides $\mathrm{lm}_{\succ_x,x}(f)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(f_i)) \leq \deg_t(\mathrm{lc}_{\succ_x,x}(f))$.*

Lemma 4.8. *Let f be a polynomial of $\mathbb{K}[t][x_1, \cdots, x_n]$ and $\succ_x$ be an admissible monomial ordering on $\mathbb{K}[x_1, \cdots, x_n]$. Then*

$$\mathrm{lm}_{\succ_x,x}(f) t^{\deg_t(\mathrm{lc}_{\succ_x,x}(f))} = \mathrm{lm}_{\succ}(f)$$

where $(\succ_x, \succ_{\deg_t}) = \succ$.

Proof. Write

$$f = \sum_{\boldsymbol{\gamma} \in M} a_{\boldsymbol{\gamma}} \boldsymbol{x}^{\boldsymbol{\gamma}}$$

with S a finite subset of $\mathbb{N}^n$ and $a_{\boldsymbol{\gamma}}$ in $\mathbb{K}[t]$ for all $\boldsymbol{\gamma}$ in S. Let $\boldsymbol{\gamma}_0$ be in M such that $\mathrm{lm}_{\succ_x,x}(f) = \boldsymbol{x}^{\boldsymbol{\gamma}_0}$. It is clear that $\boldsymbol{x}^{\boldsymbol{\gamma}_0}$ is the x part of $\mathrm{lm}_{\succ}(f)$ because else, it would not be equal to $\mathrm{lm}_{\succ_x,x}(f)$. It means $\mathrm{lc}_{\succ_x,x}(f)) = a_{\boldsymbol{\gamma}_0}$. Consider $a_{\boldsymbol{\gamma}} \boldsymbol{x}^{\boldsymbol{\gamma}_0}$, compare $t^i \boldsymbol{x}^{\boldsymbol{\gamma}_0}$ for i in $\{0, \ldots, \deg_t(a_{\boldsymbol{\gamma}_0})\}$. Obviously $t^{\deg_t(a_{\boldsymbol{\gamma}_0})} \boldsymbol{x}^{\boldsymbol{\gamma}_0}$ is the greater monomial in f for $\succ$.

□

Proposition 4.9. *Let $f_1, \ldots, f_s$ be x-homogeneous polynomials of the ring $\mathbb{K}[t][x_1, \cdots, x_n]$ with $\deg_x(f_i) = d_i$ and the ideal $I = \langle f_1, \ldots, f_s \rangle$. Let $\succ_x$ be an admissible monomial ordering on $\mathbb{K}[x_1, \cdots, x_n]$. The set $F = (f_1, \ldots, f_s)$ is a $\mathbb{K}[t]$-Gröbner basis of $(I, \succ_x)$ if and only if F is a Gröbner basis of $(I, \succ)$ with $(\succ_x, \succ_{\deg_t}) = \succ$.*

Proof.

($\Rightarrow$) Let F be a $\mathbb{K}[t]$-Gröbner basis of $(I, \succ_x)$. Let p be in I. Then there exists f in F such that $\mathrm{lm}_{\succ_x,x}(f)$ divides $\mathrm{lm}_{\succ_x,x}(p)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(p)) \geq \deg_t(\mathrm{lc}_{\succ_x,x}(f))$. By Lemma 4.8,

$$\mathrm{lm}_{\succ}(f) = \mathrm{lm}_{\succ_x,x}(f)t^{\deg_t(\mathrm{lc}_{\succ_x,x}(f))} \text{ and } \mathrm{lm}_{\succ}(p) = \mathrm{lm}_{\succ_x,x}(f)t^{\deg_t(\mathrm{lc}_{\succ_x,x}(p))}.$$

Observe that $\mathrm{lm}_{\succ}(f)$ divides $\mathrm{lm}_{\succ}(p)$.

($\Leftarrow$) Let F be a Gröbner basis of $(I, \succ)$. Let p be in I. Then there exists f in F such that $\mathrm{lm}_{\succ}(f)$ divides $\mathrm{lm}_{\succ}(p)$. By Lemma 4.8 as above, $\mathrm{lm}_{\succ_x,x}(f)$ divides $\mathrm{lm}_{\succ_x,x}(p)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(p)) \geq \deg_t(\mathrm{lc}_{\succ_x,x}(f))$.

□

Definition 4.10. *Let I be an ideal of $\mathbb{K}[t][x_1, \cdots, x_n]$. Let $f_1, \ldots, f_s$ be x-homogeneous polynomials in I. Let $\succ_x$ be an admissible monomial ordering on $\mathbb{K}[x_1, \cdots, x_n]$. The set $F = (f_1, \ldots, f_s)$ is a $(d, \mathbb{K}[t])$-Gröbner basis of $(I, \succ_x)$ if for all $f \in I$ with $\deg_x(f) \leq d$, there exists i in $\{1, \ldots, s\}$ such that $\mathrm{lm}_{\succ_x,x}(f_i)$ divides $\mathrm{lm}_{\succ_x,x}(f)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(f_i)) \leq \deg_t(\mathrm{lc}_{\succ_x,x}(f))$.*

Proposition 4.11. *Let I be an ideal of $\mathbb{K}[t][x_1, \ldots, x_n]$ and $\succ_x$ an admissible monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. There exists an integer d_0 such that for all $d \geq d_0$, if a set F is a $(d, \mathbb{K}[t])$-Gröbner basis of $(I, \succ_x)$ then F is a $\mathbb{K}[t]$-Gröbner basis of $(I, \succ_x)$.*

Proof. Let $(g_1, \ldots, g_\ell)$ be a minimal Gröbner basis of $(I, \succ)$ with $\succ = (\succ_x, \succ_{\deg(t)})$, write $d_0 = \max(\deg_x(g_1), \ldots, \deg_x(g_\ell))$. Consider $d \geq d_0$ and $F = (f_1, \ldots, f_s)$ a $(d, \mathbb{K}[t])$-Gröbner basis of $(I, \succ_x)$. Let us show that F is a $\mathbb{K}[t]$-Gröbner basis of $(I, \succ_x)$. By Proposition 4.9, we need to show that F is a Gröbner basis of $(I, \succ)$. Let i be in $\{1, \ldots, \ell\}$, by hypothesis, there exists f_j in F such that $\mathrm{lm}_{\succ_x,x}(f_j)$ divides $\mathrm{lm}_{\succ_x,x}(g_i)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(f_j)) \leq \deg_t(\mathrm{lc}_{\succ_x,x}(g_i))$. By Lemma 4.8, this implies that $\mathrm{lm}_{\succ}(f_j)$ divides $\mathrm{lm}_{\succ}(g_i)$. As

$$\langle \mathrm{lm}_{\succ}(g_1), \ldots, \mathrm{lm}_{\succ}(g_\ell) \rangle = \mathrm{lm}_{\succ}(I)$$

then

$$\langle \mathrm{lm}_{\succ}(f_1), \ldots, \mathrm{lm}_{\succ}(f_s) \rangle = \mathrm{lm}_{\succ}(I).$$

By Lemma 2.44,

$$\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_\ell \rangle = I$$

which concludes the proof. □

The following algorithm is a version of Lazard's algorithm that uses the Hermite form.

Algorithm 3 Hermite PM Lazard's Algorithm

Input: homogeneous in x polynomials $F = (f_1, \ldots, f_s)$ of $\mathbb{K}[x_1, \ldots, x_n, t]$ with $\deg_x(f_i) = d_i$, an integer $d_{\max}$, an admissible monomial ordering $\succ_x$.

Output: A $(d_{\max}, \mathbb{K}[t])$-Gröbner basis of $(\langle f_1, \ldots, f_s \rangle, \succ_x)$

1: $G = \{\}$
2: $d_{\min} = \min_{i \in \{1, \cdots, s\}}(\deg_x(f_i))$
3: **for** $d = d_{\min}$ to $d_{\max}$ **do**
4: $\quad M = \mathrm{Mac}_{\phi_3(d,F),\succ_x}$
5: $\quad m_d =$ vector column that contain all the monomials in x of degree d in decreasing order for $\succ_x$.
6: $\quad \widetilde{M} =$ the Hermite form of M
7: $\quad I = \widetilde{M} \cdot m_d$
8: $\quad G = G \bigcup \{h \in I | \forall g \in G \bigcup I, g \neq h, \mathrm{lm}_{\succ_x,x}(g)$ does not divide $\mathrm{lm}_{\succ_x,x}(h)$ or $\mathrm{lm}_{\succ_x,x}(g)$ divides $\mathrm{lm}_{\succ_x,x}(h)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(h)) < \deg_t(\mathrm{lc}_{\succ_x,x}(g))\}$
9: return G

Lemma 4.12. *Let $f_1, \ldots, f_s$ be x-homogeneous polynomials of the ring $\mathbb{K}[t][x_1, \ldots, x_n]$ and $\succ_x$ be an admissible monomial ordering on the ring $\mathbb{K}[x_1, \ldots, x_n]$. Let $d_{\max}$ be an integer. Let G be the output of Algorithm 3. Let $\widetilde{G}$ the output of Algorithm 3 but step 8 of the algorithm is replaced by:*

$$G = G \cup I.$$

The set G is a $(d_{max}, \mathbb{K}[t])$-Gröbner basis of $(I, \succ_x)$ if and only if $\widetilde{G}$ is a $(d_{max}, \mathbb{K}[t])$-Gröbner basis of $(I, \succ_x)$.

Proof.

($\Rightarrow$) Suppose G is a $(d_{max}, \mathbb{K}[t])$-Gröbner basis of $(I, \succ_x)$. As $G \subseteq \widetilde{G}$, then $\widetilde{G}$ is a $(d_{max}, \mathbb{K}[t])$-Gröbner basis of $(I, \succ_x)$.

($\Leftarrow$) Suppose that $\widetilde{G}$ is a $(d_{max}, \mathbb{K}[t])$-Gröbner basis of $(I, \succ_x)$. Let f be in I with $\deg_x(f) \leq d_{max}$, there exists g in $\tilde{G}$ such that $\mathrm{lm}_{\succ_x,x}(g)$ divides $\mathrm{lm}_{\succ_x,x}(f)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(g)) \leq \deg_t(\mathrm{lc}_{\succ_x,x}(f))$. If $g \in G$ then it concludes for this chosen f but if g is not in G then that there exists a $g' \in G$ such that $\mathrm{lm}_{\succ_x,x}(g')$ divides $\mathrm{lm}_{\succ_x,x}(g)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(g')) \leq \deg_t(\mathrm{lc}_{\succ_x,x}(g))$. Finally, that implies that $\mathrm{lm}_{\succ_x,x}(g')$ divides $\mathrm{lm}_{\succ_x,x}(f)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(g')) \leq \deg_t(\mathrm{lc}_{\succ_x,x}(f))$ which concludes the proof.

□

Proposition 4.13. *Let $f_1, \ldots, f_s$ be x-homogeneous polynomials of the ring $\mathbb{K}[t][x_1, \ldots, x_n]$ and $\succ_x$ be an admissible monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Let d_{max} be an integer. Algorithm 3 returns a $(d_{max}, \mathbb{K}[t])$-Gröbner basis of $(\langle f_1, \ldots, f_s \rangle, \succ_x)$.*

Proof. With the same notation as in Lemma 4.12, we need to prove that $\widetilde{G}$ is a $(d_{max}, \mathbb{K}[t])$-Gröbner basis of $(I, \succ_x)$.

Let f be in I with $\deg_x(f) \leq d_{max}$ and $d_{min} = \min(\deg_x(f_i))$. Write

$$f = \sum_{i=1}^{s} u_i f_i \text{ and } f = \sum_{d=d_{min}}^{d_{max}} p_d$$

with $\deg_x(p_d) = d$ and u_i in $\mathbb{K}[t][x_1, \ldots, x_n, t]$. As the f_i are homogeneous we can see that for all d, p_d is in I_d. There exists a d_0 such that $\mathrm{lm}_{\succ_x,x}(f) = \mathrm{lm}_{\succ_x,x}(p_{d_0})$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(p_{d_0})) = \deg_t(\mathrm{lc}_{\succ_x,x}(f))$. By Proposition 4.6, there exists g in $\tilde{G}$ such that $\mathrm{lm}_{\succ_x,x}(g)$ divides $\mathrm{lm}_{\succ_x,x}(p_{d_0})$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(g)) \leq \deg_t(\mathrm{lc}_{\succ_x,x}(p_{d_0}))$. By the equalities above, that implies that $\mathrm{lm}_{\succ_x,x}(g)$ divides $\mathrm{lm}_{\succ_x,x}(f)$ and $\deg_t(\mathrm{lc}_{\succ_x,x}(g)) \leq \deg_t(\mathrm{lc}_{\succ_x,x}(f))$ which means that $\tilde{G}$ is a $(d, \mathbb{K}[t])$-Gröbner basis of $(\langle f_1, \ldots, f_s \rangle, \succ_x)$. □

This algorithm computes a Gröbner basis for this order $(\succ_x, \succ_{\deg_t})$. The problem is that this new algorithm can not return us a grevlex Gröbner basis (for example $t^2 \succ_{drl} x_1$).

4.2 The Popov form for grevlex ordering

This subsection proposes an algorithm which computes a Gröbner basis for the ordering $\succ_{grlext}$ on $\mathbb{K}[x_1, \ldots, x_n, t]$ with $x_1 \succ_{grlext} x_2 \cdots \succ_{grlext} x_n \succ_{grlext} t$. The following definition is about affine $\mathbb{K}[t]$ Macaulay matrices. The changes are that the monomials that index the columns are in degree at most d and the rows represent polynomials of degree at most d (not $\deg_x$).

Notation 4.14. *Let $f_1, \ldots, f_s$ be polynomials of the ring $\mathbb{K}[t][x_1, \ldots, x_n]$ with $\deg(f_i) = d_i$. Define $\phi_4(d, F) = (\mathrm{Mon}_{\leq d,x}, \mathrm{Mon}_{\leq d-d_1,x}, \ldots, \mathrm{Mon}_{\leq d-d_s,x})$ and $\phi_5(d, F) = (\mathrm{Mon}_{\leq d,x}, \mathrm{Mon}_{d-d_1,x}, \ldots, \mathrm{Mon}_{d-d_s,x})$.*

Lemma 4.15. *Let p be a nonzero polynomial in the ring $\mathbb{K}[x_1, \ldots, x_n, t]$ with $\deg(p) = d$. Let $\succ_{grlex}$ be the grevlex ordering on $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ_{grlext}$ be the grevlex ordering on $\mathbb{K}[x_1, \ldots, x_n, t]$. Write p as a vector:*

$$P = \mathrm{Mac}_{\phi_4(d,(p)),\succ_{grlex}}.$$

Let $\mathrm{Mon}_{\leq d-d_i,x}$ be equal to $\{\boldsymbol{x}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}_\ell}\}$ with for all i and j in $\{1, \ldots, \ell\}$, $i < j$ if and only if $\boldsymbol{x}^{\boldsymbol{\alpha}_j} \succ_{grlex} \boldsymbol{x}^{\boldsymbol{\alpha}_j}$. Consider the shift s defined as follows and $\mathrm{LM}_s(P)$ the leading matrix of P for the shift s.

$$\begin{array}{r} \\ s \to \\ P \to \\ \mathrm{LM}_s(P) \to \end{array} \begin{array}{c} \begin{array}{cccccc} \boldsymbol{x}^{\boldsymbol{\alpha}_\ell} & \ldots & \underline{x}^{\underline{\alpha}_{i_0}} & \ldots & 1 \end{array} \\ \left(\begin{array}{cccccc} \deg(\boldsymbol{x}^{\boldsymbol{\alpha}_\ell}) & \ldots & \deg(\boldsymbol{x}^{\boldsymbol{\alpha}_{i_0}}) & \ldots & 0 \\ \hline q_\ell(t) & \ldots & q_{i_0}(t) & \ldots & q_1(t) \\ \hline 0 & \cdots & a_{i_0} & \ldots & a_1 \end{array}\right) \end{array}$$

The entry a_{i_0} is the pivot of $\mathrm{LM}_s(P)$ for i_0 in $\{1, \ldots, \ell\}$, so q_{i_0} is the s-pivot of P. The equality

$$\mathrm{lm}_{\succ_{grlext}}(p) = \boldsymbol{x}^{\alpha_{i_0}} t^{\deg_t(q_{i_0})}$$

holds.

Proof. As $\succ_{grlext}$ is an admissible monomial ordering, then for two monomials m_1 and m_2, if m_1 divides m_2 then $m_2 \succeq_{grlext} m_1$. This means that we need to compare the $\boldsymbol{x}^{\underline{\alpha}_i} t^{\deg_t(q_i)}$ with $i \in \{1, \ldots, \ell\}$ to find the leading monomial of p. Write $\mathrm{lm}_{\succ_{grlext}}(p) = \boldsymbol{x}^{\boldsymbol{\alpha}_{j_0}} t^{\deg_t(q_{j_0})}$. Observe that

$$\begin{aligned} \deg(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_0}} t^{\deg_t(q_{j_0})}) &= \deg(\mathrm{lm}_{\succ_{grlext}}(p)) \\ &= \max_{i \in \{1,\ldots,\ell\}} (\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_i} t^{\deg_t(q_i)})). \end{aligned}$$

On the other hand, observe that

$$\begin{aligned}\mathrm{rdeg}_s(P) &= \max_{i\in\{1,\dots,\ell\}}(\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_i}) + \deg_t(q_i)) \\ &= \max_{i\in\{1,\dots,\ell\}}(\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_i}t^{\deg_t(q_i)})).\end{aligned}$$

By Definition 2.18, for all j in $\{1,\dots,\ell\}$:

$$\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_j}t^{\deg_t(q_j)}) = \max_{i\in\{1,\dots,c\}}(\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_i}t^{\deg_t(q_i)})) \iff a_j \neq 0.$$

We have shown that $a_{j_0} \neq 0$ but now we must show that $i_0 = j_0$. Observe that if we show that for all i in $\{1,\dots,\ell\}$,

$$\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_i}t^{\deg_t(q_i)}) = \mathrm{rdeg}_s(P) \text{ implies that } j_0 \geq i$$

then we are done. Note that it is equivalent to: for all i in $\{1,\dots,\ell\}$,

$$\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_i}t^{\deg_t(q_i)}) = \mathrm{rdeg}_s(P) \text{ implies that } \boldsymbol{x}^{\boldsymbol{\alpha}_i} \preccurlyeq_{grlex} \boldsymbol{x}^{\boldsymbol{\alpha}_{j_0}}.$$

Let i be in $\{1,\dots,\ell\}$ such that $\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_i}t^{\deg_t(q_i)}) = \mathrm{rdeg}_s(P)$. We deduce that $\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_i}t^{\deg_t(q_i)}) = \deg(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_0}}t^{\deg_t(q_{j_0})})$, as $\boldsymbol{x}^{\boldsymbol{\alpha}_i}t^{\deg_t(q_i)} \preccurlyeq_{grlext} \boldsymbol{x}^{\boldsymbol{\alpha}_{j_0}}t^{\deg_t(q_{j_0})}$. There are two possibilities.

- If $\deg_t(q_{j_0}) < \deg_t(q_i)$, then $\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_i}) < \deg(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_0}})$ which implies that $\boldsymbol{x}^{\boldsymbol{\alpha}_i} \prec_{grlex} \boldsymbol{x}^{\boldsymbol{\alpha}_{j_0}}$.
- If $\deg_t(q_{j_0}) = \deg_t(q_i)$, then $\deg(\boldsymbol{x}^{\boldsymbol{\alpha}_i}) = \deg(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_0}})$. As the inequality $\boldsymbol{x}^{\boldsymbol{\alpha}_i}t^{\deg_t(q_i)} \preccurlyeq_{grlext} \boldsymbol{x}^{\boldsymbol{\alpha}_{j_0}}t^{\deg_t(q_{j_0})}$ holds, then $\boldsymbol{x}^{\boldsymbol{\alpha}_i} \preccurlyeq_{grlex} \boldsymbol{x}^{\boldsymbol{\alpha}_{j_0}}$.

□

Example 4.16. *Let $p = x^2 + (t^2 - t)y + 2t^3$ be a polynomial in $\mathbb{K}[x, y, t]$ and let $s = (2, 2, 2, 1, 1, 0)$ be a shift. We use Lemma 4.15 to find its leading monomial:*

$$P = \begin{array}{c} \begin{matrix} x^2 & xy & y^2 & x & y & 1 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & t^2-t & 2 \end{pmatrix} \end{array}$$

$$\mathrm{LM}_s(P) = \begin{array}{c} \begin{matrix} x^2 & xy & y^2 & x & y & 1 \end{matrix} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix} \end{array}$$

Observe that the s-pivots of P is $t^2 - t$ which column index is y. In fact, yt^2 is the leading monomial of p for the grevlex ordering.

For the following definition we refer the reader to [3, Definition 2.1].

Definition 4.17. *Let I be an ideal of $\mathbb{K}[x_1, \dots, x_n, t]$ and $\succ$ be an admissible monomial ordering on $\mathbb{K}[x_1, \dots, x_n, t]$. The set I is t-stabilized if for all $m \in \mathrm{lm}_\succ(I)$ such that t divides m and for all i in $\{1, \dots, n\}$, $\frac{m}{t}x_i \in \mathrm{lm}_\succ(I)$.*

Lemma 4.18. *Let I be a zero-dimensional ideal of $\mathbb{K}[x_1,\dots,x_n,t]$ and $\succ$ be an admissible monomial ordering on $\mathbb{K}[x_1,\dots,x_n,t]$. If the ideal I is t-stabilized and $G=(g_1,\dots,g_s)$ is a Gröbner basis of $(I,\succ)$. then for all monomial m in $\mathrm{lm}_\succ(\mathbb{K}[x_1,\dots,x_n,t])\setminus \mathrm{lm}_\succ(I)$ there exists i in $\{1,\cdots,s\}$ such that $\mathrm{lm}_\succ(g_i)=mt^j$ with j in $\mathbb{N}$.*

Proof. Suppose without loss of generality that G is minimal. Let m be a monomial of $\mathrm{lm}_\succ(\mathbb{K}[x_1,\dots,x_n,t])\setminus \mathrm{lm}_\succ(I)$. As I is zero-dimensional, by Proposition 2.40 there exists j in $\mathbb{N}$ such that mt^j lies in $\mathrm{lm}_\succ(I)$. Suppose that j is the smallest positive integer such that mt^j lies in $\mathrm{lm}_\succ(I)$. As m is not in $\mathrm{lm}_\succ(I)$, then $j\geq 1$. By Definition 2.36, there exists g in G such that $\mathrm{lm}_\succ(g)$ divides mt^j. If $\mathrm{lm}_\succ(g)=mt^j$, then we are done. If there is no f in G such that $\mathrm{lm}_\succ(f)=mt^j$, there exists a monomial m_0 such that $\mathrm{lm}_\succ(g)m_0=mt^j$ and $m\neq 1$. The variable t does not divide m_0 because mt^{j-1} does not lie in $\mathrm{lm}_\succ(I)$, so t divides $\mathrm{lm}_\succ(g)$. As m_0 is not 1, there exists i in $\{1,\dots,n\}$ such that there exists a monomial m_1 with $m_0=m_1x_i$. As I is t-stabilized, the monomial $\frac{\mathrm{lm}_\succ(g)}{t}x_i$ lies in $\mathrm{lm}_\succ(I)$. Observe that

$$\frac{\mathrm{lm}_\succ(g)}{t}x_im_1=mt^{j-1}.$$

As $\frac{\mathrm{lm}_\succ(g)}{t}x_im_1$ lies in $\mathrm{lm}_\succ(I)$, this is a contradiction with the minimality of j. □

Theorem 1. ***Popov-Structure theorem on Gröbner basis***
Let I be an ideal of $\mathbb{K}[x_1,\dots,x_n,t]$, let $\succ_{grlext}$ be the grevlex ordering on the ring $\mathbb{K}[x_1,\dots,x_n,t]$ and $\succ_{grlex}$ be the grevlex ordering on $\mathbb{K}[x_1,\dots,x_n]$. Let $(g_1,\dots,g_\ell)$ be a Gröbner basis of $(I,\succ_{grlext})$ with for all $i,j\in\{1,\cdots,\ell\}$, $i<j$ implies that the x part of $\mathrm{lm}_{\succ_{grlext}}(g_i)$ is greater than the x part of $\mathrm{lm}_{\succ_{grlext}}(g_j)$ for $\succ_{grlex}$. Define s the shift that gives to a column the degree of the monomial which index this column as in Lemma 4.15. Write

$$G_i=\mathrm{Mac}_{\phi_4(\deg(g_i),(g_i)),\succ_{grlex}},$$

then:

1) *The matrix*
$$G=\begin{pmatrix}G_1\\ \vdots\\ G_\ell\end{pmatrix}$$
is in s-weak-Popov form.
2) *If $(g_1,\dots,g_\ell)$ is the minimal reduced Gröbner basis of $(I,\succ_{grlext})$, then G is in s-Popov form.*
3) *If I is zero-dimensional and t-stabilized and $(g_1,\dots,g_\ell)$ is the minimal reduced Gröbner basis of $(I,\succ_{grlext})$, then the sum of maximal degrees over each column of G is equal to the cardinal of the set of monomials $\mathrm{lm}_{\succ_{grlext}}(\mathbb{K}[x_1,\dots,x_n,t])\setminus \mathrm{lm}_{\succ_{grlext}}(I)$.*

Proof. 1) Observe that

$$\mathrm{LM}_s(G) = \begin{pmatrix} \mathrm{LM}_s(G_1) \\ \vdots \\ \mathrm{LM}_s(G_\ell) \end{pmatrix}.$$

By Lemma 4.15, the pivot of $\mathrm{LM}_s(G_i)$ is in the column indexed by the x part $\mathrm{lm}_{\succ_{grlext}}(g_i)$ for all i in $\{1,\dots,\ell\}$. By our hypothesis on the x parts of the $\mathrm{lm}_{\succ_{grlext}}(g_i)$, the matrix $\mathrm{LM}_s(G)$ is in row echelon form. Then by Definition 2.20, G is in s-weak-Popov form.

2) Let m be a monomial that is the index of a column that contain a s-pivot. If an entry of this column that is not the s-pivot has a greater or equal degree than the s-pivot that means that there exists g_i and g_j such that $\mathrm{lm}_{\succ_{grlext}}(g_i)$ divides one of the monomial of g_j. That is not possible because $(g_1,\dots,g_\ell)$ is the minimal reduced Gröbner basis of $(I,\succ_{grlext})$, so by Definition 2.22 G is in s-Popov form.

3) As $(g_1,\dots,g_\ell)$ is the minimal reduced Gröbner basis of $(I,\succ_{grlext})$, the monomials in the polynomials $g_1,\dots,g_\ell$ are elements of

$$(\mathrm{lm}_{\succ_{grlext}}(\mathbb{K}[x_1,\dots,x_n,t])\setminus \mathrm{lm}_{\succ_{grlext}}(I)) \bigcup_{i\in 1,\dots,\ell} \{\mathrm{lm}_{\succ_{grlext}}(g_i)\}.$$

From this and Lemma 4.18 that can be applied as I is zero-dimensional and t-stabilized, we deduce that in the matrix G, a column that does not contain a s-pivot is a column of zeroes. Write $G_{i,j}$ the entries of G, note that

$$\begin{aligned}\sum_{j\in\{1,\dots,c\}} \max_{i\in\{1,\dots,\ell\}}(\deg_t(G_{i,j})) &= \sum_{\text{column } j \text{ with a pivot}} \max_{i\in\{1,\dots,\ell\}}(\deg_t(G_{i,j})),\\ &\text{as } (g_1,\dots,g_\ell) \text{ is minimal reduced,}\\ &= \sum_{i\in\{1,\dots,\ell\}} \deg_t(\mathrm{lm}_{\succ_{grlext}}(g_i)).\end{aligned}$$

We prove that the cardinal of the set

$$\mathrm{lm}_{\succ_{grlext}}(\mathbb{K}[x_1,\dots,x_n,t])\setminus \mathrm{lm}_{\succ_{grlext}}(I)$$

is equal to

$$\sum_{i\in\{1,\dots,\ell\}} \deg_t(\mathrm{lm}_{\succ_{grlext}}(g_i)).$$

By Lemma 4.18,

$$\mathrm{lm}_{\succ_{grlext}}(\mathbb{K}[x_1,\dots,x_n,t])\setminus \mathrm{lm}_{\succ_{grlext}}(I) = \bigsqcup_{i\in\{1,\dots,\ell\}} E_i$$

where E_i is the set of elements of $\mathrm{lm}_{\succ_{grlext}}(\mathbb{K}[x_1,\dots,x_n,t])\setminus \mathrm{lm}_{\succ_{grlext}}(I)$ that have the same x part as $\mathrm{lm}_{\succ_{grlext}}(g_i)$. Write

$$\mathrm{lm}_{\succ_{grlext}}(g_i) = mt^{\deg_t(\mathrm{lm}_{\succ_{grlext}}(g_i))}$$

with m is the x part, the cardinal of E_i is $\deg_t(\mathrm{lc}_{\succ_{grlext}}(g_i))$. As the cardinal of $\bigsqcup_{i\in\{1,\dots,\ell\}} E_i$ is equal to

$$\sum_{i\in\{1,\dots,\ell\}} \deg_t(\mathrm{lm}_{\succ_{grlext}}(g_i))$$

we are done

□

Proposition 4.19. *Let $F = (f_1,\dots,f_\ell)$ be a sequence of polynomials of the ring $\mathbb{K}[x_1,\dots,x_n,t]$ with $\deg(f_i) = d_i$ and $I = \langle f_1,\dots,f_\ell\rangle$. Let $\succ_{grlex}$ be the grevlex ordering on $\mathbb{K}[x_1,\dots,x_n]$ and $\succ_{grlext}$ be the grevlex ordering on $\mathbb{K}[x_1,\dots,x_n,t]$. Let d be an integer, write the $\mathbb{K}[t]$-module*

$$E_d = \langle \{mf_i \mid i\in\{1,\dots,\ell\}, m\in \mathrm{Mon}_{\leq d-d_i,x}\}\rangle_{\mathbb{K}[t]}$$

and the matrix

$$M = \mathrm{Mac}_{\phi_4(d,F)),\succ_{grlex}}.$$

Let s be the shift that gives to a monomial its degree. Let $\widetilde{M}$ be a s-weak-Popov form of M. Let f be a polynomial of E_d, then there exists a row of the matrix $\widetilde{M}$ that represents a polynomial g such that $\mathrm{lm}_{\succ_{grlext}}(g)$ divides $\mathrm{lm}_{\succ_{grlext}}(f)$.

Proof. It is clear that the rows of M generate the $\mathbb{K}[t]$-module E_d. By Proposition 2.11 and Proposition 2.23, the rows of the matrix $\widetilde{M}$ also generate E_d. Let f be in E_d. Then there exists a row vector B with entries in $\mathbb{K}[t]$ such that

$$\mathrm{Mac}_{\phi_5(\deg(f),(f))),\succ_{grlex}} = B\widetilde{M}.$$

As $\widetilde{M}$ is in s-weak-Popov form we can apply Proposition 2.26 and deduce that the s-pivot of $\mathrm{Mac}_{\phi_5(\deg(f),(f))),\succ_{grlex}}$ has the same column index as one of a row of $\widetilde{M}$. Moreover, the degree of the s-pivots is greater or equal than the degree of the s-pivot of this row in $\widetilde{M}$. Let us call g the polynomial that is represented by this row in $\widetilde{M}$. By Lemma 4.15 that means exactly that $\mathrm{lm}_{\succ_{grlext}}(g)$ divides $\mathrm{lm}_{\succ_{grlext}}(f)$. □

Proposition 4.20. *Let $F = (f_1,\dots,f_\ell)$ be a regular sequence of polynomials of the ring $\mathbb{K}[x_1,\dots,x_n,t]$ with $\deg(f_i) = d_i$ and $I = \langle f_1,\dots,f_\ell\rangle$.*

Let $\succ_{grlex}$ be the grevlex ordering on $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ_{grlext}$ be the grevlex ordering on $\mathbb{K}[x_1, \ldots, x_n, t]$. Let $d_{\max}$ be equal to the Macaulay bound of F:

$$\sum_{i=1}^{\ell}(d_i - 1) + 1.$$

Then Algorithm 4 return a Gröbner basis of $(I, \succ_{grlext})$.

Proof. Write the $\mathbb{K}[t]$-module

$$E_{d_{\max}} = \langle \{mf_i \mid i \in \{1, \ldots, \ell\}, m \in \mathrm{Mon}_{\leq d_{max} - d_i, x}\} \rangle_{\mathbb{K}[t]}.$$

By 3.9, the $\mathbb{K}[t]$-vector space

$$V = \langle mf_i \mid i \in \{1, \ldots, \ell\}, m \in \mathrm{Mon}_{\leq d_{\max} - d_i} \rangle_{\mathbb{K}}$$

contains a Gröbner basis G of $(I, \succ_{grlext})$ as $d_{\max}$ is the Macaulay bound and as F is regular. Let g be in G, then g is in V. As $V \subseteq E_{d_{\max}}$, g is in $E_{d_{\max}}$. Write $\widetilde{G}$ the output of Algorithm 4. By Proposition 4.19, there exists $\tilde{g}$ in $\widetilde{G}$ such that $\mathrm{lm}_{\succ_{grlext}}(\tilde{g})$ divides $\mathrm{lm}_{\succ_{grlext}}(g)$. As G is a Gröbner basis of $(I, \succ_{grlext})$, then $\widetilde{G}$ is a Gröbner basis of $(I, \succ_{grlext})$. □

Algorithm 4 grevlex PM Lazard's Algorithm

Input: polynomials $F = (f_1, \ldots, f_\ell)$ of $\mathbb{K}[x_1, \ldots, x_n, t]$ with $\deg(f_i) = d_i$ and an integer d_{max}.

Output: A Gröbner basis of $(\langle f_1, \ldots, f_\ell \rangle, \succ_{grlext})$

1: $G = \{\}$
2: $d_{min} = \min_{i \in \{1, \cdots, \ell\}}(\deg(f_i))$.
3: **for** $d = d_{min}$ to d_{max} **do**
4: $\quad M = \mathrm{Mac}_{\phi_4(d,F)), \succ_{grlex}}$
5: $\quad m_d$ = vector column that contain all the monomials in x of degree at most d in decreasing order for $\succ_{grlex}$.
6: $\quad s$ = row vector of same length as m_d that gives the degree of all the monomials in x of degree at most d in decreasing order for $\succ_{grlex}$.
7: $\quad \widetilde{M}$ = the s-Popov form of M
8: $\quad I = \widetilde{M} \times m_d$
9: $\quad G = G \bigcup \{h \in I | \forall g \in G \bigcup I, g \neq h, \mathrm{lm}_{\succ_{grlext}}(g)$ does not divide $\mathrm{lm}_{\succ_{grlext}}(h)\}$
10: return G

The foolowing definition can be found in [6, Definition 25.8]

Definition 4.21. *Let $f, g : \mathbb{N} \to \mathbb{R}$ be positive. Then we write $f \in \mathcal{O}^{\sim}(g)$, if $f(n) \in g(n)(\log_2(3 + g(n)))^{\mathcal{O}(1)}$ or equivalently, if there are constants $N, c \in \mathbb{N}$ such that $f(n) \leq g(n)(\log_2(3 + g(n)))^c$ for all $n \geq N$.*

The following theorem can be found in [16, Section 5.1].

Theorem 4.22. *Let M be a matrix in $\mathbb{K}[t]^{r\times c}$ of degree at most d with $r \leq c$ and s be a positive shift. There exists a deterministic algorithm which computes the Popov form of M using $\mathcal{O}^{\sim}(r^{\omega-1}c(d+\text{amp}(s)))$ operations in $\mathbb{K}$.*

The following result can be found in [19, Section 1].

Theorem 4.23. *Let M be a matrix in $\mathbb{K}[t]^{r\times c}$ of degree at most d with $r \geq c$. There is a deterministic algorithm which computes a row basis of M using $\mathcal{O}^{\sim}(c^{\omega-1}rd)$ operations in $\mathbb{K}$.*

Let $F = (f_1, \ldots, f_\ell)$ be a sequence of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Suppose that F is regular Definition 2.47 and that $\langle f_1, \ldots, f_\ell\rangle$ is zero-dimensional. That implies that $\ell = n$ by [11, page20,definition 19].

Let us suppose that for all i in $\{1, \ldots, n\}$, $\deg(f_i) = d$ in $\mathbb{N}$. Now write the Macaulay bound:

$$D = 1 - n + \sum_{i=1}^{n} d = 1 + n(d-1).$$

The goal is to compare the number of operations in $\mathbb{K}$ that Algorithms 2 and 4 use to compute the row echelon form and the s-Popov form of the larger Macaulay matrices that appear in those algorithms.

1) Analysis for Algorithm 2.
   As seen in Section 3.3, the number of rows is $n\binom{D-d+n}{n}$ and the number of columns is $\binom{D+n}{n}$ in the final Macaulay matrix called M. By Proposition 3.15, we can suppose there is more rows than columns in the matrix. By Theorem 3.18, it takes

$$\text{rank}(M)^{\omega-2}n\binom{D-d+n}{n}\binom{D+n}{n} \leq \binom{D+n}{n}^{\omega-1} n\binom{D-d+n}{n}$$

   operations in $\mathbb{K}$.
2) Analysis for Algorithm 4.
   In Algorithm 4, consider that $x_n = t$ to have the same situation as above. The number of rows is $n\binom{D-d+n-1}{n-1}$ and the number of columns is $\binom{D+n-1}{n-1}$ in the final Macaulay matrix called M_1 in $\mathbb{K}[t]^{r\times c}$. Observe

that the shift s in Algorithm 4 is such that $\mathrm{amp}(s) \leq D$. The first step is to compute M_2 a row basis of M_1 using

$$c^{\omega-1}rd \leq rc^{\omega-1}(d+D)$$

operations in $\mathbb{K}$ by Theorem 4.23. This theorem can be applied as there is more rows than column in the Macaulay matrix by Section 3.3. The second step is to compute the s-Popov form of M_2 (which is the one of M_1) in $\mathbb{K}[t]^{\mathrm{rank}(M_1)\times c}$, by Theorem 4.22 it takes

$$\begin{aligned}\mathrm{rank}(M_1)^{\omega-1}c(d+D) &\leq \mathrm{rank}(M_1)c^{\omega-1}(d+D)\\ &\leq rc^{\omega-1}(d+D)\end{aligned}$$

operations in $\mathbb{K}$. We deduce that it takes

$$rc^{\omega-1}(d+D) = n\binom{D-d+n-1}{n-1}\binom{D+n-1}{n-1}^{\omega-1}(d+D)$$

operations in $\mathbb{K}$ to compute the s-Popov form of M_1.

Let us compare these two numbers of operations.

$$\begin{aligned}&\frac{\binom{D+n}{n}^{\omega-1}n\binom{D-d+n}{n}}{n\binom{D-d+n-1}{n-1}\binom{D+n-1}{n-1}^{\omega-1}(d+D)}\\ &= \left(\frac{D-d+n}{n}\right)\left(\frac{D+n}{n}\right)^{\omega-1}\left(\frac{1}{D+d}\right)\\ &= \left(\frac{(n-1)d+1}{n}\right)\left(\frac{nd+1}{n}\right)^{\omega-1}\left(\frac{1}{(n+1)d-n+1}\right).\end{aligned}$$

This last result is less than

$$\left(\frac{(n-1)d}{n}\right)d^{\omega-1}\left(\frac{1}{(n+1)d}\right) = \boxed{\left(\frac{d^{\omega-1}}{n}\right)\left(\frac{n-1}{n+1}\right)}.$$

Theorem 2. *Let $F = (f_1, \ldots, f_\ell)$ be a regular sequence of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ with $\deg(f_i) = d_i$. Suppose $\langle f_1, \ldots, f_\ell\rangle$ is zero dimensional. Write $D = \sum_{i=1}^{\ell}(d_i - 1) + 1$. The number of operations in $\mathbb{K}$ that Algorithm 4 uses is*

$$\mathcal{O}^{\sim}\left(n\binom{D-d+n-1}{n-1}\binom{D+n-1}{n-1}^{\omega-1}(d+D)\right).$$

Proof. It is Item 2)

□

Conclusion: Let A and B be respectively the number of operations in $\mathbb{K}$ used in Algorithms 2 and 4. Then

$$\frac{A}{B} \geq \left(\frac{d^{\omega-1}}{n}\right)\left(\frac{n-1}{n+1}\right).$$

References

[1] Magali Bardet, Jean-Charles Faugere, and Bruno Salvy. On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

[2] Bernhard Beckermann, George Labahn, and Gilles Villard. Normal forms for general polynomial matrices. *Journal of Symbolic Computation*, pages 708–737, 2006.

[3] Jérémy Berthomieu, Vincent Neiger, and Mohab Safey El Din. Faster change of order algorithm for gröbner bases under shape and stability assumptions. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, pages 409–418, 2022.

[4] Bruno Buchberger. *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal.* PhD thesis, Ph. D. thesis, University of Innsbruck, Austria, 1965.

[5] Bruno Buchberger. Introduction to gröbner bases[1]. *Gröbner bases and applications*, 1998.

[6] Laurent Busé. Computational algebraic geometry. 2021.

[7] PETE L CLARK. Reduced row echelon form.

[8] David Cox, John Little, Donal O'Shea, and Moss Sweedler. Ideals, varieties, and algorithms. *American Mathematical Monthly*, 1994.

[9] Jean-Charles Faugere. A new efficient algorithm for computing gröbner bases (f4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.

[10] Jean Charles Faugere. A new efficient algorithm for computing gröbner bases without reduction to zero (f 5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, 2002.

[11] Jean-Charles Faugère. Résolution de systèmes polynomiaux en utilisant les bases de gröbner. 2015.

[12] Jean-Charles Faugere and Antoine Joux. Algebraic cryptanalysis of hidden field equation (hfe) cryptosystems using gröbner bases. In *Annual International Cryptology Conference*, pages 44–60. Springer, 2003.

[13] Jorge García Fontán, Abhilash Nayak, Sébastien Briot, and Mohab Safey El Din. Singularity analysis for the perspective-four and five-line problems. *International Journal of Computer Vision*, 130(4):909–932, 2022.

[14] Louise Huot. *Résolution de systèmes polynomiaux et cryptologie sur les courbes elliptiques*. PhD thesis, Citeseer, 2013.

[15] Daniel Lazard. Gröbner bases, gaussian elimination and resolution of systems of algebraic equations. In *European Conference on Computer Algebra*, pages 146–156. Springer, 1983.

[16] Vincent Neiger, Johan Rosenkilde, and Grigory Solomatov. Computing popov and hermite forms of rectangular polynomial matrices. In *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*, pages 295–302, 2018.

[17] Arne Storjohann. *Computation of Hermite and Smith normal forms of matrices*. PhD thesis, Citeseer, 1994.

[18] Arne Storjohann. *Algorithms for matrix canonical forms*. PhD thesis, ETH Zurich, 2000.

[19] Wei Zhou and George Labahn. Computing column bases of polynomial matrices. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, 2013.