On FGLM Algorithms with Tropical Gröbner bases

Yuki Ishihara, Tristan Vaccon, Kazuhiro Yokoyama

On FGLM Algorithms with Tropical Gröbner bases

Yuki Ishihara
Graduate School of Science, Rikkyo University
Tokyo, Japan
yishihara@rikkyo.ac.jp

Tristan Vaccon
Université de Limoges; CNRS, XLIM UMR 7252
Limoges, France
tristan.vaccon@unilim.fr

Kazuhiro Yokoyama
Departement of Mathematics, Rikkyo University
Tokyo, Japan
kazuhiro@rikkyo.ac.jp

ABSTRACT

Let K be a field equipped with a valuation. Tropical varieties over K can be defined with a theory of Gröbner bases taking into account the valuation of K. Because of the use of the valuation, the theory of tropical Gröbner bases has proved to provide settings for computations over polynomial rings over a p-adic field that are more stable than that of classical Gröbner bases. In this article, we investigate how the FGLM change of ordering algorithm can be adapted to the tropical setting.

As the valuations of the polynomial coefficients are taken into account, the classical FGLM algorithm's incremental way, monomomial by monomial, to compute the multiplication matrices and the change of basis matrix can not be transposed at all to the tropical setting. We mitigate this issue by developing new linear algebra algorithms and apply them to our new tropical FGLM algorithms.

Motivations are twofold. Firstly, to compute tropical varieties, one usually goes through the computation of many tropical Gröbner bases defined for varying weights (and then varying term orders). For an ideal of dimension 0, the tropical FGLM algorithm provides an efficient way to go from a tropical Gröbner basis from one weight to one for another weight. Secondly, the FGLM strategy can be applied to go from a tropical Gröbner basis to a classical Gröbner basis. We provide tools to chain the stable computation of a tropical Gröbner basis (for weight $[0, \dots, 0]$) with the p-adic stabilized variants of FGLM of [RV16] to compute a lexicographical or shape position basis.

All our algorithms have been implemented into SageMath. We provide numerical examples to illustrate time-complexity. We then illustrate the superiority of our strategy regarding to the stability of p-adic numerical computations.

CCS CONCEPTS

• **Computing methodologies → Algebraic algorithms**.

KEYWORDS

Algorithms, Tropical Geometry, Gröbner bases, FGLM algorithm, p-adic precision

ISSAC '20, July 20–23, 2020, Kalamata, Greece

ACM ISBN 978-1-4503-7100-1/20/07…$15.00
https://doi.org/10.1145/3373207.3404037

ACM Reference Format:
Yuki Ishihara, Tristan Vaccon, and Kazuhiro Yokoyama. 2020. On FGLM Algorithms with Tropical Gröbner bases. In *International Symposium on Symbolic and Algebraic Computation (ISSAC '20), July 20–23, 2020, Kalamata, Greece.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3373207.3404037

1 INTRODUCTION

The development of tropical geometry is now more than three decades old. It has generated significant applications to very various domains, from algebraic geometry to combinatorics, computer science, economics, optimisation, non-archimedean geometry and many more. We refer to [MS15] for a complete introduction.

Effective computation of tropical varieties are now available using Gfan and Singular (see [JRS19] , [GRZ19]). Those computations often rely on the computation of so-called tropical Gröbner bases (we use *GB* for Gröbner bases in the following). Since Chan and Maclagan's definition of tropical Gröbner bases taking into account the valuation in [CM19], computations of tropical GB are available over fields with trivial or non-trivial valuation, using various methods: Matrix F5 in [Va15], F5 in [VY17, VVY18] or lifting in [MR19].

An important motivation for studying the computation of tropical GB is their numerical stability. It has been proved in [Va15] that for polynomial ideals over a p-adic field, computing tropical GB (which by definition take into account the valuation), can be significantly more stable than classical GB.

Unfortunately, no tropical term ordering can be an elimination order, hence tropical GB can not be used directly for solving polynomial systems. Our work is then motivated by the following question: can we take advantage of the numerical stability of the computation of tropical GB to compute a shape position basis in dimension zero through a change of ordering algorithm?

In this article, we tackle this problem by studying the main change of ordering algorithm, FGLM [FGLM93]. On the way, we investigate some adaptations and optimizations of this algorithm designed to take advantage of some special properties of the ideal (*e.g.* Borel-fixedness of its initial ideal).

We also provide a way to go from a tropical term order to another. This produces another motivation: difficulty of computation can vary significantly depending on the term order (see §8.1 of [VVY18]), hence, using a tropical FGLM algorithm, one could go from an easy term order to a harder one in an efficient way.

Finally, we conclude with numerical data to estimate the loss in precision for the computation of a lex Gröbner basis using a tropical F5 algorithm followed by an FGLM algorithm, in an affine setting, and also numerical data to illustrate the behavior of the various variants of FGLM handled along the way.

1.1 Related works

Chan and Maclagan have developed in [CM19] a Buchberger algorithm to compute tropical GB for homogeneous input polynomials (using a special division algorithm). Following their work, adaptations of the F5 strategies have been developped in [Va15, VY17, VVY18] culminating with complete F5 algorithms for affine input polynomials.

A completely different approach has been developped by Markwig and Ren in [MR19], relating the computation of tropical GB in $K[X_1, \dots, X_n]$ to the computation of standard basis in $R[\![t]\!][X_1, \dots, X_n]$ (for R a subring of the ring of integers of K). It can be connected to the Gfanlib interface in Singular to compute tropical varieties (see: [JRS19]).

Finally, Görlach, Ren and Zhang have developped in [GRZ19] a way to compute zero-dimensional tropical varieties using shape position bases and projections. Their algorithms take as input a lex Gröbner basis in shape position. Our strategies can be used to provide such a basis stably (precision-wise) when working with p-adic numbers, and be chained with their algorithms.

1.2 Notations

Let K be a field with a discrete valuation val such that K is complete with respect to the norm defined by val. We denote by $R = O_K$ its ring of integers, m_K its maximal ideal (with π a uniformizer), and $k = O_K/m_K$ its fraction field. We refer to Serre's Local Fields [Ser79] for an introduction to such fields. Classical examples of such fields are $K = \mathbb{Q}_p$, with p-adic valuation, and $\mathbb{Q}((X))$ or $\mathbb{F}_q((X))$ with X-adic valuation.

The polynomial ring $K[X_1, \dots, X_n]$ (for some $n \in \mathbb{Z}_{>0}$) will be denoted by A, and for $u = (u_1, \dots\ , u_n) \in \mathbb{Z}^n_{\geq 0}$, we write x^u for $X_1^{u_1} \dots X_n^{u_n}$. For $g \in A$, $|g|$ denotes the total degree of g and $A_{\leq d}$ the set of all polynomials in A of total degree less than d. The matrix of a finite list of polynomials (of total degree $\leq d$ for some d) written in a basis of monomials (of total degree $\leq d$) is called a *Macaulay matrix*.

For $w \in Im(\text{val})^n \subset \mathbb{R}^n$ and $\leq_m$ a monomial order on A, we define $\leq$ a tropical term order as in the following definition:

Definition 1.1. Given $a, b \in K^* = K \setminus \{0\}$ and x^α and x^β two monomials in A, we write $ax^\alpha < bx^\beta$ if:

- $|x^\alpha| < |x^\beta|$, or
- $|x^\alpha| = |x^\beta|$, and $\text{val}(a) + w \cdot \alpha > \text{val}(b) + w \cdot \beta$, or
- $|x^\alpha| = |x^\beta|$, $\text{val}(a) + w \cdot \alpha = \text{val}(b) + w \cdot \beta$ and $x^\alpha <_m x^\beta$.

For u of valuation 0, we write $ax^\alpha =_\leq uax^\alpha$. Accordingly, $ax^\alpha \leq bx^\beta$ if $ax^\alpha < bx^\beta$ or $ax^\alpha =_\leq bx^\beta$.

Leading terms (LT) and leading monomials (LM) are defined according to this term order. See Subsec. 2.3 of [VVY18] for more information on this definition and its comparison with Def. 2.3 of [CM19].

Let $I \subset A$ be a 0-*dimensional.* Let $B_\leq$ the canonical linear K-basis of A/I made of the $x^\alpha \notin LM_\leq(I)$. Let δ be the cardinality of $B_\leq$. We denote by $\mathscr{B}_\leq$ the border of $B_\leq$ (*i.e.* the $x_k x^\alpha$ for $k \in [\![1, n]\!]$ such that $x^\alpha \in B_\leq$ and $x_k x^\alpha$ not in $B_\leq$). $NF_\leq$ is the normal form mapping defined by I and $\leq$. We define D such that $D = 1 + \max_{x^\alpha \in B_\leq} |x^\alpha|$.

2 MULTIPLICATION MATRICES

The first task in the FGLM strategy is to develop the tools for computations in A/I. The main ingredients are the multiplication matrices, $M_1, \dots, M_n$, corresponding to the matrices of the linear maps given by the multiplication by x_i written in the basis $B_\leq$.

Once they are known, it is clear that one can perform any K-algebra operation on elements of A/I written in the basis $B_\leq$.

To compute those matrices, a natural strategy is to go through the computation of the normal forms $NF(x_i x^\alpha)$ for $x^\alpha \in B_\leq$.

We investigate in this section how to proceed with this task, and how it compares to the classical case.

2.1 Linear algebra

We recall here the tropical row-echelon form algorithm of [Va15] that we use for computing normal forms using linear algebra.

```
Algorithm 1: The tropical row-echelon form algorithm
  input : $M$, a Macaulay matrix of degree $d$ in $A$, with $n_{row}$
          rows and $n_{col}$ columns, and $mon$ a list of monomials
          indexing the columns of $M$.
  output: $\widetilde{M}$, the $U$ of the tropical LUP-form of $M$
  $\widetilde{M} \leftarrow M$ ;
  for $i = 1$ to $n_{row}$ do
      Find $j$ such that $\widetilde{M}[i,j]$ has the greatest term
        $\widetilde{M}[i,j]x^{mon_j}$ for $\leq$ of the row $i$ ;
      Swap the columns $i$ and $j$ of $\widetilde{M}$, and the $i$ and $j$ entries of
        $mon$ ;
      By pivoting with the $i$-th row, eliminates the coefficients
        of the other rows on the first column; ;
  Return $\widetilde{M}$ ;
```

We refer the interested reader to [Va15, VVY18]. We illustrate this algorithm with the following example.

Example 2.1. We present the following Macaulay matrices, over $\mathbb{Q}_3[x, y]$ with $w = (0, 0)$, and $\leq_m$ be the graded lexicographical ordering. The second one is the output of the tropical LUP algorithm applied on the first one. The monomials indexing the columns are written on top of the matrix.

$$\begin{array}{cccccc} x^4 & x^3y & y^4 & x^2 & xy & y^2 \\ \hline 1 & & & & 3 & \\ & & & 1 & 9 & 3 \\ & 9 & 9 & & & \\ & 9 & 9 & 3 & 1 & 9 \end{array} \qquad \begin{array}{cccccc} x^4 & x^2 & x^3y & xy & y^4 & y^2 \\ \hline 1 & & & & 3 & \\ & 1 & & 0 & & -\frac{57}{35} \\ & & 9 & 0 & 9 & -\frac{162}{35} \\ & & & -35 & 0 & -18 \end{array} .$$

If all four polynomials represented by the matrix belong to some ideal I (and assuming that $y^4, y^2 \in B_\leq(I)$) then we can conclude that $NF_\leq(xy) = -\frac{18}{35}y^2$ and $NF_\leq(x^3y) = -y^4 + \frac{18}{35}y^2$.

2.2 Comparison with classical case

The classical strategy to compute the $NF_{\leq_m}(x_i x^\alpha)$ ($x^\alpha \in B_{\leq_m}$) when working with a monomial ordering $\leq_m$, starting with a reduced GB G, is to set apart the following only three cases possible:

(Type 1) $x_i x^\alpha \in B_{\leq_m}$; **(Type 2)** $x_i x^\alpha \in LT(G)$;
(Type 3) $x_i x^\alpha \in LT_{\leq_m}(I)$ but neither in $B_{\leq_m}$ nor in $LT(G)$.

Type 1 is the easiest, as in this case $NF_{\leq_m}(x_i x^\alpha) = x_i x^\alpha$. Type 2 is not very difficult either. If for some $g \in G$, $LM(g) = x_i x^\alpha$, $g = x_i x^\alpha + \sum_{x^\beta \in B_{\leq_m}} c_\beta x^\beta$, then as G is reduced, we get directly that $NF_{\leq_m}(x_i x^\alpha) = -\sum_{x^\beta \in B_{\leq_m}} c_\beta x^\beta$.

Type 3 is the trickiest. We assume that we have already computed all the $NF(x_j x^\beta)$ for $x_j x^\beta <_m x_i x^\alpha$. Let x_k be the smallest (for $\leq_m$) variable dividing $x_i x^\alpha$. Then the normal form

$$NF\left(\frac{x_i x^\alpha}{x_k}\right) = \sum_{x^\beta \in B_{\leq_m},\ x^\beta <_m \frac{x_i x^\alpha}{x_k}} c_\beta x^\beta$$

is already known. As in the previous sum, $x^\beta <_m \frac{x_i x^\alpha}{x_k}$, then $x_k x^\beta <_m x_i x^\alpha$, and all the $NF(x_k x^\beta)$'s are also already known. Therefore, we can write

$$NF(x_i x^\alpha) = \sum_{x^\beta \in B_{\leq_m},\ x^\beta <_m \frac{x_i x^\alpha}{x_k}} c_\beta NF(x_k x^\beta),$$

and $NF(x_i x^\alpha)$ can be obtained from the previous normal forms.

It is easy to see that the cost of computation of a normal form in the third case is in $O(\delta^2)$ field operations. The other two cases are negligible. As there are $O(n\delta)$ multiples to consider, the total cost for the computation of the multiplication matrices is in $O(n\delta^3)$ field operations.

Unfortunately, this strategy can not be completely generalized to the tropical context. There is no issue with the first two computations. However, there is no straightforward way to adapt the third one. We illustrate this failure with the following example.

Example 2.2. Over $\mathbb{Q}_3[x, y]$ with $\leq$ defined by $w = (0, 0)$, and $\leq_m$, the graded lexicographical ordering, let us take $I = \langle f_1, f_2, f_3, f_4 \rangle$ with $f_1 = x^7$, $f_2 = x^4y^2 + 3x^5y + 12x^3y^3 + 9xy^5$, $f_3 = x^2y^4 + 9x^5y + 18x^3y^3 + 9xy^5$, $f_4 = y^6 + 12x^5y + 3x^3y^3 + 6xy^5$. The first monomials of the third type arrive in degree 7, namely $xy^6, x^2y^5, x^4y^3, x^5y^2$. Due to the fact that we use a tropical term order, f_2, f_3, and f_4 all involve the monomials x^5y, x^3y^3, xy^5. In consequence if one wants to use multiples of the $NF(x^4y^2)$, $NF(x^2y^4)$, $NF(y^6)$, one gets quantity involving each three monomials among xy^6, x^2y^5, x^4y^3, and x^5y^2. They are all intertwined, and the trick we saw previously for monomials of the third type can not be used.

2.3 Tropical GB: General case

To untangle the reduction of monomials of the third type, we can use linear algebra. We have to proceed degree by degree. While monomials of the first type do not need any special proceeding, we need to interreduce the reductions of the monomials of the second and third types. The general strategy is described in Algorithm 2.

Proposition 2.3. *Algorithm 2 is correct, and is in $O(n^3\delta^3)$ field operations over K.*

Proof. The essentially different part compared to the classical case starts on Line 13. Lines 16 and 18 are crucial. By definition, monomials of the third type are in $LT(I)$. If $x^\alpha \in \overline{L}$ can not be written as $x_k x^\beta$ with x^β of type 2 or 3, it means that all its divisors are in $B_\leq$. Consequently, it is a minimal generator ot $LT(I)$ and is of type 2, which is a contradiction. Therefore, any monomial of the third type is a simple multiple of a monomial of type 2 or 3.

Algorithm 2: Multiplication matrices computation algorithm

```
input : A reduced GB $G$ of the ideal $I$ for $\leq$, a tropical term
        ordering.
output: $M_1, \ldots, M_n$ the multiplication matrices of $A/I$ (over
        the basis $B_\leq$).
1  Using $LT(G)$, compute $B_\leq$ (and $\delta = \sharp(B_\leq)$);
2  Define $M_1, \ldots, M_n$ as zero matrices in $K^{\delta\times\delta}$, their rows and
     columns are indexed by the $x^\alpha \in B_\leq$ ;
3  Compute $L = \{x_i x^\alpha,\ \text{for } i \in [\![1, n]\!] \text{ and } x^\alpha \in B_\leq\}.$ ;
4  Compute $\overline{L} = L \cap (B_\leq \cup LT(G))^c$ ;
5  for $x^\alpha \in L \cap B_\leq$ do
6      for i such that $x_i$ divides $x^\alpha$ do
7          Set $M_i[x^\alpha, \frac{x^\alpha}{x_i}] = 1$ ;
           /* The column indexed by $\frac{x^\alpha}{x_i}$ is zero, except
              on its coefficient indexed by $x^\alpha/x_i$    */
8  for $x^\alpha \in L \cap LT(G)$ do
9      Take $g \in G$ such that $g$ can be written
         $g = x^\alpha + \sum_{x^\beta \in B_\leq} g_{x^\beta} x^\beta$ ;
10     for i such that $x_i$ divides $x^\alpha$ do
11         for $x^\beta \in B_\leq$ do
12             Set $M_i[x^\beta, \frac{x^\alpha}{x_i}] = -g_{x^\beta}$ ;
13 Set $\mathscr{M}$ to be a matrix over $K$ with 0 rows and with columns
     indexed by $\overline{L} \cup LT(G) \cup B_\leq$. ;
14 for d a degree of a monomial in $\overline{L}$ (in ascending order) do
15     for $x^\alpha \in \overline{L}$ of degree d do
16         Find $x_i$, and $g$ either in $G$ or as a row of $\mathscr{M}$ such that
             $LT(x_i g) = x^\alpha$ ;
17         Stack $x_i g$ at the bottom of $\mathscr{M}$ ;
18     Using multiples of the form $x_i g$ or $g$, for $g$ either in $G$ or
         as a row of $\mathscr{M}$, find a complete set of reducers for all the
         monomials in $\overline{L} \cup LT(G)$ appearing with a non-zero
         coefficient in their column, and stack them at the
         bottom of $\mathscr{M}$ ;
19     Compute the Tropical Row-echelon form of $\mathscr{M}$ by
         Algorithm 1 and replace $\mathscr{M}$ with it ;
20     for $x^\alpha \in \overline{L}$ do
21         Take the row $s$ of $\mathscr{M}$ with leading coefficient $x^\alpha$. ;
22         for i such that $x_i$ divides $x^\alpha$ do
23             for $x^\beta \in B_\leq$ do
24                 Set $M_i[x^\beta, \frac{x^\alpha}{x_i}] = -\frac{\mathscr{M}[s, x^\beta]}{\mathscr{M}[s, x^\alpha]}$ ;
25 Return $M_1, \ldots, M_n$
```

As in the **for loop** on Line 14, we proceed by increasing degree, it is an easy induction to prove that such desired x_i and g exist.

For the complete set of reducers on Line 18, we use the fact that the monomials appearing in $\mathscr{M}$ all are in $B_\leq \cup L$, again by an easy induction (using the fact that the rows of $\mathscr{M}$ in previous degree are already reduced), and therefore, the complete set of reducers can be built.

The Tropical Row-echelon form computation then produces the desired normal forms. The correctness is then clear.

Regarding to the arithmetic complexity, we should note that both rows and columns of $\mathscr{M}$ are indexed by monomials in $L \cup B_{\leq}$ and there are $O(n\delta)$ of them. With the row-reduction, the total cost is then in $O(n^3\delta^3)$ arithmetic operations. □

Remark 2.4. The matrix $\mathscr{M}$ is sparse: any row added to the matrix on Line 17 has at most $\delta + 1$ non-zero coefficients: it is obtained as the multiple of a reduced row. Can we take advantage of this $\frac{1}{n}$ sparsity ratio for a better complexity?

Example 2.5. Let $G = (y + 2x, x^2 + 4)$ be a GB for $w = [0, 0]$ and grevlex of the ideal it spans in $\mathbb{Q}_2[x, y]$. Then $B_{\leq} = \{1, x\}$, $L = \{x, y, x^2, xy\}$ and $\overline{L} = \{xy\}$. Only $d = 2$ is considered on Line 4 of Algorithm 2. The following matrices represent respectively $\mathscr{M}$ before and after applying Algorithm 1, M_1 and M_2:

$$\begin{array}{ccc} x^2 & xy & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 4 \end{array}, \quad \begin{array}{ccc} xy & x^2 & 1 \\ 1 & 0 & -8 \\ 0 & 1 & 4 \end{array}, \quad \begin{array}{c|cc|} (x*) & 1 & x \\ 1 & 0 & -4 \\ x & 1 & 0 \end{array}, \quad \begin{array}{c|cc|} (y*) & 1 & x \\ 1 & 0 & 8 \\ x & -2 & 0 \end{array}.$$

2.4 Finite precision

We can now analyze the loss in precision when applying Algorithms 1 and 2. To prevent loss in precision to explode exponentially, we replace Line 5 of Algorithm 1 with the following two rows:

(1) By pivoting using the 'leading terms' of the rows j for $j > i$, eliminate all the coefficients possible of row i ;
(2) By pivoting with row i, eliminate all the coefficients on the i-th column.

The first row makes sense because by construction, all the rows of $\mathscr{M}$ have distinct leading terms, and this is kept unchanged during the pivoting process.

Proposition 2.6. *Let us assume that the matrix built on Line 17 of Algorithm 2 has coefficients in K known at precision $O(\pi^N)$. All rows have distinct leading terms, leading coefficient 1 and let us take Ξ be the smallest valuation of a coefficient of this matrix $\mathscr{M}$. We assume that $\Xi \leq 0$. Let $l = rank(\mathscr{M})$. We assume that $N > -l^2\Xi$. Then, after the application of Algorithm 1[1], the coefficients of the obtained matrix $\tilde{\mathscr{M}}$ are known at precision $O(\pi^{N+l^2\Xi})$, and the smallest valuation of a coefficient $\tilde{\mathscr{M}}$ is lower-bounded by $l\Xi$.*

Proof. After the reduction of row 1 by the other rows, the smallest valuation on row 1 is lower-bounded by $l\Xi$ and its coefficients are known at precision at least $O(\pi^{N+l\Xi})$. The coefficients of row 1 for the columns indexed by $\overline{L} \cup LT(G)$ are all zeros, except for its leading coefficient, which is $1 + O(\pi^{N+(l-1)\Xi})$. After the reduction of the other rows by row 1, on the rows of index > 1, the coefficients for the columns indexed by $\overline{L} \cup LT(G)$ are of valuation at least Ξ and known at precision $O(\pi^{N+l\Xi})$. The coefficients for the columns indexed by $B_{\leq}$ are of valuation at least $l\Xi$ and known at the same precision. The desired result follows by an easy induction argument. □

We then upper-bound the loss in precision for the whole computation of the multiplication matrices. Recall that: $D = 1 + \max_{x^\alpha \in B_{\leq}} |x^\alpha|$.

Proposition 2.7. *Let us assume that the smallest valuation of a coefficient of G is Ξ and that the coefficients of G are known at precision $O(\pi^N)$. As G is reduced, we get that $\Xi \leq 0$.*

Then the coefficients of the matrices $M_1, \ldots, M_n$ are of valuation at least $(n\delta)^D\,\Xi$, and are known at precision $O\left(\pi^{N+\left(\frac{(n\delta)^{2D+2}-1}{(n\delta)^2-1}\right)\Xi}\right)$.

Proof. This is a corollary to the previous proposition. There are at most D calls to the previous proposition, with matrices of ranks $l_1, \ldots, l_D$. Consequently, the upper bound on the valuation is $l_1 \ldots l_D \Xi$ and the precision is in $O(\pi^{N+(l_1^2+l_1^2l_2^2+\cdots+l_1^2\cdots l_D^2)\Xi})$ which is in $O(\pi^{N+D(l_1^2\cdots l_D^2)\Xi})$ As for all i, $l_i \leq n\delta$, we get the desired bounds. □

Remark 2.8. In the very favorable case where G is homogeneous and $w = [0, \ldots, 0]$, we get that $\Xi = 0$, and no loss in precision is happening. This is unfortunately not the most interesting case for polynomial system solving. Numerical data in Section 5 will show that loss in precision remain very reasonnable when using $w = [0, \ldots, 0]$ even in the affine case.

2.5 Using semi-stability

Following Huot's PhD thesis [Huo13], when Borel-fixedness (see Subsec. 3.2) or semi-stability properties are satisfied, many arithmetic operations can be avoided during the computation of the multiplication matrices. We begin with semi-stability.

Definition 2.9. *I is said to be semi-stable for x_n if for all x^α such that $x^\alpha \in LM(I)$ and $x_n \mid x^\alpha$ we have for all $k \in [\![1, n-1]\!]$ $\frac{x_k}{x_n}x^\alpha \in LM(I)$.*

Semi-stability's application is explained in Proposition 4.15, Theorem 4.16 and Corollary 4.19 of [Huo13] (see also Section 4 of [FGHR14]). We recall the main idea here with its adaptation to the tropical setting:

Proposition 2.10. *If I is semi-stable for x_n, M_n can be read from G and requires no arithmetic operation.*

Proof. The proof is the same as that of Theorem 8 of [FGHR14]. We prove that $\overline{L} \cap x_n B_{\leq} = \emptyset$. Let $x_n x^\alpha \in \overline{L} \cap x_n B_{\leq}$, with $x^\alpha \in B_{\leq}$. Then there is some monomial m and $g \in G$ such that $LM(mg) = x_n x^\alpha$. As $x^\alpha \in B_{\leq}$, we get that $x_n \nmid m$. Since $x_n x^\alpha \in \overline{L}$, then $|m| \geq 1$. Let $k < n$ be such that $x_k \mid m$. Then, by semi-stability for x_n, $x^\alpha = \frac{m}{x_k} \times \frac{x_k LM(g)}{x_n} \in LM(I)$, which is a contradiction. □

Thanks to Proposition 2.10, Algorithm 3 is correct, and its arithmetic cost is given by the following proposition.

Proposition 2.11. *Given a reduced GB G of the ideal I for $\leq$, a tropical term ordering, and assuming I is semi-stable for x_n, then M_n can be computed in $O(\delta^2)$ arithmetic operations, which are only computing opposites.*

[1] using the modification presented just above this proposition

Algorithm 3: Computing M_n, when semi-stable for x_n

```
input  : A reduced GB $G$ of the ideal $I$ for $\leq$, a tropical term
         ordering, assuming $I$ is semi-stable for $x_n$
output : $M_n$ the matrix of the multiplication by $x_n$ in $A/I$
Using $LT(G)$, computes $B_{\leq}$ (and $\delta = \sharp(B_{\leq})$);
Define $M_n$ as a zero matrix in $K^{\delta \times \delta}$, its rows and columns
  are indexed by the $x^\alpha \in B_{\leq}$ ;
Compute $L_n = \{x_n x^\alpha,\ \text{for } x^\alpha \in B_{\leq}\}.$ ;
for $x^\alpha \in L_n \cap B_{\leq}$ do
    Set $M_n[x^\alpha, \frac{x^\alpha}{x_n}] = 1$ ;
for $x^\alpha \in L_n \cap LT(G)$ do
    Take $g \in G$ such that $g$ can be written
      $g = x^\alpha + \sum_{x^\beta \in B_{\leq}} g_{x^\beta} x^\beta$. for $x^\beta \in B_{\leq}$ do
        Set $M_n[x^\beta, \frac{x^\alpha}{x_i}] = -g_{x^\beta}$ ;
Return $M_n$ ;
```

To apply the previous result to compute a GB in shape position in Subsection 4.2, we need to also compute the $NF(x_i)$'s. The following lemma states that this is not costly.

Lemma 2.12. *Given a reduced GB G of the ideal I for $\leq$, a tropical term ordering, then the $NF_{\leq}(x_i)$'s can be computed in $O(n\delta)$ arithmetic operations, which are only computing opposites.*

Proof. It is a consequence of the fact that $\leq$ is degree-compatible: for any i, x_i is either in $LT(G)$ or in $B_{\leq}$. □

Subsection 4.2 will apply the previous two results to obtain a fast algorithm to compute a shape-position basis.

Remark 2.13. For grevlex in the classical case, it is known that after a generic change of variable, I is semi-stable for x_n. The reason is that after a generic change of variable, $LT(I)$ is equal to the GIN of I (see Definition 4.1.3 of [HH11]) , which is known to be Borel-fixed, and Borel-fixedness implies semi-stability for x_n. In Section 3, we investigate whether this strategy is still valid in the tropical case.

3 GIN AND BOREL-FIXED INITIAL IDEAL

In this section, we introduce the tropical generic initial ideal of a 0-dimensional ideal analogously to the classical case, and study its properties of Borel-fixedness and semi-stability. The desired goal is to be able to use the fast Algorithm 3 after a (generic) change of variable.

3.1 Tropical GIN

We follow the lines of Chapter 4 of [HH11], and use the usual action of $\mathrm{GL}_n(K)$ on A: $(\eta, f(x)) \in \mathrm{GL}_n(K) \times A \mapsto \eta(f) := f(\eta^\top \cdot x)$.

Definition 3.1. An external product of monomials $x^{\alpha_1} \wedge \cdots \wedge x^{\alpha_k}$ is called a *standard exterior monomial* if $x^{\alpha_1} \geq \cdots \geq x^{\alpha_k}$. If its monomial is standard, a term $cx^{\alpha_1} \wedge \cdots \wedge x^{\alpha_k}$ is called a *standard exterior term.* We define an ordering on standard exterior terms by setting that: $cx^{\alpha_1} \wedge \cdots \wedge x^{\alpha_k} \geq dx^{\beta_1} \wedge \cdots \wedge x^{\beta_k}$ if $\mathrm{val}(c) + \sum_{i=1}^k w \cdot \alpha_i < \mathrm{val}(d) + \sum_{i=1}^k w \cdot \beta_i$, or $\mathrm{val}(c) + \sum_{i=1}^k w \cdot \alpha_i = \mathrm{val}(d) + \sum_{i=1}^k w \cdot \beta_i$ and there exists $1 \leq j \leq k$ s.t. $x^{\alpha_j} > x^{\beta_j}$ and $x^{\alpha_i} = x^{\beta_i}$ for all $i < j$. We then define the leading term of an external product of polynomials $f_1 \wedge \cdots \wedge f_k$ as its largest term, and denote it by $LT(f_1 \wedge \cdots \wedge f_k)$. The monomial of the leading term is denoted by $LM(f_1 \wedge \cdots \wedge f_k)$.

Lemma 3.2. *Let $(f_1, \ldots, f_t) \in A^t$. If $LT(f_1) > \cdots > LT(f_t)$, then $LT(f_1 \wedge \cdots \wedge f_t) = LT(f_1) \wedge \cdots \wedge LT(f_t)$.*

Proof. Let c_i be the coefficient of $LM(f_i)$ in f_i. Then, $c = \prod c_i$ is the coefficient of $\Gamma = LT(f_1) \wedge \cdots \wedge LT(f_t)$ in $f_1 \wedge \cdots \wedge f_t$. We may assume that the f_i's are ordered such that $cLT(f_1) \wedge \cdots \wedge LT(f_t)$ is a standard exterior term. Let $\Delta = dv_1 \wedge \cdots \wedge v_t$ be another term in $f_1 \wedge \cdots \wedge f_t$ and d_i the coefficient of v_i in f_i. Let $x^{\alpha_i} = LM(f_i)$ and $x^{\beta_i} = v_i$. Since $c_i x^{\alpha_i}$ is the leading term of f_i, it follows that $\mathrm{val}(c_i) + w \cdot \alpha_i \leq \mathrm{val}(d_i) + w \cdot \beta_i$. Thus, $\sum_{i=1}^t (\mathrm{val}(c_i) + w \cdot \alpha_i) \leq \sum_{i=1}^t (\mathrm{val}(d_i) + w \cdot \beta_i)$. As $\mathrm{val}(c) = \sum_{i=1}^t c_i$ and $\mathrm{val}(d) = \sum_{i=1}^t d_i$, we obtain $\mathrm{val}(c) + \sum_{i=1}^k w \cdot \alpha_i \leq \mathrm{val}(d) + \sum_{i=1}^k w \cdot \beta_i$. If the inequality is strict then Γ is strictly bigger than any permutation of the monomials of Δ such that a standard exterior term is obtained. If equality holds. Then, for all i, $\mathrm{val}(c_i) + w \cdot \alpha_i = \mathrm{val}(d_i) + w \cdot \beta_i$ and $x^{\alpha_i} \geq x^{\beta_i}$. As Γ is a standard exterior term, we deduce that also in this case, Γ is strictly bigger than any permutation of the monomials of Δ such that a standard exterior term is obtained. □

Lemma 3.3. *Let $V \subset A$ be a t-dimensional K-vector space. Let $w_1, \ldots, w_t$ be monomials with $w_1 > \cdots > w_t$. Then the following conditions are equivalent.*

1. *the monomials $w_1, \ldots, w_t$ form a K-basis of $LT(V)$,*
2. *if $(f_1, \ldots, f_t)$ is a K-basis of V, then $LM(f_1 \wedge \cdots \wedge f_t) = w_1 \wedge \cdots \wedge w_t$,*
3. *there exists a K-basis $(f_1, \ldots, f_t)$ of V s.t. $LM(f_1 \wedge \cdots \wedge f_t) = w_1 \wedge \cdots \wedge w_t$.*

Proof. (1) $\Rightarrow$ (2): We may assume that the f_j's are monic and $LT(f_1) > \cdots > LT(f_t)$. Since $LT(f_i) \in LT(V)$, there is $j(i)$ s.t. $LT(f_i) = w_{j(i)}$. As $w_1 >_1 \cdots >_1 w_t$, we obtain $j(i) = i$ and $LT(f_i) = w_i$ for all i. By Lemma 3.2, $LT(f_1 \wedge \cdots \wedge f_t) = LT(f_1) \wedge \cdots \wedge LT(f_t) = w_1 \wedge \cdots \wedge w_t$.

(2) $\Rightarrow$ (3): It is obvious by choosing a K-basis $f_1, \ldots, f_t$ of V.

(3) $\Rightarrow$ (1): Since $\dim(V) = \dim(LT(V))$ and $w_1, \ldots, w_t$ is linear independent, it is enough to show that $w_i \in LT(V)$. Let $f_1, \ldots, f_t$ be monic polynomials forming a K-basis of V with $LT(f_1) > \cdots > LT(f_t)$ and $LT(f_1 \wedge \cdots \wedge f_t) = w_1 \wedge \cdots \wedge w_t$. By Lemma 3.2, $LT(f_1 \wedge \cdots \wedge f_t) = LT(f_1) \wedge \cdots \wedge LT(f_t)$ and thus $w_i \in LT(V)$. □

Proposition 3.4. *Let $V \subset A_d$ be a t-dimensional K-vector space and $f_1, \ldots, f_t$ a basis of V. Let $cw_1 \wedge \cdots \wedge w_t$ be the largest (up to multiplication by an element of valuation 0) standard exterior term of $\bigwedge^t A_{\leq d}$ such that there exists $\eta \in \mathrm{GL}_n(R)$ with*

$$LT(\eta(f_1) \wedge \cdots \wedge \eta(f_t)) = cw_1 \wedge \cdots \wedge w_t.$$

Let $U_V = \{\eta \in \mathrm{GL}_n(R) \mid LT(\eta(f_1) \wedge \cdots \wedge \eta(f_t)) = \varepsilon \times cw_1 \wedge \cdots \wedge w_t,\ \mathrm{val}(\varepsilon) = 0\}$. Then, U_V is open in $\mathrm{GL}_n(R)$ and for any $\eta, v \in U_V$, $LT(\eta V) = LT(vV)$.

Proof. As only a finite amount of monomials are possible and $\mathrm{val}(R)$ is discrete and ≥ 0, U_V is well-defined. The valuation being discrete, U_V is open: $LT(\eta(f_1) \wedge \cdots \wedge \eta(f_t)) = \varepsilon \times cw_1 \wedge \cdots \wedge w_t$ amounts to $\mathrm{val}(q(\eta)) < v$ for carefully chosen $v \in \mathbb{R}$ and polynomial $q \in \mathbb{Z}[k^{n \times n}]$. The last statement follows from Lemma 3.3. □

From Lemma 3.3, $w_1 \wedge \cdots \wedge w_t$ in Prop 3.4 is independent of the choice of basis of V. For $d \in \mathbb{Z}_{\geq 0}$, let $I_{\leq d} = I \cap A_{\leq d}$.

Theorem 3.5. *Let I be a 0-dimensional ideal with $\delta = \dim_K K[X]/I$. We consider the finite dimensional K-vector space $I_{\leq \delta}$. Then the non-empty open set $U_I := U_{I_{\leq \delta}} \subset \mathrm{GL}_n(R)$ satisfies that $LT(\eta I) = LT(\upsilon I)$ for any $\eta, \upsilon \in U_I$.*

Proof. Let $\eta \in U_I$. We denote $LT(\eta I_{\leq d})$ by $J_{\leq d}$. Then $J_{\leq d} = LT(\upsilon I_{\leq d})$ for all $\upsilon \in U_I$ and $d > \delta$. Indeed, since $LT(\eta I_{\leq \delta})$ contains the initial terms in the reduced Gröbner basis G of ηI,

$$J_{\leq d} \subset A_{\leq d-\delta} LT(\eta I_{\leq \delta}) = A_{\leq d-\delta} LT(\upsilon I_{\leq \delta}) \subset LT(\upsilon I_{\leq d}).$$

As $\dim_K(J_d) = \dim_K(LT(\upsilon I_d))$, we obtain $J_d = LT(\upsilon I_d)$ for all $\upsilon \in U_I$. Since $LT(\eta I) = \bigcup_{d=\delta}^{\infty} J_{\leq d}$, then $LT(\eta I) = LT(\upsilon I)$ for any $\eta, \upsilon \in U_I$, which concludes the proof. □

Definition 3.6. We call $LM(\eta I)$, with $\eta \in U_I \subset \mathrm{GL}_n(R)$ as given in Theorem 3.5, the tropical generic initial ideal (tropical gin) of I.

Unfortunately, U_I is not a Zariski-open subset of $GL_n(R)$ in general, hence the *generic* in the name "tropical gin" is only given as a reference to the classical case. The following proposition is a consolation.

Proposition 3.7. *Assume k is infinite. Then*

$$U_I \bmod \pi := \{\eta \bmod \pi, \textit{ for } \eta \in U_I\}$$

is a non-empty Zariski-open set of $GL_n(k)$.

Proof. Let q be the polynomial defining $U_{I_{\leq \delta}}$ in the proof of Theorem 3.5. One can replace q by some q/π^l so that $\overline{q} = q \bmod \pi$ is non-zero, and one can check that consequently, since k is infinite, $U_I \bmod \pi = \{\overline{x} \in \mathrm{GL}_n(k) : \overline{q}(\overline{x}) \neq 0\}$ and this is a non-empty Zariski-open set of $GL_n(k)$. □

Remark 3.8. If, *e.g.*, $R = \mathbb{R}[\![t]\!]$, and one takes $\eta \in GL_n(R)$ at random using a nonatomic distribution over $\mathbb{R}$, then η belongs to U_I with probability one.

3.2 Borel-fixedness

In classical cases, a generic initial ideal is Borel-fixed ideal i.e. it is fixed under the action of the Borel subgroup $\mathcal{B} \subset \mathrm{GL}_n(K)$, which is the subgroup of all nonsingular upper triangular matrices. In tropical cases, a generic initial ideal is not always Borel-fixed. However, it can be Borel-fixed under some conditions.

Example 3.9. Let $I = (x^2, y^2)$ and $K = \mathbb{Q}_2$ (using $w = [0, 0]$ and grevlex). Then in degree two, for a generic change of variables of $x^2 \wedge y^2$ by the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we get in $K[x, y] \bigwedge K[x, y]$:

$$2(a^2bd - ab^2c)x^2 \wedge xy + (a^2d^2 - b^2c^2)x^2 \wedge y^2 + 2(acd^2 - bc^2d)xy \wedge y^2.$$

Hence the tropical GIN is $x^2 \wedge y^2$ for degree two, and is therefore not Borel-fixed, nor semi-stable for y.

Definition 3.10. Let $\mathfrak{B} \subset \mathrm{GL}_n(O_K)$ be the subgroup generated by nonsingular upper triangular matrices whose diagonal entries have valuation 0. We call $\mathfrak{B}$ a Borel subgroup. We say that a monomial ideal J is tropical Borel-fixed if J is fixed under the action of $\mathfrak{B}$.

A direct adaptation of Theorem 4.2.1 and Prop. 4.2.4 of [HH11] states that the usual properties of the GIN are preserved, under some conditions.

Proposition 3.11. *Let d be the maximal total degree of the reduced GB of the tropical generic initial ideal of I. If $K = \mathbb{Q}_p$ and $p \geq d$, or if $\mathrm{val}(\mathbb{Z} \setminus \{0\}) = \{0\}$, then the tropical generic initial ideal of I is tropical Borel-fixed and moreover, semi-stable for x_n.*

4 TROPICAL FGLM

In this section, we investigate the second part of the FGLM strategy. Namely, the multiplication matrices of A/I have been computed using the algorithms of Section 2, and we can now perform operations in A/I efficiently.

The strategy is then to go through projections in A/I of monomials and find linear relations among them. When done carefully, these relations provide polynomials in I, whose leading terms for the new term order can be read on the monomials defining the relation. When processed in the right order, we can obtain from these polynomials a minimal GB of I for our new term order.

4.1 Tropical to classical

We first begin with the easiest case of starting from a tropical GB and computing a classical GB.

It is clear that once the multiplication matrices are obtained, we can directly apply the classical FGLM algorithm (namely Algorithm 4.1 of [FGLM93], see also Algorithm 8 of [Huo13]), or its p-adic stabilized version: Algorithm 3 of [RV16]. This part is in $O(n\delta^3)$ arithmetic operations. We refer to Prop 3.6 of *loc. cit.* and obtain the following propositions.

Proposition 4.1. *The total complexity to compute a classical GB of I starting from a tropical GB is in $O(n^3\delta^3)$ arithmetic operations.*

Behavior regarding to precision can be stated the following way.

Proposition 4.2. *Let $\leq_1$ be a tropical term ordering and $\leq_2$ be a monomial ordering. Let G be an approximate reduced tropical GB for $\leq_1$ of the ideal I, with coefficients known up to precision $O(\pi^N)$. Let Ξ be the smallest valuation of a coefficient in G. Let $B_{\leq_1}$ and $B_{\leq_2}$ be the canonical bases of A/I for $\leq_1$ and $\leq_2$. Let M be the matrix whose columns are the $NF_{\leq_1}(x^\beta)$ for $x^\beta \in B_{\leq_2}$. Let $cond_{\leq_1, \leq_2}(I)$ be the biggest valuation of an invariant factor in the Smith Normal Form of M. Recall that $D = 1 + \max_{x^\alpha \in B_\leq} |x^\alpha|$.*

Then if $N > 2cond_{\leq_1, \leq_2}(I) - \left(\frac{(n\delta)^{2D+2}-1}{(n\delta)^2-1}\right)\Xi$, we can chain Algorithm 2 and Algorithm 3 of [RV16] to obtain an approximate GB G_2 of I for $\leq_2$. The coefficients of the polynomials of G_2 are known up to precision $O\left(\pi^{N+\left(\frac{(n\delta)^{2D+2}-1}{(n\delta)^2-1}\right)\Xi - 2cond_{\leq_1, \leq_2}(I)}\right)$.

4.2 Tropical to shape position

We can apply any classical FGLM algorithm if K is an exact field, or a stabilized variant using Smith Normal Form, as in Algorithm 6 of [RV16]. We refer to Prop. 4.5 of *loc. cit.*. Complexity is very favorable when we have the combination of Borel-fixedness and shape position.

Proposition 4.3. *If I is in shape position and semi-stable for x_n, then we can combine Algorithm 3 with Algorithm 6 of [RV16]). The time-complexity is in $O(n\delta^2) + O(\delta^3)$ arithmetic operations.*

Proposition 4.4. *Let G_1 be an approximate reduced GB of I, with coefficients known at precision $O(\pi^N)$. Let Ξ be the smallest valuation of a coefficient in G_1. If $\leq_2$ is lex, and if we assume that the ideal I is in shape position and $LM_{\leq_1}(I)$ is semi-stable for x_n, then the adapted FGLM in Algorithm 6 of [RV16]), computes an approximate GB G_2 of I for lex, in shape position. The coefficients of the polynomials of G_2 are known up to precision $O(\pi^{N-2cond_{\leq_1,\leq_2}+\delta\Xi})$. Moreover, we can read on M whether the precision was enough or not, and hence prove after the computation that the result is indeed an approximate GB.*

4.3 Tropical (or classical) to tropical

We conclude our series of algorithms with a new algorithm to compute a tropical GB of I of dimension 0 knowing the multiplication matrices of A/I.

In the classical case, the vanilla FGLM algorithm goes through the monomials x^α in ascending order for $\leq_2$, test whether x^α is in the vector space generated (in A/I) by the monomials x^β such that $x^\beta <_2 x^\alpha$, and if so, produce a polynomial in the GB in construction from the relation obtained by this linear relation.

In the tropical case, because of the fact that coefficients have to be taken into account, a relation (in A/I) between x^α and some monomials x^β such that $x^\beta <_2 x^\alpha$ is not enough to ensure that $x^\alpha \in LT_{\leq_2}(I)$. We deal with this issue by (1) taking all monomials of a given degree at the same time, in a big Macaulay matrix, and (2) reducing them with a special column-reduction algorithm so as to preserve the leading terms.

The linear algebra algorithm is presented in Algorithm 5, with the general tropical FGLM algorithm in Algorithm 4.

The fact that Algorithm 5 computes a column-echelon form of the matrix (up to column-swapping) along with the pivoting matrix is clear. What is left to prove is the compatibility of the pivoting process with the computation of the normal forms and the leading terms according to $\leq_2$. It relies on the following loop-invariant.

Proposition 4.5. *At any point during the execution of Algorithm 5, for any x^α, the column of M indexed by x^α corresponds to the normal form $NF_{\leq_1}(H)$ (with respect to $\leq_1$) of some polynomial H with $LT_{\leq_2}(H) = x^\alpha$.*

Proof. It is true by construction for any column when entering Algorithm 5. Also by construction, all columns are labelled by distinct monomials. Now let us assume that on Line 4, we are eliminating a coefficient d on the column labelled by x^β using a coefficient c on the column labelled by x^α as pivot. Because of the choice of pivot on Line 3, we get that $c^{-1}x^\alpha <_2 d^{-1}x^\beta$. Let us assume that the column indexed by x^α corresponds to $NF_{\leq_1}(H)$ with $LT_{\leq_2}(H) = x^\alpha$, and the column indexed by x^β corresponds to $NF_{\leq_1}(Q)$ with $LT_{\leq_2}(Q) = x^\beta$. Please note that $x^\alpha \neq x^\beta$. Then after pivoting the second column corresponds to $NF_{\leq_1}(Q - dc^{-1}H)$. As $LT_{\leq_2}(dc^{-1}H) = dc^{-1}x^\alpha <_2 x^\beta$, the loop-invariant is then preserved, which is enough to conclude the proof. □

Theorem 4.6. *Algorithm 4 terminates and is correct: its output is a GB of the ideal I for $\leq_2$. It requires $O(n\delta^3)$ arithmetic operations.*

Algorithm 4: A tropical FGLM algorithm

```
input  : $M_1, \ldots, M_n$ the multiplication matrices of $A/I$, in a
         basis $B_{\leq_1}$ for a tropical term ordering $\leq_1$, a tropical
         term ordering $\leq_2$.
output : A GB $G$ of the ideal $I$ for $\leq_2$.
1  $L \leftarrow \{1\}, G \leftarrow \emptyset, d \leftarrow 1$ ;
2  $M \leftarrow$ the matrix with $\delta$ rows and 0 columns ;
3  $P \leftarrow$ the matrix with 0 rows and 0 columns ;
4  while $L \neq \emptyset$ do
5      Stack on the right of $M$ all the monomials in $L$ of degree
         $d$, written in the basis $B_{\leq_1}$ using the multiplication
         matrices ;
6      Remove those monomials from $L$ ;
7      Apply Algorithm 5 with $M$ and $\leq_2$, to get a new $M$ and
         update the pivoting matrix $P$ ;
       /* If $M_0$ is the matrix of the $NF_{\leq_1}(x^\alpha)$ for $x^\alpha$
            indexing the columns of $M$, then $M = M_0P$. */
8      For all the new columns indexed by $x^\alpha$ that reduced to
         zero, add to $G$ the polynomial $x^\alpha - \sum_{\gamma\neq\alpha} P_{\gamma,\alpha}x^\gamma$, and
         remove the multiples of $x^\alpha$ from $L$ ;
9      Add to $L$ the $x_i x^\alpha$ for all $i$ and for all $x^\alpha$ new column in $M$
         that did not reduce to zero, and remove the duplicates ;
10     $d \leftarrow d + 1$ ;
11 Return $G$
```

Algorithm 5: Column reduction for FGLM

```
input  : $M$ a $\delta \times l$ matrix over $K$, whose rows and columns
         are indexed by monomials. A tropical term ordering
         $\leq$. An invertible $s \times s$ matrix $P$.
output : A column-reduction of $M$ compatible with $\leq$, an
         updated $P$.
1  if $M = 0$ then Return $M, P$ ;
2  Find the coefficient $M[i, j]$ of row indexed by $x^\beta$ and column
     indexed by $x^\alpha$ such that $M[i, j]^{-1}x^\alpha$ is smallest, and using
     smallest $x^\beta$ to break ties ;
3  Use this non-zero coefficient to eliminate the other
     coefficients on the same row ;
4  Update $P$ accordingly ;
5  Proceed recursively on the remaining rows and columns ;
6  Return $M, P$
```

Proof. We use the following loop-invariant: after Line 9 is executed, $LT_{\leq_2}(G)$ contains all the minimal generators in $LT_{\leq_2}(I)$ of degree $\leq d$, they each correspond to a reduced-to-zero column of M, and the x^β corresponding to non-reduced-to-zero columns of M are all in $NS_{\leq_2}(I)$. The proof for this invariant is as follows. As $\leq_2$ is degree-compatible, it is clear by linear algebra that $rank(M) = \dim(A_{\leq d}/I_{\leq d})$. Thanks to Proposition 4.5, the polynomials added to G are in I, and more precisely, $f = x^\alpha - \sum_\gamma P_{\gamma,\alpha}x^\gamma$ as in Line 8 is a polynomial such that $LT_{\leq_2}(f) = x^\alpha$ and $NF_{\leq_1}(f) = 0$, as given in the Proposition. Their $LT_{\leq_2}$'s are minimal generators of $LT_{\leq_2}(I)$ by construction (all multiples of previous generators have been erased). By a dimension argument, no minimal generator is missing.

Once d is big enough for all minimal generators of $LT_{\leq_2}(I)$ to have been produced, no monomials can be left in L and the algorithm terminates. Termination and correctness are then clear.

As columns are labelled by some $x_i x^\alpha$ with $x^\alpha \in NS_{\leq_2}(I)$ then at most $n\delta$ columns are produced in the algorithm. As the rank of M is δ and so is also its number of rows, the column-reduction of a given column costs $O(\delta^2)$ arithmetic operations. Consequently, the total cost of the algorithm is in $O(n\delta^3)$ arithmetic operations. □

Remark 4.7. The previous algorithm remarkably bears the same asymptotic complexity as the vanilla classical FGLM algorithm ($O(n\delta^3)$ arithmetic operations), regardless of the more involved linear algebra part. Could fast linear algebra also be applied here?

Example 4.8. Let $(x + \frac{1}{2}y, y^2 + 1)$ be a GB of the ideal it spans, for $w = [0, -1]$ and grevlex. We compute a GB of the same ideal for $w = [0, 0]$ and grevlex. The following matrices are: the polynomials added to M (in three batches, by degree), the final state of M and the final P. In the end, we get $(y + 2x, x^2 + \frac{1}{4})$ as the output GB.

$$\begin{array}{c|c|cc|c|} & 1 & x & y & x^2 \\ 1 & 1 & & & -2^{-2} \\ y & & -2^{-1} & 1 & \end{array}, \quad \begin{array}{c|cccc|} & 1 & x & y & x^2 \\ 1 & 1 & & 0 & 0 \\ y & & -2^{-1} & 0 & 0 \end{array}, \quad P = \begin{vmatrix} 1 & & & 2^{-2} \\ & 1 & 2 & \\ & & 1 & \\ & & & 1 \end{vmatrix}$$

5 NUMERICAL DATA

A toy implementation of our algorithms in SageMath [Sage] is available on https://gist.github.com/TristanVaccon. The following arrays gather some numerical results. The timings are expressed in seconds of CPU time.[2]

5.1 Tropical to classical

For a given p, we take three polynomials with random coefficients in $\mathbb{Z}_p$ (using the Haar measure) in $\mathbb{Q}_p[x, y, z]$ of degrees $2 \leq d_1 \leq d_2 \leq d_3 \leq 4$. $D = d_1 + d_2 + d_3 - 2$ is the Macaulay bound. We first compute a tropical GB for the weight $w = [0, 0, 0]$ and the grevlex monomial ordering, and then apply Algorithms 2 and 4 to obtain a lex GB. We compare with the strategy of computing a classical grevlex GB and then applying FGLM to obtain a lex GB. For any given choice of d_i's, the experiment is repeated 50 times. Coefficients of the initial polynomials are given at high-enough precision $O(p^N)$ for no precision issue to appear (see [RV16] for more on FGLM at finite precision).

Coefficients of the output tropical GB or classical GB are known at individual precision $O(p^{N-m})$ (for some $m \in \mathbb{Z}$)). We compute the total mean and max on those m's on the obtained GB. In the first following array, we provide the mean and max for the tropical strategy. In the second, to compare classical and tropical, we provide couples for the mean on the 50 ratios of timing per execution (t), along with the arithmetic (Σ) and geometric (π) mean of the 50 ratios of mean loss in precision per execution. Data for $p = 101$ or 65519 are not worth for these ratios as the loss in precision is 0 most of the time.

In average the tropical strategy takes longer, but save a large amount of precision (for small p). While the ratio of saved precision may decrease with the degree, the abolute amount of saved precision is often still very large. We have also noted that the standard deviations for these ratios can be very large.

precision (trop.)	$D = 4$		5		6		7		8		9	
$p = 2$	11	103	25	278	60	509	176	1253	300	1783	652	3929
3	3	21	12	97	36	396	125	634	141	1002	282	2876
101	0	1	0	1	1	79	0	2	15	408	0	2
65519	0	0	0	0	0	0	0	0	0	0	0	0

$\frac{\text{trop.}}{\text{classical}}$	$D = 4$			5			6			7			8			9		
	t	Σ	π	t	Σ	π	t	Σ	π	t	Σ	π	t	Σ	π	t	Σ	π
$p = 2$	20	.4	.3	5	.4	.2	5	.5	.2	5	.6	.2	1.5	.8	.2	9	1	.2
3	6	.6	.2	6	.5	.2	5	.5	.2	2	.4	.1	1.2	.7	.1	.9	.9	.1

5.2 Tropical to tropical

We repeat the same experiments for mean and max loss in precision, but this time we compute a tropical GB for weight $w = [0, 0, 0]$ and then use Algorithm 4 to compute a tropical GB for weight $w = [-2, 4, -8]$ (grevlex for tie-breaks in both cases). Precision-wise, it seems that there is an intrinsic difficulty in computing a lex GB compared to a tropical GB.

precision loss	$D = 4$		5		6		7		8		9	
$p = 2$	2	18	2.5	14	2.6	14	2.9	16	3	17	3.5	19
3	1	9	1	7	1	9	1.4	14	1.4	11	2	13
101	0	1	0	1	0	1	0	2	0	2	0	2
65519	0	0	0	0	0	0	0	0	0	0	0	0

5.3 Semi-stability and shape position

We adapt our setting to $\mathbb{Q}((t))$, using entries with coefficients in $\mathbb{Z}[[t]]$ given at precision 50 (using SageMath's built-in random function), and apply the ideas of Subsection 2.5 and Section 3. As $\mathbb{Q}$ is involved, computations are slow for $D \geq 7$ due to coefficients growth.

w = [0, 0, 0]+grevlex	$D = 4$		5		6	
mean timing (F5 & FGLM)	2.8	9.4	3.9	102	10	1030
precision F5 (mean & max)	0	2	0	2	0	3
precision FGLM (mean & max)	0	0	0.1	8	0.4	34

REFERENCES

[CM19] Chan A., Maclagan D., Gröbner bases over fields with valuations, Math. Comp. 88 (2019), 467-483.

[FGHR14] Faugère, J.-C., Gaudry, P., Huot, L., Renault, G., Sub-cubic Change of Ordering for Gröbner Basis: A Probabilistic Approach, in Proceedings: ISSAC 2014. ACM, Kobe, Japon, pp. 170–177, 2014

[FGLM93] Faugère, J.-C., Gianni, P., Lazard, D., Mora, T., Efficient computation of zero-dimensional Gröbner bases by change of ordering, J. of Symbolic Computation 16 (4), 329–344, 1993

[GRZ19] Görlach, P, Ren, Y, Zhang, L., Computing zero-dimensional tropical varieties via projections, arXiv:1908.03486

[HH11] Herzog J., Hibi T., Monomial Ideals, Springer, 2001

[Huo13] Huot, L., Résolution de systèmes polynomiaux et cryptologie sur les courbes elliptiques, Ph.D. thesis, Université Pierre et Marie Curie (Paris VI), http://tel.archives-ouvertes.fr/tel-00925271

[JRS19] Jensen, A., Ren, Y., Schoenemann, H., The gfanlib interface in Singular and its applications, J. of Software for Algebra and Geometry 9 (2019), 81-87

[MS15] Maclagan, D. and Sturmfels, B., Introduction to tropical geometry, Graduate Studies in Mathematics, volume 161, AMS, Providence, RI, 2015

[MR19] Markwig, T. and Ren, Y., Computing Tropical Varieties Over Fields with Valuation, Foundations of Computational Mathematics, 2019

[RV16] Renault, G. and Vaccon, T. On the p-adic stability of the FGLM algorithm, arxiv:1602.00848

[Sage] SageMath, the Sage Mathematics Software System (Version 8.6), The Sage Development Team, 2018, http://www.sagemath.org

[Ser79] Serre, J.-P., Local fields, Vol. 67 of Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, translated from the French by Marvin Jay Greenberg

[Va15] Vaccon T., Matrix-F5 Algorithms and Tropical Gröbner Bases Computation, in Proceedings: ISSAC 2015, Bath, UK. Extended version in the J. of Symbolic Computation, Dec. 2017.

[VY17] Vaccon T., Yokoyama K., A Tropical F5 algorithm, in Proceedings: ISSAC 2017, Kaiserslautern, Germany.

[2] Everything was performed on a Ubuntu 16.04 with 2 processors of 2.6GHz and 16 GB of RAM.

[VVY18] Vaccon T., Verron T., Yokoyama K., On Affine Tropical F5 algorithm, in Proceedings: ISSAC 2018, New York, USA. Extended version to appear in the J. of Symbolic Computation.