A Tropical F5 algorithm

Tristan Vaccon, Kazuhiro Yokoyama

A Tropical F5 algorithm

Tristan Vaccon[*], Kazuhiro Yokoyama[†]

2017

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. While generalizing the classical theory of Gröbner bases, it is not clear how modern algorithms for computing Gröbner bases can be adapted to the tropical case. Among them, one of the most efficient is the celebrated F5 Algorithm of Faugère.

In this article, we prove that, for homogeneous ideals, it can be adapted to the tropical case. We prove termination and correctness.

Because of the use of the valuation, the theory of tropical Gröbner bases is promising for stable computations over polynomial rings over a p-adic field. We provide numerical examples to illustrate time-complexity and p-adic stability of this tropical F5 algorithm.

1 Introduction

The theory of tropical geometry is only a few decades old. It has nevertheless already proved to be of significant value, with applications in algebraic geometry, combinatorics, computer science, and non-archimedean geometry (see [MS15], [EKL06]) and even attempts at proving the Riemann hypothesis (see [C15]).

Effective computation over tropical varieties make decisive usage of Gröbner bases, but before Chan and Maclagan's definition of tropical Gröbner bases taking into account the valuation in [C13, CM13], computations were

[*]Université de Limoges, tristan.vaccon@unilim.fr
[†]Rikkyo University, kazuhiro@rikkyo.ac.jp

only available over fields with trivial valuation where standard Gröbner bases techniques applied.

In this document, we show that following this definition, an F5 algorithms can be performed to compute tropical Gröbner bases.

Our motivations are twofold. Our first objective is to provide with the F5 algorithm a fast algorithm for tropical geometry purposes. Indeed, for classical Gröbner bases, the F5 algorithm, along with the F4, is recognized as among the fastest available nowadays.

Secondly, while our algorithms are valid and implemented for computations over $\mathbb{Q}$, we aim at computation over fields with valuation that might not be effective, such as $\mathbb{Q}_p$ or $\mathbb{Q}((t))$. Indeed, in [V15], the first author has studied the computation of tropical Gröbner bases over such fields through a Matrix-F5 algorithm. For some special term orders, the numerical stability is then remarkable. Hence, our second objective in designing a tropical F5 algorithm is to pave the way for an algorithm that could at the same time be comparable to the fast methods for classical Gröbner bases, have a termination criterion and still benefit from the stability that can be obtained for tropical Gröbner bases.

1.1 Related works on tropical Gröbner bases

We refer to the book of Maclagan and Sturmfels [MS15] for an introduction to computational tropical algebraic geometry.

The computation of tropical varieties over $\mathbb{Q}$ with trivial valuation is available in the Gfan package by Anders Jensen (see [Gfan]), by using standard Gröbner bases computations. Yet, for computation of tropical varieties over general fields, with non-trivial valuation, such techniques are not readily available. Then Chan and Maclagan have developed in [CM13] a way to extend the theory of Gröbner bases to take into account the valuation and allow tropical computations. Their theory of tropical Gröbner bases is effective and allows, with a suitable division algorithm, a Buchberger algorithm. Following their work, a Matrix-F5 algorithm has been proposed in [V15].

1.2 Main idea and results

Let G' be a finite subset of homogeneous polynomials of $A := k[X_1, \ldots, X_n]$ for k a field with valuation.[1] We assume that G' is a tropical Gröbner basis

[1] *e.g.* $\mathbb{Q}$ or $\mathbb{Q}_p$ with p-adic valuation, or $\mathbb{Q}[[X]]$ with X-adic

of the ideal I' it spans for a given tropical term order $\leq$. Let $f_1 \in A$ be homogeneous. We are interested in computing a tropical Gröbner basis of $I = I' + \langle f_1 \rangle$. In this homogeneous context, following Lazard [L83], we can perform computations in $I_d = I \cap k[X_1, \ldots, X_n]_d$. I_d can be written as a vector space as $I_d = \langle x^\alpha f_1,\ |x^\alpha| + |f_1| = d \rangle + I'_d$, with $|\,|$ denoting total degree. The second summand is already well-known as G' is a tropical Gröbner basis. Thanks to this way of writing the first summand, we can then filtrate the vector space I_d by ordering the possible x^α. The main idea of the F5 algorithm of Faugère [F02] is to use knowledge of this filtration to prevent unnecessary computations. Our main result is then:

Theorem 1.1. *The Tropical F5 algorithm (Algorithm 1 on page 18) computes a tropical Gröbner basis of I. If f_1 is not a zero-divisor in A/I' then no polynomial reduces to zero during the computation.*

1.3 Notations

Let k be a field with valuation val. The polynomial ring $k[X_1, \ldots, X_n]$ will be denoted by A. Let T be the set of monomials of A. For $u = (u_1, \ldots, u_n) \in \mathbb{Z}^n_{\geq 0}$, we write x^u for $X_1^{u_1} \ldots X_n^{u_n}$ and $|x^u|$ for its degree. For $d \in \mathbb{N}$, A_d is the vector space of polynomials in A of degree d. Given a mapping $f : U \to V$, $Im(f)$ denote the image of f. For a matrix M, $Rows(M)$ is the list of its rows, and $Im(M)$ denotes the left-image of M (*n.b.* $Im(M) = span(Rows(M))$). For $w \in Im(val)^n \subset \mathbb{R}^n$ and $\leq_1$ a monomial order on A, we define $\leq$ a tropical term order as in the following definition:

Definition 1.2. Given $a, b \in k^*$ and x^α and x^β two monomials in A, we write $ax^\alpha \geq bx^\beta$ if $val(a) + w \cdot \alpha < val(b) + w \cdot \beta$, or $val(a) + w \cdot \alpha = val(b) + w \cdot \beta$ and $x^\alpha \geq_1 x^\beta$.

This is a total term order on A. We can then define accordingly for $f \in A$ its highest term, denoted by $LT(f)$, and the corresponding monomial $LM(f)$. These defintions extend naturally to $LM(I)$ and $LT(I)$ for I an ideal of A. A tropical Gröbner bases of I (see [CM13, V15]) is then a subset of I such that its leading monomials generate as a monoid $LM(I)$. We denote by $NS(I)$ the set of monomials $T \setminus LM(I)$. We will write occasionally *tropical GB*.

Let G' be a finite subset of homogeneous polynomials of A that is a tropical Gröbner basis of the ideal I' it spans. Let $f_1 \in A$ be homogeneous. We are interested in computing a tropical Gröbner basis of $I = I' + \langle f_1 \rangle$.

Acknowledgements

We thank Jean-Charles Faugère, Pierre-Jean Spaenlehauer, Masayuki Noro, Naoyuki Shinohara and Thibaut Verron for fruitful discussions.

2 Signature

Contrary to the Buchberger or the F4 algorithm, the F5 algorithm relies on tags attached to polynomial so as to avoid unnecessary computation thanks to this extra information. Those tags are called *signature*, and they are decisive for the F5 criterion, which is one of the main ingredients of the F5 algorithm.

In this section, we provide a definition for the notion of signature we need for the F5 algorithm and deduce some of its first properties.

Definition 2.1 (Syzygies)**.** Let v be the following k-linear map defined by the multiplication by f_1:

$$v : \begin{array}{ccc} A & \to & A/I' \\ 1 & \mapsto & f_1. \end{array}$$

Let $Syz_{f_1} = Ker(v)$, $LM(Syz_{f_1})$ be the leading monomials of the polynomials in Syz_{f_1} and $NS(Syz_{f_1}) = T \setminus LM(Syz_{f_1})$ the normal set of monomials for the module of syzygies.

Proposition 2.2. $\langle v(NS(Syz_{f_1}))\rangle = Im(v)$.

Proof. We can prove this claim degree by degree. The method is quite similar to what was developped in Section 3.2 of [V15]. Let $d \in \mathbb{N}$. Let $\alpha_1, \ldots, \alpha_u$ be $LM(Syz_{f_1}) \cap A_d$. Let $f_{\alpha_1}, \ldots, f_{\alpha_u} \in A_d$ be such that for all i, $f_{\alpha_i} \in Ker(v)$ and $LM(f_{\alpha_i}) = \alpha_i$. Then, written in the basis $U_d = (LM(Syz_{f_1}) \cap A_d) \cup (NS(Syz_{f_1}) \cap A_d)$, $f_{\alpha_1}, \ldots, f_{\alpha_u}$ is under (row)-echelon form. Let $g_{\alpha_1}, \ldots, g_{\alpha_u} \in A_d$ be the corresponding reduced row-echelon form: we have $LM(g_{\alpha_i}) = \alpha_i$, $g_{\alpha_i} \in Ker(v)$ and the only monomial of g_{α_i} not in $NS(Syz_{f_1})$ is α_i. Now, clearly, if $f \in A_d$, by reduction by the g_{α_i}'s, there exists some $g \in A_d$ such that $v(f) = v(g)$ and $LM(g) \in NS(Syz_{f_1})$. □

Remark 2.3. Clearly, $LM(I') \subset LM(Syz_{f_1})$, and this is an equality if f_1 is not a zero-divisor in A/I'.

We can now proceed to define the notion of signature. It relies on a special order on the monomials of A, which is not a monomial order:

Definition 2.4. Let x^α and x^β be monomials in T. We write that $x^\alpha \leq_{sign} x^\beta$ if:

1. if $|x^\alpha| < |x^\beta|$.
2. if $|x^\alpha| = |x^\beta|$, $x^\alpha \in NS(Syz_{f_1})$ and $x^\beta \notin NS(Syz_{f_1})$.
3. if $|x^\alpha| = |x^\beta|$, $x^\alpha, x^\beta \in NS(Syz_{f_1})$ and $x^\alpha \leq x^\beta$
4. if $|x^\alpha| = |x^\beta|$, $x^\alpha, x^\beta \notin NS(Syz_{f_1})$ and $x^\alpha \leq x^\beta$.

Proposition 2.5. *$\leq_{sign}$ defines a total order on T. It is degree-refining. At a given degree, any x^α in $LM(I')$ or $LM(Syz_{f_1})$ is bigger than any $x^\beta \notin LM(Syz_{f_1})$.*

We can define naturally $LM_{sign}(g)$ for any $g \in A$. We should remark that in the general case, $LM_{sign}(g) \neq LM(g)$.

Definition 2.6 (Signature)**.** For $p \in I$, using the convention that $LM_{sign}(0) = 0$, we define the signature of p, denoted by $S(p)$, to be

$$S(p) = \min_{\leq_{sign}} \{LM_{sign}(g_1) \text{ for } g_1 \in A \text{ s.t. } (g_1 f_1 - p) \in I'\}.$$

Proposition 2.7. *The signature is well-defined.*

Remark 2.8. Clearly, $p \in I'$ if and only if $S(p) = 0$. Similarly, if $f_1 \notin I'$ then $S(f_1) = 1$.

Remark 2.9. This definition is an extension to the tropical case of that of [F15]. For trivial valuation, it coincides (after projection on last component) with that of [AP, F02] for elements in $I \setminus I'$. We have modified it to ensure that the signature takes value in $(T \setminus LM(I')) \cup \{0\}$, see Prop. 2.11 below.

With the fact that we can decompose an equality by degree, we have the following lemma:

Lemma 2.10. *If $p \in I \setminus I'$ is homogeneous of degree d, then* $\deg(S(p)) = \deg(p) - \deg(f_1)$.

Proposition 2.11. *For any $p \in I \setminus I'$, $S(p) \in NS(Syz_{f_1})$.*

Proof. This is a direct consequence of Proposition 2.2. □

This proposition can be a little refined.

Lemma 2.12. *Let $t \in T$, $f \in I \setminus I'$ then*

$$\begin{aligned} S(tf) = tS(f) &\Leftrightarrow tS(f) \in NS(Syz_{f_1}) \\ S(tf) <_{sign} tS(f) &\Leftrightarrow tS(f) \in LM(Syz_{f_1}). \end{aligned}$$

Proof. Let $S(f) = \sigma$. By definition of S, we have $f = \alpha\sigma f_1 + gf_1 + h$ with $\alpha \in k^* = k \setminus \{0\}$, $LM(g) <_{sign} \alpha\sigma$ and $h \in I'$. If $t\sigma \in NS(Syz_{f_1})$, then we get directly that the leading term of the normal form (modulo G') of $\alpha t\sigma f_1 + tgf_1 + th$ is $t\sigma$ and in this case $S(tf) = t\sigma = tS(f)$, otherwise we can provide a syzygy. In the other case, the normal form has a strictly smaller leading term, and we get that $S(tf) <_{sign} tS(f)$. □

We then have the following property, and two last lemmas to understand the behaviour of signature.

Proposition 2.13. *The following mapping Φ is a **bijection**:*

$$\begin{array}{rccl} & LM(I) \setminus LM(I') & \to & NS(Syz_{f_1}) \\ \Phi : & x^\alpha & \mapsto & \min_{\leq_{sign}}\{S(x^\alpha + g), \ \textit{with } g \textit{ s.t.} \\ & & & x^\alpha + g \in I \textit{ and } LT(g) < x^\alpha\}, \end{array}$$

Proof. It can be proved directly by computing a tropical row-echelon form of some Macaulay matrix (see Definition 4.4). □

Lemma 2.14. *Let $f_1, f_2 \in I \setminus I'$ be such that $LM(f_1) > LM(f_2)$ and $S(f_1) = S(f_2) = \sigma$. Then there exist $\alpha, \beta \in k^*$ such that*

$$S(\alpha f_1 + \beta f_2) <_{sign} \sigma.$$

Lemma 2.15. *Let $f_1, f_2 \in I$ be such that $S(f_1) > S(f_2)$. Then for any $\alpha \in k^*, \beta \in k$, $S(\alpha f_1 + \beta f_2) = S(f_1)$.*

3 Tropical $\mathfrak{S}$-Gröbner bases

The notion of signature allows the definition of a natural filtration of the vector space I by degree and signature:

Definition 3.1 (Filtration by signature)**.** For $d \in \mathbb{Z}_{\geq 0}$ and $x^\alpha \in T \cap I_d$, we define the vector space

$$I_{d,\leq x^\alpha} := \{f \in I_d,\ S(f) \leq x^\alpha\}\,.$$

Then we define the filtration by signature, $I = (I_{d,\leq x^\alpha})_{d\in\mathbb{Z}_{\geq 0},\, x^\alpha \in T\cap I_d}$.

Our goal in this section and the following is to define tropical Gröbner bases that are compatible with this filtration by signature. It relies on the notion of $\mathfrak{S}$-reduction and irreducibility.

Definition 3.2 ($\mathfrak{S}$-reduction)**.** Let $f, g \in I$, $h \in I$ and $\sigma \in T$. We say that f **$\mathfrak{S}$-reduces** to g with respect to σ and with h,

$$f \to^h_{\mathfrak{S},\sigma} g$$

if there are $t \in T$ and $\alpha \in k^*$ such that:

- $LT(g) < LT(f)$, $LM(g) \neq LM(f)$ and $f - \alpha th = g$ and
- $S(th) <_{sign} \sigma$.

If σ is not specified, then we mean $\sigma = S(f)$.

It is then natural to define what is an $\mathfrak{S}$-irreducible polynomial.

Definition 3.3 ($\mathfrak{S}$-irreducible polynomial)**.** We say that $f \in I$ is $\mathfrak{S}$-irreducible with respect to $\sigma \in T$, or up to σ, if there is no $h \in I$ which $\mathfrak{S}$-reduces it with respect to σ. If σ is not specified, then we mean $\sigma = S(f)$. If there is no ambiguity, we might omit the $\mathfrak{S} -$.

Remark 3.4. This definition clearly depends on I, I', and the given monomial ordering.

In order to better understand what are $\mathfrak{S}$-irreducible polynomials, we have the following:

Theorem 3.5. *Let $f \in I$ and $x^\alpha \in T$ such that:*

- *f is $\mathfrak{S}$-irreducible with respect to x^α,*
- *$f = (cx^\alpha + u)f_1 + h$ with $c \in k$, $u \in A$ with $LT(u) < cx^\alpha$, $h \in I'$.*

Then $f = 0$ if and only if $x^\alpha \in LM(Syz_{f_1})$. Moreover, if $f \neq 0$, then $x^\alpha = S(f) = \Phi(LM(f))$.

Proof. Suppose $f = 0$, then $0 = f = (cx^\alpha + u)f_1 + h$, hence $x^\alpha \in LM(Syz_{f_1})$. We prove the converse result by contradiction. We assume that $f \neq 0$ and $x^\alpha \in LM(Syz_{f_1})$. Let $t = LM(f)$ and $x^\beta = \Phi(t) \in NS(Syz_{f_1})$. We have $x^\beta <_{sign} x^\alpha$. There exists $g \in I$ such that $LM(g) = t$ and $S(g) = x^\beta$. Since $x^\beta < x^\alpha$, g is an $\mathfrak{S}$-reductor for f with respect to x^α. This contradicts the fact that f is irreducible. Hence $f = 0$. For the additional fact when $f \neq 0$, ssume $x^\alpha \in NS(Syz_{f_1})$. Then necessarily, $x^\alpha = S(f)$. Suppose now that $x^\alpha \neq \Phi(LM(f))$. Then $S(f) > \Phi(LM(f))$. Therefore there exists a polynomial $g \in I$ such that $t = LM(g) = LM(f)$ and $\Phi(t) = S(g) = \Phi(LM(f)) < S(f)$. It follows that g is an $\mathfrak{S}$-reductor of f, which leads to f being not $\mathfrak{S}$-irreducible. □

Corollary 3.6. *If $g \in I$ and $x^\alpha \in T$ are such that $x^\alpha g \neq 0$ is $\mathfrak{S}$-irreducible up to $x^\alpha S(g)$ then $S(x^\alpha g) = x^\alpha S(g)$.*

The previous results show that the right notion of $\mathfrak{S}$-irreducibility for f a polynomial is up to $S(f)$. Nevertheless, the previous corollary can not be used for easy computation of the signatures of irreducible polynomials as we can see on the following example:

Example 3.7. We assume that $z^4 \in G'$ and z^3, x^4 and $x^2y^2 \in NS(I')$. We assume that we have $h_1 = xy^5 + y^5z$, $h_2 = x^3y^2z - y^6$ and $h_3 = x^4y^2 + y^6$ such that $S(h_1) = x^2y$, $S(h_2) = x^3$ and $S(h_3) = z^3$ and all of them are $\mathfrak{S}$-irreducible. We assume that $x^4 >_{sign} x^2y^2$ and $\Phi(x^4y^2z) = x^4$. Then, $zh_3 = yh_1 + xh_2 = x^4y^2z + y^6z$. Its signature is $xS(h_2) = x^4$, and not z^4. With our assumptions, the polynomial zh_3 is irreducible up to $S(zh_3) = x^4$, whereas up to z^4, it is not.

In other words, it is possible that the polynomial $x^\alpha f$ is irreducible, up to $S(x^\alpha f)$, even though $S(x^\alpha f) < x^\alpha S(f)$.

We now have enough definitions to write down the notion of $\mathfrak{S}$-Gröbner bases, which will be a computational key point for the F5 algorithm.

Definition 3.8 (Tropical $\mathfrak{S}$-Gröbner basis)**.** We say that $G \subset I$ is a **tropical $\mathfrak{S}$-Gröbner basis** (or tropical $\mathfrak{S}-$GB, or just $\mathfrak{S}-$GB for short when there is no amibuity) of I with respect to G', I', and a given tropical term order if $G' = \{g \in G \text{ s.t. } S(g) = 0\}$ and for each $\mathfrak{S}$-irreducible polynomial $f \in I \setminus I'$, there exists $g \in G$ and $t \in T$ such that $LM(tg) = LM(f)$ and $tS(g) = S(f)$.

Remark 3.9. Unlike in Arri and Perry's paper [AP], we ask for $tS(g) = S(f)$ instead of the weaker condition $S(tg) = S(f)$. The main reason is to avoid misshapes like that of Example 3.7. We can nevertheless remark that thanks to Lemma 2.12, then $tS(g) = S(f)$ implies that $S(tg) = tS(g) = S(f)$.

We prove in this Section that tropical $\mathfrak{S}$-Gröbner bases are tropical Gröbner bases, allowing one of the main ideas of the F5 algorithm: compute tropical **$\mathfrak{S}$-Gröbner basis** instead of tropical Gröbner basis.

To that intent, we use the following two propositions.

Proposition 3.10. *A polynomial f is $\mathfrak{S}$-irreducible iff $S(f) = \Phi(LM(f))$.*

Proof. By definition, if $S(f) = \Phi(LM(f))$, then clearly f is $\mathfrak{S}$-irreducible. Regarding to the converse, if $S(f) >_{sign} \Phi(LM(f))$, then there exists $g \in I$ such that $LM(g) = LM(f)$ and $S(g) = \Phi(LM(f))$, and then g $\mathfrak{S}$-reduces f. □

Proposition 3.11. *If G is a tropical $\mathfrak{S}$-Gröbner basis, then for any nonzero $f \in I \setminus I'$, there exists $g \in G$ and $t \in T$ such that:*

- $LM(tg) = LM(f)$
- $S(tg) = tS(g) = S(f)$ *if f is irreducible, and* $S(tg) = tS(g) <_{sign} S(f)$ *otherwise.*

Hence, there is an $\mathfrak{S}$-reductor for f in G if f is not irreducible.

Proof. If f is irreducible, this is a result of Definition 3.8.

Let us assume that f is not $\mathfrak{S}$-irreducible. We take h $\mathfrak{S}$-irreducible such that $LM(h) = LM(f)$. Thanks to Proposition 3.10, it exists, and $S(h) <_{sign} S(f)$. So h is an $\mathfrak{S}$-reductor of f. There are then $t \in T$ and $g \in G$ such that $tLM(g) = LM(h) = LM(f)$ and $tS(g) = S(tg) = S(h)$. With Proposition 3.10, tg is irreducible. The result is proved. □

We can now prove the desired connection between tropical $\mathfrak{S}$-Gröbner bases and tropical Gröbner bases.

Proposition 3.12. *If G is a tropical $\mathfrak{S}$-Gröbner basis, then G is a tropical Gröbner basis of I, for $<$.*

Proof. Let $t \in LM(I) \setminus LM(I')$. With Proposition 2.13, there exist $\sigma \in NS(Syz_{f_1})$ such that $\Phi^{-1}(\sigma) = t$ and $f \in I \setminus I'$ such that $LM(f) = t$ and $S(f) = \sigma$. By Proposition 3.11, there exists $g \in G$, $u \in T$ such that $LM(ug) = LM(f) = t$. Hence, the span of $\{LM(g), g \in G\}$ contains $LM(I) \setminus LM(I')$, and $G \supset G'$. Therefore G is a tropical Gröbner basis of I. □

And we can also prove some finiteness result on tropical $\mathfrak{S}$-Gröbner bases, which can be usefully applied to the problem of the termination of the F5 algorithm.

Proposition 3.13. *Every tropical $\mathfrak{S}$-Gröbner basis contains a finite tropical $\mathfrak{S}$-Gröbner basis.*

Proof. Let $G = \{g_i\}_{i \in L}$ be a tropical $\mathfrak{S}$-Gröbner basis. Let

$$V : \begin{array}{ccc} G & \to & T \oplus T \\ g_i & \mapsto & (LM(g_i), S(g_i)) \end{array}$$

be a mapping. By Dickson's lemma, there exists some finite set $J \subset L$ such that the monoid generated by the image of V is generated by $H_0 = \{g_i\}_{i \in J}$. We claim that $H = H_0 \cup G'$ is a finite tropical $\mathfrak{S}$-Gröbner basis. We have taken the union with G' to avoid any issue with G' being non-minimal. Let $f \in I \setminus I'$ be an $\mathfrak{S}$-irreducible polynomial. Since G is a tropical $\mathfrak{S}$-Gröbner basis, there exists $g_i \in G$ and $t \in T$ such that $tS(g_i) = S(tg_i) = S(f)$ and $tLM(g_i) = LM(tg_i) = LM(f)$. If $i \in J$, we are fine. Otherwise, there exists some $j \in J$ and $u, v \in T$ such that $LM(g_i) = uLM(g_j)$ and $S(g_j) = vS(g_j)$. Three cases are possible. If $u = v$, then $t' = ut \in T$ satisfies $t'LM(g_j) = LM(f)$ and $t'S(g_j) = S(f)$ and we are fine. If $u <_{sign} v$ then $t' = ut \in T$ satisfies $t'LM(g_j) = LM(f)$ and $t'S(g_j) < S(f)$, contradicting the hypothesis that f is $\mathfrak{S}$-irreducible. If $u >_{sign} v$, then for $t' = vt \in T$, we can take some $\alpha \in k$ such that $p = f - \alpha t' g_j$ satisfies $LM(p) = LM(f)$ but $S(p) < S(f)$, contradicting the irreducibility of f. As a consequence, we have proved that H is a tropical $\mathfrak{S}$-Gröbner basis. □

The elements of H_0 we have used are of special importance, hence we give them a special name.

Definition 3.14. We say that a non-zero polynomial $f \in I \setminus I'$, $\mathfrak{S}$-irreducible (with respect to $S(f)$), is **primitive $\mathfrak{S}$-irreducible** if there are no polynomials $f' \in I \setminus I'$ and terms $t \in T \setminus \{1\}$ such that f' is $\mathfrak{S}$-irreducible, $LM(tf') = LM(f)$ and $S(tf') = S(f)$.

The proof of Proposition 3.13 implies that we can obtain a finite tropical $\mathfrak{S}$-Gröbner basis by keeping a subset of primitive $\mathfrak{S}$-irreducible polynomials with different leading terms. Also, it proves there exists a finite tropical $\mathfrak{S}$-Gröbner basis with only primitive $\mathfrak{S}$-irreducible polynomials (in its $I \setminus I'$ part).

4 Linear algebra and tropical $\mathfrak{S}$-Gröbner bases

When the initial polynomials from which we would like to compute a Gröbner basis are homogeneous, the connection between linear algebra and Gröbner bases is well known.

Definition 4.1. Let $c_{n,d} = \begin{pmatrix} n+d-1 \\ n-1 \end{pmatrix}$, and $B_{n,d} = (x^{d_i})_{1 \leq i \leq c_{n,d}}$ be the monomials of A_d. Then for $f_1, \ldots, f_s \in A$ homogeneous polynomials, with $|f_i| = d_i$, and $d \in \mathbb{N}$, we define $Mac_d(f_1, \ldots, f_s)$ to be the matrix whose rows are the polynomials $x^{\alpha_{i,j}} f_i$ written in the basis $B_{n,d}$ of A_d.

We note that $Im(Mac_d(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle \cap A_d$.

Theorem 4.2 ([L83])**.** *For an homogeneous ideal $I = \langle f_1, \ldots, f_s \rangle$, $(f_1, \ldots, f_s)$ is a Gröbner basis of I for a monomial order $\leq_0$ if and only if: for all $d \in \mathbb{N}$, written in a decreasingly ordered $B_{n,d}$ (according to $\leq_0$), $Mac_d(f_1, \ldots, f_s)$ contains an echelon basis of $Im(Mac_d(f_1, \ldots, f_s))$.*

By *echelon basis*, we mean the following

Definition 4.3. Let $g_1, \ldots, g_r$ be homogeneous polynomials of degree d. Let M be the matrix whose i-th row is the row vector corresponding to g_i written in $B_{n,d}$. Then we say that $(g_1, \ldots, g_r)$ is an *echelon basis* of $Im(M)$ if there is a permutation matrix P such that PM is under row-echelon form.

In other words, $G = (g_1, \ldots, g_s)$ is a Gröbner basis of I if and only if for all d, an echelon (linear) basis of I_d is contained in the set $\{x^\alpha g_i, i \in [\![1, s]\!],\ x^\alpha \in T,\ |x^\alpha g_i| = d\}$.

We have an analogous property for tropical Gröbner bases and tropical $\mathfrak{S}$-GB. It follows from the study in [V15] of a tropical Matrix-F5 algorithm. We first need to adapt to the tropical setting the definitions of row-echelon form and echelon basis.

Definition 4.4 (Tropical row-echelon form)**.** Let M be a $l \times m$ matrix which is a Macaulay matrix, written in the basis $B_{n,d}$ of the monomials of A of degree d. We say that $(P, Q) \in GL_n(k) \times GL_m(k)$, Q being a permutation matrix, realize a tropical row-echelon form of M if:

1. PMQ is upper-triangular and under row-echelon form.
2. The first non-zero coefficient of a row corresponds to the leading term of the polynomial corresponding to this row.

We can then define a *tropical echelon basis*:

Definition 4.5 (Tropical echelon basis)**.** Let $g_1, \ldots, g_r$ be homogeneous polynomials of degree d. Let M be the matrix whose i-th row is the row vector corresponding to g_i written in $B_{n,d}$. Then we say that $g_1, \ldots, g_r$ is a *tropical echelon basis* of a vector space $V \subset A_d$ if there are two permutation matrices P, Q such that PMQ realizes a tropical row-echelon form of M and $span(Rows(M)) = V$.

This can be adapted to the natural filtration of the vector space I by $(I_{d,x^\alpha})_{d,x^\alpha}$ we have defined in 3.1.

Theorem 4.6. *Suppose that G is a set of $\mathfrak{S}$-irreducible homogeneous polynomials of the homogeneous ideal I such that $\{g \in G,\ S(g) = 0\} = G'$. Then G is a tropical $\mathfrak{S}$-Gröbner basis of I if and only if* ***for all*** *$x^\alpha \in T$, taking $d = |x^\alpha| + |f_1|$, the set*

$$\{x^\beta g,\ \textit{irreducible s.t. } g \in G,\ x^\beta \in T, |x^\beta g| = d,\ x^\beta S(g) = S(x^\beta g) \leq x^\alpha\}$$

contains a tropical echelon basis of $I_{d,\leq x^\alpha}$.

Proof. Using Proposition 3.10, it is clear that if G satisfy the above-written condition, then it satisfies Definition 3.8 of tropical $\mathfrak{S}$-GB. The converse is also easy using Proposition 3.11 on an echelon basis of $I_{d,\leq x^\alpha}$ and remarking that to get an echelon basis, it is enough to reach all the leading monomials of $I_{d,\leq x^\alpha}$. □

An easy consequence of the previous theorem is the following result of existence:

Proposition 4.7. *Given G' and f_1, consisting of homogeneous polynomials, there exists a tropical $\mathfrak{S}$-GB for $I = \langle G', f_1 \rangle$.*

Proof. It is enough to compute a tropical echelon basis for all the $I_{d,\leq x^\alpha}$, by tropical row-echelon form computation (see [V15]), and take the set of all these polynomials. □

Even with Proposition 3.13, the idea of the proof of Proposition 4.7 is not enough to obtain an efficient algorithm. This is why we introduce the F5 criterion and design an F5 algorithm.

5 F5 criterion

In this section, we explain a criterion, the F5 criterion, which yields an efficient algorithm to compute tropical Gröbner bases.

We need a slightly different notion of S-pairs, called here normal pairs.

Definition 5.1 (Normal pair)**.** Given $g_1, g_2 \in I$, not both in I', let $Spol(g_1, g_2) = u_1 g_1 - u_2 g_2$ be the S-polynomial of g_1 and g_2, where $u_i = \frac{lcm(LM(g_1), LM(g_2))}{LT(g_i)}$. We say that (g_1, g_2) is a **normal pair** if:

1. the g_i's are primitive $\mathfrak{S}$-irreducible polynomials.
2. $S(u_i g_i) = LM(u_i) S(g_i)$ for $i = 1, 2$.
3. $S(u_1 g_1) \neq S(u_2 g_2)$.

Remark 5.2. With this definition, if (g_1, g_2) is a normal pair, using Lemma 2.15, $S(Spol(g_1, g_2)) = \max(S(u_1 g_1), S(u_2 g_2))$ holds. Moreover, if $S(u_1 g_1) > S(u_2 g_2)$ then $u_1 \neq 1$ as if otherwise, g_2 would be an $\mathfrak{S}$-reductor of g_1. Therefore $S(Spol(g_1, g_2)) > max(S(g_1), S(g_2))$.

Theorem 5.3 (F5 criterion)**.** *Suppose that G is a set of $\mathfrak{S}$-irreducible homogeneous polynomials of I such that:*

1. $\{g \in G,\ S(g) = 0\} = G'$.
2. *if $f_1 \notin I'$, there exists $g \in G$ such that $S(g) = 1$.*
3. *for any $g_1, g_2 \in G$ such that (g_1, g_2) is a normal pair, there exists $g \in G$ and $t \in T$ such that tg is $\mathfrak{S}$-irreducible and $tS(g) = S(tg) = S(Spol(g_1, g_2))$.*

Then G is a $\mathfrak{S}$-Gröbner basis of I.

Remark 5.4. The converse result is clearly true.

Remark 5.5. The g given in the second condition is primitive $\mathfrak{S}$-irreducible, by definition and using Lemma 2.10.

Theorem 5.3 is an analogue of the Buchberger criterion for tropical $\mathfrak{S}$-Gröbner bases. To prove it, we adapt the classical proof of the Buchberger criterion. We need three lemmas, the first two being very classical.

Lemma 5.6. *Let $P_1, \dots, P_r \in A$, $c_1, \dots, c_r \in k$ and β a term in A, $\sigma \in T$ be such that for all i $LC(P_i) = 1$, $LT(c_i P_i) = \beta$, $P_i \in I$ and $S(P_i) \leq \sigma$. Let $P = c_1 P_1 + \cdots + c_r P_r$. If $LT(P) < \beta$, then there exist some $c_{i,j} \in k$ such that $P = \sum_{i,j} c_{i,j} Spol(P_i, P_j)$ and $LT(c_{i,j} Spol(P_i, P_j)) < \beta$.*

Lemma 5.7. *Let $x^\alpha, x^\beta, x^\gamma, x^\delta \in T$ and $P, Q \in A$ be such that $LM(x^\alpha P) = LM(x^\beta Q) = x^\gamma$ and $x^\delta = lcm(LM(P), LM(Q))$. Then*

$$Spol(x^\alpha P, x^\beta Q) = x^{\gamma - \delta} Spol(P, Q).$$

Lemma 5.8. *Let G be an $\mathfrak{S}$-Gröbner basis of I up to signature $< \sigma \in T$. Let $f \in I$, homogeneous of degree d, be such that $S(f) \leq \sigma$. Then there exist $r \in \mathbb{N}$, $g_1, \dots, g_r \in G$, $Q_1, \dots, Q_r \in A$ such that for all i and x^α a monomial of Q_i, $S(x^\alpha g_i) = x^\alpha S(g_i) \leq \sigma$ and $LT(Q_i g_i) \leq LT(f)$. The $x^\alpha S(g_i)$'s are all distinct, when non-zero.*

Proof. It is clear by linear algebra. One can form a Macaulay matrix in degree d whose rows corresponds to polynomials τg with $\tau \in T, g \in G$ such that $S(\tau g) = \tau S(g) \leq \sigma$. Only one per non-zero signature, and each of them reaching an element of $LM(I_{d,\leq\sigma})$. It is then enough to stack f at the bottom of this matrix and perform a tropical LUP form computation (see Algorithm 3) to read the Q_i on the reduction of f. □

We can now provide a proof of Theorem 5.3.

Proof. We prove this result by induction on $\sigma \in T$ such that G is an $\mathfrak{S}$-GB up to σ. It is clear for $\sigma = 1$.

Let us assume that G is an $\mathfrak{S}$-GB up to signature $< \sigma$ for some some $\sigma \in T$. We can assume that all $g \in G$ satisfy $LC(g) = 1$. Let $P \in I$ be irreducible and such that $S(P) = \sigma$. We prove that there is $\tau \in T, g \in G$ such that $LM(P) = LM(\tau g)$ and $\tau S(g) = \sigma$.

Our second assumption for G implies that there exist at least one primitive $\mathfrak{S}$-irreducible $g \in G$ and some $\tau \in T$ such that $\tau S(g) = S(f) = \sigma$. If $LM(\tau g) = LM(f)$ we are done. Otherwise, by Lemma 2.14, there exist some $a, b \in k^*$ such that $S(af + b\tau g) = \sigma'$ for some $\sigma' <_{sign} \sigma$.

We can apply Lemma 5.8 to $af + b\tau g$ and obtain that there exist $r \in \mathbb{N}$, $Q_i \in A$, $g_i \in G$ such that $P = \sum_{i=1}^{r} Q_i g_i$, $LT(Q_i g_i) \leq P$ and for all i, and x^γ monomial of Q_i, the $x^\gamma S(g_i) = S(x^\gamma g_i) \leq_{sign} \sigma$ are all distinct. We remark that $LT(P) \leq \max_i(LT(g_i Q_i))$. We denote by $m_i := LT(g_i Q_i)$.

Moreover, we can assume that all the g_i's are primitive $\mathfrak{S}$-irreducible. Indeed, if among them some g' is not primitive $\mathfrak{S}$-irreducible, then there exists h_0, t_0 in $I \times T \setminus \{1\}$ such that h_0 is $\mathfrak{S}$-irreducible and $LM(t_0 h_0) = LM(g')$ and $t_0 S(h_0) = S(g') = S(t_0 h_0)$. We have $S(h_0) \leq_{sign} S(g') <_{sign} \sigma$. Hence, we can apply the $\mathfrak{S}$-GB property for h_0 and we obtain g'_0, τ_0 in $G \times T$ such that $LM(h_0) = LM(\tau_0 g'_0)$ and $S(h_0) = S(\tau_0 g'_0) = \tau_0 S(g'_0)$. We then have $LM(g') = LM(t_0 \tau_0 g'_0)$ and $S(g') = t_0 \tau_0 S(g'_0) = S(t_0 \tau_0 g'_0)$, with $\deg(LM(g')) > \deg(LM(g'_0))$. As a consequence, this process can only be applied a finite number of times before we obtain a $g'_k \in G$ which is primitive $\mathfrak{S}$-irreducible and some $b \in T$ such that $LM(bg'_k) = LM(\tau g)$ and $bS(g'_k) = S(bg'_k) = \sigma' <_{sign} \sigma = S(\tau g)$. Thus, we can assume that all the g_i's are primitive $\mathfrak{S}$-irreducible.

Among all such possible way of writing P as $\sum_{i=1}^{r} Q_i g_i$, we define β as the **minimum** of the $\max_i(LT(g_i Q_i))$'s. β exists thanks to Lemma 2.10 of [CM13].

If $LT(P) = \beta$, then we are done. Indeed, there is then some i and τ in the terms of Q_i such that $LT(\tau g_i) = \beta$ and $S(\tau g_i) \leq \sigma$.

We now show that $LT(P) < \beta$ leads to a contradiction.

In that case, we can write that:

$$\begin{aligned} P &= \sum_{m_i=\beta} Q_i g_i + \sum_{m_i<\beta} Q_i g_i, \\ &= \sum_{m_i=\beta} LT(Q_i) g_i + \sum_{m_i=\beta} (Q_i - LT(Q_i)) g_i + \sum_{m_i<\beta} Q_i g_i. \end{aligned}$$

As $LT(P) < \beta$ and this is also the case for the two last summands in the second part of the previous equation, $LT(\sum_{m_i=\beta} LT(Q_i)g_i) < \beta$. We write $LT(Q_i) = c_i x^{\alpha_i}$, with $c_i \in k$ and $\beta = c_0 x^{\beta_0}$ for some $c_0 \in k$. Thanks to Lemma 5.6 and 2.14, there are some $c_{j,k} \in k$ and $x^{\beta}_{j,k} = lcm(LM(g_j), LM(g_k))$ such that

$$\sum_{m_i=\beta} LT(Q_i) g_i = \sum_{m_i, m_j=\beta} c_{j,k} x^{\beta_0 - \beta_{j,k}} Spol(g_j, g_k).$$

Moreover, we have for all j, k involved, $S(x^{\beta_0-\beta_{j,k}} Spol(g_j, g_k)) \leq \sigma$ and $LT(c_{j,k} x^{\beta_0-\beta_{j,k}} Spol(g_j, g_k)) < \sigma$.

If there is j, k such that $S(Spol(g_j, g_k)) = \sigma$, then, by the way the Q_i were chosen (distinct signatures, multiplicativity of the signatures), the pair (g_j, g_k) is normal and the third assumption is enough to conclude.

Otherwise, we have for all j, k involved, $S(Spol(g_j, g_k)) < \sigma$. We can apply Lemma 5.8 to obtain $c_{j,k} x^{\beta_0-\beta_{j,k}} Spol(g_j, g_k) = \sum_i Q_i^{j,k} g_i$ such that for all i and x^γ monomial of $Q_i^{j,k}$ $LT(Q_i^{j,k} g_i) < \beta$ and $x^\gamma S(g_i) = S(x^\gamma g_i) \leq \sigma$.

All in all, we obtain some $\tilde{Q}_i$ such that $P = \sum_i \tilde{Q}_i g_i$ and for all i $LT(\tilde{Q}_i g_i) < \beta$. This contradicts with the definition of β as a minimum. So $LT(P) = \beta$, which concludes the proof. □

Remark 5.9. This theorem holds for $\mathfrak{S}$-GB up to a given signature or, as we work with homogeneous entry polynomials, for $\mathfrak{S}$-GB up to a given degree (*i.e.* $d - \mathfrak{S}$-GB).

6 A tropical F5 algorithm

Theorem 5.3 gives a first idea on how to do a Buchberger-style algorithm for $\mathfrak{S}$-GB. Yet, deciding in advance whether a pair is a normal pair does not seem to be easy. Indeed, the second condition require some knowledge on $LM(Syz_{f_1})$ which we usually do not have. There are two natural ways to

handle this question: Firstly, we could keep track during the algorithm of the syzygies encountered, and use a variable L as a place holder for their leading monomials. The second condition can then be replaced by $LM(u_i)S(g_i) \notin \langle L \rangle$. This is what is used in [AP]. Another way is to only consider the trivial syzygies. This amounts to take $\langle L \rangle = LM(I')$ and use the same replacement for the second condition. This is what is used in [F02] and [F15].

We opt for the **second choice** (only handling trivial syzygies). This give rise to the notion of admissible pair.

Definition 6.1 (Admissible pair)**.** Given $g_1, g_2 \in I$, not both in I', let $Spol(g_1, g_2) = u_1 g_1 - u_2 g_2$ be the S-polynomial of g_1 and g_2. We have $u_i = \frac{lcm(LM(g_1),LM(g_2))}{LT(g_i)}$. We say that (g_1, g_2) is an **admissible pair** if:

1. the g_i's are primitive $\mathfrak{S}$-irreducible polynomials.
2. if $S(g_i) \neq 0$, then $LM(u_i)S(g_i) \notin LM(I')$.
3. $S(u_1 g_1) \neq S(u_2 g_2)$.

We can then remark that handling admissible pairs instead of normal pairs is harmless, as the latter is a subset of the former.

Lemma 6.2. *If a set G satisfies the conditions of Theorem 5.3 for all its admissible pairs then it is an $\mathfrak{S}$-GB.*

In the general case, $LM(Syz_{f_1})$ is not known in advance. However, it can be determined **inductively** on signatures. This is how the following algorithm will proceed. From a polynomial g, the signature of $x^\alpha g$ will be **guessed** as $x^\alpha S(g)$, and after an $\mathfrak{S}$-GB up to signature $< x^\alpha S(g)$ is computed, we can decide whether $S(x^\alpha g) = x^\alpha S(g)$, or else $x^\alpha g$ happens to be reduced to zero. In the following, we certify inductively whether for a processed $x^\alpha g$, the **guessed** signature $x^\alpha S(g)$ equals the **true** signature $S(x^\alpha g)$. Similarly, **guessed** admissible pairs are inductively certified to be **true** admissibles pairs or not once condition 3 of 6.1 is certified. Using this idea, we provide a first version of an F5 algorithm in Algorithm 1, using Algorithm 2 for Symbolic Preprocessing.

Remark 6.3. Only signature zero is allowed to appear multiple times in the matrix in construction.

Algorithm 1: A first F5 algorithm

input : G' a tropical GB of I' consisting of homogeneous polynomials, f_1 an homogeneous polynomial, not in I'

output: A tropical $\mathfrak{S}$-GB G of $I' + \langle f_1 \rangle$

$G \leftarrow \{(0, g) \text{ for g in } G'\}$;

$f \leftarrow f \mod G'$ (classical reduction) ;

$G \leftarrow G \cup \{(1, f)\}$;

$B \leftarrow \{\text{guessed admissible pairs of } G\}$;

$d \leftarrow 1$;

while $B \neq \emptyset$ **do**

  P **receives** the pop of the guessed admissible pairs in B of degree d ;

  Write them in a Macaulay matrix M_d, along with their $\mathfrak{S}$-reductors obtained from G (one per non-zero signature) by **Symbolic-Preprocessing**(P, G) (Algorithm 2);

  Apply Algorithm 3 to compute the U in the tropical LUP form of M (no choice of pivot) ;

  Add to G all the polynomials obtained from $\widetilde{M}$ that provide new leading monomial up to their signature ;

  Add to B the corresponding new admissible pairs ;

  $d \leftarrow d + 1$;

Return G ;

The reason is the following: because of Proposition 3.10, for an irreducible polynomial with a given signature, its leading monomial is determined by its signature. After performing the tropical row-echelon form computation, all rows corresponds to irreducible polynomials, hence two rows produced with the same signature are redundant: either they will produce the same leading monomial or they would reduce to zero.

Algorithm 2: Symbolic-Preprocessing

input : P, a set of admissible pairs of degree d and G, a $\mathfrak{S}$-GB up to degree $d-1$
output: A Macaulay matrix of degree d

$D \leftarrow$ the set of the **leading monomials** of the polynomials in P ;
$C \leftarrow$ the set of the **monomials** of the polynomials in P ;
$U \leftarrow$ the polynomials of P ;
while $C \neq D$ **do**
  $m \leftarrow \max(C \setminus D)$;
  $D \leftarrow D \cup \{m\}$;
  $V \leftarrow \emptyset$;
  for $g \in G$ **do**
    if $LM(g) \mid m$ **then**
      $V \leftarrow V \cup \{(g, \frac{m}{LM(g)})\}$;
  $(g, \delta) \leftarrow$ the element of V with δg of **smallest signature**, with tie-breaking by taking minimal δ (for degree then for $\leq_{sign}$) ;
  $U \leftarrow U \cup \{\delta g\}$;
  $D \leftarrow D \cup \{\text{monomials of } \delta g\}$;
$M \leftarrow$ the polynomials of U, written in Macaulay matrix of degree d and ordered by increasing signature, with no repetition of signature outside of signature 0 (choosing smallest leading monomial to break a tie of signature) ;
Return M ;

The tropical LUP form computation to obtain a row-echelon matrix, with no choice of pivot, is described in Algorithm 3. See [V15] for more details. The result we want to prove is then:

Theorem 6.4. *Algorithm 1 computes an $\mathfrak{S}$-GB of I.*

Algorithm 3: The tropical LUP 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

$\widetilde{M} \leftarrow M$;

if $n_{col} = 1$ *or* $n_{row} = 0$ *or* M *has no non-zero entry* **then**

  Return $\widetilde{M}$;

else

  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 1 and j of $\widetilde{M}$, and the 1 and j entries of mon;

    By **pivoting** with the first row, eliminates the coefficients of the other rows on the first column;

    Proceed recursively on the submatrix $\widetilde{M}_{i\geq 2, j\geq 2}$;

  Return $\widetilde{M}$;

Proof. **Termination:** Assuming correctness, after (theoretically) performing the algorithm for all degree d in $\mathbb{N}$, we obtain an $\mathfrak{S}$-GB. Since by Proposition 3.13 all $\mathfrak{S}$-GB contain a finite $\mathfrak{S}$-GB then at some degree d we have computed a finite $\mathfrak{S}$-GB. As a consequence, all S-pairs from degree $d+1$ to degree $2d$ (at most) will not yield any new polynomial in G (no new leading monomial), and thus there will be no S-pair of degree more than $2d$, which proves the termination of the algorithm.

Correctness: We proceed by induction on the signature to prove that the result of Algorithm 1 is a tropical $\mathfrak{S}$-GB. The result is clear for signature $\leq_{sign} 1$.

For the induction step, we assume that the result is proved up to signature $\leq_{sign} x^\alpha$, with $|x^\alpha f_1| = d$. Let x^β be the smallest guessed signature of M_d of signature $>_{sign} x^\alpha$.

We first remark that if there are rows of guessed signature $>_{sign} x^\beta$ that are of true signature $<_{sign} x^\beta$ then: **1.** We can conclude that there is no normal pair popped from B with second half of a pair with signature x^γ such that $x^\alpha <_{sign} x^\gamma <_{sign} x^\beta$ because of condition 2 of Definition 5.1 (which prevents such signature to drop). **2.** Using the F5 Criterion Theorem 5.3, it proves that we have in G (and the rows of M_d up to signature x^α that are added to G) an $\mathfrak{S}$-GB up to signature $<_{sign} x^\beta$. **3.** As a consequence, using Theorem 4.6 the Symbolic Preprocessing has produced exactly enough rows of guessed (and true) signature $<_{sign} x^\beta$ from G to $\mathfrak{S}$-reduce the row of guessed signature x^β. Indeed, since we have an $\mathfrak{S}$-GB up to $<_{sign} x^\beta$, all necessary leading monomials could be attained by product monomial-polynomial of G with guessed signature $<_{sign} x^\beta$ or through the echelon form up to $<_{sign} x^\beta$ of M_d. The last consequence is of course also true if there is no such row with a gap between the guessed and the true signature.

Two possibilities can occur for the result of the reduction of the row of guessed signature x^β: **1.** The row reduces to zero. Then the signature x^β is not possible. We then have in G an $\mathfrak{S}$-GB up to signature $\leq_{sign} x^\beta$. **2.** The row does not reduce to zero. Then, depending on whether the reduced row provide a new leading monomial for $I_{\leq_{sign} x^\beta}$, we add it to G. We then have in G an $\mathfrak{S}$-GB up to signature $\leq_{sign} x^\beta$. This concludes the proof by induction. We then can apply the modified F5 Criterion, Lemma 6.2 to conclude that the output of Algorithm 1 is indeed an $\mathfrak{S}$-GB. □

To conclude the proof of Theorem 1.1, the main result on the efficiency of the F5 algorithm is still valid for its tropical version:

Proposition 6.5. *If f_1 is not a zero-divisor in A/I', then all the processed matrices M_d are (left-) injective. In other words, no row reduces to zero.*

Proof. In this case, $LM(Syz_{f_1}) = LM(I')$. Hence, with the choice of rows of M_d avoiding guessed signature in $LM(Syz_{f_1})$ no syzygy can be produced. □

Remark 6.6 (Rewritability)**.** Thanks to Theorem 5.3, it is possible to replace the polynomials in P in the call to **Symbolic-Preprocessing** on Line 8 of Algorithm 1. They can be replaced by any other multiple of element of G of the same signature. Indeed, if one of them, h, is of signature x^α, the algorithm computes a tropical $\mathfrak{S}$-Gröbner basis up signature $< x^\alpha$. Hence, h can be replaced by any other polynomial of same signature, it will be reduced to the same polynomial. By induction, it proves all of them can be replaced at the same time. This paves the way for the Rewritten techniques of [F02]. The idea, as far as we understand it, is then to use the polynomial that has been the most reduced to produce a polynomial of signature $S(tg)$ for the upcoming reduction. Taking the $x^\beta g$ ($g \in G$) of signature x^α such that g has the biggest signature possible is a first reasonnable idea.[2] It actually can lead to a substantial reduction of the running time of the F5 algorithm.

7 Implementation and numerical results

A toy implementation of our algorithms in Sagemath [Sage] is available on `https://gist.github.com/TristanVaccon`.

Remark 7.1. It is possible to apply Algorithm 1 to compute a tropical Gröbner basis of I given by $F = (P_1, \ldots, P_s)$ by performing complete computation succesively for (P_1), (P_1, P_2), $(P_1, P_2, P_3), \ldots$ adding a polynomial at a time playing the part f_1 played in the rest of the article. As we only deal with homogeneous polynomials, it is also possible to do the global computation degree by degree, and at a given degree iteratively on the initial polynomials. By indexing accordingly the signatures, as in [F02], the algorithm can be adapted straightforwardly. This is what has been chosen in the implementation we have achieved.

We have gathered some numerical results in the following array. Timings are in seconds of CPU time.[3] We have compared ours with that of the

[2]Indeed, such a g is at first glance the most reduced possible.

[3]Everything was performed in a guest Ubuntu 14.04 inside a Virtual Machine, with 4 processors and 29 GB of RAM.

algorithms of Chan and Maclagan in [CM13] (in Macaulay 2) and Markwig and Ren in [MY15] (in Singular), provided in [MY15]. A dot means that the computation could not complete. Entry systems are homogenized. Base field is $\mathbb{Q}$.

	Katsura 3	4	5	6	7	Cyclic 4	5	6
[CM13]	≤ 1	•	•	•	•	•	•	•
[MY15]	≤ 1	≤ 1	≤ 1	•	•	≤ 1	≤ 1	•
Trop. F5	≤ 1	5	74	513	•	4	353	•

Loss in precision has also been estimated in the following setting. 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 degree $2 \leq d_1 \leq d_2 \leq d_3 \leq 4$. For any given choice of d_i's, we repeat the experiment 50 times. Coefficients of the initial polynomials are all given at some high enough precision $O(p^N)$. Coefficients of the output tropical GB are known at individual precision $O(p^{N-m})$. We compute the total mean and max on those m's on the obtained tropical GB. Results are compiled in the following array as couples of mean and max, with $D = d_1 + d_2 + d_3 - 2$ the Macaulay bound.

$w = [0, 0, 0]$	$D = 4$	5	6	7	8	9	10
$p = 2$	(.3,8)	(.4,11)	(.1,10)	(.1,11)	(.1,13)	(.1,9)	(.2,12)
3	(.1,4)	(.1,5)	(.2,7)	(.1,13)	(.1,16)	(.1,5)	(0,6)
101	(0,1)	(0,0)	(0,0)	(0,1)	(0,1)	(0,0)	(0,1)
65519	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)

$w = [1, -3, 2]$	$D = 4$	5	6	7	8	9	10
$p = 2$	(.2,7)	(.5,12)	(3.3,45)	(3.5,29)	(3.7,24)	(4.8,85)	(4.8,86)
3	(1.5,13)	(1.2,9)	(4.2,20)	(3.6,19)	(4.3,22)	(6,33)	(5.8,43)
101	(.1,2)	(.1,3)	(.1,4)	(.1,4)	(0,3)	(.2,5)	(.3,6)
65519	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)

As for Tropical Matrix-F5, a weight differing from $w = [0, 0, 0]$ yields bigger loss in precision. Regarding to precision in row-reduction, in F5, this weight always use the best pivot on each row. For Matrix-F5, it is always the best pivot available in the matrix. In view of our data, we can observe that the loss in precision for Tropical F5 on these examples, even though it is, as expected, bigger, has remained reasonnable compared to the one of [V15] that allowed full choice of pivot.

8 Future works

In this article, we have investigated the main step for a complete F4-style tropical F5 algorithm. We would like to understand more deeply the Rewritten critertion of [F02]. We would also like to understand the natural extension of our work to a Tropical F4 and to a Tropical F5 for non-homogeneous entry polynomials.

References

[AP] Alberto Arri and John Perry. The F5 criterion revised. Journal of Symbolic Computation, 2011, plus *corrigendum* in 2017.

[C13] Chan, Andrew J., Gröbner bases over fields with valuations and tropical curves by coordinate projections, PhD Thesis, University of Warwick, August 2013.

[CM13] Chan, Andrew J. and Maclagan, Diane Gröbner bases over fields with valuations, `http://arxiv.org/pdf/1303.0729`, 2013.

[C15] Connes, Alain, An essay on the Riemann Hypothesis, `http://arxiv.org/pdf/1509.05576`, 2015.

[EKL06] Einsiedler, Manfred and Kapranov, Mikhail and Lind, Douglas Non-archimedean amoebas and tropical varieties, Journal für die reine und angewandte Mathematik (Crelles Journal), 2006.

[F02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), Proceedings of the 2002 international symposium on Symbolic and algebraic computation, ISSAC '02, Lille, France.

[F15] Jean-Charles Faugère. Résolution de systèmes polynomiaux en utilisant les bases de Gröbner, `http://www.lifl.fr/jncf2015/files/lecture-notes/faugere.pdf`, 2015.

[Gfan] Jensen, Anders N. Gfan, a software system for Gröbner fans and tropical varieties, Available at `http://home.imf.au.dk/jensen/software/gfan/gfan.html`.

[L83] Daniel Lazard. Gröbner-Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations, Proceedings of the European Computer Algebra Conference on Computer Algebra, EUROCAL '83.

[MS15] Maclagan, Diane and Sturmfels, Bernd, Introduction to tropical geometry, Graduate Studies in Mathematics, volume 161, American Mathematical Society, Providence, RI, 2015, ISBN 978-0-8218-5198-2.

[MY15] Markwig, Thomas and Ren, Yue Computing tropical varieties over fields with valuation, `http://arxiv.org/pdf/1612.01762`, 2015.

[Sage] SageMath, the Sage Mathematics Software System (Version 7.3.beta7), The Sage Development Team, 2016, http://www.sagemath.org.

[V14] Vaccon Tristan, Matrix-F5 algorithms over finite-precision complete discrete valuation fields, Proceedings of 39th International Symposium on Symbolic and Algebraic Computation, ISSAC'14, Kobe, Japan.

[V15] Vaccon Tristan, Matrix-F5 Algorithms and Tropical Gröbner Bases Computation, Proceedings of the 40th International Symposium on Symbolic and Algebraic Computation, ISSAC 2015, Bath, United Kingdom.