Signature-based Möller's algorithm for strong Gröbner bases over PIDs

Maria Francis
Indian Institute of Technology Hyderabad
Hyderabad, India
mariaf@iith.ac.in

Thibaut Verron
Institute for Algebra / Johannes Kepler University
Linz, Austria
thibaut.verron@jku.at

ABSTRACT

Signature-based algorithms are the latest and most efficient approach as of today to compute Gröbner bases for polynomial systems over fields. Recently, possible extensions of these techniques to general rings have attracted the attention of several authors.

In this paper, we present a signature-based version of Möller's classical variant of Buchberger's algorithm for computing strong Gröbner bases over Principal Ideal Domains (or PIDs). It ensures that the signatures do not decrease during the algorithm, which makes it possible to apply classical signature criteria for further optimization. In particular, with the F5 criterion, the signature version of Möller's algorithm computes a Gröbner basis without reductions to zero for a polynomial system given by a regular sequence. We also show how Buchberger's chain criterion can be implemented so as to be compatible with the signatures.

We prove correctness and termination of the algorithm. Furthermore, we have written a toy implementation in Magma, allowing us to quantitatively compare the efficiency of the various criteria for eliminating S-pairs.

KEYWORDS

Algorithms, Gröbner bases, Signature-based algorithms, Polynomials over rings, Principal Ideal Domains

ACM Reference Format:
Maria Francis and Thibaut Verron. 2019. Signature-based Möller's algorithm for strong Gröbner bases over PIDs. In *Proceedings of Conference'19, July 2019, Washington, DC, USA (Conference'19).* ACM, New York, NY, USA, 8 pages.

1 INTRODUCTION

Motivation and main results. Ever since Gröbner bases were introduced by Buchberger in 1965 [4], they have become a valuable tool for solving polynomial systems in many different applications, for example in cryptography or in engineering. For many applications, restricting Gröbner basis computations to polynomials over a field is enough. However, some applications require the computation of Gröbner bases over rings. For instance, Gröbner bases over $\mathbb{Z}$ can be used in lattice-based cryptography [10], or as a multi-purpose tool in integer linear algebra [15].

This work was started when the first author was supported by the Austrian FWF grant Y464. The second author is supported by the Austrian FWF grant F5004.

Conference'19, 2018

In the case of polynomials over a field, many algorithms have been developed to make Gröbner basis computations more and more efficient. The latest generation of Gröbner basis algorithms for fields is the class of signature-based algorithms. They introduce signatures, which are defined as the leading terms of a module representation of polynomials in terms of the generators of the ideal. This notion makes it possible to eliminate redundant computations and reductions of S-polynomials, by enforcing the key invariant that *signatures always increase during the algorithm.* With this information, algorithms are able to use criteria such as the F5 criterion [9], which allows to compute a Gröbner basis for an ideal given by a regular sequence without any reduction to zero.

Several algorithms have been developed for Gröbner bases over rings. In [16], Möller sketched an algorithm for computing so-called weak Gröbner bases over general commutative rings (described in detail in [1, Sec.4.2]) and presented a specialized version, computing strong Gröbner bases over Principal Ideal Domains (PIDs). In this paper, to avoid ambiguity, we call the former algorithm *Möller's weak GB algorithm* and the latter *Möller's strong GB algorithm* (or *Möller's algorithm* when clear from the context).

In this paper, we show how to add signatures to Möller's strong GB algorithm. We prove that our signature-variant of the algorithm is able to compute a strong Gröbner basis of any polynomial ideal over a PID, and that the crucial invariant holds: the algorithm never encounters a signature smaller than that of a previously computed polynomial.

Möller's algorithm maintains a weak Gröbner basis G_w and a strong Gröbner basis G_s. The basis G_w is obtained by reducing S-polynomials by elements of the strong basis; the basis G_s is obtained by computing (but not reducing) G-polynomials (called T-polynomials in [16]) of elements of the weak basis.

The signature version of Möller's algorithm maintains a signature of each element in G_w. As for elements of G_s, requiring the computation of G-polynomials to maintain a matching signature is too restrictive. However, we prove that maintaining an upper bound on their signature is sufficient to ensure that the signature of S-polynomials in G_w does not drop when reduced by elements of G_s, and that the algorithm as a whole is correct.

Additional criteria can be implemented to further eliminate redundant S-polynomials, such as Buchberger's criteria [3]. In particular, we show that Buchberger's chain criterion can be implemented in a similar fashion as Gebauer-Möller's criteria, with an order compatible with the selection strategy by smallest signature. The fact that signatures do not drop implies that the algorithm is also compatible with additional criteria such as the singular criterion, the syzygy criterion or the F5 criterion. We prove that the algorithm is correct and terminates.

We have written a toy implementation of Möller's algorithm with signatures[1] in the computer algebra system Magma [2], and we use it to give experimental data on the number of computed and eliminated pairs for some systems. We also discuss some optimizations which can be applied when implementing the algorithm.

Related work. Signature-based algorithms for fields have a long history. Early work in this direction was described in [17], where the authors use computations in a polynomial module for a similar purpose, and Algo. F5 [9] showed that module computations can be avoided by considering only signatures. From there, significant work has gone into studying signature-based algorithms from a theoretical standpoint and extending them. An excellent survey of this is given in [6].

Several algorithms have been developed for Gröbner bases over rings. Möller's work [16], on an algorithm for weak GBs over general rings and an algorithm for strong GBs over PIDs, was already mentioned. It also gives a survey of precursor works regarding Gröbner bases over rings. Similar ideas, notably G-polynomials, are present in different variations of Buchberger's algorithm for PIDs[18] or Euclidean domains [13, 14].

Extending signature techniques to rings has been the focus of recent research, starting in 2017 with Eder and Popescu [8]. In that work, the authors consider a signature-based version of Gröbner basis algorithms for Euclidean domains. The authors showed with a counter-example that implementing *totally ordered* signatures for rings cannot ensure that the crucial invariant holds. However, their algorithm can detect signature drops and fall back to existing algorithms without signatures. It can nonetheless serve as an efficient preprocessing step.

In [11], we described a way to add signatures to Möller's weak GB algorithm, and proved that the resulting algorithm is correct and terminates over PIDs. In particular, there is no signature drop in the algorithm, and additional criteria such as the F5 criterion can be used to eliminate reductions to zero in the case of a regular sequence. The main difference with the approach of [8] is that signatures are only partially ordered, and the coefficient parts of signatures are never compared.

In the present paper, we incorporate the same signature techniques into Möller's strong GB algorithm [16].

The main ingredients for the proofs of correctness of the algorithm with signatures and criteria are the relation between regular weak S-polynomials and weak signature-Gröbner bases from [11], and the characterization of Gröbner bases in terms of syzygies of the leading terms, given by the Lifting Theorem [16, Th. 1], which we generalize to a signature setting.

2 PRELIMINARIES

2.1 Notations

Let R be a principal ideal domain (PID), which is assumed to have a unit element and be commutative. We assume that the ring R is *effective* in the sense that:

(1) there are algorithms for all arithmetic operations ($+$, $*$, comparison to zero and to one) in R;
(2) there is an algorithm which, given a and $b \in R$, computes their greatest common divisor d and the Bézout coefficients u and v such that $au + bv = d$;
(3) there is an algorithm which, given a and $b \in R$, tests whether a divides b and if so, computes the quotient b/a.

Remark 2.1. *Effective Euclidean rings (in the sense that there are algorithms for (1) and an algorithm for Euclidean division), thanks to the extended Euclid algorithm, are effective PIDs.*

Let $A = R[x_1, \dots, x_n]$ be the polynomial ring in n indeterminates $x_1, \dots, x_n$ over R. A monomial in A is $x^a := x_1^{a_1} \dots x_n^{a_n}$ where $a = (a_1, \dots, a_n) \in \mathbb{N}^n$. A term in A is kx^a, where $k \in R \setminus \{0\}$. The set of terms (resp. monomials) of A is denoted by $\mathrm{Ter}(A)$ (resp. $\mathrm{Mon}(A)$).

We use the notation $\mathfrak{a}$ for ideals in the polynomial algebra A and I for ideals in the coefficient ring R.

The notion of monomial order can be directly extended from $\mathbb{K}[x_1, \dots, x_n]$ to A. In the rest of the paper, we assume that A is endowed with an implicit monomial order $\prec$, and we define as usual the leading monomial LM, the leading term LT and the leading coefficient LC of a given polynomial.

Given a tuple of polynomials $(g_1, \dots, g_s)$ and $i \in \{1, \dots, s\}$, we will frequently denote, for brevity, $M(i) = \mathrm{LM}(g_i)$, $C(i) = \mathrm{LC}(g_i)$ and $T(i) = \mathrm{LT}(g_i) = C(i)M(i)$. Given $i, j \in \{1, \dots, s\}$, we will frequently denote $M(i,j) = \mathrm{lcm}(M(i), M(j))$, $T(i,j) = \mathrm{lcm}(T(i), T(j))$ and $C(i,j) = \mathrm{lcm}(C(i), C(j))$.

2.2 Signatures

We consider the free A-module A^m with basis $\mathbf{e}_1, \dots, \mathbf{e}_m$. A term (resp. monomial) in A^m is $kx^a\mathbf{e}_i$ (resp. $x^a\mathbf{e}_i$) for some $k \in R \setminus \{0\}$, $x^a \in \mathrm{Mon}(A)$, $i \in \{1, \dots, m\}$. The set of terms of A^m is denoted by $\mathrm{Ter}(A^m)$. In this paper, terms in A^m are ordered using the Position Over Term (POT) order, defined by

$$kx^a\mathbf{e}_i \prec lx^b\mathbf{e}_j \iff i \lneq j \text{ or } (i = j \text{ and } x^a \prec x^b).$$

Given two terms $kx^a\mathbf{e}_i$ and $lx^b\mathbf{e}_j$ in A^m, we write $kx^a\mathbf{e}_i \simeq lx^b\mathbf{e}_j$ if they are incomparable, *i.e.* if $a = b$ and $i = j$.

Given a set of polynomials $f_1, \dots, f_m \in A$, we define an A-module homomorphism $\bar{\cdot} : A^m \to A$, by setting $\overline{\mathbf{e}}_i = f_i$ and extending linearly to A^m.

We recall the concept of signatures in A^m. Let $\mathbf{p} = \sum_{i=1}^m p_i\mathbf{e}_i$ be a module element. Under the POT ordering, the signature of $\mathbf{p}$ is $\mathrm{LT}(p_i)\mathbf{e}_i$ where i is such that $p_{i+1} = \dots = p_m = 0$ and $p_i \neq 0$. Signatures are of the form $kx^a\mathbf{e}_i$, where $k \in R, x^a \in \mathrm{Mon}(A)$ and $\mathbf{e}_i$ is a standard basis vector.

Note that we have two ways of comparing two similar signatures $\mathfrak{s}(\boldsymbol{\alpha}) = kx^a\mathbf{e}_i$ and $\mathfrak{s}(\boldsymbol{\beta}) = lx^b\mathbf{e}_j$. We write $\mathfrak{s}(\boldsymbol{\alpha}) = \mathfrak{s}(\boldsymbol{\beta})$ if $k = l, a = b$ and $i = j$, and we write $\mathfrak{s}(\boldsymbol{\alpha}) \simeq \mathfrak{s}(\boldsymbol{\beta})$ if $a = b$ and $i = j$, k and l being possibly different. If R is a field, one can assume that the coefficient is 1, and so this distinction is not important.

Note also that when we order signatures, we only compare the corresponding module monomials, and disregard the coefficients. This is a different approach from the one used in [8], where both signatures and coefficients are ordered.

3 ALGORITHM

3.1 Definitions

Möller's algorithm for computing strong Gröbner bases over PIDs uses the classical constructions of S-polynomials and reductions, together with G-polynomials. For each polynomial f, we want to keep track of a signature $\mathfrak{s}(f)$, such that $\mathfrak{s}(f) = \mathfrak{s}(\mathbf{p})$ for some $\mathbf{p} \in A^m$ with $\overline{\mathbf{p}} = f$. For that reason, the algorithm will maintain lists

[1] Available online: https://github.com/ThibautVerron/SignatureMoller

of *labelled* polynomials, where the label encodes the information available regarding the signature.

Definition 3.1. *Let $f_1, \dots, f_m \in A$, $\mathfrak{a} = \langle f_1, \dots, f_m \rangle$, and $(f, l) \in \mathfrak{a} \times \mathrm{Ter}(A^m)$. We say that (f, l) is:*

- *a S-*labelled polynomial*, with* signature *l if $l = \mathfrak{s}(\mathbf{p})$ for some $\mathbf{p} \in A^m$ with $\overline{\mathbf{p}} = f$;*
- *a G-*labelled polynomial*, with G-*signature *l if $l \succeq \mathfrak{s}(\mathbf{p})$ for some $\mathbf{p} \in A^m$ with $\overline{\mathbf{p}} = f$.*

By abuse of notation, we say that f is S-labelled (resp. G-labelled) and we denote $\mathfrak{s}(f) := l$ (resp. $\sigma(f) := l$).

Remark 3.2. *S-labelled polynomials are naturally G-labelled.*

Remark 3.3. *The base polynomials f_i are naturally S-labelled with signature $\mathbf{e}_i$.*

We go through the required constructions, with the signature-related restrictions allowing to maintain the labelling, starting with S-polynomials and reductions:

Definition 3.4. *Let $G = \{g_1, \dots, g_t\} \subset A$ be a set of S-labelled polynomials. For all $i \in \{1, \dots, t\}$, let $M(i)$, $T(i)$ and $C(i)$ be respectively $\mathrm{LM}(g_i)$, $\mathrm{LT}(g_i)$ and $\mathrm{LC}(f_i)$. Given $i, j \in \{1, \dots, t\}$, let $M(i, j)$, $T(i, j)$ and $C(i, j)$ be respectively $\mathrm{lcm}(M(i), M(j))$, $\mathrm{lcm}(T(i), T(j))$ and $\mathrm{lcm}(C(i), C(j))$.*

The S-polynomial of g_i and g_j is the polynomial

$$S\text{-Pol}(g_i, g_j) = \frac{T(i,j)}{T(i)} g_i - \frac{T(i,j)}{T(j)} g_j.$$

The leading term of its polynomial evaluation is $\precnsim M(i, j)$.

*The S-*pair *(i, j) is called* regular *if $\frac{M(i,j)}{M(i)}\mathfrak{s}(g_i) \neq \frac{M(i,j)}{M(j)}\mathfrak{s}(g_j)$ and* singular *otherwise. The S-pair (i, j) is called* strictly singular *if $\frac{T(i,j)}{T(i)}\mathfrak{s}(g_i) = \frac{T(i,j)}{T(j)}\mathfrak{s}(g_j)$, and* admissible *otherwise. Note that regular pairs are admissible.*

Let (i, j) be an admissible S-pair, we extend the S-labelling of G to $S\text{-Pol}(g_i, g_j)$ by defining $\mathfrak{s}(S\text{-Pol}(g_i, g_j)) = S(i, j)$, defined as:

(1) $S(i, j) = \max\left(\frac{T(i,j)}{T(i)}\mathfrak{s}(g_i), \frac{T(i,j)}{T(j)}\mathfrak{s}(g_j)\right)$ if (i, j) is a regular S-pair;

(2) $S(i, j) = \left(\frac{C(i,j)}{C(i)} - \frac{C(i,j)}{C(j)}\right)\frac{M(i,j)}{M(i)}\mathfrak{s}(g_i)$ if (i, j) is a singular, non strictly singular, S-pair.

Remark 3.5. *If (i, j) is not an admissible S-pair, it is strictly singular, and knowing the signature of g_i and g_j is not enough to know a signature for $S\text{-Pol}(g_i, g_j)$. All we know is that $S(i, j) \succnsim \mathfrak{s}(\mathbf{p})$ for some $\mathbf{p} \in A^m$ with $\overline{\mathbf{p}} = S\text{-Pol}(g_i, g_j)$. Such a situation is called a* signature drop.

Definition 3.6. *Let $G = \{g_1, \dots, g_t\} \subset A$ be a set of G-labelled polynomials, let $f \in A$ be a S-labelled polynomial and let $g \in A$. We say that f* (strongly) $\mathfrak{s}$-reduces in one step *to f modulo F if there exists $g_i \in F$ such that*

(1) $\mathrm{LT}(g_i)$ divides $\mathrm{LT}(f)$, say $\mathrm{LT}(f) = c\mu\mathrm{LT}(g_i)$ with $c \in R$ and $\mu \in \mathrm{Mon}(A)$;

(2) $g = f - c\mu g_i$;

(3) $\mu\sigma(g_i) \precsim \mathfrak{s}(f)$

We say that f (strongly) regular reduces in one step *to g modulo F if the signature inequality is strict: $x^a\sigma(g_i) \precnsim \mathfrak{s}(f)$.*

We say that f $\mathfrak{s}$-reduces (resp. regular reduces) to g modulo G if g is the result of a sequence of successive $\mathfrak{s}$-reductions (resp. regular reductions) in one step from f.

If g is the result of regular *reducing f modulo G, then we can extend the S-labelling to g by letting $\mathfrak{s}(g) = \mathfrak{s}(f)$.*

Using those definitions, we recall the definition of a (strong) signature Gröbner basis.

Definition 3.7. *Let $f_1, \dots, f_m \in A$, and $G = g_1, \dots, g_t$ a set of G-labelled polynomials in $\langle f_1, \dots, f_m \rangle$. Let $\mathbf{T} \in \mathrm{Ter}(A^m)$, the set G is called a* (strong) $\mathfrak{s}$-Gröbner basis up to signature $\mathbf{T}$ *if for all $g \in \langle f_1, \dots, f_m \rangle$ with signature $\precsim \mathbf{T}$, g (strongly) $\mathfrak{s}$-reduces to 0 modulo G.* [2] *It is called a* strong $\mathfrak{s}$-Gröbner basis *if it is a strong $\mathfrak{s}$-GB up to signature $\mathbf{T}$ for all $\mathbf{T} \in \mathrm{Ter}(A^m)$.*

Next, we recall the definition of GCD-polynomials (or G-polynomials for short) [3] and how to equip them with a G-labelling.

Definition 3.8. *Let $f \in A$ be a G-labelled polynomial, and $g \in A$ a S-labelled polynomial, such that $\mathrm{LT}(f) = a\mu$, $\mathrm{LT}(g) = bv$, with $a, b \in R$, $\mu, v \in \mathrm{Mon}(A)$. Let $d = \gcd(a, b)$ and u and v be the Bézout coefficients such that $ua + vb = d$. The G-polynomial of f and g is the module element*

$$G\text{-Pol}(f, g) = u\frac{\mathrm{lcm}(\mu, v)}{\mu} f + v\frac{\mathrm{lcm}(\mu, v)}{v} g.$$

The leading term of its polynomial evaluation is $d\,\mathrm{lcm}(\mu, v)$.

We extend the G-labelling by defining the G-signature of $G\text{-Pol}(f, g)$ to be

$$\sigma(G\text{-Pol}(f, g)) := S_G(f, g) = \max\left(\frac{\mathrm{lcm}(\mu, v)}{\mu}\sigma(f), \frac{\mathrm{lcm}(\mu, v)}{v}\mathfrak{s}(g)\right).$$

Since we do not require that the pair be admissible in any sense, this is really only a G-labelling. However, we will prove that this G-labelling for G-polynomials preserves enough information regarding the signature of the polynomials participating in the construction (Lem. 5.3), and that it is sufficient to ensure that subsequent reductions preserve the signature, which is a key point in proving that the algorithm is correct.

3.2 Algorithm

Möller's algorithm with signatures is presented in Algo. 1. It is a straightforward adaptation of Möller's algorithm, extended to keep track of the signature of computed polynomials, similar to the generic algorithm described in [7]. Note that any time the algorithm mentions a S-labelled polynomial f (resp. a G-labelled polynomial f), it means a pair $(f, \mathfrak{s}(f))$ (resp. a pair $(f, \sigma(f))$).

Algo. 1 maintains two sets of generators, G_w which will be a weak $\mathfrak{s}$-Gröbner basis and G_s which will be a (strong) $\mathfrak{s}$-Gröbner basis. The basis G_s is the *completion* of G_w, defined as follows.

Definition 3.9. *Let $F \subset A$ be a non-empty finite set of G-labelled polynomials, the completion $C(F)$ of F is the set of G-labelled polynomials defined recursively as:*

- $C(f) = \{f\}$;
- $C(f_1, \dots, f_r) = \{G\text{-Pol}(g, f_r) : g \in C(f_1, \dots, f_{r-1})\}$.

It is known that over a PID, the completion of a weak Gröbner basis is a strong Gröbner basis [16, Cor. after Th. 4], we will prove in Cor. 5.5 that it also holds for $\mathfrak{s}$-Gröbner bases.

Most of the book-keeping work, maintaining the bases and the list of pairs to consider together with signature information, is

[2] In the literature, it is sometimes only required that all elements with signature $\precsim \mathbf{T}$ $\mathfrak{s}$-reduce to 0.

[3] In the literature, G-polynomials are sometimes called T-polynomials [16].

Algorithm 1 Möller's algorithm with signatures

Input $\{f_1, \ldots, f_m\} \subset A = R[x_1, \ldots, x_n]$, R a PID
Output G_s a set of G-labelled polynomials in A, which is a (strong) $\mathfrak{s}$-Gröbner basis of $\langle f_1, \ldots, f_m \rangle$
Local variables

- $G_w = \{g_1, \ldots, g_r\}$ a set of S-labelled polynomials in A, which is a weak Gröbner basis of $\langle f_1, \ldots, f_m \rangle$
- $\mathcal{P} \subset \mathbb{N}^2$ a set of admissible S-pairs

$G_s, G_w, \mathcal{P} \leftarrow \emptyset$
for $i \in \{1, \ldots, m\}$ **do**
  Update$(G_w, G_s, \mathcal{P}, f_i, \mathbf{e}_i)$
  while $\mathcal{P} \neq \emptyset$ **do**
    Pick and remove (i, j) from $\mathcal{P}$ with minimal $S(i, j)$
    $g \leftarrow \mathrm{SPol}(g_i, g_j)$
    Update$(G_w, G_s, \mathcal{P}, g, S(i, j))$
  end while
end for
Return G_s

Algorithm 2 Procedure Update: update the weak and the strong Gröbner bases, and the list of pairs, eliminating pairs with Buchberger's chain criterion and signature restrictions

Input $G_w \subset A$ set of S-labelled polynomials, $G_s \subset A$ set of G-labelled polynomials, $\mathcal{P} \subset \mathbb{N}^2$, $f \in A$, $\mathfrak{s}(f) \in \mathrm{Ter}(A^m)$

$g \leftarrow \mathsf{RegularReduce}(f, \mathfrak{s}(f), G_s)$
if $g \neq 0$ **then**
  $r \leftarrow \#G_w + 1$; $g_r \leftarrow g$ // Index of the new element
  $G_w \leftarrow G_w \cup \{(g_r, \mathfrak{s}(f))\}$
  $G_s \leftarrow G_s \cup \{(g_r, \mathfrak{s}(f))\}$
  for all $h \in G_s$ **do**
    $G_s \leftarrow G_s \cup (G\text{-Pol}(h, g_r), S_G(h, g_r))$
  end for
  for all $i \in \{1, \ldots, r-1\}$
      such that (i, r) is an admissible S-pair
      and $\forall k \in \{1, \ldots, r-1\}$, $\mathsf{Chain}(i, r; k)$ does not hold,
  do
    Add (i, r) to $\mathcal{P}$
  end for
  for all $(i, j) \in \mathcal{P}$ **such that** $\mathsf{Chain}(i, j; r)$ holds **do**
    Remove (i, j) from $\mathcal{P}$
  end for
end if

delegated to the subroutine Update (Algo. 2). The most important feature of this subroutine is that it implements the following restrictions, which ensure that we can maintain a S-labelling in G_w:

(1) all reductions have to be *regular* (that is, the signatures of reducers have to be strictly less than the signature of the reducee);
(2) all S-pairs have to be *admissible* (that is, the signatures must not be an exact match);
(3) no restriction on G-pairs.

We shall prove in Sec. 5 that with those restrictions, the algorithm is correct and terminates.

The routine RegularReduce implements regular strong reduction modulo the already computed basis, due to space constraints it is not presented in details.

Additionally, Buchberger introduced two criteria to make the algorithm more efficient by eliminating S-polynomials: the coprime criterion [5, Sec. 2.10, Prop. 1] and the chain criterion [5, Sec. 2.10, Prop. 8][4]. Implementing the coprime criterion is straightforward and not detailed here. In order to implement the chain criterion, we use ideas similar to Gebauer and Möller's implementation [12], adapted to our selection order by smallest signatures first.

Definition 3.10. *Let $\{g_1, \ldots, g_t\} \subset A$ be a set of S-labelled polynomials. Let $(i, j, k) \in \{1, \ldots, t\}^3$, we say that* $\mathsf{Chain}(i, j; k)$ *holds if*

$$T(k) \mid T(i, j) \text{ and } S(i, j) \geq \frac{T(i, j)}{T(k)} \mathfrak{s}(g_k).$$

The consequence of that criterion is that S-pairs (i, j) such that $\mathsf{Chain}(i, j, r)$ holds for some r can be removed from consideration.

The criterion is also implemented as part of the Update subroutine (Algo. 2).

Similar to what was done with the signature-version of Möller's weak GB algorithm [11], further criteria can be added to the algorithm to make the computations more efficient: polynomials which have been regular reduced by are 1-singular reducible can be eliminated, and the Syzygy, the F5 and the Singular criteria can eliminate redundant polynomials before any reduction. In particular, the F5 criterion ensures that the algorithm does not perform any reduction to 0 for polynomial systems given as a regular sequence. Due to space constraints, we refer to [11] for details.

4 TOOLS FOR THE PROOFS

The rest of the paper will be devoted to proving that Algo. 1 is correct and terminates. In this section, we recall necessary definitions for the proofs in Sec. 5.

4.1 Weak Gröbner bases

The main ingredient of the proof will be the fact that Möller's algorithm with signatures ensures that G_w is a weak Gröbner basis. In this section, we briefly recall relevant definitions and results.

Definition 4.1. *Let $f, g_1, \ldots, g_s, h \in A$. We say that f* weakly (top) reduces *in one step to h modulo $g_1, \ldots, g_s$ if there exists $J \subset \{1, \ldots, s\}$ such that*

- *for all $i \in J$, there exists $x^{a_i} \in \mathrm{Mon}(A)$ such that $x^{a_i} \mathrm{LM}(g_i) = \mathrm{LM}(f)$*
- *there exists $c_i \in A, i \in J$ such that $\sum_{i \in J} c_i \mathrm{LC}(g_i) = \mathrm{LC}(f)$*
- *$h = f - \sum_{i \in J} c_i x^{a_i} g_i$.*

In particular, $\mathrm{LT}(h) \precnsim \mathrm{LT}(f)$.

If f is S-labelled and $g_1, \ldots, g_s$ are G-labelled, we call the one-step reduction a

- weak $\mathfrak{s}$-reduction *if for all $i \in J$, $x^{a_i} \sigma(g_i) \preceq \mathfrak{s}(f)$, and a*
- regular weak $\mathfrak{s}$-reduction *if for all $i \in J$, $x^{a_i} \sigma(g_i) \precnsim \mathfrak{s}(f)$.*

As in the case of strong reductions, the terminology extends to sequences of reductions in one step.

[4] In older editions of that book, those criteria can be found in Sec. 2.9, Prop. 4 and Prop. 10 respectively.

Weak Gröbner bases (resp. weak $\mathfrak{s}$-Gröbner bases) are defined as strong Gröbner bases (resp. strong $\mathfrak{s}$-Gröbner bases), replacing strong reductions (resp. strong $\mathfrak{s}$-reductions) with weak ones.

Weak Gröbner bases can be computed with Möller's weak GB algorithm [1, Algo. 4.2.1]. A signature version of this algorithm, for PIDs, was presented in [11]. This algorithm is similar to Buchberger's algorithm, but it replaces strong reductions with weak reductions and strong S-polynomials with weak S-polynomials, defined as follows in the context of PIDs.

Definition 4.2. *Let $g_1, \dots, g_t \in A$ be S-labelled polynomials. Let J be a subset of $\{1, \dots, t\}$, define $M(J) = \operatorname{lcm}(\{M(j) : j \in J\})$. Let $s \in J$ and $J^* = J \setminus \{s\}$. We say that J is* regular saturated*, with* signature index *s, if*

$$J^* = \left\{ j \in \{1, \dots, t\} : M(j) \mid M(J) \text{ and } \frac{M(J)}{M(s)}\mathfrak{s}(g_s) \right\}.$$

Let $c \in R$ be such that $\langle c \rangle = \langle C(j) : j \in J^* \rangle : \langle C(s) \rangle$. Then there exists $(b_j)_{j \in J^*}$ such that $cC(s) = \sum_{j \in J^*} b_j C(j)$ and the regular weak S-polynomial *associated to J and (b_j) is*

$$c\frac{M(J)}{M(s)}g_s - \sum_{j \in J^*} b_i \frac{M(J)}{M(s)}.$$

This weak S-polynomial can be S-labelled with signature $S(J) = c\frac{M(J)}{M(s)}\mathfrak{s}(g_s)$.

4.2 Syzygies

A crucial tool for the proofs will be the syzygy characterization of Gröbner bases, using the syzygy lifting theorem of Möller [16]. This characterization gives a framework for proving that criteria eliminating S-pairs do not break the correctness or termination of the algorithm. The central notion is that of term-syzygies, of which we recall the definition.[5]

Definition 4.3. *Let $G = (g_1, \dots, g_t)$ be a tuple of nonzero S-labelled polynomials in A. We consider the free module A^t with basis $\epsilon_1, \dots, \epsilon_t$. For any element $\Sigma = \sum_{i=1}^t s_i \epsilon_i \in A^t$, we define $\overline{\Sigma} = \sum_{i=1}^t s_i g_i$. We say that Σ is a* term-syzygy *of G if*

$$\operatorname{LT}(\overline{\Sigma}) \precnsim \max\{\operatorname{LT}(s_i)T(i) : i \in \{1, \dots, t\}\}.$$

The polynomial $\overline{\Sigma}$ is called the syzygy polynomial *of Σ.*

The set of all term-syzygies of G is denoted by $\operatorname{TSyz}(G)$, it is a submodule of A^t called the syzygy module *of $\operatorname{LT}(G)$.*

If there exists a monomial μ s.t. for all $i \in \{1, \dots, t\}$, $\operatorname{LM}(s_i g_i) = \mu$ or 0, the term-syzygy Σ is called homogeneous with term degree *μ.*

The signature *of Σ is $\mathfrak{s}(\Sigma) = \max_i\{s_i\mathfrak{s}(g_i)\}$.*

*A tuple $(\Sigma_1, \dots, \Sigma_s)$ of $\operatorname{TSyz}(G)$ is called a S-*basis *of $\operatorname{TSyz}(G)$ if for all $\Sigma \in \operatorname{TSyz}(G)$, there exists $p_1, \dots, p_s \in A$ such that*

- $\Sigma = \sum_{i=1}^s p_i \Sigma_i$
- $\mathfrak{s}(\Sigma) \succeq \max_i\{\operatorname{LM}(p_i)\mathfrak{s}(\Sigma_i)\}$.

Definition 4.4. *A strong (resp. weak) S-polynomial is the syzygy polynomial $\overline{\Sigma}$ for some homogeneous term-syzygy $\Sigma \in \operatorname{Syz}(F)$. We call those syzygies strong (resp. weak) S-pol. syzygies.*

Strong S-pol. syzygies are homogeneous term-syzygies with exactly two non-zero coefficients, and are sometimes called principal *term-syzygies in the literature.*

[5] In the literature, term-syzygies are sometimes simply called syzygies, and syzygy polynomials, S-polynomials.

The characterization of Gröbner bases using term-syzygies is given in Möller's lifting theorem [16, Th. 4], of which we give a signature version here.

Theorem 4.5. *Let $\mathfrak{a} = \langle f_1, \dots, f_m \rangle$ be an ideal in A and $G = (g_1, \dots, g_t)$ be a tuple of nonzero S-labelled polynomials in $\mathfrak{a}$ such that for all $i \in \{1, \dots, m\}$, f_i $\mathfrak{s}$-reduces to 0 modulo G. Let $\mathbf{T} \in \operatorname{Ter}(A^m)$, and let $\operatorname{TSyz}_{\mathbf{T}}(G)$ be the module of term-syzygies generated by term-syzygies with signature at most $\mathbf{T}$.*

Let $\Sigma_1, \dots, \Sigma_s \in \operatorname{TSyz}(G)$ be a homogeneous S-basis of $\operatorname{TSyz}_{\mathbf{T}}(G)$, where $\Sigma_i = \sum_{j=1}^t \sigma_{ij}\epsilon_j$, and define for $i \in \{1, \dots, s\}$ the syzygy polynomial $\overline{\Sigma_i} = \sum_{j=1}^t \sigma_{ij} g_j$.

Then G is a strong $\mathfrak{s}$-Gröbner basis of $\mathfrak{a}$ up to signature $\mathbf{T}$ if and only if for all $i \in \{1, \dots, s\}$, $\overline{\Sigma_i}$ strongly $\mathfrak{s}$-reduces to 0 modulo G.

Proof. The proof is similar to that of [16, Th. 1 and Th. 4]: indeed, if $f \in \mathfrak{a}$ has signature $\mathbf{T} \in \operatorname{Ter}(A^m)$, f has a representation $\sum_{i=1}^m q_i f_i$ with $\max_i \operatorname{LT}(q_i)\mathbf{e}_i \preceq \mathbf{T}$. Since all f_i's $\mathfrak{s}$-reduce to 0 modulo G, f also has a representation $\sum_{j=1}^t h_j g_j$ such that $\max_i \operatorname{LT}(h_i)\mathfrak{s}(g_i) \preceq \mathbf{T}$.

Following the proof of [16, Th. 1] allows to use term-syzygies with signature $\preceq \mathbf{T}$ to rewrite this representation into a Gröbner representation, that can be decomposed into a sequence of reductions.

Conversely, if all $f \in \mathfrak{a}$ $\mathfrak{s}$-reduce to 0, in particular it is true for the syzygy polynomials of term-syzygies of G. □

5 CORRECTNESS AND TERMINATION

5.1 Signature properties

In this subsection, we prove useful lemmas, related to the behavior of signatures throughout the algorithm, and generalizing with signatures the correspondence between weak and strong constructions (reductions and S-polynomials) described in [16].

Lemma 5.1. *Let $\{g_1, \dots, g_r\}$ be the value of G_w at any point in the course of Algo. 1. Then $\mathfrak{s}(g_1) \preceq \mathfrak{s}(g_2) \preceq \cdots \preceq \mathfrak{s}(g_r)$.*

Proof. The proof is similar to that of [11, Lem. 5.2]. Assume that there exists i such that $\mathfrak{s}(g_i) \succ \mathfrak{s}(g_{i+1})$ and that i is the smallest index with this property. Let (j_i, k_i) (resp. (j_{i+1}, k_{i+1})) be the admissible pair used to compute g_i (resp. g_{i+1}).

If i is not one of j_{i+1}, k_{i+1}, then (j_{i+1}, k_{i+1}) was already in the queue $\mathcal{P}$ when (j_i, k_i) was selected, and so, by the selection criterion in the algorithm, $S(j_i, k_i) \prec S(j_{i+1}, k_{i+1})$.

If i is either j_{i+1} or k_{i+1}, wlog we can assume that $i = j_{i+1}$. Then

$$\begin{aligned} S(j_{i+1}, k_{i+1}) &\simeq \max\left(\frac{T(i, k_{i+1})}{\operatorname{LT}(g_i)}\mathfrak{s}(g_i), \frac{T(i, k_{i+1})}{\operatorname{LT}(g_{k_{i+1}})}\mathfrak{s}(g_{k_{i+1}})\right) \\ &\succeq \frac{T(i, k_{i+1})}{\operatorname{LT}(g_i)}\mathfrak{s}(g_i) \succeq \mathfrak{s}(g_i). \end{aligned}$$

□

It allows us to prove that the signatures of elements in G_s are also non-decreasing.

Lemma 5.2. *Let $\{g_1, \dots, g_{r-1}\}$ be the value of G_w at any point in the course of Algo. 1, and let g_r be the next computed element in the basis. Then all elements added to G_s have G-signature $\succeq \mathfrak{s}(g_r)$.*

More generally, all elements added to G_s in later steps have G-signature $\succeq \mathfrak{s}(g_r)$.

Proof. The elements added to G_s in the call to Update with g_r as new element, are g_r (with signature $\mathfrak{s}(g_r)$) and all G-polynomials G-Pol(h, g_r) for h already in G_s (with G-signature $S_G(\sigma(h), \mathfrak{s}(g_r))$). Those G-labelled polynomials all have G-signature $\succeq \mathfrak{s}(g_r)$.

The generalized statement follows from the fact that $\mathfrak{s}(g_s) \succeq \mathfrak{s}(g_r)$ for $s > r$ (Lem. 5.1). □

The next lemma is a more precise description of elements of G_s.

Lemma 5.3. *Let $G_w = \{g_1, \dots, g_r\}$ be a set of S-labelled polynomials, and G_s be its (G-labelled) completion. Let $h \in G_s$, then there exists $i_1, \dots, i_k \in \{1, \dots, r\}$ such that*

$$h = G\text{-Pol}(G\text{-Pol}(\cdots G\text{-Pol}(g_{i_1}, g_{i_2}), \dots, g_{i_{k-1}}), g_{i_k}).$$

Furthermore, there exists $c_j \in R$, $m_j \in \mathrm{Mon}(A)$, $j \in \{1, \dots, k\}$ such that $\mathrm{LT}(h) = \sum_{j=1}^{k} c_j m_j T(i_j)$ and $\sigma(h) \simeq \max(m_j \mathfrak{s}(g_{i_j}))$.

Proof. The existence of $i_1, \dots, i_k$ and the decomposition of h and $\mathrm{LT}(h)$ are clear by definition of the completion.

For the inequality regarding the signature, we proceed by induction on k, where the base case $k = 1$ is clear.

Let $k > 1$, and let h_{k-1} be the result of the innermost $k-1$ G-polynomials in the expansion of h. So $h = G\text{-Pol}(h_{k-1}, g_{i_k})$ and h_{k-1} expands as $k-1$ successive G-polynomials of $g_{i_1}, \dots, g_{i_{k-1}}$, with $m'_j M(i_j) = \mathrm{LM}(h_{k-1})$ for all $j \in \{1, \dots, k-1\}$. Note that for all $j \in \{1, \dots, k-1\}$, $\mu m'_j = m_j$.

There exists $\mu \in \mathrm{Mon}(A)$ such that $\mathrm{LM}(h) = \mu \mathrm{LM}(h_{k-1}) = m_k M(i_k)$, and

$$\begin{aligned}
\sigma(h) &\simeq \max(\mu\sigma(h_{k-1}), m_k \mathfrak{s}(g_{i_k})) \text{ by def. of the } G\text{-signature} \\
&\simeq \max\left(\mu \max_{j \le k-1}(m'_j \mathfrak{s}(g_{i_j})), m_k \mathfrak{s}(g_{i_k})\right) \text{ by induction hyp.} \\
&\simeq \max_{j \le k}(m_j \mathfrak{s}(g_{i_j})).
\end{aligned}$$ □

The last results of this section generalize the correspondence between weak and strong Gröbner bases [16], adding some control over the signatures. First, we generalize the equivalence between weak reduction and strong reduction through completion of the reducers [16, Prop. 2].

Lemma 5.4. *Let $G_w = \{g_1, \dots, g_r\}$ be a weak $\mathfrak{s}$-GB up to signature $\mathbf{T}$, and G_s be its completion. Let f be a S-labelled polynomial with signature $\mathfrak{s}(f) \prec \mathbf{T}$, then the following properties are equivalent:*

(1) f is weakly $\mathfrak{s}$-reducible (resp. weakly regular $\mathfrak{s}$-reducible) mod. G_w;
(2) f is strongly $\mathfrak{s}$-reducible (resp. strongly regular $\mathfrak{s}$-reducible) mod. G_s.

Proof. For (1) ⇒ (2), we proceed by induction on r. The case $r = 1$ is clear, because then both G_w and G_s contain only the element g_1.

For the general case, let f be a S-labelled polynomial with signature $\mathfrak{s}(f) \prec \mathbf{T}$ and weakly $\mathfrak{s}$-reducible modulo G_w. Let $H_w = \{g_j : j \in J \subseteq \{1, \dots, r\}\} \subseteq G_w$ be a set of weak $\mathfrak{s}$-reducers of f, and consider its completion $H_s = C(H_w) \subseteq G_s$. By [16, Prop. 2], f is strongly reducible modulo H_s. Let $h \in H_s$ be a strong reducer of f. In particular, there exists $\mu \in \mathrm{Mon}(A)$ such that $\mu \mathrm{LM}(h) = \mathrm{LM}(f)$. In order to prove that h is a strong $\mathfrak{s}$-reducer of f, we need to prove that $\mu\sigma(h) \preceq \mathfrak{s}(f)$.

By Lem. 5.3, h expands as iterated G-polynomials of elements $h_1, \dots, h_k$ of H_w such that for all $j \in \{1, \dots, k\}$, there exists $m_j \in \mathrm{Mon}(A)$ such that $m_j \mathrm{LM}(h_j) = \mathrm{LM}(h)$ and $\sigma(h) = \max(m_j \mathfrak{s}(h_j))$.

Let $j \in \{1, \dots, k\}$. Since $h_j \in H_w$, it is a weak $\mathfrak{s}$-reducer of f, so there exists μ_j such that $\mu_j \mathrm{LM}(h_j) = \mathrm{LM}(f)$, and $\mu_j \mathfrak{s}(h_j) \preceq \mathfrak{s}(f)$. Note that $\mu_j = m_j \mu$. So

$$\mu\sigma(h) \simeq \mu \max(m_j \mathfrak{s}(h_j)) \simeq \max(\mu_j \mathfrak{s}(h_j)) \preceq \mathfrak{s}(f).$$

The fact that (2) ⇒ (1) is an immediate consequence of Lem. 5.3: if $h \in G_s$ is a strong $\mathfrak{s}$-reducer of f, then it expands as iterated G-polynomials of elements $g_{i_1}, \dots, g_{i_k} \in G_w$ which are weak $\mathfrak{s}$-reducers of f.

The statements with regular $\mathfrak{s}$-reductions are proved similarly, replacing $\preceq$ with $\precneqq$ throughout. □

As a consequence, like in [16], the completion of a weak $\mathfrak{s}$-GB is a strong $\mathfrak{s}$-GB.

Corollary 5.5. *Let $G_w = \{g_1, \dots, g_r\}$ be a set of S-labelled polynomials, and G_s its (G-labelled) completion. Let $\mathbf{T} \in \mathrm{Ter}(A^m)$. Then*

- *G_w is a weak $\mathfrak{s}$-GB up to signature $\mathbf{T}$ iff G_s is a strong $\mathfrak{s}$-GB up to signature $\mathbf{T}$;*
- *G_w is a weak $\mathfrak{s}$-GB iff G_s is a strong $\mathfrak{s}$-GB.*

The last lemmas of this section generalizes the expression of a weak S-polynomial in terms of strong S-polynomials, with control over the signatures. First, we take care of weak S-polynomials, without any regularity assumption.

Lemma 5.6. *Let $(g_1, \dots, g_r)$ be a tuple of S-labelled polynomials. Let $J \subset \{1, \dots, r\}$, and let $\mathbf{p} \subset A^r$ (with basis (ϵ_j)) be a homogeneous term syzygy associated to a weak S-pol. with support J. Then there exists coefficients $a_{i,j} \in R$, and monomials $m_{i,j}$, $i<j \in J$, such that*

$$\mathbf{p} = \sum_{i,j \in J} a_{i,j} m_{i,j} S\text{-Pol}(\epsilon_i, \epsilon_j).$$

In this decomposition:

(1) for all $i, j \in J$, $m_{i,j} M(i,j) = M(J)$
(2) for all $i, j \in J$, $m_{i,j} S(i,j) \preceq \max(\frac{M(J)}{M(i)} \mathfrak{s}(g_i))$.

Proof. The existence of $a_{i,j}$ and $m_{i,j}$, $i<j \in J$, is given by [16, Th. 2 and Prop. 1], and it follows from that proof that $m_{i,j} M(i,j) = M(J)$. So for all $i, j \in J$,

$$m_{i,j} S(i,j) = \frac{M(J)}{M(i,j)} S(i,j) \preceq \frac{M(J)}{M(i,j)} \frac{M(i,j)}{M(i)} \mathfrak{s}(f_i) \simeq \frac{M(J)}{M(i)} \mathfrak{s}(f_i),$$

and similarly for j. □

Lemma 5.7. *Let $(g_1, \dots, g_r)$ be a tuple of S-labelled polynomials. Let $J \subset \{1, \dots, r\}$ be a regular subset, with signature index s, and let $J^* = J \setminus \{s\}$. Let $\mathbf{p} \subset A^r$ be a homogeneous term syzygy associated to a regular weak S-polynomial. With the notations of 5.6, denote $a_i := a_{i,s}$ if $i<s$ and $a_{s,i}$ otherwise, and define similarly $m_{i,j}$, so that we have the decomposition*

$$\mathbf{p} = \sum_{i \in J^*} a_i m_i S\text{-Pol}(\epsilon_i, \epsilon_s) + \sum_{i,j \in J^*} a_{i,j} m_{i,j} S\text{-Pol}(\epsilon_i, \epsilon_j)$$

In this decomposition:

(1) $\sum_{i \in J^*} a_i C(i,s) = C(J)$
(2) $\forall i \in J^*$, the S-pair (i,s) is regular and $m_i S(i,s) \simeq S(J)$
(3) $\sum_{i \in J^*} a_i m_i S(i,s) = S(J) = \mathfrak{s}(\mathbf{p})$

(4) $\forall i,j \in J^*,\ m_{i,j}\, S(i,j) \lesssim S(J)$

Proof. In the proof of [16, Prop. 1] a_i and m_i, for $i \in J^*$, are defined as follows. Let c be the generator of $\langle C(i) : i \in J^* \rangle : \langle C(s) \rangle$, and for $i \in J^*$, let $d_i = \frac{C(i,s)}{C(s)}$. Then there exists $(a_i)_{i \in J^*}$, such that $c = \sum_{i \in J^*} a_i d_i$. In particular, $C(J) = \sum_{i \in J^*} a_i C(i,s)$. For $i \in J^*$, define $m_i = \frac{M(J)}{M(i,s)}$. With those a_i and m_i, property 1 is satisfied.

Since the set J is regular with signature index s, by definition, $S(J) \simeq \frac{M(J)}{M(s)} \mathfrak{s}(f_s)$, and for all $i \in J^*$, $\frac{M(J)}{M(s)} \mathfrak{s}(f_s) \gtrsim \frac{M(J)}{M(s)} \mathfrak{s}(f_i)$. So for all $i \in J^*$, $\frac{M(i,s)}{M(s)} \mathfrak{s}(f_s) \gtrsim \frac{M(i,s)}{M(s)} \mathfrak{s}(f_i)$, so the S-pair (i,s) is regular and $S(J) \simeq \frac{M(J)}{M(i,s)} S(i,s) = m_i S(i,s)$. This proves property 2.

By definition, $S(J) = \frac{C(J)}{C(s)} M(J) M(s) \mathfrak{s}(f_s)$ and for all $i \in J^*$, $S(i,s) = \frac{C(i,s)}{C(s)} M(J) M(s) \mathfrak{s}(f_s)$. So, expanding $C(J) = \sum_{i \in J^*} a_i C(i,s)$ again, property 3 is satisfied.

Now consider $\mathbf{q} = \sum_{i,j \in J^*} a_{i,j} m_{i,j} S\text{-Pol}(\epsilon_i, \epsilon_j)$. It corresponds to a homogeneous term syzygy, with term degree $\simeq M(J)$. We have seen above that for all $i \in J^*$, $\frac{M(J)}{M(s)} \mathfrak{s}(f_s) \gtrsim \frac{M(J)}{M(s)} \mathfrak{s}(f_i)$. From Lem. 5.6, for all $i,j \in J^*$, $m_{i,j} S(i,j) \preceq \max(\frac{M(J)}{M(s)} \mathfrak{s}(f_i)) \lesssim S(J)$. □

Remark 5.8. *Property (4) actually gives another proof of property (3), by proving that* $\mathbf{q}$ *has signature* $\lesssim \mathfrak{s}(\mathbf{p})$. *Writing* $\mathbf{q} = \mathbf{p} - \sum_{i \in J^*} a_i m_i S\text{-Pol}(\epsilon_i, \epsilon_s)$, *it means that the signature of the two terms of the difference have to cancel out.*

5.2 Proof of the algorithm

The proof of correctness makes use of the following result for weak signature Gröbner bases, proved in [11].

Proposition 5.9 ([11, Th. 5.5]). *Let* $G_w = \{g_1, \ldots, g_r\}$ *be a set of* S*-labelled polynomials. Let* $\mathbf{T} \in \mathrm{Ter}(A^m)$. *Assume that all regular weak* S*-polynomials with signature* $\preceq \mathbf{T}$ $\mathfrak{s}$*-reduce to* 0 *modulo* G_w. *Then* G_w *is a weak signature Gröbner basis up to signature* $\mathbf{T}$.

Corollary 5.10. *Let* $G = \{g_1, \ldots, g_t\}$ *be a set of* S*-labelled polynomials,* $\mathbf{T} \in \mathrm{Ter}(A^m)$,

$$\mathcal{S}_{\prec \mathbf{T}}(G) = \{\textit{homo. term-syz. of } G \textit{ with sig. } \lesssim \mathbf{T}\}$$

and

$$\mathcal{S}_{\mathbf{T}}(G) = \mathcal{S}_{\prec \mathbf{T}}(G) \cup \{\textit{regular weak } S\textit{-pol. syz. of } G \textit{ with sig. } \simeq \mathbf{T}\}\,.$$

Then $\mathcal{S}_{\mathbf{T}}(G)$ *is a* S*-basis of* $\mathrm{TSyz}_{\mathbf{T}}(G)$.

Proof. The notion of S-basis of term-syzygies only depends on the leading terms and labels of the family G. Extend the polynomial algebra $A = R[x_1, \ldots, x_n]$ into $A_{\mathrm{ext}} = R[x_1, \ldots, x_n, y_1, \ldots, y_t]$, with a block order ordering the x_i's first according to the monomial order on A. Consider the set $G_{\mathrm{ext}} = \{g_i - y_i\} \subset A_{\mathrm{ext}}$, where $g_i - y_i$ is given the signature $\mathfrak{s}(g_i)$. S-bases of syzygies of $\mathrm{TSyz}_{\mathbf{T}}(G_{\mathrm{ext}})$ and $\mathrm{TSyz}_{\mathbf{T}}(G)$ are in natural one-to-one correspondence.

Let $\Sigma \in \mathrm{TSyz}_{\mathbf{T}}$. If $S(\Sigma) \lesssim \mathbf{T}$ there is nothing to prove, so assume that $S(\Sigma) \simeq \mathbf{T}$. Write $\Sigma = \sum_{i=1}^t \sigma_i \epsilon_i$, $\bar{\Sigma} = \sum_{i=1}^t \sigma_i g_i$ and $\Sigma(y) = \sum_{i=1}^t \sigma_i y_i$, in particular the syzygy polynomial associated to Σ in A_{ext} is $\bar{\Sigma} - \Sigma(y)$.

Let $S_1, \ldots, S_k$ be the regular weak S-pol. syzygies of G_{ext} with signature $\simeq \mathbf{T}$. Regular reducing them, in A_{ext}^t, yields module elements of the form $S_i' = S_i - \sum(\text{elements with sig. } \lesssim \mathbf{T})$. Note that since we are only performing regular reductions and the signature of S_i is not divisible by any y_j, those module elements remain linear in y. By Prop. 5.9, adding to G all the S_i' ensures that all polynomials with signature at most $\mathbf{T}$ $\mathfrak{s}$-reduce to 0, in particular, the syzygy polynomial of Σ (in A_{ext}) $\mathfrak{s}$-reduces to 0. In other words, there exist $\tau_1, \ldots, \tau_k \in \mathrm{Ter}(A)$ such that

$$\bar{\Sigma} - \Sigma(y) = \sum_{i=1}^k \tau_i \left(\bar{S}_i' - S_i'(y)\right) \text{ in } A_{\mathrm{ext}}$$

and, again since the reduction cannot increase the signature, the equality also holds in A: $\bar{\Sigma} = \sum_{i=1}^k \tau_i \bar{S}_i$ in A. So in the end, we get that

$$\Sigma(y) = \sum_{i=1}^k S_i'(y) = \sum_{i=1}^k S_i(y) + \sum(\text{elements with sig. } \lesssim \mathbf{T}),$$

and substituting back $y_i \leftarrow \epsilon_i$ gives a representation of Σ as a linear combination of elements of $\mathcal{S}_{\mathbf{T}}$, where all summands have signature at most $\mathbf{T} = S(\Sigma)$. □

Theorem 5.11 (Correctness and termination of Algo. 1). *Given* $f_1, \ldots, f_m \in A$, *Algo. 1 terminates and returns a strong* $\mathfrak{s}$*-Gröbner basis of* $\mathfrak{a} = \langle f_1, \ldots, f_m \rangle$.

Proof. The proof of termination is a transposition of that of [11, Th. 5.6] (which follows the proof of termination in [19]), to prove that G_w, and thus G_s, cannot grow infinitely large.

As for correctness, let G_w and G_s be as computed by Algo. 1. Assume that G_s is not a strong $\mathfrak{s}$-GB of $\mathfrak{a}$, then there exists $\mathbf{u} \in \mathrm{Ter}(A^m)$ such that G_s is not a $\mathfrak{s}$-GB up to signature $\mathbf{u}$. Assume that $\mathbf{u}$ is minimal for this property, in particular, for all $\mathbf{T} \lesssim \mathbf{u}$, G_s is a strong $\mathfrak{s}$-GB up to signature $\mathbf{T}$.

Equivalently, from Cor. 5.5, G_w is a weak $\mathfrak{s}$-GB up to signature $\mathbf{T}$ but not a weak $\mathfrak{s}$-GB up to signature $\mathbf{u}$. By Cor. 5.10, $\mathcal{S}_{\mathbf{u}}(G_w)$ is a S-basis of the module $\mathrm{TSyz}_{\mathbf{u}}(G_w)$. Let $\mathcal{S}_{\prec} = \mathcal{S}_{\prec \mathbf{u}}(G_w)$. Then by Lem. 5.7, the set

$$\mathcal{S}_{\prec} \cup \{\text{regular strong } S\text{-pol. sygygies of } G_w \text{ with sig. } \simeq \mathbf{u}\}$$

is a S-basis of the module $\mathrm{TSyz}_{\mathbf{u}}(G_w)$.

Let $\Sigma(i,j)$ be a strong S-pol. syzygy associated with an S-pair (i,j) such that Criterion $\mathrm{Chain}(i,j;k)$ holds for some $k \in \mathbb{N}$. Then as in the classical case [5, Sec. 2.10, Prop. 8], $\Sigma(i,j)$ can be rewritten as

$$\Sigma(i,j) = \frac{T(i,j)}{T(i,k)} \Sigma(i,k) - \frac{T(i,j)}{T(j,k)} \Sigma(j,k).$$

The signature condition in Chain implies that this rewriting does not make the signature increase. So $\Sigma(i,j)$ can be removed from the S-basis of term-syzygies.

Iterating the process, we get that the set

$$\mathcal{S}_{\prec} \cup \{\text{regular } S\text{-pairs of } G_w \text{ with sig. } \simeq \mathbf{u} \text{ not excluded by Chain}\}$$

is a S-basis of the module $\mathrm{TSyz}_{\mathbf{u}}(G_w)$.

The algorithm ensures that all regular strong S-polynomials obtained from a S-pair not excluded by Chain strongly $\mathfrak{s}$-reduce to 0 modulo G_s. Furthermore, by minimality of $\mathbf{u}$, for all syzygies Σ in $\mathcal{S}_{\prec}$, the syzygy-polynomial $\bar{\Sigma}$ strongly $\mathfrak{s}$-reduces to zero modulo G_s. So all syzygy-polynomials associated with all term-syzygies in our basis strongly $\mathfrak{s}$-reduce to 0 modulo G_s, and by the lifting theorem 4.5, G_s is a strong $\mathfrak{s}$-Gröbner basis up to signature $\mathbf{u}$. □

System	Pairs	S-pols	Coprime	Chain	F5	Singular	1-Singular	Red. to 0
Katsura-3	504	178	157	153	115	1	6	0
Katsura-4	1660	603	509	517	388	9	84	0
Generic (3;2;10)	383	192	73	99	117	1	19	0
Generic (3;3;5)	2211	1161	155	911	842	0	78	0

Table 1: Experimental data on Möller's algorithm with signatures.

6 IMPLEMENTATION AND FUTURE WORK

We have written a toy implementation[6] in Magma [2] of the algorithm, with the F5, Singular and 1-singular criteria. We give experimental data related to the computation of Gröbner bases for various polynomial systems over $\mathbb{Z}$: Katsura-n systems, and random systems with fixed degree and size of the coefficients. The data is given in Table 1 ("Generic $(n; d; s)$" is a random system of n polynomials in n variables with degree d and coefficients in $[-s; s]$). For each system, we give the number of considered S-pairs and reduced S-polynomials, as well as how many polynomials were excluded by the Coprime or Chain criterion (before being considered as a S-pair), by the F5 or Singular criterion (counted in S-pairs, not in S-polynomials), or because they are 1-singular reducible (after regular reducing). We also give the number of reductions to 0 appearing in the algorithm, which is 0 as expected for regular sequences.

Möller's weak GB algorithm involved a combinatorial bottleneck with cost exponential in the size of the current basis, making it impractical as soon as the basis exceeds 30 elements. Möller's strong GB algorithm for PIDs replaces it with the computations of S-pairs, with quadratic cost. As a result, the algorithm is faster, but nonetheless becomes slow as the basis grows. As is frequently the case with Gröbner basis algorithms, the main bottleneck appears to be the reduction step.

We implemented two additional optimizations, for $\mathbb{Z}$, in order to reduce the size of the basis. The first one is a heuristic at the selection step in the algorithm: when we pick a pair (i, j) with minimal signature $S(i, j)$, we typically have a choice between many such pairs. Selecting the one with the smallest coefficient part (in absolute value) appears to help eliminating subsequent S-polynomials faster, and makes the algorithm significantly faster: for instance, the Katsura-4 example was impractical before this change, and terminates in less than 30s after.

The second optimization relies on the following idea: for a given $i \in \{1, \dots, m\}$, when we enter the "for" loop at index i, we know that all subsequent polynomials will have a signature of the form $\bullet\, \mathbf{e}_k$ with $k \geq i$, and all preceding polynomials have a signature of the form $\bullet\, \mathbf{e}_k$ with $k < i$. In particular, we do not need to consider the individual signatures of already computed elements, beyond the information that this signature is $\precnsim \mathbf{e}_i$.

As such, we may inter-reduce the strong basis G_s and replace both G_w and G_s with the result, all elements being given signature $\mathbf{e}_1$. For this inter-reduction step, at least in the case of $\mathbb{Z}$, we could use Magma's highly optimized routines.

The consequence is that after each pass through the "for" loop, the weak and strong bases are made shorter, which slows down the growth of the list of pairs in the remainder of the algorithm.

One difficulty arising when computing signature Gröbner bases over rings is that the Singular criterion requires the signature to match exactly, including their coefficient. This leads to the computation of many polynomials having similar signatures and leading monomials. The heuristic presented above helps mitigate the issue, but it will be the object of future work to examine whether the Singular criterion can be extended to eliminate more elements, in the case of principal rings.

For computations over $\mathbb{Z}$ or $K[X]$, it would also be interesting to use the additional structure of an euclidean ring to make the computations faster. It will be the focus of future research to investigate whether leading coefficient reductions [13, 14] can be added to the algorithm without breaking signature invariants.

Acknowledgements The authors thank C. Eder for helpful suggestions, M. Ceria and T. Mora for a fruitful discussion on the syzygy paradigm for Gröbner basis algorithms, and M. Kauers for his valuable insights and comments all through the elaboration of this work.

[6] Available online: https://github.com/ThibautVerron/SignatureMoller

REFERENCES

[1] W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases.* American Mathematical Society, 7 1994.
[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
[3] B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner-bases. In *Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979)*, volume 72 of *Lecture Notes in Comput. Sci.*, pages 3–21. Springer, Berlin-New York, 1979.
[4] B. Buchberger. Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation*, 41:475–511, 2006.
[5] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.
[6] C. Eder and Jean-Charles Faugère. A Survey on Signature-based Algorithms for Computing Gröbner Bases. *Journal of Symbolic Computation*, 80:719–784, 2017.
[7] C. Eder and J.E. Perry. Signature-based Algorithms to Compute Gröbner Bases. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, pages 99–106. ACM, 2011.
[8] C. Eder, G. Pfister, and A. Popescu. On Signature-Based Gröbner Bases over Euclidean Rings. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 141–148, New York, NY, USA, 2017. ACM.
[9] Jean Charles Faugère. A New Efficient Algorithm for Computing GrÖbner Bases without Reduction to Zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.
[10] M. Francis and A. Dukkipati. On Ideal Lattices, Gröbner Bases and Generalized Hash Functions. *Journal of Algebra and Its Applications*, 2017.
[11] Maria Francis and Thibaut Verron. Signature-based Criteria for Möller's Algorithm for Computing Gröbner Bases over Principal Ideal Domains. *preprint*, abs/1802.01388, 2018.
[12] R. Gebauer and H. M. Möller. On an Installation of Buchberger's Algorithm. *Journal of Symbolic Computation*, 6(2-3):275–286, 1988.
[13] A. Kandri-Rody and D. Kapur. Computing a Gröbner Basis of a Polynomial Ideal over a Euclidean Domain. *J. Symbolic Comput.*, 6(1):37–57, 1988.
[14] D. Lichtblau. Effective Computation of Strong Gröbner Bases over Euclidean Domains. *Illinois J. Math.*, 56(1):177–194 (2013), 2012.
[15] D. Lichtblau. Applications of Strong Gröbner Bases over Euclidean Domains. *Int. J. Algebra*, 7(5-8):369–390, 2013.
[16] H. M. Möller. On the Construction of Gröbner Bases using Syzygies. *Journal of Symbolic Computation*, 6(2-3):345–359, 1988.
[17] H. M. Möller, T. Mora, and C. Traverso. Gröbner bases computation using syzygies. In *Papers from the International Symposium on Symbolic and Algebraic Computation*, ISSAC '92, pages 320–328, New York, NY, USA, 1992. ACM.
[18] Luquan Pan. On the D-bases of polynomial ideals over principal ideal domains. *J. Symbolic Comput.*, 7(1):55–69, 1989.
[19] B. H. Roune and M. Stillman. Practical Gröbner Basis Computation. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, pages 203–210. ACM, 2012.