A Signature-based Algorithm for Computing Gröbner Bases over Principal Ideal Domains

Maria Francis and Thibaut Verron

Abstract. Signature-based algorithms have become a standard approach for Gröbner basis computations for polynomial systems over fields, but how to extend these techniques to coefficients in general rings is not yet as well understood.

In this paper, we present a proof-of-concept signature-based algorithm for computing Gröbner bases over commutative integral domains. It is adapted from a general version of Möller's algorithm (1988) which considers reductions by multiple polynomials at each step. This algorithm performs reductions with non-decreasing signatures, and in particular, signature drops do not occur. When the coefficients are from a principal ideal domain (*e.g.* the ring of integers or the ring of univariate polynomials over a field), we prove correctness and termination of the algorithm, and we show how to use signature properties to implement classic signature-based criteria to eliminate some redundant reductions. In particular, if the input is a regular sequence, the algorithm operates without any reduction to 0.

We have written a toy implementation of the algorithm in Magma. Early experimental results suggest that the algorithm might even be correct and terminate in a more general setting, for polynomials over a unique factorization domain (*e.g.* the ring of multivariate polynomials over a field or a PID).

1. Introduction

The theory of Gröbner bases was introduced by Buchberger in 1965 [5] and has since become a fundamental algorithmic tool in computer algebra. Over the past decades, many algorithms have been developed to compute Gröbner bases more and more efficiently. The latest iteration of such algorithms is the class of signature-based algorithms, which introduce the notion of signatures and use it to detect and prevent unnecessary or redundant reductions. Following early work in [20], the technique of signatures was first formally introduced for Algorithm F5 [11], allowing to compute a Gröbner basis for a regular sequence without any reduction to zero. Since then, there have been many research works in this direction [13, 2, 7, 8].

All these algorithms are for ideals in polynomial rings over fields. Gröbner bases can be defined and computed over commutative rings [1, Ch. 4]. This can be used in many applications, *e.g.* for polynomials over $\mathbb{Z}$ in lattice-based cryptography [12] or for polynomials over a polynomial ring as an elimination tool [21]. Many other examples are described in [18].

If the coefficient ring is not a field, there are two ways to define Gröbner bases, namely weak and strong bases. Strong Gröbner bases ensure that normal forms can be computed as in the case of fields. But a strong Gröbner basis is in general larger than a weak one, and if the base ring is not a Principal Ideal Domain (PID), then some ideals exist which do not admit a strong Gröbner basis. On the other hand, weak Gröbner bases, or simply Gröbner bases, always exist for polynomial ideals over a Noetherian commutative ring. They do not necessarily define a unique normal form, but they can be used to decide ideal membership. If necessary, over a PID, a post-processing phase performing coefficient reductions can be used to obtain a strong Gröbner basis.

Recent works have focused on generalizing signature-based techniques to Gröbner basis algorithms over rings. First steps in this direction, adding signatures to a modified version of Buchberger's algorithm for strong Gröbner bases over Euclidean rings [17], were presented in [9]. That paper proves that a signature-based Buchberger's algorithm for strong Gröbner bases cannot ensure correctness of the result after encountering a "signature-drop", but can nonetheless be used as a prereduction step in order to significantly speed up the computations.

In this paper, we prove that it is possible to compute a weak signature-Gröbner bases of polynomial ideals over PIDs (including Euclidean rings) using signature-based techniques. The proof-of-concept algorithm that we present is adapted from the weak Gröbner basis algorithm due to Möller [19] [1, Sec. 4.2], which is designed to compute a basis for a polynomial ideal over any ring, and does so by considering combinations and reductions by multiple polynomials at once. The main difference with the results of [9] is that we use a stricter definition of regular reductions, effectively preventing more reductions from happening, and at the same time adding more polynomials to the basis.

This ensures that no reductions leading to signature-drops can happen in the algorithm, and as a consequence, we prove that the algorithm terminates and computes a signature Gröbner basis with elements ordered with non-decreasing signatures. This property allows us to examine classic signature-based criteria, such as the syzygy criterion, the F5 criterion and the singular criterion, and show how they can be adapted to the case of PIDs. In particular, when the input forms a regular sequence, the algorithm performs no reductions to zero. To the best of our knowledge, this is the first algorithm that, given a regular sequence of polynomials with coefficients in a PID, can compute a Gröbner basis of the corresponding ideal without any reduction to zero.

Möller also presented an efficient algorithm that computes (strong) Gröbner basis for polynomial ideals where the coefficients are from Principal Ideal Rings [19, Section 4]. That algorithm skips the combinatorial bottleneck of computing saturated sets. Instead, it uses two polynomials to build S-polynomials and makes use of Gebauer-Möller criteria [15], previously introduced for fields, to discard redundant S-polynomials.

Whenever necessary, for clarity, we shall refer to that algorithm as Möller's *strong* algorithm. The algorithm at the center of our focus, computing weak Gröbner bases, will be referred to as Möller's *weak* algorithm, or simply Möller's algorithm.

We have written a toy implementation of the algorithms presented, with the F5 and the singular criteria, in the Magma Computational Algebra System [4], and compared its efficiency, in terms of number of excluded pairs, with Möller's strong algorithm. Experimentally, on all considered examples, Möller's (weak) algorithm with signatures does compute and reduce fewer S-polynomials than Möller's strong algorithm.

Möller's (weak) algorithm, without signatures, works for polynomial systems over any Noetherian commutative ring. The signature-based algorithm is only proved to be correct and to terminate for PIDs, but with very few changes, it can be made to accommodate inputs with coefficients in a more general ring. Interestingly, early experimental data with coefficients in a multivariate polynomial ring (a Unique Factorization Domain but not a PID) suggest that the signature-based algorithm might work over more general rings than just PIDs. For that reason, and because it does not overcomplicate the exposition, we choose to present Möller's algorithms, with and without signatures, in their most general form, accepting input over any Noetherian commutative ring.

Previous works. Signature-based Gröbner basis algorithms over fields have been extensively studied, and an excellent survey of those works can be found in [6]. The technical details of most proofs can be found in [22, 10]. The theory of Gröbner bases for polynomials over Noetherian commutative rings dates back to the 1970s [23, 19] and a good exposition of these approaches can be found in [1]. Algorithms exist for both flavors of Gröbner bases: Buchberger's algorithm [5] computes weak Gröbner bases over a PID, and Möller's weak algorithm [19] extends this approach to Noetherian commutative rings. As for strong Gröbner bases, they can be computed using an adapted version of Buchberger's algorithm [16] or Möller's strong algorithm [19]. Algorithms for computing signature Gröbner bases over Euclidean rings have been investigated in [9].

2. Notations

Let R be a Noetherian integral domain, which is assumed to have a unit and be commutative. Let $A = R[x_1, \ldots, x_n]$ be the polynomial ring in n indeterminates $x_1, \ldots, x_n$ over R. A monomial in A is $x^a = x_1^{a_1} \ldots x_n^{a_n}$ where $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$. A term is kx^a, where $k \in R$ and $k \neq 0$. We will denote all the terms in A by $\mathrm{Ter}(A)$ and all the monomials in A by $\mathrm{Mon}(A)$. We use the notation $\mathfrak{a}$ for polynomial ideals in $A = R[x_1, \ldots, x_n]$ and I for ideals in the coefficient ring R.

The notion of monomial order can be directly extended from $\mathbb{K}[x_1, \ldots, x_n]$ 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 $(g_1, \ldots, g_s)$ and $i \in \{1, \ldots, s\}$, we will frequently denote, for brevity, $M(i) = \mathrm{LM}(g_i)$, $C(i) = \mathrm{LC}(g_i)$ and $T(i) = \mathrm{LT}(g_i) = C(i)M(i)$.

3. Gröbner Bases in Polynomial Rings over R

For more details about the contents of this section, one can refer to [1, Chapter 4].

3.1. Computations in R

We assume that our coefficient ring R is *effective* in the following sense.

(1) There are algorithms for arithmetic operations $(+, *, \text{zero test})$ in R.
(2) There is an algorithm LinDecomp:
  - Input: $\{k_1, \ldots, k_s\} \subset R$, $k \in R$
  - Output: TRUE iff $k \in \langle k_1, \ldots, k_s \rangle$ and if yes, $l_1, \ldots, l_s \in R$ such that $k = k_1 l_1 + \cdots + k_s l_s$.
(3) There is an algorithm SatIdeal:
  - Input: $\{k_1, \ldots, k_s\} \subset R$, $k \in R$
  - Output: $\{l_1, \ldots, l_r\} \subset R$ generators of the saturated ideal $\langle k_1, \ldots, k_s \rangle : \langle k \rangle$.

The condition that an algorithm LinDecomp exists is called *linear equations being solvable in R* in [1, Def. 4.1.5].

Example. Euclidean rings are effective, because one can implement those algorithms using GCD computations and Euclidean reductions. For example over $\mathbb{Z}$, LinDecomp$(\{4\}, 12)$ is $(\mathrm{TRUE}, \{3\})$, since 12 is in the ideal $\langle 4 \rangle$ and $12 = 3 \cdot 4$. The output of SatIdeal$(\{4\}, 6)$ is $\{2\}$ since $\langle 4 \rangle : \langle 6 \rangle = \frac{1}{6}(\langle 4 \rangle \cap \langle 6 \rangle) = \frac{1}{6}\langle 12 \rangle = \langle 2 \rangle$.

The ring of multivariate polynomials over a field is also effective, using Gröbner bases and normal forms to perform the same ideal computations.

3.2. Weak Gröbner bases over rings

For reduction in fields it is enough to check if the leading term of f is divisible by the leading monomial of g even though the actual reduction happens with the leading term of g. Clearly, in rings this is not a sufficient condition : $\mathrm{LC}(g)$ may not divide $\mathrm{LC}(f)$ even if $\mathrm{LM}(g)$ divides $\mathrm{LM}(f)$. Requiring that $\mathrm{LT}(g)$ divide $\mathrm{LT}(f)$ leads to the notion of strong Gröbner basis, more details can be found in [1, Sec. 4.5].

Here we are interested in computing weak Gröbner bases, and we recall the main definitions in this section. First, following [19, 1], we expand the definition of reduction to allow for a linear combination of reducers. We define saturated sets [1, Def.4.2.4] (called maximal sets in [19]).

Definition 3.1. Given a tuple of monomials $(x^{a_1}, \ldots, x^{a_s})$, the *saturated set* for a monomial x^b w.r.t. $(x^{a_1}, \ldots, x^{a_s})$ is defined as

$$\mathrm{Sat}(x^b; x^{a_1}, \ldots, x^{a_s}) = \{i \in \{1, \ldots, s\} : x^{a_i} \mid x^b\}.$$

A set $J \subseteq \{1, \ldots, s\}$ is said to be *saturated* w.r.t. $(x^{a_1}, \ldots, x^{a_s})$ if $J = \mathrm{Sat}(M(J); x^{a_1}, \ldots, x^{a_s})$ where $M(J) = \mathrm{lcm}(x^{a_i} : i \in J)$. When clear from the context, we shall omit the list of monomials and write $J_{x^b} = \mathrm{Sat}(x^b)$.

Given a tuple of polynomials $(f_1, \ldots, f_s)$ and a set of indices $J \subset \{1, \ldots, s\}$, we denote by I_J the ideal of R defined as $I_J := \langle \mathrm{LC}(f_i) : i \in J \rangle$ and we define $M(J) = \mathrm{lcm}(\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_s))$.

Definition 3.2. Let $f \in A$. Let $f_1, \ldots, f_s \in A$ and $x^{a_1}, \ldots, x^{a_s} \in \mathrm{Mon}(A)$ be such that $x^{a_i}\mathrm{LM}(f_i) = \mathrm{LM}(f)$ for all i. We say that we can *weakly top reduce* f by $f_1, \ldots, f_s \in A$ if there exist $l_1, \ldots, l_s$ in R such that

$$\mathrm{LT}(f) = \sum_{i=1}^{s} l_i x^{a_i} \mathrm{LT}(f_i).$$

In our setting we will only perform top reductions, so we will simply call them *weak reductions*.

The outcome of the total reduction step is $g = f - \sum_{i=1}^{s} l_i x^{a_i} f_i$ and the f_i's are called the *weak reducers*. A polynomial $f \in A$ is *weakly reducible* if it can be weakly reduced, otherwise it is *weakly reduced*.

If g is the outcome of reducing f, then $\mathrm{LM}(g) \prec \mathrm{LM}(f)$.

Example. Consider the polynomial ring $\mathbb{Z}[x, y]$ with the lex ordering $y \prec x$, and consider the set $F = \{f_1, f_2, f_3, f_4, f_5\}$ in $\mathbb{Z}[x, y]$, with $f_1 = 4xy + x$, $f_2 = 3x^2 + y$, $f_3 = 5x$, $f_4 = 4y^2 + y$, $f_5 = 5y$. Let $f = 2xy + 13y - 5$. We have $\mathrm{LT}(f) = 2xy = (2y)\mathrm{LT}(f_3) - (2)\mathrm{LT}(f_1)$. This implies we can weakly reduce f with f_1, f_3 to get $g = f - (2yf_3 - 2f_1) = 2x + 13y - 5$.

We are now prepared to give the definition of (weak) Gröbner bases for an ideal in A.

Definition 3.3. Let $\mathfrak{a}$ be an ideal in A and $G = \{g_1, \ldots, g_t\}$ be a finite set of nonzero polynomials in $\mathfrak{a}$. The set G is called a *weak Gröbner basis* of $\mathfrak{a}$ in A if it satisfies the following equivalent properties.

1. $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(\mathfrak{a}) \rangle$;
2. for any $f \in \mathfrak{a}$, f is weakly reducible modulo G;
3. for any $f \in A$, $f \in \mathfrak{a}$ if and only if f weakly reduces to 0 modulo G.

Remark 3.4. Even though the notion of weak Gröbner bases is a weaker notion than that of strong Gröbner bases, one can use weak polynomial reductions to test for ideal membership. One can also define normal forms modulo a polynomial ideal. However, for those normal forms to be unique, one needs to perform further reductions on the coefficients, to "coset representative form", and one needs to perform reductions on non-leading coefficients as well [1, Th. 4.3.3]. Finally, note that, over a PID, one can easily recover a strong basis from a weak one [19, Th. 4].

3.3. Möller's algorithm for general rings

In this section, we present Möller's (weak) algorithm [19] for computing Gröbner bases over rings satisfying the conditions of Sec. 3.1. This algorithm is analogous to Buchberger's algorithm for rings, where the polynomial reduction is as defined above and S-polynomials are replaced with linear combinations of several (possibly more than 2) polynomials, defined in the following sense.

Consider a set $\{g_1, \ldots, g_t\}$ of polynomials. For $i \in \{1, \ldots, t\}$, let $M(i) = \mathrm{LM}(g_i)$, $C(i) = \mathrm{LC}(g_i)$ and $T(i) = \mathrm{LT}(g_i)$. Let J be a saturated subset of $\{1, \ldots, t\}$ w.r.t. $\{M(1), \ldots, M(t)\}$. Recall that $M(J) = \mathrm{lcm}(M(j) : j \in J)$. By definition, for all $j \in J$, $M(j)$ divides $M(J)$ and J is maximal with this property.

Let $s \in J$ and $J^* = J \setminus \{s\}$. Similar to the idea behind S-polynomials, we want to eliminate the leading term $C(s)M(J)$ of $\frac{M(J)}{M(s)}g_s$. This can only be done if we multiply $\frac{M(J)}{M(s)}g_s$ by an element of the saturated ideal $\langle C(i) : i \in J, i \neq s \rangle : \langle C(s) \rangle$. We want to consider all such multipliers, so we need to consider generators of this saturated ideal.

Let c be such a generator, by definition $cC(s) \in \langle C(i) : i \in J, i \neq s \rangle$ so there exists $(b_i)_{i \in J^*} \in R$ such that $cC(s) = \sum_{i \in J^*} b_i C(i)$. The (weak) S-polynomial associated with J, s and c, for some suitable (b_i), is defined as

$$\text{S-Pol}((g_i)_{i \in J^*}; g_s; c) = c\frac{M(J)}{M(s)}g_s - \sum_{i \in J^*} b_i \frac{M(J)}{M(i)}g_i.$$

If the ring R is a PID, the saturated ideal $\langle C(i) : i \in J, i \neq s \rangle : \langle C(s) \rangle$ admits a unique generator c and we define

$$C(J; s) = \mathrm{LC}(cg_s) = cC(s) = \mathrm{lcm}(\gcd(\{C(j) : j \in J^*\}), C(s))$$
$$T(J; s) = \mathrm{LT}(cg_s) = C(J; s)M(J).$$

Then the S-polynomial associated with J, s, c, for some suitable (b_i), can be written in the following form

$$\text{S-Pol}((g_i)_{i \in J^*}; g_s) = \frac{T(J; s)}{T(s)} g_s - \sum_{i \in J^*} b_i \frac{M(J)}{M(i)} g_i.$$

Using this definition of S-polynomials, we recall Möller's algorithm (Algo. 1) for computing a Gröbner basis of an ideal given by a set of generators over R. The correctness and termination of this algorithm are shown in [1, Th. 4.2.8 and Th. 4.2.9].

Algorithm 1 Möller's algorithm [1, Algo. 4.2.2], [19]

Input $F = \{f_1, \dots, f_m\} \subseteq A \setminus \{0\}$, $\prec$ a monomial order on A
Output $G = \{g_1, \dots, g_t\}$, a Gröbner basis of $\langle F \rangle$

$G \leftarrow F, \sigma \leftarrow 1, s \leftarrow m$
while $\sigma \neq s$ **do**
   $S \leftarrow \big\{\text{subsets of } \{1, \dots, \sigma\} \text{ saturated w.r.t. } \text{LM}(g_1), \dots, \text{LM}(g_\sigma) \text{ which contain } \sigma \big\}$
   for each $J \in S$ **do**
      $M(J) \leftarrow \text{lcm}(\text{LM}(g_j) : j \in J)$
      $J^* \leftarrow J \setminus \{\sigma\}$
      $\{c_1, \dots, c_\mu\} \leftarrow \text{SatIdeal}(\{\text{LC}(g_j) : j \in J^*\}, \text{LC}(g_\sigma))$
          // $\langle c_1, \dots, c_\mu \rangle = \langle C(j) : j \in J^* \rangle : \langle C(\sigma) \rangle$
      for $i \in \{1, \dots, \mu\}$ **do**   // For PIDs, $\mu = 1$
         $p \leftarrow \text{S-Pol}((g_j)_{j \in J^*}; g_\sigma; c_i)$
         $r \leftarrow \text{Reduce}(p, G)$
         if $r \neq 0$ **then**
            $g_{s+1} \leftarrow r, G \leftarrow G \cup \{g_{s+1}\}, s \leftarrow s + 1$
   $\sigma \leftarrow \sigma + 1$
return G

Algorithm 2 Reduce (Def. 3.2)

Input $G = \{g_1, \dots, g_s\} \subseteq A \setminus \{0\}$, $\prec$ a monomial order on A
Output r result of reducing p modulo G

reducible $\leftarrow$ TRUE, $r \leftarrow p$
while *reducible* **is** TRUE **do**
   $J \leftarrow \{j \in \{1, \dots, s\} : \text{LM}(g_j) \mid \text{LM}(r)\}$
   reducible, $(k_j)_{j \in J} \leftarrow \text{LinDecomp}(\{\text{LC}(g_j) : j \in J\}, \text{LC}(r))$
      // If *reducible* is TRUE, then $\text{LC}(r) = \sum_{j \in J} k_j \text{LC}(g_j)$
   if *reducible* **then**
      $r \leftarrow r - \sum_{j \in J} k_j \frac{\text{LM}(r)}{\text{LM}(g_j)} g_j$
return r

---

4. Signatures in A^m

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 $k \in R \setminus \{0\}$, $x^a \in \text{Mon}(A)$, $i \in \{1, \dots, m\}$. 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 $f_1, \ldots, f_m \in A$, elements of A^m encode elements of the ideal $\langle f_1, \ldots, f_m \rangle$ through the A-module homomorphism $\bar{\cdot} : A^m \to A$, defined by setting $\bar{\mathbf{e}}_i = f_i$ and extending linearly to A^m. In particular, $\overline{\sum_{i=1}^m p_i \mathbf{e}_i} = \sum_{i=1}^m p_i f_i$.

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 $\mathfrak{s}(\mathbf{p}) = \mathrm{LT}(p_i)\mathbf{e}_i$ where i is such that $p_{i+1} = \ldots = p_m = 0$ 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 [9], where both signatures and coefficients are ordered.

Given a tuple $(\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s)$ of module elements in A^m and $i, j \in \{1, \ldots, s\}$, we shall frequently denote $S(i) = \mathfrak{s}(\boldsymbol{\alpha}_i)$ for brevity.

In order to keep track of signatures we modify Def. 3.2 to introduce the notion of $\mathfrak{s}$-reduction.

Definition 4.1. Let $\mathbf{p} \in A^m$. We say that we can *signature-reduce* (or $\mathfrak{s}$-*reduce*) $\mathbf{p}$ by $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_s \in A^m$ if we can reduce $\bar{\mathbf{p}}$ by $\bar{\boldsymbol{\beta}}_1, \ldots, \bar{\boldsymbol{\beta}}_s$ (in the sense of Def. 3.2) and $\mathfrak{s}(x^{a_i}\boldsymbol{\beta}_i) \preceq \mathfrak{s}(\mathbf{p})$ for all $i = 1, \ldots, s$, where $x^{a_i} = \frac{\mathrm{LM}(\bar{\mathbf{p}})}{\mathrm{LM}(\bar{\boldsymbol{\beta}}_i)}$. We can define similarly $\mathfrak{s}$-reduced module elements.

If $\mathfrak{s}(x^{a_i}\boldsymbol{\beta}_i) \simeq \mathfrak{s}(\mathbf{p})$ for some i in the above $\mathfrak{s}$-reduction, then it is called a *singular* $\mathfrak{s}$-reduction step. Otherwise it is called a *regular* $\mathfrak{s}$-reduction step.

If $\mathfrak{s}(x^{a_i}\boldsymbol{\beta}_i) \simeq \mathfrak{s}(\mathbf{p})$ for exactly one i and it is actually an equality $\mathfrak{s}(l_i x^{a_i}\boldsymbol{\beta}_i) = \mathfrak{s}(\mathbf{p})$, it is called a *1-singular* $\mathfrak{s}$-reduction step.

Remark 4.2. For simplicity, we only carry out weak top reductions, and in particular all $\mathfrak{s}$-reductions are weak top $\mathfrak{s}$-reductions. But performing regular $\mathfrak{s}$-reduction to eliminate trailing terms does not affect the correctness of the algorithm.

Just like $\mathfrak{s}$-reduction over fields, one can interpret $\mathfrak{s}$-reduction as polynomial reduction with an extra condition on the signature of the reducers. The difference with fields is that in $R[x_1, \ldots, x_n]$ polynomial reduction is defined differently from the classic polynomial reduction. Additionally, in the case of fields, all singular $\mathfrak{s}$-reductions are 1-singular.

The outcome $\mathbf{q}$ of $\mathfrak{s}$-reducing $\mathbf{p}$ is such that $\mathrm{LT}(\bar{\mathbf{q}}) \prec \mathrm{LT}(\bar{\mathbf{p}})$ and $\mathfrak{s}(\mathbf{q}) \preceq \mathfrak{s}(\mathbf{p})$. If $\mathbf{q}$ is the result of a regular $\mathfrak{s}$-reduction, then $\mathfrak{s}(\mathbf{q}) = \mathfrak{s}(\mathbf{p})$. In signature-based algorithms, in order to keep track of the signatures of the basis elements, we only allow regular $\mathfrak{s}$-reductions. Later, we will also prove that elements which are 1-singular $\mathfrak{s}$-reducible can be discarded.

Remark 4.3. In [9, Ex. 2], a signature drop appears when $\mathfrak{s}$-reducing an element of signature $6y\mathbf{e}_2$ with an element of signature $y\mathbf{e}_2$ causing the signature to "drop" to $5y\mathbf{e}_2$. With our definition, since we only compare the module monomial part of the signatures, this is a (forbidden) singular $\mathfrak{s}$-reduction.

Definition 4.4. Let $\mathfrak{a} = \langle f_1, \ldots, f_m \rangle$ be an ideal in A. A finite subset $\mathcal{G}$ of A^m is a (weak) *signature Gröbner basis* (or $\mathfrak{s}$-GB for short) of $\mathfrak{a}$ if all $\mathbf{u} \in A^m$ $\mathfrak{s}$-reduce to zero mod $\mathcal{G}$.

Given a signature $\mathbf{T}$, we say that $\mathcal{G}$ is a (partial) signature Gröbner basis up to $\mathbf{T}$ if all $\mathbf{u} \in A^m$ with signature $\prec \mathbf{T}$ $\mathfrak{s}$-reduce to 0 mod $\mathcal{G}$.

Using this definition, we can give the following characterization of 1-singular reducibility, which allows for an easy algorithmic test.

Lemma 4.5 (Characterization of 1-singular $\mathfrak{s}$-reducibility). *Let* $\mathcal{G} = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s\} \subset A^m$ *and* $\mathbf{p} \in A^m$ *such that* $\mathcal{G}$ *is a signature Gröbner basis up to signature* $\mathfrak{s}(\mathbf{p})$. *Then* $\mathbf{p}$ *is 1-singular* $\mathfrak{s}$-*reducible if and only if there exist* $j \in \{1, \ldots, s\}$ *and* $k \in R$ *and a monomial* x^a *in* A *such that* $\mathrm{LM}(x^a\bar{\boldsymbol{\alpha}}_j) = \mathrm{LM}(\bar{\mathbf{p}})$ *and* $kx^a\mathfrak{s}(\boldsymbol{\alpha}_j) = \mathfrak{s}(\mathbf{p})$.

Proof. If **p** is 1-singular $\mathfrak{s}$-reducible, then such j, k and x^a exist by definition. Conversely, given such j, k and x^a, if $kx^a\mathrm{LT}(\overline{\boldsymbol{\alpha}}_j) = \mathrm{LT}(\overline{\mathbf{p}})$, then **p** is 1-singular $\mathfrak{s}$-reducible. If not, then $\mathrm{LM}(\overline{\mathbf{p}} - kx^a\boldsymbol{\alpha}_j) = \mathrm{LM}(\overline{\mathbf{p}})$. Furthermore, $\mathfrak{s}(\mathbf{p} - kx^a\boldsymbol{\alpha}_j) \prec \mathfrak{s}(\mathbf{p})$, so $\mathbf{p} - kx^a\boldsymbol{\alpha}_j$ $\mathfrak{s}$-reduces to 0. In particular, there exist $(\mu_i)_{i\in\{1,\dots,s\}}$ terms in A such that for all i with $\mu_i \neq 0$, $\mathrm{LM}(\mu_i\overline{\boldsymbol{\alpha}}_i) = \mathrm{LM}(\overline{\mathbf{p}} - kx^a\overline{\boldsymbol{\alpha}}_j)$, $\mathrm{LT}(\overline{\mathbf{p}} - kx^a\overline{\boldsymbol{\alpha}}_j) = \sum_{i=1}^{s} \mu_i\mathrm{LT}(\overline{\boldsymbol{\alpha}}_i)$ and $\mu_i\mathfrak{s}(\boldsymbol{\alpha}_i) \preceq \mathfrak{s}(\mathbf{p} - kx^a\boldsymbol{\alpha}_j) \prec \mathfrak{s}(\mathbf{p})$. So putting together the two $\mathfrak{s}$-reductions, we obtain that

$$\mathrm{LT}(\overline{\mathbf{p}}) = kx^a\mathrm{LT}(\overline{\boldsymbol{\alpha}}_j) + \sum_{i=1}^{s} \mu_i\mathrm{LT}(\overline{\boldsymbol{\alpha}}_i)$$

and this is a 1-singular $\mathfrak{s}$-reduction of **p**. $\qquad\square$

We now define (weak) *semi-strong signature Gröbner bases*, which form a subclass of weak $\mathfrak{s}$-Gröbner bases. In the case of rings, it is easier to compute them than to directly compute weak $\mathfrak{s}$-Gröbner bases.

Definition 4.6. Let $\mathfrak{a} = \langle f_1, \dots, f_m \rangle$ be an ideal in A. A finite subset $\mathcal{G}$ of A^m is a *semi-strong signature Gröbner basis* (or s-s $\mathfrak{s}$-GB for short) of $\mathfrak{a}$ if, for all $\mathbf{u} \in A^m$,

- either **u** is (weakly) regular $\mathfrak{s}$-reducible modulo $\mathcal{G}$;
- or **u** is 1-singular $\mathfrak{s}$-reducible modulo $\mathcal{G}$;
- or $\overline{\mathbf{u}} = 0$.

Given a signature **T**, *semi-strong signature Gröbner bases up to* **T** are defined similarly by only considering module elements with signature $\prec$ **T**.

Lemma 4.7 ([6, Lem. 4.6]). *Let $\mathfrak{a} = \langle f_1, \dots, f_m \rangle$ be an ideal in A and let $\mathcal{G} \subset A^m$. Then*

1. *If $\mathcal{G}$ is a s-s $\mathfrak{s}$-GB of $\mathfrak{a}$, then $\mathcal{G}$ is a $\mathfrak{s}$-GB of $\mathfrak{a}$.*
2. *If $\mathcal{G}$ is a $\mathfrak{s}$-GB of $\mathfrak{a}$, then $\{\overline{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in \mathcal{G}\}$ is a Gröbner basis of $\mathfrak{a}$.*

Proof. The definition of a semi-strong Gröbner basis implies that all $\mathbf{u} \in A^m$ with $\overline{\mathbf{u}} \neq 0$ are $\mathfrak{s}$-reducible modulo $\mathcal{G}$, and so such $\mathfrak{s}$-reductions form a chain which can only terminate at 0.

The proof that a signature Gröbner basis is a Gröbner basis is classical [6, Lem. 4.1]. $\qquad\square$

In order to compute signature Gröbner bases, similar to the case of fields, we will restrict the computations to regular S-polynomials. For this purpose, we first introduce the signature of a set of indices, and regular sets.

Definition 4.8. Let $\mathcal{G} = (\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_t)$ be a tuple of module elements in A^m and a set $J \subseteq \{1, \dots, t\}$. For $i \in \{1, \dots, t\}$, let $M(i) = \mathrm{LM}(\overline{\boldsymbol{\alpha}}_i)$, and $S(i) = \mathfrak{s}(\boldsymbol{\alpha}_i)$. The *presignature* of J is defined as

$$S_J = \max_{s \in J} \left\{ \frac{M(J)}{M(s)} S(s) \right\}.$$

We say that J is a *regular set* if there exists exactly one $s \in J$ such that $S_J \simeq \frac{M(J)}{M(s)}\mathfrak{s}(\boldsymbol{\alpha}_s)$. The index s is called the *signature index* of J. We say that J is a *regular saturated set* if $J \setminus \{s\}$ contains all j such that $M(j) \mid M(J)$ and $\frac{M(J)}{M(j)}S(j) \prec S_J$.

Note that given a regular set J, one can always compute a regular saturated set J' containing J, by adding those indices j such that $M(j) \mid M(J)$ and $\frac{M(J)}{M(j)}S(j) \prec S_J$.

Definition 4.9. Let $(\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_t)$ be a tuple of module elements in A^m. For $i \in \{1, \dots, t\}$, let $M(i) = \mathrm{LM}(\overline{\boldsymbol{\alpha}}_i)$, $C(i) = \mathrm{LC}(\overline{\boldsymbol{\alpha}}_i)$ and $S(i) = \mathfrak{s}(\boldsymbol{\alpha}_i)$. Let $J \subset \{1, \dots, t\}$ be a regular saturated set with signature index s, and let $J^* = J \setminus \{s\}$. Let c be an element of a family of generators of $\langle C(j) : j \in J^* \rangle : \langle C(s) \rangle$. Let $(b_j)_{j \in J^*}$ be a tuple of elements of R such that $cC(s) = \sum_{j \in J^*} b_j C(j)$. Then the (weak) S-polynomial associated with J and c is defined as

$$\mathrm{S\text{-}Pol}((g_j)_{j \in J}; c) = c\frac{M(J)}{M(s)}\boldsymbol{\alpha}_s - \sum_{j \in J^*} b_j \frac{M(J)}{M(j)}\boldsymbol{\alpha}_j.$$

Its signature is

$$S(J;c) = \mathfrak{s}(\text{S-Pol}((g_j)_{j \in J};c)) = c S_J = c \frac{M(J)}{M(s)} S(s).$$

Remark 4.10. When dealing with regular saturated sets, unlike in Sec. 3.2, we do not need to specify which $s \in J$ is singled out when computing the S-polynomial: the only possible s is the signature index of J.

Remark 4.11. If the coefficient ring is a PID, the ideal $\langle C(j) : j \in J^* \rangle : \langle C(s) \rangle$ is principal, and c is uniquely determined up to an invertible factor. As such, it can be omitted, and in that case we shall simply write S-Pol(J) for the S-polynomial, and $S(J)$ for its signature. The signature can then be written as $S(J) = \frac{C(J)}{C(s)} S_J = \frac{C(J)}{C(s)} \frac{M(J)}{M(s)} S(s)$.

5. Adding signatures to Möller's weak algorithm

Recall that all $\mathfrak{s}$-reductions are weak top $\mathfrak{s}$-reductions. In this section, all S-polynomials are weak S-polynomials.

5.1. Algorithms

Algorithm SigMöller (Algo. 3) is a signature-based version of Möller's algorithm which, given an ideal $\mathfrak{a}$ in $R[x_1, \dots, x_n]$ where R is a PID, computes a signature Gröbner basis of $\mathfrak{a}$.

   The algorithm proceeds by maintaining a list of regular saturated sets $\mathcal{P}$ and computing weak S-polynomials obtained from these saturated sets. At each step, it selects the next regular saturated set $J \in \mathcal{P}$ such that J has minimal presignature amongst elements of $\mathcal{P}$. This ensures that the algorithm computes new elements for the signature Gröbner basis with nondecreasing signatures (Prop. 5.2).

   The algorithm then regular $\mathfrak{s}$-reduces these S-polynomials w.r.t. the previous elements, and adds to the basis those which are not equal to 0 and are not 1-singular $\mathfrak{s}$-reducible. Signature-based Gröbner basis algorithms over fields typically discard all new elements which are singular $\mathfrak{s}$-reducible, but this may be too restrictive for rings. On the other hand, the proof of Lem. 5.4 justifies that 1-singular $\mathfrak{s}$-reducible module elements can be safely discarded in the computations. The correctness of the criterion for 1-singular $\mathfrak{s}$-reducibility (Algo. 4) was justified in Lem. 4.5. The correctness and termination of Algorithm SigMöller are proved in Th. 5.5 and Th. 5.6 respectively.

   Due to space constraints, the subroutine RegularReduce is not explicitly written. It implements regular $\mathfrak{s}$-reduction of a module element $\mathbf{p}$ w.r.t. a set of module elements $\{\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_s\}$. It is a straightforward transposition of Reduce (Algo. 2), with the additional condition that we only consider as reducers of $\mathbf{r}$ those $\boldsymbol{\alpha}_j$ with $\text{LM}(\overline{\boldsymbol{\alpha}}_j) \mid \text{LM}(\overline{\mathbf{r}})$ and $\frac{\text{LM}(\overline{\mathbf{r}})}{\text{LM}(\overline{\boldsymbol{\alpha}}_j)} \mathfrak{s}(\boldsymbol{\alpha}_j) \prec \mathfrak{s}(\mathbf{r})$.

Remark 5.1. Note that the algorithms, as presented, perform computations on module elements. However, for practical implementations, this represents a significant overhead. On the other hand, for any module element $\boldsymbol{\alpha}$, we only need its polynomial value $\overline{\boldsymbol{\alpha}}$ and its signature $\mathfrak{s}(\boldsymbol{\alpha})$. Hence the algorithm only needs to keep track of the signatures of elements, which is made possible by the restriction to regular S-polynomials and regular $\mathfrak{s}$-reductions.

Example. An example run of Algorithm 3 is provided in Appendix A.

5.2. Proof of correctness

In this section we prove the correctness of the algorithms presented in Sec. 5.1. The first result states that Algorithm SigMöller computes elements of the signature Gröbner basis in nondecreasing order on their signatures.

Proposition 5.2. *Let* $(\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_t)$ *be the value of* $\mathcal{G}$ *at any point in the course of Algorithm SigMöller. Then* $\mathfrak{s}(\boldsymbol{\alpha}_1) \preceq \mathfrak{s}(\boldsymbol{\alpha}_2) \preceq \cdots \preceq \mathfrak{s}(\boldsymbol{\alpha}_t)$.

Algorithm 3 Signature-based Möller's algorithm (SigMöller)

Input $F = \{f_1, \ldots, f_m\} \subseteq A \setminus \{0\}$, $\prec$ a monomial order on A
Output $\mathcal{G} = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t\}$ a semi-strong signature-Gröbner basis of $\langle F \rangle$

$\mathcal{G} \leftarrow \emptyset, \sigma \leftarrow 0$
for $i \in \{1, \ldots, m\}$ **do**
    $\mathbf{e}'_i \leftarrow \mathsf{RegularReduce}(\mathbf{e}_i, \mathcal{G})$
    if $\overline{\mathbf{e}}'_i \neq 0$ **then**
        $\mathcal{G} = \mathcal{G} \cup \{\mathbf{e}'_i\}, s \leftarrow |\mathcal{G}|$ // $\boldsymbol{\alpha}_s = \mathbf{e}'_i$
        $\mathcal{P} \leftarrow \{\text{Regular saturated sets of } \{1, \ldots, s\} \text{ containing } s\}$
        while $\mathcal{P} \neq \emptyset$ **do**
            Pick and remove from $\mathcal{P}$ a regular saturated set with minimal presignature S_J
            $M(J) \leftarrow \mathrm{lcm}(\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j) : j \in J)$
            $\tau \leftarrow$ signature index of J
            $J^* \leftarrow J \setminus \{\tau\}$
            $\{c_1, \ldots, c_\mu\} \leftarrow \mathsf{SatIdeal}(\{\mathrm{LC}(\overline{\boldsymbol{\alpha}}_j) : j \in J^*\}, \mathrm{LC}(\overline{\boldsymbol{\alpha}}_\tau))$
            for $i \in \{1, \ldots, \mu\}$ **do**   // For PIDs, $\mu = 1$
                $p \leftarrow \text{S-Pol}((g_j)_{j \in J}; c_i)$
                $\mathbf{r} \leftarrow \mathsf{RegularReduce}(\mathbf{p}, \mathcal{G})$
                if $\mathbf{r} \neq 0$ **and not** 1-$\mathsf{SingularReducible}(\mathbf{r}, \mathcal{G})$ **then**
                    $\boldsymbol{\alpha}_{s+1} \leftarrow \mathbf{r}$ // $\boldsymbol{\alpha}_{s+1}$ has signature $S(J) = c_i S_J$
                    $\mathcal{G} \leftarrow \mathcal{G} \cup \{\boldsymbol{\alpha}_{s+1}\}$
                    $\mathcal{P} \leftarrow \mathcal{P} \cup \{\text{Regular saturated sets of } \{1, \ldots, s+1\} \text{ containing } s+1\}$
                    $s \leftarrow s + 1$
return $\mathcal{G}$

Proof. Assume that this is not the case, and let i be the smallest index such that $\mathfrak{s}(\boldsymbol{\alpha}_i) \succ \mathfrak{s}(\boldsymbol{\alpha}_{i+1})$. Let J_i (resp. J_{i+1}) be the saturated set used to compute $\boldsymbol{\alpha}_i$ (resp. $\boldsymbol{\alpha}_{i+1}$). Note that $\mathfrak{s}(\boldsymbol{\alpha}_i) \simeq S(J_i)$ and $\mathfrak{s}(\boldsymbol{\alpha}_{i+1}) \simeq S(J_{i+1})$.

If $i \notin J_{i+1}$, then J_{i+1} was already in the queue $\mathcal{P}$ when J_i was selected, and so, by the selection criterion in the algorithm, $S(J_i) \preceq S(J_{i+1})$.

If $i \in J_{i+1}$, then $S(J_{i+1}) \succeq \frac{x^{J_{i+1}}}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_i)} \mathfrak{s}(\boldsymbol{\alpha}_i) \succeq \mathfrak{s}(\boldsymbol{\alpha}_i)$. $\qquad\square$

The following useful lemma gives consequences of the fact that two regular $\mathfrak{s}$-reduced elements share the same signature.

Lemma 5.3. *Let $\mathcal{G} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s)$ be a signature Gröbner basis up to signature $\mathbf{L}$. Let $\mathbf{p}, \mathbf{q} \in A^m$ such that $\mathfrak{s}(\mathbf{p}) = \mathfrak{s}(\mathbf{q}) = \mathbf{L}$, and $\mathbf{p}$ and $\mathbf{q}$ are regular $\mathfrak{s}$-reduced. Then $\mathrm{LM}(\overline{\mathbf{p}}) = \mathrm{LM}(\overline{\mathbf{q}})$ and either $\mathrm{LT}(\overline{\mathbf{p}}) = \mathrm{LT}(\overline{\mathbf{q}})$, or $\mathrm{LC}(\overline{\mathbf{p}} - \overline{\mathbf{q}})$ lies in the ideal*

$$C := \left\langle \mathrm{LC}(\overline{\boldsymbol{\alpha}}_j) : \mathrm{LM}(\overline{\boldsymbol{\alpha}}_j) \mid m \text{ and } \frac{m}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j)} \mathfrak{s}(\boldsymbol{\alpha}_j) \simeq \mathfrak{s}(\mathbf{p}) \right\rangle.$$

Proof. Let $\mathbf{r} = \mathbf{p} - \mathbf{q}$. Since $\mathfrak{s}(\mathbf{p}) = \mathfrak{s}(\mathbf{q})$, we have $\mathfrak{s}(\mathbf{r}) \prec \mathfrak{s}(\mathbf{p}) = \mathbf{L}$, and so $\mathbf{r}$ $\mathfrak{s}$-reduces to 0 modulo $\mathcal{G}$. Assume first that $\mathrm{LM}(\overline{\mathbf{p}}) \neq \mathrm{LM}(\overline{\mathbf{q}})$, then w.l.o.g. we may assume that $\mathrm{LM}(\overline{\mathbf{p}}) \succ \mathrm{LM}(\overline{\mathbf{q}})$, so $\mathrm{LM}(\overline{\mathbf{r}}) = \mathrm{LM}(\overline{\mathbf{p}})$. Since $\mathbf{r}$ is regular $\mathfrak{s}$-reducible, $\mathbf{p}$ is $\mathfrak{s}$-reducible. This is a contradiction with the assumption that $\mathbf{p}$ is $\mathfrak{s}$-reduced.

So $\mathrm{LM}(\overline{\mathbf{p}}) = \mathrm{LM}(\overline{\mathbf{q}}) =: m$. If $\mathrm{LT}(\overline{\mathbf{p}}) \neq \mathrm{LT}(\overline{\mathbf{q}})$, C is the ideal of leading coefficients of polynomials which can eliminate m, and since $\mathbf{r}$ is $\mathfrak{s}$-reducible, $\mathrm{LC}(\overline{\mathbf{p}}) - \mathrm{LC}(\overline{\mathbf{q}}) \in C$. $\qquad\square$

We now prove the correctness of Algorithm SigMöller. The proof follows the structure of the proof in the case of fields [22], and adapts it to Möller's algorithm over PIDs. In particular, it takes into account weak $\mathfrak{s}$-reductions instead of classical $\mathfrak{s}$-reductions. The algorithm ensures that all regular

---

Algorithm 4 Test of 1-singular $\mathfrak{s}$-reducibility modulo a partial $\mathfrak{s}$-GB (1-SingularReducible)

Input $\mathcal{G} = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s\} \subset A^m$ and $\mathbf{p} \in A^m$ such that $\mathbf{p}$ is regular $\mathfrak{s}$-reduced w.r.t. $\mathcal{G}$ and $\mathcal{G}$ is a signature Gröbner basis up to $\mathfrak{s}(\mathbf{p})$
Output TRUE iff $\mathbf{p}$ is 1-singular $\mathfrak{s}$-reducible modulo $\mathcal{G}$

$$J \leftarrow \left\{ j \in \{1, \ldots, s\} \, : \, \mathrm{LM}(\overline{\boldsymbol{\alpha}}_j) \mid \mathrm{LM}(\overline{\mathbf{p}}) \text{ and } \frac{\mathrm{LM}(\overline{\mathbf{p}})}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j)} \mathfrak{s}(\boldsymbol{\alpha}_j) \preceq \mathfrak{s}(\mathbf{p}) \right\}$$

return $\exists j \in J, \exists k_j \in R, k_j \frac{\mathrm{LM}(\overline{\mathbf{p}})}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j)} \mathfrak{s}(\boldsymbol{\alpha}_j) = \mathfrak{s}(\mathbf{p})$

S-polynomials up to a given signature $\mathbf{T}$ $\mathfrak{s}$-reduce to 0, and proving the correctness of the algorithm requires proving that this implies that all module elements with signature $\prec \mathbf{T}$ $\mathfrak{s}$-reduce to 0.

The key lemma of the proof is the following.

Lemma 5.4. *Let $\mathcal{G} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s) \subseteq A^m$. Let $\mathbf{u} \in A^m \setminus \{0\}$ be $\mathfrak{s}$-reduced such that $\overline{\mathbf{u}} \neq 0$. Assume that $\mathcal{G}$ is a s-s $\mathfrak{s}$-GB basis up to signature $\mathfrak{s}(\mathbf{u})$. Then there exists an S-polynomial $\mathbf{p}$ w.r.t. $\mathcal{G}$, such that:*

1. *the signature of $\mathbf{p}$ divides the signature of $\mathbf{u}$: $kx^a \mathfrak{s}(\mathbf{p}) = \mathfrak{s}(\mathbf{u})$ with $k \in R$ and $x^a \in \mathrm{Mon}(A)$;*
2. *if $\mathbf{p}'$ is the result of regular $\mathfrak{s}$-reducing $\mathbf{p}$ w.r.t. $\mathcal{G}$, then $kx^a \mathbf{p}'$ is regular $\mathfrak{s}$-reduced.*

Proof. The proof is in two steps: first, we construct a S-polynomial $\mathbf{p}$ whose signature divides $\mathfrak{s}(\mathbf{u})$, and then, starting from $\mathbf{p}$, we show that there exists an S-polynomial satisfying the conditions of the lemma.

In the remainder of the proof, for $i \in \{1, \ldots, s\}$, let $M(i) = \mathrm{LM}(\overline{\boldsymbol{\alpha}}_i)$, $C(i) = \mathrm{LC}(\overline{\boldsymbol{\alpha}}_i)$, $T(i) = \mathrm{LT}(\overline{\boldsymbol{\alpha}}_i)$ and $S(i) = \mathfrak{s}(\boldsymbol{\alpha}_i)$.

Existence of a S-polynomial satisfying 1. For the first step, let $\mathfrak{s}(\mathbf{u})$ be $lx^b \mathbf{e}_i$ for some $l \in R$, x^b a monomial and $\mathbf{e}_i$ a basis vector. Let $\mathbf{e}'_i$ be the result of regular $\mathfrak{s}$-reducing $\mathbf{e}_i$. If $\overline{\mathbf{e}}'_i = 0$, then $\mathbf{u}$ regular $\mathfrak{s}$-reduces to 0, which is a contradiction since we assumed $\mathbf{u}$ to be $\mathfrak{s}$-reduced and $\overline{\mathbf{u}} \neq 0$. Let $\mathbf{L} = lx^b \mathbf{e}'_i$, it has signature $lx^b \mathbf{e}_i$. Then $\mathbf{u} - \mathbf{L}$ has a smaller signature than $\mathbf{u}$, so it $\mathfrak{s}$-reduces to zero and in particular it is $\mathfrak{s}$-reducible. Also, $\mathbf{L}$ is $\mathfrak{s}$-reducible by $\mathbf{e}'_i$. Consider the sum $(\mathbf{u} - \mathbf{L}) + \mathbf{L} = \mathbf{u}$. It is not $\mathfrak{s}$-reducible, which implies that $\mathrm{LT}(\overline{\mathbf{u} - \mathbf{L}}) = -\mathrm{LT}(\overline{\mathbf{L}})$.

Let $J_{\mathrm{LM}(\overline{\mathbf{L}})}$ be the maximal regular saturated set J with $M(J) \mid \mathrm{LM}(\overline{\mathbf{L}})$. Since $\mathbf{u} - \mathbf{L}$ $\mathfrak{s}$-reduces to zero, there exists $(m_j)_{j \in J_{\mathrm{LM}(\overline{\mathbf{L}})}}$ monomials in A, and $(k_j)_{j \in J_{\mathrm{LM}(\overline{\mathbf{L}})}}$ coefficients in R such that

$$\mathrm{LT}(\overline{\mathbf{u}} - \overline{\mathbf{L}}) = \sum_{j \in J_{\mathrm{LM}(\overline{\mathbf{L}})}} k_j m_j T(j) \tag{5.1}$$

with $m_j M(j) = \mathrm{LM}(\overline{\mathbf{u}} - \overline{\mathbf{L}})$ and $\mathfrak{s}(k_j m_j \boldsymbol{\alpha}_j) = k_j m_j S(j) \preceq \mathfrak{s}(\mathbf{u} - \mathbf{L}) \prec \mathfrak{s}(\mathbf{u})$ for all i such that $k_j \neq 0$. Let σ be the index of $\mathbf{e}'_i$ in $\mathcal{G}$, that is $\boldsymbol{\alpha}_\sigma = \mathbf{e}'_i$. Consider the set $J' = \{j \, : \, m_j \neq 0\} \cup \{\sigma\} \subseteq J_{\mathrm{LM}(\overline{\mathbf{L}})}$, it is regular by construction.

Let J be a regular saturated set containing J'. Then, since for all $j \in J'$, $M(j) \mid \mathrm{LM}(\overline{\mathbf{L}}) = x^b M(\sigma)$, $M(J) = \mathrm{lcm}\left\{ M(j) : j \in J' \right\} \mid x^b M(\sigma)$. Furthermore, looking at the leading coefficients in Eq. (5.1), we have

$$l \, C(\sigma) = - \sum_{j \in J'} k_j C(j)$$

and so $l \in \langle C(j) \, : \, j \in J, j \neq \sigma \rangle : \langle C(\sigma) \rangle$. Since R is a PID, this ideal is principal. Let b_J be its generator, then $b_J \mid l$. Let $\mathbf{p}$ be the S-polynomial corresponding to J and b_J. It is regular by construction since J is a regular saturated set, and its signature is $\mathfrak{s}(\mathbf{p}) = b_J \frac{M(J)}{M(\sigma)} S(\sigma) = b_J \frac{M(J)}{\mathrm{LM}(\overline{\mathbf{e}'_i})} \mathbf{e}_i$.

Since b_J divides l and $M(J)$ divides $x^b M(\sigma)$, $\mathfrak{s}(\mathbf{p})$ divides $lx^b s\mathbf{e}'_i = \mathfrak{s}(\mathbf{L}) = \mathfrak{s}(\mathbf{u})$.

Existence of a S-polynomial satisfying 1. and 2. Let $\mathbf{p}$ be an S-polynomial whose signature divides $\mathfrak{s}(\mathbf{u})$, and let $\mathbf{p}'$ be the regular $\mathfrak{s}$-reduced form of $\mathbf{p}$. Write $\mathfrak{s}(\mathbf{u}) = \mathfrak{s}(kx^a\mathbf{p})$, where $k \in R$ and x^a is a monomial.

We can assume that $kx^a\mathbf{p}'$ is regular $\mathfrak{s}$-reducible or else we are done. We then construct an S-polynomial $\mathbf{q}$ such that $\mathfrak{s}(lx^b\mathbf{q}) = \mathfrak{s}(\mathbf{u})$ and $\mathrm{LM}(\overline{kx^a\mathbf{p}}) > \mathrm{LM}(\overline{lx^b\mathbf{q}})$. If $lx^b\mathbf{q}'$, where $\mathbf{q}'$ is obtained by regular $\mathfrak{s}$-reducing $\mathbf{q}$, is not regular $\mathfrak{s}$-reducible then we are done. Otherwise we can do the same process again and get a third S-polynomial with the same properties and keep repeating. Since the initial terms are strictly decreasing and we have a well order there are only finitely many such S-polynomials.

First, we show that we can assume that $x^a > 1$. Indeed, assume that $a = 0$ and $k\mathbf{p}'$ is regular $\mathfrak{s}$-reducible. Since R is an integral domain, $\mathrm{LM}(k\overline{\mathbf{p}}') = \mathrm{LM}(\overline{\mathbf{p}}')$. Let $J_{\mathrm{LM}(\overline{\mathbf{p}}')}$ be the maximal regular saturated set J with $M(J) \mid \mathrm{LM}(\overline{\mathbf{p}}')$. Then $k\mathrm{LC}(\overline{\mathbf{p}}')$ lies in the ideal $\langle \mathrm{LC}(\alpha_j) : j \in J_{\mathrm{LM}(\overline{\mathbf{p}}')} \rangle$. Since R is a PID, this ideal is principal, let $b_{J_{\mathrm{LM}(\overline{\mathbf{p}}')}}$ be its generator, then $b_{J_{\mathrm{LM}(\overline{\mathbf{p}}')}} \mid k$. Let $\overline{\mathbf{q}}$ be the S-polynomial corresponding to the regular saturated set $J_{\mathrm{LM}(\overline{\mathbf{p}}')}$ and the generator $b_{J_{\mathrm{LM}(\overline{\mathbf{p}}')}}$, its signature divides $\mathfrak{s}(\mathbf{u})$ and is strictly divisible by $\mathfrak{s}(\mathbf{p})$. Repeating the process as needed, we obtain a strictly increasing sequence of elements dividing the coefficient of $\mathfrak{s}(\mathbf{u})$, and since R is a PID and in particular a unique-factorization domain, this sequence has to be finite. So we can assume that $x^a > 1$.

We will construct two reductions of $\mathrm{LT}(kx^a\overline{\mathbf{p}}')$, which taken together will give the S-polynomial $\mathbf{q}$. For the first reduction, the module element $\mathbf{p}' \in A^m$ is regular $\mathfrak{s}$-reduced modulo the s-s $\mathfrak{s}$-GB $\mathcal{G}$, and its signature is smaller than $\mathfrak{s}(\mathbf{u})$. Furthermore, by assumption $kx^a\mathbf{p}'$ is not regular $\mathfrak{s}$-reduced, so $\overline{\mathbf{p}}'$ cannot be 0. So, by definition of a s-s $\mathfrak{s}$-GB, $\mathbf{p}'$ is 1-singular $\mathfrak{s}$-reducible. So there exists $(t_i^{(1)})_{i \in J_1}$ terms in A, with $J_1 \subset \{1, \dots, s\}$ and for all $i \in J_1$, $t_i^{(1)} \neq 0$, and such that

$$\mathrm{LT}(\overline{\mathbf{p}}') = \sum_{i \in J_1} t_i^{(1)} \mathrm{LT}(\overline{\alpha}_i) = \sum_{i \in J_1} t_i^{(1)} T(i) \tag{5.2}$$

with for all $i \in J_1$, $\mathrm{LM}(t_i^{(1)}\overline{\alpha}_i) = \mathrm{LM}(t_i^{(1)})M(i) = \mathrm{LM}(\overline{\mathbf{p}}')$. Furthermore, there exists τ in J_1, $t_\tau^{(1)}S(\tau) = \mathfrak{s}(\overline{\mathbf{p}})$ and for all $i \in J_1 \setminus \{\tau\}$, $t_i^{(1)}S(i) \prec \mathfrak{s}(\mathbf{p})$.

We now build the second reduction. Since $kx^a\mathbf{p}'$ is regular $\mathfrak{s}$-reducible, there exists $(t_i^{(2)})_{i \in J_2}$ terms in A, with $J_2 \subset \{1, \dots, s\}$ and for all $i \in J_2$, $t_i^{(2)} \neq 0$, such that

$$\mathrm{LT}(kx^a\overline{\mathbf{p}}') = \sum_{i \in J_2} t_i^{(2)} \mathrm{LT}(\overline{\alpha}_i) = \sum_{i \in J_2} t_i^{(2)} T(i), \tag{5.3}$$

and for all $j \in J_2$, $\mathrm{LM}(t_j^{(2)})M(j) = \mathrm{LM}(kx^a\overline{\mathbf{p}}')$ and $t_j^{(2)}S(j) \prec \mathfrak{s}(kx^a\mathbf{p}')$.

Now let $J = J_1 \cup J_2$, and let $t_i^{(1)} = 0$ if $i \in J_2 \setminus J_1$, $t_j^{(2)} = 0$ if $j \in J_1 \setminus J_2$. Note that $\tau \notin J_2$, so $t_\tau^{(2)} = 0$. Combining Eqs. (5.2) and (5.3), we obtain a decomposition of $kx^a t_\tau T(\tau)$ as

$$kx^a t_\tau T(\tau) = - \sum_{i \in J \setminus \{\tau\}} t_i T(i).$$

where for all $i \in J$, $t_i = kx^a t_i^{(1)} - t_i^{(2)}$. Furthermore, for all $i \in J \setminus \{\tau\}$, $\mathrm{LM}(t_i)M(i) = \mathrm{LM}(x^a\overline{\mathbf{p}}') = \mathrm{LM}(x^a t_\tau)M(\tau)$ and $t_i S(i) \prec \mathfrak{s}(\overline{\mathbf{p}}) = kx^a t_\tau S(\tau)$.

The same argument as the one used, in the first part of the proof, to construct an S-polynomial based on Eq. (5.1) yields an S-polynomial $\mathbf{q}$ such that $\mathfrak{s}(\mathbf{q})$ divides $\mathfrak{s}(\mathbf{u})$, say $lx^b\mathfrak{s}(\mathbf{q}) = \mathfrak{s}(\mathbf{u})$. Furthermore, since the leading term is eliminated in the construction of an S-polynomial, $\mathrm{LT}(lx^b\overline{\mathbf{q}}) \prec \mathrm{LT}(kx^a\overline{\mathbf{p}}')$, which concludes the proof. $\qquad\square$

Theorem 5.5 (Correctness of Algorithm SigMöller). *Let* $\mathbf{T}$ *be a term of* A^m *and let* $\mathcal{G} = (\alpha_1, \dots, \alpha_s) \subseteq A^m$ *be a finite basis as computed by Algo. 3. Assume that all regular S-polynomials* $\mathbf{p}$ *with* $\mathfrak{s}(\mathbf{p}) \prec \mathbf{T}$ $\mathfrak{s}$*-reduce to* 0 *w.r.t.* $\mathcal{G}$ *. Then* $\mathcal{G}$ *is a semi-strong signature-Gröbner basis up to signature* $\mathbf{T}$.

Proof. To get a contradiction assume there exists a $\mathbf{u} \in A^m$ with $\mathfrak{s}(\mathbf{u}) \prec \mathbf{T}$ such that $\mathbf{u}$ does not $\mathfrak{s}$-reduce to zero. Assume w.l.o.g. that $\mathfrak{s}(\mathbf{u})$ is $\prec$-minimal such that $\mathbf{u}$ does not $\mathfrak{s}$-reduce to zero and also that $\mathbf{u}$ is regular $\mathfrak{s}$-reduced.

By Lem. 5.4 there is an S-polynomial $\mathbf{p}$ with $\mathfrak{s}(kx^a\mathbf{p}) = \mathfrak{s}(\mathbf{u})$ with $k \in R$, $x^a \in \mathrm{Mon}(A)$. Also, $kx^a\mathbf{p}'$ is regular $\mathfrak{s}$-reduced where $\mathbf{p}'$ is the result of regular $\mathfrak{s}$-reducing $\mathbf{p}$.

Let $J_{\mathrm{LM}(\overline{\mathbf{u}})}$ be the maximal regular saturated set J with $M(J) \mid \mathrm{LM}(\overline{\mathbf{u}})$. Since $\mathfrak{s}(kx^a\mathbf{p}) = \mathfrak{s}(\mathbf{u})$ and both $kx^a\mathbf{p}'$ and $\mathbf{u}$ are regular $\mathfrak{s}$-reduced, we have by Lem. 5.3 that $\mathrm{LM}(kx^a\overline{\mathbf{p}}') = \mathrm{LM}(\overline{\mathbf{u}})$, and either $\mathrm{LT}(kx^a\overline{\mathbf{p}}') = \mathrm{LT}(\overline{\mathbf{u}})$, or

$$\mathrm{LC}(\overline{\mathbf{u}} - kx^a\overline{\mathbf{p}}') \in \left\langle \mathrm{LC}(\overline{\boldsymbol{\alpha}}_j) : j \in J_{\mathrm{LM}(\overline{\mathbf{u}})} \right\rangle.$$

So in either case, there exists $(t_i)_{i \in J_{\mathrm{LM}(\overline{\mathbf{u}})}}$ terms in A, possibly all zero, such that

$$\mathrm{LT}(\overline{\mathbf{u}}) - \mathrm{LT}(kx^a\overline{\mathbf{p}}') = \sum_{i \in J_{\mathrm{LM}(\overline{\mathbf{u}})}} t_i \mathrm{LT}(\overline{\boldsymbol{\alpha}}_i)$$

and $t_i\mathrm{LM}(\overline{\boldsymbol{\alpha}}_i) = \mathrm{LM}(\overline{\mathbf{r}}) = \mathrm{LM}(\overline{\mathbf{u}})$ for all i such that $t_i \neq 0$.

Since $\mathbf{p}'$ is a regular S-polynomial with $\mathfrak{s}(\mathbf{p}') \preceq \mathfrak{s}(\mathbf{u}) \prec \mathbf{T}$, $\mathbf{p}'$ is $\mathfrak{s}$-reducible, and so $kx^a\mathbf{p}'$ is $\mathfrak{s}$-reducible. So there exists $(\tau_i)_{i \in J_{\mathrm{LM}(\overline{\mathbf{u}})}}$ terms in A such that

$$\mathrm{LT}(kx^a\overline{\mathbf{p}}') = \sum_{i \in J_{\mathrm{LM}(\overline{\mathbf{u}})}} \tau_i \mathrm{LT}(\overline{\boldsymbol{\alpha}}_i),$$

and $\tau_i\mathrm{LM}(\overline{\boldsymbol{\alpha}}_i) = \mathrm{LM}(kx^a\overline{\mathbf{p}}') = \mathrm{LM}(\overline{\mathbf{u}})$ for all i such that $\tau_i \neq 0$. So

$$\mathrm{LT}(\overline{\mathbf{u}}) = \left(\mathrm{LT}(\overline{\mathbf{u}}) - \mathrm{LT}(kx^a\overline{\mathbf{p}}') \right) + \mathrm{LT}(kx^a\overline{\mathbf{p}}') = \sum_{i \in J_{\mathrm{LM}(\overline{\mathbf{u}})}} (t_i + \tau_i)\mathrm{LT}(\overline{\boldsymbol{\alpha}}_i),$$

and $\mathbf{u}$ is $\mathfrak{s}$-reducible which is a contradiction. $\qquad\square$

5.3. Proof of termination

The usual proofs of termination of signature-based Gröbner basis algorithms (*e.g.* [22, Th. 11]) rely on the fact that all elements which are singular $\mathfrak{s}$-reducible are discarded in the computations. Algorithm SigMöller only discards those which are 1-singular $\mathfrak{s}$-reducible. For this reason, we adapt the proof of termination of Algorithm RB [10, Th. 20], which handles singular $\mathfrak{s}$-reducible elements in a different way.

Theorem 5.6. *Algorithm SigMöller terminates.*

Proof. Let $\mathcal{G} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t, \ldots)$ be the sequence of basis elements computed by SigMöller. By construction, for all $t \geq 1$, $\overline{\boldsymbol{\alpha}_t}$ is not $\mathfrak{s}$-reducible by $\mathcal{G}_{t-1} := \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{t-1}\}$, and all $\mathbf{v} \in A^m$ with $\mathfrak{s}(\mathbf{v}) \prec \mathfrak{s}(\boldsymbol{\alpha}_t)$ $\mathfrak{s}$-reduce to zero w.r.t. $\mathcal{G}_{t-1}$.

For $i \geq 1$, let $M(i) = \mathrm{LM}(\overline{\boldsymbol{\alpha}}_i)$, $T(i) = \mathrm{LT}(\overline{\boldsymbol{\alpha}}_i)$. We define the sig-lead ratio $r(\boldsymbol{\alpha}_i)$ of $\boldsymbol{\alpha}_i$ as $\frac{\mathfrak{s}(\boldsymbol{\alpha}_i)}{M(i)}$. Those ratios are ordered naturally by $\frac{s}{m} \prec \frac{s'}{m'} \iff sm' \prec s'm$.

We partition $\mathcal{G}$ into subsets $\mathcal{G}_r = \{\boldsymbol{\alpha}_i \mid r(\boldsymbol{\alpha}_i) \simeq r\}$, where $\simeq$ denotes equality up to a coefficient in R. We prove that only finitely many $\mathcal{G}_r$ are non-empty, and that they are all finite, hence $\mathcal{G}$ is finite.

First, we prove that only finitely many $\mathcal{G}_r$ are non-empty. We do so by counting minimal basis elements, where $\boldsymbol{\alpha}_i$ is minimal if and only if there is no $\boldsymbol{\alpha}_j \in \mathcal{G}$ with $\mathfrak{s}(\boldsymbol{\alpha}_j) \mid \mathfrak{s}(\boldsymbol{\alpha}_i)$ and $T(j) \mid T(i)$. A non-minimal module element $\boldsymbol{\alpha}_i$ is $\mathfrak{s}$-reducible by $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{i-1}\}$ ([22, Lem. 12]), and since all basis elements are regular $\mathfrak{s}$-reduced by construction, $\boldsymbol{\alpha}_i$ is singular $\mathfrak{s}$-reducible. In particular, there exists at least one $\boldsymbol{\alpha}_j$, $j < i$ and a monomial m with $\mathfrak{s}(m\boldsymbol{\alpha}_j) \simeq \mathfrak{s}(\boldsymbol{\alpha}_i)$ and $mM(j) = M(i)$, so $\boldsymbol{\alpha}_i$ and $\boldsymbol{\alpha}_j$ lie in the same subset $\mathcal{G}_r$. Hence there are at most as many non-empty $\mathcal{G}_r$'s as there are minimal basis elements. This is finitely many because A and A^m are Noetherian.

Then we prove by induction on the finitely many non-empty sets $\mathcal{G}_r$ that each $\mathcal{G}_r$ is finite. Let r be a sig-lead ratio, assume that for all $r' < r$, $\mathcal{G}_{r'}$ is finite. Let $\boldsymbol{\alpha}_t \in \mathcal{G}_r$. If $\boldsymbol{\alpha}_t$ is $\mathbf{e}_i$ for some i,

then it only counts for one. Otherwise, let J be the regular saturated set, and $\mathbf{p}$ the corresponding S-polynomial, that SigMöller regular $\mathfrak{s}$-reduced to obtain $\boldsymbol{\alpha}_t$. Then $\mathbf{p} = \sum_{j \in J} b_j \frac{M(J)}{M(j)} \boldsymbol{\alpha}_j$ for $b_j \in R$, and there exists $\tau \in J$ such that for all $j \in J \setminus \{\tau\}$, $\frac{M(J)}{M(j)}\mathfrak{s}(\boldsymbol{\alpha}_j) \prec \frac{M(J)}{M(\tau)}\mathfrak{s}(\boldsymbol{\alpha}_\tau)$. Also $T(t) \prec LT(\frac{M(J)}{M(\tau)}\overline{\boldsymbol{\alpha}}_\tau)$ and $\mathfrak{s}(\boldsymbol{\alpha}_t) = \frac{M(J)}{M(\tau)}\mathfrak{s}(\boldsymbol{\alpha}_\tau)$. So $r = \frac{\mathfrak{s}(\boldsymbol{\alpha}_t)}{M(t)} \succ \frac{\mathfrak{s}(\boldsymbol{\alpha}_\tau)}{M(\tau)} \succ \frac{\mathfrak{s}(\boldsymbol{\alpha}_j)}{M(j)}$ for $j \in J \setminus \{\tau\}$. Hence all $\boldsymbol{\alpha}_j$, $j \in J$ are in some $\mathcal{G}_{r_j}$ with $r_j < r$, so for computing elements of $\mathcal{G}_r$, the algorithm will consider at most as many saturated subsets as there are subsets of $\bigcup_{r' < r} \mathcal{G}_r$, which is finite by induction. Furthermore, since R is a PID and in particular Noetherian, with each saturated subset J, the algorithm only builds finitely many S-polynomials (actually, it only builds one). So overall, we find that $\mathcal{G}_r$ is finite, which concludes the proof by induction. □

5.4. Eliminating S-polynomials

It is well known in the case of fields that additional criteria can be implemented to detect that a regular S-pair will lead to an element which $\mathfrak{s}$-reduces to 0. In this section, we show how we can implement three such criteria, namely the syzygy criterion, the F5 criterion and the singular criterion.

5.4.1. Syzygy Criterion. Syzygy criteria rely on the fact that, if the signature of an S-polynomial can be written as a linear combination of signatures of syzygies, then this S-polynomial would be a syzygy itself. Signatures of syzygies can be identified in two ways:

- the Koszul syzygy between basis elements $\mathbf{p}$ and $\mathbf{q}$ such that $\mathfrak{s}(\mathbf{p}) = m_{\mathbf{p}}\mathbf{e}_i$, $\mathfrak{s}(\mathbf{q}) = m_{\mathbf{q}}\mathbf{e}_j$, $i < j$ is $\overline{\mathbf{p}}\mathbf{q} - \overline{\mathbf{q}}\mathbf{p}$, and it has signature $LT(\overline{\mathbf{p}})\mathfrak{s}(\mathbf{q})$;
- if a regular S-polynomial $\mathbf{p}$ $\mathfrak{s}$-reduces to 0, then $\mathfrak{s}(\mathbf{p})$ and its multiples are signatures of syzygies; thus, the algorithm may maintain a set of generators of signatures of syzygies by adding to this set $\mathfrak{s}(\mathbf{p})$ for each S-polynomial $\mathbf{p}$ $\mathfrak{s}$-reducing to 0.

For regular sequences, all syzygies are Koszul syzygies.

Proposition 5.7 (Syzygy criterion). *Assume that* $\mathbf{T}$ *is a signature such that all module elements with signature less than* $\mathbf{T}$ $\mathfrak{s}$*-reduce to 0. Let* $\mathbf{p} \in A^m$ *be such that there exist syzygies* $\mathbf{z}_1, \dots, \mathbf{z}_k$ *and terms* $m_1, \dots, m_k$ *in* A *with* $\mathfrak{s}(\mathbf{p}) = \sum_{i=1}^{k} m_i \mathfrak{s}(\mathbf{z}_i)$*, and* $\mathfrak{s}(\mathbf{p}) \leq \mathbf{T}$*. Then* $\mathbf{p}$ *regular* $\mathfrak{s}$*-reduces to 0.*

Proof. Let $\mathbf{r} = \mathbf{p} - \sum_{i=1}^{k} m_i \mathbf{z}_i$, then $\mathfrak{s}(\mathbf{r}) \prec \mathfrak{s}(\mathbf{p}) \leq \mathbf{T}$ so $\mathbf{r}$ $\mathfrak{s}$-reduces to 0. But $\overline{\mathbf{r}} = \overline{\mathbf{p}} - \sum_{i=1}^{k} m_i \overline{\mathbf{z}}_i = \overline{\mathbf{p}}$, so $\mathbf{p}$ also $\mathfrak{s}$-reduces to 0 with reducers of signature at most $\mathfrak{s}(\mathbf{r}) \prec \mathfrak{s}(\mathbf{p})$. □

Koszul syzygies can be eliminated with the same technique, but it is more efficient to use the F5 criterion [22, Sec. 3.3].

Proposition 5.8 (F5 criterion, [11, 3]). *Let* $\mathbf{p} \in A^m$ *with signature* $\mu \mathbf{e}_i$*, and let* $\{\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_t\}$ *be a signature Gröbner basis of* $\langle f_1, \dots, f_{i-1} \rangle$*. Then* $\mathbf{p}$ *is a Koszul syzygy if and only if* μ *is* $\mathfrak{s}$*-reducible modulo* $\{\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_t\}$*.*

Proof. By definition, $\mathbf{p}$ is a Koszul syzygy if and only if $m \in LT(\langle f_1, \dots, f_{i-1} \rangle)$, and the conclusion follows by definition of a weak Gröbner basis. □

5.4.2. Singular Criterion. The singular criterion states that the algorithm only needs to consider one S-polynomial with a given signature. So when computing a new S-polynomial, if there already exists a $\mathfrak{s}$-reduced module element with the same signature, we may discard the current S-polynomial without performing any $\mathfrak{s}$-reduction.

Proposition 5.9 (Singular criterion). *Let* $\mathcal{G} = \{\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_s\}$ *be a signature Gröbner basis up to signature* $\mathbf{T}$*. Let* $\mathbf{p} \in A^m$ *be such that there exists* $\boldsymbol{\alpha}_i \in \mathcal{G}$ *with* $\mathfrak{s}(\boldsymbol{\alpha}_i) = \mathfrak{s}(\mathbf{p})$ *and* $\mathfrak{s}(\mathbf{p}) = \mathfrak{s}(\mathbf{T})$*. Then* $\mathbf{p}$ $\mathfrak{s}$*-reduces to 0.*

Proof. Let $\mathbf{p}'$ be the result of regular $\mathfrak{s}$-reducing $\mathbf{p}$ w.r.t. $\mathcal{G}$. By construction, the basis element $\boldsymbol{\alpha}_i$ is regular $\mathfrak{s}$-reduced w.r.t. $\mathcal{G}$. So by Lem. 5.3, $LM(\overline{\mathbf{p}}') = LM(\overline{\boldsymbol{\alpha}}_i)$, and applying Lem. 4.5, with $k = 1$ and $x^a = 1$, shows that $\mathbf{p}'$ is 1-singular $\mathfrak{s}$-reducible. The result of that $\mathfrak{s}$-reduction has signature $\prec \mathfrak{s}(\mathbf{p}) = \mathbf{T}$, so it $\mathfrak{s}$-reduces to 0. □

TABLE 1. Computation of a grevlex GB of the Katsura-2 system in $\mathbb{Z}[X_1, X_2, X_3]$

Algorithm	Pairs / sat. sets	S-polynomials	Reductions to 0
Möller strong	78	20	7
SigMöller (with criteria)	170	13	0

TABLE 2. Computation of a grevlex GB of the Katsura-3 system in $\mathbb{Z}[X_1, X_2, X_3, X_4]$

Algorithm	Pairs / sat. sets	S-polynomials	Reductions to 0
Möller strong	861	246	159
SigMöller (with criteria)	2227	51	0

6. Experimental results and future work

We have written a toy implementation of Algo. SigMöller[1], with the F5 and Singular criteria. We provide functions LinDecomp and SatIdeal for Euclidean rings, fields and multivariate polynomial rings.

Since our focus is on the feasibility of signature-compatible computations and not their efficiency, we give data about the number of considered S-polynomials, saturated sets and reductions to 0, when computing Gröbner bases over $\mathbb{Z}$ for the polynomial systems Katsura-2 (Table 1) and Katsura-3 (Table 2). The statistics are compared with a run of Möller's strong algorithm [19]. Even though the proposed algorithm, adapted from Möller's weak algorithm, considers more saturated sets than Möller's strong algorithm, thanks to the signatures, it ends up computing and reducing significantly less S-polynomials, and no reductions to zero appear.

Running Algo. SigMöller on larger examples would require optimizations, but it appears that the most expensive step is the generation of the saturated sets, which takes time exponential in the size of the current basis. This step may be accelerated in different ways. First, it is known that in the case of PIDs, the reductions of Möller's algorithm can be recovered from those of Möller's strong algorithm [1, Sec. 4.4], which may allow to run the algorithms considering only pairs instead of arbitrary tuples of polynomials. Additionally, Gebauer and Möller's criteria for fields can be used to make Möller's strong algorithm over PIDs more efficient [19]. We will investigate whether it is possible to prove that these algorithms are compatible with signatures in the future. Finally, future research will be focused on further signature-based criteria, such as the cover criterion described in [14] and the more general rewriting criteria.

The algorithm accepts as input polynomials over any ring, provided that the necessary routines are defined. In particular, our implementation can run the algorithms on polynomials on the base ring $\mathbb{K}[y_1, \ldots, y_k]$. On small examples in this setting, it appears that the algorithm terminates and returns a correct output. Understanding the behavior of SigMöller over UFDs or even more general rings will also be the focus of future research.

References

[1] W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases*. American Mathematical Society, 7 1994.

[2] A. Arri and J. Perry. The F5 Criterion Revised. *Journal of Symbolic Computation*, 46(9):1017–1029, 2011.

[3] M. Bardet, J.-C. Faugère, and B. Salvy. On the Complexity of the F_5 Gröbner Basis Algorithm. *J. Symbolic Comput.*, 70:49–70, 2015.

[4] 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).

[5] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, Austria, 1965.

[6] C. Eder and J.-C. Faugère. A Survey on Signature-based Algorithms for Computing Gröbner Bases. *Journal of Symbolic Computation*, 80:719–784, 2017.

[7] C. Eder and J. Perry. F5C: a Variant of Faugere's F5 Algorithm with Reduced Gröbner Bases. *Journal of Symbolic Computation*, 45(12):1442–1458, 2010.

---

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

[8] C. Eder and J. 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.

[9] 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.

[10] C. Eder and B. H. Roune. Signature Rewriting in Gröbner Basis Computation. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, pages 331–338. ACM, 2013.

[11] J.-C. 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.

[12] M. Francis and A. Dukkipati. On Ideal Lattices, Gröbner Bases and Generalized Hash Functions. *Journal of Algebra and Its Applications*, 2017.

[13] S. Gao, Y. Guan, and F. Volny IV. A New Incremental Algorithm for Computing Gröbner bases. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ISSAC '10, pages 13–19. ACM, 2010.

[14] S. Gao, F. Volny IV, and M. Wang. A New Framework for Computing Gröbner Bases. *Mathematics of Computation*, 85(297):449–465, 2016.

[15] R. Gebauer and H. M. Möller. On an Installation of Buchberger's Algorithm. *Journal of Symbolic Computation*, 6(2-3):275–286, 1988.

[16] 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.

[17] D. Lichtblau. Effective Computation of Strong Gröbner Bases over Euclidean Domains. *Illinois J. Math.*, 56(1):177–194 (2013), 2012.

[18] D. Lichtblau. Applications of Strong Gröbner Bases over Euclidean Domains. *Int. J. Algebra*, 7(5-8):369–390, 2013.

[19] H. M. Möller. On the Construction of Gröbner Bases using Syzygies. *Journal of Symbolic Computation*, 6(2-3):345–359, 1988.

[20] 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.

[21] K. Nabeshima. Reduced Gröbner Bases in Polynomial Rings over a Polynomial Ring. *Mathematics in Computer Science*, 2(4):587–599, 2009.

[22] 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.

[23] G. Zacharias. Generalized Gröbner Bases in Commutative Polynomial Rings. Master's thesis, MIT, Cambridge, MA, 1978.

Acknowledgments

Maria Francis
Dept of Computer Science and Engineering, Indian Institute of Technology, Hyderabad, India
mariaf@iith.ac.in

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

Appendix A. Example run of Algorithm SigMöller (Algo. 3)

As an illustration, consider the ring $A = \mathbb{Z}[x, y]$ with the lexicographical ordering with $x > y$, and the ideal generated by $f_1 = 3xy + x + y^2$ and $f_2 = x^2$.

The algorithm maintains a signature Gröbner basis G and a queue of saturated pairs $\mathcal{P}$. Both are finite ordered sequences (lists), which we denote with square brackets, *e.g.* $G = [\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_t]$. The elements of G are pairs (polynomial, signature), for which we use the notations $\mathbf{g}_i = (g_i, \mathfrak{s}(\mathbf{g}_i))$. To simplify the notations, given a basis $G = [\mathbf{g}_1, \dots, \mathbf{g}_t]$, m a monomial of A and $k \in \mathbb{N}$, we use the notation

$$J_m^{(k)} = \mathrm{Sat}(m; \mathrm{LM}(g_1), \dots, \mathrm{LM}(g_k)) = \left\{ i : i \in \{1..k\} : \mathrm{LM}(g_i) \mid m \right\}$$

for the saturated sets.

In a saturated set, we will use the notation $*$ to denote those indices which contribute the maximal signature. For example, in the saturated set $J = \{1, 2, 4^*, 5, 8^*\}$, we would have

$$S_J \simeq \frac{M(J)}{\mathrm{LM}(g_4)} \mathfrak{s}(\mathbf{g}_4) \simeq \frac{M(J)}{\mathrm{LM}(g_8)} \mathfrak{s}(\mathbf{g}_8) \succcurlyeq \frac{M(J)}{\mathrm{LM}(g_i)} \mathfrak{s}(\mathbf{g}_i) \text{ for } i \in \{1, 2, 5\}.$$

If only one index is marked with a star, the saturated set is regular and that index is the signature index.

The algorithm starts with an empty basis $G = []$ and an empty queue of regular saturated sets $\mathcal{P} = []$. We first add f_1 with signature $\mathbf{e}_1$ to G, that is, we add the element $\mathbf{g}_1 = (3xy + x + y^2, \mathbf{e}_1)$ to G.

We observe that no saturated sets can be formed, so $G_1 = [\mathbf{g}_1]$ is a weak signature Gröbner basis of $\langle f_1 \rangle$.

We then introduce f_2, with signature $\mathbf{e}_2$. It cannot be reduced modulo G, so we add to the basis the element $\mathbf{g}_2 = (x^2, \mathbf{e}_2)$.

To form regular saturated sets, we consider all possible least common multiples of leading monomials of g_i involving g_2. Here, the set of leading monomials is $\{xy, x^2\}$, and the only nontrivial LCM that we can form is $x^2 y$. For each least common multiple m, the set

$$J = J_m^{(2)} = \mathrm{Sat}(m; \mathrm{LM}(g_1), \mathrm{LM}(g_2)) = \{i \in \{1, 2\} : \mathrm{LM}(g_i) \text{ divides } m\}$$

is a saturated set, with $M(J) = m$. Here, for $m = x^2 y$, we get $J_1 = J_{x^2 y}^{(2)} = \{1, 2^*\}$.

We have $M(J_1) = x^2 y = x\mathrm{LM}(g_1) = y\mathrm{LM}(g_2)$. We multiply the corresponding signatures and we compare: here, $x\mathfrak{s}(\mathbf{g}_1) = x\mathbf{e}_1 \precnsim y\mathfrak{s}(\mathbf{g}_2) = y\mathbf{e}_2$, so the presignature of J_1 is $S_{J_1} = y\mathbf{e}_2$, and it is regular with signature index 2.

We now compute a S-polynomial associated to J_1, namely $h_3 = 3yg_2 - xg_1 = -x^2 - xy^2$ with signature $\mathfrak{s}(\mathbf{h}_3) = 3y\mathfrak{s}(\mathbf{g}_2) = 3y\mathbf{e}_2$. Since $\mathrm{LM}(h_3) = -\mathrm{LM}(g_2)$ and $\mathfrak{s}(\mathbf{h}_3) \succcurlyeq \mathfrak{s}(\mathbf{g}_2)$, h_3 is regular $\mathfrak{s}$-reducible modulo G, and the result is $g_3 = -xy^2$. It still has signature $3y\mathbf{e}_2$, because we only performed a regular $\mathfrak{s}$-reduction. We add to G the element $\mathbf{g}_3 = (-xy^2, 3y\mathbf{e}_2)$.

The next few steps are identical, so we give a fast-forward version:

4. Regular saturated set $J_2 = J_{xy^2}^{(3)} = \{1, 3^*\}$ with $M(J_2) = xy^2$ and $S_{J_2} = y\mathbf{e}_2$
   $\rightarrow \mathbf{g}_4 = (xy + y^3, 9y\mathbf{e}_2)$;
5. Regular saturated set $J_3 = J_{xy}^{(4)} = \{1, 4^*\}$ with $M(J_3) = xy$ and $S_{J_3} = y\mathbf{e}_2$
   $\rightarrow \mathbf{g}_5 = (-x + 3y^3 - y^2, 27y\mathbf{e}_2)$;
6. Regular saturated set $J_4 = J_{xy}^{(5)} = \{1, 4, 5^*\}$ with $M(J_4) = xy$ and $S_{J_4} = y^2\mathbf{e}_2$
   $\rightarrow \mathbf{g}_6 = (3y^4, 27y^2\mathbf{e}_2)$;
7. Regular saturated set $J_5 = J_{xy^2}^{(4)} = \{1, 3, 4^*\}$ with $M(J_5) = xy^2$ and $S_{J_5} = y^2\mathbf{e}_2$
   $\rightarrow \mathbf{g}_7 = (y^4, 9y^2\mathbf{e}_2)$.

Both J_3 and J_5 were added to $\mathcal{P}$ after Step 4 (construction of $\mathbf{g}_4$). But at Step 5, since $S_{J_3} \precnsim S_{J_5}$, we have to consider J_3 first, and keep J_5 for later. After Step 5, $\mathcal{P}$ contains both J_4 and J_5, whose

presignatures are incomparable: $S_{J_4} \simeq S_{J_5}$. So we could have considered J_5 before J_4, the result would still have been correct.

After introducing $\mathbf{g}_7$, the basis G has 7 elements:

$$G = [(3xy + \dots, \mathbf{e}_1), (x^2, \mathbf{e}_2), (-xy^2, 3y\mathbf{e}_2), (xy + \dots, 9y\mathbf{e}_2),$$
$$(-x + \dots, 27y\mathbf{e}_2), (3y^4, 27y^2\mathbf{e}_2), (y^4, 9y^2\mathbf{e}_2)].$$

The queue $\mathcal{P}$ is not empty at this point, but before continuing, we need to form regular saturated sets using the latest addition $\mathbf{g}_7$.

We go through the same process as before to form saturated sets:

1. List all possible least common multiples of leading monomials involving $\mathrm{LM}(g_7)$: those are y^4, xy^4, x^2y^4.
2. For each of them, compute the corresponding saturated set:
   - y^4 gives $J_{y^4}^{(7)} = \{6^*, 7^*\}$ with presignature $y^2\mathbf{e}_2$;
   - xy^4 gives $J_{xy^4}^{(7)} = \{1, 3, 4, 5, 6^*, 7^*\}$, with presignature $xy^2\mathbf{e}_2$;
   - x^2y^4 gives $J_{x^2y^4}^{(7)} = \{1, 2, 3, 4, 5, 6^*, 7^*\}$ with presignature $x^2y^2\mathbf{e}_2$.

None of those 3 saturated sets is regular: there is always a signature collision between $\mathbf{g}_6$ and $\mathbf{g}_7$. For example, with $J_{x^4}^{(7)}$, $\mathfrak{s}(\mathbf{g}_6) \simeq \mathfrak{s}(\mathbf{g}_7) \simeq y^2\mathbf{e}_2$.

So we need to make them regular, which is done by forming new sets with just one of the colliding signatures. From $J_{y^4}^{(7)}$, we could form $\{6^*\}$ and $\{7^*\}$, which are trivial.

From $J_{xy^4}^{(7)}$, we can form the regular saturated sets $\{1, 3, 4, 5, 6^*\}$ and $\{1, 3, 4, 5, 7^*\}$. Since the set $\{1, 3, 4, 5, 6^*\}$ does not contain 7, it is already in $\mathcal{P}$. And we add the new regular saturated set $\{1, 3, 4, 5, 7^*\}$ to $\mathcal{P}$.

Similarly, from $J_{x^2y^4}^{(7)}$, we find the new regular saturated set $\{1, 2, 3, 4, 5, 7^*\}$ to add to $\mathcal{P}$.

Then we continue with the regular saturated set $J_6 = \{1, 3, 4, 5^*\}$ with $M(J_2) = x^2y$ and $S(J_2) = 27y^3\mathbf{e}_2$. It gives rise to $h_8 = 3y^5 + y^4$ with signature $\mathfrak{s}(\mathbf{h}_8) = 27y^3\mathbf{e}_2$.

Since $\mathrm{LM}(h_8) = y\mathrm{LM}(g_6)$ and $\mathfrak{s}(\mathbf{h}_8) = y\mathfrak{s}(\mathbf{g}_6)$, we know that h_8 is 1-singular reducible modulo G and can be discarded. Note that we only needed to compare the leading *monomials* (without coefficients) of h_8 and g_6, and not verify whether there is an actual linear combination eliminating that term.

Remark A.1. If we had considered J_5 before J_4 at Step 6, $\mathbf{g}_7$ would have been built before $\mathbf{g}_6$, and $\mathbf{g}_6$ would have been discarded for being 1-singular reducible modulo $\mathbf{g}_7$. In that case, the non-regular saturated sets $J_{y^4}^{(7)}$, $J_{xy^4}^{(7)}$ and $J_{x^2y^4}^{(7)}$ would never have been considered.

The remainder of the run proceeds differently, depending on whether the F5 criterion (Prop. 5.8) is implemented. If it is not, the remaining regular saturated sets all give rise to polynomials regular $\mathfrak{s}$-reducing to 0, and the algorithm terminates, returning the 7-elements basis written above.

On the other hand, if the F5 criterion is implemented, those reductions to zero are excluded. Let us illustrate it with the next saturated set in the queue: $J_7 = \{2, 5^*\}$, with signature $27xy\mathbf{e}_2$. We need to test whether $27xy$ lies in the ideal of leading terms of $\langle f_1 \rangle$, which is equivalent to testing whether $27xy$ is reducible modulo the already computed basis $G_1 = \{(3xy^2 + x + y^2, \mathbf{e}_1)\}$. Since it is indeed reducible, this regular saturated set indeed satisfies the F5 criterion, and can be discarded without further calculation. The criterion eliminates all subsequent regular saturated sets in the same way.