# Signature-based Criteria for Möller's Algorithm for Computing Gröbner Bases over Principal Ideal Domains

Maria Francis
Institute for Algebra / Johannes Kepler University
4040 Linz, Austria
maria.francis@jku.at

Thibaut Verron
Institute for Algebra / Johannes Kepler University
4040 Linz, Austria
thibaut.verron@jku.at

## 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 signature-based algorithm for computing Gröbner bases over principal ideal domains (*e.g.* the ring of integers or the ring of univariate polynomials over a field). It is adapted from Möller's algorithm (1988) which considers reductions by multiple polynomials at each step. This ensures that, in our signature-based adaptation, signature drops are not a problem, and it allows us to implement classic signature-based criteria to eliminate some redundant reductions.

A toy implementation in Magma confirms that the signature-based algorithm is more efficient in terms of the number of $S$-polynomials computed. Early experimental results suggest that the algorithm might even work for polynomials over more general rings, such as unique factorization domains (*e.g.* the ring of multivariate polynomials over a field or a PID).

## CCS CONCEPTS

• **Computing methodologies → Algebraic algorithms**;

## KEYWORDS

Gröbner bases, Signature-based algorithms, Principal Ideal Domains

**ACM Reference Format:**
Maria Francis and Thibaut Verron. 2018. Signature-based Criteria for Möller's Algorithm for Computing Gröbner Bases over Principal Ideal Domains. In *Proceedings of Conference'18, July 2018, Washington, DC, USA (Conference'18).* ACM, New York, NY, USA, 8 pages.

## 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. This technique was first introduced for Algorithm F5 [12], and there have been many research works in this direction [2, 7, 8, 14].

All these algorithms are for ideals in polynomial rings over fields. Gröbner bases can be defined and computed over commutative rings [1, Ch. 4], and can be used in many applications, *e.g.* for polynomials over $\mathbb{Z}$ in lattice-based cryptography [13] or for polynomials over a polynomial ring as an elimination tool [19]. Many other examples are described in [17].

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 computing a strong Gröbner basis is more expensive 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.

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 [16], were presented in [9]. The 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 consider the problem of computing a weak Gröbner basis of a polynomial ideal with coefficients in a PID, using signature-based techniques. The algorithm that we present is adapted from that of Möller [18], which considers combinations and reductions by multiple polynomials at once. The way the signatures are ordered ensures that no reductions leading to signature-drops can happen. 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.

We have written a toy implementation of the algorithms presented, with the F5 and the singular criteria, in the Magma Computational Algebra System [4]. Möller's 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 little changes, it can be made to accomodate inputs with coefficients in a more general ring. Interestingly, early experimental data with coefficients in a multivariate polynomial ring (a Unique Factorization Domain which is not a PID) suggest that the signature-based algorithm might work

The authors are supported by the Austrian FWF grants Y464 and F5004 respectively.


*Conference'18, 2018*

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 [10, 20]. The theory of Gröbner bases for polynomials over Noetherian commutative rings dates back to the 1970s [18, 21] 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 algorithm [18] extends this approach to Noetherian commutative rings. As for strong Gröbner bases, they can be computed using an adapted version of Buchberger's algorithm [15].

As said before, Möller's algorithm can use more than two polynomials when building $S$-polynomials. This idea is similar to the selection technique introduced in Algorithm F4 [11] to replace polynomial reductions with linear algebra reductions.

## 2 NOTATIONS

Let $A$ be a Noetherian integral domain, which is assumed to have a 1 and be commutative. Let $R = A[x_1, \dots, x_n]$ be the polynomial ring in $n$ indeterminates $x_1, \dots, x_n$ over $A$. A monomial in $R$ 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 is $kx^a$, where $k \in A$ and $k \neq 0$. We will denote all the terms in $R$ by $\mathrm{Ter}(R)$ and all the monomials in $R$ by $\mathrm{Mon}(R)$. We use the notation $\mathfrak{a}$ for polynomial ideals in $A[x_1, \dots, x_n]$ and $I$ for ideals in the coefficient ring $A$.

The notion of monomial order can be directly extended from $\mathbb{K}[x_1, \dots, x_n]$ to $R$. In the rest of the paper, we assume that $R$ 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.

We consider the free $R$-module $R^m$ with basis $\mathbf{e}_1, \dots, \mathbf{e}_m$. A term (resp. monomial) in $R^m$ is $kx^a\mathbf{e}_i$ (resp. $x^a\mathbf{e}_i$) for some $k \in A \setminus \{0\}$, $x^a \in \mathrm{Mon}(R)$, $i \in \{1, \dots, m\}$. In this paper, monomials in $R^m$ 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 $R^m$, 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 $f_1, \dots, f_m \in R$, we define an $R$-module homomorphism $\bar{\cdot} : R^m \to R$, by setting $\bar{\mathbf{e}}_i = f_i$ and extending linearly to $R^m$.

We recall the concept of signatures in $R^m$. 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 $k \in A, x^a \in \mathrm{Mon}(R)$ and $\mathbf{e}_i$ is a standard basis vector.

Note that we have two ways of comparing two similar signatures $s(\boldsymbol{\alpha}) = kx^a\mathbf{e}_i$ and $s(\boldsymbol{\beta}) = lx^b\mathbf{e}_j$. We write $s(\boldsymbol{\alpha}) = s(\boldsymbol{\beta})$ if $k = l$, $a = b$ and $i = j$, and we write $s(\boldsymbol{\alpha}) \simeq s(\boldsymbol{\beta})$ if $a = b$ and $i = j$, $k$ and $l$ being possibly different. If $A$ 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 signatures and coefficients are ordered.

## 3 GRÖBNER BASES IN POLYNOMIAL RINGS OVER $A$

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

### 3.1 Computations in $A$

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

(1) There are algorithms for arithmetic operations ($+$, $*$, zero test) in $A$.
(2) There is an algorithm LinDecomp:
   - Input: $\{k_1, \dots, k_s\} \subset A, k \in A$
   - Output: TRUE iff $k \in \langle k_1, \dots, k_s\rangle$ and if yes, $l_1, \dots, l_s \in A$ such that $k = k_1l_1 + \dots + k_sl_s$.
(3) There is an algorithm SatIdeal:
   - Input: $\{k_1, \dots, k_s\} \subset A, k \in A$
   - Output: $\{l_1, \dots, l_r\} \subset A$ generators of the saturated ideal $\langle k_1, \dots, k_s\rangle : \langle k\rangle$.

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

*Example 3.1.* Euclidean rings are effective, because one can implement those algorithms using GCD computations and Euclidean reductions. For example over $\mathbb{Z}$, $\mathsf{LinDecomp}(\{4\}, 12)$ is $(\mathsf{TRUE}, \{3\})$, since 12 is in the ideal $\langle 4\rangle$ and $12 = 3{\cdot}4$. The output of $\mathsf{SatIdeal}(\{4\}, 6)$ 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.

In the rest of the paper, we assume that the ring $A$ is a PID.

### 3.2 Polynomial reduction

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 $\mathrm{LM}(f)$. One of the obvious workarounds for this problem is to include a very restrictive condition that $\mathrm{LT}(g)$ should divide $\mathrm{LT}(f)$ to the definition of reduction. This definition leads to the notion of strong Gröbner bases.

Here we are only interested in computing (weak) Gröbner bases. For that purpose, following [1, 18], we expand the definition to allow for a linear combination of reducers. Before defining reductions, we define saturated sets [1, Def.4.2.4] (called maximal sets in [18]).

*Definition 3.2.* Given a tuple of monomials $(x^{a_1}, \dots, x^{a_s})$, the *saturated set* for a monomial $x^b$ w.r.t. $(x_{a_1}, \dots, x_{a_s})$ is defined as

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

A set $J \subseteq \{1, \dots, s\}$ is said to be *saturated* w.r.t. $(x^{a_1}, \dots, x^{a_s})$ if $J = \mathrm{Sat}(x^J; x^{a_1}, \dots, x^{a_s})$ where $x^J = \mathrm{lcm}(x^{a_i} : i \in J)$. 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 $A$ defined as $I_J := \langle \mathrm{LC}(f_i) : i \in J \rangle$.

*Definition 3.3.* Let $f \in R$. Let $f_1, \ldots, f_s \in R$ and $x^{a_1}, \ldots, x^{a_s} \in \mathrm{Mon}(R)$ be such that $x^{a_i}\mathrm{LM}(f_i) = \mathrm{LM}(f)$ for all $i$. We say that we can *top reduce* $f$ by $f_1, \ldots, f_s \in R$ if there exist non-zero $l_1, \ldots, l_s$ in $A$ 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 *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 *reducers*. A polynomial $f \in R$ is *reducible* if it can be reduced, otherwise it is *reduced*.

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

*Example 3.4.* 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 top 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 Gröbner bases and strong Gröbner bases for an ideal in $R$.

*Definition 3.5.* Let $\mathfrak{a}$ be an ideal in $R$ and $G = \{g_1, \ldots, g_t\}$ be a set of nonzero polynomials in $\mathfrak{a}$. The set $G$ is called a *(weak) Gröbner basis* of $\mathfrak{a}$ in $R$ if and only if $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(\mathfrak{a}) \rangle$. The set $G$ is called a *strong Gröbner basis* of $\mathfrak{a}$ if and only if for any polynomial $f \in \mathfrak{a}$, there exists $g_i \in G$ such that $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$.

*Example 3.6.* Consider the set $G = \{2x, 3x\} \subset \mathbb{Z}[x]$, it is a weak Gröbner basis of $\mathfrak{a} := \langle G \rangle$, but it is not a strong Gröbner basis: $5x \in \mathfrak{a}$, and it is divisible by neither $2x$ nor $3x$.

Remark 3.7. *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].*

## 3.3 Computation of Gröbner bases in $R$

In this section, we present Möller's algorithm [18] 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 $\{g_1, \ldots, g_s\}$ of polynomials, and let $J$ be a saturated subset of $\{1, \ldots, s\}$ containing $s$ w.r.t. $\{\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)\}$. Recall that $x^J = \mathrm{lcm}(\mathrm{LM}(g_j) : j \in J)$. By definition, it means that for all $j \in J$, $\mathrm{LM}(g_j)$ divides $x^J$, $s \in J$ and $J$ is maximal with this property.

Similar to the idea behind $S$-polynomials, we want to eliminate the leading term of $\frac{x^J}{\mathrm{LM}(g_j)} g_s = \mathrm{LC}(g_s) x^J$. This can only be done if we multiply $\frac{x^J}{\mathrm{LM}(g_j)} g_s$ by an element of the saturated ideal $\langle \mathrm{LC}(g_i) : i \in J, i \neq s \rangle : \langle \mathrm{LC}(g_s) \rangle$. 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 $c\mathrm{LC}(g_s) \in \langle \mathrm{LC}(g_i) : i \in J, i \neq s \rangle$ so there exists $(b_i)_{i \in J \setminus \{s\}} \in A$ such that

$$c\mathrm{LC}(g_s) = \sum_{i \in J \setminus \{s\}} b_i \mathrm{LC}(g_i).$$

The $S$-polynomial associated with $J$ and $c$ is

$$c \frac{x^J}{\mathrm{LM}(g_s)} g_s - \sum_{i \in J \setminus \{s\}} b_i \frac{x^J}{\mathrm{LM}(g_i)} g_i.$$

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 $A$. 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], [18]

**Input** $F = \{f_1, \ldots, f_m\} \subseteq R \setminus \{0\}$
**Output** $G = \{g_1, \ldots, g_t\}$, a Gröbner basis of $\langle F \rangle$

$G \leftarrow F$, $\sigma \leftarrow 1$, $s \leftarrow m$
**while** $\sigma \neq s$ **do**
  $\mathcal{S} \leftarrow \{$subsets of $\{1, \ldots, \sigma\}$ saturated w.r.t. $\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_\sigma)$ which contain $\sigma\}$
  **for each** $J \in \mathcal{S}$ **do**
    $x^J \leftarrow \mathrm{lcm}(\mathrm{LM}(g_j) : j \in J)$
    $\{c_1, \ldots, c_\mu\} \leftarrow \mathsf{SatIdeal}(\{\mathrm{LC}(g_j) : j \in J \setminus \{\sigma\}\}, \mathrm{LC}(g_\sigma))$
      // $\langle c_1, \ldots, c_\mu \rangle = \langle \mathrm{LC}(g_j) : j \in J \setminus \{\sigma\} \rangle : \langle \mathrm{LC}(g_\sigma) \rangle$
    **for** $i \in \{1, \ldots, \mu\}$ **do**  // For PIDs, $\mu = 1$
      *test*, $\{b_j\}_{j \in J \setminus \{\sigma\}} \leftarrow \mathsf{LinDecomp}(\{\mathrm{LC}(g_j) : j \in J \setminus \{\sigma\}\}, c_i \mathrm{LC}(g_\sigma))$
        // *test* is TRUE and $c_i \mathrm{LC}(g_\sigma) = \sum_{j \in J \setminus \{\sigma\}} b_j \mathrm{LC}(g_j)$
      $p \leftarrow c_i \frac{x^J}{\mathrm{LM}(g_\sigma)} g_\sigma - \sum_{j \in J \setminus \{\sigma\}} b_j \frac{x^J}{\mathrm{LM}(g_j)} g_j$
      $r \leftarrow \mathsf{Reduce}(p, G)$
      **if** $r \neq 0$ **then**
        $g_{s+1} \leftarrow r$, $G \leftarrow G \cup \{g_{s+1}\}$
        $s \leftarrow s + 1$
      **end if**
    **end for**
  **end for**
  $\sigma \leftarrow \sigma + 1$
**end while**
**return** $G$

# 4 SIGNATURE BASED ALGORITHMS IN $R^m$

## 4.1 Definitions

In order to keep track of signatures we modify Def. 3.3 to introduce the notion of $s$-reduction. Recall that we only perform top reductions.

*Definition 4.1.* Let $\mathbf{p} \in R^m$. We say that we can *signature-reduce* (or *s-reduce*) $\mathbf{p}$ by $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_s \in R^m$ if we can reduce $\overline{\mathbf{p}}$ by $\overline{\boldsymbol{\beta}}_1, \ldots, \overline{\boldsymbol{\beta}}_s$ (in the sense of Def. 3.3) and $s(x^{a_i} \boldsymbol{\beta}_i) \preceq s(\mathbf{p})$ for all $i = 1, \ldots, s$, where $x^{a_i} = \frac{\mathrm{LM}(\overline{\mathbf{p}})}{\mathrm{LM}(\overline{\boldsymbol{\beta}}_i)}$. We can define similarly $s$-reduced module elements.

**Algorithm 2** Reduce (Def. 3.3)

**Input** $G = \{g_1, \ldots, g_s\} \subseteq R \setminus \{0\}$
**Output** $r$ result of reducing $p$ modulo $G$

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

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

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

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

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

Remark 4.2. *In [9, Ex. 2], a signature drop appears when 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 reduction.*

*Definition 4.3.* Let $\mathfrak{a} = \langle f_1, \ldots, f_m \rangle$ be an ideal in $R$. A finite subset $\mathcal{G}$ of $R^m$ is a *signature Gröbner basis* of $\mathfrak{a}$ if all $\mathbf{u} \in R^m$ $s$-reduce to zero w.r.t. $\mathcal{G}$.

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

Lemma 4.4 ([6, Lem. 4.6]). *Let* $\mathfrak{a}$ *be an ideal in* $R$*. If* $\mathcal{G}$ *is a signature Gröbner basis of* $\mathfrak{a}$ *then* $\{\overline{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in \mathcal{G}\}$ *is a Gröbner basis of* $\mathfrak{a}$*.*

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

*Definition 4.5.* Given a tuple of module elements $(\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s)$ and a set $J \subseteq \{1, \ldots, s\}$, the *signature* of $J$ is defined as

$$s(J) = \max_{\tau \in J} \left\{ \frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_\tau)} s(\boldsymbol{\alpha}_\tau) \right\},$$

where $x^J = \mathrm{lcm}(\mathrm{LM}(\overline{\boldsymbol{\alpha}}_i) : i \in J)$.

We say that $J$ is a *regular set* if there exists exactly one $\tau \in J$ such that $s(J) = \frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_\tau)} s(\boldsymbol{\alpha}_\tau)$. We say that $J$ is a *regular saturated set* if $J \setminus \tau$ contains all $j$ such that $\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j) \mid x^J$ and $\frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j)} s(\boldsymbol{\alpha}_j) \prec s(J)$.

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 $\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j) \mid x^J$ and $\frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j)} s(\boldsymbol{\alpha}_j) \prec s(J)$.

*Definition 4.6.* Let $(\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s)$ be a tuple of module elements. For each set $J \subseteq \{1, \ldots, \sigma\}$ containing $\sigma$, let $x^J = \mathrm{lcm}(\mathrm{LM}(\overline{\boldsymbol{\alpha}_j}) : j \in J)$ and $c$ be an element of $\langle \mathrm{LC}(\overline{\boldsymbol{\alpha}_j}) : j \in J, j \neq \sigma \rangle : \langle \mathrm{LC}(\overline{\boldsymbol{\alpha}_\sigma}) \rangle$. Let $b_j \in A, j \in J \setminus \{\sigma\}$ be such that

$$c\mathrm{LC}(\overline{\boldsymbol{\alpha}_\sigma}) = \sum_{j \in J \setminus \{\sigma\}} b_j \mathrm{LC}(\overline{\boldsymbol{\alpha}_j}).$$

Then the $S$-vectorset associated with $J$ and $c$ is defined as

$$c \frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}_\sigma})} \boldsymbol{\alpha}_\sigma - \sum_{j \in J \setminus \{\sigma\}} b_j \frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}_j})} \boldsymbol{\alpha}_j.$$

We say that an $S$-vectorset is regular if $J$ is a regular saturated set.

## 4.2 Algorithms

Algorithm SigMöller (Algo. 3) is a signature-based version of Möller's algorithm which, given an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$ where $A$ 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 $S$-vectorsets obtained from these saturated sets. At each step, it selects the next regular saturated set $J \in \mathcal{P}$ such that $J$ has minimal signature amongst elements of $\mathcal{P}$. This ensures that the algorithm computes new elements for the signature Gröbner basis with nondecreasing signatures (Lem. 4.8).

The algorithm then regular reduces these $S$-vectorsets w.r.t. the previous elements, and adds to the basis those which are not equal to 0 or 1-singular reducible. Signature-based Gröbner basis algorithms over fields typically discard all new elements which are singular reducible, but this may be too restrictive for rings. On the other hand, the proof of Lem. 4.10 justifies that 1-singular reducible module elements can be safely discarded in the computations. The correctness of the criterion for 1-singular reducibility (Algo. 4) is justified in Lem. 4.12. The correctness and termination of Algorithm SigMöller are proved in Th. 4.9 and Th. 4.13 respectively.

Due to space constraints, the subroutine RegularReduce is not explicitly written. It implements regular reduction of a module element $\mathbf{p}$ w.r.t. a set of module elements $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s\}$. 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 $\mathrm{LM}(\overline{\boldsymbol{\alpha}_j}) \mid \mathrm{LM}(\overline{\mathbf{r}})$ and $\frac{\mathrm{LM}(\overline{\mathbf{r}})}{\mathrm{LM}(\overline{\boldsymbol{\alpha}_j})} s(\boldsymbol{\alpha}_j) \prec s(\mathbf{r})$.

Remark 4.7. *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* $s(\boldsymbol{\alpha})$*. Hence the algorithm only needs to keep track of the signatures of elements, which is made possible by the restriction to regular S-vectorsets and regular reductions.*

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

**Input** $F = \{f_1, \ldots, f_m\} \subseteq R \setminus \{0\}$
**Output** $\mathcal{G} = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t\}$ signature-Gröbner basis of $\langle F \rangle$

$\mathcal{G} \leftarrow \emptyset, \sigma \leftarrow 0$
**for** $i \in \{1, \ldots, m\}$ **do**
  $\mathbf{e}_i' \leftarrow \text{RegularReduce}(\mathbf{e}_i, \mathcal{G})$
  **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**
      $J \leftarrow$ element of $J$ with minimal signature $s(J)$
      $\mathcal{P} \leftarrow \mathcal{P} \setminus \{J\}$
      $x^J \leftarrow \text{lcm}(\text{LM}(g_j) : j \in J)$
      $\tau \leftarrow$ element of $J$ with maximal $\frac{x^J}{\text{LM}(\overline{\boldsymbol{\alpha}}_\tau)} s(\boldsymbol{\alpha}_\tau)$
      $J^* \leftarrow J \setminus \{\tau\}$
      $\{c_1, \ldots, c_\mu\} \leftarrow \text{SatIdeal}(\{\text{LC}(\overline{\boldsymbol{\alpha}}_j) : j \in J^*\}, \text{LC}(\overline{\boldsymbol{\alpha}}_\tau))$
      **for** $i \in \{1, \ldots, \mu\}$ **do** // For PIDs, $\mu = 1$
        $test, \{b_j\}_{j \in J^*} \leftarrow \text{LinDecomp}(\{\text{LC}(\overline{\boldsymbol{\alpha}}_j) : j \in J^*\}, c_i \text{LC}(\overline{\boldsymbol{\alpha}}_\tau))$
        $\mathbf{p} \leftarrow c_i \frac{x^J}{\text{LM}(\overline{\boldsymbol{\alpha}}_\tau)} \boldsymbol{\alpha}_\tau - \sum_{j \in J^*} b_j \frac{x^J}{\text{LM}(\overline{\boldsymbol{\alpha}}_j)} \boldsymbol{\alpha}_j$
        $\mathbf{r} \leftarrow \text{RegularReduce}(\mathbf{p}, \mathcal{G})$
        **if** $\mathbf{r} \neq 0$ **and not** 1-SingularReducible$(\mathbf{p}, \mathcal{G})$ **then**
          $\boldsymbol{\alpha}_{s+1} \leftarrow \mathbf{r}$ // $\boldsymbol{\alpha}_{s+1}$ has signature $c_i s(J)$
          $\mathcal{G} \leftarrow \mathcal{G} \cup \{\boldsymbol{\alpha}_{s+1}\}$
          $s \leftarrow s + 1$
          $\mathcal{P} \leftarrow \mathcal{P} \cup \{\text{Reg. sat. sets of } \{1, \ldots, s\} \text{ containing } s\}$
        **end if**
      **end for**
    **end while**
  **end if**
**end for**
**return** $\mathcal{G}$

**Algorithm 4** Test of 1-singular reducibility modulo a partial signature-Gröbner basis (1-SingularReducible)

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

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

**return** $\exists j \in J, \exists k_j \in A, k_j \frac{\text{LM}(\overline{\mathbf{p}})}{\text{LM}(\overline{\boldsymbol{\alpha}}_j)} s(\boldsymbol{\alpha}_j) = s(\mathbf{p})$

## 4.3 Proof of correctness

In this section we prove the correctness of the algorithms presented in Sec. 4.2. The first result states that Algorithm SigMöller computes elements of the signature Gröbner basis in nondecreasing order on their signatures.

Lemma 4.8. *Let $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t\}$ be the value of $\mathcal{G}$ at any point in the course of Algorithm SigMöller. Then $s(\boldsymbol{\alpha}_1) \preceq s(\boldsymbol{\alpha}_2) \preceq \cdots \preceq s(\boldsymbol{\alpha}_t)$.*

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

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 $s(J_{i+1}) \succeq \frac{x^{J_{i+1}}}{\text{LM}(\overline{\boldsymbol{\alpha}}_i)} s(\boldsymbol{\alpha}_i) \succeq s(\boldsymbol{\alpha}_i)$. □

We now prove the correctness of Algorithm SigMöller. The proof follows the structure of the proof in the case of fields [20], and adapts it to Möller's algorithm over PIDs. In particular, it takes into account weak $s$-reductions instead of classical $s$-reductions. The algorithm ensures that all regular $S$-vectorsets up to a given signature $\mathbf{T}$ $s$-reduce to 0, and proving the correctness of the algorithm requires proving that this implies that all module elements with signature $\prec \mathbf{T}$ $s$-reduce to 0.

Theorem 4.9 (Correctness of Algorithm SigMöller). *Let $\mathbf{T}$ be a term of $R^m$ and let $\mathcal{G} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s) \subseteq R^m$ be a finite basis as computed by Algo. 3. Assume that all regular $S$-vectorsets $\mathbf{p}$ with $s(\mathbf{p}) \prec \mathbf{T}$ $s$-reduce to 0 w.r.t. $\mathcal{G}$ . Then $\mathcal{G}$ is a signature Gröbner basis up to signature $\mathbf{T}$.*

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

By Lem. 4.10 there is an S-vectorset $\mathbf{p}$ with $s(kx^a\mathbf{p}) = s(\mathbf{u})$ with $k \in A$, $x^a \in \text{Mon}(R)$. Also, $kx^a\mathbf{p}'$ is regular reduced where $\mathbf{p}'$ is the result of regular reducing $\mathbf{p}$.

Since $s(kx^a\mathbf{p}) = s(\mathbf{u})$ and both $kx^a\mathbf{p}'$ and $\mathbf{u}$ are regular top-reduced, we have by Lem. 4.11 that $\text{LM}(kx^a\overline{\mathbf{p}}') = \text{LM}(\overline{\mathbf{u}})$, and either $\text{LT}(kx^a\overline{\mathbf{p}}') = \text{LT}(\overline{\mathbf{u}})$, or

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

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

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

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

Since $\mathbf{p}'$ is an $S$-vectorset with $s(\mathbf{p}') \preceq s(\mathbf{u}) \prec \mathbf{T}$, $\mathbf{p}'$ is top-$s$-reducible, and so $kx^a\mathbf{p}'$ is top-$s$-reducible. So there exists $(\mu_i)_{i \in J_{\text{LM}(\overline{\mathbf{u}})}}$ terms in $R$ such that

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

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

$$\text{LT}(\overline{\mathbf{u}}) = \big(\text{LT}(\overline{\mathbf{u}}) - \text{LT}(kx^a\overline{\mathbf{p}}')\big) + \text{LT}(kx^a\overline{\mathbf{p}}') = \sum_{i \in J_{\text{LM}(\overline{\mathbf{u}})}} (m_i + \mu_i)\text{LT}(\overline{\boldsymbol{\alpha}}_i),$$

and $\mathbf{u}$ is top-$s$-reducible which is a contradiction. □

Lemma 4.10. *Let $\mathcal{G} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s) \subseteq R^m$. Let $\mathbf{u} \in R^m \setminus \{0\}$ be $s$-reduced such that $\overline{\mathbf{u}} \neq 0$. Assume that $\mathcal{G}$ is a signature Gröbner basis up to signature $s(\mathbf{u})$. Then there exists an S-vectorset $\mathbf{p}$ w.r.t. $\mathcal{G}$, such that:*

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

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

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

Since $\mathbf{u}-\mathbf{L}$ $s$-reduces to zero, there exists $(m_j)_{j\in J_{\mathrm{LM}(\overline{\mathbf{L}})}}$ terms in $R$ such that

$$\mathrm{LT}(\overline{\mathbf{u}}-\overline{\mathbf{L}}) = \sum_{j\in J_{\mathrm{LM}(\overline{\mathbf{L}})}} m_j\mathrm{LT}(\overline{\boldsymbol{\alpha}}_j) \tag{1}$$

with $m_j\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j) = \mathrm{LM}(\overline{\mathbf{u}}-\overline{\mathbf{L}})$ and $s(m_j\boldsymbol{\alpha}_j) \preceq s(\mathbf{u}-\mathbf{L}) \prec s(\mathbf{u})$ for all $i$ such that $m_j \neq 0$. Let $\sigma$ be the index of $\mathbf{e}'_i$ in $\mathcal{G}$, that is $\boldsymbol{\alpha}_\sigma = \mathbf{e}'_i$. Consider the following 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 $j \in J'$, $\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j) \mid \mathrm{LM}(\overline{\mathbf{L}}) = x^b\mathrm{LM}(\overline{\boldsymbol{\alpha}}_\sigma)$,

$$x^J = x^{J'} = \mathrm{lcm}\left\{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j) : j \in J'\right\} \mid x^b\mathrm{LM}(\overline{\boldsymbol{\alpha}}_\sigma).$$

Furthermore, looking at the leading coefficients in Eq. (1), we have

$$l\,\mathrm{LC}(\overline{\boldsymbol{\alpha}}_\sigma) = -\sum_{j\in J'} \mathrm{LC}(m_j)\mathrm{LC}(\overline{\boldsymbol{\alpha}}_j)$$

and so $l \in \langle \mathrm{LC}(\overline{\boldsymbol{\alpha}}_j) : j \in J, j \neq \sigma\rangle : \langle \mathrm{LC}(\alpha_\sigma)\rangle$. Since $A$ is a PID, this ideal is principal. Let $b_J$ be its generator, then $b_J \mid l$. Let $\mathbf{p}$ be the $S$-vectorset corresponding to $J$ and $b_J$. It is regular by construction since $J$ is a regular saturated set, and its signature is $s(\mathbf{p}) = b_J\frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_\sigma)}s(\boldsymbol{\alpha}_\sigma) = b_J\frac{x^J}{\mathrm{LM}(\overline{\mathbf{e}}'_i)}\mathbf{e}_i$. Since $b_J$ divides $l$ and $x^J$ divides $x^b\mathrm{LM}(\overline{\boldsymbol{\alpha}}_\sigma)$, $s(\mathbf{p})$ divides $lx^b s\mathbf{e}'_i = s(\mathbf{L}) = s(\mathbf{u})$.

*Existence of an S-vectorset as required.* Let $\mathbf{p}$ be an $S$-vectorset whose signature divides $s(\mathbf{u})$, and let $\mathbf{p}'$ be the regular reduced form of $\mathbf{p}$. Write $s(\mathbf{u}) = s(kx^a\mathbf{p})$, where $k \in A$ and $x^a$ is a monomial.

We can assume that $kx^c\mathbf{p}'$ is regular reducible or else we are done. We then construct an $S$-vectorset $\mathbf{q}$ such that $s(lx^b\mathbf{q}) = s(\mathbf{u})$ and $\mathrm{LM}(\overline{kx^a\mathbf{p}}) \succ \mathrm{LM}(\overline{lx^b\mathbf{q}})$. If $lx^b\mathbf{q}'$, where $\mathbf{q}'$ is obtained by regular reducing $\mathbf{q}$, is not regular reducible then we are done. Otherwise we can do the same process again and get a third $S$-vectorset 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-vectorsets.

First, we show that we can assume that $x^a \succ 1$. Indeed, assume that $a = 0$ and $k\mathbf{p}'$ is regular reducible. Since $A$ 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 $x^J \mid \mathrm{LM}(\overline{\mathbf{p}}')$. 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 $A$ 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 $S$-vectorset 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 $s(\mathbf{u})$ and is strictly divisible by $s(\mathbf{p})$. Repeating the process as needed, we obtain a strictly increasing sequence of elements dividing the coefficient of $s(\mathbf{u})$, and since $A$ is a PID and in particular a unique-factorization domain, this sequence has to be finite. So we can assume that $x^a \succ 1$.

*Constructing a singular reducer.* Since $\mathbf{p}'$ is the result of regular reducing the regular $S$-vectorset $\mathbf{p}$, either of the following situations happened:

- $\overline{\mathbf{p}}' = 0$, but this is not the case because then $kx^a\overline{\mathbf{p}}'$ would be regular reduced.
- 1-SingularReducible$(\mathbf{p}', \mathcal{G})$ is TRUE, then by Lem. 4.12, $\mathbf{p}'$ is 1-singular reducible. Then there exists $(m_i^{(1)})_{i\in J_1}$ terms in $R$, with $J_1 \subset \{1,\ldots,s\}$ and for all $i \in J_1$, $m_i^{(1)} \neq 0$, and such that
$$\mathrm{LT}(\overline{\mathbf{p}}') = \sum_{i\in J_1} m_i^{(1)}\mathrm{LT}(\overline{\boldsymbol{\alpha}}_i) \tag{2}$$
with for all $i \in J_1$, $\mathrm{LM}(m_i^{(1)}\overline{\boldsymbol{\alpha}}_i) = \mathrm{LM}(\overline{\mathbf{p}}')$. Furthermore, there exists $\tau$ in $J_1$, $m_\tau s(\boldsymbol{\alpha}_i) = s(\overline{\mathbf{p}})$ and for all $i \in J_1 \setminus \{\tau\}$, $m_i^{(1)}s(\boldsymbol{\alpha}_i) \prec s(\mathbf{p})$.
- $\overline{\mathbf{p}}'$ was added as a new element to the basis, say with index $\tau$, and we have a decomposition of $\mathrm{LT}(\overline{\mathbf{p}}')$ like in Eq. (2), with $J_1 = \{\tau\}$ and $m_\tau^{(1)} = 1$.

*Constructing a regular reducer.* Since $kx^a\mathbf{p}'$ is regular reducible, there exists $(m_i^{(2)})_{i\in J_2}$ terms in $R$, with $J_2 \subset \{1,\ldots,s\}$ and for all $i \in J_2$, $m_i^{(2)} \neq 0$, such that

$$\mathrm{LT}(kx^a\overline{\mathbf{p}}') = \sum_{i\in J_2} m_i^{(2)}\mathrm{LT}(\overline{\boldsymbol{\alpha}}_i), \tag{3}$$

and for all $j \in J_2$, $\mathrm{LM}(m_i^{(2)}\overline{\boldsymbol{\alpha}}_j) = \mathrm{LM}(kx^a\overline{\mathbf{p}}')$ and $s(m_j^{(2)}\boldsymbol{\alpha}_j) \prec s(kx^a\mathbf{p}')$.

*Constructing an S-vectorset.* Let $J = J_1 \cup J_2$, and let $m_i^{(1)} = 0$ if $i \in J_2\setminus J_1$, $m_i^{(2)} = 0$ if $i \in J_1\setminus J_2$. Note that $\tau \notin J_2$, so $m_\tau^{(2)} = 0$. Combining Eqs. (2) and (3), we obtain a decomposition of $\mathrm{LT}(kx^a m_\tau\overline{\boldsymbol{\alpha}}_\tau)$ as

$$\mathrm{LT}(kx^a m_\tau\overline{\boldsymbol{\alpha}}_\tau) = -\sum_{i\in J\setminus\{\tau\}} m_i\mathrm{LT}(\overline{\boldsymbol{\alpha}}_i).$$

where for all $i \in J$, $m_i = kx^a m_i^{(1)} - m_i^{(2)}$. Furthermore, for all $i \in J\setminus\{\tau\}$, $\mathrm{LM}(m_i\overline{\boldsymbol{\alpha}}_i) = \mathrm{LM}(x^a\overline{\mathbf{p}}') = \mathrm{LM}(x^a m_\tau\overline{\boldsymbol{\alpha}}_\tau)$ and $s(m_i\boldsymbol{\alpha}_i) \prec s(\overline{\mathbf{p}}) = s(kx^a m_\tau\overline{\boldsymbol{\alpha}}_\tau)$.

The same argument as the one used, in the first part of the proof, to construct an $S$-vectorset based on Eq. (1) yields an $S$-vectorset $\mathbf{q}$ such that $s(\mathbf{q})$ divides $s(\mathbf{u})$, say $lx^b s(\mathbf{q}) = s(\mathbf{u})$. Furthermore, since the leading term is eliminated in the construction of an $S$-vectorset, $\mathrm{LT}(lx^b\overline{\mathbf{q}}) \prec \mathrm{LT}(kx^a\overline{\mathbf{p}}')$, which concludes the proof. □

Lemma 4.11. *Let $\mathcal{G} = (\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_s)$ be a signature Gröbner basis up to signature $\mathbf{L}$.Let $\mathbf{p},\mathbf{q} \in R^m$ such that $s(\mathbf{p}) = s(\mathbf{q}) = \mathbf{L}$, and such that $\mathbf{p}$ and $\mathbf{q}$ are regular 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*

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

Proof. Let $\mathbf{r} = \mathbf{p}-\mathbf{q}$. Since $s(\mathbf{p}) = s(\mathbf{q})$, we have $s(\mathbf{r}) \prec s(\mathbf{p}) = \mathbf{L}$, and so $\mathbf{r}$ 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 $\mathrm{LM}(\overline{\mathbf{p}}) > \mathrm{LM}(\overline{\mathbf{q}})$, so $\mathrm{LM}(\overline{\mathbf{r}}) = \mathrm{LM}(\overline{\mathbf{p}})$. Since $\mathbf{r}$ is regular top-reducible and $\mathbf{p}$ is top-reduced, this is a contradiction.

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 top-reducible, $\mathrm{LC}(\overline{\mathbf{p}}) - \mathrm{LC}(\overline{\mathbf{q}}) \in C$. □

Lemma 4.12 (Correctness of 1-SingularReducible (Algo. 4)). *Let $\mathcal{G} = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s\} \subset R^m$ and $\mathbf{p} \in R^m$ such that $\mathbf{p}$ is regular reduced modulo $\mathcal{G}$ and $\mathcal{G}$ is a signature Gröbner basis up to signature $s(\mathbf{p})$. Then $\mathbf{p}$ is 1-singular reducible if and only if there exist $j \in \{1, \ldots, s\}$ and $k \in A$ and $x^a$ a monomial in $R$ such that $\mathrm{LM}(x^a\overline{\boldsymbol{\alpha}}_j) = \mathrm{LM}(\overline{\mathbf{p}})$ and $kx^a s(\boldsymbol{\alpha}_j) = s(\mathbf{p})$.*

Proof. If $\mathbf{p}$ is 1-singular 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 $\mathbf{p}$ is 1-singular reducible. If not, then $\mathrm{LM}(\overline{\mathbf{p}} - kx^a\overline{\boldsymbol{\alpha}}_j) = \mathrm{LM}(\overline{\mathbf{p}})$. Furthermore, $s(\mathbf{p} - kx^a\boldsymbol{\alpha}_j) \prec s(\mathbf{p})$, so $\mathbf{p} - kx^a\boldsymbol{\alpha}_j$ $s$-reduces to 0. In particular, there exist $(\mu_i)_{i\in\{1,\ldots,s\}}$ terms in $R$ 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 $\mu_i s(\boldsymbol{\alpha}_i) \preceq s(\mathbf{p} - kx^a\boldsymbol{\alpha}_j) \prec s(\mathbf{p})$. So putting together the two 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 reduction of $\mathbf{p}$. □

## 4.4 Proof of termination

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

Theorem 4.13. *Algorithm SigMöller terminates.*

Proof. Let $\mathcal{G} = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t, \ldots\}$ be the sequence of basis elements computed by SigMöller. In particular, for all $i \geq 1$, $\overline{\boldsymbol{\alpha}_t}$ is not reducible by $\mathcal{G}_{t-1} := \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{t-1}\}$, and all $\mathbf{v} \in R^m$ with $s(\mathbf{v}) \prec s(\boldsymbol{\alpha}_t)$ $s$-reduce to zero w.r.t. $\mathcal{G}_{t-1}$. For each $i$, let $r(\boldsymbol{\alpha}_i) = \frac{s(\boldsymbol{\alpha}_i)}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_i)}$ be the sig-lead ratio of $\boldsymbol{\alpha}_i$, they 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 $A$. 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 $s(\boldsymbol{\alpha}_j) \mid s(\boldsymbol{\alpha}_i)$ and $\mathrm{LT}(\overline{\boldsymbol{\alpha}}_j) \mid \mathrm{LT}(\overline{\boldsymbol{\alpha}}_i)$. A non-minimal module element $\boldsymbol{\alpha}_i$ is $s$-reducible by $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{i-1}\}$ ([20, Lem. 12]), and since all basis elements are regular reduced by construction, $\boldsymbol{\alpha}_i$ is singular top-reducible. In particular, there exists at least one $\boldsymbol{\alpha}_j$, $j < i$ and a monomial $m$ with $s(m\boldsymbol{\alpha}_j) \simeq s(\boldsymbol{\alpha}_i)$ and $\mathrm{LM}(m\overline{\boldsymbol{\alpha}}_j) = \mathrm{LM}(\overline{\boldsymbol{\alpha}}_i)$, 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, which is a finite amount since $R$ and $R^m$ are Noetherian.

Then we prove by induction on the finitely many non-empty sets $\mathcal{G}_r$ that each $\mathcal{G}_r$ is finite. 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 $S$-vectorset, that SigMöller regular reduced to obtain $\boldsymbol{\alpha}_t$. Then $\mathbf{p} = \sum_{j\in J} b_j \frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j)}\boldsymbol{\alpha}_j$ for $b_j \in A$, and there exists $\tau \in J$ such that for all $j \in J \setminus \{\tau\}$, $\frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j)}s(\boldsymbol{\alpha}_j) \prec \frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_\tau)}s(\boldsymbol{\alpha}_\tau)$. Also $\mathrm{LT}(\overline{\boldsymbol{\alpha}}_t) \prec \mathrm{LT}(\frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_\tau)}\overline{\boldsymbol{\alpha}}_\tau)$ and $s(\boldsymbol{\alpha}_t) = \frac{x^J}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_\tau)}s(\boldsymbol{\alpha}_\tau)$. So

$$r = \frac{s(\boldsymbol{\alpha}_t)}{\mathrm{LM}(\boldsymbol{\alpha}_t)} > \frac{s(\boldsymbol{\alpha}_\tau)}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_\tau))} > \frac{s(\boldsymbol{\alpha}_j)}{\mathrm{LM}(\overline{\boldsymbol{\alpha}}_j))}$$

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 $A$ is a PID and in particular Noetherian, with each saturated subset $J$, the algorithm only builds finitely many $S$-vectorsets (actually, it only builds one). So overall, we find that $\mathcal{G}_r$ is finite, which concludes the proof by induction. □

# 5 ELIMINATING $S$-VECTORSETS

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 $s$-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.

## 5.1 Syzygy Criterion

Syzygy criteria rely on the fact that, if the signature of an $S$-vectorset can be written as a linear combination of signatures of syzygies, then this $S$-vectorset 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 $s(\mathbf{p}) = m_{\mathbf{p}}\mathbf{e}_i$, $s(\mathbf{q}) = m_{\mathbf{q}}\mathbf{e}_j$, $i < j$ is $\overline{\mathbf{p}}\mathbf{q} - \overline{\mathbf{q}}\mathbf{p}$, and it has signature $\mathrm{LT}(\overline{\mathbf{p}})s(\mathbf{q})$;
- if a regular $S$-vectorset $\mathbf{p}$ reduces to 0, then $s(\mathbf{p})$ 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 $s(\mathbf{p})$ for each $S$-vectorset $\mathbf{p}$ reducing to 0.

For regular sequences, all syzygies are Koszul syzygies.

Proposition 5.1 (Syzygy criterion). *Assume that $\mathbf{T}$ is a signature such that all module elements with signature less than $\mathbf{T}$ $s$-reduce to 0. Let $\mathbf{p} \in R^m$ be such that there exist syzygies $\mathbf{z}_1, \ldots, \mathbf{z}_k$ and terms $m_1, \ldots, m_k$ in $R$ with $s(\mathbf{p}) = \sum_{i=1}^{k} m_i s(\mathbf{z}_i)$, and $s(\mathbf{p}) \preceq \mathbf{T}$. Then $\mathbf{p}$ regular reduces to 0.*

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

Koszul syzygies can be eliminated with the same technique, but it is more efficient to use the F5 criterion [20, Sec. 3.3].

Proposition 5.2 (F5 criterion,[3, 12]). *Let $\mathbf{p} \in R^m$ with signature $m\mathbf{e}_i$, and let $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t\}$ be a signature Gröbner basis of $\langle f_1, \ldots, f_{i-1}\rangle$. Then $\mathbf{p}$ is a Koszul syzygy if and only if $m$ is reducible modulo $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t\}$.*

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

## 5.2 Singular Criterion

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

Proposition 5.3 (Singular criterion). *Let $\mathcal{G} = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_s\}$ be a signature Gröbner basis up to signature $\mathbf{T}$. Let $\mathbf{p} \in R^m$ be such that there exists $\boldsymbol{\alpha}_i \in \mathcal{G}$ with $s(\boldsymbol{\alpha}_i) = s(\mathbf{p})$ and $s(\mathbf{p}) = s(\mathbf{T})$. Then $\mathbf{p}$ s-reduces to 0.*

Proof. Let $\mathbf{p}'$ be the result of regular reducing $\mathbf{p}$ w.r.t. $\mathcal{G}$. By construction, the basis element $\boldsymbol{\alpha}_i$ is regular reduced w.r.t. $\mathcal{G}$. So by Lem. 4.11, $\mathrm{LM}(\overline{\mathbf{p}'}) = \mathrm{LM}(\overline{\boldsymbol{\alpha}_i})$, and applying Lem. 4.12, with $k = 1$ and $x^a = 1$, shows that $\mathbf{p}'$ is 1-singular reducible. The result of that reduction has signature $\prec s(\mathbf{p}) = \mathbf{T}$, so it $s$-reduces to 0. □

# 6 IMPLEMENTATION

We have written a toy implementation of Möller's algorithm, with and without signature[1], with the F5 and Singular criteria. We provide functions LinDecomp and SatIdeal for Euclidean rings, for fields and for multivariate polynomial rings.

To the best of our knowledge, there is no reference implementation of Möller's algorithm, so no relevant comparisons of computation time can be done. Instead, we give data about the number of considered $S$-vectorsets, saturated sets and reductions to 0 in each algorithm, on two small examples (Tab. 1 and 2)[2].

Running Möller's algorithm on larger examples would require further 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 Buchberger's algorithm [1, Sec. 4.4], which may allow to run the algorithms considering only pairs instead of arbitrary tuples of polynomials. It may also be possible to compute saturated sets in a similar way to F4's selection technique, reducing the associated overhead.

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 gives correct output. Understanding the behavior of the algorithms over UFDs or even more general rings will be the focus of future research.

**Acknowledgements** The authors thank Manuel Kauers for his valuable insights and comments during the elaboration of this work.

| Algorithm | $S$-vectorsets | Sat. sets | Red. to 0 | Time |
|---|---|---|---|---|
| Möller | 707 | 707 | 687 | 41.2 s |
| SigMöller | 90 | 90 | 81 | 6.8 s |
| — with F5 and Singular crit. | 9 | 90 | 0 | 6.7 s |

**Table 1: Computation of a GB of $\langle 3xy+7yz, 4y^2-5xz, x-2y+z\rangle$ in $\mathbb{Z}[x,y,z]$**

| Algorithm | $S$-vectorsets | Sat. sets | Red. to 0 | Time |
|---|---|---|---|---|
| Möller[3] | >800 | >800 | | >6h |
| SigMöller | 279 | 279 | 255 | 197.5 s |
| — with F5 and Singular crit. | 20 | 211 | 0 | 98.2s |

**Table 2: Computation of a GB of $\langle 3xy+7yz, 4y^2-5xz, x^2-2yz+z^2\rangle$ in $\mathbb{Z}[x,y,z]$**

# REFERENCES


[1] Adams, W. & Loustaunau, P. (1994). *An Introduction to Gröbner Bases.* American Mathematical Society.

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

[3] Bardet, M., Faugère, J.-C. & Salvy, B. (2015). On the Complexity of the $F_5$ Gröbner Basis Algorithm. *J. Symbolic Comput.* **70**, 49–70. URL https://doi.org/10.1016/j.jsc.2014.09.025.

[4] Bosma, W., Cannon, J. & Playoust, C. (1997). The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24**(3-4), 235–265. URL http://dx.doi.org/10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993).

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

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

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

[8] Eder, C. & Perry, J. (2011). Signature-based Algorithms to Compute Gröbner Bases. In: *Proceedings of the 36th international symposium on Symbolic and algebraic computation.* ACM.

[9] Eder, C., Pfister, G. & Popescu, A. (2017). On Signature-Based Gröbner Bases over Euclidean Rings. In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17. New York, NY, USA: ACM. URL http://doi.acm.org/10.1145/3087604.3087614.

[10] Eder, C. & Roune, B. H. (2013). Signature Rewriting in Gröbner Basis Computation. In: *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation.* ACM.

[11] Faugère, J.-C. (1999). A New Efficient Algorithm for Computing Gröbner Bases (F4). *Journal of Pure and Applied Algebra* **139**(1), 61–88.

[12] Faugère, J. C. (2002). 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. New York, NY, USA: ACM. URL http://doi.acm.org/10.1145/780506.780516.

[13] Francis, M. & Dukkipati, A. (2017). On Ideal Lattices, Gröbner Bases and Generalized Hash Functions. *Journal of Algebra and Its Applications* URL http://www.worldscientific.com/doi/abs/10.1142/S0219498818501128.

[14] Gao, S. & Guan, F., Y.and Volny IV (2010). A New Incremental Algorithm for Computing Gröbner bases. In: *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ISSAC '10. ACM. URL http://doi.acm.org/10.1145/1837934.1837944.

[15] Kandri-Rody, A. & Kapur, D. (1988). Computing a Gröbner Basis of a Polynomial Ideal over a Euclidean Domain. *J. Symbolic Comput.* **6**(1), 37–57. URL https://doi.org/10.1016/S0747-7171(88)80020-8.

[16] Lichtblau, D. (2012). Effective Computation of Strong Gröbner Bases over Euclidean Domains. *Illinois J. Math.* **56**(1), 177–194 (2013). URL http://projecteuclid.org/euclid.ijm/1380287466.

[17] Lichtblau, D. (2013). Applications of Strong Gröbner Bases over Euclidean Domains. *Int. J. Algebra* **7**(5-8), 369–390. URL https://doi.org/10.12988/ija.2013.13037.

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

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

[20] Roune, B. H. & Stillman, M. (2012). Practical Gröbner Basis Computation. In: *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation.* ACM.

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


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

[2] Computations were run on a laptop (Intel Celeron N2830 @ 2.16GHz, 2GB memory).

[3] Algo. Möller ran out of memory.