A Signature-based Algorithm for Computing the Nondegenerate Locus of a Polynomial System*

Christian Eder † Pierre Lairez ‡ Rafael Mohr †§ Mohab Safey El Din §

July 25, 2022

Abstract

Polynomial system solving arises in many application areas to model non-linear geometric properties. In such settings, polynomial systems may come with degeneration which the end-user wants to exclude from the solution set. The nondegenerate locus of a polynomial system is the set of points where the codimension of the solution set matches the number of equations.

Computing the nondegenerate locus is classically done through ideal-theoretic operations in commutative algebra such as saturation ideals or equidimensional decompositions to extract the component of maximal codimension.

By exploiting the algebraic features of signature-based Gröbner basis algorithms we design an algorithm which computes a Gröbner basis of the equations describing the closure of the nondegenerate locus of a polynomial system, without computing first a Gröbner basis for the whole polynomial system.

1 Introduction

Problem Statement Fix a field \( K \) with an algebraic closure \( \overline{K} \) and a polynomial ring \( R := \mathbb{K}[x_1, \ldots, x_n] \) over \( \mathbb{K} \). Let \( f_1, \ldots, f_c \in R \) and \( V := \{ p \in \overline{K}^n \mid f_1(p) = \cdots = f_c(p) = 0 \} \). Further define the ideal \( I := \langle f_1, \ldots, f_c \rangle = \{ \sum_{i=1}^{c} q_i f_i \mid q_i \in R \} \). The algebraic set \( V \) is a finite union of irreducible components. By the Principal Ideal Theorem [21, Theorem 10.2] the codimension of the \( K \)-irreducible components of \( V \) is at most \( c \). Let \( V_c \) denote the union of the components of \( V \) of codimension exactly \( c \). In particular \( V_c = \emptyset \) when \( c > n \).

The goal of this paper is to compute a Gröbner basis of an ideal whose zero set is \( V_c \), which we call the nondegenerate locus of the system \( f_1, \ldots, f_c \) (note that we may not compute a radical ideal).

Prior works and scientific locks. State-of-the-art algorithms to compute the nondegenerate locus of \( f_1, \ldots, f_c \) rely on the more general problem of computing the equidimensional decomposition of the ideal that they generate. There is a vast body of literature split along what data structure is used for the output into two research lines.

The first family of algorithms computes a Gröbner basis of the ideal of each component. There are two different approaches in this line. The first uses projections, computed with elimination orderings, to reduce

---

*This work has been supported by European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Actions, grant agreement 813211 (POEMA) by European Research Council under the European Union’s Horizon Europe research and innovation programme, grant agreement 101040794 (10000 DIGITS); by the joint ANR-FWF grant ANR-19-CE48-0015 (ECARP), the ANR grant ANR-19-CE40-0018 (De Rerum Natura), the DFG Sonderforschungsbereich TRR 195, and the Forschunginitiative Rheinland-Pfalz.

†TU Kaiserslautern, Germany
‡Inria, Univ. Paris-Saclay, Palaiseau, France
§Sorbonne Uni., CNRS, Paris, France
the problem to a problem for hypersurfaces [5, 26, 34]. The second relies on homological characterizations of the dimension and the computation of free resolutions [22]. See [14, 30, 43] and references therein for further references. Both approaches use Gröbner basis algorithms as a black box for performing various ideal-theoretic operations, in particular ideal quotients (also known as colon ideals).

A second family of algorithms outputs equidimensional components of $I$ or its radical through lazy representations, i.e. as complete intersections over a non-empty Zariski open set. This is the case for the so-called regular chains which go back to Wu-Ritt characteristic sets [10].

These put into practice a kind of D5 principle [17] to split geometric objects by enforcing an equiprojectability property. See [1, 11, 31, 37, 44, 45] and references therein for further references. When the base field $\mathbb{K}$ has characteristic 0 (or large enough characteristic), geometric resolution algorithms [27] can also be used. These culminate with the incremental algorithm in [33, 36] which avoids equiprojectability issues by performing a linear change of variables to ensure Noether position properties. One feature is that input polynomials are encoded with straight-line programs to take advantage of evaluation properties. See also [33] for a similar approach. It also gives the best known complexity for equidimensional decomposition: linear in the evaluation complexity of the input system and polynomial in some algebraic degree.

As software, the computer algebra systems Singular [16], Macaulay2 [29] and Magma [5] implement the algorithm of [22] to perform equidimensional decomposition. Maple implements algorithms for computing regular chains [5, 3, 12, 13, 38] and algorithms based on Gröbner bases. The algorithm by Gianni et al. [26] is used for prime decomposition and, combined with techniques from [2], for equidimensional decomposition. All these implementations use Gröbner basis algorithms as a black box.

**Main results** By contrast with previous work, we only focus on computing the nondegenerate locus of a system, not the full equidimensional decomposition of the corresponding ideal. The main difference to other Gröbner basis based techniques to compute equidimensional decompositions is that we enlarge $I$ while a Gröbner basis for $I$ is computed and return a Gröbner basis of a nondegenerate locus of $I$ when this Gröbner basis computation is finished. Modifying or splitting the ideal in question in the middle of Gröbner basis algorithms is a natural and appealing idea [e.g. 28].

This idea requires one to answer (i) when the ideal in question should be enlarged and (ii) how to minimize the cost of enlarging the ideal in question. The algorithm we propose taclest both issues.

We tackle problem (i) by following the incremental structure of the sGB algorithms on which our work is based [24, 25]. We describe this sGB algorithm in section 3. Incremental means here that these algorithms proceed by computing first a Gröbner basis for $\langle f_1, f_2 \rangle$ then use the result to compute a Gröbner basis for $\langle f_1, f_2, f_3 \rangle$ and so on. In addition, sGB algorithms keep track of an auxiliary data structure, called a signature, which is attached to each considered polynomial. This enables one to exclude certain polynomials from the set of polynomials to be processed by reduction in Buchberger’s algorithm.

As a consequence they have the feature that, having computed a Gröbner basis for $I_{i-1} := \langle f_1, \ldots, f_{i-1} \rangle$, a reduction to zero happens in the Gröbner basis computation for $I_i$ if any only if $f_i$ is a zero divisor modulo $I_{i-1}$. In this case $V_{i-1} := V(I_{i-1})$ has irreducible components on which $f_i$ is identically zero (the union of which is henceforth denoted $V_{i-1, f_i=0}$) and components which are not contained in the hypersurface $V(f_i)$ (the union of which is henceforth denoted $V_{i-1, f_i \neq 0}$). Assuming that $V(I_{i-1})$ is equidimensional of codimension $i - 1$, to compute an ideal representing the nondegenerate locus of $V(I_i)$ we may then proceed as follows (see Algorithm 1):

1. Compute ideals representing $V_{i-1, f_i=0}$ and $V_{i-1, f_i \neq 0}$ (via the ideal-theoretic operation of saturation).
2. Compute an ideal representing $W := V_{i-1, f_i \neq 0} \cap V(f_i)$.
3. Remove from $W$ all components contained in $V_{i-1, f_i=0}$ (again via saturation).
Iterating over the set of input equations with these three steps, using the result of each iterative step as input for the next invocation of this loop and slightly adapting the third step to remove all components which are contained in components of higher dimension then yields an ideal representing the nondegenerate locus of \( I \). We describe this algorithm from a purely algebraic perspective in section \( \text{[2]} \).

To tackle problem \( (ii) \) we exploit a feature of the incremental sGB algorithms first captured in the G2V algorithm \([22]\). The data of a signature can be enlarged so as to simultaneously compute a Gröbner basis for \( I \) and the quotient ideal \( \langle I_{i-1} : f_i \rangle := \{ g \in R \mid g f_i \in I_{i-1} \} \) (which, if \( I_{i-1} \) is a radical ideal, corresponds precisely to \( V(I_{i-1,f_i}) \}) in each incremental step.

Using this idea we modify the baseline sGB algorithm we use to simultaneously perform steps 1 and 2 of the above loop (i.e. in a single Gröbner basis computation). This is done essentially by immediately inserting an element \( g \in \langle I_{i-1} : f_i \rangle \) once it is identified during the run of the sGB algorithm. We manage this insertion of elements that do not lie in the original ideal \( I \) with a data structure we call an sGB tree (see section \( \text{[3]} \) which allows us to perform this modification with the needed technical properties of signatures ensured. This yields a signature-based version of Algorithm \([1]\) Algorithm \([8]\). Besides managing the insertion of new generators into some initial ideal, the sGB data structure also leaves open the future possibility of designing signature-based ideal decomposition algorithms.

We finally show experimentally in section \( \text{[5,2]} \) that the consequence of this simple modification is a massive cost reduction in the overhead compared to a “naive” implementation of Algorithm \([1]\) where one uses saturation procedures as a blackbox. As is also shown, it additionally enables us to compute the nondegenerate locus of systems which are out of the reach of equidimensional decomposition algorithms available in state of the art computer algebra systems.

### 2 The basic algorithm

Consider a codimension \( k \) irreducible variety \( X \subseteq \mathbb{R}^n \) and a polynomial \( f \in R \). Either \( X \subseteq V(f) \), and so \( X \cap V(f) = X \), or \( X \cap V(f) \) is equidimensional of codimension \( k+1 \) (that is, all the irreducible components of \( X \cap V(f) \) have codimension \( k+1 \)). If \( X \) is not irreducible, then \( X \cap V(f) \) may not be equidimensional. Yet, the alternative above applies to each irreducible component of \( X \). The components of \( X \) which are not included in \( V(f) \) are exactly the components of the closure of \( X \setminus V(f) \), while the components of \( X \) which included in \( V(f) \) are exactly the components of the closure of \( X \setminus (X \setminus V(f)) \). This leads to the decomposition of \( X \cap V(f) \) as the union of two equidimensional varieties of codimension \( k \) and \( k+1 \) respectively:

\[
X = \left( X \setminus X \setminus V(f) \right) \cup \left( X \setminus V(f) \cap V(f) \right).
\]

This is the basic identity that we leverage to compute, incrementally, the codimension \( c \) components of an ideal \( \langle f_1, \ldots, f_c \rangle \). In an ideal theoretic language, this reformulates as follows.

For two ideals \( I, J \subseteq R \), we write \( I \sqsubseteq J \) for the equality of the radicals \( \sqrt{I} = \sqrt{J} \). An ideal \( I \) is equidimensional if all the irreducible components of \( V(I) \) have the same dimension. Recall that \( I : J \) is the ideal \( \{ p \in R \mid pJ \subseteq I \} \). Recall also that \( I : J^k \) yields an increasing sequence of ideals as \( k \to \infty \), so it eventually stabilizes in an ideal denoted \( I : J^\infty \), the saturation of \( I \) by \( J \). If \( J \) is generated by a single element \( f \), it is simply denoted \( I : f^\infty \).

**Lemma 2.1.** For any ideal \( J \subseteq R \) and any \( f \in R \) we have

\[
J + \langle f \rangle \sqsubseteq \langle J : f^\infty \rangle.
\]

Moreover, if \( J \) is equidimensional of codimension \( c < n \) and if \( f \notin \sqrt{J} \) then \( \langle J : f^\infty \rangle + \langle f \rangle \) is equidimensional of codimension \( c+1 \) and \( J : (J : f^\infty) \) is equidimensional of codimension \( c \).
Algorithm 1 Computation of the nondegenerate locus

Input: A set of generators \( f_1, \ldots, f_c \) for an ideal \( I \) in \( R \) where \( c \leq n \)
Output: A set of generators \( G \) for the nondegenerate part of \( f_1, \ldots, f_c \)

1: \( J \leftarrow 0 \), as an ideal of \( R \)
2: \( K \leftarrow \varnothing \)
3: for \( k \in \{1, \ldots, c\} \) do
  4: \( H \leftarrow J : f_k^\infty \)
  5: \( K \leftarrow K \cup \{ J : H \} \)
  6: \( J \leftarrow H + \langle f_k \rangle \)
  7: for \( K \in K \) do
  8: \( J \leftarrow J : K^\infty \)
  9: end for
10: end for
11: return \( J \)

Proof. For the left-to-right inclusion, it is clear that \( J \) is included in the right-hand side, so it remains to check that \( f \) is in the radical of both terms of the intersection. It is obvious that \( f \in (J : f^\infty) + \langle f \rangle \), so it remains to prove that \( f \) is in the radical of \( J : (J : f^\infty) \). So let \( g \in J : f^\infty \), that is \( g f^\ell \in J \) for some \( \ell \geq 0 \), which we may rewrite as \( f \in \sqrt{J : g} \). To conclude, we observe that
\[
\sqrt{J : (J : f^\infty)} = \bigcap_{g \in J : f^\infty} \sqrt{J : g},
\]
so \( f \in \sqrt{J : (J : f^\infty)} \).

Conversely, let \( p \in ((J : f^\infty) + \langle f \rangle) \cap (J : (J : f^\infty)) \). Write \( p = q + af \) where \( q \in (J : f^\infty) \) and \( a \in R \). Since \( p \in (J : (J : f^\infty)) \), we have \( pq \in J \). But \( pq = q^2 + aqf \), so \( q^2 \in J + \langle f \rangle \). It follows that \( q \in \sqrt{J + \langle f \rangle} \), thus proving the stated equality.

For the statement on equidimensionality, we may rely on the geometric interpretation above: the zero set of \( J : f^\infty + \langle f \rangle \) is \( X \setminus V(f) \cap V(f) \), where \( X = V(J) \). The equidimensionality of \( J : (J : f^\infty) \) is slightly more technical because the geometric interpretation only gives information on \( J : (J : f^\infty) \). Yet, both are equal up to radical: \( V(J : (J : f^\infty)) \) is the union of the component of \( V(J) \) that are included in \( V(f) \) \cite[Proposition 23]{33}.

We are now ready to describe Algorithm \[1\]. To do this we suppose for now that we have an algorithm for computing the quotient ideal \( J : K \) and the saturation \( J : K^\infty \), given generators for \( J \) and \( K \). Given \( c \leq n \) elements \( f_1, \ldots, f_c \in R \) the core loop of Algorithm \[1\] starts with the ideal \( J = \langle f_1 \rangle \) and to continuously replace it with \( (J : f_k^\infty) + f_k \) for each \( k \). By Lemma \[24\] the resulting ideal will be equidimensional of codimension \( c \).

Example 2.2. Let \( R = k[x, y, z] \) and \( f_1 = xy, f_2 = xz \). Then \( (xy : xz^\infty) + xz = \langle y, xz \rangle \) which has the component \( \langle y, x \rangle \) which is not a component of \( \langle f_1, f_2 \rangle = \langle x \rangle \cap (y, z) \).

To prove the correctness of Algorithm \[1\] we also need the following proposition:

Lemma 2.3. For any ideals \( I, J \subseteq R \) and any \( f \in R \), we have
\[(i) \ (I \cap J) + \langle f \rangle = (I + \langle f \rangle) \cap (J + \langle f \rangle));\]
Theorem 2.4. On input \( J \) we prove by induction on \( i \):

(ii) \( I \cap J^\rad = (I : J^\infty) \cap J \);

(iii) if \( f \in I \), then \( I : J^\infty = I : (J + \langle f \rangle)^\infty \).

Proof. For the first item,

\[
(I + \langle f \rangle) \cap (J + \langle f \rangle)^\rad = (I + \langle f \rangle)(J + \langle f \rangle)^\rad IJ + \langle f \rangle^\rad (I \cap J) + \langle f \rangle.
\]

For the second one, the left-to-right inclusion is clear. Conversely, let \( f \in (I : J^\infty) \cap J \) and let \( k > 0 \) such that \( f J^k \in I \). In particular, \( f^{k+1} \in I \). So \( f \in \sqrt{I} \).

For the last item is trivial from the definition of saturation. \( \square \)

Theorem 2.4. On input \( f_1, \ldots, f_c \in R \) with \( c \leq n \), Algorithm \( \square \) terminates and outputs an ideal \( J \) such that \( V(J) \) is the nondegenerate locus of the input system.

Proof. We define \( J_0 := (0) \), and then, by induction on \( i \),

\[
K_i := (J_i-1 : (J_i-1 : f_i^\infty)),
\]

and \( J_i := ((J_i-1 : f_i^\infty) + \langle f_i \rangle : (\prod_{j=1}^{i} K_j)^\infty) \).

It is clear that Algorithm \( \square \) returns the ideal \( J_c \). Now, let \( I_i = \langle f_1, \ldots, f_i \rangle \). The main loop invariant, that we prove by induction on \( i \), is

\[
I_i \equiv J_i \cap \bigcap_{j=1}^{i} (K_j + \langle f_{j+1}, \ldots, f_i \rangle).
\] (1)

From this, we deduce that the zero set of \( J_c \) is contained in the algebraic set defined by \( f_1 = \cdots = f_c = 0 \). We will prove later that \( J_c \) is equidimensional of codimension \( c \), that the components of the ideals \( (K_j + \langle f_{j+1}, \ldots, f_c \rangle) \) have codimension less than \( c \) and do not contain any components of \( J_c \).

It is trivially true that (1) holds for \( i = 0 \). For \( i > 0 \), we have

\[
I_i = I_{i-1} + \langle f_i \rangle = J_{i-1} \cap \bigcap_{j=1}^{i-1} (K_j + \langle f_{j+1}, \ldots, f_i \rangle) + \langle f_i \rangle
\]

\[
\rad (J_{i-1} + \langle f_i \rangle) \cap \bigcap_{j=1}^{i-1} (K_j + \langle f_{j+1}, \ldots, f_i \rangle), \quad \text{by Lemma 2.3.1}
\]

Besides, by Lemma 2.4,

\[
J_{i-1} + \langle f_i \rangle^\rad = ((J_{i-1} : f_i^\infty) + \langle f_i \rangle) \cap (J_{i-1} : f_i^\infty)
\]

\[
= ((J_{i-1} : f_i^\infty) + \langle f_i \rangle) \cap K_i.
\]

For short, let \( J'_i = (J_{i-1} : f_i^\infty) + \langle f_i \rangle \). Combining the equalities above, we have

\[
I_i \equiv J'_i \cap \bigcap_{j=1}^{i} (K_j + \langle f_{j+1}, \ldots, f_i \rangle)
\]

\[
\equiv \left( J'_i : (\prod_{j=1}^{i} K_j)^\infty \right) \cap \bigcap_{j=1}^{i} (K_j + \langle f_{j+1}, \ldots, f_i \rangle),
\]
we conclude that \( V_j \) for observed that its zero set is contained in the one defined by the input polynomials \( J \). Indeed, using Lemma 2.1, we check by induction on \( i \) that \( J_i \) is equidimensional of codimension \( i \) (unless \( J_i = \{ 1 \} \)) and that \( K_i \) is equidimensional of codimension \( i - 1 \) (unless \( K_i = \{ 1 \} \)). It follows that all the components of \( K_j + (f_{j+1}, \ldots, f_r) \) have codimension at most \( i - 1 \). Moreover, no component of \( J_i \) is included in any \( K_j \), for \( j \leq i \), since \( J_i \) is saturated by the \( K_j \). Therefore, using (1), the codimension \( i \) components of \( I_i \) are exactly the components of \( J_i \).

Hence, we deduce that \( J_i \) is equidimensional of codimension \( c \) whose components are not contained in the ones of \( K_j + (f_{j+1}, \ldots, f_r) \), the components of which have codimention less than \( c \). Besides, we already observed that its zero set is contained in the one defined by the input polynomials \( f_1, \ldots, f_c \). Since (1) holds, we conclude that \( V(J_i) \) is the nondegenerate locus of the input system.

\[ \square \]

3 Signature-based Gröbner basis computations

We will rely on the theory of signature-based Gröbner bases in order to implement efficiently Algorithm 1.

3.1 Signatures and extended sig-poly pairs

We fix in the following a monomial order on \( R \) and a sequence of polynomials \( f_1, \ldots, f_r \in R \). Let \( I := \langle f_1, \ldots, f_r \rangle \) and \( J_i := \langle 1, \ldots, f_i \rangle \). We describe an algorithm which computes simultaneously a Gröbner basis for \( I \) and presents the following features:

1. It computes a Gröbner basis for \( I \) incrementally, i.e. first for \( \langle f_1 \rangle \) then for \( \langle f_1, f_2 \rangle \) etc.
2. It simultaneously computes Gröbner bases for each ideal \( \langle f_1, \ldots, f_{i-1} : f_i \rangle \), \( i = 2, \ldots, r \).

This algorithm belongs to the class of so called signature based Gröbner basis algorithms, the first of which was the F5 algorithm presented in [24]. Since then the class of signature-based algorithms has been greatly extended, see [18] for a survey. The idea of leveraging signature-based algorithms to compute simultaneously some colon ideals first appeared in [25]. The algorithm we present here is closely related, with some elements from the F5 algorithm. The algorithm presented in this section is fully encompassed by the general algorithmic framework presented in [18].

We start by defining signatures.

**Definition 3.1.** A signature is a pair \( \sigma = (i, n) \) of an index in \( \{1, \ldots, r\} \) and a monomial in \( R \). The first component is called the index, and denoted \( \text{ind}(\sigma) \). The second component is called the monomial part of \( \sigma \).

We order the signatures lexicographically, i.e. by writing

\[(i, m) < (j, n) \iff i < j \text{ or } i = j \text{ and } m < n.\]

The product of a monomial \( a \in R \) and a signature \( \sigma = (i, h) \) is defined by \( a \sigma = (i, ah) \). A signature \( \sigma \) divides another signature \( \tau \) if there is a monomial \( a \) such that \( a \sigma = \tau \), in particular \( \text{ind}(\sigma) = \text{ind}(\tau) \).

The possible indices of a signature are the indices of the input equations. This relation between the index of a signature and one of the equations \( f_i \) is made stronger by the following object:

**Definition 3.2.** An extended sig-poly pair is a triple \( \alpha = (f, \sigma, h) \), where \( f, h \in R \) and \( \sigma \) is a signature such that \( h \sigma = \text{ind}(\sigma) \) is equal to the monomial part of \( \sigma \). The first component \( f \) is called the polynomial part of \( \alpha \), denoted \( \text{poly}(\alpha) \), the second component \( \sigma \) is called the signature, denoted \( \sigma(\alpha) \), and the third component is called the quotient, denoted \( \text{quo}(\alpha) \). The index of \( \alpha \), denoted \( \text{ind}(\alpha) \) is the index of its signature. We further impose that

\[ \text{poly}(\alpha) = \text{quo}(\alpha) f_{\text{ind}(\alpha)} \in I_{\text{ind}(\alpha)-1}. \]  

(2)
The product of a monomial $a \in R$ and an extended sig-poly pair $\gamma$ is defined by

$$\text{poly}(aa) = \text{poly}(a), \quad s(aa) = as(a), \quad \text{and} \quad \text{quo}(aa) = a \text{quo}(a).$$

The concept of an S-pair from Buchberger’s algorithm extends to extended sig-poly pairs. Given two extended sig-poly pairs $\alpha$ and $\beta$ with $s(\alpha) > s(\beta)$ let $c = \text{lcm}(\text{lm}(\text{poly}(\alpha)), \text{lm}(\text{poly}(\beta)))$, $a = c/\text{lt}(\text{poly}(\alpha))$ and $b = c/\text{lt}(\text{poly}(\beta))$, then define the S-pair of $\alpha$ and $\beta$, denoted $sp(\alpha, \beta)$ by

$$\text{poly}(sp(\alpha, \beta)) = \text{poly}(\alpha) - b \text{poly}(\beta), \quad s(sp(\alpha, \beta)) = \max(s(\alpha a), s(b\beta)),$$

and

$$\text{quo}(sp(\alpha, \beta)) = \begin{cases} a \text{quo}(\alpha) & \text{if ind}(\alpha) > \text{ind}(\beta), \\ a \text{quo}(\alpha) - b \text{quo}(\beta) & \text{if ind}(\alpha) = \text{ind}(\beta). \end{cases}$$

In particular, the polynomial part of $sp(\alpha, \beta)$ is the usual S-pair of $\text{poly}(\alpha)$ and $\text{poly}(\beta)$. We say that $\alpha$ and $\beta$ form a regular S-pair if $s(aa) \neq s(b\beta)$. (We will only consider such S-pairs.) It is easy to check that Invariant (2) is preserved.

The regular reduction of an extended sig-poly pair $\alpha$ with respect to a set $G$ of sig-poly pairs is defined to be the output of Algorithm 2. The procedure tries to reduce the leading term of $\text{poly}(\alpha)$ using some multiple $b\beta$ of an extended sig-poly pair $\beta \in G$ such that $bs(\beta) < s(\alpha)$. The procedure stops when there is no such reducer. Compared to the usual division algorithm in polynomial rings, only reduction by lower signature elements is allowed. Moreover, there is some extra computations to preserve Invariant (2).

We may now describe a variant of Buchberger’s using extended sig-poly pairs and regular reduction, see Algorithm 3. In line 6 we always choose the S-pair with minimal signature for reduction, and signatures are ordered first by indices. As a result, signatures are processed in index 1 (which may produce further S-pairs with index $\geq 1$), then in index 2 (which may produce further S-pairs with index $\geq 2$), etc. So a Gröbner basis for $I$ is computed incrementally: first for $\langle f_1 \rangle$, then for $\langle f_1, f_2 \rangle$ etc. Computing with extended sig-poly pairs makes it possible to simultaneously compute a Gröbner basis for $I$ and for all the ideals $\langle f_1, \ldots, f_{i-1} : f_i \rangle$ for $i = 2, \ldots, r$. Indeed, if for an extended sig-poly pair $\gamma$ we find during the run of Algorithm 3 that $\text{poly}(\gamma) = 0$, then $\text{quo}(\gamma)$ is an element of the quotient ideal $I_{\text{ind}(\gamma)-1} : f_{\text{ind}(\gamma)}$, in view of Definition 2.

---

**Algorithm 2: Regular reduction**

1. procedure **RegularReduction**(\(\alpha, G\))
2. \(f \leftarrow \text{poly}(\alpha)\)
3. \(h \leftarrow \text{quo}(\alpha)\)
4. while \(\{\beta \in G \mid \text{lm}(\text{poly}(\beta)) \text{ divides } \text{lm}(f)\} \neq \emptyset\) do
5. \(\beta \leftarrow \text{some element of } \{\beta \in G \mid \text{lm}(\text{poly}(\beta)) \text{ divides } \text{lm}(f)\}\)
6. \(b \leftarrow \text{lt}(\text{poly}(\beta))/\text{lt}(f)\)
7. if \(bs(\beta) < s(\alpha)\) then
8. \(f \leftarrow f - b \text{poly}(\beta)\)
9. if \(\text{ind}(\beta) = \text{ind}(\alpha)\) then
10. \(h \leftarrow h - b \text{quo}(\beta)\)
11. end if
12. end if
13. end while
14. return \((f, s(\alpha), h)\)
15. end procedure
Algorithm 3 Buchberger with signatures

Input: $f_1, \ldots, f_r \in R$
Output: Gröbner bases of $\langle f_1, \ldots, f_r \rangle$ and of $\langle f_1, \ldots, f_{k-1} \rangle : f_k$ ($1 \leq k \leq r$)

1: procedure BUCHBERGER($f_1, \ldots, f_r$)
2: $G \leftarrow \{e_i \mid 1 \leq i \leq r\}$
3: $S_1, \ldots, S_r \leftarrow \emptyset$
4: $P \leftarrow \{\{\alpha, \beta\} \mid \alpha, \beta \in G\}$ form a regular S-pair
5: while $P \neq \emptyset$ do
6: $(\alpha, \beta) \leftarrow$ the pair in $P$ with $s(sp(\alpha, \beta))$ minimal
7: $P \leftarrow P \setminus \{\{\alpha, \beta\}\}$
8: $\gamma \leftarrow$ REGULARREDUCTION($sp(\alpha, \beta), G$)
9: $G \leftarrow G \cup \{\gamma\}$
10: if $\text{poly}(\gamma) \neq 0$ then
11: $P \leftarrow P \cup \{\{\gamma, \beta\} \mid \beta \in G\}$ forms a regular S-pair with $\gamma\}$
12: else (record the quotient of the zero reduction)
13: $S_{\text{ind}(\gamma)} \leftarrow S_{\text{ind}(\gamma)} \cup \{\text{quo}(\gamma)\}$
14: end if
15: end while
16: return $\{\text{poly}(\beta) \mid \beta \in G\}, S_1, \ldots, S_r$
17: end procedure

Proposition 3.3. On input $f_1, \ldots, f_r \in R$, Algorithm 3 terminates and the set $\{\text{poly}(\alpha) \mid \alpha \in G\}$ is a Gröbner basis of the ideal $\langle f_1, \ldots, f_r \rangle$. The sets $S_i$ are Gröbner bases of the ideals $\langle f_1, \ldots, f_i-1 \rangle : f_i$ for each $i = 2, \ldots, r$.

We skip the proof as we will only rely on the stronger Theorem 3.5 below.

3.2 From Buchberger to sGB

The signature and the quotient of each extended sig-poly pair in the data makes it possible to compute the colon ideals $\langle f_1, \ldots, f_{i-1} \rangle : f_i$ as a by-product of an incremental computation of a Gröbner basis of $\langle f_1, \ldots, f_r \rangle$. Moreover, this is the discovery of Faugère [24], signatures make it possible to discard many S-pairs while preserving the essential properties of Algorithm 3. The overarching principle is the following: at most one sig-poly pair has to be regular-reduced at each signature. This is made precise by the following statement.

Lemma 3.4 ([24, Lemma 4]). In the course of Algorithm 3 assume that only $S$-pairs in signature $\geq \sigma := (i, m)$ are left in $P$. Then for any extended sig-poly pairs $\gamma$ and $\gamma'$ with $s(\gamma) = s(\gamma') = \sigma$,

$$\text{REGULARREDUCTION}(\gamma, G) = \text{REGULARREDUCTION}(\gamma', G)$$

This leads to Algorithm 5. It is similar to Algorithm 3, the only difference is the check on line 9, the rewritability check, which trim many computations. At a given signature, this check will retain at most one element of $P$. The condition on line 7 discards even more S-pairs by predicting that they will reduce to zero.

More precisely, in the context of Lemma 3.4 we can predict that all S-pairs with signature $\gamma$ will reduce to the same element. The first effect of the rewritability check is the discarding of all S-pairs with signature $\sigma$, except at most one. Secondly, Lemma 3.4 may be used to predict that a S-pair will reduce to zero. There are two criteria for that:
Algorithm 4 The rewritability criterion  
**Input:** $\alpha$ a sig-poly pair, $m$ a monomial, $G$ a set of sig-poly pairs with $\alpha \in G$  
**Output:** Returns true if $ma$ is rewritable w.r.t. $G$; false otherwise  
1: procedure Rewritable($\alpha$, $m$, $G$)  
2: for $\delta \in G$ do  
3: if $s(\delta)$ divides $s(ma)$ and $\delta$ was added to $G$ later than $\alpha$ then  
4: return true (Singular criterion)  
5: else if $s(\delta)$ divides $s(ma)$ and $\text{poly}(\delta) = 0$ then  
6: return true (Syzygy criterion)  
7: else if $\text{ind}(\delta) < \text{ind}(\alpha)$ and $\text{lm}(\text{poly}(\delta))$ divides $\text{lm}(\text{quo}(\alpha))$ then  
8: return true (Koszul criterion)  
9: end if  
10: end for  
11: return false  
12: end procedure

Algorithm 5 sGB with recording of syzygies  
**Input:** $f_1, \ldots, f_r \in R$  
**Output:** See Theorem 3.5  
1: procedure sGB($f_1, \ldots, f_r$)  
2: $G \leftarrow \{ (f_i, (i, 1), 1) \mid 1 \leq i \leq r \}$  
3: $S_1, \ldots, S_r \leftarrow \emptyset$  
4: $P \leftarrow \{ (\alpha, \beta) \mid \alpha, \beta \in G \text{ form a regular S-pair} \}$  
5: while $P \neq \emptyset$ do  
6: $(\alpha, \beta) \leftarrow$ the element in $P$ with minimal signature  
7: $P \leftarrow P \setminus \{ (\alpha, \beta) \}$  
8: $a, b \leftarrow$ the monomials such that $a \text{poly}(\alpha) - b \text{poly}(\beta) = \text{poly}(\text{sp}(\alpha, \beta))$  
9: if not Rewritable($\alpha$, $a$, $G$) and not Rewritable($\beta$, $b$, $G$) then  
10: $\gamma \leftarrow \text{RegularReduction}(\text{sp}(\alpha, \beta), G)$  
11: $G \leftarrow G \cup \{ \gamma \}$  
12: if $\text{poly}(\gamma) \neq 0$ then  
13: $P \leftarrow P \cup \{ (\gamma, \beta) \mid \beta \in G \text{ forms a regular S-pair with } \gamma \}$  
14: else (record the quotient of the zero reduction)  
15: $S_{\text{ind}(\gamma)} \leftarrow S_{\text{ind}(\gamma)} \cup \{ \text{quo}(\gamma) \}$  
16: end if  
17: end if  
18: end while  
19: return $\{ \text{poly}(\beta) \mid \beta \in G \}$, $S_1, \ldots, S_r$  
20: end procedure
Syzygy criterion If an element in signature \( \tau \) has reduced to zero, then every element in signature \( a\tau \) (for any monomial \( a \)) will reduce to zero;

Koszul criterion If we have a sig-poly pair \( h \) with index \( < \text{ind}(\sigma) \) and, then every element in signature \((a \text{lm}(h), \text{ind}(\sigma))\) will reduce to zero, (because \( hf_{\text{ind}(\sigma)} \) will obviously reduce to zero).

This explains the different checks in the rewritability criterion (Algorithm 5, see [18, section 7.1] for a detailed discussion.

**Theorem 3.5.** On input \( f_1, \ldots, f_r \in R \), Algorithm 5 terminates and outputs subsets \( G, S_1, \ldots, S_r \) of \( R \) such that:

(i) \( G \) is a Gröbner basis of \( \langle f_1, \ldots, f_r \rangle \);

(ii) \( I_{i-1} + \langle S_i \rangle = I_{i-1} : f_i \).

Moreover, on line 13 when a polynomial \( g \) is inserted in some \( S_i \), then \( \text{lm}(g) \) is not divided by the leading monomial of any element of \( I_{i-1} \) or any element previously inserted in \( S_i \).

**Proof.** Termination and the first two points are a special case of [18, Theorem 7.1], where we only compute partial information about the syzygy module.

The last point is a consequence from the rewritability check. We first note that every time a polynomial \( h \) is inserted into \( S_i \), the extended sig-poly pair \( (0, (i, \text{lm}(h)), h) \) has been inserted into \( G \) just before. (The monomial part of the signature is always the leading monomial of the quotient, this is an invariant of sig-poly pairs.) Next, in the context of line 13, if \( g = \text{quo}(\gamma) \), then \( s(\gamma) = (\text{ind}(\gamma), \text{lm}(g)) \). Moreover, \( \gamma \) comes from a S-pair \( sp(\alpha, \beta) \), so \( s(\gamma) = a\delta(\alpha) \) or \( b\delta(\beta) \), and both \text{Rewritable}(\alpha, a, G) \) and \text{Rewritable}(\beta, b, G) were false.

The Syzygy criterion implies that \( s(\gamma) \) is not divided by any \( s(\delta) \), where \( \delta \in G \) and \( \text{poly}(\delta) = 0 \). In other words, \( \text{lm}(g) \) is not divided by \( \text{any} \) \( \text{lm}(h) \), where \( h \) has been previously inserted into \( S_i \).

The Koszul criterion implies that \( \text{lm}(g) \) is not divided by any \( \text{lm}(\text{poly}(\delta)) \), where \( \delta \in G \) and \( \text{ind}(\delta) < i \). But due to the incremental nature of the algorithm, the set \( \{\text{poly}(\delta) \mid \delta \in G, \text{ind}(\delta) < i \} \) is a Gröbner basis of \( I_{i-1} \). So \( \text{lm}(g) \) is not divided by any element in \( I_{i-1} \).

3.3 The sGB tree datastructure

3.3.1 Specification

We now specify a data structure, called sGB tree. It is meant to extend the sGB algorithm presented above in two ways: by offering the possibility to add new input equations during the computation; and by offering the possibility to split the computation into different branches while sharing the common base.

An sGB tree represents a rooted tree \( T \) where each node holds an element of the polynomial ring \( R \). The nodes are partially ordered by the ancestor-descendant relation: \( \nu \leq_T \mu \) if \( \nu \) is on the unique path from \( \mu \) to the root of \( T \) (or, equivalently, if \( \mu \) is in the subtree rooted at \( \nu \)). For a node \( \nu \), the polynomial contained in \( \nu \) is denoted \( \text{poly}(\nu) \), and the ideal generated by the polynomials contained by the ancestors of \( \nu \) (not including \( \nu \)) is denoted \( I_{<\nu} \). An sGB tree offers the following three operations. How we implement them is the matter of the next section.

**Node insertion** Insert a new node, containing a given polynomial \( f \), anywhere in the tree, as a new leaf or on an existing edge. Denoted \text{InsertNode}(T, f, \text{position}).

**Gröbner basis** Given a node \( \nu \), outputs a Gröbner basis of the ideal generated by the polynomials contained in the nodes \( \leq_T \nu \). Denoted \text{Basis}(T, \nu).
**Get a syzygy** Given a node \( \nu \), outputs an element of \( I_{\preceq \nu} : \text{poly}(\nu) \). Denoted \( \text{GetSyzygy}(\mathcal{T}, \nu) \).

If \( \text{GetSyzygy}(\mathcal{T}, \nu) \) outputs zero, then \( I_{\preceq \nu} + J = I_{\preceq \nu} : \text{poly}(\nu) \), where \( J \) is the ideal generated by all previous invocations of \( \text{GetSyzygy}(\mathcal{T}, \nu) \).

It is guaranteed that \( \text{GetSyzygy}(\mathcal{T}, \nu) \) eventually outputs zero after sufficiently many invocation, even if nodes are inserted or \( \text{GetSyzygy} \) is called on other nodes in between.

### 3.3.2 Implementation

From the point of implementation, an sGB tree is made of:

- (a) a rooted tree \( T \) containing whose nodes are labelled with integers;
- (b) a set \( G \) of extended sig-poly pairs whose indices are nodes of \( T \) (see below);
- (c) a set \( P \) of pairs of elements of \( G \) forming regular S-pairs;
- (d) for each node \( \nu \) of \( T \), a subset \( S_\nu \) of \( R \).

The sets \( G, P \) and \( S_\nu \) have the same role as their counterparts in the sGB algorithm (Algorithm 5). The main difference is a twist in the definition of signatures and indices. In §3.1 an index (that is the first component of a signature) is a nonnegative integer. From now on, indices are nodes in \( T \). Indices are partially ordered by the ancestor-descendant relation \( \leq_T \). Note that for a given node \( \nu \), the subset \( \{ \mu \mid \mu \leq_T \nu \} \) is totally ordered: it is the set of nodes on the path from the root of \( T \) to \( \nu \). Lastly, we adjust the definition of a regular S-pair: \( \alpha \) and \( \beta \) form a regular S-pair if \( \text{ind}(\alpha) \) and \( \text{ind}(\beta) \) are comparable (that is either \( \text{ind}(\alpha) \leq_T \text{ind}(\beta) \) or \( \text{ind}(\beta) \leq_T \text{ind}(\alpha) \)) and \( \text{s}(a\alpha) \neq \text{s}(b\beta) \), with \( a \) and \( b \) as in §3.1.

To analyze the behavior of the sGB-tree data structure, we always consider totally ordered subsets of indices, thus reducing to the context of Algorithm 5.

To implement \( \text{Basis}(\mathcal{T}, \nu) \), we process the S-pairs with index \( \leq_T \nu \). The indices of these S-pairs are totally ordered, so we are actually in the situation of §3.2 and we may apply the main loop of Algorithm 5. The body of this loop is isolated in procedure \( \text{ProcessSPair} \) (Algorithm 6), with the appropriate alterations.

The implementation of \( \text{GetSyzygy}(\mathcal{T}, \nu) \) is similar, with the difference that we abort the computation as soon as the set \( S_\nu \) is not empty and return an element of it, see Algorithm 6. If \( S_\nu \) is still empty after having processed all S-pairs which may lead to new elements in \( S_\nu \), the value 0 is returned.

We assume that the state of a sGB tree always results from a sequence of calls to \( \text{InsertNode} \), \( \text{Basis} \) or \( \text{GetSyzygy} \) applied to an initially empty tree.

**Proposition 3.6.** Let \( \mathcal{T} \) be a sGB tree and let \( \nu \) be a node of \( \mathcal{T} \). \( \text{Basis}(\mathcal{T}, \nu) \) (Algorithm 6) terminates and outputs a Gröbner basis of \( I_\nu \).

**Proof.** This algorithm considers only S-pairs whose signatures are above a given node \( \nu \). After this restriction, the signature are totally ordered, so \( \text{Basis} \) behaves exactly like Algorithm 5 (sGB). We note that, contrary to sGB, \( \text{Basis} \) may start in a state where several S-pairs have already been processed, in an unspecified order, by earlier calls to \( \text{Basis} \) or \( \text{GetSyzygy} \) on different nodes. This does not invalidate neither the termination proof given in [20], nor the proof of correctness. \( \blacksquare \)

**Proposition 3.7.** Let \( \mathcal{T} \) be a sGB tree and let \( \nu \) be a node of \( \mathcal{T} \). \( \text{GetSyzygy}(\mathcal{T}, \nu) \) (Algorithm 6) terminates and outputs some \( f \in R \) such that:

(i) \( f \in I_{\preceq \nu} : \text{poly}(\nu) \);

(ii) if \( f \neq 0 \), then \( \text{lm}(f) \) is not divisible by the leading monomial of any other polynomial previously output by \( \text{GetSyzygy}(\mathcal{T}, \nu) \), or any polynomial in \( I_{\preceq \nu} \);
Algorithm 6 Implementation of the sGB tree data structure

**Input:** An sGB tree $T$ and a label of $T$

**Output:** Process the pair in $P$ with index above $\nu$ with smallest signature

1. **procedure** `ProcessSPair(T, \nu)`
2. 
3. $(\alpha, \beta) \leftarrow$ the pair in $P'$ with $s(sp(\alpha, \beta))$ minimal
4. $P \leftarrow P \setminus \{(\alpha, \beta)\}$
5. $\gamma \leftarrow$ `RegularReduction(sp(\alpha, \beta), G)`
6. $G \leftarrow G \cup \{\gamma\}$
7. if `poly(g) \neq 0` then
8. $P \leftarrow P \cup \{(\gamma, \beta) \mid \beta \in G\}$
9. else (record the quotient of the zero reduction)
10. $S_{\text{ind}(\gamma)} \leftarrow S_{\text{ind}(\gamma)} \cup \{\text{quo}(\gamma)\}$
11. end if
12. end if
13. end procedure

**Input:** A sGB tree $T$ and a label $\nu$ of $T$

**Output:** A Gröbner basis of $I_{<\nu}$

1. **procedure** `Basis(T, \nu)`
2. while there is a pair in $P$ with index $\leq_T \nu$ do
3. `ProcessSPair(T, \nu)`
4. end while
5. return $\{\text{poly}(\alpha) \mid \alpha \in G\}$ and $\text{ind}(\alpha) \leq_T \nu$
6. end procedure

**Input:** A sGB tree $T$ and a label $\nu$ of $T$

**Output:** An element of the quotient ideal $I_{<\nu}$: $\text{poly}(\nu)$ not contained in $I_{<\nu}$

1. **procedure** `GetSyzygy(T, \nu)`
2. while there is a pair in $P$ with index $\leq_T \nu$ and $S_\nu = \emptyset$ do
3. `ProcessSPair(T, \nu)`
4. end while
5. if $S_\nu \neq \emptyset$ then
6. pick and remove some $h \in S_\nu$
7. return $h$
8. else
9. return $0$
10. end if
11. end procedure
Algorithm 7 The sGB tree data structure, insertion of a node

Input: A sGB tree $T$, a polynomial $f$ and a description of the position of the new node in $T$
Output: The label of the newly inserted node

1: procedure InsertNode$(T, f, \text{position})$
2: \hspace{1em} $\nu \leftarrow \text{largest label in } T + 1$
3: \hspace{1em} insert a node in $T$ with label $\nu$, as described by “position”
4: \hspace{1em} $S_\nu \leftarrow \emptyset$
5: \hspace{1em} $\epsilon \leftarrow (f, (\nu, 1), 1)$
6: \hspace{1em} $P \leftarrow \{(\epsilon, \beta) \mid \beta \in G$ and $(\epsilon, \beta)$ is regular$\}$
7: \hspace{1em} $G \leftarrow G \cup \{\epsilon\}$
8: \hspace{1em} return $\nu$
9: end procedure

(iii) if $f = 0$, then $I_{<\nu} : \text{poly}(\nu)$ is generated by $I_{<\nu}$ and the polynomials previously output by GetSyzygy$(T, \nu)$.

Proof. Termination follows from the termination of Basis since the main loop is similar, but with the possibility of earlier termination. Correctness follows from Theorem 3.5 after restricting to indices above $\nu$.

As a consequence of Proposition 3.7(ii), it is guaranteed that GetSyzygy$(T, \nu)$ eventually outputs zero after sufficiently many invocation, even if nodes are inserted or GetSyzygy is called on other nodes in between. Indeed, the leading monomial of a nonzero output of GetSyzygy$(T, \nu)$ is constrained to be outside the monomial ideal generated by the leading monomials of previous output. By Dickson’s lemma, this may only happen finitely many times.

4 Computation of the nondegenerate locus

The sGB-tree data structure may can be used to implement an efficient variant of Algorithm 1 for computing the nondegenerate locus. We use a sGB tree to compute efficiently saturations $I : f^\infty$, and also double quotient $I : (I : f^\infty)$, with the idea to exploit as soon as possible newly discovered relations to simplify further computations. This leads to Algorithm 8 which we describe informally as follows.

Similarly to Algorithm 1, we introduce the equations $f_1, \ldots, f_r$ one after the other. We maintain a sGB tree which, at the beginning of the $k$th iteration, that is after having processed $f_1, \ldots, f_{k-1}$, has the following shape:

\[
\begin{align*}
g_1 \leftarrow f_1 \leftarrow p_1 \leftarrow \cdots \leftarrow g_{k-1} \leftarrow f_{k-1} \leftarrow p_{k-1} \leftarrow 0 \leftarrow \nu \leftarrow h_1 \leftarrow \cdots \leftarrow h_2,
\end{align*}
\]

where bold letters represent a sequence of zero, one or several nodes. The tree grows from the node labeled $\nu$, by adding new leaf nodes, or inserting nodes just above $\nu$. Using the notations of Algorithm 1 the nodes $g_i$ are related to the saturation $G : f_i^\infty$, the leaf nodes $h_i$ are generic elements of the ideals in the set $K$, and the nodes $p_i$ are related to the cleaning steps $G : K^\infty$. The leaf nodes $h_i$ are generic in the sense that they are either each a random linear combination of generators of the ideals in $K$ or each a linear combination of of generators of the ideals in $K$ with each coefficient a new variable.
The $k$th iteration proceeds as follows. Firstly, a new node $\mu$ containing $f_k$ is created just above $\nu$:

$\cdots \leftarrow f_k \leftarrow \underbrace{0 \leftarrow \cdots}_{\mu}.$

As long as $\text{GetSyzygy}(T, \mu)$ returns nonzero elements $(g_1, g_2, \ldots)$, we insert them above $\mu$:

$\cdots \leftarrow g_1 \leftarrow g_2 \leftarrow \cdots \leftarrow f_k \leftarrow \underbrace{0 \leftarrow \cdots}_{\nu}.$

This saturation has the effect of completing $I_{<\mu}$ into $I_{<\mu} : f_k^\infty$. Each time we insert a polynomial $g_i$ in a node, say $\gamma$, we also record the syzygies $\text{GetSyzygy}(T, \gamma)$, take a generic linear combination and insert it as a new leaf node. These syzygies are related to the double quotient

$I_{<\mu} : \text{pol}(\beta) \cap \cdots \cap \text{pol}(\beta)_{\text{child of } \nu}.$

Moreover, by (3), we obtain that before line 23, we have

$I_{<\mu} = J_{k-1} : f_k^\infty.$

This saturation has the effect of completing $I_{<\mu}$ into $I_{<\mu} : f_k^\infty$. Each time we insert a polynomial $g_i$ in a node, say $\gamma$, we also record the syzygies $\text{GetSyzygy}(T, \gamma)$, take a generic linear combination and insert it as a new leaf node. These syzygies are related to the double quotient $I_{<\mu} : (I_{<\mu} : f_k^\infty)$. Before going to the next iteration, insert above $\nu$ all the syzygies obtained from the children of $\nu$. Which again has the effect of saturating $I_{<\nu}$ by the polynomials contained in these nodes.

After all the input equations have been processed, the ideal $I_{<\nu}$ is a nondegenerate part of the input ideal, which we prove by comparing with Algorithm 1.

**Theorem 4.1.** Algorithm 8 terminates and is correct.

**Proof.** Termination follows from the assumption that for any node $\nu$ of an sGB tree $T$, $\text{GetSyzygy}(T, \nu)$ eventually returns 0 after sufficiently many calls.

To prove correctness, we show that Algorithm 8 computes the same ideal as Algorithm 1. Let $J_{k-1}$ be the value of $I_\nu$ at the beginning of the $k$th iteration. After line 3 we also have $I_{<\mu} = J_{k-1}$, while $I_{<\nu} = I_{<\mu} + (f_k)$.

We first examine the loop on line 5. It inserts above the node $\mu$ all the polynomials obtained from $\text{GetSyzygy}(T, \mu)$. Every node inserted on line 11 is in $I_{<\mu} : f_k$. No other node is inserted above $\mu$. So by induction, it follows that all along the loop, we have $I_{<\mu} \subseteq J_{k-1} : f_k^\infty$. Moreover, after the loop terminates, we have $I_{<\mu} : f_k = I_{<\mu}$, due to the specification of $\text{GetSyzygy}$ (Proposition 3.7). It follows that before line 23 we have

$I_{<\mu} = J_{k-1} : f_k^\infty$ and $I_{<\nu} = (J_{k-1} : f_k^\infty) + (f_k).$ (3)

Next, we examine the loop on line 26 and its inner loop on line 24. By the same argument as above, the inner loop has the effect of saturating $I_{<\nu}$ by $\text{pol}(\beta)$. So after the loop on line 23 we have

$I_{<\nu} = J_k = ((J_{k-1} : f_k^\infty) + (f_k)) : \prod_{\beta \text{ child of } \nu} \text{pol}(\beta)^\infty.$ (4)

It remains to understand the nature of the children of $\nu$. They all come from the insertion of $h$ on line 21. And $h$ is simply a generic linear combination of the return values of $\text{GetSyzygy}(T, \gamma)$. So $h$ is a generic linear combination of some $h_1, \ldots, h_r$ such that $I_{<\gamma} + (h_1, \ldots, h_r) = I_{<\gamma} : \text{pol}(\gamma)$ (by Proposition 3.7). For each node $\gamma$ inserted on line 11 let $L_{\gamma}$ denote the ideal $I_{<\gamma} : \text{pol}(\gamma)$. If $g_1, \ldots, g_r$ are the successive return values of $\text{GetSyzygy}(T, \mu)$ on line 6 and $\gamma_1, \ldots, \gamma_r$ the corresponding nodes, we have $L_{<\gamma_1} = I_{<\gamma_1} : g_1$ and $I_{<\gamma_1} = J_{k-1} + (g_1, \ldots, g_r)$. By Lemma 4.2 it follows that

$L_{\gamma_1} \cap \cdots \cap L_{\gamma_r} = J_{k-1} : (g_1, \ldots, g_r)^\infty.$ (5)

Moreover, by (3), we obtain that before line 23

$I_{<\mu} = J_{k-1} + (g_1, \ldots, g_r) = J_{k-1} : f_k^\infty,$ (6)
Algorithm 8: Computation of the nondegenerate locus with an sGB tree

**Input:** $f_1, \ldots, f_c \in R$

**Output:** A Gröbner basis $G$ of a nondegenerate locus of $(f_1, \ldots, f_c)$

1. $\mathcal{T} \leftarrow$ an empty sGB tree
2. $\nu \leftarrow \text{InsertNode}(\mathcal{T}, 0)$
3. for $k$ from 1 to $c$ do
4.   $\mu \leftarrow \text{InsertNode}(\mathcal{T}, f_k, \text{just above } \nu)$
5.   loop
6.     $g \leftarrow \text{GetSyzygy}(\mathcal{T}, \mu)$
7.     if $g = 0$ then
8.        break
9.     end if
10.    $P \leftarrow P \cup \{(\text{poly}(\mu), (\mu, 1), 1)\}$
11.    $\gamma \leftarrow \text{InsertNode}(\mathcal{T}, g, \text{just above } \mu)$
12.    $h \leftarrow 0$
13.    $t \leftarrow$ a random scalar (or the slack variable, see Remark 4.1)
14.   loop
15.     $h' \leftarrow \text{GetSyzygy}(\mathcal{T}, \gamma)$
16.     if $h' = 0$ then
17.        break
18.     end if
19.     $h \leftarrow th + h'$
20.   end loop
21.   $\text{InsertNode}(\mathcal{T}, h, \text{as a child of } \nu)$
22. end loop
23. for all child $\beta$ of $\nu$ do
24.   loop
25.     $b \leftarrow \text{GetSyzygy}(\mathcal{T}, \beta)$
26.     if $b = 0$ then
27.        break
28.     end if
29.     $\text{InsertNode}(\mathcal{T}, b, \text{just above } \nu)$
30.   end loop
31. end for
32. end for
33. $\text{return Basis}(\nu)$
so, combining with (5),
\[
L_{\gamma_1} \cap \cdots \cap L_{\gamma_r} \stackrel{\text{rad}}{=} J_{k-1} : (g_1, \ldots, g_r)_{\infty} \tag{7}
\]
\[= J_{k-1} : (J_{k-1} + (g_1, \ldots, g_r))_{\infty} \tag{8}
\]
\[\stackrel{\text{rad}}{=} J_{k-1} : (J_{k-1} : f_{k}^{\infty}). \tag{9}
\]

As remarked above, the loop on line 24 has the effect of saturating \( I_{<\nu} \) by \( \text{pol}(\beta) \). By the analysis above, \( \text{pol}(\beta) \) is actually a generic linear combination of some \( h_1, \ldots, h_r \) such that \( I_{<\gamma} + (h_1, \ldots, h_r) = L_{\gamma} \), for some node \( \gamma \) above \( \nu \). By Lemma 4.3, saturating by \( \text{pol}(\beta) \) is the same as saturating by \( \langle h_1, \ldots, h_r \rangle \). Besides, \( I_{<\nu} \) contains \( I_{<\gamma} \), so saturating \( I_{<\nu} \) by \( \langle h_1, \ldots, h_r \rangle \) is the same as saturating by \( L_{\gamma} \). Back to (11), we conclude from (9) that saturating \( I_{<\nu} \) by all the \( \text{pol}(\beta) \) is the same as saturating by all the ideals \( J_{i-1} : (J_{i-1} : f_i^{\infty}) \), for \( i \leq k \).

Therefore \( J_k \) satisfies the same recurrence relation as its analogue defined the proof of Theorem 2.4.

\[
J_k = \left( (J_{k-1} : f_k^{\infty}) + (f_k) : \bigcap_{i \leq k} (J_{i-1} : (J_{i-1} : f_i^{\infty})) \right)_{\infty}. \tag{10}
\]

This proves that Algorithm 8 and Algorithm 4 compute the same ideal. \( \square \)

**Lemma 4.2.** Let \( I, J \subseteq R \) be two ideals and let \( J = \langle g_1, \ldots, g_i \rangle \). Then
\[
\left( I : J \right)^{\text{rad}} \cap (I : \{g_1\}) \cap (I : \{g_2\}) \cap \cdots \cap (I : \{g_{i-1}\}) : g_i.
\]

**Proof.** The inclusion "\( \subseteq \)" is obvious. Now, let \( p \in R \) be such that
\[
p^m \in (I : g_1) \cap (I + \{g_1\}) : g_2 \cap \cdots \cap (I + \{g_{i-1}\}) : g_i
\]
for some \( m \in \mathbb{N} \). Then we have in particular \( p^{m} g_i \in I \). Now let \( i > 1 \). By induction, if for some \( k \in \mathbb{N} \) we have \( p^k g_i \in I \) for all \( j \leq i \) then
\[
p^{km} g_{i+1} = p^k f + p^k a_1 g_1 + \cdots + p^k a_i g_i \in I
\]
for a suitable \( f \in I, a_1, \ldots, a_i \in R \) and so \( p^{km} \in (I : g_{i+1}) \). We deduce that a power of \( p \) actually lies in \( (I : J) \) which ends the proof. \( \square \)

**Lemma 4.3.** Let \( I, J \subseteq R \) be two ideals with \( J = \langle g_1, \ldots, g_i \rangle \).

1. There exists a Zariski-open subset \( D \subseteq K^i \) such that for any \( (a_1, \ldots, a_i) \in D \) we have \( (I : J)_{\infty} = (I : (\sum_{j=1}^{i} a_j g_j))_{\infty}. \)

2. If \( K^{\text{rad}} = J \) then \( (I : K_{\infty})_{\text{rad}}^{\text{rad}} = (I : J_{\infty}). \)

**Proof.** (1) easily follows e.g. from [21] Exercise 15.41. For (2), if \( p \in R \) such that \( p^k J^l \in I \) for \( k, l \in \mathbb{N} \) then for a suitably large \( m \in \mathbb{N} \) we have \( K^m \subseteq J^l \) so \( p^k K^m \in I \) and hence \( p \in \sqrt{(I : K_{\infty})} \). \( \square \)

**Remark 4.1** (Deterministic variant). The cleaning steps in Algorithm 8 can be made in a randomized way, with a possibility of undetected error, or in a deterministic way. The only change to operate is on line 14. For a randomized algorithm, favoring speed over certain correctness, choose \( t \) to be a random scalar. For a deterministic algorithm, choose \( t \) to be a slack variable, unused in the input equation. It is guaranteed that such a \( t \) is generic enough. Whenever we introduce such a slack variable we can extend the monomial ordering on \( R \) in any way we like, since all cofactors of syzygies that are inserted as new nodes only involve the variables of \( R \). The implementation discussed in the next section exclusively chooses \( t \) to be a random scalar.
5 Implementation and Experiments

5.1 Further Implementational Considerations

We start by describing some further optimizations in our implementations of Algorithms 5 and 8.

Both these implementations use an $F_4$-like reduction strategy. This means that several $S$-pairs are selected out of the pairset at once and are subsequently, together with their regular reducers, organized in a matrix whose rows are labeled by the selected extended sig-poly pairs and whose columns are labeled by all the monomials occurring in the polynomial parts of these extended sig-poly pairs. This matrix is then put into row echelon form and the rows of this reduced matrix whose first entry has changed during the computation of this row echelon form are then processed as new basis elements or newly identified zero divisors, depending on if this reduced row is zero or not. We refer to [22] for the original $F_4$ algorithm or to [18, section 13] for an explanation as to how to combine the $F_4$ algorithm with signature-based techniques.

For Algorithm 8 this has the consequence that the $\text{GetSyzygy}$ routine has the ability to return several zero divisors $g_1, \ldots, g_s$ at once and Algorithm 8 may benefit from it. We implemented the following probabilistic optimization: We replaced $g_1$ by a random linear combination $g'_1 := \sum_{j=1}^s a_j g_j$. Let $\nu_1, \ldots, \nu_s$ be the nodes assigned to $g'_1, g_2, \ldots, g_s$ in Algorithm 8. Then, if the choice of the $a_i$ was "sufficiently random", we know by Lemma 4.3 that for $h \in R$ we have

$$hg'_1 \in I_{<\nu_1} \Leftrightarrow hg_i \in I_{<\nu_i} \forall i.$$ 

If then $\text{GetSyzygy}(T, \nu_1)$ returned such an element $h \neq 0$ we regarded the signatures $(\nu_2, \text{lm}(h)), \ldots, (\nu_s, \text{lm}(h))$ as known signatures of syzygies during the calls to $\text{Rewriteable}$, i.e. $\text{GetSyzygy}(T, \nu_1)$ would, for $i = 2, \ldots, s$, only return a non-zero result if there exists an element $h' \in (I_{<\nu_1} : g_i)$ with $\text{lm}(h')$ not divisible by $\text{lm}(h)$. Furthermore, only the zero divisors of $h$ of $g'_1$ as above were considered in the loop from line 14-20 of Algorithm 8.

We implemented both Algorithm 5 and 8 in the programming language Julia [4] with an interface to the Singular.jl Julia-library [16]. An interface to the new computer algebra system OSCAR [41] is planned for the future. The implementation is available at

https://github.com/RafaelDavidMohr/SignatureGB.jl

In this implementation we use our own data structures for polynomials and polynomial arithmetic. The linear algebra routines for computing row echelon forms in our implementations closely follow the corresponding routines presented in [40]. Additionally, our implementation makes use of the modifications to Algorithm 5 presented in [19]. Currently the implementation works only for fields of finite characteristic.

While our implementation is currently not competitive with optimized implementations of Gröbner basis algorithms such as in Maple [39] or msolve [3], we do make use of some standard optimization techniques in Gröbner basis algorithm implementations such as monomial hash tables and divisor bitmasks (see e.g. [42] for a description of these techniques).

5.2 Experimental Results

We used the following examples to benchmark our implementations:

1. Cyclic(8), coming from the classical Cyclic(n) benchmark.

2. Pseudo(n), encoding pseudo-singularities as follows

$$f_1 = \cdots = f_{n-1} = g_1 \cdots = g_{n-1}$$

with $f_i \in K[x_1, \ldots, x_{n-2}, z_1, z_2], f_i \in K[y_1, \ldots, y_{n-2}, z_1, z_2], f_i$ being chosen as a random dense quadric and $g_i$ equalling $f_i$ when substituting $y_1, \ldots, y_{n-2}$ by $x_1, \ldots, x_{n-2}$.
3. Sos($s$, $n$), encoding the critical points of the restriction of the projection on the first coordinate to a hypersurface which is a sum of $s$ random dense quadrics in $\mathbb{K}[x_1, \ldots, x_n]$.

\[
f, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n}, \quad f = \sum_{i=1}^{s} g_i^2.
\]

4. Sing($n$), encoding the critical points of the restriction of the projection on the first coordinate to a (generically singular) hypersurface which is defined by the resultant of two random dense quadrics $A, B$ in $\mathbb{K}[x_1, \ldots, x_{n+1}]$:

\[
f, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n}, \quad f = \text{resultant}(A, B, x_{n+1}).
\]

5. The Steiner polynomial system, coming from $[6]$. All these systems are generated by a number of polynomials equal to the number of variables of the underlying polynomial ring. They all have components of different dimensions, one of those being zero-dimensional, i.e. they have a nontrivial nondegenerate locus.

In Table 1 we compare Algorithm 8 and a straightforward implementation of ours of Algorithm 1 in Maple. In this implementation, we saturated an ideal $J$ by an ideal $K$ by picking a random linear combination $p$ of generators of $K$ and saturating $J$ by $p$ using Maple’s internal saturation routine. Table 1 shows the improvement of Algorithm 8 over Algorithm 1. While Maple’s Gröbner basis engine beats our implementation of Algorithm 5 by a wide margin the ratio between the timings of our F5 implementation and our implementation of Algorithm 8 is much better than the ratio between the time it took to compute a Gröbner basis in Maple and our Maple implementation of Algorithm 1. This can be seen by looking at the two respect “ratio”-columns of Table 1. To additionally show the overhead of Algorithm 8 over Algorithm 5 we noted the number of arithmetic operations in $\mathbb{K}$ when running each of the two algorithms on the polynomial system in question. Our implementation of Algorithm 8 never takes more than 10 times the number of arithmetic operations Algorithm 5 takes, on certain examples we compare very favorably in terms of arithmetic operations to Algorithm 5.

In Table 2 we compare Algorithm 8 to other ideal decomposition methods available in the computer algebra systems Singular, Maple and Macaulay2 $[29]$. In Singular there is an elimination method $[15]$ and an implementation of the algorithm for equidimensional decomposition presented in $[22]$. In Maple we compared against the Regular Chains package $[9; 10]$. In Macaulay2 one is able to compute the intersection of all components of non-minimal dimension again with the method presented in $[22]$. We then saturated the original ideal by the result to obtain the nondegenerate locus. On a high level, our algorithm works similarly, incrementally obtaining information about the component of higher dimension and then removing it via saturation. One should keep in mind that all of these methods, compared to Algorithm 8, work more generally: Except for what we tried in Macaulay2 they are all able to obtain a full equidimensional decomposition of the input ideal.

We gave all of these methods at least an hour for each polynomial system and at most roughly 50 times the time our implementation of Algorithm 8 took. We indicated when these times were exceeded by using ”>” in Table 2. We computed all examples on a single Intel Xeon Gold 6244 CPU @ 3.60GHz with a limit of 200G memory. If this limit was exceeded, or if another segfault occurred, we indicate it with ‘segfault’ in Table 2.
### Table 1: Comparing Algorithm 1 and Algorithm 8

|          | Alg. 1 arith. op | Alg. 2 arith. op | Alg. 1 | Alg. 2 | Ratio | GB in Maple | Alg. 1 in Maple | Ratio |
|----------|------------------|------------------|--------|--------|-------|-------------|-----------------|-------|
| Cyclic   | 1.2·10^{10}     | 1.3·10^{11}     | 4m     | 40m    | 10    | 1.2s        | 154m           | 7700  |
| Pseudo(2, 10) | 5.6·10^{7}     | 6.5·10^{7}     | 1.16s  | 5.2s   | 4.5   | 0.268s      | 3.44s          | 13.0  |
| Sing(2, 9)  | 2.5·10^{7}      | 2.9·10^{7}      | 1.1s   | 1.4s   | 1.27  | 0.06s       | 0.788s         | 13.1  |
| Sos(2,5,4)  | 1.3·10^{8}      | 1.1·10^{8}      | 8.5s   | 7.3s   | 0.85  | 0.022s      | 0.479s         | 21.3  |
| Sos(2,6,3)  | 2.1·10^{7}      | 2.1·10^{7}      | 1.11s  | 1.4s   | 1.26  | 0.021s      | 0.261s         | 12.4  |
| Sos(2,6,4)  | 4.8·10^{9}      | 3.8·10^{9}      | 148s   | 169s   | 1.14  | 0.172s      | 22.7s          | 132.0 |
| Sos(2,7,3)  | 4.2·10^{9}      | 2.0·10^{9}      | 75s    | 43s    | 0.57  | 0.458s      | 10.38s         | 22.7  |
| Sos(2,7,4)  | 1.3·10^{8}      | 6.7·10^{8}      | 5.2s   | 41s    | 7.9   | 0.047s      | 7.162s         | 152.4 |
| Sos(2,7,5)  | 6.5·10^{9}      | 4.5·10^{10}     | 3m     | 32m    | 10.7  | 0.433s      | 1h             | 8314  |
| Sos(2,7,6)  | 7.2·10^{10}     | 3.5·10^{11}     | 25m    | 20h    | 48    | 2.294s      | >359h          | >4.4·10^{6} |
| Sos(2,7,7)  | 1.7·10^{12}     | 3.0·10^{12}     | 31h    | 73h    | 2.4   | 14.348s     | 5.5h           | 23    |
| Sos(2,8)    | 3.1·10^{10}     | 2.3·10^{11}     | 4.2m   | 42m    | 10    | 27s         | 13m            | 28.9  |

### Table 2: Comparing with other Decomposition Methods

| Algorithm | Singular: Elimination Method | Singular: Algorithm in [22] | Maple: Regular Chains | Macaulay2 |
|-----------|-----------------------------|-----------------------------|-----------------------|----------|
| Cyclic    | segfault                    | >35h                        | >35h                  | >35h     |
| Pseudo(2, 10) | 0.3s                       | >1h                         | >1h                   | >1h      |
| Pseudo(2, 12) | 5.2s                      | >1h                         | >1h                   | >1h      |
| Pseudo(2, 6)  | 0.008s                     | <1s                         | 0.29s                 | 0.07s    |
| Pseudo(2, 8)  | 0.03s                      | <1s                         | 5.82s                 | 13.78s   |
| Sing(2, 10)  | 2.9s                       | >1h                         | >1h                   | >1h      |
| Sing(2, 4)   | 0.02s                      | 1s                          | 91.32s                | 0.42s    |
| Sing(2, 5)   | 0.07s                      | 4s                          | >1h                   | 1.94s    |
| Sing(2, 6)   | 0.15s                      | 56s                         | >1h                   | 16.64s   |
| Sing(2, 7)   | 0.35s                      | 8m                          | >1h                   | 289s     |
| Sing(2, 8)   | 0.68s                      | 23m                         | >1h                   | >1h      |
| Sing(2, 9)   | 1.4s                       | >1h                         | >1h                   | >1h      |
| Sos(2,4,2)   | 0.03s                      | <1s                         | 19.4s                 | 0.16s    |
| Sos(2,4,3)   | 0.03s                      | 1s                          | 14m                   | 0.63s    |
| Sos(2,5)     | 0.02s                      | <1s                         | >1h                   | 0.37s    |
| Sos(2,5,3)   | 0.34s                      | >1h                         | >1h                   | 9.35s    |
| Sos(2,5,4)   | 7.3s                       | >1h                         | >1h                   | 183s     |
| Sos(2,6,2)   | 0.17s                      | <1s                         | >1h                   | 0.7s     |
| Sos(2,6,3)   | 1.4s                       | >1h                         | >1h                   | 107s     |
| Sos(2,6,4)   | 169s                       | >140m                       | >140m                 | >140m    |
| Sos(2,6,5)   | 43s                        | >1h                         | >1h                   | >1h      |
| Sos(2,7,2)   | 2.91s                      | <1s                         | 2.94s                 | 0.18s    |
| Sos(2,7,3)   | 41s                        | >1h                         | >1h                   | >1h      |
| Sos(2,7,4)   | 32m                        | >26h                        | segfault              | >26h     |
| Sos(2,7,5)   | 20h                        | segfault                    | segfault              | >200h    |
| Sos(2,7,6)   | 73h                        | segfault                    | segfault              | >500h    |
| Steiner     | 42m                        | >50h                        | segfault              | >50h     |

### References

[1] P. Aubry, D. Lazard, and M. Moreno Maza. “On the Theories of Triangular Sets”. In: *J. Symb. Comput.*, 28.1 (1999), pp. 105–124.

[2] T. Becker and V. Weispfenning. *Gr"obner bases*. Vol. 141. Graduate Texts in Mathematics. A computational approach to commutative algebra, In cooperation with Heinz Kredel. Springer-Verlag, New York, 1993.

[3] J. Berthomieu, C. Eder, and M. Safey El Din. “msolve: A Library for Solving Polynomial Systems”. In: *ISSAC’21*. Saint Petersburg, Russia, 2021.
[4] J. Bezanson, A. Edelman, S. Karpinski, and V. B. Shah. “Julia: A fresh approach to numerical computing”. In: SIAM review 59.1 (2017), pp. 65–98.
[5] W. Bosma, J. Cannon, and C. Playoust. “The Magma Algebra System. I. The User Language”. In: J. Symbolic Comput. 24.3–4 (1997), pp. 235–265.
[6] P. Breiding, B. Sturmfels, and S. Timme. “3264 conics in a second”. In: Notices Amer. Math. Soc. 67.1 (2020), pp. 30–37.
[7] M. Caboara, P. Conti, and C. Traverse. “Yet Another Ideal Decomposition Algorithm”. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Lecture Notes in Computer Science. Springer, 1997, pp. 39–54.
[8] C. Chen, O. Golubitsky, F. Lemaire, M. M. Maza, and W. Pan. “Comprehensive triangular decomposition”. In: International Workshop on Computer Algebra in Scientific Computing. Springer. 2007, pp. 73–101.
[9] C. Chen, F. Lemaire, M. M. Maza, W. Pan, and Y. Xie. “Efficient computations of irredundant triangular decompositions with the regularchains library”. In: International Conference on Computational Science. Springer. 2007, pp. 268–271.
[10] C. Chen and M. Moreno Maza. “Algorithms for computing triangular decomposition of polynomial systems”. In: J. Symbolic Comput. 47.6 (2012). Advances in Mathematics Mechanization, pp. 610–642.
[11] S.-C. Chou and X.-S. Gao. “Ritt-Wu's Decomposition Algorithm and Geometry Theorem Proving”. In: 10th International Conference on Automated Deduction. Lecture Notes in Computer Science. Springer, 1990, pp. 207–220.
[12] X. Dahan, X. Jin, M. M. Maza, and E. Schost. “Change of order for regular chains in positive dimension”. In: Theoretical Computer Science 392.1-3 (2008), pp. 37–65.
[13] X. Dahan, M. Moreno Maza, E. Schost, W. Wu, and Y. Xie. “Lifting techniques for triangular decompositions”. In: ISSAC'05. ACM, New York, 2005, pp. 108–115.
[14] W. Decker, G.-M. Greuel, and G. Pfister. “Primary Decomposition: Algorithms and Comparisons”. In: Algorithmic Algebra and Number Theory. Springer, 1999, pp. 187–220.
[15] W. Decker, G.-M. Greuel, and G. Pfister. “Primary Decomposition: Algorithms and Comparisons”. In: Algorithmic Algebra and Number Theory. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 187–220.
[16] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. Singular 4.3.0 — A Computer Algebra System for Polynomial Computations. 2022.
[17] J. Della Dora, C. Dicrescenzo, and D. Duval. “About a New Method for Computing in Algebraic Number Fields”. In: Research Contributions from the European Conference on Computer Algebra-Volume 2. EUROCAL ’85. Springer-Verlag, 1985, pp. 289–290.
[18] C. Eder and J.-C. Faugère. “A survey on signature-based algorithms for computing Gröbner bases”. In: J. Symbolic Comput. 80 (2017), pp. 719–784.
[19] C. Eder and J. Perry. “F5C: A variant of Faugère’s F5 algorithm with reduced Gröbner bases”. In: J. Symbolic Comput. 45.12 (2010), pp. 1442–1458.
[20] C. Eder and B. H. Roune. “Signature Rewriting in Gröbner Basis Computation”. In: Proceedings of ISSAC 2013. ACM, 2013, pp. 331–338.
[21] D. Eisenbud. Commutative Algebra: with a View Toward Algebraic Geometry. New York, NY: Springer New York, 1995.
[43] W. Vasconcelos. *Computational Methods in Commutative Algebra and Algebraic Geometry*. Algorithms and Computation in Mathematics. Springer-Verlag, 1998.

[44] D. Wang. “An Elimination Method for Polynomial Systems”. In: *J. Symb. Comput.* 16.2 (1993), pp. 83–114.

[45] D. Wang. *Elimination Methods*. Texts and Monographs in Symbolic Computation. Springer Vienna, 2001.

[46] W.-T. Wu. “Basic Principles of Mechanical Theorem Proving in Elementary Geometries”. In: *J. Autom. Reason.* 2.3 (1986), pp. 221–252.