# Parametric Gröbner bases

## Geometry & applications

*Andreas Bøgh Poulsen* *201805425*


AARHUS
UNIVERSITET
INSTITUT FOR MATEMATIK

Supervisor: Niels Lauritzen

# Contents

# Introduction

Gröbner bases of ideals in multivariate polynomial rings are a vital tool when doing computational algebra and computational algebraic geometry. They often feature as an intermidiary step in all sorts of problems, ranging from intersecting ideals and solving polynomial equations, to backwards kinematics and determining the behaviour of chemical reaction networks[1]. As such, the study of Gröbner bases have developed into a large field of its own.

In some situations, we may be interested in not just one ideal, but a family of ideals. For example, we might have a fixed algebraic curve, and we want to calculate the distance between a point and the curve. This can be done by computing a Gröbner basis for a system of equations, given by the Lagrange multipliers. Keeping the coordinates of the point as parameters, we would like to quickly compute this distance for many points. From a purely mathematical view, we might be interested in the behaviour of a Gröbner basis as we change the base ring. Given an ideal $I$ in a polynomial ring $K[U][X]$, we would like to describe the Gröbner basis obtained from $I$, by evaluating each $u \in U$ to a fixed value. In this way, we can see $I$ as a parameterized family of ideals, with $U$ being the parameters. A parametric Gröbner basis is a Gröbner basis of $I$, which remains a Gröbner basis for some choices of values for $U$ and a comprehensive parametric Gröbner basis remains a Gröbner basis for all choices of values for $U$. See definition 2.1 for the precise definition.

Volker Weispfenning introduced the notion of a comprehensive parametric[1] Gröbner basis in [14] in 1992 and gave an algorithm to compute them. He also gave some results on the computational complexity of this algorithm as well as some early applications. However, the computation of Gröbner bases, and by extension parametric Gröbner bases, is a difficult problem. Many optimizations and heuristics exist, which means the computation of Gröbner bases should be performed using highly optimized software. Reimplementing all this for parametric Gröbner bases might not be feasible. In 2006, Suzuki and Sato produced an algorithm for computing parametric Gröbner bases, that utilize existing software for computing Gröbner bases. Even though the theoretical complexity didn't change, the execution time certainly did, as the algorithm could exploit existing optimized algorithms for computing Gröbner bases. Kapur, Sun and Wang improved on this algorithm in 2010 [4][3].

After parametric Gröbner bases were established, the search began for a unique object, a parametric analogue of the reduced Gröbner basis. Weispfenning introduced what he called a canonical comprehensive Gröbner basis in [13], which only depends on the ideal and the monomial order on the variables and the parameters. However, no object comparable to the reduced Gröbner basis, which was independent of assumptions on the ground ring was found until Michael Wibmer introduced Gröbner covers in [15]. By drawing on machinery from modern algebraic geometry, including the language of

[1] Our terminology differs from the original terminology. What Weispfenning called a *comprehensive Gröbner basis* we call a *comprehensive parametric Gröbner basis.*

sheaves and schemes, he found a parametric way of describing the reduced Gröbner basis of every specialization of the ideal in question, called Gröbner covers. He also proved the existence of a canonical Gröbner cover if $I$ is homogenous. This rather abstract paper was quickly followed up by [9], which described an algorithm to compute Gröbner covers. It should be noted, that even though the canonical Gröbner cover described by Wibmer is unique in a mathematical sense, there is no canonical, finite description of it, without adding in some assumptions on the base ring.

The focus of this paper is to serve as an introduction to parametric Gröbner bases. First, we establish parametric Gröbner bases, Gröbner systems and some initial results on parametric Gröbner bases. In particular, a fundamental theorem by Kalkbrener[2] on when a Gröbner basis specializes to a Gröbner basis, as well as a tool called pseudo-division. Then, we cover the algorithm introduced by Suzuki and Sato. From here, we move on to Gröbner covers as introduced by Wibmer, to give an introduction into this, quite different framing of parametric Gröbner bases. We tie this theory together with the Suzuki-Sato algorithm, and provide plenty of examples to help get a feeling for the subject. Finally, we cover some applications of parametric Gröbner bases and Gröbner covers.

We purposefully do not cover Kapur, Sun and Wangs algorithm nor the implementation of Wibmers theory by Antonio Montes[9]. These are seen as refinements of the material already covered, and covering them would exceed the scope of this introduction. Instead, we focus on tying the algorithm of Suzuki and Sato to the theory of Wibmer. This is how modern implementations of parametric Gröbner bases are implemented, but doesn't seem to be described in detail in the literature.

New contributions of this project include

- Fixing edge-case bugs in the pseudo-code in [11], see algorithm 1
- Modifying the Suzuki-Sato algorithm to produce Gröbner covers, see theorem 3.5
- Placing pseudo-division as a central tool of Gröbner covers and comprehensive Gröbner bases, see section 2.2 and 5.2
- Identifying a mistake in [10] and fixing it using comprehensive Gröbner bases, see section 5.3
- A new implementation of comprehensive Gröbner bases in the Julia programming language with demonstrations of their applications.

# 1 Preliminaries

This project will assume familiarity with commutative ring theory and multivariate polynomials over fields. A familiarity with Gröbner bases will be beneficial, but we will introduce the necessary notations and definitions.

Let $A$ be a Noetherian, commutative ring and $X = (x_1, x_2, \dots, x_n)$ be an ordered collection of variables. We denote the ring of polynomials in these variables $A[X]$. Given two disjoint sets of variables $X$ and $Y$, we will use $A[X, Y]$ to mean $A[X \cup Y]$, which is isomorphic to $A[X][Y]$. A *monomial* is a product of variables and a *term* is a monomial times a coefficient. We denote a monomial as $X^\nu$ for some $\nu \in \mathbb{N}^n$. For a polynomial

$$f = \sum_{\nu \in \mathbb{N}^n} a_\nu X^\nu$$

we denote the coefficient of the term $t = a_\nu X^\nu$ by $\operatorname{coef}(f, X^\nu) = a_\nu$. Note, that $\operatorname{coef}(f, X^\nu)$ is defined for any monomial $X^\nu$, but we can only have $\operatorname{coef}(f, X^\nu) \neq 0$ for finitely many $\nu \in \mathbb{N}^n$. For example in $f = xy + 2$, we have $\operatorname{coef}(f, xy) = 1$, $\operatorname{coef}(f, 1) = 2$ and $\operatorname{coef}(f, x) = 0$.

**1.1 · Definition (Monomial order, leading term).** A *monomial order* is a well-order[a] $<$ on the set of monomials satisfying that $u < v \implies wu < wv$ for all monomials $u, v, w$.

Given a monomial order $<$ and a polynomial $f \in A[X]$, the *leading term* of $f$ is the term with the largest monomial w.r.t. $<$ and is denoted by $\operatorname{lt}_<(f)$. If $\operatorname{lt}_<(f) = a \cdot m$ for some monomial $m$ and $a \in A$, then we denote $\operatorname{lm}_<(f) = m$ and $\operatorname{lc}_<(f) = a$. If $<$ is clear from context, it will be omitted.

[a] A total order, for which any chain $a > b > c > \dots$ must be finite.

These definitions naturally extend to sets of polynomials, so given a set of polynomials $F \subset A[X]$, we denote $\operatorname{lm}_<(F) := \{\operatorname{lm}_<(f) \mid f \in F\}$. With this, we can give the definition of a Gröbner basis. Usually, this is done over a field. For a reference on Gröbner bases over rings, see [7]. The standard reference on Gröbner bases is [1].

**1.2 · Definition (Gröbner basis).** Let $G \subset A[X]$ be a finite set of polynomials and $<$ be a monomial order. We say $G$ is a *Gröbner basis* if the ideal generated by leading terms of $G$ is equal to the ideal generated by leading terms of the ideal generated by $G$, i.e. $\langle \operatorname{lt}_<(G) \rangle = \langle \operatorname{lt}_<(\langle G \rangle) \rangle$.

Note, that if $A$ is a field, then it is enough that $\langle \operatorname{lm}_<(G) \rangle = \langle \operatorname{lm}_<(\langle G \rangle) \rangle$. We say $G$ is a Gröbner basis for an ideal $I$ if $G$ is a Gröbner basis and $\langle G \rangle = I$. We will also use an alternative description of Gröbner bases.

**1.3 · Definition (Reduction modulo).** Let $f, g \in A[X]$ be polynomials and $<$ be a monomial order order. We say $f$ *reduces modulo* $g$ if $\operatorname{lt}_<(g) \mid \operatorname{lt}_<(f)$, since in that case $\operatorname{lt}_<(\operatorname{lc}_<(g) \cdot f - p \cdot \operatorname{lc}_<(f) \cdot g) < \operatorname{lt}_<(f)$ where $\operatorname{lm}_<(f) = p \cdot \operatorname{lm}_<(g)$. We say a polynomial reduces modulo a set of polynomials $F$ if it reduces modulo any polynomial in $F$. We say

a polynomial *reduces to zero* modulo $F$ if there is a chain of reductions that end in the zero polynomial.

**1.4 · Theorem.** *Let $G \subset A[X]$. Then $G$ is a Gröbner basis if and only if every polynomial in $\langle G \rangle$ reduces to 0 modulo $G$.*

*Proof.* A good exercise. □

A Gröbner basis need not be unique. Indeed, given a Gröbner basis G, we can add any element of $\langle G \rangle$ to $G$ and it is still a Gröbner basis. However, reduced Gröbner bases are unique.

**1.5 · Definition (Reduced Gröbner basis).** A Gröbner basis $G$ is called *reduced* if, for all $g \in G$, $g$ is a monic polynomial (i.e. $\mathrm{lc}_<(g) = 1$) and the only term of $g$ in $\mathrm{lt}_<(\langle G \rangle)$ is $\mathrm{lt}_<(g)$.

**1.6 · Theorem.** *Let $I \subset k[X]$ be an ideal in a polynomial ring over a field. Then there is a unique reduced Gröbner basis of $I$.*

It is worth noting, that the second condition of reduced Gröbner bases is equivalent to saying that every term of $g$ is irreducible modulo $G$, except for its leading term.

# 2 Definitions and initial results

## 2.1 Parametric Gröbner bases and their motivation

Gröbner bases are a central tool when doing almost any computations on ideals in multivariate polynomial rings. Gröbner bases helps us to decide ideal membership, and when using a suitable term order it helps us to intersect ideals, eliminate variables, decide radical membership etc. Sometimes, we wish to study a family of ideals, parameterized by some variables. We could for instance ask for which values of $a$ and $b$ we have $ax - 1 \in \langle bx - 1 \rangle$. While this example is admittedly simple, answering such questions in general would require us to be able to describe a Gröbner basis for a parameterized ideal, no matter what value the parameters take. In this simple example, $ax - 1 \in \langle bx - 1 \rangle$ if and only if $a = b$ unless $b = 0$ in which case the inclusion hold for any value of $a$. This corresponds to the observation that $bx - 1$ is a Gröbner basis for the ideal and when $b = 0$, 1 is a Gröbner basis.

We will gradually look at more structured ways of describing the Gröbner basis of a parameterized ideal. The first definition was introduced by Volker Weispfenning in [14].

**2.1 · Definition (Comprehensive parametric Gröbner basis).** Let $A$ be a commutative, Noetherian ring, $k_1$ be a field, $X$ be a set of variables and let $F \subset A[X]$ be a finite set of polynomials. A *comprehensive parametric Gröbner basis* of $\langle F \rangle$ is a finite set of polynomials $G \subset \langle F \rangle$ such that $\sigma(G)$ is a Gröbner basis of $\langle \sigma(\langle F \rangle) \rangle$ for any ring homomorphism $\sigma : A \to k_1$. Here $\sigma(f)$ for an $f \in A[X]$ denotes the coefficient-wise application of $\sigma$ on $f$.

*Remark.* Most of this text will focus on the special case when $k$ is a field contained in $k_1$, $U$ is another set of variables with $U \cap X = \emptyset$ and $A = k[U]$. Then $\sigma : k[U] \to k_1$ corresponds to a choice of value for each variable in $U$. Since $k[U][X]$ is isomorphic to $k[X, U]$, we will often refer to parametric Gröbner bases of an ideal $I \subset k[X, U]$. It is also important to see, that $\langle \sigma(F) \rangle = \langle \sigma(\langle F \rangle) \rangle$ for any finite $F \subset A[X]$ and any specialization $\sigma$.

For example, consider the ideal $I = \langle ux + y, y^2 + 1 \rangle \subset \mathbb{C}[u][x, y]$. The given generators form a Gröbner basis of $I$ w.r.t. the lexicographic monomial order, and also for every choice of $u$, except $u = 0$. In this case, the generators become $\{y, y^2 + 1\}$, which is not a Gröbner basis. Indeed, $\langle y, y^2+1 \rangle = \mathbb{C}[x, y]$, so $1 \in \langle \mathrm{lm}(\langle y, y^2+1 \rangle) \rangle$. But $\langle \mathrm{lm}(\{y, y^2+1\}) \rangle = \langle y \rangle$, which does not contain 1.

We call a ring homomorphism $\sigma : k[U] \to k_1$ a *specialization*. Since $\sigma|k : k \to k_1$ is always injective, we can assume without loss of generality that $k \subset k_1$ and that $\sigma$ restricted to $k$ is the identity, i.e. $\sigma|k = id$. By the linearity of $\sigma$, we can characterize $\sigma$ uniquely by its image of $U$. Thus, we can identify $\{\sigma : k[U] \to k_1 \mid \sigma \text{ is a ring hom.}\}$ with the affine space $k_1^{|U|}$. For $\alpha \in k_1^{|U|}$ we'll denote the corresponding map

$$\sigma_\alpha(u_i) = \alpha_i \quad \text{for } u_i \in U$$

extended linearly.

It should be noted, that for computing Gröbner bases of ideals in the ring $k[U][X]$, it suffices to compute a Gröbner basis of the ideal, just viewing it as an ideal in $k[X,U]$ with respect to a monomial order where $X^{v_1} > U^{v_2}$ for all vectors of natural numbers $v_1, v_2$. This is proven in lemma 2.8.

**2.2 · Example.** The behaviour of the ideal of leading monomials is highly erratic under specializations. If $F$ is a generating set for some ideal $I \subset A[X]$ and $\sigma : A \to k_1$ is a specialization, then we can have all of the following scanarios:

- $\langle \mathrm{lm}(\sigma(I))\rangle = \langle \mathrm{lm}(I)\rangle$
  If $F = \{x^2 + u\} \subset \mathbb{C}[u][x]$ and $\sigma : \mathbb{C}[u] \to \mathbb{C}$ sets $\sigma(u) = 0$, then $\sigma(F) = \{x^2\}$, hence $\langle x^2\rangle = \langle \mathrm{lm}(\sigma(I))\rangle = \langle \mathrm{lm}(I)\rangle = \langle x^2\rangle$.
- $\langle \mathrm{lm}(\sigma(I))\rangle \subsetneq \langle \mathrm{lm}(I)\rangle$
  If $F = \{ux, y\} \subset \mathbb{C}[u][x]$ and $\sigma : \mathbb{C}[u] \to \mathbb{C}$ sets $\sigma(u) = 0$, then $\sigma(F) = \{y\}$, hence $\langle y\rangle = \langle \mathrm{lm}(\sigma(I))\rangle \subsetneq \langle \mathrm{lm}(I)\rangle = \langle x, y\rangle$.
- $\langle \mathrm{lm}(I)\rangle \subsetneq \langle \mathrm{lm}(\sigma(I))\rangle$
  If $F = \{ux^2 + x\} \subset \mathbb{C}[u][x]$ and $\sigma : \mathbb{C}[u] \to \mathbb{C}$ sets $\sigma(u) = 0$, then $\sigma(F) = \{x\}$, hence $\langle x^2\rangle = \langle \mathrm{lm}(I)\rangle \subsetneq \langle \mathrm{lm}(\sigma(I))\rangle = \langle x\rangle$.
- $\langle \mathrm{lm}(I)\rangle \not\subset \langle \mathrm{lm}(\sigma(I))\rangle$ and $\langle \mathrm{lm}(\sigma(I))\rangle \not\subset \langle \mathrm{lm}(I)\rangle$
  If $F = \{ux^2 + x, uy\} \subset \mathbb{C}[u][x]$ and $\sigma : \mathbb{C}[u] \to \mathbb{C}$ sets $\sigma(u) = 0$, then $\sigma(F) = \{x\}$, hence $\langle \mathrm{lm}(I)\rangle = \langle x^2, y\rangle$ which is neither a subset nor a superset of $\langle \mathrm{lm}(\sigma(I))\rangle = \langle x\rangle$.

As can be seen from the above example, a set of generators can form a parametric Gröbner basis for a restricted set of specializations. Sometimes we are only interested in a subset of specializations. Since a specialization is uniquely determined by its image of the parameters, we use subsets of $k_1^{|U|}$ to describe these restrictions. Since the end goal of this is to compute parametric Gröbner bases, we want to work with subsets that can be described in a computationally feasible way. We use the Zariski topology, where closed sets (and hence open sets) can be described by a finite set of polynomials.

**2.3 · Definition (Vanishing sets & locally closed sets).** Let $k \supset k_1$ be fields and $E \subset k[X]$. Then the *vanishing set* of $E$ is $\mathbf{V}(E) := \{v \in k_1^n \mid e(v) = 0 \ \ \forall e \in E\}$. If $f \in k[X]$ we will write $\mathbf{V}(f)$ to mean $\mathbf{V}(\{f\})$.

A *locally closed set*[a] is a set of the form $\mathbf{V}(E) \setminus \mathbf{V}(N)$ for two closed sets $\mathbf{V}(E)$ and $\mathbf{V}(N)$.

[a] Called such because if $Y = C \setminus D$ is a locally closed set, then $Y$ is closed set in the subspace topology on $D^c$

For example, when working over $k = \mathbb{R}$, we have $\mathbf{V}(0) = \mathbb{R}^n$, $\mathbf{V}(1) = \emptyset$ and $\mathbf{V}(x^2+y^2-1)$ is the unit circle in $\mathbb{R}^2$. $\mathbf{V}(x^2 + y^2 - 1) \setminus \mathbf{V}(x)$ is the unit circle in $\mathbb{R}^2$ with the $x$-axis removed. The Zariski topology is defined as having a subset $C \subset k_1^n$ being closed if and only if $C = \mathbf{V}(E)$ for some $E \subset k[X]$. It should be noted, that $\mathbf{V}(E) = \mathbf{V}(\langle E\rangle)$ for all

$E \subset k[X]$.

**2.4 · Definition (Parametric Gröbner basis).** Let $k \supset k_1$ be fields, let $X$ be a set of variables, let $F \subset k[U[X]$ be a finite set of polynomials and let $Y \subset k_1^{|U|}$ be a locally closed set. A *parametric Gröbner basis* of $\langle F\rangle$ on $Y$ is a finite set of polynomials $G \subset \langle F\rangle$ such that $\sigma(G)$ is a Gröbner basis of $\langle\sigma(\langle F\rangle)\rangle$ for any ring homomorphism $\sigma_\alpha : k[U] \to k_1$ with $\alpha \in Y$.

**2.5 · Definition (Gröbner system).** Let $Y$ be a locally closed set and $F, G \subset k[U][X]$ be finite sets. Then $(Y, G)$ is called a *segment of a Gröbner system for* $F$ if $\sigma_\alpha(G)$ is a Gröbner basis of $\langle\sigma_\alpha(F)\rangle$ for all $\alpha \in Y$. A set $\{(Y_1, G_1), \dots, (Y_t, G_t)\}$ is called a *Gröbner system* if each $(Y_i, G_i)$ is a segment of a Gröbner system.

We call the locally closed sets $Y_i$ for the *conditions* on a segment.

A Gröbner system $\{(Y_1, G_1), \dots, (Y_t, G_t))\}$ is called *comprehensive*, if $\bigcup_{i=1}^t Y_i = k_1^{|U|}$. We also say a Gröbner system is *comprehensive on* $L \subset k_1^{|U|}$ if $\bigcup_{i=1}^t Y_i = L$.

We will sometimes call a triple $(E, N, G)$ for a segment of a Gröbner system. By this we mean that $(V(E) \setminus V(N), G)$ is a segment of a Gröbner system. Do also note, that for segments of a Gröbner system, we relax the restriction that $G \subset \langle F\rangle$ to just $G \subset A[X]$.

Gröbner systems and parametric Gröbner bases are restricted to ideals in $k[U][X]$ instead of over a more general ring $A[X]$. Section 4 will cover the more general case.

**2.6 · Example.** Consider again the ideal $J = \langle ux^2 + y, y^2 + 1\rangle \subset \mathbb{C}[u][x, y]$. It shouldn't be hard to convince yourself that the given generators form a Gröbner basis under any specialization where $\sigma(u) \neq 0$. For the specialization setting $\sigma(u) = 0$, we have $\langle\sigma(J)\rangle = \langle 1\rangle$. Hence, we have the following comprehensive Gröbner system:

$$\{(\mathbf{V}(0) \setminus \mathbf{V}(u), \{ux^2 + y, y^2 + 1\}), \quad (\mathbf{V}(u) \setminus \mathbf{V}(1), \{1\})\}$$

The first segment gives a parametric Gröbner basis of $J$ on $\mathbf{V}(0)\setminus\mathbf{V}(u)$. But since $1 \notin \mathbf{J}$, the second segment does not give a parametric Gröbner basis of $J$ on $\mathbf{V}(u) \setminus \mathbf{V}(1)$. However, $-y(ux^2 + y) + (y^2 + 1) = -ux^2y + 1 \in J$ specializes to 1 when $\sigma(u) = 0$. Hence, we also have the following Gröbner system, which also gives a comprehensive parametric Gröbner basis:

$$\{(\mathbf{V}(0) \setminus \mathbf{V}(1), \{ux^2 + y, y^2 + 1, -ux^2y + 1\})\}$$

**2.7 · Definition (Leading coefficient w.r.t. variables).** Let $f \in k[U][X]$. Then the leading term of $f$ is denoted $\mathrm{lt}_U(f)$, the leading coefficient is $\mathrm{lc}_U(f)$ and the leading monomial is $\mathrm{lm}_U(f)$. These notations are also used when $f \in k[X, U]$, just viewing $f$ as a polynomial in $k[U][X]$.

Note that $\mathrm{lc}_U(f) \in k[U]$, i.e. the leading term is a polynomial in $k[U]$ times a monomial in $X$. For example, the polynomial $f = ux + vx + 1 \in C[x, u, v]$ has $\mathrm{lc}_{\{u,v\}}(f) = u + v$, $\mathrm{lm}_{\{u,v\}}(f) = x$ and $\mathrm{lt}_{\{u,v\}}(f) = (u + v)x$.

From this point, we assume that the monomial order on $k[X,U]$ satisfies $X^{v_1} > U^{v_2}$ for all $v_1 \in \mathbb{N}^{|X|}$ and $v_2 \in \mathbb{N}^{|U|}$. We will write this property as $X \gg U$. This monomial order restricts to a monomial order on $k[X]$, denoted by $<_X$. Note that this assumption is not too restrictive, as we're usually only interested in a certain monomial order on the variables, since the parameters will be specialized away anyway. Thus for a given monomial order $<_X$, we can construct a suitable monomial order on $k[X,U]$, by using $<_X$ and breaking ties with any monomial order on $k[U]$. The lexicographic order with $X > U$ satisfies $X \gg U$. The reason for this assumption is the following lemma:

**2.8 · Lemma.** *Let $<$ be a monomial order on $k[X,U]$ such that $X \gg U$, let $I \subset k[X,U]$ be an ideal and let $G = \{g_1, \dots, g_n\}$ be a Gröbner basis of $I$ w.r.t. $<$. Then $G$ can be seen as a Gröbner basis of $I \subset k[U][X]$ w.r.t. the restricted monomial order $<_X$.*

*Proof.* Let $f \in I \subset k[X,U]$., then we need to prove that $\mathrm{lt}_U(f) \in \langle \mathrm{lt}_U(G) \rangle$. Since $G$ is a Gröbner basis of $I$ in $k[X,U]$, we can write

$$f = \sum_{i=1}^{n} h_i g_i$$

where $\mathrm{lm}(f) \geq \mathrm{lm}(g_i, h_i)$ for each $i$. Since $X \gg U$ this implies $\mathrm{lm}_U(f) \geq \mathrm{lm}_U(g_i, h_i)$ for each i. Since we have the inequality $\mathrm{lm}_U(f) \geq \mathrm{lm}_U(g_i h_i)$, the leading term of $f$ can only be produced by leading terms of $g_i h_i$. Now, the equation above still holds when we see $f, g_1, \dots, g_n, h_1, \dots, h_n$ as elements of $k[U][X]$. Let $J = \{i \in \{1, \dots, n\} \mid \mathrm{lm}_U(h_i g_i) = \mathrm{lm}_U(f)\}$. Since $\mathrm{lt}_U(g_i h_i) = \mathrm{lt}_U(g_i)\,\mathrm{lt}_U(h_i)$, we have

$$\mathrm{lt}_U(f) = \sum_{i \in J} \mathrm{lt}_U(h_i)\,\mathrm{lt}_U(g_i)$$

so $\mathrm{lt}_U(f) \in \langle \mathrm{lt}_U(G) \rangle$, and so $G$ is a Gröbner basis of $I \subset k[U][X]$. □

## 2.2 Pseudo-division

The division algorithm for polynomial rings over fields form the basis of most of the applications of Gröbner bases. One could even say that having a well-behaved remainder under the division algorithm is one of the primary motivations behind Gröbner bases. Pseudo-division will turn out to be equally important in the parametric setting. The idea is straight-forward. Suppose you want to divide $ax$ by $bx$ in $k[a,b][x]$. Since $b$ does not divide $a$, it seems we are stuck. But that is only due to the nature of the ring we work over (specifically that it's not a field) rather than the structure of the polynomials. Had $a$ and $b$ been any non-zero field elements, the division would be easy.

Pseudo-division is a way to overcome the fact, that our ground ring may not be a field. The idea is to allow ourselves to scale the polynomial by an appropriate scalar from the ground ring. In the case above, we can't divide $ax$ by $bx$, but we can divide $b(ax)$ by $bx$ and get a remainder of zero. Pseudo-division in a restricted setting over $k[U][X]$ can be found in [1]. I am not aware that the rest of the results in this subsection appear in literature, but they have been extracted from proofs of other theorems in [15], [9].

**2.9 · Definition (Pseudo-division).** Let $f, f_1, f_2, \dots, f_n, g_1, g_2, \dots, g_n, r \in A[X]$ be polynomials and let $c \in A$. A *pseudo-division of $f$ modulo $g_1, \dots, g_n$* is a relation

$$cf = r + \sum_{i=1}^{n} f_i g_i$$

where the following is satisfied:

1. $c = \prod_{j \in J} \operatorname{lc}(g_j)^{p_j}$ for some subset $J \subset \{1, 2, \dots, n\}$ and powers $p_j \in \mathbb{N}$.
2. $\operatorname{lm}(f_i) \operatorname{lm}(g_i) \leq \operatorname{lm}(f)$ for all $i \in \{1, 2, \dots, n\}$.
3. No term of $r$ is divisible by $\operatorname{lm}(g_i)$ for any $i$.
4. $\operatorname{coef}(f_i, m) \in \langle \operatorname{coef}(f, m') \mid m' \geq \operatorname{lm}(g_i m) \rangle$ for all $i \in \{1, 2, \dots, n\}$ and monomials $m$.

We call $r$ a *pseudo-remainder* and the $f_i$'s are called *pseudo-quotients*.

**2.10 · Theorem.** *Let $f, g_1, g_2, \dots, g_n \in A[X]$ be polynomials. Then there exists a pseudo-division of $f$ modulo $g_1, \dots, g_n$.*

*Proof.* See the appendix, section A.1 □

Pseudo-division allows us to overcome the problem, that our ground ring isn't a field, but we still have to be careful. If $b$ happened to be zero, then we cannot divide $ax$ by $bx$. Hence, we need some assumptions on the leading terms we divide with. The reason is that, after specialization, a pseudo-division turns into a regular multivariate division. Hence, parametric Gröbner bases and pseudo-division inherit all the nice properties Gröbner bases has under regular division.

**2.11 · Lemma.** *Let $f \in A[X]$, let $\{g_1, \dots, g_n\} \subset A[X]$, let $\sigma : A \to k_1$ be a ring homomorphism and let*

$$cf = r + \sum_{i=1}^{n} f_i g_i$$

*be a pseudo-division. Then*

$$\sigma(cf) = \sigma(r) + \sum_{i=1}^{n} \sigma(f_i)\sigma(g_i)$$

*satisfies $\operatorname{lm}(\sigma(f_i g_i)) \leq \operatorname{lm}(\sigma(f))$. Furthermore, if $\sigma(\operatorname{lc}(g_i)) \neq 0$ for all $i$, then either $\sigma(r) = 0$ or none of the terms of $\sigma(r)$ is divisible by any leading term of the $\sigma(g_i)$'s.*

*Proof.* The first equality follows directly since $\sigma$ is a ring homomorphism. For the inequality $\operatorname{lm}(\sigma(f_i g_i)) \leq \operatorname{lm}(\sigma(f))$, we have the fourth condition from pseudo-divisions: $\operatorname{coef}(f_i, m) \in \langle \operatorname{coef}(f, m') \mid m' \geq m \operatorname{lm}(g_i) \rangle$. Hence for any monomial $m$ with $m \operatorname{lm}(g_i) \geq \operatorname{lm}(\sigma(f))$, we have $\sigma(\operatorname{coef}(f_i, m \operatorname{lm}(g_i))) = 0$, since $\langle \operatorname{coef}(f, m) \mid m \geq \operatorname{lm}(\sigma(f)) \rangle = \langle 0 \rangle$.

For the remainder, we have from pseudo-division that no term of $r$ is divisible by any

$\mathrm{lt}(g_i)$. Assuming $\sigma(\mathrm{lc}(g_i)) \neq 0$ for all $i$, we have $\mathrm{lm}(g_i) = \mathrm{lm}(\sigma(g_i))$ for all $i$. Hence, no term of $\sigma(r)$ is divisible by any $\mathrm{lm}(\sigma(g_i))$, and since we work over a field, no term of $\sigma(r)$ is divisible by any $\mathrm{lt}(\sigma(g_i))$. □

If we have a Gröbner basis after specialization, then that division "lifts" to a pseudo-division before specialization. That is the content of this rather technical lemma.

**2.12 · Lemma.** *Let $G = \{g_1, \dots, g_n\} \subset A[X]$, let $f \in \langle G \rangle$ and let $\sigma : A \to K_1$ be a specialization such that $\sigma(\mathrm{lc}(g_i)) \neq 0$ for all $i$. If $\sigma(f)$ reduces to zero mod $\sigma(g_1), \dots, \sigma(g_n)$, then there is some $h \in \langle G \rangle$ and $b \in A \setminus \ker(\sigma)$ such that $\sigma(bf) = \sigma(h)$ and $\mathrm{lm}(h) = \mathrm{lm}(\sigma(f))$.*

*Proof.* The proof is by induction on the monomial order $<$ in $\mathrm{lm}(\sigma(f))$. The base case is $\sigma(f) = 0$, in which case we can choose $h = 0 \in \langle G \rangle$ and $b = 1$.

Now, let $\sigma(f) \neq 0$ reduce to zero mod $\sigma(g_1), \dots, \sigma(g_n)$, and suppose for every $f' \in \langle G \rangle$ with $\mathrm{lm}(\sigma(f')) < \mathrm{lm}(\sigma(f))$, there is some $h' \in \langle G \rangle$ and $b \in A \setminus \ker(\sigma)$ such that $\sigma(b' f') = \sigma(h')$ and $\mathrm{lm}(h') = \mathrm{lm}(\sigma(f'))$. Let

$$\sigma(f) = \frac{\mathrm{lc}(\sigma(f))}{\mathrm{lc}(\sigma(g_i))}\sigma(g_i) + r$$

with $\mathrm{lm}(r) < \mathrm{lm}(\sigma(g))$ be the first step of the reduction to zero. Since $\sigma(\mathrm{lc}(g_i)) \neq 0$, we have that $\mathrm{lc}(\sigma(g_i)) = \sigma(\mathrm{lc}(g_i))$. Then we have

$$\sigma(f) = \frac{\mathrm{lc}(\sigma(f))}{\sigma(\mathrm{lc}(g_i))}\sigma(g_i) + r \iff \sigma(\mathrm{lc}(g_i) f) = \mathrm{lc}(\sigma(f))\sigma(g_i) + \mathrm{lc}(g_i) r$$

Thus, $\mathrm{lc}(\sigma(f)) = \sigma(\mathrm{coef}(f, \mathrm{lm}(\sigma(f))))$, and so

$$f' = \mathrm{lc}(g_i) f - \mathrm{coef}(f, \mathrm{lm}(\sigma(f)))g_i \in \langle G \rangle$$

satisfies either $\sigma(f') = 0$ or $\mathrm{lm}(\sigma(f')) < \mathrm{lm}(\sigma(f))$. In the first case, we've reached the base case, so we are done. Otherwise, $\sigma(f')$ is reducible to zero mod $\sigma(g_1), \dots, \sigma(g_n)$ via the rest of the reduction of $\sigma(f)$, so we can find $b' \in A \setminus \ker(\sigma)$ and $h' \in \langle G \rangle$ such that $\mathrm{lm}(h') = \mathrm{lm}(\sigma(f'))$ and $\sigma(b' f') = \sigma(h)$. Then let $b = b' \,\mathrm{lc}(g_i)$ and $h = h' + b' \,\mathrm{coef}(f, \mathrm{lm}(\sigma(f)))g_i$, so

$$\begin{aligned}
\sigma(bf) &= \sigma(\mathrm{lc}(g_i) b' f) \\
&= \sigma(b'(f' + \mathrm{coef}(f, \mathrm{lm}(\sigma(f)))g_i)) \\
&= \sigma(h' + b' \,\mathrm{coef}(f, \mathrm{lm}(\sigma(f)))g_i) \\
&= \sigma(h)
\end{aligned}$$

and $\mathrm{lm}(h) = \mathrm{lm}(g_i) = \mathrm{lm}(\sigma(g_i)) = \mathrm{lm}(\sigma(f))$. Finally, since $b', \mathrm{lc}(g_i) \notin \ker(\sigma)$, we have $b \notin \ker(\sigma)$. This uses that $\ker(\sigma)$ is a prime ideal, which is true since its codomain is a field. □

Since remainders modulo a Gröbner basis $G$ are unique, we have that $f \in \langle G \rangle$ if and only if $f$ leaves a remainder of 0 under division modulo $G$. We have the following analogous statement for parametric Gröbner bases and pseudo-division.

**2.13 · Lemma.** *Let $(Y, G)$ be a segment of a parametric Gröbner basis with $G = \{g_1, \dots, g_n\} \subset A[X]$, let $f \in A[X]$ and let*

$$cf = r + \sum_{i=1}^{n} f_i g_i, \quad c'f = r' + \sum_{i=1}^{n} f_i' g_i$$

*be pseudo-divisions. If $\sigma_\alpha(\mathrm{lc}(g)) \neq 0$ for all $\alpha \in Y$ and $g \in G$, then*

$$\sigma_\alpha(r'c) = \sigma_\alpha(rc')$$

*for all specializations $\sigma_\alpha$ with $\alpha \in Y$, and $\sigma_\alpha(f) \in \langle \sigma_\alpha(G) \rangle$ if and only if $\sigma_\alpha(r) = 0$.*

*Proof.* Consider

$$\begin{aligned} 0 &= \sigma_\alpha(c'cf) - \sigma_\alpha(c'cf) \\ &= \sigma_\alpha(cr') - \sigma_\alpha(c'r) + \sum_{i=1}^{n} \left(\sigma_\alpha(cf_i') - \sigma_\alpha(c'f_i)\right) \sigma_\alpha(g_i). \end{aligned}$$

Since $\sum_{i=1}^{n} (\sigma_\alpha(cf_i') - \sigma_\alpha(c'f_i))\sigma_\alpha(g_i) \in \langle \sigma_\alpha(G) \rangle$, we must have $\sigma_\alpha(c'r) - \sigma_\alpha(cr') \in \langle \sigma_\alpha(G) \rangle$. If $\sigma_\alpha(c't) - \sigma_\alpha(cr') \neq 0$ then, since $\sigma_\alpha(G)$ is a Gröbner basis, that would imply that the leading term of $\sigma_\alpha(c'r) - \sigma_\alpha(cr')$ is divisible by some $\mathrm{lm}(\sigma_\alpha(g_i))$. But that would imply some term of either $\sigma_\alpha(c'r)$ or $\sigma_\alpha(cr')$ is divisible by that $\mathrm{lm}(\sigma_\alpha(g_i))$. Since $\mathrm{lm}(\sigma_\alpha(g_i)) = \mathrm{lm}(g_i)$ and no term of $r$ is divisible by any $\mathrm{lm}(g_i)$ (by the properties of pseudo-division), this cannot happen. Hence $\sigma_\alpha(c'r) - \sigma_\alpha(cr') = 0$.

For the last assertion, if $\sigma_\alpha(r) = 0$, then clearly $\sigma_\alpha(f) \in \langle \sigma_\alpha(G) \rangle$. On the other hand, if $\sigma_\alpha(f) \in \langle \sigma_\alpha(G) \rangle$, then $\sigma_\alpha(f)$ reduces to 0 mod $\sigma_\alpha(G)$ since $\sigma_\alpha(G)$ is a Gröbner basis. Hence, by lemma 2.12, there is a $h \in \langle G \rangle$ and $b \in A \setminus \ker(\sigma_\alpha)$ such that $\sigma_\alpha(h) = \sigma_\alpha(bf)$. Hence, we can find a pseudo-reduction $h = \sum h_i g_i$ and hence $bf = r + h = r + \sum h_i g_i$ for some $r \in \ker(\sigma_\alpha)$ is a pseudo-reduction with $\sigma_\alpha(r) = 0$. □

**2.14 · Example.** Consider the comprehensive parametric Gröbner basis $G = \{ax + y, bx + y, (a-b)y\} \subset \mathbb{C}[a,b,c][x,y]$ and the element $f = cxy + 1 \in \mathbb{C}[a,b,c][x,y]$. On the segment $\mathbf{V}(0) \setminus \mathbf{V}(ab(a-b))$, we can find a pseudo-reduction. First, reduce the term $cxy$ using $ax + y$:

$$(a)(cxy + 1) = (cy)(ax + y) - cy^2 + a$$

leaving a remainder of $-cy^2 + a$. This remainder can be reduced using $(a-b)y$:

$$(a-b)(a)(cxy + 1) = (a-b)(cy)(ax + y) - (cy)((a-b)y) + a^2 - ab$$

giving us the multiplier $c = a(a-b)$ and remainder $r = a^2 - ab$.

We could also have reduced the term $cxy$ using $(a-b)y$:

$$(a-b)(cxy + 1) = (cx)((a-b)y) + a - b$$

giving us a mulitplier $c' = (a-b)$ and remainder $a-b$. We see that $cr' = (a-b)(a^2-ab) =$

$(a-b)((a-b)a) = c'r$ in accordance with the theorem above.

If the segment induces relations between leading coefficients, this might show up in the pseudo-remainders. Consider the segment $(\mathbf{V}(a-b), \{ax+1, bx+1\})$ and the polynomial $abx$. Here, we find two different pseudo-remainders:

$$abx = (b)(ax+1) - b$$
$$abx = (a)(bx+1) - a$$

In accordance with the theorem, we have that $\sigma_\alpha(a) = \sigma_\alpha(b)$ for all $\alpha \in \mathbf{V}(a-b)$. Do note, that for $\alpha \notin \mathbf{V}(a-b)$, $\sigma_\alpha(\{ax+1, bx+1\})$ is not a Gröbner basis, hence the theorem does not apply here.

## 2.3 A criterion on stability

In this section we will prove a criterion to decide when a Gröbner basis $G$ of an ideal $\langle F \rangle$ maps to a Gröbner basis $\sigma(G)$ if the ideal $\langle \sigma(F) \rangle$. This is theorem 3.1 in [2].

**2.15 · Lemma.** *Let $G$ be a Gröbner basis of an ideal $\langle F \rangle \subset A[X]$ w.r.t. $<$, let $\sigma : A \to K$ be a ring homomorphism to a field $K$ and set $G_\sigma = \{g \in G \mid \sigma(\mathrm{lc}(g)) \neq 0\} = \{g_1, g_2, \dots, g_l\} \subset A[X]$. Then $\sigma(G_\sigma)$ is a Gröbner basis of the ideal $\langle \sigma(F) \rangle$ w.r.t. $<_X$ if and only if $\sigma(g)$ is reducible to 0 modulo $\sigma(G_\sigma)$ for every $g \in G$.*

*Proof.* First, we prove "$\Longrightarrow$": Suppose $\sigma(G_\sigma)$ is a Gröbner basis of $\langle \sigma(F) \rangle$. Since $\sigma(g) \in \langle \sigma(F) \rangle$, we get that $\sigma(g)$ reduces to zero modulo any Gröbner basis of $\langle \sigma(F) \rangle$ by theorem 1.4, in particular $\sigma(G_\sigma)$.

Next, we prove "$\Longleftarrow$": Assume that $\sigma(g)$ is reducible to 0 modulo $G_\sigma$ for every $g \in G$ and let $f \in \langle F \rangle$ such that $\sigma(f) \neq 0$. It's enough to show that

$$\exists\, h \in \langle F \rangle \,:\, \sigma(\mathrm{lc}(h)) \neq 0 \wedge \mathrm{lm}(h) \mid \mathrm{lm}(\sigma(f)).$$

Indeed, since $G$ is a Gröbner basis of $\langle F \rangle$, that implies there is some $g \in G$ such that $\mathrm{lm}(g) \mid \mathrm{lm}(h)$ and $\mathrm{lm}(h) = \mathrm{lm}(\sigma(h)) \mid \mathrm{lm}(\sigma(f))$. Furthermore, since $\mathrm{lc}(g) \mid \mathrm{lc}(h)$ and $\sigma(\mathrm{lc}(h)) \neq 0$, we have that $\sigma(\mathrm{lc}(g)) \neq 0$, hence $\mathrm{lt}(\sigma(g)) \mid \mathrm{lt}(\sigma(f))$. Thus, if the above holds for any $f$, then $\sigma(G)$ is a Gröbner basis of $\langle \sigma(F) \rangle$. We prove this claim by induction on $<_X$.

The base case is when $\mathrm{lm}(f) = 1$, which means $f \in A$. Since we assumed $\sigma(f) \neq 0$, we have $\mathrm{lm}(\sigma(f)) = \mathrm{lm}(f)$ and $\sigma(\mathrm{lc}(f)) \neq 0$.

Now, the induction step. Let $f \in \langle F \rangle$ with $\sigma(\mathrm{lc}(f)) \neq 0$ and assume that every $f' \in \langle F \rangle$ with $\mathrm{lm}(f') < \mathrm{lm}(f)$ we have $\exists\, h \in \langle F \rangle \,:\, \sigma(\mathrm{lc}(h)) \neq 0 \wedge \mathrm{lm}(h) \mid \mathrm{lm}(\sigma(f'))$. If $\sigma(\mathrm{lc}(f)) \neq 0$, we can simply use $h = f$, so consider the case when $\sigma(\mathrm{lc}(f)) = 0$. If there is some $\sigma(g) \in G_\sigma$ such that $\mathrm{lm}(g) \mid \mathrm{lm}(f)$, then we can reduce $f$ by $g$ to get $f' = \mathrm{lc}(g) \cdot f - \mathrm{lc}(f) \cdot \frac{\mathrm{lm}(f)}{\mathrm{lm}(g)} g$. Then $\mathrm{lm}(\sigma(f')) = \mathrm{lm}(\sigma(f))$ since $\sigma(\mathrm{lc}(f)) = 0$ and $\mathrm{lm}(f') < \mathrm{lm}(f)$, so the assertion holds by the induction hypothesis.

On the other hand, if there is no such $\sigma(g) \in G_\sigma$, then we must have some $g \in G \setminus G_\sigma$ such that $\operatorname{lm}(g) \mid \operatorname{lm}(f)$. However, we can't simply reduce by $g$, since the factor $\operatorname{lc}(g)$ is zero under $\sigma$. Instead, we can find a subset with $\{g_{j_1}, \dots, g_{j_r}\} \subset G \setminus G_\alpha$ such that

$$\operatorname{lt}(f) = \sum_{i=1}^{r} c_i \frac{\operatorname{lm}(f)}{\operatorname{lm}(g_{j_i})} \operatorname{lt}(g_{j_i}).$$

Since each of the $\sigma(g_{j_i})$ are reducible to 0 modulo $G_\sigma$, by lemma 2.12 we can find some $h_i \in \langle F \rangle$ and $b_i \in A \setminus \ker(\sigma)$ such that $\sigma(b_i g_{j_i}) = \sigma(h_i)$ and $\operatorname{lm}(\sigma(h_i)) = \operatorname{lm}(\sigma(g_{j_i})) > \operatorname{lm}(g_{j_i})$ for each $i \in \{1, \dots, r\}$. Let $b = \prod_{i=1}^{r} b_i$, which is non-zero, then

$$f' = bf - \sum_{i=1}^{r} c_i \frac{b}{b_i} \frac{\operatorname{lm}(f)}{\operatorname{lm}(g_{j_i})} (b_i g_{j_i} - h_i)$$

is a new polynomial with

$$\sigma(f') = \sigma(bf) - \sum_{i=1}^{r} \sigma\left( c_i \frac{b}{b_i} \frac{\operatorname{lm}(f)}{\operatorname{lm}(g_{j_i})} \right) (\sigma(b_i g_{j_i}) - \sigma(h_i)) = \sigma(bf)$$

hence $\operatorname{lm}(\sigma(f')) = \operatorname{lm}(\sigma(f))$ but also $\operatorname{lm}(f') < \operatorname{lm}(f)$ since $\operatorname{lm}(g_{j_i}) > \operatorname{lm}(h_i)$. Thus the conclusion follows from the induction hypothesis. □

**2.16 · Corollary.** *Let $G$ be a Gröbner basis of an ideal $\langle F \rangle \subset A[X]$ w.r.t. $<$ and let $\sigma : A \to K$ be a ring homomorphism to a field $K$. If $\sigma(\operatorname{lc}(g)) \neq 0$ for all $g \in G$, then $\sigma(G)$ is a Gröbner basis of $\langle \sigma(F) \rangle$.*

*Proof.* Let $G_\sigma = \{g \in G \mid \sigma(\operatorname{lc}(g)) \neq 0\}$. By assumption, $G_\sigma = G$, so lemma 2.15 applies immediately. □

We will use a consequence of this lemma, which uses a test that is much easier to check. We use the above lemma with $A = k[U]$.

**2.17 · Lemma.** *Let $G = \{g_1, g_2, \dots, g_k\}$ be a Gröbner basis of an ideal $\langle F \rangle$ in $k[X, U]$ w.r.t $<$ and let $\alpha \in k_1^{|U|}$. If $\sigma_\alpha(\operatorname{lc}_U(g)) \neq 0$ for each $g \in G \setminus k[U]$, then $\sigma_\alpha(G)$ is a Gröbner basis of $\langle \sigma_\alpha(F) \rangle$.*

*Proof.* First note that since $X^{v_1} > U^{v_2}$, any Gröbner basis of $\langle F \rangle \subset k[X, U]$ is also a Gröbner basis of $\langle F \rangle \subset k[U][X]$ by lemma 2.8. Let $G_\alpha = \{\sigma_\alpha(g) \mid \sigma_\alpha(\operatorname{lc}_U(g)) \neq 0\}$. If there is any $g \in G$, such that $\sigma_\alpha(g) \in k_1 \setminus \{0\}$, then $g \in G \cap k[U]$ since $\sigma_\alpha(\operatorname{lc}_U(g)) \neq 0$ for all $g \in G \setminus K[U]$. Furthermore, since $g \in \langle F \rangle$, we get that $\langle \sigma_\alpha(F) \rangle = k_1[X]$ and $\sigma_\alpha(G)$ is a Gröbner basis as it contains a unit.

If there is no such $g$, then $\alpha \in \mathbf{V}(G \cap k[U])$. Take any $g \in G$. If $\sigma_\alpha(g) \in G_\alpha$, then $\sigma_\alpha(g)$ is reducible to 0 modulo $G_\alpha$, since it's leading term is divisible by its own leading term.

On the other hand, if $\sigma_\alpha(g) \notin G_\alpha$, then we must have $g \in G \cap k[U]$. Since $\alpha \in \mathbf{V}(G \cap k[U])$ then $\sigma_\alpha(g) = 0$, so is immediately reducible to zero. Thus $\sigma_\alpha(G)$ is a Gröbner basis of $\langle \sigma_\alpha(F) \rangle$ by lemma 2.15. □

With lemma 2.17 in mind, we can start constructing Gröbner systems. Let $G$ be a reduced Gröbner basis of an ideal $\langle F\rangle \subset k[X,U]$, and let $H = \{\mathrm{lc}_U(g) \mid g \in G \setminus k[U]\}$. Then $\big(\mathbf{V}(0) \setminus \bigcup_{h\in H} \mathbf{V}(h), G\big)$ is a segment of a Gröbner system. Thus, to make a Gröbner system, we need to find segments covering $\bigcup_{h\in H} V(h) = V(\mathrm{lcm}(H))$. As we will see later, we can find a Gröbner basis under the condition $\mathbf{V}(S)$ for some $S \subset k[U]$, by computing a Gröbner basis of $\langle F \cup S\rangle$ and remove everything in $\langle S\rangle$.

**2.18 · Example.** Consider the ideal $I = \langle ax + cy, bx + dy\rangle \subset \mathbb{C}[a,b,c,d][x,y]$. The reduced Gröbner basis for $I$ w.r.t. the lexicographic order with $x > y$ is $G = \{ax + cy, bx+dy, (ad-bc)y\}$. The leading coefficients are $\{a, b, ad-bc\}$, so for any specialization with $\sigma(a), \sigma(b), \sigma(ad - bc) \neq 0$, this specializes to a Gröbner basis. This is equivalent to requiring that $\sigma(ab(ad - bc)) \neq 0$.

Now, we need to produce Gröbner systems covering the rest. If $\sigma(a) = 0$, then the ideal becomes $\langle cy, bx+dy, bcy\rangle$ with leading coefficients $\{c, b, bc\}$. Since $\sigma(bc) \neq 0 \iff \sigma(b) \neq 0 \wedge \sigma(c) \neq 0$ and we can reduce $bcy$ using $cy$, we have that $\{cy, bx + dy\}$ is a Gröbner basis of the segment $\mathbf{V}(a) \setminus \mathbf{V}(bc)$.

Moving on to the segment where $\sigma(a) = \sigma(b) = 0$, we're left with the generating set $\{cy, dy\}$, which is a Gröbner basis as long as $\sigma(c), \sigma(d) \neq 0$. It remains unchanged if only one of them vanishes, but when we add $\sigma(c) = \sigma(d) = 0$, we're left with the zero ideal.

Backtracking, we consider the case when $\sigma(a) = \sigma(c) = 0$. In this case the generating set is $\{bx + dy\}$ with leading coefficient $b$. Hence $\{bx + dy\}$ is a Gröbner basis when $\sigma(b) \neq 0$. Setting $\sigma(a) = \sigma(b) = \sigma(c) = 0$, we get a segment we have already computed. Hence, we have found the following partial Gröbner system. The indentations are meant to represent the recursive nature of the computation.

$$
\begin{aligned}
&\{(\mathbf{V}(0) \setminus \mathbf{V}(ab(ad-bc)), && \{ax + cy, bx + dy, (ad - bc)y\})\\
&\quad(\mathbf{V}(a) \setminus \mathbf{V}(bc), && \{cy, bx + dy\})\\
&\qquad(\mathbf{V}(a,b) \setminus \mathbf{V}(cd), && \{cy, dy\})\\
&\qquad\quad(\mathbf{V}(a,b,c) \setminus \mathbf{V}(d), && \{dy\})\\
&\qquad\qquad(\mathbf{V}(a,b,c,d) \setminus \mathbf{V}(1), && \{0\})\\
&\qquad\quad(\mathbf{V}(a,b,d) \setminus \mathbf{V}(c), && \{cy\})\\
&\qquad(\mathbf{V}(a,c) \setminus \mathbf{V}(b), && \{bc + dy\})\}
\end{aligned}
$$

A similar pattern emerges when we start by setting $\sigma(b) = 0$, which the reader is invited to work out themselves. When we set $\sigma(ad - bc) = 0$, we're left with the leading coefficients $\{a, b\}$, and when they do not vanish, we get the Gröbner basis $\{ax + cy, bx + dy\}$.

Setting $\sigma(ad - bc) = \sigma(a) = 0$, we get the generating set $\{cy, bx + dy\}$ with leading coefficients $\{b, c\}$. Hence $\{cy, bx+dy\}$ is a Gröbner basis of the segment $\mathbf{V}(ad-bc, a)\setminus\mathbf{V}(bc)$.

However, since $\mathbf{V}(ad-bc,a) = \mathbf{V}(a,bc)$, we see that this segment is actually empty.

Similarly, when we set $\sigma(ad-bc) = \sigma(b) = 0$, we get the leading coefficients $\{a,d\}$, hence the segment $\mathbf{V}(ad-bc,b) \setminus \mathbf{V}(ad)$. However, since $\mathbf{V}(ad-bc,b) = \mathbf{V}(ad,b)$, this segment is also empty. Thus, we have found a comprehensive Gröbner system for $I$.

It should be noted, that in this example we did not have to recompute the Gröbner basis because the Gröbner basis remained a Gröbner basis after specialization. If we take the example of $J = \langle ux+y, y^2+1\rangle \subset \mathbb{C}[u][x,y]$, the situation is different. The generators form a Gröbner basis, with leading coefficients $\{u,1\}$. Hence, $\{ux+y, y^2+1\}$ is a Gröbner basis on the segment $\mathbf{V}(0) \setminus \mathbf{V}(u)$. However, when we set $\sigma(u) = 0$, the remaining generating set is $\{y, y^2+1\}$, which is not a Gröbner basis. Instead, we compute the Gröbner basis of this segment to be $\{1\}$. Since $\sigma(1) = 0$ is never satisfied, we have the following Gröbner system for $J$:

$$\{\mathbf{V}(0) \setminus \mathbf{V}(u), \{ux+y, y^2+1\}, \quad (\mathbf{V}(u) \setminus \mathbf{V}(1), \{1\})\}$$

# 3 Computing Gröbner systems

In this section, we will see how to compute Gröbner systems. We will develop algorithms based on the ones in [11]. Part of this project included developing a full implementation of these algorithms in the Julia language, which can be found at https://github.com/0708andreas/ParametricGrobnerBases.jl. The code includes both a direct implementation of algorithm 1, as well as an optimized version, utilizing a few optimizations not described here. The code is developed with an emphasis on readability. If the reader is more familiar with Macaulay2, an implementation of the **CGS** algorithm is also implemented in Macaulay2, and can be found at https://github.com/0708andreas/ParametricGrobnerBases.M2.

Let us consider in more detail how we can construct Gröbner systems. Let $G$ be a reduced Gröbner basis of an ideal $\langle F\rangle \subset k[X,U]$, and let $H = \{\mathrm{lc}_U(g) \mid g \in G \setminus k[U]\}$. Then $\left(k_1^m \setminus \bigcup_{h\in H} V(h), G\right)$ is a segment of a Gröbner system. Thus, to make a Gröbner system, we need to find segments covering $\bigcup_{h\in H} V(h) = V(\mathrm{lcm}(H))$.

If we take $G$ to be a reduced Gröbner basis, then $h \notin \langle F\rangle$ for any $h \in H$ since then the corresponding leading term would be divisible by a leading term in $G$. This is not allowed when $G$ is reduced. Hence, we can find a Gröbner basis $G_1$ of $F \cup \{h\}$, which will then form a segment $(V(h) \setminus \bigcup_{h_1\in H_1} V(h_1), G_1)$ where $H_1 = \{\mathrm{lc}_U(g) \mid g \in G_1\}$. Since $k[X,U]$ is Noetherian, this will eventually stop, forming a Gröbner system.

This gives us the ingredients for a simple algorithm for computing Gröbner systems, Algorithm 1. We use **groebner** do denote a function computing the reduced Gröbner basis of an ideal, given a set of generators.

**Algorithm 1:** $\mathbf{CGS_{simple}}$, an algorithm for computing comprehensive Gröbner systems on $\mathbf{V}(S)$

INPUT: Two finite sets $F \subset k[X,U]$, $S \subset k[U]$
OUTPUT: A finite set of triples $(E,N,G)$, each forming a segment of a comprehensive Gröbner system on $\mathbf{V}(S)$.

```
if ∅ ≠ S ∩ (k \ {0}) then
    return ∅;
else
    G ← groebner(F ∪ S);
    H ← {lc_U(g) | g ∈ G \ ⟨S⟩};
    h ← lcm(H);
    return {(S, {h}, G \ ⟨S⟩)} ∪ ⋃_{h'∈H} CGS_simple(G, S ∪ {h'})
end
```

**3.1 · Theorem.** *Let $F \subset k[X,U]$ and $S \subset k[U]$ be finite sets of polynomials. Then $\mathbf{CGS_{simple}}(\mathbf{F},\mathbf{S})$ terminates and the output $\mathscr{H}$ is a comprehensive Gröbner system on $\mathbf{V}(S)$. Furthermore, if $(E,N,G) \in \mathscr{H}$, then $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for all $\alpha \in \mathbf{V}(E)\setminus\mathbf{V}(N)$ and $g \in G\setminus\langle E\rangle$.*

*Proof.* First, we prove termination. Let $F$ and $S$ be inputs to $\mathbf{CGS_{simple}}$, let $G$ be the reduced Gröbner basis of $F \cup S$ and let $H = \{\mathrm{lc}_U(g) \mid g \in G \setminus \langle S \rangle\}$. Take any $h \in H$. Since $G$ is reduced, $h \notin \langle S \rangle$. Indeed, take $g \in G$ to have $\mathrm{lc}(g) = h$. If $g \in G \cap k[U]$, then $g = h$, so $h \notin \langle S \rangle$ by construction. If $g \in G \setminus k[U]$, then $h \notin \langle S \rangle$, since if it was, then $G$ would contain a $h'$ that divides $h$. Then $g$ would be reducible by $h'$, which is not allowed when $G$ is reduced. Thus $\langle S \rangle \subsetneq \langle S \cup \{h\} \rangle$. Since this is the case at every recursive call, each successive call to $\mathbf{CGS_{simple}}$ will have a strictly greater ideal $\langle S \rangle$. Since $k[X, U]$ is Noetherian, this must stop eventually.

Next, we prove that if $(E, N, G) \in \mathscr{H}$, then $(\mathbf{V}(E) \setminus \mathbf{V}(N), G)$ is a segment of a Gröbner system. By the algorithm, $N = \{\mathrm{lcm}(H)\}$, where $H = \{\mathrm{lc}_U(g) \mid g \in G \setminus \langle S \rangle\}$ as before, for $G$ being the reduced Gröbner basis of $\langle F \cup S \rangle$. Hence, for any $\alpha \in \mathbf{V}(E) \setminus \mathbf{V}(N)$, we have that $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for every $g \in G \setminus \langle S \rangle \supset G \setminus k[U]$. Thus $\sigma_\alpha(G)$ is a Gröbner basis of $\langle \sigma_\alpha(F \cup S) \rangle$ by lemma 2.17. Also, $E = S$, so $\sigma_\alpha(S) = 0$. Hence $\langle \sigma_\alpha(F \cup S) \rangle = \langle \sigma_\alpha(F) \rangle$, so $\sigma_\alpha(G) \cup 0 = \sigma_\alpha(G \setminus \langle E \rangle) \cup \{0\}$ is a Gröbner basis of $\langle \sigma_\alpha(F) \rangle$. This also proves that that $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for all $\alpha \in \mathbf{V}(E) \setminus \mathbf{V}(h)$ and $g \in G \setminus \langle E \rangle$.

Finally, we need to prove that

$$\bigcup_{(E,N,G) \in \mathscr{H}} \mathbf{V}(E) \setminus \mathbf{V}(N) = \mathbf{V}(S).$$

Note, that since $\mathbf{V}(\mathrm{lcm}(H)) = \bigcup_{h \in H} \mathbf{V}(h)$, we have the following:

$$\begin{aligned} V(S) &= (\mathbf{V}(S) \setminus \mathbf{V}(\mathrm{lcm}(H))) \cup \bigcup_{h \in H} \mathbf{V}(h) \\ &= (\mathbf{V}(S) \setminus \mathbf{V}(\mathrm{lcm}(H))) \cup \bigcup_{h \in H} \mathbf{V}(S \cup \{h\}) \end{aligned}$$

Inductively, the recursive calls to $\mathbf{CGS_{simple}}$ will compute Gröbner systems covering $\bigcup_{h \in H} \mathbf{V}(S \cup \{h\})$. The base case is when $\langle S \rangle = k[U]$. In that case, $\mathbf{V}(S) = \emptyset$, so $\emptyset$ is a comprehensive Gröbner system on $\mathbf{V}(S)$. □

## 3.1 Reducing segments

The segments $(Y, G)$ computed by $\mathbf{CGS_{simple}}(F)$ are very well-behaved, because we're guaranteed that $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for all $g \in G$ and $\alpha \in Y$. This fact means that $\langle \mathrm{lm}(G) \rangle = \langle \mathrm{lm}(\sigma_\alpha(G)) \rangle$ for all $\alpha \in Y$. This suggests, that we might be able to describe not only a Gröbner basis of $\langle \sigma_\alpha(F) \rangle$ but perhaps even the reduced Gröbner basis. Usually, we interreduce a Gröbner basis to find the reduced Gröbner basis. In the parametric setting, pseudo-division is our preferred division, so perhaps we can simply inter-pseudo-reduce $G$? We switch to seeing $G \subset K[U][X]$, because that is where we've defined pseudo-division. First, we need a standard lemma about Gröbner bases.

**3.2 · Lemma.** *Let $G$ be a Gröbner basis and let $g, g' \in G$ such that $g \neq g'$ and $\mathrm{lt}(g) \mid \mathrm{lt}(g')$. Then $G' = G \setminus \{g'\}$ satisfies that $\langle G' \rangle = \langle G \rangle$ and $G'$ is also a Gröbner basis.*

*Proof.* Find an $m$ such that $\mathrm{lt}(g') = m\,\mathrm{lt}(g)$ and let $f = g' - mg$. Then $f \in \langle G \rangle$ with $\mathrm{lm}(f) < \mathrm{lm}(g')$, hence $f$ reduces to 0 mod $G$, and $g'$ cannot be a part of this reduction. This means $g'$ reduces to zero mod $G \setminus \{g'\}$, so $g'$ is redundant. □

With that, we are ready to prove the theorem.

**3.3 · Theorem.** *Let $(Y, G)$ be a segment of a Gröbner system for an ideal $\langle F \rangle \subset K[X, U]$ and assume that $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for all $g \in G$ and $\alpha \in Y$. First, let $G'' \subset G$ be a subset such that $\mathrm{lm}_U(g)$ is not divisible by any monomial in $\mathrm{lm}_U(G'' \setminus \{g\})$ for all $g \in G''$. Let*

$$G' = \{\text{ps-rem}(g, G'' \setminus \{g\}) \mid g \in G''\} \setminus \{0\}$$

*where* ps-rem$(g, G)$ *returns a pseudo-remainder of $g$ mod $G$. Then $G^* = \{\sigma_\alpha(g)/\,\mathrm{lc}(\sigma_\alpha(g)) \mid g \in G'\}$ is the reduced Gröbner basis of $\langle \sigma_\alpha(F) \rangle$ for all $\alpha \in Y$.*

*Proof.* First, note that $\mathrm{lm}_U(f) = \mathrm{lm}(f)$ for any $f \in K[X, U]$ since $X \gg U$, so $\langle \mathrm{lm}(\langle F \rangle) = \langle \mathrm{lm}(\sigma_\alpha(G)) \rangle = \langle \mathrm{lm}(G) \rangle$ since $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$. Since any monomial of $\mathrm{lm}(G)$ is also in $\langle \mathrm{lm}(G'') \rangle$, we have $\langle \mathrm{lm}(G) \rangle = \langle \mathrm{lm}(G'') \rangle$. Now, for every $g \in G''$, $\mathrm{lm}(g)$ is not reducible mod $G'' \setminus \{g\}$, so $\langle \mathrm{lm}(G'') \rangle = \langle \mathrm{lm}(G') \rangle$. Finally, since $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for all $g \in G''$, we have $\langle \mathrm{lm}(G') \rangle = \langle \mathrm{lm}(\sigma_\alpha(G')) \rangle$ for all $\alpha \in Y$. In total, $\langle \mathrm{lm}(\langle F \rangle) \rangle = \langle \mathrm{lm}(\sigma_\alpha(G)) \rangle = \langle \mathrm{lm}(G) \rangle = \langle \mathrm{lm}(G'') \rangle = \langle \mathrm{lm}(G') \rangle = \langle \mathrm{lm}(\sigma_\alpha(G')) \rangle$. Furthermore, $\langle \sigma_\alpha(G'') \rangle = \langle \sigma_\alpha(G') \rangle$ by lemma 2.11 and $\langle \sigma_\alpha(G') \rangle = \langle \sigma_\alpha(G) \rangle$ by lemma 3.2. Hence $(Y, G')$ is also a segment of a Gröbner system.

To see that $G*$ is reduced, assume for contradiction there is some $g \in G^*$ where any term of $g$ is reducible mod $G^* \setminus \{g\}$. Then that means there is some $g' \in G^*$ such that $\mathrm{lm}(g')$ divides some term of $g$. Since $g$ was the specialization of a pseudo-remainder, there is some $h \in G'$ such that $\sigma(h)/\,\mathrm{lc}(\sigma(h)) = g$. Similary, there is some $h' \in G'$ such that $\sigma_\alpha(h')/\,\mathrm{lc}(\sigma_\alpha(h')) = g'$. Furthermore, there is a $h'' \in G$, such that $h' = \text{ps-rem}(h'', G \setminus \{h''\})$. Since $\mathrm{lm}(\sigma_\alpha(h')) = \mathrm{lm}(h') = \mathrm{lm}(h'')$, there is a term of $h$, which is divisible by $\mathrm{lm}(h'')$. But this is not allowed, since $h$ was a pseudo-remainder. Thus $g$ cannot be reducible mod $G^* \setminus \{g\}$.

Finally, since every polynomial in $G^*$ is monic, we have that $G^*$ is the reduced Gröbner basis of $\langle \sigma_\alpha(F) \rangle$ for all $\alpha \in Y$. □

**3.4 · Example.** Consider the ideal $I = \langle ax + ay, ax + by \rangle \subset \mathbb{C}[a, b][x, y]$. $\mathbf{CGS}_{\mathbf{simple}}(I)$ returns (among others) the segment $(\mathbf{V}(0) \setminus \mathbf{V}(ab(a-b)), \{(a-b)y, ax + by, xyb + y^2 b\})$. Since $xy$ is divisible by $x$, we first remove the third polynomial, leaving us with $\{(a - b)y, ax + by\}$. The first polynomial is not pseudo-reducible by the other, but pseudo-reducing the second polynomial by the first, we get

$$(a - b)(ax + by) = (b)((a - b)y) + (a - b)ax$$

thus $\{(a-b)y, (a-b)ax\}$ maps (up to scaling) to the reduced Gröbner basis of $\langle \sigma_\alpha(I) \rangle$ for all $\alpha \in \mathbf{V}(0) \setminus \mathbf{V}(ab(a-b))$ Indeed, whenever $a, b, (a-b) \neq 0$, we get that $(ax+ay)-(ax-by) = (a-b)y \neq 0 \in I$ and whatever $a-b$ is, it divides $a$, hence $(a-b)ax \in I$. Thus $\langle \sigma_\alpha(I) \rangle = \langle x, y \rangle$

for any $\alpha \in \mathbf{V}(0) \setminus \mathbf{V}(ab(a-b))$, and we have found its reduced Gröbner basis.

If we call a segment, which specializes to the reduced Gröbner basis up to multiplication by a scalar, for a *reduced* segment, then we now have a way to compute reduced segments. In light of this, we introduce a post-processing step to the $\mathbf{CGS_{simple}}$ algorithm, which pseudo-reduces the elements to produce a reduced segment.

**Algorithm 2: CGS**, an algorithm for computing comprehensive, reduced Gröbner systems on $\mathbf{V}(S)$

INPUT: Two finite sets $F \subset k[X,U]$, $S \subset k[U]$
OUTPUT: A finite set of triples $(E,N,G)$, each forming a reduced segment of a comprehensive Gröbner system on $\mathbf{V}(S)$.

$\mathscr{G} \leftarrow \mathbf{CGS_{simple}}(F,S)$;
$\mathscr{G}' \leftarrow \emptyset$;
**for** $(E,N,\{g_1,g_2,\dots,g_n\}) \in \mathscr{G}$ **do**
  $G'' \leftarrow \{g_i \mid g_i \notin \langle E\rangle \wedge \nexists j < i : \mathrm{lm}_U(g_j) \mid \mathrm{lm}_U(g_i)\}$;
  $G' \leftarrow \{\text{ps-rem}(g, G'' \setminus \{g\}) \mid g \in G''\} \setminus \{0\}$;
  $\mathscr{G}' \leftarrow \mathscr{G}' \cup \{(E,N,G')\}$;
**end**
**return** $\mathscr{G}'$;

**3.5 · Theorem.** *Let $F \subset K[X,U]$ and $S \subset K[U]$ be finite sets and let $\mathscr{G} = \mathbf{CGS}(F,S)$. Then $\mathscr{G}$ is a comprehensive Gröbner system for $F$ on $\mathbf{V}(S)$. Furthermore, if $(E,N,G) \in \mathscr{G}$, then $\{\sigma_\alpha(g)/\operatorname{lc}(\sigma_\alpha(g)) \mid g \in G\}$ is the reduced Gröbner basis of $\langle\sigma_\alpha(F)\rangle$ and $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for all $g \in G$ and $\alpha \in Y$.*

*Proof.* By theorem 3.1, the result of $\mathbf{CGS_{simple}}$ is a comprehensive Gröbner system, and **CGS** doesn't change the conditions of the segments. We need to show that each modified segment specializes to the reduced Gröbner basis on the conditions of that segment.

Let $(E,N,G)$ be a segment in $\mathbf{CGS_{simple}}(F,S)$. Note that $\sigma_\alpha(G) \cup \{0\} = \sigma_\alpha(G \setminus \langle E\rangle) \cup \{0\}$ for all $\alpha \in \mathbf{V}(E)$, hence $G'' = \{g \in G \mid g \notin \langle E\rangle\}$ will still specialize to a Gröbner basis. Furthermore, by theorem 3.1, we have $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for all $g \in G''$. Hence, by theorem 3.3, the segment computed by **CGS** specialize (up to scaling) to the reduced Gröbner basis. □

## 3.2 Parametric Gröbner bases

We now move on to the problem of computing parametric Gröbner bases, which is the problem Weispfenning tackled in his original article [14]. Recall the definition of parametric Gröbner bases from definition 2.1. We supplement it with the following definition.

**3.6 · Definition (Faithful Gröbner system).** A Gröbner system $\{(A_1,G_1),\dots,(A_t,G_t)\}$ of an ideal $\langle F\rangle$ is called *faithful* if $G_i \subset \langle F\rangle$ for all $i$.

**3.7 · Corollary.** *Let $\mathcal{G} = \{(A_1, G_1), \ldots, (A_t, G_t)\}$ be a faithful comprehensive Gröbner system of an ideal $\langle F \rangle$. Then $\bigcup_{(A,G)\in\mathcal{G}} G$ is a comprehensive parametric Gröbner basis of $\langle F \rangle$.*

*Proof.* Let $\sigma_\alpha$ be a specialization. Since $\mathcal{G}$ was comprehensive, there is some $j$ such that $\alpha \in A_j$. Then $\sigma_\alpha(G_j)$ is a Gröbner basis of $\langle \sigma_\alpha(F) \rangle$, so $\mathrm{lt}(\langle \sigma_\alpha(G_j) \rangle) = \mathrm{lt}(\langle \sigma_\alpha(\langle F \rangle) \rangle)$. Since for all $i$ we have that $\langle \sigma_\alpha(G_i) \rangle \subset \langle \sigma_\alpha(F) \rangle$, we have that $\mathrm{lt}(\langle \sigma_\alpha(G_i) \rangle) \subset \mathrm{lt}(\langle \sigma_\alpha(\langle F \rangle) \rangle)$, so $\sum_{i=1}^{t} \mathrm{lt}(\langle \sigma_\alpha(G_i) \rangle) = \mathrm{lt}(\langle \sigma_\alpha(\langle F \rangle) \rangle)$, thus $\sigma_\alpha\left(\bigcup_{(A,G)\in\mathcal{G}} G\right)$ is a Gröbner basis for $\langle \sigma_\alpha(F) \rangle$. □

The path to computing parametric Gröbner bases seem clear. We simply need to modify the segments of a comprehensive Gröbner system to be faithful, then we're done. While this is surprisingly easy to implement, proving that the way we do it works is a little more cumbersome.

## 3.3 Computing faithful segments

We follow the path laid out in [11], by introducing a new variable $t$ and extend the monomial order such that $t^n > X^{v_1} > U^{v_2}$ for all $n \in \mathbb{N}$ and vectors $v_1, v_2$. In the CGS algorithm we added leading coefficients $h$ to a set $S \subset k[U]$, and computed reduced Gröbner bases of $\langle F \cup S \rangle$ to produce the segments. However, this "mixes up" the original ideal with the added leading coefficients. We need a way to seperate them. We do this by replacing $F \cup S$ with $t \cdot F \cup (1-t) \cdot S$, where $t$ is a new auxilliary variable that does not occur in $F$ or $S$. Here we use the convention, that for a polynomial $a$ and a set of polynomials $F$, $a \cdot F := \{a \cdot f \mid f \in F\}$. Note, that $F$ need not be an ideal.

In this way we can seperate the original ideal from the added polynomials by specializing away $t$. That is the content of this first lemma.

**3.8 · Lemma.** *Let $F, S \subset k[X,U]$ be finite sets and let $g \in \langle t \cdot F \cup (1-t) \cdot S \rangle_{k[t,X,U]}$. Then $g(0,X,U) \in \langle S \rangle_{k[X,U]}$ and $g(1,X,U) \in \langle F \rangle_{k[X,U]}$.*

*Proof.* By assumption, we can find $f_1, \ldots, f_n \in F$, $s_1, \ldots, s_m \in S$ and $q_1, \ldots, q_n, p_1, \ldots, p_m \in k[t,X,U]$ such that

$$g = \sum_{i=1}^{n} t\, q_i\, f_i + \sum_{j=1}^{m} (1-t) p_j\, s_j.$$

Since the evaluation map is a ring homomorphism, we get that

$$g(0,X,U) = \sum_{j=1}^{m} p_j(0,X,U)\, s_j(X,U) \in \langle S \rangle_{k[X,U]}$$

and

$$g(1,X,U) = \sum_{i=1}^{n} q_i(1,X,U)\, f_i(X,U) \in \langle F \rangle_{k[X,U]}.$$

□

We're going to need these two specializations a lot, so we'll give them names. Let $\sigma^0(f) = f(0,X,U)$ and $\sigma^1(f) = f(1,X,U)$. We also need that Gröbner bases are preserved under

$\sigma^1$. While that is not true in general, the following is good enough for our uses.

**3.9 · Lemma.** *Let $F \subset k[X,U]$, $S \subset k[U]$ be finite sets and let $G$ be the reduced Gröbner basis of $\langle t \cdot F \cup (1-t) \cdot S \rangle$. Let also*

$$H = \{\mathrm{lc}_U(g) \mid g \in G,\ \mathrm{lt}(g) \notin k[X,U],\ \mathrm{lc}_{X,U}(g) \notin \langle S \rangle\}.$$

*Then $\sigma_\alpha(\sigma^1(G))$ is a Gröbner basis of $\langle \sigma_\alpha(F) \rangle$ for any $\alpha \in \mathbf{V}(S) \setminus \mathbf{V}(\mathrm{lcm}(H))$.*

*Proof.* First note, that $\mathrm{lt}(g) \notin k[X,U]$ means that the leading term of $g$ contains the variable $t$ and, since $t$ dominates the other variables, this means that $g \in k[t,X,U] \setminus k[X,U]$. Also, any polynomial in $G$ has degree at most 1 in $t$, again since $t$ dominates the other variables. To see this, follow Buchbergers algorithm, and use that S-polynomials maintain this property and so does reduction. For any polynomial $g \in G$ we can therefor write $g = t\, g^t + g_t$ where $g_t = \sigma^0(g)$ and $g^t = \sigma^1(g) - \sigma^0(g)$.

Let $\alpha \in \mathbf{V}(S) \setminus \mathbf{V}(\mathrm{lcm}(H))$. By lemma 3.8 we have that $\langle \sigma^1(G) \rangle = \langle F \rangle$ and thus $\langle \sigma_\alpha(\sigma^1(G)) \rangle = \langle \sigma_\alpha(F) \rangle$ for any specialization $\sigma_\alpha$. Thus we only need to show that $\sigma_\alpha(\sigma^1(G))$ is a Gröbner basis for itself.

Let $G' = \{g \in G \mid \mathrm{lt}(g) \notin k[X,U],\ \mathrm{lc}_{X,U}(g) \notin \langle S \rangle\}$. Then $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for any $g \in G'$ since $\alpha \notin V(\mathrm{lcm}(H))$. We will show later, that if $g \in G \setminus G'$ then $\sigma_\alpha(g) = 0$. Thus $\sigma_\alpha(G) = \sigma_\alpha(G') \cup \{0\}$. By lemma 2.17 this means that both $\sigma_\alpha(G)$ and $\sigma_\alpha(G')$ are Gröbner bases in $k_1[t,X]$.

Now we only need to show, that $\sigma_\alpha(\sigma^1(G'))$ is a Gröbner basis in $k_1[X]$. We can momentarily see $\sigma_\alpha$ as a map from $k[t,X,U]$ to $k_1[t,X]$ with $\sigma_\alpha(t) = t$. For any $g \in G'$ we have that $\sigma_\alpha(g) = t\sigma_\alpha(g^t) + \sigma_\alpha(g_t)$. Since $g_t = \sigma^0(g) \in \langle S \rangle$ by lemma 3.8 and $\alpha \in \mathbf{V}(S)$, we have that $\sigma_\alpha(g_t) = 0$, thus $\sigma_\alpha(g) = t\sigma_\alpha(g^t)$. This means that $\sigma_\alpha(G') = \sigma_\alpha(\{t \cdot g^t \mid g \in G'\})$. Since $t$ divides every polynomial, and thus term, in $\langle \sigma_\alpha(G') \rangle$, divisibility of leading terms is independent of $t$. Thus $\sigma_\alpha(\sigma^1(G'))$ is a Gröbner basis.

To finish the proof, we need to prove the assertion that if $g \in G \setminus G'$ then $\sigma_\alpha(g) = 0$. If $g \in G \setminus G'$, then either $\mathrm{lt}(g) \in k[X,U]$ or $\mathrm{lc}_{X,U}(g) \in \langle S \rangle$. In the first case, since $t$ dominates the other variables, $g$ cannot contain $t$ as a variable. Thus $g = \sigma^0(g) \in \langle S \rangle_{k[X,U]}$ by lemma 3.8. Since $\alpha \in \mathbf{V}(S)$, $\sigma_\alpha(g) = 0$. On the other hand, if $\mathrm{lt}(g) \notin k[X,U]$ but $\mathrm{lc}_{X,U}(g) \in \langle S \rangle$, we note that $g^t = \mathrm{lc}_{X,U}(g)$. Since $g = tg^t + \sigma^0(g)$, and $\sigma^0(g) \in \langle S \rangle$ by lemma 3.8, we get $\sigma_\alpha(g) = t\sigma_\alpha(g^t) + \sigma_\alpha(\sigma^0(g)) = 0$. This finishes the proof. □

This lemma is a variation of lemma 2.17, and as such, it leads us to an algorithm for computing faithful Gröbner systems on the vanishing set of some $S \subset k[U]$. We compute the reduced Gröbner basis of $\langle t \cdot F \cup (1-t) \cdot S \rangle$, which gives a faithful Gröbner segment on $\mathbf{V}(S) \setminus \mathbf{V}(\mathrm{lcm}(H))$, where $H = \{\mathrm{lc}_U(g) \mid g \in G,\ \mathrm{lt}(g) \notin k[X,U],\ \mathrm{lc}_{X,U}(g) \notin k[U]\}$. Then, we recursively compute faithful Gröbner segments on each $\mathbf{V}(S \cup \{h\})$ for $h \in H$, by adding $h$ to $S$. The following lemma will ensure, that we finish this process.

**3.10 · Lemma.** *Let $F \subset k[X,U]$, $S \subset k[U]$ be finite sets and let $G$ be the reduced Gröbner basis of $\langle t \cdot F \cup (1-t) \cdot S \rangle$. Let also*

$$H = \{\mathrm{lc}_U(g) \mid g \in G, \mathrm{lt}(g) \notin k[X,U], \mathrm{lc}_{X,U}(g) \notin \langle S \rangle\}.$$

*Then $h \notin \langle S \rangle$ for every $h \in H$.*

*Proof.* Let $G$ be the reduced Gröbner basis of $\langle t \cdot F \cup (1-t) \cdot S \rangle$, and let $h \in \{\mathrm{lc}_U(g) \mid g \in G,\ \mathrm{lt}(g) \notin k[X,U],\ \mathrm{lc}_{X,U}(g) \notin \langle S \rangle\}$. Let $g \in G$ be the element in $G$ such that $\mathrm{lc}_U(g) = h$. By assumption, $g$ is of the form $h \cdot t \cdot X^v + g'$ for some vector $v$ and $g' \in k[t,X,U]$ with $\mathrm{lm}_U(g') < \mathrm{lm}_U(g)$. Now, if $h \in \langle S \rangle$, then $(1-t) \cdot h \in \langle G \rangle$, by the construction of $G$. This means that $\mathrm{lt}((1-t) \cdot h) = \mathrm{lt}(t \cdot h)$ is divisible by some leading term of $G$. We now have two cases. If $X^v \neq 1$, then leading term of $g$ doesn't divide $\mathrm{lt}(t \cdot h)$, so $\mathrm{lt}(t \cdot h)$ must be divisible by some leading term of $G \setminus \{g\}$. But this implies that the leading term of $g$ is divisible by some leading term in $G \setminus \{g\}$, which is not allowed as $G$ is a *reduced* Gröbner basis. On the other hand, if $X^v = 1$, then $\mathrm{lc}_U(g) = \mathrm{lc}_{X,U}(g)$. But by assumption $\mathrm{lc}_{X,U}(g) \notin \langle S \rangle$, so this cannot happen. In both cases we reach a contradiction, so $h \notin \langle S \rangle$. □

**Algorithm 3: $\mathbf{CGB_{aux}}$**

INPUT: $F \subset k[X,U]$ and $S \subset k[U]$, two finite sets
OUTPUT: A finite set of triples $(E,N,G)$ forming a comprehensive, faithful Gröbner system on $\mathbf{V}(S)$

**if** $1 \in \langle S \rangle$ **then**
  **return** $\emptyset$;
**else**
  $G \leftarrow$ **groebner**$(t \cdot F \cup (1-t) \cdot S)$;
  $H \leftarrow \{\mathrm{lc}_U(g) \mid g \in G,\ \mathrm{lt}(g) \notin k[X,U],\ \mathrm{lc}_{X,U}(g) \notin \langle S \rangle\}$;
  $h \leftarrow \mathrm{lcm}(H)$;
  **return** $\{(S, \{h\}, \sigma^1(G))\} \cup \bigcup_{h' \in H} \mathbf{CGB_{aux}}(F, S \cup \{h'\})$;
**end**

**3.11 · Theorem.** *Let $F \subset k[X,U]$ and $S \subset k[U]$ be finite sets. Then $\mathbf{CGB_{aux}}(F,S)$ terminates, and the result is a faithful, comprehensive Gröbner system for $\langle F \rangle$ on $\mathbf{V}(S)$.*

*Proof.* We first show termination. Let $G$ be the reduced Gröbner basis of $\langle t \cdot F \cup (1-t) \cdot S \rangle$, and let $h \in \{\mathrm{lc}_U(g) \mid g \in G,\ \mathrm{lt}(g) \notin k[X,U],\ \mathrm{lc}_{X,U}(g) \notin \langle S \rangle\}$. By lemma 3.10, we have $\langle S \rangle \subsetneq \langle S \cup \{h\} \rangle$. Since $k[U]$ is Noetherian, we can only expand this ideal finitely many times. Thus the algorithm terminates.

If $(S, \{h\}, G)$ is in the output of $\mathbf{CGB_{aux}}(F,S)$, then $(\mathbf{V}(S) \setminus \mathbf{V}(h), G)$ is a segment of a Gröbner system by lemma 3.9. It is also faithful by lemma 3.8.

Finally, we need to show that $\mathbf{V}(S) = \bigcup_{(E,N,G) \in \mathbf{CGB_{aux}}(\mathbf{F},\mathbf{S})} \mathbf{V}(E) \setminus \mathbf{V}(N)$. Let $H = \{\mathrm{lc}_U(g) \mid$

$g \in G,\ \mathrm{lt}(g) \notin k[X,U],\ \mathrm{lc}_{X,U}(g) \notin \langle S \rangle\}$ and $h = \mathrm{lcm}(H)$. Then

$$\begin{aligned}\mathbf{V}(S) &= (\mathbf{V}(S) \setminus \mathbf{V}(h)) \cup \bigcup_{h' \in H} \mathbf{V}(h') \\ &= (\mathbf{V}(S) \setminus \mathbf{V}(h)) \cup \bigcup_{h' \in H} \mathbf{V}(S \cup \{h'\})\end{aligned}$$

By induction, the recursive calls to $\mathbf{CGB_{aux}}$ computes segments covering each $\mathbf{V}(S \cup \{h'\})$. The base case is when $S \cup \{h'\} = k[U]$, but in this case $\mathbf{V}(S \cup \{h'\}) = \emptyset$, and $\emptyset$ is a comprehensive Gröbner system on $\emptyset$. □

**Algorithm 4: CGB**

INPUT: $F \subset k[X,U]$ a finite set of polynomials
OUTPUT: $G \subset k[X,U]$ a comprehensive Gröbner basis of $\langle F \rangle$
$\mathscr{H} \leftarrow \mathbf{CGB_{aux}}(F, \emptyset)$;
**return** $S \cup \bigcup_{(E,N,G) \in \mathscr{H}} G$;

**3.12 · Theorem.** *Let $F \subset k[X,U]$ be a finite set of polynomials. Then* $\mathbf{CGB}(F)$ *terminates and the output is a parametric Gröbner basis of $\langle F \rangle$.*

*Proof.* **CGB** doesn't loop, and every subroutine it calls terminates, so it terminates. By theorem 3.11, $\mathscr{H} = \mathbf{CGB_{aux}}(F, \emptyset)$ is a faithful, comprehensive Gröbner system on $\mathbf{V}(\emptyset) = \mathbf{V}(0)$. By corollary 3.7 we get that $S \cup \bigcup_{(E,N,G) \in \mathscr{H}} G$ is a parametric Gröbner basis for $\langle F \rangle$.□

Let us work through an example, to see how the algorithm works.

**3.13 · Example.** Consider the ideal $I = \langle ax + ay, ax + by \rangle \subset \mathbb{C}[x, y, a, b]$ where we consider $a$ and $b$ to be parameters.

First, compute $\mathbf{CGB_{aux}}(G, \emptyset)$. We compute the reduced Gröbner basis of the ideal $\langle ax + ay, ax + by \rangle$ to be $G_1 = \{(a-b)ty, atx + bty, btxy + bty^2\}$. Thus $H_1 = \{(a-b), a, b\}$, with least common multiple $h = \mathrm{lcm}(H) = ab(a-b)$. Hence

$$(\mathbf{V}(\emptyset) \setminus \mathbf{V}(ab(a-b)), \{(a-b)y, ax + by, bxy + by^2\})$$

is the first segment of our faithful Gröbner system. Now, we need to compute Gröbner systems covering $\mathbf{V}(a)$, $\mathbf{V}(b)$ and $\mathbf{V}(a-b)$.

First, we take the segment $\mathbf{V}(a)$. We compute the reduced Gröbner basis of the ideal $\langle (a-b)ty, atx + bty, btxy + bty^2, (1-t)a \rangle$ and find it to be

$$G_2 = \{(a^2 - ab)y, ax + ay, at - a, bty - ay\}.$$

Thus $H_2 = \{b\}$, since the two first polynomials doesn't contain $t$ as a variable, and $\mathrm{lc}_{\{a,b\}}(at - a) = a \in \langle a \rangle$. This means that the second segment of our faithful Gröbner system is

$$(\mathbf{V}(a) \setminus \mathbf{V}(b), \{(a^2 - ab)y, ax + ay, by - ay\}).$$

Note, that since $\sigma_\alpha(a) = 0$ on this segment, we have a lot of redundant stuff. This is the price to pay for faithfulness. We will see in remark 3.14 how to remove some of it.

Next, consider the segment $\mathbf{V}(\{a, b\})$. Computing a reduced Gröbner basis of $\langle (a-b)ty, atx + bty, btxy + bty^2, (1-t)a, (1-t)b\rangle$, we get

$$G_3 = \{(a-b)y, ax + by, bxy + by^2, bt - b, at - a\}.$$

This time, $H_3 = \emptyset$, so $\operatorname{lcm}(H_3) = 1$. Hence, the final segment along this branch of the tree is

$$(\mathbf{V}(\{a, b\}) \setminus \mathbf{V}(1), \{(a-b)y, ax + by, bxy + by^2\}).$$

Do note that $I$ specializes to $\langle 0\rangle$ when we set $a = b = 0$, and so does every element of $G_3$.

Backtracking, we consider the segment $\mathbf{V}(b)$. Computing the reduced Gröbner basis of $\langle (a-b)ty, atx + bty, btxy + bty^2, (1-t)b\rangle$, we get

$$G_4 = \{(ab - b^2)y, abx + b^2y, bxy + by^2, bt - b, aty - by, atx + by\}.$$

Only the last two polynomials have a leading term containing $t$ and not being in $\langle b\rangle$, hence $H_4 = \{a\}$, with $\operatorname{lcm}(H_4) = a$. Hence, we have that

$$\mathbf{V}(b) \setminus \mathbf{V}(a), \{(ab - b^2)y, abx + b^2y, bxy + by^2, ay - by, ax + by\}$$

is a segment of our faithful Gröbner system. The next segment, $\mathbf{V}(\{a, b\})$ has already been computed, so we are done along this branch.

Remember, we still need to compute a Gröbner system covering $\mathbf{V}(a - b)$. We compute the reduced Gröbner basis of $\langle (a-b)ty, atx + bty, btxy + bty^2, (1-t)(a-b)\rangle$ and find it to be

$$G_5 = \{(a-b)y, (a^2 - ab)x, (a-b)t - a + b, btx + bty + (a-b)x\}.$$

Note, that only the last two polynomials contain $t$ as a variable. Further, $\operatorname{lc}_{\{a,b\}}((a-b)t - a + b) = a - b \in \langle a - b\rangle$, so we don't consider that either. Hence, $H_5 = \{b\}$. This means that

$$(\mathbf{V}(a-b) \setminus \mathbf{V}(b), \{(a-b)y, (a^2 - ab)x, ax + by\})$$

is the fifth segment of our Gröbner system.

To compute the final segment, we consider $\mathbf{V}((a-b), b) = \mathbf{V}(a, b)$. However, this segment was already computed, so we are done. Taking all the segments together, we have the

following comprehensive, faithful Gröbner system:

$$(\mathbf{V}(\emptyset) \setminus \mathbf{V}(a(a-b)), \{(a-b)y, ax+by, bxy+by^2\})$$
$$(\mathbf{V}(a) \setminus \mathbf{V}(b), \{(a^2-ab)y, ax+ay, by-ay\})$$
$$(\mathbf{V}(a,b) \setminus \mathbf{V}(1), \{(a-b)y, ax+by, bxy+by^2\})$$
$$(\mathbf{V}(b) \setminus \mathbf{V}(a), \{(ab-b^2)y, abx+b^2y, bxy+by^2, ay-by, ax+by\})$$
$$(\mathbf{V}(a-b) \setminus \mathbf{V}(b), \{(a-b)y, (a^2-ab)x, ax+by\})$$

To produce a parametric Gröbner basis, we simply union all the elements from each segment. Hence

$$\mathcal{G} = \{(a-b)y, ax+by, bxy+by^2, (a^2-ab)y, ax+ay, by-ay, (a^2-ab)x, (ab-b^2)y, abx+b^2y, ay-by\}$$

is a parametric Gröbner basis of $I$.

**3.14 · Remark.** We can use the $\mathbf{CGB_{aux}}$ algorithm to compute reduced Gröbner systems and faithful Gröbner systems simultanously. Let $G$ be the reduced Gröbner basis of $\langle t \cdot F \cup (1-t) \cdot S \rangle$ at some step in the algorithm, let $G' = \{g \in G \mid \mathrm{lt}(g) \notin k[X,U], \mathrm{lc}_{X,U}(g) \notin \langle S \rangle\}$, let $H = \{\mathrm{lc}_U(g) \mid g \in G'\}$ and let $Y = \mathbf{V}(S) \setminus \mathbf{V}(h)$. Then $(Y, \{\sigma^1(g) - \sigma^0(g) \mid g \in G'\})$ will also be a segment of a Gröbner system, with the property that $\sigma_\alpha(\mathrm{lc}(\sigma^1(g) - \sigma^0(g))) \neq 0$ for any $\alpha \in Y$. Indeed, any $g \in G'$ will have the form $tg^t + g_t$, where $g^t, g_t \in k[X,U]$, $\sigma^1(g) = g^t + g_t$ and $\sigma^0(g) = g_t$. Note, that $\mathrm{lt}(\sigma^1(g) - \sigma^0(g)) = \mathrm{lt}(g^t)$, and by construction we have $\sigma_\alpha(\mathrm{lc}(g^t)) \neq 0$ for all $\alpha \in Y$.

This also means, that by following the reduction procedure of theorem 3.3, we can compute reduced Gröbner segments simultanously with fathful Gröbner segments. Furthermore, by performing the same reduction process on $\sigma^1(G')$ as we do on $\{\sigma^1(g) - \sigma^0(g) \mid g \in G'\}$, we can compute a faithful Gröbner segment, which specializes to the reduced Gröbner basis, i.e. a reduced, faithful segment. In other words, if we write $G^f = \sigma^1(G') = \{g_1^f, \ldots, g_n^f\}$, then we can write $G^r = \{\sigma^1(g) - \sigma^0(g) \mid g \in G'\} = \{g_1^r, \ldots, g_n^r\}$ such that $\sigma_\alpha(g_i^f) = \sigma_\alpha(g_i^r)$ for all $i$ and $\alpha \in Y$. First, remove elements from $G^r$ until no leading term of $G^r$ is divisible by another leading term of $G^r$. Remove the corresponding elements from $G^f$. Let $n$ be the new size of $G^r$, and number its elements $g_1^r, \ldots, g_n^r$. Do the same for $G^f$, maintaining that $\sigma_\alpha(g_i^r) = \sigma_\alpha(G_i^f)$ for all $i$ and $\alpha \in Y$. Then, for a $g_j^r \in G^r$, which we pseudo-reduce modulo $G^r \setminus \{g_j^r\}$ as follows

$$cg_j^r = r_j^r + \sum_{i \neq j} h_i g_i^r$$

we can write

$$cg_j^f = r_j^f + \sum_{i \neq j} h_i g_i^f$$

Then $\sigma_\alpha(r_j^r) = \sigma_\alpha(r_j^f)$ for all $j$ and $\alpha \in Y$. Since $\{\sigma_\alpha(r_1^r)/\operatorname{lc}(\sigma_\alpha(r_1^r)), \dots, \sigma_\alpha(r_n^r)/\sigma_\alpha(r_n^r)\}$ is the reduced Gröbner basis of $\langle \sigma_\alpha(F) \rangle$, so is $\{\sigma_\alpha(r_1^f)/\operatorname{lc}(\sigma_\alpha(r_1^f)), \dots, \sigma_\alpha(r_n^f)/\sigma_\alpha(r_n^f)\}$.

At `https://github.com/0708andreas/ParametricGrobnerBases.jl`, there is an implementation of this reduction prodecure. A similar, but ultimately different, technique for computing Gröbner systems and faithful Gröbner bases in a single algorithm is presented in [5], but producing faithful, reduced segments is to my knowledge not described in the literature.

# 4 Geometric description & Gröbner covers

In this section, we develop a geometric description of Gröbner systems. We follow the development of [15] quite closely. The description makes heavy use of terms from modern algebraic geometry, specifically the language of sheaves. However, in section 4.5, we relate this abstract description to the **CGS** algorithm, which hopefully will provide a translation into more concrete terms. We also provide worked examples throughout, to relate the abstract concepts to the more classical setting.

We will now work over a Noetherian, commutative, reduced (with no nil-potent elements) ring $A$, which in concrete cases can be thought of as $k[U]$, the polynomial ring over the parameters. We let $\mathrm{Spec}(A)$ be the set of prime ideals in $A$, equipped with the Zariski topology, where the closed sets are of the form $\mathbf{V}(I) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid I \subset \mathfrak{p}\}$. Note that maximal ideals are prime ideals, and in the case when $A = k[U]$, ideals on the form $\langle u_1 - \alpha_1, \dots, u_n - \alpha_n\rangle$ are maximal. Note also, that there is a natural bijection between $\mathrm{Spec}(A/I)$ and $\mathbf{V}(I)$, which we will use implicitly. Given a closed set $Y \subset \mathrm{Spec}(A)$, there is a radical ideal $\mathbf{I}(Y) := \bigcap\{I \mid I \subset \mathfrak{p} \ \ \forall \mathfrak{p} \in Y\}$ such that $Y = \mathbf{V}(\mathbf{I}(Y))$.

Specializations are now given by prime ideals (elements of $\mathrm{Spec}(A)$). Given a prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$, let $A_\mathfrak{p}$ denote the localization of $A$ at $\mathfrak{p}$, which is the set of fractions of the form $\frac{f}{g}$ where $f \in A$ and $g \notin \mathfrak{p}$. The residue field at $\mathfrak{p}$ is then $k(\mathfrak{p}) := A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$, and there is a canonical map $A \to A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ given by $a \mapsto \frac{a}{1} + \mathfrak{p}_\mathfrak{p}$. The specialization $\sigma_\mathfrak{p} : A[X] \to k(\mathfrak{p})[X]$ is this canonical map, applied to each coefficient. If $A = k[U]$ and $\mathfrak{p}$ is a maximal ideal $\langle u_1 - \alpha_1, \dots, u_n - \alpha_n\rangle$, then $\sigma_\mathfrak{p}$ is simply the evaluation of the parameters at $(\alpha_1, \dots, \alpha_n)$.

Given an open subset $U \subset \mathrm{Spec}(A)$, there is a ring of regular functions on $U$. Let $\mathfrak{a}$ be the readical of the closure of $U$, $\mathfrak{a} = \mathbf{I}(\overline{U})$, then a regular function $f$ is a function from $U$ to $\coprod_{\mathfrak{p}\in U}(A/\mathfrak{a})_\mathfrak{p}$ which is locally a fraction and $f(\mathfrak{p}) \in (A/\mathfrak{a})_\mathfrak{p}$. This means, that any $\mathfrak{p} \in U$ there is an open $\mathfrak{p} \in U' \subset U$ and $p, q \in A/\mathfrak{a}$ such that $f(\mathfrak{p}') = \frac{p}{q} \in (A/\mathfrak{a})_{\mathfrak{p}'}$ for every $\mathfrak{p}' \in U'$. Note that this means $s \notin \mathfrak{p}'$.

**4.1 · Example.** In classical terms, we can think of regular functions as functions, which can locally be written as fractions of polynomials. For example, on $\mathbf{V}(ad-bc) \setminus \mathbf{V}(a,b) \subset \mathbb{C}^4$, there is a regular function $f$ given by $\frac{c}{a}$ when $a \neq 0$ and $\frac{d}{b}$ when $b \neq 0$. Even though $\mathbf{V}(ad-bc) \setminus \mathbf{V}(a,b)$ isn't open in $\mathbb{C}^4$, we can see $\mathbf{V}(ad-bc)$ as a topological subspace of $\mathbb{C}^4$ in which $\mathbf{V}(ad-bc) \setminus \mathbf{V}(a,b)$ is open.

Moving from $\mathbb{C}^4$ to $\mathrm{Spec}(\mathbb{C}[a,b,c,d])$, we can identify $\mathbf{V}(ad-bc)$ with $\mathrm{Spec}(\mathbb{C}[a,b,c,d]/\langle ad-bc\rangle)$, so we can equivalently see $f$ as a regular function on $\mathrm{Spec}(\mathbb{C}[a,b,c,d]/\langle ad-bc\rangle) \setminus \mathbf{V}(\langle a,b\rangle)$. This means, for any prime ideal $\mathfrak{p} \in \mathrm{Spec}(\mathbb{C}[a,b,c,d]/\langle ad-bc\rangle)$ which doesn't contain $\langle a,b\rangle$, $f$ assigns it an element of $(\mathbb{C}[a,b,c,d]/\langle ad-bc\rangle)_\mathfrak{p}$. In this case, whenever $\mathfrak{p} \not\supset \langle a\rangle$, $f(\mathfrak{p}) = \frac{c}{a}$ and whenever $\mathfrak{p} \not\supset \langle b\rangle$, $f(\mathfrak{p}) = \frac{d}{b}$. When $\mathfrak{p}$ is a maximal ideal, this is equivalent to saying that when $\sigma_\mathfrak{p}$ doesn't evaluate $a$ to 0, then $f(\mathfrak{p}) = \frac{c}{a}$, and when

$\sigma_{\mathfrak{p}}(b) \neq 0$, then $f(\mathfrak{p}) = \frac{d}{b}$. Since we work in $\mathbb{C}[a,b,c,d]/\langle ad - bc\rangle$, these two fractions agree whenever $\sigma_{\mathfrak{p}}(a) \neq 0 \neq \sigma_{\mathfrak{p}}(b)$. We are sure that we never have $\sigma_{\mathfrak{p}}(a) = \sigma_{\mathfrak{p}}(b) = 0$ since $\langle a, b\rangle \not\subset \mathfrak{p}$ by assumption.

Similarly to this example, we will often work with regular functions on a locally closed set $S = Y \cap U$, denoted by $\mathcal{O}_Y(U)$ or $\mathcal{O}_S$. We will make good use of the following result about $\mathcal{O}_Y(U)$.

**4.2 · Lemma.** *An element of $\mathcal{O}_Y(U)$ is uniquely determined by its images in $k(\mathfrak{p})$ for each $\mathfrak{p} \in Y \cap U$.*

*Proof.* Let $\mathfrak{a} = \mathbf{I}(Y)$ and let $\rho_{\mathfrak{p}} : \mathcal{O}_Y(U) \to (A/\mathfrak{a})_{\mathfrak{p}}/(\mathfrak{p}/\mathfrak{a})_{\mathfrak{p}}$ be the map given by $\rho_{\mathfrak{p}}(f) = f(\mathfrak{p}) + (\mathfrak{p}/\mathfrak{a})_{\mathfrak{p}}$. Let $f \in \mathcal{O}_Y(U)$. It is enough to prove that if $\rho_{\mathfrak{p}}(f) = 0$ for all $\mathfrak{p} \in Y \cap U$, then $f = 0$, so assume $f(\mathfrak{p}) \in (\mathfrak{p}/\mathfrak{a})_{\mathfrak{p}}$ for any $\mathfrak{p} \in Y \cap U$. Then $f(\mathfrak{p}) \in \bigcap_{\mathfrak{p}' \in \operatorname{Spec}(A/\mathfrak{a})} \mathfrak{p}' = \sqrt{\langle 0\rangle} \subset A/\mathfrak{a}$, using theorem A.3. So if $A/\mathfrak{a}$ has no nil-potent elements, then $\sqrt{\langle 0\rangle} = \langle 0\rangle$ and thus $f = 0$. Since $\mathfrak{a}$ was radical, this follows from the assumption that $A$ has no nil-potent elements. □

Given a locally closed set $S = Y \cap U \subset \operatorname{Spec}(A)$, take the radical ideal $\mathfrak{a} = \mathbf{I}(\overline{S})$, and consider the polynomial ring $(A/\mathfrak{a})[X]$. Let $I \subset A[X]$ be an ideal, and let $\overline{I}$ denote its image in $(A/\mathfrak{a})[X]$. Then we can consider the regular functions in $\overline{I}$ on $S$, which we denote by $\mathcal{I}_S$ or $\mathcal{I}_Y(U)$, and is given by functions $f$, which can be described locally as fractions $f(\mathfrak{p}) = \frac{p}{q}$ where $p \in \overline{I}$ and $q \in (A/\mathfrak{a}) \setminus \mathfrak{p}$. Let $f \in \mathcal{I}_S$, then, since $\operatorname{Spec}(A)$ is a compact topological space, we can find a finite open cover $\mathcal{U}$ of $\operatorname{Spec}(A)$ such that for every $U \in \mathcal{U}$ there is some $p, q$ such that $f(\mathfrak{p}) = p/q$ for all $\mathfrak{p} \in U$. In this light, we can also see $\mathcal{I}_S$ as an ideal in the polynomial ring $\mathcal{O}_S[X]$, i.e. as a polynomial with regular functions as coefficients, which is how we'll use it most of the time.

In an abuse of notation, for a $\mathfrak{p} \in \operatorname{Spec}(A/\mathfrak{a})$, we denote the map $\mathcal{I}_S \to k(\mathfrak{p})[X] = ((A/\mathfrak{a})_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}})[X]$ given by mapping $\frac{p}{q} \in \mathcal{I}_S$ to $\frac{\sigma_{\mathfrak{p}}(p)}{\sigma_{\mathfrak{p}}(q)}$ by $\sigma_{\mathfrak{p}}$. We can see $\mathcal{O}_S$ as a subring of $\mathcal{O}_S[X]$, so $\sigma_{\mathfrak{p}}$ also denotes the evaluation of an element in $\mathcal{O}_S$ at $\mathfrak{p}$.

The idea is to describe segments of Gröbner systems, not as point-sets in $k^{|U|}$ with a set of polynomials, but as point-sets in $\operatorname{Spec}(k[U])$ with a set of regular functions. These functions can be evaluated at a maximal ideal, giving a fraction of two polynomials, which can then be specialized at the same maximal ideal, giving a polynomial in $k[X]$. Using regular functions instead of polynomials will allow us to describe not only a Gröbner basis, but the reduced Gröbner basis of a whole segment.

**4.3 · Example.** Consider the ideal $I = \langle ax + cy, bx + dy\rangle \subset \mathbb{C}[a,b,c,d][x,y]$ with a term order such that $x > y$ as well as the subset $S = Y \cap U$ where $Y = \mathbf{V}(ad - bc)$ and $U = \mathbb{C}[a,b,c,d] \setminus \mathbf{V}(a,b)$. For any specialization where $ad - bc = 0$ and $a \neq 0$, we can divide the first polynomial by $a$ and reduce the second polynomial with it:

$$bx + dy - b\left(x + \frac{c}{a}y\right) = \left(d - \frac{bc}{a}\right)y = 0$$

Hence the reduced Gröbner basis is $\{x + \frac{c}{a}y\}$. Similarly, if $b \neq 0$, then $\{x + \frac{d}{b}y\}$ is the reduced Gröbner basis. Let's see how we can describe this using regular functions. The star of the show will be the regular function $f \in \mathcal{O}_Y(U)$ from example 4.1 given by $f(\mathfrak{p}) = \frac{c}{a}$ if $\mathfrak{p} \not\supset \langle a \rangle$ and $f(\mathfrak{p}) = \frac{d}{b}$ if $\mathfrak{p} \not\supset \langle b \rangle$.

Consider now the polynomial $P = x + f \cdot y \subset \mathcal{O}_Y(U)[x, y]$, and let $\mathfrak{m} \in \operatorname{Spec}(\mathbb{C}[a, b, c, d]/\mathbf{V}(ad - bc))$ be a maximal ideal which doesn't contain $\langle a, b \rangle$. This is equivalent to $\mathfrak{m}$ being a maximal ideal in $\mathbb{C}[a, b, c, d]$ of the form $\langle a - m_1, b - m_2, c - m_3, d - m_3 \rangle$ with the condition that $m_1 m_4 - m_2 m_3 = 0$ and $m_1$ and $m_2$ not both being zero. Then $f(\mathfrak{m}) = x + \frac{c}{a}y$ if $m_1 \neq 0$ and $f(\mathfrak{m}) = x + \frac{d}{b}x$ if $m_2 \neq 0$.

Hence

$$\sigma_{\mathfrak{m}}(P) = \begin{cases} x + \frac{m_3}{m_1}y & m_1 \neq 0 \\ x + \frac{m_4}{m_2}y & m_2 \neq 0 \end{cases}$$

Notice, for any such choice of $m_1, \ldots, m_4$, $\{\sigma_{\mathfrak{m}}(P)\}$ is indeed the reduced Gröbner basis of $\sigma_{\mathfrak{m}}(I) \subset \mathbb{C}[x, y]$. Lasly, we can write $P = (ax + cy)/a \in I_{\mathfrak{p}}$ when $a \neq 0$ and $P = (bx + dy)/b$ when $b \neq 0$. Hence $P \in \mathcal{I}_Y(U)$.

## 4.1 Parametric sets

Parametric Gröbner bases are nice for applications because we have a single object, which is easily translated into a Gröbner basis for any given specialization. However, that translation may include zeros and redundant elements. In particular, there is no way in general to produce a "parametric reduced Gröbner basis", i.e. a Gröbner basis which specializes to the reduced Gröbner basis of $\sigma(\langle G \rangle)$ for any specialization $\sigma$. Hence, we might want to find the segments, where we can find such a parametric reduced Gröbner basis. This is the following definition.

**4.4 · Definition (Parametric set).** Let $I \subset A[X]$ be an ideal and let $S \subset \operatorname{Spec}(A)$ be locally closed. We say $S$ is a *parametric set for* $I$ if there is a finite set $G \subset \mathcal{I}_S$ such that

1. $\sigma_{\mathfrak{p}}(G)$ is the reduced Gröbner basis of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ for each $\mathfrak{p} \in S$.
2. For any $g \in G$ and $\mathfrak{p}, \mathfrak{p}' \in S$, we have $\operatorname{lt}(\sigma_{\mathfrak{p}}(g)) = \operatorname{lt}(\sigma_{\mathfrak{p}'}(g))$.

Reduced Gröbner bases are unique, and the set $G$ is the definition of parametric sets inherit this property. To prove this, we'll first need a lemma.

**4.5 · Lemma.** *Let $Y \subset \operatorname{Spec}(A)$ be a closed set and $f, g \in \mathcal{I}_Y$. If $\sigma_{\mathfrak{p}}(f) = \sigma_{\mathfrak{p}}(g)$ for all $\mathfrak{p} \in Y$, then $f = g$.*

*Proof.* By linearity of $\sigma_{\mathfrak{p}}$, we can assume without loss of generality that $f = 0$. We can see $g$ as a polynomial with coefficients in $\mathcal{O}_Y(Y)$. Then $\sigma_{\mathfrak{p}}(g) = 0$ means that every coefficient of $g$ lies in $\mathfrak{p}_{\mathfrak{p}}$. Since this hold for every $\mathfrak{p} \in Y$, $g = 0$ by lemma 4.2 □

**4.6 · Theorem.** *Let $S \subset \operatorname{Spec}(A)$ be a parametric set for an ideal $I$ and let $G \subset \mathcal{J}_Y$ be a finite set such that $\sigma_\mathfrak{p}(G)$ is the reduced Gröbner basis of $\langle \sigma_\mathfrak{p}(I) \rangle$ for every $\mathfrak{p} \in S$. Then $G$ is unique and every $g \in G$ is monic (has 1 as leading coefficient) with $\operatorname{lm}(g) = \operatorname{lm}(\sigma_\mathfrak{p}(g))$ for every $\mathfrak{p} \in Y$.*

*Proof.* Let $F \subset \mathcal{J}_Y$ be a finite set satisfying the two conditions for $Y$ to be a parametric set. For any fixed $f \in F$ and $\mathfrak{p} \in Y$, there is then a $g \in G$ such that $\sigma_\mathfrak{p}(f) = \sigma_\mathfrak{p}(g)$. Then we have $\operatorname{lm}(\sigma_\mathfrak{p}(f)) = \operatorname{lm}(\sigma_\mathfrak{p}(g))$ for all $\mathfrak{p} \in Y$. Since $\sigma_\mathfrak{p}(F) = \sigma_\mathfrak{p}(G)$ is the reduced Gröbner basis, there can only be one polynomial with that leading monomial. Hence $\sigma_\mathfrak{p}(f) = \sigma_\mathfrak{p}(g)$ for all $\mathfrak{p} \in Y$, so $f = g$ by lemma 4.5. Thus $F \subset G$, and since the situation is symmetric, $F = G$.

To see that every $g \in G$ is monic, we observe that since $\sigma_\mathfrak{p}(g)$ is an element of a reduced Gröbner basis, it's leading coefficient is 1 for all $\mathfrak{p} \in Y$. Since $\operatorname{lm}(\sigma_{\mathfrak{p}'}(g)) = \operatorname{lm}(\sigma_\mathfrak{p}(g))$ for all $\mathfrak{p}, \mathfrak{p}' \in S$, we have $\sigma_\mathfrak{p}(\operatorname{lc}(g)) \neq 0$ for all $\mathfrak{p} \in S$. Thus $1 = \operatorname{lc}(\sigma_\mathfrak{p}(g)) = \sigma_\mathfrak{p}(\operatorname{lc}(g))$, hence $\operatorname{lc}(g) = 1$ by lemma 4.2. And since $\sigma_\mathfrak{p}(1) = 1$ for any $\mathfrak{p}$, we get that $\operatorname{lm}(g) = \operatorname{lm}(\sigma_\mathfrak{p}(g))$.□

In light of this theorem, for a parametric set $S$, we will call its uniquely determined set of polynomials for its reduced Gröbner basis. In certain ways, they are even more well-behaved than classical reduced Gröbner bases, which the following proposition will show.

**4.7 · Proposition.** *Let $S \subset \operatorname{Spec}(A)$ be a parametric set for an ideal $I$ and let $S' \subset S$ be locally closed. Then $S'$ is also parametric, and there is a canonical map $\mathcal{J}_S \to \mathcal{J}_{S'}$ which maps the reduced Gröbner basis of $S$ to the reduced Gröbner basis of $S'$.*

*Proof.* To construct the canonical map, let $\mathfrak{a} = \mathbf{I}(\overline{S})$, $\mathfrak{a}' = \mathbf{I}(\overline{S'})$. Let $\overline{I}$ and $\overline{I'}$ be the images of $I$ in $(A/\mathfrak{a})[X]$ and $(A/\mathfrak{a}')[X]$ respectively. Since $\overline{S}' \subset \overline{S}$, we get $\mathfrak{a} \subset \mathfrak{a}'$ and thus a quotient map $\iota : A/\mathfrak{a} \to A/\mathfrak{a}'$. This extends to $\phi : \overline{I} \to \overline{I'}$, which we can localize for every $\mathfrak{p} \in S'$, giving $\phi_\mathfrak{p} : \overline{I}_\mathfrak{p} \to \overline{I'}_\mathfrak{p}$. Then the map

$$(g \in \mathcal{J}_S) \mapsto (\mathfrak{p} \mapsto \phi_\mathfrak{p}(g(\mathfrak{p})))$$

is well-defined since it agrees on every open set, and gives us the desired map, call it $\Phi : \mathcal{J}_S \to \mathcal{J}_{S'}$.

Since $\phi_p$ was just the localization of a quotient map, we get that $\sigma_\mathfrak{p}(\phi_\mathfrak{p}(g)) = \sigma_\mathfrak{p}(g)$ for any $g$ in $\overline{I}_\mathfrak{p}$. Thus we also have $\sigma_\mathfrak{p}(\Phi(g)) = \sigma_\mathfrak{p}(g)$ for any $g \in \mathcal{J}_S$. Thus, by lemma 4.5 $\Phi(G) = G'$ where $G$ and $G'$ are the reduced Gröbner bases for $S$ and $S'$ respectively. □

We can see parametric sets as segments of a Gröbner system, only a bit more constrained because we want to describe the reduced Gröbner basis parametrically, not just any Gröbner basis. The object corresponding to a Gröbner system is called a Gröbner cover.

**4.8 · Definition (Gröbner cover).** Let $I \subset A[X]$ be an ideal. A finite set of pairs $\mathcal{G} = \{(S_1, G_1), (S_2, g_2), \dots, (S_n, G_n)\}$ is called a *Gröbner cover* if each $S_i$ is parametric, $G_i \subset \mathcal{O}_{S_i}[X]$ is the reduced Gröbner basis of $S_i$ and $\operatorname{Spec}(A) = \bigcup_{(S,G)\in\mathcal{G}} S$.

## 4.2 Monic ideals and the reduced Gröbner basis of $\mathscr{I}_S$

Another pleasant surprise is that the unique reduced Gröbner basis of a parametric set for an ideal $I$, is actually the reduced Gröbner basis of the ideal $\mathscr{I}_S \subset \mathscr{O}_S[X]$. Since a reduced Gröbner basis consists of monic polynomials, this will imply that $\mathscr{I}_S$ is a monic ideal. In fact, that is a sufficient condition for $S$ to be a parametric set. This subsection will be spent proving this, as well as some lemmas which will be useful later.

**4.9 · Definition (Monic ideal).** An ideal $I \subset A[X]$ is called *monic* if, for every monomial $m \in \operatorname{lm}(I)$, there is a monic $f \in I$ with $\operatorname{lm}(f) = m$.

We will use without proof that reduced Gröbner bases exists for monic ideals. If the base ring is a field, then every ideal is monic.

**4.10 · Proposition.** *Let $I \subset A[X]$ be an ideal. Then there exists a unique reduced Gröbner basis of $I$ if and only if $I$ is monic.*

Before we prove the main content, we need two lemmas. First, for any localized polynomial, we can represent it by a fraction of a polynomial with the same terms.

**4.11 · Lemma.** *Let $I \subset A[X]$ be an ideal, $\mathfrak{p} \in \operatorname{Spec}(A)$ and $f \in I_{\mathfrak{p}}$. Then there exists a $P \in I$ and $Q \in A \setminus \mathfrak{p}$ such that $f = \frac{P}{Q} \in I_{\mathfrak{p}}$ and $\operatorname{coef}(f, m) = 0 \implies \operatorname{coef}(P, m) = 0$ for all monomials $m$.*

*Proof.* By definition of $I_{\mathfrak{p}}$, there is some $P \in I$ and $Q \in A \setminus \mathfrak{p}$ such that $f = \frac{P}{Q}$. If $\operatorname{coef}(f, m) = 0$, then $\operatorname{coef}(P, m)/Q = 0$. Hence there is a $Q_m \in A \setminus \mathfrak{p}$ such that $\operatorname{coef}(P, m) \cdot Q_m = 0 \in A$. Then

$$f = \frac{P \cdot \prod_m Q_m}{Q \cdot \prod_m Q_m}$$

satisfies what we want. □

Secondly, when we embed polynomials in $\mathscr{I}_S$, we preserve their leading monomial.

**4.12 · Lemma.** *Let $S \subset \operatorname{Spec}(A)$ be a locally closed set and $\mathfrak{a} = \mathbf{I}(\overline{Y})$. Let $I \subset A[X]$ be an ideal, let $\overline{I} \subset (A/\mathfrak{a})[X]$ be its image in $(A/\mathfrak{a})[X]$, let $P \in \overline{I}$. Then the leading monomial of $\frac{P}{1} \in \mathscr{I}_S \subset \mathscr{O}_S[X]$ is equal to the leading monomial of $P$.*

*Proof.* We will show that there is a $\mathfrak{p} \in S$ with $\operatorname{lc}(P) \notin \mathfrak{p}$. Indeed, if that was not the case, then $\operatorname{lc}(P) \in \mathfrak{p}$ for every $\mathfrak{p} \in S$, which would imply $\sigma_{\mathfrak{p}}(\operatorname{lc}(P)) = 0$ for every $\mathfrak{p} \in S$. Thus $\operatorname{lc}\left(\frac{P}{1}\right) = 0$ since elements of $\mathscr{O}_S$ are determined by $\sigma_{\mathfrak{p}}$ by lemma 4.2.

So assume for a contradiction that $\operatorname{lc}(P) \in \mathfrak{p}$ for all $\mathfrak{p} \in S$. Then $S \subset W := \mathbf{V}(\operatorname{lc}(P)) = \{\mathfrak{p} \in \mathbf{V}(\mathfrak{a}) \mid \operatorname{lc}(P) \in p\}$. Since $W$ is closed and $S \subset W \subset \overline{S}$, we get that $W = \mathbf{V}(\mathfrak{a})$, thus $\operatorname{lc}(P) \in \mathfrak{p}$ for all $\mathfrak{p} \in \mathbf{V}(\mathfrak{a})$. But since $\mathfrak{a}$ is radical and so $A/\mathfrak{a}$ has no nil-potents, by theorem A.3 this means

$$\operatorname{lc}(P) \in \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A/\mathfrak{a})} \mathfrak{p} = \sqrt{\langle 0 \rangle} = 0$$

hence $\operatorname{lc}(P) = 0$, which is a contradiction. □

**4.13 · Theorem.** *Let $I \subset A[X]$ be an ideal and $S \subset \operatorname{Spec}(A)$ be a locally closed set. Then*

1. *$S$ is parametric for $I$ if and only if $\mathscr{I}_S$, when seen as a ideal in $\mathcal{O}_S[X]$ is monic.*
2. *In the above case, the reduced Gröbner of $\mathscr{I}_S$ is equal to the reduced Gröbner basis for the parametric set $S$.*

*Proof.* For the first implication, assume $S$ is parametric for $I$ and let $G \subset \mathscr{I}_S$ be its reduced Gröbner basis. First, we show that $\mathscr{I}_S$ is monic, so let $f \in \mathscr{I}_S$. Then there is some $\mathfrak{p} \in S$ such that $\operatorname{lc}(f) \notin \mathfrak{p}$, i.e. $\sigma_\mathfrak{p}(\operatorname{lc}(f)) \neq 0$, since otherwise $\operatorname{lc}(f) = 0$ by lemma 4.2. Since $\sigma_\mathfrak{p}(G)$ is a Gröbner basis for $\langle \sigma_\mathfrak{p}(\mathscr{I}_S) \rangle$, there is some $g \in G$ where $\operatorname{lm}(\sigma_\mathfrak{p}) \mid \operatorname{lm}(\sigma_\mathfrak{p}(f))$. Since $\operatorname{lm}(g) = \operatorname{lm}(\sigma_\mathfrak{p}(g))$ by theorem 4.6 and $\operatorname{lm}(f) = \operatorname{lm}(\sigma_\mathfrak{p}(f))$, we get $\operatorname{lm}(g) \mid \operatorname{lm}(f)$. Since $g$ is monic, every leading monomial of $\mathscr{I}_S$ is found as the leading monomial of a monic polynomial, so $\mathscr{I}_S$ is monic.

For the other implication, assume $\mathscr{I}_S$ is monic, let $G = \{g_1, \dots, g_n\} \subset \mathscr{I}_S$ denote its unique reduced Gröbner basis and let $f \in \mathscr{I}_S$. By theorem 2.10, we can find a pseudo-division

$$cf = r + \sum_{i=1}^{n} f_i g_i$$

with $\operatorname{lm}(f_i)\operatorname{lm}(g_i) \leq \operatorname{lt}(f)$ and $\operatorname{coef}(f_i, m) \in \langle \operatorname{coef}(f, m') \mid m' \geq m \operatorname{lt}(g_i) \rangle \subset A/\mathbf{I}(S)$ for all monomials $m$. Since all elements in $G$ are monic, and $c$ is a product of leading coefficients from $G$, we get $c = 1$, and since $f \in \mathscr{I}_S$ and $G$ is a monic Gröbner basis, we get $r = 0$.

The last condition gives us, for any $\mathfrak{p} \in S$ that if $\operatorname{lm}(f_i)\operatorname{lm}(g_i) > \operatorname{lm}(\sigma_\mathfrak{p}(f))$, then $\sigma_\mathfrak{p}(\operatorname{lc}(f_i)\operatorname{lc}(g_i)) \in \langle 0 \rangle$, thus $\sigma_\mathfrak{p}(\operatorname{lc}(f_i)) = 0$ since $\sigma_\mathfrak{p}(\operatorname{lc}(g_i)) = 1$. Since this holds for every other term of $f_i$ as well, we get that $\operatorname{lm}(\sigma_\mathfrak{p}(f_i))\operatorname{lm}(\sigma_\mathfrak{p}(g_i)) \leq \operatorname{lm}(\sigma_\mathfrak{p}(f))$. Since $\sigma_\mathfrak{p}$ is a ring homomorphism, $\sigma_\mathfrak{p}(f) = \sum_{i=1}^{n} \sigma_\mathfrak{p}(f_i)\sigma_\mathfrak{p}(g_i)$, there must be some $g_i$ for which $\operatorname{lm}(\sigma_\mathfrak{p}(g_i)) \mid \operatorname{lm}(\sigma_\mathfrak{p}(f))$. Since every element of $\langle \sigma_\mathfrak{p}(I) \rangle$ is a scalar multiple of $\sigma_\mathfrak{p}(f)$ for some $f \in \mathscr{I}_S$, we get that $\sigma_\mathfrak{p}(G)$ is a Gröbner basis of $\langle \sigma_\mathfrak{p}(I) \rangle$. Since every $g \in G$ is monic, $\sigma_\mathfrak{p}(g)$ is also monic, and $\sigma_\mathfrak{p}(G)$ is reduced because $G$ is. Thus, $\sigma_\mathfrak{p}(G)$ is the reduced Gröbner basis of $\sigma_\mathfrak{p}(I)$ for every $\mathfrak{p} \in S$, so $S$ is parametric. Furthermore, since $G$ was defined to be the reduced Gröbner basis of $\mathscr{I}_S$, the second assertion follows immediately. □

This theorem gives us, that the parametric Gröbner basis, which was defined as specialising to a reduced Gröbner basis in all points, lifts to a reduced Gröbner basis of $\mathscr{I}_S$. The next theorem is a local test to determine parametricity.

**4.14 · Theorem.** *Let $S \subset \operatorname{Spec}(A)$ be locally closed, let $\mathfrak{a} = \mathbf{I}(\overline{S})$ and let $\overline{I}$ be the image of $I$ in $(A/\mathfrak{a})[X]$. Then $S$ is parametric if and only if $\overline{I}_\mathfrak{p}$ is monic for every $\mathfrak{p} \in S$ and $\mathfrak{p} \mapsto \operatorname{lm}(\overline{I}_\mathfrak{p})$ is constant on $S$. Furthermore, in this case $\operatorname{lm}(\mathscr{I}_S) = \operatorname{lm}(\overline{I}_\mathfrak{p})$ for all $\mathfrak{p} \in S$.*

*Proof.* For the first implication, assume $S$ is parametric and let $G \subset \mathscr{I}_S$ be its reduced Gröbner basis. Fix some $\mathfrak{p} \in S$ and let $\frac{P}{Q} \in \overline{I}_\mathfrak{p}$. By lemma 4.11 we can assume $\operatorname{lm}(P) = \operatorname{lm}\left(\frac{P}{Q}\right)$. By lemma 4.12 the leading monomial $P$ is preserved when we embed it in $\mathscr{I}_S$.

Hence $\operatorname{lm}\left(\frac{P}{Q}\right) \in \operatorname{lm}(\mathcal{I}_S)$, and since the image of $G$ in $\overline{I}_\mathfrak{p}$ is monic, it is a reduced Gröbner basis of $\overline{I}_\mathfrak{p}$. Hence $\overline{I}_\mathfrak{p}$ is monic and $\operatorname{lm}(\overline{I}_\mathfrak{p}) = \operatorname{lm}(\mathcal{I}_S)$, giving that $\mathfrak{p} \mapsto \operatorname{lm}(\overline{I}_\mathfrak{p})$ is a constant function on $S$.

For the other implication, assume $\overline{I}_\mathfrak{p}$ is monic for every $\mathfrak{p} \in S$, and $\operatorname{lm}(\overline{I}_\mathfrak{p}) = \operatorname{lm}(\overline{I}_{\mathfrak{p}'})$ for all $\mathfrak{p}, \mathfrak{p}' \in S$. Let $\{m_1, \dots, m_n\}$ be a minimal set of generators of the monomial ideal $\operatorname{lm}(\overline{I}_\mathfrak{p})$ (which is independent of $\mathfrak{p}$). For each $\mathfrak{p} \in S$, let $g_i(\mathfrak{p})$ denote the element of the reduced Gröbner basis of $\overline{I}_\mathfrak{p}$ with $\operatorname{lm}(g_i(\mathfrak{p})) = m_i$. Then $g_i$ is a function $(\mathfrak{p} \in \operatorname{Spec}(S)) \to \overline{I}_\mathfrak{p}$, and so is potentially an element of $\mathcal{I}_S$. We just need that it locally can be described by the same fraction. Fix a $\mathfrak{p} \in S$ and find $P/Q = g_i(\mathfrak{p}) \in \overline{I}_\mathfrak{p}$ such that $\operatorname{lm}(P) = \operatorname{lm}(g_i(\mathfrak{p}))$, which exists by lemma 4.11. Also by lemma 4.11, we may assume that $\operatorname{coef}(P, m) = 0$ for all monomials $m \in \operatorname{lm}(\overline{I}_\mathfrak{p}) \setminus m_i$, since that is the case for $g_i(\mathfrak{p})$ because it comes from a reduced Gröbner basis. Because $g_i(\mathfrak{p})$ is monic, we have $\operatorname{lc}(P)/Q = 1$. Consider the open set $U = \{\mathfrak{p}' \in S \mid Q \notin \mathfrak{p}'\}$, which is an open neighborhood of $\mathfrak{p}$. Then $g_i(\mathfrak{p}') = P/Q \in \overline{I}_{\mathfrak{p}'}$ for all $\mathfrak{p}' \in U$ since $P/Q \in \overline{I}_{\mathfrak{p}'}$ is monic and has leading monomial $m_i$ and $\operatorname{coef}(P/Q, m) = 0$ for all $m \in \operatorname{lm}(\overline{I}_{\mathfrak{p}'})$, which is the defining properties of $g_i(\mathfrak{p}')$. Thus $g_i \in \mathcal{I}_S$.

This makes the set $G = \{g_1, \dots, g_n\} \subset \mathcal{I}_S$ a good candidate for a Gröbner basis of $\mathcal{I}_S$, which would make $S$ parametric by theorem 4.13 because the $g_i$ are monic. So take an $f \in \mathcal{I}_S$. By lemma 4.2 there is a $\mathfrak{p} \in S$ such that $\sigma_\mathfrak{p}(\operatorname{lc}(f)) \neq 0$. Letting $\overline{f}$ denote the image of $f$ in $\overline{I} \subset (A/\mathfrak{a})[X]$ and $\overline{f}_\mathfrak{p}$ its image in $\overline{I}_\mathfrak{p}$, this implies that $\operatorname{lc}(\overline{f}) \neq 0$, hence $\operatorname{lm}(f) = \operatorname{lm}(\overline{f}) = \operatorname{lm}(\overline{f}_\mathfrak{p})$. Thus $\operatorname{lm}(\mathcal{I}_S) = \operatorname{lm}(\overline{I}_\mathfrak{p}) \ni \operatorname{lm}(\overline{f}_\mathfrak{p})$, so $\langle \operatorname{lm}(\mathcal{I}_S) \rangle = \langle \operatorname{lm}(\overline{I}_\mathfrak{p}) \rangle = \langle \operatorname{lm}(G) \rangle$. Thus $\mathcal{I}_S$ is monic, so $S$ is parametric by theorem 4.13. □

This theorem allows us to characterize the leading monomials of $\mathcal{I}_S$.

**4.15 · Corollary.** *Let $I \subset A[X]$ be an ideal, $S \subset \operatorname{Spec}(A)$ be parametric for $I$, $\mathfrak{a} = \mathbf{I}(S)$ and let $\overline{I}$ be the image of $I$ in $(A/\mathfrak{a})[X]$. Then $\operatorname{lm}(\mathcal{I}_S) = \operatorname{lm}(\overline{I})$.*

*Proof.* Let $m \in \operatorname{lm}(\mathcal{I}_S)$ and $\mathfrak{p} \in S$. Theorem 4.14 gives us that $\overline{I}_\mathfrak{p} \subset (A/\mathfrak{a})_\mathfrak{p}[X]$ is monic with $\operatorname{lm}(\overline{I}_\mathfrak{p}) = \operatorname{lm}(\mathcal{I}_S)$. So take some $P/Q \in \overline{I}_\mathfrak{p}$ with $\operatorname{lm}(P/Q) = m$. By lemma 4.11 we can take $P/Q$ such that $\operatorname{lm}(P) = m$. Hence $\operatorname{lm}(\mathcal{I}_S) \subset \operatorname{lm}(\overline{I})$.

For the reverse inclusion, let $P \in \overline{I}$. By lemma 4.12 the element $P/1 \in \mathcal{I}_S$ has $\operatorname{lm}(P/1) = \operatorname{lm}(P)$, so $\operatorname{lm}(\overline{I}) \subset \operatorname{lm}(\mathcal{I}_S)$. □

## 4.3 The singular ideal

In the last section, we showed that a locally closed set $S$ is parametric for an ideal $I$ if and only if $\mathcal{I}_S$ is a monic ideal in $\mathcal{O}_S[X]$. Given a locally closed set, we can use this to find the maximal parametric subset of $S$. This maximal set is closely linked to the concept of a *lucky* prime ideal. Here, we will only include what we need. For a more in-depth discussion, see [15].

**4.16 · Definition (Lucky prime).** A prime ideal $\mathfrak{p} \in \operatorname{Spec}(A)$ is called *lucky* if $\operatorname{lc}(I, m) \not\subset \mathfrak{p}$ for all $m \in \operatorname{lm}(I)$.

**4.17 · Definition (Singular ideal).** Let $I \subset A[X]$ be an ideal and let $M$ be the unique minimal set of generators of $\langle \operatorname{lm}(I) \rangle$. The *singular ideal* of $I$ is the radical ideal

$$\mathbf{J}(I) = \sqrt{\prod_{m \in M} \operatorname{lc}(I, m)} \subset A$$

where $\operatorname{lc}(I, m) = \langle \{ \operatorname{lc}(g) \mid g \in I \wedge \operatorname{lm}(g) = m \} \rangle$.

We have the following connection between lucky primes and the singular ideal.

**4.18 · Lemma.** *Let $I \subset A[X]$ be an ideal, then a prime $\mathfrak{p} \in \operatorname{Spec}(A)$ is lucky if and only if $\mathbf{J}(I) \not\subset \mathfrak{p}$, i.e. $\mathfrak{p} \notin \mathbf{V}(\mathbf{J}(I))$.*

*Proof.* Let $M$ be the unique minimal set of generators of $\langle \operatorname{lm}(I) \rangle$. For the first implication, let $p \in \operatorname{Spec}(A)$ be lucky. For each $m \in M$, let $f_m \in I$ have $\operatorname{lm}(f_m) = m$. Since $\mathfrak{p}$ is lucky, we can choose the $f_m$ such that $\operatorname{lc}(f_m) \notin \mathfrak{p}$ for every $m \in M$. Since $\mathfrak{p}$ is prime, we thus have $\prod_{m \in M} \operatorname{lc}(f_m) \notin \mathfrak{p}$. Hence $\mathbf{J}(I) \not\subset \mathfrak{p}$.

The reverse implication we prove by contraposition, so assume that $\mathfrak{p}$ is unlucky. $\mathfrak{p}$ being unlucky means there is some $m \in \operatorname{lm}(I)$ with $\operatorname{lc}(I, m) \subset \mathfrak{p}$. Now, there is some $m' \in M$ with $m' | m$. We have $\operatorname{lc}(I, m') \subset \operatorname{lc}(I, m)$, thus there is some $m' \in M$ with $\operatorname{lc}(I, m') \subset \mathfrak{p}$. Since $\mathfrak{p}$ is an ideal, this gives $\prod_{m \in M} \operatorname{lc}(I, m) \subset \mathfrak{p}$. Since $\mathfrak{p}$ is prime, this gives that $\sqrt{\prod_{m \in M} \operatorname{lc}(I, m)} \subset \mathfrak{p}$ and we are done. □

If we have a Gröbner basis of $I$, then $\mathbf{J}(I)$ is particularly easy to compute.

**4.19 · Proposition.** *Let $I \subset A[X]$ be an ideal, let $G$ be a Gröbner basis for $I$ and let $M$ be the minimal set of generators of* $\operatorname{lm}(I)$*. Then*

$$\mathbf{J}(I) = \sqrt{\prod_{m \in M} \langle \operatorname{lc}(g) \mid g \in G, \operatorname{lm}(g) = m \rangle}$$

*Proof.* We will prove the following equality:

$$\operatorname{lc}(I, m) = \langle \operatorname{lc}(g) \mid g \in G, \operatorname{lm}(g) = m \rangle \quad \text{for all } m \in M$$

A generator $c$ on the left side is the leading coefficient of a polynomial $f \in I$ with leading monomial $m \in M$. Since $G$ is a Gröbner basis and $m \in M$ is minimal, there is some subset $\{g_1, \ldots, g_j\} \in G$ with $\operatorname{lt}(f) = \sum_{i=1}^{j} \operatorname{lt}(g_i)$. Thus $\operatorname{lc}(f) = \sum_{i=1}^{j} \operatorname{lc}(g_i)$, so $\operatorname{lc}(I, m) \subset \langle \operatorname{lc}(g) \mid g \in G, \operatorname{lm}(g) = m \rangle$.

On the other hand, each generator on the right side is by definition a generator on the left side. □

**4.20 · Example.** Consider again the ideal $I = \langle ax + cy, bx + dy \rangle \subset A[x, y]$ where $A = \mathbb{C}[a, b, c, d]$ with a term order such that $x > y$. A Gröbner basis of $I$ can be found by

computing a reduced Gröbner basis of $I$ in $\mathbb{C}[x, y, a, b, c, d]$ and is given by

$$G = \{ax + cy, bx + dy, (ad - bc)y\}.$$

The minimal set of generators of $\operatorname{lm}(I)$ is $M = \{x, y\}$, so by proposition 4.19 we find that

$$\mathbf{J}(I) = \sqrt{\langle a, b\rangle\langle ad - bc\rangle} = \langle ad - bc\rangle.$$

For any $\mathfrak{p} \in \operatorname{Spec}(A) \setminus \mathbf{V}(ad - bc)$, we have $ad - bc \notin \mathfrak{p}$, so $\frac{(ad-bc)y}{ad-bc} \in \mathcal{I}_{\operatorname{Spec}(A)}(\mathbf{V}(ad - bc))$. Furthermore, we cannot have both $a \in \mathfrak{p}$ and $b \in \mathfrak{p}$. Thus either $\frac{(ax+cy)-cy}{a} = \frac{ax}{a} \in \mathcal{I}_{\operatorname{Spec}(A)}(\mathbf{V}(ad - bc))$ or $\frac{(bx+dy)-dy}{b} = \frac{bx}{b} \in \mathcal{I}_{\operatorname{Spec}(A)}(\mathbf{V}(ad - bc))$. Hence, we see that the reduced Gröbner basis of the ideal $\langle \sigma_{\mathfrak{p}}(I)\rangle$ is $\{x, y\}$.

Clearly, the leading monomial ideal of $I$ will remain unchanged, if we specialize with a point away from the singular ideal, as illutrated above. However, it is not enough to have the function $\mathfrak{p} \mapsto \operatorname{lm}(\sigma_{\mathfrak{p}}(I))$ be constant on $\operatorname{Spec}(A)$. The leading monomials might stay the same, even though some leading coefficients of $I$ vanishes.

**4.21 · Example.** Consider the ideal $I = \langle u^2x - u, ux^2 - x\rangle \subset \mathbb{C}[u][x]$. Here, we have $\operatorname{lm}(\sigma_{\mathfrak{p}}(I)) = \{x\}$ for all $\mathfrak{p} \in \operatorname{Spec}(\mathbb{C}[u])$, but $\operatorname{Spec}(\mathbb{C}[u])$ is not parametric for $I$. Indeed $I_{\langle u\rangle}$ is not monic, since we can't divide by $u$ in $\mathbb{C}[u]_{\langle u\rangle}$, so $\operatorname{Spec}(\mathbb{C}[u])$ is not parametric for $I$ by theorem 4.14.

The generators given above turns out to be a Gröbner basis of $I$:

$$G = \{u^2x - u, ux^2 - x\}$$

which means that the minimal set of generators of $\operatorname{lm}(I)$ is $M = \{x\}$, hence

$$\mathbf{J}(I) = \sqrt{\langle u^2\rangle} = \langle u\rangle.$$

Considering the two cases, we see that

$$\langle \sigma_{\mathfrak{p}}(I)\rangle = \begin{cases} \left\langle x - \frac{1}{\sigma_{\mathfrak{p}}(u)}\right\rangle & \sigma_{\mathfrak{p}}(u) \neq 0 \\ \langle x\rangle & \sigma_{\mathfrak{p}}(u) = 0 \end{cases}$$

which should make it clear why there is no parametric reduced Gröbner basis for $I$ on all of $\mathbb{C}[u]$.

As seen in this example, the singular ideal captures something more subtle than just the leading monomials staying unchanged. In fact, the singular ideal expresses exactly the points, that prevents a set from being parametric.

**4.22 · Theorem.** *Let $I \subset A[X]$ be an ideal, let $Z \subset \operatorname{Spec}(A)$ be closed and $\mathfrak{a} = \mathbf{I}(Z)$ and let $\bar{I}$ be the image of $I$ in $(A/\mathfrak{a})[X]$. Then*

1. *$Z_{gen} := Z \setminus \mathbf{V}(\mathbf{J}(\bar{I}))$ is parametric for $I$ with $\operatorname{lm}(\mathcal{I}_{Z_{gen}}) = \operatorname{lm}(\bar{I})$.*

2. *$Z_{gen}$ is maximal with that property, i.e. if $Y \subset Z$ is parametric for $I$ with $\operatorname{lm}(\mathscr{I}_Y) = \operatorname{lm}(\bar{I})$, then $Y \subset Z_{gen}$.*

*Proof.* First, let's show that $Z_{gen}$ is parametric. It is locally closed, so we just need to show that $\mathscr{I}_{Z_{gen}}$ has a reduced Gröbner basis. Let $M = \{m_1, \dots, m_n\}$ the minimal generating set of $\operatorname{lm}(\bar{I})$ and fix a $\mathfrak{p} \in Z_{gen}$. Since $\prod_{m \in M} \operatorname{lc}(\bar{I}, m) \not\subset \mathfrak{p}$, we can find $P_1, \dots, P_n \in \bar{I}$ such that $\operatorname{lm}(P_i) = m_i$ and $\operatorname{lc}(P_i) \notin \mathfrak{p}$ for all $i$. For each $i$, let $R_i$ be a pseudo-remainder of $P_i$ modulo $\{P_1, \dots, P_n\} \setminus \{P_i\}$, which exists by lemma 2.10. Since $M$ is a minimal generating set of $\operatorname{lm}(\bar{I})$, we have that $\operatorname{lm}(P_i)$ is not divisible by the leading monomial of $P_j$ for any $j \neq i$. Hence, $\operatorname{lm}(R_i) = \operatorname{lm}(P_i)$. Furthermore, if $cP_i = R_i + \sum_{j \neq i} h_j P_j$ is the pseudo-division, we have $\operatorname{lc}(R_i) = c \operatorname{lc}(P_i)$, hence $\operatorname{lc}(R_i) \notin \mathfrak{p}$ since $\mathfrak{p}$ is prime. Define now the open neighborhood of $\mathfrak{p}$

$$U^{\mathfrak{p}} = \{\mathfrak{q} \in Z_{gen} \mid \operatorname{lc}(P_i) \notin \mathfrak{q} \forall i \in \{1, \dots, n\}\}.$$

Then $\mathfrak{q} \mapsto R_i / \operatorname{lc}(R_i)$ is an element of $\mathscr{I}_Z(U)$, which we will denote by $f_i^{\mathfrak{p}}$.

Repeating the above construction for any other $\mathfrak{p}' \in Z_{gen}$, we obtain $f^{\mathfrak{p}'}$ and $U^{\mathfrak{p}'}$. To show that these $f^{\mathfrak{p}}$'s glue together to global elements, we need to show that

$$f_i^{\mathfrak{p}}(\mathfrak{q}) = f_i^{\mathfrak{p}'}(\mathfrak{q}) \quad \forall \mathfrak{q} \in U^{\mathfrak{p}} \cap U^{\mathfrak{p}'}.$$

Find $R_i, R_i' \in \bar{I}$ such that $f_i^{\mathfrak{p}}(\mathfrak{q}) = R_i / \operatorname{lc}(R_i)$ and $f_i^{\mathfrak{p}'}(\mathfrak{q}) = R_i' / \operatorname{lc}(R_i')$ for all $\mathfrak{q} \in U^{\mathfrak{p}} \cap U^{\mathfrak{p}'}$ and note that $\operatorname{lm}(R_i) = \operatorname{lm}(R_i') = m_i$. Then $\operatorname{lm}(\operatorname{lc}(R_i')R_i - \operatorname{lc}(R_i)R_i') < m_i$ and by construction, no term in neither $R_i$ nor $R_i'$ is divisible by any monomial in $M \setminus \{m_i\}$. Since $\operatorname{lc}(R_i')R_i - \operatorname{lc}(R_i)R_i' \in \bar{I}$, this implies that $\operatorname{lc}(R_i')R_i - \operatorname{lc}(R_i)R_i' = 0$. Thus, the mapping $\mathfrak{q} \mapsto f_i^{\mathfrak{q}}(\mathfrak{q})$ defines an element in $\mathscr{I}_{Z_{gen}}$, say $f_i$. Since each $f_i$ is monic, and $\langle \operatorname{lm}(\mathscr{I}_{Z_{gen}}) \rangle = \langle \operatorname{lm}(f_1), \dots, \operatorname{lm}(f_n) \rangle$, we have shown that $\mathscr{I}_{Z_{gen}}$ is a monic ideal. Thus $Z_{gen}$ is a parametric set for $I$ by lemma 4.13.

Now, to show that $Z_{gen}$ is maximal, let $Y \subset Z$ be parametric and assume $\operatorname{lm}(\mathscr{I}_Y) = \operatorname{lm}(\bar{I})$. Let $\mathfrak{b} = \mathbf{I}(\overline{Y})$ and let $G \subset \mathscr{I}_Y$ be the reduced Gröbner basis of $\mathscr{I}_Y$. Fix a $\mathfrak{p} \in Y$ and a $g \in G$. By lemma 4.11 we find a $P/Q = g(\mathfrak{p})$ with $\operatorname{lm}(P) = \operatorname{lm}(g(\mathfrak{p}))$. Since $\operatorname{lm}(P) = \operatorname{lm}(g(\mathfrak{p})) = \operatorname{lm}(g) = \operatorname{lm}(\sigma_{\mathfrak{p}}(g))$, we have $\operatorname{lc}(P) \notin \mathfrak{p}$. Since $Y \subset Z$, that $\mathfrak{p}$ is also in $Z$. Furthermore, since $Y \subset Z$, we have $\mathfrak{a} \subset \mathfrak{b}$, so $P$ is the image of some $P' \in \bar{I} \subset (A/\mathfrak{a})[X]$ in $(A/\mathfrak{b})[X]$. Thus $\operatorname{lc}(P)$ is the image of $\operatorname{lc}(P')$ in $A/\mathfrak{b}$. This means $\operatorname{lc}(P') \notin \mathfrak{p}$, hence $\mathbf{J}(\bar{I}) \not\subset \mathfrak{p}$. Since $\mathfrak{p}$ was arbitrary, $Y \cap \mathbf{V}(\mathbf{J}(\bar{I})) = \emptyset$, so $Y \subset Z_{gen}$. □

We can use this theorem to compute Gröbner covers.

**4.23 · Example.** Consider again the ideal $I = \langle ax+cy, bx+dy \rangle \subset A[x,y] = \mathbb{C}[a,b,c,d][x,y]$ with a term order such that $x > y$. A Gröbner basis of $I$ is given by

$$G = \{ax + cy, bx + dy, (ad - bc)y\}.$$

The minimal set of generators of $\mathrm{lm}(I)$ is $M = \{x, y\}$, so by proposition 4.19 we find that

$$\mathbf{J}(I) = \sqrt{\langle a, b\rangle\langle ad - bc\rangle} = \langle ad - bc\rangle.$$

Let $Z = \mathrm{Spec}(A)$, then $Z_{gen} = \mathrm{Spec}(A) \setminus \mathbf{V}(ad - bc)$ is a parametric set by theorem 4.22. Let's find its reduced Gröbner basis.

We can find elements $P_1, P_1 \in I$ such that $\mathrm{lm}(P_1) = x$ and $\mathrm{lm}(P_2) = y$. We choose $P_1 = ax + cy$ and $P_2 = (ad - bc)y$. Pseudo-reducing $P_1$ by $P_2$, we get

$$\begin{aligned} R_1 &= (ad - bc)(ax + cy) - c((ad - bc)y) && = (a(ad - bc))x \\ R_2 & && = (ad - bc)y \end{aligned}$$

We have $\mathrm{lc}(R_2) \notin \mathfrak{p}$ for all $\mathfrak{p} \in Z_{gen}$, i.e. $\{\mathfrak{p} \in Z_{gen} \mid ad - bc \notin \mathfrak{p}\} = Z_{gen}$. This means

$$f_2(\mathfrak{p}) = \frac{(ad - bc)y}{ad - bc} \in \mathcal{I}_{Z_{gen}}$$

defines an element on $\mathcal{I}_{Z_{gen}}$.

However, we don't always have $a(ad - bc) \notin \mathfrak{p}$, so $R_1$ does not define a global element of $\mathcal{I}_{Z_{gen}}$. To remedy this, we find a different element

$$P_1' = bc + dy \quad \text{giving} \quad R_1' = (b(ad - bc))x$$

We see that $\{\mathfrak{p} \in Z_{gen} \mid a(ad-bc) \notin \mathfrak{p} \vee b(ad-bc) \notin \mathfrak{p}\} = Z_{gen}$, since if $a(ad-bc), b(ad-bc) \in \mathfrak{p}$ and $ad - bc \notin \mathfrak{p}$, then both $a, b \in \mathfrak{p}$. But then $ad - bc \in \mathfrak{p}$, which is a contradiction. Hence, we get that

$$f_1(\mathfrak{p}) = \begin{cases} \frac{(a(ad-bc))x}{a(ad-bc)}, & a \notin \mathfrak{p} \\ \frac{(b(ad-bc))x}{b(ad-bc)}, & b \notin \mathfrak{p} \end{cases}$$

is an element of $\mathcal{I}_{Z_{gen}}$. Hence $\{f_1, f_2\}$ is the reduced Gröbner basis of the parametric set $Z_{gen} = \mathrm{Spec}(A) \setminus \mathbf{V}(ad - bc)$ for $I$. We also see that $\langle \sigma_{\mathfrak{p}}(I)\rangle = \langle x, y\rangle$ for all $\mathfrak{p} \in \mathbb{Z}_{gen}$.

Let's now move on to the segment $\mathbf{V}(ad-bc)$. Let $\overline{I}$ be the image of $I$ in $(\mathbb{C}[a, b, c, d]/\langle ad - bc\rangle)[x, y]$. For any $f \in I$, we denote its image in $\overline{I}$ by $\overline{f}$. By applying lemma 4.27, we can compute the following Gröbner basis of $\overline{I}$:

$$G = \{\overline{ax + cy}, \overline{bx + dy}\}$$

The minimal set of generators of $\mathrm{lm}(\overline{I})$ is $M = \{x\}$, so by proposition 4.19 we find that

$$\mathbf{J}(\overline{I}) = \sqrt{\langle a, b\rangle} = \langle a, b\rangle$$

Let $Z = \mathrm{Spec}(A/\langle ad - bc\rangle)$, then $Z_{gen} = Z \setminus \mathbf{V}(a, b)$ is parametric for $\overline{I}$ by theorem 4.22. We can find its reduced Gröbner basis.

First, we can find an element $P_1 \in \overline{I}$ such that $\operatorname{lm}(P_1) = x$, say $P_1 = \overline{ax + cy}$. We don't always have $a \notin \mathfrak{p}$ for any $\mathfrak{p} \in Z_{gen}$. However, we always that either $a \notin \mathfrak{p}$ or $b \notin \mathfrak{p}$. Thus, we can supplement with $P_1' = \overline{bx + dy}$. Thus, the regular function

$$f_1(\mathfrak{p}) = \begin{cases} \frac{ax+cy}{a}, & a \notin \mathfrak{p} \\ \frac{bx+dy}{b}, & b \notin \mathfrak{p} \end{cases}$$

forms the reduced Gröbner basis of $\overline{I}$ on the segment $\operatorname{Spec}(A/\langle ad - bc\rangle) \setminus \mathbf{V}(a, b)$.

The next segment we need to cover is $\operatorname{Spec}(A/\langle a, b\rangle)$. Let's again denote the image of $I$ in $(A/\langle a, b, \rangle)[X]$ by $\overline{I}$, and similarly for polynomials. By applying lemma 4.27, we find the following Gröbner basis of $\overline{I}$:

$$G = \{cy, dy\}$$

giving the singular ideal

$$\mathbf{J}(\overline{I}) = \sqrt{\langle c, d\rangle} = \langle c, d\rangle$$

Hence,

$$f_1(\mathfrak{p}) = \begin{cases} \frac{cy}{c}, & c \notin \mathfrak{p} \\ \frac{dy}{d}, & d \notin \mathfrak{p} \end{cases}$$

is the reduced Gröbner basis of the parametric set $\operatorname{Spec}(A/\langle a, b\rangle) \setminus \mathbf{V}(c, d)$.

The final segment is on $\mathbf{V}(a, b, c, d)$ on which $\overline{I} = \langle 0\rangle$. Thus, we have found a complete Gröbner cover of $I$.

## 4.4 The projective case

Let $I \subset A[X]$ be an ideal. In the affine case we've seen that, even though $\operatorname{lm}(\sigma_{\mathfrak{p}}(I))$ is constant over all $\mathfrak{p}$ in some locally closed set $S$, that does not mean that $S$ is parametric. Thus, it is quite difficult to give a "canonical" cover of $\operatorname{Spec}(A)$ with parametric sets. If $I$ is homogenous, we are in luck.

**4.24 · Theorem.** *Let $I \subset A[X]$ be a homogenous ideal and $\mathfrak{p} \in \operatorname{Spec}(A)$. Then $\mathfrak{p}$ is lucky for $I$ if and only if $\operatorname{lm}(\sigma_{\mathfrak{p}}(I)) = \operatorname{lm}(I)$.*

*Proof.* By theorem 4.22, we have the first implication. For the reverse implication, assume that $\operatorname{lm}(\sigma_{\mathfrak{p}}(I)) = \operatorname{lm}(I)$ and assume for a contradiction that $\mathfrak{p}$ is unlucky for $I$, i.e. there is some $m \in \operatorname{lm}(I)$ with $\operatorname{lc}(I, m) \subset \mathfrak{p}$. Since there are only finitely many monomials with the same degree as $m$, we can assume that for every $m'$ with $\deg(m') = \deg(m)$, we have $\operatorname{lc}(I, m') \subset \mathfrak{p} \implies m' < m$. Since by assumption $\operatorname{lm}(I) = \operatorname{lm}(\sigma_{\mathfrak{p}}(I))$, we can find a $P \in I$ with $\operatorname{lm}(\sigma_{\mathfrak{p}}(P)) = m$, and since $I$ is homogenous, we can assume that $P$ is homogenous by lemma A.4. Because $<$ is a well-order, we can take $P$ to have minimal leading monomial, i.e. if $P' \in I$ with $\operatorname{lm}(\sigma_{\mathfrak{p}}(P')) = m$ then $\operatorname{lm}(P) < \operatorname{lm}(P')$.

Since $\mathrm{lc}(I, m) \subset P$, we have $\mathrm{lt}(P) \gtrsim m$, and because $\deg(\mathrm{lt}(P)) = m$, we have $\mathrm{lc}(I, \mathrm{lm}(P)) \notin \mathfrak{p}$ since we assumed $m$ to be maximal among the monomials of its degree. Therefor we can find some $Q \in I$ with $\mathrm{lm}(Q) = m = \mathrm{lm}(P)$ and $\mathrm{lc}(Q) \notin \mathfrak{p}$. Now, we can construct a new polynomial

$$P' = \mathrm{lc}(Q)P - \mathrm{lc}(P)Q$$

which has $\mathrm{lm}(P') < \mathrm{lm}(P)$. However, see that $\mathrm{coef}(P, m') \in \mathfrak{p}$ for every $m' > m$ and $\mathrm{lc}(P) \in \mathfrak{p}$.Hence, we have $\mathrm{coef}(P', m') \in \mathfrak{p}$ for every $m' > m$ since the corresponding terms on both sides of the subtraction has coefficients in $p$. Hence $\mathrm{lm}(\sigma_{\mathfrak{p}}(P')) \leq m$. But $\mathrm{lc}(q) \notin \mathfrak{p}$ and $\mathrm{coef}(P, m) \notin \mathfrak{p}$, so $\mathrm{lc}(Q)\,\mathrm{coef}(P, m) \notin \mathfrak{p}$ since $\mathfrak{p}$ is prime. But $\mathrm{lc}(P) \in \mathfrak{p}$, so $\mathrm{coef}(P', m) \notin \mathfrak{p}$, thus $\mathrm{lc}(\sigma_{\mathfrak{p}}(P')) = m$. However, this contradicts the minimality of $P$. □

We are now ready for the grand finale in the projective case, namely that partitioning $\mathrm{Spec}(A)$ with respect to $\mathrm{lm}(\sigma_{\mathfrak{p}}(I))$ gives a canonical partition into (maximal) parametric sets. Specifically, if we partition $\mathrm{Spec}(A)$ be the equivalence relation $\mathfrak{p} \sim \mathfrak{p}'$ exactly when $\mathrm{lm}(\sigma_{\mathfrak{p}}(I)) = \mathrm{lm}(\sigma_{\mathfrak{p}'}(I))$, then the equivalence classes are parametric sets. Since the leading monomials of a parametric set must remain constant, these equivalence classes are maximal and disjoint, giving us the most natural and canonical Göbner cover.

Before we can prove this theorem, we need a technical lemma.

**4.25 · Lemma.** *Let $S_1, S_2, \ldots, S_n \subset \mathrm{Spec}(A)$ be locally closed sets and let $C = \bigcup_{i=1}^{n} S_i$. Then the closure of $C$ can be written uniquely as a union of irreducible closed sets, where none is contained in another:*

$$\overline{C} = Z_1 \cup Z_2 \cup \cdots \cup Z_m.$$

*Furthermore, for each $i \in \{1, 2, \ldots, m\}$ there is a $j$ such that $Z_i \cap S_j \neq \emptyset$.*

*Proof.* The unique decomposition is a standard theorem, see f.ex. proposition 3.6.15 in [12].

For the second part, fix an $i \in \{1, 2, \ldots, m\}$ and find a $j$ such that $Z_i \cap \overline{S_j} \neq \emptyset$. By applying proposition 3.6.15 in [12] again, we can split $\overline{S_j}$ into irreducible closed sets, and find one which intersects non-emptily with $Z_i$. Hence we can assume that $\overline{S_j}$ is irreducible.

Since $\overline{S_j}$ is irreducible, we must have $\overline{S_j} \subset Z_i$. If that was not the case, then

$$\overline{S_j} = (\overline{S_j} \cap Z_i) \cup (\overline{S_j} \cap \bigcup_{i' \neq i} Z_{i'})$$

and thus $\overline{S_j}$ would not be irreducible. Hence, $S_j \subset \overline{S_j} \subset Z_i$ as wanted. □

We're now ready to prove the main theorem.

**4.26 · Theorem.** *Let $I \subset A[X]$ be a homogenous ideal and let $S \subset \mathrm{Spec}(A)$ be locally closed. Then the equivalence classes of $S/\sim$ by the equivalence relation described above are*

*parametric sets for $I$.*

*Proof.* By proposition 4.7, we can assume $S = \operatorname{Spec}(A)$. Indeed, if we prove that an equivalence class $Y \subset \operatorname{Spec}(A)$ is parametric, then $S \cap Y$ is a locally closed subset of $Y$. Thus $S \cap Y$ is parametric by Proposition 4.7. Since every equivalence of $S/\sim$ is of the form $S \cap Y$ for some equivalence class $Y$ of $\operatorname{Spec}(A)/\sim$, this gives us what we want.

Let $Y \subset \operatorname{Spec}(A)$ be an equivalence class and let $M$ we the constant value of $\operatorname{lm}(\sigma_{\mathfrak{p}}(I))$ for any $\mathfrak{p} \in Y$. Let $Z = \overline{Y}$ be the closure of $Y$, let $\mathfrak{a} = \mathbf{I}(Z)$ and let $\bar{I}$ be the image of $I$ in $(A/\mathfrak{a})[X]$. The goal is to show that $Y = \overline{Y} \setminus \mathbf{V}(\mathbf{J}(\bar{I}))$, which is parametric by theorem 4.22. Note that for any $f \in I$ and $\mathfrak{p} \in Y$, we have $\sigma_{\mathfrak{p}}(f) = \sigma_{\mathfrak{p}}(f + \mathfrak{a})$, hence $M = \operatorname{lm}(\sigma_{\mathfrak{p}}(I)) = \operatorname{lm}(\sigma_{\mathfrak{p}}(\bar{I}))$. Since $\bar{I}$ is also homogenous, by theorem 4.24 (applied to $\bar{I}$) and lemma 4.18, we have for all $\mathfrak{p} \in \overline{Y}$ that if $\operatorname{lm}(\bar{I}) = \operatorname{lm}(\sigma_{\mathfrak{p}}(I))$ then $\mathfrak{p} \notin \mathbf{V}(\mathbf{J}(\bar{I}))$. Since $Y$ is exactly those $\mathfrak{p}$, where $\operatorname{lm}(\sigma_{\mathfrak{p}}(I)) = M$, we just need to show that $\operatorname{lm}(\bar{I}) = M$.

By lemma 4.25, we can write $Z$ as a union of irreducible, closed sets:

$$Z = Z_1 \cup Z_2 \cup \cdots \cup Z_n.$$

For each $i$, let $\bar{I}_i$ denote the image of $I$ in $(A/\mathbf{I}(Z_i))[X]$ and let $S_i = Z_i \setminus \mathbf{V}(\mathbf{J}(\bar{I}_i))$. Notice that since $\mathbf{I}(Z) \subset \mathbf{I}(Z_i)$, we have that $\sigma_{\mathfrak{p}}(\bar{I}_i) = \sigma_{\mathfrak{p}}(\bar{I})$ for all $\mathfrak{p} \in Z_i \subset \overline{Y}$. Also, by theorem 4.22 we have that $S_i$ is parametric with $\operatorname{lm}(\mathcal{J}_{S_i}) = \operatorname{lm}(\bar{I}_i)$ and by theorem 4.6 $\operatorname{lm}(\mathcal{J}_{S_i}) = \operatorname{lm}(\sigma_{\mathfrak{p}}(\bar{I}_i))$ for all $\mathfrak{p} \in S_i$. By the second part of lemma 4.25, there is some $\mathfrak{p} \in S_i \cap Y$, so $\operatorname{lm}(\sigma_{\mathfrak{p}}(\bar{I}_i)) = M$ for all $\mathfrak{p} \in S_i$. Hence,

$$M = \operatorname{lm}(\sigma_{\mathfrak{p}}(\bar{I})) = \operatorname{lm}(\sigma_{\mathfrak{p}}(\bar{I}_i)) = \operatorname{lm}(\mathcal{J}_{S_i}) = \operatorname{lm}(\bar{I}_i) \quad \text{for all } \mathfrak{p} \in S_i.$$

Now, we use this to show that $\operatorname{lm}(\bar{I}) = M$. Let $P \in \bar{I}$, and let $\overline{P_i}$ denote the image of $P$ in $\bar{I}_i$. If there is an $i$ such that $\operatorname{lm}(P) = \operatorname{lm}(\overline{P_i})$, then $\operatorname{lm}(P) \in \operatorname{lm}(\bar{I}_i) = M$. On the other hand, if $\operatorname{lm}(P) > \operatorname{lm}(\overline{P_i})$ for all $i$, then $\operatorname{lc}(P) \in \mathbf{I}(Z_1) \cap \cdots \cap \mathbf{I}(Z_n) = \mathfrak{a}$. Thus, $\operatorname{lc}(P) = 0$, which is not allowed. This gives $\operatorname{lm}(\bar{I}) \subset M$.

For the reverse inclusion, take an $m \in M$. Since $M = \operatorname{lm}(\bar{I}_1)$, we can find some $P \in \bar{I}$ such that $\operatorname{lm}(\overline{P_1}) = m$ ($\overline{P_1}$ being the image of $P$ in $\mathbf{I}(Z_1)$ as before). This means $\operatorname{coef}(P, m) \notin \mathbf{I}(Z_1)$ but $\operatorname{coef}(P, m') \in \mathbf{I}(Z_1)$ for all $m' > m$. If $n = 1$, then $Z = Z_1$ and we are done, so assume $n > 1$ and find some $c \in \bigcap_{i=2}^{n} \mathbf{I}(Z_i) \setminus \mathbf{I}(Z_1)$. Such an element exist, because the $\mathbf{I}(Z_i)$'s are a minimal primary decomposition of $\mathbf{I}(Z)$, so by minimality $\mathbf{I}(Z_1) \not\supset \bigcap_{i=2}^{n} \mathbf{I}(Z_i)$. Consider now the polynomial $cP$, which has the property that $\operatorname{coef}(cP, m') \in \mathbf{I}(Z)$ for all $m' > m$. Furthermore, since $\mathbf{I}(Z_1)$ is a radical, primary ideal, it is prime, so $\operatorname{coef}(cP, m) \notin \mathbf{I}(Z_1)$. This gives $\operatorname{coef}(cP, m) \notin \mathbf{I}(Z)$. Thus every term in $cP$ larger than $m$ is zero, so $\operatorname{lm}(cP) = m$. Thus $M \subset \operatorname{lm}(\bar{I})$, which completes the proof. □

## 4.5 Relation to the CGS algorithm

The **CGS** algorithm can be seen as an algorithm that computes Gröbner covers. Indeed, by inspecting the construction, we see that if $(E, \{h\}, G)$ is a segment in the output of

**CGS**$(F, S)$, then $V(E) \setminus V(\{h\})$ is a parametric set.

Before we can prove that **CGS** produces Gröbner covers, we need two lemmas, which bridge the gap between the abstract setting with the more concrete setting. First, we need a way to compute Gröbner bases in polynomial rings over quotient rings.

**4.27 · Lemma.** *Let $\langle F\rangle \subset A[X]$ and $\langle S\rangle \subset A$ be ideals and let $G$ be a Gröbner basis of $\langle F \cup S\rangle$. Consider the ring $A/\langle S\rangle$, and denote the image of a polynomial $f \in A[X]$ in $(A/\langle S\rangle)[X]$ by $\overline{f}$. Then $\overline{G}$ is a Gröbner basis of $\langle \overline{F}\rangle \subset (A/\langle S\rangle)[X]$.*

*Proof.* First note, that $\langle \overline{S}\rangle = \langle 0\rangle \subset (A/\langle S\rangle)[X]$, so $\langle \overline{F}\rangle = \langle \overline{F \cup S}\rangle$. Take any $\overline{f} \in \langle \overline{F}\rangle$. Then we can find a representative $f \in \langle F \cup S\rangle$ of $\overline{f}$ such that either $f \in A$ or $\operatorname{lc}(f) \notin \langle S\rangle$. Indeed, if we found a representative $f \notin A$ with $\operatorname{lc}(f) \in \langle S\rangle$, then $f' = f - \operatorname{lt}(f) \in \langle F \cup S\rangle$ is also a representative of $\overline{f}$ with strictly smaller leading monomial. By repeating this procedure, we can find a representative with the desired properties. We can now take care of those two cases:

- If $f \in A$, then there is some $g \in G$ with $\operatorname{lt}(g) \mid \operatorname{lt}(f)$, implying that $g \in A$. Thus $g \mid f$, which is preserved under quotients, so $\overline{g} \mid \overline{f}$.
- If $\operatorname{lc}(f) \notin \langle S\rangle$, then $\operatorname{lt}(f) \in \langle \operatorname{lt}(\langle F\rangle)\rangle$, hence there is some $g \in G$ with $\operatorname{lt}(g) \mid \operatorname{lt}(f)$. Since $\operatorname{lc}(f) \notin \langle S\rangle$, we have $\operatorname{lm}(f) = \operatorname{lm}(\overline{f})$, so $\operatorname{lt}(\overline{g}) \mid \operatorname{lt}(\overline{f})$.

Thus $\langle \operatorname{lt}(\overline{G})\rangle = \langle \operatorname{lt}(\langle \overline{F}\rangle)\rangle$, so $\overline{G}$ is a Gröbner basis of $\langle \overline{F}\rangle$. □

Next, it seems like Gröbner covers are not as powerful as Gröbner systems. Recall, that a specialization of a Gröbner system can have any extension field of $k$ as codomain, wheres specializations of a Gröbner cover can only go to $k(\mathfrak{p})$ for $\mathfrak{p} \in \operatorname{Spec}(A)$. However, no power is actually lost by this restriction.

**4.28 · Lemma.** *Let $I \subset k[U][X], E \subset k[U], N \subset k[U]$ be ideals and let $G \subset k[U][X]$ be a finite set. Then $\sigma_\alpha(G)$ is a Gröbner basis of $\langle \sigma_\alpha(I)\rangle$ for all $\alpha \in \mathbf{V}(E) \setminus \mathbf{V}(N) \subset k_1^{|U|}$ for all field extensions $k_1 \supset k$ if and only if $\sigma_\mathfrak{p}(G)$ is a Gröbner basis of $\langle \sigma_\mathfrak{p}(I)\rangle$ for all $\mathfrak{p} \in \mathbf{V}(E) \setminus \mathbf{V}(N) \subset \operatorname{Spec}(k[U])$.*

*Proof.* First, assume $\sigma_\alpha(G)$ is a Gröbner basis for any $\alpha$. Take $k_1 = k(\mathfrak{p})$ to be the residue field of $k[U]$ at $\mathfrak{p}$. Then we have the canonical map $\sigma_\mathfrak{p} : k[U] \to k(\mathfrak{p})$. Denoting $U = \{u_1, u_2, \dots, u_m\}$, we take $\alpha = (\sigma_\mathfrak{p}(u_1), \sigma_\mathfrak{p}(u_2), \dots, \sigma_\mathfrak{p}(u_m))$. Then $\sigma_\alpha = \sigma_\mathfrak{p}$ as ring homomorphisms, hence $\sigma_\mathfrak{p}(G)$ is a Gröbner basis.

For the reverse implication, let $k_1 \supset k$ be a field extension and let $\sigma_\alpha : k[U] \to k_1$. Since the codomain of $\sigma_\alpha$ is a field, $\ker(\sigma_\alpha)$ is a prime ideal. Hence, we can see $k_1$ as a field extension of the residue field $k(\ker(\sigma_\alpha))$ with $\operatorname{Im}(\sigma_\alpha) \subset k(\ker(\sigma_\alpha))$. Under these identifications, we again have $\sigma_\alpha = \sigma_{\ker(\sigma_\alpha)}$ as ring homomorphisms, only with a larger codomain. Since $\sigma_{\ker(\sigma_\alpha)}(G)$ is a Gröbner basis in $k(\ker(\sigma_\alpha))$, we have that it is also a Gröbner basis in $k_1 \supset k(\ker(\sigma_\alpha))$. Hence $\sigma_\alpha(G)$ is a Gröbner basis. □

**4.29 · Theorem.** *Let $F \subset k[X,U]$ and $T \subset k[U]$ be finite sets of polynomials and let $\mathscr{H} = \mathbf{CGS}(F,T)$. If $(S,\{h\},G) \in \mathscr{H}$, then $\mathbf{V}(S) \setminus \mathbf{V}(\{h\})$ is a parametric set and $G$ is its reduced Gröbner basis.*

*Proof.* Let $(S,\{h\},G) \in \mathscr{H}$ be a segment, and let $(S,\{h\},G')$ be the corresponding segment computed by $\mathbf{CGS}_{\mathbf{simple}}$. Let $I = \langle F \rangle$, let $\overline{I}$ denote the image of $I$ in $(k[U]/\langle S \rangle)[X]$, and for a polynomial $f \in k[U][X]$, let $\overline{f}$ denote its image in $(k[U]/\langle S \rangle)[X]$. By construction, $G'$ is a Gröbner basis of $\langle F \cup S \rangle$ and $h = \operatorname{lcm}(\{\operatorname{lc}_U(g) \mid g \in G \setminus \langle S \rangle\})$. By lemma 4.27 we then have, that $\overline{G'} = \{\overline{g} \mid g \in G'\}$ forms a Gröbner basis of $\overline{I}$.

By theorem 3.1, we have that $\operatorname{lm}_U(G') = \operatorname{lm}(\overline{G'})$, so using proposition 4.19 we get that $\langle h \rangle \subset \mathbf{J}(\overline{I})$. This implies that $\mathbf{V}(S) \setminus \mathbf{V}(h)$ is parametric by theorem 4.22 and proposition 4.7. Finally, by theorem 3.5, we have that $\sigma_\alpha(G)$ is the reduced Gröbner basis of $\langle \sigma_\alpha(F) \rangle$ for all $\alpha \in \mathbf{V}(S) \setminus \mathbf{V}(\{h\})$. Thus the image of $G$ in $\mathscr{I}_{\mathbf{V}(S)}(\mathbf{V}(\{h\})^{\mathsf{C}})$ is the reduced Gröbner basis of the parametric set $\mathbf{V}(S) \setminus \mathbf{V}(\{h\})$ □

# 5 Applications

## 5.1 Quantifier elimination

One of the first applications of parametric Gröbner bases was presented by its inventor Weispfenning [14] in the original article. It concerns the problem of computing a system of polynomial equations, whose solutions are equivalent to solutions to a set of logical expressions involving polynomial equations, con- and disjunctions, negations and existential quantifiers.

Sepcifically, we're given a formula $\exists x_1, \dots, x_n : \phi(U, x_1, \dots, x_n)$ where $\phi$ is a combination using $\wedge$ and $\vee$ of polynomial equalities and inequalities in $k[U, X]$. If $k_1$ is an extension field of $k$, then that formula determines a partioning of $k_1^{|U|}$, namely those values of $U$ where the formula is true and those where it isn't. Our goal is to find a system of polynomial equations in $k[U]$ that is satisfied in exactly the same points.

First, we need to normalize the logical expressions, to fit a format we can work with.

**5.1 · Definition (Positive, primitive formula).** A logical formula $\varphi$ is called *positive and primitive* if it only involves polynomial equalities in $k[X]$, conjunctions and existential quantifiers.

**5.2 · Lemma.** *Let $\phi$ be a logical formula involving polynomial equalities, conjunctions, disjunctions, negations and existential quantifiers. Then there exists a finite set of positive, primitive formula $\varphi_1, \varphi_2, \dots, \varphi_r$ such that $\phi \iff (\varphi_1 \vee \dots \vee \varphi_r)$.*

*Proof.* Using standard logical rules, we can find $\phi_1, \dots, \phi_r$ containing only polynomial equalities, conjunction, negation and existential quantifiers such that

$$\phi \iff \bigvee_{i=1}^{r} \phi_r.$$

Using De Morgans law and distributivity we can assume that negations are at the lowest level of the formulas. Thus, we can see the $\phi_i$'s as existstential formulas containing conjunctions of polynomial equations and inequations.

Now, to eliminate the inequalities, we use the following trick:

$$f(X) \neq 0 \iff \exists t : f(X) \cdot t - 1 = 0. \qquad \square$$

Thus we can solve each of the positive, primitive formulas independently, and see if any of them are satifiable.

**5.3 · Theorem.** *Let $F \subset k[U, X]$ be a finite set of polynomials over an algebraically closed field and let $G$ be a parametric Gröbner basis of $F$. For a polynomial $f \in k[U][X]$, let*

$C(f) \subset k[U]$ *denote the set of coefficients of non-constant terms in* $f$*. Then*

$$\left(\exists x_1, \dots, x_n : \bigwedge_{f \in F} f(U, x_1, \dots, x_n) = 0\right) \iff \bigwedge_{g \in G} \left(g(U, 0, \dots, 0) = 0 \vee \bigvee_{c \in C(g)} c(U) \neq 0\right)$$

*in any extension field* $k_1 \supset k$*.*

*Proof.* Let $\alpha \in k_1^{|U|}$. Then the question of whether $\exists x_1, \dots, x_n : \bigwedge_{f \in F} f(U, x_1, \dots, x_n) = 0$ is satisfied in $U = \alpha$ is equivalent to whether $\langle \sigma_\alpha(F) \rangle$ has a common zero, i.e. if $V(\langle \sigma_\alpha(F) \rangle) \neq \emptyset$.

For the first implication, assume $\exists x_1, \dots, x_n : \bigwedge_{f \in F} f(U, x_1, \dots, x_n) = 0$ is satisfied at some $\alpha \in k_1^{|U|}$. Let $\beta \in k_1^{|X|}$ be a vector of $(x_1, \dots, x_n)$ such that $f(\alpha, \beta) = 0$ for all $f \in F$. Then, since all $g \in G$ are also in $\langle F \rangle$, we get $g(\alpha, \beta) = 0 \ \forall g \in G$. Hence, if $g(\alpha, 0, \dots, 0) \neq 0$, then there has to be some non-constant term in $g$, which is also non-zero at $\alpha$.

For the other implication, assume every $g \in G$ has zero constant term or some non-zero non-constant term, when viewed as a polynomial in $k[U][X]$. Assume for a contradiction that $V(\langle \sigma_\alpha(F) \rangle) = \emptyset$. By the weak Nullstellensatz we get that $1 \in \langle \sigma_\alpha(F) \rangle$. Since $G$ is a parametric Gröbner basis, there is some $g \in G$ such that $\mathrm{lt}(\sigma_\alpha(g)) \mid 1$. Thus $\sigma_\alpha(g)$ is a constant polynomial with non-zero constant term, contradicting the assumption. □

## 5.2 Parametric ideal membership

**5.4 · Theorem.** *Let* $(Y, G)$ *be a segment of a parametric Gröbner basis where* $G = \{g_1, \dots, g_n\} \subset A[X]$*, and let* $f \in A[X]$ *and assume that* $\sigma_\alpha(\mathrm{lc}(g)) \neq 0$ *for all* $g \in G$ *and* $\alpha \in Y$*. Then* $\sigma_\alpha(f) \in \langle \sigma(G) \rangle$ *for all* $\alpha \in Y$ *if and only if any pseudo-remainders* $r$ *of* $f$ *under pseudo-division modulo* $G$ *satisfies* $\sigma_\alpha(r) = 0$ *for all* $\alpha \in Y$*.*

*Proof.* If any pseudo-remainder of $f$ under pseudo-division modulo $G$ is zero, then

$$cf = \sum_{i=1}^{n} f_i g_i$$

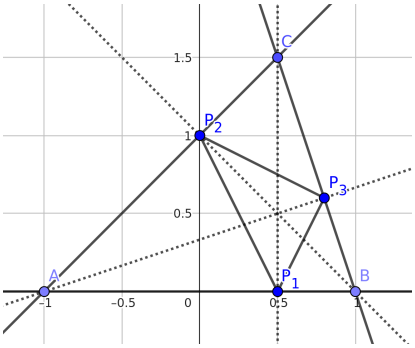
for some $f_i \in A[X]$ and $c \in A$, where $c$ is a product of leading coefficients of $G$. Since none of those leading coefficients vanish under $\sigma_\alpha$, we have $\sigma_\alpha(c) \neq 0$. Hence

$$\sigma_\alpha(f) = \frac{1}{\sigma_\alpha(c)} \sum_{i=1}^{n} \sigma_\alpha(f_i g_i)$$

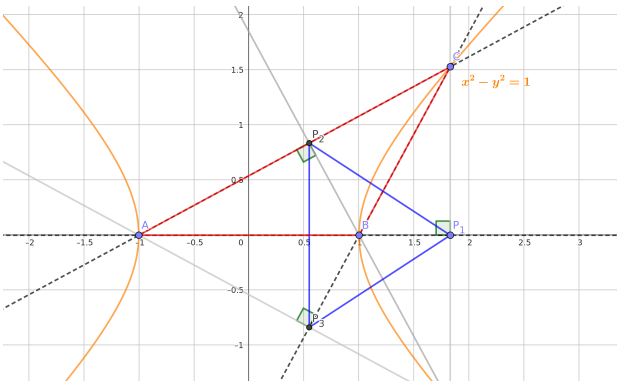
so $\sigma_\alpha(f) \in \langle \sigma_\alpha(G) \rangle$.

On the other hand, assume $\sigma_\alpha(f) \in \langle \sigma_\alpha(G) \rangle$ for all $\alpha \in Y$. Fix a specialization $\sigma_\alpha$, and note that if

$$cf = r + \sum_{i=1}^{n} f_i g_i$$




(a) A triangle with its orthic triangle drawn.




(b) A triangle with a non-obvious isosceles orthic triangle.

Figure 1: Orthic triangles

is a pseudo-division, then $\sigma_\alpha(f) \in \langle \sigma_\alpha(G) \rangle$ if and only if $\sigma_\alpha(r) = 0$. Thus $\sigma_\alpha(r) = 0$ for all $\alpha \in Y$, since $\sigma_\alpha(f) \in \langle \sigma_\alpha(G) \rangle$ for all $\alpha$. □

We can use this theorem to discover geometric theorems in the complex plane. Let us look at an example from [9].

**5.5 · Example.** Consider a triangle with vertices $A = (-1, 0)$, $B = (1, 0)$ and $C = (a, b)$. Now, draw the three altitudes of the triangle $ABC$, and label their basepoints $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $P_3 = (x_3, y_3)$, see figure 1a. The triangle $P_1P_2P_3$ is called the *orthic* triangle of $ABC$. We wish to determine when the orthic triangle is isosceles with $|P_1P_2| = |P_1P_3|$.

To solve this problem, we produce a parametric ideal that describes the setup. First, observe that $x_1 = a$ and $y1 = 0$, so we make that substitution immediately. This also ensures that the line $P_1C$ is orthogonal to the line $AB$. Next, we need that the line $BP_2$ is orthogonal to the line $AC$. This means $0 = BP_2 \cdot AC = (a+1)(x_2 - 1) + by_2$. Similarly, to ensure that $AP_3$ is orthogonal to $BC$, we have $0 = (a-1)(x_3 + 1) + by_3$. We also need to ensure that the points $P_2$ and $P_3$ lies on the edges of the triangle. This is done by forcing $0 = b(x_2 + 1) - (a+1)y_2$ and similarly $0 = b(x_3 - 1) - (a-1)y_3$. Hence, the following ideal describes the setup:

$$\begin{aligned} I = \langle\ & (a+1)(x_2-1) + by_2, \quad b(x_2+1) - (a+1)y_2, \\ & (a-1)(x_3+1) + by_3, \quad b(x_3-1) - (a-1)y_3\ \rangle \end{aligned}$$

If you're following along with the code, you here is the setup:

```
using AbstractAlgebra
using ParametricGrobnerBases
R, (a, b) = QQ[:a, :b]
S, (x2, x3, y2, y3) = R[:x2, :x3, :y2, :y3]
```

```
I = [(a + 1)*(x2 - 1) + b*y2, b*(x2 + 1) - (a + 1)*y2, (a - 1)*(x3 +
↪  1) + b*y3, b*(x3 - 1) - (a - 1)*y3]
```

We want to determine for which values of $a$ and $b$ we have that $|P_1P_2| = |P_1P_3|$, i.e. that $0 = f = (x_3-a)^2+y_3^2-(x_2-a)^2+y_2^2$. This is equivalent to asking whether $\sigma(f) \in \langle\sigma(I)\rangle$ for some specialization $\sigma : \mathbb{C}[a,b] \to \mathbb{C}$.

```
f = (x3 - a)^2 + y3^2 - (x2 - a)^2 - y2^2
```

To answer this question, we can use the output of $\mathbf{CGS}(I)$. It returns several segments, but most of them has the condition $b = 0$, leading to a degenerate triangle. There is only one case, which is interesting:

$$V(0) \setminus \mathbf{V}((a^2+2a+b^2+1)(a^2-2a+b^2+1)b)\ ,\ G$$

where

$$\begin{aligned} G = \{\ & (a^2-2a+b^2+1)y_3 + 2ab - 2b \\ & (a^2+2a+b^2+1)y_2 - 2ab - 2b \\ & (a^2b-2ab+b^3+b)x_3 + a^2b - 2ab - b^3 + b \\ & (a^2b+2ab+b^3+b)x_2 - a^2b - 2ab + b^3 - b\ \} \end{aligned}$$

To determine whether $f$ lies in this segment, we compute a pseudo-remainder of $f$ modulo $G$. Like this in Julia:

```
G = CGS(I)[1][3]
r = pseudo_reduce(f, G)[2]
```

This gives

$$\begin{aligned} r =& 4a^{17}b^4 + 24a^{15}b^6 - 32a^{15}b^4 + 56a^{13}b^8 - 120a^{13}b^6 + 112a^{13}b^4 + 56a^{11}b^{10} - \\ & 144a^{11}b^8 + 216a^{11}b^6 - 224a^{11}b^4 - 40a^9b^{10} + 72a^9b^8 - 120a^9b^6 + 280a^9b^4 - \\ & 56a^7b^{14} - 16a^7b^{10} + 32a^7b^8 - 120a^7b^6 - 224a^7b^4 - 56a^5b^{16} - 72a^5b^{14} - \\ & 16a^5b^{10} + 72a^5b^8 + 216a^5b^6 + 112a^5b^4 - 24a^3b^{18} - 80a^3b^{16} - 72a^3b^{14} - \\ & 40a^3b^{10} - 144a^3b^8 - 120a^3b^6 - 32a^3b^4 - 4ab^{20} - 24ab^{18} - 56ab^{16} - 56ab^{14} + \\ & 56ab^{10} + 56ab^8 + 24ab^6 + 4ab^4 \\ =& 4b^4 \cdot (a^2+2a+b^2+1)^3 \cdot (a^2-2a+b^2+1)^3 \cdot a \cdot (a^2-b^2-1) \cdot (a^2+b^2-1) \end{aligned}$$

Factorizing multivariate polynomials isn't in Julia yet, unfortunately. It can be done in Macaulay2 or WolframAlpha.

Since, $\sigma(f) \in \langle\sigma(I)\rangle$ if and only if $\sigma(r) = 0$, we just need to find values of $a$ and $b$, that set $r$ to zero. By considering the factorization, we have five factors, we can make 0, in

order to get $r$ to be 0. However, neither $a^2 + 2a + b^2 + 1$, $a^2 - 2a + b^2 + 1$ nor $b$ can be 0 by the conditions on the segment. So, we're left with three options.

1. $a = 0$ means that the triangle $ABC$ is isosceles. This immediately gives that $x_3 = -x_2$ and $y_2 = y_3$, which indeed gives us that $|P_1P_2| = |P_1P_3|$.

2. $a^2 + b^2 - 1 = 0$ In this case, the triangle has a right angle in vertex $C$, which implies that $P_2 = P_3 = C$. Hence, $|P_1P_2| = |P_1P_3|$.

3. $a^2 - b^2 - 1 = 0$. This equation traces out a hyperbola, and gives a surprising solution to the problem. Here, the orthic triangle does not sit inside the triangle $ABC$, and the points $P_1, P_2$ and $P_3$ might not be between the vertices. Instead, they lie on the infinite lines described by the vertices. See figure 1b.

We also get that for every other value of $a$ and $b$, we have $\sigma(r) \neq 0$ since $\mathbb{C}$ is an integral domain. Hence $\sigma(f) \notin \langle \sigma(I) \rangle$, meaning that the triangle does not have an isosceles orthic triangle. In this way, we have found nescessary and sufficient conditions for the geometric theorem.

It should be noted, that even though the example of finding an isosceles orthic triangle has been worked through in [9], the method is completely different. In that paper, they computed a Gröbner cover of $I + \langle f \rangle$. While their output is arguably simpler, the method described above has the benefit of being indifferent to the conclusion. In other words, if instead we wanted to ask whether a side of the orthic triangle was parallel to a side of $ABC$, we can do that immediately from $G$ using pseudo-divisions[2]. In the other approach, we would need to recompute the Gröbner system, which may well take a long time for more complex applications. Let us take one more example, to illustrate why this approach works better in the complex plane than the real plane.

**5.6 · Example.** Let $I$ and $G$ be given as before. We want to answer when the area of the orthic triangle is one fifth of the area of the whole triangle. The area of the triangle $ABC$ is $A_{ABC} = b$, and by using Herons formula we find that the area of the orthic triangle is $A_o = \frac{1}{2}(a(y_2 - y_3) + x_2y_3 - x_3y_2)$. By pseudo-reducing $f = 5A_o - A_{ABC}$, we get a pseudo-remainder

$$\begin{aligned} r =& 11a^{12}b^3 + 56a^{10}b^5 - 66a^{10}b^3 + 115a^8b^7 - 188a^8b^5 + 165a^8b^3 + 120a^6b^9 - \\ & 172a^6b^7 + 192a^6b^5 - 220a^6b^3 + 65a^4b^{11} - 48a^4b^9 + 34a^4b^7 - 8a^4b^5 + 165a^4b^3 + \\ & 16a^2b^{13} - 2a^2b^{11} - 8a^2b^9 - 12a^2b^7 - 88a^2b^5 - 66a^2b^3 + b^{15} - 4b^{13} - 15b^{11} + \\ & 35b^7 + 36b^5 + 11b^3 \\ =& b^3(a^2 + b^2 - 2a + 1)^2(a^2 + b^2 + 2a + 1)^2(11a^4 + 12a^2b^2 + b^4 - 22a^2 - 8b^2 + 11) \end{aligned}$$

We see that $\sigma(f) \in \langle \sigma(I) \rangle$ is and only if $\sigma(11a^4 + 12a^2b^2 + b^4 - 22a^2 - 8b^2 + 11) = 0$. In the complex plane, this is fine. The polynomial is quartic in both $a$ and $b$, so for every fixed

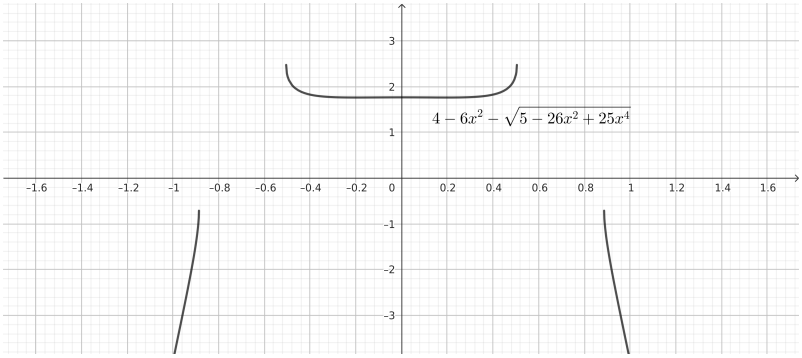
[2]The answer is rather boring: it never happens for a non-degenerate triangle.

$a$-value, we get four solutions for $b$, counted with multiplicity. The real case, however, is not as simple.

Using a CAS system we get the following roots of the polynomial:

$$b = \pm\sqrt{4 - 6a^2 \pm \sqrt{5 - 26a^2 + 25a^4}}$$

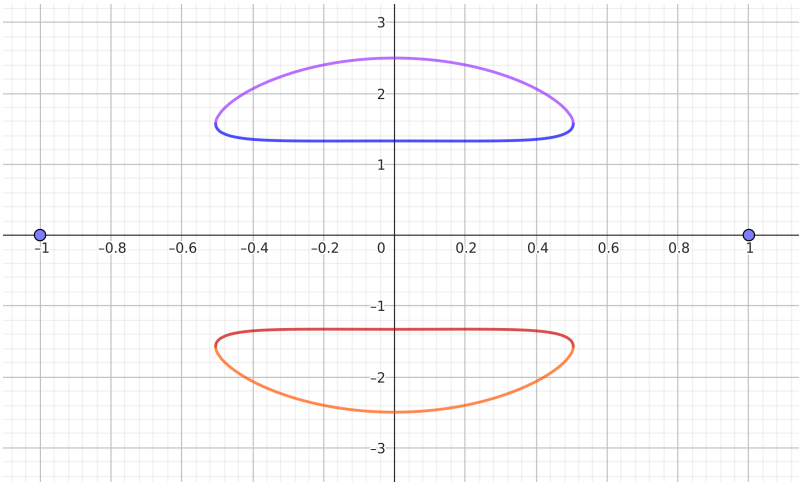
We can plot the inner function:




This shows us, that when $a$ lies between $-0.51$ and $0.51$, the polynomial above has a solution in the real plane. By looking at the other branches of the solution, we see that there is also an isolated solution in $a = 1, b = 0$ corresponding to the degenerate triangle. For other values of $a$ there is no solution over the reals.

We're lucky in this case, as the quartic is solvable in radicals. Had the pseudo-remainder been of fifth degree, we might not be able to say much about the real case. Hence this method of discovering geomtric theorems may not always work in the real plane. It could, however, be a useful first step, as we do get nescesary and sufficient conditions for the theorem to be true. Those conditions just might be difficult to analyse, but more sophisticated tools could use this as a first step.

By doing a bit of manual analysis and plotting parts of the graph seperately, this what the complete set of solutions in the real plane looks like:



## 5.3 Bernds conjecture[3]

In the article [10], Bernd Sturmfels states the following theorem without proof.

**5.7 · Theorem.** *Let $K$ be an algebraically closed field and $F = \{f_1, \dots, f_k\} \subset K[x_1, \dots, x_n]$ a finite set of polynomials. Assume that $\mathbf{V}(F) = \emptyset$ and consider the ideal $I = \langle y_1 - f_1, \dots, y_k - f_k \rangle \subset K[x_1, \dots, x_n, y_1, \dots, y_k]$. Let $G$ be a Gröbner basis of $I$ with respect to the lexicographic order with $x_1 > \cdots > x_n > y_1 > \cdots > y_k$. Then $G$ contains a polynomial $p$ (called a final polynomial) such that*

1. $p(x_1, \dots, x_n, 0, 0, \dots, 0) \in K \setminus \{0\}$
2. $p(x_1, \dots, x_n, f_1, \dots, f_k) = 0$.

He writes that the proof is "straightforward but fairly technical". In a private communication[6] with Sturmfels, he encourages us to write a proof or find a counterexample. He also writes, that the gist of the argument he had in mind was, was using specializations of Gröbner bases. Since since $\{x_1, \dots, x_n\} \gg \{y_1, \dots, y_k\}$, the Gröbner basis of $I$ should behave nicely when we specialize the $y_i$'s to zero. However, as we have seen, Gröbner bases can be most unstable under specializations. Indeed, the following counterexample disproves the theorem.

**5.8 · Example.** Let $F = \{f_1, f_2\}$ where $f_1 = x_1x_2 + 1$ and $f_2 = x_2$. Then, the corresponding ideal $I = \langle y_1 - f_1, y_2 - f_2 \rangle$ has the following reduced Gröbner basis w.r.t. the lexicographic order with $x_1 > x_2 > y_1 > y_2$: $G = \{g_1, g_2\}$ where $g_1 = x_2 - y_2$ and $g_2 = y_2x_1 - y_1 + 1$. Consider now $G' = \{g_1, g_1 - g_2\} = \{x_2 - y_2, y_2x_1 + x_2 - y_1 - y_2 + 1\}$. Clearly $\langle G' \rangle = \langle G \rangle = I$, and it is still a Gröbner basis since $\mathrm{lt}(G') = \mathrm{lt}(G)$. However, letting $\sigma$ be the specialization setting $\sigma(y_1) = \sigma(y_2) = 0$, we see that

$$\sigma(G') = \{x_2, 1 + x_2\}$$

which is not a Gröbner basis. Furthermore, we see that $G'$ does not contain a final polynomial.

While this example is admittedly a bit contrived, the theorem if false, even if we require the reduced Gröbner basis.

**5.9 · Example.** Let $F = \{f_1, f_2, f_3\}$ where $f_1 = x_2 + x_3$, $f_2 = x_2x_3$ and $f_3 = x_1x_3 + 1$. The reduced Gröbner basis of $\langle F \rangle$ is $\{1\}$, so $F$ has no common zeros. The graph ideal of $F$, $I = \langle y_1 - f_1, y_2 - f_2, y_3 - f_3 \rangle$ has the reduced Gröbner basis

$$G = \{x_1y_2 + x_3y_3 - x_3 - y_1y_3 + y_1, x_3^2 - x_3y_1 + y_2, x_2 + x_3 - y_1, x_1x_3 - y_3 + 1\}.$$

When specializing $y_1 = y_2 = y_3 = 0$, $G$ turns into

$$\bar{G} = \{x_3^2, x_2 + x_3, -x_3, x_1x_3 + 1\}$$

[3] Named such by Bernd Sturmfels in a private communication to the supervisor of this project.

which is not a Gröbner basis, and does not contain a constant. Hence, $G$ does not contain a final polynomial.

To fix the theorem, we can turn to parametric Gröbner bases. To shorten notation, let $X = \{x_1, \dots, x_n\}$ and $Y = \{y_1, \dots, y_k\}$.

**5.10 · Theorem.** *Let $K$ be an algebraically closed field and $F = \{f_1, \dots, f_k\} \subset K[X]$ a finite set of polynomials. Assume that $\mathbf{V}(F) = \emptyset$ and consider the ideal $I = \langle y_1 - f_1, \dots, y_k - f_k \rangle \subset K[X, Y]$. Let $G$ be a parametric Gröbner basis of $I$ with respect to the lexicographic order with $x_1 > \cdots > x_n > y_1 > \cdots > y_k$. Then $G$ contains a final polynomial.*

*Proof.* First, notice that every polynomial in $I$ satisfies the second property of final polynomials, since the generators does, and the evaluation map is linear. Thus, we only need to prove that a parametric Gröbner basis contains an element satisfying the first property.

Let $G$ be a parametric Gröbner basis of $I$, and let $\sigma$ be the specialization setting $\sigma(y_i) = 0$ for every $i$. Since $\langle \sigma(I) \rangle = \langle F \rangle = \langle 1 \rangle$, there must be some element $g \in G$ where $\operatorname{lm}(G) \mid 1$, implying that $g$ is a final polynomial. □

However, parametric Gröbner bases can be quite expensive to compute since we need to repeatedly compute Gröbner bases, and furthermore we don't have nice bounds on the degrees. But we only care about one single specialization. This means we don't need a parametric Gröbner basis, we just need a faithful segment of a Gröbner system covering the origin. Here, we can use lemma 3.9. Let $\sigma^1 : K[t, X, Y] \to K[X, Y]$ be the map evaluating $t$ to 1, and let $\sigma^0 : K[t, X, Y] \to K[X, Y]$ be the map evaluating $t$ to 0.

**5.11 · Theorem.** *Let $K$ be an algebraically closed field and $F = \{f_1, \dots, f_k\} \subset K[X]$ a finite set of polynomials. Assume that $\mathbf{V}(F) = \emptyset$ and consider the ideal $I = \langle \hat{F} \rangle$ where $\hat{F} = \{y_1 - f_1, \dots, y_k - f_k\}$. Now, let $G$ be the reduced Gröbner basis of the ideal $\langle t \cdot \hat{F} \cup (1-t) \cdot Y \rangle \subset K[t, X, Y]$ w.r.t. the lexicographic order with $t > X > Y$. Then $\sigma^1(G)$ contains a final polynomial.*

*Proof.* As before, we only need to show that $\sigma^1(G)$ contains a polynomial satisfying the first property of final polynomials. Let $\sigma : K[X, Y] \to K[X]$ be the specialization setting $\sigma(y_i) = 0$ for every $i$ and let $H = \{\operatorname{lc}_Y(g) \mid g \in G, \operatorname{lt}(g) \notin K[X, Y], \operatorname{lc}_{X,Y}(g) \notin \langle Y \rangle\}$. If we have $0 \in \mathbf{V}(Y) \setminus \mathbf{V}(\operatorname{lcm}(H))$, then lemma 3.9, gives us that $\sigma(\sigma^1(G))$ is a Gröbner basis of $\langle \sigma(I) \rangle = \langle F \rangle$. By the Nullstellensatz, $\langle F \rangle = \langle 1 \rangle$, so $\sigma(\sigma^1(G))$ has to contain a constant. This implies, that $\sigma^1(G)$ contains a polynomial $g$, satisfying the first condition of a final polynomial.

Now, we just need that $0 \in \mathbf{V}(Y) \setminus \mathbf{V}(\operatorname{lcm}(H))$. Note that $\mathbf{V}(Y) = \{0\}$, so we just need that $0 \notin \mathbf{V}(\operatorname{lcm}(H))$. By lemma 3.10 we have that $h \notin \langle Y \rangle$ for each $h \in H$. Since $\langle Y \rangle$ is a prime ideal, this implies that $\operatorname{lcm}(H) \notin \langle S \rangle$. Thus $0 \notin \mathbf{V}(\operatorname{lcm}(H))$. □

This counterexample and theorem was developed in colaboration with Peter Lundgaard, and resulted in an article[8]. In that article, it is also proven that it is enough to compute a Gröbner basis of $\langle y_1 - z f_1, \dots, y_k - z f_k \rangle$. However, that proof requires a little more care,

whereas this proof follows directly from the theory of parametric Gröbner bases.

# References


[1] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer, 2015.

[2] Michael Kalkbrener. "On the Stability of Gröbner Bases Under Specializations". In: *Journal of Symbolic Computation* 24.1 (1997), pp. 51–58. ISSN: 0747-7171. DOI: https://doi.org/10.1006/jsco.1997.0113. URL: https://www.sciencedirect.com/science/article/pii/S0747717197901139.

[3] Deepak Kapur, Yao Sun, and Dingkang Wang. "A new algorithm for computing comprehensive Gröbner systems". In: *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*. ISSAC '10. Association for Computing Machinery, 2010, pp. 29–36. ISBN: 9781450301503. DOI: 10.1145/1837934.1837946. URL: https://doi.org/10.1145/1837934.1837946.

[4] Deepak Kapur, Yao Sun, and Dingkang Wang. "An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system". In: *Journal of Symbolic Computation* 49 (2013). The International Symposium on Symbolic and Algebraic Computation, pp. 27–44. ISSN: 0747-7171. DOI: https://doi.org/10.1016/j.jsc.2011.12.015. URL: https://www.sciencedirect.com/science/article/pii/S0747717111002082.

[5] Deepak Kapur, Yao Sun, and Dingkang Wang. "Computing comprehensive Gröbner systems and comprehensive Gröbner bases simultaneously". In: *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*. ISSAC '11. San Jose, California, USA: Association for Computing Machinery, 2011, pp. 193–200. ISBN: 9781450306751. DOI: 10.1145/1993886.1993918. URL: https://doi.org/10.1145/1993886.1993918.

[6] Niels Lauritzen and Bernd Sturmfels. Personal communication. May 6, 2024.

[7] W.W.A.P. Loustaunau. *An Introduction to Grobner Bases*. American Mathematical Soc., 1994. ISBN: 9780821872161. URL: https://books.google.dk/books?id=Caoxi78WaIAC.

[8] Peter Lundgaard and Andreas Bøgh Poulsen. "Gröbner bases and Hilberts Nullstellensatz". unpublished. 2024.

[9] Antonio Montes and Michael Wibmer. "Gröbner bases for polynomial systems with parameters". In: *Journal of Symbolic Computation* 45.12 (2010). MEGA'2009, pp. 1391–1425. ISSN: 0747-7171. DOI: https://doi.org/10.1016/j.jsc.2010.06.017. URL: https://www.sciencedirect.com/science/article/pii/S0747717110000970.

[10] Bernd Sturmfels. "Computational algebraic geometry of projective configurations". In: *Journal of Symbolic Computation* 11.5 (1991), pp. 595–618. ISSN: 0747-7171. DOI: https://doi.org/10.1016/S0747-7171(08)80121-6. URL: https://www.sciencedirect.com/science/article/pii/S0747717108801216.

[11] Akira Suzuki and Yosuke Sato. “A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases”. In: Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC. Association for Computing Machinery (ACM), 2006, pp. 326–331. ISBN: 1595932763. DOI: 10.1145/1145768.1145821.

[12] Ravi Vakil. The Rising Sea – *Foundations of Algebraic Geometry.*

[13] Volker Weispfenning. “Canonical comprehensive Gröbner bases”. In: *Journal of Symbolic Computation* 36.3 (2003). ISSAC 2002, pp. 669–683. ISSN: 0747-7171. DOI: https://doi.org/10.1016/S0747-7171(03)00099-3. URL: https://www.sciencedirect.com/science/article/pii/S0747717103000993.

[14] Volker Weispfenning. “Comprehensive Gröbner bases”. In: *Journal of Symbolic Computation* 14.1 (1992), pp. 1–29. ISSN: 0747-7171. DOI: https://doi.org/10.1016/0747-7171(92)90023-W. URL: https://www.sciencedirect.com/science/article/pii/074771719290023W.

[15] Michael Wibmer. “Gröbner bases for families of affine or projective schemes”. In: *Journal of Symbolic Computation* 42.8 (2007), pp. 803–834. ISSN: 0747-7171. DOI: https://doi.org/10.1016/j.jsc.2007.05.001. URL: https://www.sciencedirect.com/science/article/pii/S0747717107000624.

# A Miscellaneous results

In this section, we prove results that we need in the main text, but don't fit in the flow of the text. These are well-known results, which nevertheless aren't usually covered in introductionary algebra courses. Hence, we present them here.

## A.1 The pseudo-division algorithm

The pseudo-division algorithm is a slight modification of the normal division algorithm.

**A.1 · Theorem.** *Let $f \in A[X]$ and $G = \{g_1, \dots, g_n\} \subset A[X]$. Then there exists $\{h_1, \dots, h_n\} \subset A[X]$, $r \in A[X]$ and $c \in A$ such that*

$$cf = r + \sum_{i=1}^{n} h_i g_i$$

*and the following properties are satisfied:*

1. *$c = \prod_{j \in J} \operatorname{lc}(g_j)^{p_j}$ for some subset $J \subset \{1, 2, \dots, n\}$ and powers $p_j$.*
2. *$\operatorname{lm}(h_i g_i) \leq \operatorname{lm}(f)$ for all $i \in \{1, \dots, n\}$.*
3. *No term of $r$ is divisible by $\operatorname{lm}(g_i)$ for any $i$,*
4. *$\operatorname{coef}(h_i g_i, m) \in \langle \operatorname{coef}(f, m') \mid m' \geq m \rangle$ for all $i \in \{1, \dots, n\}$ and all monomials $m$.*

*Proof.* First, we present the division algorithm to compute such a representation. To start, let $f^0 = f$, $r^0 = 0$, $c^0 = 1$ and $h_1^0 = h_2^0 = \cdots = h_n^0 = 0$. Then we iteratively define the state at step $i$ in terms of the state at step $i - 1$:

- If $f^{i-1} = 0$, we are done. Set $r = r^{i-1}$, set $c = c^{i-1}$ and set $h_j = h_j^{i-1}$ for all $j \in \{1, \dots, n\}$.
- If there is some $g_j \in G$ such that $\operatorname{lm}(g_j) \mid \operatorname{lm}(f^{i-1})$, then find a $\gamma$ such that $\operatorname{lm}(g_j)\gamma = \operatorname{lm}(f^{i-1})$ and set $h_j^i = \operatorname{lc}(g_j)h_j^{i-1} + \operatorname{lc}(f^{i-1})\gamma$, set $f^i = \operatorname{lc}(g_j)f^{i-1} - \operatorname{lc}(f^{i-1})\gamma g_j$, set $r^i = \operatorname{lc}(g_j)r^{i-1}$, and set $h_l^i = \operatorname{lc}(g_j)h_l^{i-1}$ for $l \neq j$.
- If no $g \in G$ satisfies $\operatorname{lt}(g) \mid \operatorname{lt}(f^{i-1})$, then set $r^i = r^{i-1} + \operatorname{lt}(f)$, set $f^i = f^{i-1} - \operatorname{lt}(f^{i-1})$ and set $h_j^i = h_j^{i-1}$ for $j \in \{1, \dots, n\}$.

Since for all $i$, we have $\operatorname{lm}(f^i) < \operatorname{lm}(f^{i-1})$ and $<$ is a well-order, this procedure must terminate eventually. The equality

$$cf = r + \sum_{j=1}^{n} h_j g_j$$

follows from the fact that

$$c^i f - f^i = r^i + \sum_{j=1}^{n} h_j^i g_j$$

at every step $i$ of the algorithm, and when the algorithm terminates $f^i = 0$.

The two first properties of the division are invariants for the algoritm. Since we have $\mathrm{lm}(f^i) \leq \mathrm{lm}(f)$ for all $i$, property (1) follows from the construction of the $h_j$'s. Property (2) is an invariant of $r^i$.

The final property follows from the invariant, that at every step $i$, we have that $\mathrm{coef}(f^i, m) \in \langle \mathrm{coef}(f, m') \mid m' \geq m \rangle$. Indeed, it is true at step $i = 0$. At step $i$, note that when $\mathrm{lt}(g_j)\gamma = \mathrm{lt}(f^i)$, then $\mathrm{coef}(g_j\gamma, m) \in \langle \mathrm{lc}(f^i) \rangle$. Since $\mathrm{lm}(g_j\gamma) \geq m$ for every monomial $m$, that occurs in a term of $f^i$, we get that $\mathrm{coef}(f^i - g_j\gamma) \in \langle \mathrm{coef}(f^i, m') \mid m' \geq m \rangle$. □

## A.2 The nilradical

The nilradical is the ideal of all nilpotent elements of a ring. It is widely used in the study of general rings. In our case, where the base ring is assumed to have no nilpotents, it is zero, but we still need a different characterization of it.

**A.2 · Definition (Nilradical).** Let $A$ be a commutative ring. Then the ideal

$$\sqrt{\langle 0 \rangle} = \{a \in A \mid \exists n \in \mathbb{N} : a^n = 0\}$$

is called the *nilradical*.

**A.3 · Theorem.** *Let $A$ be a commutative, Neotherian ring, and let* $\mathrm{Spec}(A)$ *be the set of prime ideals of $A$. Then*

$$\sqrt{\langle 0 \rangle} = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$$

*Proof.* First, a quick induction proof gives that every nilpotent element is in every $\mathfrak{p} \in \mathrm{Spec}(A)$. Indeed, $0 \in \mathfrak{p}$ and if $a^n = 0 \in \mathfrak{p}$, then either $a$ or $a^{n-1}$ is in $p$, since $\mathfrak{p}$ is prime. By induction, $a \in \mathfrak{p}$.

For the converse inclusion, we apply Zorns lemma. Let $f \in A \setminus \sqrt{\langle 0 \rangle}$, then we need to find a prime ideal that does not contain $f$. Let $S$ be the set of ideals in $A$ not containing any power of $f$. $S$ is non-empty, since $\langle 0 \rangle \in S$, and each chain of ideals in $S$ stabilizes since $A$ is Noetherian. Hence, Zorns lemma applies, and gives us a maximal element $\mathfrak{m} \in S$. To finish the proof, we just need that $\mathfrak{m}$ is a prime ideal. Let $g, h \notin \mathfrak{m}$, then we show that $gh \notin \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, we must have $\mathfrak{m} + \langle g \rangle \notin S$ and $\mathfrak{m} + \langle h \rangle \notin S$. Hence, we can find $m, n$ such that $f^n \in \mathfrak{m} + \langle g \rangle$ and $f^m \in \mathfrak{m} + \langle h \rangle$. Now, if $gh \in \mathfrak{m}$, then $\mathfrak{m} + \langle gh \rangle = \mathfrak{m}$, and hence $f^{n+m} = f^n f^m \in (\mathfrak{m} + \langle g \rangle)(\mathfrak{m} + \langle h \rangle) = \mathfrak{m} + \langle gh \rangle = \mathfrak{m}$, meaning $m \notin S$. This is a contradiction, so $gh \notin \mathfrak{m}$. □

## A.3 Homogenous ideals

Here, we present a basic lemma about homogenous ideals.

**A.4 · Lemma.** *Let $I \subset A[X]$ be a homogenous ideal and let $f \in I$. Writing*

$$f = \sum_i f_i$$

*where each $f_i$ is homogenous, each $f_i \in I$.*

*Proof.* Let $\{g_1, \dots, g_n\} \subset I$ be a finite set of homogenous generators of $I$, and let $f \in I$. Then we can write

$$f = \sum_{i=0}^{n} h_i g_i$$

for some $h_i \in A[X]$. Consider a single term of this sum, which we can write as

$$h_i g_i = \sum_j a_{i,j} X^{\nu_{i,j}} g_i, \quad \text{where } h_i = \sum_j a_{i.j} X^{\nu_{i,j}}.$$

Each term of this sum is homogenous and $a_{i,j} X^{\nu_{i,j}} g_i \in I$. Since

$$f = \sum_{i,j} a_{i,j} X^{\nu_{i,j}} g_i$$

is a sum of homogenous polynomials, and each term of the sum is homogenous and in $I$, each homogenous component of $f$ is in $I$. □