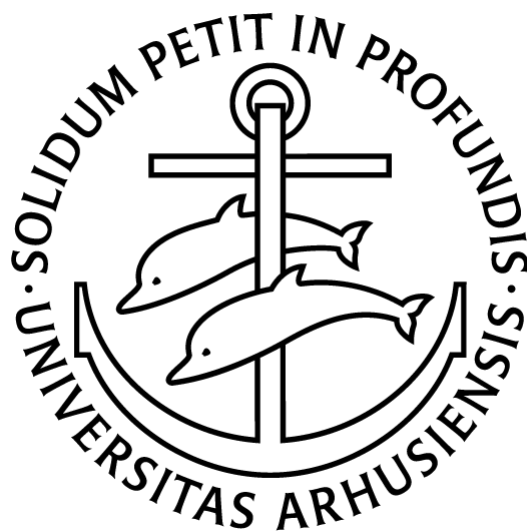


# Parametric Gröbner bases

## GEOMETRY & APPLICATIONS

*Andreas Bøgh Poulsen*

201805425



Supervisor: Niels Lauritzen



# Contents

<b>1</b>	<b>Preliminaries</b>	<b>1</b>
<b>2</b>	<b>Definitions and initial results</b>	<b>2</b>
2.1	A criterion on stability . . . . .	4
2.2	Pseudo-division . . . . .	7
<b>3</b>	<b>Computing Gröbner systems</b>	<b>8</b>
3.1	Parametric Gröbner bases . . . . .	9
3.2	Computing faithful segments . . . . .	10
<b>4</b>	<b>Geometric description &amp; Gröbner covers</b>	<b>13</b>
4.1	Parametric sets . . . . .	16
4.2	Monic ideals and the reduced Gröbner basis of $\mathcal{I}_S$ . . . . .	17
4.3	An aside on flatness . . . . .	20
4.4	The singular ideal . . . . .	20
4.5	The projective case . . . . .	23
4.6	Relation to the <b>CGS</b> algorithm . . . . .	25
<b>5</b>	<b>Applications</b>	<b>27</b>
5.1	Quantifier elimination . . . . .	27
5.2	Bernds conjecture . . . . .	28
<b>A</b>	<b>Miscellaneous results</b>	<b>31</b>
A.1	Reduced Gröbner bases . . . . .	31
A.2	Pseudo-division . . . . .	31
A.3	The nilradical . . . . .	31
A.4	Homogenous ideals . . . . .	31

# Introduction

## 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 symbols. 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  $X^v$  for some  $v \in \mathbb{N}^n$ . For a polynomial

$$f = \sum_{v \in \mathbb{N}^n} a_v X^v$$

we denote the coefficient of the term  $t = a_v X^v$  by  $\text{coef}(f, X^v)$ .

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

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  $\text{lt}_<(f)$ . If  $\text{lt}_<(f) = a \cdot m$  for some monomial  $m$  and  $a \in A$ , then we denote  $\text{lm}_<(f) = m$  and  $\text{lc}_<(f) = a$ . If  $<$  is clear from context, it will be omitted.

<sup>a</sup>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  $\text{lm}_<(F) := \{\text{lm}_<(f) \mid f \in F\}$ . When  $I \subset A[X]$  is an ideal, we use  $\text{lm}_<(I)$  to denote  $\langle \text{lm}_<(I) \rangle$  to ease notation, and similarly for  $\text{lt}_<(I)$ . With this, we can give the definition of a Gröbner basis.

**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  $\text{lt}_<(G) = \text{lt}_<(\langle G \rangle)$ .

Note, that if  $A$  is a field, then it is enough that  $\text{lm}_<(G) = \text{lm}_<(\langle G \rangle)$ . 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 have to use an alternative description of Gröbner bases.

**1.3 · Definition (Reduction modulo).** Let  $f, g \in A[X]$  be polynomials and  $<$  be a term order. We say  $f$  *reduces modulo*  $g$  if  $\text{lt}(g) \mid \text{lt}(f)$ , since in that case  $\text{lt}(\text{lc}(g) \cdot f - p \cdot \text{lc}(f) \cdot g) < \text{lt}(f)$  where  $\text{lm}(f) = p \cdot \text{lm}(g)$ . We say a polynomial reduces modulo a set of polynomials if it reduces modulo any polynomial in the set. We say a polynomial *reduces to zero* 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.  $\text{lc}(g) = 1$ ) and the only term of  $g$  in  $\text{lt}(\langle G \rangle)$  is  $\text{lt}(g)$ .

**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 coefficient.

## 2 Definitions and initial results

The purpose of this project is to study parametric Gröbner bases, so let's introduce those. The bare concept is rather simple.

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

Most of this text will focus on the special case when  $k$  is another field,  $U$  is another set of variables with  $U \cap X = \emptyset$  and  $A = k[U]$ . Then  $\sigma : k[U] \rightarrow k_1$  corresponds to a choice of value for each variable in  $U$ .

We call such a  $\sigma : k[U] \rightarrow k_1$  a *specialization*. By the linearity of  $\sigma$ , all such ring homomorphisms can be characterized by their image of  $U$ . Thus, we can identify  $\{\sigma : k[U] \rightarrow k_1 \mid \sigma \text{ is a ring hom.}\}$  with the affine space  $k_1^m$  when  $U$  has  $m$  elements. For  $\alpha \in k_1^m$  we'll denote the corresponding map

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

extended linearly.

**2.2 · Example.** Consider the ideal  $I = \langle ux - 1, vx - 1 \rangle \subset \mathbb{C}[u, v][x, y]$  and a specialization  $\sigma : \mathbb{C}[u, v] \rightarrow \mathbb{C}$ . To analyze the behaviour of  $I$  under different specializations, let's split into cases.

1. If either  $\sigma(u) = 0$  or  $\sigma(v) = 0$ , then  $\langle \sigma(I) \rangle = \langle 1 \rangle \subset \mathbb{C}[x, y]$ . If  $\sigma(u) = 0$ , then

$\sigma(ux - 1) = -1$ , hence the generators above form a Gröbner basis of  $\langle I \rangle$ . The other polynomial becomes redundant, so we don't have a reduced Gröbner basis.

2. If  $\sigma(u) = \sigma(v)$ , then  $\langle \sigma(I) \rangle = \langle \sigma(u)x - 1 \rangle$ . In this case the generators also form a Gröbner basis.
3. If  $\sigma(u) \neq \sigma(v)$  and neither of them are 0, then  $\sigma(v)(\sigma(u)x - 1) - \sigma(u)(\sigma(v)x - 1) = \sigma(v) - \sigma(u) \in \langle \sigma(I) \rangle$ , hence  $\langle \sigma(I) \rangle = \langle 1 \rangle$ . In this case the generators do not form a Gröbner basis of  $\langle \sigma(I) \rangle$ .

The reduced Gröbner basis of  $I$  is  $\{u - v, ux - 1\}$ , which always specializes to a Gröbner basis, as can be seen above. However, it is not always enough to compute a reduced Gröbner basis.

Consider the ideal  $J = \langle ux^2 + y, y^2 + 1 \rangle$ , where the generators form the reduced Gröbner basis of  $J$ . And indeed, whenever  $\sigma(u) \neq 0$ , it specializes to the reduced Gröbner basis of  $\langle \sigma(J) \rangle$ . However, when  $\sigma(u) = 0$ , we get  $\langle \sigma(J) \rangle = \langle 1 \rangle$ , but  $\sigma(\{ux^2 + y, y^2 + 1\}) = \{y, y^2 + 1\}$ , which is not a Gröbner basis.

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 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  $E \subset k[X]$ . Then the *vanishing set* of  $E$  is  $V(E) := \{v \in k^n \mid e(v) = 0 \ \forall e \in E\}$ .

A *locally closed set* is a set of the form  $V(E) \setminus V(N)$  for two subsets  $E$  and  $N$  of  $k[X]$ .

**2.4 · Definition (Gröbner system).** Let  $A$  be a locally closed set and  $F, G \subset k[X, U]$  be finite sets. Then  $(A, G)$  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  $\alpha \in A$ . A set  $\{(A_1, G_1), \dots, (A_t, G_t)\}$  is called a *Gröbner system* if each  $(A_i, G_i)$  is a segment of a Gröbner system.

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

A Gröbner system  $\{(A_1, G_1), \dots, (A_t, G_t)\}$  is called *comprehensive*, if  $\bigcup_{i=1}^t A_i = k_1^{|U|}$ . We also say a Gröbner system is *comprehensive on  $L \subset k_1^{|U|}$*  if  $\bigcup_{i=1}^t A_i = L$ .

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.

**2.5 · Example.** Consider again the ideal  $J = \langle ux^2 + y, y^2 + 1 \rangle \subset \mathbb{C}[u][x, y]$ . We saw in the last example that the given generators form a Gröbner basis under any specialization

where  $\sigma(u) \neq 0$ . Hence, we have the following Gröbner system:

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

Note, that  $-y(ux^2 + y) + (y^2 + 1) = -ux^2y + 1 \in J$  specializes to 1 when  $\sigma(u) = 0$ . Hence we also have the following Gröbner system, which is also a parametric Gröbner basis:

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

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

Note that  $\text{lc}_U(f) \in k[U]$ , i.e. the leading term is a polynomial in  $k[U]$  times a monomial in  $X$ .

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  $v_2 \in \mathbb{N}^{|U|}$ . 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  $k[U]$ .

## 2.1 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 [1].

**2.7 · Lemma.** Let  $G$  be a Gröbner basis of an ideal  $\langle F \rangle \subset A[X]$  w.r.t.  $<$ , let  $\sigma : A \rightarrow K$  be a ring homomorphism to a field  $K$  and set  $G_\sigma = \{g \in G \mid \sigma(\text{lc}(g)) \neq 0\} = \{g_1, g_2, \dots, g_l\} \subset A[X]$ . 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 “ $\implies$ ”: 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 “ $\impliedby$ ”: 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

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

Indeed, since  $G$  is a Gröbner basis of  $\langle F \rangle$ , that implies there is some  $g \in G$  such that  $\text{lm}(g) \mid \text{lm}(h)$  and  $\text{lm}(h) = \text{lm}(\sigma(h)) \mid \text{lm}(\sigma(f))$ . Furthermore, since  $\text{lc}(g) \mid \text{lc}(h)$ , we have

that  $\sigma(\text{lc}(g)) \neq 0$ , hence  $\text{lt}(\sigma(g)) \mid \text{lt}(\sigma(f))$ . 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  $\text{lm}(f) = 1$ , which means  $f \in A$ . Since we assumed  $\sigma(f) \neq 0$ , we have  $\text{lm}(\sigma(f)) = \text{lm}(f)$  and  $\sigma(\text{lc}(f)) \neq 0$ .

Now, the induction step. Let  $f \in \langle F \rangle$  with  $\sigma(\text{lc}(f)) \neq 0$  and assume that every  $f' \in \langle F \rangle$  with  $\text{lm}(f') < \text{lm}(f)$  we have  $\exists h \in \langle F \rangle : \sigma(\text{lc}(h)) \neq 0 \wedge \text{lm}(h) \mid \text{lm}(\sigma(f'))$ . If  $\sigma(\text{lc}(f)) \neq 0$ , we can simply use  $h = f$ , so consider the case when  $\sigma(\text{lc}(f)) = 0$ . If there is some  $\sigma(g) \in G_\sigma$  such that  $\text{lm}(g) \mid \text{lm}(f)$ , then we can reduce  $f$  by  $g$  to get  $f' = \text{lc}(g) \cdot f - \text{lc}(f) \cdot \frac{\text{lm}(f)}{\text{lm}(g)} g$ . Then  $\text{lm}(\sigma(f')) = \text{lm}(\sigma(f))$  since  $\sigma(\text{lc}(f)) = 0$  and  $\text{lm}(f') < \text{lm}(f)$ , 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  $\text{lm}(g) \mid \text{lm}(f)$ . However, we can't simply reduce by  $g$ , since the factor  $\text{lc}(g)$  is zero under  $\sigma$ . Instead, we can find a subset  $\{g_{j_1}, \dots, g_{j_r}\} \subset G \setminus G_\sigma$  such that

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

Since each of the  $\sigma(g_{j_i})$  are reducible to 0 modulo  $G_\sigma$ , 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  $\text{lm}(\sigma(h_i)) = \text{lm}(\sigma(g_{j_i})) > \text{lm}(g_{j_i})$  for each  $i \in \{1, \dots, r\}$ . Let  $b = \prod_{i=1}^r b_i$ , which is non-zero, then

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

is a new polynomial with

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

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

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

**2.8 • 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  $\alpha \in k_1^m$ . If  $\sigma_\alpha(\text{lc}_U(g)) \neq 0$  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  $\langle F \rangle \subset k[U][X]$ . Let  $G_\alpha = \{\sigma_\alpha(g) \mid \sigma_\alpha(\text{lc}_U(g)) \neq 0\}$ . 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  $\sigma_\alpha(\text{lc}_U(g)) \neq 0$  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.

If there is no such  $g$ , then  $\alpha \in V(G \cap k[U])$ . Take any  $g \in G$ . If  $\sigma_\alpha(g) \in G_\alpha$ , then  $\text{lt}(\sigma_\alpha(g)) = a \cdot \text{lm}_U(g)$  for some  $a \in k_1$  since  $X^{v_1} > U^{v_2}$ . Thus the monomial of its leading

term is preserved by  $\sigma_\alpha$ , so  $\sigma_\alpha(g)$  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  $\alpha \in V(G \cap k[U])$  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 2.7.  $\square$

Let's see how this can be used to produce a Gröbner system. The idea is to compute a Gröbner basis and find the leading coefficients. Then that Gröbner basis gives a segment of a Gröbner system where none of the leading coefficients specialize to zero. Then, we walk through the leading coefficients, and specialize each one away. Then we compute a Gröbner basis for that case, and see what the leading coefficients are. We do this iteratively, until there are no more leading coefficients.

**2.9 • 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.

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

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  $\sigma(ad - bc) = \sigma(a) = 0$ ,

## 2.2 Pseudo-division

In the classical setting when we have acquired a Gröbner basis, we can use the multivariate division algorithm<sup>1</sup>. However, in the parametric case, this is more tricky. Consider for example the set  $\{ux - 1, vx - 1\}$ . Each polynomial is irreducible modulo the other, but for any specialization where  $u \neq 0 \neq v$ , we can reduce both polynomials modulo the other. To handle this in the parametric setting, we introduce pseudo-division.

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

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

**2.11 · 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.2 □

Pseudo-division turns out to be “the right kind of division” when working with parameterized ideals. 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.

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

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

<sup>1</sup>The multivariate division algorithm simply reduces a polynomial  $f$  modulo a set of polynomials. If  $f$  is irreducible, record  $\text{lt}(f)$  in a remainder and reduce  $f - \text{lt}(f)$ .

be a pseudo-division. Then

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

satisfies  $\text{lm}(\sigma(f_i g_i)) \leq \text{lm}(\sigma(f))$ . Furthermore, if  $\sigma(\text{lc}(g_i)) \neq 0$  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 from linearity of  $\sigma$ . For the inequality  $\text{lm}(\sigma(f_i g_i)) \leq \text{lm}(\sigma(f))$ , we have the fourth condition from pseudo-divisions:  $\text{coef}(f_i, m) \in \langle \text{coef}(f, m') \mid m' \geq m \text{lm}(g_i) \rangle$ . Hence for any monomial  $m$  with  $m \text{lm}(g_i) \geq \text{lm}(\sigma(f))$ , we have  $\sigma(\text{coef}(f_i, m)) = 0$ .

For the remainder, we have from pseudo-division that no term of  $r$  is divisible by any  $\text{lt}(g_i)$ . Assuming  $\sigma(\text{lc}(g_i)) \neq 0$  for all  $i$ , we have  $\text{lm}(g_i) = \text{lm}(\sigma(g_i))$  for all  $i$ . Hence, no term of  $\sigma(r)$  is divisible by any  $\text{lm}(\sigma(g_i))$ , and since we work over a field, no term of  $\sigma(r)$  is divisible by any  $\text{lt}(\sigma(g_i))$ .  $\square$

### 3 Computing Gröbner systems

With lemma 2.8 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  $H = \{\text{lc}_U(g) \mid g \in G \setminus k[U]\}$ . Then  $(k_1^m \setminus \bigcup_{h \in H} V(h), G)$  is a segment of a Gröbner system. Thus, to make a Gröbner system, we need to find segments covering  $\bigcup_{h \in H} V(h) = V(\text{lcm}(H))$ .

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  $H_1 = \{\text{lc}_U(g) \mid g \in G_1\}$ . 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.

**3.1 • Theorem.** *Let  $F \subset k[X, U]$  and  $S \subset k[U]$  be finite sets of polynomials. Then  $\text{CGS}_{\text{simple}}(F, S)$  terminates and the output  $\mathcal{H}$  is a comprehensive Gröbner system on  $V(S)$ .*

*Proof.* First, we prove termination. Let  $F$  and  $S$  be inputs to  $\text{CGS}_{\text{simple}}$ , let  $G$  be the reduced Gröbner basis of  $F \cup S$  and let  $H = \{\text{lc}_U(g) \mid g \in G \setminus k[U]\}$ . Take any  $h \in H$ . Since  $G$  is reduced,  $h \notin \langle F \cup S \rangle$ , since then its leading term would be divisible by an element in  $G$ , but that cannot be the case. Indeed, since  $h \in k[U]$ , it cannot be reduced by any  $g \in G \setminus k[U]$  (as  $X^{v_1} > U^2$ , so the leading terms of  $G \setminus k[U]$  must contain a variable from  $X$ ), and if it was reducible by a  $p \in G \cap k[U]$ , then that  $p$  would also reduce one of the elements of  $G \setminus k[U]$ , which is not allowed when  $G$  is reduced. Thus  $\langle F \cup S \rangle \subsetneq \langle F \cup S \cup \{h\} \rangle$ . Since this is the case at every recursive call, each successive call to  $\text{CGS}_{\text{simple}}$  will have a strictly greater ideal  $\langle F \cup S \rangle$ . Since  $k[X, U]$  is Noetherian, this must stop eventually. Note also, that since  $F$  stays constant, this means that  $\langle S \rangle \subsetneq \langle S \cup \{h\} \rangle$ .

---

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

---

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  $V(S)$ .

```

if  $\exists g \in S \cap (k \setminus \{0\})$  then
  | return  $\emptyset$ ;
else
  |  $G \leftarrow \text{groebner}(F \cup S)$ ;
  |  $H \leftarrow \{\text{lc}_U(g) \mid g \in G \setminus k[U]\}$ ;
  |  $h \leftarrow \text{lcm}(H)$ ;
  | return  $\{(S, \{h\}, G)\} \cup \bigcup_{h' \in H} \text{CGS}_{\text{simple}}(G \cup \{h'\}, S \cup \{h'\})$ 
end

```

---

Next, we prove that if  $(E, N, G) \in \mathcal{H}$ , then  $(V(E) \setminus V(N), G)$  is a segment of a Gröbner system. By the algorithm,  $N = \text{lcm}(H)$ , where  $H = \{\text{lc}_U(g) \mid g \in G \setminus k[U]\}$  as before, for  $G$  being the reduced Gröbner basis of  $\langle F \cup S \rangle$ . Hence, for any  $\alpha \in V(E) \setminus V(N)$ , we have that  $\sigma_\alpha(\text{lc}_U(g)) \neq 0$  for every  $g \in G \setminus k[U]$ . Thus  $\sigma_\alpha(G)$  is a Gröbner basis of  $\langle \sigma_\alpha(F \cup S) \rangle$  by lemma 2.8. Also,  $E = S$ , so  $\sigma_\alpha(S) = 0$ . Hence  $\langle \sigma_\alpha(F \cup S) \rangle = \langle \sigma_\alpha(F) \rangle$ , so  $\sigma_\alpha(G)$  is a Gröbner basis of  $\langle \sigma_\alpha(F) \rangle$ .

Finally, we need to prove that

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

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

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

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

Note that in the implementation, we use  $G \setminus S$  instead of  $G$  for the Gröbner segments. This has no impact on the validity of the segments, it just removes elements, which would specialize to 0 on that segment anyway.

### 3.1 Parametric Gröbner bases

We now move on to the problem of computing parametric Gröbner bases, which is the problem which Weispfenning tackled in his original article [5]. Recall the definition of parametric Gröbner bases from definition 2.1

**3.2 · 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  $i$ .

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

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

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.

## 3.2 Computing faithful segments

We follow the path laid out by [3], and introduce 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 separate 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 this need not be an ideal.

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

**3.4 · 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  $f_1, \dots, f_n \in F$ ,  $s_1, \dots, s_m \in S$  and  $q_1, \dots, q_n, p_1, \dots, p_m \in k[t, X, U]$  such that

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

By linearity of the evaluation map, 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

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

$\square$

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.

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

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

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

*Proof.* First note, that  $\text{lt}(g) \notin k[X, U]$  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. For any polynomial  $g \in G$  we can therefore write  $g = t \cdot g^t + g_t$  where  $g_t = \sigma^0(g)$  and  $g^t = \sigma^1(g) - \sigma^0(g)$ .

Let  $\alpha \in V(S) \setminus V(\text{lcm}(H))$ . By lemma 3.4 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  $G' = \{g \in G \mid \text{lt}(g) \notin k[X, U], \text{lc}_{X,U}(g) \notin k[U]\}$ . Then  $\sigma_\alpha(\text{lc}_U(g)) \neq 0$  for any  $g \in G'$  since  $\alpha \notin V(\text{lcm}(H))$ . 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 2.8 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  $k_1[X]$ . For any  $g \in G'$  we have that  $\sigma_\alpha(g) = \sigma_\alpha(t \cdot g^t) + \sigma_\alpha(g_t)$ . Since  $g_t = \sigma^0(g) \in \langle S \rangle$  by lemma 3.4 and  $\alpha \in V(S)$ , we have that  $\sigma_\alpha(g_t) = 0$ , thus  $\sigma_\alpha(g) = \sigma_\alpha(t \cdot g^t)$ . 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 that ideal, 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  $\text{lt}(g) \in k[X, U]$  or  $\text{lc}_{X,U}(g) \in k[U]$ . 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 3.4. Since  $\alpha \in V(S)$ ,  $\sigma_\alpha(g) = 0$ . On the other hand, if  $\text{lt}(g) \notin k[X, U]$  but  $\text{lc}_{X,U}(g) \in k[U]$ , we note that  $g^t = \text{lc}_{X,U}(g)$ . Since  $g^t = \sigma^1(g) - \sigma^0(g)$ , we get from lemma 3.4 that  $g^t \in \langle F \rangle + \langle S \rangle = \langle F \cup S \rangle$ . Since we also had  $g^t \in k[U]$ , we have  $g^t \in \langle F \cup S \rangle \cap k[U]$ . But by assumption  $V(S) \subset V(\langle F \rangle \cap k[U])$ , thus  $\alpha \in V(S) \cap V(\langle F \rangle \cap k[U]) = V(\langle F \cup S \rangle \cap k[U])$ . Hence,  $\sigma_\alpha(g^t) = 0$ . But we proved earlier that for any  $g \in G$  we have  $\sigma_\alpha(g_t) = 0$ , so as  $\sigma_\alpha(g) = t \cdot \sigma_\alpha(g^t) + \sigma_\alpha(g_t) = 0$ , we are done.  $\square$

This lemma is a generalization of lemma 2.8, and as such, it leads us to an algorithm for computing comprehensive, faithful Gröbner systems, at least 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  $V(S) \setminus V(\text{lcm}(H))$ , where  $H = \{\text{lc}_U(g) \mid g \in G, \text{lt}(g) \notin k[X, U], \text{lc}_{X,U}(g) \notin k[U]\}$ . Then, we recursively compute faithful Gröbner segments on

each  $V(h)$  for  $h \in H$ , by adding  $h$  to  $S$ .

---

**Algorithm 2:  $\mathbf{CGB}_{\text{aux}}$**

---

INPUT:  $F \subset k[X, U]$  and  $S \subset k[U]$ , two finite sets such that  $V(S) \subset V(\langle F \rangle \cap k[U])$

OUTPUT: A finite set of triples  $(E, N, G)$  forming a comprehensive, faithful Gröbner system on  $V(S)$

**if**  $1 \in \langle S \rangle$  **then**

**return**  $\emptyset$ ;

**else**

$G \leftarrow \text{groebner}(t \cdot F \cup (1 - t) \cdot S)$ ;

$H \leftarrow \{\text{lc}_U(g) \mid g \in G, \text{lt}(g) \notin k[X, U], \text{lc}_{X,U}(g) \notin k[U]\}$ ;

$h \leftarrow \text{lcm}(H)$ ;

**return**  $\{(S, \{h\}, \sigma^1(G))\} \cup \bigcup_{h' \in H} \mathbf{CGB}_{\text{aux}}(F, S \cup \{h'\})$ ;

**end**

---

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

*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  $h \in \{\text{lc}_U(g) \mid g \in G, \text{lt}(g) \notin k[X, U], \text{lc}_{X,U}(g) \notin k[U]\}$ . Let  $g \in G$  be the element such that  $\text{lc}_U(g) = h$ . By assumption,  $g$  is of the form  $h \cdot t \cdot X^v + g'$  for some vector  $v$  and  $g' \in k[X, U]$ . If  $g \in \langle S \rangle$ , then  $(1 - t) \cdot h \in \langle G \rangle$ , by the construction of  $G$ . This means that  $\text{lt}((1 - t) \cdot h) = \text{lt}(t \cdot h)$  is divisible by some leading term of  $G$ , and since the leading term of  $g$  doesn't divide it,  $\text{lt}(t \cdot h)$  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. Thus  $\langle S \rangle \subsetneq \langle S \cup \{h\} \rangle$ . Since  $k[t, X, U]$  is Noetherian, we can only expand this ideal finitely many times. Thus the algorithm terminates.

Next, observe that the precondition  $V(S) \subset V(\langle F \rangle \cap k[U])$  always hold if it held initially, as  $V(S') \subset V(S)$  for any  $S' \supset S$ . Apply this to  $S' = S \cup \{h\}$ .

If  $(S, \{h\}, G)$  is in the output of  $\mathbf{CGB}_{\text{aux}}(F, S)$ , then  $(V(S) \setminus V(h), G)$  is a segment of a Gröbner system by lemma 3.5. It is also faithful by lemma 3.4.

Finally, we need to show that  $V(S) = \bigcup_{E, N, G \in \mathbf{CGB}_{\text{aux}}(F, S)} V(E) \setminus V(N)$ . Let  $H = \{\text{lc}_U(g) \mid g \in G, \text{lt}(g) \notin k[X, U], \text{lc}_{X,U}(g) \notin k[U]\}$  and  $h = \text{lcm}(H)$ . Then

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

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

The only thing left is to figure out what to do with that  $V(S)$ . With the **CGS** algorithm we could choose  $S = \emptyset$ , then  $V(S) = k_1^{[U]}$ , but that doesn't work here, as it violates the assumption that  $V(S) \subset V(\langle F \rangle \cap k[U])$ . However, we can choose  $S$  to be a set of generators of the ideal  $\langle F \rangle \cap k[U]$ . Then  $S \subset \langle F \rangle$  and  $\langle \sigma_\alpha(S) \rangle$  is either zero or  $k_1[X]$ , depending whether  $\alpha \in V(S)$  or not. Hence,  $(k^{[U]} \setminus V(S), S)$  is a faithful segment of a Gröbner system.

---

**Algorithm 3: CGB**

---

INPUT:  $F \subset k[X, U]$  a finite set of polynomials  
 OUTPUT:  $G \subset k[U, X]$  a comprehensive Gröbner basis of  $F$   
 $S \leftarrow \mathbf{groebner}(F) \cap k[U]$ ;  
 $\mathcal{H} \leftarrow \mathbf{CGB}_{\mathbf{aux}}(F, S)$ ;  
**return**  $S \cup \bigcup_{(E, N, G) \in \mathcal{H}} G$ ;

---

**3.7 · 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. Since  $S$  is a set of generator of the ideal  $\langle F \rangle \cap k[U]$ , we have that  $V(S) = V(\langle F \rangle \cap k[U])$ , so by theorem 3.6,  $\mathcal{H}$  is a faithful, comprehensive Gröbner system on  $V(S)$ . Since  $\langle \sigma_\alpha(S) \rangle$  is either 0 or  $k_1[X]$ ,  $(k^{[U]} \setminus V(S), S)$  is a segment of a faithful, comprehensive Gröbner system. Hence

$$\{(V(\emptyset) \setminus V(S), S)\} \cup \mathcal{H}$$

is a faithful, comprehensive Gröbner system for  $\langle F \rangle$ . By corollary 3.3 we get that  $S \cup \bigcup_{(E, N, G) \in \mathcal{H}} G$  is a parametric Gröbner basis for  $\langle F \rangle$ .  $\square$

## 4 Geometric description & Gröbner covers

In this section, we develop a geometric description of Gröbner systems. We follow the development of [6] quite closely, albeit with a slightly different focus. The description makes heavy use of terms from modern algebraic geometry, specifically the language of sheaves. However, in section 4.6, 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 unique 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  $\text{Spec}(A)$ ). Given a prime ideal  $\mathfrak{p} \in \text{Spec}(A)$ , let  $A_{\mathfrak{p}}$  denote the localization of  $A$  by  $\mathfrak{p}$ , 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  $A \rightarrow A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$  given by  $a \mapsto \frac{a}{1} + \mathfrak{p}_{\mathfrak{p}}$ . The specialization  $\sigma_{\mathfrak{p}} : A[X] \rightarrow k(\mathfrak{p})[X]$  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  $U \subset \text{Spec}(A)$ , there is a ring of regular functions on  $U$ . Let  $\mathfrak{a} = \mathbf{I}(\overline{U})$ , then a regular function  $f$  is a function from  $U$  to  $\prod_{\mathfrak{p} \in U} (A/\mathfrak{a})_{\mathfrak{p}}$  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  $\text{Spec}(\mathbb{C}[a, b, c, d])$ , we can identify  $\mathbf{V}(ad - bc)$  with  $\text{Spec}(\mathbb{C}[a, b, c, d]/\langle ad - bc \rangle)$ , so we can equivalently see  $f$  as a regular function on  $\text{Spec}(\mathbb{C}[a, b, c, d]/\langle ad - bc \rangle) \setminus \mathbf{V}(\langle a, b \rangle)$ . This means, for any prime ideal  $\mathfrak{p} \in \text{Spec}(\mathbb{C}[a, b, c, d]/\langle ad - bc \rangle)$  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  $\rho_{\mathfrak{p}} : \mathcal{O}_Y(U) \rightarrow (A/\mathfrak{a})_{\mathfrak{p}}/(\mathfrak{p}/\mathfrak{a})_{\mathfrak{p}}$  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  $(\forall \mathfrak{p} \in Y \cap U : \rho_{\mathfrak{p}}(f) = 0) \implies f = 0$ , so assume  $f(\mathfrak{p}) \in (\mathfrak{p}/\mathfrak{a})_{\mathfrak{p}}$  for any  $\mathfrak{p} \in Y \cap U$ . Then  $f \in \bigcap_{\mathfrak{p} \in \text{Spec}(A/\mathfrak{a})} \mathfrak{p} = \sqrt{\langle 0 \rangle} \subset A/\mathfrak{a}$ , 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.  $\square$

Given a locally closed set  $S = Y \cap U \subset \text{Spec}(A)$  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  $\mathcal{J}_S$  or  $\mathcal{J}_Y(U)$ , and is given by functions  $f$ , which can be described locally as fractions  $f(\mathfrak{p}) = \frac{p}{q}$  where  $p \in \bar{I}$  and  $q \in (A/\mathfrak{a}) \setminus \mathfrak{p}$ . In this light, we can also see  $\mathcal{J}_S$  as an ideal in the polynomial ring  $\mathcal{O}_S[X]$ , which is how we'll use it most of the time.

In an abuse of notation, for a  $\mathfrak{p} \in \text{Spec}(A/\mathfrak{a})$ , we denote the map  $\mathcal{J}_S \rightarrow k(\mathfrak{p}) = (A/\mathfrak{a})_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$  given by mapping  $\frac{p}{q} \in \mathcal{J}_S$  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  $\text{Spec}(k[U])$  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  $\mathfrak{p} \supset \langle b \rangle$ .

Consider now the polynomial  $P = x + f \cdot y \in \mathcal{O}_Y(U)[x, y]$ , and let  $\mathfrak{m} \in \text{Spec}(\mathbb{C}[a, b, c, d]/\mathbf{V}(ad - bc))$  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  $\langle a - m_1, b - m_2, c - m_3, d - m_4 \rangle$  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  $f(\mathfrak{m}) = x + \frac{d}{b}y$  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  $m_1, \dots, m_4$ ,  $\sigma_{\mathfrak{m}}(P)$  is indeed the reduced Gröbner basis of  $\sigma_{\mathfrak{m}}(I) \subset \mathbb{C}[x, y]$ . Lastly, 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  $P \in \mathcal{J}_Y(U)$ .

## 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 maximal 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  $S \subset \text{Spec}(A)$  be locally closed. We say  $S$  is a *parametric set* for  $I$  if there is a finite set  $G \subset \mathcal{J}_S$  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  $\langle \text{lt}(\sigma_{\mathfrak{p}}(g)) \rangle = \langle \text{lt}(\sigma_{\mathfrak{p}'}(g)) \rangle$ .

Reduced Gröbner bases are supposed to be unique, and indeed that's also the case for the set  $G$  in the definition of parametric sets. To prove this, we'll first need a lemma.

**4.5 · Lemma.** Let  $Y \subset \text{Spec}(A)$  be a closed set and  $f, g \in \mathcal{J}_Y$ . 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 holds for every  $\mathfrak{p} \in Y$ ,  $g = 0$  by lemma 4.2  $\square$

**4.6 · Theorem.** Let  $S \subset \text{Spec}(A)$  be a parametric set for an ideal  $I$  and let  $G \subset \mathcal{J}_Y$  be the 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 invertible leading coefficient) with  $\text{lm}(g) = \text{lm}(\sigma_{\mathfrak{p}}(g))$  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  $\sigma_{\mathfrak{p}}(f) = \sigma_{\mathfrak{p}}(g)$ . Since  $\text{lm}(\sigma_{\mathfrak{p}}(f))$  and  $\text{lm}(\sigma_{\mathfrak{p}}(g))$  is independent of  $\mathfrak{p}$ , we have  $\text{lm}(\sigma_{\mathfrak{p}}(f)) = \text{lm}(\sigma_{\mathfrak{p}}(g))$  for all  $\mathfrak{p} \in Y$ . Since  $\sigma_{\mathfrak{p}}(F) = \sigma_{\mathfrak{p}}(G)$  is a 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, its leading coefficient is 1 for all  $\mathfrak{p} \in Y$ . Since  $\text{lm}(\sigma_{\mathfrak{p}'}(g)) = \text{lm}(\sigma_{\mathfrak{p}}(g))$  for all  $\mathfrak{p}, \mathfrak{p}' \in S$ , we have  $\sigma_{\mathfrak{p}}(\text{lc}(g)) \neq 0$  for all  $\mathfrak{p} \in S$ . Thus  $1 = \text{lc}(\sigma_{\mathfrak{p}}(g)) = \sigma_{\mathfrak{p}}(\text{lc}(g))$ , hence  $\text{lc}(g) = 1$  by lemma 4.2. And since  $\sigma_{\mathfrak{p}}(1) = 1$  for any  $\mathfrak{p}$ , we get that  $\text{lm}(g) = \text{lm}(\sigma_{\mathfrak{p}}(g))$ .  $\square$

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  $S \subset \text{Spec}(A)$  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  $\mathcal{J}_S \rightarrow \mathcal{J}_{S'}$  which maps the reduced Gröbner basis of  $S$  to the reduced Gröbner basis of  $S'$ .

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

Since  $\phi_{\mathfrak{p}}$  was just the localization of an inclusion, we get that  $\sigma_{\mathfrak{p}}(\phi_{\mathfrak{p}}(g)) = \sigma_{\mathfrak{p}}(g)$  for any  $g$  in  $\bar{I}_{\mathfrak{p}}$ . 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.  $\square$

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  $\text{Spec}(A) = \bigcup_{(S,G) \in \mathcal{G}} S$ .

## 4.2 Monic ideals and the reduced Gröbner basis of $\mathcal{J}_S$

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  $\mathcal{J}_S \subset \mathcal{O}_S[X]$ . Since a reduced Gröbner basis consists of monic polynomials, this will imply that  $\mathcal{J}_S$  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  $m \in \text{lm}(I)$ , there is a monic  $f \in I$  with  $\text{lm}(f) = m$ .

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,  $\mathfrak{p} \in \text{Spec}(A)$  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  $\text{coef}(f, t) = 0 \implies \text{coef}(P, t) = 0$ .

*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  $\text{coef}(f, t) = 0$ , then  $\text{coef}(P, t)/Q = 0$ . Hence there is a  $Q_t \in A \setminus \mathfrak{p}$  such that  $\text{coef}(P, t) \cdot Q_t = 0 \in A$ . Then

$$f = \frac{P \cdot \prod_t Q_t}{Q \cdot \prod_t Q_t}$$

satisfies what we want.  $\square$

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

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

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

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

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

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

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

1.  $S$  is parametric for  $I$  if and only if  $\mathcal{J}_S$ , when seen as a ideal in  $\mathcal{O}_S[X]$  is monic.
2. In the above case, the reduced Gröbner of  $\mathcal{J}_S$  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  $G \subset \mathcal{J}_S$  be its reduced Gröbner basis. First, we show that  $\mathcal{J}_S$  is monic, so let  $f \in \mathcal{J}_S$ . Then there is some  $\mathfrak{p} \in S$  such that  $\text{lc}(f) \notin \mathfrak{p}$ , i.e.  $\sigma_{\mathfrak{p}}(\text{lc}(f)) \neq 0$ , since otherwise  $\text{lc}(f) = 0$  by lemma 4.2. Since  $\sigma_{\mathfrak{p}}(G)$  is a Gröbner basis for  $\langle \sigma_{\mathfrak{p}}(\mathcal{J}_S) \rangle$ , there is some  $g \in G$  where  $\text{lm}(\sigma_{\mathfrak{p}}) \mid \text{lm}(\sigma_{\mathfrak{p}}(f))$ . Since  $\text{lm}(g) = \text{lm}(\sigma_{\mathfrak{p}}(g))$  by theorem 4.6 and  $\text{lm}(f) = \text{lm}(\sigma_{\mathfrak{p}}(f))$ , we get  $\text{lm}(g) \mid \text{lm}(f)$ . Since  $g$  is monic, every leading monomial of  $\mathcal{J}_S$  is found as the leading monomial of a monic polynomial, so  $\mathcal{J}_S$  is monic.

For the other implication, assume  $\mathcal{J}_S$  is monic, let  $G = \{g_1, \dots, g_n\}$  denote its unique reduced Gröbner basis and let  $f \in \mathcal{J}_S$ . By the division algorithm we can write

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

with  $\text{lm}(f_i)\text{lm}(g_i) \leq \text{lt}(f)$  and  $\text{coef}(f_i, m) \in \langle \text{coef}(f, m') \mid m' \geq m \text{lt}(g_i) \rangle \subset A/\mathbf{I}(S)$  for all monomials  $m$ . The last condition may be unfamiliar if you're used to work over fields, but it simply states that the coefficients of each  $f_i$  "comes from" coefficients in  $f$ . In other words, we don't use different  $g_i$  to reduce another  $g_j$ , we only use the  $g_i$ s to reduce  $f$ .

The last condition gives us, for any  $\mathfrak{p} \in S$  that if  $\text{lm}(f_i)\text{lm}(g_i) > \text{lm}(\sigma_{\mathfrak{p}}(f))$ , then  $\sigma_{\mathfrak{p}}(\text{lc}(f_i)) \in \langle 0 \rangle$ , thus  $\sigma_{\mathfrak{p}}(\text{lc}(f_i)) = 0$ . Since this holds for every other term of  $f_i$  as well, we get that  $\text{lm}(\sigma_{\mathfrak{p}}(f_i))\text{lm}(\sigma_{\mathfrak{p}}(g_i)) \leq \text{lm}(\sigma_{\mathfrak{p}}(f))$ . Since  $\sigma_{\mathfrak{p}}$  is linear so  $\sigma_{\mathfrak{p}}(f) = \sum_{i=1}^n \sigma_{\mathfrak{p}}(f_i)\sigma_{\mathfrak{p}}(g_i)$ , there must be some  $g_i$  for which  $\text{lm}(\sigma_{\mathfrak{p}})(g_i) \mid \text{lm}(\sigma_{\mathfrak{p}}(f))$ . Since every element of  $\langle \sigma_{\mathfrak{p}}(I) \rangle$  is a scalar multiple of  $\sigma_{\mathfrak{p}}(f)$  for some  $f \in \mathcal{J}_S$ , 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  $\mathcal{J}_S$ , the second assertion follows immediately.  $\square$

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  $\mathcal{J}_S$ . The next theorem is a local test, to determine parametricity.

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

*Proof.* For the first implication, assume  $S$  is parametric and let  $G \subset \mathbf{I}_S$  be its reduced Gröbner basis. Fix some  $\mathfrak{p} \in S$  and let  $\frac{P}{Q} \in \bar{I}_{\mathfrak{p}}$ . By lemma 4.11 we can assume  $\text{lm}(P) = \text{lm}\left(\frac{P}{Q}\right)$ . By lemma 4.12 the leading monomial  $P$  is preserved when we embed it in  $\mathcal{J}_S$ . Hence  $\text{lm}\left(\frac{P}{Q}\right) \in \text{lm}(\mathcal{J}_S)$ , and since the image of  $G$  in  $\bar{I}_{\mathfrak{p}}$  is monic, it is a reduced Gröbner basis of  $\bar{I}_{\mathfrak{p}}$ . Hence  $\mathbf{I}_{\mathfrak{p}}$  is monic and its leading monomials are constant with  $\text{lm}(\bar{I}_{\mathfrak{p}}) = \text{lm}(\mathcal{J}_S)$ .

For the other implication, assume  $\bar{I}_{\mathfrak{p}}$  is monic for every  $\mathfrak{p} \in S$ , and  $\text{lm}(\bar{I}_{\mathfrak{p}}) = \text{lm}(\bar{I}_{\mathfrak{p}'})$  for all  $\mathfrak{p}, \mathfrak{p}' \in S$ . Let  $\{t_1, \dots, t_n\}$  be a minimal set of generators of the monomial ideal  $\text{lm}(\bar{I}_{\mathfrak{p}})$  (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  $\bar{I}_{\mathfrak{p}}$  with  $\text{lm}(g_i(\mathfrak{p})) = t_i$ . Then  $g_i$  is a function  $(\mathfrak{p} \in \text{Spec}(S)) \rightarrow \bar{I}_{\mathfrak{p}}$ , and so is potentially an element of  $\mathcal{J}_S$ . We just need that it locally can be described by the same fraction. Fix a  $\mathfrak{p} \in S$  and find  $P/Q = g_i(\mathfrak{p}) \in \bar{I}_{\mathfrak{p}}$  such that  $\text{lm}(P) = \text{lm}(g_i(\mathfrak{p}))$ , which exists by lemma 4.11. Also by lemma 4.11, we may assume that  $\text{coef}(P, m) = 0$  for all  $m \in \text{lm}(\bar{I}_{\mathfrak{p}}) \setminus t_i$ , 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  $\text{lc}(P)/Q = 1$ . Consider the open set  $U = \{\mathfrak{p}' \in S \mid Q \notin \mathfrak{p}'\}$ , which is an open neighborhood of  $\mathfrak{p}$ . Then  $g_i(\mathfrak{p}') = P/Q \in \bar{I}_{\mathfrak{p}'}$  for all  $\mathfrak{p}' \in U$  since  $P/Q \in \bar{I}_{\mathfrak{p}}$  is monic and has leading monomial  $t_i$  and  $\text{coef}(P/Q, m) = 0$  for all  $m \in \text{lm}(\bar{I}_{\mathfrak{p}'})$ , which is the defining properties of  $g_i(\mathfrak{p}')$ . Thus  $g_i \in \mathcal{J}_S$ .

This makes the set  $G = \{g_1, \dots, g_n\} \subset \mathbf{I}_S$  a good candidate for a Gröbner basis of  $\mathcal{J}_S$ ,

which would make  $S$  parametric by theorem 4.13 because the  $g_i$  are monic. So take an  $f \in \mathcal{J}_S$ . By lemma 4.2 there is a  $\mathfrak{p} \in S$  such that  $\sigma_{\mathfrak{p}}(\text{lc}(f)) \neq 0$ . Letting  $\bar{f}$  denote the image of  $f$  in  $\bar{I} \subset (A/\mathfrak{a})[X]$  and  $\bar{f}_{\mathfrak{p}}$  its image in  $\bar{I}_{\mathfrak{p}}$ , this implies that  $\text{lc}(\bar{f}) \neq 0$ , hence  $\text{lm}(f) = \text{lm}(\bar{f}) = \text{lm}(\bar{f}_{\mathfrak{p}})$ . Thus  $\text{lm}(\mathcal{J}_S) = \text{lm}(\bar{I}_{\mathfrak{p}}) = \text{lm}(\bar{f}_{\mathfrak{p}})$ , so  $\text{lm}(\mathcal{J}_S) = \text{lm}(\bar{I}_{\mathfrak{p}}) = \text{lm}(G)$ . Thus  $\mathcal{J}_S$  is monic, so  $S$  is parametric by theorem 4.13.  $\square$

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

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

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

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

### 4.3 An aside on flatness

It is proven in [6] that if  $S$  is parametric for an ideal  $I$ , then the canonical morphism  $\phi : \text{Spec}(A[X](I)) \rightarrow \text{Spec}(A)$  is flat over  $S$ . However, the flatness of  $\phi$  has no dependence on the monomial order on  $I$ , while the parametricity of  $S$  does. Thus we have the stronger proposition, that  $\phi$  is flat over  $S$  if there is any monomial order, such that  $S$  is parametric for  $I$ . For example, the ideal  $I = \langle ux + y \rangle \subset A[x, y]$  where  $A = k[u]$ , we have that  $\text{Spec}(A)$  is parametric if  $y > x$ , but not if  $x > y$ . So flatness of  $\phi$  doesn't capture fully the parametricity of  $S$ .

Consider instead the family of rings  $\mathcal{O}_{\{\mathfrak{p}\}}/\mathcal{J}_{\{\mathfrak{p}\}}$  indexed by closed points  $\mathfrak{p} \in S$  for some locally closed set  $S \subset \text{Spec}(A)$ . We wish to show that  $S$  is parametric if and only if this family is a flat

### 4.4 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  $\mathcal{J}_S$  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 [6].

**4.16 · Definition (Lucky prime).** A prime ideal  $\mathfrak{p} \in \text{Spec}(A)$  is called *lucky* if  $\text{lc}(I, m) \notin \mathfrak{p}$  for all  $m \in \text{lm}(I)$ .

**4.17 · Definition (Singular ideal).** Let  $I \subset A[X]$  be an ideal and let  $M$  be the (unique)

minimal set of generators of  $\langle \text{lm}(I) \rangle$ . The *singular ideal* of  $I$  is the radical ideal

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

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

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  $\mathfrak{p} \in \text{Spec}(A)$  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  $\langle \text{lm}(I) \rangle$ . For the first implication, let  $p \in \text{Spec}(A)$  be lucky. For each  $m \in M$ , let  $f_m \in I$  have  $\text{lm}(f) = m$ . Since  $\mathfrak{p}$  is lucky, we can choose the  $f_m$  such that  $\text{lc}(f_m) \notin \mathfrak{p}$  for every  $m \in M$ . Since  $\mathfrak{p}$  is prime, we thus have  $\prod_{m \in M} \text{lc}(f_m) \notin \mathfrak{p}$ . 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  $m \in \text{lm}(I)$  with  $\text{lc}(I, m) \subset \mathfrak{p}$ . Now, there is some  $m' \in M$  with  $m' \mid m$ . We have  $\text{lc}(I, m') \subset \text{lc}(I, m)$ , thus there is some  $m' \in M$  with  $\text{lc}(I, m') \subset \mathfrak{p}$ . Since  $\mathfrak{p}$  is an ideal, this gives  $\prod_{m \in M} \text{lc}(I, m) \subset \mathfrak{p}$ . Since  $\mathfrak{p}$  is prime, this gives that  $\sqrt{\prod_{m \in M} \text{lc}(I, m)} \subset \mathfrak{p}$  and we are done.  $\square$

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  $\text{lm}(I)$ . Then*

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

*Proof.* This follows from the equality

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

A generator  $c$  on the left side is the leading coefficient of a polynomial  $f \in I$  with leading monomial  $m$ . Since  $G$  is a Gröbner basis, there is some  $g \in G$  with  $\text{lt}(g) \mid \text{lt}(f)$ . By the minimality of  $M$ , we have  $\text{lm}(g) = \text{lm}(f) = m$ , thus  $\text{lc}(g) \mid \text{lc}(f) = c$ , so  $\text{lc}(I, m) \subset \langle \text{lc}(g) \mid g \in G, \text{lm}(g) = m \rangle$ .

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

**4.20 • Example.** Consider again the ideal  $I = \langle ax + cy, bx + dy \rangle \subset A = \mathbb{C}[a, b, c, d][x, y]$  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  $\text{lm}(I)$  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  $\mathfrak{p} \in A \setminus \mathbf{V}(ad - bc)$ , we have  $ad - bc \notin \mathfrak{p}$ , so  $\frac{(ad-bc)y}{ad-bc} \in \mathcal{J}_A(\mathbf{V}(ad - bc))$ . Hence, we get the reduced Gröbner basis  $\{x, y\}$  for the ideal  $\sigma_{\mathfrak{p}}(I)$ .

Clearly, the leading monomial ideal of  $I$  will remain unchanged, if we specialize with a point away from the singular ideal, as illustrated above. However, it is not enough to have the function  $\mathfrak{p} \mapsto \text{lm}(\sigma_{\mathfrak{p}}(I))$  be constant on  $\text{Spec}(A)$ . 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  $\text{lm}(\sigma_{\mathfrak{p}}(I)) = \{x\}$  for all  $\mathfrak{p} \in \text{Spec}(\mathbb{C}[u])$ , but  $\text{Spec}(\mathbb{C}[u])$  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  $\text{Spec}(\mathbb{C}[u])$  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  $\text{lm}(I)$  is  $M = \{x\}$ , hence

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

Considering the two cases, we see that

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

which should make it clear why there is no parametric 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  $Z \subset \text{Spec}(A)$  be closed and  $\mathfrak{a} = \mathbf{I}(Z)$  and let  $\bar{I}$  be the image of  $I$  in  $(A/\mathfrak{a})[X]$ . Then

1.  $Z_{\text{gen}} := Z \setminus \mathbf{V}(\mathbf{J}(\bar{I}))$  is parametric for  $I$  with  $\text{lm}(\mathcal{J}_{Z_{\text{gen}}}) = \text{lm}(\bar{I})$ .
2. If  $Y \subset Z$  is parametric for  $I$  with  $\text{lm}(\mathcal{J}_Y) = \text{lm}(\bar{I})$ , then  $Y \subset Z_{\text{gen}}$ .

*Proof.* First, let's show that  $Z_{\text{gen}}$  is parametric. It is locally closed, so we just need to show that  $\mathcal{J}_{Z_{\text{gen}}}$  has a reduced Gröbner basis. Let  $m \in \text{lm}(\mathcal{J}_{Z_{\text{gen}}})$ . Let  $f \in \mathcal{J}_{Z_{\text{gen}}}$  and for each  $\mathfrak{p} \in Z_{\text{gen}}$  let  $P_{\mathfrak{p}} \in \bar{I}$  and  $Q_{\mathfrak{p}} \in (A/\mathfrak{a}) \setminus \mathfrak{p}$  such that  $f(\mathfrak{p}) = P_{\mathfrak{p}}/Q_{\mathfrak{p}} \in \bar{I}_{\mathfrak{p}}$ , with  $\text{coef}(f, m) = 0 \implies \text{coef}(P_{\mathfrak{p}}, m) = 0$  for all monomials  $m$ . Then  $\text{lm}(f) = \text{lm}(P_{\mathfrak{p}})$ , so



$\text{lm}(P_{\mathfrak{p}}) = \text{lm}(P_{\mathfrak{p}'})$  for all  $\mathfrak{p}, \mathfrak{p}' \in Z_{\text{gen}}$ . By possibly multiplying with a generator of  $\mathfrak{p}$ , we can assume  $\text{lc}(P_{\mathfrak{p}}) \in \mathfrak{p}$  for all  $\mathfrak{p} \in Z_{\text{gen}}$ .

Now, we need to produce a monic polynomial  $f'$  with the same leading monomial as  $f$ . Since for each  $\mathfrak{p} \in Z_{\text{gen}}$  we have  $\mathfrak{p} \notin \mathbf{V}(\mathbf{J}(\bar{I}))$ , we can find some  $P \in \bar{I}$

Now, we need to produce a monic polynomial  $f'$  with the same leading monomial as  $f$ . Take a finite cover  $\{U_{\mathfrak{p}} \mid \mathfrak{p} \in \mathfrak{P}\}$  of  $Z_{\text{gen}}$  such that  $f(\mathfrak{p}') = \frac{P_{\mathfrak{p}}}{Q_{\mathfrak{p}}}$  for every  $\mathfrak{p}' \in U_{\mathfrak{p}}$ . Let  $d = \prod_{\mathfrak{p} \in \mathfrak{P}} \text{lc}(P'_{\mathfrak{p}})$  and let  $d_{\mathfrak{p}} = d / \text{lc}(P'_{\mathfrak{p}})$ . Since the  $\mathfrak{p}$  are prime, we have  $d \notin \mathfrak{p}$  for any  $\mathfrak{p} \in \mathfrak{P}$ . Thus  $\text{lc}(d_{\mathfrak{p}} P'_{\mathfrak{p}}) \notin \mathfrak{p}$ . Also

have  $\text{lc}(P) \notin \mathfrak{p}$ , which gives  $\text{lc}(P) Q_{\mathfrak{p}} \notin \mathfrak{p}$  since  $\mathfrak{p}$  is a prime ideal. Hence

$$f'(\mathfrak{p}) = \frac{P_{\mathfrak{p}}}{\text{lc}(P_{\mathfrak{p}}) Q_{\mathfrak{p}}}$$

is a monic polynomial in  $\mathcal{S}_{Z_{\text{gen}}}$  with  $\text{lm}(f) = \text{lm}(f')$ . So  $\mathcal{S}_{Z_{\text{gen}}}$  is a monic ideal in  $\mathcal{O}_{Z_{\text{gen}}}[X]$ , and so  $Z_{\text{gen}}$  is parametric by theorem 4.13.

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

## 4.5 The projective case

Let  $I \subset A[X]$  be an ideal. In the affine case we've seen that, even though  $\text{lm}(\sigma_{\mathfrak{p}}(I))$  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  $\text{Spec}(A)$  with parametric sets. If  $I$  is homogenous, we are in luck.

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

*Proof.* By theorem 4.22, we have the first implication. For the reverse implication, assume that  $\text{lm}(\sigma_{\mathfrak{p}}(I)) = \text{lm}(I)$  and assume for a contradiction that  $\mathfrak{p}$  is unlucky for  $I$ , i.e. there is some  $m \in \text{lm}(I)$  with  $\text{lc}(I, m) \subset \mathfrak{p}$ . 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  $\text{lc}(I, m') \subset \mathfrak{p} \implies m' < m$ . Since by assumption  $\text{lm}(I) = \text{lm}(\sigma_{\mathfrak{p}}(I))$ , we can find a  $P \in I$  with  $\text{lm}(\sigma_{\mathfrak{p}}(P)) = m$ , and since  $I$  is homogenous, we can assume that  $P$  is homogenous by lemma A.3. Because  $<$  is a well-order, we can take  $P$  to have minimal leading monomial, i.e. if  $P' \in I$  with  $\text{lm}(\sigma_{\mathfrak{p}}(P')) = m$  then  $\text{lm}(P) < \text{lm}(P')$ .

Since  $\text{lc}(I, m) \subset \mathfrak{p}$ , we have  $\text{lt}(P) \geq m$ , and because  $\deg(\text{lt}(P)) = m$ , we have  $\text{lc}(I, \text{lm}(P)) \not\subset$

$\mathfrak{p}$  since we assumed  $m$  to be maximal among the monomials of its degree. Therefore we can find some  $Q \in I$  with  $\text{lm}(Q) = m = \text{lm}(P)$  and  $\text{lc}(Q) \notin \mathfrak{p}$ . Now, we can construct a new polynomial

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

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

We are now ready for the grand finale in the projective case, namely that partitioning  $\text{Spec}(A)$  with respect to  $\text{lm}(\sigma_{\mathfrak{p}}(I))$  gives a canonical partition into (maximal) parametric sets. Specifically, if we partition  $\text{Spec}(A)$  by the equivalence relation  $\mathfrak{p} \sim \mathfrak{p}'$  exactly when  $\text{lm}(\sigma_{\mathfrak{p}}(I)) = \text{lm}(\sigma_{\mathfrak{p}'}(I))$ , 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 G bner cover.

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

**4.24 • Lemma.** *Let  $S_1, S_2, \dots, S_n \subset \text{Spec}(A)$  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:*

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

*Furthermore, for each  $i \in \{1, 2, \dots, m\}$  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 [4].

For the second part, fix an  $i \in \{1, 2, \dots, m\}$  and find a  $j$  such that  $Z_i \cap \overline{S_j} \neq \emptyset$ . By applying proposition 3.6.15 in [4] 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.  $\square$

We're now ready to prove the main theorem.

**4.25 • Theorem.** *Let  $I \subset A[X]$  be a homogenous ideal and let  $S \subset \text{Spec}(A)$  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  $S = \text{Spec}(A)$ . Indeed, if we prove that an equivalence class  $Y \subset \text{Spec}(A)$  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  $\text{Spec}(A)/\sim$ , this gives us what we want.

Let  $Y \subset \text{Spec}(A)$  be an equivalence class and let  $M$  be the constant value of  $\text{lm}(\sigma_{\mathfrak{p}}(I))$  for any  $\mathfrak{p} \in Y$ . Let  $Z = \bar{Y}$  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  $Y = \bar{Y} \setminus \mathbf{V}(\mathbf{J}(\bar{I}))$ , 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  $M = \text{lm}(\sigma_{\mathfrak{p}}(I)) = \text{lm}(\sigma_{\mathfrak{p}}(\bar{I}))$ . Since  $\bar{I}$  is also homogenous, by theorem 4.23 (applied to  $\bar{I}$ ) and lemma 4.18, we have for all  $\mathfrak{p} \in \bar{Y}$  that if  $\text{lm}(\bar{I}) = \text{lm}(\sigma_{\mathfrak{p}}(\bar{I}))$  then  $\mathfrak{p} \notin \mathbf{V}(\mathbf{J}(\bar{I}))$ . Since  $Y$  is exactly those  $\mathfrak{p}$ , where  $\text{lm}(\sigma_{\mathfrak{p}}(I)) = M$ , we just need to show that  $\text{lm}(\bar{I}) = M$ .

By lemma 4.24, we can write  $Z$  as a union of irreducible, closed sets:

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

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  $\mathfrak{p} \in Z_i \subset \bar{Y}$ . Also, by theorem 4.22 we have that  $S_i$  is parametric with  $\text{lm}(\mathcal{J}_{S_i}) = \text{lm}(\bar{I}_i)$  and by theorem 4.6  $\text{lm}(\mathcal{J}_{S_i}) = \text{lm}(\sigma_{\mathfrak{p}}(\bar{I}_i))$  for all  $\mathfrak{p} \in S_i$ . By the second part of lemma 4.24, there is some  $\mathfrak{p} \in S_i \cap Y$ , so  $\text{lm}(\sigma_{\mathfrak{p}}(\bar{I}_i)) = M$  for all  $\mathfrak{p} \in S_i$ . Hence,

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

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

For the reverse inclusion, take an  $m \in M$ . Since  $M = \text{lm}(\bar{I}_1)$ , we can find some  $P \in \bar{I}$  such that  $\text{lm}(\bar{P}_1) = m$  ( $\bar{P}_1$  being the image of  $P$  in  $\mathbf{I}(Z_1)$  as before). This means  $\text{coef}(P, m) \notin \mathbf{I}(Z_1)$  but  $\text{coef}(P, m') \in \mathbf{I}(Z_1)$  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  $\text{coef}(cP, m') \in \mathbf{I}(Z)$  for all  $m' > m$ . Furthermore, since  $\mathbf{I}(Z_1)$  is a radical, primary ideal, it is prime, so  $\text{coef}(cP, m) \notin \mathbf{I}(Z_1)$ . This gives  $\text{coef}(cP, m) \notin \mathbf{I}(Z)$ . Thus every term in  $cP$  larger than  $m$  is zero, so  $\text{lm}(cP) = m$ . Thus  $M \subset \text{lm}(\bar{I})$ , which completes the proof.  $\square$

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

**4.26 • Theorem.** Let  $F \subset k[X, U]$  and  $S \subset k[U]$  be finite sets of polynomials and let  $\mathcal{H} = \mathbf{CGS}(F, S)$ . If  $(S, \{h\}, G) \in \mathcal{H}$ , then  $V(S) \setminus V(\{h\})$  is a parametric set. Furthermore, if  $M$  is the minimal generating set of  $\langle \text{lm}(G) \rangle$ , then

$$\left\{ \frac{g}{\text{lc}_U(g)} \mid g \in G, \text{lm}_U(g) \in M \right\} \subset \mathcal{O}_{V(S)}[X]$$

is its reduced Gröbner basis.

*Proof.* By the algorithm,  $G$  is the reduced Gröbner basis of  $\langle F \cup S \rangle$  w.r.t. a term order where  $X^{v_1} > U^{v_2}$  and  $h = \text{lcm}(\{\text{lc}_U(g) \mid g \in G \setminus k[U]\})$ . Let  $I = \langle F \rangle$ , let  $\bar{I}$  denote the image of  $I$  in  $(k[U]/\langle S \rangle)[X]$  and for a polynomial  $f \in k[U][X]$  let  $\bar{f}$  denote the image of  $f$  in  $(k[U]/\langle S \rangle)$ .  $G \setminus S$  is a set of polynomials with the property that there is a Gröbner basis  $G'$  of  $\langle F \rangle$ , such that for each  $g' \in G'$  there is a unique  $g \in G$  such that  $\bar{g}' = \bar{g}$ . Furthermore,  $\text{coef}(g, m) = 0 \iff \text{coef}(\bar{g}, m) = 0$ . Thus  $\{\bar{g} \mid g \in G\}$  is a Gröbner basis of  $\bar{I}$ .

From proposition 4.19 we get that  $\langle h \rangle \subset \mathbf{J}(\bar{I})$ . Hence  $V(S) \setminus V(h)$  is parametric by theorem 4.22. Finally, we need to show that

$$G_{red} = \left\{ \frac{g}{\text{lc}_U(g)} \mid g \in G, \text{lm}_U(g) \in M \right\}$$

is the reduced Gröbner basis of  $\mathbf{V}(S) \setminus \mathbf{V}(h)$ . First, note that each  $g \in G_{red}$  is monic and an element of  $k[U]_{\mathfrak{p}}(X)$  for each prime ideal  $\mathfrak{p} \subset \langle S \rangle$ . Hence,  $G_{red} \subset \mathcal{J}_{\mathbf{V}(S)}$  by the reasoning above, that  $G$  maps to a Gröbner basis of  $\bar{I}$ . Let  $\mathfrak{p}$  be a maximal ideal in  $V(S) \setminus V(h)$  and take any  $f \in \sigma_{\mathfrak{p}}(I)$ , then there is some  $g \in G$  such that  $\text{lm}(\sigma_{\mathfrak{p}}) \mid f$ . Since  $M$  generates  $\text{lm}(G)$ , there is some  $g' \in G_{red}$  such that  $\text{lm}(\sigma_{\mathfrak{p}}(g')) \mid \text{lm}(\sigma_{\mathfrak{p}}(g)) \mid \text{lm}(f)$   $\square$

## 5 Applications

### 5.1 Quantifier elimination

One of the first applications of parametric Gröbner bases was presented by its inventor Weispfenning [5] 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.

Specifically, 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 partitioning 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  $\phi$  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  $\phi_1, \phi_2, \dots, \phi_r$  such that  $\phi \iff (\phi_1 \vee \dots \vee \phi_r)$ .

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

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

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 existential formulas containing conjunctions of polynomial equations and inequations.

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

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

□

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

**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  $\text{lt}(\sigma_\alpha(g)) \mid 1$ . Thus  $\sigma_\alpha(g)$  is a constant polynomial with non-zero constant term, contradicting the assumption.  $\square$

## 5.2 Bernds conjecture<sup>2</sup>

In the article [2], Bernd Sturmfels states the following theorem without proof.

**5.4 · 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  $V(F) = \emptyset$  and consider the ideal  $\langle y_1 - f_1, \dots, y_k - f_k \rangle \subset K[x_1, \dots, x_n, y_1, \dots, y_k]$ . Let  $G$  be a Gröbner basis of  $I$  with respect to the lexicographic order with  $x_1 > \dots > x_n > y_1 > \dots > y_k$ . Then  $G$  contains a polynomial  $p$  (called a final polynomial) such that*

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

He writes that the proof is “straightforward but fairly technical”. Here is a relatively clean proof, using the theory of parametric Gröbner bases.

*Proof.* We will only prove the existence of a polynomial satisfying the first property, and will refer to any polynomial satisfying that property as a final polynomial. Let  $I = \langle y_1 - f_1, \dots, y_k - f_k \rangle \subset K[y_1, \dots, y_k][x_1, \dots, x_n]$  and let  $\mathcal{G}$  be a parametric Gröbner basis of  $I$ . Let  $\sigma : K[y_1, \dots, y_k] \rightarrow K$  be the specialization setting every  $y_i$  to 0. Then  $\mathcal{G}$  contains a final polynomial. To see this, notice that  $\sigma(\mathcal{G})$  is a Gröbner basis of  $\langle \sigma(I) \rangle$

<sup>2</sup>Named such by Bernd Sturmfels in a private communication to the supervisor of this project.

which, by the Nullstellensatz, is equal to  $\langle 1 \rangle$ . Hence there is some  $g \in \mathcal{G}$  such that  $\text{lm}(\sigma(g)) \mid 1$ , implying that  $\sigma(g) \in K \setminus \{0\}$ .

Now, we let  $\mathcal{G}' = \{g \in \mathcal{G} \mid \sigma(g) \notin K\} = \{g_1, \dots, g_t\}$ . Assume that  $\mathcal{G}'$  is still a Gröbner basis for  $I$  w.r.t. the lexicographic order. Since  $I$  contains a final polynomial, say  $p$ , we can apply the division algorithm to write

$$p = \sum_{i=1}^t g_i h_i$$

which in particular is a pseudo-division. Since pseudo-divisions are stable under specializations by lemma 2.12, we get that

$$1 = \sigma(p) = \sum_{i=1}^t \sigma(g_i h_i)$$

and  $\text{lm}(\sigma(g_i h_i)) \leq 1$ . Hence, every  $g_i$  where  $h_i \neq 0$  satisfies  $\sigma(g) \in K$ , but that is a contradiction. Thus  $\mathcal{G}'$  is not a Gröbner basis of  $I$ .

To drive it home, let  $G$  be a Gröbner basis of  $I \subset K[x_1, \dots, x_n, y_1, \dots, y_k]$  w.r.t. the lexicographic order and assume  $G$  doesn't contain a final polynomial. Since any product of  $y$ 's is smaller than any product of  $x$ 's, we can see  $G$  as a Gröbner basis of  $I \subset K[y_1, \dots, y_k][x_1, \dots, x_n]$ . Then, there is a parametric Gröbner basis  $\mathcal{G}$  containing  $G$ . Let  $\mathcal{G}' = \{g \in \mathcal{G} \mid \sigma(g) \notin K\}$ . Then  $G \subset \mathcal{G}'$ , but  $\mathcal{G}'$  is not a Gröbner basis by the above. Thus  $G$  cannot be a Gröbner basis.  $\square$

## References

- [1] 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>.
- [2] 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](https://doi.org/10.1016/S0747-7171(08)80121-6). URL: <https://www.sciencedirect.com/science/article/pii/S0747717108801216>.
- [3] 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](https://doi.org/10.1145/1145768.1145821).
- [4] Ravi Vakil. *THE RISING SEA – Foundations of Algebraic Geometry*.
- [5] 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](https://doi.org/10.1016/0747-7171(92)90023-W). URL: <https://www.sciencedirect.com/science/article/pii/074771719290023W>.
- [6] 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 introductory algebra courses. Hence, we present them here.

### A.1 Reduced Gröbner bases

### A.2 Pseudo-division

### A.3 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.1 · 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.2 · Theorem.** Let  $A$  be a commutative ring, and let  $\text{Spec}(A)$  be the set of prime ideals of  $A$ . Then

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

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

For the converse inclusion, □

### A.4 Homogenous ideals

Here, we present a basic lemma about homogenous ideals.

**A.3 · 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

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

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

$$h_i g_i = \sum_j h_{i,j} g_i, \quad \text{where } h_i = \sum_j h_{i,j}.$$

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

$$f = \sum_{i,j} h_{i,j} g_i$$

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