Gröbner Bases for Families of Affine or Projective Schemes

Michael Wibmer *

May 15, 2006

Abstract

Let I be an ideal of the polynomial ring $A[x] = A[x_1, \dots, x_n]$ over the commutative, noetherian ring A. Geometrically I defines a family of affine schemes over $\mathrm{Spec}(A)$: For $\mathfrak{p} \in \mathrm{Spec}(A)$, the fibre over $\mathfrak{p}$ is the closed subscheme of affine space over the residue field $k(\mathfrak{p})$, which is determined by the extension of I under the canonical map $\sigma_\mathfrak{p} : A[x] \to k(\mathfrak{p})[x]$. If I is homogeneous there is an analogous projective setting, but again the ideal defining the fibre is $\langle \sigma_\mathfrak{p}(I) \rangle$. For a chosen term order this ideal has a unique reduced Gröbner basis which is known to contain considerable geometric information about the fibre. We study the behavior of this basis for varying $\mathfrak{p}$ and prove the existence of a canonical decomposition of the base space $\mathrm{Spec}(A)$ into finitely many, locally closed subsets over which the reduced Gröbner bases of the fibres can be parameterized in a suitable way.

Introduction

Let A be a commutative, noetherian ring with identity and $A[x] = A[x_1, \dots, x_n]$ the polynomial ring in the variables $x_1, \dots, x_n$ over A. We denote the residue field at $\mathfrak{p} \in \mathrm{Spec}(A)$ by $k(\mathfrak{p})$. Geometrically an ideal $I \subset A[x]$ defines a family of affine schemes over $\mathrm{Spec}(A)$: The canonical map $A \to A[x]/I$ gives rise to a morphism of affine schemes

$$\varphi : \mathrm{Spec}(A[x]/I) \to \mathrm{Spec}(A).$$

For $\mathfrak{p} \in \mathrm{Spec}(A)$ the fibre $\varphi^{-1}(\mathfrak{p})$ is the closed subscheme of $\mathbb{A}^n_{k(\mathfrak{p})} = \mathrm{Spec}(k(\mathfrak{p})[x])$ determined by $\langle \sigma_\mathfrak{p}(I) \rangle$ where $\sigma_\mathfrak{p} : A[x] \to k(\mathfrak{p})[x]$ denotes the trivial extension of the canonical map $A \to k(\mathfrak{p})$.

If I is a homogeneous ideal we analogously obtain a family of projective schemes from

$$\varphi : \mathrm{Proj}(A[x]/I) \to \mathrm{Spec}(A).$$

The fibre $\varphi^{-1}(\mathfrak{p})$ is the closed subscheme of $\mathbb{P}^n_{k(\mathfrak{p})} = \mathrm{Proj}(k(\mathfrak{p})[x])$ again determined by $\langle \sigma_\mathfrak{p}(I) \rangle$.

For a chosen term order we wish to study – simultaneously for all $\mathfrak{p} \in \mathrm{Spec}(A)$ – the unique reduced Gröbner basis of $\langle \sigma_\mathfrak{p}(I) \rangle$. It is well known that such a

*Supported by the FWF (Project P16641)

Gröbner basis grants "easy access" to geometric information about the fibre $\varphi^{-1}(\mathfrak{p})$. It also seems reasonable to compare two fibres by "comparing" the corresponding Gröbner bases. Well, of course we can compare the leading terms but it is not quite clear what comparing the Gröbner bases should mean. We will make precise this notion by introducing parametric sets. Rather vaguely a parametric set w.r.t. I is a locally closed subset Y of $\operatorname{Spec}(A)$ such that over Y the reduced Gröbner bases of the fibres can be parameterized in a suitable way. The main result of this article is to establish existence and uniqueness of a canonical decomposition of the base space $\operatorname{Spec}(A)$ into finitely many parametric sets.

Many concrete mathematical problems can be stated in the above described framework of families of affine or projective schemes and knowing the Gröbner basis structure of the fibres may be the first step to their solution, if not yet the solution itself. For example if A is a polynomial ring over some field, then we obtain the case of algebraic systems with parameters, which is important for many "real life" applications such as robotics or electrical engineering (see e.g. [6] chapter 6 and [16]). From a more theoretical point of view parametric sets are a tool to explore the geometry of families of affine or projective schemes. Related theoretical applications range from efficient Gröbner basis computation (see e.g. [2] and [17]) to cohomology (see [18]).

The naive hope that for a Gröbner basis G of I the specialized Gröbner basis $\sigma_{\mathfrak{p}}(G)$ is a Gröbner basis of the specialized ideal $\langle \sigma_{\mathfrak{p}}(I) \rangle$ is in general not fulfilled. The behavior of Gröbner bases under specialization (or extension of scalars) has actually been studied by many authors, e.g. [5], [12], [3], [4], [8]. In [3] the case of standard bases in the ring of formal power series is treated. Relations to flatness are explored in [4] and also in [5]. Articles focusing more on the fibres are [19], [20], [15] and [14]. These last articles were written from a more computational point of view which led to a rather rash use of the word "canonical". So one main objective of the present article is to establish a proper theoretical foundation for the underlying ideas of these articles.

The outline of the article is the following: Section 1 *(Parametric sets)* introduces the fundamental notion of parametric sets and their basic properties. The main theorem of section 2 *(Lucky primes and pseudo division)* is a characterization of parametric sets in terms of lucky primes (see [9]). This theorem can also be understood as giving the geometric meaning of luckiness. Finally in section 3 *(Gröbner covers)* we achieve the main objective of the article by proving existence and uniqueness of a canonical finite covering of $\operatorname{Spec}(A)$ with parametric subsets.

Preliminaries and notation

A parametric subset Y of $\operatorname{Spec}(A)$ allows for an object which parameterizes the reduced Gröbner bases of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ for $\mathfrak{p} \in Y$. To assure uniqueness of this object, which will be called the reduced Gröbner basis of I over Y we have to work with reduced schemes $(Y, \mathcal{O}_Y)$. In particular we would like to assume that our base ring A is reduced. This can be done without loss of generality, so to speak:

Let $\operatorname{Nil}(A)$ denote the nilradical of A and define $A' = A / \operatorname{Nil}(A)$ then there is a natural homeomorphism

$$\begin{aligned} \mathrm{Spec}(A) &\to \mathrm{Spec}(A') \\ \mathfrak{p} &\mapsto \mathfrak{p}' \end{aligned}$$

and $k(\mathfrak{p}) = k(\mathfrak{p}')$. Moreover if $I' \subset A'[x]$ denotes the extension of I under the canonical map $A[x] \to A'[x]$ then $\langle \sigma_{\mathfrak{p}}(I) \rangle = \langle \sigma_{\mathfrak{p}'}(I') \rangle$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$.

Throughout A denotes a commutative, noetherian, reduced ring with identity and I an ideal of the polynomial ring $A[x] = A[x_1, \dots, x_n]$. We only consider reduced subschemes of $\mathrm{Spec}(A)$. So by a subscheme of $\mathrm{Spec}(A)$ we mean a locally closed subset Y of $\mathrm{Spec}(A)$ with the induced reduced subscheme structure $\mathcal{O}_Y$. $\mathfrak{a}$ denotes a radical ideal of A – typically with $\overline{Y} = \mathrm{V}(\mathfrak{a})$. (As usual $\mathrm{V}(\mathfrak{a}) \subset \mathrm{Spec}(A)$ denotes the closed set of all prime ideals containing $\mathfrak{a}$.) We will continuously identify $\mathrm{Spec}(A/\mathfrak{a})$ with $\mathrm{V}(\mathfrak{a}) \subset \mathrm{Spec}(A)$. For an A-module M the localization at $\mathfrak{p} \in \mathrm{Spec}(A)$ is denoted by $M_{\mathfrak{p}}$ and $k(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$ is the residue field at $\mathfrak{p}$. $\sigma_{\mathfrak{p}} : A[x] \to k(\mathfrak{p})[x]$ denotes the coefficientwise extension of the canonical map $A \to k(\mathfrak{p})$.

The set of terms (i.e. powerproducts) is denoted by $\mathcal{T} = \mathcal{T}(x_1, \dots, x_n)$. Throughout we fix a term order $<$ on $\mathcal{T}$. For a non zero polynomial $P = \sum_{t \in \mathcal{T}} a_t t \in A[x]$ we define

- the *coefficient of* P *at* t by $\mathrm{coef}(P, t) = a_t$,
- the *support of* P by $\mathrm{supp}(P) = \{t \in \mathcal{T};\ a_t \neq 0\}$,
- the *leading term* $\mathrm{lt}(P)$ *of* P to be the maximal element of $\mathrm{supp}(P)$,
- the *leading coefficient of* P by $\mathrm{lc}(P) = \mathrm{coef}(P, \mathrm{lt}(P))$ and
- the *leading monomial of* P by $\mathrm{lm}(P) = \mathrm{lc}(P)\,\mathrm{lt}(P)$.

For $G \subset A[x]$ we set $\mathrm{lt}(G) = \{\mathrm{lt}(P);\ P \in G \smallsetminus \{0\}\}$ and similarly $\mathrm{lm}(G) = \{\mathrm{lm}(P);\ P \in G \smallsetminus \{0\}\}$. A finite subset G of I is called a Gröbner basis of I if $\langle \mathrm{lm}(G) \rangle = \langle \mathrm{lm}(I) \rangle$. For $t \in \mathcal{T}$ we define the ideal of leading coefficients at t by

$$\mathrm{lc}(I, t) = \{\mathrm{lc}(P);\ P \in I \text{ with } \mathrm{lt}(P) = t\}.$$

Note that $\mathrm{lc}(I, t)$ can conveniently be read of from a Gröbner basis G of I. In fact $\mathrm{lc}(I, t)$ is generated by $\{\mathrm{lc}(g);\ g \in G \text{ with } \mathrm{lt}(g) \text{ divides } t\}$. For a general reference for Gröbner bases over rings see [1].

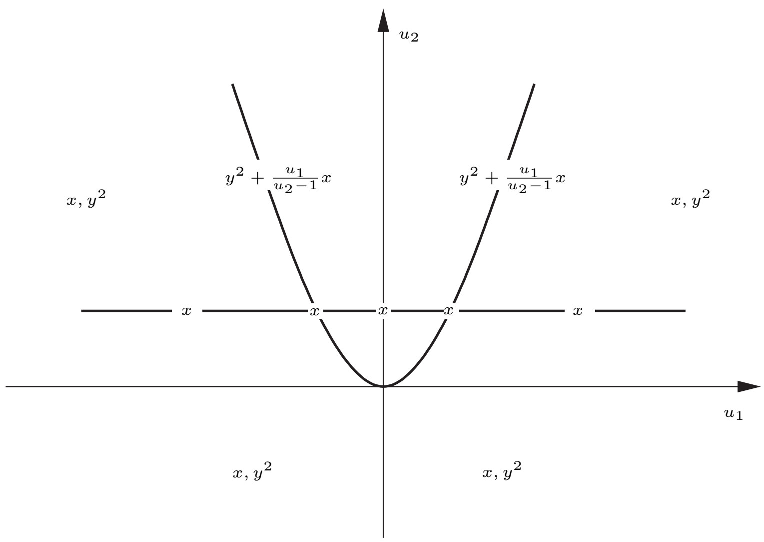
Before really getting started we do two warmup examples:

Example 1. *Let k be a field and $A = k[u_1, u_2]$ the polynomial ring in the two parameters u_1, u_2. Consider the ideal*

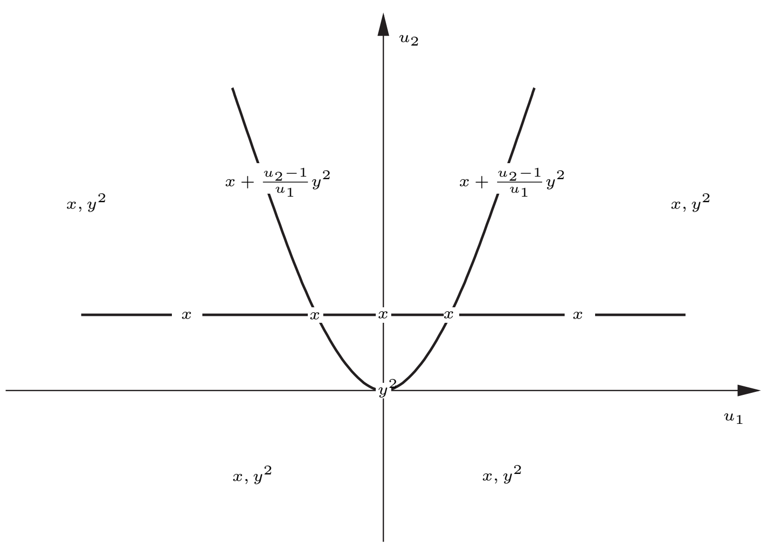
$$I = \left\langle (u_1^2 - u_2)x, (u_2 - 1)y^2 + u_1 x \right\rangle \subset A[x, y].$$

When faced with the task to describe the Gröbner basis structure of the fibres I guess most mathematicians would come up with the following pictures:

term order with $y^2 > x$:



term order with $x > y^2$:



The above pictures illustrate a decomposition of the base space $\mathbb{A}_k^2 = \mathrm{Spec}(A)$ into locally closed subsets. In short the objective of this article is to find this decomposition in general.

Example 2. *Let k be an algebraically closed field and $A = k[u_1, u_2, u_3, u_4]$ the polynomial ring in the parameters u_1, u_2, u_3, u_4. We consider the ideal*

$$I = \langle u_2u_3 - u_4u_1, u_1x + u_2, u_3x + u_4\rangle \subset A[x].$$

(Here x denotes just one variable.) Let $v = (v_1, v_2, v_3, v_4) \in k^4$ and

$$\mathfrak{p}_v = \langle u_1 - v_1, u_2 - v_2, u_3 - v_3, u_4 - v_4 \rangle.$$

If $v_2v_3 - v_4v_1$ is non zero then the reduced Gröbner basis of $\langle \sigma_{\mathfrak{p}_v}(I) \rangle$ is 1. If v_1 and v_3 are zero and one of v_2, v_4 is non zero then the reduced Gröbner basis of $\langle \sigma_{\mathfrak{p}_v}(I) \rangle$ is also 1. (In particular the set of all $v \in k^4$ such that the reduced Gröbner basis of $\langle \sigma_{\mathfrak{p}_v}(I) \rangle$ is 1 is not locally closed.) If v lies in the quasi-affine variety $Y = \mathrm{V}(\langle u_2u_3 - u_4u_1 \rangle) \smallsetminus \mathrm{V}(\langle u_1, u_3 \rangle)$ then the reduced Gröbner bases of $\langle \sigma_{\mathfrak{p}_v}(I) \rangle$ is given by $x + f(v)$ where f denotes the regular function on Y defined by

$$f(v) = \begin{cases} \frac{v_2}{v_1} & \text{if } v_1 \neq 0 \\ \frac{v_4}{v_3} & \text{if } v_3 \neq 0. \end{cases}$$

The above example illustrates the "local nature" of the problem and suggests to work with sheaves and not just with polynomials in I, as was common practice in [20] or [14].

1 Parametric sets

The idea of "parameterizing Gröbner bases" can nicely be captured using sheaves. For every subscheme Y of $\mathrm{Spec}(A)$ we will define a quasi-coherent sheaf $\mathcal{I}_Y$ on Y which intuitively might be thought of as the restriction of I to Y.

Let Y be a locally closed subset of $\mathrm{Spec}(A)$ and $\mathfrak{a} \subset A$ the radical ideal such that $\overline{Y} = \mathrm{V}(\mathfrak{a})$ and let $\overline{I}$ denote the extension of I in $(A/\mathfrak{a})[x]$. We define $\mathcal{I}_Y$ to be the restriction of the quasi-coherent sheaf associated to the $A/\mathfrak{a}$ -module $\overline{I}$ on $\mathrm{Spec}(A/\mathfrak{a}) = \mathrm{V}(\mathfrak{a})$ to Y. That is

$$\mathcal{I}_Y = \widetilde{\overline{I}}\Big|_Y.$$

More explicitly for an open subset U of Y the $\mathcal{O}_Y(U)$-module $\mathcal{I}_Y(U)$ consists of all functions g from U into the disjoint union $\coprod_{\mathfrak{p} \in U} \overline{I}_{\mathfrak{p}}$ which are locally fractions, i.e. for every $\mathfrak{p} \in U$ there exists an open neighborhood U' of $\mathfrak{p}$ in U such that for all $\mathfrak{q} \in U'$ we have $g(\mathfrak{q}) = \frac{P}{s} \in \overline{I}_{\mathfrak{q}}$, where $P \in \overline{I}$ and $s \in (A/\mathfrak{a}) \smallsetminus \mathfrak{q}$ for all $\mathfrak{q} \in U'$.

Since A is noetherian, $\mathrm{Spec}(A)$ is a noetherian topological space and thus every open subset U of Y is quasi-compact. This implies that we can consider $\mathcal{I}_Y(U)$ as an ideal of the polynomial ring $\mathcal{O}_Y(U)[x]$. (If U was not quasi-compact we could not be sure that an element of $\mathcal{I}_Y(U)$ has finite support.)

Note that for $\mathfrak{p} \in Y$ the stalk $\mathcal{I}_{Y,\mathfrak{p}} = \overline{I}_{\mathfrak{p}}$ is just the extension of I under $A[x] \to (A/\mathfrak{a})_{\mathfrak{p}}[x]$. Let $\mathfrak{m}_{\mathfrak{p}}$ denote the unique maximal ideal of $\mathcal{O}_{Y,\mathfrak{p}} = (A/\mathfrak{a})_{\mathfrak{p}}$, then in analogy to the sequence

$$A \to \mathcal{O}_Y(Y) \to \mathcal{O}_{Y,\mathfrak{p}} \to \mathcal{O}_{Y,\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} = k(\mathfrak{p})$$

of natural maps we obtain natural maps

$$I \to \mathcal{I}_Y(Y) \to \mathcal{I}_{Y,\mathfrak{p}} \to \langle \sigma_{\mathfrak{p}}(I) \rangle.$$

For $g \in \mathcal{I}_Y(Y)$ the image of g in $\langle \sigma_{\mathfrak{p}}(I) \rangle$ is denoted by $\overline{g}^{\mathfrak{p}}$.

Now we are prepared to give precise meaning to the intuitive idea of parameterizing Gröbner bases: We are looking for subschemes Y of $\mathrm{Spec}(A)$ with the property that there exist global sections $g_1, \dots, g_m \in \mathcal{I}_Y(Y)$ such that for all $\mathfrak{p} \in Y$ their images $\overline{g_1}^{\mathfrak{p}}, \dots, \overline{g_m}^{\mathfrak{p}}$ are the unique reduced Gröbner basis of $\langle \sigma_{\mathfrak{p}}(I) \rangle$. We will need the following easy lemma.

Lemma 1. *Let Y be a subscheme of $\mathrm{Spec}(A)$ and $g, f \in \mathcal{I}_Y(Y)$. Then the set*

$$\left\{ \mathfrak{p} \in Y;\ \overline{g}^{\mathfrak{p}} = \overline{f}^{\mathfrak{p}} \right\}$$

is a closed subset of Y and $\overline{g}^{\mathfrak{p}} = \overline{f}^{\mathfrak{p}}$ for all $\mathfrak{p} \in Y$ implies $g = f$.

Proof: It suffices to treat the case $f = 0$. We can cover Y with open sets U_i such that

$$g(\mathfrak{p}) = \frac{P}{s} \in \overline{I}_{\mathfrak{p}}$$

for $P \in \overline{I} \subset (A/\mathfrak{a})[x]$ and $s \in (A/\mathfrak{a}) \setminus \mathfrak{p}$ for all $\mathfrak{p} \in U_i$. We have

$$\{\mathfrak{p} \in Y;\ \overline{g}^{\mathfrak{p}} = 0\} \cap U_i = \{\mathfrak{p} \in U_i;\ \mathrm{coef}(P, t) \in \mathfrak{p} \text{ for all } t \in \mathrm{supp}(P)\}$$

which is a closed subset of U_i. Hence $\{\mathfrak{p} \in Y;\ \overline{g}^{\mathfrak{p}} = 0\}$ is closed.

If we interpret g as a polynomial with coefficients c_t in $\mathcal{O}_Y(Y)$, then $\overline{g}^{\mathfrak{p}} = 0$ is equivalent to saying that for all $t \in \mathcal{T}$ the image of c_t in the stalk $\mathcal{O}_{Y,\mathfrak{p}} = (A/\mathfrak{a})_{\mathfrak{p}}$ lies in the maximal ideal $\mathfrak{m}_{\mathfrak{p}}$ of $\mathcal{O}_{Y,\mathfrak{p}}$. Since this holds for all $\mathfrak{p} \in Y$ and Y is a reduced scheme we obtain $c_t = 0 \in \mathcal{O}_Y(Y)$. Hence $g = 0$. □

Theorem 1. *If Y is a connected subscheme of $\mathrm{Spec}(A)$ and there exists a finite subset G of $\mathcal{I}_Y(Y)$ such that for all $\mathfrak{p} \in Y$ the set $\overline{G}^{\mathfrak{p}} = \{\overline{g}^{\mathfrak{p}};\ g \in G\}$ is the reduced Gröbner basis of $\langle \sigma_{\mathfrak{p}}(I) \rangle$, then G is uniquely determined and for each $g \in G$ the function $\mathfrak{p} \mapsto \mathrm{lt}(\overline{g}^{\mathfrak{p}})$ is constant on Y. In particular the function $\mathfrak{p} \mapsto \mathrm{lt}(\langle \sigma_{\mathfrak{p}}(I) \rangle)$ is constant on Y.*

Proof: First we will show that for $g \in G$ and $t \in \mathcal{T}$ the set

$$W(t) = \{\mathfrak{p} \in Y;\ \mathrm{lt}(\overline{g}^{\mathfrak{p}}) = t\}$$

is a closed subset of Y. We can cover Y with open sets U_i such that

$$g(\mathfrak{p}) = \frac{P}{s} \in \overline{I}_{\mathfrak{p}} \text{ for all } \mathfrak{p} \in U_i.$$

Here $P \in \overline{I} \subset (A/\mathfrak{a})[x]$ and $s \in (A/\mathfrak{a}) \setminus \mathfrak{p}$ for all $\mathfrak{p} \in U_i$.

Let $\mathfrak{p} \in Y$ and $\phi : (A/\mathfrak{a})_{\mathfrak{p}} \to (A/\mathfrak{a})_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} = k(\mathfrak{p})$ the canonical map. We will need that $\phi(\frac{c}{s}) = 1$ implies $c - s \in \mathfrak{p}$ for $c \in A/\mathfrak{a}$ and $s \in (A/\mathfrak{a}) \setminus \mathfrak{p}$. But $\phi(\frac{c}{s}) = 1$ is equivalent to saying that there exists $c' \in \mathfrak{p}$ and $s' \in (A/\mathfrak{a}) \setminus \mathfrak{p}$ such that

$$\frac{c}{s} = 1 + \frac{c'}{s'} = \frac{s' + c'}{s'}.$$

This implies the existence of an $s'' \in (A/\mathfrak{a}) \setminus \mathfrak{p}$ such that

$$(cs' - s(s' + c'))s'' = 0 \in \mathfrak{p}.$$

Hence $cs' - ss' \in \mathfrak{p}$ and therefore $c - s \in \mathfrak{p}$.

Using the above result we see that for $\mathfrak{p} \in U_i$ we have $\operatorname{lt}(\overline{g}^{\mathfrak{p}}) = t$ if and only if $\mathfrak{p}$ contains $\operatorname{coef}(P, t')$ for $t' > t$ and $\operatorname{coef}(P, t) - s$ (Use that $\overline{g}^{\mathfrak{p}}$ is monic). Therefore $W(t) \cap U_i$ is a closed subset of U_i and thus $W(t) \subset Y$ is closed.

Since $\operatorname{Spec}(A)$ is a noetherian topological space, a finite number of the U_i's will do and therefore the function $\mathfrak{p} \mapsto \operatorname{lt}(\overline{g}^{\mathfrak{p}})$ takes only finitely many values on Y. Consequently Y is the disjoint union of finitely many $W(t)$'s. By the connectedness assumption on Y we can conclude that the function $\mathfrak{p} \mapsto \operatorname{lt}(\overline{g}^{\mathfrak{p}})$ is constant on Y.

Assume that for $F \subset \mathcal{I}_Y(Y)$ it also holds that $\overline{F}^{\mathfrak{p}}$ is the reduced Gröbner basis of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ for every $\mathfrak{p} \in Y$. Then for $f \in F$ and a chosen $\mathfrak{p} \in Y$ there exists a $g \in G$ such that $\overline{f}^{\mathfrak{p}} = \overline{g}^{\mathfrak{p}}$. Since the leading term of $\overline{f}^{\mathfrak{p}}$ respectively $\overline{g}^{\mathfrak{p}}$ is independent of $\mathfrak{p}$ this implies $\operatorname{lt}(\overline{f}^{\mathfrak{p}}) = \operatorname{lt}(\overline{g}^{\mathfrak{p}})$ for all $\mathfrak{p} \in Y$, but as $\overline{F}^{\mathfrak{p}} = \overline{G}^{\mathfrak{p}}$ is the reduced Gröbner basis we can conclude $\overline{f}^{\mathfrak{p}} = \overline{g}^{\mathfrak{p}}$ for all $\mathfrak{p} \in Y$ and therefore $f = g \in G$ by lemma 1. □

The following example shows that both assertions of the above theorem may be violated if Y is not connected.

Example 3. *Let $Y = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are two distinct, closed points of* $\operatorname{Spec}(A)$. *Note that $\mathcal{O}_Y(Y)$ is just $k(\mathfrak{p}_1) \times k(\mathfrak{p}_2)$. For $j = 1, 2$ let G_j denote the reduced Gröbner bases of $\langle \sigma_{\mathfrak{p}_j}(I) \rangle$. Then for any subset G of*

$$G_1 \times G_2 \subset \langle \sigma_{\mathfrak{p}_1}(I) \rangle \times \langle \sigma_{\mathfrak{p}_2}(I) \rangle = \mathcal{I}_Y(Y)$$

with the property that the projections $G \to G_i$ are surjective we have that $\overline{G}^{\mathfrak{p}}$ is the reduced Gröbner basis of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ for every $\mathfrak{p} \in Y$.

As we wish to have a definition suitable for all (not necessarily connected) subschemes of $\operatorname{Spec}(A)$ we simply demand what we want.

Definition 1. *A locally closed subset Y of* $\operatorname{Spec}(A)$ *is called* parametric for Gröbner bases w.r.t. I (and $<$) *if there exist a finite subset G of $\mathcal{I}_Y(Y)$ with the following properties:*

(1) *$\overline{G}^{\mathfrak{p}}$ is the reduced Gröbner bases of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ for every $\mathfrak{p} \in Y$.*

(2) *For each $g \in G$ the function $\mathfrak{p} \mapsto \operatorname{lt}(\overline{g}^{\mathfrak{p}})$ is constant on Y.*

Since I is clear from the context we usually omit the reference to I and simply talk about parametric subschemes.

Theorem 2. *Let $Y \subset \operatorname{Spec}(A)$ be parametric and G a finite subset of $\mathcal{I}_Y(Y)$ satisfying the two conditions of the above definition, then G is uniquely determined and the function $\mathfrak{p} \mapsto \operatorname{lt}(\langle \sigma_{\mathfrak{p}}(I) \rangle)$ is constant on Y. Furthermore every $g \in G$ is monic with $\operatorname{lt}(g) = \operatorname{lt}(\overline{g}^{\mathfrak{p}})$ for every $\mathfrak{p} \in Y$.*

Proof: Because of condition (2) we can repeat the uniqueness prove as in the last paragraph of the proof of theorem 1.

To show that every $g \in G$ is monic with $\operatorname{lt}(g) = \operatorname{lt}(\overline{g}^{\mathfrak{p}})$ observe that the coefficients of g are just elements of $\mathcal{O}_Y(Y)$. Since $(Y, \mathcal{O}_Y)$ is a reduced scheme every element of $\mathcal{O}_Y(Y)$ is uniquely determined by its images in $k(\mathfrak{p})$ where $\mathfrak{p}$ ranges over all of Y. □

Definition 2. *Let $Y \subset \mathrm{Spec}(A)$ be parametric, then the uniquely determined subset $G = G_Y$ of $\mathcal{I}_Y(Y)$ of the above theorem is called the* reduced Gröbner bases of I over Y.

To give the reader some idea where the journey is going we give the following definition at this early stage although we won't need it before section 3.

Definition 3. *A* Gröbner cover of $\mathrm{Spec}(A)$ w.r.t. I (and $<$) *is a finite set $\mathcal{G}$ consisting of pairs (Y, G_Y) with $Y \subset \mathrm{Spec}(A)$ parametric and G_Y the reduced Gröbner basis of I over Y such that*

$$\bigcup_{(Y,G_Y)\in\mathcal{G}} Y = \mathrm{Spec}(A).$$

Parametric sets are well behaved with respect to inclusion:

Theorem 3. *Let $Y \subset \mathrm{Spec}(A)$ be parametric, then every locally closed subset Y' of Y is parametric and the canonical map $\mathcal{I}_Y(Y) \to \mathcal{I}_{Y'}(Y')$ maps the reduced Gröbner bases of I over Y to the reduced Gröbner bases of I over Y'.*

Proof: First of all let us construct the canonical map of the theorem: Assume $\overline{Y} = \mathrm{V}(\mathfrak{a})$ and $\overline{Y'} = \mathrm{V}(\mathfrak{a}')$ for radical ideals $\mathfrak{a}$ and $\mathfrak{a}'$ of A. Let $\overline{I} \subset (A/\mathfrak{a})[x]$ and $\overline{I}' \subset (A/\mathfrak{a}')[x]$ denote the corresponding extensions of I. As $\overline{Y'} \subset \overline{Y}$ we have $\mathfrak{a} \subset \mathfrak{a}'$ and a canonical map $A/\mathfrak{a} \to A/\mathfrak{a}'$ which extends to $\varphi : \overline{I} \to \overline{I}'$. Then for $\mathfrak{p} \in Y' \subset Y$ we have a canonical map

$$\varphi_{\mathfrak{p}} : \overline{I}_{\mathfrak{p}} \to \overline{I}'_{\mathfrak{p}}.$$

Now an element $g \in \mathcal{I}_Y(Y)$ gives rise to a function

$$g' : Y' \to \prod_{\mathfrak{p}\in Y'} \overline{I}'_{\mathfrak{p}}$$

by $g'(\mathfrak{p}) = \varphi_{\mathfrak{p}}(g(\mathfrak{p}))$. One easily verifies that $\mathcal{I}_Y(Y) \to \mathcal{I}_{Y'}(Y'),\ g \mapsto g'$ is well defined and a morphism. For $\mathfrak{p} \in Y'$ the commutative diagram

$$\begin{array}{ccc} \overline{I}_{\mathfrak{p}} & \longrightarrow & \overline{I}'_{\mathfrak{p}} \\ & \searrow \quad \swarrow & \\ & \langle \sigma_{\mathfrak{p}}(I) \rangle & \end{array}$$

gives rise to a commutative diagram

$$\begin{array}{ccc} \mathcal{I}_Y(Y) & \longrightarrow & \mathcal{I}_{Y'}(Y') \\ & \searrow \quad \swarrow & \\ & \langle \sigma_{\mathfrak{p}}(I) \rangle & \end{array}$$

From this the claim of the theorem follows. $\square$

Next we will give a characterization of parametric sets in terms of monic ideals (see [17]).

Definition 4. *An ideal $I \subset A[x]$ is called monic if $\mathrm{lc}(I,t) \in \{\langle 0\rangle, \langle 1\rangle\}$ for all $t \in \mathcal{T}$.*

There are quite a few definitions of reduced Gröbner bases in the literature. We will use the one strictly paralleling the field case.

Definition 5. *A Gröbner basis $G = \{g_1, \ldots, g_m\}$ of I is called reduced if for $j = 1 \ldots, m$*

- *g_j is monic and*
- *$\mathrm{supp}(g_j) \cap \mathrm{lt}(I) = \{\mathrm{lt}(g_j)\}$.*

With this definition not every ideal has a reduced Gröbner basis, but as in the field case one easily shows that if it exists, it is unique. Concerning existence we have the following (cf. [17] and [3] theorem 2.11).

Theorem 4. *Let $I \subset A[x]$ be an ideal, then there exists a reduced Gröbner basis of I if and only if I is monic.*

Proof: If there exists a reduced Gröbner basis of I then clearly I is monic. Conversely if I is monic then we can choose monic polynomials $g_1, \ldots, g_m \in I$ such that $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)$ is the unique minimal generating set of $\mathrm{lt}(I)$. Now if we mutually reduce the g_j's we end up with the desired reduced Gröbner basis of I. $\square$

The connection to parametric subschemes is the following:

Theorem 5. *A subscheme Y of $\mathrm{Spec}(A)$ is parametric if and only if $\mathcal{I}_Y(Y)$ is monic, and in this case the reduced Gröbner bases of I over Y is the reduced Gröbner bases of $\mathcal{I}_Y(Y) \subset \mathcal{O}_Y(Y)[x]$. In particular $\mathrm{lt}(\mathcal{I}_Y(Y)) = \mathrm{lt}(\langle \sigma_{\mathfrak{p}}(I)\rangle)$ for every $\mathfrak{p} \in Y$.*

Proof: Suppose that Y is parametric and let $G \subset \mathcal{I}_Y(Y)$ denote the reduced Gröbner basis of I over Y. We will show that the leading term of every $f \in \mathcal{I}_Y(Y)$ is divisible by $\mathrm{lt}(g)$ for some $g \in G$. Since $(Y, \mathcal{O}_Y)$ is a reduced scheme there exists a $\mathfrak{p} \in Y$ such that the image of $\mathrm{lc}(f) \in \mathcal{O}_Y(Y)$ in $k(\mathfrak{p})$ is non zero. For such a $\mathfrak{p}$ we know that $\mathrm{lt}(f) = \mathrm{lt}(\overline{f}^{\mathfrak{p}})$ is divisible by $\mathrm{lt}(\overline{g}^{\mathfrak{p}}) = \mathrm{lt}(g)$ for some $g \in G$. Since the elements of G are monic this shows that $\mathcal{I}_Y(Y)$ is monic.

Now suppose that $\mathcal{I}_Y(Y)$ is monic and let $G = \{g_1, \ldots, g_m\}$ denote the reduced Gröbner basis of $\mathcal{I}_Y(Y)$. For $f \in \mathcal{I}_Y(Y)$ the usual division (or reduction) algorithm shows that there exists a representation

$$f = f_1 g_1 + \cdots + f_m g_m$$

such that for $i = 1, \ldots, m$ we have $\mathrm{lt}(f_i)\,\mathrm{lt}(g_i) \le \mathrm{lt}(f)$ and

$$\mathrm{coef}(f_i, t) \in \left\langle \mathrm{coef}(f, t');\ t' \ge t\,\mathrm{lt}(g_i) \right\rangle \text{ for all } t \in \mathcal{T}.$$

This last condition implies that for $\mathfrak{p} \in Y$ we have $\mathrm{lt}(\overline{f_i}^{\mathfrak{p}})\,\mathrm{lt}(\overline{g_i}^{\mathfrak{p}}) \le \mathrm{lt}(\overline{f}^{\mathfrak{p}})$. Because $\overline{f}^{\mathfrak{p}} = \overline{f_1}^{\mathfrak{p}}\overline{g_1}^{\mathfrak{p}} + \cdots + \overline{f_m}^{\mathfrak{p}}\overline{g_m}^{\mathfrak{p}}$ this shows that $\mathrm{lt}(\overline{f}^{\mathfrak{p}})$ is divisible by $\mathrm{lt}(\overline{g_i}^{\mathfrak{p}})$

for some $i \in \{1, \ldots, m\}$. Since every element of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ is of the form $\lambda \overline{f}^{\mathfrak{p}}$ for $\lambda \in k(\mathfrak{p})$ and $f \in \mathcal{I}_Y(Y)$ we can conclude that $\overline{G}^{\mathfrak{p}}$ is a Gröbner basis of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ for every $\mathfrak{p} \in Y$. As $g \in G$ is monic the function $\mathfrak{p} \mapsto \operatorname{lt}(\overline{g}^{\mathfrak{p}})$ is clearly constant and since G is reduced also $\overline{G}^{\mathfrak{p}}$ is reduced. Thus we have shown that Y is parametric and that G is the reduced Gröbner basis of I over Y. □

So the reduced Gröbner basis G of I over Y is indeed a Göbner basis. In fact by theorem 3 $G|_U = \{g|_U;\ g \in G\}$ is the reduced Gröbner basis of $\mathcal{I}_Y(U) \subset \mathcal{O}_Y(U)[x]$ for every open subset U of Y.

Corollary 1. $\operatorname{Spec}(A)$ *is parametric w.r.t* I *if and only if* I *is monic and in this case the reduced Gröbner basis of* I *over* $\operatorname{Spec}(A)$ *is the reduced Gröbner basis of* I.

Proof: This follows directly from the theorem because $\mathcal{I}_{\operatorname{Spec}(A)}(\operatorname{Spec}(A)) = I$ (see [11], chapter II, proposition 5.1). □

2 Lucky primes and pseudo division

To proceed we will need the concept of pseudo division (cf. [6] and [15]). This is basically just the usual division without fractions. The idea behind pseudo division already appeared in the proof of theorem 5.

Definition 6. *Let* $f, g_1, \ldots, g_m \in A[x]$. *A representation*

$$cf = f_1 g_1 + \cdots + f_m g_m + r$$

is called a pseudo division of f modulo $g_1, \ldots, g_m$ (w.r.t. $<$) *if the following assertions are satisfied:*

- $f_1, \ldots, f_m, r \in A[x]$ *and* $c \in A$ *is a product of leading coefficients of the* g_j*'s.*
- $\operatorname{lt}(f_j)\operatorname{lt}(g_j) \le \operatorname{lt}(f)$ *for* $j = 1, \ldots, m$.
- *No term in* $\operatorname{supp}(r)$ *is divisible by a leading term of the* g_j*'s.*
- $\operatorname{coef}(f_j, t) \in \left\langle \operatorname{coef}(f, t');\ t' \ge \operatorname{lt}(g_j)t \right\rangle$ *for all* $j \in \{1, \ldots, m\}$ *and* $t \in \mathcal{T}$.

r is called a remainder of f after pseudo division modulo $g_1, \ldots, g_m$. A pseudo division of f modulo $g_1, \ldots, g_m$ can be obtained by successively applying pseudo reduction steps:

If there exists a $t \in \operatorname{supp}(f)$ which is divisible by a leading term of any of the g_j's then choose $t \in \operatorname{supp}(f)$ which is maximal with this property. Then $t = t' \operatorname{lt}(g_j)$ holds for some $j \in \{1, \ldots, m\}$ and $t' \in \mathcal{T}$. Now substitute f by

$$\operatorname{lc}(g_j) f - \operatorname{coef}(f, t) t' g_j.$$

Iterating this process and keeping track of the monomials used, we obtain the desired representation.

The nice thing about pseudo reductions is that they are stable under specialization in the sense that

$$\operatorname{lt}(\overline{f_j})\operatorname{lt}(\overline{g_j}) \le \operatorname{lt}(\overline{f})$$

for $j = 1, \ldots, m$. Here $\overline{g}$ denotes the coefficient wise reduction of $g \in A[x]$ modulo some ideal of A. (This follows directly from the last assertion of the definition.)

Definition 7. *A prime ideal of A is called lucky for I if for every $t \in \mathrm{lt}(I)$ it does not contain* $\mathrm{lc}(I, t)$.

To my knowledge the expression lucky was coined by mathematicians working on modular algorithms to compute Gröbner bases over $\mathbb{Q}$ (see [2], [17], [9]). Mod - p arithmetic avoids the phenomenon of coefficient growth but it is not a priori clear which prime numbers p can be used for lifting a Gröbner basis over $\mathbb{Z}/\mathbb{Z}p$ to a Gröbner basis over $\mathbb{Q}$. So mathematicians must have considered themselves lucky if they picked a prime doing the job.

Let T be the unique minimal generating set of $\mathrm{lt}(I)$. Because $\mathrm{lc}(I, t) \subset \mathrm{lc}(I, t')$ if t divides t' a prime $\mathfrak{p} \in \mathrm{Spec}(A)$ is lucky for I if and only if $\mathfrak{p}$ does not contain $\prod_{t \in T} \mathrm{lc}(I, t)$. In particular luckiness is an open condition.

Definition 8. *The ideal*

$$J = J(I) = \sqrt{\prod_{t \in T} \mathrm{lc}(I, t)} \subset A$$

is called the singular ideal of I (w.r.t. $<$).

So a prime $\mathfrak{p} \in \mathrm{Spec}(A)$ is unlucky (i.e. not lucky) for I if and only if it is an element of the singular variety $\mathrm{V}(J)$.

In [20] Weispfenning introduced another discriminant ideal which however can only be constructed if A is an integral domain. So for the time being assume that A is an integral domain. In this case we can consider the reduced Gröbner basis G of I over the quotient field of A. For $g \in G$ the set

$$J_g = \{a \in A;\ ag \in I\}$$

clearly is an ideal of A and we can define Weispfenning's discriminant ideal by

$$J' = \sqrt{\prod_{g \in G} J_g}.$$

Clearly $J_g \subset \mathrm{lc}(I, \mathrm{lt}(g))$ always holds but the inclusion may be strict as illustrated by the following example.

Example 4. *Let k be a field and $A = k[u_1, u_2]$ the polynomial ring in the parameters u_1, u_2. We consider the ideal*

$$I = \langle u_1 x + u_2,\ u_1 y^2 - 1\rangle \subset A[x, y].$$

With respect to any term order the reduced Gröbner basis of I over the quotient field of A is

$$G = \left\{ x + \frac{u_2}{u_1},\ y^2 - \frac{1}{u_1} \right\}.$$

But as $u_2 y^2 + x = y^2(u_1 x + u_2) - x(u_1 y^2 - 1) \in I$ we have w.r.t. any term order with $y^2 > x$

$$J_{y^2 - \frac{1}{u_1}} = \langle u_1\rangle \subsetneqq \langle u_1, u_2\rangle \subset \mathrm{lc}(I, y^2).$$

However our discriminant ideal is not larger than Weispfenning's, in fact they are the same.

Theorem 6. *In the above described situation we have* $J = J'$.

Proof: Let I' denote the extension of I in the polynomial ring over the quotient field of A. First of all observe that $\mathrm{lt}(I) = \mathrm{lt}(I')$: As $I \subset I'$ the inclusion $\mathrm{lt}(I) \subset \mathrm{lt}(I')$ is clear. For the other inclusion it suffices to notice that every $P \in I'$ is of the form $P = \frac{Q}{a}$ with $Q \in I$ and $a \in A$.

Let $G = \{g_1, \ldots, g_m\}$ denote the unique reduced Gröbner basis of I' over the quotient field of A. Then as $\mathrm{lt}(I) = \mathrm{lt}(I')$ the unique minimal generating set T of $\mathrm{lt}(I)$ equals $\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_m)\}$. With the abbreviations $t_j = \mathrm{lt}(g_j)$ and $J_j = J_{g_j}$ for $j = 1, \ldots, m$ we may assume $t_1 < \cdots < t_m$. We have to show

$$\mathrm{V}\left(\mathrm{lc}(I, t_1) \cdots \mathrm{lc}(I, t_m)\right) = \mathrm{V}(J_1 \cdots J_m).$$

As $J_j \subset \mathrm{lc}(I, t_j)$ for $j = 1, \ldots, m$ the inclusion " $\subset$ " is clear. For the other inclusion it will suffice to show that for $j \in \{1, \ldots, m\}$ and $\mathfrak{p} \in \mathrm{Spec}(A)$

$$J_j \subset \mathfrak{p} \ \Rightarrow \ \mathrm{lc}(I, t_1) \cdots \mathrm{lc}(I, t_j) \subset \mathfrak{p}.$$

We will prove this by contradiction. So assume $\mathrm{lc}(I, t_1) \cdots \mathrm{lc}(I, t_j) \not\subset \mathfrak{p}$. Then we can find $f_1, \ldots, f_j \in I$ with $\mathrm{lt}(f_i) = t_i$ and $\mathrm{lc}(f_i) \notin \mathfrak{p}$ for $i = 1, \ldots, j$. Pseudo reduction of f_j modulo $f_1, \ldots, f_{j-1}$ yields a polynomial $g \in I$ with $\mathrm{lt}(g) = t_j$, $\mathrm{lc}(g) \notin \mathfrak{p}$ and no term in $\mathrm{supp}(g)$ divisible by any $t_1, \ldots, t_{j-1}$. So no term in the support of $g - \mathrm{lc}(g) g_j \in I'$ is divisible by any $t_1, \ldots, t_m$. Hence $\mathrm{lc}(g) g_j = g \in I$ and we conclude $\mathrm{lc}(g) \in J_j \subset \mathfrak{p}$ (in contradiction to $\mathrm{lc}(g) \notin \mathfrak{p}$). □

The above theorem asserts that the concept of (in)essential specializations as introduced by Weispfenning in [20] is equivalent to the older concept of (un)lucky prime ideals. The advantage of the idea of luckiness is of course that it works for more general rings, i.e. not only for integral domains. Observe that it is quite natural to work with rings which are not integral domains, because even if you start with an integral domain (e.g. the polynomial ring over a field in some parameters), the singular ideal J will typically not be prime and so A/J will not be an integral domain. The relevance of this will become clear in due time (We will see that the set of all lucky primes of A is parametric).

We will need the following two rather technical lemmas to proof the main theorem of this section, which gives a characterization of parametric subsets in terms of luckiness.

Lemma 2. *Let* $Y \subset \mathrm{Spec}(A)$ *be parametric,* $\mathfrak{a} \subset A$ *the radical ideal such that* $Y = \mathrm{V}(\mathfrak{a})$ *and* $\overline{I}$ *the extension of* I *in* $(A/\mathfrak{a})[x]$. *Furthermore let* $\mathfrak{p} \in Y$ *and* $g \in \mathcal{I}_Y(Y)$ *an element of the reduced Gröbner basis of* I *over* Y. *Then there exists an open neighborhood* $U \subset Y$ *of* $\mathfrak{p}$, $P \in \overline{I}$ *with* $\mathrm{lt}(P) = \mathrm{lt}(g)$ *and* $s \in A/\mathfrak{a}$ *such that* $s \notin \mathfrak{q}$ *and*

$$g(\mathfrak{q}) = \frac{P}{s} \in \overline{I}_{\mathfrak{q}} \text{ for all } \mathfrak{q} \in U.$$

Proof: By definition of $\mathcal{I}_Y$ there exists an open neighborhood $U' \subset Y$ of $\mathfrak{p}$, $P' \in \overline{I}$ and $s' \in A/\mathfrak{a}$ such that $s' \notin \mathfrak{q}$ and $g(\mathfrak{q}) = \frac{P'}{s'} \in \overline{I}_{\mathfrak{q}}$ for all $\mathfrak{q} \in U'$. Now let

$t \in \operatorname{supp}(P')$ be maximal with the property that $\operatorname{coef}(P', t) \notin \mathfrak{p}$. ($\operatorname{coef}(P', t) \in \mathfrak{p}$ for all t would yield $\overline{g}^{\mathfrak{p}} = 0$, which can not be an element of a reduced Gröbner basis.) Then $t = \operatorname{lt}(\overline{g}^{\mathfrak{p}}) = \operatorname{lt}(g)$. Since $\mathfrak{q} \mapsto \operatorname{lt}(\overline{g}^{\mathfrak{q}})$ is constant on U' we have

$$U' \subset \mathrm{V}(\langle \operatorname{coef}(P', t');\ t' > t \rangle).$$

As $\mathfrak{a}$ is assumed to be radical the zero ideal of $A/\mathfrak{a}$ is radical and thus has a unique primary decomposition

$$\langle 0 \rangle = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m.$$

We may assume that the prime ideals $\mathfrak{p}_i \in \operatorname{Spec}(A/\mathfrak{a})$ are numbered in such a way that $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in U'$ and $\mathfrak{p}_{r+1}, \ldots, \mathfrak{p}_m \notin U'$. This means that

$$\mathrm{V}(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r) = \mathrm{V}(\mathfrak{p}_1) \cup \cdots \cup \mathrm{V}(\mathfrak{p}_r) \subset \overline{U'} \subset \mathrm{V}(\langle \operatorname{coef}(P', t');\ t' > t \rangle).$$

Hence $\operatorname{coef}(P', t') \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ for $t' > t$. Note that $\mathfrak{p}_i \notin U'$ is equivalent to $V(\mathfrak{p}_i) \cap U' = \emptyset$, so $\mathfrak{p}_i \not\subseteq \mathfrak{p}$ for $i = r+1, \ldots, m$. This implies that we can find an $s'' \in \mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_m \smallsetminus \mathfrak{p}$. Define $U = \{\mathfrak{q} \in U';\ s'' \notin \mathfrak{q}\}$, $P = s''P'$ and $s = s''s'$, then U is an open neighborhood of $\mathfrak{p}$ in Y and for $t' > t$ we have

$$\operatorname{coef}(P, t') = s'' \operatorname{coef}(P', t') \in \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_m = \langle 0 \rangle,$$

but $\operatorname{coef}(P, t) = s'' \operatorname{coef}(P', t) \notin \mathfrak{p}$. Hence $\operatorname{lt}(P) = t = \operatorname{lt}(g)$ and for all $\mathfrak{q} \in U$ we have $g(\mathfrak{q}) = \frac{P'}{s'} = \frac{P}{s} \in \overline{I}_{\mathfrak{q}}$. □

Lemma 3. *Let $Y \subset \operatorname{Spec}(A)$ be parametric and $\mathfrak{a} \subset A$ the radical ideal such that $\overline{Y} = \mathrm{V}(\mathfrak{a})$. If $\overline{I}$ denotes the extension of I in $(A/\mathfrak{a})[x]$ then $\operatorname{lt}(\mathcal{I}_Y(Y)) = \operatorname{lt}(\overline{I})$.*

Proof: From the above lemma 2 and theorem 5 we know $\operatorname{lt}(\mathcal{I}_Y(Y)) \subset \operatorname{lt}(\overline{I})$. For the reverse inclusion it suffices to show that for $P \in \overline{I}$ the image of P in $\mathcal{I}_Y(Y)$ has the same leading term as P. This is equivalent to saying that the image of $\operatorname{lc}(P)$ in $\mathcal{O}_Y(Y)$ is non zero. So suppose the image of $\operatorname{lc}(P)$ in $\mathcal{O}_Y(Y)$ is zero. Then $\operatorname{lc}(P) \in \mathfrak{p}$ for all $\mathfrak{p} \in Y$ and $Y \subset \{\mathfrak{p} \in \mathrm{V}(\mathfrak{a});\ \operatorname{lc}(P) \in \mathfrak{p}\}$. As the latter set is closed we see that $\operatorname{lc}(P) \in \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{V}(\mathfrak{a})$. Since $\mathfrak{a}$ is radical this yields the contradiction $\operatorname{lc}(P) = 0$. □

Now we are prepared to prove the main theorem of this section. This theorem can also be interpreted as giving the "geometric meaning" of luckiness.

Theorem 7. *Let Y be a locally closed subset of $\operatorname{Spec}(A)$ and $\mathfrak{a} \subset A$ the radical ideal such that $\overline{Y} = \mathrm{V}(\mathfrak{a})$. Denote by $\overline{I}$ the image of I in $(A/\mathfrak{a})[x]$. Then Y is parametric for Gröbner bases w.r.t. I if and only if*

$$Y \cap \mathrm{V}(J(\overline{I})) = \emptyset.$$

In other words: Y is parametric if and only if every $\mathfrak{p} \in Y$ is lucky for $\overline{I}$.

Proof: Assume Y is parametric and $\{g_1, \ldots, g_m\} \subset \mathcal{I}_Y(Y)$ is the reduced Gröbner basis of I over Y. Then by lemma 3 and theorem 5 the minimal generating set T of $\operatorname{lt}(\overline{I})$ equals $\{\operatorname{lt}(g_1), \ldots, \operatorname{lt}(g_m)\}$. Let $\mathfrak{p} \in Y$, then by lemma 2 for $i = 1, \ldots, m$ there exists $P_i \in \overline{I}$ with $\operatorname{lt}(P_i) = \operatorname{lt}(g_i)$ and $s_i \in (A/\mathfrak{a}) \smallsetminus \mathfrak{p}$

such that $g_i(\mathfrak{p}) = \frac{P_i}{s_i} \in \overline{I}_{\mathfrak{p}}$. Because $\operatorname{lt}(P_i) = \operatorname{lt}(g_i) = \operatorname{lt}(\overline{g_i}^{\mathfrak{p}})$ we have $\operatorname{lc}(P_i) \notin \mathfrak{p}$, i.e. $\operatorname{lc}(\overline{I}, \operatorname{lt}(P_i)) \nsubseteq \mathfrak{p}$. Hence

$$J(\overline{I}) = \prod_{t \in T} \operatorname{lc}(\overline{I}, t) \nsubseteq \mathfrak{p}.$$

For the converse direction first fix a $\mathfrak{p} \in Y$ and let $T = \{t_1, \ldots, t_m\}$ denote the minimal generating set of $\operatorname{lt}(\overline{I})$. By assumption

$$\prod_{i=1}^{m} \operatorname{lc}(\overline{I}, t_i) \nsubseteq \mathfrak{p}.$$

Hence there exist polynomials $P_1, \ldots, P_m \in \overline{I}$ with $\operatorname{lt}(P_i) = t_i$ and $\operatorname{lc}(P_i) \notin \mathfrak{p}$. For $i = 1, \ldots, m$ let $Q_i \in \overline{I}$ denote a remainder of P_i after pseudo division modulo $\{P_1, \ldots, P_m\} \setminus \{P_i\}$. Note that $\operatorname{lt}(Q_i) = \operatorname{lt}(P_i) = t_i$ and $\operatorname{lc}(Q_i)$ is a product of leading coefficients of the P_j's. Define

$$U = \{\mathfrak{q} \in Y;\ \operatorname{lc}(P_1) \cdots \operatorname{lc}(P_m) \notin \mathfrak{q}\},$$

then U is an open neighborhood of $\mathfrak{p} \in Y$ and $\frac{Q_i}{\operatorname{lc}(Q_i)}$ defines an element of $\mathcal{I}_Y(U)$ which by abuse of notation we again denote by $\frac{Q_i}{\operatorname{lc}(Q_i)}$.

We can repeat the above construction for any $\mathfrak{p}' \in Y$ to obtain U' and Q_i' (analogously defined). To obtain global sections $g_i \in \mathcal{I}_Y(Y)$ we have to show that

$$\left.\frac{Q_i}{\operatorname{lc}(Q_i)}\right|_{U \cap U'} = \left.\frac{Q_i'}{\operatorname{lc}(Q_i')}\right|_{U \cap U'}.$$

The leading term of

$$\operatorname{lc}(Q_i')Q_i - \operatorname{lc}(Q_i)Q_i' \in \overline{I}$$

is strictly smaller than t_i and by construction no term in the support of $\operatorname{lc}(Q_i')Q_i - \operatorname{lc}(Q_i)Q_i'$ is divisible by an element of $\{t_1, \ldots, t_m\} \setminus \{t_i\}$. Thus $\operatorname{lc}(Q_i')Q_i - \operatorname{lc}(Q_i)Q_i' = 0$ and we can glue together the sections $\frac{Q_i}{\operatorname{lc}(Q_i)} \in \mathcal{I}_Y(U)$ to obtain global sections $g_i \in \mathcal{I}_Y(Y)$.

To show that Y is parametric we will prove that $G = \{g_1, \ldots, g_m\}$ satisfies the conditions of definition 1. Clearly $\operatorname{lt}(\overline{g_i}^{\mathfrak{p}}) = t_i$ for every $\mathfrak{p} \in Y$. So it remains to show that $\overline{G}^{\mathfrak{p}}$ is the reduced Gröbner basis of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ for every $\mathfrak{p} \in Y$. Let $\mathfrak{p} \in Y$ and $P \in \overline{I}$. For a pseudo division (see definition 6)

$$cP = P_1 Q_1 + \cdots + P_m Q_m + r$$

of P modulo $Q_1, \ldots, Q_m$ we have $r \in \overline{I}$, but no term in the support of r is divisible by an element of $\{\operatorname{lt}(Q_1), \ldots, \operatorname{lt}(Q_m)\} = T$. Thus $r = 0$ and

$$cP = P_1 Q_1 + \cdots + P_m Q_m.$$

Let $\phi : (A/\mathfrak{a})[x] \to k(\mathfrak{p})[x]$ denote the natural map then

$$\phi(c)\phi(P) = \phi(P_1)\phi(Q_1) + \cdots + \phi(P_m)\phi(Q_m)$$

and $\operatorname{lt}(\phi(P_i))\operatorname{lt}(\phi(Q_i)) \leq \operatorname{lt}(\phi(P))$. Since $\operatorname{lc}(Q_i) \notin \mathfrak{p}$ and c is a product of leading coefficients of the Q_i's we know that $\phi(c), \phi(\operatorname{lc}(Q_1)), \ldots, \phi(\operatorname{lc}(Q_m))$ are all non zero. Consequently $\mathrm{lt}(\phi(P))$ is divisible by $\mathrm{lt}(\phi(Q_i)) = t_i$ for some $i \in \{1, \dots, m\}$. Since every element of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ is of the form λf for $\lambda \in k(\mathfrak{p})$ and $f \in \phi(\overline{I}) = \sigma_{\mathfrak{p}}(I)$ this shows that $\mathrm{lt}(\langle \sigma_{\mathfrak{p}}(I) \rangle)$ is generated by T and so indeed $\overline{G}^{\mathfrak{p}}$ is a Gröbner basis of $\langle \sigma_{\mathfrak{p}}(I) \rangle$. $\overline{g_i}^{\mathfrak{p}}$ is clearly monic and by construction of the Q_i's no term in the support of $\overline{g_i}^{\mathfrak{p}}$ is divisible by an element of $T \setminus \{t_i\}$. Thus $\overline{G}^{\mathfrak{p}}$ is the reduced Gröbner basis of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ and we are done. □

Definition 9. *Let Z be a closed subset of* $\mathrm{Spec}(A)$ *and $\mathfrak{a} \subset A$ the radical ideal such that $Z = \mathrm{V}(\mathfrak{a})$. Let furthermore $\overline{I}$ denote the extension of I in $(A/\mathfrak{a})[x]$, then we define*

$$Z_{gen} = Z \setminus \mathrm{V}(J(\overline{I})).$$

Theorem 8. *Let $Z \subset \mathrm{Spec}(A)$ be closed, $\mathfrak{a} \subset A$ the radical ideal such that $Z = \mathrm{V}(\mathfrak{a})$ and $\overline{I}$ the extension of I in $(A/\mathfrak{a})[x]$. Then Z_{gen} is parametric with $\mathrm{lt}(\mathcal{I}_{Z_{gen}}(Z_{gen})) = \mathrm{lt}(\overline{I})$. Furthermore if Y is an open subset of Z such that Y is parametric with $\mathrm{lt}(\mathcal{I}_Y(Y)) = \mathrm{lt}(\overline{I})$ then $Y \subset Z_{gen}$.*

In other words: Z_{gen} is the largest open parametric subset of Z with the same leading terms as $\overline{I}$.

Proof: To show that Z_{gen} is parametric with the same leading terms as $\overline{I}$, just repeat the second part of the proof of theorem 7 (with Z_{gen} instead of Y) and use that $\mathcal{I}_Z(Z_{gen})$ is canonically isomorphic to $\mathcal{I}_{Z_{gen}}(Z_{gen})$.

Now let Y be an open and parametric subset of Z with $\mathrm{lt}(\mathcal{I}_Y(Y)) = \mathrm{lt}(\overline{I})$ and assume $Y \not\subseteq Z_{gen}$. Then there exist a $\mathfrak{p} \in Y \setminus Z_{gen}$. Let T denote the minimal generating set of $\mathrm{lt}(\overline{I})$. Since $\mathfrak{p} \notin Z_{gen} = Z \setminus \mathrm{V}(J(\overline{I}))$ there exists a $t \in T$ such that $\mathrm{lc}(\overline{I}, t) \subset \mathfrak{p}$.

Let $\mathfrak{a}' \subset A$ be the radical ideal such that $\overline{Y} = \mathrm{V}(\mathfrak{a}')$ then $\mathfrak{a} \subset \mathfrak{a}'$ and we have a canonical map $\phi : (A/\mathfrak{a})[x] \to (A/\mathfrak{a}')[x]$. Let $\overline{I}'$ denote the extension of I in $(A/\mathfrak{a}')[x]$ then $\phi(\overline{I}) = \overline{I}'$. Since $\mathrm{lt}(\mathcal{I}_Y(Y)) = \mathrm{lt}(\overline{I})$ there exist a $g \in G_Y$ with $\mathrm{lt}(g) = t$. By lemma 2 there exist a $Q \in \overline{I}'$ with $\mathrm{lt}(Q) = t$ and $s \in A/\mathfrak{a}' \setminus \mathfrak{p}$ such that

$$g(\mathfrak{p}) = \frac{Q}{s} \in \overline{I}'_{\mathfrak{p}}.$$

Let $\mathfrak{a} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_m$ be the unique minimal primary decomposition of $\mathfrak{a}$ and $P \in \overline{I}$ such that $\phi(P) = Q$. Since $\mathrm{lc}(Q) \notin \mathfrak{p}$ we know that $\mathrm{coef}(P, t) \notin \mathfrak{p}$ and that $\mathrm{coef}(P, t')$ lies in the extension of $\mathfrak{a}'$ in $A/\mathfrak{a}$ for $t' > t$. We may assume that the $\mathfrak{p}_i$'s are numbered in such a way that $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in Y$ and $\mathfrak{p}_{r+1}, \dots, \mathfrak{p}_m \notin Y$. Note that $\mathfrak{p}_i \notin Y$ implies $\mathrm{V}(\mathfrak{p}_i) \cap Y = \emptyset$ because Y is an open subset of Z. So in particular $\mathfrak{p}_i \not\subseteq \mathfrak{p}$ for $i = r+1, \dots, m$. This implies that there exists an $s' \in \mathfrak{p}_{r+1} \cap \dots \cap \mathfrak{p}_m \setminus \mathfrak{p}$. For $1 \le i \le r$ we have $\mathrm{V}(\mathfrak{p}_i) \subset \overline{Y} = \mathrm{V}(\mathfrak{a}')$ and thus $\mathfrak{a}' \subset \mathfrak{p}_i$. Let s'' denote the image of s' in $A/\mathfrak{a}$, then for $t' > t$ we have $\mathrm{coef}(s''P, t') = 0$ since $\mathrm{coef}(s''P, t')$ is contained in every $\mathfrak{p}_i$ for $i = 1, \dots, m$. On the other side $\mathrm{coef}(s''P, t) \notin \mathfrak{p}$, thus $\mathrm{lt}(s''P) = t$ and $\mathrm{lc}(s''P) \notin \mathfrak{p}$ in contradiction to $\mathrm{lc}(\overline{I}, t) \subset \mathfrak{p}$. □

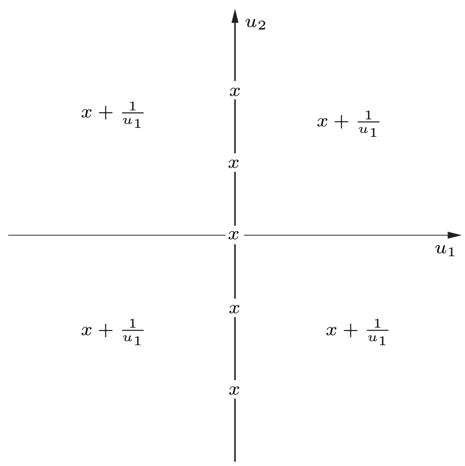
If we take $Z = \mathrm{Spec}(A)$ in the above theorem, then we see that the set of all lucky primes of A ($= \mathrm{Spec}(A) \setminus \mathrm{V}(J(I))$) is the largest open parametric subset of $\mathrm{Spec}(A)$ with the same leading terms as I. This more or less comes down to saying that J is the optimal discriminant ideal.

Caution: It is not true that $\mathfrak{p} \in \operatorname{Spec}(A)$ is lucky for I if and only if $\operatorname{lt}(I) = \operatorname{lt}(\langle\sigma_{\mathfrak{p}}(I)\rangle)$. We have seen above that the "only if" direction is correct but the following example illustrates the failure of the "if" direction. In fact this example illustrates that knowing $\operatorname{lt}(\langle\sigma_{\mathfrak{p}}(I)\rangle)$ for every $\mathfrak{p} \in \operatorname{Spec}(A)$ is completely insufficient to understand the Gröbner basis structure of the fibres.

Example 5. *Let k be a field and $A = k[u_1, u_2]$ the polynomial ring in the two parameters u_1, u_2. Consider the ideal*

$$I = \big\langle u_1(u_1 x + 1), (u_1 x + 1)x \big\rangle \subset A[x].$$

(In this example x denotes just one variable.) $\operatorname{lt}(\langle\sigma_{\mathfrak{p}}(I)\rangle)$ *is generated by x for every $\mathfrak{p} \in \operatorname{Spec}(A)$ but clearly* $\operatorname{Spec}(A)$ *is not parametric. The corresponding picture picture would be:*



The following simple example illustrates that Z_{gen} may well be the empty set.

Example 6. *Assume that A is not an integral domain, then there exist $a, b \in A \setminus \{0\}$ such that $ab = 0$. If we take I to be the ideal of $A[x_1, x_2]$ generated by ax_1 and bx_2 then (w.r.t. any term order) $J(I) = \langle 0\rangle$ and so* $\operatorname{Spec}(A)_{gen} = \emptyset$.

However this can not happen if Z is irreducible, because then $Z = \mathrm{V}(\mathfrak{a})$ for some prime ideal $\mathfrak{a}$ of A and since $A/\mathfrak{a}$ is an integral domain $J(\overline{I})$ is not the zero ideal and thus Z_{gen} is non empty. In particular Z_{gen} is dense in Z and contains the generic point of Z.

The following examples have been included to convince the reader that the singular ideal J is quite a reasonable object.

Example 7. *Let $I \subset A[x]$ be the ideal generated by a square linear system*

$$\begin{aligned} P_1 &= b_{11}x_1 + b_{12}x_2 + \cdots + b_{1n}x_n - c_1 \\ &\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ P_n &= b_{n1}x_1 + b_{n2}x_2 + \cdots + b_{nn}x_n - c_n \end{aligned}$$

and let

$$B = \big(b_{ij}\big)_{1 \le i,j \le n} \in A^{n \times n}$$

denote the matrix of the system. Suppose $\det = \det(B) \in A$ *is not a zero divisor, then the singular ideal* J *of* I *is independent of the chosen term order and* $\mathrm{V}(J)$ *equals* $\mathrm{V}(\det)$*. In other words* $J = \sqrt{\langle \det \rangle}$*.*

Proof: Let $B' \in A^{n\times n}$ denote the adjoint matrix of B. A classical linear algebra theorem (see e.g. [13], chapter 8, § 4, proposition 8) asserts that

$$B'B = BB' = \det \cdot \mathbb{I}, \tag{1}$$

where $\mathbb{I}$ denotes the $n \times n$ identity matrix.

First we show that $1 \notin \mathrm{lt}(I)$. Suppose the contrary. Let A' denote the total ring of fractions of A, i.e. the localization at the multiplicative subset of all non zero divisors, then we may regard A as a subring of A'. With the abbreviations

$$c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \text{ and } \xi = \frac{1}{\det} \cdot B'c$$

identity (1) shows that ξ is a solution to our linear system. Now $1 \in \mathrm{lt}(I)$ simply means that there exist an $a \in A \smallsetminus \{0\}$ and $Q_1, \ldots, Q_n \in A[x]$ such that

$$Q_1P_1 + \cdots + Q_nP_n = a.$$

Evaluation at ξ yields the contradiction $a = 0$.

Identity (1) also shows that det lies in $\mathrm{lc}(I, x_i)$ for $i = 1, \ldots, m$. Therefore $\det \in J$ and $\mathrm{V}(J) \subset \mathrm{V}(\det)$. Now for the reverse inclusion assume $\mathfrak{p} \in \mathrm{V}(\det)$, i.e. $\det \in \mathfrak{p}$. From theorem 8 we know that for every $\mathfrak{q} \in \mathrm{Spec}(A) \smallsetminus \mathrm{V}(J)$ the leading terms of $\langle \sigma_{\mathfrak{q}}(I) \rangle$ are generated by $x_1, \ldots, x_n$. But $\det \in \mathfrak{p}$ implies that $\mathrm{lt}(\langle \sigma_{\mathfrak{p}}(I) \rangle)$ is not generated by $x_1, \ldots, x_n$ and consequently $\mathfrak{p} \in \mathrm{V}(J)$. □

Example 8. *Let* k *be a field and* $I' \subset k[x] = k[x_1, \ldots, x_n]$ *a (homogeneous) ideal. For* $1 \le i, j \le n$ *let* u_{ij} *be additional indeterminates and abbreviate*

$$ux = (u_{11}x_1 + \cdots + u_{n1}x_n, \ldots\ldots, u_{1n}x_1 + \cdots + u_{nn}x_n).$$

Let A *be the polynomial ring over* k *in the* u_{ij}*'s and define*

$$I = \langle P(ux);\ P \in I' \rangle \subset A[x].$$

Then for $\mathfrak{p} \in \mathrm{Spec}(A)_{gen}$ *the ideal of* $k[x]$ *generated by* $\mathrm{lt}(\langle \sigma_{\mathfrak{p}}(I) \rangle)$ *is the generic initial ideal of* I' *usually denoted by* $\mathrm{Gin}(I')$ *(see e.g. [7] or [10]).*

Example 9. *Suppose that* $<$ *is a graded order and* A *is an integral domain, i.e.* $\mathrm{Spec}(A)$ *is irreducible, then* $\mathrm{Spec}(A)_{gen}$ *is a non empty, open (and thus dense) subset of* $\mathrm{Spec}(A)$ *such that the function*

$$\mathfrak{p} \mapsto \textit{affine Hilbert function of } \langle \sigma_{\mathfrak{p}}(I) \rangle$$

is constant on $\mathrm{Spec}(A)_{gen}$*. This is clear because the affine Hilbert function of* $\langle \sigma_{\mathfrak{p}}(I) \rangle$ *is determined by* $\mathrm{lt}(\langle \sigma_{\mathfrak{p}}(I) \rangle)$ *(see [6], chapter 9, § 3, proposition 4). Of course there is an analogous "projective" statement.*

3 Gröbner covers

Now that we have (at least to some extend) explored the nature of parametric sets, it is time to see the complete picture.

Definition 10. *Let L be a locally closed subset of* $\operatorname{Spec}(A)$. *A finite set $\mathcal{G}$ consisting of pairs (Y, G_Y) with $Y \subset \operatorname{Spec}(A)$ parametric and G_Y the reduced Gröbner bases of I over Y is called a* Gröbner cover of L w.r.t. I (and $<$) *if*

$$L = \bigcup_{Y \in \mathcal{G}} Y.$$

A Gröbner cover $\mathcal{G}$ is called irreducible *if every $Y \in \mathcal{G}$ is irreducible.*

A Gröbner cover $\mathcal{G}$ of L is called locally maximal *if for every $Y \in \mathcal{G}$ the following holds: If $Y' \subset \operatorname{Spec}(A)$ is parametric with $Y' \subset L$ and $Y \subset Y' \subset \overline{Y}$ then $Y = Y'$.*

A Gröbner cover $\mathcal{G}$ is called small *if for every $Y \in \mathcal{G}$ we have*

$$\overline{Y \setminus \bigcup_{Y' \in \mathcal{G} \setminus \{Y\}} Y'} = \overline{Y}.$$

As already in the above definition we write $Y \in \mathcal{G}$ instead of unhandy $(Y, G_Y) \in \mathcal{G}$ and refer to Y as an element of $\mathcal{G}$. To say that a Gröbner cover is small basically means that its elements are not unnecessarily large. Our main interest of course is in Gröbner covers of $\operatorname{Spec}(A)$ but (with a view towards applications) it seems reasonable to also treat the relative case.

Definition 11. *Let L be a locally closed subset of* $\operatorname{Spec}(A)$ *and G a finite subset of I. G is called a* comprehensive Gröbner basis of I w.r.t. L (and $<$) *if $\sigma_{\mathfrak{p}}(G) = \{\sigma_{\mathfrak{p}}(g);\ g \in G\}$ is a Gröbner basis of $\langle \sigma_{\mathfrak{p}}(I) \rangle$ for every $\mathfrak{p} \in L$.*

Comprehensive Gröbner bases were introduced by Weispfenning in [19] and advanced in [20]. There is a rather obvious connection between Gröbner covers of L and comprehensive Gröbner bases of I w.r.t. L which we will now describe.

Let $\mathcal{G}$ be a Gröbner cover of L. Choose a $Y \in \mathcal{G}$ and let $\mathfrak{a} \subset A$ be the radical ideal such that $\overline{Y} = \mathrm{V}(\mathfrak{a})$, furthermore let $\overline{I}$ denote the image of I in $(A/\mathfrak{a})[x]$. Since $\operatorname{Spec}(A)$ is a noetherian topological space Y is quasi-compact and so for every $g \in G_Y$ we can find finitely many open subsets U_i of Y which cover Y and have the following property: There exists a $P \in I$ and $s \in A/\mathfrak{a}$ such that

$$g(\mathfrak{p}) = \frac{\overline{P}}{s} \in \overline{I}_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in U_i.$$

Here $\overline{P}$ denotes the image of P in $\overline{I} \subset (A/\mathfrak{a})[x]$. Now taking together all such P's (for all U_i's, all $g \in G_Y$ and all $Y \in \mathcal{G}$) we end up with a finite subset of I which clearly is a comprehensive Gröbner basis of I w.r.t. L.

The main theorem of this section asserts that for every locally closed subset L of $\operatorname{Spec}(A)$, there exists a unique irreducible, small and locally maximal Gröbner cover of L. For the proof we will need a few basic facts about constructible sets (cf. [11]).

Definition 12. *Let X be a topological space. A constructible subset of X is a subset which belongs to the smallest family $\mathfrak{F}$ of subsets such that*

(1) *every open subset is in $\mathfrak{F}$,*

(2) *a finite intersection of elements in $\mathfrak{F}$ is in $\mathfrak{F}$, and*

(3) *the complement of an element in $\mathfrak{F}$ is in $\mathfrak{F}$.*

One easily shows that the constructible sets of a topological space are exactly the finite unions of locally closed sets.

Lemma 4. *Let C be a constructible subset of* $\mathrm{Spec}(A)$ *and*

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

the unique minimal decomposition of $\overline{C}$ into irreducible and closed sets. Then for $j = 1, \ldots, m$ there exists a non empty open subset of Z_j contained in C.

Proof: A constructible set C can be written as a finite union

$$C = L_1 \cup \cdots \cup L_{m'}$$

of non empty, locally closed and irreducible sets L_i.

$$Z_1 \cup \cdots \cup Z_m = \overline{C} = \overline{L_1} \cup \cdots \cup \overline{L_{m'}}$$

Fix a $j \in \{1, \ldots, m\}$. As Z_j is irreducible there exists an $i \in \{1, \ldots, m'\}$ such that $Z_j \subset \overline{L_i}$. Similarly, as $\overline{L_i}$ is irreducible there exist a $j' \in \{1, \ldots, m\}$ such that $\overline{L_i} \subset Z_{j'}$. Hence

$$Z_j \subset \overline{L_i} \subset Z_{j'}.$$

This yields $j = j'$ and $Z_j = \overline{L_i}$. So L_i is a non empty open subset of Z_j contained in C. □

Lemma 5. *Let L be a locally closed and irreducible subset of* $\mathrm{Spec}(A)$. *For a constructible subset C of* $\mathrm{Spec}(A)$ *which is contained in L we have $\overline{C} = \overline{L}$ if and only if C contains the generic point of L.*

Proof: If C contains the generic point $\mathfrak{p}$ of L we have $\overline{L} = \overline{\{\mathfrak{p}\}} \subset \overline{C}$. Hence by assumption $\overline{L} = \overline{C}$.

Conversely if $\overline{C} = \overline{L}$ by Lemma 4 we know that there exists a nonempty open subset U of $\overline{L}$ contained in C. As $U \cap L$ is a non empty open subset of L we have

$$\mathfrak{p} \in U \cap L \subset C.$$

□

Theorem 9. *Let $L \subset$ $\mathrm{Spec}(A)$ be a locally closed set and $\mathcal{G}$ an irreducible Gröbner cover of L. The following are equivalent:*

(1) *$\mathcal{G}$ is small.*

(2) *Every $Y \in \mathcal{G}$ is the only element of $\mathcal{G}$ containing the generic point of Y.*

(3) *For $Y, Y' \in \mathcal{G}$ with $Y \neq Y'$ and $Y \subset \overline{Y'}$ we have $Y \cap Y' = \emptyset$.*

Proof: The equivalence of (1) and (2) follows from lemma 5.

For two distinct, locally closed and irreducible subsets Y and Y' of $\mathrm{Spec}(A)$ the generic point of Y is contained in Y' if and only if $Y \subset \overline{Y'}$ and $Y \cap Y' \neq \emptyset$. Therefore (3) is equivalent to (2). □

Now we are prepared to prove the main theorem.

Theorem 10. *Let L be a locally closed subset of* $\mathrm{Spec}(A)$*. Then there exists exactly one irreducible, small and locally maximal Gröbner cover of L.*

Proof: First we will construct a Gröbner cover $\mathcal{G}$ of L and prove that it has the desired properties. Then we will prove uniqueness. We construct $\mathcal{G}$ recursively:

> Set $C_1 = L$ and $i = 1$.
> ($\star$) Let
> $$\overline{C_i} = Z_{i1} \cup \cdots \cup Z_{im_i}$$
> be the unique minimal decomposition of $\overline{C_i}$ into irreducible and closed sets. For $j = 1, \ldots, m_i$ define
> $$Y_{ij} = Z_{ij,gen} \cap \big(\text{union of all open subsets of } Z_{ij} \text{ contained in } L\big)$$
> and
> $$C_{i+1} = C_i \setminus (Y_{i1} \cup \cdots \cup Y_{im_i}).$$
> If $C_{i+1} \neq \emptyset$ substitute i by $i+1$ and go to ($\star$).

This yields a sequence of constructible sets C_i with

$$L = C_1 \supset C_2 \supset \cdots .$$

To prove termination we will show that the sequence

$$\overline{C_1} \supset \overline{C_2} \supset \cdots$$

is strictly decreasing. For $i \geq 1$ and $j = 1, \ldots, m_i$ by lemma 4 there exists a non empty open subset of Z_{ij} contained in $C_i \subset L$. Hence Y_{ij} is a non empty open subset of Z_{ij} contained in L.

$$\begin{aligned}\overline{C_{i+1}} &= \overline{C_i \setminus (Y_{i1} \cup \cdots \cup Y_{im_i})} \subset \overline{Z_{i1} \cup \cdots \cup Z_{im_i} \setminus Y_{i1} \cup \cdots \cup Y_{im_i}} \\ &\subset \overline{(Z_{i1} \setminus Y_{i1}) \cup \cdots \cup (Z_{im_i} \setminus Y_{im_i})} = (Z_{i1} \setminus Y_{i1}) \cup \cdots \cup (Z_{im_i} \setminus Y_{im_i}) \\ &\subsetneq Z_{i1} \cup \cdots \cup Z_{im_i} = \overline{C_i}\end{aligned}$$

This shows that there exists a (minimal) $r \in \mathbb{N}$ such that $C_{r+1} = \emptyset$. Hence

$$\begin{aligned}\emptyset &= C_{r+1} = C_r \setminus (Y_{r1} \cup \cdots \cup Y_{rm_r}) \\ &= C_{r-1} \setminus (Y_{r-1,1} \cup \cdots \cup Y_{r-1,m_{r-1}} \cup Y_{r1} \cup \cdots \cup Y_{rm_r}) = \cdots \\ &= C_1 \setminus (Y_{11} \cup \cdots \cup Y_{1m} \cup \cdots \cup Y_{r1} \cup \cdots \cup Y_{rm_r}).\end{aligned}$$

So we obtain

$$L = C_1 = Y_{11} \cup \cdots \cup Y_{1m} \cup \cdots \cup Y_{r1} \cup \cdots \cup Y_{rm_r}.$$

As the Y_{ij}'s are parametric by construction this shows that

$$\mathcal{G} = \{(Y_{ij}, G_{Y_{ij}})\ ;\ 1 \le i \le r,\ 1 \le j \le m_i\}$$

is a Gröbner cover of L. It is clearly irreducible. Next we will show that $\mathcal{G}$ is locally maximal. So let $Y \subset L$ be parametric with

$$Y_{ij} \subset Y \subset \overline{Y_{ij}} = Z_{ij}.$$

Then Y is an open parametric subset of Z_{ij} and so by theorem 8 we have $Y \subset Z_{ij,gen}$. From the definition of Y_{ij} we obtain $Y \subset Y_{ij}$ and thus $Y = Y_{ij}$.

Now we will show that $\mathcal{G}$ is small. Let $Y_{ij}, Y_{i'j'} \in \mathcal{G}$ with $(i,j) \ne (i',j')$.

We want to show that for $i \le i'$ we have $Y_{ij} \not\subset \overline{Y_{i'j'}}$. Assume the contrary. Then

$$\overline{Y_{i'j'}} = Z_{i'j'} \subset \overline{C_{i'}} \subset \overline{C_i} = Z_{i1} \cup \dots \cup Z_{im_i}.$$

Consequently there exists an $l \in \{1, \dots, m_i\}$ such that $Z_{i'j'} \subset Z_{il}$. This yields

$$Z_{ij} = \overline{Y_{ij}} \subset \overline{Y_{i'j'}} = Z_{i'j'} \subset Z_{il}.$$

Therefore $j = l$ and $Z_{ij} = Z_{i'j'}$. For $i = i'$ this directly gives the contradiction $j = j'$. For $i < i'$ we have

$$Z_{ij} = Z_{i'j'} \subset \overline{C_{i'}} \subset \overline{C_{i+1}} \subset (Z_{i1} \setminus Y_{i1}) \cup \dots \cup (Z_{im_i} \setminus Y_{im_i}).$$

Consequently $Z_{ij} \subset Z_{ij} \setminus Y_{ij}$ and we obtain the contradiction $Y_{ij} = \emptyset$.

Now to prove that $\mathcal{G}$ is small by theorem 9 it suffices to show that for $i > i'$ and $Y_{ij} \subset \overline{Y_{i'j'}}$ we have $Y_{ij} \cap Y_{i'j'} = \emptyset$. Note that $Y_{ij} \subset \overline{Y_{i'j'}}$ implies that $Z_{ij} \setminus Y_{i'j'}$ is a closed subset of $\mathrm{Spec}(A)$. By construction we have

$$C_i = C_{i'} \setminus \big(Y_{i'1} \cup \dots \cup Y_{i'm_{i'}} \cup \dots \cup Y_{i-1,1} \cup \dots \cup Y_{i-1,m_{i-1}}\big). \tag{2}$$

For subsets B, C, D of an arbitrary topological space with $D \subset C$ there is the trivial identity

$$\overline{\overline{B \setminus C} \setminus D} = \overline{B \setminus C}.$$

Together with (2) this yields

$$\begin{aligned} \overline{C_i} &= \overline{\overline{C_i} \setminus Y_{i'j'}} = \overline{Z_{i1} \cup \dots \cup Z_{im_i} \setminus Y_{i'j'}} \subset \overline{Z_{i1} \cup \dots \cup (Z_{ij} \setminus Y_{i'j'}) \cup \dots \cup Z_{im_i}} \\ &= Z_{i1} \cup \dots \cup (Z_{ij} \setminus Y_{i'j'}) \cup \dots \cup Z_{im_i} \subset Z_{i1} \cup \dots \cup Z_{im_i} = \overline{C_i}. \end{aligned}$$

Therefore

$$Z_{i1} \cup \dots \cup Z_{im_i} = Z_{i1} \cup \dots \cup (Z_{ij} \setminus Y_{i'j'}) \cup \dots \cup Z_{im_i}$$

and $Z_{ij} \subset Z_{ij} \setminus Y_{i'j'}$. Thus $Y_{ij} \cap Y_{i'j'} = \emptyset$.

So far we have shown that $\mathcal{G}$ is an irreducible, small and locally maximal Gröbner cover of L. It remains to prove uniqueness. Assume $\mathcal{G}'$ is another irreducible, small and locally maximal Gröbner cover of L. First we will show $\mathcal{G} \subset \mathcal{G}'$. More precisely by induction on $i = 1, \dots, r$ we will show that $Y_{i1}, \dots, Y_{im_i} \in \mathcal{G}'$. We denote the generic point of Y_{ij} by $\mathfrak{p}_{ij}$.

First assume $i = 1$. Let $j \in \{1, \dots, m_1\}$. As

$$\bigcup_{Y \in \mathcal{G}} Y = L = \bigcup_{Y' \in \mathcal{G}'} Y'$$

there exists a $Y'_{1j} \in \mathcal{G}'$ such that $\mathfrak{p}_{1j} \in Y'_{1j}$. We want to show $Y_{1j} = Y'_{1j}$. As Y'_{1j} is irreducible and $\overline{Y'_{1j}} \subset \overline{L} = Z_{11} \cup \dots \cup Z_{1m_1}$ there exist a $j' \in \{1, \dots, m_1\}$ such that $\overline{Y'_{1j}} \subset Z_{1j'}$. Together with $\mathfrak{p}_{1j} \in Y'_{1j}$ this gives

$$Z_{1j} \subset \overline{Y'_{1j}} \subset Z_{1j'}.$$

Therefore $j = j'$ and $\overline{Y'_{1j}} = Z_{1j}$. Thus Y'_{1j} is an open subset of Z_{1j} contained in L and by theorem 8 $Y'_{1j} \subset Z_{1j,gen}$. So by definition of Y_{1j} we have $Y'_{1j} \subset Y_{1j}$. Since $\mathcal{G}'$ is locally maximal we obtain $Y_{1j} = Y'_{1j} \in \mathcal{G}'$.

Now we do the induction step. Suppose

$$Y_{11}, \dots, Y_{1m_1}, \dots, Y_{i-1,1}, \dots, Y_{i-1,m_{i-1}} \in \mathcal{G}'.$$

We have to show $Y_{i1}, \dots, Y_{im_i} \in \mathcal{G}'$. For $j \in \{1, \dots, m_i\}$ there exists a $Y'_{ij} \in \mathcal{G}'$ such that $\mathfrak{p}_{ij} \in Y'_{ij}$. Using that $\mathcal{G}'$ is small and the induction hypothesis we obtain

$$\overline{Y'_{ij}} = \overline{Y'_{ij} \smallsetminus \bigcup_{Y' \in \mathcal{G}' \smallsetminus \{Y'_{ij}\}} Y'} \subset \overline{L \smallsetminus \bigcup_{\substack{1 \le i' \le i-1 \\ 1 \le j' \le m_{i'}}} Y_{i'j'}} = \overline{C_i} = Z_{i1} \cup \dots \cup Z_{im_i}.$$

Hence there exists a $j' \in \{1, \dots, m_i\}$ such that $\overline{Y'_{ij}} \subset Z_{ij'}$. Together with $\mathfrak{p}_{ij} \in Y'_{ij}$ this gives

$$Z_{ij} \subset \overline{Y'_{ij}} \subset Z_{ij'}.$$

Therefore $j = j'$ and $\overline{Y'_{ij}} = Z_{ij}$. Now using that $\mathcal{G}'$ is locally maximal, a similar argument as for the case $i = 1$ above, proves $Y_{ij} = Y'_{ij} \in \mathcal{G}'$. Thus we have shown $\mathcal{G} \subset \mathcal{G}'$.

Assume this is a proper inclusion. Then there exist a $Y' \in \mathcal{G}'$ such that $Y' \notin \mathcal{G}$ and therefore

$$\overline{Y'} = \overline{Y' \smallsetminus \bigcup_{Y \in \mathcal{G}' \smallsetminus \{Y'\}} Y} \subset \overline{Y' \smallsetminus \bigcup_{Y \in \mathcal{G}} Y} = \overline{Y' \smallsetminus L} = \emptyset.$$

This is a contradiction as by definition the empty set is not irreducible. □

Definition 13. *Let L be a locally closed subset of* Spec(A)*. The uniquely determined irreducible, small and locally maximal Gröbner cover of L is called the* canonical irreducible Gröbner cover of L (w.r.t. I and $<$).

In [20] Weispfenning gave a rather ad hoc kind of construction for what he called canonical Gröbner systems. This construction bears some analogy with the existence proof of the above theorem, however there are some differences between the concept of canonical Gröbner systems and the concept of canonical irreducible Gröbner covers. For example the canonical Gröbner system may contain redundant elements. The persistent reader is invited to verify this with the example $A = k[u_1, u_2]$ and $I = \langle u_1 u_2, u_1 x^2 + x\rangle$. (The point is simply that if $\mathrm{Spec}(A) = Z_1 \cup \cdots \cup Z_m$ is the decomposition of $\mathrm{Spec}(A)$ into irreducible closed sets, then it may happen that the singular part of Z_i ($= Z_i \setminus Z_{i,gen}$) is contained in some $Z_{j,gen}$.)

Note that theorem 10 implies that the equivalence relation on $\mathrm{Spec}(A)$, given by comparing the leading terms of $\langle \sigma_{\mathfrak{p}}(I)\rangle$, has only finitely many equivalence classes and that every equivalence class is a constructible set. Indeed the next example shows that these equivalence classes are only constructible and not locally closed. The following example also illustrates that the canonical irreducible Gröbner cover may not be of minimal cardinality compared to all other irreducible Gröbner covers.

Example 10. *Let k be a field and $A = k[u_1, u_2]$ the polynomial ring in the two parameters u_1, u_2. We consider the ideal*

$$I = \langle u_1 x, (u_2^2 - 1)x^2 + x\rangle \subset A[x].$$

(Here x denotes just one variable.) Obviously $J = J(I) = \langle u_1\rangle$ and the affine plane without the u_2-axis has generic Gröbner basis x, i.e. $Y_1 = \mathbb{A}^2_{gen} = \mathrm{Spec}(A) \setminus \mathrm{V}(u_1)$ and $x \in \mathcal{I}_{Y_1}(Y_1) = I_{u_1}$ (= localization of I at $\{1, u_1, u_1^2, \ldots\}$) is the reduced Gröbner basis of I over Y_1. By factoring mod $J = \langle u_1\rangle$ and identifying A/J with $k[u_2]$ we obtain

$$\overline{I} = \langle (u_2^2 - 1)x^2 + x\rangle \subset k[u_2][x].$$

On the u_2-axis the generic Gröbner basis is $x^2 + \frac{1}{u_2^2-1}x$, i.e.

$$J(\overline{I}) = \langle u_2^2 - 1\rangle = \langle u_2 + 1\rangle \cap \langle u_2 - 1\rangle,$$

$Y_2 = \mathrm{V}(u_1)_{gen} = \mathrm{V}(u_1) \setminus \mathrm{V}(u_2^2 - 1)$ and $x^2 + \frac{1}{u_2^2-1}x \in \mathcal{I}_{Y_2}(Y_2) = \overline{I}_{u_2^2-1}$ is the reduced Gröbner bases of I over Y_2. Finally over the two closed points $Y_3 = \langle u_1, u_2 - 1\rangle$ and $Y_4 = \langle u_1, u_2 + 1\rangle$ we have the reduced Gröbner basis x again. To summarize

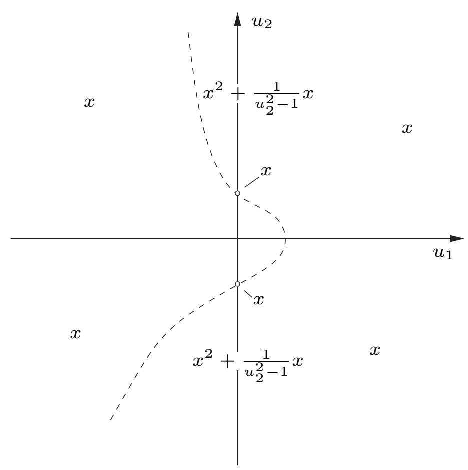
$$\mathcal{G} = \big\{(Y_1, \{x\}), (Y_2, \{x^2 + \tfrac{1}{u_2^2-1}x\}), (Y_3, \{x\}), (Y_4, \{x\})\big\}$$

is the canonical irreducible Gröbner cover of $\mathbb{A}^2 = \mathrm{Spec}(A)$.

Let $f \in k[u_1, u_2]$ be an irreducible polynomial such that $f(0, u_2) = u_2^2 - 1$ (e.g. $f = u_1 + u_2^2 - 1$). Then there exist $h \in A = k[u_1, u_2]$ such that $f = hu_1 + u_2^2 - 1$, thus $fx^2 + x = (hx)(u_1 x) + (u_2^2 - 1)x^2 + x \in I$. Therefore the extension of I in $(A/\langle f\rangle)[x]$ is just $\langle x\rangle$ and $\mathrm{V}(f)$ is parametric with reduced Gröbner basis x. Consequently

$$\mathcal{G}' = \{(Y_1, \{x\}), (Y_2, \{x^2 + \tfrac{1}{u_2^2-1}x\}), (\mathrm{V}(f), x)\}$$

is an irreducible Gröbner cover of $\mathbb{A}^2$ with smaller cardinality then the canonical irreducible Gröbner cover. However choosing an irreducible Gröbner cover of $\mathrm{Spec}(A)$ with minimal cardinality in a canonical way, is as impossible as choosing a curve which meets the u_2-axes only in $(0, -1)$ and $(0, 1)$ in a canonical way.



The above example also can be used to show that a parametric subset of Spec(A) need not be contained in a maximal parametric subset.

Conclusion and open questions

We have introduced two concepts for studying the geometry of fibres: parametric sets and Gröbner covers. It seems possible to generalize these notions to more general (i.e. not necessarily affine) bases schemes.

One of the main reasons for the success of Gröbner bases in the last decade clearly was the fact, that in many cases they actually could be computed. The focus of this article was not on algorithms but of course an efficient implementation of an algorithm to compute Gröbner covers is desirable. The existence proof for the canonical irreducible Gröbner cover is in principle constructive, but an algorithm for the computation of the canonical irreducible Gröbner cover would necessarily involve successive primary decompositions and thus would be of modest practical value. The obvious solution is to skip irreducibility.

The problem of determining the Gröbner basis structure of the fibres has already been considered from an algorithmic point of view (see [14], [15], [20], [19]). Most notably Antonio Montes released an implementation in Maple (see `http://www-ma2.upc.edu/∼montes`) for the important case where A is the polynomial ring over $\mathbb{Q}$. In fact the output of his algorithm BUILDTREE can be interpreted as a Gröbner cover, but the problem is that you can not say a priori which Gröbner cover the algorithm will compute, furthermore the result depends on a term order on the parameters. The most desirable thing of course would be to establish a canonical (not necessarily irreducible) Gröbner cover and then to compute it.

Acknowledgement

I am grateful for the financial support from the Austrian Science Fund FWF (Project P16641) and the caring backup of the project leader Kurt Girstmair. Furthermore I'd like to give credit to RISC and RICAM for supporting my stay at the “Special Semester on Göbner Bases and Related Methods” in Linz and to all the people who discussed the topic of this article with me.

References

[1] Williams W. Adams and Philippe Loustaunau. *An Introduction to Gröbner Bases*, volume 3 of *Grad. Stud. Math.* AMS, 1994.

[2] Elizabeth A. Arnold. Modular algorithms for computing Gröbner bases. *J. Symb. Comput.*, 35(4):403–419, 2003.

[3] Matthias Aschenbrenner. Reduction mod p of standard bases. *Commun. Algebra*, 33(5):1635–1661, 2005.

[4] Abdallah Assi. On flatness of generic projections. *J. Symb. Comput.*, 18(5):447–462, 1994.

[5] Dave Bayer, André Galligo, and Mike Stillman. Gröbner bases and extension of scalars. In David Eisenbud and Lorenzo Robbiano, editors, *Computational Algebraic Geometry and Commutative Algebra*, volume 24 of *Symposia Mathematica*, pages 198–215, 1991.

[6] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties and Algorithms.* UTM. Springer, second edition, 1997.

[7] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Number 150 in GTM. Springer, 2004.

[8] Elisabetta Fortuna, Patrizia Gianni, and Barry Trager. Degree reduction under specialization. *J. Pure Appl. Algebra*, 164(1-2):153–163, 2001.

[9] Hans-Gert Gräbe. On lucky primes. *J. Symb. Comput.*, 15(2):199–209, 1993.

[10] Mark L. Green. Generic initial ideals. In J. Elias, J. M. Giral, R. M. Miró-Roig, and S. Zarzuela, editors, *Six Lectures on Commutative Algebra*, volume 166 of *Progress in Mathematics*, pages 119–186, 1998.

[11] Robin Hartshorne. *Algebraic Geometry.* Number 52 in GTM. Springer, 1977.

[12] Michael Kalkbrenner. On the stability of Gröbner bases under specializations. *J. Symb. Comput.*, 24(1):51–58, 1997.

[13] Serge Lang. *Algebra.* World Student Series. Addison-Wesley, 1977.

[14] Antonio Montes. Canonical discussion of polynomial systems with parameters, preprint, available at `http://www-ma2.upc.edu/∼montes`.

[15] Antonio Montes. A new algorithm for discussing Gröbner bases with parameters. *J. Symb. Comput.*, 33(2):183–208, 2002.

[16] Antonio Montes and Jordi Castro. Solving the load flow problem using Gröbner bases. *SIGSAM Bulletin*, 29(1):1–13, 1995.

[17] Franz Pauer. On lucky ideals for Gröbner basis computations. *J. Symb. Comput.*, 14(1):471–482, 1992.

[18] Uli Walther. Cohomology, stratifications and parametric Gröbner bases in characteristic zero. *J. Symb. Comput.*, 35(5):527–542, 2003.

[19] Volker Weispfenning. Comprehensive Gröbner bases. *J. Symb. Comput.*, 14(1):1–29, 1992.

[20] Volker Weispfenning. Canonical comprehensive Gröbner bases. *J. Symb. Comput.*, 36(3-4):669–683, 2003.

Michael Wibmer
Institute of Mathematics
University Innsbruck
Technikerstr. 25
A-6020 Innsbruck, Austria

e-mail: `csac8728@uibk.ac.at`
homepage: `http://relationproject.at.tt`