Computational Algebra

9. Further applications of Gröbner bases

For this second round of applications of Gröbner bases, we consider the computation of three important pillars of ideal theory:

- colon ideals
- radical of an ideal
- primary decomposition of an ideal

First of all, we start recalling the definitions of these objects.

Def: let R be a commutative ring, let $I \subseteq R$ be an ideal and let $F \subseteq R$ be a subset; we define the colon ideal $I:F$ as

$$I:F := \{ r \in R : rf \in I \text{ for all } f \in F \}$$

Exercise: show that $I:F$ is an ideal and that $I:F = I:(F)$

Lemma: $I:F = \bigcap_{f \in F} I:f$

Proof: "$\subseteq$" if $r \in I:F$, then $rf \in I$ for all $f \in F$, i.e. $r \in I:f$ for all $f \in F$.

"$\supseteq$" if $r \in I:f$ $\forall f \in I$, then $rf \in I$ $\forall f \in F$, i.e. $r \in I:F$

Since we know how to compute intersections of ideals via Gröbner bases, the previous lemma reduces the computation of an arbitrary colon

ideal to the one of colon ideals of the form $I:f$.

The next proposition shows how we can reduce also this task to the one of the computation of an elimination ideal. (via the computation of an intersection)

Prop: let R be a commutative ring, let $I \subseteq R$ be an ideal, let $f \in R$; then $I:f = \frac{1}{f}(J \cap (f))$

Proof: "$\subseteq$" if $g \in I:f$, then $gf \in I$, i.e. $g \in \frac{1}{f}(I \cap (f))$

"$\supseteq$" if $g \in \frac{1}{f}(I \cap (f))$, then $gf \in I$, hence $g \in I:f$.

Next, let us describe an operation that is similar to the one of the colon ideal, which is called saturation.

Lemma: let R be a Noetherian commutative ring, let $I \subseteq R$ and let $f \in R$; then there exists $s \in \mathbb{N}$ such that

$$I:f^s = \bigcup_{j \in \mathbb{N}} I:f^j$$

Proof: from the definition of colon ideals, we have that

$$I \subseteq I:f \subseteq \dots \subseteq I:f^k \subseteq \dots$$

since R is Noetherian, this chain must stabilize, so there exists $s \in \mathbb{N}$ such that $I:f^s = I:f^{s+1} = \dots$; this proves the statement.

Def: the previous lemma shows that $\bigcup_{r \in \mathbb{N}} I:f^r$ is an ideal, which is called the saturation of I with respect to f and denoted $I:f^\infty$

The next proposition clarifies how we can compute the saturation with a single elimination, and at the same time how to detect the number $s \in \mathbb{N}$ from the previous lemma.

Prop. Let $I \subset k[x_1, \dots, x_n]$ be an ideal, let $f \in k[x_1, \dots, x_n]$ be a non-zero element; define $J := (I, 1-wf) \subseteq k[x_1, \dots, x_n, w]$; then

$$I : f^\infty = J \cap k[x_1, \dots, x_n]$$

moreover, if $\{f_1, \dots, f_r\}$ are generators for I and $\{g_1, \dots, g_s\}$ are generators for $J \cap k[x_1, \dots, x_n]$ and we write

$$g_i = (1 - wf) h_{i0} + \sum_{j=1}^{r} h_{ij} f_j \quad \forall i \in \{1, \dots, s\} \text{ with } h_{i0}, h_{ij} \in k[x_1, \dots, x_n, w]$$

then the number

$$s := \max \{ \deg_w (h_{ij}) : i \in \{1, \dots, s\}, j \in \{1, \dots, r\} \}$$

satisfies $I : f^s = I : f^\infty$.

Proof: Let us first show that $I : f^\infty = J \cap k[x_1, \dots, x_n]$.

"$\subseteq$" let $g \in I : f^\infty$, then $f^d g \in I$ for some $d \in \mathbb{N}$; we want to show that $g \in J$, i.e. $g \equiv 0 \pmod J$; now,

$$1 \equiv wf \pmod J, \text{ so } 1 \equiv w^d f^d \pmod J, \text{ so}$$

$$g \equiv w^d f^d g \equiv 0 \pmod J \text{ since } f^d g \in J$$

"$\supseteq$" let $g \in J \cap k[x_1, \dots, x_n]$, then $g = \sum_{i=1}^{m} r_i h_{i1} + (1 - wf) h_2$ with $r_i \in I$, $h_{i1}, h_2 \in k[x_1, \dots, x_n, w]$; now, let $d := \max \{ \deg_w (h_{i1}) \}$, perform the substitution $w \to \frac{1}{f}$ and multiply the right

hand side by f^d, then we get an element of the form $\sum r_i \tilde{h}_i$ with $\tilde{h}_i \in k[x_1, \dots, x_n]$, which means that $f^d \cdot g \in I$, namely, that $g \in I : f^\infty$

we are left to show that $I : f^\infty = I : f^s$ for the choice of s as in the statement; we only need to prove $I : f^\infty \subseteq I : f^s$;

let $g \in I : f^\infty$, then there exist $q_1, \dots, q_s \in k[x_1, \dots, x_n]$ such that

$$g = \sum_{i=1}^{s} q_i g_i =$$

$$= \sum_{i=1}^{s} q_i \left((1 - wf) k_i + \sum_{j=1}^{r} h_{ij} f_j \right)$$

now by again substituting $w \longrightarrow 1/f$ and multiplying by f^s, the choice of f^s implies that $f^s \cdot g \in I$, i.e. $g \in I : f^s$.

Let us now introduce the radical of an ideal.

Def: let R be a commutative ring, let $I \subseteq R$ be an ideal; we define the radical of I, denoted $\sqrt{I}$, as

$$\sqrt{I} := \{ r \in R : r^d \in I \text{ for some } d \in \mathbb{N} \}$$

Exercise: prove that the radical of an ideal is an ideal, and that $I \subseteq \sqrt{I}$.

Remark: to an ideal $I \subseteq k[x_1, \dots, x_n]$ we can associate its zeros, or solutions, or vanishing set, namely the set

$$V(I) := \{ a \in k^n : f(a) = 0 \ \ \forall f \in I \}$$

one then notices that the vanishing locus only depends on $\sqrt{I}$:

$$V(I) = V(\sqrt{I})$$

We hence see that the possibility of computing saturations gives a method to check ideal membership. In fact, by definition

$$f \in \sqrt{I} \iff 1 \in I : f^\infty$$

This, however, does not explain how to compute the radical of a given ideal. To understand how to do so, we need to do a little detour into the notion of dimension for polynomial ideals.

Notation: we write $\underline{x}$ for $\{x_1, \dots, x_n\}$, and so $k[\underline{x}]$ means $k[x_1, \dots, x_n]$; similarly, for a subset $\underline{u} \subseteq \underline{x}$, $\underline{u} = \{u_1, \dots, u_m\}$, we write $k[\underline{u}]$ for $k[u_1, \dots, u_m]$.

Def: let $I \subseteq k[\underline{x}]$ be a proper ideal, let $\underline{u} \subseteq \underline{x}$; then $\underline{u}$ is called independent modulo I if $I \cap k[\underline{u}] = (0)$; moreover, $\underline{u}$ is called maximally independent modulo I if it is independent modulo I and it is not strictly contained in any independent set modulo I.

Using what we have learnt about elimination ideals, we can test for independence noting that, if $\underline{u} \subseteq \underline{x}$ and if $\leq$ is an elimination term order with the $\underline{x} \setminus \underline{u}$ larger than the $\underline{u}$, and if we use the convention (which we have already implicitly used) that 0

is never an element of a Gröbner basis, then if G is a Gröbner basis of an ideal I with respect to $\leq$, then

$$\underline{u} \text{ is independent modulo } I \iff G \cap k[\underline{u}] = \emptyset$$

We derive the notion of dimension from the one of independence:

Def: let $I \subseteq k[\underline{x}]$ be a proper ideal, we define

$$\dim(I) := \max\{|\underline{u}| : \underline{u} \subseteq \underline{x} \text{ is independent modulo } I\}$$

Hence the dimension of an ideal can be computed by determining all independent sets. There is a (often better) way of computing the dimension, based on Hilbert functions, which however we will not address in this course.

The proof of the following lemma is immediate.

Lemma: let $I, J \subseteq k[\underline{x}]$ be proper ideals such that $I \subseteq J$; then

$$\dim(J) \leq \dim(I).$$

We will first focus on zero-dimensional ideals. The goal is to prove how we can construct the radical of such an ideal, and then to reduce the general case to the zero-dimensional one via the process of extension and reduction. First of all, let us start understanding a bit more zero-dimensional ideals.

Lemma: let $I \subseteq k[\underline{x}]$ be a proper ideal; I is zero-dimensional if and only if I contains a non-constant univariate polynomial in each of the variables $x_1, \dots, x_n$

Proof: "$\Rightarrow$" suppose that I is zero dimensional, fix $i \in \{1, \dots, n\}$ and set $\underline{u} = \{x_i\}$, then by assumption $I \cap k[\underline{u}] = I \cap k[x_i]$ is non-zero, hence it is generated by a non-constant polynomial $f_i \in k[x_i]$

"$\Leftarrow$" if $\forall i \in \{1, \dots, n\}$ there exists a non-constant polynomial $f_i \in k[x_i]$ such that $f_i \in I$, then $I \cap k[x_i] \neq (0)$, which implies that $\dim(I) < 1$, so $\dim(I) = 0$

Lemma: let $I \subseteq k[\underline{x}]$ be a proper ideal; if I is zero-dimensional, then so is every proper ideal $J \subseteq k[\underline{x}]$ containing I, and every elimination ideal $I \cap k[\underline{u}]$ with $\underline{u} \subseteq \underline{x}$.

Proof: since $I \subseteq J$, we have $\dim(J) \leq \dim(I)$, so $\dim(J) = 0$; now let $\underline{u} \subseteq \underline{x}$ with $\underline{u} \neq \emptyset$ and set $I' := I \cap k[\underline{u}]$; let now $x_i \in \underline{u}$, then we know that $I' \cap k[x_i] \neq (0)$ since I is zero-dimensional; hence I' is itself zero-dimensional.

Theorem: let $I \subseteq k[\underline{x}]$ be a proper ideal; then the following are equivalent:

(1.) $\dim(I) = 0$

(2.) $k[\underline{x}]/I$ is finite-dimensional as a k-vector space

(3.) there exists a term order and a Gröbner basis G for I such that $\forall i \in \{1, \dots, n\}$, there exists $g_i \in G$ with $LT_{\leq}(g_i) = x_i^{\nu_i}$ for some $\nu_i \in \mathbb{N}$, $\nu_i \neq 0$

(4.) for every term order and every Gröbner basis G for I we have that $\forall i \in \{1, \dots, n\}$, there exists $g_i \in G$ with $LT_{\leq}(g_i) = x_i^{\nu_i}$ for some $\nu_i \in \mathbb{N}$, $\nu_i \neq 0$

Proof: (1.) $\Rightarrow$ (4.) let G be any Gröbner basis of I and let $i \in \{1, \dots, n\}$; now, I is zero-dimensional, so there exists $f_i \in I \cap k[x_i]$ with $f_i \neq 0$; since $f_i \xrightarrow{G} 0$, then $LT_{\leq}(f_i)$ must be divisible by some $LT_{\leq}(g_i)$ for some $g_i \in G$, so $LT_{\leq}(g_i) = x_i^{\nu_i}$ for some $\nu_i \in \mathbb{N}$, $\nu_i \neq 0$.

(4.) $\Rightarrow$ (3.) immediate from the definition

(3.) $\Rightarrow$ (2.) let B be the set of terms in T^n that are irreducible with respect to G; then for every $t \in B$, we must have $\deg_{x_i}(t) < \nu_i$; then, only finitely many terms can satisfy this requirement, since B is a k-vector basis for $k[x]/I$, the statement is proven.

(2.) $\Rightarrow$ (1.) to prove that I is zero-dimensional, we show that it contains a univariate polynomial for each variable $x_1, \dots, x_n$

fix $i \in \{1, \dots, n\}$; consider the set

$$C_i := \{ [x_i^k], \ k \in \mathbb{N} \}$$

if C_i is finite, then there exist $\bar{k}, \bar{l} \in \mathbb{N}$ such that $[x_i^{\bar{k}}] = [x_i^{\bar{l}}]$, so $x_i^{\bar{k}} - x_i^{\bar{l}} \in I$; if C_i is infinite, then the elements of C_i must be linearly dependent, which implies that there exists a univariate $f_i \in k[x_i]$ belonging to I.

The goal is now to find algorithms that can detect whether a zero-dimensional ideal is radical, and can compute the radical of a zero-dimensional ideal. For this, we need to recall a few facts.

Def: a field k is called ~~perfect~~ if every irreducible polynomial $f \in k[x]$ is separable.

The reason why we are interested in perfect fields are the following two results.

Theorem: let k be a field; the following are equivalent

(i) k is perfect

(ii) a non-constant polynomial $f \in k[x]$ is squarefree if and only if $\gcd(f, f') = 1$.

Prop: finite fields and fields of characteristic zero are perfect.

Theorem: let $I \subseteq k[x_1, \dots, x_n]$ be a zero-dimensional ideal; then $\sqrt{I}$ equals the intersection of all maximal ideals of

$k[x_1, \dots, x_n]$ containing I; moreover, I is radical if and only if it is an intersection of maximal ideals.

Now we start building the theory for our algorithms.

Lemma: let R be a UFD and let $I \subseteq R$ be an ideal; let $a \in I$, then the squarefree part of a belongs to $\sqrt{I}$.

Proof: we can write $a = p_1^{r_1} \cdot \dots \cdot p_t^{r_t}$, then the squarefree part of a is $p_1 \cdot \dots \cdot p_t$ and we see that if $r = \max\{r_i : i \in \{1, \dots t\}\}$, then $p_1^r \cdot \dots \cdot p_t^r = a \cdot b$ for some $b \in k[x_1, \dots, x_n]$, so this element belongs to I, which implies that $p_1 \cdot \dots \cdot p_t \in \sqrt{I}$

Lemma: if R is a ring and $I, J \subseteq R$ are ideals such that

$$I \subseteq J \subseteq \sqrt{I}$$

then $\sqrt{J} = \sqrt{I}$.

Proof: from $I \subseteq J$, it follows $\sqrt{I} \subseteq \sqrt{J}$; from $J \subseteq \sqrt{I}$ it follows that $\sqrt{J} \subseteq \sqrt{I}$ since if $a \in \sqrt{J}$, then $a^r \in J$, so $a^r \in \sqrt{I}$, hence $a \in \sqrt{I}$.

Lemma: a zero-dimensional ideal $I \subseteq k[x_1, \dots x_n]$ which is radical contains a univariate squarefree polynomial in each of the n variables.

Proof: this follows from the fact that a zero-dimensional ideal con-

takes a univariate polynomial in each of the variables, and the previous lemma shows that if it is radical it contains the squarefree parts of those univariate polynomials.

Lemma: (Seidenberg's Lemma) Let $I \subseteq k[x_1, \dots, x_n]$ be a zero-dimensional ideal and assume that

$$\forall i \in \{1, \dots, n\}, \ \exists f_i \in I \text{ such that } \gcd(f_i, f_i') = 1$$

then I is the intersection of finitely many maximal ideals, so in particular it is radical.

Proof: Let us start noticing that each f_i is squarefree; in fact, had f_i a multiple factor, a computation would show that this would be a factor of f_i' as well, contradicting the hypothesis; we now show the statement by induction

$\boxed{n=1}$ in this case the generator f of I must be squarefree, because otherwise no element in I (which are nothing but multiples of f) would be squarefree, thus contradicting the hypothesis; write $f = g_1 \cdot \dots \cdot g_r$ where the g_i are irreducible and pairwise non-associated (they do not simply differ by an invertible element); since the $\{g_i\}$ are pairwise relatively prime, it holds

$$(f) = \bigcap_{i=1}^{r} (g_i)$$

and all the ideals (g_i) are maximal in $k[x_1]$, so the statement is proven.

$\boxed{n-1 \Rightarrow n}$ now we suppose that the result holds for $n-1$ and we show that it holds for n; as before, we write $f_1 = g_1 \cdots g_r$ with g_i irreducible and pairwise non-associated; then

$$I + (f_1) = \bigcap_{i=1}^{r} I + (g_i)$$

now it is enough to show that each of the $I + (g_i)$ is the intersection of finitely many maximal ideals; this hence means that we can suppose f_1 to be irreducible and show the result in that case; if f_1 is irreducible, then

$$K := k[x_1]/(f_1)$$

is a field and $k \subseteq K$ is a field extension, so we have a surjective homomorphism of rings

$$\varphi: k[x_1][x_2, \dots, x_n] \longrightarrow K[x_2, \dots, x_n]$$

by construction $\ker(\varphi) = (f_1)$ and $J := \varphi(I)$ is an ideal in $K[x_2, \dots, x_n]$; by construction $\varphi(f_i) = f_i$ when $i \in \{2, \dots, n\}$ and so $f_i \in J$ for $i \in \{2, \dots, n\}$; moreover, sin=

ce the computation of gcd's is not affected by field extensions we have that $\gcd(f_i, f_i') = 1$ for all $f_i \in J$, namely J satisfies the hypothesis of the lemma, and then by induction hypothesis J is the intersection of finitely many maximal ideals; then their preimages under φ are maximal ideals containing $\ker(\varphi) = (f_1 \dots f_t)$ and whose intersection is I, namely $J = M_1 \cap \dots \cap M_t$, then

$$I = \varphi^{-1}(J) = \varphi^{-1}(M_1) \cap \dots \cap \varphi^{-1}(M_t)$$

In this proof we have used the following lemma.

Lemma: let $I \subseteq k[x_1, \dots, x_n]$ be an ideal; suppose that $f \in k[x_1]$ admits a factorization $f = g_1 \cdot \dots \cdot g_r$ in $k[x_1]$ into pairwise relatively prime factors; then

$$I + (f) = \bigcap_{i=1}^{r} I + (g_i)$$

Proof: "$\subseteq$" follows from the construction

"$\supseteq$" let $h \in I + (g_i)$ for all $i \in \{1, \dots, r\}$; then there exists $q_1, \dots, q_r \in k[x_1, \dots x_n]$ and $s_1, \dots s_r \in I$ such that

$$h = q_i g_i + s_i \qquad \forall i \in \{1, \dots r\}$$

now set

$$f_i := \prod_{\substack{j=1 \\ j \neq i}}^{r} g_j \qquad \text{for } i \in \{1, \dots r\}$$

by construction and noting the previous equalities, we have that $h \cdot f_i \in I + (f)$ for all $i \in \{1, \dots, r\}$; since all the $\{g_i\}$ are relatively prime, it follows that the $\{f_i\}$ are relatively prime so $(f_1, \dots, f_r) = 1$ in $k[x_1]$, namely

$$1 = t_1 f_1 + \dots + t_r f_r$$

for some $t_1, \dots, t_r \in k[x_1]$, so $h = \sum_{i=1}^{r} t_i h f_i$ belongs to $I + (f)$.

From the discussion so far we get the following corollary:

Cor: let k be a perfect field, let $I \subset k[x_1, \dots, x_n]$ be a zero-dimensional ideal; then I is radical if and only if I contains a univariate squarefree polynomial in each variable

Lemma: let $I \subset k[x_1, \dots, x_n]$ be a proper ideal; if I contains a squarefree polynomial f in some variable x_i, then the unique monic univariate polynomial h of minimal degree in $I \cap k[x_i]$ is squarefree.

Proof: since $I \cap k[x_i] = (h)$, then f is a multiple of h. hence h must be squarefree

Lemma: let K be a perfect field, let $I \subset k[x_1, \dots, x_n]$ be a zero-dimensional ideal; for all $i \in \{1, \dots, n\}$, let

f_i be the unique monic polynomial of minimal degree in $I \cap k[x_i]$ and let h_i be its squarefree part; then

$$\sqrt{I} = I + (h_1, \dots, h_n)$$

Proof: let $J = I + (h_1, \dots h_n)$; by construction

$$I \subseteq J \subseteq \sqrt{I}$$

which implies that $\sqrt{J} = \sqrt{I}$, on the other hand, because of the way J is constructed, it is radical, hence $\sqrt{I} = J$.

So far we developed the theory of radicals of zero-dimensional ideals and of their computation. We now see how to extend this to the case of arbitrary dimension. The technique that we are going to use is the reduction to the zero-dimensional case. We perform this via the two constructions of <u>extension</u> and <u>contraction</u>.

<u>Def</u>, let $I \subseteq k[\underline{x}]$ be an ideal, let $\underline{u} \subseteq \underline{x}$; consider the ring $I \cdot k(\underline{u})[\underline{x} \setminus \underline{u}]$, where $k(\underline{u})[\underline{x} \setminus \underline{u}]$ is

the polynomial ring with variables $\underline{x}, \underline{u}$ and coefficients in the field of rational functions in the variables $\underline{u}$; the ideal $I \cdot k(\underline{u})[\underline{x}, \underline{u}]$ is called the extension of I.

Def: let $\underline{u} \subseteq \underline{x}$ and let $J \subseteq k(\underline{u})[\underline{x}, \underline{u}]$ be an ideal; the ideal $J \cap k[\underline{x}]$ is called the contraction of J.

Notation: the extension of I is denoted I^e;
the contraction of J is denoted J^c.

Lemma: the following two properties hold.

i. $I \subseteq I^{ec}$

ii. $J = J^{ce}$

Proof: i. follows from the definitions of extension and contraction

ii. "$\subseteq$" let $j \in J$, then there exists $f \in k[\underline{u}]$ such that $fj \in k[\underline{x}]$, i.e. $fj \in J^c$; then $j = \frac{fj}{f}$, so $j \in J^{ce}$

"$\supseteq$" let $j \in J^{ce}$, namely $j = \frac{\tilde{j}}{f}$ with $\tilde{j} \in J \cap k[\underline{x}]$ and $f \in k[\underline{u}]$; then $fj = \tilde{j}$, so $fj \in J$, hence $\frac{1}{f} \cdot fj \in J$, namely $j \in J$.

The key result for the reduction of the computation of radicals to the zero-dimensional case is the following:

Lemma: let $I \subsetneq k[\underline{x}]$ be an ideal and let $\underline{u} \subseteq \underline{x}$ be a maximally independent set with respect to I; then $I^e \subseteq k(\underline{u})[\underline{x} \setminus \underline{u}]$ is a zero-dimensional ideal

Proof: by assumption, for each $x_i \in \underline{x} \setminus \underline{u}$ we know that I contains a non-zero polynomial $f_i \in k[\underline{u} \cup \{x_i\}]$; we can view

$$f_i \in k(\underline{u})[x_i]$$

as a univariate polynomial in x_i which belongs to I^e; therefore I^e is zero-dimensional, since it is proper.

Let us now see how we can effectively compute contractions and extensions of polynomial ideals.

Lemma: let $\leq$ be a term order on $\mathbb{T}(\underline{x} \setminus \underline{u})$; let $J \subseteq k(\underline{u})[\underline{x} \setminus \underline{u}]$ be an ideal and let G be a Gröbner basis of J with respect to $\leq$; let us suppose that $G \subseteq k[\underline{x}]$ and set

$$f := \operatorname{lcm}\{ lc(g) : g \in G \}$$

and let I be the ideal generated by G in $k[\underline{x}]$; then $J^c = I : f^\infty$.

Proof: "$\supseteq$" let $g \in I : f^\infty$, then $f^s g \in I$ for some $n \in \mathbb{N}$, then

$$g = \frac{1}{f^s} \cdot f^s g \Rightarrow g \in J \cap k[\underline{x}]$$

"$\subseteq$" let $g \in J^c$; then $g \in J$, so $g \xrightarrow{G} 0$; we prove by induction on the length l of the reduction chain that gives $g \xrightarrow{G} 0$, that $g \in I : f^\infty$; if $l = 0$, then $g = 0$, so the statement holds; suppose now $l > 0$ and let $g_1 \in k(\underline{u})[\underline{x} \setminus \underline{u}]$ be such that $g \longrightarrow g_1 \xrightarrow{G} 0$; then

$$g_1 = g - \frac{h}{lc(p)} \cdot s \cdot p$$

with $p \in G$, $h \in k(\underline{u})$ and $s \in \mathbb{T}(\underline{x} \setminus \underline{u})$; now, f is a scalar in $k(\underline{u})[\underline{x} \setminus \underline{u}]$, so $f \cdot g_1 \xrightarrow{G} 0$; now, by the way how f is constructed, $lc(p)$ divides f, so $f g_1 \in J^c$; by induction hypothesis, then $f g_1 \in I : f^\infty$, which implies that $fg \in I : f^\infty$, hence $g \in I : f^\infty$

The previous lemma shows that contractions can be computed, since we can always reach the condition $G \subseteq k[\underline{u}]$ by clearing denominators of a Gröbner basis of an ideal in $k(\underline{u})[\underline{x} \setminus \underline{u}]$.

Lemma: let $\underline{u} \subseteq \underline{x}$ and let $\leq$ be an elimination term order on

$\mathbb{T}^n(x)$ with the $x \setminus y$ larger than the y; let $I \subseteq k[x]$ be an ideal and let G be a Gröbner basis of I with respect to $\leq$; let J be the ideal generated by G in $k(y)[x \setminus y]$ and then G is a Gröbner basis for J with respect to the restriction of $\leq$ to $\mathbb{T}^n(x \setminus y)$

Proof: we show that for each $f \in J$, there exists $g \in G$ such that $lt_{\leq}(g)$ divides $lt_{\leq}(f)$ where leading terms are considered in $k(y)[x \setminus y]$; by construction, there exists $q \in k(y)$ such that qf is in I; by assumption, there exists $g \in G$ such that $lt_{\leq}(g)$ divides $lt_{\leq}(qf)$ where the polynomials are considered in $k[x]$; a moment of reflection shows that then $lt_{\leq}(g)$ divides $lt_{\leq}(qf)$ also when these polynomials are considered in $k(y)[x \setminus y]$; however, when we work with coefficients in $k(y)$, the polynomial q is a scalar, so actually $lt_{\leq}(g)$ divides $lt_{\leq}(f)$.

Prop: let $y \subseteq x$ and let $\leq$ be a term order on $\mathbb{T}^n(x)$ with the $x \setminus y$ larger than the y; let $I \subseteq k[x]$ be an ideal and let G be a Gröbner basis of I with respect to $\leq$; set

$$f := \operatorname{lcm}\{ lc_{\leq}(g) : g \in G \}$$

where the polynomials in G are considered as polynomials in the ring $k(\underline{u})[\underline{x}, \underline{u}]$; then $I^{ec} = I : f^\infty$

Proof: notice that G generates I^e in $k(\underline{u})[\underline{x}, \underline{u}]$; by the previous lemma, G is actually a Gröbner basis of I^e in $k(\underline{u})[\underline{x}, \underline{u}]$; then the earlier lemma applies, proving the statement.

Recall that we have proved that, given an ideal I and a polynomial f, it is possible to compute a number $s \in \mathbb{N}$ such that

$$I : f^s = I : f^\infty$$

This is going to be useful in view of the following result.

Lemma: let R be a commutative ring, let $I \subseteq R$ be an ideal; let $q \in R$ and $s \in \mathbb{N}$ such that $I : q^s = I : q^\infty$, then

$$I = (I + (q^s)) \cap (I : q^\infty)$$

Proof: "$\subseteq$" follows from the definitions

"$\supseteq$" let $g \in (I + (q^s)) \cap (I : q^\infty)$; then $q^s \cdot g \in I$ and there exist $h \in I$ and $r \in R$ such that $g = h + q^s r$; then $q^{2s} \cdot r = q^s \cdot g - q^s \cdot h$, so $q^{2s} \cdot r \in I$, therefore $I : q^{2s} \ni r$, so $r \in I : q^s$, then $q^s r \in I$, hence $g \in I$.

As a corollary, we see that in the situation of the previous proposition, whenever $s \in \mathbb{N}$ is such that $I : f^s = I : f^\infty$, then

$$I = (I + (f^s)) \cap I^{ec}$$

Now the strategy to compute the radical of an ideal $I \subset k[\underline{x}]$ is the following:

1. Determine a set $\underline{u} \subseteq \underline{x}$ that is maximally independent with respect to I.
2. Consider $I^e \subseteq k(\underline{u})[\underline{x} \setminus \underline{u}]$, which is a zero-dimensional ideal, and compute its radical with the methods that we have already developed.
3. Contract this radical to $k[\underline{x}]$
4. Repeat the procedure with the ideal I' that satisfies the relation $I = I' \cap I^{ec}$

To make this into an actual algorithm, we need to make sure that certain compatibilities between radicals and contractions and extensions hold in our setting.

Lemma. Let $\underline{u} \subseteq \underline{x}$, let $J \subseteq k(\underline{u})[\underline{x} \setminus \underline{u}]$ be an ideal, then

$$\sqrt{J}^c = \sqrt{J^c}$$

Proof: "$\subseteq$" let $f \in \sqrt{J}^c$, then $f \in k[\underline{x}]$ and $f^s \in J$ for some $s \in \mathbb{N}$; hence $f^s \in k[\underline{x}]$, so $f^s \in J^c$, hence $f \in \sqrt{J^c}$

"$\supseteq$" let $f \in \sqrt{J^c}$, then $f^s \in k[\underline{x}] \cap J$ for some $s \in \mathbb{N}$; then $f \in \sqrt{J}$; moreover $f \in k[\underline{x}]$, so $f \in \sqrt{J}^c$

Lemma: let R be a commutative ring, let $I_1, I_2 \subseteq R$ be ideals, then $\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$.

Proof: "$\subseteq$" let $f \in \sqrt{I_1 \cap I_2}$, then $f^s \in I_1$ and $f^s \in I_2$ for some $s \in \mathbb{N}$, so $f \in \sqrt{I_1} \cap \sqrt{I_2}$

"$\supseteq$" let $f \in \sqrt{I_1} \cap \sqrt{I_2}$, so $f^{s_1} \in I_1$ and $f^{s_2} \in I_2$ for some $s_1, s_2 \in \mathbb{N}$; let $s \in \mathbb{N}$, $s = \max\{s_1, s_2\}$, then $f^s \in$

$\in \sqrt{I_1 \cap I_2}$, so $f \in \sqrt{I_1 + I_2}$.

Lemma: let $J_1, J_2 \subseteq k(\underline{u})[\underline{x} \setminus \underline{u}]$ be ideals, then $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$.

Proof: this immediately follows from the definitions.

We are then now ready to state the algorithm that computes the radical of an ideal. To use the results about zero-dimensional ideals we are going to assume that for every subset $\underline{u} \subseteq \underline{x}$ of indeterminates, the field of fractions $k(\underline{u})$ is perfect.

Algorithm Radical

Input: a set $F \subseteq k[\underline{x}]$ of polynomials

Output: a system of generators for $\sqrt{(F)}$.

1. Set $G = \{1\}$
2. If $1 \notin (F)$:
3. Compute $\{u_1, \dots, u_r\}$, a maximally independent set modulo $I := (F)$
4. Compute a system of generators Z of $\sqrt{I^e}$, where $I^e \subseteq k(\underline{u})[\underline{x}, \underline{u}]$
5. Compute a system of generators C for the contraction $\sqrt{I^e}^c \subseteq k[\underline{x}]$
6. Compute an element $f \in k[\underline{u}]$ such that

$$I = (I + (f^s)) \cap I^{ec}$$

for some $s \in \mathbb{N}$

7. Let G be a system of generators of $(I + (f)) \cap \sqrt{I^e}^c$
8. Return G.

Theorem: Algorithm Radical terminates in finite time and is correct

Proof: let us start with termination; if $1 \in (F)$, termination is clear;

if $1 \notin (F)$, then $\{u_1, \dots, u_r\}$ is computed so that $(F) \cap k[\underline{u}] = (0)$,

and so by construction $(F) \subsetneq (F) + (f)$; hence during the algorithm

a strictly increasing chain of ideals in $k[\underline{x}]$, is created, which

by Noetherianity must stop after finitely many steps;

to prove correctness, since the algorithm is recursive, we show that it is correct when $1 \in (F)$ and then we show correctness when (F) is proper and we assume that the algorithm is correct for all ideals strictly containing (F); if $1 \in (F)$, the algorithm is clearly correct, what we are left to show is that, if $I = (F)$

$$\sqrt{I} = \sqrt{I + (f)} \cap \sqrt{I^e}^c$$

in fact, from what we have seen, $\sqrt{I^e}^c = \sqrt{I^{ec}}$ and

$$\sqrt{I} = \sqrt{(I + (f^s)) \cap I^{ec}} =$$

$$= \sqrt{I + (f^s)} \cap \sqrt{I^{ec}}$$

$$= \sqrt{I + (f)} \cap \sqrt{I^{ec}}$$

so we know that $I \subsetneq I + (f)$ and hence we can suppose that the algorithm performs the computation of the radical correctly.

The last topic we are going to discuss in this section is the computation of primary decompositions of ideals. We will just sketch a few aspects, since the needed theory would need several hour.

Recall that, given an integer $p \in \mathbb{Z}$, we can write it as

$$p = p_1^{r_1} \cdot \ldots \cdot p_s^{r_s}$$

where $p_1, \dots, p_s$ are pairwise distinct and non-opposite prime numbers. At level of ideals, this means that

$$(p) = (p_1^{r_1}) \cap \dots \cap (p_s^{r_s})$$

Primary decomposition is a vast generalization of this result which holds in any Noetherian ring, and which states that any ideal I can be decomposed as an intersection

$$I = Q_1 \cap \dots \cap Q_s$$

of primary ideals, namely ideals J such that if $F \cdot G \in J$, then $F \in J$ or $G^d \in J$ for some $d \in \mathbb{N}$; this decomposition has some unguess properties which we are not going to analyze. Basic properties of primary ideals show that their radicals are prime ideals, and so if we set $P_i := \sqrt{Q_i}$, then $\sqrt{I} = P_1 \cap \dots \cap P_s$. From a geometric point of view, primary decomposition determines the ideals of the "atomic algebraic constituents" of the zero-set of an ideal. For example, if

$$I = (xy, xz)$$

then the zero set of I is given by the union of a plane and a line, and the primary decomposition of I is in fact

$$I = (x) \cap (y, z)$$

As we did for the computation of radicals, we start by examining the primary decomposition of zero-dimensional ideals and then we are going to use extension and contraction to reduce from the general case to the zero-dimensional one. Let us start clarifying the geometry of zero-dimensional ideals.

Prop. Let $I \subseteq k[x]$ be an ideal, then the following are equivalent:

i. $\dim(I) = 0$

ii. there exists an algebraically closed extension L of k such that I has only finitely many zeroes in L^n

iii. for every algebraically closed extension of k, I has only finitely many zeros.

Proof: i. $\Rightarrow$ iii. Suppose that $\dim(I) = 0$ and that $k \subseteq L$ is an algebraically closed field extension; we know that $\forall i \in \{1, \dots, n\}$, I contains an element $f_i \in I \cap k[x_i]$; if $a = (a_1, \dots, a_n)$ is a zero of I, then $f_i(a) = 0$, namely $f_i(a_i) = 0$, which means that each a_i can take only finitely many values since $f_i \neq 0$

iii. $\Rightarrow$ ii. follows since algebraic closures exist.

ii. $\Rightarrow$ i. we are not going to prove this

We are now going to state several results concerning the primary decomposition of zero-dimensional ideals.

Def: if $\underline{a} \in k^n$, we set

$$I_{\underline{a}} := (x_1 - a_1, \dots, x_n - a_n)$$

Lemma: i. if $\underline{a} \in k^n$, then $I_{\underline{a}}$ is a maximal ideal that contains every ideal of which $\underline{a}$ is a zero

ii. if k is algebraically closed, then every maximal ideal of $k[\underline{x}]$ is of the form $I_{\underline{a}}$ for some $\underline{a} \in k^n$

Prop: let I be a zero-dimensional ideal of $k[\underline{x}]$ and suppose that $\underline{a} \in k^n$ is a zero of I; then $I_{\underline{a}}$ is the radical of some primary ideal Q in the primary decomposition of I; if the different zeros $\underline{a}_1, \dots, \underline{a}_r \in k^n$ of I are all in k^n, then the radicals of the primary ideals in the primary decomposition of I are precisely $I_{\underline{a}_1}, \dots, I_{\underline{a}_r}$.

Lemma: let I and $\underline{a}$ as in the proposition above and suppose that k is perfect; for $i \in \{1, \dots n\}$, let f_i be the monic generator of $I \cap k[x_i]$; for $i \in \{1, \dots n\}$, let ν_i be the multiplicity of a_i as a zero of f_i; let $\nu = 1 + \sum_{i=1}^{n} (\nu_i - 1)$; then the primary ideal in the primary decomposition of I whose radical is $I_{\underline{a}}$ is $I + I_{\underline{a}}^{\nu}$.

We put ourself in a very special position, in which everything goes very easily. After that, we show that we can always reduce to this easy situation.

Def: an ideal $I \subseteq k[\underline{x}]$ is said to be in <u>normal position</u> with respect to x_i if the x_i-components of the zeroes of I in $\bar{k}^n$ are all pairwise distinct.

Lemma: let $I \subseteq k[\underline{x}]$ be a zero-dimensional ideal in normal position with respect to x_1; assume that $I \cap k[x_1]$ contains a polynomial of the form p^ν with p irreducible and $\nu \in \mathbb{N}$; then I is primary.

Prop: let $I \subseteq k[\underline{x}]$ be a zero-dimensional ideal in normal position with respect to x_1; let f_1 be the unique monic generator of $k[x_1] \cap I$ and let $f = p_1^{\nu_1} \cdot \ldots \cdot p_s^{\nu_s}$ be its decomposition into irreducible pairwise non associated factors; then the primary decomposition of I is given by

$$I = \bigcap_{i=1}^{s} \left(I + (p_i^{\nu_i}) \right)$$

However, most ideals are not in general position with respect to a variable. The strategy in this case is to introduce a new

variable so that the ideal is in normal position with respect to it, compute the primary decomposition via the previous proposition and then retrieve the primary decomposition we were initially interested in via elimination.

Lemma: let $I \subseteq k[\underline{x}]$ be an ideal; let $c \in k^n$ and set

$$g := z - c_1 x_1 - \dots - c_n x_n$$

let $J = I + (g) \subseteq k[\underline{x}, z]$; then the following are equivalent:

i. if z_1, z_2 are two different zeros of I in $\bar{k}^n$, then

$$\sum c_i z_{1i} \neq \sum c_i z_{2i}$$

ii. J is in normal position with respect to z.

Lemma: let $I \subseteq k[\underline{x}]$ be an ideal, let $c \in k^n$, set

$$g := z - c_1 x_1 - \dots - c_n x_m$$

and let $J := I + (g)$; then

i. if I is zero-dimensional then J is zero-dimensional

ii. $J \cap k[\underline{x}] = I$

iii. if I is radical, so is J

iv. if I is zero-dimensional and radical, and

$$J = P_1 \cap \dots \cap P_s$$

is the primary decomposition of J, then if we set

$$P_i' = P_i \cap k[\underline{x}] \quad \text{for all } i \in \{1, \dots, n\}$$

then $I = P_1' \cap \dots \cap P_s'$ is the primary decomposition of I.

Lemma: if k is perfect and infinite then we can find an element $c \in k^n$ s.t. that the ideal $I + (g)$ is in the previous statements is in normal position with respect to z.

These results allow one to cook up an algorithm that computes the primary decomposition of a zero-dimensional ideal. Then, as we did for radicals, using contractions and extensions we can provide an algorithm that works for ideals of arbitrary dimension.