Lecture Notes 2.

MA 722

1 Positive Dimensional Varieties

Our main focus now is on polynomial systems which have positive dimensional solutions. Solution of such systems first raises the question of how to represent the roots. The most commonly used families to represent higher dimensional varieties are as follows:

- Parametric equations
- Implicit equations, such as:
  - Gröbner bases
  - Triangular representation
  - Rational univariate representation
- "Generic" points on the irreducible components

In this lecture note we concentrate on implicit representation of algebraic varieties:

- We already learned about Gröbner bases. Here we will summarize how to answer some geometric questions about varieties using Gröbner bases.
- We will define triangular representations, and see what kind of geometric questions can be answered by them. We will also outline a method, named after Wu, to compute triangular representation which is usually more efficient than Gröbner basis computation.
- As a special case of triangular representation we will define rational univariate representation, and see when it can be applied.

We will follow the approach in [CLO97, Chapter 6].

2 Representation by Gröbner bases

In this section we give a method using Gröbner bases to decide whether a polynomial vanishes on an algebraic variety. We will use the fact (proved in the last lecture notes) that the division algorithm for Gröbner bases solves the ideal membership problem.

Problem 2.1 (Radical Membership Problem)**.** *Given*

$$\begin{aligned} h_1(x_1,\ldots,x_n) &= 0 \\ &\vdots \\ h_t(x_1,\ldots,x_n) &= 0 \\ &\textit{and} \\ g(x_1,\ldots,x_n) &= 0, \end{aligned}$$

polynomials in $k[x_1,\ldots,x_n]$*. Question: Does* $g = 0$ follow strictly *from* $h_1,\ldots,h_t$*, i.e. does* g *vanish whenever* $h_1,\ldots,h_t$ *vanish?*

The following solution works if k is algebraically closed:

Solution. Assume that k is algebraically closed and let $V := \mathbf{V}(h_1,\ldots,h_t)$. Then $g = 0$ strictly follows from $h_1,\ldots,h_n$ if and only if $g \in \mathbf{I}(V)$. Therefore, by Hilbert's Nullstellensatz, we have that $g = 0$ strictly follows from $h_1,\ldots,h_n$ if and only if

$$\exists\, m \geq 1 \text{ such that } g^m \in \langle h_1,\ldots,h_t\rangle.$$

In the next proposition we will prove that this is equivalent to

$$1 \in \langle h_1,\ldots,h_t, 1-yg\rangle \subseteq k[x_1,\ldots,x_n,y].$$

Now

$$1 \in \langle h_1,\ldots,h_t, 1-yg\rangle$$

can be decided by computing a Gröbner basis for the ideal $\langle h_1,\ldots,h_t,1-yg\rangle \subseteq k[x_1,\ldots,x_n,y]$. □

Proposition 2.2. *Let* $h_1,\ldots h_t, g$ *be as above. Then*

$$\exists\, m \geq 1 \text{ such that } g^m \in \langle h_1,\ldots,h_t\rangle$$

if and only if

$$1 \in \langle h_1,\ldots,h_t, 1-yg\rangle \subseteq k[x_1,\ldots,x_n,y].$$

Proof. To prove the equivalence, on one hand, if $g^m \in \langle h_1, \ldots, h_n \rangle$ then

$$1 = y^m g^m + (1 - y^m g^m) = y^m g^m + (1 - yg)(1 + yg + \ldots y^{m-1} g^{m-1})$$

and the right hand side is in $\langle h_1, \ldots, h_n, 1 - yg \rangle$. On the other hand, assume that

$$1 = \sum_{i=1}^{t} p_i h_i + q(1 - yg)$$

for some $p_i, q \in k[x_1, \ldots, x_n, y]$. Set $y = 1/g$, so we get

$$1 = \sum_{i=1}^{t} p_i(x_1, \ldots, x_n, 1/g) h_i.$$

Let $m := \max_i(\deg_y(p_i))$. Then multiplying both sides of the equation by g^m we clear all denominators, and get

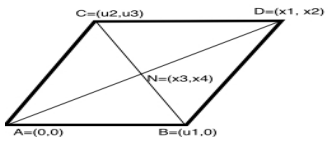
$$g^m = \sum_{i=1}^{t} A_i h_i$$

where $A_i \in k[x_1, \ldots, x_n]$. This proves the equivalence. □

3 Triangular Representation

3.1 Motivation

The following simple example is in Automatic Geometric Theorem Proving:



Example 3.1. Let A, B, C, D be the vertices of a parallelogram in the plane. We will prove using coordinate geometry that the two diagonals $\overline{AD}$ and $\overline{BC}$ of any parallelogram intersects at a point N which bisects the diagonals, i.e. $\|AN\| = \|DN\|$ and $\|BN\| = \|CN\|$.

We place the parallelogram in a coordinate system such that we have $A = (0, 0)$, $B = (u_1, 0)$, and $C = (u_2, u_3)$, where u_1, u_2, u_3 are "free" variables. Since D is uniquely determined by A, B, C, we give coordinates $D = (x_1, x_2)$, where x_1, x_2 are "dependent" variables, and introduce the equations:

$$x_2 = u_3 \text{ and } \frac{u_3}{u_2} = \frac{x_2}{x_1 - u_1}.$$

To get polynomial equations, we multiply both sides by the product of the denominators. The intersection N of the diagonals is also uniquely determined by A, B, C, D, and introducing the dependent variables x_3, x_4 for its coordinates we get the following equations from the collinearity of A, N, D and B, N, C, respectively:

$$\frac{x_4}{x_3} = \frac{u_3}{x_1} \text{ and } \frac{x_4}{u_1 - x_3} = \frac{u_3}{u_1 - u_2}.$$

Again, we will clear denominators. The claim $\|AN\| = \|DN\|$ can be expressed by the equations

$$x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2.$$

Therefore, we have a system

$$\begin{aligned} h_1 &:= x_2 - u_3 \\ h_2 &:= (x_1 - u_1)u_3 - x_2u_2 \\ h_3 &:= x_4x_1 - x_3u_3 \\ h_4 &:= x_4(u_2 - u_1) - (x_3 - u_1)u_3 \\ g &:= x_3^2 + x_4^2 - (x_3 - x_1)^2 - (x_4 - x_2)^2. \end{aligned}$$

If we could prove that $g = 0$ whenever $h_1, \ldots, h_4$ vanishes, then we proved the claim. However,

$$1 \notin \langle h_1, h_2, h_3, h_4, 1 - yg \rangle.$$

What is wrong here? The claim is still true!

The reason why the Radical Ideal Membership Problem does not apply here is as follows:

$$\mathbf{V}(h_1, h_2, h_3, h_4) = V' \cup U_1 \cup U_2 \cup U_3$$

where

$$V' = V(x_1 - u_1 - u_2, x_2 - u_3, 2x_3 - u_1 - u_2, 2x_4 - u_3)$$

and U_1, U_2, U_3 correspond to degenerate cases

$$\begin{aligned} U_1 &= \mathbf{V}(x_2, x_4, u_3) \\ U_2 &= \mathbf{V}(x_1, x_2, u_1 - u_2, u_3) \\ U_3 &= \mathbf{V}(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1). \end{aligned}$$

It is easy to see that g vanishes on V' but doesn't vanish on U_1, U_2, U_3 (for example g becomes $2x_1x_3 - x_1^2 \neq 0$ on U_1).

In the next definitions we will capture the property that g vanishes on the non-degenerate components but does not necessarily vanish on the degenerate components.

Definition 3.2. Let W be an irreducible variety in the affine space k^{n+m} with coordinates $u_1, \ldots, u_m, x_1, \ldots, x_n$. We say that the functions $u_1, \ldots, u_m$ are *algebraically independent on* W if no non-zero polynomial in $k[u_1, \ldots, u_m]$ vanishes identically on W, i.e. $\mathbf{I}(W) \cap k[u_1, \ldots, u_m] = \{0\}$.

Definition 3.3. Let

$$\begin{aligned} h_1(u_1, \ldots, u_m, x_1, \ldots, x_n) &= 0 \\ &\vdots \\ h_n(u_1, \ldots, u_m, x_1, \ldots, x_n) &= 0 \\ &\text{and} \\ g(u_1, \ldots, u_m, x_1, \ldots, x_n) &= 0, \end{aligned}$$

be polynomials in $k[u_1, \ldots, u_m, x_1, \ldots, x_n]$. We say that g *follows generically* from $h_1, \ldots, h_n$ if

$$g \in \mathbf{I}(V') \subset k[u_1, \ldots, u_m, x_1, \ldots, x_n]$$

where V' is the union of the components of $\mathbf{V}(h_1, \ldots, h_n)$ on which $u_1, \ldots, u_m$ are algebraically independent.

In the next proposition we prove that over algebraically closed fields we can decide whether g follows generically from $h_1, \ldots, h_n$ without computing the irreducible decomposition of $\mathbf{V}(h_1, \ldots, h_n)$.

Proposition 3.4. *Let k be an algebraically closed field. Let $h_1, \ldots, h_n$ and g be as above. Then g follows generically from $h_1, \ldots, h_n$ if and only if there exists $c(u_1, \ldots, u_m) \in k[u_1, \ldots, u_m]$ such that*

$$cg \in \sqrt{\langle h_1, \ldots, h_n \rangle} \subset k[u_1, \ldots, u_m, x_1, \ldots, x_n].$$

Proof. $\Leftarrow$ Denote $V = \mathbf{V}(h_1, \ldots, h_n)$ and let W be an irreducible component of V'. Since $cg \in \sqrt{\langle h_1, \ldots, h_n \rangle}$, thus cg vanishes on V, which contains W. Thus $cg \in \mathbf{I}(W)$. Since W is irreducible, therefore $\mathbf{I}(W)$ is prime, thus either $c \in \mathbf{I}(W)$ or $g \in \mathbf{I}(W)$. However, $c \in \mathbf{I}(W)$ would imply that $u_1, \ldots, u_m$ is not algebraically independent over W, so we have that $g \in \mathbf{I}(W)$. This implies that $g \in \mathbf{I}(V')$ as was claimed. (Note that for this direction we didn't use that k is algebraically closed.)
$\Rightarrow$ Assume that $g \in \mathbf{I}(V')$. Let $V = V' \cup U_1 \cup \cdots \cup U_k$ where $u_1, \ldots, u_m$ are algebraically dependent over U_i for $i = 1 \ldots, k$. Thus there exists $c_i \in k[u_1, \ldots, u_m]$ such that $c_i \in \mathbf{I}(U_i)$ for $i = 1 \ldots, k$. If we define $c := \prod_{i=1}^{k} c_i$ then $cg \in \mathbf{I}(V)$. Using Hilbert's Nullstellensatz we get that $cg \in \sqrt{\langle h_1, \ldots, h_n \rangle}$. □

Using the next proposition we can reduce the computation of whether g follows generically from $h_1, \ldots, h_n$ to the radical ideal membership problem.

Proposition 3.5. *Let $h_1, \ldots, h_n$ and g be as above. Then the following are equivalent:*

(i) $\exists\, c \in k[u_1, \ldots, u_m]$ *such that* $cg \in \sqrt{\langle h_1, \ldots, h_n \rangle}$.

(ii) $g \in \sqrt{H}$ *where H is the ideal generated by $h_1, \ldots, h_n$ in the ring $k(u_1, \ldots u_m)[x_1, \ldots, x_n]$. (Note that $k(u_1, \ldots u_m)$ denotes the fraction field of $k[u_1, \ldots u_m]$, and in $k(u_1, \ldots u_m)[x_1, \ldots, x_n]$ the variables $u_1, \ldots, u_m$ are considered as part of the coefficients of polynomials in $x_1, \ldots, x_n$.)*

(iii) $1 \in \langle h_1, \ldots, h_n, 1 - yg \rangle \subseteq k(u_1, \ldots u_m)[x_1, \ldots, x_n, y]$.

Proof. (ii)⇔(iii) follows from Proposition 2.2.
(i)⇒(ii) is true since if $(cg)^m = \sum_{i=1}^n A_i h_i$ for some $A_i \in k[u_1, \dots u_m, x_1, \dots, x_n]$ then $g^m = \sum_{i=1}^n \frac{A_i}{c^m} h_i$ where $A_i/c^m \in k(u_1, \dots u_m)[x_1, \dots, x_n]$.
(ii)⇒(i) is true since if $g^m = \sum_{i=1}^n B_i h_i$ for some $B_i \in k(u_1, \dots u_m)[x_1, \dots, x_n]$ and c is the least common multiple of the denominators of the B_i's, then $(cg)^m = \sum_{i=1}^n B_i' h_i$ and B_i' has no denominators. □

3.2 Pseudo-division

Next we describe an alternative to computing Gröbner bases, the so called Wu's method to compute a triangular representation of an affine variety, which allows to decide if a polynomial vanishes generically over the variety. Wu's method is usually more efficient than computing Gröbner bases.

The first ingredient of Wu's method is a version of the multivariate division with remainder, known as "pseudo-division". Let $f, g \in k[x_1, \dots, x_n, y]$ and we consider them as univariate polynomials in the variable y with coefficients depending on $x_1, \dots, x_n$. The main idea of the pseudo-division is to imitate the univariate division with remainder algorithm. However, in the univariate case we can only make division if we are allowed to divide by the leading coefficient of g. In order to avoid division by polynomials in the multivariate case, in the pseudo-division algorithm we allow to multiply f by a sufficiently large power of the leading coefficient of g. We have the following algorithm:

Pseudo-division
Input: $f = a_p y^p + a_{p-1} y^{p-1} + \dots + a_0$ and $g = b_s y^s + b_{s-1} y^{s-1} + \dots + b_0$, where $a_i, b_j \in k[x_1, \dots, x_n]$, $s \leq p$, and $b_s \neq 0$.
Output: $q, r \in k[x_1, \dots, x_n, y]$ such that there exists $m \leq p - s + 1$ such that

$$b_s^m f = qg + r$$

and either $r = 0$ or $\deg_y(r) < \deg_y(g)$.

$r := f$; $q := 0$;

WHILE $r \neq 0$ AND $\deg_y(r) \geq s$ DO
$r := b_s r - \mathrm{LC}_y(r) g y^{\deg_y(r) - s}$;

$$q := b_s q + \mathrm{LC}_y(r) g y^{\deg_y(r)-s};$$

Correctness. Note that in the above algorithm we denoted by $\deg_y(r)$ the degree of r in the variable y and by $\mathrm{LC}_y(r)$ the leading coefficient of r as a polynomial in y. The WHILE loop is executed at most $p - s + 1$ times, therefore the power m in $b_s^m f = qg + r$ can be chosen as $m \leq p = s + 1$. The rest of the proof follows easily from the construction. Note that since $r = b_s^m f - qg$, therefore $r \in \langle f, g \rangle$. □

Definition 3.6. The polynomials r and q in the pseudo-division algorithm are called *pseudo-remainder* and *pseudo-quotient*, and denoted by $\mathrm{prem}(f, g, y)$ and $\mathrm{pquo}(f, g, y)$, respectively.

Remark 3.7. Another interpretation of the pseudo-division algorithm is to conduct the usual univariate division with remainder of f by g in the ring $k(x_1, \ldots, x_n)[y]$ and then multiply the results by the least common multiple of the denominators. It is easy to see that the denominators are powers of $\mathrm{LC}_y(g)$.

Example 3.8. Let $f = x^2y^3 - y$ and $g = x^3y - 2$. Then we have

$$(x^3)^3 f = (x^8y^2 + 2x^5y + 4x^2 - x^6)g + 8x^2 - 2x^6.$$

3.3 Wu's Method

Let us get back to the problem of deciding whether g follows generically from $h_1, \ldots, h_n$ for $h_1, \ldots, h_n, g \in k[u_1, \ldots, u_m, x_1, \ldots, x_n]$. Recall that V' is the union of the components of $V = \mathbf{V}(h_1, \ldots, h_s)$ such that $u_1, \ldots, u_m$ are algebraically independent over them. The first, elementary version of Wu's method that we present here assumes that V' is irreducible.

Wu's method consists of two main steps: First to compte a "triangular set" $\{f_1, \ldots, f_n\}$ for $h_1, \ldots, h_n$, where $f_i \in [u_1, \ldots, u_m, x_1, \ldots, x_i]$. Secondly, using successive pseudo-division of g by $f_1, \ldots, f_n$, we will be able to decided whether g follows generically from $h_1, \ldots, h_n$. More precisely:

Step 1. Reduction to triangular form

Below we outline the algorithm. We work on one variable at a time starting with x_n.

Triangularization
Input: $H_n := \{h_1, \ldots, h_n\} \in k[u_1, \ldots, u_m, x_1, \ldots, x_n]$
Output: $f_1, \ldots, f_n$ such that $f_i \in [u_1, \ldots, u_m, x_1, \ldots, x_i]$ and

$$V' \subseteq V \subseteq V(f_1, \ldots, f_n).$$

1. Let $S \subset \{h_1, \ldots, h_n\}$ be the set of polynomials containing the variable x_n, and let $H_{n-1} := H_n - S$.

2. If $S = \emptyset$ then ERROR(Probably no component with $u_1, \ldots, u_m$ algebraically independent);

3. If $|S| = 1$ then let f_n be the polynomial in S, and continue for $n - 1$.

4. If $|S| \geq 2$ then do

   While $|S| \geq 2$ pick $a, b \in S$ such that $\deg_{x_n}(a) \geq \deg_{x_n}(b)$;
   $S := S - \{a\}$;
   $r := \text{prem}(a, b, x_n)$;
   If $r = 0$ then ERROR(V' is probably reducible);
   If $\deg_{x_n}(r) > 0$ then $S := S \cup \{r\}$ else $H_{n-1} = H_{n-1} \cup \{r\}$;

Correctness. Throughout the algorithm we maintain that $|H_{n-1} \cup S| = n$, otherwise we return an ERROR message. Since $|S| = 1$ when we go to the $n - 1$ case, thus $|H_{n-1}| = n - 1$ and the induction hypothesis is maintained. Also, the polynomials both in S and H_{i-1} are in the ideal $\langle h_1, \ldots, h_n \rangle \subset k[u_1, \ldots, u_m, x_1, \ldots, x_n]$, since they are pseudo-remainders of polynomials in this ideal. This implies that $V' \subseteq V \subseteq \mathbf{V}(f_1, \ldots, f_n)$. Note that the output of the above algorithm is not unique, it depends on the order we chose the elements $a, b \in S$. □

Example 3.9. We continue the example on the parallelogram, i.e.

$$\begin{aligned} h_1 &:= x_2 - u_3 \\ h_2 &:= (x_1 - u_1)u_3 - x_2u_2 \\ h_3 &:= x_4x_1 - x_3u_3 \\ h_4 &:= x_4(u_2 - u_1) - (x_3 - u_1)u_3. \end{aligned}$$

We have two polynomials which contain the variable x_4, therefore $S := \{h_3, h_4\}$. Then

$$\begin{aligned} r &:= \mathrm{prem}(h_4, h_3, x_4) \\ &= (u_2 - u_1)x_1x_4 - (u_2 - u_1)x_3u_3 - x_1x_4(u_2 - u_1) + x_1(x_3 - u_1)u_3 \\ &= x_1x_3u_3 - x_1u_1u_3 + x_3u_3u_1 - x_3u_3u_2. \end{aligned}$$

Thus, $H_3 = \{h_1, h_2, r\}$ and $f_4 := h_3$. We continue for $n = 3$. Since there is only one polynomial in H_3 depending on x_3, therefore we define $f_3 := r$ and $H_2 := \{h_1, h_2\}$. For $n = 2$ we compute

$$r := \mathrm{prem}(h_2, h_1, x_2) = x_1u_3 - u_1u_3 - u_2u_3.$$

Thus $f_2 := h_1$ and $f_1 := x_1u_3 - u_1u_3 - u_2u_3$ gives a triangular set. Note that $\mathbf{V}(u_3, x_2, x_1) \subset \mathbf{V}(f_1, f_2, f_3, f_4)$ but $\mathbf{V}(u_3, x_2, x_1) \not\subset V$, therefore, $V \neq \mathbf{V}(f_1, f_2, f_3, f_4)$.

Step 2. Successive pseudo-division

Assume that we are given a triangular set $\{f_1, \ldots, f_n\}$, where $f_i \in k[u_1, \ldots, u_m, x_1, \ldots, x_i]$, and $g \in k[u_1, \ldots, u_m, x_1, \ldots, x_n]$. We define the sequence

$$\begin{aligned} R_{n-1} &:= \mathrm{prem}(g, f_n, x_n) \\ R_{n-2} &:= \mathrm{prem}(R_{n-1}, f_{n-1}, x_{n-1}) \\ &\vdots \\ R_1 &:= \mathrm{prem}(R_2, f_2, x_2) \\ R_0 &:= \mathrm{prem}(R_1, f_1, x_1). \end{aligned}$$

Then the following theorem holds:

Theorem 3.10. *Let $\{f_1, \ldots, f_n\}$ and g be as above. Let*

$$d_i := \mathrm{LC}_{x_i}(f_i) \in k[u_1, \ldots, u_m, x_1, \ldots, x_{i-1}]$$

be the leading coefficient of f_i for $i = 1, \ldots, n$. Then

(i) there exist R_0, $s_1, \ldots, s_n \in \mathbb{N}$ *and* $A_1, \ldots, A_n \in k[u_1, \ldots, u_m, x_1, \ldots, x_n]$ *such that*

$$d_1^{s_1} \cdots d_n^{s_n} g = A_1 f_1 + \cdots + A_n f_n + R_0,$$
$$\deg_{x_i}(R_0) < \deg_{x_i}(f_i) \;\; i = 1, \ldots, n.$$

(ii) If $R_0 = 0$ *then* g *is zero at every point of* $\mathbf{V}(f_1, \ldots, f_n) - \mathbf{V}(\prod_{i=1}^n d_i)$, *and in particular at the points of* $V' - \mathbf{V}(\prod_{i=1}^n d_i)$.

Proof. (i) By the pseudo-division algorithm there exist s_n and q_n such that

$$R_{n-1} = d_n^{s_n} g - q_n f_n.$$

Similarly,

$$R_{n-2} = d_{n-1}^{s_{n-1}}(d_n^{s_n} g - q_n f_n) - q_{n-1} f_{n-1} = d_{n-1}^{s_{n-1}} d_n^{s_n} g - q_{n-1} f_{n-1} - q_n' f_n.$$

Therefore, by induction we get that

$$R_0 = d_1^{s_1} \cdots d_n^{s_n} g - (A_1 f_1 + \cdots + A_n f_n)$$

for some $A_1, \ldots, A_n$ as claimed.
(ii) If $R_0 = 0$ then $d_1^{s_1} \cdots d_n^{s_n} g$ vanishes on $\mathbf{V}(f_1, \ldots, f_n)$. Thus if $\xi \in \mathbf{V}(f_1, \ldots, f_n) - \mathbf{V}(\prod_{i=1}^n d_i)$ then $d_1^{s_1} \cdots d_n^{s_n}(\xi) \neq 0$, so $g(\xi)$ must be zero. □

Example 3.11. Continuing the previous example, we have

$$\begin{aligned} f_1 &= x_1 u_3 - u_1 u_3 - u_2 u_3 \\ f_2 &= x_2 - u_3 \\ f_3 &= x_3(x_1 u_3 + u_3 u_1 - u_3 u_2) - x_1 u_1 u_3 \\ f_4 &= x_4 x_1 - x_3 u_3 \end{aligned}$$

and

$$g = x_1^2 - 2x_1 x_3 - 2x_4 x_2 + x_2^2.$$

We compute the successive pseudo-remainders:

$$\begin{aligned} R_3 &= x_3(2x_2 u_3 - 2x_1^2) + x_1^3 - x_1 x_2^2 \\ R_2 &= (x_1 u_3 + u_3 u_1 - u_3 u_2)(x_1^3 - x_1 x_2^2) + (2x_2 u_3 - 2x_1^2) x_1 u_1 u_3 \\ R_1 &= x_1^4 u_3 + x_1^3 u_3 u_1 - x_1^3 u_3 u_2 - x_1^2 u_3^3 - x_1 u_3^3 u_1 + x_1 u_3^3 u_2 + 2u_3^3 x_1 u_1 - 2x_1^3 u_1 u_3 \\ &= x_1^4 u_3 - x_1^3 u_3 u_1 - x_1^3 u_3 u_2 - x_1^2 u_3^3 + x_1 u_3^3 u_1 + x_1 u_3^3 u_2 \\ R_0 &= R_1 - (x_1^3 - x_1) f_1 = 0. \end{aligned}$$

Since $R_0 = 0$, the previous theorem asserts that g vanishes on V' minus the points where any of the leading coefficients of $f_1, \ldots, f_4$ vanish. Since

$$\mathrm{LC}_{x_1}(f_1) = u_3,\ \mathrm{LC}_{x_2}(f_2) = 1,\ \mathrm{LC}_{x_3}(f_3) = (x_1u_3 + u_3u_1 - u_3u_2),\ \mathrm{LC}_{x_4}(f_4) = x_1,$$

therefore

$$\mathbf{V}(\prod_{i=1}^{4} \mathrm{LC}_{x_i}(f_i)) \cap \mathbf{V}(f_1, \ldots, f_4) = \mathbf{V}(u_1u_3(u_1 + u_2)).$$

This gives a proof of the original geometric theorem whenever u_1, u_3 and $u_1 + u_2$ are not-zero.
Note that we could have simplified our computation if we "self-pseudo-reduced" our triangular set, and if we divided out the common denominators of the coefficients $f_1, \ldots, f_4$ as polynomials in $x_1, \ldots, x_4$. By this self-reduction we get the following triangular set:

$$\begin{aligned} f_1' &= x_1u_3 - u_1u_3 - u_2u_3 \\ f_2' &= x_2 - u_3 \\ f_3' &= (2u_3u_2)x_3 - x_1u_1u_3 \\ f_4' &= (u_1u_3 + u_2u_3)x_4 - x_3u_3^2 \end{aligned}$$

Here all leading coefficients are polynomials in $k[u_1, u_2, u_3]$, so they cannot vanish on the generic components V'. Therefore g pseudo-reduces to 0 by $F = \{f_1, \ldots, f_4\}$ if and only if g generically follows from F.

The following example demonstrates that it is not always possible to find triangular sets such that the leading coefficients do not vanish over the generic components.

Example 3.12. This example is a zero dimensional ideal, so $m = 0$, no free variables. Let

$$F = \{x_1^2 - x_1,\ x_1x_2^2 - 3x_2 + 2\}.$$

F is a triangular set, and $\mathrm{LC}_{x_1}(f_1) = 1$, $\mathrm{LC}_{x_2}(f_2) = x_1$. In this case

$$\mathbf{V}(\mathrm{LC}(f_1)\mathrm{LC}(f_2)) \cap \mathbf{V}(f_1, f_2) = \mathbf{V}(x_1, -3x_2 + 2) = \{(0, 2/3)\},$$

which is a proper subset of $V(F) = \{(0, 2/3), (1, 1), (1, 2)\}$. This also implies that there are polynomials g which identically vanish on $V(F)$, but do not

pseudo-reduce to 0, e.g. $g = (x_1^2 - x_1)x_2^2$, which reduces to $(x_1 - 1)(3x_2 - 2)$. Note that there is no triangular set in this coordinate system that would represent $V(F)$. However, a linear change of variables remedies the situation, for example, by switching x_1 and x_2 we get a triangular set with constant leading coefficients

$$\{-4 + 12x_2 - 11x_2^2 + 3x_2^3,\ 9x_2^2 + 14 - 27x_2 + 4x_1\}.$$

This will be the subject of the next lecture notes on Geometric Representation.

Another kind of remedy for the situation in the previous example is a decomposition algorithm, called **Ritt-Wu decomposition**. The precise description of the Ritt-Wu decomposition is out of the scope of these lecture notes, so we just mention the main ideas here.

In order to eliminate the problem of vanishing leading coefficients over generic components, we will need to decompose $V' = V_1 \cup \cdots \cup V_k$ into components such that each component will be represented by a triangular set, and the leading coefficients of the polynomials in the triangular sets will only depend on the free variables $u_1, \ldots, u_m$, thus do not vanish identically over any of the generic components.

The main idea of the Ritt-Wu decomposition algorithm is the following. We take the leading coefficient d_n of f_n and decompose the variety corresponding to H_{n-1} into components where d_n vanishes identically, and into irreducible components where it doesn't vanish identically. Over the first group of components we simply add the equation $d_n = 0$, and over the second group of components we can compute the "pseudo inverse" of d_n, i.e. polynomials $e_n \in k[u_1, \ldots, u_m, x_1, \ldots, x_{n-1}]$ and $c_n \in k[u_1, \ldots, u_m]$ such that $e_n d_n \equiv c_n$ over that component, thus the leading coefficient of $e_n f_n$ is in $k[u_1, \ldots, u_m]$ over that irreducible component.

References

[CLO97] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Springer, 1997.