Elimination Theory

December 12, 2016

In this chapter, we'll study the application of Groebner bases to algorithmic methods for eliminating variables from systems of polynomial equations, thus reducing systems of multivariate polynomial equations to a single polynomial in one variable. Specifically, of the many applications of elimination theory, we will study the implicitization problem and the envelope of a family of curves.
One minor note - throughout the chapter the notation $\text{LT}(S) := \{\text{LT}(s), s \in S\}$ will be used, for set S.

1 Elimination and Extension Theorems

As we vaguely touched on in the last section of the previous chapter, Groebner bases are very useful in solving systems of polynomial equations. This is because the Groebner basis for the ideal generated by a set of polynomials has the same zero set as that set of polynomials. Moreover, the Groebner basis follows the pattern that its elements tend to be in "triangular" form, to borrow a term from linear algebra; what this means is that one polynomial will be in one variable, another in two, another in three, and so on. Thus, we can leverage the initial polynomial in one variable's solution to turn the second polynomial in two variables into a polynomial in one variable, whose solution combined with the first polynomials solutions we can leverage to turn the third polynomial in three variables into a polynomial in one variable once more, and so on.
The study of this pattern of solving polynomial equations is known as elimination theory, and the process typically consists of two phases: the elimination phase, in which a set of polynomials is transformed into a set of polynomials in the above defined triangular form, and the extension phase, in which each polynomial equation of the Groebner basis are successively solved and extended to solve the next polynomial equation.
In accordance with the above intuition, notice that a polynomial in the Groebner basis for $I \subset F[x_1, \cdots, x_n]$ in k variables can be expressed as a polynomial in the ideal $I \cap F[x_1, \cdots, x_k]$. To further study such polynomials, we study this surrounding ideal, which motivates the following definition.

(Definition) Elimination ideal: *Let $I = \langle f_1, \cdots, f_s \rangle \subset F[x_1, \cdots, x_n]$ be a polynomial ideal. We define the l^{th}* ***elimination ideal****, denoted I_l, by*

$$I_l = I \cap F[x_{l+1}, \cdots, x_n]$$

- Thus, I_l consists of the polynomials in I which have eliminated the first l variables.

It follows now that eliminating the first l variables corresponds to finding non-zero polynomials in I_l. If we can find a basis which consists of a polynomial from each of $I_l, 1 \leq l \leq s$, then we will have successfully eliminated enough variables to begin the extension step. Groebner bases are deeply related to this idea; the next theorem is the foundational starting point for understanding this connection.

(Theorem) Elimination theorem: *Let $I \subset F[x_1, \cdots, x_n]$ by a polynomial ideal, and let G be a Groebner basis for I with respect to the lexicographic ordering $x_1 > \cdots > x_n$. Then*

$$G_l := G \cap F[x_{l+1}, \cdots, x_n]$$

is a Groebner basis for I_l.

- *Proof*: We wish to show that $\text{LT}(I_l) = \langle \text{LT}(I_l) \rangle = \langle \text{LT}(G_l) \rangle$. Clearly, $G_l \subset I_l \rightarrow \langle \text{LT}(G_l) \rangle \subset \langle \text{LT}(I_l) \rangle$, so let's prove the opposite direction by showing that for any $f \in I_l$, $\text{LT}(f)$ is divisible by some $\text{LT}(g)$ for some $g \in G_l$.
$I_l \subset I \rightarrow f \in I \rightarrow \exists g \in G$ s.t. $\text{LT}(f)$ is divisible by $\text{LT}(g)$, since G is a Groebner basis for I. Multiplying polynomials will never reduce the number of variables in either of the two polynomials, so $\text{LT}(f) \in I_l$ implies $\text{LT}(g) \in F[x_{l+1}, \cdots, x_n]$. But we defined our Groebner basis with respect to lexicographic order, so if $\text{LT}(g)$ consists only of variables $x_{l+1}, \cdots, x_n$, then so does g, which means $g \in F[x_{l+1}, \cdots, x_n]$, which means that because $g \in G$, $g \in G_l$, which proves the theorem. $\square$

Since the elimination theorem holds for any Groebner basis with respect to $>_{lex}$ it follows that every Groebner basis with respect to this monomial ordering must contain at least one polynomial in $F[x_l, \cdots, x_n]$ for each $1 \leq l \leq n-1$. This shows that any Groebner basis can be used to perform the elimination step when solving a system of polynomial equations. In

other words, to put a system of polynomial equations in "triangular" form, we simply compute a Groebner basis with respect to lexicographic order for the ideal generated by the polynomials in the system.

Having settled the elimination step, let's move on to the extension step. Given an ideal $I = \langle f_1, \cdots, f_s \rangle$, consider the variety of the ideal: $\mathbf{V}(I) := \{(a_1, \cdots, a_n) \in F^n \text{ where } \forall f \in I : f(a_1, \cdots, a_n) = 0\}$. Then the solutions to the system $f_1 = \cdots = f_s = 0$ are precisely the points in $\mathbf{V}(I)$. To explicitly describe points in $\mathbf{V}(I)$ we will build up the points one coordinate at a time, in accordance with the intuition of back-substituting solutions to one polynomial equation into the next to turn the latter into a polynomial equation in a single variable. We'll call $(a_{l+1}, \cdots, a_n) \in \mathbf{V}(I_l)$ a *partial solution* to the original system of equations; our goal is to extend $(a_{l+1}, \cdots, a_n)$ to $(a_l, a_{l+1}, \cdots, a_n) \in \mathbf{V}(I_{l-1})$ so we can inductively build solutions to the original system of equations by explicitly describing $\mathbf{V}(I_0) = \mathbf{V}(I)$.
If we let $I_{l-1} = \langle g_1, \cdots, g_r \rangle$ then this is equivalent to solving the system of equations

$$g_1(x, a_{l+1}, \cdots, a_n) = \cdots = g_r(x, a_{l+1}, \cdots, a_n) = 0$$

for x. Although the above polynomials are all only in a single variable, it's possible that these polynomials don't have a common root, in which case $(a_{l+1}, \cdots, a_n)$ is a partial solution which doesn't extend. Let's now search for a way to determine beforehand which partial solutions extend all the way to complete solutions and which don't. The following theorem shows that this can be done in the degenerate case, extending $(a_1, \cdots, a_n)$ to $(a_1, \cdots, a_n) \in \mathbf{V}(I)$.

(Theorem) Extension theorem: *Let $I = \langle f_1, \cdots, f_s, \rangle$ be an ideal in $\mathbb{C}[x_1, \cdots, x_n]$, and let I_1 be the first elimination ideal. Suppose we have the partial solution $(a_2, \cdots, a_n) \in \mathbf{V}(I_1)$ to $f_1 = \cdots = f_s = 0$. Then, if we write*

$$f_i(x_1, \cdots, x_n) = c_i(x_2, \cdots, x_n)x_1^{N_i} + r_i$$

where r_i contains x_1's with degree lower than N_i, we can extend the partial solution to a full solution precisely when it doesn't cause all the leading terms of the f_i's above to vanish; that is, when $(a_2, \cdots, a_n) \notin \mathbf{V}(c_1, \cdots, c_s)$.

- *Proof*: TODO
- *Intuition*: Intuitively the theorem is stating that if we are given a partial solution to the system $f_1 = \cdots = f_s = 0$, then in accordance with our intuition, we can extend it to a full solution by "back-substituting" the partial solution into successive polynomials in one variable which we haven't solved for yet. For this back-substitution to work, we require first that we can express the polynomials as polynomials in one variable we haven't solved for, which is true precisely when we can write $f_i = c_i(x_2, \cdots, x_n)x_1^{N_i} + r_i$; second, we require that the partial solution doesn't cause the crucial terms to automatically vanish, which would be the case if $c_1(a_2, \cdots, a_n) = \cdots = c_s(a_2, \cdots, a_n) = 0$, which is equivalent to $(a_2, \cdots, a_n) \in \mathbf{V}(c_1, \cdots, c_s)$. If the partial solutions cause the polynomials' leading coefficients to simultaneously vanish, then this has the potential to lead to nonsensical consequences. The theorem states that if these two conditions are satisfied, then we can back-substitute to extend the partial solution to a full solution.
- Note that the extension theorem applies to polynomials over $\mathbb{C}$; this is because the theorem is false over $\mathbb{R}$.

Although the extension theorem only applies to the base case where a single coordinate is extended, we can iteratively apply it in an inductive fashion to extend partial solutions of any length up to a full solution. This is because if we have partial solution $(a_l, \cdots, a_n)$, we can extend it to $(a_{l-1}, a_l, \cdots, a_n)$ by applying the extension theorem, which applies because I_l is the first elimination ideal of I_{l-1}.

2 Geometric Interpretations of Elimination

In this section, we view the elimination and extension theorems from a geometric perspective, and give a visual intuition for the theorems' statements. We'll show that one can visualize elimination as projecting an affine variety onto a lower dimensional subspace. To build this intuition, we begin with some useful definitions.

(Definition) Projection map: *Let $V = \mathbf{V}(f_1, \cdots, f_s) \subset \mathbb{C}[x_1, \cdots, x_n]$ be an affine variety. We define the **projection map**, which eliminates the first l variables, as*

$$\pi_l : \mathbb{C}^n \to \mathbb{C}^{n-l} \text{ s.t. } \pi_l(a_1, \cdots, a_n) = (a_{l+1}, \cdots, a_n)$$

Intuitively, the l^{th} projection mapping simply eliminates the first l variables in an affine variety, effectively discarding the information contained in the first l variables and mapping it from an n-dimensional space to an $(n-l)$-dimensional space. Seeing as projections discard variables, it's not surprising that we can relate them to elimination ideals in a natural way.

(Theorem) Projection maps and elimination ideals: *Let $I = \langle f_1, \cdots, f_s \rangle \subset \mathbb{C}^n$ be an ideal. Then*

$$\pi_l(\mathbf{V}(I)) \subseteq \mathbf{V}(I_l)$$

• *Proof*: For any $(a_{l+1}, \cdots, a_n) \in \pi_l(\mathbf{V}(I))$, there was some $(a_1, \cdots, a_n) \in \mathbf{V}(I)$ that the point came from. Since $f(a_1, \cdots, a_n) = 0, \forall f \in I_l$ and $f \in I_l$ implies f consists only of $x_{l+1}, \cdots, x_n$, it follows that $f(a_{l+1}, \cdots, a_n) = 0$, which shows that $(a_{l+1}, \cdots, a_n) \in \mathbf{V}(I_l)$. □

This shows that $\pi_l(V)$, for affine variety V, consists precisely of the partial solutions that extend to full solutions, since every point in $\pi_l(V)$ came from a point in V. We can therefore restate the extension theorem with this geometric interpretation in mind.

(Theorem) Geometric Extension Theorem: *Let $I = \langle f_1, \cdots, f_s \rangle \subset \mathbb{C}[x_1, \cdots, x_n]$ be an ideal, and, as in the original extension theorem, write*

$$f_i = c_i(x_2, \cdots, x_n)x^{N_i} + r_i$$

Then we have

$$\mathbf{V}(I_1) = \pi_1(\mathbf{V}(I)) \cup (\mathbf{V}(c_1, \cdots, c_s) \cap \mathbf{V}(I_1))$$

• *Proof*: TODO

• *Intuition*: For $V := \mathbf{V}(f_1, \cdots, f_s)$, this theorem implies that projecting the space of full solutions down one dimension nearly gives us the entire space of partial solutions for free, except for the part of the space of full solutions that exists due to $c_1 = \cdots = c_s = 0$, instead of $f_1 = \cdots = f_s = 0$. In accordance with the extension theorem, then, if a partial solution doesn't cause the c_i's to simultaneously vanish, then it wouldn't be an element of $\mathbf{V}(c_1, \cdots, c_s)$, and so by virtue of being a member of $\mathbf{V}(I_1)$ by definition, it would necessarily be a member of $\pi_1(V)$, meaning that the partial solution was projected down from some full solution, which is to say that the partial solution can be extended to a full solution (namely, the one from which it was projected down).

To further formalize the intuition that $\pi_1(V)$ "almost" fills up $\mathbf{V}(I_1)$, we make the following strong statements on the relationship between $\pi_1(V)$ and $\mathbf{V}(I_l)$.

(Theorem) Closure Theorem: *Let $I = \langle f_1, \cdots, f_s \rangle \subset \mathbb{C}[x_1, \cdots, x_n]$ be an ideal. Then*

1. $V := \mathbf{V}(I_l)$ is the smallest affine variety containing $\pi_l(V)$, in the sense that if V' is some other affine variety containing $\pi_l(V)$, then $V \subseteq V'$.
2. Assuming $V \neq \{\}$, there exists some affine sub-variety $W \subset V$ such that $V - W \subseteq \pi_l(V)$.

• *Proof*: The proof of this theorem requires the Nullstellensatz, which we'll cover in the next chapter. The proof will be given then.

• The second part of the theorem states that $\pi_l(V)$ fills up most of V, in the sense that what's missing lies in some strictly smaller affine variety.

3 Implicitization

In this section, we give a complete solution to the implicitization problem using elimination theory. Before going into the details of the solution, note the caveat that because the implicit description of an affine variety may not always completely fill up the variety, what we will really be finding is, given a set of parametric equations, the smallest affine variety containing the solutions to the equations. This leads to some more interesting questions - once we've found the affine variety associated with a set of parametric equations, does the parameterization completely fill up the variety, and if not, how do we find the missing points? We'll use Groenber bases and the extension theorem to answer these questions.

Let's begin the solution to the implicitization problem with the special case of polynomial parameterization, when we have, for $f_1, \cdots, f_n \in F[t_1, \cdots, t_m]$ the equations

$$\begin{aligned} x_1 &= f_1(t_1, \cdots, t_m) \\ &\vdots \\ x_n &= f_n(t_1, \cdots, t_m) \end{aligned}$$

which describe a curve in F^n. We can regard the above parametric equations as a function $f : F^m \to F^n$, given by $f(t_1, \cdots, t_m) = (f_1(t_1, \cdots, t_m), \cdots, f_m(t_1, \cdots, t_m))$. Then the range of f, denoted $f(F^m) := \{f(t_1, \cdots, t_m), (t_1, \cdots, t_m) \in F^m\}$ is the subset of F^n parameterized by the above equations, and the implicitization problem is equivalent to finding the smallest affine variety in F^n which contains $f(F^m)$.

We'll apply elimination theory to finding this smallest affine variety by first recasting the problem in terms of affine varieties and projections. To link the parameterization to affine varieties, let's shift our perspective up to $F[t_1, \cdots, t_m, x_1, \cdots, x_n]$, which contains polynomials in $n+m$ indeterminates (our reason for naming the indeterminates t_i followed by x_i is to reinforce the following intuition). Consider the polynomial $x_i - f_i(t_1, \cdots, t_m) \in F[t_1, \cdots, t_m, x_1, \cdots, x_n]$; this polynomial vanishes

precisely over points $(t_1, \cdots, t_m, x_1, \cdots, x_n) \in F^{n+m}$ for which $x_i = f_i(t_1, \cdots, t_m)$. It follows that the above parametric equations trivially define the variety $V := \mathbf{V}(x_1 - f_1, \cdots x_n - f_n) \subset F^{n+m}$; that is, the system of equations $x_i - f_i = 0$ is solved by the full range of the parameterization. We can regard V as the *graph* of f, if we write points in V as

$$(t_1, \cdots, t_m, f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m))$$

We can relate V to projections by defining the functions

$$\rho : F^m \to F^{n+m}, \rho(t_1, \cdots, t_m) := (t_1, \cdots, t_m, f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m))$$

$$\pi_m : F^{n+m} \to F^n, \pi(t_1, \cdots, t_m, x_1, \cdots, x_n) = (x_1, \cdots, x_n)$$

Notice that π_m is simply the m^{th} projection map. By design, we have $f = \pi_m \circ \rho$, so we have

$$f(F^m) = \pi_m(\rho(F^m)) = \pi_m(V)$$

This is merely a formal statement of the obvious statement that the image of the parameterization is precisely a projection of the parameterization's graph. However, it will allow us to use elimination theory to V in order to find the smallest variety containing $f(F^m)$.

(Theorem) Solution to Polynomial Implicitization: *Let F be an infinite field, and $f : F^m \to F^n$ be the function associated with the polynomial parameterization*

$$\begin{aligned} x_1 &= f_1(t_1, \cdots, t_m) \\ &\vdots \\ x_n &= f_n(t_1, \cdots, t_m) \end{aligned}$$

given by $f(t_1, \cdots, t_m) = (x_1, \cdots, x_n)$. Then $\mathbf{V}(I_m)$ is the smallest variety in F^n containing $f(F^m)$, where $I = \langle x_1 - f_1, \cdots, x_n - f_n \rangle \subset F[t_1, \cdots, t_m, x_1, \cdots, x_n]$.

• *Intuition*: The ideal I is specifically designed so as to give an explicit description of a set of polynomials in which every polynomial vanishes over the entirety of $f(F^m)$. The theorem states that, since we obtained the explicit description by "lifting" to a higher dimensional space, going from $F[x_1, \cdots, x_n]$ to $F[t_1, \cdots, t_m, x_1, \cdots, x_n]$, if we filter this explicit description for the polynomials that we want, i.e. polynomials only over $x_1, \cdots, x_n$, then we'll have found precisely the polynomials defining the affine variety we seek. This process of first lifting equations into a higher dimensions space of polynomials and then filtering out the variables we don't want is called *eliminating* the variables $t_1, \cdots, t_m$.

• *Proof*: We've already established that $f(F^m) = \pi_m(V)$, where $V = \mathbf{V}(x_1 - f_1, \cdots, x_n - f_n)$. We showed in the last section that $\pi_m(V) \subseteq \mathbf{V}(I_m)$, so it's clear that $\mathbf{V}(I_m)$ contains $f(F^m)$; we need to show that it's the smallest variety to do so. It's obvious that each of $x_i - f_i$ vanishes over $f(F^m)$; we'll show that every polynomial which vanishes over $f(F^m)$ is in I_m. This will prove the theorem because then if there were some other affine variety W which contained $f(F^m)$, then the polynomials defining W (that is, the polynomials composing the system of equations defining W) are all zero over $f(F^m)$, which allows us to invoke the above assumption to conclude that each of the defining polynomials of W belongs to $I_m \subset \langle x_i - f_i \rangle$. This means that if a point is in $\mathbf{V}(I_m)$, meaning that it causes every polynomial in I_m to be zero, then that point must cause every defining polynomial of W to be zero, which shows that $\mathbf{V}(I_m) \subset W$, proving the theorem.

To prove the above assumption, suppose $g \in F[x_1, \cdots, x_n]$ vanishes over all of $f(F^m)$. Viewing g as a degenerate polynomial in $F[t_1, \cdots, t_m, x_1, \cdots, x_n]$, if we can show that the remainder of g divided by $x_1 - f_1, \cdots, x_n - f_n$ is zero, then we'll have shown $g \in I_m$. To see this, divide g by $x_i - f_i$ with respect to the lexicographic order $x_1 > \cdots > x_n > t_1 > \cdots > t_m$ to obtain

$$g = q_1 \cdot (x_1 - f_1) + \cdots + q_n \cdot (x_n - f_n) + r(t_1, \cdots, t_m)$$

Notice that the remainder r is in variables $t_1, \cdots, t_m$ since $\text{LT}(x_i - f_i) = x_i$. Since F is infinite, it follows that r is zero, since $r(a_1, \cdots, a_m) = g(x_1, \cdots, x_n) - q_1 \cdot 0 + \cdots + q_n \cdot 0 = 0$ since we assumed h vanishes on F^m and since each of $x_i - f_i$ vanish on F^m by definition. Finally, since h is a polynomial only in $x_1, \cdots, x_n$, it follows that

$$g = q_1 \cdot (x_1 - f_1) + \cdots + q_n \cdot (x_n - f_n) \in I \cap F[x_1, \cdots, x_n] = I_m$$

which proves the theorem. □

We can use the above theorem to algorithmically solve the polynomial implicitization problem, by first finding a Groebner basis G for the ideal $I = \langle x_1 - f_1, \cdots, x_n - f_n \rangle$ with respect to a lexicographic order that puts every t_i above every x_j. G_m is then, by the elimination theorem, a Groebner basis for I_m, which has zero set $\mathbf{V}(I_m)$, which is, by the above theorem, an implicit description of the smallest affine variety containing the parameterization. Thus, the elements of G_m are

the defining polynomials of the smallest variety containing the parameterization.
Next, let's turn to rational implicitization, where the parameterization is given by rational functions:

$$x_1 = \frac{f_1(t_1, \cdots, t_m)}{g_1(t_1, \cdots, t_m)}$$
$$\vdots$$
$$x_n = \frac{f_n(t_1, \cdots, t_m)}{g_n(t_1, \cdots, t_m)}$$

We can no longer define the mapping $f : F^m \to F^n$ by $f(t_1, \cdots, t_m) = (x_1, \cdots, x_n)$ as the mapping is not defined where $g_i = 0$. However, f does define a map from $F^m - V'$ to F^n, where $V' := \mathbf{V}(g)$ for $g := g_1 \cdots g_n$. As before, the implicitization problem is now equivalent to finding the smallest variety in F^n which contains $f(F^m - V')$. As before, we can try defining an ideal $I := \langle x_i - \frac{f_i}{g_i} \rangle$, but this doesn't account for the removal of V' from the domain of f. We might instead try clearing denominators, with $I := \langle g_i x_i - f_i \rangle$, but it actually turns out that $\mathbf{V}(I)$ is not necessarily guaranteed to be the smallest variety containing $f(F^m - V')$. We must add another variable to I to "control" the denominators:

$$I := \langle g_1 x_1 - f_1, \cdots, g_n x_n - f_n, 1 - gy \rangle \subset F[y, t_1, \cdots, t_m, x_1, \cdots, x_n]$$

The inclusion of $1 - gy$ in the ideal forces all the denominators g_i to obey $gy = 1$, which prevents any of them from vanishing on $\mathbf{V}(I)$. Let's define the corresponding functions:

$$\rho : F^m - V' \to F^{1+m+n}, \rho(t_1, \cdots, t_m) = \left(\frac{1}{g(t_1, \cdots, t_m)}, t_1, \cdots, t_m, \frac{f_1(t_1, \cdots, t_m)}{g_1(t_1, \cdots, t_m)}, \cdots, \frac{f_n(t_1, \cdots, t_m)}{g_n(t_1, \cdots, t_m)} \right)$$

$$\pi_{1+m} : F^{1+m+n} \to F^n, \pi_{1+m}(y, t_1, \cdots, t_m, x_1, \cdots, x_n) = (x_1, \cdots, x_n)$$

so that, as before, $f = \pi_{1+m} \circ \rho$. It turns out that $\rho(F^m - V') = \mathbf{V}(I)$. Obviously, it follows from the definitions that $\rho(F^m - V') \subseteq \mathbf{V}(I)$; to see why the converse is true, for any $(y, t_1, \cdots, t_m, x_1, \cdots, x_n) \in \mathbf{V}(I)$, then $1 - gy = 0$ implies $y = \frac{1}{g(t_1, \cdots, t_m)}$. Moreover, $g_i(t_1, \cdots, t_m)x_i - f_i(t_1, \cdots, t_m) = 0$ implies $x_i = \frac{f(t_1, \cdots, t_m)}{g(t_1, \cdots, t_m)}$, which shows that the point has a pre-image over ρ, and therefore is in $\rho(F^m - V')$. As before, we also see that

$$f(F^m - V') = \pi_{1+m}(\rho(F^m - \mathbf{V}(g))) = \pi_{1+m}(\mathbf{V}(I))$$

(Theorem) Solution to Rational Implicitization: *Let F be an infinite field, and define $f : F^m - V' \to F^n$, for $V' := \mathbf{V}(g), g = g_1 \cdots g_n$, as the function associated with the rational parameterization*

$$x_1 = \frac{f_1(t_1, \cdots, t_m)}{g_1(t_1, \cdots, t_m)}$$
$$\vdots$$
$$x_n = \frac{f_n(t_1, \cdots, t_m)}{g_n(t_1, \cdots, t_m)}$$

given by $f(t_1, \cdots, t_m) = (x_1, \cdots, x_n)$. Then $\mathbf{V}(I_{m+1})$ is the smallest affine variety in F^n containing $f(F^m - V')$, where $I = \langle g_1 x_1 - f_1, \cdots, g_n x_n - f_n, 1 - gy \rangle \subset F[y, t_1, \cdots, t_m, x_1, \cdots, x_n]$.

Proof: As before, clearly $f(F^m - V') = \pi_{m+1}(\mathbf{V}(I)) \subset \mathbf{V}(I_{m+1})$ as proven in the last section, so it only remains to prove that $\mathbf{V}(I_{m+1})$ is the smallest containing variety. As in the proof of the polynomial implicitization theorem, we will show that any polynomial $h \in F[x_1, \cdots, x_n]$ which vanishes on the range of the parameterization, that is, $f(F^m - V')$, is a member of I_{m+1}. This will prove the theorem because this means that the defining polynomials of any affine variety containing $f(F^m - V')$ are in I_{m+1}, which shows that the ideal J generated by the defining polynomials of the affine variety, is a subset of I_m, which implies $\mathbf{V}(I_m) \subset \mathbf{V}(J) = W$, as proven in an earlier chapter.

To prove this assumption, suppose $h \in F[x_1, \cdots, x_n]$ vanishes on $f(F^m - V')$. As with the polynomial implicitization theorem, we can show that $h \in I_m$ by showing that the remainder when h is divided by $g_i x_i - f_i$ is zero. However, this division is not enough to guarantee that r is only in variables $t_1, \cdots, t_m$; we first need to multiply by a sufficiently high power of g, say g^N:

$$g^N h = \sum_{i=1}^{n} q_i \cdot (g_i x_i - f_i) + r \text{ for some } r \in F[t_1, \cdots, t_m]$$

It follows that

$$\forall \left(a_1, \cdots, a_m, \frac{f_1(a_1, \cdots, a_m)}{g_1(a_1, \cdots, a_m)}, \cdots, \frac{f_n(a_1, \cdots, a_m)}{g_n(a_1, \cdots, a_m)} \right) \in F^{n+m} :$$

$$g(a_1,\cdots,a_m)^N h(a_1,\cdots,a_m) = g(a_1,\cdots,a_m)^N \cdot 0 = 0 = 0+\cdots+0+r(t_1,\cdots,t_m)$$

which implies that r is zero, since F and hence F^m are infinite.

It follows that $g^N h \in \langle g_1x_1 - f_1, \cdots, g_nx_n - f_n\rangle$. To account for the missing generator $1-gy$, we make use of the identity

$$h = g^N y^N h + h\cdot(1-g^N y^N) = y^N\cdot(g^N h) + h\cdot(1-gy)\sum_{k=1}^{N-1} g^k y^k$$

which follows from factoring $(1^N - (gy)^N)$ as a difference of N^{th} powers. Since $g^N h$ is a linear combination of $g_ix_i - f_i$, it follows that the above identity is an explicit description of h as a linear combination of $g_ix_i - f_i$ and $(1-gy)$. Hence, $h \in I$, and since $h \in F[x_1,\cdots,x_n]$ it follows that $h \in I_m$, which proves the theorem. □

We solved the polynomial implicitization problem by eliminating the parameters $t_1,\cdots,t_m$ from the equations $x_i = f(t_1,\cdots,t_m)$. The above solution to rational implicitization is similar - we transform the equations $x_i = \frac{f_i}{g_i}$ by clearing the denominators and adding a control to disallow the denominators from vanishing, thus preserving the integrity of the original equations, to obtain

$$\begin{aligned} g_1(t_1,\cdots,t_m)x_1 &= f_1(t_1,\cdots,t_m)\\ &\vdots\\ g_n(t_1,\cdots,t_m)x_n &= f_n(t_1,\cdots,t_m)\\ y\prod_{i=1}^{n} g_i(t_1,\cdots,t_m) &= 1 \end{aligned}$$

If we now eliminate the parameters $t_1,\cdots,t_m$ from this equation, the same way we eliminated them in polynomial implicitization, we reach the above solution. This gives rise to Kalkbrener's algorithm for solving rational implicitization - if we have $x_i = \frac{f_i}{g_i}$ for $f_i, g_i \in F[t_1,\cdots,t_m]$, then we can introduce a new variable y and form the ideal $I = \langle g_ix_i - f_i, 1-gy\rangle$ in $F[y,t_1,\cdots,t_m,x_1,\cdots,x_n]$, for $g = g_1\cdots g_n$. We can then compute a Groebner basis for I with respect to the lexicographic ordering $y > t_1 > \cdots > t_m > x_1 > \cdots > x_n$. The affine variety defined by the elements of the Groebner basis which contain only the variables we want, $x_1,\cdots,x_n$, is the smallest affine variety containing the parameterization.

4 Singular Points and Envelopes

This section will focus on the geometric aspects of elimination theory, and introduce some new geometric concepts concerning curves, and their relationship to polynomial equations. The topics we'll study are quite general and are studied in depth in many fields of math, from number theory to analysis. We'll show how many of the resulting equations and problems that arise with the study of these geometric topics can be solved with the techniques we've studied thus far. Specifically, we'll cover the singular points of a curve, and the envelope of a family of curves.

4.1 Singular Points

Singular points are points of polynomial curves which are not well-behaved, in the sense that there is no unique or even existing tangent line at that point. The notion of a tangent line really only makes sense for curves in the plane, so we'll focus on polynomial curves in two variables, though it is possible to generalize to curves in arbitrarily high dimensions.

More precisely, we can formalize polynomial curves as curves in F^2 defined by the level curves of a higher dimensional polynomial: $f(x,y) = 0$ for $f \in F[x,y]$. That is, we can recast the more general idea of a polynomial curve in terms of algebraic geometry, by simply defining it to be the equivalent affine variety, $\mathbf{V}(f)$. To formalize the notion of a tangent line, we'll give an algebraic definition: we can parameterize a line L passing through point $(a,b) \in \mathbf{V}(f)$ with

$$\begin{aligned} x &= a + m_1 t\\ y &= b + m_2 t \end{aligned}$$

Notice that by eliminating the parameter t, we get $y = b + m\cdot(x-a)$, the equation of a line in point-slope form, where $m = \frac{m_1}{m_2}$. By varying the slopes m_1, m_2, we can "rotate" the line through (a,b), covering all lines in the plane which pass through (a,b), and so we can use calculus to find the exact m_1, m_2 which give the tangent line to (a,b).

Let's first try to find the tangent line without calculus. For a polynomial $f \in F[x,y]$, if we want to find where the polynomial intersects line L, we might first force x, y to be on the line L, and then search for valid combinations of x and y which are also on the polynomial curve. To do this, we first let $x := a + m_1 t$ and $y = b + m_2 t$, and then search for points where $f(x,y) = 0$ (this is the equation which determines the polynomial curve). It follows that the roots of the polynomial $g(t) := f(a + m_1 t, b + m_2 t)$ determine where the line intersects $\mathbf{V}(f)$. If g has multiple roots, then there's more than one t which maps to points on the curve which intersect the line, implying that the curve intersects L multiple times. The exception

to this rule is when g has multiple roots in the special case of a single root t with multiplicity greater than one. Specifically, since the "first" intersection occurs, by design, at $t = 0$, the multiplicity of the root $t = 0$, which is always a root, is especially telling, and connected to the tangency of L to the curve at (a, b). This leads us to the following useful definition.

(Definition) Multiplicity between polynomial curve and line: *Let $\mathbf{V}(f)$, for $f \in F[x, y]$, be a polynomial curve in the plane, and L be a line intersecting $\mathbf{V}(f)$ at (a, b), parameterized by $\{(x, y) = (a + m_1 t, b + m_2 t), t \in \mathbb{R}\}$ in the plane. We say L **meets** $\mathbf{V}(f)$ **with multiplicity** m if $t = 0$ is a root of multiplicity m of the polynomial $f(a + m_1 t, b + m_2 t)$.*

Let's now prove the intuitively appealing idea that if a line meets a curve at a point with multiplicity greater than one, we've found the tangent line.

(Theorem) Tangent lines have non-unit multiplicity: *For $f \in F[x, y]$, let $\mathbf{V}(f)$ be a polynomial curve in the plane. Then for any $(a, b) \in \mathbf{V}(f)$, there is a unique line through (a, b) which meets $\mathbf{V}(f)$ with multiplicity greater than one if and only if $\nabla f(a, b) = (0, 0)$; otherwise, every line through (a, b) meets $\mathbf{V}(f)$ with multiplicity greater than one.*

• *Proof*: Let L be a line through $(a, b) \in \mathbf{V}(f)$, parameterized with

$$x = a + m_1 t$$
$$y = b + m_2 t$$

Seeing as we're using the gradient of f in this theorem, it shouldn't come as a surprise that we'll be making use of the lemma that for root $t = 0$ of polynomial $g(x)$, t has multiplicity greater than one if and only if $g'(t) = g'(0) = 0$. This is easy to see, since upon factoring t into real roots, $t = 0$ has multiplicity greater than one if $(x - t)^k$ divides $g(x)$, for $k > 1$ (recall that in elementary algebra, k was our definition of multiplicity), in which case clearly $g'(t) = 0$.
Let's compute $g'(t)$ using the chain rule:

$$g'(t) = m_1 \frac{\partial f}{\partial x}(a + m_1 t, b + m_2 t) + m_2 \frac{\partial f}{\partial y}(a + m_1 t, b + m_2 t)$$

$$\rightarrow g'(0) = m_1 \frac{\partial f}{\partial x}(a, b) + m_2 \frac{\partial f}{\partial y}(a, b)$$

If $\nabla f(a, b) \neq (0, 0)$, then $g'(0) = 0$ precisely when

$$\frac{m_1}{m_2} = -\frac{f_y(a, b)}{f_x(a, b)}$$

Recall that the above parameterization of L is equivalent to the point-slope form

$$y = b + m \cdot (x - a), m = \frac{m_1}{m_2}$$

It follows that because $m = \frac{m_1}{m_2} = -\frac{f_y(a,b)}{f_x(a,b)}$ is constant, all (m_1, m_2) which make $g'(t)$ zero parameterize the same line, which proves that L is unique, and that since $g'(t) = 0$, L meets the curve with multiplicity greater than one.
Conversely, if $\nabla f(a, b) = (0, 0)$ then $g'(0) = 0$, and thus $t = 0$ is a root of multiplicity greater than one, and so L meets $\mathbf{V}(f)$ at (a, b) with multiplicity greater than one. Since L was arbitrary, this proves the converse above, that $\nabla f(a, b) = (0, 0) \rightarrow$ every line meets with multiplicity greater than one. □

As we touched on above, the above theorem now allows us to conclude our formalization of the notion of a tangent line.

(Definition) Tangent line: *Let $\mathbf{V}(f)$, for $f \in F[x, y]$, be a polynomial curve in the plane. For $(a, b) \in \mathbf{V}(f)$, if $\nabla f(a, b) = (0, 0)$, then we define the **tangent line** at (a, b) to be the unique line which meets $\mathbf{V}(f)$ at (a, b) with multiplicity greater than one. In this case, we call (a, b) a **non-singular point** of $\mathbf{V}(f)$.*

*If instead $\nabla f(a, b) = (0, 0)$, then we say (a, b) is a **singular point** of $\mathbf{V}(f)$.*

It may appear that we've taken a roundabout approach to defining the notion of a tangent line; after all, in calculus we defined the notion quite simply with derivatives. However, as hinted by the relationship to the gradient of the polynomial, the above approach is an extension of the calculus approach, and applies to more general, less well-defined curves as the explicit smooth curves dealt with in basic calculus. Moreover, computing singular points using the above definition is very easy, as we have only to solve the system of equations

$$f = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial x} = 0$$

4.2 Envelopes

Envelopes are mathematical structures associated with families of curves in the plane. In the context in which we'll be studying them, a polynomial curve in the plane F^2, like the ones with which we've been working, that depends on some extra parameters defines a family of curves, depending on the value of the parameter. For example, $\{(x-t)^2+(y+t^2)^2=r^2\}$ defines the family of circles with centers on the parabola $f(t)=t^2$, with radius parameterized by r. The *envelope* of this family of curves is a curve which is simultaneously tangent to every curve in the family. In the above example, if the radius is constant, then the "bottom" (translated down by r) of the parabola on which the centers lie is simultaneously tangent to every circle in the family. To formalize these ideas, let's first precisely define the notion of a family of curves.

(Definition) Family of curves: *Given a polynomial $f \in F[x,y,t]$, fix $t \in F$ and denote the resulting variety $f(x,y,t)=0$ in F^2 as $\mathbf{V}(f_t)$. The **family of curves** determined by f is the set of varieties $\mathbf{V}(f_t)$ as t varies through F.*

Although technically f is a polynomial in x,y,t, we view it as determining a curve in F^2 with x,y; t is simply a "global" parameter used by f, and varying t gives new curves every single time. Let's now define envelopes.

(Definition) Envelope: *The **envelope** of a family of curves $\mathbf{V}(f_t)$ is*

$$\left\{(x,y) \in F^2 \text{ where } \exists t \text{ s.t. } f(x,y,t)=\frac{\partial f}{\partial t}(x,y,t)=0\right\}$$

• *Motivation*: We can link the above definition to the intuitive description of envelopes we gave, viewing the envelope of $\mathbf{V}(f_t)$ as a curve C where every point on C is tangent to some $f_t=0$ in the family. Suppose C is parameterized by

$$x=g(t)$$
$$y=h(t)$$

where we assume, in order for C to be a valid envelope, that every $(g(t),h(t))$ lies on $\mathbf{V}(f_t)$, to ensure that C meets every member of the family at least once. This gives the condition

$$f(g(t),h(t),t)=0$$

C meets $\mathbf{V}(f_t)$ at $(g(t),h(t))$, but to ensure that C is tangent to $\mathbf{V}(f_t)$ at $(g(t),h(t))$, we require that the tangent vector to C at $(g(t),h(t))$, given by $(g'(t),h'(t))$, is perpendicular to the gradient of $\mathbf{V}(f_t)$ at $(g(t),h(t))$. Thus, we can express this condition using the dot product of the two vectors:

$$\frac{\partial f}{\partial x}(g(t),h(t),t)\cdot g'(t)+\frac{\partial f}{\partial y}(g(t),h(t),t)\cdot h'(t)=0$$

Notice that if we differentiate the first condition, $f(g(t),h(t),t)=0$ with respect to t, we find

$$\frac{\partial f}{\partial t}(g(t),h(t),t)=0=\frac{\partial f}{\partial x}(g(t),h(t),t)\cdot g'(t)+\frac{\partial f}{\partial y}(g(t),h(t),t)\cdot h'(t)+\frac{\partial f}{\partial t}(g(t),h(t),t)=0+\frac{\partial f}{\partial t}(g(t),h(t),t)$$

if the second (dot product) condition is satisfied. Thus, the first and second conditions are equivalent to the third condition

$$\frac{\partial f}{\partial t}(g(t),h(t),t)=0$$

which leads to our definition above.

To find an explicit description of the envelope C, we need to use the above two conditions and eliminate the parameter t, giving a complete description of C as a polynomial curve in F^2. We can use the tools from elimination theory that we've been studying to accomplish this, using the same techniques we to solve the implicitization problem. First, we compute a Groebner basis G for $I=\langle f_t, \frac{\partial f_t}{\partial t}\rangle$ with respect to the lexicographic order $t>x>y$. Then, by the elimination theorem, the envelope must lie on the curve given by $\mathbf{V}(G_1)$, where $G_1=G\cap F[x,y]$. We know that the envelope must lie completely on this curve, but the question of whether every point on the curve is also on the envelope - this is equivalent to asking if every solution (x,y) of $f_t(x,y)=\frac{\partial f_t}{\partial t}(x,y)=0$ extends to complete solutions, which we can answer using the extension theorem.