Chapter 16

Algebraic Geometry for CAGD

Initially, the field of computer aided geometric design and graphics drew most heavily from differential geometry, approximation theory, and vector geometry. Since the early 1980's, some of the tools of algebraic geometry have been introduced into the CAGD literature. This chapter presents some of those tools, which can address the following problems:

1. Given a planar curve defined parametrically as $x = \frac{x(t)}{w(t)}$, $y = \frac{y(t)}{w(t)}$ where $x(t)$, $y(t)$, and $w(t)$ are polynomials, find an implicit equation $f(x, y) = 0$ which defines the same curve. This process of parametric to implicit conversion will be referred to as *implicitization.*

2. Given the (x, y) coordinates of a point which lies on a parametric curve $x = \frac{x(t)}{w(t)}$, $y = \frac{y(t)}{w(t)}$, find the parameter value t which corresponds to that point. This problem will be referred to as the *inversion* problem.

3. Compute the points of intersection of two parametric curves using the implicitization and inversion techniques.

Section 1.4 presents some preliminary terminology and theorems. Sections 16.1 through 16.4 discuss the implicitization and inversion of planar curves, and Section 16.5 applies those tools to computing curve intersections. Section 16.8 discusses some special properties of parametric cubic curves and Section 16.9 overviews surface implicitization. Section 16.11 discusses Gróbner bases.

16.1 Implicitization

It was noted that there are basically two ways that a planar curve can be defined: parametrically ($x = x(t)/w(t)$, $y = y(t)/w(t)$) and implicitly ($f(x, y) = 0$).

Obviously, the parametric equation of a curve has the advantage of being able to quickly compute the (x, y) coordinates of several points on the curve for plotting purposes. Also, it is simple to define a curve *segment* by restricting the parameter t to a finite range, for example $0 \leq t \leq 1$. On the other hand, the implicit equation of a curve enables one to easily determine whether a given point lies on the curve, or if not, which side of the curve it lies on.

Given these two different equations for curves, it is natural to wonder if it is possible to convert between representations for a given curve. The answer is that it is *always* possible to find an implicit equation of a parametric curve, but a parametric equation can generally be found only

for implicit curves of degree two or one. The process of finding the implicit equation of a curve which is expressed parametrically is referred to as *implicitization.* In Section 16.4, we will discuss how this can be accomplished using an important algebraic tool, the *resultant,* and Section 16.3 discusses resultants. Section 16.2 suggests how someone might tackle the implicitization problem before learning about resultants. Section 16.5 applies these ideas to the problem of intersecting two parametric curves.

16.2 Brute Force Implicization

Consider this simple example of parametric-to-implicit conversion: Given a line

$$x = t + 2 \qquad y = 3t + 1,$$

we can easily find an implicit equation which identically represents this line by solving for t as a function of x

$$t = x - 2$$

and substituting into the equation for y:

$$y = 3(x - 2) + 1$$

or $3x - y - 5 = 0$. Note that this implicit equation defines *precisely* the same curve as does the parametric equation. We can also identify two inversion equations (for finding the parameter value of a point on the line): $t = x - 2$ or $t = (y - 1)/3$.

This approach to implicitization also works for degree two parametric curves. Consider the parabola

$$x = t^2 + 1 \qquad y = t^2 + 2t - 2.$$

Again, we can solve for t as a function of x:

$$t = \pm\sqrt{x - 1}$$

and substitute into the equation for y:

$$y = (\sqrt{x - 1})^2 \pm 2\sqrt{x - 1} - 2.$$

We can isolate the radical and square both sides

$$(y - (x - 1) + 2)^2 = (\pm 2\sqrt{x - 1})^2$$

to yield

$$x^2 - 2xy + y^2 - 10x + 6y + 13 = 0$$

which is the desired implicit equation. Again, this implicit equation defines exactly the same curve as does the parametric equation.

We run into trouble if we try to apply this implicitization technique to curves of degree higher than two. Note that the critical step is that we must be able to express t as a function of x. For cubic and quartic equations, this can be done, but the resulting expression is hopelessly complex. For curves of degree greater than four, it is simply not possible.

We cannot obtain an inversion equation for this parabola the way we did for the straight line. For example, suppose we want to find the parameter of the point $(5, -2)$ which we know to lie on the curve. The brute force approach would be to find the values of t which satisfy the equation

$$x \;=\; 5 \;=\; t^2 \;+\; 1$$

and then to compare them with the values of t which satisfy the equation

$$y \;=\; -2 \;=\; t^2 \;+\; 2t \;-\; 2.$$

In the first case, we find t = -2 or 2, and in the second case, t = -2 or 0. The value of t which satisfies both equations is -2, which must therefore be the parameter value of the point (5,-2).

This unsuccessful attempt at implicitization and inversion motivates the following discussion of *resultants,* which will provide an elegant, general solution to the implicitization and inversion problems.

16.3 Polynomial Resultants

16.3.1 Definition of the Resultant of Two Polynomials

Polynomial resultants address the question of whether two polynomials have a common root. Consider the two polynomials

$$f(t) \;=\; \sum_{i=0}^{n} a_i t^i \qquad\qquad g(t) \;=\; \sum_{i=0}^{n} b_i t^i \tag{16.1}$$

The resultant of $f(t)$ and $g(t)$, written $R(f, g)$, is an expression for which $R(f, g) \;=\; 0$ if and only if$f(t)$ and $g(t)$ have a common root.

Consider the resultant of two polynomials given in factored form:

$$f(t) = (t - f_1)(t - f_2)\cdots(t - f_m), \qquad g(t) = (t - g_1)(t - g_2)\cdots(t - g_n) \tag{16.2}$$

where f_1, f_2, ... f_m are the roots of $f(t)$ and g_1, g_2, ... g_n are the roots of $g(t)$. The resultant of $f(t)$ and $g(t)$ is the unique polynomial expression that will be zero if and only if at least one f_i is the same as at least one g_i:

$$R(f, g) = \prod_{i=1}^{m}\prod_{j=1}^{n}(f_i - g_j)$$

For example, the resultant of $f(t) = t^2 - 7t + 12 = (t-3)(t-4)$ and $g(t) = t^2 - 3t + 2 = (t-2)(t-1)$ is

$$R(f, g) = (3 - 2)(3 - 1)(4 - 2)(4 - 1) = 12 \tag{16.3}$$

while the resultant of $f(t) = t^2 - 7t + 12 = (t - 3)(t - 4)$ and $g(t) = t^2 - 5t + 6 = (t - 2)(t - 3)$ is

$$R(f, g) = (3 - 2)(3 - 3)(4 - 2)(4 - 3) = 0.$$

Of course, if $f(t)$ and $g(t)$ are given in factored form, it is a trivial matter to detect if they have any common roots. However, it takes a fair amount of computation to determine all roots of a polynomial, and those roots are typically not rational and often complex. Therefore, of much greater value would an equation for a resultant that does *not* require the polynomials to be given in factored form, but can be computed directly from equations (16.1). The good news is that such equations for a resultant do exist and are relatively easy to compute, without needing to first compute any polynomial roots. Such an equation for the resultant can be written in closed form. Furthermore, if the polynomial coefficients are integers, the resultant will also be an integer, even if the roots are complex!

16.3.2 Resultant of Two Degree One Polynomials

The simplest resultant is for the case when $f(t)$ and $g(t)$ are degree one:

$$f(t) = a_1 t + a_0; \qquad g(t) = b_1 t + b_0.$$

The root of $f(t)$ and the root of $g(t)$ are easily found:

$$a_1 t + a_0 = 0 \;\rightarrow\; t = -\frac{a_0}{a_1}; \qquad b_1 t + b_0 = 0 \;\rightarrow\; t = -\frac{b_0}{b_1};$$

Since each polynomial has exactly one root, $f(t)$ and $g(t)$ have a *common* root if and only if

$$-\frac{a_0}{a_1} = \frac{b_0}{b_1}, \quad \text{or} \quad a_1 b_0 - b_1 a_0 = 0.$$

The resultant of $f(t)$ and $g(t)$ is thus

$$R(f, g) = a_1 b_0 - b_1 a_0. \tag{16.4}$$

We can also derive this resultant using matrix algebra. This will make more sense if we use the homogeneous form

$$f(T, U) = a_1 T + a_0 U; \qquad g(T, U) = b_1 T + b_0 U$$

where $t = T/U$ The equations $f(T, U) = 0$ and $g(T, U) = 0$ can be written

$$\begin{bmatrix} a_1 & a_0 \\ b_1 & b_0 \end{bmatrix} \begin{bmatrix} T \\ U \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \tag{16.5}$$

This is a system of homogeneous linear equations. We know from linear algebra that the necessary and sufficient condition for this system to have a solution is if the determinant of the matrix is zero, that is, if

$$\begin{vmatrix} a_1 & a_0 \\ b_1 & b_0 \end{vmatrix} = a_1 b_0 - b_1 a_0 = 0$$

This is the same equation as the resultant that we arrived at earlier.

This resultant can answer for us the question of whether two degree-one polynomials have a common root.

Example: Do $f(t) = 2t + 1$ and $g(t) = t + 3$ have a common root? They have a common root if and only if their resultant is zero. Since $R(f, g) = 2 \cdot 3 - 1 \cdot 1 = 5 \neq 0$, they do not have a common root.

Example: Do $f(t) = t - 2$ and $g(t) = 3t - 6$ have a common root? Since $R(f, g) = 1 \cdot (-6) - 3 \cdot (-2) = 0$, they do have a common root.

16.3.3 Resultants of Degree-Two Polynomials

The degree one resultant is obvious. Higher-degree resultants are not so obvious. Consider the degree two polynomials

$$f(t) = a_2 t^2 + a_1 t + a_0, \qquad g(t) = b_2 t^2 + b_1 t + b_0.$$

It does not work so well to solve for the roots of these two polynomials and check for a common root. The roots of $f(t)$ and $g(t)$ are, respectively,

$$t = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2a_0}}{2a_2}, \quad t = \frac{-b_1 \pm \sqrt{b_1^2 - 4b_2b_0}}{2b_2}$$

So, $f(t)$ and $g(t)$ have a common root if and only if

$$\frac{-a_1 + \sqrt{a_1^2 - 4a_2a_0}}{2a_2} = \frac{-b_1 + \sqrt{b_1^2 - 4b_2b_0}}{2b_2}, \text{ or } \frac{-a_1 + \sqrt{a_1^2 - 4a_2a_0}}{2a_2} = \frac{-b_1 - \sqrt{b_1^2 - 4b_2b_0}}{2b_2}, \text{ or}$$

$$\frac{-a_1 - \sqrt{a_1^2 - 4a_2a_0}}{2a_2} = \frac{-b_1 + \sqrt{b_1^2 - 4b_2b_0}}{2b_2}, \text{ or } \frac{-a_1 - \sqrt{a_1^2 - 4a_2a_0}}{2a_2} = \frac{-b_1 - \sqrt{b_1^2 - 4b_2b_0}}{2b_2}$$

But, the resultant we are looking for is a single expression in terms of a_0, a_1, a_2, b_0, b_1, and b_2 that will be zero if and only if one or more of the above expressions is true. We could accomplish that some algebraic manipulation of these equations, but there is an easier way, one that extends to polynomials of any degree.

For this degree-two case, the idea is to create a pair of degree-one polynomials $h_1(t)$ and $h_2(t)$ that will have a common root if and only if $f(t)$ and $g(t)$ have a common root. Those polynomials are:

$$\begin{aligned} h_1(t) &= a_2g(t) - b_2f(t) = a_2(b_2t^2 + b_1t + b_0) - b_2(a_2t^2 + a_1t + a_0) \\ &= (2,1)t + (2,0) \end{aligned} \tag{16.6}$$

where the notation $(a_ib_j) = a_ib_j - a_jb_i$. We also create

$$\begin{aligned} h_2(t) &= (a_2t + a_1)g(t) - (b_2t + b_1)f(t) \\ &= (a_2t + a_1)(b_2t^2 + b_1t + b_0) - (b_2t + b_1)(a_2t^2 + a_1t + a_0) \\ &= (a_2b_0)t + (a_1b_0) \end{aligned} \tag{16.7}$$

It is easy to verify that $h_1(t)$ and $h_2(t)$ will each vanish for any value of t that is a common root of $f(t)$ and $g(t)$. Therefore, any common root of $f(t)$ and $g(t)$ is also a common root of $h_1(t)$ and $h_2(t)$. Since we already have a resultant for two linear polynomials (16.4), the resultant of our two quadratic polynomials is

$$R(f,g) = \begin{vmatrix} (a_2b_1) & (a_2b_0) \\ (a_2b_0) & (a_1b_0) \end{vmatrix} \tag{16.8}$$

Example We again compute the resultant of $f(t) = t^2 - 7t + 12 = (t-3)(t-4)$ and $g(t) = t^2 - 3t + 2 = (t-2)(t-1)$, which we saw from (16.3) is equal to 12, but this time we use (**??**).

$$R(f,g) = \begin{vmatrix} (a_2b_1) & (a_2b_0) \\ (a_2b_0) & (a_1b_0) \end{vmatrix} = R(f,g) = \begin{vmatrix} 4 & -10 \\ -10 & 22 \end{vmatrix} = -12 \tag{16.9}$$

We should here note that a resultant computed by (**??**) and a resultant computed using (16.8) can differ by a sign, and that their absolute value will be equal if $a_2 = b_2 = 1$.

16.3.4 Resultants of Degree-Three Polynomials

We illustrate by finding the resultant of two cubic polynomials

$$f(t) = a_3t^3 + a_2t^2 + a_1t + a_0 \quad g(t) = b_3t^3 + b_2t^2 + b_1t + b_0.$$

In other words, we want to determine whether there exists a value α such that $f(\alpha) = g(\alpha) = 0$ without having to actually find all roots of both polynomials and comparing. We begin by forming three auxiliary polynomials $h_1(t)$, $h_2(t)$ and $h_3(t)$ as follows:

$$\begin{aligned} h_1(t) &= a_3g(t) - b_3f(t) \\ &= (a_3b_2)t^2 + (a_3b_1)t + (a_3b_0) \end{aligned}$$

where $(a_ib_j) \equiv (a_ib_j - a_jb_i)$ and

$$\begin{aligned} h_2(t) &= (a_3t + a_2)g(t) - (b_3t + b_2)f(t) \\ &= (a_3b_1)t^2 + [(a_3b_0) + (a_2b_1)]t + (a_2b_0) \end{aligned}$$

$$\begin{aligned} h_3(t) &= (a_3t^2 + a_2t + a_1)g(t) - (b_3t^2 + b_2t + b_1)f(t) \\ &= (a_3b_0)t^2 + (a_2b_0)t + (a_1b_0) \end{aligned}$$

Note that if there exists a value α such that $f(\alpha) = g(\alpha) = 0$, then $h_1(\alpha) = h_2(\alpha) = h_3(\alpha) = 0$. We can therefore say that $f(t)$ and $g(t)$ have a common root if and only if the set of equations

$$\begin{bmatrix} (a_3b_2) & (a_3b_1) & (a_3b_0) \\ (a_3b_1) & (a_3b_0) + (a_2b_1) & (a_2b_0) \\ (a_3b_0) & (a_2b_0) & (a_1b_0) \end{bmatrix} \begin{Bmatrix} t^2 \\ t \\ 1 \end{Bmatrix} = 0$$

has a solution. [1] However, we know from linear algebra that this set of homogeneous linear equations can have a solution if and only if

$$\begin{vmatrix} (a_3b_2) & (a_3b_1) & (a_3b_0) \\ (a_3b_1) & (a_3b_0) + (a_2b_1) & (a_2b_0) \\ (a_3b_0) & (a_2b_0) & (a_1b_0) \end{vmatrix} = 0$$

and therefore,

$$R(f,g) = \begin{vmatrix} (a_3b_2) & (a_3b_1) & (a_3b_0) \\ (a_3b_1) & (a_3b_0) + (a_2b_1) & (a_2b_0) \\ (a_3b_0) & (a_2b_0) & (a_1b_0) \end{vmatrix}$$

This same approach can be used to construct the resultant of polynomials of any degree.

Let's try this resultant on a couple of examples. First, let $f(t) = t^3 - 2t^2 + 3t + 1$ and $g(t) = 2t^3 + 3t^2 - t + 4$. For this case,

$$R(f,g) = \begin{vmatrix} 7 & -7 & 2 \\ -7 & -5 & -11 \\ 2 & -11 & 13 \end{vmatrix} = -1611$$

[1] Actually, we have only shown that this is a necessary condition. The proof that it is also sufficient can be found in [GSA84].

We aren't so much interested in the actual numerical value of the resultant, just whether it equals zero or not. In this case, $R(f,g) = -1611 \neq 0$, so we conclude that $f(t)$ and $g(t)$ do *not* have a common root.

Consider next the pair of polynomials $f(t) = t^3 - t^2 - 11t - 4$ and $g(t) = 2t^3 - 7t^2 - 5t + 4$. In this case,

$$R(f,g) = \begin{vmatrix} -5 & 17 & 12 \\ 17 & -60 & -32 \\ 12 & -32 & -64 \end{vmatrix} = 0$$

Since $R(f,g) = 0$, $f(t)$ and $g(t)$ *do* have a common root. Note that the resultant simply determines the existence or non-existence of a common root, but it does not directly reveal the value of a common root, if one exists. In fact, if the resultant is zero, there may actually be several common roots. Section 16.4 discusses how to compute the common root(s).

16.3.5 Resultants of Higher Degree Polynomials

The formulation of the resultant that we have presented is known as Bezout's resultant. For two polynomials of equal degree, Bezout's resultant is the determinant of an $n \times n$ matrix. The pattern you can observe in the resultants of degree two and degree three polynomials extends to any degree. Resultants for two polynomials of different degree also exist.

Another formulation for resultants, called Sylvester's resultant, is the determinant of a square matrix of size $2n \times 2n$. The pattern for Sylvester's resultant is even easier to see. For two degree-three polynomials, Sylvester's resultant is

$$R(f,g) = \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & 0 & 0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & 0 & a_3 & a_2 & a_1 & a_0 & 0 \\ b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & b_3 & b_2 & b_1 & b_0 & 0 \end{vmatrix}$$

Sylvester's resultant is equivalent to Bezout's resultant. Clearly, Bezout's resultant is more simple to expand.

16.4 Determining the Common Root

We present two basic approaches to finding the common root of two polynomials: by solving a set of linear equations, or by using Euclid's algorithm.

Linear Equation Approach Our intuitive development of the resultant of two cubic polynomials led us to a set of three linear equations in three "unknowns": t^2, t and 1. In general, we could create the resultant of two degree n polynomials $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$, $g(t) = b_n t^n + b_{n-1} t^{n-1} + \cdots + b_1 t + b_0$, as the determinant of the coefficient matrix of n homogeneous linear equations:

$$\begin{bmatrix} (a_n b_{n-1}) & . & . & . & (a_n b_0) \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ (a_n b_0) & . & . & . & (a_1 b_0) \end{bmatrix} \begin{Bmatrix} t^{n-1} \\ t^{n-2} \\ . \\ . \\ t \\ 1 \end{Bmatrix} = 0$$

It may be a bit confusing at first to view this as a set of homogeneous *linear* equations, since the unknowns are all powers of t. Let us temporarily switch to homogeneous variables T and U:

$$\begin{bmatrix} (a_n b_{n-1}) & . & . & . & (a_n b_0) \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ (a_n b_0) & . & . & . & (a_1 b_0) \end{bmatrix} \begin{Bmatrix} T^{n-1} \\ T^{n-2}U \\ . \\ . \\ TU^{n-2} \\ U^{n-1} \end{Bmatrix} = 0$$

where $t = T/U$. After solving for any two adjacent terms $T^{n-i}U^{i-1}$, the common root of $f(t)$ and $g(t)$ can be obtained as $t = \frac{T^{n-i+1}U^{i-2}}{T^{n-i}U^{i-1}}$.

Cramer's Rule There are several well known methods for solving for the $T^{n-i}U^{i-1}$. One way is to apply Cramer's rule. A non-trivial solution exists (that is, a solution other than all $T^{n-i}U^{i-1} = 0$) only if the determinant of the matrix is zero. But, that implies that the n equations are linearly dependent and we can discard one of them without losing any information. We discard the *last* equation, and can then solve for $n-1$ homogeneous equations in n homogeneous unknowns using Cramer's rule. It turns out that occasionally we run into trouble if we discard an equation other than the last one. We illustrate Cramer's rule for the case $f(t) = t^3 - t^2 - 11t - 4$ and $g(t) = 2t^3 - 7t^2 - 5t + 4$. Recall that this is the pair for which we earlier found that $R(f, g) = 0$. We have the set of equations

$$\begin{bmatrix} -5 & 17 & 12 \\ 17 & -60 & -32 \\ 12 & -32 & -64 \end{bmatrix} \begin{Bmatrix} T^2 \\ TU \\ U^2 \end{Bmatrix} = 0$$

Discarding the last equation, we obtain

$$\begin{bmatrix} -5 & 17 & 12 \\ 17 & -60 & -32 \end{bmatrix} \begin{Bmatrix} T^2 \\ TU \\ U^2 \end{Bmatrix} = 0$$

from which we find the common root using Cramer's rule:

$$t = \frac{TU}{U^2} = -\frac{\begin{vmatrix} -5 & 12 \\ 17 & -32 \end{vmatrix}}{\begin{vmatrix} -5 & 17 \\ 17 & -60 \end{vmatrix}} = 4$$

Gauss Elimination A numerically superior algorithm for solving this set of equations is to perform Gauss elimination. Two other advantages of Gauss elimination are that it can be used to determine whether the determinant is zero to begin with, and also it reveals *how many* common roots there are. We will illustrate this approach with three examples, using integer preserving Gauss elimination. We choose the integer preserving Gauss elimination because then the lower right hand element of the upper triangular matrix is the value of the determinant of the matrix.

Example 1

Our first example is one we considered earlier: $f(t) = t^3 - 2t^2 + 3t + 1$ and $g(t) = 2t^3 + 3t^2 - t + 4$. We set up the following set of linear equations, and triangularize the matrix using integer preserving Gauss elimination:

$$\begin{bmatrix} 7 & -7 & 2 \\ -7 & -5 & -11 \\ 2 & -11 & 13 \end{bmatrix} \begin{Bmatrix} T^2 \\ TU \\ U^2 \end{Bmatrix} =$$

$$\begin{bmatrix} 7 & -7 & 2 \\ 0 & -84 & 0 \\ 0 & 0 & -1611 \end{bmatrix} \begin{Bmatrix} T^2 \\ TU \\ U^2 \end{Bmatrix} = 0$$

We observe that the only solution to this set of equations is $T = U = 0$, and conclude that $f(t)$ and $g(t)$ do not have a common root. Note that the lower right element -1611 is the determinant of the original matrix, or the resultant.

Example 2

We next examine the pair of polynomials $f(t) = t^3 - t^2 - 11t - 4$ and $g(t) = 2t^3 - 7t^2 - 5t + 4$. In this case, we have

$$\begin{bmatrix} -5 & 17 & 12 \\ 17 & -60 & -32 \\ 12 & -32 & -64 \end{bmatrix} \begin{Bmatrix} T^2 \\ TU \\ U^2 \end{Bmatrix} =$$

$$\begin{bmatrix} -5 & 17 & 12 \\ 0 & 11 & -44 \\ 0 & 0 & 0 \end{bmatrix} \begin{Bmatrix} T^2 \\ TU \\ U^2 \end{Bmatrix} = 0$$

Again, the bottom right element is the value of the determinant, which verifies that the resultant is zero. It is now simple to compute the solution: $TU = 4U^2$, $T^2 = 4TU$. Since $t = T/U$, the common root is $t = 4$.

Example 3

For our final example we analyze the polynomials $f(t) = t^3 - 6t^2 + 11t - 6$ and $g(t) = t^3 - 7t^2 + 14t - 8$. Our linear equations now are:

$$\begin{bmatrix} -1 & 3 & -2 \\ 3 & -9 & 6 \\ -2 & 6 & -4 \end{bmatrix} \begin{Bmatrix} T^2 \\ TU \\ U^2 \end{Bmatrix} = \begin{bmatrix} -1 & 3 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{Bmatrix} T^2 \\ TU \\ U^2 \end{Bmatrix} = 0$$

In this case, not only is the resultant zero, but the matrix is rank 1. This means that there are *two* common roots, and they can be found as the solution to the quadratic equation $-t^2 + 3t - 2$, which is $t = 1$ and $t = 2$. Another way of saying this is that $-t^2 + 3t - 2$ is the *Greatest Common Divisor* of $f(t)$ and $g(t)$.

Euclid's GCD Algorithm An alternative approach to finding the common root(s) of two polynomials is to use Euclid's algorithm. This ancient algorithm can be used to find the *Greatest Common Divisor* of two integers or two polynomials. A clear proof of Euclid's algorithm can be found in [Kurosh '75]. Our presentation consists of a series of examples. This algorithm works beautifully in exact integer arithmetic but we have experienced numerical instability in floating point.

Integer Example

We illustrate first on a pair of integers: 42 and 30. For the first step, we assign the larger to be the numerator, and the other to be the denominator:

Step 1: $\frac{42}{30} = 1$ remainder 12.

We now take the remainder of the first step and divide it into the denominator of the first step:

Step 2: $\frac{30}{12} = 2$ remainder 6.

We continue dividing the remainder of the preceding step into the denominator of the preceding step until we obtain a zero remainder. This happens to occur in the third step for this problem:

Step 3: $\frac{12}{6} = 2$ exactly.

According to Euclid's algorithm, the second to last remainder is the GCD. In this case, the second to last remainder is 6, which is clearly the largest integer that evenly divides 30 and 42.

Polynomial Example 1

We illustrate how Euclid's algorithm works for polynomials by using the same three examples we used in the previous section. For the polynomials $f(t) = t^3 - 2t^2 + 3t + 1$ and $g(t) = 2t^3 + 3t^2 - t + 4$, we have:

- Step 1: $\frac{2t^3 + 3t^2 - t + 4}{t^3 - 2t^2 + 3t + 1} = 2$ remainder $7t^2 - 7t + 2$.
- Step 2: $\frac{t^3 - 2t^2 + 3t + 1}{7t^2 - 7t + 2} = \frac{t - 1}{7}$ remainder $\frac{12t+9}{7}$
- Step 3: $\frac{7t^2 - 7t + 2}{(12t + 9)/7} = \frac{196t - 343}{48}$ remainder $\frac{1253}{16}$
- Step 4: $\frac{(12t + 9)/7}{1253/16} = \frac{192t}{8771} + \frac{144}{8771}$ remainder 0.

In this case, the GCD is $\frac{1253}{16}$, which is merely a constant, and so $f(t)$ and $g(t)$ do not have a common root.

Polynomial Example 2

We next analyze the polynomials $f(t) = t^3 - t^2 - 11t - 4$ and $g(t) = 2t^3 - 7t^2 - 5t + 4$:

- Step 1: $\frac{2t^3 - 7t^2 - 5t + 4}{t^3 - t^2 - 11t - 4} = 2$ remainder $-5t^2 + 17t + 12$.
- Step 2: $\frac{t^3 - t^2 - 11t - 4}{-5t^2 + 17t + 12} = -5t - \frac{12}{25}$ remainder $\frac{-11t + 44}{25}$
- Step 3: $\frac{-5t^2 + 17t + 12}{(-11t + 44)/25} = 125t + \frac{75}{11}$ remainder 0.

In this case, the GCD is $\frac{-11t + 44}{25}$, and the common root is $t = 4$.

Polynomial Example 3

Finally, consider $f(t) = t^3 - 6t^2 + 11t - 6$ and $g(t) = t^3 - 7t^2 + 14t - 8$:

- Step 1: $\frac{t^3 - 6t^2 + 11t - 6}{t^3 - 7t^2 + 14t - 8} = 1$ remainder $t^2 - 3t + 2$
- Step 2: $\frac{t^3 - 7t^2 + 14t - 8}{t^2 - 3t + 2} = t - 4$ remainder 0.

The GCD is $t^2 - 3t + 2$, and the common roots are the roots of the equation $t^2 - 3t + 2 = 0$ which are $t = 1$ and $t = 2$.

You may have realized that there is a close connection between Euclid's algorithm and resultants, and obviously Euclid's algorithm does everything for us that resultants do.

We are now prepared to apply these tools to the problems of implicitizing and inverting curves.

16.5 Implicitization and Inversion

We discussed in the previous section a tool for determining whether two polynomials have a common root. We want to apply that tool to converting the parametric equation of a curve given by $x = \frac{x(t)}{w(t)}$, $y = \frac{y(t)}{w(t)}$ into an implicit equation of the form $f(x, y) = 0$. We proceed by forming two auxiliary polynomials:

$$p(x,t) = w(t)x - x(t) \qquad q(y,t) = w(t)y - y(t)$$

Note that $p(x, t) = q(y, t) = 0$ only for values of x, y, and t which satisfy the relationships $x = \frac{x(t)}{w(t)}$ and $y = \frac{y(t)}{w(t)}$. View $p(x, t)$ as a polynomial in t whose coefficients are linear in x, and view $q(y, t)$ as a polynomial in t whose coefficients are linear in y. If

$$x(t) = \sum_{i=0}^{n} a_i t^i, \qquad y(t) = \sum_{i=0}^{n} b_i t^i, \qquad w(t) = \sum_{i=0}^{n} d_i t^i$$

then

$$\begin{aligned} p(x,t) &= (d_n x - a_n)t^n + (d_{n-1}x - a_{n-1})t^{n-1} + \cdots \\ &\quad + (d_1 x - a_1)t + (d_0 x - a_0) \\ q(y,t) &= (d_n y - b_n)t^n + (d_{n-1}y - b_{n-1})t^{n-1} + \cdots \\ &\quad + (d_1 y - b_1)t + (d_0 y - b_0) \end{aligned}$$

If we now compute the resultant of $p(x, t)$ and $q(y, t)$, we do not arrive at a numerical value, but rather a *polynomial* in x and y which we shall call $f(x, y)$. Clearly, any (x, y) pair for which $f(x, y) = 0$ causes the resultant of p and q to be zero. But, if the resultant is zero, then we know that there exists a value of t for which $p(x, t) = q(y, t) = 0$. In other words, all (x, y) for which $f(x, y) = 0$ lie on the parametric curve and therefore $f(x, y) = 0$ is the implicit equation of that curve. This should be clarified by the following examples.

Implicitization Example 1

Let's begin by applying this technique to the parabola we implicitized earlier using a brute force method:

$$x = t^2 + 1 \qquad y = t^2 + 2t - 2.$$

We begin by forming $p(x,t) = -t^2 + (x-1)$ and $q(y,t) = -t^2 - 2t + (y+2)$. The resultant of two quadratic polynomials $a_2t^2 + a_1t + a_0$ and $b_2t^2 + b_1t + b_0$ is

$$\begin{vmatrix} (a_2b_1) & (a_2b_0) \\ (a_2b_0) & (a_1b_0) \end{vmatrix}$$

and so the resultant of $p(x,t)$ and $q(y,t)$ is

$$R(p,q) = \begin{vmatrix} 2 & x-y-3 \\ x-y-3 & 2x-2 \end{vmatrix} =$$

$$-x^2 + 2xy - y^2 + 10x - 6y - 13$$

which is the implicit equation we arrived at earlier.

We can write an inversion equation for this curve – something which eluded us in our ad hoc approach:

$$\begin{bmatrix} 2 & x-y-3 \\ x-y-3 & 2x-2 \end{bmatrix} \begin{Bmatrix} t \\ 1 \end{Bmatrix} = 0$$

From which $t = \frac{-x+y+3}{2}$ or $t = \frac{-2x+2}{x-y-3}$.

Implicitization Example 2

We now implicitize the cubic curve for which

$$x = \frac{2t^3 - 18t^2 + 18t + 4}{-3t^2 + 3t + 1}$$

$$y = \frac{39t^3 - 69t^2 + 33t + 1}{-3t^2 + 3t + 1}$$

We begin by forming $p(x,t)$ and $q(y,t)$:

$$p(x,t) = -2t^3 + (-3x + 18)t^2 + (3x - 18)t + (x - 4)$$

$$q(y,t) = -39t^3 + (-3y + 69)t^2 + (3y - 33)t + (y - 1)$$

Recalling from Section 16.3 that the resultant of two cubic polynomials $a_3t^3 + a_2t^2 + a_1t + a_0$ and $a_3t^3 + a_2t^2 + a_1t + a_0$ is

$$\begin{vmatrix} (a_3b_2) & (a_3b_1) & (a_3b_0) \\ (a_3b_1) & (a_3b_0)+(a_2b_1) & (a_2b_0) \\ (a_3b_0) & (a_2b_0) & (a_1b_0) \end{vmatrix},$$

we have

$$R(p,q) = f(x,y) =$$

$$\begin{vmatrix} -117x + 69y + 564 & 117x - 6y - 636 & 39x - 2y - 154 \\ 117x - 6y - 636 & -69x - 2y + 494 & -66x + 6y + 258 \\ 39x - 2y - 154 & -66x - 2y + 258 & 30x - 6y - 114 \end{vmatrix}.$$

We can expand the determinant to get

$$f(x,y) = -156195x^3 + 60426x^2y - 7056xy^2 + 224y^3 + 2188998x^2 - 562500xy + 33168y^2 - 10175796x + 1322088y + 15631624$$

We can obtain an inversion equation using Cramer's rule:

$$t = \frac{T^2}{TU} = -\frac{\begin{vmatrix} (117x - 6y - 636) & (39x - 2y - 154) \\ (-69x - 2y + 494) & (-66x + 6y + 258) \end{vmatrix}}{\begin{vmatrix} (-117x + 69y + 564) & (39x - 2y - 154) \\ (117x - 6y - 636) & (-66x + 6y + 258) \end{vmatrix}}$$

Alternately, we could use Gauss elimination to compute the parameter of a point on the curve. Cramer's rule has the appeal that it actually generates an *equation.*

We have intentionally carried out all computations in exact integer arithmetic to emphasize the rational, non-iterative nature of implicitization and inversion. Since the coefficients of the implicit equation are obtained from the coefficients of the parametric equations using only multiplication, addition and subtraction, it is possible to obtain an implicit equation which *precisely* defines the same point set as is defined by the parametric equations.

16.6 Implicitization in Bézier Form

From the paper [SP86a], a Bézier curve can be implicitized as follows. (Note that the value l_{ij} in these notes is equivalent to the value $L_{j,k+1}$ in the paper).

A degree 2 Bézier curve can be implicitized:

$$f(x,y) = \begin{vmatrix} l_{01}(x,y) & l_{02}(x,y) \\ l_{02}(x,y) & l_{12}(x,y) \end{vmatrix}$$

and a degree 3 Bézier curve can be implicitized

$$f(x,y) = \begin{vmatrix} l_{01}(x,y) & l_{02}(x,y) & l_{03}(x,y) \\ l_{02}(x,y) & l_{03}(x,y) + l_{12}(x,y) & l_{13}(x,y) \\ l_{03}(x,y) & l_{13}(x,y) & l_{23}(x,y) \end{vmatrix}$$

where

$$l_{ij}(x,y) = \binom{n}{i}\binom{n}{j} w_i w_j \begin{vmatrix} x & y & 1 \\ x_i & y_i & 1 \\ x_j & y_j & 1 \end{vmatrix}$$

with n the degree of the curve, and x_i, y_i, w_i the coordinates and weight of the i^{th} control point.

For a general degree n curve, the implicit equation is

$$f(x,y) = \begin{vmatrix} L_{0,0}(x,y) & \cdot & \cdot & \cdot & L_{0,n-1}(x,y) \\ \cdot & & \cdot & \cdot & \cdot \\ L_{n-1,0}(x,y) & \cdot & \cdot & \cdot & L_{n-1,n-1}(x,y) \end{vmatrix}$$

where

$$L_{i,j} = \sum_{\substack{k \le \min(i,j) \\ k+m=i+j+1}} l_{km}.$$

16.6.1 Inversion of Bézier Curves

Inversion is accomplished by solving a set of equation. For the degree-two case, we solve

$$\begin{bmatrix} l_{01}(x,y) & l_{02}(x,y) \\ l_{02}(x,y) & l_{12}(x,y) \end{bmatrix} \begin{Bmatrix} (1-t) \\ t \end{Bmatrix} = 0.$$

For example, using the top row of the matrix, we can compute

$$t = \frac{l_{01}}{l_{01} - l_{02}}.$$

For the degree-three case, we can solve

$$\begin{bmatrix} l_{01}(x,y) & l_{02}(x,y) & l_{03}(x,y) \\ l_{02}(x,y) & l_{03}(x,y) + l_{12}(x,y) & l_{13}(x,y) \\ l_{03}(x,y) & l_{13}(x,y) & l_{23}(x,y) \end{bmatrix} \begin{Bmatrix} (1-t)^2 \\ t(1-t) \\ t^2 \end{Bmatrix} = 0 \tag{16.10}$$

using Cramer's rule. This will give us an inversion equation

$$t = \frac{f(x,y)}{g(x,y)}$$

where $f(x,y)$ and $g(x,y)$ are degree-two polynomials in x and y.

For a degree-three curve, we can obtain an inversion equation for which $f(x,y)$ and $g(x,y)$ are linear in x and y. If $\mathbf{P}_0$, $\mathbf{P}_1$, and $\mathbf{P}_2$ are not collinear, there exist constants c_1 and c_2,

$$c_1 = \frac{w_3 \begin{vmatrix} x_0 & y_0 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix}}{3w_1 \begin{vmatrix} x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{vmatrix}}, \qquad c_2 = -\frac{w_3 \begin{vmatrix} x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \\ x_3 & y_3 & 1 \end{vmatrix}}{3w_2 \begin{vmatrix} x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{vmatrix}}$$

such that if we multiple the first row of the matrix in (16.10) by c_1 and the second row by c_2 and add them to the third row, the lower-left entry of the matrix vanishes. Let

$$l_a(x,y) = c_1 l_{02}(x,y) + c_2[l_{03}(x,y) + l_{12}(x,y)] + l_{13}(x,y)$$

and

$$l_b(x,y) = c_1 l_{03}(x,y) + c_2 l_{13}(x,y) + l_{23}(x,y).$$

The resulting third row of the matrix is thus

$$[0 \quad l_a(x,y) \quad l_b(x,y)]$$

and the equation corresponding to that row is

$$l_a(x,y)t(1-t) + l_b(x,y)t^2 = 0$$

from which

$$t = \frac{l_a(x,y)}{l_a(x,y) - l_b(x,y)}.$$

16.7 Curve Inversion Using Linear Algebra

We now present a simple approach to curve inversion that does not involve resultants. For a rational curve of degree n, we can generally write the inversion equation in the form:

$$t = \frac{f(x,y)}{g(x,y)} \tag{16.11}$$

where $f(x,y)$ and $g(x,y)$ are polynomials of degree $n-2$ if $n > 2$, and degree one if $n = 2$. Since we are mainly interested in curves of degree two and three, $f(x,y)$ and $g(x,y)$ are just degree one in those cases.

Suppose we want to find the inversion equation for a rational cubic curve (in homogeneous form)

$$x(t) = x_0 + x_1 t + x_2 t^2 + x_3 t^3$$
$$y(t) = y_0 + y_1 t + y_2 t^2 + y_3 t^3$$
$$w(t) = w_0 + w_1 t + w_2 t^2 + w_3 t^3$$

Denote

$$f(x,y,w) = a_2 x + b_2 y + c_2 w; \qquad g(x,y,w) = a_1 x + b_1 y + c_1 w. \tag{16.12}$$

To find an inversion equation for a cubic curve, we need just determine the coefficients $a_1, a_2, b_1, b_2, c_1, c_2$ such that

$$\frac{f(x(t),y(t),w(t))}{g(x(t),y(t),w(t))} \equiv t \tag{16.13}$$

or

$$t \cdot g(x(t),y(t),w(t)) - f(x(t),y(t),w(t)) \equiv 0 \tag{16.14}$$

or

$$t \cdot [a_1(x_0 + x_1 t + x_2 t^2 + x_3 t^3) + b_1(y_0 + y_1 t + y_2 t^2 + y_3 t^3) + c_1(w_0 + w_1 t + w_2 t^2 + w_3 t^3)]$$
$$-[a_2(x_0 + x_1 t + x_2 t^2 + x_3 t^3) + b_2(y_0 + y_1 t + y_2 t^2 + y_3 t^3) + c_2(w_0 + w_1 t + w_2 t^2 + w_3 t^3)] \equiv 0$$

or

$$\begin{aligned}
t^4 &\quad [a_1 x_3 + b_1 y_3 + c_1 w_3] \\
+t^3 &\quad [a_1 x_2 + b_1 y_2 + c_1 w_2 + a_2 x_3 + b_2 y_3 + c_2 w_3] \\
+t^2 &\quad [a_1 x_1 + b_1 y_1 + c_1 w_1 + a_2 x_2 + b_2 y_2 + c_2 w_2] \\
+t^1 &\quad [a_1 x_0 + b_1 y_0 + c_1 w_0 + a_2 x_1 + b_2 y_1 + c_2 w_1] \\
+ &\quad [a_2 x_0 + b_2 y_0 + c_2 w_0] \equiv 0.
\end{aligned} \tag{16.15}$$

This equation will be identically equal to zero if and only if all of the coefficients of the power of t are all zero. Thus, we can solve for the a_i, b_i, and c_i from the set of linear equations:

$$\begin{bmatrix} x_3 & y_3 & w_3 & 0 & 0 & 0 \\ x_2 & y_2 & w_2 & x_3 & y_3 & w_3 \\ x_1 & y_1 & w_1 & x_2 & y_2 & w_2 \\ x_0 & y_0 & w_0 & x_1 & y_1 & w_1 \\ 0 & 0 & 0 & x_0 & y_0 & w_0 \end{bmatrix} \begin{bmatrix} a_1 \\ b_1 \\ c_1 \\ a_2 \\ b_2 \\ c_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{16.16}$$

Of course, degree two curves are even more simple. Note that we can also find inversion equations for 3D curves using this method.

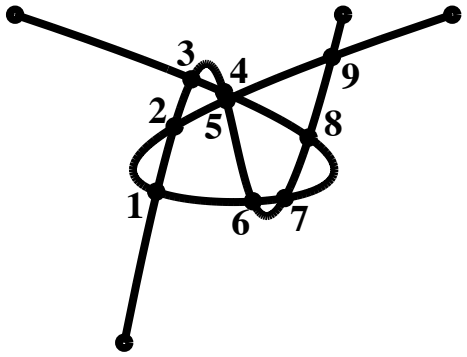

Figure 16.1: Two cubic curves intersecting nine times

16.8 Curve-Curve Intersections

Given one curve defined by the implicit equation $f(x,y) = 0$ and a second curve defined by the parametric equations $x = x(t)$, $y = y(t)$, we replace all occurrences of x in the implicit equation by $x(t)$, and replace all occurrences of y in the implicit equation by $y(t)$. These substitutions create a polynomial $f(x(t),y(t)) = g(t)$ whose roots are the parameter values of the points of intersection. Of course, if we start off with two parametric curves, we can first implicitize one of them.

We illustrate this process by intersecting the curve

$$x = \frac{2t_1^3 - 18t_1^2 + 18t_1 + 4}{-3t_1^2 + 3t_1 + 1}$$

$$y = \frac{39t_1^3 - 69t_1^2 + 33t_1 + 1}{-3t_1^2 + 3t_1 + 1}$$

with the curve

$$x = \frac{-52t_2^3 + 63t_2^2 - 15t_2 + 7}{-37t_2^2 + 3t_2 + 1}$$

$$y = \frac{4}{-37t_2^2 + 3t_2 + 1}$$

The two curves intersect nine times, which is the most that two cubic curves can intersect. [2] We already implicitized the first curve (in Section 16.3), so our intersection problem requires us to make the substitutions $x = \frac{-52t_2^3 + 63t_2^2 - 15t_2 + 7}{-37t_2^2 + 3t_2 + 1}$ and $y = \frac{4}{-37t_2^2 + 3t_2 + 1}$ into the implicit equation of curve 1:

$$f(x,y) = -156195x^3 + 60426x^2y - 7056xy^2 + 224y^3 +$$

[2] Bezout's theorem states that two curves of degree m and n respectively, intersect in mn points, if we include complex points, points at infinity, and multiple intersections.

$$2188998x^2 - 562500xy + 33168y^2 - 10175796x + 1322088y + 15631624.$$

After multiplying through by $(-37t_2^2 + 3t_2 + 1)^3$, we arrive at the intersection equation:

$$984100t_2^9 - 458200t_2^8 + 8868537t_2^7 - 9420593t_2^6 + 5949408t_2^5 - 2282850t_2^4 + 522890t_2^3 - 67572t_2^2 + 4401t_2 - 109 = 0.$$

Again, we have carried out this process in exact integer arithmetic to emphasize that this equation is an *exact* representation of the intersection points.

We now compute the roots of this degree 9 polynomial. Those roots are the parameter values of the points of intersection. The (x, y) coordinates of those intersection points can be easily found from the parametric equation of the second curve, and the parameter values on the first curve for the intersection points can be found from the inversion equations. The results are tabulated below.

Intersection Number	t_1 **Parameter of Curve 1**	**Coordinates of Point**	t_2 **Parameter of Curve 2**
1	0.0621	(4.2982,2.3787)	0.3489
2	0.1098	(4.4556,2.9718)	0.1330
3	0.1785	(4.6190,3.4127)	0.9389
4	0.3397	(4.9113,3.2894)	0.9219
5	0.4212	(4.9312,3.2186)	0.0889
6	0.6838	(5.1737,2.2902)	0.5339
7	0.8610	(5.4676,2.3212)	0.5944
8	0.9342	(5.6883,2.8773)	0.8463
9	0.9823	(5.9010,3.6148)	0.0369

The most common curve intersection algorithms are currently based on subdivision. Tests indicate that this implicitization algorithm is faster than subdivision methods for curves of degree two and three, and subdivision methods are faster for curves of degree five and greater [Sederberg et al '86].

16.9 Surfaces

Implicitization and inversion algorithms exist for surfaces, also (see [Sederberg '83] or [Sederberg et al. '84b]). But, whereas curve implicitization yields implicit equations of the same degree as the parametric equations, surface implicitization experiences a degree explosion. A triangular surface patch, whose parametric equations are of the form

$$x = \frac{\sum_{i+j\le n} x_{ij} s^i t^j}{\sum_{i+j\le n} w_{ij} s^i t^j} \qquad y = \frac{\sum_{i+j\le n} y_{ij} s^i t^j}{\sum_{i+j\le n} w_{ij} s^i t^j}$$

$$z = \frac{\sum_{i+j\le n} z_{ij} s^i t^j}{\sum_{i+j\le n} w_{ij} s^i t^j} \qquad i, j \ge 0,$$

generally has an implicit equation of degree n^2. A tensor product surface patch, whose parametric equations are of the form

$$x = \frac{\sum_{i=0}^{n}\sum_{j=0}^{m} x_{ij} s^i t^j}{\sum_{i=0}^{n}\sum_{j=0}^{m} w_{ij} s^i t^j} \qquad y = \frac{\sum_{i=0}^{n}\sum_{j=0}^{m} y_{ij} s^i t^j}{\sum_{i=0}^{n}\sum_{j=0}^{m} w_{ij} s^i t^j}$$

$$z = \frac{\sum_{i=0}^{n}\sum_{j=0}^{m} z_{ij}s^i t^j}{\sum_{i=0}^{n}\sum_{j=0}^{m} w_{ij}s^i t^j},$$

generally has an implicit equation of degree 2mn. Thus, a bicubic patch generally has an implicit equation $f(x, y, z) = 0$ of degree 18. Such an equation has 1330 terms!

Algebraic geometry shares important information on the nature of intersections of parametric surfaces. Recall that Bezout's theorem states that two surfaces of degree m and n respectively intersect in a curve of degree mn. Thus, two bicubic patches generally intersect in a curve of degree 324.

We have noted that bilinear patches have an implicit equation of degree 2; quadratic patches have an implicit equation of degree 4; biquadratic patches have an implicit equation of degree 8, etc. It seems highly curious that there are gaps in this sequence of degrees. Are there no parametric surfaces whose implicit equation is degree 3 or 5 for example? It turns out that parametric surfaces of degree n only *generally* have implicit equations of degree n^2 and that under certain conditions that degree will decrease. To understand the nature of those conditions, we must understand why the implicit equation of a parametric surface is generally n^2. The *degree* of a surface can be thought of either as the degree of its implicit equation, or as the number of times it is intersected by a line. Thus, the degree of the implicit equation of a parametric surface can be found by determining the number of times it is intersected by a line. Consider a parametric surface given by

$$x = \frac{x(s,t)}{w(s,t)} \quad y = \frac{y(s,t)}{w(s,t)} \quad z = \frac{z(s,t)}{w(s,t)},$$

where the polynomials are of degree n. One way we can compute the points at which a line intersects the surface is by intersecting the surface with two planes which contain the line. If one plane is $Ax + By + Cz + Dw = 0$, its intersection with the surface is a curve of degree n in s, t space: $Ax(s,t) + By(s,t) + Cz(s,t) + Dw(s,t) = 0$. The second plane will also intersect the surface in a degree n curve in parameter space. The points at which these two section curves intersect will be the points at which the line intersects the surface. According the Bezout's theorem, two curves of degree n intersect in n^2 points. Thus, the surface is generally of degree n^2.

16.10 Base Points

It may happen that there are values of s, t for which $x(s,t) = y(s,t) = z(s,t) = w(s,t) = 0$. These are known as *base points* in contemporary algebraic geometry. If a base point exists, any plane section curve will contain it. Therefore, it will belong to the set of intersection points of any pair of section curves. However, since a base point maps to something that is undefined in x, y, z space, it does not represent a point at which the straight line intersects the surface, and thus *the existence of a base point diminishes the degree of the implicit equation by one.* Thus, if there happen to be r base points on a degree n parametric surface, the degree of its implicit equation is $n^2 - r$.

For example, it is well known that any quadric surface can be expressed in terms of degree 2 parametric equations. However, in general, a degree 2 parametric surface has an implicit equation of degree 4, and we conclude that there must be two base points. Consider the parametric equations of a sphere of radius r centered at the origin:

$$x = 2rs^u$$

$$y = 2rtu$$

$$z = r(u^2 - s^2 - t^2)$$

$$w \;=\; s^2 \;+\; t^2 \;+\; u^2$$

Homogeneous parameters s, t, u are used to enable us to verify the existence of the two base points: $s = 1,\ t = i,\ u = 0$ and $s = 1,\ t = -i,\ u = 0$.

16.11 Ideals and Varieties

This section presents a brief overview of ideals and varieties and suggests some ways how these topics fit into CAGD. An excellent treatment of ideals and varieties and their application to CAGD can be found in [CLO92].

16.11.1 Ideals of Integers

An ideal I of integers is an infinite set of integers such that, if $a, b \in I$, then $a + b \in I$ and if c is any integer, then $c \cdot a \in I$. Ideals can be defined by a set of "generators" as follows. If $\{i_1, \ldots, i_n\}$ is a set of integers, then we denote by

$$I = \langle i_1, i_2, \ldots, i_n \rangle$$

the ideal generated by $\{i_1, \ldots, i_n\}$. This means that I is the infinite set of all integers that can be expressed as $c_1 i_1 + c_2 i_2 + \ldots + c_n i_n$ where the c_j are integers. We refer to $\{i_1, \ldots, i_n\}$ as a generating set of I.

For example, consider the ideal $I = \langle 6, 9 \rangle$. Obviously, all members of the generating set belong to the ideal: in this case, $6, 9 \in I$. Also, zero belongs to every ideal. For this ideal, we can see that $21 \in I$, because $21 = 6 \cdot 2 + 9 \cdot 1$, and $3 \in I$, because $3 = 2 \cdot 6 - 1 \cdot 9$.

A powerful concept in ideal theory is that every ideal has more than one set of generators.
Theorem: Two ideals $A = \langle i_1, \ldots, i_n \rangle$ and $B = \langle j_1, \ldots, j_m \rangle$ are equivalent if and only if

$$i_k \in B, k = 1, \ldots, n \quad \text{and} \quad j_k \in A,\ k = 1, \ldots, m.$$

The proof is straightforward.

From this theorem, we see that $\langle 6, 9 \rangle = \langle 12, 15 \rangle$ because $6, 9 \in \langle 12, 15 \rangle$ and $12, 15 \in \langle 6, 9 \rangle$. We also see that $\langle 6, 9 \rangle = \langle 3 \rangle$! An ideal that can be generated by a single generator is called a principal ideal. All ideals of integers are principal ideals. Furthermore, the single generator of $A = \langle i_1, \ldots, i_n \rangle$ is the greatest common divisor of $i_1, \ldots, i_n$.

16.11.2 Ideals of Polynomials in One Variable

Given a set of polynomials in t with real coefficients $\{f_1(t), f_2(t), \ldots f_n(t)\}$,

$$I = \langle f_1(t), f_2(t), \ldots, f_n(t) \rangle$$

is the ideal generated by $\{f_1(t), f_2(t), \ldots f_n(t)\}$ and is defined as the infinite set of polynomials in t that can be created as $f_1(t)g_1(t) + f_2(t)g_2(t) + \ldots + f_n(t)g_n(t)$ where the $g_i(t)$ are any polynomials in t with real coefficients. All ideals of polynomials in one variable are principle ideals, and the single generator is the GCD of all polynomials in the ideal.

16.11.3 Polynomials in Several Variables

In general, a polynomial in n variables $x_1, \ldots, x_n$ is defined

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{\tau} c_i x_1^{e_{1,i}} x_2^{e_{2,i}} \cdots x_n^{e_{n,i}}. \tag{16.17}$$

Each summand $c_i x_1^{e_{1,i}} x_2^{e_{2,i}} \cdots x_n^{e_{n,i}}$ is called a *term*, $x_1^{e_{1,i}} x_2^{e_{2,i}} \cdots x_n^{e_{n,i}}$ is a *monomial*, and c_i is the *coefficient* of the monomial. By convention, any given monomial occurs in at most one term in a polynomial.

$k[x_1, \ldots, x_n]$ signifies the set of all polynomials in the variables $x_1, \ldots, x_n$ whose coefficients belong to a field k. For example, $R[x, y]$ is the set of all polynomials

$$\sum c_i x^{e_{1,i}} y^{e_{2,i}} \tag{16.18}$$

where $c_i \in R$ and $e_{1,i}, e_{2,i} \in \{0, 1, 2, \ldots\}$. Thus, "$f \in R[x, y, z]$" means that f is a polynomial whose variables are x, y and z and whose coefficients are real numbers. All polynomials in this chapter have coefficients that are real numbers.

Term order

It is often useful to list the terms of a polynomial in decreasing order, beginning with the *leading term*. This is done using a *term order* — a way to compare any two distinct terms of a polynomial and declare which is "greater. "

For linear polynomials, term order amounts to merely declaring an order on the variables. For example, the terms of the polynomial

$$2x + 3y - 4z$$

are in proper order if we declare $x > y > z$. If we declare $y > z > x$, the proper order would be $3y - 4z + 2x$. For non-linear polynomials, we begin by declaring an order on the variables, and then we must also choose one of several schemes that decide how the exponents in a polynomial influence term order. One such scheme is called *lexicographical order* (nicknamed *lex*), defined as follows. If the variables of a polynomial are ordered $x_1 > x_2 > \ldots > x_n$, then given two distinct terms $T_i = c_i x_1^{e_{1,i}} x_2^{e_{2,i}} \cdots x_n^{e_{n,i}}$ and $T_j c_j x_1^{e_{1,j}} x_2^{e_{2,j}} \cdots x_n^{e_{n,j}}$, $T_i > T_j$ if

1. $e_{1,i} > e_{1,j}$, or if
2. $e_{1,i} = e_{1,j}$ and $e_{2,i} > e_{2,j}$, or, in general, if
3. $e_{k,i} = e_{k,j}$ for $k = 1, \ldots, m-1$ and $e_{m,i} > e_{m,j}$.

For example, the polynomial

$$3x^2y^2z + 4xy^3z^2 + 5x^3z + 6y^2 + 7xz^3 + 8$$

using lex with $x > y > z$ would be written $5x^3z + 3x^2y^2z + 4xy^3z^2 + 7xz^3 + 6y^2 + 8$ and its leading term is $5x^3z$. Using lex with $z > x > y$ it would be written $7z^3x + 4z^2xy^3 + 5zx^3 + 3zx^2y^2 + 6y^2 + 8$ and the leading term would be $7z^3x$. Or using lex with $y > z > x$ would be written $4y^3z^2x + 3y^2zx^2 + 6y^2 + 7z^3x + 5zx^3 + 8$ and the leading term would be $4y^3z^2x$.

Another choice for term order is the *degree lexicographical order* (abbreviated *deglex*). If the variables are ordered $x_1 > x_2 > \ldots > x_n$, then using deglex, $T_i > T_j$ if

1. $e_{1,i} + e_{2,i} + \ldots + e_{n,i} > e_{1,j} + e_{2,j} + \ldots + e_{n,j}$, or
2. $e_{1,i} + e_{2,i} + \ldots + e_{n,i} = e_{1,j} + e_{2,j} + \ldots + e_{n,j}$ and $T_i > T_j$ with respect to lex.

Using deglex with $x > y > z$, the terms of $3x^2y^2z + 4xy^3z^2 + 5x^3z + 6y^2 + 7xz^3 + 8$ would be ordered $4xy^3z^2 + 3x^2y^2z + 5x^3z + 7xz^3 + 6y^2 + 8$.

As obverved in the lex and deglex examples, term orders ignore the coefficient of a term, so a term order might more properly be called a monomial order.

Other term orders can also be defined, such as degree reverse lexicographical order. The precise requirements for any term order are discussed in reference [AL94], page 18.

The n-dimensional real affine space is denoted R^n and is the set of n-tuples:

$$R^n = (a_1, \ldots, a_n) : a_1, \ldots, a_k \in R \tag{16.19}$$

16.11.4 Polynomial Ideals and Varieties

The *polynomial ideal* generated by $f_1, ..., f_s \in k[x_1, ..., x_n]$, denoted $\langle f_1, ..., f_s \rangle$, is defined

$$I = \langle f_1, ..., f_s \rangle = \{p_1 f_1 + ... + p_s f_s : p_i \in k[x_1, ..., x_n]\}. \tag{16.20}$$

The polynomials $f_1, ..., f_s$ are called *generators* of this ideal. As in integer ideals, any polynomial ideal can be defined using different generating sets.

Consider a set of polynomials $f_1, f_2, \cdots, f_s \in k[x_1, ..., x_n]$. Let $(a_1, ..., a_n)$ be a point in k^n satisfying $f_i(a_1, ..., a_n) = 0$, $i = 1, ..., s$. The set of all such points $(a_1, ..., a_n)$ is called the *variety* defined by $f_1, ..., f_s$, and is denoted by $V(f_1, ..., f_s)$:

$$V(f_1, ..., f_s) = \{(a_1, ..., a_n) \in k^n | f_i(a_1, ..., a_n) = 0, i = 0, \ldots, s\}. \tag{16.21}$$

A more familiar way to refer to a variety is simply the set of solutions to a set of polynomial equations.

A variety defined by a single polynomial—called a *hypersurface*—is the most familiar instance of a variety. A hypersurface in R^2 is a planar curve defined using an implicit equation, and a hypersurface in R^3 is what is normally called an implicit surface in CAGD. For example, $V(x^2 + y^2 - 1)$ is a circle defined in terms of the implicit equation $x^2 + y^2 - 1 = 0$ and $V(2x + 4y - z + 1)$ is the plane whose implicit equation is $2x + 4y - z + 1 = 0$. A variety $V(f_1, \ldots, f_s)$ defined by more than one polynomial ($s > 1$) is the intersection of the varieties $V(f_1) \ldots V(f_s)$.

An ideal is a set of polynomials that is infinite in number. The *variety of an ideal* is the set of all points $(a_1, ..., a_n)$ that make each polynomial in the ideal vanish. It is easy to see that the variety of an ideal is the variety of generating set for the ideal. Two generating sets for the same ideal define the same variety.

This is a very powerful concept, because some generating sets are more useful than others. For example, consider the ideal

$$I = \langle x + y + z - 6, x - y - z, x - 2y + z - 3 \rangle$$

which can also be generated by $\langle x - 3, y - 1, z - 2 \rangle$. This second set of generators is much more helpful, because we can immediately see that $V(I)$ is $x = 3, y = 1, z = 2$. One method for converting the generating set $\langle x + y + z - 6, x - y - z, x - 2y + z - 3 \rangle$ into $\langle x - 3, y - 1, z - 2 \rangle$ is to use the familiar Gauss elimination method.

As another example, consider the ideal

$$I = \langle t^4 - 3t^3 + 4t^2 - t - 4, t^6 - 4t^3 + 3 \rangle$$

An alternative generator for this ideal is simply $\langle t-1 \rangle$, which can be obtained using Euclid's algorithm. Thus, $t = 1$ is the variety of this ideal, or, the common zero.

As we saw in our discussion of ideals of integers, necessary and sufficient conditions for $\langle f_1, \ldots, f_n \rangle = \langle g_1, \ldots, g_m \rangle$ are $f_1, \ldots, f_n \in \{g_1, \ldots, g_m\}$ and $g_1, \ldots, g_m \in \{f_1, \ldots, f_n\}$. This general process can be used to prove that Gauss elimination and Euclid's algorithm, respectively, are algorithms that create equivalent generating sets for ideals.

16.11.5 Gröbner Bases

Gauss elimination and Euclid's algorithm create generating sets which make it simple to compute the variety of an ideal (or, the set of all solutions to a set of polynomial equations). These algorithms are special cases of a completely general method for robustly finding all solutions to a set of polynomial equations in any number of variables. This method is based on the notion of *Gröbner bases*.

A *Gröbner basis* of an ideal I is a set of polynomials $\{g_1, \ldots, g_t\}$ such that the leading term of any polynomial in I is divisible by the leading term of at least one of the polynomials $g_1, \ldots, g_t$. This, of course, requires that a term order be fixed for determining the leading terms: different term orders produce different Gröbner bases. Several excellent books have been written on Gröbner bases that do not presuppose that the reader has an advanced degree in mathematics [CLO92, AL94, BW93]

A Gröbner basis is a particularly attractive set of generators for an ideal, as illustrated by two familiar examples. If $\{f_1, \ldots, f_s\}$ are polynomials in one variable, the Gröbner basis of $\langle f_1, \ldots, f_n \rangle$ consists of a single polynomial: the GCD of $f_1, \ldots, f_s$. If $\{f_1, \ldots, f_s\}$ are linear polynomials in several variables, the Gröbner basis is an uppertriangular form of a set of linear equations. The Gröbner basis of these special cases provides significant computational advantage and greater insight, and the same is true of the Gröbner basis of a more general ideal.

Gröbner bases are the fruit of Bruno Buchberger's Ph.D. thesis [Buc65], and are named in honor of his thesis advisor. Buchberger devised an algorithm for computing Gröbner bases [Buc85, CLO92]. Also, commercial software packages such as Maple and Mathematica include capabilities for computing Gröbner bases.