REPRESENTATIONS OF EPITROCHOIDS AND HYPOTROCHOIDS

by

Michelle Natalie Rene Marie Bouthillier

Submitted in partial fulfillment of the requirements
for the degree of Master of Science

at

Dalhousie University
Halifax, Nova Scotia
March 2018

Table of Contents

List of Figures

Abstract

Representations of a given curve may consist of implicit or parametric equations, along with any envelopes that produce that curve. We will describe the different methods of passing from one of these representations to another, then apply these methods with regards to epitrochoids and hypotrochoids. These are the families of curves that are produced by tracing the path of a point affixed to a circle as it rolls around the inside or outside of a stationary circle. Epicycloids and hypocycloids are produced when the point affixed to the moving circle is on the circumference. We will provide several conjectures and results on the representations of epitrochoids and hypotrochoids, with emphasis on epicycloids and hypocycloids, including their implicit representations and their construction as envelopes.

Acknowledgements

I would like to express my sincerest appreciation to:

My supervisor, Dr. Keith Johnson, for his invaluable expertise, support, time and patience.

Dr. Karl Dilcher and Dr. Robert Noble for their time and recommendations.

My beloved, Andrew Jordan Graf, whose love knows no bounds, limits, or asymptotes.

Chapter 1

Introduction

We will begin by formally defining implicit and parametric representations. Converting an implicit representation to a parametric one is called parametrization. Conversely, converting a parametric representation to an implicit one is called implicitization. We will focus on implicitization, describing three general solutions for algebraic varieties that have a rational parametrization. These methods are the Sylvester resultant, the Bézout resultant, and Gröbner bases. We will then apply these methods to two families of curves, epitrochoids and hypotrochoids, which are both roulettes.

Definition 1. *A **roulette** is a curve that is produced by the path of a point associated with a curve, which is fixed with respect to that curve, as that curve rolls on another fixed curve [10].*

Examples of roulettes include epitrochoids, hypotrochoids, and trochoids.

Definition 2. ***Epitrochoids*** *are parametrized curves that are traced out by a point attached to a circle that is rolling outside of a fixed circle where both circles are on the same plane. Let d be the distance from the center of the rolling circle to the point that is fixed on this circle. If the center of the fixed circle is at the origin and has radius R, the rolling circle has radius r, and the angle between a line through the center of both circles and the x-axis is θ; then a parametric representation for this epitrochoid is:*

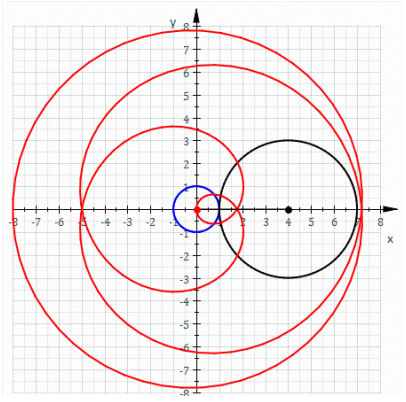


Figure 1.1: Epitrochoid with $R = 1$, $r = 3$, $d = 4$.

$$x(\theta) = (R+r)\cos\theta - d\cos\left(\frac{R+r}{r}\theta\right) \tag{1.1}$$
$$y(\theta) = (R+r)\sin\theta - d\sin\left(\frac{R+r}{r}\theta\right)$$

If the distance from the fixed point on the moving circle to the center is equal to the radius of the moving circle (that is, $d = r$), then the resulting curve is called an ***epicycloid*** *and the parametric equations become:*

$$x(\theta) = (R+r)\cos\theta - r\cos\left(\frac{R+r}{r}\theta\right) \tag{1.2}$$
$$y(\theta) = (R+r)\sin\theta - r\sin\left(\frac{R+r}{r}\theta\right)$$

We also have the equivalent parametric representation:

$$x(\theta) = r(k+1)\cos\theta - r\cos((k+1)\theta) \tag{1.3}$$
$$y(\theta) = r(k+1)\sin\theta - r\sin((k+1)\theta)$$

where $k = R/r$ [1, 10].

Definition 3. *Similarly,* ***hypotrochoids*** *are parametrized curves that are traced out by a point attached to a circle that is rolling inside of a fixed circle. Using the same notation as above, a parametric representation for this hypotrochoid is:*

$$x(\theta) = (R-r)\cos\theta + d\cos\left(\frac{R-r}{r}\theta\right) \tag{1.4}$$
$$y(\theta) = (R-r)\sin\theta - d\sin\left(\frac{R-r}{r}\theta\right)$$

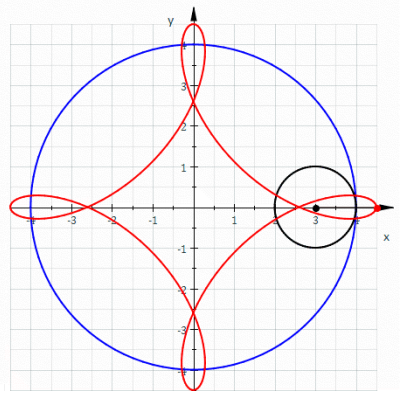


Figure 1.2: Hypotrochoid with $R = 4$, $r = 1$, $d = 3/2$.

If the distance from the fixed point on the moving circle to the center is equal to the radius of the moving circle (that is, $d = r$), then the resulting curve is called a ***hypocycloid*** *and the parametric equations become:*

$$x(\theta) = (R-r)\cos\theta + r\cos\left(\frac{R-r}{r}\theta\right) \tag{1.5}$$
$$y(\theta) = (R-r)\sin\theta - r\sin\left(\frac{R-r}{r}\theta\right)$$

We also have the equivalent parametric representation:

$$x(\theta) = r(k-1)\cos\theta + r\cos((k-1)\theta) \tag{1.6}$$
$$y(\theta) = r(k-1)\sin\theta - r\sin((k-1)\theta)$$

where $k = R/r$ *[1, 10].*

The form of the resulting epicycloid or hypocycloid depends on the value of k. If k is rational, then the epicycloid or hypocycloid is a closed algebraic curve. If k is irrational, then the curve will never return to the initial starting point and will have infinitely many branches [11, 12].

Definition 4. *A* ***trochoid*** *is a curve that is traced out by a point attached to a circle that is rolling along a straight line, where the circle and line are on the same plane. If the straight line is the* x*-axis, the point on the circle* P *starts at the origin, and the circle has radius* r*; then a parametric representation for this trochoid is:*

$$x(\theta) = r\theta - a\sin\theta \tag{1.7}$$
$$y(\theta) = r - a\cos\theta$$

where θ *is the angle through which* P *is rotated and* a *is the distance from the center of the circle to* P*.*

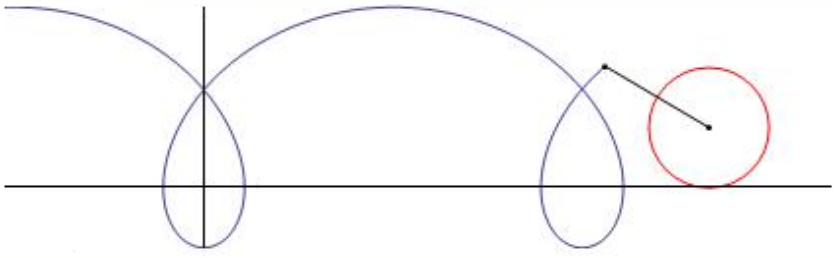


Figure 1.3: A trochoid with $a = 2r$

If the distance from the fixed point on the moving circle to the center is equal to the radius of the moving circle (that is, the point is on the boundary), then the parametric equations become:

$$x(\theta) = r(\theta - \sin\theta) \tag{1.8}$$
$$y(\theta) = r(1 - \cos\theta)$$

The resulting curve is called a ***cycloid*** *[10].*

Hence, we cannot use cycloid as a general term for epicycloids and hypocycloids. It should also be noted that there is some disagreement in the literature regarding these definitions (for an example, see [6]). However, the above is the most common categorization of these curves, and hence, is the one we will use.

Applying these methods of implicitization will provide us with several conjectures and results on the implicit representations of epitrochoids and hypotrochoids, particularly for epicycloids and hypocycloids.

Lastly, we will briefly discuss envelopes; a representation of a curve produced by a family of curves. We then present four different constructions of epicycloids and hypocycloids as envelopes.

Chapter 2

The Implicitization Problem

2.1 Introduction

Definition 5. *Let K be a field, and let $F_1, \ldots, F_s \in K[x_1, \ldots, x_n]$. Let*

$$V(F_1, \ldots, F_s) = \{(a_1, \ldots, a_n) \in K^n \mid F_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}.$$

*Then the set $V(F_1, \ldots, F_s)$ is called the **variety** defined by $F_1, \ldots, F_s$ [5].*

There are two standard forms for representing algebraic varieties, which include curves and surfaces, implicit and parametric representations.

Definition 6. *An **implicit representation** of an algebraic variety in $\mathbb{R}^n$ is of the form*

$$\begin{aligned} F_1(x_1, \ldots, x_n) &= 0, \\ &\vdots \\ F_m(x_1, \ldots, x_n) &= 0, \end{aligned} \tag{2.1}$$

where the algebraic variety consists of the points $(x_1, \ldots, x_n) \in \mathbb{R}^n$ which satisfy all of the above equations. If $m = n - 1$ then the algebraic variety is a curve.

Curves and surfaces that have polynomial implicit representations are called algebraic curves and surfaces.

Therefore, the set of solutions to the system of equations from an implicit representation of an algebraic variety in $\mathbb{R}^n$;

$$F_1(x_1, \ldots, x_n) = F_2(x_1, \ldots, x_n) = \cdots = F_m(x_1, \ldots, x_n) = 0$$

is the variety $V(F_1, \ldots, F_m)$ [5].

Example 1. *The implicit representation of the unit circle in* $\mathbb{R}^2$ *is*

$$x^2 + y^2 - 1 = 0. \tag{2.2}$$

As in the above example, implicit curves have the form $f(x, y) = 0$ and an implicit representation of a surface has the form $f(x, y, z) = 0$. However, the implicit representation of a curve in $\mathbb{R}^3$ will require two equations. In general, curves with implicit representations in higher dimensions will consist of more than one equation. Alternatively, a curve may be described or defined by a parametric representation.

Definition 7. *A* ***parametric representation*** *of an algebraic variety in* $\mathbb{R}^n$ *is of the form*

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m), \end{aligned} \tag{2.3}$$

where the algebraic variety consists of the points $(x_1, \ldots, x_n) \in \mathbb{R}^n$ *for which there exists* $(t_1, \ldots, t_m)$ *such that* $(f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)) = (x_1, \ldots, x_n)$. *If* $m = 1$ *then the algebraic variety is a curve.*

If $f_1, \ldots, f_n$ in the above definition are polynomials, then it is called a polynomial parametric representations. Additionally, if the parametric representation is of the form

$$\begin{aligned} x_1 &= \frac{f_1(t_1, t_2, \ldots, t_m)}{g_1(t_1, t_2, \ldots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, t_2, \ldots, t_m)}{g_n(t_1, t_2, \ldots, t_m)}. \end{aligned} \tag{2.4}$$

where $f_1, \ldots, f_n, g_1, \ldots, g_n$ are polynomials, then it is called a rational parametric representation.

Example 2. *A rational parametric representation of the unit circle in* $\mathbb{R}^2$ *is*

$$\begin{aligned} x &= \frac{1 - t^2}{1 + t^2}, \\ y &= \frac{2t}{1 + t^2}. \end{aligned} \tag{2.5}$$

Another parametric representation of the unit circle is $x = \cos(t), y = \sin(t)$. In Section 3.1 we will show that all trigonometric rational parametric representations (where the trigonometric aspect can be expressed in terms of sin and cos) can be expressed as rational parametric representations.

As in the above example, parametric curves have a single parameter; and rational parametric surfaces are functions of two parameters.

Parametric representations are effective for generating points along a given curve or surface, but not for determining whether a given point lies on this curve or surface. Conversely, implicit forms are effective for determining whether a point lies on a curve or surface, but not for generating points along this curve or surface. Additionally, finding the intersection of two curves can be simplified if one is expressed implicitly and the other parametrically. Then the parametric representation of one curve can be substituted into the implicit representation of the other to give the curve of intersection implicitly. Hence, it is desirable to be able to convert between these representations. Converting from a parametric representation to an implicit one is called **implicitization**; converting from an implicit representation to a parametric one is called **parametrization** [14, 15].

Note that not all algebraic curves have rational parametric representations. For example, most elliptic curves such as

$$x^3 + x^2y + xy^2 + y^3 + x^2 + xy + y^2 + x + y + 1 = 0$$

can not be parametrized with rational functions. A proof of this can be found in *Parametrizing Algebraic Curves* by Lemmermeyer [8].

Consider the following curve (fig. 2.1) given by

$$\begin{aligned} x(\theta) &= 8\cos\theta + 3\cos(8\theta/3)\,, \\ y(\theta) &= 8\sin\theta - 3\sin(8\theta/3)\,. \end{aligned} \tag{2.6}$$

Is this curve algebraic? In other words, is it possible to find an implicit polynomial representation for this curve? If there are multiple methods, which requires the least amount of computational time and memory? And lastly, is there a general formula for the implicit representation of curves like the one above? We will find that curves described as the one above are rational parametric curves for which an implicit representation, in theory, can always be found.

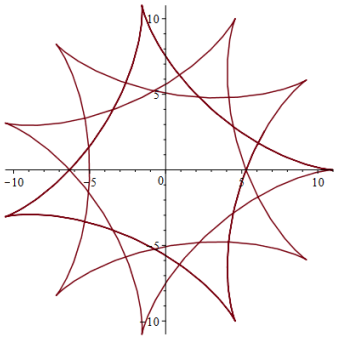


Figure 2.1: Example of a curve that we may wish to implicitize

There are two common methods for implicitization, using resultants and Gröbner bases. In particular, we will focus on Sylvester and Bézout resultants.

2.2 Resultants

Definition 8. *Let K be a field and $f, g \in K[x]$ such that*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_n \neq 0,$$

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0, \qquad b_m \neq 0,$$

*where $n \geq m$. Then the **Sylvester matrix** of f and g with respect to x is the following $(m+n) \times (m+n)$ matrix:*

$$\begin{bmatrix}
a_n & a_{n-1} & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 & 0 \\
0 & a_n & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & a_1 & a_0 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & & & & & & & & & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & a_n & a_{n-1} & a_{n-2} & a_{n-3} & \cdots & \cdots & \cdots & \cdots & \cdots & a_0 & 0 \\
0 & 0 & \cdots & 0 & a_n & a_{n-1} & a_{n-2} & \cdots & \cdots & \cdots & \cdots & \cdots & a_1 & a_0 \\
b_m & b_{m-1} & \cdots & b_2 & b_1 & b_0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 \\
0 & b_m & \cdots & b_3 & b_2 & b_1 & b_0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & & & & & \ddots & & & & & \vdots & \vdots \\
\vdots & \vdots & & \ddots & & & & & \ddots & & & & \vdots & \vdots \\
\vdots & \vdots & & & \ddots & & & & & \ddots & & & \vdots & \vdots \\
\vdots & \vdots & & & & \ddots & & & & & \ddots & & \vdots & \vdots \\
\vdots & \vdots & & & & & \ddots & & & & & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & b_m & b_{m-1} & \cdots & \cdots & \cdots & b_0 & 0 \\
0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & b_m & \cdots & \cdots & \cdots & b_1 & b_0
\end{bmatrix}$$

*The **Sylvester resultant** is the determinant of the Sylvester matrix, denoted by $Res_x(f, g)$ [5, 7].*

Definition 9. *Let K be a field and $f, g \in K[x]$ be as above. Consider the polynomial*

$$P(x, y) = \frac{f(x)g(y) - f(y)g(x)}{x - y} = \sum_{i,j=0}^{n-1} b_{i,j} x^i y^j. \tag{2.7}$$

*Then the **Bézout matrix** of f and g with respect to x is the following $n \times n$ matrix:*

$$\begin{bmatrix} b_{0,0} & b_{0,1} & \cdots & b_{0,n-1} \\ b_{1,0} & b_{1,1} & \cdots & b_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,0} & b_{n-1,1} & \cdots & b_{n-1,n-1} \end{bmatrix} \tag{2.8}$$

The ***Bézout resultant*** *is the determinant of the Bézout matrix, denoted by* $det(Bez_x(f,g))$ *[9, 14].*

Sylvester and Bézout's methods of using resultants consists of creating a particular Sylvester or Bézout's matrix (or matrices) with respect to the parametric representation. To begin, consider the following cases in K^2.

Theorem 1. *Suppose we have a polynomial parametric representation of a curve in* K^2 *given by*

$$x = x(t), \quad y = y(t). \tag{2.9}$$

Then an implicit representation is

$$F(x,y) = Res_t(x - x(t), y - y(t)) = 0.$$

Proof. We can rewrite equation (2.9) as

$$x - x(t) = 0, \quad y - y(t) = 0. \tag{2.10}$$

Let $x(t) = \sum_{i=0}^{n} b_i t^i$ and $y(t) = \sum_{j=0}^{m} d_j t^j$ where b_n, d_m are nonzero and $N = \max\{n,m\}$. Then $x - x(t) = \sum_{i=0}^{n}(a_i x - b_i)t^i = \sum_{i=0}^{n} \alpha_i t^i = 0$ and $y - y(t) = \sum_{j=0}^{m}(c_j y - d_j)t^j = \sum_{j=0}^{m} \beta_i t^i = 0$, where $a_i = b_j = 0$ for nonzero i, j and $a_0 = b_0 = 1$. By multiplying through by $t^m, \ldots, t, 1$ and $t^n, \ldots, t, 1$, respectively, we obtain the following $n + m$ equations:

$$\begin{aligned} \alpha_n t^{n+m} + \alpha_{n-1} t^{n+m-1} + \alpha_{n-2} t^{n+m-2} + \cdots + \alpha_1 t^{m+1} + \alpha_0 t^m &= 0 \\ \alpha_n t^{n+m-1} + \alpha_{n-1} t^{n+m-2} + \cdots + \alpha_1 t^m + \alpha_0 t^{m-1} &= 0 \\ \vdots \end{aligned}$$

$$
\begin{aligned}
\alpha_n t^{n+1} + \alpha_{n-1} t^n + \alpha_{n-2} t^{n-1} + \cdots + \alpha_1 t^2 + \alpha_0 t &= 0 \\
\alpha_n t^n + \alpha_{n-1} t^{n-1} + \cdots + \alpha_1 t \ \ + \alpha_0 \ &= 0 \\
\beta_m t^{n+m} + \beta_{m-1} t^{n+m-1} + \beta_{m-2} t^{n+m-2} + \cdots + \beta_1 t^{n+1} + \beta_0 t^n \ &= 0 \\
\beta_m t^{n+m-1} + \beta_{m-1} t^{n+m-2} + \cdots + \beta_1 t^n \ \ + \beta_0 t^{n-1} &= 0 \\
\vdots & \\
\beta_m t^{m+1} + \beta_{m-1} t^m + \beta_{m-2} t^{m-1} + \cdots + \beta_1 t^2 + \beta_0 t &= 0 \\
\beta_m t^m + \beta_{m-1} t^{m-1} + \cdots + \beta_1 t \ \ + \beta_0 \ &= 0
\end{aligned}
$$

Note that any nonzero solution t will satisfy (2.10) if and only if it also satisfies the above system of equations.

Consider the field $K_1 = K[x, y]$. Then, since K_1 is a field, $K_1[t]$ is a vector space over K_1 with $\{t^i\}_{i=0}^{n+m}$ as a K_1-basis. Hence, we can arrange this system in the following way:

$$
\begin{bmatrix}
\alpha_n & \alpha_{n-1} & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \alpha_0 & 0 & \cdots & 0 & 0 \\
0 & \alpha_n & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \alpha_1 & \alpha_0 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & & & & & & & & & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & \alpha_n & \alpha_{n-1} & \alpha_{n-2} & \alpha_{n-3} & \cdots & \cdots & \cdots & \cdots & \cdots & \alpha_0 & 0 \\
0 & 0 & \cdots & 0 & \alpha_n & \alpha_{n-1} & \alpha_{n-2} & \cdots & \cdots & \cdots & \cdots & \cdots & \alpha_1 & \alpha_0 \\
\beta_m & \beta_{m-1} & \cdots & \beta_2 & \beta_1 & \beta_0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 \\
0 & \beta_m & \cdots & \beta_3 & \beta_2 & \beta_1 & \beta_0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & & & & & \ddots & & & & & \vdots & \vdots \\
\vdots & \vdots & & \ddots & & & & & \ddots & & & & \vdots & \vdots \\
\vdots & \vdots & & & \ddots & & & & & \ddots & & & \vdots & \vdots \\
\vdots & \vdots & & & & \ddots & & & & & \ddots & & \vdots & \vdots \\
\vdots & \vdots & & & & & \ddots & & & & & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \beta_m & \beta_{m-1} & \cdots & \cdots & \cdots & \beta_0 & 0 \\
0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & \beta_m & \cdots & \cdots & \cdots & \beta_1 & \beta_0
\end{bmatrix}
\begin{bmatrix}
t^{n+m} \\ t^{n+m-1} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ t^m \\ t^{m-1} \\ \vdots \\ t \\ 1
\end{bmatrix}
=
\begin{bmatrix}
0 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0
\end{bmatrix}
$$

From Linear Algebra, given such a system of the form $Ax = 0$, there is a nontrivial solution if and only if the determinant of A vanishes. Note that by the form of this

matrix, $|A|$ is the Sylvester resultant of f and g with respect to t where $f(x,t) = x - x(t)$ and $g(y,t) = y - y(t)$. Therefore, as the resultant vanishing is the relationship that must exist for a solution t to exist that satisfies equation (2.10), the Sylvester resultant $Res_t(x - x(t), y - y(t)) = 0$ is an implicit representation [14]. □

Theorem 2. *Suppose we have a polynomial parametric representation of a curve in* K^2 *given by*

$$x = x(t), \quad y = y(t). \tag{2.11}$$

Then an implicit representation is

$$F(x,y) = det(Bez_t(x - x(t), y - y(t))) = 0.$$

Proof. Without loss of generality, assume $x(t)$ and $y(t)$ are of degree m and n, respectively, and that $n \geq m$. We can rewrite equation (2.11) as

$$x - x(t) = 0, \qquad y - y(t) = 0. \tag{2.12}$$

Let $f(x,t) = x - x(t)$ and $g(y,t) = y - y(t)$, and consider the following polynomial:

$$P(t,s) = \frac{f(x,t)g(y,s) - f(x,s)g(y,t)}{t - s}. \tag{2.13}$$

This is a polynomial of degree $n-1$ in t and also in s. Hence,

$$P(t,s) = P_0(t) + P_1(t)s + P_2(t)s^2 + \cdots + P_{n-1}(t)s^{n-1} \tag{2.14}$$

where $P_i(t) = \sum_{j=0}^{n-1} b_{i,j}t^j$. Consider the field $K_2 = K(x,y)$ where $f, g \in K_2[t]$. Then, since K_2 is a field, $K_2[t]$ is a vector space over K_2 where $\{t^i\}_{i=0}^{n-1}$ is a K_2-basis. Hence, these polynomials can be written as:

$$\begin{bmatrix} P_0(t) \\ P_1(t) \\ P_2(t) \\ \vdots \\ P_{n-1}(t) \end{bmatrix} = \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & \cdots & b_{0,n-1} \\ b_{1,0} & b_{1,1} & b_{1,2} & \cdots & b_{1,n-1} \\ b_{2,0} & b_{2,1} & b_{2,2} & \cdots & b_{2,n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{n-1,0} & b_{n-1,1} & b_{n-1,2} & \cdots & b_{n-1,n-1} \end{bmatrix} \begin{bmatrix} 1 \\ t \\ t^2 \\ \vdots \\ t^{n-1} \end{bmatrix} \tag{2.15}$$

where $b_{i,j} \in K$ for $0 \leq i, j \leq n-1$. Note that any solution t will satisfy equation (2.12)

if and only if $P(t,s) = 0$. Additionally, $P(t,s) = 0$ if and only if $P_i(t) = 0$ for all $0 \le i \le n-1$. Lastly, $P_i(t) = 0$ for all $0 \le i \le n-1$ if and only if the following system is satisfied:

$$\begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & \cdots & b_{0,n-1} \\ b_{1,0} & b_{1,1} & b_{1,2} & \cdots & b_{1,n-1} \\ b_{2,0} & b_{2,1} & b_{2,2} & \cdots & b_{2,n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{n-1,0} & b_{n-1,1} & b_{n-1,2} & \cdots & b_{n-1,n-1} \end{bmatrix} \begin{bmatrix} 1 \\ t \\ t^2 \\ \vdots \\ t^{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{2.16}$$

From Linear Algebra, given such a system of the form $Ax = 0$, there is a nontrivial solution if and only if the determinant of A vanishes. Note that by the form of this matrix, $|A|$ is the Bézout resultant of f and g with respect to t. Therefore, as the resultant vanishing is the relationship that must exist for a solution t to exist that satisfies equation (2.12), the Bézout resultant $det(Bez(x - x(t), y - y(t)) = 0$ is the implicit representation [9, 14]. □

Recall the general form of a polynomial parametric representation of an algebraic variety in K^n:

$$\begin{aligned} x_1 &= f_1(t_1, t_2, \ldots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, t_2, \ldots, t_m). \end{aligned} \tag{2.17}$$

The following provides us with a method to find an implicit representation of such an algebraic variety.

Theorem 3. *Suppose we have a polynomial parametric representation of an algebraic variety in K^n given by* (2.17)*. Then an implicit representation can be found using Sylvester resultants.*

Proof. We can rewrite (2.17) as

$$\begin{aligned} y_1 &= x_1 - f_1(t_1, t_2, \ldots, t_m), \\ &\vdots \\ y_n &= x_n - f_n(t_1, t_2, \ldots, t_m). \end{aligned} \tag{2.18}$$

Where $y_1 = \cdots = y_n = 0$. We wish to eliminate $t_1, \ldots, t_m$; which can be achieved through the following algorithm: Begin by pairing the y_i's together in the following fashion: $\{y_1, y_2\}, \{y_3, y_4\}, \ldots, \{y_{n-1}, y_n\}$. If n is odd, use one of the y_i's twice in a pairing. Note that every y_i can be written as a polynomial in terms of t_1 as follows:

$$y_i = \sum_{j=0}^{n_i} (a_j x_i + g_j(t_2, \ldots, t_m)) t_1^j = \sum_{j=0}^{n_i} \alpha_{i,j} t_1^j \tag{2.19}$$

where $\alpha_{i,j} = a_j x_i + g_j(t_2, \ldots, t_m)$. Therefore, for every pairing $\{y_i, y_{i+1}\}$ we may write

$$y_i = \sum_{j=0}^{n_i} \alpha_{i,j} t_1^j, \qquad y_{i+1} = \sum_{j=0}^{n_{i+1}} \alpha_{i+1,j} t_1^j. \tag{2.20}$$

We can now follow the procedure from the proof of Theorem 1 with respect to each pairing. This will result in a new set of equations,

$$\begin{aligned} Res_{t_1}(x_1 - f_1(t_1, t_2, \ldots, t_m), x_2 - f_2(t_1, t_2, \ldots, t_m)) &= 0, \\ &\vdots \\ Res_{t_1}(x_{n-1} - f_{n-1}(t_1, t_2, \ldots, t_m), x_n - f_n(t_1, t_2, \ldots, t_m)) &= 0. \end{aligned} \tag{2.21}$$

Repeat this process with respect to $t_2, \ldots, t_m$. From the reasoning of the proof of Theorem 1, $(t_1, \ldots, t_m)$ satisfies equation (2.18) if and only if all of the final resultants vanish. Therefore, the remaining set of equations will be an implicit representation. □

Theorem 4. *Suppose we have a polynomial parametric representation of an algebraic variety in K^n given by* (2.17)*. Then an implicit representation can be found using Bézout resultants.*

Proof. We can rewrite (2.17) as

$$\begin{aligned} f_1(x_1, t_1, \ldots, t_m) &= x_1 - f_1(t_1, t_2, \ldots, t_m), \\ &\vdots \\ f_n(x_n, t_1, \ldots, t_m) &= x_n - f_n(t_1, t_2, \ldots, t_m). \end{aligned} \tag{2.22}$$

We wish to eliminate $t_1, \ldots, t_m$; which can be achieved through the following algorithm: Begin by pairing the f_i's together in the following fashion: $\{f_1, f_2\}, \{f_3, f_4\}, \ldots,$

$\{f_{n-1}, f_n\}$. If n is odd, use one of the f_i's twice in a pairing. Consider the pair $\{f_i, f_{i+1}\}$ and let $n_{i,i+1} = \max\{\deg_{t_1}(f_i), \deg_{t_1}(f_{i+1})\}$. Now consider the following polynomial:

$$P_{i,i+1}(t_1, s) = \frac{f_i(x_i, t_1, \ldots, t_m) f_{i+1}(x_{i+1}, s, \ldots, t_m) - f_i(x_i, s, \ldots, t_m) f_{i+1}(x_{i+1}, t_1, \ldots, t_m)}{t_1 - s}$$

This is a polynomial of degree $n_{i,i+1} - 1$ in t_1 and also in s. Hence, we may write

$$P_{i,i+1}(t_1, s) = P_0(t_1) + P_1(t_1)s + \cdots + P_{n_{i,i+1}-1}(t_1)s^{n_{i,i+1}-1} \tag{2.23}$$

with $P_j(t_1) = \sum_{k=0}^{n_{i,i+1}-1} \beta_{j,k} t_1^k$ where the $\beta_{j,k}$ are polynomials in $x_i, x_{i+1}, t_2, \ldots, t_m$. Therefore, for every pair we can follow the procedure from the proof of Theorem 2. This will result in a new set of equations,

$$\begin{aligned} det(Bez_{t_1}(x_1 - f_1(t_1, t_2, \ldots, t_m), x_2 - f_2(t_1, t_2, \ldots, t_m))) &= 0, \\ &\vdots \\ det(Bez_{t_1}(x_{n-1} - f_{n-1}(t_1, t_2, \ldots, t_m), x_n - f_n(t_1, t_2, \ldots, t_m)) &= 0. \end{aligned} \tag{2.24}$$

Repeat this process with respect to $t_2, \ldots, t_m$. From the reasoning of the proof of Theorem 2, $(t_1, \ldots, t_m)$ satisfies equation (2.22) if and only if all of the final resultants vanish. Therefore, the remaining set of equations will be an implicit representation. □

Note that the order of the parametric equations and the order in which the $t_1, \ldots, t_m$ are eliminated may be altered in the above proofs. Therefore, there are $(n!)(m!)$ potential implicit representations which can be found by using the above algorithms.

Recall the general form of a rational parametric representation of an algebraic variety in K^n:

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}. \end{aligned} \tag{2.25}$$

The following provides us with a method with which to find an implicit representation of such an algebraic variety.

Theorem 5. *Suppose we have a rational parametric representation of an algebraic variety in K^n given by (2.25). Then an implicit representation can be found using Sylvester resultants.*

Proof. Let $g = g_1 \cdot g_2 \cdots g_n$ and affix $1 - gy = 0$ to the set of equations. This will ensure that for any solution to our implicit representation, the denominators $g_1, \ldots, g_n$ never vanish. We can then rewrite (2.25) as

$$\begin{aligned} y_1 &= x_1 \cdot g_1(t_1, \ldots, t_m) - f_1(t_1, \ldots, t_m), \\ &\vdots \\ y_n &= x_n \cdot g_n(t_1, \ldots, t_m) - f_n(t_1, \ldots, t_m), \\ y_{n+1} &= 1 - gy, \end{aligned} \tag{2.26}$$

where $y_1 = \cdots = y_n = y_{n-1} = 0$. We wish to eliminate $t_1, \ldots, t_m, y$; which can be achieved through the following algorithm: Begin by pairing the y_i's together in the following fashion: $\{y_1, y_2\}, \{y_3, y_4\}, \ldots, \{y_n, y_{n+1}\}$. If $n+1$ is odd, use one of the y_i's twice in a pairing. Note that for $1 \leq i \leq n$ every y_i can be written as a polynomial in terms of t_1 in the following fashion;

$$y_i = \sum_{j=0}^{n_i} (x_j \cdot g_{i,j}(t_2, \ldots, t_m) - f_{i,j}(t_2, \ldots, t_m)) t_1^j = \sum_{j=0}^{n_i} \alpha_{i,j} t_1^j \tag{2.27}$$

where $\alpha_{i,j} = x_j \cdot g_{i,j}(t_2, \ldots, t_m) - f_{i,j}(t_2, \ldots, t_m)$ and $n_i = \max\{\deg_{t_1}(f_i), \deg_{t_1}(g_i)\}$. Lastly, for y_{n+1} we have that

$$y_{n+1} = \sum_{j=0}^{n_{n+1}} (a_j - y \cdot g_j) t_1^j = \sum_{j=0}^{n_{n+1}} \alpha_{n+1,j} t_1^j \tag{2.28}$$

where $\alpha_{n+1,j} = a_j - y \cdot g_j$, $a_0 = 1$ and $a_j = 0$ for all $1 \leq j \leq n_{n+1}$. Therefore, for every pairing $\{y_i, y_{i+1}\}$ we may write

$$y_i = \sum_{j=0}^{n_i} \alpha_{i,j} t_1^j, \qquad y_{i+1} = \sum_{j=0}^{n_{i+1}} \alpha_{i+1,j} t_1^j. \tag{2.29}$$

We can now follow the procedure from the proof of Theorem 1 with respect to each pairing. This will result in a new set of equations,

$$\begin{aligned} &Res_{t_1}(x_1 \cdot g_1(t_1, \ldots, t_m) - f_1(t_1, \ldots, t_m), x_2 \cdot g_2(t_1, \ldots, t_m) - f_2(t_1, \ldots, t_m)) = 0, \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ &Res_{t_1}(x_n \cdot g_n(t_1, \ldots, t_m) - f_n(t_1, \ldots, t_m), 1 - gy) = 0. \end{aligned} \tag{2.30}$$

Repeat this process with respect to $t_2, \ldots, t_m, y$. From the reasoning of the proof of Theorem 1, $(t_1, \ldots, t_m, y)$ satisfies equation (2.26) if and only if the final resultants vanish. Therefore, the remaining set of equations will be an implicit representation. □

Theorem 6. *Suppose we have a rational parametric representation of an algebraic variety in K^n given by* (2.25)*. Then an implicit representation can be found using Bézout resultants.*

Proof. Let $g = g_1 \cdot g_2 \cdots g_n$ and affix $1 - gy = 0$ to the set of equations. This will ensure that, for any solution to our implicit representation, the denominators $g_1, \ldots, g_n$ never vanish. We can then rewrite (2.25) as

$$\begin{aligned} h_1(x_1, t_1, \ldots, t_m) &= x_1 \cdot g_1(t_1, \ldots, t_m) - f_1(t_1, \ldots, t_m), \\ &\vdots \\ h_n(x_n, t_1, \ldots, t_m) &= x_n \cdot g_n(t_1, \ldots, t_m) - f_n(t_1, \ldots, t_m), \\ h_{n+1}(y, t_1, \ldots, t_m) &= 1 - gy. \end{aligned} \tag{2.31}$$

We wish to eliminate $t_1, \ldots, t_m, y$, which can be achieved through the following algorithm: Begin by pairing the h_i's together in the following fashion: $\{h_1, h_2\}$, $\{h_3, h_4\}$, $\ldots$, $\{h_n, h_{n+1}\}$. If $n+1$ is odd, use one of the h_i's twice in a pairing. Consider the pair $\{h_i, h_{i+1}\}$ where $1 \le i \le n+1$ and let $n_{i,i+1} = \max\{\deg_{t_1}(h_i), \deg_{t_1}(h_{i+1})\}$. Now consider the following polynomial:

$$P_{i,i+1}(t_1, s) = \frac{h_i(x_i, t_1, \ldots, t_m) h_{i+1}(x_{i+1}, s, \ldots, t_m) - h_i(x_i, s, \ldots, t_m) h_{i+1}(x_{i+1}, t_1, \ldots, t_m)}{t_1 - s}$$

This is a polynomial of degree $n_{i,i+1} - 1$ in t_1 and also in s. Hence, we may write

$$P_{i,i+1}(t_1, s) = P_0(t_1) + P_1(t_1)s + \cdots + P_{n_{i,i+1}-1}(t_1)s^{n_{i,i+1}-1} \tag{2.32}$$

with $P_j(t_1) = \sum_{k=0}^{n_{i,i+1}-1} \beta_{j,k} t_1^k$ where $\beta_{j,k}$ are polynomials in $x_i, x_{i+1}, t_2, \ldots, t_m$ (or, if h_{n+1} was in the pairing, in $y, x_i, t_2, \ldots, t_m$). Therefore, for every pair we can follow the procedure from the proof of Theorem 2. This will result in a new set of equations,

$$\begin{aligned} det(Bez_{t_1}(h_1(x_1, t_1, \ldots, t_m), h_2(x_2, t_1, \ldots, t_m))) &= 0, \\ &\vdots \\ det(Bez_{t_1}(h_n(x_n, t_1, \ldots, t_m), h_{n+1}(y, t_1, \ldots, t_m))) &= 0. \end{aligned} \tag{2.33}$$

Repeat this process with respect to $t_2, \ldots, t_m, y$. From the reasoning of the proof of Theorem 2, $(t_1, \ldots, t_m, y)$ satisfies equation (2.31) if and only if the final resultants vanish. Therefore, the remaining set of equations will be an implicit representation. □

Note that the order of the parametric equations, with $1 - gy = 0$, and the order in which the $t_1, \ldots, t_m, y$ are eliminated may be altered in the above proofs. Therefore, there are $(n+1)!(m+1)!$ potential implicit representations which can be found by using the above algorithms.

Lastly, for Theorem 5 and Theorem 6, note that $y_{n+1} = 1 - gy = 0$ need not be affixed to the parametric equations if g never vanishes over K^n.

2.3 Gröbner Bases

All information in this section is from *Ideals, Varieties, and Algorithms* by Cox, Little, and O'Shea (see [5]) unless stated otherwise. We begin with several definitions, lemmas, and propositions that will be necessary to define, and prove the existence of, Gröbner bases. Let K be a field; we will specify when K must be infinite as required.

Definition 10. *A relation $>$ on the set of monomials $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$, or equivalently, a relation on $\mathbb{Z}^n_{\geq 0}$, is a* ***monomial ordering*** *on $K[x_1, \ldots, x_n]$ if:*
(1) $>$ *is a well-ordering on $\mathbb{Z}^n_{\geq 0}$.*
(2) $\alpha > \beta$ *and* $\gamma \in \mathbb{Z}^n_{\geq 0}$ *implies that* $\alpha + \gamma > \beta + \gamma$.

Recall that a well-ordering for a relation is a total ordering for which every non-empty subset has a smallest element under that relation. The following lemma will be used to show that various algorithms terminate after finitely many steps, and illustrates the importance of the well-ordering condition in the above definition.

Lemma 1. *Let $>$ be an order relation on $\mathbb{Z}^n_{\geq 0}$. Then $>$ is a well-ordering if and only if every strictly decreasing sequence in $\mathbb{Z}^n_{\geq 0}$,*

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots, \tag{2.34}$$

terminates.

Proof. Consider the contrapositive form: $>$ is not a well-ordering if and only if there exists an infinite strictly decreasing sequence in $\mathbb{Z}_{\geq 0}^n$.

If $>$ is not a well-ordering, then there exists a non-empty subset $S \subseteq \mathbb{Z}_{\geq 0}^n$ with no least element. Select an $\alpha(1) \in S$. As $\alpha(1)$ is not the least element, we can find an $\alpha(2) \in S$ such that $\alpha(1) > \alpha(2)$. Since $\alpha(2)$ is also not the least element, we can find an $\alpha(3) \in S$ such that $\alpha(2) > \alpha(3)$. Continuing this process, we obtain an infinite strictly decreasing sequence

$$\alpha 1 > \alpha(2) > \alpha(3) > \cdots \tag{2.35}$$

Conversely, suppose we are given such an infinite sequence. Then $\{\alpha(1), \alpha(2), \dots\}$ is a non-empty subset of $\mathbb{Z}_{\geq 0}^n$ without a least element. Therefore, $>$ is not a well-ordering. □

The ordering that we will use throughout this section is called lexicographical ordering.

Definition 11. *Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ be such that $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n)$. A **lexicographical ordering** is defined by the following condition: if the leftmost nonzero entry of the vector difference $\alpha - \beta \in \mathbb{Z}^n$ is positive, then we say that $\alpha >_{lex} \beta$. If $\alpha >_{lex} \beta$, then we write $x^\alpha >_{lex} x^\beta$.*

For completeness, we will now show that the lexicographical ordering satisfies the conditions of Definition 10.

Proposition 1. *The lexicographical ordering on $\mathbb{Z}_{\geq 0}^n$ is a monomial ordering.*

Proof. (1) The lexicographical ordering $>_{lex}$ is a total ordering. This follows from the definition and the fact that the usual ordering on $\mathbb{Z}_{\geq 0}$ is a total ordering.

Now assume towards contradiction that the lexicographical ordering is not a well-ordering. Then by Lemma 1, there exists an infinite strictly descending sequence of elements in $\mathbb{Z}_{\geq 0}^n$ of the form:

$$\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) >_{lex} \cdots \tag{2.36}$$

From the definition of the lexicographical order, the first entries of the vectors $\alpha(i) \in \mathbb{Z}_{\geq 0}^n$ form a non-increasing sequence of non-negative integers. As $\mathbb{Z}_{\geq 0}$ is well-ordered, there exists an ℓ_1 for which the first entries of all $\alpha(i)$ with $i \geq \ell_1$ are equal.

Then the second entries of $\alpha(\ell_1), \alpha(\ell_1 + 1), \ldots$ also form a non-increasing sequence of non-negative integers. By the same reasoning, there exists an ℓ_2 for which the second entries of all $\alpha(j)$ with $j \geq \ell_2$ are equal. Continuing this process, we find that for some ℓ, the $\alpha(\ell), \alpha(\ell + 1), \ldots$ are all equal. This contradicts (2.36) being a strictly descending sequence.

(2) Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ be such that $\alpha >_{lex} \beta$. This implies that $\alpha_i - \beta_i$, the leftmost nonzero entry in $\alpha - \beta$, is positive. But $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ and $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. So in $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$, the leftmost entry is again $\alpha_i - \beta_i > 0$. □

Note that in general, for n variables, there are $n!$ possible lexicographical orders. For example, given the variables x, y, z we may have $x > y > z$, $x > z > y$, $y > x > z$, $y > z > x$, $z > x > y$, or $z > y > x$. We will use the following terminology to simplify future calculations and algorithms.

Definition 12. *Let $>$ be a monomial order on $K[x_1, \ldots, x_n]$ and $f \in K[x_1, \ldots, x_n]$ be a nonzero polynomial where $f = \sum_\alpha a_\alpha x^\alpha$.*

(*i*) *The* ***multidegree*** *of f, where the maximum is taken with respect to $>$, is defined by*

$$multideg(f) = \max(\alpha \in \mathbb{Z}_{\geq 0}^n \mid a_\alpha \neq 0).$$

(*ii*) *From this we define the* ***leading monomial*** *of f to be*

$$LM(f) = x^{multideg(f)}.$$

(*iii*) *The* ***leading coefficient*** *of f as*

$$LC(f) = a_{multideg(f)} \in K.$$

(*iv*) *Hence, the* ***leading term*** *of f is*

$$LT(f) = LC(f) \cdot LM(f).$$

It can be easily shown that the multidegree has the following useful properties.

Lemma 2. *If $f, g \in K[x_1, \ldots, x_n]$ are nonzero polynomials, then:*

(i) $multideg(fg) = multideg(f) + multideg(g)$.

(ii) If $f + g \neq 0$, then $multideg(f + g) \leq \max(multideg(f), multideg(g))$. Equality occurs when $multideg(f) \neq multideg(g)$.

Now recall the division algorithm for the one-variable case.

Proposition 2. *(The Division Algorithm). Let g be a nonzero polynomial in $K[x]$. Then for every $f \in K[x]$, there exists $q, r \in K[x]$ such that*

$$f = qg + r,$$

where either $r = 0$ or $deg(r) < deg(g)$. Furthermore, q and r are unique and can be found through an algorithm.

Proof. We begin with the pseudocode for the algorithm for finding q and r:

Input : g, f

Output : q, r

$q := 0; r := f$

WHILE $r \neq 0$ AND $LT(g)$ divides $LT(r)$ DO

    $q := q + LT(r)/LT(g)$

    $r := r - (LT(r)/LT(g))g$

RETURN q, r

To show that the algorithm produces the desired result, we must show that it terminates and that the final values of q and r have the desired properties.

First note that $f = qg + r$ always holds, because

$$f = qg + r = (q + LT(r)/LT(g))g + (r - (LT(r)/LT(g))g).$$

Next, note that the WHILE...DO loop terminates when either $r = 0$ or $LT(g)$ does not divide $LT(r)$. This is equivalent to $r = 0$ or $deg(r) < deg(g)$. Hence, q and r with the desired properties are produced when the algorithm terminates.

It remains to show that the algorithm terminates. We claim that $r-(LT(r)/LT(g))g$ either has a smaller degree than r or is 0. Suppose that

$$r = c_0x^m + \cdots + c_m, \qquad LT(r) = c_0x^m, \tag{2.37}$$

$$g = d_0x^\ell + \cdots + d_\ell, \qquad LT(g) = d_0x^\ell, \tag{2.38}$$

and that $m \geq \ell$. Then

$$r - (LT(r)/LT(g))g = (c_0x^m + \cdots) - (c_0/d_0)x^{m-\ell}(d_0x^\ell + \cdots).$$

It follows that the degree of r must decrease. Hence, since the degree can only decrease finitely many times, the algorithm must terminate.

Lastly, we will show that q and r are unique. Suppose that $f = qg + r = q'g + r'$ where $deg(r), deg(r') < deg(g)$ (unless one or both are 0). If $r \neq r'$, then $deg(r'-r) < deg(g)$. Furthermore, since

$$(q - q')g = r' - r, \tag{2.39}$$

we have that $q - q' \neq 0$, and consequently,

$$deg(r - r') = deg((q - q')g) = deg(q - q') + deg(g) \geq deg(g).$$

This contradiction implies that $r = r'$, which can then be combined with equation (2.39) to show that $q = q'$. □

We wish to formulate a division algorithm for polynomials in $K[x_1, \ldots, x_n]$ that extends this algorithm in $K[x]$. In general, we wish to divide $f \in K[x_1, \ldots, x_n]$ by $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. As we will see, this means expressing f in terms of the $f_1, \ldots, f_s$ so that

$$f = q_1f_1 + \cdots + q_sf_s + r,$$

where $q_1, \ldots, q_s, r \in K[x_1, \ldots, x_n]$. In order to characterize the remainder r, we will utilize the properties of monomial ordering.

The basic idea of the multivariate division algorithm is the same as in the one-variable case: we wish to cancel the leading term of f by multiplying some f_i by an appropriate monomial and subtracting. This monomial then becomes a term in the corresponding quotient q_i.

Theorem 7. *(Division Algorithm in $K[x_1, \ldots, x_n]$). Let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $K[x_1, \ldots, x_n]$ and $>$ be a monomial order on $\mathbb{Z}^n_{\geq 0}$. Then for every $f \in K[x_1, \ldots, x_n]$ there exists $q_i, r \in K[x_1, \ldots, x_n]$, such that*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

where either $r = 0$ or r is a linear combination of monomials, with coefficients in K, none of which is divisible by any of $LT(f_1), \ldots, LT(f_s)$. We define r as being the ***remainder*** *of f on division by F. Additionally, if $q_i f_i \neq 0$, then*

$$multideg(f) \geq multideg(q_i f_i).$$

Proof. We begin by giving an algorithm for the construction of $q_1, \ldots, q_s$ and r to prove their existence, then show that it operates correctly for any given input. This algorithm is a generalization of the division algorithm in $K[x]$ given in Proposition 2:

Input : $f_1, \ldots, f_s, f$

Output : $q_1, \ldots, q_s, r$

$q_1 := 0; \cdots; q_s := 0; r := 0$

$p := f$

WHILE $p \neq 0$ DO

    $i := 1$

    $divisionoccured :=$ `false`

    WHILE $i \leq s$ AND $divisionoccurred =$ `false` DO

        IF $LT(f_i)$ divides $LT(p)$ THEN

            $q_i := q_i + LT(p)/LT(f_i)$

$p := p - (LT(p)/LT(f_i))f_i$

$divisionoccured :=$ `true`

ELSE

$i := i + 1$

IF $divisionoccured =$ `false` THEN

$r := r + LT(p)$

$p := p - LT(p)$

RETURN $q_1, \ldots, q_s, r$

In the example below we illustrate this algorithm with p representing the intermediate dividend at each stage, the variable r representing the column on the right-hand side, and the quotients listed above the division are the variables $q_1, \ldots, q_s$. Finally, the boolean variable "divisionoccurred" indicates when some $LT(f_i)$ divides the leading term of the intermediate dividend. Every time we pass through the main WHILE...DO loop, one of the following occurs:

- (Division Step) Some $LT(f_i)$ divides $LT(p)$: the algorithm then proceeds as in the one-variable case.
- (Remainder Step) No $LT(f_i)$ divides $LT(p)$: the algorithm then adds $LT(p)$ to the remainder.

To prove that this algorithm works, we will first show that at every stage

$$f = q_1 f_1 + \cdots + q_s f_s + p + r. \tag{2.40}$$

For the initial values of $q_1, \ldots, q_s, p$, and r, this is clearly true. Now suppose that, at one step of the algorithm, (2.40) holds. If the next step is a Division Step, then

$$q_i f_i + p = (q_i + LT(p)/LT(f_i))f_i + (p - (LT(p)/LT(f_i))f_i)$$

which shows that $q_i f_i + p$ is unchanged. As none of the other variables are affected, (2.40) remains true. If the next step is a Remainder Step, then p and r will be changed, however

$$p + r = (p - LT(p)) + (r + LT(p)).$$

so $p + r$ does not change, preserving (2.40).

Next, note that the algorithm stops when $p = 0$. In this case, (2.40) becomes

$$f = q_1 f_1 + \cdots + q_s f_s + r.$$

Since terms are only added to r when they are not divisible by any of the $LT(f_i)$, when the algorithm terminates, $q_1, \ldots, q_s$ and r have the desired properties.

Finally, we will show that the algorithm does indeed terminate. We claim that each time the variable p is redefined, either its multidegree drops (relative to our term ordering) or it becomes 0. We first consider the case that occurs during a Division Step, where p is redefined to be

$$p' = p - \frac{LT(p)}{LT(f_i)} f_i.$$

Then by Lemma 2, we have that

$$LT\left(\frac{LT(p)}{LT(f_i)} f_i\right) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p),$$

so that p and $(LT(p)/LT(f_i))f_i$ have the same leading term. Hence, when their difference $p' \neq 0$, it must have a strictly smaller multidegree. Now consider the case that occurs during a Remainder Step, where p is redefined to be

$$p' = p - LT(p).$$

Clearly, $multideg(p') < multideg(p)$ when $p' \neq 0$. Consequently, in either case, the multidegree must decrease. Hence, if the algorithm never terminated, we would have an infinite decreasing sequence of multidegrees. However, as stated in Lemma 1, the well-ordering property of $>$ guarantees that this will never occur. Thus, we will eventually have that $p = 0$, so that the algorithm terminates after finitely many steps.

Lastly, we will examine the relation between $multideg(f)$ and $multideg(q_i f_i)$. Note that every term of any given q_i is of the form $LT(p)/LT(f_i)$ for some value of the variable p. The algorithm begins with $p = f$, and, as shown above, the multidegree of p decreases; hence, $LT(p) \leq LT(f)$. Using condition (ii) of the definition of a monomial ordering, it follows that $multideg(q_i f_i) \leq multideg(f)$ when $q_i f_i \neq 0$. $\square$

We will now apply this algorithm in a relatively simple example to illustrate the procedure.

Example 3. *Suppose we wish to divide* $f = x^2y + xy^2 + y^2$ *by* $f_1 = xy - 1$ *and* $f_2 = y^2 - 1$ *with lexicographical order* $x > y$*. Listing the quotients* q_1, q_2 *and the divisors* f_1, f_2 *vertically, we have the following setup:*

$$\begin{array}{rl} q_1\text{:} & \\ q_2\text{:} & \\ xy-1 & \overline{\big)\, x^2y + xy^2 + y^2} \\ y^2-1 & \end{array}$$

Applying the division algorithm, and recalling that if both leading terms divide, we use f_1*, we find that:*

$$\begin{array}{rl} q_1\text{:} & x+y \\ q_2\text{:} & 1 \\ xy-1 & \overline{\big)\, x^2y + xy^2 + y^2} \\ y^2-1 & \end{array} \qquad \begin{array}{c} r \\ \hline \\ \\ \\ \\ \\ \\ \\ \end{array}$$

$$\begin{array}{l} x^2y - x \\ \hline \\ xy^2 + x + y^2 \\ xy^2 - y \\ \hline \\ x + y^2 + y \\ \hline \\ y^2 + y \qquad \longrightarrow \qquad x \\ y^2 - 1 \\ \hline \\ y + 1 \\ \hline \\ 1 \qquad \longrightarrow \qquad x + y \\ - \\ 0 \qquad \longrightarrow \qquad x + y + 1 \end{array}$$

We continue dividing until the polynomial at the bottom of the division, which we call the intermediate dividend, is zero. If neither $LT(f_1)$ *nor* $LT(f_2)$ *divides the intermediate dividend, then we move the intermediate dividend's leading term to the remainder column* r *and continue, as in the case of* $x + y^2 + y$*. At the end of the process, we find that* $x + y + 1$ *is the remainder and*

$$x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + (x + y + 1).$$

Note that the remainder consists of monomials, none of which are divisible by $LT(f_1)$ or $LT(f_2)$.

Both the monomial ordering and the ordering of the s-tuple of polynomials $(f_1, \ldots, f_s)$ can change the q_i and r along with the number of steps the algorithm will take to complete the calculation.

We will now turn our attention to monomial ideals, which are also required to define, and prove the existence of, Gröbner bases.

Definition 13. *An ideal $I \subseteq K[x_1, \ldots, x_n]$ is a **monomial ideal** if there exists $A \subseteq \mathbb{Z}_{\geq 0}^n$, which may be infinite, such that I consists of all polynomials that are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in K[x_1, \ldots, x_n]$. We express this as $I = \langle x^\alpha \mid \alpha \in A \rangle$.*

We will now characterize all monomials that lie in a given monomial ideal.

Lemma 3. *Let $I = \langle x^\alpha \mid \alpha \in A \rangle$ be a monomial ideal and x^β be a monomial. Then $x^\beta \in I$ if and only if x^β is divisible by x^α for some $\alpha \in A$.*

Proof. By the definition of an ideal, if x^β is a multiple of x^α for some $\alpha \in A$, then $x^\beta \in I$. Conversely, if we have that $x^\beta \in I$, then $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$, where $h_i \in K[x_1, \ldots, x_n]$ and $\alpha(i) \in A$ since I is a monomial ideal. Now expand each h_i as a sum of terms to obtain,

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)} = \sum_{i=1}^{s} \left(\sum_j c_{i,j} x^{\beta(i,j)} \right) x^{\alpha(i)} = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}. \tag{2.41}$$

Note that after collecting terms of the same multidegree, every term on the right side of the equation is divisible by some $x^{\alpha(i)}$, and hence divisible by some x^α. Therefore the left side must also be divisible by this x^α. □

The following lemma tells us that, by examining the monomials of f, we can determine whether a given polynomial f lies in a monomial ideal.

Lemma 4. *Let I be a monomial ideal and $f \in K[x_1, \ldots, x_n]$. Then the following are equivalent:*

(i) $f \in I$.

(ii) Every term of f lies in I.

(iii) f is a K-linear combination of the monomials in I.

Proof. The implications $(iii) \Rightarrow (ii) \Rightarrow (i)$ are trivial since ideals are closed under addition and scalar multiplication. We will now show that $(i) \Rightarrow (iii)$. As I is a monomial ideal, $f \in I$ it can be written in the form $f = \sum_{\alpha \in A} h_\alpha x^\alpha$ where $h_\alpha \in K[x_1, \ldots, x_n]$. Now write each h_α as a K-linear combination of monomials and expand, giving us f as a K-linear combination of monomials. By construction, all of these monomials are multiples of monomials in $\{x^\alpha \mid \alpha \in A\}$. Hence, by Lemma 3, these monomials also lie in I. Therefore, f is a K-linear combination of monomials in I [2]. □

An immediate consequence of this lemma is that a monomial ideal is uniquely determined by its monomials, giving us the following corollary.

Corollary 1. *Let I and J be monomial ideals. Then $I = J$ if and only if I and J contain the same monomials.*

Proof. Trivially, if two monomial ideals are the same, then they contain the same monomials. Conversely, from the proof of Lemma 4, every element of a monomial ideal can be constructed from monomials of the ideal. Therefore, if two monomial ideals contain the same monomials then every other element of those ideals will be the same [2]. □

The following theorem states that all monomial ideals of $K[x_1, \ldots, x_n]$ are finitely generated.

Theorem 8 (Dickson's Lemma)**.** *Let $I = \langle x^\alpha \mid \alpha \in A \rangle \subseteq K[x_1, \ldots, x_n]$ be a monomial ideal. Then there exists $\alpha(1), \ldots, \alpha(s) \in A$, such that $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. In particular, I has a finite basis.*

Proof. We proceed by induction on n, the number of variables. If $n = 1$, then $A \subseteq \mathbb{Z}_{\geq 0}$ and $I = \langle x_1^\alpha \mid \alpha \in A \rangle$. Let β be such that $\beta \leq \alpha$ for all $\alpha \in A$. Then x_1^β divides all the other generators x_1^α. It follows from Lemma 3 that $I = \langle x_1^\beta \rangle$.

Now assume that $n > 1$ and that our induction hypothesis holds for $n - 1$. We begin by writing the variables as $x_1, \ldots, x_{n-1}, y$, so that any monomial in $K[x_1, \ldots, x_{n-1}, y]$ can be written as $x^\alpha y^m$, where $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ and $m \in \mathbb{Z}_{\geq 0}$.

Let $I \subseteq K[x_1, \ldots, x_{n-1}, y]$ be a monomial ideal. In order to find generators for I, let J be the ideal in $K[x_1, \ldots, x_{n-1}]$ generated by the monomials x^α with the property

that $x^\alpha y^m \in I$ for some $m \geq 0$. Our inductive hypothesis implies that finitely many of the x^α's generate J, since J is a monomial ideal in $K[x_1, \ldots, x_{n-1}]$. Say $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ for $x^{\alpha(1)}, \ldots, x^{\alpha(s)} \in A$.

From the definition of J, for each i between 1 and s, we have that $x^{\alpha(i)} y^{m_i} \in I$ for some $m_i \geq 0$. Let $m \geq m_i$ for all $m_i \in \mathbb{Z}_{\geq 0}$. Then for every ℓ between 0 and $m-1$, let $J_\ell \subseteq K[x_1, \ldots, x_{n-1}]$ be the ideal generated by the monomials x^β for which $x^\beta y^\ell \in I$. From our inductive hypothesis, every J_ℓ has a finite generating set of monomials, say $J_\ell = \langle x^{\alpha_\ell(1)}, \ldots, x^{\alpha_\ell(s_\ell)} \rangle$.

We claim that the monomials in the following list generate I:

$$\begin{aligned}
\text{from } J &: x^{\alpha(1)} y^m, \ldots, x^{\alpha(s)} y^m, \\
\text{from } J_0 &: x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)}, \\
\text{from } J_1 &: x^{\alpha_1(1)} y, \ldots, x^{\alpha_1(s_1)} y, \\
&\vdots \\
\text{from } J_{m-1} &: x^{\alpha_{m-1}(1)} y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})} y^{m-1}.
\end{aligned}$$

Let $x^\alpha y^p \in I$. By the construction of J, if $p \geq m$, then $x^\alpha y^p$ is divisible by some $x^{\alpha(i)} y^m$. Otherwise, by the construction of J_p, if $p \leq m-1$, then $x^\alpha y^p$ is divisible by some $x^{\alpha_p(j)} y^p$. Therefore, every monomial in I is divisible by one on the list. Hence, from Lemma 3, the above monomials generate an ideal that has the same monomials as I. From Corollary 1, it follows that the ideals are the same, proving our claim.

If we now write the variables as $x_1, \ldots, x_n$, then our monomial ideal is $I = \langle x^\alpha \mid \alpha \in A \rangle \subseteq K[x_1, \ldots, x_n]$. We wish to show that finitely many x^α's generate I. From the previous paragraph, $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle$ for some monomials $x^{\beta(i)}$ in I. Since $x^{\beta(i)} \in I = \langle x^\alpha \mid \alpha \in A \rangle$, we have from Lemma 3 that each $x^{\beta(i)}$ is divisible by $x^{\alpha(i)}$ for some $\alpha(i) \in A$. From this it is easily seen that $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. □

As we have seen, leading terms play an important role in the division algorithm. This leads us to define the ideal of leading terms for any ideal I.

Definition 14. *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal with $I \neq \{0\}$, and fix a monomial ordering on $K[x_1, \ldots, x_n]$. Then:*

(i) *We denote the set of leading terms of nonzero elements of* I *by* $LT(I)$*. Hence,*

$$LT(I) = \{cx^\alpha \mid \text{there exists } f \in I \setminus \{0\} \text{ with } LT(f) = cx^\alpha\} \tag{2.42}$$

(ii) *We denote the ideal generated by the elements of* $LT(I)$ *by* $\langle LT(I)\rangle$*.*

A subtle but important detail is that if $I = \langle f_1, \ldots, f_s\rangle$, then $\langle LT(f_1), \ldots, LT(f_s)\rangle$ and $\langle LT(I)\rangle$ may be different ideals.

In the following proposition, we will show that $\langle LT(I)\rangle$ is a monomial ideal. This will allow us to apply some of our previous results to show that $\langle LT(I)\rangle$ is generated by finitely many leading terms.

Proposition 3. *Let* $I \subseteq K[x_1, \ldots, x_n]$ *be an ideal with* $I \neq \{0\}$*.*
(i) $\langle LT(I)\rangle$ *is a monomial ideal.*
(ii) *There exists* $g_1, \ldots, g_t \in I$ *such that* $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$*.*

Proof. (i) The leading monomials $LM(g)$ of $g \in I \setminus \{0\}$ generate the monomial ideal $\langle LM(g) \mid g \in I \setminus \{0\}\rangle$. As $LT(g)$ and $LM(g)$ only differ by a nonzero constant, $\langle LM(g) \mid g \in I \setminus \{0\}\rangle = \langle LT(g) \mid g \in I \setminus \{0\}\rangle = \langle LT(I)\rangle$. Therefore, $\langle LT(I)\rangle$ is a monomial ideal.

(ii) Since the monomials $LM(g)$ for $g \in I \setminus \{0\}$ generate $\langle LT(I)\rangle$ we have, from Theorem 8, that $\langle LT(I)\rangle = \langle LM(g_1), \ldots, LM(g_t)\rangle$ for finitely many $g_1, \ldots, g_t \in I$. As $LT(g_i)$ and $LM(g_i)$ only differ by a nonzero constant, this implies $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. □

We can now prove the existence of a finite generating set for every polynomial ideal by using Proposition 3 and the division algorithm for multivariate polynomials.

Theorem 9 (Hilbert Basis Theorem)**.** *If* $I \subseteq K[x_1, \ldots, x_n]$ *is an ideal, then* I *has a finite generating set. That is,* $I = \langle g_1, \ldots, g_t\rangle$ *for some* $g_1, \ldots, g_t \in I$*.*

Proof. Trivially, if $I = \{0\}$ then the generating set is $\{0\}$, which is finite. If I contains a nonzero polynomial, then we can construct a generating set $g_1, \ldots, g_t$ for I as follows.

First select a particular monomial ordering to be used in computing leading terms and in the division algorithm. Then $\langle LT(I)\rangle$ is an ideal of I and by Proposition 3,

there exists $g_1, \ldots, g_t \in I$ such that $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. We claim that $I = \langle g_1, \ldots, g_t \rangle$.

Clearly $\langle g_1, \ldots, g_t \rangle \subseteq I$ since every $g_i \in I$. To show the converse, begin by selecting a polynomial $f \in I$. Apply the division algorithm as described in Theorem 7 to divide f by $(g_1, \ldots, g_t)$, resulting in an expression of the form

$$f = q_1 g_1 + \cdots + q_t g_t + r \tag{2.43}$$

where r is the remainder, and hence, no term of r is divisible by any of $LT(g_1)$, $\ldots$, $LT(g_t)$. We wish to show that $r = 0$. Note that, by rearranging equation (2.43) we have

$$r = f - q_1 g_1 - \cdots - q_t g_t \in I. \tag{2.44}$$

Assume towards contradiction that $r \neq 0$. Then $LT(r) \in \langle LT(I) \rangle$ where $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. It follows that $LT(r)$ must be divisible by some $LT(g_i)$. This contradicts r being a remainder, hence, r must be zero. Therefore,

$$f = q_1 g_1 + \cdots + q_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle. \tag{2.45}$$

As f was an arbitrary element of I, this shows that $I \subseteq \langle g_1, \ldots, g_t \rangle$. □

In the proof of Theorem 9, the basis used $\{g_1, \ldots, g_t\}$ has the special property that $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. We will call these special bases by the following name.

Definition 15. *Fix a monomial order on the polynomial ring $K[x_1, \ldots, x_n]$ and let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal. Then a finite subset $G = \{g_1, \ldots, g_t\}$ of I is called a* ***Gröbner basis*** *if*

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Equivalently, for a set $G = \{g_1, \ldots, g_t\} \subseteq I$ the leading term of any element of I is divisible by one of the $LT(g_i)$ if and only if G is a Gröbner basis of I. Also, we define the Gröbner basis of the zero ideal $\{0\}$ to be the empty set $\varnothing$.

The following result is also established in the proof of Theorem 9.

Theorem 10. *Fix a monomial ordering on $K[x_1, \ldots, x_n]$. If $I \subseteq K[x_1, \ldots, x_n]$ is an ideal, then I has a Gröbner basis. Furthermore, any Gröbner basis of I is a basis of I.*

Proof. By definition, the set $G = \{g_1, \ldots, g_t\}$ constructed in the proof of Theorem 9 is a Gröber basis of I. For the second claim, if $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$, then from Theorem 9 we have that $I = \langle g_1, \ldots, g_t\rangle$. Therefore, G is a basis of I. □

The following theorem is an application of the Hilbert Basis Theorem (Theorem 9) which will be crucial in Buchberger's algorithm for constructing Gröbner bases.

Theorem 11. *(The Ascending Chain Condition). If*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

is an ascending chain of ideals in $K[x_1, \ldots, x_n]$, then there exists an $N \in \mathbb{Z}_{>0}$ such that

$$I_N = I_{N+1} = I_{N+2} = \cdots.$$

Proof. Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an ascending chain of ideals in $K[x_1, \ldots, x_n]$ and consider the set $I = \bigcup_{i=1}^{\infty} I_i$. We claim that I is also an ideal in $K[x_1, \ldots, x_n]$. Since $0 \in I_i$ for every i, we have that $0 \in I$. Next, if $f, g \in I$ then we must have that $f \in I_i$, and $g \in I_j$ for some i and j. However, since the ideals form an ascending chain, we must have that if $i \leq j$, then $f, g \in I_j$. Since I_j is an ideal, $f + g \in I_j \subseteq I$. Similarly, if $f \in I$ and $r \in K[x_1, \ldots, x_n]$, then for some i, $f \in I_i$ and $r \cdot f \in I_i \subseteq I$. Hence, I is an ideal.

By Theorem 9 (Hilbert Basis Theorem), I has a finite generating set: $I = \langle f_1, \ldots, f_s\rangle$. Additionally, each of these generators is contained in some I_j from the ascending chain of ideals, say $f_i \in I_{j_i}$ for some $j_i, i = 1, \ldots, s$. Let N be the maximum of the j_i's. Hence, $f_i \in I_N$ for all i giving us that

$$I = \langle f_1, \ldots, f_s\rangle \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I.$$

Therefore, the ascending chain stabilizes with I_N. □

We will now discuss the properties of Gröbner bases that are necessary for solving the implicitization problem. We begin by showing that, when we divide by a Gröbner basis, the remainder is uniquely determined.

Proposition 4. *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal and $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for I. Then given $f \in K[x_1, \ldots, x_n]$, there exists a unique $r \in K[x_1, \ldots, x_n]$ with the following properties:*

(i) No term of r is divisible by $LT(g_1), \ldots, LT(g_t)$.

(ii) There exists a $g \in I$ such that $f = g + r$.

In particular, no matter how the elements of G are listed, r is the remainder on division of f by G when using the division algorithm.

Proof. From the division algorithm (Theorem 7), we have that $f = q_1 g_1 + \cdots + q_t g_t + r$, where r satisfies (i). Also, by setting $g = q_1 g_1 + \cdots + q_t g_t \in I$, (ii) is satisfied. Hence, an r exists that satisfies these properties.

For uniqueness, suppose (i) and (ii) are also satisfied by $f = g + r = g' + r'$. Then $r - r' = g' - g \in I$, so if $r \neq r'$, then $LT(r - r') \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Hence, by Lemma 3, $LT(r - r')$ is divisible by some $LT(g_i)$. However, this is impossible as no term of r, r' is divisible by any $LT(g_1), \ldots, LT(g_t)$. Therefore, $r - r'$ must be zero, giving us that r is unique.

The last part of the proposition is a result of the uniqueness of r. □

If we list the generators of a Gröbner basis in a different order, then, although the remainder r is unique, the quotients produced by the division algorithm can change.

We obtain the following criterion for when a given polynomial lies in an ideal as a corollary of Proposition 4.

Corollary 2. *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal, $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for I, and let $f \in K[x_1, \ldots, x_n]$. Then $f \in I$ if and only if, on division of f by G, the remainder is zero.*

Proof. We have already observed that $f \in I$ when the remainder is zero. Conversely, given $f \in I$, then the two conditions of Proposition 4 are satisfied by $f = f + 0$. Hence, the remainder of f on division by G is 0. □

For simplicity, we will use the following notation.

Definition 16. *We denote the remainder on division of f by the ordered s-tuple $F = (f_1, \ldots, f_s)$ as $\overline{f}^F$. By Proposition 4, we can regard F as a set (without any particular order) if F is a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$.*

We wish to be able to distinguish when a given generating set of an ideal is a Gröbner basis. This will require the following definitions.

Definition 17. *Let $f, g \in K[x_1, \ldots, x_n]$ where f, g are nonzero polynomials*

*(i) Let $multideg(f) = \alpha$ and $multideg(g) = \beta$, then set $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. Then the **least common multiple** of $LM(f)$ and $LM(g)$ is $x^\gamma = lcm(LM(f), LM(g))$.*

*(ii) The **S-polynomial** of f and g is:*

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$$

The following lemma shows that every cancellation of leading terms among polynomials of the same multidegree is a result of the cancellation that happens for S-polynomials.

Lemma 5. *Consider the sum $\sum_{i=1}^s p_i$, where $multideg(p_i) = \delta \in \mathbb{Z}_{\geq 0}^n$ for all i. If $multideg(\sum_{i=1}^s p_i) < \delta$, then $\sum_{i=1}^s p_i$ is a linear combination of the S-polynomials $S(p_j, p_l)$ for $1 \leq j$ and $l \leq s$, with coefficients in K. Furthermore, the multidegree of every $S(p_j, p_l)$ is strictly less than δ.*

Proof. Let $d_i = LC(p_i)$, so that the leading term of p_i is $d_i x^\delta$. Since the sum $\sum_{i=1}^s p_i$ has strictly smaller multidegree, it easily follows that $\sum_{i=1}^s d_i = 0$.

Now, since p_i and p_j have the same leading monomial, their S-polynomial is

$$S(p_i, p_j) = \frac{1}{d_i} p_i - \frac{1}{d_j} p_j. \tag{2.46}$$

It follows that

$$\sum_{i=1}^{s-1} d_i S(p_i, p_s) = d_1\left(\frac{1}{d_1}p_1 - \frac{1}{d_s}p_s\right) + d_2\left(\frac{1}{d_2}p_2 - \frac{1}{d_s}p_s\right) + \cdots \tag{2.47}$$
$$= p_1 + p_2 + \cdots + p_{s-1} - \frac{1}{d_s}(d_1 + \cdots + d_{s-1})p_s.$$

However, $\sum_{i=1}^{s} d_i = 0$ implies that $d_1 + \cdots d_{s-1} = -d_s$, hence we have from (2.47) that

$$\sum_{i=1}^{s-1} d_i S(p_i, p_s) = p_1 + \cdots + p_{s-1} + p_s.$$

Therefore, $\sum_{i=1}^{s} p_i$ is a linear combination of S-polynomials of the desired form, and it can be easily seen from equation (2.46) that the multidegree of $S(p_i, p_j)$ is strictly less than δ. □

We can now prove the following criterion for when a basis of an ideal is a Gröbner basis by using S-polynomials and Lemma 5.

Theorem 12. *(Buchberger's Criterion). Let $I \subseteq K[x_1, \ldots, x_n]$ be a polynomial ideal. A basis $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I if and only if for all i and j, $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.*

Proof. If G is a Gröbner basis, then by Corollary 2 we have that the remainder on division by G is zero, since $S(g_i, g_j) \in I$.

For the converse, let $f \in I$ be a nonzero polynomial. We will show that $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$ and begin by writing

$$f = \sum_{i=1}^{t} h_i g_i, \qquad h_i \in K[x_1, \ldots, x_n].$$

It follows from Lemma 2 that

$$multideg(f) \leq \max(multideg(h_i g_i) \mid h_i g_i \neq 0). \tag{2.48}$$

Our strategy for this proof consists of selecting the most efficient representation of f, that is, among all of the expressions $f = \sum_{i=1}^{t} h_i g_i$ we choose the one for which

$$\delta = \max(multideg(h_i g_i) \mid h_i g_i \neq 0)$$

is minimal. We know that such a δ exists by the well-ordering property of our monomial ordering. It follows that $multideg(f) \leq \delta$ by equation (2.48).

In the case that $multideg(f)$ is equal to the minimal δ, then $multideg(f)$ is equal to $multideg(h_i g_i)$ for some i. It easily follows that $LT(f)$ is divisible by $LT(g_i)$, giving us that $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$, as desired.

In the case that the minimal δ satisfies $multideg(f) < \delta$, we find a new expression for f using $\overline{S(g_i, g_j)}^G = 0$ for $i \neq j$ that will decrease δ. This will contradict the minimality of δ, eliminating the possibility of this case and completing the proof.

Given the selected expression with minimal δ, $f = \sum_{i=1}^{t} h_i g_i$, we begin by isolating the part where multidegree δ occurs:

$$\begin{aligned} f &= \sum_{multideg(h_i g_i)=\delta} h_i g_i + \sum_{multideg(h_i g_i)} h_i g_i \qquad (2.49) \\ &= \sum_{multideg(h_i g_i)=\delta} LT(h_i) g_i + \sum_{multideg(h_i g_i)=\delta} (h_i - LT(h_i)) g_i + \sum_{multideg(h_i g_i)<\delta} h_i g_i. \end{aligned}$$

On the second line, the monomials in the second and third sums all have multidegree strictly less than δ. Since $multideg(f) < \delta$, this implies that the multidegree of the first sum on the second line also is also strictly less than δ.

We will proceed to decrease δ by rewriting the first sum in two stages: first we will use Lemma 5 to rewrite it in terms of S-polynomials, then rewrite the S-polynomials without cancellation by using $\overline{S(g_i, g_j)}^G = 0$.

To rewrite the first sum in terms of S-polynomials, note that in

$$\sum_{multideg(h_i g_i)=\delta} LT(h_i) g_i \qquad (2.50)$$

each $p_i = LT(h_i) g_i$ has multidegree δ and that the multidegree of the sum is strictly less than δ. Hence, the hypothesis of Lemma 5 is satisfied, giving us that the first sum is a linear combination of the S-polynomials $S(p_i, p_j)$ with coefficients in K. It can be easily shown that

$$S(p_i, p_j) = x^{\delta - \gamma_{ij}} S(g_i, g_j), \qquad (2.51)$$

where $x^{\gamma_{ij}} = lcm(LM(g_i), LM(g_j))$. Hence, the first sum, equation (2.50), can be expressed as a linear combination of $x^{\delta-\gamma_{ij}}S(g_i, g_j)$ for certain pairs (i, j).

Now consider one of these S-polynomials, $S(g_i, g_j)$. Since $\overline{S(g_i, g_j)}^{G} = 0$, we can use the division algorithm (Theorem 7) to find the following expression

$$S(g_i, g_j) = \sum_{l=1}^{t} A_l g_l, \tag{2.52}$$

where $A_l \in K[x_1, \ldots, x_n]$ and

$$multideg(A_l g_l) \leq multideg(S(g_i, g_j)) \tag{2.53}$$

when $A_l g_l \neq 0$. Now multiply equation (2.52) through by $x^{\delta-\gamma_{ij}}$ to obtain

$$x^{\delta-\gamma_{ij}}S(g_i, g_j) = \sum_{l=1}^{t} B_l g_l, \tag{2.54}$$

where $B_l = x^{\delta-\gamma_{ij}}A_l$. When $B_l g_l \neq 0$, equation (2.53) implies that

$$multideg(B_l g_l) \leq multideg(x^{\delta-\gamma_{ij}}S(g_i, g_j)) < \delta \tag{2.55}$$

since $LT(S(g_i, g_j)) < lcm(LM(g_i), LM(g_j)) = x^{\gamma_{ij}}$.

Hence, equation (2.50) is a linear combination of certain $x^{\delta-\gamma_{ij}}S(g_i, g_j)$, which all satisfy equations (2.54) and (2.55). Therefore, we can rewrite the first sum as

$$\sum_{multideg(h_i g_i)=\delta} LT(h_i)g_i = \sum_{l=1}^{t} \tilde{B}_l g_l \tag{2.56}$$

where, when $\tilde{B}_l g_l \neq 0$, we have that

$$multideg(\tilde{B}_l g_l) < \delta. \tag{2.57}$$

Substituting equation (2.56) into the second line of equation (2.49) results in an expression for f as a polynomial combination of the g_i's where the multidegree of all terms is strictly less than δ. This contradicts the minimality of δ, as desired. □

The Buchberger criterion makes it easy to show whether a given basis is a Gröbner basis, but it also naturally leads to an algorithm for constructing Gröbner bases.

Theorem 13. *(Buchberger's Algorithm). Let $I = \langle f_1, \ldots, f_s \rangle \neq 0$ be a polynomial ideal. Then a Gröbner basis for I can be constructed by the following algorithm in a finite number of steps:*

Input : $F = (f_1, \ldots, f_s)$

Output : *a Gröbner basis* $G = (g_1, \ldots, g_t)$ *for* I, *with* $F \subseteq G$

$G := F$

REPEAT

$G' := G$

FOR each pair $\{p, q\}$, $p \neq q$ *in* G' *DO*

$r := \overline{S(p,q)}^{G'}$

IF $r \neq 0$ *THEN* $G := G \cup \{r\}$

UNTIL $G = G'$

RETURN G

Proof. If $G = \{g_1, \ldots, g_t\}$, then:

$$\langle G \rangle = \langle g_1, \ldots, g_t \rangle,$$
$$\langle LT(G) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

We first show that $G \subseteq I$ at every stage of the algorithm. This is true initially, and in every step afterwards for which we enlarge G, we add the remainder $r = \overline{S(p,q)}^{G'}$ for $p, q \in G' \subseteq G$. Thus, if $G \subseteq I$, then p, q and $S(p,q)$ are in I. Hence, we have that $G \cup \{r\} \subseteq I$ since we are dividing by $G' \subseteq I$. We also note that G is a basis of I as G contains the basis F of I.

The algorithm terminates when $G = G'$, which occurs when $r = \overline{S(p,q)}^{G'} = 0$ for all $p, q \in G$. Hence by Theorem 12, G is a Gröbner basis of $\langle G \rangle = I$. However, we must show that the algorithm does terminate. Consider what happens after each pass through the main loop has completed. The set G consists of G' and the nonzero remainders of S-polynomials of elements of G'. Then, since $G' \subseteq G$, we have that

$$\langle LT(G') \rangle \subseteq \langle LT(G) \rangle \tag{2.58}$$

Furthermore, we claim that $\langle LT(G')\rangle$ is strictly smaller than $\langle LT(G)\rangle$ if $G' \neq G$. To see this, suppose that r is adjoined to G where r is a nonzero remainder of an S-polynomial. Since r is a remainder on division by G', $LT(r)$ is not divisible by the leading terms of elements of G', and hence, by Lemma 3, $LT(r) \notin \langle LT(G')\rangle$. However, $LT(r) \in \langle LT(G)\rangle$, which proves our claim.

From successive iterations of the loop, the ideals $\langle LT(G')\rangle$ form an ascending chain of ideals in $K[x_1, \ldots, x_n]$ by equation 2.58. Thus, the ascending chain condition (Theorem 11) implies that the chain will stabilize after a finite number of iterations, so that eventually $\langle LT(G')\rangle = \langle LT(G)\rangle$. This implies that $G' = G$ by the previous paragraph, and hence, the algorithm will terminate after a finite number of steps. □

The above algorithm was chosen due to its clarity. However, there are more efficient algorithms for computing Gröbner bases.

We require a few more definitions, theorems, lemmas and propositions before we can utilize the properties of Gröbner bases for implicitization. We begin with the following definition.

Definition 18. *Let $I = \langle f_1, \ldots, f_s\rangle \subseteq K[x_1, \ldots, x_n]$, then the l^{th}* ***elimination ideal*** *of I with respect to the lexicographical ordering $x_1 > x_2 > \cdots > x_n$ is defined by*

$$I_l = I \cap K[x_{l+1}, \ldots, x_n].$$

Hence, eliminating $x_1, \ldots, x_l$ is equivalent to finding nonzero polynomials in the l^{th} elimination ideal I_l. With the proper term ordering, we can do this instantly with Gröbner bases.

Theorem 14 (The Elimination Theorem)**.** *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal and let a Gröbner basis of I with respect to the lexicographical order $x_1 > x_2 > \cdots > x_n$ be G. Then, for every $0 \leq l \leq n$, a Gröbner basis of the l^{th} elimination ideal I_l is the set*

$$G_l = G \cap K[x_{l+1}, \ldots, x_n].$$

Proof. Fix an l such that $0 \leq l \leq n$. By construction, $G_l \subseteq I_l$ so, by the definition of a Gröbner basis, it suffices to show that

$$\langle LT(I_l)\rangle = \langle LT(G_l)\rangle. \tag{2.59}$$

That $\langle LT(G_l)\rangle \subseteq \langle LT(I_l)\rangle$ is obvious. For the other inclusion $\langle LT(I_l)\rangle \subseteq \langle LT(G_l)\rangle$, we need only show that for a polynomial $f \in I_l$, its leading term $LT(f)$ is divisible by $LT(g)$ for some $g \in G_l$.

First note that $f \in I$; since G is a Gröbner basis of I this implies that $LT(f)$ is divisible by $LT(g)$ for some $g \in G$. As $f \in I_l$, this implies that $LT(g)$ only involves the variables $x_{l+1}, \ldots, x_n$. Since we are using the lexicographical ordering $x_l > x_2 > \cdots > x_n$, any monomial involving an x_i from $x_1, \ldots, x_l$ is greater than all monomials in $K[x_{l+1}, \ldots, x_n]$. Therefore, as $LT(g) \in K[x_{l+1}, \ldots, x_n]$, we must have that $g \in K[x_{l+1}, \ldots, x_n]$. As $g \in G$ and $g \in K[x_{l+1}, \ldots, x_n]$, we have that $g \in G_l$, as desired. □

We wish to connect elimination ideals to varieties in order to implicitize multivariate parametric representations; this will require the following definition.

Definition 19. *The map*

$$\pi_l : \mathbb{C}^n \to \mathbb{C}^{n-l} \tag{2.60}$$

which sends $(a_1, \ldots, a_n)$ *to* $(a_{l+1}, \ldots, a_n)$ *is called the* ***projection map****.*

Let $V = V(f_1, \ldots, f_s) \subseteq \mathbb{C}^n$ and note that $\pi_l(V) \subseteq \mathbb{C}^{n-l}$. This eliminates the first l variables $x_1, \ldots, x_l$, hence, we can relate $\pi_l(V)$ to the l^{th} elimination ideal.

Lemma 6. *Using the above notation, let* $I_l = \langle f_1, \ldots, f_s\rangle \cap \mathbb{C}[x_{l+1}, \ldots, x_n]$ *be the* l^{th} *elimination ideal. Then* $\pi_l(V) \subseteq V(I_l)$ *in* $\mathbb{C}^{n-l}$*.*

Proof. Fix $f \in I_l$ and let $(a_1, \ldots, a_n) \in V$. Since $f \in \langle f_1, \ldots, f_s\rangle$, we have that $f(a_1, \ldots, a_n) = 0$. However, f only involves the variables $x_{l+1}, \ldots, x_n$, hence

$$f(a_{l+1}, \ldots, a_n) = f(\pi_l(a_1, \ldots, a_n)) = 0. \tag{2.61}$$

Therefore, f vanishes at all points of $\pi_l(V)$. □

With the aid of the following proposition, we now have all the information required to state and prove the implicitization theorems.

Proposition 5. *Let* K *be an infinite field and* $f \in K[x_1, \ldots, x_n]$*. Then* f *is the zero polynomial if and only if* $f : K^n \to K$ *is the zero function.*

Before we begin, it is imperative that we clarify the distinction between the zero polynomial and the zero function. The zero polynomial is a polynomial for which all of its coefficients a_i are zero. However, we call $f \in K[x_1, \ldots, x_n]$ a zero function if $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in K^n$. For example, consider the case where $K = \mathbb{Z}/2\mathbb{Z}$ and let $f = x^2x = x(x-1) \in K[x]$. Clearly f is a zero function, however, it is not a zero polynomial.

Proof. One direction is obvious since the zero polynomial clearly gives the zero function. For the converse we will show that if $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in K^n$, then f is the zero polynomial. We proceed by induction on the number of variables n.

For $n = 1$, recall that a nonzero polynomial in $K[x]$ of degree m has at most m distinct roots. Given $f \in K[x]$, where $f(a) = 0$ for all $a \in K$, since K is infinite, this implies that f has infinitely many roots. This can only be true if f is the zero polynomial.

Now assume that the converse statement is true for $n-1$, and let $f \in K[x_1, \ldots, x_n]$ be a zero function. We can rewrite f as

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1}) x_n^i,$$

where $g_i \in K[x_1, \ldots, x_{n-1}]$. We claim that each g_i is the zero polynomial, from which it follows that f is the zero polynomial in $K[x_1, \ldots, x_n]$.

If we fix $(a_1, \ldots, a_{n-1}) \in K^{n-1}$, then $f(a_1, \ldots, a_{n-1}, x_n) \in K[x_n]$. This vanishes for every $a_n \in K$, by our hypothesis on f. From the $n = 1$ case, it follows that $f(a_1, \ldots, a_{n-1}, x_n)$ is the zero polynomial in $K[x_n]$, and hence $g_i(a_1, \ldots, a_{n-1}) = 0$ for all i. Since $(a_1, \ldots, a_{n-1})$ was arbitrary, each $g_i \in K[x_1, \ldots, x_{n-1}]$ is the zero function on K^{n-1}. Then, using our induction hypothesis, this implies that each g_i is the zero polynomial in $K[x_1, \ldots, x_{n-1}]$. Therefore, f must be the zero polynomial in $K[x_1, \ldots, x_n]$. □

We begin our discussion of the implicitization theorems with polynomial parametrizations and then discuss rational parametrizations. However, some care must be taken

as the parametrization need not fill up all of the variety V. Even when considering the smallest variety containing the parametrization, the question of whether a parametrization fills up all of this variety can be difficult to answer and must be analyzed for each case.

Consider a polynomial parametrization of an algebraic variety given by

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m), \end{aligned} \tag{2.62}$$

where $f_1, \ldots, f_n$ are polynomials in $K[t_1, \ldots, t_m]$. Geometrically, this is the function

$$F : K^m \to K^n \tag{2.63}$$

defined by

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)). \tag{2.64}$$

Then the subset of K^n parametrized by equation (2.62) is $F(K^m) \subseteq K^n$. However, $F(K^m)$ may not be an affine variety, hence, a solution of the implicitization problem will require finding the smallest affine variety that contains $F(K^m)$.

Note that equation (2.62) defines a variety $V = V(x_1 - f_1, \ldots, x_n - f_n) \subseteq K^{m+n}$ where the points of V can be written as

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

This shows that V can be viewed as the graph of F. We also have the following two functions

$$\begin{aligned} i &: K^m \longrightarrow K^{m+n}, \\ \pi_m &: K^{m+n} \longrightarrow K^n, \end{aligned}$$

which are defined by

$$i(t_1, \ldots, t_m) = (t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m))$$

and

$$\pi_m(t_1, \ldots, t_m, x_1, \ldots, x_n) = (x_1, \ldots, x_n),$$

respectively. We can utilize these functions to produce the following diagram of sets and maps:

$$\begin{array}{ccc} & K^{m+n} & \\ {\scriptstyle i}\nearrow & & \searrow{\scriptstyle \pi_m} \\ K^m & \xrightarrow{\quad F \quad} & K^n \end{array} \tag{2.65}$$

Note that $F = \pi_m \circ i$, and it is straightforward to show that $i(K^m) = V$. Hence, we obtain

$$F(K^m) = \pi_m(i(K^m)) = \pi_m(V). \tag{2.66}$$

This means that the image of the parametrization is the projection of its graph. We can now find the smallest variety containing $F(K^m)$ by using elimination theory.

Theorem 15 (Polynomial Implicitization)**.** *If K is an infinite field, let I be the ideal $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle \subseteq K[t_1, \ldots, t_m, x_1, \ldots, x_n]$. Also let the m^{th} elimination ideal be $I_m = I \cap K[x_1, \ldots, x_n]$ and the function determined by the parametrization be $F : K^m \to K^n$. Then the smallest variety in K^n containing $F(K^m)$ is $V(I_m)$.*

Proof. From equation (2.66) and Lemma 6, $F(K^m) = \pi_m(V) \subseteq V(I_m)$. Hence, $V(I_m)$ is a variety containing $F(K^m)$ but we must also show that it is the smallest such variety. Consider $h \in K[x_1, \ldots, x_n]$ such that h vanishes on $F(K^m)$. We wish to show that $h \in I_m$. If we consider h as a polynomial in $K[t_1, \ldots, t_m, x_1, \ldots, x_n]$, then we can divide h by $x_1 - f_1, \ldots, x_n - f_n$, using the lexicographical order $x_1 > \cdots > x_n > t_1 > \cdots > t_m$. Since $LT(x_j - f_j) = x_j$, this produces the following equation

$$h(x_1, \ldots, x_n) = q_1 \cdot (x_1 - f_1) + \cdots + q_n \cdot (x_n - f_n) + r(t_1, \ldots, t_m). \tag{2.67}$$

Now for any $\mathbf{a} = (a_1, \ldots, a_m) \in K^m$, we can substitute $t_i = a_i$ and $x_i = f_i(\mathbf{a})$ into equation (2.67) to obtain

$$0 = h(f_1(\mathbf{a}), \ldots, f_n(\mathbf{a})) = 0 + \cdots + 0 + r(\mathbf{a}). \tag{2.68}$$

Therefore, $r(\mathbf{a}) = 0$ for all $\mathbf{a} \in K^m$. From Proposition 5, $r(t_1, \ldots, t_m)$ is the zero polynomial since K is infinite. Hence, as $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$, we have

$$h(x_1, \ldots, x_n) = q_1 \cdot (x_1 - f_1) + \cdots + q_n \cdot (x_n - f_n) \in I \cap K[x_1, \ldots, x_n] = I_m \tag{2.69}$$

Now suppose $Z = V(h_1, \ldots, h_s)$ is also a variety of K^n such that $F(K^m) \subseteq Z$. By the previous paragraph, each h_i vanishes on $F(K^m)$ and, consequently, is in I_m. Hence,

$$V(I_m) \subseteq V(h_1, \ldots, h_s) = Z. \tag{2.70}$$

Therefore, $V(I_m)$ is the smallest variety of K^n containing $F(K^m)$, as desired. □

If we have a parametrization as given in (2.62), and K is infinite, let I and I_m be as described in Theorem 15. With respect to a lexicographical ordering where all t_i are greater than every x_i, compute a Gröbner basis. Then by the Elimination Theorem and Theorem 15, the smallest variety in K^n that contains the parametrization are the elements of the Gröbner basis not involving $t_1, \ldots, t_m$.

We now consider the general situation of a rational parametrization given by

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}, \end{aligned} \tag{2.71}$$

where $f_1, \ldots, f_n, g_1, \ldots, g_n$ are polynomials in $K[t_1, \ldots, t_m]$. The map $F : K^m \longrightarrow K^n$ given by equation (2.71) may not be defined on all of K^m due to the denominators. However, if we let $W = V(g_1 g_2 \cdots g_n) \subseteq K^m$, then

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right)$$

defines a map

$$F : K^m \backslash W \longrightarrow K^n.$$

Solving the implicitization problem will now require finding the smallest variety of K^n containing $F(K^m \backslash W)$.

Adapting diagram (2.65) to this case, we have that

$$\begin{array}{ccc} & K^{m+n} & \\ {\scriptstyle i}\nearrow & & \searrow{\scriptstyle \pi_m} \\ K^m \backslash W & \xrightarrow{\quad F \quad} & K^n \end{array} \tag{2.72}$$

It is straightforward to check that $i(K^m \backslash W) \subseteq V(I)$, where $I = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n \rangle$ is the ideal that would be obtained by "clearing denominators." However, $V(I)$ may not be the smallest variety containing $i(K^m \backslash W)$.

To avoid this, we will use a new variable to slightly alter the ideal I in order to control the denominators. Consider the polynomial ring $K[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$ with affine space K^{1+m+n}. Let $g = g_1 \cdot g_2 \cdots g_n$, so that $W = V(g)$, and consider the ideal

$$J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle \subseteq K[y, t_1, \ldots, t_m, x_1, \ldots, x_n].$$

Note that $1 - gy = 0$ ensures that the denominators $g_1, \ldots, g_n$ never vanish on $V(J)$. Before we adapt diagram (2.72) to this new situation, consider the following maps

$$j : K^m \backslash W \longrightarrow K^{1+m+n},$$
$$\pi_{1+m} : K^{1+m+n} \longrightarrow K^n,$$

defined by

$$j(t_1, \ldots, t_m) = \left(\frac{1}{g_{t_1,\ldots,t_m}}, t_1, \ldots, t_m, \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right)$$

and

$$\pi_{1+m}(y, t_1, \ldots, t_m, x_1, \ldots, x_n) = (x_1, \ldots, x_n),$$

respectively. We can utilize these functions to produce the following diagram:

$$\begin{array}{ccc} & & K^{1+m+n} \\ & \overset{j}{\nearrow} & \quad \searrow^{\pi_{1+m}} \\ K^m \backslash W & \xrightarrow{\qquad F \qquad} & K^n \end{array} \tag{2.73}$$

Note that $F = \pi_{1+m} \circ j$ as before. Perhaps more surprising is that $j(K^m \backslash W) = V(J)$ in K^{1+m+n}. Clearly $j(K^m \backslash W) \subseteq V(J)$, since this easily follows from the definitions of j and J. Conversely, if $(y, t_1, \ldots, t_m, x_1, \ldots, x_n) \in V(J)$, then $g(t_1, \ldots, t_m)y = 1$ gives us that none of the g_i's vanish at $(t_1, \ldots, t_m)$ and, hence, that $g_i(t_1, \ldots, t_m)x_i = f_i(t_1, \ldots, t_m)$ can be solved for $x_i = f_i(t_1, \ldots, t_m) \backslash g_i(t_1, \ldots, t_m)$. It follows that our point lies in $j(K^m \backslash W)$, since $y = 1 \backslash g(t_1, \ldots, t_m)$. Therefore, $V(J) \subseteq j(K^m \backslash W)$.

From $F = \pi_{1+m} \circ j$ and $j(K^m \backslash W) = V(J)$, we have that

$$F(K^M \backslash W) = \pi_{1+m}(j(K^m \backslash W)) = \pi_{1+m}(V(J)). \tag{2.74}$$

This means that the image of the parametrization is the projection of the variety $V(J)$. We can now find the smallest variety containing $F(K^M \backslash W)$ by using elimination theory.

Theorem 16 (Rational Implicitization)**.** *Consider a rational parametrization as given in equation* (2.71) *and a new variable* y*. If* K *is an infinite field, let* g *be* $g_1 \cdot g_2 \cdots g_n$*,* $W = V(g)$*, and* J *be the ideal* $J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle \subseteq K[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$*. Also let the* $(1+m)^{th}$ *elimination ideal be* $J_{1+m} = J \cap K[x_1, \ldots, x_n]$ *and the function determined by the rational parametrization be* $F : K^m \backslash W \to K^n$*. Then the smallest variety in* K^n *containing* $F(K^m \backslash W)$ *is* $V(J_{1+m})$*.*

Proof. Similar to Theorem 15, we wish to show that $V(J_{1+m})$ is the smallest variety containing $F(K^m \backslash W)$. Consider $h \in K[x_1, \ldots, x_n]$ such that h vanishes on $F(K^m \backslash W)$. We begin by showing that $h \in J_{1+m}$. In the proof of Theorem 15, to obtain equation (2.67) we divided h by $x_i - f_i$. Similarly, we divide h by $g_i x_i - f_i$ in this case, however, we must also multiply h by a power of $g = g_1 \cdots g_n$. This results in equation (2.67) getting replaced by

$$g^N h(x_1, \ldots, x_n) = q_1 \cdot (g_1 x_1 - f_1) + \cdots + q_n \cdot (g_n x_n - f_n) + r(t_1, \ldots, t_m) \tag{2.75}$$

in $K[t_1, \ldots, t_m, x_1, \ldots, x_n]$, where N is a sufficiently large integer.

Now note that for any given $\mathbf{a} = (a_1, \ldots, a_m) \in K^m \backslash W$, we have that $g_i(\mathbf{a}) \neq 0$ for all i. Hence, we can substitute $t_i = a_i$ and $x_i = f_i(\mathbf{a})/g_i(\mathbf{a})$ into equation (2.75) to obtain

$$0 = g(\mathbf{a})^N h(f_1(\mathbf{a})/g_1(\mathbf{a})), \ldots, f_n(\mathbf{a})/g_n(\mathbf{a})) = 0 + \cdots + 0 + r(\mathbf{a}). \tag{2.76}$$

Therefore, $r(\mathbf{a}) = 0$ for all $\mathbf{a} \in K^m \backslash W$. This implies that $r(t_1, \ldots, t_m)$ is the zero polynomial, since K is infinite. Hence, we obtain

$$g^N h(x_1, \ldots, x_n) = q_1 \cdot (g_1 x_1 - f_1) + \cdots + q_n \cdot (g_n x_n - f_n), \tag{2.77}$$

which implies that $g^N h \in \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n \rangle \subseteq K[t_1, \ldots, t_m, x_1, \ldots, x_n]$. Now consider the following identity,

$$h = g^N y^N h + h(1 - g^N y^N) = y^N (g^N h) + h(1 + gy + \cdots + g^{N-1} y^{N-1})(1 - gy). \tag{2.78}$$

Combining this with equation (2.77), we see that in $K[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$,

$$h(x_1, \ldots, x_n) \in \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle \cap K[x_1, \ldots, x_n] = J_{1+m} \tag{2.79}$$

by the definition of J. From here, we may follow the procedure from the proof of Theorem 15. □

If we have a rational parametrization as given in (2.71), and K is infinite, let g, W, J, and J_{1+m} be as described in Theorem 16. With respect to a lexicographical ordering where y and all t_i are greater than every x_i, compute a Gröbner basis. Then the smallest variety in K^n that contains the parametrization are the elements of the Gröbner basis not involving $y, t_1, \ldots, t_m$.

Note that the implicit representation produced when using Gröbner bases depends on the lexicographical ordering as well as the order of the parametric equations.

2.4 Resultants versus Gröbner Basis

Relationship between Resultants and Gröbner Bases:

Consider the case of a polynomial parametric representation of n equations with m parameters. From the note following Theorem 4, there are $(n!)(m!)$ potential implicit representations which can be found using resultants. Similarly for Gröbner bases, there are $m!$ ways that we may order the parameters $t_1, \ldots, t_m$ to be eliminated and $n!$ ways to order the $x_1 - f_1, \ldots, x_n - f_n$ in our ideal I, giving us $(n!)(m!)$ potential implicit representations. Furthermore, for rational parametric representations with n equations and m parameters, both resultants and Gröbner bases produce $(n+1)!(m+1)!$ potential implicit representations. These observations and experimental data leads us to the following conjecture:

Conjecture 1. *Every implicit representation of an algebraic variety that can be found through resultants can also be found using the the Gröbner basis method of implicitization and vice versa.*

With this in mind, one may wonder which method is preferred for implicitization, to address this we will consider extraneous factors and computational complexity.

Extraneous Factors:

Implicitization using Sylvester or Bézout resultants can result in extraneous factors that may be difficult to recognize and eliminate, as in the following example [7].

Example 3. *A parametrization of the unit sphere is given by*

$$x = \frac{1 - s^2 - t^2}{1 + s^2 + t^2},$$
$$y = \frac{2s}{1 + s^2 + t^2},$$
$$z = \frac{2t}{1 + s^2 + t^2}.$$

Following the procedure from Theorem 5 or Theorem 6, we begin by rewriting the parametric equations as

$$y_1 = x(1 + s^2 + t^2) - (1 - s^2 - t^2) = 0,$$
$$y_2 = y(1 + s^2 + t^2) - 2s = 0,$$
$$y_3 = z(1 + s^2 + t^2) - 2t = 0.$$

We then pair together y_1, y_2 and y_2, y_3 and eliminate s to find:

$$4(t^2x^2 + 2t^2x + t^2 + 4x^2 + y^2 - 4) = 0$$
$$4(t^2y^2 + t^2z^2 - 2tz + z^2) = 0$$

We may remove the common factor of four and proceed to eliminate t, giving us

$$(x^2 + y^2 + z^2 - 1)(x^2y^4 + y^6 + y^4z^2 - 4xy^2z^2 + 4x^2z^2 - y^4 - 4y^2z^2 + 8xz^2 + 4z^2) = 0.$$

The first factor is the implicit representation of the unit sphere, hence, the second factor is extraneous.

However, Gröber bases do not generate extraneous factors. This is due to the presence of S-polynomials, which are essentially designed to produce the cancellation of leading terms, in combination with the division algorithm being utilized in Buchberger's Algorithm [13].

Example 4. *Returning to the parametrization of the unit sphere given above, let*

$$I = \langle x(1 + s^2 + t^2) - (1 - s^2 - t^2), y(1 + s^2 + t^2) - 2s, z(1 + s^2 + t^2) - 2t \rangle$$

where $I \subseteq \mathbb{R}[x, y, z, s, t]$. Then, using the lexicographical ordering $s > t > x > y > z$ and fixing the order of the polynomials in the ideal as given, the Gröbner basis of I is:

$$sz - ty,$$
$$tx + t - z,$$
$$ty^2 + tz^2 + xz - z,$$
$$x^2 + y^2 + z^2 - 1.$$

We recognize the last element as the implicit representation of the unit sphere with no extraneous factors.

Computational Complexity:

Sylvester resultants have the advantage that the corresponding determinants are easy to construct, however, these determinants can become quite large very quickly. This can result in Sylvester resultants taking an extremely long time or requiring a particularly large amount of memory to compute. On the other hand, the determinants of Bézout resultants can be as small as half the size of the equivalent Sylvester resultants' determinant. However, the division required to find the entries of this determinant can be costly, taking an immense amount of time or memory to compute.

Unfortunately, even with the best currently known versions of the algorithm, Gröbner bases can also take a tremendously long time or require an extremely large amount of memory to compute. There are several reasons for this, including that the intermediate polynomials that must be generated can have total degrees that are quite large as the algorithm proceeds: and that, even if the coefficients of the original ideal generators were small integers, the coefficients of the elements of a Gröbner basis can be complicated rational numbers.

Example 5. *Consider the ideal $I = \langle x^{n+1} - yz^{n-1}w, xy^{n-1} - z^n, x^n z - y^n w \rangle \subseteq \mathbb{R}[x, y, z, w]$. Using the lexicographical ordering $x > y > z > w$ and fixing the order of the polynomials in the ideal as given, it can be shown that the Gröbner basis of I contains the polynomial $z^{n^2+1} - y^{n^2}w$. This shows that the total degrees of the intermediate polynomials can be quite large for large values of n [5].*

Example 6. *Now consider the ideal*

$$J = \langle 3x^2 + 2yz - 2x, 2xz - 2yw, 2xy - 2z - 2zw, x^2 + y^2 + z^2 - 1 \rangle \subseteq \mathbb{R}[x, y, z, w].$$

Using the lexicographical ordering $w > x > y > z$ and fixing the order of the polynomials in the ideal as given, we find that the Gröbner basis of J is:

$$\begin{aligned}
&w - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 + \frac{36717}{590}z^4 - \frac{134419}{7670}z^2,\\
&x^2 + y^2 + z^2 - 1,\\
&xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z,\\
&xz + yz^2 - \frac{1152}{3835}z^5 - \frac{108}{295}z^3 + \frac{2556}{3835}z,\\
&y^3 + yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z,\\
&y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z,\\
&yz^3 - yz - \frac{576}{59} + \frac{1605}{118}z^4 - \frac{453}{118}z^2\\
&z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z.
\end{aligned}$$

This is an example of an ideal where the coefficients of the generators were small integers, but the coefficients of the elements of the Gröbner basis are relatively complicated rational numbers [5].

In conclusion, there are many applications where resultant methods are more efficient than Gröbner basis methods [4]. However, Gröbner bases are generally more efficient when there are many multivariate polynomials involved.

Chapter 3

Implicitization of Hypotrochoids and Epitrochoids

3.1 Implicitization Method

Theorem 17. *All trigonometric rational parametric representations of the form*

$$\begin{aligned} x_1 &= \frac{f_1(\sin(k_1\theta),\ldots,\sin(k_j\theta),\cos(k_1\theta),\ldots,\cos(k_j\theta),t_1,\ldots,t_m)}{g_1(\sin(k_1\theta),\ldots,\sin(k_j\theta),\cos(k_1\theta)\ldots,\cos(k_j\theta),t_1,\ldots,t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(\sin(k_1\theta),\ldots,\sin(k_j\theta),\cos(k_1\theta)\ldots,\cos(k_j\theta),t_1,\ldots,t_m)}{g_n(\sin(k_1\theta)\ldots,\sin(k_j\theta),\cos(k_1\theta)\ldots,\cos(k_j\theta),t_1,\ldots,t_m)}. \end{aligned} \tag{3.1}$$

can be expressed as a rational parametric representation of the form

$$\begin{aligned} x_1 &= \frac{f_1(z,t_1,\ldots,t_m)}{g_1(z,t_1,\ldots,t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(z,t_1,\ldots,t_m)}{g_n(z,t_1,\ldots,t_m)}. \end{aligned} \tag{3.2}$$

Proof. Recall that:

$$\cos(k\theta) = \frac{e^{-ik\theta}+e^{ik\theta}}{2}, \qquad \sin(k\theta) = \frac{ie^{-ik\theta}-ie^{ik\theta}}{2}.$$

Hence, we can replace every sine and cosine in $f_1,\ldots,f_n,g_1,\ldots,g_n$ with these alternate forms. We may view $k_1,\ldots,k_j$ as fractions with $l_1,\ldots,l_j$ as denominators. Let $\ell = lcm(l_1,\ldots,l_j)$, then we may then use the substitution $z = e^{i\theta/\ell}$ to obtain a rational parametric representation. □

We may use Theorem 17 with regards to roulettes, in particular, for epitrochoids and hypotrochoids.

Theorem 18. *Epitrochoids are rational parametric curves and, hence, have a representation that can be used for implicitization.*

Proof. Using equation (1.1) and Theorem 17, with $z = e^{i\theta/r}$, we obtain the following equation for epitrochoids:

$$x = \frac{(R+r)(z^r + z^{-r}) - d(z^{R+r} + z^{-(R+r)})}{2},$$
$$y = \frac{i(R+r)(z^r - z^{-r}) - id(z^{R+r} - z^{-(R+r)})}{2}.$$

As $R, r > 0$, we can multiply the right side by z^{R+r}/z^{R+r} in order to make all z powers positive:

$$x = \frac{(R+r)(z^{R+2r} + z^R) - d(z^{2R+2r} + 1)}{2z^{R+r}},$$
$$y = \frac{i(R+r)(z^{R+2r} - z^R) - id(z^{2R+2r} - 1)}{2z^{R+r}}.$$

Multiplying both sides by $2z^{R+r}$, and the second equation through by i, and then rearranging we obtain:

$$\begin{aligned} 0 &= dz^{2R+2r} - (R+r)z^{R+2r} + 2xz^{R+r} - (R+r)z^R + d, \\ 0 &= dz^{2R+2r} - (R+r)z^{R+2r} - 2iyz^{R+r} + (R+r)z^R - d. \end{aligned} \tag{3.3}$$

Therefore, for all epitrochoids, there is a rational parametric representation that can be used to implicitize the curve with Gröbner bases and resultant methods. □

Theorem 19. *Hypotrochoids are rational parametric curves and, hence, have a representation that can be used for implicitization.*

Proof. Using equation (1.4) and Theorem 17, with $z = e^{i\theta/r}$, we obtain the following equation for hypotrochoids:

$$x = \frac{(R-r)(z^r + z^{-r}) + d(z^{R-r} + z^{-(R-r)})}{2},$$
$$y = \frac{i(R-r)(z^r - z^{-r}) - id(z^{R-r} - z^{-(R-r)})}{2}.$$

Now multiply through by $2z^{R-r}$:

$$\begin{aligned} 2xz^{R-r} &= (R-r)z^R + (R-r)z^{R-2r} + dz^{2R-2r} + d, \\ 2yz^{R-r} &= (R-r)iz^R - (R-r)iz^{R-2r} - diz^{2R-2r} + di. \end{aligned} \tag{3.4}$$

Case 1. $k < 1$:

Note that $k < 1$ implies that $(R - r) < 0$. We begin by multiplying equation (3.4) through by $z^{-2(R-r)} = z^{2r-2R}$:

$$2xz^{r-R} = (R-r)z^{2r-R} + (R-r)z^{-R} + d + dz^{2r-2R},$$
$$2yz^{r-R} = (R-r)iz^{2r-R} - (R-r)iz^{-R} - di + diz^{2r-2R}.$$

Now multiply through by z^R to make all z powers positive:

$$2xz^r = (R-r)z^{2r} + (R-r) + dz^R + dz^{2r-R},$$
$$2yz^r = (R-r)iz^{2r} - (R-r)i - diz^R + diz^{2r-R}.$$

Lastly, rearranging and multiplying the second equation through by i we achieve a form that can be used with Gröbner bases and the Sylvester resultant:

$$0 = (R-r)z^{2r} - 2xz^r + dz^{2r-R} + dz^R + (R-r), \tag{3.5}$$
$$0 = (R-r)z^{2r} + 2iyz^r + dz^{2r-R} - dz^R - (R-r).$$

Case 2. $k = 1$:

For $k = 1$, equation (1.6) becomes

$$x(\theta) = d, \qquad y(\theta) = 0,$$

which produces the point $(d, 0)$.

Case 3. $1 < k < 2$:

Note that $k > 1$ implies that $(R - r) > 0$ and $k < 2$ that $(R - 2r) < 0$. Hence, the only negative power is $(R - 2r)$, so we begin by multiplying equation (3.4) through by z^{2r-R}:

$$2xz^r = (R-r)z^{2r} + (R-r) + dz^R + dz^{2r-R},$$
$$2yz^r = (R-r)iz^{2r} - (R-r)i - diz^R + diz^{2r-R}.$$

Rearranging, then multiplying the second equation through by i, we achieve the form:

$$0 = (R-r)z^{2r} + dz^R - 2xz^r + dz^{2r-R} + (R-r), \tag{3.6}$$
$$0 = (R-r)z^{2r} - dz^R + 2iyz^r + dz^{2r-R} - (R-r).$$

Note that $k < 1$ and $1 < k < 2$ result in the same form and that $k = 1$ shares this rational parametric representation. However, we will continue to separate these cases due to Theorem 20.

Case 4. $k = 2$:
Returning to equation (1.6), we obtain:

$$x(\theta) = (r + d)\cos\theta, \tag{3.7}$$
$$y(\theta) = (r - d)\sin\theta.$$

This is the parametric representation of an ellipse.

Case 5. $k > 2$:

Note that $k > 2$ implies that $(R - 2r) > 0$ and $(R - r) > 0$. Hence, all the powers of equation (3.4) are positive. Rearranging and multiplying the second equation through by i we obtain the form:

$$0 = dz^{2R-2r} + (R - r)z^R - 2xz^{R-r} + (R - r)z^{R-2r} + d, \tag{3.8}$$
$$0 = dz^{2R-2r} - (R - r)z^R - 2iyz^{R-r} + (R - r)z^{R-2r} - d.$$

Therefore, for all hypotrochoids, there is a rational parametric representation that can be used to implicitize the curve with Gröbner bases and resultant methods. □

Although the above differences in the number of cases for epitrochoids and hypotrochoids may seem odd, consider the following theorems:

Theorem 20. *If $k < 1$, then the hypotrochoid produced will be an epitrochoid.*

Proof. If $k < 1$, then the given hypotrochoid can be expressed in the following form:

$$x = \frac{d}{r}\left[(R - (R + r))\cos t + \frac{r(R + r)}{d}\cos\left(\frac{R - (R + r)}{R + r}t\right)\right],$$
$$y = \frac{d}{r}\left[(R - (R + r))\sin t - \frac{r(R + r)}{d}\sin\left(\frac{R - (R + r)}{R + r}t\right)\right].$$

Simplifying we obtain:

$$x = -d\cos t + (R + r)\cos\left(\frac{-r}{R + r}t\right),$$
$$y = -d\sin t - (R + r)\sin\left(\frac{-r}{R + r}t\right).$$

Recall that $\cos(-t) = \cos t$ and $\sin(-t) = -\sin t$. Applying this and rearranging the terms produce:

$$x = (R+r)\cos\left(\frac{r}{R+r}t\right) - d\cos t,$$
$$y = (R+r)\sin\left(\frac{r}{R+r}t\right) - d\sin t.$$

Lastly, let $t = r^{-1}(R+r)\theta$, giving us:

$$x = (R+r)\cos\theta - d\cos\left(\frac{R+r}{r}\theta\right),$$
$$y = (R+r)\sin\theta - d\sin\left(\frac{R+r}{r}\theta\right).$$

This is the equation of an epitrochoid as given in Definition 2. □

Theorem 21. *If $k_1 > 2$, then there exists k_2, where $1 < k_2 < 2$, such that k_2 produces the same hypotrochoid as k_1.*

Proof. Suppose the hypotrochoid produced by $k_1 > 2$ has the form:

$$x = (R-r)\cos\theta + d\cos\left(\frac{R-r}{r}\theta\right), \tag{3.9}$$
$$y = (R-r)\sin\theta - d\sin\left(\frac{R-r}{r}\theta\right).$$

Consider the following hypotrochoid:

$$x = \frac{d}{(R-(R-r))}\left[(R-(R-r))\cos t + \frac{r(R-r)}{d}\cos\left(\frac{R-(R-r)}{R-r}t\right)\right], \tag{3.10}$$
$$y = \frac{d}{(R-(R-r))}\left[(R-(R-r))\sin t - \frac{r(R-r)}{d}\sin\left(\frac{R-(R-r)}{R-r}t\right)\right].$$

This hypotrochoid has $k_2 = R/(R-r)$. Clearly, $k_2 > 1$ and since $k_1 = R/r > 2$, we have that $r < R/2$. Hence, $k_2 = R/(R-r) < R/(R-R/2) = 2$.

Simplifying equation (3.10) we obtain:

$$x = d\cos t + (R-r)\cos\left(\frac{r}{R-r}t\right),$$
$$y = d\sin t - (R-r)\sin\left(\frac{r}{R-r}t\right).$$

Let $t = -r^{-1}(R-r)\theta$, then:

$$x = d\cos\left(-\frac{R-r}{r}\theta\right) + (R-r)\cos(-\theta),$$
$$y = d\sin\left(-\frac{R-r}{r}\theta\right) - (R-r)\sin(-\theta).$$

Rearranging and using that $\cos(-\theta) = \cos\theta$ and $\sin(-\theta) = -\sin\theta$, we obtain:

$$x = (R-r)\cos(\theta) + d\cos\left(\frac{R-r}{r}\theta\right),$$
$$y = (R-r)\sin(\theta) - d\sin\left(\frac{R-r}{r}\theta\right).$$

Therefore, equation (3.10) with $1 < k_2 < 2$ produces the same hypotrochoid as described by equation (3.9) with $k_1 > 2$. □

3.2 Results for Small Values of m and n

In the following corollaries and conjectures, we will wish to distinguish between the values of the original radii and the values obtained from expressing $k \in \mathbb{Q}$ as an irreducible fraction. With this in mind, we will express the original radii as m and n where $m = cR$ and $n = cr$ with $gcd(R, r) = 1$.

Theorem 22. *The following parametric representation can be used to implicitize an epicycloid with Gröbner bases and resultants:*

$$0 = anz^{2m+2n} - a(m+n)z^{m+2n} + 2nxz^{m+n} - a(m+n)z^m + an, \tag{3.11}$$
$$0 = anz^{2m+2n} - a(m+n)z^{m+2n} - 2niyz^{m+n} + a(m+n)z^m - an.$$

Proof. Recall that an epicycloid is an epitrochoid for which $d = r$. Therefore, from the proof of Theorem 18, we have that,

$$0 = rz^{2R+2r} - (R+r)z^{R+2r} + 2xz^{R+r} - (R+r)z^R + r, \tag{3.12}$$
$$0 = rz^{2R+2r} - (R+r)z^{R+2r} - 2iyz^{R+r} + (R+r)z^R - r.$$

As the above parametric form was obtained from the radii, we now have

$$0 = nz^{2m+2n} - (m+n)z^{m+2n} + 2xz^{m+n} - (m+n)z^m + n, \tag{3.13}$$
$$0 = nz^{2m+2n} - (m+n)z^{m+2n} - 2iyz^{m+n} + (m+n)z^m - n.$$

Lastly, multiply these equations through by n and substitute $a = n$ in any coefficient that does not contain n. This will result in the desired form. □

Theorem 23. *The following parametric representation can be used to implicitize a hypocycloid with Gröbner bases and resultants:*
For $k < 1$:

$$0 = a(m-n)z^{2n} - 2nxz^n + anz^{2n-m} + anz^m + a(m-n), \tag{3.14}$$
$$0 = a(m-n)z^{2n} + 2niyz^n + anz^{2n-m} - anz^m - a(m-n).$$

For $1 < k < 2$:

$$0 = a(m-n)z^{2n} + anz^m - 2nxz^n + anz^{2n-m} + a(m-n), \tag{3.15}$$
$$0 = a(m-n)z^{2n} - anz^m + 2niyz^n + anz^{2n-m} - a(m-n).$$

For $k > 2$:

$$0 = anz^{2m-2n} + a(m-n)z^m - 2nxz^{m-n} + a(m-n)z^{m-2n} + an, \tag{3.16}$$
$$0 = anz^{2m-2n} - a(m-n)z^m - 2niyz^{m-n} + a(m-n)z^{m-2n} - an.$$

Recall that $k = 1$ and $k = 2$ produce a point and an ellipse, respectively. Hence, we will focus on the other values of k. Also, due to Theorem 20, we wish to separate $k < 1$ and $1 < k < 2$ despite the parametric representations above being identical.

Proof. Recall that a hypocycloid is an hypotrochoid for which $d = r$. Therefore, from the proof of Theorem 19, we have:
For $k < 1$:

$$0 = (R-r)z^{2r} - 2xz^r + rz^{2r-R} + rz^R + (R-r), \tag{3.17}$$
$$0 = (R-r)z^{2r} + 2iyz^r + rz^{2r-R} - rz^R - (R-r).$$

For $1 < k < 2$:

$$0 = (R-r)z^{2r} + rz^R - 2xz^r + rz^{2r-R} + (R-r), \tag{3.18}$$
$$0 = (R-r)z^{2r} - rz^R + 2iyz^r + rz^{2r-R} - (R-r).$$

For $k > 2$:

$$0 = rz^{2R-2r} + (R-r)z^R - 2xz^{R-r} + (R-r)z^{R-2r} + r, \tag{3.19}$$
$$0 = rz^{2R-2r} - (R-r)z^R - 2iyz^{R-r} + (R-r)z^{R-2r} - r.$$

From here we may follow the proof of Theorem 22 for each case. This will result in the desired forms. □

The following conjectures are a result of the data obtained using the forms from Theorem 22 and 23 (see Examples and Appendix).

Conjecture 2. *The implicit representation of an epicycloid where R is odd is of the form:*

$$F(x,y) = \sum_{i=0}^{R+r} p_{(2R+2r-2i)}(m,n)n^{2R+2r-2i}(x^2+y^2)^i + n^{R+2r}\sum_{i=0}^{(R-1)/2} p_{(R+2r,i)}(m,n)x^{R-2i}y^{2i} \tag{3.20}$$

where $p_{(j)}(m,n)$ and $p_{(R+2r,j)}(m,n)$ are polynomials in terms of m and n. Before we describe these polynomials, we require the following function:

$$G(n) = \begin{cases} n & \text{if } n \geq 0, \\ 0 & \text{if } n < 0. \end{cases}$$

If $R+2r < j \leq 2R+2r$, then $j = 2R-2r-2i$ for some $i \in \mathbb{Z}$ and

$$p_{(j)}(m,n) = m^{G(R-2i)}n^{2i}(m+2n)^{G(R-2i)}\sum_{h=0}^{2i}\alpha_h m^{2i-h}n^h.$$

For $0 \leq i \leq R/2$, the coefficient of $x^{R-2i}y^{2i}$ is

$$p_{(R+2r,i)}(m,n) = (-1)^{1+i}\binom{R}{2i}2n^{R-r}(m+n)^{R+r}.$$

If $\lfloor R/2+2r \rfloor_{2,1} \leq j < R+2r$, where $\lfloor \cdot \rfloor_{2,1}$ indicates to round to the closest even integer, then $j = 2R-2r-2i$ for some $i \in \mathbb{Z}$ and

$$p_{(j)}(m,n) = n^{G(2R-d)}\sum_{h=0}^{2+d}\beta_h m^{(2+d)-h}n^h.$$

where $d = j - \lfloor R/2+2r \rfloor_{2,1}$. If $0 \leq j < \lfloor R/2+2r \rfloor_{2,1}$, then $j = 2R-2r-2i$ for some $i \in \mathbb{Z}$ and

$$p_j(m,n) = (-1)^r n^{2R-j}\sum_{h=0}^{j}\gamma_h m^{j-h}n^h.$$

Conjecture 3. *The implicit representation of an epicycloid where R is even is of the form:*

$$F(x,y) = \sum_{\substack{i=0 \\ i\neq R/2}}^{R+r} p_{(2R+2r-2i)}(m,n)n^{2R+2r-2i}(x^2+y^2)^i + n^{R+2r}\sum_{i=0}^{R/2} p_{(R+2r,i)}(m,n)x^{R-2i}y^{2i} \tag{3.21}$$

where $p_{(j)}(m,n)$ and $p_{(R+2r,j)}(m,n)$ are polynomials in terms of m and n.

If $R+2r < j \le 2R+2r$, then $j = 2R+2r-2i$ for some $i \in \mathbb{Z}$ and

$$p_{(j)}(m,n) = m^{G(R-2i)}n^{2i}(m+2n)^{G(R-2i)}\sum_{h=0}^{2i}\alpha_h m^{2i-h}n^h$$

where G is the function defined above. For $0 \le i \le R/2$, the coefficient of $x^{R-2i}y^{2i}$ is

$$p_{(R+2r,i)}(m,n) = (-1)^{i+1}n^{R-r}\sum_{h=0}^{R+r}\beta_{h,i}m^{(R+r)-h}n^h.$$

If $\lfloor R/2+2r\rfloor_{2,2} \le j < R+2r$, where $\lfloor\cdot\rfloor_{2,2}$ indicates to round down to the closest even integer, then $j = 2R-2r-2i$ for some $i \in \mathbb{Z}$ and

$$p_{(j)}(m,n) = \sum_{h=0}^{i}\beta_h m^{i-h}n^h.$$

Lastly, if $0 \le j < \lfloor R/2+2r\rfloor_{2,2}$, then $j = 2R-2r-2i$ for some $i \in \mathbb{Z}$ and

$$p_j(m,n) = (-1)^{r+i}n^{2R-j}\sum_{h=0}^{j}\gamma_h m^{j-h}n^h.$$

Conjecture 4. *The implicit representation of a hypocycloid where R is odd and $k < 1$ is of the form:*

$$\begin{aligned} F(x,y) = &\sum_{i=0}^{r}p_{(2r-2i)}(m,n)n^{2r-2i}(x^2+y^2)^i \\ &+ n^{2r-R}\sum_{i=0}^{(R-1)/2}p_{(2r-R,i)}(m,n)x^{R-2i}y^{2i} \end{aligned} \tag{3.22}$$

where $p_{(j)}(m,n)$ and $p_{(2r-R,j)}(m,n)$ are polynomials in terms of m and n.

If $2r-R < j \le 2r$, then $j = 2r-2i$ for some $i \in \mathbb{Z}$ and

$$p_{(j)}(m,n) = (-1)^i m^{G(R-2i)}n^{2i}(m-n)^{2r-2R}(m-2n)^{G(R-2i)}\sum_{h=0}^{2i}\alpha_h m^{2i-h}n^h.$$

For $0 \le i \le (R-1)/2$, the coefficient of $x^{R-2i}y^{2i}$ is

$$p_{(2r-R,i)}(m,n) = (-1)^{i+1}\binom{R}{2i}2n^{R+r}(m-n)^{r-R}.$$

If $2R-r \le j < 2r-R$, then

$$p_{(j)}(m,n) = (-1)^{r+j/2}n^{2r-j}(m-n)^{2r-2R}\sum_{h=0}^{d}\beta_h m^{d-h}n^h.$$

where $d = 2 + j - (2R - r)$. *Lastly, if* $0 \le j < 2R - r$, *then* $j = 2r - 2i$ *for some* $i \in \mathbb{Z}$ *and*

$$p_{(j)}(m,n) = (-1)^{r+j} n^{2r-j} \sum_{h=0}^{j} \gamma_h m^{j-h} n^h.$$

Conjecture 5. *The implicit representation of a hypocycloid where* R *is odd and* $1 < k < 2$ *is of the form:*

$$\begin{aligned} F(x,y) = &\sum_{\substack{i=0 \\ i \neq (R-1)/2}}^{r} p_{(2r-2i)}(m,n) n^{2r-2i} (x^2+y^2)^i \\ &+ n^{2r-R} \sum_{i=0}^{(R-1)/2} p_{(2r-R,i)}(m,n) x^{R-2i} y^{2i} \end{aligned} \tag{3.23}$$

where $p_{(j)}(m,n)$ *and* $p_{(2r-R,i)}(m,n)$ *are polynomials in terms of* m *and* n.

If $2r - R < j \le 2r$, *then* $j = 2r - 2i$ *for some* $i \in \mathbb{Z}$ *and*

$$p_{(j)}(m,n) = (-1)^i m^{G(R-2i)} n^{2i} (m-2n)^{G(R-2i)} \sum_{h=0}^{2i} \alpha_h m^{2i-h} n^h.$$

For $0 \le i \le (R-1)/2$, *the coefficient of* $x^{R-2i} y^{2i}$ *is*

$$p_{(2r-R,i)}(m,n) = (-1)^i \binom{R}{2i} 2n^{R+r} (m-n)^{R-r}.$$

Lastly, if $0 \le j \le 2r - R$, *then* $j = 2r - 2i$ *for some* $i \in \mathbb{Z}$ *and*

$$p_{(j)}(m,n) = (-1)^{r+j/2} n^{2r-j} (m-n)^{2R-2r} \sum_{h=0}^{j} \beta_h m^{j-h} n^h.$$

Conjecture 6. *The implicit representation of a hypocycloid where* R *is odd and* $k > 2$ *is of the form:*

$$\begin{aligned} F(x,y) = &\sum_{i=0}^{R-r} p_{(2R-2r-2i)}(m,n) n^{2R-2r-2i} (x^2+y^2)^i \\ &+ n^{R-2r} \sum_{i=0}^{(R-1)/2} p_{(R-2r,i)}(m,n) x^{R-2i} y^{2i} \end{aligned} \tag{3.24}$$

where $p_{(j)}(m,n)$ *and* $p_{(R-2r,j)}(m,n)$ *are polynomials in terms of* m *and* n.

If $(2R - 4r - 2) < j \le 2R - 2r$, *then* $j = 2R - 2r - 2i$ *for some* $i \in \mathbb{Z}$ *and*

$$p_{(j)}(m,n) = (-1)^i m^{G(R-2i)} n^{2i} (m-2n)^{G(R-2i)} \sum_{h=0}^{2i} \alpha_h m^{2i-h} n^h.$$

If $R-2r < j \le (2R-4r-2)$*, then* $j = 2R-2r-2i$ *for some* $i \in \mathbb{Z}$ *and*

$$p_{(j)}(m,n) = (-1)^r m^{G(R-2i)} n^{G(2R-j)} (m-2n)^{G(R-2i)} \sum_{h=0}^{2+d} \beta_h m^{(2+d)-h} n^h.$$

where $d = (2R-4r-2) - j$*. For* $0 \le i \le (R-1)/2$*, the coefficient of* $x^{R-2i}y^{2i}$ *is*

$$p_{(R-2r,i)}(m,n) = (-1)^i \binom{R}{2i} 2n^{R+r} (m-n)^{R-r}.$$

Lastly, if $0 \le j \le R-2r$*, then* $j = 2R-2r-2i$ *for some* $i \in \mathbb{Z}$ *and*

$$p_{(j)}(m,n) = (-1)^r n^{2R-j} \sum_{h=0}^{j} \gamma_h m^{j-h} n^h.$$

Conjecture 7. *The implicit representation of a hypocycloid where* R *is even and* $k < 1$ *is of the form:*

$$\begin{aligned} F(x,y) = &\sum_{\substack{i=0 \\ i \neq R/2}}^{r} p_{(2r-2i)}(m,n) n^{2r-2i} (x^2+y^2)^i \\ &+ n^{2r-R} \sum_{i=0}^{R/2} p_{(2r-R,i)}(m,n) x^{R-2i} y^{2i} \end{aligned} \tag{3.25}$$

where $p_{(j)}(m,n)$ *and* $p_{(2r-R,j)}(m,n)$ *are polynomials in terms of* m *and* n*.*

If $2r-R < j \le 2r$*, then* $j = 2r-2i$ *for some* $i \in \mathbb{Z}$ *and*

$$p_{(j)}(m,n) = (-1)^i m^{G(R-2i)} n^{2i} (m-n)^{2r-2R} (m-2n)^{G(R-2i)} \sum_{h=0}^{2i} \alpha_h m^{2i-h} n^h.$$

For $0 \le i \le (R-1)/2$*, the coefficient of* $x^{R-2i}y^{2i}$ *is*

$$p_{(2r-R,i)}(m,n) = (-1)^{R/2} n^r (m-n)^{r-R} \sum_{h=0}^{r} \beta_{i,h} m^{r-h} n^h.$$

If $2r-2R+2 \le j < 2r-R$*, then*

$$p_{(j)}(m,n) = (-1)^{r+j/2} n^{2r-j} (m-n)^{2r-2R} \sum_{h=0}^{d} \gamma_h m^{d-h} n^h.$$

where $d = 2 + j - (2r-2R+2)$*. Lastly, if* $0 \le j < 2r-2R+2$*, then* $j = 2r-2i$ *for some* $i \in \mathbb{Z}$ *and*

$$p_{(j)}(m,n) = (-1)^{r+j} n^{2r-j} \sum_{h=0}^{j} \zeta_h m^{j-h} n^h.$$

Conjecture 8. *The implicit representation of a hypocycloid where R is even and $1 < k < 2$ is of the form:*

$$F(x,y) = \sum_{\substack{i=0 \\ i \neq R/2}}^{r} p_{(2r-2i)}(m,n) n^{2r-2i} (x^2+y^2)^i + n^{2r-R} \sum_{i=0}^{R/2} p_{(2r-R,i)}(m,n) x^{R-2i} y^{2i} \tag{3.26}$$

where $p_{(j)}(m,n)$ and $p_{(2r-R,i)}(m,n)$ are polynomials in terms of m and n.

If $2r - R < j \leq 2r$, then $j = 2r - 2i$ for some $i \in \mathbb{Z}$ and

$$p_{(j)}(m,n) = (-1)^i m^{G(R-2i)} n^{2i} (m-2n)^{G(R-2i)} \sum_{h=0}^{2i} \alpha_h m^{2i-h} n^h.$$

For $0 \leq i \leq (R-1)/2$, the coefficient of $x^{R-2i} y^{2i}$ is

$$p_{(2r-R,i)}(m,n) = (-1)^{R/2} n^r (m-n)^{R-r} \sum_{h=0}^{r} \beta_{i,h} m^{r-h} n^h.$$

Lastly, if $0 \leq j \leq 2r - R$, then $j = 2r - 2i$ for some $i \in \mathbb{Z}$ and

$$p_{(j)}(m,n) = (-1)^{r+j/2} n^{2r-j} (m-n)^{2R-2r} \sum_{h=0}^{j} \gamma_h m^{j-h} n^h.$$

Conjecture 9. *The implicit representation of a hypocycloid where R is even and $k > 2$ is of the form:*

$$F(x,y) = \sum_{\substack{i=0 \\ i \neq R/2}}^{R-r} p_{(2R-2r-2i)}(m,n) n^{2R-2r-2i} (x^2+y^2)^i + n^{R-2r} \sum_{i=0}^{R/2} p_{(R-2r,i)}(m,n) x^{R-2i} y^{2i} \tag{3.27}$$

where $p_{(j)}(m,n)$ and $p_{(R-2r,j)}(m,n)$ are polynomials in terms of m and n.

If $(2R - 4r - 2) < j \leq 2R - 2r$, then $j = 2R - 2r - 2i$ for some $i \in \mathbb{Z}$ and

$$p_{(j)}(m,n) = (-1)^i m^{G(R-2i)} n^{2i} (m-2n)^{G(R-2i)} \sum_{h=0}^{2i} \alpha_h m^{2i-h} n^h.$$

If $R - 2r < j \leq (2R - 4r - 2)$, then $j = 2R - 2r - 2i$ for some $i \in \mathbb{Z}$ and

$$p_{(j)}(m,n) = (-1)^r m^{G(R-2i)} n^{G(2R-j)} (m-2n)^{G(R-2i)} \sum_{h=0}^{2+d} \beta_h m^{(2+d)-h} n^h.$$

where $d = (2R - 4r - 2) - j$. *For* $0 \le i \le R/2$, *the coefficient of* $x^{R-2i}y^{2i}$ *is*

$$p_{(R-2r,i)}(m,n) = (-1)^i n^{R+r} \sum_{h=0}^{R-r} \gamma_{h,i} m^{(R-r)-h} n^h.$$

Lastly, if $0 \le j \le R - 2r$, *then* $j = 2R - 2r - 2i$ *for some* $i \in \mathbb{Z}$ *and*

$$p_{(j)}(m,n) = (-1)^r n^{2R-j} \sum_{h=0}^{j} \zeta_h m^{j-h} n^h.$$

Corollary 3. *Suppose we have an epicycloid (or hypocycloid) with* $k = R/r$ *where* $gcd(R,r) = 1$, *so that the parametric representation of the curve is*

$$\begin{aligned} x_1 &= r(k \pm 1)\cos\theta \mp r\cos((k \pm 1)\theta), \\ y_1 &= r(k \pm 1)\sin\theta - r\sin((k \pm 1)\theta). \end{aligned} \tag{3.28}$$

Now suppose that the implicit representation of this curve is

$$F_1(x_1, y_1) = \sum_{i,j,\kappa,\lambda} p_\lambda(R,r) r^i x_1^j y_1^\kappa = 0, \tag{3.29}$$

where $i + j + \kappa = 2R \pm 2r$ *and the* $p_\lambda(R,r)$ *are polynomials. If another epicycloid (or hypocycloid) has* $k = m/n$, $gcd(m,n) = c$, *and parametric representation*

$$\begin{aligned} x_2 &= n(k \pm 1)\cos\theta \mp n\cos((k \pm 1)\theta), \\ y_2 &= n(k \pm 1)\sin\theta - n\sin((k \pm 1)\theta), \end{aligned} \tag{3.30}$$

then an implicit representation of this curve is

$$F_2(x_2, y_2) = \sum_{i,j,\kappa,\lambda} p_\lambda(m,n) n^i x_2^j y_2^\kappa. \tag{3.31}$$

Proof. Since the $gcd(m,n) = c$ we have that $cR = m$ and $cr = n$. Therefore,

$$\begin{aligned} x_2 &= c[r(k \pm 1)\cos\theta \mp r\cos((k \pm 1)\theta)] = cx_1, \\ y_2 &= c[r(k \pm 1)\sin\theta - r\sin((k \pm 1)\theta)] = cx_2. \end{aligned} \tag{3.32}$$

As can be seen from the data below, $p_\lambda(m,n) = c^{2R} p_\lambda(R,r)$. Therefore,

$$\begin{aligned} F_2(x_2, y_2) &= \sum_{i,j,\kappa,\lambda} p_\lambda(m,n) n^i x_2^j y_2^\kappa \\ &= \sum_{i,j,\kappa,\lambda} c^{2R} p_\lambda(R,r)(cr)^i (cx_1)^j (cy_1)^\kappa \\ &= \sum_{i,j,\kappa,\lambda} c^{2R} c^{2R\pm 2r} p_\lambda(R,r) r^i x_1^j y_1^\kappa \\ &= c^{4R\pm 2r} F_1(x_1, y_1) \\ &= 0, \end{aligned} \tag{3.33}$$

giving us that $F_2(x_2, y_2) = 0$ is an implicit representation, as desired. □

Therefore, from Corollary 3, if given the implicit representation of an epicycloid (or hypocycloid) with respect to radii R and r, where R/r is a reduced fraction, then we also have the implicit representation for all epicycloids (or hypocycloids) with the same value of k. Hence, to find the implicit representation with respect to particular generating circles of radii m and n, one may simply consider calculating the implicit representation with regards to R and r and make the appropriate substitutions afterwards.

3.3 Examples

Implicit forms have been computed for m and n varying from 1 to 10. The following sample of this data is presented to illustrate the above corollaries. It was obtained from *Maple* by using resultants and utilizing the forms from Theorem 22 and 23 where the values of m and n were specified only for the exponents (see Appendix).

Examples of Conjecture 2

Example 7. $m = 3,\ n = 1$

The corresponding alternate parametric equations are:

$$0 = anz^8 - a(m+n)z^5 + 2nxz^4 - a(m+n)z^3 + an,$$
$$0 = anz^8 - a(m+n)z^5 - 2inyz^4 + a(m+n)z^3 - an.$$

The implicit representation was found to be:

$$F(x,y) = p_8a^8 + p_6a^6(x^2+y^2) + a^5(p_{5,0}x^3 + p_{5,1}xy^2) + p_4a^4(x^2+y^2)^2 + p_2a^2(x^2+y^2)^3 + p_0(x^2+y^2)^4$$

where:

$p_8 = m^3(m+2n)^3$

$p_6 = mn^2(m-n)(m+2n)(m+3n)$

$p_{5,0} = -2n^2(m+n)^4$

$p_{5,1} = 6n^2(m+n)^4$

$p_4 = n^4(m^2+2mn-5n^2)$

$p_2 = n^4(m^2 + 2mn + 5n^2)$

$p_0 = -n^6$

Example 8. $m = 5,\ n = 2$

The corresponding alternate parametric equations are:

$$0 = anz^{14} - a(m+n)z^9 + 2nxz^7 - a(m+n)z^5 + an,$$
$$0 = anz^{14} - a(m+n)z^9 - 2niyz^7 + a(m+n)z^5 - an.$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{14}a^{14} + p_{12}a^{12}(x^2+y^2) + p_{10}a^{10}(x^2+y^2)^2 \\ & + a^9(p_{9,0}x^5 + p_{9,1}x^3y^2 + p_{9,2}xy^4) + p_8a^8(x^2+y^2)^3 \\ & + p_6a^6(x^2+y^2)^4 + p_4a^4(x^2+y^2)^5 + p_2a^2(x^2+y^2)^6 \\ & + p_0(x^2+y^2)^7 \end{aligned}$$

where:

$p_{14} = m^5(m+2n)^5$

$p_{12} = m^3n^2(m+2n)^3(2m^2+4mn-5n^2)$

$p_{10} = mn^4(m+2n)(3m^4+12m^3n-m^2n^2-26mn^3+5n^4)$

$p_{9,0} = -2n^3(m+n)^7$

$p_{9,1} = 20n^3(m+n)^7$

$p_{9,2} = -10n^3(m+n)^7$

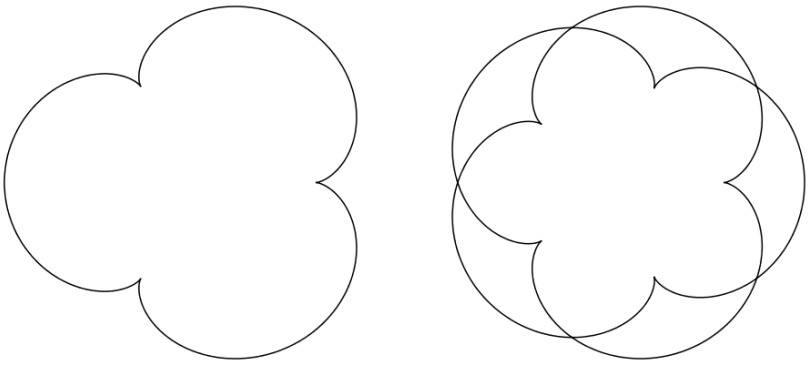
$p_8 = n^6(4m^4+16m^3n-6m^2n^2-44mn^3+9n^4)$

$p_6 = n^8(5m^2+10mn-30n^2)$

$p_4 = n^6(m^4+4m^3n+11m^2n^2+14mn^3+27n^4)$

$p_2 = -n^8(2m^2+4mn+9n^2)$

$p_0 = n^{10}$



(a) Example 7: $m = 3$, $n = 1$ (b) Example 8: $m = 5$, $n = 2$

Figure 3.1: Epicycloids with implicit forms described by Conjecture 2

Examples of Conjecture 3

Example 9. $m = 4$, $n = 3$

The corresponding alternate parametric equations are:

$$0 = anz^{14} - a(m+n)z^{10} + 2nxz^7 - a(m+n)z^4 + an,$$
$$0 = anz^{14} - a(m+n)z^{10} - 2inyz^7 + a(m+n)z^4 - an.$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{14}a^{14} + p_{12}a^{12}(x^2+y^2) + a^{10}(p_{10,0}x^4 + p_{10,1}x^2y^2 + p_{10,0}y^4) \\ & + p_8a^8(x^2+y^2)^3 + p_6a^6(x^2+y^2)^4 + p_4a^4(x^2+y^2)^5 \\ & + p_2a^2(x^2+y^2)^6 + p_0(x^2+y^2)^7 \end{aligned}$$

where:

$p_{14} = m^4(m+2n)^4$

$p_{12} = m^2n^2(m+2n)^2(3m^2+6mn-4n^2)$

$p_{10,0} = -n(2m^7+14m^6n+42m^5n^2+64m^4n^3+46m^3n^4+31m^2n^5+40mn^6)$

$p_{10,1} = n(12m^7+84m^6n+252m^5n^2+432m^4n^3+468m^3n^4+274m^2n^5+32mn^6+16n^7)$

$p_8 = n^6(10m^2+20mn-25n^2)$

$p_6 = n^2(m^6+6m^5n+19m^4n^2+36m^3n^3+49m^2n^4+42mn^5+50n^6)$

$p_4 = -n^4(3m^4+12m^3n+29m^2n^2+34mn^3+35n^4)$

$p_2 = n^6(3m^2+6mn+10n^2)$

$p_0 = -n^8$

Example 10. $m = 6,\ n = 1$

The corresponding alternate parametric equations are:

$$0 = anz^{14} - a(m+n)z^8 + 2nxz^7 - a(m+n)z^6 + an,$$
$$0 = anz^{14} - a(m+n)z^8 - 2inyz^7 + a(m+n)z^6 - an.$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{14}a^{14} + p_{12}a^{12}(x^2+y^2) + p_{10}a^{10}(x^2+y^2)^2 \\ & + a^8(p_{8,0}x^6 + p_{8,1}x^4y^2 + p_{8,2}x^2y^4 + p_{8,3}y^6) + p_6a^6(x^2+y^2)^4 \\ & + p_4a^4(x^2+y^2)^5 + p_2a^2(x^2+y^2)^6 + p_0(x^2+y^2)^7 \end{aligned}$$

where:

$p_{14} = m^6(m+2n)^6$

$p_{12} = m^4n^2(m+2n)^4(m^2+2mn-6n^2)$

$p_{10} = m^2n^4(m+2n)^2(m^4+4m^3n-7m^2n^2-22mn^3+9n^4)$

$p_{8,0} = -n^5(2m^7+13m^6n+36m^5n^2+73m^4n^3+122m^3n^4+85m^2n^5-20mn^6+4n^7)$

$p_{8,1} = n^5(30m^7+213m^6n+648m^5n^2+1041m^4n^3+894m^3n^4+501m^2n^5+312mn^6+24n^7)$

$p_{8,2} = -n^5(30m^7+207m^6n+612m^5n^2+1059m^4n^3+1206m^3n^4+759m^2n^5+108mn^6+36n^7)$

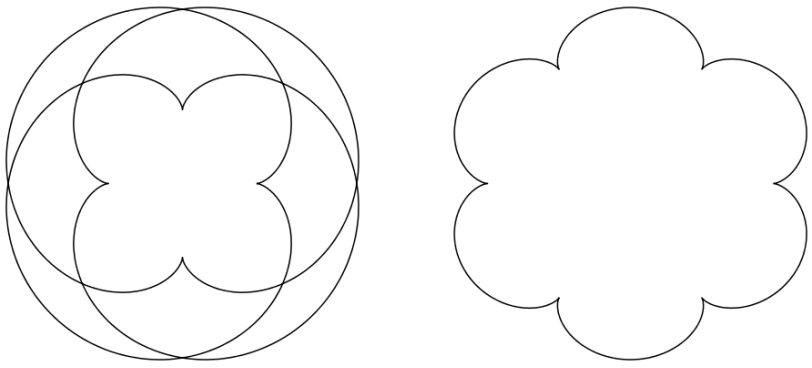
$p_{8,3} = n^5(2m^7+15m^6n+48m^5n^2+67m^4n^3+18m^3n^4-m^2n^5+48mn^6)$

$p_6 = n^8(m^4+4m^3n-14m^2n^2-36mn^3+16n^4)$

$p_4 = n^{10}(m^2+2mn-20n^2)$

$p_2 = n^{10}(m^2+2mn+8n^2)$

$p_0 = -n^{12}$



(a) Example 9: $m = 4,\ n = 3$ (b) Example 10: $m = 6,\ n = 1$

Figure 3.2: Epicycloids with implicit forms described by Conjecture 3

Examples of Conjecture 4

Example 11. $m = 1,\ n = 5\ (k < 1)$

The corresponding alternate parametric equations are:

$$0 = a(m-n)z^{10} - 2nxz^5 + anz^9 + anz + a(m-n),$$
$$0 = a(m-n)z^{10} + 2inyz^5 + anz^9 - anz - a(m-n).$$

The implicit representation was found to be:

$$F(x,y) = p_{10}a^{10} + p_{9,1}a^9x + p_8a^8(x^2+y^2) + p_6a^6(x^2+y^2)^2 + p_4a^4(x^2+y^2)^3 + p_2a^2(x^2+y^2)^4 + p_0(x^2+y^2)^5$$

where:

$p_{10} = m(m-2n)(m-n)^8$

$p_{9,1} = 2n^6(m-n)^4$

$p_8 = -n^2(5m^8 - 40m^7n + 141m^6n^2 - 286m^5n^3 + 366m^4n^4 - 304m^3n^5 + 162m^2n^6 - 52mn^7 + 9n^8)$

$p_6 = n^4(10m^6 - 60m^5n + 159m^4n^2 - 236m^3n^3 + 211m^2n^4 - 110mn^5 + 30n^6)$

$p_4 = -n^6(10m^4 - 40m^3n + 71m^2n^2 - 62mn^3 + 27n^4)$

$p_2 = n^8(5m^2 - 10mn + 9n^2)$

$p_0 = -n^{10}$

Example 12. $m = 5,\ n = 6\ (k < 1)$

The corresponding alternate parametric equations are:

$$0 = a(m-n)z^{12} - 2nxz^6 + anz^7 + anz^5 + a(m-n),$$
$$0 = a(m-n)z^{12} + 2inyz^6 + anz^7 - anz^5 - a(m-n).$$

The implicit representation was found to be:

$$F(x,y) = p_{12}a^{12} + p_{10}a^{10}(x^2+y^2) + p_8a^8(x^2+y^2)^2 + a^7(p_{7,0}x^5 + p_{7,1}x^3y^2 + p_{7,2}xy^4) + p_6a^6(x^2+y^2)^3 + p_4a^4(x^2+y^2)^4 + p_2a^2(x^2+y^2)^5 + p_0(x^2+y^2)^6$$

where:

$p_{12} = m^5(m-n)^2(m-2n)^5$

$p_{10} = -n^2m^3(m-n)^2(m-2n)^3(6m^2-12mn+5n^2)$

$p_8 = n^4m(m-n)^2(m-2n)(15m^4-60m^3n+79m^2n^2-38mn^3+5n^4)$

$p_{7,0} = -2n^{11}(m-n)$

$p_{7,1} = 20n^{11}(m-n)$

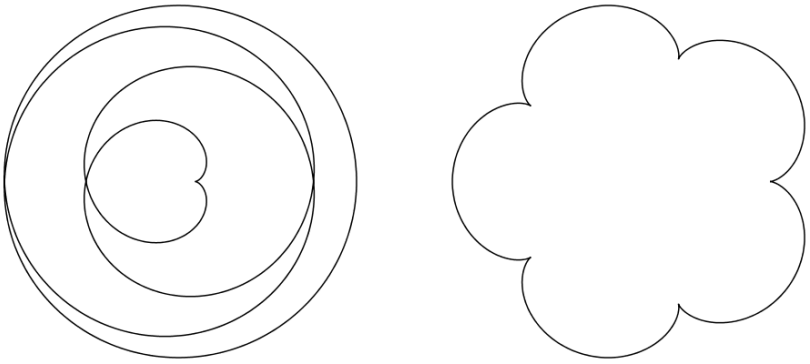
$p_{7,2} = -10n^{11}(m-n)$

$p_6 = -n^6(m-n)^2(20m^4-80m^3n+106m^2n^2-52mn^3+7n^4)$

$p_4 = n^8(m-n)^2(15m^2-30mn+14n^2)$

$p_2 = -n^{10}(6m^2-12mn+7n^2)$

$p_0 = n^{12}$



(a) Example 11: $m = 1$, $n = 5$ (b) Example 12: $m = 5$, $n = 6$

Figure 3.3: Hypocycloids with implicit forms described by Conjecture 4

Examples of Conjecture 5

Example 13. $m = 7$, $n = 5$ $(1 < k < 2)$

The corresponding alternate parametric equations are:

$$0 = a(m-n)z^{10} + anz^7 - 2nxz^5 + anz^3 + a(m-n),$$
$$0 = a(m-n)z^{10} - anz^7 + 2niyz^5 + anz^3 - a(m-n).$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{10}a^{10} + p_8a^8(x^2+y^2) + p_6a^6(x^2+y^2)^2 + p_4a^4(x^2+y^2)^3 \\ & + a^3(p_{3,1}x^7 + p_{3,2}x^5y^2 + p_{3,3}x^3y^4 + p_{3,4}xy^6) \\ & + p_2a^2(x^2+y^2)^4 + p_0(x^2+y^2)^5 \end{aligned}$$

where:

$p_{10} = m^7(m-2n)^7$

$p_8 = -m^5n^2(m-2n)^5(5m^2-10mn+7n^2)$

$p_6 = m^3n^4(m-2n)^3(10m^4-40m^3n+63m^2n^2-46mn^3+14n^4)$

$p_4 = -mn^6(m-2n)(10m^6-60m^5n+147m^4n^2-188m^3n^3+132m^2n^4-48mn^5+7n^6)$

$p_{3,1} = 2n^{12}(m-n)^2$

$p_{3,2} = -42n^{12}(m-n)^2$

$p_{3,3} = 70n^{12}(m-n)^2$

$p_{3,4} = -14n^{12}(m-n)^2$

$p_2 = n^8(m-n)^4(5m^2-10mn+3n^2)$

$p_0 = -n^{10}(m-n)^4$

Example 14. $m = 7,\ n = 6\ (1 < k < 2)$

The corresponding alternate parametric equations are:

$$0 = a(m-n)z^{12} + anz^7 - 2nxz^6 + anz^5 + a(m-n),$$
$$0 = a(m-n)z^{12} - anz^7 + 2niyz^6 + anz^5 - a(m-n).$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{12}a^{12} + p_{10}a^{10}(x^2+y^2) + p_8a^8(x^2+y^2)^2 + p_6a^6(x^2+y^2)^3 \\ & + a^5(p_{5,0}x^7 + p_{5,1}x^5y^2 + p_{5,2}x^3y^4 + p_{5,3}xy^6) + p_4a^4(x^2+y^2)^4 \\ & + p_2a^2(x^2+y^2)^5 + p_0(x^2+y^2)^6 \end{aligned}$$

where:

$p_{12} = m^7(m-2n)^7$

$p_{10} = -m^5n^2(m-2n)^5(6m^2-12mn+7n^2)$

$p_8 = m^3n^4(m-2n)^3(15m^4-60m^3n+89m^2n^2-58mn^3+14n^4)$

$p_6 = -mn^6(m-2n)(20m^6-120m^5n+286m^4n^2-344m^3n^3+217m^2n^4-66mn^5+7n^6)$

$p_{5,0} = -2n^{13}(m-n)$

$p_{5,1} = 42n^{13}(m-n)$

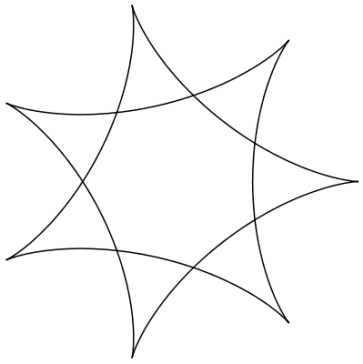
$p_{5,2} = -70n^{13}(m-n)$

$p_{5,3} = 14n^{13}(m-n)$

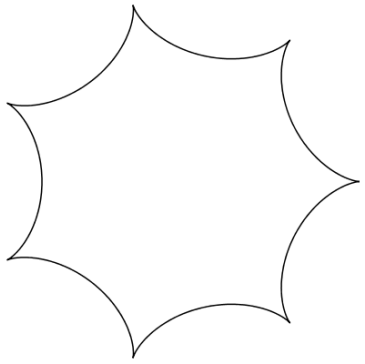
$p_4 = n^8(m-n)^2(15m^4-60m^3n+79m^2n^2-38mn^3+5n^4)$

$p_2 = -n^{10}(m-n)^2(6m^2 - 12mn + 5n^2)$

$p_0 = n^{12}(m-n)^2$



(a) Example 13: $m = 7$, $n = 5$



(b) Example 14: $m = 7$, $n = 6$

Figure 3.4: Hypocycloids with implicit forms described by Conjecture 5

Examples of Conjecture 6

Example 15. $m = 7$, $n = 1$ $(k > 2)$

The corresponding alternate parametric equations are:

$$0 = anz^{12} + a(m-n)z^7 - 2nxz^6 + a(m-n)z^5 + an,$$
$$0 = anz^{12} - a(m-n)z^7 - 2niyz^6 + a(m-n)z^5 - an.$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{12}a^{12} + p_{10}a^{10}(x^2+y^2) + p_8a^8(x^2+y^2)^2 + p_6a^6(x^2+y^2)^3 \\ & + a^5(p_{5,1}x^7 + p_{5,2}x^5y^2 + p_{5,3}x^3y^4 + p_{5,4}xy^6) + p_4a^4(x^2+y^2)^4 \\ & + p_2a^2(x^2+y^2)^5 + p_0(x^2+y^2)^6 \end{aligned}$$

where:

$p_{12} = m^7(m-2n)^7$

$p_{10} = -m^5n^2(m-2n)^5(m^2 - 2mn + 7n^n)$

$p_8 = -m^3n^6(m-2n)^3(m^2 - 2mn - 14n^2)$

$p_6 = -mn^8(m-2n)(m^4 - 4m^3n - 8m^2n^2 + 24mn^3 + 7n^4)$

$p_{5,1} = 2n^8(m-n)^6$

$p_{5,2} = -42n^8(m-n)^6$

$p_{5,3} = 70n^8(m-n)^6$

$p_{5,4} = -14n^8(m-n)^6$

$p_4 = -n^{10}(m^4 - 4m^3n - 5m^2n^2 + 18mn^3 + 5n^4)$

$p_2 = -n^{12}(m^2 - 2mn - 5n^2)$

$p_0 = -n^{14}$

Example 16. $m = 7,\ n = 2\ (k > 2)$

The corresponding alternate parametric equations are:

$$0 = anz^{10} + a(m-n)z^7 - 2nxz^5 + a(m-n)z^3 + an,$$
$$0 = anz^{10} - a(m-n)z^7 - 2niyz^5 + a(m-n)z^3 - an.$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{10}a^{10} + p_8a^8(x^2+y^2) + p_6a^6(x^2+y^2)^2 \\ & + p_4a^4(x^2+y^2)^3 + a^3(p_{3,0}x^7 + p_{3,1}x^5y^2 + p_{3,2}x^3y^4 + p_{3,3}xy^6) \\ & + p_2a^2(x^2+y^2)^4 + p_0(x^2+y^2)^5 \end{aligned}$$

where:

$p_{10} = m^7(m-2n)^7$

$p_8 = -m^5n^2(m-2n)^5(2m^2 - 4mn + 7n^2)$

$p_6 = m^3n^4(m-2n)^3(m^4 - 4m^3n + 9m^2n^2 - 10mn^3 + 14n^4)$

$p_4 = mn^{10}(m-2n)(3m^2 - 6mn - 7n^2)$

$p_{3,0} = -2n^9(m-n)^5$

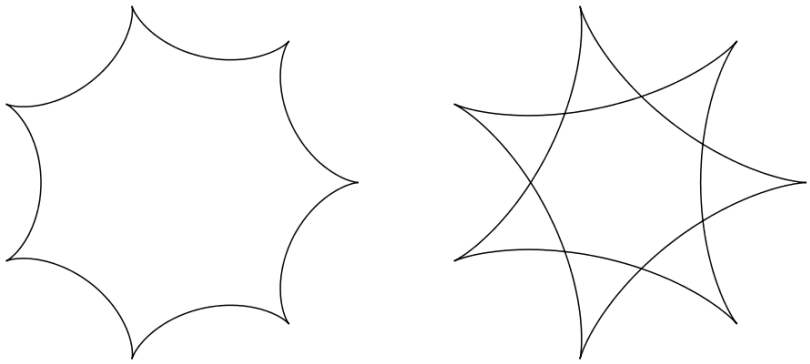
$p_{3,1} = 42n^9(m-n)^5$

$p_{3,2} = -70n^9(m-n)^5$

$p_{3,3} = 14n^9(m-n)^5$

$p_2 = n^{12}(2m^2 - 4mn - 3n^2)$

$p_0 = n^{14}$



(a) Example 15: $m = 7$, $n = 1$ (b) Example 16: $m = 7$, $n = 2$

Figure 3.5: Hypocycloids with implicit forms described by Conjecture 6

Examples of Conjecture 7

Example 17. $m = 4$, $n = 5$ $(k < 1)$

The corresponding alternate parametric equations are:

$$0 = a(m-n)z^{10} - 2nxz^5 + anz^6 + anz^4 + a(m-n),$$
$$0 = a(m-n)z^{10} + 2inyz^5 + anz^6 - anz^4 - a(m-n).$$

The implicit representation was found to be:

$$F(x,y) = p_{10}a^{10} + p_8a^8(x^2+y^2) + a^6(p_{6,0}x^4 + p_{6,1}x^2y^2 + p_{6,0}y^4) + p_4a^4(x^2+y^2)^3 + p_2a^2(x^2+y^2)^4 + p_0(x^2+y^2)^5$$

where:

$p_{10} = m^4(m-n)^2(m-2n)^4$

$p_8 = -n^2m^2(m-n)^2(m-2n)^2(5m^2-10mn+4n^2)$

$p_{6,0} = n^4(m-n)(10m^5-50m^4n+91m^3n^2-73m^2n^3+24mn^4)$

$p_{6,1} = n^4(m-n)(20m^5-100m^4n+182m^3n^2-146m^2n^3+48mn^4-16n^5)$

$p_4 = -n^6(m-n)^2(10m^2-20mn+9n^2)$

$p_2 = n^8(5m^2-10mn+6n^2)$

$p_0 = -n^{10}$

Example 18. $m = 4$, $n = 7$ $(k < 1)$

The corresponding alternate parametric equations are:

$$0 = a(m-n)z^{14} - 2nxz^7 + anz^{10} + anz^4 + a(m-n),$$
$$0 = a(m-n)z^{14} + 2niyz^7 + anz^{10} - anz^4 - a(m-n).$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{14}a^{14} + p_{12}a^{12}(x^2+y^2) + a^{10}(p_{10,0}x^4 + p_{10,1}x^2y^2 + p_{10,0}y^4) \\ & + p_8a^8(x^2+y^2)^3 + p_6a^6(x^2+y^2)^4 + p_4a^4(x^2+y^2)^5 \\ & + p_2a^2(x^2+y^2)^6 + p_0(x^2+y^2)^7 \end{aligned}$$

where:

$p_{14} = m^4(m-2n)^4(m-n)^6$

$p_{12} = -m^2n^2(m-2n)^2(m-n)^6(7m^2-14mn+4n^2)$

$p_{10,0} = n^4(m-n)^3(21m^7-147m^6n+416m^5n^2-610m^4n^3+491m^3n^4-209m^2n^5+40mn^6)$

$p_{10,1} = n^4(m-n)^3(42m^7-294m^6n+832m^5n^2-1220m^4n^3+982m^3n^4-418m^2n^5+80mn^6 - 16n^7)$

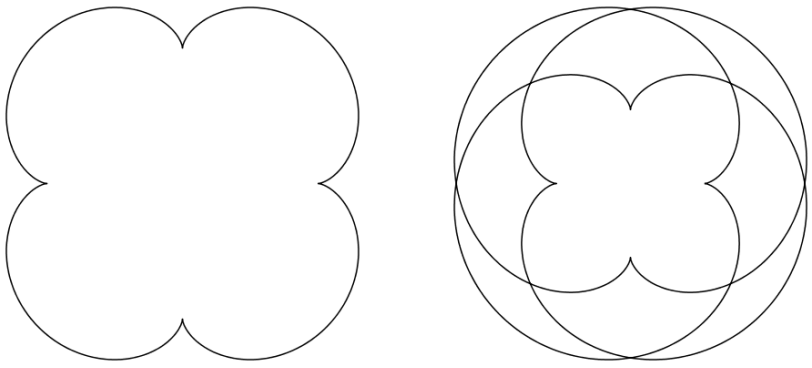
$p_8 = -n^6(m-n)^6(35m^2-70mn+25n^2)$

$p_6 = n^8(35m^6-210m^5n+535m^4n^2-740m^3n^3+589m^2n^4-258mn^5+50n^6)$

$p_4 = -n^{10}(21m^4-84m^3n+137m^2n^2-106mn^3+35n^4)$

$p_2 = n^{12}(7m^2-14mn+10n^2)$

$p_0 = -n^{14}$



(a) Example 17: $m = 4$, $n = 5$ (b) Example 18: $m = 4$, $n = 7$

Figure 3.6: Hypocycloids with implicit forms described by Conjecture 7

Examples of Conjecture 8

Example 19. $m = 6,\ n = 5\ (1 < k < 2)$

The corresponding alternate parametric equations are:

$$0 = a(m-n)z^{10} + anz^6 - 2nxz^5 + anz^4 + a(m-n),$$
$$0 = a(m-n)z^{10} - anz^6 + 2niyz^5 + anz^4 - a(m-n).$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{10}a^{10} + p_8a^8(x^2+y^2) + p_6a^6(x^2+y^2)^2 \\ & + a^4(p_{4,0}x^6 + p_{4,1}x^4y^2 + p_{4,2}x^2y^4 + p_{4,3}y^6) \\ & + p_2a^2(x^2+y^2)^4 + p_0(x^2+y^2)^5 \end{aligned}$$

where:

$p_{10} = m^6(m-2n)^6$

$p_8 = -m^4n^2(m-2n)^4(5m^2-10mn+6n^2)$

$p_6 = m^2n^4(m-2n)^2(10m^4-40m^3n+59m^2n^2-38mn^3+9n^4)$

$p_{4,0} = -n^6(m-n)(10m^5-50m^4n+91m^3n^2-73m^2n^3+24mn^4-4n^5)$

$p_{4,1} = -n^6(m-n)(30m^5-150m^4n+273m^3n^2-219m^2n^3+72mn^4+24n^5)$

$p_{4,2} = -n^6(m-n)(30m^5-150m^4n+273m^3n^2-219m^2n^3+72mn^4-36n^5)$

$p_{4,3} = -n^6(m-n)(10m^5-50m^4n+91m^3n^2-73m^2n^3+24mn^4)$

$p_2 = n^8(m-n)^2(5m^2-10mn+4n^2)$

$p_0 = -n^{10}(m-n)^2$

Example 20. $m = 8,\ n = 5\ (1 < k < 2)$

The corresponding alternate parametric equations are:

$$0 = a(m-n)z^{10} + anz^8 - 2nxz^5 + anz^2 + a(m-n),$$
$$0 = a(m-n)z^{10} - anz^8 + 2inyz^5 + anz^2 - a(m-n).$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{10}a^{10} + p_8a^8(x^2+y^2) + p_6a^6(x^2+y^2)^2 + p_4a^4(x^2+y^2)^3 \\ & + a^2(p_{2,0}x^8 + p_{2,1}x^6y^2 + p_{2,2}x^4y^4 + p_{2,1}x^2y^6 + p_{2,0}y^8) \\ & + p_0(x^2+y^2)^5 \end{aligned}$$

where:

$p_{10} = m^8(m-2n)^8$

$p_8 = -m^6n^2(m-2n)^6(5m^2-10mn+8n^2)$

$p_6 = m^4n^4(m-2n)^4(10m^4-40m^3n+67m^2n^2-54mn^3+20n^4)$

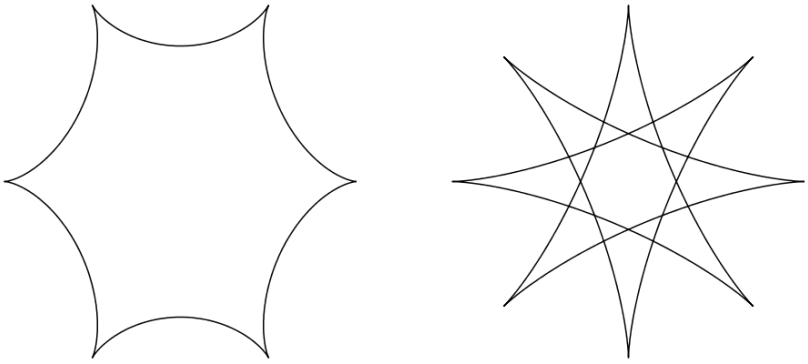
$p_4 = -m^2n^6(m-2n)^2(10m^6-60m^5n+153m^4n^2-212m^3n^3+170m^2n^4-76mn^5+16n^6)$

$p_{2,1} = n^8(m-n)^3(5m^5-25m^4n+47m^3n^2-41m^2n^3+16mn^4)$

$p_{2,2} = n^8(m-n)^3(20m^5-100m^4n+188m^3n^2-164m^2n^3+64mn^4-64n^5)$

$p_{2,3} = n^8(m-n)^3(30m^5-150m^4n+282m^3n^2-246m^2n^3+96mn^4+128n^5)$

$p_0 = -n^{10}(m-n)^6$



(a) Example 19: $m = 6$, $n = 5$ (b) Example 20: $m = 8$, $n = 5$

Figure 3.7: Hypocycloids with implicit forms described by Conjecture 8

Examples of Conjecture 9

Example 21. $m = 8$, $n = 1$ $(k > 2)$

The corresponding alternate parametric equations are:

$$0 = anz^{14} + a(m-n)z^8 - 2nxz^7 + a(m-n)z^6 + an,$$
$$0 = anz^{14} - a(m-n)z^8 - 2inyz^7 + a(m-n)z^6 - an.$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{14}a^{14} + p_{12}a^{12}(x^2+y^2) + p_{10}a^{10}(x^2+y^2)^2 + p_8a^8(x^2+y^2)^3 \\ & + a^6(p_{6,0}x^8 + p_{6,1}x^6y^2 + p_{6,2}x^4y^4 + p_{6,1}x^2y^6 + p_{6,0}y^8) \\ & + p_4a^4(x^2+y^2)^5 + p_2a^2(x^2+y^2)^6 + p_0(x^2+y^2)^7 \end{aligned}$$

where:

$p_{14} = m^8(m-2n)^8$

$p_{12} = -m^6n^2(m-2n)^6(m^2-2mn+8n^2)$

$p_{10} = -m^4n^6(m-2n)^4(m^2-2mn-20n^2)$

$p_8 = -m^2n^8(m-2n)^2(m^4-4m^3n-14m^2n^2+36mn^3+16n^4)$

$p_{6,0} = n^9(2m^7-15m^6n+48m^5n^2-67m^4n^3+18m^3n^4+m^2n^5+48mn^6)$

$p_{6,1} = -n^9(56m^7-388m^6n+1152m^5n^2-1972m^4n^3+2168m^3n^4-1348m^2n^5+256mn^6 - 64n^7)$

$p_{6,2} = n^9(140m^7-986m^6n+2976m^5n^2-4882m^4n^3+4588m^3n^4-2682m^2n^5+1184mn^6 - 128n^7)$

$p_4 = -n^{12}(m^4-4m^3n-7m^2n^2+22mn^3+9n^4)$

$p_2 = -n^{14}(m^2-2mn-6n^2)$

$p_0 = -n^{16}$

Example 22. $m = 8,\ n = 3\ (k > 2)$

The corresponding alternate parametric equations are:

$$0 = anz^{10} + a(m-n)z^8 - 2nxz^5 + a(m-n)z^2 + an,$$
$$0 = anz^{10} - a(m-n)z^8 - 2inyz^5 + a(m-n)z^2 - an.$$

The implicit representation was found to be:

$$\begin{aligned} F(x,y) = {} & p_{10}a^{10} + p_8a^8(x^2+y^2) + p_6a^6(x^2+y^2)^2 + p_4a^4(x^2+y^2)^3 \\ & + a^2(p_{2,0}x^8 + p_{2,1}x^6y^2 + p_{2,2}x^4y^4 + p_{2,1}x^2y^6 + p_{2,0}y^8) \\ & + p_0(x^2+y^2)^5 \end{aligned}$$

where:

$p_{10} = m^8(m-2n)^8$

$p_8 = -m^6n^2(m-2n)^6(3m^2-6mn+8n^2)$

$p_6 = m^4n^4(m-2n)^4(3m^4-12m^3n+25m^2n^2-26mn^3+20n^4)$

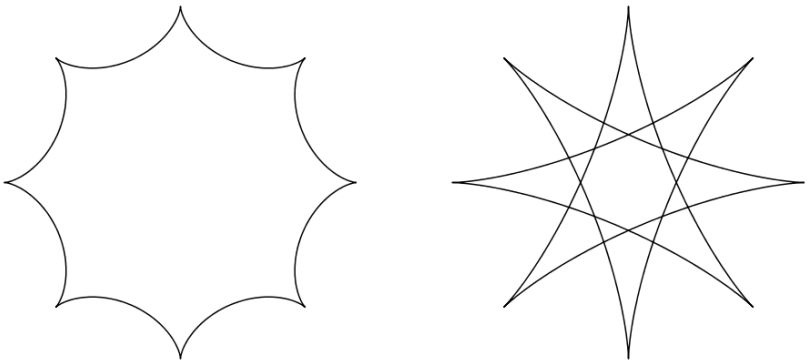
$p_4 = -m^2n^6(m-2n)^2(m^6-6m^5n+17m^4n^2-28m^3n^3+30m^2n^4-20mn^5+16n^6)$

$p_{2,0} = n^{11}(2m^5-10m^4n+20m^3n^2-23m^2n^3+16mn^4)$

$p_{2,1} = -n^{11}(56m^5-280m^4n+560m^3n^2-548m^2n^3+256mn^4-64n^5)$

$p_{2,2} = n^{11}(140m^5-700m^4n+1400m^3n^2-1418m^2n^3+736mn^4-128n^5)$

$p_0 = -n^{16}$



(a) Example 21: $m = 8$, $n = 1$ (b) Example 22: $m = 8$, $n = 3$

Figure 3.8: Hypocycloids with implicit forms described by Conjecture 9

Chapter 4

Envelopes

4.1 Introduction

Suppose we have a family of curves, such as a series of circles or lines. The envelope of this family is a curve that is tangent to all of the curves in this family [5].

Example 23. *Consider a family of circles of radius* 1 *centered on the* x*-axis in the Cartesian plane. The envelope visibly consists of the lines* $y = \pm 1$*, since both lines are tangent to every circle (fig. 4.1) [3].*

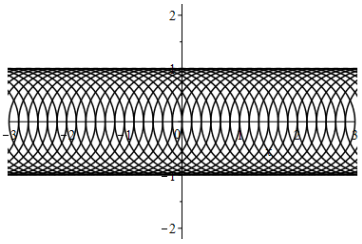


Figure 4.1: Family of circles centered on x-axis

To formalize the idea of an envelope, we begin by formalizing the concept of a family of curves.

Definition 20. *Let* $F : \mathbb{R} \times \mathbb{R}^r \to \mathbb{R}$ *be a smooth map. Express the coordinates on the left as* $(t, x_1, \ldots, x_r)$*; we view* F *as a family of functions of* x*, parametrized by* t*. Denote* $F_t : \mathbb{R}^r \to \mathbb{R}$ *for the functions* $F_t(x) = F(t, x)$*. Then the* ***family of curves*** *is determined by* F *and consists of* $V(F_t)$*, the varieties of* F_t *as* t *varies over* $\mathbb{R}$ *[3, 5].*

We can now give the general definition of an envelope.

Definition 21. *The set*

$$\mathscr{D}_F = \{\mathbf{x} \in \mathbb{R}^r : \text{there exists } t \in \mathbb{R} \text{ such that } F(t, \mathbf{x}) = \partial F/\partial t(t, \mathbf{x}) = 0\} \tag{4.1}$$

is the ***envelope****, or* ***discriminant****, of the family* F *[3, 5].*

Since these equations involve $x_1, \ldots, x_r$, and t; to find the equation of the envelope we will need to eliminate t [5]. In general, this can be achieved by using the methods discussed in chapter 2.

4.2 Epicycloids

Theorem 24. *The envelope of the family of curves given by*

$$F(t,x) = x_1(\sin(mt) + \sin(nt)) - x_2(\cos(nt) + \cos(mt)) - \sin(t(m-n)) \tag{4.2}$$

where $m, n \in \mathbb{Z}_{>0}$ is an epicycloid with $k = (m-n)/n$.

Some examples are given in figure 4.4.

Proof. Let $nt = \theta$, then $m/n = \ell$, so that;

$$\tilde{F}(\theta,x) = x_1(\sin(\ell\theta) + \sin(\theta)) - x_2(\cos(\theta) + \cos(\ell\theta)) - \sin(\theta(\ell-1)).$$

From the conditions given by Definition 21, we wish to find all $x \in \mathbb{R}^2$ such that:

$$x_1(\sin(\ell\theta) + \sin(\theta)) - x_2(\cos(\theta) + \cos(\ell\theta)) - \sin(\theta(\ell-1)) = 0, \tag{4.3}$$

$$x_1(\ell\cos(\ell\theta) + \cos(\theta)) + x_2(\sin(\theta) + \ell\sin(\ell\theta)) - (\ell-1)\cos(\theta(\ell-1)) = 0. \tag{4.4}$$

From equation (4.3) we have

$$x_2 = \frac{x_1(\sin(\theta) + \sin(\ell\theta)) - \sin(\theta(\ell-1))}{\cos(\theta) + \cos(\ell\theta)}. \tag{4.5}$$

Substituting equation (4.5) into (4.4) and simplifying the trigonometric expressions involved, we eventually find:

$$x_1 = \frac{\ell\cos(\theta) - \cos(\ell\theta)}{\ell+1}. \tag{4.6}$$

Now, substituting equation (4.6) into (4.3) and simplifying we obtain:

$$x_2 = \frac{\ell\sin(\theta) - \sin(\ell\theta)}{\ell+1}. \tag{4.7}$$

Returning to our substitutions, namely $\ell = m/n$, we have that:

$$x_1 = \frac{m\cos(\theta) - n\cos(m\theta/n)}{m+n},$$
$$x_2 = \frac{m\sin(\theta) - n\sin(m\theta/n)}{m+n}.$$

To show that this is equivalent to an epicycloid with $k = (m-n)/n$, first apply a uniform scaling with a scaling factor of $m+n$ so that:

$$x_1 = m\cos(\theta) - n\cos(m\theta/n),$$
$$x_2 = m\sin(\theta) - n\sin(m\theta/n).$$

Lastly, let $R = (m-n)$ and $r = n$. Then we obtain:

$$x_1 = (R+r)\cos(\theta) - r\cos\left(\frac{R+r}{r}\theta\right),$$
$$x_2 = (R+r)\sin(\theta) - r\sin\left(\frac{R+r}{r}\theta\right).$$

This is the equation of an epicycloid from Definition 2 with $k = R/r = (m-n)/n$. □

Theorem 25. *The envelope of the family of curves given by*

$$F(t,x) = x_1(\sin(mt) - \sin(nt)) + x_2(\cos(nt) - \cos(mt)) - \sin(t(m-n)) \tag{4.8}$$

where $m, n \in \mathbb{Z}_{>0}$ with $m \neq n$ is an epicycloid with $k = (m-n)/n$.

Proof. Let $nt = \theta$, then $m/n = \ell$, so that;

$$\tilde{F}(\theta,x) = x_1(\sin(\ell\theta) - \sin(\theta)) + x_2(\cos(\theta) - \cos(\ell\theta)) - \sin(\theta(\ell-1)).$$

From the conditions given by Definition 21, we wish to find all $x \in \mathbb{R}^2$ such that:

$$x_1(\sin(\ell\theta) - \sin(\theta)) + x_2(\cos(\theta) - \cos(\ell\theta)) - \sin(\theta(\ell-1)) = 0, \tag{4.9}$$
$$x_1(\ell\cos(\ell\theta) - \cos(\theta)) + x_2(\ell\sin(\ell\theta) - \sin(\theta)) - (\ell-1)\cos(\theta(\ell-1)) = 0. \tag{4.10}$$

From equation (4.9) we have

$$x_2 = \frac{x_1(\sin(\theta) - \sin(\ell\theta)) - \sin(\theta(\ell-1))}{\cos(\theta) - \cos(\ell\theta)}. \tag{4.11}$$

Substituting equation (4.11) into (4.10) and simplifying the trigonometric expressions involved, we eventually find:

$$x_1 = \frac{\ell\cos(\theta) + \cos(\ell\theta)}{\ell+1}. \tag{4.12}$$

Now, substituting equation (4.12) into (4.9) and simplifying we obtain:

$$x_2 = \frac{\ell\sin(\theta) + \sin(\ell\theta)}{\ell+1}. \tag{4.13}$$

Returning to our substitutions, namely $\ell = m/n$, we have that:

$$x_1 = \frac{m\cos(\theta) + n\cos(\ell\theta)}{m+n}, \qquad (4.14)$$
$$x_2 = \frac{m\sin(\theta) + n\sin(\ell\theta)}{m+n}.$$

We claim that equation (4.14) produces an epicycloid with $k = (m-n)/n$. To see this, first apply a uniform scaling with a scaling factor of $m+n$ so that:

$$x_1 = m\cos(\theta) + n\cos(\ell\theta), \qquad (4.15)$$
$$x_2 = m\sin(\theta) + n\sin(\ell\theta).$$

Let $\alpha = n\pi/(m-n)$ and $\beta = \pi(3n-2m)/(m-n)$. Apply a rotation of β followed by the substitution $\theta = \varphi - \alpha$. After simplifying, we obtain:

$$x_1 = m\cos(\varphi - (\alpha-\beta)) + n\cos(\ell\varphi - (\ell\alpha - \beta)), \qquad (4.16)$$
$$x_2 = m\sin(\varphi - (\alpha-\beta)) + n\sin(\ell\varphi - (\ell\alpha - \beta)).$$

Note that $\alpha - \beta = 2\pi$ and $\ell\alpha - \beta = 3\pi$. Hence,

$$x_1 = m\cos(\varphi) - n\cos(\ell\varphi), \qquad (4.17)$$
$$x_2 = m\sin(\varphi) - n\sin(\ell\varphi).$$

Lastly, let $R = (m-n)$ and $r = n$. Then we obtain:

$$x_1 = (R+r)\cos(\varphi) - r\cos\left(\frac{R+r}{r}\varphi\right),$$
$$x_2 = (R+r)\sin(\varphi) - r\sin\left(\frac{R+r}{r}\varphi\right).$$

This is the equation of an epicycloid from Definition 2 with $k = R/r = (m-n)/n$. □

As mentioned in the introduction of this chapter, envelopes are produced by a family of curves; hence, one may wonder what family of curves is being described in Theorem 24 or Theorem 25.

With regards to Theorem 24, we begin by considering the family of functions that determined the envelope given by:

$$F(t,x) = x_1(\sin(mt) + \sin(nt)) - x_2(\cos(nt) + \cos(mt)) - \sin(t(m-n)) = 0. \qquad (4.18)$$

Let $c = -\sin(t(m-n))$ and note that

$$(\cos(nt) + \cos(mt))\sin(nt) = (\sin(nt) + \sin(mt))\cos(nt) + c. \tag{4.19}$$

Hence, dividing through by $\cos(nt) + \cos(mt)$,

$$\sin(nt) = \left(\frac{\sin(nt) + \sin(mt)}{\cos(nt) + \cos(mt)}\right)\cos(nt) + b \tag{4.20}$$

where, of course,

$$b = \frac{c}{\cos(nt) + \cos(mt)}. \tag{4.21}$$

One may recognize that equation (4.20) as the slope-intercept form of a straight line for which the slope is $(\sin(nt) + \sin(mt))/(\cos(nt) + \cos(mt))$ and the line passes through the point $(\cos(nt), \sin(nt))$ in Cartesian coordinates. Since the slope of a straight line can be determined from any two (distinct) points that the line passes through, we may we use this to determine the other point; which we find to be $(-\cos(mt), -\sin(mt))$.

Lastly, from the above, we have that equation (4.20) can also be written as

$$x_2 = \left(\frac{\sin(nt) + \sin(mt)}{\cos(nt) + \cos(mt)}\right)x_1 + \frac{-\sin(t(m-n))}{\cos(nt) + \cos(mt)}. \tag{4.22}$$

This is equivalent to the defining equation given in Theorem 24. Therefore, the family of curves is a series of lines which pass through the points $(\cos(nt), \sin(nt))$ and $(-\cos(mt), -\sin(mt))$.

Through a similar analysis, we find that the family of curves described in Theorem 25 is a series of lines which pass through the points $(\cos(nt), \sin(nt))$ and $(\cos(mt), \sin(mt))$.

Figure 4.3 illustrates the construction of an envelope for an epicycloid with $n = 4$ and $m = 9$ as produced by Theorem 24. Figure 4.2 is the completed envelope. Only the integer values of t are shown as t varies from 0 to 360 degrees. The color of the lines that produce the envelope transition as t varies.[1]

Figure 4.4 illustrates the envelopes produced by Theorem 24. The first row illustrates the progression of the family of lines as t varies, the second emphasizes the curve that is tangent to all of the curves in this family (the envelope), and the final row consists of the corresponding epicycloids as produced by their parametric equations. The envelopes produced by Theorem 25 are similar.

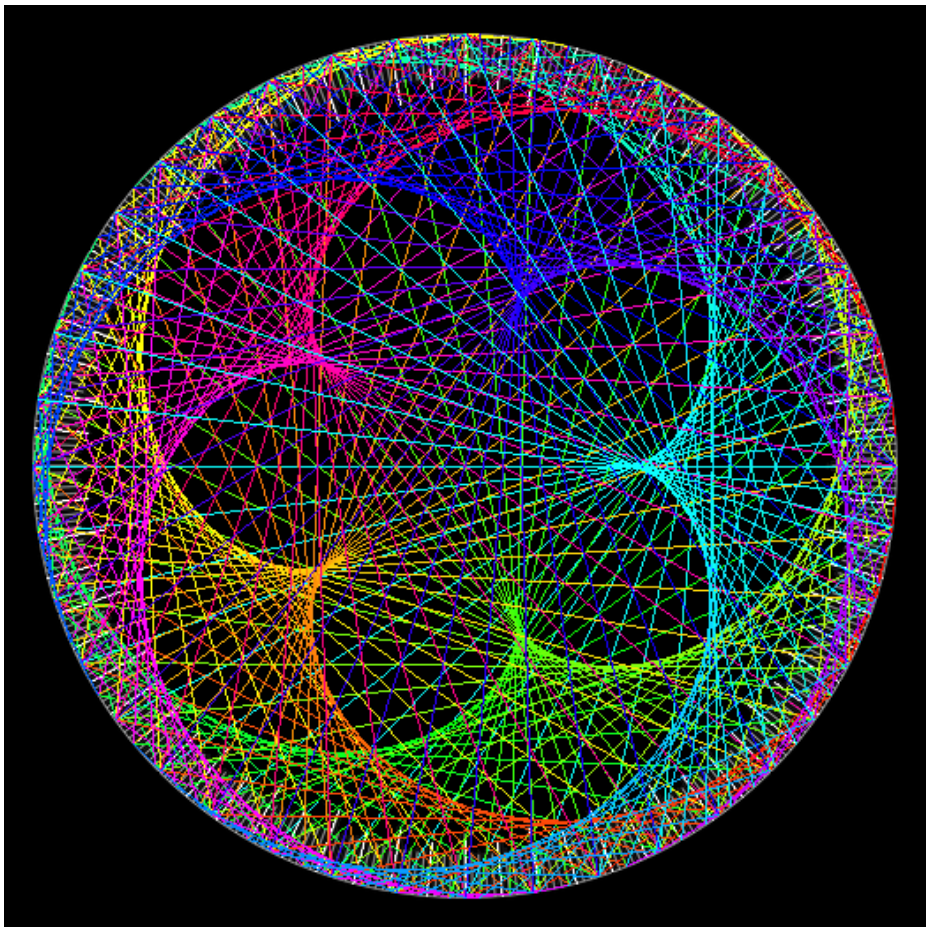
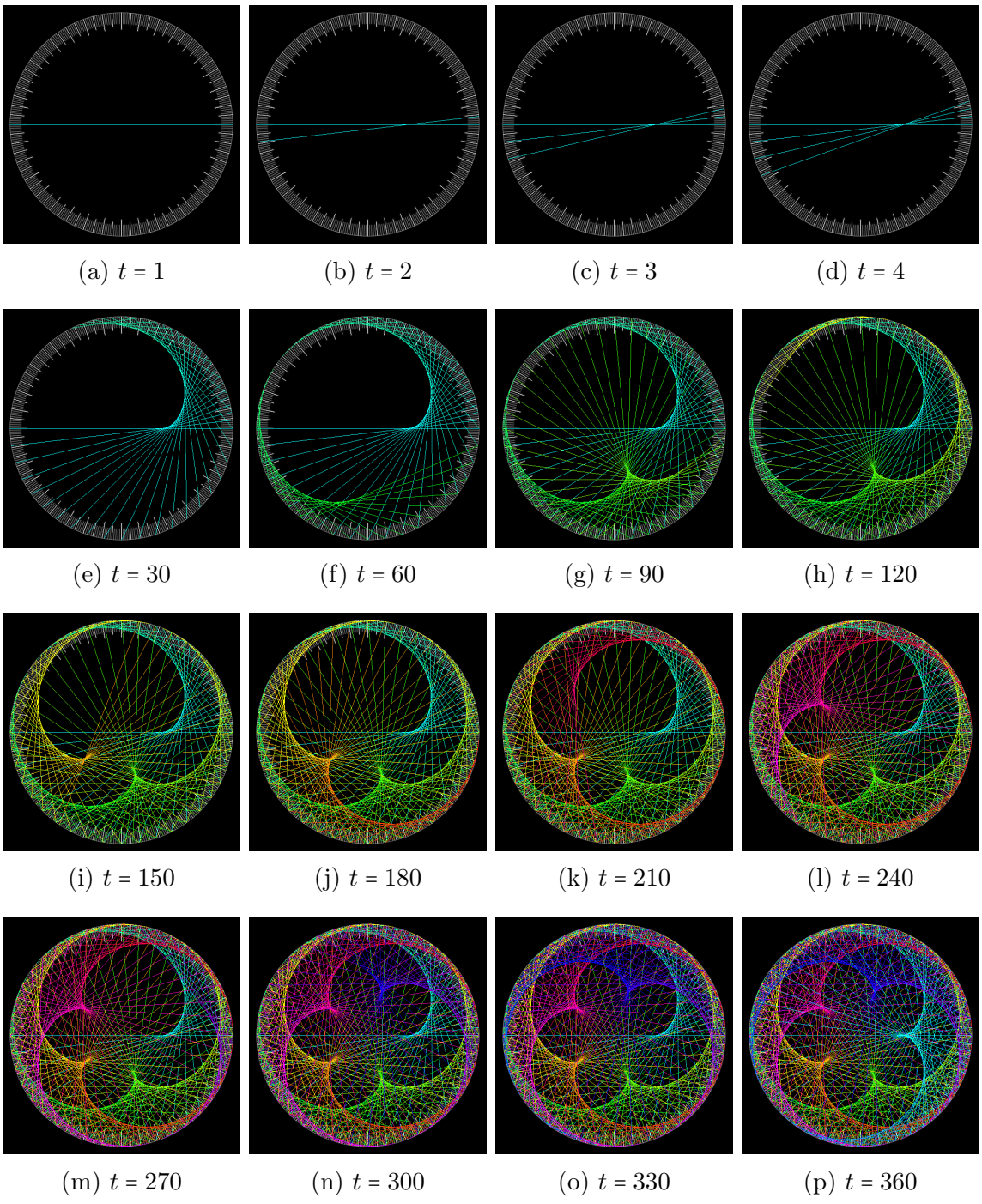


Figure 4.2: Epicycloid envelope for $m = 9$, $n = 4$

[1]For an animation of this process, please visit
`https://www.youtube.com/playlist?list=PLfD1Gv_NLdCx9ANJy9gamy5b6etzBAwvp`.



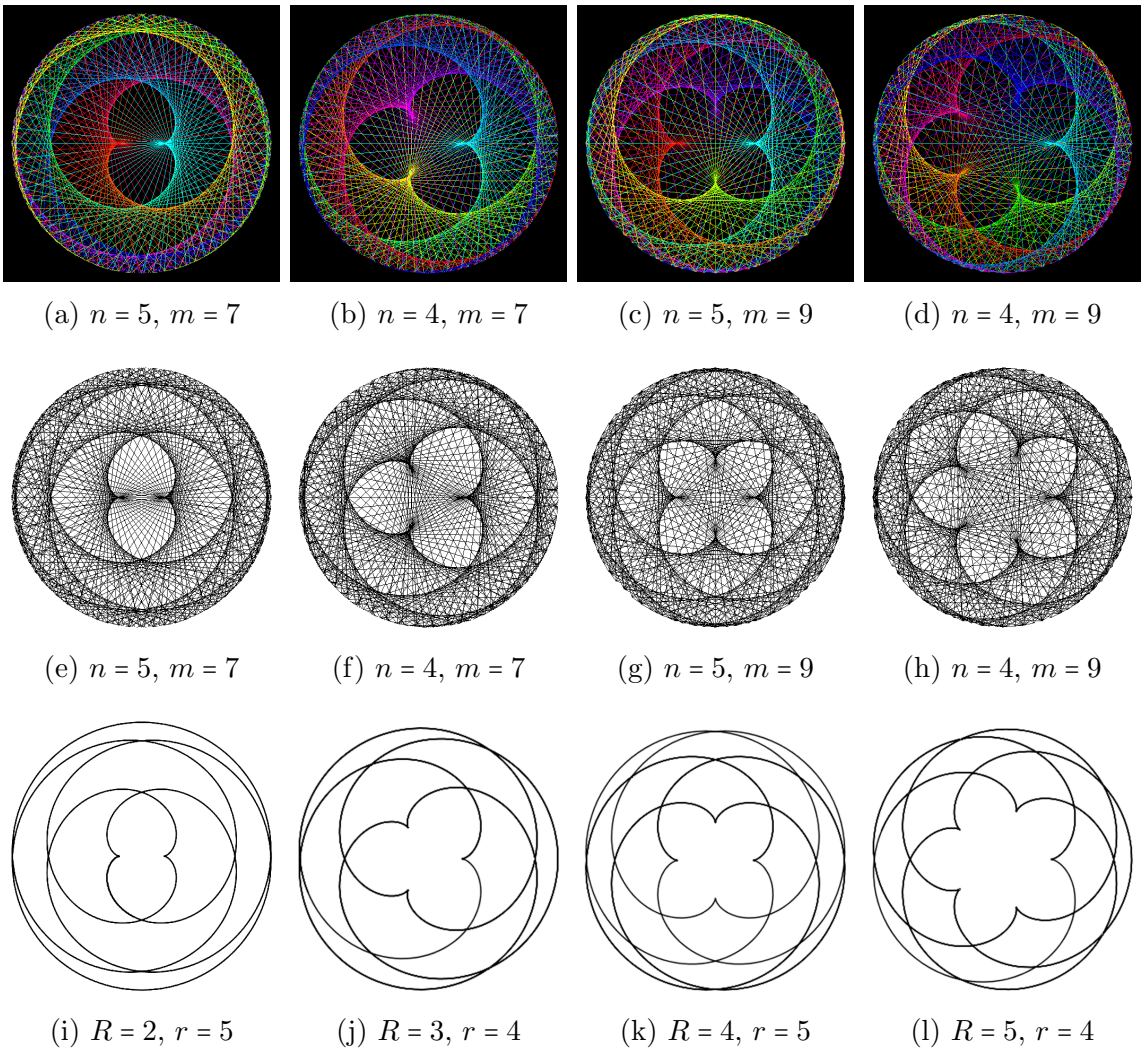
(a) $t = 1$ (b) $t = 2$ (c) $t = 3$ (d) $t = 4$

(e) $t = 30$ (f) $t = 60$ (g) $t = 90$ (h) $t = 120$

(i) $t = 150$ (j) $t = 180$ (k) $t = 210$ (l) $t = 240$

(m) $t = 270$ (n) $t = 300$ (o) $t = 330$ (p) $t = 360$

Figure 4.3: Epicycloid envelope construction for $m = 9$, $n = 4$



(a) $n = 5$, $m = 7$ (b) $n = 4$, $m = 7$ (c) $n = 5$, $m = 9$ (d) $n = 4$, $m = 9$

(e) $n = 5$, $m = 7$ (f) $n = 4$, $m = 7$ (g) $n = 5$, $m = 9$ (h) $n = 4$, $m = 9$

(i) $R = 2$, $r = 5$ (j) $R = 3$, $r = 4$ (k) $R = 4$, $r = 5$ (l) $R = 5$, $r = 4$

Figure 4.4: Envelopes with their respective epicycloids

4.3 Hypocycloids

Theorem 26. *The envelope of the family of curves given by*

$$F(t,x) = x_1(\sin(nt) - \sin(mt)) - x_2(\cos(mt) + \cos(nt)) + \sin(t(m+n)) \tag{4.23}$$

where $m, n \in \mathbb{Z}_{>0}$ with $m \neq n$ is a hypocycloid with $k = (m+n)/n$.

Some examples are given in figure 4.7.

Proof. Let $nt = \theta$, then $m/n = \ell$, so that;

$$\tilde{F}(\theta,x) = x_1(\sin(\theta) - \sin(\ell\theta)) - x_2(\cos(\ell\theta) + \cos(\theta)) + \sin(\theta(\ell+1)).$$

From the conditions given by Definition 21, we wish to find all $x \in \mathbb{R}^2$ such that:

$$x_1(\sin(\theta) - \sin(\ell\theta)) - x_2(\cos(\ell\theta) + \cos(\theta)) + \sin(\theta(\ell+1)) = 0, \tag{4.24}$$

$$x_1(\cos(\theta) - \ell\cos(\ell\theta)) + x_2(\sin(\theta) + \ell\sin(\ell\theta)) + (\ell+1)\cos(\theta(\ell+1)) = 0. \tag{4.25}$$

From equation (4.24) we have

$$x_2 = \frac{x_1(\sin(\theta) - \sin(\ell\theta)) + \sin(\theta(\ell+1))}{\cos(\theta) + \cos(\ell\theta)}. \tag{4.26}$$

Substituting equation (4.26) into (4.25) and simplifying the trigonometric expressions involved, we eventually find:

$$x_1 = \frac{\ell\cos(\theta) + \cos(\ell\theta)}{\ell - 1}. \tag{4.27}$$

Now, substituting equation (4.27) into (4.24) and simplifying we obtain:

$$x_2 = \frac{\ell\sin(\theta) - \sin(\ell\theta)}{\ell - 1}. \tag{4.28}$$

Returning to our substitutions, namely $\ell = m/n$, we have that:

$$x_1 = \frac{m\cos(\theta) + n\cos(m\theta/n)}{m-n},$$
$$x_2 = \frac{m\sin(\theta) - n\sin(m\theta/n)}{m-n}.$$

To show that this is equivalent to a hypocycloid with $k = (m+n)/n$; first apply a uniform scaling with a scaling factor of $m-n$ so that:

$$x_1 = m\cos(\theta) + n\cos\left(m\theta/n\right),$$
$$x_2 = m\sin(\theta) - n\sin\left(m\theta/n\right).$$

Lastly, let $R = (m+n)$ and $r = n$. Then we obtain:

$$x_1 = (R-r)\cos(\theta) + r\cos\left(\frac{R-r}{r}\theta\right),$$
$$x_2 = (R-r)\sin(\theta) - r\sin\left(\frac{R-r}{r}\theta\right).$$

This is the equation of a hypocycloid from Definition 3 with $k = R/r = (m+n)/n$. □

Theorem 27. *The envelope of the family of curves given by*

$$F(t,x) = x_1(\sin(nt) + \sin(mt)) + x_2(\cos(mt) - \cos(nt)) - \sin(t(m+n)) \tag{4.29}$$

where $m, n \in \mathbb{Z}_{>0}$ with $m \neq n$ is a hypocycloid with $k = (m+n)/n$.

Proof. Let $nt = \theta$, then $m/n = \ell$, so that;

$$\tilde{F}(\theta,x) = x_1(\sin(\theta) + \sin(\ell\theta)) + x_2(\cos(\ell\theta) - \cos(\theta)) - \sin(\theta(\ell+1)).$$

From the conditions given by Definition 21, we wish to find all $x \in \mathbb{R}^2$ such that:

$$x_1(\sin(\theta) + \sin(\ell\theta)) + x_2(\cos(\ell\theta) - \cos(\theta)) - \sin(\theta(\ell+1)) = 0, \tag{4.30}$$
$$x_1(\cos(\theta) + \ell\cos(\ell\theta)) + x_2(\sin(\theta) - \ell\sin(\ell\theta)) - (\ell+1)\cos(\theta(\ell+1)) = 0. \tag{4.31}$$

From equation (4.30) we have

$$x_2 = \frac{x_1(\sin(\theta) + \sin(\ell\theta)) - \sin(\theta(\ell+1))}{\cos(\theta) - \cos(\ell\theta)}. \tag{4.32}$$

Substituting equation (4.32) into (4.31) and simplifying the trigonometric expressions involved, we eventually find:

$$x_1 = \frac{\ell\cos(\theta) - \cos(\ell\theta)}{\ell - 1}. \tag{4.33}$$

Now, substituting equation (4.33) into (4.30) and simplifying we obtain:

$$x_2 = \frac{\ell\sin(\theta) + \sin(\ell\theta)}{\ell - 1}. \tag{4.34}$$

Returning to our substitutions, namely $\ell = m/n$, we have that:

$$\begin{aligned} x_1 &= \frac{m\cos(\theta) - n\cos(\ell\theta)}{m-n}, \\ x_2 &= \frac{m\sin(\theta) + n\sin(\ell\theta)}{m-n}. \end{aligned} \tag{4.35}$$

We claim that equation (4.35) produces a hypocycloid with $k = (m+n)/n$. To see this, first apply a uniform scaling with a scaling factor of $m-n$ so that:

$$\begin{aligned} x_1 &= m\cos(\theta) - n\cos(\ell\theta), \\ x_2 &= m\sin(\theta) + n\sin(\ell\theta). \end{aligned}$$

Let $\alpha = n\pi/(m+n)$ and $\beta = \pi(3n+2m)/(m+n)$. Apply a rotation of β followed by the substitution $\theta = \varphi - \alpha$. After simplifying, we obtain:

$$\begin{aligned} x_1 &= m\cos(\varphi - (\alpha - \beta)) - n\cos(\ell\varphi - (\ell\alpha + \beta)), \\ x_2 &= m\sin(\varphi - (\alpha - \beta)) + n\sin(\ell\varphi - (\ell\alpha + \beta)). \end{aligned}$$

Note that $\alpha - \beta = -2\pi$ and $\ell\alpha + \beta = 3\pi$. Hence,

$$\begin{aligned} x_1 &= m\cos(\varphi) + n\cos(\ell\varphi), \\ x_2 &= m\sin(\varphi) - n\sin(\ell\varphi). \end{aligned}$$

Lastly, let $R = (m+n)$ and $r = n$. Then we obtain:

$$\begin{aligned} x_1 &= (R-r)\cos(\theta) + r\cos\left(\frac{R-r}{r}\theta\right), \\ x_2 &= (R-r)\sin(\theta) - r\sin\left(\frac{R-r}{r}\theta\right). \end{aligned}$$

This is the equation of a hypocycloid from Definition 3 with $k = R/r = (m+n)/n$. □

As mentioned in the introduction of this chapter, envelopes are produced by a family of curves; hence, one may wonder what family of curves are being described in Theorem 26 or Theorem 27.

For Theorem 27, we begin by considering the family of functions that determined the envelope:

$$F(t,x) = x_1(\sin(nt) + \sin(mt)) + x_2(\cos(mt) - \cos(nt)) - \sin(t(m+n)) = 0. \tag{4.36}$$

Let $c = -\sin(t(m+n))$ and note that,

$$(\cos(nt) - \cos(mt))\sin(nt) = (\sin(nt) + \sin(mt))\cos(nt) + c. \tag{4.37}$$

Hence, dividing through by $\cos(nt) - \cos(mt)$,

$$\sin(nt) = \left(\frac{\sin(nt) + \sin(mt)}{\cos(nt) - \cos(mt)}\right)\cos(nt) + b \tag{4.38}$$

where, of course,

$$b = \frac{c}{\cos(nt) - \cos(mt)}. \tag{4.39}$$

One may recognize equation (4.38) as the slope-intercept form of a straight line for which the slope is $(\sin(nt)+\sin(mt))/(\cos(nt)-\cos(mt))$ and the line passes through the point $(\cos(nt), \sin(nt))$ in Cartesian coordinates. Since the slope of a straight line can be determined from any two (distinct) points that the line passes through, we may we use this to determine the other point; which we find to be $(\cos(mt), -\sin(mt))$.

Lastly, from the above, we have that equation (4.38) can also be written as

$$x_2 = \left(\frac{\sin(nt) + \sin(mt)}{\cos(nt) - \cos(mt)}\right)x_1 + \frac{-\sin(t(m+n))}{\cos(nt) - \cos(mt)}. \tag{4.40}$$

This is equivalent to the defining equation given in Theorem 27. Therefore, the family of curves is a series of lines which pass through the points $(\cos(nt), \sin(nt))$ and $(\cos(mt), -\sin(mt))$.

Through a similar analysis, we find that the family of curves described in Theorem 26 is a series of lines which pass through the points $(\cos(nt), \sin(nt))$ and $(-\cos(mt), \sin(mt))$.

Figure 4.6 illustrates the construction of an envelope for a hypocycloid with $m = 11$ and $n = 5$ as produced by Theorem 26. Figure 4.5 is the completed envelope. Only the integer values of t are shown as t varies from 0 to 360 degrees. The color of the lines that produce the envelope transition as t varies.[2]

Figure 4.7 illustrates the envelopes produced by Theorem 26. The first row illustrates the progression of the family of lines as t varies, the second emphasizes the curve that is tangent to all of the curves in this family (the envelope), and the final row consists of the corresponding hypocycloids as produced by their parametric equations. The envelopes produced by Theorem 27 are similar.

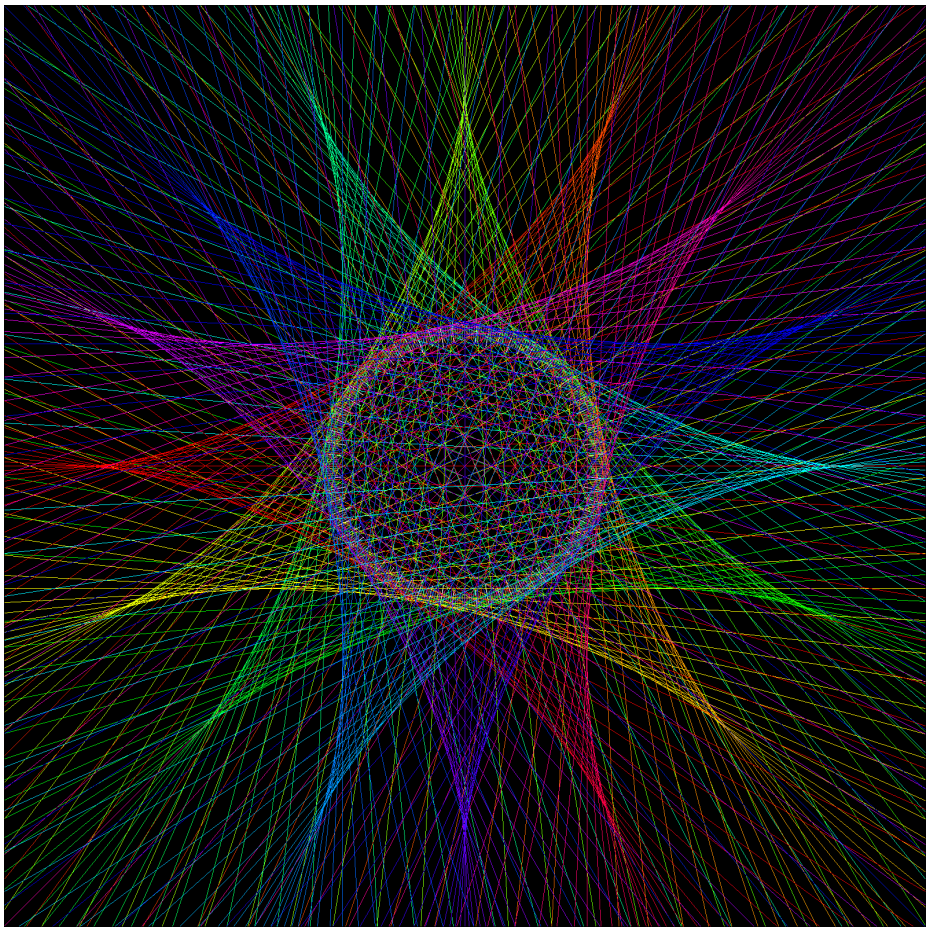
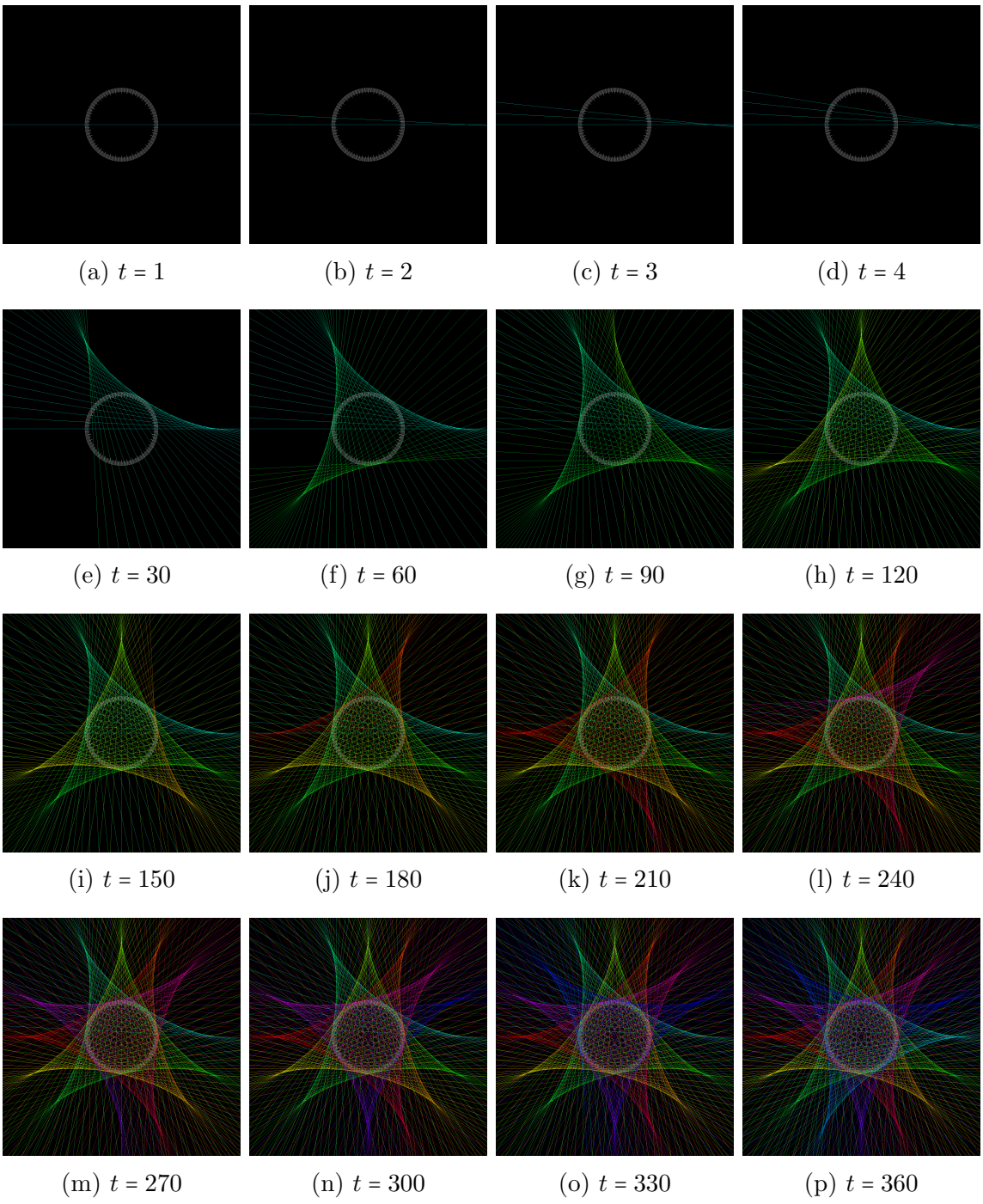


Figure 4.5: Hypocycloid envelope for $m = 11, n = 5$

[2]For an animation of this process, please visit
`https://www.youtube.com/playlist?list=PLfD1Gv_NLdCwRxn0svDr-baCKD7rHnU-i`.



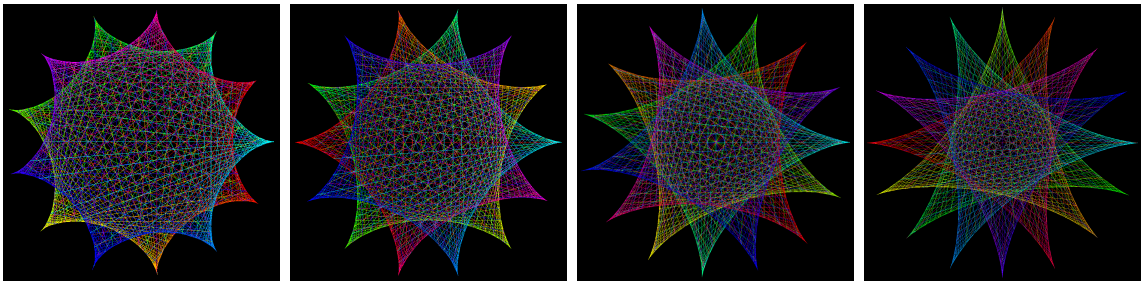
(a) $t = 1$ (b) $t = 2$ (c) $t = 3$ (d) $t = 4$

(e) $t = 30$ (f) $t = 60$ (g) $t = 90$ (h) $t = 120$

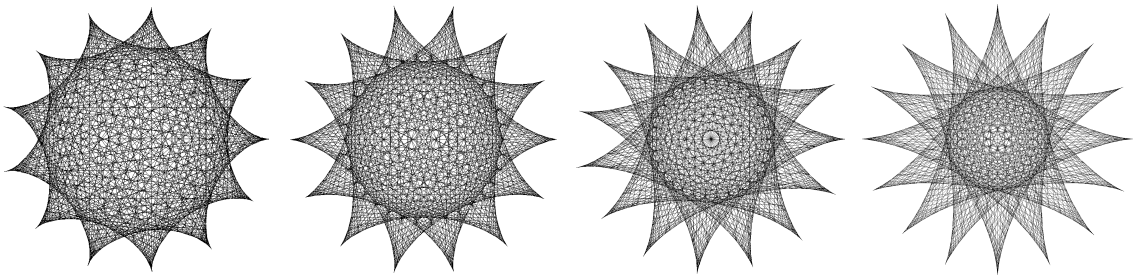
(i) $t = 150$ (j) $t = 180$ (k) $t = 210$ (l) $t = 240$

(m) $t = 270$ (n) $t = 300$ (o) $t = 330$ (p) $t = 360$

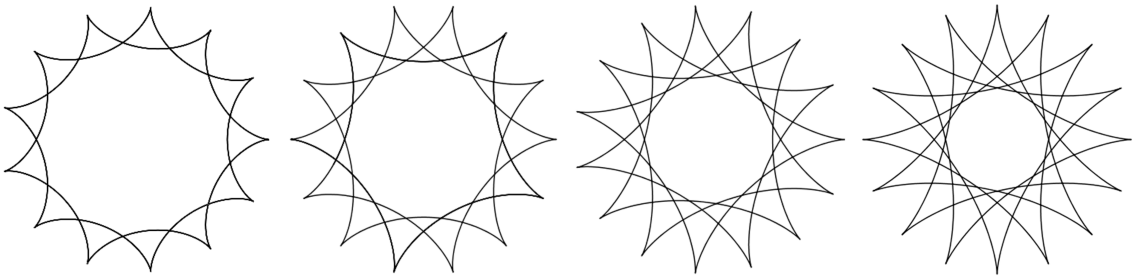
Figure 4.6: Hypocycloid envelope construction for $m = 11, n = 5$



(a) $n = 2$, $m = 11$ (b) $n = 3$, $m = 11$ (c) $n = 4$, $m = 11$ (d) $n = 5$, $m = 11$



(e) $n = 2$, $m = 11$ (f) $n = 3$, $m = 11$ (g) $n = 4$, $m = 11$ (h) $n = 5$, $m = 11$



(i) $R = 13$, $r = 2$ (j) $R = 14$, $r = 3$ (k) $R = 15$, $r = 4$ (l) $R = 16$, $r = 5$

Figure 4.7: Envelopes with their respective hypocycloids

Chapter 5

Conclusion

We began by examining two solutions to the implicitization problem; resultants and Gröbner bases. This included proving their algorithms for implicitization and comparing them with regards to their relationship, extraneous factors, and computational complexity.

We then presented the result that all trigonometric rational parametric equations can be expressed as rational parametric equations and applied this to epitrochoids and hypotrochoids. Through this application, we found equivalent representations of hypotrochoids and epitrochoids that can be used for implicitization.

With these results, we specified equivalent parametric forms for epicycloids and hypocycloids that will emphasize that the implicit forms appear to be homogeneous functions. From the data obtained by using these forms, we formulated several conjectures regarding the general implicit representations of epicycloids and hypocycloids. Lastly we showed, assuming that the implicit forms are homogeneous, that the implicit representation of a given epicycloid or hypocycloid may be obtained by finding the implicit form of the similar curve produced by circles with radii that have no common factors.

Lastly, we discussed envelopes and the construction of epicycloids and hypocycloids as envelopes. In particular, that all epicycloids and hypocycloids, for which k is rational, can be constructed as the envelope of a family of straight lines.

Bibliography

[1] E. Abbena, S. Salamon, and A. Gray. *Modern Differential Geometry of Curves and Surfaces with Mathematica*. CRC Press, Florida, United States of America, 3 edition, 2006.

[2] C. Bright. Ideals, varieties and algorithms talk 2. `https://cs.uwaterloo.ca/~cbright/reports/IVATalk2notes.pdf`. Accessed: 2018-02-08.

[3] J. W. Bruce and P. J. Giblin. *Curves and Singularities*. Cambridge University Press, New York, United States of America, 2 edition, 1992.

[4] D. A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer Science & Business Media, New York, United States of America, 2 edition, 2005.

[5] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer, Switzerland, 4 edition, 2015.

[6] M. Hazewinkel, editor. *Encyclopaedia of Mathematics*. Kluwer Academic Publishers, Dordrecht, Netherlands, 1989.

[7] C. M. Hoffmann. *Geometric and Solid Modeling*. Morgan Kaufmann, California, United States of America, 1989.

[8] F. Lemmermeyer. Parametrization of algebraic curves from a number theorist's point of view. *The American Mathematical Monthly*, 119:573–583, 9 2012.

[9] D. Manocha and J. Demmel. Algorithms for intersecting parametric and algebraic curves. *Graphics Interface*, pages 232–241, 1992.

[10] D. Nelson. *The Penguin Dictionary of Mathematics*. Penguin Books, London, England, 2 edition, 1998.

[11] R. Pinch. Epicycloid. `https://www.encyclopediaofmath.org//index.php?title=Epicycloid&oldid=42503`. Accessed: 2018-02-08.

[12] R. Pinch. Hypocycloid. `https://www.encyclopediaofmath.org//index.php?title=Hypocycloid&oldid=42491`. Accessed: 2018-02-08.

[13] J. R. Rice. *Mathematical Aspects of Scientific Software*. Springer Science & Business Media, New York, United States of America, 2012.

[14] T. W. Sederberg, D. C. Anderson, and R. N. Goldman. Implicit representation of parametric curves and surfaces. *Computer Vision, Graphics, and Image Processing*, 28:72–84, 10 1984.

[15] Y. Sun and J. Yu. *Artificial Intelligence and Symbolic Computation*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

Appendix

Maplecode 1: Epicycloid Resultant Coefficient Replacement

```
# This procedure will calculate the determinant
# of the Sylvester or Bézout matrix with the coefficients
# in terms of m and n, which determine our epicycloid.

with(LinearAlgebra):

# l corresponds to m, and k corresponds to n.
# Select the values of m and n.
# These values will determine the size of the matrix,
# and hence the amount of time required to obtain the result.

l := m;
k := n;

# The Fun and Dun procedures create the desired parametric equations
# where the powers are specified but the coefficients are not.

Fun := proc(l, k) local f1, f2:
   f1 := a·n·t^(2·m+2·n) − a·(m+m)·t^(m+2·n) + 2·n·n·x·t^(m+n) − a·(m+n)·t^m + a·n;
   f2 := a·n·t^(2·l+2·k) − a·(m+n)·t^(l+2·k) + 2·n·x·t^(l+k) − a·(m+n)·t^l + a·n;
   return f2;
end proc;

q := Fun(l, k);

Dun := proc(l, k) local g1, g2;
   g1 := a·n·t^(2·m+2·n) − a·(m+m)·t^(m+2·n) − 2·n·I·y·t^(m+n) + a·(m+n)·t^m − a·n;
   g2 := a·n·t^(2·l+2·k) − a·(m+n)·t^(l+2·k) − 2·n·I·y·t^(l+k) + a·(m+n)·t^l − a·n;
   return g2;
```

```
end proc;

p :  = Dun(l, k);

# The procedure Res creates the matrix using the above parametric
# equations, calculates the determinant of this matrix, and then
# factors the result.  This will produce the desired implicit
# representation when set equal to 0.

Res := proc(p, q) local R1, F;
   R1 := resultant(q, p, t);
   F := factor((R1));
end proc;

Res(p, q);
```

Maplecode 2: Hypocycloid Resultant Coefficient Replacement for k < 1

```
# This procedure will calculate the determinant
# of the Sylvester or Bézout matrix with the coefficients
# in terms of m and n, which determine our hypocycloid for k < 1.

with(LinearAlgebra):

# l corresponds to m, and k corresponds to n.
# Select the values of m and n.
# These values will determine the size of the matrix,
# and hence the amount of time required to obtain the result.

l := m;
k := n;

# The Fun and Dun procedures create the desired parametric equations
# where the powers are specified but the coefficients are not.
```

```
Fun := proc(l, k) local f1, f2;
   f1 := a·(m − n)·t^(2·n) − 2·n·x·t^n + a·n·t^(2·n−m) + a·n·t^m + a·(m − n);
   f2 := a·(m − n)·t^(2·k) − 2·n·x·t^k + a·n·t^(2·k−l) + a·n·t^l + a·(m − n);
return f2;
end proc;

q := Fun(l, k);

Dun := proc(l, k) local g1, g2;
   g1 := −a·(m − n)·t^(2·n) − 2·I·n·y·t^n − a·n·t^(2·n−m) + a·n·t^m + a·(m − n);
   g2 := −a·(m − n)·t^(2·k) − 2·I·n·y·t^k − a·n·t^(2·k−l) + a·n·t^l + a·(m − n);
   return g2;
end proc;

p := Dun(l, k);

# The procedure Res creates the matrix using the above parametric
# equations, calculates the determinant of this matrix, and then
# factors the result.  This will produce the desired implicit
# representation when set equal to 0.

Res := proc(p, q) local R1, F;
   R1 := resultant(q, p, t);
   F := factor((R1));
end proc;

Res(p, q);
```

Maplecode 3: Hypocycloid Resultant Coefficient Replacement for $1 < k < 2$

```
# This procedure will calculate the determinant
# of the Sylvester or Bézout matrix with the coefficients
# in terms of m and n, which determine our hypocycloid for 1 < k < 2.
```

```
with(LinearAlgebra):

# l corresponds to m, and k corresponds to n.
# Select the values of m and n.
# These values will determine the size of the matrix,
# and hence the amount of time required to obtain the result.

l := m;
k := n;

# The Fun and Dun procedures create the desired parametric equations
# where the powers are specified but the coefficients are not.

Fun := proc(l, k) local f1, f2;
   f1 := a·(m−n)·t^(2·n) + a·n·t^m − 2·n·x·t^n + a·n·t^(2·n−m) + a·(m−n);
   f2 := a·(m−n)·t^(2·k) + a·n·t^l − 2·n·x·t^k + a·n·t^(2·k−l) + a·(m−n);
return f2;
end proc;

q := Fun(l, k);

Dun := proc(l, k) local g1, g2;
   g1 := −a·(m−n)·t^(2·n) + a·n·t^m − 2·I·n·y·t^n − a·n·t^(2·n−m) + a·(m−n);
   g2 := −a·(m−n)·t^(2·k) + a·n·t^l − 2·I·n·y·t^k − a·n·t^(2·k−l) + a·(m−n);
   return g2;
end proc;

p := Dun(l, k);

# The procedure Res creates the matrix using the above parametric
# equations, calculates the determinant of this matrix, and then
# factors the result.  This will produce the desired implicit
# representation when set equal to 0.

Res := proc(p, q) local R1, F;
```

```
   R1 := resultant(q, p, t);
   F := factor((R1));
end proc;

Res(p, q);
```

Maplecode 4: Hypocycloid Resultant Coefficient Replacement for k > 2

```
# This procedure will calculate the determinant
# of the Sylvester or Bézout matrix with the coefficients
# in terms of m and n, which determine our hypocycloid for k > 2.

with(LinearAlgebra):

# l corresponds to m, and k corresponds to n.
# Select the values of m and n.
# These values will determine the size of the matrix,
# and hence the amount of time required to obtain the result.

l := m;
k := n;

# The Fun and Dun procedures create the desired parametric equations
# where the powers are specified but the coefficients are not.

Fun := proc(l, k) local f1, f2;
   f1 := a·n·t^(2·m−2·n) + a·(m − n)·t^m − 2·n·x·t^(m−n) + a·(m − n)·t^(m−2·n) + a·n;
   f2 := a·n·t^(2·l−2·k) + a·(m − n)·t^l − 2·n·x·t^(l−k) + a·(m − n)·t^(l−2·k) + a·n;
   return f2;
end proc;

q := Fun(l, k);

Dun := proc(l, k) local g1, g2;
   g1 := a·n·t^(2·m−2·n) − a·(m − n)·t^m − 2·n·I·y·t^(m−n) + a·(m − n)·t^(m−2·n) − a·n;
```

```
   g2 := a·n·t^(2·l-2·k) - a·(m-n)·t^l - 2·n·I·y·t^(l-k) + a·(m-n)·t^(l-2·k) - a·n;
   return g2;
end proc;

p := Dun(l, k);

# The procedure Res creates the matrix using the above parametric
# equations, calculates the determinant of this matrix, and then
# factors the result.
# This will produce the desired implicit representation when set
# equal to 0.

Res := proc(p, q) local R1, F;
   R1 := resultant(q, p, t);
   F := factor((R1));
end proc;

Res(p, q);
```