The University of Alberta

Intersection of Curves and Surfaces Using Elimination Theory

by

© Hang Khanh Du

A thesis
submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements for the degree
of Masters of Science

Department of Computing Science

Edmonton, Alberta
Fall 1989

National Library of Canada
Bibliothèque nationale du Canada

Canadian Theses Service
Service des thèses canadiennes

Ottawa, Canada
K1A 0N4

ISBN 0-315-70170-6

THE UNIVERSITY OF ALBERTA

RELEASE FORM

NAME OF AUTHOR: Hang Khanh Du

TITLE OF THESIS: Intersection of Curves and Surfaces
Using Elimination Theory

DEGREE: Masters of Science

YEAR THIS DEGREE GRANTED: 1989

(Signed) ....

Permanent Address:
8804 33 Avenue,
Edmonton, Alberta,
Canada, T6K 2Y1

Date: Sept 6, 1989

THE UNIVERSITY OF ALBERTA

FACULTY OF GRADUATE STUDIES AND RESEARCH

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research, for acceptance, a thesis entitled **Intersection of Curves and Surfaces Using Elimination Theory** submitted by **Hang Khanh Du** in partial fulfillment of the requirements for the degree of Masters of Science.

Stan Cabay

(Co-supervisor)

(Co-supervisor)

Joseph Culberson

Xiaobo Li

Date: Sept. 6, 1989.

Dedicated to My Parents

Abstract

Geometric modeling is one of the active topics of research in computer science. One of the toughest problems in this area is the problem of finding the intersections of curves and surfaces. Recently, reseachers have focused their attention on applying algebraic geometry to this problem. It turns out that elimination theory can be effectively used to solve the intersection problems. This thesis discusses the issues of how to evaluate curve and surface intersections using elimination theory. First, it provides a comprehensive study of the elimination techniques. Second, it presents the implemention issues of three curve/curve intersection algorithms: projection, resolvent, and Gröbner basis methods. To test the algorithms, a methodology for generating random problems (pairs of 3D parametric rational curves) with known intersections is presented. Experimental results obtained from the random problems identify the classes of the problems for which each method is better. Also, experiments are performed to illustrate the difficulties which arise when using floating point implementations of the projection and resolvent intersection algorithms.

Acknowledgements

I would like to express my sincere acknowledgement to my supervisors, Dr. S. Cabay and Dr. B. Joe, who have supported my efforts as I have studied in this field. They have sparked my interests in this particular area of computer science and helped me to develop my ability to fulfil this thesis. This thesis owes much to their constructive and insightful criticisms and suggestions. Their remarkable skills and enthusiasm are gratefully appreciated. May everyone have such helpful supervisors.

The thesis has benefited much from the discussions I have had and the comments I have received from the committee members, Dr. J. Culberson, Dr. H. Brungs, and Dr. X. Li.

Special thanks are also forwarded to The Department of Computing Science at the University of Alberta and The Natural Science and Engineering Research Council of Canada for providing resources, technical support, and financial support. In addition, I would like to thank my friends for their supports; especially Gordon Fong and Kris Ng for guiding me in using UNIX and Latex.

Finally, none of this would have been possible without the unlimited kindness and patience of Christine Chau Pham and the ever present support of my parents, my sisters Chinh and Trang, and my brothers Van and Ham.

Table Of Contents

1 Introduction 1

2 Curves and Surfaces 6

2.1 Definitions of Curves and Surfaces 8

2.2 Intersection Problems 12

3 Elimination Theory 16

3.1 Polynomial Module and Ideal 17

3.1.1 Modules 17

3.1.2 Polynomial Ideal 18

3.2 The Resultants 19

3.2.1 Bezout's Resultant of Two Polynomials 20

3.2.2 Resultant of 2 Bivariate Homogeneous Polynomials 23

3.2.3 Resultant of n Homogeneous Polynomials in n Variables . 37

3.2.4 The u-Resultant 50

3.3 The Resolvent 53

3.3.1 The General Case 54

3.3.2 Special Resolvent of Three Independent Cubic Polynomials 58

3.4 The Gröbner Basis 63

3.4.1 Orderings and Leading Terms 64

3.4.2 Gröbner Basis 66

3.4.3 Solving Algebraic Equations with Gröbner Basis 70

4 Applying Elimination Theory to Intersection Problems 72

4.1 Solutions of Intersection Problems 72

4.2 Generation of Random Problems 77

4.3 Implementation Issues for Problem 2.1 81

4.4 Experimental Results 83

4.4.1 Exact Arithmetic Implementation 83

4.4.2 Floating Point Arithmetic Implementation 88

5 Concluding Remarks 91
5.1 Multivariate Resultant 92
5.2 Curve and Surface Intersections 95
5.3 Floating Point Implementation of Intersection Algorithms 96

Bibliography 98

A The Multivariate Resultant 102

BLANK PAGE INSERTED

List of Tables

4.1 Times in seconds for parametric rational curves 84
4.2 Times in seconds for parametric polynomial curves 85

Chapter 1

Introduction

Geometric modeling is concerned with the design, representation, and processing of curves, surfaces, and solids. It plays an important role in many areas of computer science and industry. This includes computer graphics, computer-aided design (CAD), computer-aided manufacturing (CAM), computer-aided geometric design (CAGD), robotics, automotive and aircraft industries. Computer models are apparently replacing physical models in many applications in industrial design and manufacture. They are cheaper to construct, easier to change, and simpler to analyze. Computer simulations save both time and money, and computer analyses of geometric models lead to better and cheaper products.

There are two distinct aspects of geometric modeling (1) Design: first, the physical shape of an object is given and presumed to be fixed, and we determine a mathematical approximation; (2) Processing: we usually need subsequent operations on the design such as viewing, intersections, transformations, etc.

In the design aspect of geometric modeling, designing curves and surfaces plays an important role in the construction of quite different products such as car bodies, ship hulls, airplane fuselages and wings, propeller blades, shoe insoles, bottles, etc., as well as in the description of geological, physical, and even medical phenomena.

Choosing a good representation of curves and surfaces can improve the accuracy with which the actual curves and surfaces are modeled. In addition, the representation also plays an important role in the effectiveness of the processing aspect of geometric modeling. For example, intersecting an implicit curve and a parametric polynomial one is a simple problem, but intersecting two implicit curves is a hard problem. Finally, the nature of the application also determines what type of representation we must choose. For instance, discrete representation of curves and surfaces is suitable for the image processing area but is awkward in CAGD.

Of all of the representations of curves and surfaces, parametric polynomial and parametric rational are the most commonly used in geometric modeling systems. The parametric rational representation can approximate with a high degree of accuracy most of the curves and surfaces that arise in real life applications [Bohm].

On the processing side of geometric modeling, intersection of curves and surfaces is a fundamental operation. This operation is performed repeatedly as part of many operations in geometric processing. We give some examples. Firstly, curve/curve intersection is used to find a physically meaningful offset curve (an offset curve is a curve offset from a given curve by a small amount) since one must first determine the self-intersections of this curve. An offset curve is useful in generating a cutter path[Farin]. Secondly, surface/surface intersection plays an important role in the construction of fillet surfaces, i.e., surfaces that round off sharp corners or edges between surfaces, since we must know that edge which is very often the intersection line between two surfaces. Thirdly, in solid modeling, the Boolean operations for solids require accurate intersection algorithms. In fact, most current solid modelers restrict themselves to plane and quadratic surface faces simply to ensure that intersections can be found reliably. Finally, curve/surface intersection is used in computing the contour lines which are the intersections between a plane and the graph of a given multivariate function. This is used very often in finding the lines of constant temperature in meteorology.

The intersection problem is not an easy one, and continues to be an active topic of research. Some of the reasons for this continuing activity are not hard to identify. A good curve and surface intersection technique has to balance three conflicting goals: efficiency, robustness, and accuracy. In this thesis, we will focus our attention on the intersection of parametric polynomial and parametric rational curves and surfaces. In Chapter 2, these intersection problems are described.

There are several known methods of handling the intersection problem. The first one that comes to our mind is the numerical method. Due to the scope of our thesis, this method is not covered here. The second method is the subdivision method. It is usually used for B-spline or Bezier curves and surfaces, which are defined by control polygons or graphs [Morton, Farin]. For example, to compute the intersection of two Bezier curves we proceed as follows: Compare the convex hulls of the two control polygons. If they do not overlap, the curves do not intersect. If they do overlap, each curve is subdivided into two parts and represented by refined control polygons and new convex hulls are checked for overlap. As this procedure continues, each iteration rejects parts of the curves which do not contain intersection points. We will not discuss this method further since it is beyond the scope of the thesis.

The third method is to use the elimination technique. Elimination theory can be viewed as two classes. The first is the classical one. This class deals with the existence of the solutions to polynomial equations. It evolved during the constructive period in algebra, beginning in the latter part of the nineteenth century. Sylvester, Cayley and Bezout did some pioneer works on the bivariate case. Later, Hurwitz and Mertens [Hurwit, Mertens] extended this result for the multivariate case using an abstract method. At the beginning of the twentieth century, Macaulay introduced an explicit expression for the multivariate resultant. More recently, Buchberger advanced elimination techniques by introducing the notion of Gröbner basis, a modern elimination technique.

In Chapter 3 and in the Appendix, we provide a comprehensive survey of these elimination techniques. First, we present the construction of the Bezout matrix of two univariate polynomials. Then, we provide a complete, correct, and constructive proof for the bivariate case, which involves the Sylvester resultant. Furthermore, we rewrite the constructive method to derive an explicit expression for the resultant in the multivariate case (the original descriptions in Macaulay [Mac02, Mac16] are hard to follow and appear to contain errors). Also in Chapter 3, the concepts of the complete and special resolvent are discussed and the notion of Gröbner basis is presented.

In Chapter 4, we describe the implementation issues of three curve/curve intersection algorithms: projection, resolvent, and Gröbner basis methods. A method for generating 3D parametric rational curves from random points in 3-space with known intersections is given. Experimental results obtained from these problems identify classes of problems for which each method is better. Also included in this chapter are experiments which illustrate difficulties with floating point implementations of the projection and resolvent intersection algorithms.

Concluding remarks and future considerations arising from this thesis are presented in Chapter 5.

Chapter 2

Curves and Surfaces

Designing curves and surfaces is one of the most important areas in geometric modeling. There are two classes of representations of curves and surfaces. The first one is the discrete class. It includes the tessellation of objects, such as curves and surfaces; for example, the raster format, quadtree, running code, chain code, etc., [Ball, Carlbo, Rosenf] techniques belong to this subclass of the discrete class. In addition, this class also contains the graphic or vector representation of objects. This subclass represents an object by its boundary vectors. In practice, the discrete representation class is often used in computer vision and image processing.

The second class is the continuous representation. It represents or approximates an object by a set of continuous functions. For example, spline curves and surfaces [Bohm, Farin, Morten] belong to this class. In this thesis, we restrict ourselves to curves and surfaces which can be represented *implicitly* as polynomials in independent variables with real coefficients. It looks like we are imposing a large constraint, but in practice, this subclass can approximate a lot of objects to any desirable accuracy. With any implicit representation, however, it is hard to determine the points on the curve or surface. Thus, we define a subclass of this implicit polynomial class; namely the class of curves and surfaces which can be represented by *parametric* rational polynomials. This representation is the most widely used one in geometric modeling systems because it has many advantages over other representations. First, it usually offers more degrees of freedom for controlling the shape of curves and surfaces than the non-parametric form. Second, transformations such as translation and rotation can be performed directly on parametric equations. Third, parametric forms readily handle infinite slopes without breaking down computationally. Fourth, parametric equations completely separate the roles of the dependent and independent variables, both algebraically and geometrically, and allow any numbers of variables. Fifth, parametrically defined geometric elements are inherently bounded because the parametric variables are bounded. Sixth, we can easily express these parametric equations in the form of vectors and matrices; this allows us to use computers economically. Finally, we can have the parametric polynomial meet certain special conditions, such as a common form for all curves and a common form for all surfaces. Because they have these nice properties, in this thesis, we focus only on curves and surfaces in parametric rational form. In practice, curves and surfaces are parametric piecewise rational, i.e., they consist of several parametric rational curves or surfaces joined together with a few degrees of continuity at the endpoints or boundary curves.

Before we give the definition of these curves and surfaces, we want to state that all parametric rational curves and surfaces can be implicitized to the polynomial form, but the converse is not always true. An implicit polynomial curve can be parametrized as a rational curve if and only if the curve has genus zero [Seder84b]. In the case of implicit cubic polynomial curves, not all curves can be parametrized;

Figure 2.1 has been removed
due to the unavailability of
copyright permission

Figure 2.1: [Pat88b] Graph of $-10x^3 + 30xy^2 - 30x^2 - 30y^2 + 22 = 0$

for example, the planar curve [Pat88b]

$$-10x^3 + 30xy^2 - 30x^2 - 30y^2 + 22 = 0$$

is nonparametrizable using rational form (see Figure 1). There are some works in the literature that deal with this problem [Pat88a, Pat88b, Abhy87a, Abhy87b, Abhy88a, Abhy88b]. They use polynomials and/or trigonometric functions such as *sin* or *cos* to parametrize the curves and surfaces.

In this chapter we give the definitions of various types of curves and surfaces, and we state several intersection problems involving them.

2.1 Definitions of Curves and Surfaces

The simplest curve in geometric modeling is the planar parametric polynomial curve.

Definition 2.1 *A planar parametric polynomial curve of degree n, C(t)=(x(t), y(t)), is defined by the equations*

$$\begin{aligned} x(t) &= a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0, \\ y(t) &= b_n t^n + b_{n-1} t^{n-1} + \cdots + b_1 t + b_0, \end{aligned} \qquad (2.1)$$

where $t_0 \leq t \leq t_1$ and at least one of a_n and b_n is nonzero.

We can see that the class of planar parametric polynomial curves is a small subclass of the implicit curves. For example, in the quadratic case, we can use planar parametric polynomial curves to represent the parabolas only. To represent all other conic curves such as ellipses and hyperbolas, we need the concept of planar parametric rational curves. For example, we can represent a semicircle which passes through $P_0 = (x_0, y_0)$ and $P_2 = (x_2, y_2)$, has center at the midpoint of the line segment P_0P_2, and has radius $r = \frac{1}{2}\sqrt{(x_0 - x_2)^2 + (y_0 - y_2)^2}$, by the parametric rational curve

$$\begin{aligned} x(t) &= \frac{(x_0 - 2x_1 + x_2)t^2 - 2(x_0 - x_1)t + x_0}{2t^2 - 2t + 1}, \\ y(t) &= \frac{(y_0 - 2y_1 + y_2)t^2 - 2(y_0 - y_1)t + y_0}{2t^2 - 2t + 1}, \end{aligned}$$

where $t \in [0, 1]$, and

$$x_1 = \frac{y_2 - y_0}{2}, \qquad y_1 = \frac{x_0 - x_2}{2}.$$

In addition, we can get the other half of this circle by using the same parametric rational equations $x(t)$ and $y(t)$ with the new values of x_1 and y_1 being the negative of the above values of x_1 and y_1 . Thus, in order to exactly represent or approximate some more complicated planar curves, we need the definition of planar parametric rational curve.

Definition 2.2 *A planar parametric rational curve of degree n, C(t)=(x(t), y(t)), is defined by the equations*

$$\begin{aligned} x(t) &= \frac{a_nt^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0}{d_nt^n + d_{n-1}t^{n-1} + \cdots + d_1t + d_0}, \\ y(t) &= \frac{b_nt^n + b_{n-1}t^{n-1} + \cdots + b_1t + b_0}{d_nt^n + d_{n-1}t^{n-1} + \cdots + d_1t + d_0}, \end{aligned} \qquad (2.2)$$

where $t_0 \leq t \leq t_1$ and at least one of a_n, b_n and d_n is nonzero. Also, at least one of d_i's is nonzero.

In practice, sometimes we have to used 3D curves; these curves can be thought of as the intersection of two 3D surfaces. It is noted that the set of all planar parametric polynomial curves is a subset of the set of all 3D parametric polynomial curves. Similar to the planar case, 3D parametric rational curves can be used to represent or approximate a larger set of curves than the class of 3D parametric polynomial curves. The definition of the 3D parametric rational curves is as follows.

Definition 2.3 *A 3D parametric rational curve of degree n, C(t)=(x(t), y(t), z(t)), is defined by the equations*

$$\begin{aligned} x(t) &= \frac{a_nt^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0}{d_nt^n + d_{n-1}t^{n-1} + \cdots + d_1t + d_0}, \\ y(t) &= \frac{b_nt^n + b_{n-1}t^{n-1} + \cdots + b_1t + b_0}{d_nt^n + d_{n-1}t^{n-1} + \cdots + d_1t + d_0}, \\ z(t) &= \frac{c_nt^n + c_{n-1}t^{n-1} + \cdots + c_1t + c_0}{d_nt^n + d_{n-1}t^{n-1} + \cdots + d_1t + d_0}, \end{aligned} \qquad (2.3)$$

where $t_0 \leq t \leq t_1$ and at least one of a_n, b_n, c_n and d_n is nonzero. Also, at least one of d_i's is nonzero.

Note that when $d_n = \ldots = d_1 = 0$ and $d_0 = 1$, we have the representation of a 3D parametric polynomial curve as mentioned above.

We can easily extend this definition for the k-dimensional parametric rational curves as

Definition 2.4 *A k-dimensional parametric rational curve of degree n, $C(t) = (x_1(t), x_2(t), \ldots, x_k(t))$ is defined by the equations*

$$\begin{aligned} x_1(t) &= \frac{a_{1,n}t^n + a_{1,n-1}t^{n-1} + \cdots + a_{1,1}t + a_{1,0}}{d_nt^n + d_{n-1}t^{n-1} + \cdots + d_1t + d_0}, \\ x_2(t) &= \frac{a_{2,n}t^n + a_{2,n-1}t^{n-1} + \cdot \quad + a_{2,1}t + a_{2,0}}{d_nt^n + d_{n-1}t^{n-1} + \cdots + d_1t + d_0}, \\ & \cdots\cdots\cdots \\ x_k(t) &= \frac{a_{k,n}t^n + a_{k,n-1}t^{n-1} + \cdots + a_{k,1}t + a_{k,0}}{d_nt^n + d_{n-1}t^{n-1} + \cdots + d_1t + d_0}, \end{aligned} \tag{2.4}$$

where $t_0 \le t \le t_1$ and at least one of $a_{1,n}$, $a_{2,n}$, $\ldots, a_{k,n}$ and d_n is nonzero. Also, at least one of d_i's is nonzero.

The parametric representation of the surface is similarly defined as in the case of the curves; hence, we have the definition of a parametric polynomial surface as

Definition 2.5 *A parametric polynomial surface, S(u,v)=(x(u,v), y(u,v), z(u,v)), is defined by the equations*

$$\begin{aligned} x(u,v) &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij}u^iv^j, \\ y(u,v) &= \sum_{i=0}^{n}\sum_{j=0}^{m} b_{ij}u^iv^j, \\ z(u,v) &= \sum_{i=0}^{n}\sum_{j=0}^{m} c_{ij}u^iv^j, \end{aligned} \tag{2.5}$$

where $u_0 \le u \le u_1$ and $v_0 \le v \le v_1$, and at least one of a_{nm}, b_{nm}, and c_{nm} is nonzero.

In geometric modeling, we also have the concept of a parametric rational surface, which is similarly defined, and the concept of a k-dimensional parametric rational surface, which can be defined easily by extending the definition of the parametric rational surface, but due to the scope of this thesis, we will not discuss these surfaces here.

2.2 Intersection Problems

The intersection problem is one of the most fundamental problems when processing curves and surfaces in geometric modeling. For example, *ray tracing* is a standard technique for the realistic rendering of objects. One of the major components in that method is the computation of intersections between straight lines (rays) and the objects to be rendered.

There are several different intersection problems; namely, the intersection between two curves, the intersection between two surfaces, and the intersection between a curve and a surface. The representation of the curves and surfaces in these problems determines the level of difficulty in obtaining the solution. The easiest intersection problem is the intersection between an implicit curve/surface and a parametric one. The problems of finding the intersection of two implicit or two parametric curves/surfaces has the same level of difficulty, in our opinion. In this thesis, we discuss only the intersection problems involving parametric curves and surfaces.

To solve these problems using algebraic methods, we have to solve the implicitization and inversion problems.

(1) The implicitization problem is to find the implicit polynomial equation $F(x,y) = 0$, for a given planar parametric curve, or two implicit surfaces $F(x,y,z) = 0$ and $G(x,y,z) = 0$ whose intersection is a given 3D parametric

curve, or the $k-1$ hypersurfaces whose intersection is a given k-dimensional parametric curve.

(2) The inversion problem is to find the parameter(s) t corresponding to the coordinates of a given point $P=(x,y)$, or $P=(x,y,z)$ for the 3D curve, or $P=(x_1,x_2,\ldots,x_k)$ in the k–dimensional case, known to lie on the curve.

Now we are in the position to give the description of the intersection problems in geometric modeling.

Problem 2.1 *Curve/Curve intersection*

Let $C_1(s)=(x_1(s),y_1(s),z_1(s))$ and $C_2(t)=(x_2(t),y_2(t),z_2(t))$ be curves represented by x-, y- and z-coordinate functions which are rational polynomials in s and t, i.e., $x_1(s)=\frac{a_1(s)}{d_1(s)}$, $y_1(s)=\frac{b_1(s)}{d_1(s)}$, $z_1(s)=\frac{c_1(s)}{d_1(s)}$, and $x_2(t)=\frac{a_2(t)}{d_2(t)}$, $y_2(t)=\frac{b_2(t)}{d_2(t)}$, $z_2(t)=\frac{c_2(t)}{d_2(t)}$, where $a_1(s),b_1(s),c_1(s),d_1(s)$ are polynomials in s and $a_2(t),b_2(t),c_2(t),d_2(t)$ are polynomials in t. Note that if $c_1(s)=c_2(t)=0$ then the curves are planar, and if $d_1(s)=d_2(t)=1$ then the curves are non-rational. Finding all the intersection points of these two curves by algebraic techniques is equivalent to solving the following system of equations:

$$\begin{aligned} \frac{a_1(s)}{d_1(s)}-\frac{a_2(t)}{d_2(t)} &= 0, \\ \frac{b_1(s)}{d_1(s)}-\frac{a_2(t)}{d_2(t)} &= 0, \\ \frac{c_1(s)}{d_1(s)}-\frac{c_2(t)}{d_2(t)} &= 0. \end{aligned} \tag{2.6}$$

We can also implicitize one curve, say $C_1(s)$, to get the implicit equations $P(x,y,z)=0$ and $Q(x,y,z)=0$ for the surfaces whose intersection curve is

$C_1(s)$. Substitute $x = x_2(t), y = y_2(t)$ and $z = z_2(t)$ into $P(x,y,z) = 0$ and $Q(x,y,z) = 0$, to get the following system of equations:

$$P(t) = 0, \qquad Q(t) = 0.$$

Similarly, for the k-dimensional case, the problem reduces to solving a system of k of equations in two unknowns, s and t, or a system of $k-1$ equations in one unknown, t.

Problem 2.2 *Curve/Surface intersection*

Let $S(u,v) = (x(u,v), y(u,v), z(u,v))$ denote a surface as in (2.5). Let line L be represented as the intersection of two planes whose equations are $F(x,y,z) = a_1x+b_1y+c_1z+d_1 = 0$ and $G(x,y,z) = a_2x+b_2y+c_2z+d_2 = 0$. Let the curve $C_1(s)$ be defined as in the previous problem. Because of the complexity of the problem, we separate it into two subproblems as follows:

Problem 2.2a *Line/Surface intersection*

The solution for this problem is straightforward. We simply substitute $x = x(u,v), y = y(u,v), z = z(u,v)$ into $F(x,y,z)$ and $G(x,y,z)$ to get two polynomials in u and v :

$$P_1(u,v) = 0, \qquad P_2(u,v) = 0. \tag{2.7}$$

Problem 2.2b *Curve/Surface intersection*

In this case, we can obtain the system of equations :

$$\begin{aligned} \frac{a_1(s)}{d_1(s)} - x(u,v) &= 0, \\ \frac{b_1(s)}{d_1(s)} - y(u,v) &= 0, \\ \frac{c_1(s)}{d_1(s)} - z(u,v) &= 0. \end{aligned} \tag{2.8}$$

Problem 2.3 *Surface/Surface intersection*

Let the two surfaces be parametrically defined by $S_1(u,v) = (x_1(u,v), y_1(u,v), z_1(u,v))$ and $S_2(s,t) = (x_2(s,t), y_2(s,t), z_2(s,t))$ where the coordinate functions are bivariate polynomials. As in the above curve/surface subproblem, we can obtain the system of equations:

$$\begin{aligned} x_1(u,v) - x_2(s,t) &= 0, \\ y_1(u,v) - y_2(s,t) &= 0, \\ z_1(u,v) - z_2(s,t) &= 0. \end{aligned} \tag{2.9}$$

Hence, the intersection problems can be expressed algebraically as a system of k equations in n unknowns, where k can be greater, less than, or equal to n.

Chapter 3

Elimination Theory

Classical elimination theory evolved during the period of constructive methods in algebra, beginning in the latter part of the nineteenth century. It is the study of conditions for the existence of solutions to a system of polynomial equations. The main idea here is to find a single condition for a system of k equations in n unknowns to have a solution. In the case of n homogeneous polynomials in n unknowns, we have the concept of resultant. This resultant is zero if and only if the system has a nontrivial solution, a solution in which at least one of the unknowns is nonzero. When there are k homogeneous polynomials in n unknowns where $k \leq n$ and the system has a finite number of solutions, we have the concept of u-resultant. From this resultant, we can get the solution of this system. Here, we are interested in more than the existence of the solutions of the system; we are interested in the constructive aspects of these resultants and how to find the solutions of the system from them. For the case $n < k$, we have to use a more powerful notion; here, the concept of resolvent is used to determine the existence of the nontrivial solution. The resolvent provides the necessary and sufficient condition for the system to not have a finite number of solutions.

Modern elimination theory is based on the concept of the Gröbner basis. After computing this basis, we have a list of criteria to determine the existence of the common zeros of the system of polynomials.

In this chapter, we examine these concepts in detail.

3.1 Polynomial Module and Ideal

In this section we introduce some basic concepts in polynomial theory. These concepts will be used throughout this chapter. The first one is the concept of a module of a set of polynomials; understanding this concept is useful for the development of classical elimination theory. The second concept, polynomial ideals, is an extension of the first one. This idea plays an important role in the development of the Gröbner basis.

3.1.1 Modules

First we introduce the concept of a module system of polynomials whose coefficients are in an arbitrary field.

Definition 3.1 : *A module system is an aggregate of polynomials in n variables $x_1, \ldots, x_n$ defined by the property that if P, P_1, P_2 belong to the system then $P_1 + P_2$ and AP also belong to the system where A is any polynomial in $x_1, \ldots, x_n$.*

We can see that if $P_1, \ldots, P_m$ belong to a module system then so does $A_1P_1 + \cdots + A_mP_m$, where $A_1, \ldots, A_m$ are arbitrary polynomials.

Let $P_1, \ldots, P_n$ be polynomials in $x_1, \ldots, x_n$, then $(P_1, \ldots, P_n)$ denotes the module system of these polynomials. Of all the members of the module $(P_1, \ldots, P_n)$, we are interested only in a small subset, namely those which are called the elementary members.

Definition 3.2 : *An elementary member of the module $(P_1, \ldots, P_n)$ is any member of the type wP_i $(i = 1, \ldots, n)$, where w is any power product of $x_1, \ldots, x_n$.*

Thus, the number of elementary members of a given module system of a given degree is finite.

Another way to think of the notion of a module is that the module is a generalization of a vector space; instead of restricting the scalars to lie in a field we allow them to be elements of an arbitrary ring. In our case, the ring is the ring of multivariate polynomials. Thus, we have the notion of linearly independent members of a module and the notion of bases as in a vector space [Herst].

3.1.2 Polynomial Ideal

Let $\mathcal{K}$ be a commutative ring, i.e., the ring of multivariate polynomials.

Definition 3.3 : *A non-empty subset $\mathcal{I}$ of a commutative ring $\mathcal{K}$ with identity is called an ideal if*

(1) $F - G \in \mathcal{I}$,

(2) $PF \in \mathcal{I}$,

for all $F, G \in \mathcal{I}, \quad P \in \mathcal{K}$.

The simplest examples are the *null ideal* (consisting of the 0 element only) and the *unit ideal* (consisting of the entire ring). The set

$$< P >= \{PQ \mid Q \in \mathcal{K}\}$$

of all multiples of $P \in \mathcal{K}$ is called a *principal ideal* generated by P. Clearly the unit ideal is $< 1 >$. Similarly, for the ring elements $P_1, \ldots, P_n \in \mathcal{K}$, the ideal generated by these elements is

$$< P_1, \ldots, P_n >= \{\sum_{i=1}^{n} P_i Q_i \mid Q_i \in \mathcal{K}\}.$$

Thus, a set of polynomials (algebraic equations) $\mathcal{P} = \{P_1, \ldots, P_n\}$ may be viewed as the generators of $< \mathcal{P} >$.

3.2 The Resultants

In this section, we give a general definition of resultant. In addition, we present the construction of the Bezout matrix of two univariate polynomials. Using the concept of modules, we discuss the construction of Sylvester and Macaulay matrices of two bivariate homogeneous polynomials and n homogeneous polynomials in n unknowns, respectively. Furthermore, we will show that the determinants of the Bezout and Sylvester matrices are the resultants of these polynomials while the resultant of the multivariate polynomials is the ratio between the determinant of the Macaulay matrix and the determinant of one of its submatrices.

Definition 3.4 : *A resultant of a set of polynomials is an expression involving the coefficients of these polynomials such that the vanishing of the resultant is a necessary and sufficient condition for the set of polynomials to have a nontrivial common zero.*

Note that in the case the coefficients of these polynomials are real numbers, complex zeros are allowed. In general, the zeros can be in an extension field of the coefficients.

3.2.1 Bezout's Resultant of Two Polynomials

Let P_1 and $P_2 \in R[t]$, for R an arbitrary Unique Factorization Domain, UFD. This domain includes the rings of polynomials in one or more variables over an arbitrary field. Assume $deg(P_1) = deg(P_2) = n > 0$, $a_i, b_j \in R$; we have

$$P_1(t) = \sum_{i=0}^{n} a_i t^i, \quad \text{and} \quad P_2(t) = \sum_{j=0}^{n} b_j t^j,$$

where at least one of a_n, b_n are nonzero.

Let

$$f(t) = P_1(t)P_2(t_0) - P_2(t)P_1(t_0),$$

where t_0 is a constant. Then $f(t_0) = 0$, even if there is no common root. Thus, $g(t) = \frac{f(t)}{t-t_0}$ is a polynomial in t of degree at most $n-1$, and the symmetry of $f(t)$ implies that the coefficients of $g(t)$ are also polynomials of degree $n-1$ in t_0. Thus, we can write $g(t)$ as

$$g(t) = \sum_{p=0}^{n-1}(\sum_{q=0}^{n-1} c_{pq} t_0^q)t^p, \tag{3.1}$$

where the c_{pq} are functions of a_i and b_j. Now if t_0 is a common root of $P_1(t)$ and $P_2(t)$, then

$$g(t) = \frac{P_1(t)}{(t-t_0)}P_2(t_0) - \frac{P_2(t)}{(t-t_0)}P_1(t_0) = 0$$

for all t. Hence, we can say that

$$\sum_{q=0}^{n-1} c_{pq} t_0^q = 0, \qquad \text{for all } p,\ 0 \le p \le n-1. \tag{3.2}$$

This yields the homogeneous system of linear equations:

$$\begin{bmatrix} c_{0,0} & \cdots & c_{0,n-1} \\ c_{1,0} & \cdots & c_{1,n-1} \\ \vdots & & \vdots \\ c_{n-1,0} & \cdots & c_{n-1,n-1} \end{bmatrix} \begin{bmatrix} 1 \\ t_0 \\ \vdots \\ t_0^{n-1} \end{bmatrix} = 0. \tag{3.3}$$

The matrix C $= [c_{pq}]$ is called the Cayley matrix or the Bezout matrix. Since t_0 is a common root of $P_1(t), P_2(t)$, system (3.3) has a nontrivial solution. This implies that the determinant of the above matrix is zero. De Montaudouin and Tiller [Montau] give the expression for entries c_{pq} of the Bezout matrix as:

$$c_{pq} = \sum_{k=mx}^{mn} (a_k b_{p+1+q-k} - a_{p+1+q-k} b_k), \qquad 0 \leq p, q \leq n-1 \ . \qquad (3.4)$$

where $mn = \min(p,q)$ and $mx = \max(0, q-n+1+p)$.

Using the vector approach, Goldman, Sederberg and Anderson [Goldm84] get the same expression for the c_{pq} as in (3.4)

$$c_{pq} = \sum_{k=mx}^{mn} |\mathrm{v}_k, \mathrm{v}_{p+1+q-k}|, \qquad 0 \leq p, q \leq n-1 \ . \qquad (3.5)$$

where mn and mx are defined as in (3.4), and $\mathrm{v}_i = [a_i, b_i]^T$. We wi'' discuss the advantages of this vector notation in solving the implicitization, inversion, and intersection of planar parametric rational curves in a later chapter.

It is clear that if $P_1 = kP_2$, where $k \neq 0$, then all the entries of the Bezout matrix are zeros. Also, De Montaudouin and Tiller [Montau] show that the determinant of the Bezout matrix is the resultant of polynomials P_1 and P_2, i.e., the vanishing of the determinant of the Bezout matrix of P_1, P_2 is a necessary and sufficient condition for them to have a common root. In addition, they show that if the rank of $[c_{pq}]$ is $n-r$ then the degree of the gcd of P_1 and P_2 is r and the $(n-r)$-th order submatrix in the lower right of $[c_{pq}]$ is nonsingular. Thus, if P_1 and P_2 have a unique common root, we can get it by solving for t_0 in system (3.3). Using the vector notation approach, Goldman, Sederberg and Anderson [Goldm84] show that if the number of common roots of P_1 and P_2 is more than one and less than n, then we can find them by first finding the gcd of P_1 and

P_2 by constructing the Bezout matrix, as in (3.3), of P_1 and P_2 and performing Gaussian elimination on the rows of this Bezout matrix bottom up using $c_{n-1,n-1}$ as a starting pivot. After elimination, the Bezout matrix look like this

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ & & \vdots & \vdots & & \\ c_{n-i,0} & \cdots & c_{n-i,n-i} & \cdots & 0 & 0 \\ & & & \ddots & & \\ c_{n-2,0} & c_{n-2,1} & \cdots & \cdots & c_{n-2,n-2} & 0 \\ c_{n-1,0} & c_{n-1,1} & \cdots & \cdots & c_{n-1,n-2} & c_{n-1,n-1} \end{bmatrix} . \tag{3.6}$$

The first non-zero row of $C = [c_{ij}]$ will be of the form

$$(e_0, e_1, \ldots, e_r, 0, \ldots, 0), \qquad e_r \neq 0,$$

and the gcd of P_1 and P_2 is $H(t) = \sum_{i=0}^{r} e_i t^i$. Thus, the common roots of P_1 and P_2 are the roots of $H(t)$. For a complete proof of the above results see [Goldm84].

Now, we can give the treatment for the case $deg(P_1) = m > deg(P_2) = n$. There are two ways to increase the degree of P_2 from n to m (to obtain P_2^*) :

(a) Regard P_2 as a polynomial of degree m, with the leading $m - n$ coefficients equal to zero, i.e., $P_2^* = P_2$.

(b) Multiply P_2 by t^{m-n}, i.e., $P_2^* = t^{m-n} P_2$.

De Montaudouin and Tiller [Montau] show that the Bezout resultant of P_1 and P_2^*, denoted by $\mathcal{R}(P_1, P_2^*)$, is the Bezout resultant of P_1 and P_2, denoted by $\mathcal{R}(P_1, P_2)$, multiplied by an extraneous factor. This factor is $(a_0)^{m-n}$ if we use method (a) and $(a_m)^{m-n}$ if we use method (b). Thus, in computer implementations, it should be checked which of a_0, a_m is simpler to apply the appropriate method; then

$\mathcal{R}(P_1, P_2)$ must be divided by the simple extraneous factor. Also, when one of the polynomials is a multiple of another, all the entries in $[c_{pq}]$ are zeros. Finally, it is easy to show that the Bezout resultant of two univariate polynomials is exactly, without regarding the sign, the Sylvester resultant of them. The Sylvester resultant is defined in the next section.

3.2.2 Resultant of 2 Bivariate Homogeneous Polynomials

Let

$$\begin{aligned} P_1 &= a_{d_1} x_1^{d_1} + a_{d_1-1} x_1^{d_1-1} x_2 + \cdots + a_0 x_2^{d_1}, \\ P_2 &= b_{d_2} x_1^{d_2} + b_{d_2-1} x_1^{d_2-1} x_2 + \cdots + b_0 x_2^{d_2}, \end{aligned} \tag{3.7}$$

where $d_1, d_2 \geq 1$, and let $d = d_1 + d_2 - 1$. We assume that a_{d_1}, b_{d_2}, a_0, and b_0 are nonzero (if P_1 and P_2 do not satisfy this assumption, then a factor x_1^k or x_2^k can be removed from P_1 or P_2 to satisfy this assumption). With this assumption, we can avoid the case of infinitely many solutions of $P_1 = P_2 = 0$, and a solution is either $x_1 = x_2 = 0$ or $x_1 = \alpha_1, x_2 = \alpha_2$ where α_1 and α_2 are both nonzero. The solutions (α_1, α_2) and $(c\alpha_1, c\alpha_2)$, where $c \neq 0$, are regarded as identical solutions.

The array of the coefficients of all elementary members of (P_1, P_2) of degree d, viz, $x_1^{d_2-1}P_1$, $x_1^{d_2-2}x_2P_1, \ldots,$ $x_2^{d_2-1}P_1$, $x_1^{d_1-1}P_2$, $x_1^{d_1-2}x_2P_2, \ldots,$ $x_2^{d_1-1}P_2$, has d_2 rows corresponding to P_1 and d_1 rows corresponding to P_2. This array can be expressed as

$$\begin{bmatrix} x_1^{d_2-1}P_1 \\ \vdots \\ x_2^{d_2-1}P_1 \\ x_1^{d_1-1}P_2 \\ \vdots \\ x_2^{d_1-1}P_2 \end{bmatrix} = \mathsf{S} \begin{bmatrix} x_1^{d} \\ \vdots \\ x_1^{d_1}x_2^{d_2-1} \\ x_1^{d_1-1}x_2^{d_2} \\ \vdots \\ x_2^{d} \end{bmatrix}, \tag{3.8}$$

where

$$\mathsf{S} = \begin{bmatrix} a_{d_1} & a_{d_1-1} & \cdots & \cdots & a_0 & & & \\ & a_{d_1} & a_{d_1-1} & \cdots & \cdots & a_0 & & \\ & & \ddots & & & & \ddots & \\ & & & a_{d_1} & a_{d_1-1} & \cdots & \cdots & a_0 \\ b_{d_2} & b_{d_2-1} & \cdots & \cdots & b_0 & & & \\ & b_{d_2} & b_{d_2-1} & \cdots & \cdots & b_0 & & \\ & & \ddots & & & & \ddots & \\ & & & b_{d_2} & b_{d_2-1} & \cdots & \cdots & b_0 \end{bmatrix}. \tag{3.9}$$

We will show that the determinant, $\mathcal{R}$, of the matrix S is the resultant of P_1 and P_2. $\mathcal{R}$ and S are known as the Sylvester resultant and the Sylvester matrix, respectively.

First, we show an important property of S, which plays an important role in the constructive proof for the Sylvester resultant, given by

Lemma 3.1 . *If the rank of* S *is r where $max(d_1, d_2) \leq r = d+1-k \leq d+1$, then*

(1) *the first (last) r columns of* S *are linearly independent, and*

(2) *the first (last) r rows of* S *are linearly independent.*

(3) *Furthermore, if $k \geq 1$ then* $\mathbf{S}$ *can be reduced by elementary row operations to*

$$\begin{bmatrix} \mathbf{U}_r & \mathbf{V} \\ \mathbf{0} & \mathbf{0} \end{bmatrix},$$

where $\mathbf{U}_r$ *is an order r upper triangular matrix with nonzero diagonal elements, and the last row of* $\mathbf{V}$ *is a nonzero row.*

Proof : We present the proof for the case of the first r columns and the first r rows; for the other cases, the proof is similar.

We will show that elementary row operations, without moving the last k rows, can be used to reduce $\mathbf{S}$ to a matrix of the form

$$\begin{bmatrix} \mathbf{U}_r & \mathbf{V} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}, \tag{3.10}$$

where $\mathbf{U}_r$ is an order r upper triangular matrix with nonzero diagonal elements (r may be $d+1$, in which case the other 3 submatrices are nonexistent). This means that the rank of $\mathbf{S}$ is r, and the first r columns of $\mathbf{S}$ are linearly independent, and the first r rows of $\mathbf{S}$ are linearly independent.

Suppose after some elementary row operations, we have the matrix

$$\begin{bmatrix} \mathbf{U}_p & \mathbf{V} \\ \mathbf{0} & \mathbf{S}_{q_1,q_2} \end{bmatrix}, \tag{3.11}$$

where $\mathbf{U}_p$ is an order $p \geq 0$ upper triangular matrix with nonzero diagonal elements, $\mathbf{V}$ is arbitrary, and $\mathbf{S}_{q_1,q_2}$ is a Sylvester matrix formed by polynomials of degree $q_1 \geq 1$ and $q_2 \geq 1$ with $q_1+q_2 = d_1+d_2-p$ and coefficients $c_{q_1}, c_{q_1-1}, \ldots, c_0$ and $e_{q_2}, e_{q_2-1}, \ldots, e_0$, such that not both c_{q_1} and e_{q_2} are zero, and $c_0 = a_0$. Note that initially, $p = 0, q_1 = d_1 \geq 1, q_2 = d_2 \geq 1$, $c_i = a_i, e_i = b_i$ and both c_{d_1} and e_{d_2} are nonzero.

Consider the submatrix $\mathbf{S}_{q_1,q_2}$. There are 3 cases :

(a) $c_{q_1} \neq 0, e_{q_2} = 0$,

(b) $c_{q_1} = 0, e_{q_2} \neq 0$,

(c) $c_{q_1} \neq 0, e_{q_2} \neq 0$.

Now, we will give the treatment for each case :

Case (a) : First suppose $q_2 > 1$. Then $\mathbf{S}_{q_1,q_2}$ can be partitioned as

$$\begin{bmatrix} c_{q_1} & \mathbf{v}^T \\ \mathbf{0} & \hat{\mathbf{S}}_{q_1,q_2-1} \end{bmatrix}$$

where $\hat{\mathbf{S}}_{q_1,q_2-1}$ is a Sylvester matrix of polynomials with degree $q_1 \geq 1, q_2 - 1 \geq 1$ and coefficients are $\hat{e}_{q_2-1} = e_{q_2-1}, \ldots, \hat{e}_1 = e_1, \hat{e}_0 = e_0$, and $\hat{c}_{q_1} = c_{q_1}, \ldots, \hat{c}_1 = c_1, \hat{c}_0 = c_0$. Since $c_{q_1} \neq 0$, we have a matrix of the form (3.11) with p increased to $p+1$, and this argument can be repeated.

Now, suppose $q_2 = 1$. Then

$$\mathbf{S}_{q_1,1} = \begin{bmatrix} c_{q_1} & c_{q_1-1} & \cdots & c_0 \\ 0 & e_0 & & \\ & \ddots & \ddots & \\ & & 0 & e_0 \end{bmatrix}$$

If $e_0 = 0$ then we have a matrix of form (3.10) with $r = p + 1$. Furthermore, the last row of matrix $\mathbf{V}$, as in (3.10), i.e., $(c_{q_1-1}, \ldots, c_0)$, is a nonzero row. If $e_0 \neq 0$ then $\mathbf{S}$ has full rank.

Case (b) : Suppose $q_1 > 1$, then moving row $q_2 + 1$ to the top of $\mathbf{S}_{q_1,q_2}$ yields

$$\begin{bmatrix} e_{q_2} & \mathbf{v}^T \\ \mathbf{0} & \hat{\mathbf{S}}_{q_1-1,q_2} \end{bmatrix}$$

where $\hat{\mathbf{S}}_{q_1-1,q_2}$ is a Sylvester matrix of polynomials with degree $q_1 - 1 \geq 1, q_2 \geq 1$ and coefficients $\hat{c}_{q_1-1} = c_{q_1-1}, \ldots, \hat{c}_1 = c_1, \hat{c}_0 = c_0$, and $\hat{e}_{q_2} = e_{q_2}, \ldots, \hat{e}_1 = e_1, \hat{e}_0 = e_0$. Thus, we have a matrix of the form (3.11) with p increased to $p+1$, and this argument can be repeated.

Now, suppose $q_1 = 1$. Then

$$\mathbf{S}_{1,q_2} = \begin{bmatrix} 0 & c_0 & & & \\ & \ddots & \ddots & & \\ & & 0 & c_0 & \\ e_{q_2} & e_{q_2-1} & \cdots & e_0 & \end{bmatrix}.$$

In this case, we have $c_0 \neq 0$ since c_0 is a_0 of the original matrix $\mathbf{S}$. Thus, $\mathbf{S}$ has full rank.

Case (c) : If $q_1 > q_2$, then for rows $1, \ldots, q_2$, subtract (c_{q_1}/e_{q_2}) times rows $q_2+1, \ldots, 2q_2$, respectively, and move row q_2+1 to be the first row, resulting in

$$\begin{bmatrix} e_{q_2} & e_{q_2-1} & \cdots & e_0 & & & & \\ 0 & \tilde{c}_{q_1-1} & \cdots & \tilde{c}_{q_1-q_2} & \cdots & c_0 & & \\ & \ddots & & & \ddots & & \ddots & \\ & & 0 & \tilde{c}_{q_1-1} & \cdots & \tilde{c}_{q_1-q_2} & \cdots & c_0 \\ & e_{q_2} & e_{q_2-1} & \cdots & e_0 & & & \\ & & \ddots & & & \ddots & & \\ & & & e_{q_2} & e_{q_2-1} & \cdots & e_0 & \\ & & & & e_{q_2} & e_{q_2-1} & \cdots & e_0 \end{bmatrix} = \begin{bmatrix} e_{q_2} & \mathbf{v}^T \\ 0 & \hat{\mathbf{S}}_{q_1-1,q_2} \end{bmatrix},$$

which satisfies the conditions below (3.11) and the value of c_0 remains as a_0, so this argument can be repeated.

If $q_1 \leq q_2$, then, first suppose $q_2 > 1$. In this case, for rows $q_2+1, \ldots, q_2+q_1$, subtract (e_{q_2}/c_{q_1}) times row $1, \ldots, q_1$, respectively, so matrix $\mathbf{S}_{q_1,q_2}$ reduces to

$$\left[\begin{array}{cccccccc}
c_{q_1} & c_{q_1-1} & \cdots & \cdots & c_0 & & & \\
 & c_{q_1} & c_{q_1-1} & \cdots & \cdots & c_0 & & \\
 & & \ddots & & & & \ddots & \\
 & & & c_{q_1} & c_{q_1-1} & \cdots & \cdots & c_0 \\
0 & \hat{e}_{q_2-1} & \cdots & \cdots & \hat{e}_0 & & & \\
 & 0 & \hat{e}_{q_2-1} & \cdots & \cdots & \hat{e}_0 & & \\
 & & \ddots & & & & \ddots & \\
 & & & 0 & \hat{e}_{q_2-1} & \cdots & \cdots & \hat{e}_0
\end{array}\right] = \left[\begin{array}{cc} c_{q_1} & \mathbf{v}^T \\ \mathbf{0} & \hat{\mathbf{S}}_{q_1,q_2-1} \end{array}\right],$$

which satisfies the conditions below (3.11) and the value of c_0 remains as a_0, so this argument can be repeated.

Second, suppose $q_2 = 1$. Then $q_1 = q_2 = 1$, and

$$\mathbf{S}_{1,1} = \left[\begin{array}{cc} c_1 & c_0 \\ e_1 & e_0 \end{array}\right] \text{ can be reduced to } \left[\begin{array}{cc} c_1 & c_0 \\ 0 & \hat{e}_0 \end{array}\right].$$

If $\hat{e}_0 = 0$ then $r = d_1 + d_2 - 1$, otherwise $r = d_1 + d_2$. In both cases, the matrix has the form (3.10), and the last row of $\mathbf{V}$, if it exists, is a nonzero row. □□

Let $\mathbf{S}_{d-1}$ be a matrix obtained from $\mathbf{S}_d = \mathbf{S}$ by removing the last row of each set of rows corresponding to the coefficients of P_1 and P_2, respectively, and the last column. Then the following corollary shows some important properties of $\mathbf{S}_{d-1}$ which will be useful for the proof of the next theorem.

Corollary 3.2 . *Let $rank(\mathbf{S}_d) = r = d+1-k$, where $min(d_1, d_2) \geq k \geq 1$. Then $rank(\mathbf{S}_{d-1}) = rank(\mathbf{S}_d) - 1 = r - 1$, and the first (last) $r-1$ columns of S_{d-1} are linearly independent.*

Proof : Let $\hat{\mathbf{S}}_{d-1}$ be the matrix obtained by removing the last row of $\mathbf{S}_d$. Then by part (2) of Lemma 3.1, $rank(\hat{\mathbf{S}}_{d-1}) = rank(\mathbf{S}_d)$. In matrix $\hat{\mathbf{S}}_{d-1}$, the d_2-th row, i.e., the last row of the block of rows corresponding to the coefficients of P_1, is contributing to the rank of this matrix since the only nonzero entry of the last column belongs to this row. Thus, removing this row will reduce the rank of $\hat{\mathbf{S}}_{d-1}$ by 1. Therefore, $rank(\mathbf{S}_{d-1}) = rank(\mathbf{S}_d) - 1 = r - 1$.

To prove that the first (last) $r-1$ columns of S_{d-1} are linearly independent, we can use an argument similar to the proof of Lemma 3.1. In this case, we use the $\mathbf{S}_{d-1}$ type matrix instead of the $\mathbf{S}_d$ type matrix. □□

Now we are in position to investigate the solution of $\mathbf{S}_d\mathbf{c} = \mathbf{0}$. If $\mathbf{S}_d$ has full rank then $\mathbf{c}$ is the zero vector. Suppose that $rank(\mathbf{S}_d) = d + 1 - k$, where $k > 0$; then $\mathbf{c}$ has k degrees of freedom, and by part (1) of Lemma 3.1, there exists a solution $\mathbf{c} = [c_d, c_{d-1}, \ldots, c_1, c_0]^T$ of $\mathbf{S}_d\mathbf{c} = \mathbf{0}$ of the form

$$c_0 = s_1, \quad c_1 = s_2, \quad \ldots, \quad c_{k-1} = s_k, \tag{3.12}$$

$$c_k = g_k(s_1, \ldots, s_k), \quad \ldots, \quad c_d = g_d(s_1, \ldots, s_k), \tag{3.13}$$

where $s_1, \ldots, s_k$ are arbitrary parameters and $g_i(s_1, \ldots, s_k)$ are unique linear combinations of these parameters.

Let $\hat{\mathbf{c}} = [c_d, c_{d-1}, \ldots, c_2, c_1]^T$ and $\check{\mathbf{c}} = [c_{d-1}, c_{d-2}, \ldots, c_1, c_0]^T$, where c_i's are given in (3.12) and (3.13). Then $\mathbf{S}_d\mathbf{c} = \mathbf{0}$ if and only if $\mathbf{S}_{d-1}\hat{\mathbf{c}} = \mathbf{0}$ and $\mathbf{S}_{d-1}\check{\mathbf{c}} = \mathbf{0}$. This result will be useful in proving the most important property of $\mathcal{R}$, that it is the resultant of P_1, P_2.

Theorem 3.3 : *A necessary and sufficient condition that the equations $P_1 = P_2 = 0$ have a nontrivial solution (i.e., a solution other than $x_1 = x_2 = 0$) is the vanishing of $\mathcal{R}$.*

Proof : The original version of this proof is due to Macauley [Mac16], but his proof is valid only when P_1 and P_2 have one common root. The constructive proof given here is valid for the case P_1 and P_2 have more than one common root. In addition, this proof has a potential to extend to the general case.

Suppose $P_1 = P_2 = 0$ has a nontrivial solution $x_1 = \alpha_1, x_2 = \alpha_2$. With this substitution, the left hand side (LHS) of (3.8) is $\mathbf{0}$ which implies that the right hand side (RHS) of (3.8) is $\mathbf{0}$. Since the vector on RHS of (3.8) is nonzero, $\mathcal{R} = |\mathbf{S}_d| = 0$.

Suppose $\mathcal{R} = 0$ and $rank(\mathbf{S}_d) = d + 1 - k$, where $min(d_1, d_2) \geq k \geq 1$. Let $Q(x_1, x_2)$ and $\hat{Q}(x_1, x_2)$ be the general members of the module (P_1, P_2) of degree d and $d-1$, respectively, i.e.,

$$Q(x_1, x_2) = \sum_{i+j=d} q_i x_1^i x_2^j \quad \text{and} \quad \hat{Q}(x_1, x_2) = \sum_{i+j=d-1} \hat{q}_i x_1^i x_2^j. \tag{3.14}$$

Thus, $Q(x_1, x_2)$ has $d+1$ monomials of degree d in x_1 and x_2. On the other hand, we have

$$Q(x_1, x_2) = R_1 P_1 + R_2 P_2, \tag{3.15}$$

where R_1 and R_2 are homogeneous polynomials in x_1 and x_2 and $deg(R_1) = d_2 - 1$, $deg(R_2) = d_1 - 1$. Hence,

$$\begin{aligned} Q(x_1, x_2) &= (e_1 x_1^{d_2-1} + e_2 x_1^{d_2-2} x_2 + \cdots + e_{d_2} x_2^{d_2-1}) P_1 + \\ &\quad (f_1 x_1^{d_1-1} + f_2 x_1^{d_1-2} x_2 + \cdots + f_{d_1} x_2^{d_1-1}) P_2. \end{aligned} \tag{3.16}$$

Let

$$\mathbf{q} = [q_d, \ldots, q_{d_1}, q_{d_1-1}, \ldots, q_0]^T,$$

$$\mathbf{c} = [c_d, \ldots, c_{d_1}, c_{d_1-1}, \ldots, c_0]^T,$$

$$\mathbf{g} = [e_1, \ldots, e_{d_2}, f_1, \ldots, f_{d_1}]^T,$$

where the elements of **c** are defined in (3.12) and (3.13). Then writing equation (3.16) in the form of system (3.8) and equating the coefficients with equation (3.14), we obtain

$$\mathbf{q}^{\mathrm{T}} = \mathbf{g}^{\mathrm{T}} \mathbf{S}_d. \tag{3.17}$$

Post-multiplying both sides of equation (3.17) by vector **c**, we have

$$\mathbf{q}^T \mathbf{c} = \mathbf{g}^T \mathbf{S}_d \mathbf{c}. \tag{3.18}$$

In order for (3.18) to be **0** for all values of **g**, i.e., for all members of module (P_1, P_2) of degree d, vector **c** must be a solution vector of the system $\mathbf{S}_d\mathbf{c} = 0$. Since $\mathcal{R} = 0$, there exists a nonzero solution **c**.

Let $s \neq 0$ be an arbitrary parameter and set $s_i = s^{i-1}$ for $i = 1, \ldots, k$ in (3.12) and (3.13), so that

$$c_0 = 1, \;\; c_1 = s, \;\; \ldots, \;\; c_{k-1} = s^{k-1}, \tag{3.19}$$

$$c_k = g_k(1, s, \ldots, s^{k-1}), \;\; \ldots, \;\; c_d = g_d(1, s, \ldots, s^{k-1}). \tag{3.20}$$

Note that $g_i(1, s, \ldots, s^{k-1})$ are uniquely determined in terms of $1, s, \ldots, s^{k-1}$. In addition, by part (3) of Lemma 3.1,

$$c_k = g_k(1, s, \ldots, s^{k-1}) \neq 0.$$

Now we want to show that $P_1 = P_2 = 0$ has a nontrivial solution $x_1 = \hat{s}, x_2 = 1$ where $\hat{s}$ is a solution of

$$g_k(1, s, \ldots, s^{k-1}) = s^k \tag{3.21}$$

in the extension field of the coefficients of P_1, P_2. In order to do it, we have to consider the linear relation between the coefficients of a general member of the module (P_1, P_2) of degree d as follows:

With the c_i's as given by (3.19) and (3.20), it follows from (3.18) that there is a unique linear relation between the coefficients of all general members $Q(x_1, x_2)$ of module (P_1, P_2) of degree d :

$$c_d q_d + c_{d-1} q_{d-1} + \cdots + c_1 q_1 + c_0 q_0 = 0. \tag{3.22}$$

The uniqueness of this relation is defined in the sense that if $\mathbf{y} = [y_d, y_{d-1}, \ldots, y_1, y_0]^T$ is a solution of $\mathbf{S}_d \mathbf{y} = \mathbf{0}$ and

$$y_0 = 1, \;\; y_1 = s, \;\; \ldots, \;\; y_{k-1} = s^{k-1}$$

then

$$y_k = g_k(1, s, \ldots, s^{k-1}), \;\; \ldots, \;\; y_d = g_d(1, s, \ldots, s^{k-1}).$$

Similarly, by Corollary 3.2 we have the following unique linear relation between the coefficients of all general members $\hat{Q}(x_1, x_2)$ of module (P_1, P_2) of degree $d-1$:

$$c_{d-1} \hat{q}_{d-1} + c_{d-2} \hat{q}_{d-2} + \cdots + c_1 \hat{q}_1 + c_0 \hat{q}_0 = 0, \tag{3.23}$$

where c_i's are given in (3.19) and (3.20).

Consider $x_1 \hat{Q}(x_1, x_2)$ and $x_2 \hat{Q}(x_1, x_2)$, then

$$x_1 \hat{Q}(x_1, x_2) = \hat{q}_{d-1} x_1^d + \hat{q}_{d-2} x_1^{d-1} x_2 + \cdots + \hat{q}_0 x_1 x_2^{d-1} \tag{3.24}$$

$$x_2\hat{Q}(x_1,x_2) = \hat{q}_{d-1}x_1^{d-1}x_2 + \hat{q}_{d-2}x_1^{d-2}x_2^2 + \cdots + \hat{q}_0 x_2^d \tag{3.25}$$

are the members of (P_1, P_2) of degree d whose coefficients must satisfy equation (3.22). Hence we have the following relations:

$$\hat{\mathbf{q}}^T\hat{\mathbf{c}} = c_d\hat{q}_{d-1} + c_{d-1}\hat{q}_{d-2} + \cdots + c_2\hat{q}_1 + c_1\hat{q}_0 = 0, \tag{3.26}$$

$$\hat{\mathbf{q}}^T\tilde{\mathbf{c}} = c_{d-1}\hat{q}_{d-1} + c_{d-2}\hat{q}_{d-2} + \cdots + c_1\hat{q}_1 + c_0\hat{q}_0 = 0, \tag{3.27}$$

where $\hat{\mathbf{q}} = [\hat{q}_{d-1}, \ldots, \hat{q}_0]^T$, $\hat{\mathbf{c}} = [c_d, \ldots, c_1]^T$, and $\tilde{\mathbf{c}} = [c_{d-1}, \ldots, c_0]^T$. By Corollary 3.2, $\mathbf{S}_{d-1}\tilde{\mathbf{c}} = \mathbf{0}$ for all values of s. In addition, there always exists $\hat{s} \neq 0$ that is a solution of

$$g_k(1, s, \ldots, s^{k-1}) - s^k = 0$$

in the extension field of the coefficients of the polynomials P_1, P_2, since $g_k(1, s, \ldots, s^{k-1}) \neq 0$. Thus, $\hat{\mathbf{c}}$ evaluated at $s = \hat{s}$ is

$$[g_d(1, \hat{s}, \ldots, \hat{s}^{k-1}), \ldots, g_{k+1}(1, \hat{s}, \ldots, \hat{s}^{k-1}), \hat{s}^k, \ldots, \hat{s}]^T.$$

This implies that $\mathbf{c}_* = (1/\hat{s})\hat{\mathbf{c}}$ evaluated at $s = \hat{s}$ also satisfies $\mathbf{S}_{d-1}\mathbf{c}_* = \mathbf{0}$. Hence, by the uniqueness of (3.23), the following ratios hold for the c_i's evaluated at $\hat{s}$:

$$\frac{c_d}{c_{d-1}} = \frac{c_{d-1}}{c_{d-2}} = \ldots = \frac{c_{d+1-k}}{c_{d-k}} = \ldots = \frac{c_2}{c_1} = \frac{c_1}{c_0} = \frac{\hat{s}}{1}.$$

Therefore, it is easy to see that

$$\frac{c_0}{1} = \frac{c_1}{\hat{s}} = \frac{c_2}{\hat{s}^2} = \ldots \frac{c_k}{\hat{s}^k} = \ldots \frac{c_{d-2}}{\hat{s}^{d-2}} = \frac{c_{d-1}}{\hat{s}^{d-1}} = \frac{c_d}{\hat{s}^d}. \tag{3.28}$$

Thus, equation (3.22) can be written as

$$q_0 + q_1\hat{s} + q_2\hat{s}^2 + \cdots + q_{d-2}\hat{s}^{d-2} + q_{d-1}\hat{s}^{d-1} + q_d\hat{s}^d = 0, \tag{3.29}$$

or we have

$$\mathbf{g}^T\mathbf{S}_d\mathbf{c} = 0,$$

where $\mathbf{c} = [\hat{s}^d, \hat{s}^{d-1}, \dots, \hat{s}, 1]^T$, and $\hat{s}$ is a solution of

$$g_k(1, s, \dots, s^{k-1}) - s^k = 0,$$

i.e., $P_1 = P_2 = 0$ has a nontrivial solution $(x_1, x_2) = (\hat{s}, 1)$. □□

Therefore, $\mathcal{R}$ is a resultant of P_1, P_2, called the Sylvester resultant.

From the above proof, it follows that

$$(g_k(x_2^k, x_2^{k-1}x_1, \dots, x_2x_1^{k-1}) - x_1^k)|\mathrm{gcd}(P_1, P_2).$$

because any solution of $(g_k(x_2^k, x_2^{k-1}x_1, \dots, x_2x_1^{k-1}) - x_1^k) = 0$ is a common solution of $P_1 = P_2 = 0$. Furthermore, we have

$$\mathrm{gcd}(P_1, P_2)|(g_k(x_2^k, x_2^{k-1}x_1, \dots, x_2x_1^{k-1}) - x_1^k)$$

because for any common solution of $P_1 = P_2 = 0, (x_1, x_2) = (\alpha_1, \alpha_2)$, there exists $\mathbf{c} = [\alpha_1^d, \alpha_1^{d-1}\alpha_2, \dots, \alpha_2^d]^T$ that is a solution of $\mathbf{S}_d\mathbf{c} = \mathbf{0}$. Therefore,

$$(g_k(x_2^k, x_2^{k-1}x_1, \dots, x_2x_1^{k-1}) - x_1^k) = \mathrm{gcd}(P_1, P_2).$$

Thus, solving for the roots of $g_k(x_2^k, x_2^{k-1}x_1, \dots, x_2x_1^{k-1}) - x_1^k = 0$ yields all the solutions of $P_1 = P_2 = 0$.

Before leaving this section, we give an example to illustrate the results of the above theorem.

Example 3.2.1: Let

$$\begin{aligned} P_1 &= (2x - 3y)(3x + y)(x - y)(4x - y), \\ P_2 &= (2x - 3y)(3x + y)(x - y)(x - 3y). \end{aligned}$$

The Sylvester matrix is

$$\mathbf{S} = \begin{bmatrix} 24 & -58 & 29 & 8 & -3 & 0 & 0 & 0 \\ 0 & 24 & -58 & 29 & 8 & -3 & 0 & 0 \\ 0 & 0 & 24 & -58 & 29 & 8 & -3 & 0 \\ 0 & 0 & 0 & 24 & -58 & 29 & 8 & -3 \\ 6 & -31 & 43 & -9 & -9 & 0 & 0 & 0 \\ 0 & 6 & -31 & 43 & -9 & -9 & 0 & 0 \\ 0 & 0 & 6 & -31 & 43 & -9 & -9 & 0 \\ 0 & 0 & 0 & 6 & -31 & 43 & -9 & -9 \end{bmatrix}.$$

We can determine that the rank of $\mathbf{S}$ is 5, so the rank deficiency is 3. Solving for $\mathbf{c}$ in $\mathbf{Sc} = \mathbf{0}$, we get

$$c_0 = t_0 \qquad c_1 = t_1$$
$$c_2 = t_2 \qquad c_3 = -\tfrac{1}{2}t_0 - \tfrac{2}{3}t_1 + \tfrac{13}{6}t_2$$
$$c_4 = -\tfrac{13}{12}t_0 - \tfrac{35}{18}t_1 + \tfrac{145}{36}t_2 \qquad c_5 = -\tfrac{145}{72}t_0 + \tfrac{1465}{216}t_1 - \tfrac{407}{108}t_2$$
$$c_6 = -\tfrac{1465}{432}t_0 - \tfrac{4235}{648}t_1 + \tfrac{14161}{1296}t_2 \qquad c_7 = -\tfrac{14161}{2592}t_0 - \tfrac{41507}{3888}t_1 - \tfrac{133273}{7776}t_2$$

Substitute $t_0 = 1, t_1 = t, t_2 = t^2$, we have

$$c_0 = 1 \qquad c_1 = t$$
$$c_2 = t^2 \qquad c_3 = -\tfrac{1}{2} - \tfrac{2}{3}t + \tfrac{13}{6}t^2$$
$$c_4 = -\tfrac{13}{12} - \tfrac{35}{18}t + \tfrac{145}{36}t^2 \qquad c_5 = -\tfrac{145}{72} + \tfrac{1465}{216}t - \tfrac{407}{108}t^2$$
$$c_6 = -\tfrac{1465}{432} - \tfrac{4235}{648}t + \tfrac{14161}{1296}t^2 \qquad c_7 = -\tfrac{14161}{2592} - \tfrac{41507}{3888}t - \tfrac{133273}{7776}t^2$$

We can find the roots of the equation

$$-\frac{1}{2} - \frac{2}{3}t + \frac{13}{6}t^2 - t^3 = (t - \frac{3}{2})(t + \frac{1}{3})(t - 1) = 0$$

Therefore, (3/2,1),(-1/3,1) and (1,1) are solutions of P_1, P_2. Also, we obtain

$$\begin{aligned}\gcd(P_1,P_2) &= g_3(y^3,y^2x,yx^2)-x^3 \\ &= -\frac{1}{6}(6x^3-13x^2y+4xy^2+3y^3).\end{aligned}$$

Note that this method of finding the roots of $P_1 = P_2 = 0$ is valid only when these polynomials have a finite number of roots; i.e., when there are no common factors of these polynomials in the form x_1^k or x_2^k. If these polynomials have an infinite number of roots, then either the first k, in the case when the common factor is x_1^k, or the last k, in the case when the common factor is x_2^k, columns of S will be all zeros. We can then find the other roots of $P_1 = P_2 = 0$ by considering a general member of degree $d-k$ instead of a general member of degree d.

The second important property of $\mathcal{R}$, which is used for the proof of the general case, is given in the following theorem.

Theorem 3.4 : *$\mathcal{R}$ is irreducible in the sense that it cannot be resolved into two factors each of which is a function of the coefficients of P_1, P_2.*

Proof : The origin of this proof is due to Macaulay [Macl6]. $\mathcal{R}$ has the term $a_{d_1}^{d_2}b_0^{d_1}$ obtained from the diagonal of the matrix S, and this is only term of $\mathcal{R}$ containing $b_0^{d_1}$ or $a_{d_1}^{d_2}$. Also $\mathcal{R}$ has a term $(-1)^{d_2}b_{d_2}a_{d_1-1}^{d_2}b_0^{d_1-1}$, and this is the only term of $\mathcal{R}$ containing $b_0^{d_1-1}$ when $a_{d_1} = 0$. This can be seen by expanding about the first column of S. Hence, when $\mathcal{R}$ is expanded in the powers of b_0 to two terms, we have

$$\mathcal{R} = r_{d_1}b_0^{d_1} + r_{d_1-1}b_0^{d_1-1} + \cdots, \tag{3.30}$$

where $r_{d_1} = a_{d_1}^{d_2}$ and $r_{d_1-1} \bmod a_{d_1} = (-1)^{d_2}b_{d_2}a_{d_1-1}^{d_2}$. Thus, if $\mathcal{R}$ can be written as a product of two factors, then

$$\mathcal{R} = (a_{d_1}^{p_2} b_0^{p_1} + \cdots)(a_{d_1}^{q_2} b_0^{q_1} + \cdots),$$

where $p_1 + q_1 = d_1$ and $p_2 + q_2 = d_2$, and either p_2 or q_2 is zero because otherwise the coefficient r_{d_1-1} of $b_0^{d_1-1}$ would be zero or divisible by a_{d_1}, which is not the case. Therefore, one of the factors of $\mathcal{R}$ is independent of the coefficients of P_1, since both factors must be homogeneous in the coefficients of P_1. Similarly, one of the factors must be independent of the coefficients of P_2, i.e.,

$$\mathcal{R} = (a_{d_1}^{d_2} + \cdots)(b_0^{d_1} + \cdots) = a_{d_1}^{d_2} b_0^{d_1} + B b_0^{d_1} + D a_{d_1}^{d_2} + \cdots . \tag{3.31}$$

Now, if each factor contains only one term, then (3.31) would contradict (3.30) since $r_{d_1-1} \neq 0$. On the other hand, if one factor contains more than one term, then B and D are not both zero and (3.31) contradicts (3.30) since $a_{d_1}^{d_2} b_0^{d_1}$ is the only term of $\mathcal{R}$ containing $a_{d_1}^{d_2}$ or $b_0^{d_1}$. Therefore, $\mathcal{R}$ is irreducible. □□

3.2.3 Resultant of n Homogeneous Polynomials in n Variables

In this section, we introduce a general theory of resultant. It will parallel that already given in the bivariate case but with greater complexity. Another method of finding the resultant is given in [Waerd], and Canny explains this method more clearly in his Ph.D. thesis [Can87]. Although the multivariate resultant given here is for n homogeneous polynomials in n variables, we can find the multivariate resultant for n non-homogeneous polynomials in $n-1$ variables by finding the corresponding homogeneous polynomials of the same degrees obtained by introducing a variable x_n of homogeneity.

Lct

$$\begin{aligned} P_1 &= a^{(1)}_{d_1,\ldots,0}x_1^{d_1} + \cdots + a^{(1)}_{0,d_1,\ldots,0}x_2^{d_1} + \cdots + a^{(1)}_{0,\ldots,d_1}x_n^{d_1}, \\ P_2 &= a^{(2)}_{d_2,\ldots,0}x_1^{d_2} + \cdots + a^{(2)}_{0,d_2,\ldots,0}x_2^{d_2} + \cdots + a^{(2)}_{0,\ldots,d_2}x_n^{d_2}, \qquad (3.32) \\ &\cdots\cdots\cdots \\ P_n &= a^{(n)}_{d_n,\ldots,0}x_1^{d_n} + \cdots + a^{(n)}_{0,d_n,\ldots,0}x_2^{d_n} + \cdots + a^{(n)}_{0,\ldots,d_n}x_n^{d_n}. \end{aligned}$$

be n homogeneous polynomials in n variables, $x_1, \ldots, x_n$, of degree $d_1, \ldots, d_n$ respectively, with indeterminate coefficients.

In addition, we have

$$d = 1 + \sum_{i=1}^{n} (d_i - 1).$$

We define a polynomial reduced in $x_1, \ldots, x_i$ as

Definition 3.5 *A polynomial containing no monomials $x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$ divisible by any of $x_1^{d_1}$, $x_2^{d_2}$, $\ldots$, $x_i^{d_i}$ is said to be reduced in $x_1, \ldots, x_i$.*

Let $\alpha = (\alpha_1, \ldots, \alpha_n)$, $|\alpha| = \sum_1^n \alpha_i$, and let x^α denote $x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$.

Also, let $\hat{\mathcal{X}}_m$ be the set of monomials of degree m in $x_1, \ldots, x_n$, such that

$$\hat{\mathcal{X}}_m = \{x^\alpha \mid \alpha_1 + \alpha_2 + \cdots + \alpha_n = m\}. \qquad (3.33)$$

We observe that the cardinality of $\hat{\mathcal{X}}_m$ is [Can87]

$$|\hat{\mathcal{X}}_m| = N_m = \begin{pmatrix} m+n-1 \\ m \end{pmatrix}. \qquad (3.34)$$

Let π be a permutation of $1, 2, \ldots, n$. We now partition $\hat{\mathcal{X}}_m$ into $n+1$ subsets with respect to the permutation π as follows: $\hat{\mathcal{X}}^\pi_{i-1,m}$ is the set of monomials which are multiples of $x_{\pi(i)}^{d_{\pi(i)}}$, but which are not multiples of $x_{\pi(j)}^{d_{\pi(j)}}$ for any $j < i$, so that

$$\hat{\mathcal{X}}^\pi_{0,m} = \{x^\alpha \in \hat{\mathcal{X}}_m \mid \alpha_{\pi(1)} \geq d_{\pi(1)}\}$$

$$\hat{\mathcal{X}}^{\pi}_{1,m} = \{x^{\alpha} \in \hat{\mathcal{X}}_m \mid \alpha_{\pi(2)} \geq d_{\pi(2)} \text{ and } \alpha_{\pi(1)} < d_{\pi(1)}\}$$

$$\cdots \qquad \cdots \tag{3.35}$$

$$\hat{\mathcal{X}}^{\pi}_{n-1,m} = \{x^{\alpha} \in \hat{\mathcal{X}}_m \mid \alpha_{\pi(n)} \geq d_{\pi(n)} \text{ and } \alpha_{\pi(i)} < d_{\pi(i)} \text{ for } i = 1, \ldots, n-1\},$$

$$\hat{\mathcal{X}}^{\pi}_{n,m} = \{x^{\alpha} \in \hat{\mathcal{X}}_m \mid \alpha_{\pi(i)} < d_{\pi(i)} \text{ for } i = 1, \ldots, n\}.$$

It is readily shown that the $\hat{\mathcal{X}}^{\pi}_{i,m}$ are disjoint, and that every element of $\hat{\mathcal{X}}_m$ is contained in exactly one of them. In addition, for $m \geq d$, $\hat{\mathcal{X}}^{\pi}_{n,m} = \emptyset$.

Also, for each $\hat{\mathcal{X}}^{\pi}_{i,m}$, where $0 \leq i \leq n-1$, we define a set of monomials $\mathcal{X}^{\pi}_{i,m}$ such that

$$\mathcal{X}'^{\pi}_{i,m} = \{x^{\alpha}/x^{d_{\pi(i+1)}}_{\pi(i+1)} \mid x^{\alpha} \in \hat{\mathcal{X}}^{\pi}_{i,m}\}.$$

Thus, we can easily see that the monomials in $\mathcal{X}^{\pi}_{i,m}$ are reduced in $x_{\pi(1)}, \ldots, x_{\pi(i)}$ for $i = 1, \ldots, n$.

Let $\Omega^{\pi}_{i,m}$ be the set of polynomials such that

$$\Omega^{\pi}_{i,m} = \{\sum_j a_j x^{\alpha_j} \mid x^{\alpha_j} \in \mathcal{X}^{\pi}_{i,m}\}.$$

Then the product $P_{\pi(i)}Q_{i-1}$, where $Q_{i-1} \in \Omega^{\pi}_{i-1,m}$ is a homogeneous polynomial of degree d in $x_1, \ldots, x_n$.

Also, let $\hat{\Omega}^{\pi}_{i,m}$ be the set of polynomials such that

$$\hat{\Omega}^{\pi}_{i,m} = \{\sum_j a_j x^{\alpha_j} \mid x^{\alpha_j} \in (\bigcup_{q=i}^{n} \hat{\mathcal{X}}^{\pi}_{q,m})\},$$

and $\hat{\mathcal{X}}_{i,m} = \hat{\mathcal{X}}^{\pi}_{i,m}$, $\mathcal{X}_{i,m} = \mathcal{X}^{\pi}_{i,m}$, $\hat{\Omega}_{i,m} = \hat{\Omega}^{\pi}_{i,m}$, $\Omega_{i,m} = \Omega^{\pi}_{i,m}$ with identity permutation.

For simplicity, we now assume π is the identity permutation, although the following results apply for any permutation π. Let

$$G = P_1Q_0 + \cdots + P_pQ_{p-1} + \hat{Q}_p,$$

where $1 \leq p \leq n$, $Q_i \in \Omega_{i,m}$ for $i = 0, 1, \ldots, p-1$, and $\hat{Q}_p \in \hat{\Omega}_{p,m}$ are homogeneous polynomials of degree m in $x_1, \ldots, x_n$. In vector notation, we have

$$\mathbf{g}^T\mathbf{x} = \mathbf{c}^T\mathbf{M}_p(n,m)\mathbf{x}, \tag{3.36}$$

where $\mathbf{g}$ and $\mathbf{x}$ are the vectors of the coefficients and the corresponding monomials in G, $\mathbf{c}$ is a vector of the coefficients of the polynomials $Q_0, \ldots, Q_{p-1}, \hat{Q}_p$, and $\mathbf{M}_p(n,m)$ is the Macaulay matrix of $P_1, \ldots, P_n$ whose construction we now describe.

First, we construct $n+1$ sets $\mathcal{X}_{0,m}, \ldots, \mathcal{X}_{n,m}$. For $0 \leq i \leq p-1$, define a set of polynomials F_i such that

$$F_i = \mathcal{X}_{i,m}' P_{i+1}(x_1, \ldots, x_n). \tag{3.37}$$

Then the polynomials in F_i, for $i = 0, \ldots, p-1$ are elementary members of the module $(P_1, \ldots, P_n)$ of degree m. The union F of $F_0, \ldots, F_{p-1}, \hat{\mathcal{X}}_{p,m}, \ldots, \hat{\mathcal{X}}_{n,m}$ is a collection of N_m polynomials of degree m. Thus, we can construct a square matrix $\mathbf{M}_p(n,m)$ whose rows contain the coefficients of the N_m polynomials in F and whose columns correspond to the N_m monomials in $\hat{\mathcal{X}}_m$.

To illustrate the above construction process, we give the following example.

Example 3.2.2: We construct the Macaulay matrices, $\mathbf{M}_2(3,3)$, $\mathbf{M}_3(3,3)$ and $\mathbf{M}_3(3,4)$, of a system of 3 quadrics in three variables x, y, z. The polynomials are:

$$\begin{aligned}
P_1 &= a_{xx}x^2 + a_{xy}xy + a_{xz}xz + a_{yy}y^2 + a_{yz}yz + a_{zz}z^2,\\
P_2 &= b_{xx}x^2 + b_{xy}xy + b_{xz}xz + b_{yy}y^2 + b_{yz}yz + b_{zz}z^2,\\
P_3 &= c_{xx}x^2 + c_{xy}xy + c_{xz}xz + c_{yy}y^2 + c_{yz}yz + c_{zz}z^2.
\end{aligned}$$

We have $d_1 = d_2 = d_2 = 2,\ d = 4$.

Now, we construct $\mathbf{M}_2(3,3)$ is as follows: First, we have

$$\begin{aligned} \hat{\mathcal{X}}_{0,3} &= \{x^3, x^2y, x^2z\}, \\ \hat{\mathcal{X}}_{1,3} &= \{y^3, xy^2, y^2z\}, \\ \hat{\mathcal{X}}_{2,3} &= \{z^3, xz^2, yz^2\}, \\ \hat{\mathcal{X}}_{3,3} &= \{xyz\}. \end{aligned} \tag{3.38}$$

Dividing $\hat{\mathcal{X}}_{0,3}$, $\hat{\mathcal{X}}_{1,3}$ by x^2, y^2, respectively, we obtain

$$\begin{aligned} \mathcal{X}'_{0,3} &= \{x, y, z\}, \\ \mathcal{X}_{1,3} &= \{x, y, z\}. \end{aligned} \tag{3.39}$$

Hence, the 10 by 10 matrix $\mathbf{M}_2(3,3)$ is

$$M_2(3,3) = \begin{bmatrix} a_{xx} & a_{xy} & a_{xz} & a_{yy} & a_{zz} & a_{yz} & 0 & 0 & 0 & 0 \\ 0 & a_{xx} & 0 & a_{xy} & 0 & a_{xz} & a_{yy} & a_{yz} & 0 & a_{zz} \\ 0 & 0 & a_{xx} & 0 & a_{xz} & a_{xy} & 0 & a_{yy} & a_{zz} & a_{yz} \\ b_{xx} & b_{xy} & b_{xz} & b_{yy} & b_{zz} & b_{yz} & 0 & 0 & 0 & 0 \\ 0 & b_{xx} & 0 & b_{xy} & 0 & b_{xz} & b_{yy} & b_{yz} & 0 & b_{zz} \\ 0 & 0 & b_{xx} & 0 & b_{xz} & b_{xy} & 0 & b_{yy} & b_{zz} & b_{yz} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

where

$$\begin{bmatrix} xP_1 \\ yP_1 \\ zP_1 \\ xP_2 \\ yP_2 \\ zP_2 \\ xz^2 \\ xyz \\ z^3 \\ yz^2 \end{bmatrix} = M_2(3,3) \begin{bmatrix} x^3 \\ x^2y \\ x^2z \\ xy^2 \\ xz^2 \\ xyz \\ y^3 \\ y^2z \\ z^3 \\ yz^2 \end{bmatrix} .$$

The construction of $\mathrm{M}_3(3,3)$ is as follows: first we have

$$\begin{array}{rcll} \hat{\mathcal{X}}_{0,3} & = & \{x^3, x^2y, x^2z\}, & \\ \hat{\mathcal{X}}_{1,3} & = & \{y^3, xy^2, y^2z\}, & (3.40) \\ \hat{\mathcal{X}}_{2,3} & = & \{z^3, xz^2, yz^2\}, & (3.41) \\ \hat{\mathcal{X}}_{3,3} & = & \{xyz\}. & \end{array}$$

Divide $\hat{\mathcal{X}}_{0,3}$, $\hat{\mathcal{X}}_{1,3}$, $\hat{\mathcal{X}}_{2,3}$ by x^2, y^2, z^2, respectively, to obtain

$$\begin{array}{rcll} \mathcal{X}_{0,3} & = & \{x, y, z\}, & \\ \mathcal{X}_{1,3} & = & \{x, y, z\}, & (3.42) \\ \mathcal{X}_{2,3} & = & \{x, y, z\}. & \end{array}$$

Hence, the 10 by 10 matrix $\mathbf{M}_3(3,3)$ is

$$M_3(3,3) = \begin{bmatrix} a_{xx} & a_{xy} & a_{xz} & a_{yy} & a_{zz} & a_{yz} & 0 & 0 & 0 & 0 \\ 0 & a_{xx} & 0 & a_{xy} & 0 & a_{xz} & a_{yy} & a_{yz} & 0 & a_{zz} \\ 0 & 0 & a_{xx} & 0 & a_{xz} & a_{xy} & 0 & a_{yy} & a_{zz} & a_{yz} \\ b_{xx} & b_{xy} & b_{xz} & b_{yy} & b_{zz} & b_{yz} & 0 & 0 & 0 & 0 \\ 0 & b_{xx} & 0 & b_{xy} & 0 & b_{xz} & b_{yy} & b_{yz} & 0 & b_{zz} \\ 0 & 0 & b_{xx} & 0 & b_{xz} & b_{xy} & 0 & b_{yy} & b_{zz} & b_{yz} \\ c_{xx} & c_{xy} & c_{xz} & c_{yy} & c_{zz} & c_{yz} & 0 & 0 & 0 & 0 \\ 0 & c_{xx} & 0 & c_{xy} & 0 & c_{xz} & c_{yy} & c_{yz} & 0 & c_{zz} \\ 0 & 0 & c_{xx} & 0 & c_{xz} & c_{xy} & 0 & c_{yy} & c_{zz} & c_{yz} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Similarly, the construction of $\mathbf{M}_3(3,4)$ begins with getting the following sets :

$$\begin{aligned} \hat{\mathcal{X}}_{0,4} &= \{x^4, x^3y, x^3z, x^2y^2, x^2z^2, x^2yz\}, \\ \hat{\mathcal{X}}_{1,4} &= \{y^4, xy^3, y^3z, y^2z^2, xy^2z\}, && (3.43) \\ \hat{\mathcal{X}}_{2,4} &= \{z^4, xz^3, yz^3, xyz^2\}, && (3.44) \\ \hat{\mathcal{X}}_{3,4} &= \emptyset. \end{aligned}$$

Divide $\hat{\mathcal{X}}_{0,4}$, $\hat{\mathcal{X}}_{1,4}$, $\hat{\mathcal{X}}_{2,4}$ by x^2, y^2, z^2, respectively, we have

$$\begin{aligned} \mathcal{X}'_{0,4} &= \{x^2, xy, xz, y^2, z^2, yz\}, \\ \mathcal{X}'_{1,4} &= \{y^2, xy, yz, z^2, xz\}, && (3.45) \\ \mathcal{X}'_{2,4} &= \{z^2, xz, yz, xy\}. \end{aligned}$$

Hence, the 15 by 15 matrix $M_3(3,4)$ is

$$\begin{bmatrix}
a_{xx} & a_{xy} & a_{xz} & a_{yy} & a_{zz} & a_{yz} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & a_{xx} & 0 & a_{xy} & 0 & a_{xz} & 0 & a_{yy} & 0 & 0 & a_{yz} & 0 & 0 & 0 & a_{zz} \\
0 & 0 & a_{xx} & 0 & a_{xz} & a_{xy} & 0 & 0 & 0 & 0 & a_{yy} & 0 & a_{zz} & 0 & a_{yz} \\
0 & 0 & 0 & a_{xx} & 0 & 0 & a_{yy} & a_{xy} & a_{yz} & a_{zz} & a_{xz} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & a_{xx} & 0 & 0 & 0 & 0 & a_{yy} & 0 & a_{zz} & a_{xz} & a_{yz} & a_{xy} \\
0 & 0 & 0 & 0 & 0 & a_{xx} & 0 & 0 & a_{yy} & a_{yz} & a_{xy} & 0 & 0 & a_{zz} & a_{xz} \\
0 & 0 & 0 & b_{xx} & 0 & 0 & b_{yy} & b_{xy} & b_{yz} & b_{zz} & b_{xz} & 0 & 0 & 0 & 0 \\
0 & b_{xx} & 0 & b_{xy} & 0 & b_{xz} & 0 & b_{yy} & 0 & 0 & b_{yz} & 0 & 0 & 0 & b_{zz} \\
0 & 0 & 0 & 0 & 0 & b_{xx} & 0 & 0 & b_{yy} & b_{yz} & b_{xy} & 0 & 0 & b_{zz} & b_{xz} \\
0 & 0 & 0 & 0 & b_{xx} & 0 & 0 & 0 & 0 & b_{yy} & 0 & b_{zz} & b_{xz} & b_{yz} & b_{xy} \\
0 & 0 & b_{xx} & 0 & b_{xz} & b_{xy} & 0 & 0 & 0 & 0 & b_{yy} & 0 & b_{zz} & 0 & b_{yz} \\
0 & 0 & 0 & 0 & c_{xx} & 0 & 0 & 0 & 0 & c_{yy} & 0 & c_{zz} & c_{xz} & c_{yz} & c_{xy} \\
0 & 0 & c_{xx} & 0 & c_{xz} & c_{xy} & 0 & 0 & 0 & 0 & c_{yy} & 0 & c_{zz} & 0 & c_{yz} \\
0 & 0 & 0 & 0 & 0 & c_{xx} & 0 & 0 & c_{yy} & c_{yz} & c_{xy} & 0 & 0 & c_{zz} & c_{xz} \\
0 & c_{xx} & 0 & c_{xy} & 0 & c_{xz} & 0 & c_{yy} & 0 & 0 & c_{yz} & 0 & 0 & 0 & c_{zz}
\end{bmatrix},$$

where the monomials corresponding to the columns are in order $x^4, x^3y, x^3z, x^2y^2, x^2z^2, x^2yz, y^4, xy^3, y^3z, y^2z^2, xy^2z, z^4, xz^3, yz^3, xyz^2$. Note that a different order of the polynomials P_i gives us a different matrix $M_p(n,m)$.

Now, we are in position to show the relationship between the resultant of the polynomials $P_1, \dots, P_n$ and the determinant of the Macaulay matrix $M_n(n,d)$.

Let $|M_n(n,m)|$ denote the determinant of the matrix $M_n(n,m)$, and $\mathcal{R}(n,m)$ denote the gcd of the n determinants formed in a similar way to matrix $M_n(n,m)$ when $P_1, \dots, P_n$ are arranged in n orders: $\{P_1, \dots, P_n\}$, $\{P_2, \dots, P_n, P_1\}$, $\dots$,

$\{P_{n-1}, P_n, P_1, \ldots, P_{n-2}\}$, $\{P_n, P_1, \ldots, P_{n-1}\}$. Thus,

$$\mathcal{R}(n, m) = \gcd(|\mathbf{M}_n(n,m)_1|, \ldots, |\mathbf{M}_n(n,m)_n|), \tag{3.46}$$

where $|\mathbf{M}_n(n,m)_1|, \ldots, |\mathbf{M}_n(n,m)_n|$ are the determinants of the Macaulay matrices corresponding to the n above arrangements of the polynomials.

Let $\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_n$ be a specialization of $P_1, P_2, \ldots, P_n$, i.e., not all coefficients in $\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_n$ are indeterminates. Also, let $\hat{\mathcal{R}}(n,d)$ be $\mathcal{R}(n,d)$ evaluated at the coefficients of $\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_n$. Then we have the first important property of $\hat{\mathcal{R}}(n,d)$ in the following theorem.

Theorem 3.5 : *A necessary and sufficient condition that the equations $\hat{P}_1 = \hat{P}_2 = \cdots = \hat{P}_n = 0$ have a nontrivial solution is the vanishing of $\hat{\mathcal{R}}(n,d)$.*

Proof : A nonconstructive proof of this theorem is given in [Waerd]. □□

Let $\hat{\mathbf{M}}_n(n,d)$ be $\mathbf{M}_n(n,d)$ evaluated at the coefficients of $\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_n$. Macaulay [Mac16] gives a constructive proof for this theorem by extending the proof of Theorem 3.3 for the general case, but, in our opinion, his proof is incorrect. In this proof he shows that the coefficients of the general member of the module $(\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_n)$ of degree $d-1$ satisfy only one linear relation, whether $\hat{\mathcal{R}}(n,d)$ vanishes or not. He claims that the above result can be obtained by showing that the number N of linearly independent members of the module $(\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_n)$ of degree $d-1$ is one less than the number

$$N_{d-1} = \begin{pmatrix} d+n-2 \\ d-1 \end{pmatrix}$$

of the monomials of $x_1, \ldots, x_n$ of degree $d-1$. But in general $N \neq N_{d-1} - 1$ because $N = rank(\tilde{\mathbf{M}}_n(n, d-1))$, where $\tilde{\mathbf{M}}_n(n, d-1)$ is obtained from $\hat{\mathbf{M}}_n(n, d-1)$

by removing the rows containing a 1, and we know that not all the rows in $\tilde{\mathbf{M}}_n(n, d-1)$ are linearly independent for any particular values of the coefficients of the polynomials $P_1, P_2, \ldots, P_n$.

In his paper [Mac02], Macaulay gives another proof for this theorem, but again his arguments are not constructive. He argues that if $\mathcal{R}(n,d) = 0$, then $|\hat{\mathbf{M}}_n(n,d)|$ vanishes, and consequently the system $\hat{\mathbf{M}}_n(n,d)\mathbf{w} = \mathbf{0}$ has a nontrivial solution $\mathbf{w}$. This is correct. However, he next concludes that $\mathbf{w}$ provides a solution to $P_1 = P_2 = \ldots = P_n = 0$,i.e.,

$$\mathbf{w} = [\hat{x}_1^d, \hat{x}_1^{d-1}\hat{x}_2, \ldots, \hat{x}_2^d, \ldots, \hat{x}_{n-1}\hat{x}_n^{d-1}, \hat{x}_n^d]^T,$$

such that $(\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_{n-1}, \hat{x}_n)$ is a nontrivial solution of the equations $P_1 = P_2 = \cdots = P_n = 0$. The following example illustrates that $(\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_{n-1}, \hat{x}_n)$ is not easy to find.

Example 3.2.3: The polynomials are:

$$\begin{aligned} P_1 &= x^2 + xy + 2xz + yz - z^2 = 0, \\ P_2 &= x^2 + 3xz - y^2 + 2yz - z^2 = 0, \\ P_3 &= x + 2y + z. \end{aligned} \tag{3.47}$$

We have $d_1 = d_2 = 2, d_3 = 1$, and $d = 3$. Thus, we have the system:

$$\begin{bmatrix} xP_1 \\ yP_1 \\ zP_1 \\ xP_2 \\ yP_2 \\ zP_2 \\ xyP_3 \\ xzP_3 \\ yzP_3 \\ z^2P_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & -1 \\ 1 & 0 & 3 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 3 & 0 & -1 & 2 & -1 \\ 0 & 1 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} x^3 \\ x^2y \\ x^2z \\ xy^2 \\ xyz \\ xz^2 \\ y^3 \\ y^2z \\ yz^2 \\ z^3 \end{bmatrix}, \qquad (3.48)$$

where the matrix in (3.48) is the Macaulay matrix $\hat{\mathrm{M}}_3(3,3)$ for (3.47). We know that $\hat{\mathcal{R}}(3,3) = 0$ and the system has a solution $(-3,1,1)$ [Can88]. The rank of this matrix is 8; thus, solving $\hat{\mathrm{M}}_3(3,3)\mathrm{w} = 0$ for w, we have

$$\mathrm{w} = [-14t - 13s,\ 5t + 4s,\ 4t + 5s,\ -2t - s,\ -2s - t,\ -2t - s,\ t,\ s,\ t,\ s]^T,$$

where t, s are indeterminates. The question arises here is, in general, how do we systematically choose the values of s and t for w, which is in the form

$$[x^3,\ x^2y,\ x^2z,\ xy^2,\ xyz,\ xz^2,\ y^3,\ y^2z,\ yz^2,\ z^3]^T.$$

The answer is we do not know. But, with a little bit of luck, if we choose $s = t = 1$ then

$$\mathrm{w} = [-27,\ 9,\ 9,\ -3,\ -3,\ -3,\ 1,\ 1,\ 1,\ 1]^T,$$

and we get the solution of (3.47).

The difficulty in Example 3.2.3 is a consequence of the fact that the solution w has dimension greater than 1. In this case, it is required to show that a solution of the form

$$\mathrm{w} = [\hat{x}_1^d, \hat{x}_1^{d-1}\hat{x}_2, \ldots, \hat{x}_2^d, \ldots, \hat{x}_{n-1}\hat{x}_n^{d-1}, \hat{x}_n^d]^T,$$

where at least one the $\hat{x}_i$'s is not equal zero, can be obtained. This can be done, since by Theorem 3.5 a nontrivial solution to $P_1 = P_2 = \ldots = P_n$ always exists. The matter of its construction, however, is nontrivial and is left as a subject for future research.

The development in the remainder of this section is concerned with finding necessary and sufficient conditions for the *existence* of a solution only. The definition of $\mathcal{R}(n,m)$ given in (3.46) is not practical because we have to find the gcd of n determinants. Thus, we have to explore another approach. From now on, for simplicity, we denote $\mathbf{M}_n(n,m)$ by $\mathbf{M}(n,m)$.

Let

$$|\Delta\mathbf{M}(n,m)| = \frac{|\mathbf{M}(n,m)|}{\mathcal{R}(n,m)} \tag{3.49}$$

for one of the arrangements of these polynomials, say $P_1, \ldots, P_n$. We will show that $\Delta\mathbf{M}(n,m)$ is a particular submatrix of $\mathbf{M}(n,m)$ in the appendix. In addition, the construction of this submatrix is as follows:

For each $\hat{\mathcal{X}}^\pi_{i,m}$, we define its subset

$$\hat{\mathcal{Y}}^\pi_{i,m} = \{x^\alpha \in \hat{\mathcal{X}}^\pi_{i,m} \mid \exists p, q \text{ such that } \alpha_{\pi(p)} \geq d_{\pi(p)} \text{ and } \alpha_{\pi(q)} \geq d_{\pi(q)}\}. \tag{3.50}$$

Thus, set $\hat{\mathcal{Y}}^\pi_{n-1,m}$ is empty. Also, for each set $\hat{\mathcal{Y}}^\pi_{i,m}$, we define a set of monomials $\mathcal{Y}^\pi_{i,m}$ such that

$$\mathcal{Y}^\pi_{i,m} = \{x^\alpha / x_{\pi(i+1)}^{d_{\pi(i+1)}} \mid x^\alpha \in \hat{\mathcal{Y}}^\pi_{i,m}\}. \tag{3.51}$$

Hence, all monomials in $\mathcal{Y}^{\pi}_{i,m}$ are of degree $m - d_{\pi(i+1)}$ and non-reduced in at least one of the variables $x_{\pi(i+2)}, \ldots, x_{\pi(n)}$. In addition, it is not very hard to get the total monomials in the sets $\mathcal{Y}^{\pi}_{i,m}$ [Can88]

$$\Delta N_m = | \bigcup_{i=0}^{n-2} (\mathcal{Y}^{\pi}_{i,m}) | = N_m - \sum_{i=1}^{n} D_{\pi(i)},$$

where

$$D_{\pi(i)} = \sum_{j=1, j \neq i}^{n} d_{\pi(j)}.$$

Let $\Phi^{\pi}_{i,m}$ be the set of polynomials such that

$$\Phi^{\pi}_{i,m} = \{ \sum_{j} b_j x^{\alpha_j} \mid x^{\alpha_j} \in \mathcal{Y}^{\pi}_{i,m} \}.$$

Hence, any polynomial belonging to set $\Phi^{\pi}_{i,m}$ will have the same properties as the monomials belonging to set $\mathcal{Y}^{\pi}_{i,m}$.

Let $\hat{\Phi}^{\pi}_{m}$ be the set of polynomials such that

$$\hat{\Phi}^{\pi}_{m} = \{ \sum_{j} b_j x^{\alpha_j} \mid x^{\alpha_j} \in (\bigcup_{q=0}^{n-1} (\hat{\mathcal{X}}^{\pi}_{q,m} - \hat{\mathcal{Y}}^{\pi}_{q,m})) \}.$$

Then, for $m \leq$ [illegible] any polynomial $\hat{Q}^{\pi}_{m} \in \hat{\Phi}^{\pi}_{m}$ is reduced in at least $n-1$ variables. Again, let $\mathcal{Y}^{\pi}_{i,m} = \mathcal{Y}_{i,m}$, $\hat{\mathcal{Y}}^{\pi}_{i,m} = \hat{\mathcal{Y}}_{i,m}$, $\Phi^{\pi}_{i,m} = \Phi_{i,m}$, and $\hat{\Phi}^{\pi}_{m} = \hat{\Phi}_{m}$, for the identity permutation. $\Phi^{\pi}_{i,m}$ and $\hat{\Phi}^{\pi}_{m}$ are referenced in the appendix.

For each $\mathcal{Y}_{i,d}$, we define a set of polynomials ΔF_i such that

$$\Delta F_i = \mathcal{Y}_{i,d} P_{i+1}(x_1, \ldots, x_n). \tag{3.52}$$

Thus, we can construct a square matrix $\Delta \mathrm{M}(n, m)$ whose columns correspond to the ΔN_m monomials in the $\mathcal{Y}_{i,m}$, and each row of which contains the coefficients of those monomials in some polynomial in ΔF_i.

Referring back to Example 3.2.2, for the construction of the submatrix $\Delta\mathrm{M}(3,4)$, we have

$$\begin{aligned} \hat{\mathcal{Y}}_{0,4} &= \{x^2y^2, x^2z^2\}, \\ \hat{\mathcal{Y}}_{1,4} &= \{y^2z^2\}, \\ \hat{\mathcal{Y}}_{2,4} &= \emptyset. \end{aligned} \tag{3.53}$$

Divide $\hat{\mathcal{Y}}_{0,4}$, $\hat{\mathcal{Y}}_{1,4}$ by x^2, y^2, respectively, to obtain

$$\begin{aligned} \mathcal{Y}_{0,4} &= \{y^2, z^2\}, \\ \mathcal{Y}_{1,4} &= \{z^2\}. \end{aligned} \tag{3.54}$$

Hence, the 3 by 3 matrix $\Delta\mathrm{M}(3,4)$ is

$$\begin{bmatrix} a_{xx} & 0 & a_{zz} \\ 0 & a_{xx} & a_{yy} \\ 0 & b_{xx} & b_{yy} \end{bmatrix}$$

We can see that, $\Delta\mathrm{M}(3,4)$ is independent of the coefficients of $P_3(x,y,z)$.

3.2.4 The u-Resultant

We can use the resultant defined in the previous section to find the solutions of a system of polynomials when the number of solutions is finite. Let $P_1, P_2, \ldots, P_{n-1}$ be $n-1$ homogeneous polynomials in the unknowns $x_1, x_2, \ldots, x_n$. If $(\alpha_1, \ldots, \alpha_n)$ is a solution of $P_1 = P_2 = \cdots = P_n = 0$, then we regard $(\alpha_1, \ldots, \alpha_n)$ and $(c\alpha_1, \ldots, c\alpha_n)$, where $c \neq 0$, as identical solutions. Assume that the resultant $\mathcal{R}_{n-1}$ of the polynomials $P_1, P_2, \ldots, P_{n-1}$ with respect to $x_1, x_2, \ldots, x_{n-2}, x_0$, where x_0 is a homogenizing variable (i.e., $\mathcal{R}_{n-1}$ is a polynomial in x_{n-1}, x_n) does not vanish. If $\mathcal{R}_{n-1} = 0$, we must use the resolvent which is introduced in the next section.

We introduce the linear polynomial with indeterminate coefficients:

$$P_u = x - (u_1x_1 + u_2x_2 + \cdots + u_{n-1}x_{n-1}).$$

Then, we regard $P_1 = P_2 = \ldots = P_{n-1} = P_u = 0$ as a system of equations in the variables $x_1, \ldots, x_{n-1}, x$. Also, let $\mathcal{R}_u$ be the resultant of $P_1, P_2, \ldots, P_{n-1}, P_u$ in the variables $x_0, x_1, x_2, \ldots, x_{n-1}$, where x_0 is a homogenizing variable. Then we obtain a homogeneous polynomial in x whose degree D_n is the product of degrees of the P_i's for $i = 1, \ldots, n-1$. This polynomial is called the *u-resultant* [Mac16] of $P_1, P_2, \ldots, P_{n-1}$.

Now we want to show that we can obtain the solution of $P_1 = \ldots = P_{n-1}$ from their u-resultant. The following theorem confirms it.

Theorem 3.6 : *If $\mathcal{R}_{n-1} \neq 0$, then the u-resultant $\mathcal{R}_u$ factors completely over the extension field of the coefficients of P_i's into linear factors of the form*

$$\hat{x}^{(i)}x - (s_1^{(i)}u_1 + s_2^{(i)}u_2 + \cdots + s_{n-1}^{(i)}u_{n-1}),$$

and for each factor, $x_1 = s_1^{(i)}$, $x_2 = s_2^{(i)}$, ..., $x_{n-1} = s_{n-1}^{(i)}$, $x_n = \hat{x}^{(i)}$, is a solution of $P_1 = P_2 = \ldots = P_{n-1} = 0$.

Proof :[Mac16] Let $P_i^{(n)}$ be P_i with the substitutions $x_n = 0$; we have

$$\mathcal{R}_{n-1} = \mathcal{R}_n^{(0)} x_{n-1}^{D_n} + \cdots,$$

where $\mathcal{R}_n^{(0)}$ is the resultant of $P_1^{(n)}, P_2^{(n)}, \ldots, P_{n-1}^{(n)}$ with respect to $x_1, x_2, \ldots, x_{n-1}$, and does not vanish since $\mathcal{R}_{n-1}$ does not vanish. To each solution of $x_{n-1} = x_{n-1}^{(i)}$ of $\mathcal{R}_{n-1} = 0$, we have a corresponding solution $(x_1^{(i)}, x_2^{(i)}, \ldots, x_{n-1}^{(i)})$ of the equations $P_1 = P_2 = \ldots = P_{n-1} = 0$ for $x_1, x_2, \ldots, x_{n-1}$, by Theorem 3.5. There are D_n solutions altogether.

Similarly,

$$\mathcal{R}_u = \mathcal{R}_n^{(0)} x^{D_n} + \cdots$$

where $\mathcal{R}_n^{(0)} \neq 0$. Hence, to each of the D_n solutions $x = \hat{x}^{(i)}$ of $\mathcal{R}_u = 0$, there corresponds a solution $(\hat{x}_1^{(i)}, \hat{x}_2^{(i)}, \ldots, \hat{x}_{n-1}^{(i)}, \hat{x}^{(i)})$ of the equations $P_1 = P_2 = \ldots = P_{n-1} = P_u = 0$, by Theorem 3.5. In addition, the D_n solutions $(\hat{x}_1^{(i)}, \hat{x}_2^{(i)}, \ldots, \hat{x}_{n-1}^{(i)})$ must be the same as those obtained by solving $\mathcal{R}_{n-1} = 0$. Furthermore, if $\hat{x}^{(i)} \neq 0$, then set $\hat{x}_j^{(i)}$ to $\hat{x}_j^{(i)}/\hat{x}^{(i)}$ for $j = 1, \ldots, n-1$, and $\hat{x}^{(i)} = 1$. Thus,

$$\hat{x}^{(i)} x = u_1 s_1^{(i)} + u_2 s_2^{(i)} + \cdots + u_{n-1} s_{n-1}^{(i)},$$

where $s_1^{(i)} = \hat{x}_1^{(i)}$, $s_2^{(i)} = \hat{x}_2^{(i)}, \ldots, s_{n-1}^{(i)} = \hat{x}_{n-1}^{(i)}$ are independent of $u_1, u_2, \ldots, u_{n-1}$, or

$$\mathcal{R}_u = \mathcal{R}_n^{(0)} \prod_{i=1}^{D_n} (\hat{x}^{(i)} x - u_1 s_1^{(i)} - u_2 s_2^{(i)} - \cdots - u_{n-1} s_{n-1}^{(i)}).$$

Therefore, $\mathcal{R}_u$ is a product of D_n factors which are linear in $u_1, u_2, \ldots, u_{n-1}, x$ and the coefficients of $u_1, u_2, \ldots, u_{n-1}, x$ in each factor supply a solution of the equations $P_1 = P_2 = \ldots = P_{n-1} = 0$. □□

Note that Van der Waerden [Waerd] uses

$$P_u = u_1 x_1 + u_2 x_2 + \cdots + u_n x_n.$$

Then

$$\mathcal{R}_u = \mathcal{R}_n^{(0)} \prod_{i=1}^{D_n} (u_1 s_1^{(i)} + u_2 s_2^{(i)} + \cdots + u_n s_n^{(i)}).$$

Now, we give an example to illustrate the above concepts.

Example 3.2.4:[Can88] Using the notation in [Waerd], we have the following equations :

$$P_1 \;=\; x_1^2 + x_1 x_2 + 2 x_1 x_3 + x_2 x_3 - x_3^2 = 0,$$

$$
\begin{aligned}
P_2 &= x_1^2 + 3x_1x_3 - x_2^2 + 2x_2x_3 - x_3^2 = 0, \\
P_u &= u_1x_1 + u_2x_2 + u_3x_3 = 0.
\end{aligned}
$$

Then

$$\mathcal{R}_u = -(u_1 - u_2 + u_3)(-3u_1 + u_2 + u_3)(u_2 + u_3)(u_1 - u_2).$$

Thus, there are $D_3 = 4$ solutions, $(1,-1,1), (-3,1,1), (0,1,1)$ and $(1,-1,0)$, for $P_1 = P_2 = 0$.

Using Macaulay's notation, we have

$$
\begin{aligned}
P_1 &= x_1^2 + x_1x_2 + 2x_3x_1x_0 + x_3x_2x_0 - x_3^2x_0^2 = 0, \\
P_2 &= x_1^2 + 3x_3x_1x_0 - x_2^2 + 2x_3x_2x_0 - x_3^2x_0^2 = 0, \\
P_u &= xx_0 - u_1x_1 - u_2x_2 = 0,
\end{aligned}
$$

where x_1, x_2, x_0 are the variables. Then

$$\mathcal{R}_u = x_3(x - x_3u_2)(-u_1 + u_2)(x + 3x_3u_1 - x_3u_2)(x - x_3u_1 + x_3u_2).$$

Thus, there are $D_3 = 4$ solutions $(0,1,1), (-1,1,0), (-3,1,1)$ and $(1,-1,1)$, for $P_1 = P_2 = 0$.

3.3 The Resolvent

For the completeness of elimination theory, we introduce the concept of resolvent in this section. Namely, the method of solving k equations, $P_1 = P_2 = \ldots = P_k = 0$, in n unknowns, $x_1, x_2, \ldots, x_n$, whether k is greater or less than n, is explained. The polynomials given here are not necessarily homogeneous. In the case of homogeneous polynomials, note that we cannot use the concept of resultant in the previous section to solve all of these problems. That is, the concept of resultant fails when either $k > n$ or the system has an infinite number of solutions. This method is due to Kronecker [Mac16]. The solutions we seek are

(i) those, if any, which exist for x_1 when $x_2, x_3, \ldots, x_n$, have arbitrary values;

(ii) those which exist for x_1, x_2 not included in (i), when $x_3, x_4, \ldots, x_n$, have arbitrary values;

(iii) those which exist for x_1, x_2, x_3 not included in (i) or (ii), when $x_4, x_5, \ldots, x_n$, have arbitrary values; and so on.

Also, for the purpose of geometric modeling, i.e., the curve/curve intersection problem, we are particularly interested in the special resolvent for three cubic polynomials in one variable [Goldm85].

3.3.1 The General Case

In this section we give a definition of the complete resolvent, $\mathcal{D}$, of $P_1, P_2, \ldots, P_k$, and provide a procedure for its determination. We also show that any solution of $\mathcal{D} = 0$ is a solution of $P_1 = P_2 = \ldots = P_k = 0$ and vice versa.

Let $k = k_0$ and $P_i^{(0)} = P_i$, for $i = 1, \ldots, k_0$. We treat $P_1^{(0)}, P_2^{(0)}, \ldots, P_{k_0}^{(0)}$ as polynomials in x_1. Find

$$D^{(0)} = \gcd(P_1^{(0)}(x_1), P_2^{(0)}(x_1), \ldots, P_{k_0}^{(0)}(x_1)).$$

If $D^{(0)}$ does not involve x_1 then set it to be 1.

Set $Q_i^{(0)} = P_i^{(0)}/D^{(0)}$, for $i = 1, 2, \ldots, k_0$. Then $Q_1^{(0)}, Q_2^{(0)}, \ldots, Q_{k_0}^{(0)}$ have no common factor involving x_1, and

$$\begin{aligned} A_1^{(0)} &= \lambda_1 Q_1^{(0)} + \lambda_2 Q_2^{(0)} + \cdots + \lambda_{k_0} Q_{k_0}^{(0)}, \\ A_2^{(0)} &= \mu_1 Q_1^{(0)} + \mu_2 Q_2^{(0)} + \cdots + \mu_{k_0} Q_{k_0}^{(0)}, \end{aligned}$$

where λ's and μ's are arbitrary quantities, do not have a common factor involving x_1. Regarding them as two polynomials in a single variable x_1, we calculate their resultant, $\mathcal{R}^{(0)}$, and arrange it in the form

$$M_1 P_1^{(1)} + M_2 P_2^{(1)} + \cdots + M_{k_1} P_{k_1}^{(1)},$$

where $M_1, M_2, \ldots, M_{k_1}$ are different power products of λ's and μ's, and $P_1^{(1)}, P_2^{(1)}, \ldots, P_{k_1}^{(1)}$ are polynomials in $x_2, x_3, \ldots, x_n$ not involving the λ's and μ's. We will stop if $k_1 = 0$, and set $D^{(1)} = \ldots = D^{(n-1)} = 1$.

Again, treat $P_1^{(1)}, P_2^{(1)}, \ldots, P_{k_1}^{(1)}$ as [illegible] in x_2, find

$$D^{(1)} = \gcd(P_1^{(1)}(x_2), \; [illegible] \; \ldots, P_{k_1}^{(1)}(x_2)),$$

and set $Q_i^{(1)} = P_i^{(1)}/D^{(1)}$ $(i = 1, 2, \ldots, k_1$ [illegible]en find the resultant, $\mathcal{R}^{(1)}$, of

$$\begin{aligned} A_1^{(1)} &= \lambda_1 Q_1^{(1)} + \lambda_2 Q_2^{(1)} + \cdots + \lambda_{k_1} Q_{k_1}^{(1)} \quad \text{and} \\ A_2^{(1)} &= \mu_1 Q_1^{(1)} + \mu_2 Q_2^{(1)} + \cdots + \mu_{k_1} Q_{k_1}^{(1)}, \end{aligned}$$

and arrange it in the form

$$M_1 P_1^{(2)} + M_2 P_2^{(2)} + \cdots + M_{k_2} P_{k_2}^{(2)}$$

as before, where $P_1^{(2)}, P_2^{(2)}, \ldots, P_{k_2}^{(2)}$ are polynomials in $x_3, x_4, \ldots, x_n$. Continuing the above process, we get the following series in succession :

$$\begin{array}{llll} P_1^{(0)}, P_2^{(0)}, \ldots, P_{k_0}^{(0)} & \text{with gcd } D^{(0)} & \text{and} & Q_1^{(0)}, Q_2^{(0)}, \ldots, Q_{k_0}^{(0)} \\ P_1^{(1)}, P_2^{(1)}, \ldots, P_{k_1}^{(1)} & \text{with gcd } D^{(1)} & \text{and} & Q_1^{(1)}, Q_2^{(1)}, \ldots, Q_{k_1}^{(1)} \\ \ldots & \ldots & & \ldots \\ P_1^{(n-1)}, P_2^{(n-1)}, \ldots, P_{k_{n-1}}^{(n-1)} & \text{with gcd } D^{(n-1)} & \text{and} & Q_1^{(n-1)}, Q_2^{(n-1)}, \ldots, Q_{k_{n-1}}^{(n-1)}. \end{array}$$

Note that we stop the process if $k_i = 0$, and set $D^{(i)} = \ldots = D^{(n-1)} = 1$. Let $\mathcal{D} = D^{(0)} D^{(1)} \ldots D^{(n-1)}$, then we have a formal definition of resolvent.

Definition 3.6 *: $\mathcal{D}$ is called the complete resolvent of the equations $P_1 = P_2 = \cdots = P_k = 0$ and of the module $(P_1, P_2, \ldots, P_k)$. $D^{(i-1)}$ is called the resolvent of rank i, and any factor of $D^{(i-1)}$ is called a partial resolvent of rank i.*

Now we will prove an important property of the resolvent, which shows us how to obtain the solutions of $P_1 = \ldots = P_k = 0$ from $\mathcal{D} = 0$.

Theorem 3.7 . *Any solution of $P_1 = P_2 = \cdots = P_k = 0$ is a solution of $\mathcal{D} = 0$ and vice versa.*

Proof: Macaulay [Mac16] provided a sketch proof of this theorem. Any solution of $P_1 = P_2 = \cdots = P_k = 0$ is a solution of $D^{(0)} = 0$ or of $Q_1^{(0)} = Q_2^{(0)} = \cdots = Q_{k_0}^{(0)} = 0$. And any solution of $Q_1^{(0)} = Q_2^{(0)} = \cdots = Q_{k_0}^{(0)} = 0$, is a solution of $P_1^{(1)} = P_2^{(1)} = \cdots = P_{k_1}^{(1)} = 0$, since $\mathcal{R}^{(0)} = 0$, and $P_i^{(1)} M_i = 0$, for $i = 1, \ldots, k_1$, where M_i are nonzero monomials in λ_i's and μ_i's. Thus, any solution of $Q_1^{(0)} = Q_2^{(0)} = \cdots = Q_{k_0}^{(0)} = 0$, is a solution of $D^{(1)} = 0$ or of $Q_1^{(1)} = Q_2^{(1)} = \cdots = Q_{k_1}^{(1)} = 0$. Hence, any solution of $P_1 = P_2 = \cdots = P_k = 0$ is a solution of $D^{(0)} = 0$ or $D^{(1)} = 0$ or $Q_1^{(1)} = Q_2^{(1)} = \cdots = Q_{k_1}^{(1)} = 0$. Proceeding in a similar way we find that any solution of $P_1 = P_2 = \cdots = P_k = 0$ is a solution of $D^{(0)} D^{(1)} \ldots D^{(n-1)} = 0$, since $Q_1^{(n-1)}, Q_2^{(n-1)}, \ldots, Q_{k_{n-1}}^{(n-1)}$ are univariate polynomials in x_n, and have no common factor.

Conversely, suppose we have a solution of $\mathcal{D} = 0$, i.e., a solution of $D^{(i)} = 0$, for $0 \leq i \leq n-1$. We will consider the case of $i = 2$, since the other cases are similar.

Suppose $\alpha_3, x_4, \ldots, x_n$ is any solution of $D^{(2)} = 0$, then it also is a solution of the equations $P_1^{(2)} = P_2^{(2)} = \cdots = P_{k_2}^{(2)} = 0$. It follows that the resultant $\mathcal{R}^{(1)}$ with respect to x_2 vanishes when $x_3 = \alpha_3$. This means the polynomials $A_1^{(1)}$ and $A_2^{(1)}$

have a common root $x_2 = \alpha_2$, or in other words, $Q_1^{(1)} = Q_2^{(1)} = \cdots = Q_{k_1}^{(1)} = 0$ have a solution with $x_2 = \alpha_2$. Thus, $P_1^{(1)} = P_2^{(1)} = \cdots = P_{k_1}^{(1)} = 0$ have a solution $\alpha_2, \alpha_3, x_4, \ldots, x_n$. And by the same reasoning, the equations $P_1 = P_2 = \cdots = P_k = 0$ have a solution $\alpha_1, \alpha_2, \alpha_3, x_4, \ldots, x_n$. Similarly, to any solution of $D^{(0)}D^{(1)} \ldots D^{(n-1)} = 0$, say a solution $\alpha_i, x_{i+1}, \ldots, x_n$ of $D^{(i-1)} = 0$, there corresponds a solution $\alpha_1, \alpha_2, \ldots, \alpha_i, x_{i+1}, \ldots, x_n$ of the equations $P_1 = P_2 = \cdots = P_k = 0$. Hence, from the solution of a single equation $\mathcal{D} = D^{(0)}D^{(1)} \ldots D^{(n-1)} = 0$ we can get all solutions of the system $P_1 = P_2 = \cdots = P_k = 0$ since all the solutions of the latter satisfy the former. □□

From this theorem, we can easily prove the following corollary.

Corollary 3.8 : *The equations $P_1 = P_2 = \cdots = P_k = 0$ have no solution if and only if the complete resolvent $\mathcal{D} = 1$.*

Now, we give an example to illustrate the above concepts.

Example 3.3.1 : Let

$$\begin{aligned} P_1 &= (t-1)(2t^2+t+4) - x = 2t^3 - t^2 + 3t - (4+x), \\ P_2 &= (t-1)(t^2-t+1) - y = t^3 - 2t^2 + 2t - (1+y), \\ P_3 &= (t-1)^3 - z = t^3 - 3t^2 + 3t - (1+z), \end{aligned}$$

be three polynomials in t. Thus, $\gcd(P_1, P_2, P_3) = 1$ and

$$\begin{aligned} A_1 &= (2\lambda_1 + \lambda_2 + \lambda_3)t^3 - (\lambda_1 + 2\lambda_2 + 3\lambda_3)t^2 + (3\lambda_1 + 2\lambda_2 + 3\lambda_3)t - \\ &\quad ((4+x)\lambda_1 + (1+y)\lambda_2 + (1+z)\lambda_3), \\ A_2 &= (2\mu_1 + \mu_2 + \mu_3)t^3 - (\mu_1 + 2\mu_2 + 3\mu_3)t^2 + (3\mu_1 + 2\mu_2 + 3\mu_3)t - \\ &\quad ((4+x)\mu_1 + (1+y)\mu_2 + (1+z)\mu_3), \end{aligned}$$

The resultant of these polynomials is too big to give in here, because there are about 100 polynomials in x, y, and z.

From the construction of the resolvent $\mathcal{D}$, we can see that this method of solving system of polynomials equations is impractical because the number of polynomials in each step grows exponentially. Thus, we only apply this technique in some restricted situations and have to use some tricks. For a system of three independent cubic polynomials in one variable where the constant terms are symbolic, we have a very good technique to find the resolvent. We explain this technique in detail in the next section.

3.3.2 Special Resolvent of Three Independent Cubic Polynomials

In this section we present a simple version of resolvent described in the previous section. The resolvent presented here is in the sense of the *resultant system* [Waerd] rather than in the sense of the *partial resolvent* [Macl6]. This result will be used in the implementation of an algorithm for the curve/curve intersection problem. Also, it is easy to show that $F_1 = a_1(t) - d_1(t)x, F_2 = b_1(t) - d_1(t)y$ and $F_3 = c_1(t) - d_1(t)z$, where $a_1(t), b_1(t), c_1(t)$ and $d_1(t)$ are cubic polynomials, are linearly independent. In fact, $\frac{a_1(t)}{d_1(t)}, \frac{b_1(t)}{d_1(t)}, \frac{c_1(t)}{d_1(t)}$ constitute a 3D parametric rational cubic polynomial curve (see Chapter 2). Thus, in this section, we deal with 3 linearly independent cubic polynomials only.

Let

$$\begin{aligned} P_1 &= a_3t^3 + a_2t^2 + a_1t + a_0, \\ P_2 &= b_3t^3 + b_2t^2 + b_1t + b_0, \qquad (3.55) \end{aligned}$$

$$P_3 \;=\; c_3t^3 + c_2t^2 + c_1t + c_0,$$

be three independent cubic polynomials, where at least one of a_3, b_3, c_3 is nonzero. Notice that these polynomials have at most one common root since if they have two common roots, they are linearly dependent. We want to find necessary and sufficient conditions for these polynomials to have a common root. In addition, we want to find the common root, when one exists, without actually solving for the roots of all three polynomials.

In [Goldm85], Goldman uses the standard properties of determinants to eliminate the t^3 and t^2 terms from the original polynomials. This allows him to replace the cubic polynomials P_1, P_2, P_3 by three linear polynomials F_1, F_2, F_3 which have a common root if and only if P_1, P_2, P_3 have a common root.

Using vector notation, let

$$\mathbf{v}_k = [a_k, b_k, c_k]^T, \quad \text{for } k = 0,1,2,3 \quad \text{and} \quad \mathbf{p} = \mathbf{v}_3t^3 + \mathbf{v}_2t^2 + \mathbf{v}_1t + \mathbf{v}_0.$$

Then by the construction

$$\mathbf{p} = [P_1, P_2, P_3]^T, \quad \text{and} \quad \mathbf{p}(t_0) = 0 \Longleftrightarrow P_1(t_0) = P_2(t_0) = P_3(t_0) = 0.$$

Let $|\mathbf{v}_i, \mathbf{v}_j, \mathbf{v}_k|$ denotes the determinant of a 3 by 3 matrix whose columns are the 3–elements vectors $\mathbf{v}_i, \mathbf{v}_j, \mathbf{v}_k$. Define

$$\begin{aligned} F_1 &= |\mathbf{v}_3, \mathbf{v}_2, \mathbf{p}|. \\ F_2 &= |\mathbf{v}_3, \mathbf{v}_2t + \mathbf{v}_1, \mathbf{p}|. \\ F_3 &= |\mathbf{v}_3t + \mathbf{v}_2, \mathbf{v}_1, \mathbf{p}|. \end{aligned} \tag{3.56}$$

Then clearly

$$\mathbf{p}(t_0) = 0 \Longrightarrow F_1(t_0) = F_2(t_0) = F_3(t_0) = 0.$$

It is easy to see that the F_i's are linear in t, in fact,

$$\begin{aligned} F_1 &= |\mathbf{v}_3,\mathbf{v}_2,\mathbf{v}_1|t + |\mathbf{v}_3,\mathbf{v}_2,\mathbf{v}_0|. \\ F_2 &= |\mathbf{v}_3,\mathbf{v}_2,\mathbf{v}_0|t + |\mathbf{v}_3,\mathbf{v}_1,\mathbf{v}_0|. \\ F_3 &= |\mathbf{v}_3,\mathbf{v}_1,\mathbf{v}_0|t + |\mathbf{v}_2,\mathbf{v}_1,\mathbf{v}_0|. \end{aligned} \tag{3.57}$$

To show (3.57), we just use the fact that the determinant of any matrix which has 2 identical columns is zero and

$$|\mathbf{v}_1,\ldots,\mathbf{v}_n,\sum_{i=1}^{m}\hat{\mathbf{v}}_i| = \sum_{i=1}^{m}|\mathbf{v}_1,\ldots,\mathbf{v}_n,\hat{\mathbf{v}}_i|.$$

Next, if P_1, P_2, P_3 are linearly independent and F_1, F_2, F_3 have a common root at $t = t_0$, then $|\mathbf{v}_3,\mathbf{v}_2,\mathbf{v}_1| \neq 0$. This can be seen by substituting $t = t_0$ into (3.57), so we have

$$\begin{aligned} F_1(t_0) &= |\mathbf{v}_3,\mathbf{v}_2,\mathbf{v}_1|t_0 + |\mathbf{v}_3,\mathbf{v}_2,\mathbf{v}_0| = 0, \\ F_2(t_0) &= |\mathbf{v}_3,\mathbf{v}_2,\mathbf{v}_0|t_0 + |\mathbf{v}_3,\mathbf{v}_1,\mathbf{v}_0| = 0, \\ F_3(t_0) &= |\mathbf{v}_3,\mathbf{v}_1,\mathbf{v}_0|t_0 + |\mathbf{v}_2,\mathbf{v}_1,\mathbf{v}_0| = 0. \end{aligned} \tag{3.58}$$

Now, if $|\mathbf{v}_3,\mathbf{v}_2,\mathbf{v}_1| = 0$, then it follows immediately that $|\mathbf{v}_i,\mathbf{v}_j,\mathbf{v}_k| = 0$ for all i,j,k. Thus, P_1, P_2, P_3 are linearly dependent. This contradicts the assumption that P_1, P_2, P_3 are linearly independent. Hence, $|\mathbf{v}_3,\mathbf{v}_2,\mathbf{v}_1| \neq 0$.

Now, we are in position to show the relationship between $\mathbf{p}(t_0)$ and $F_1(t_0), F_2(t_0)$ in

Lemma 3.9 *[Goldm85]. Suppose that $P_1(t), P_2(t), P_3(t)$ are linearly independent cubic polynomials. Then the following two statements are equivalent:*

(1) $\mathbf{p}(t_0)|\mathbf{v}_3$, *i.e.,* $\mathbf{p}(t_0) = d\mathbf{v}_3$ *where d is a constant.*

(2) $F_1(t_0) = F_2(t_0) = 0$.

Proof : See [Goldm85]. □□

In addition, we have a stronger statement about the relationship between the root of the linear polynomials F_1, F_2, F_3 and the root of the linearly independent cubic polynomials P_1, P_2, P_3 as follows:

$$P_1(t_0) = P_2(t_0) = P_3(t_0) = 0 \Longleftrightarrow F_1(t_0) = F_2(t_0) = F_3(t_0) = 0.$$

Thus, the polynomials P_1, P_2, P_3 have a common root if and only if

$$\begin{aligned}
R_1(\mathrm{p}) &= \begin{vmatrix} |\mathrm{v}_3, \mathrm{v}_2, \mathrm{v}_1| & |\mathrm{v}_3, \mathrm{v}_2, \mathrm{v}_0| \\ |\mathrm{v}_3, \mathrm{v}_2, \mathrm{v}_0| & |\mathrm{v}_3, \mathrm{v}_1, \mathrm{v}_0| \end{vmatrix} = 0, \\
R_2(\mathrm{p}) &= \begin{vmatrix} |\mathrm{v}_3, \mathrm{v}_2, \mathrm{v}_1| & |\mathrm{v}_3, \mathrm{v}_2, \mathrm{v}_0| \\ |\mathrm{v}_3, \mathrm{v}_1, \mathrm{v}_0| & |\mathrm{v}_2, \mathrm{v}_1, \mathrm{v}_0| \end{vmatrix} = 0 \qquad (3.59) \\
R_3(\mathrm{p}) &= \begin{vmatrix} |\mathrm{v}_3, \mathrm{v}_2, \mathrm{v}_0| & |\mathrm{v}_3, \mathrm{v}_1, \mathrm{v}_0| \\ |\mathrm{v}_3, \mathrm{v}_1, \mathrm{v}_0| & |\mathrm{v}_2, \mathrm{v}_1, \mathrm{v}_0| \end{vmatrix} = 0,
\end{aligned}$$

since two linear polynomials have a common root if and only if they are linearly dependent. Here, $R_1(\mathrm{p})$=0, $R_2(\mathrm{p})$=0, and $R_3(\mathrm{p})$=0 are the necessary and sufficient conditions that three pairs of linear polynomials in t, $(F_1, F_2), (F_1, F_3)$ and (F_2, F_3), have a common root. The determinants $R_1(\mathrm{p}), R_2(\mathrm{p}), R_3(\mathrm{p})$ are called the *special resolvents* of $\mathrm{p}(t)$. Note that these determinants are equivalent to the $P_1^{(1)}, P_2^{(1)}, \ldots, P_{k_1}^{(1)}$ in the general case. That is, the vanishing of these determinants is a necessary and sufficient condition for $\mathrm{p}(t)$ to have a solution. From now on we call these determinants the resolvents of $\mathrm{p}(t)$.

Now we can see that if a common root t_0 exists then $|\mathrm{v}_3, \mathrm{v}_2, \mathrm{v}_1| \neq 0$. Conversely, if $|\mathrm{v}_3, \mathrm{v}_2, \mathrm{v}_1| \neq 0$ and $R_1(P) = R_2(P) = 0$ then a common root t_0 exists.

Hence, we can easily obtain this common root by solving for it in $F_1 = 0$. It follows that

$$t_0 = -\frac{|\mathbf{v}_3, \mathbf{v}_2, \mathbf{v}_0|}{|\mathbf{v}_3, \mathbf{v}_2, \mathbf{v}_1|}. \tag{3.60}$$

Equation (3.60) is called the inversion equation of $\mathbf{p}(t_0)$.

Going back to Example 3.3.1, we have the following vectors :

$$\begin{aligned}
\mathbf{v}_0 &= [-(4+x), -(1+y), -(1+z)]^T, \\
\mathbf{v}_1 &= [3, 2, 3]^T, \\
\mathbf{v}_2 &= [-1, -2, -3]^T, \\
\mathbf{v}_3 &= [2, 1, 1]^T.
\end{aligned}$$

Then we have the following determinants:

$$\begin{aligned}
|\mathbf{v}_3, \mathbf{v}_2, \mathbf{v}_0| &= x - 5y + 3z + 2, \\
|\mathbf{v}_3, \mathbf{v}_2, \mathbf{v}_1| &= -2, \\
|\mathbf{v}_3, \mathbf{v}_1, \mathbf{v}_0| &= -x + 3y - z - 2, \\
|\mathbf{v}_2, \mathbf{v}_1, \mathbf{v}_0| &= 6y - 4z + 2.
\end{aligned}$$

Hence, the resolvents of the system are:

$$\begin{aligned}
R_1(\mathbf{p}) &= -x^2 + 10xy - 6xz - 25y^2 + 30yz - 9z^2 - 2x + 14y - 10z, \\
R_2(\mathbf{p}) &= x^2 - 8xy + 4xz + 15y^2 - 14yz + 3z^2 + 4x - 28y + 16z, \\
R_3(\mathbf{p}) &= -x^2 + 12xy - 6xz - 39y^2 + 44yz - 13z^2 - 2x + 14y - 6z.
\end{aligned}$$

We can see that one of the solutions for the above system is $x = y = z = 0$. Thus, $P_1 = P_2 = P_3 = 0$ in this example, with $x = y = z = 0$, has a common root at

$$t_0 = -\frac{|\mathbf{v}_3, \mathbf{v}_2, \mathbf{v}_0|}{|\mathbf{v}_3, \mathbf{v}_2, \mathbf{v}_1|} = \frac{-2}{-2} = 1.$$

Comparing with the method to find the resolvent in the previous section, we have the optimal set of resolvents for three linearly independent cubic polynomials. In this case, we have 3 resolvents of degree 2 in x, y, z. In addition, we can get the common root of the system easily.

3.4 The Gröbner Basis

In his Ph.D. thesis, Buchberger [Buch65] introduced the concept of a standard basis of a polynomial ideal, which he named after his supervisor, Gröbner. In [Buch65] and [Buch70] he presented an algorithm for computing such a basis. The notion of Gröbner basis is refined and analyzed in [Buch76a] and [Buch76b], after which it became more widely known as an important constructive technique in polynomial ideal theory. There are many works such as [Lazard, Buch83, Buch85] to further explained Gröbner basis theoretically. Czapor [Czapor] used a heuristic approach to construct a Gröbner basis for a set of polynomials faster. Application of these bases have been also developed recently in curve and surface intersection evaluation [Hoffm88, Neff88].

We want to consider the following problem: Given a polynomial G, is it in the ideal $< \mathcal{P} >$, where $\mathcal{P} = \{P_1, \ldots, P_k\}$, i.e., can it be written in the form $G = Q_1P_1 + P_2Q_2 + \ldots + P_kQ_k$, where the Q_i's are some polynomials. We will show that this problem can be solved algorithmically by using the Gröbner basis. Furthermore, the theory of Gröbner basis also provides an effective mechanism for solving for the roots of $P_1 = \ldots = P_k = 0$.

In this section, we will introduce the concept of a standard basis for a polynomial ideal and present the basic algorithm, known as Buchberger's algorithm, to construct such a basis. Also, after computing the Gröbner basis of the set of algebraic equations, we give the criteria for them to have nontrivial solutions.

3.4.1 Orderings and Leading Terms

We need a notation for "this polynomial is simpler than that one". We introduce an ordering on the terms and declare F to be more complicated than G if the most complicated term in F is later in this ordering than the most complicated term in G.

Define the set of n-variate terms by

$$\mathcal{T}_n = \{x^\alpha | \alpha \in Z^n\}.$$

Then a *total* ordering $\prec_T$ on $\mathcal{T}_n$ satisfies

(1) $1 \prec_T t$,

(2) $su \prec_T tu$, whenever $s \prec_T t$,

for all $s, t, u \in \mathcal{T}_n$. Any order satisfying the above conditions will suffice. However, in practice one of the following two is almost always chosen.

Lexicographic term ordering is defined by

$$s = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \prec_L x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n} = t \Longleftrightarrow$$

$$\exists i \quad \text{such that} \;\; \alpha_i < \beta_i \;\; \text{and} \; \alpha_j = \beta_j \;\; \text{for} \;\; 1 \leq j < i.$$

Note that this establishes the precedence of the variables

$$x_n \prec_L x_{n-1} \prec_L \dots \prec_L x_2 \prec_L x_1$$

in the ring $\mathcal{K}[x_1, \dots, x_n]$. In the case of terms in $[x, y, z]$ for example

$$1 \prec_L z \prec_L z^2 \prec_L \dots \prec_L y \prec_L yz \prec_L \dots \prec_L x \prec_L xy \prec_L \dots.$$

On the other hand, *graduated* (or *total degree*) term ordering is defined by

$$s \prec_G t \iff$$

$$deg(s) < deg(t), \quad \text{or} \quad deg(s) = deg(t) \quad \text{and}$$

$$\exists i \quad \text{such that} \quad \alpha_i > \beta_i \text{ and } \alpha_j = \beta_j \text{ for } i < j \leq n.$$

That is, terms of the same degree are "graduated" using an inverse lexicographic ordering. For terms in $[x, y, z]$, we have

$$1 \prec_G z \prec_G y \prec_G x \prec_G z^2 \prec_G yz \prec_G y^2 \prec_G xz \prec_G xy \prec_G x^2 \prec_G \cdots.$$

Every term in a polynomial G consists of a coefficient and a power product. The term whose power product is largest with respect to the ordering $\prec_T$ is called the *leading term* of G, written $lt(G)$. The leading term consists of the *leading coefficient, lcf(G)*, and the *leading power product, lpp(G)*. From now on, when we say that the polynomial F is *simpler* than the polynomial G with respect to lexicographic or graduated ordering, respectively, we mean *lpp(F)$\prec_L$lpp(G)*, or *lpp(F)$\prec_G$lpp(G)*, respectively.

Also, define the leading term of a set of polynomials $P_1, \ldots, P_n$, $lt(P_1, \ldots, P_n)$ to be the *least common multiple* of the leading term of each polynomial.

Example 3.4.1: Let Q be the field of rational numbers. Referring back to Example 3.2.2, let the set of polynomials of $Q[x, y, z]$ be specialized as follows:

$$\begin{aligned} P_1 &= 8x^2 - 14xy + 2xz + 3y^2 + 2yz - z^2, \\ P_2 &= 6xy - 6xz - 9y^2 + 6yz - z^2, \\ P_3 &= 2x^2 - 9xy + xz + 9y^2 - 6yz. \end{aligned}$$

Then, with respect to the lexicographic ordering, we have

$$lt(P_1) = 8x^2, \quad lpp(P_2) = xy, \quad lcf(P_3) = 2, \quad \text{and} \quad lt(P_1, P_2, P_3) = 24x^2y.$$

3.4.2 Gröbner Basis

Let $\mathcal{F}$ be a field. We start this section with the notion of *reduction.*

Definition 3.7 *: A polynomial $F \in \mathcal{F}[x_1, \ldots, x_n]$ reduces with respect to Q (and with respect to a fixed ordering) if there exists a monomial in F which is divisible by $lpp(Q)$.*

In particular, if

$$F = ct + R \quad \text{where} \quad c \in \mathcal{F},\ t \in \mathcal{T}_n,\ R \in \mathcal{F}[x_1, \ldots, x_n]$$

$$\text{and} \quad t = u\ lpp(Q), \quad u \in \mathcal{T}_n;$$

then we write

$$F \rightsquigarrow_Q F - ct\frac{Q}{lt(Q)} = \hat{F}.$$

Otherwise, we say that F is *irreducible* with respect to Q.

If F is reducible with respect to some polynomial in $\mathcal{P} = \{P_1, \ldots, P_k\}$, then we say *$F$ reduces modulo $\mathcal{P}$*; otherwise F is in *fully reduced* (or *"normal") form modulo $\mathcal{P}$*. In addition, if $lt(F)$ reduces modulo $\mathcal{P}$, we say that F is *lt-reducible modulo $\mathcal{P}$*.

Thus, given a polynomial G and $\mathcal{P}$, we can establish the reduction sequence

$$G \rightsquigarrow_{\mathcal{P}} G_1 \rightsquigarrow_{\mathcal{P}} G_2 \rightsquigarrow_{\mathcal{P}} G_3 \rightsquigarrow_{\mathcal{P}} \ldots$$

until we get a polynomial G_i which is the *normal form* of G modulo $\mathcal{P}$. At this moment one may ask whether there exists such a G_i. The answer is yes because of the following fundamental property of reduction introduced by Buchberger [Buch65].

Lemma 3.10 *: The relation $\rightsquigarrow_{\mathcal{P}}$ is Noetherian, i.e., there is no infinite sequence*

$$G \rightsquigarrow_{\mathcal{P}} G_1 \rightsquigarrow_{\mathcal{P}} G_2 \rightsquigarrow_{\mathcal{P}} G_3 \rightsquigarrow_{\mathcal{P}} \ldots.$$

Let $\rightsquigarrow_{\mathcal{P}}^{+}$ denote the transitive closure of $\rightsquigarrow_{\mathcal{P}}$. Then as a consequence of the above lemma, we can construct an algorithm *reduce*$(G, \mathcal{P})$ to return Q such that $G \rightsquigarrow_{\mathcal{P}}^{+} Q$ and Q is irreducible modulo $\mathcal{P}$.

Example 3.4.2: Let $G = xy - z$ and let P_2 be as in the previous example. Then, with respect to the graduated ordering, we have

$$G = 1(xy) - z, \quad lpp(P_2) = xy, \quad lt(P_2) = 6xy \text{ and}$$

$$G \rightsquigarrow_{P_2} (xy - z) - (xy - xz - \frac{3}{2}y^2 + yz - \frac{1}{6}z^2) = xz + \frac{3}{2}y^2 - yz + \frac{1}{6}z^2 - z = Q.$$

Also, we note that in this case $G \rightsquigarrow_{\mathcal{P}}^{+} Q$, since $Q \rightsquigarrow_{P_1}^{+} Q, Q \rightsquigarrow_{P_2}^{+} Q$, and $Q \rightsquigarrow_{P_3}^{+} Q$.

Now we are in position to define a Gröbner basis as follows :

Definition 3.8 *An ideal basis $\mathcal{G}$ is called a Gröbner basis if*

$$F \in < \mathcal{G} > \quad \Longrightarrow \quad reduce(F, \mathcal{G}) = 0.$$

The above definition of Gröbner basis presents many difficulties. For example, it does not give us a means of testing whether a given ideal basis is a Gröbner basis. In addition, it does not tell us how to construct a Gröbner basis for a given ideal $< \mathcal{P} >$. One of Buchberger's many contributions was to give an algorithm to compute the Gröbner basis.

Definition 3.9 *The S-polynomial of P and Q is*

$$\text{Spoly}(P, Q) = lt(P, Q)[\frac{P}{lt(P)} - \frac{Q}{lt(Q)}].$$

Then, Buchberger [Buch76a] gave the alternative characterizations of Gröbner basis according to

Theorem 3.11 (Buch76a) . *The following are equivalent:*

(1) *$\mathcal{G}$ is a Gröbner basis;*

(2) *If* reduce$(F,\mathcal{G}) = G$ *and* reduce$(F,\mathcal{G}) = H$, *then* $G = H$;

(3) reduce(Spoly$(F,G),\mathcal{G}) = 0$ *for all* $F, G \in \mathcal{G}$.

Proof : See [Buch76a] since the proof is nontrivial, and it will be omitted for brevity. □□

From the above theorem we can obtain the following algorithm.

Buchberger's Algorithm :

```
procedure Gbasis($\mathcal{P}$)
    $\mathcal{G} \leftarrow \mathcal{P}$;   $k \leftarrow length(\mathcal{G})$
    $\mathcal{B} \leftarrow \{[i,j] \mid 1 \leq i < j \leq k\}$
    while $\mathcal{B} \neq \emptyset$ do
        $[i,j] \leftarrow selectpair(\mathcal{B},\mathcal{G})$;  $\mathcal{B} \leftarrow \mathcal{B} - \{[i,j]\}$
        $F \leftarrow reduce(Spoly(G_i, G_j), \mathcal{G})$
        if $F \neq 0$ then
            $\mathcal{G} \leftarrow \mathcal{G} \cup \{F\}$;  $k \leftarrow k + 1$
            $\mathcal{B} \leftarrow \mathcal{B} \cup \{[i,k] \mid 1 \leq i < k\}$
        endif
```

```
endwhile
return($\mathcal{G}$)
```

Example 3.4.3: For the polynomials $\mathcal{P} = \{P_1, P_2, P_3\}$ of Example 3.4.1,

$$\mathcal{G} = \{P_1, P_2, P_3,\ x^2 - \frac{9}{4}y^2 + \frac{6}{4}yz - \frac{1}{4}z^2,\ xy - \frac{3}{2}y^2 + \frac{1}{2}yz,\ xz - \frac{3}{2}yz + \frac{1}{2}z^2\}$$

is a Gröbner basis (with respect to the total degree ordering for terms in $[x, y, z]$) such that $<\mathcal{P}>=<\mathcal{G}>$.

Now, we can easily solve the ideal membership problem algorithmically since any polynomial G belongs to an ideal $\mathcal{P}$ if and only if the normal form of G with respect to the Gröbner basis of $\mathcal{P}$ is 0. For example, the normal form of $G = xy - z$ with respect to $\mathcal{G}$ in the previous example is $3y^2 - yz - 2z$. Hence, G is not in the ideal generated by $\mathcal{P}$.

Going back to Buchberger's algorithm, a first glance gives an impression that this algorithm can produce complex calculations for apparently simple input. The problem here is how to choose the appropriate pair of polynomials in $\mathcal{G}$ to avoid the reductions leading to 0. There are many works in the literature to develop a set of criteria for determining a priori a large proportion of those pairs whose reductions will yield 0. For the interested reader, [Czapor] is a good reference.

We can easily see that in general, a Gröbner basis is not unique. For example, the Gröbner basis we found in the previous example is not unique since we can leave out P_1, P_2, P_3 and $\mathcal{G} - \mathcal{P}$ is still a Gröbner basis of $<\mathcal{P}>$. Hence, the following definition will help us to solve this problem.

Definition 3.10 *A Gröbner basis is* reduced *if all* $F \in \mathcal{G}$, $F = \text{reduce}(F, \mathcal{G} - F)$ *and* $lcf(F) = 1$.

Thus, $\mathcal{G} - \mathcal{P}$ is a reduced Gröbner basis of $\mathcal{P}$ in the previous example. In addition, Buchberger showed that if $< \mathcal{G}_1 > = < \mathcal{G}_2 >$, and $\mathcal{G}_1, \mathcal{G}_2$ are reduced Gröbner bases then $\mathcal{G}_1 = \mathcal{G}_2$.

3.4.3 Solving Algebraic Equations with Gröbner Basis

We will briefly discuss the criteria for the solvability of the system of algebraic equations $P_1 = P_2 = \cdots = P_k = 0$ using a Gröbner basis. Note that these polynomials do not have to be homogeneous. The first criterion gives a condition for $\mathcal{P}$ to have solutions in an algebraic extension of $\mathcal{F}$; namely, the reduced Gröbner basis, $\mathcal{G}$, of a set of polynomials $\mathcal{P}$ contains 1 if and only if these polynomials do not have a common root, including the trivial one. The second criterion indicates the number of solutions of $P_1 = \ldots = P_k = 0$. Let $\mathcal{H}$ be the set

$$\mathcal{H} = \{lpp(G) \mid G \in \mathcal{G}\};$$

then $\mathcal{P}$ has finitely many solutions if and only if for all $i, 1 \leq i \leq n$, there exists p such that $x_i^p \in \mathcal{H}$.

We will give some examples to illustrate the solvability of the system of polynomial equations by the mean of Gröbner basis. First, $\mathcal{P}$ in Example 3.4.1 has infinitely many solutions because its reduced Gröbner basis does not satisfy the second criterion.

For the second example, let $\hat{\mathcal{P}} = \{\hat{P}_1, \hat{P}_2, \hat{P}_3\}$, where

$$\begin{aligned}
\hat{P}_1 &= (x - y - z)^2, \\
\hat{P}_2 &= (2x - y + 3z)^2, \\
\hat{P}_3 &= (x + 2y - z)^2.
\end{aligned}$$

Then $\hat{\mathcal{P}}$ has only the trivial solution $(0,0,0)$ because its reduced Gröbner basis $\hat{\mathcal{G}}$, with respect to $[x,y,z]$ and lexicographic order, is

$$\begin{aligned}\hat{\mathcal{G}} &= \{2x^2+3y^2-2yz+3z^2,\ y^3,\ z^4-2xy-y^2+2yz,\\ &\quad -4xz+y^2+2yz-z^2,\ -3y^2z-5z^3,\ -3yz^2-4z^3\}.\end{aligned}$$

Finally, let [Can88]

$$\begin{aligned}\tilde{P}_1 &= x^2+xy+2x-y-1,\\ \tilde{P}_2 &= x^2+3x-y^2-2y-1.\end{aligned}$$

Then the reduced Gröbner basis of $\tilde{\mathcal{P}} = \{\tilde{P}_1, \tilde{P}_2\}$, with respect to $[x,y,z]$ and graduated order, is

$$\hat{\mathcal{G}} = \{x^2+3x+2y-2,\ y^2-1,\ xy-x-y+1\}.$$

Thus, $\tilde{\mathcal{P}}$ has $(0,1),(-3,1),(1,-1)$ as solutions.

Before leaving this section, we want to mention that there are many methods for finding the solutions when different orderings are used. The interested reader can consult [Czapor] for further details. We will discuss the strategy for evaluating curve intersections using a Gröbner basis in the next chapter.

Chapter 4

Applying Elimination Theory to Intersection Problems

The intersection problem is one of the most fundamental problems in the area of processing curves and surfaces in geometric modeling. In this chapter, we first show that elimination techniques can be used to solve the intersection problems effectively. Secondly, we present a method to randomly generate 3D parametric polynomial and 3D parametric rational curve intersection problems with known solutions. Thirdly, the implementation issues for the projection, resolvent, and Gröbner basis methods for the above problems are discussed. Finally, we analyse the experimental results for the curve/curve intersections with rational and real coefficients.

4.1 Solutions of Intersection Problems

First, we give the formulae of the Bezout resultant, in vector notation, when

$$P_1(t) = \frac{a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0}{d_n t^n + d_{n-1} t^{n-1} + \cdots + d_1 t + d_0} - x,$$

$$P_2(t) \;=\; \frac{b_n t^n + b_{n-1}t^{n-1} + \cdots + b_1 t + b_0}{d_n t^n + d_{n-1}t^{n-1} + \cdots + d_1 t + d_0} - y,$$

where x, y are treated as constants. Rewriting $P_1(t) = 0, P_2(t) = 0$ in polynomial form, we have

$$\begin{aligned} P_1(t) &= (a_n - xd_n)t^n + (a_{n-1} - xd_{n-1})t^{n-1} + \cdots + (a_0 - xd_0) = 0, \\ P_2(t) &= (b_n - yd_n)t^n + (b_{n-1} - yd_{n-1})t^{n-1} + \cdots + (b_0 - yd_0) = 0. \end{aligned}$$

Let

$$\mathbf{p} = [x, y, 1]^T, \quad \mathbf{v}_k = [a_k, b_k, d_k]^T \quad \text{for } k = 0, \ldots, n;$$

then the entry c_{pq} of the Bezout matrix $\mathbf{C}$ of $P_1(t), P_2(t)$ [Goldm84] is

$$c_{pq} = \sum_{k=mx}^{mn} |\mathbf{p}, \mathbf{v}_k, \mathbf{v}_{p+1+q-k}| \qquad 0 \le p, q \le n-1, \qquad (4.1)$$

where $mn = min(p, q)$ and $mx = max(0, q - n + 1 + p)$. Thus, this expression gives us a compact formula for the implicitization of a 2D parametric rational curve (cf. Section 3.2.1).

Similarly, there are formulae for the resolvents of the three components of a 3D parametric rational curve

$$\begin{aligned} P_1(t) &= \frac{a_3t^3 + a_2t^2 + a_1t + a_0}{d_3t^3 + d_2t^2 + d_1t + d_0} - x, \\ P_2(t) &= \frac{b_3t^3 + b_2t^2 + b_1t + b_0}{d_3t^3 + d_2t^2 + d_1t + d_0} - y, \\ P_3(t) &= \frac{c_3t^3 + c_2t^2 + c_1t + c_0}{d_3t^3 + d_2t^2 + d_1t + d_0} - z. \end{aligned}$$

Rewrite $P_1(t) = 0, P_2(t) = 0$, and $P_3(t) = 0$ in polynomial form, to obtain

$$\begin{aligned} P_1(t) &= (a_3 - xd_3)t^3 + (a_2 - xd_2)t^2 + (a_1 - xd_1)t + (a_0 - xd_0) = 0, \\ P_2(t) &= (b_3 - yd_3)t^3 + (b_2 - yd_2)t^2 + (b_1 - yd_1)t + (b_0 - yd_0) = 0, \\ P_3(t) &= (c_3 - zd_3)t^3 + (c_2 - zd_2)t^2 + (c_1 - zd_1)t + (c_0 - zd_0) = 0. \end{aligned}$$

Using vector notation, let

$$\mathbf{u}_k = [a_k, b_k, c_k, d_k]^T, \quad \text{for } k = 0, 1, 2, 3 \quad \text{and} \quad \mathbf{q} = [x, y, z, 1]^T.$$

Then, we have the following resolvents (cf. Section 3.3.2): [Goldm85]

$$\begin{aligned}
R_1 &= \begin{vmatrix} |\mathbf{u}_3, \mathbf{u}_2, \mathbf{u}_1, \mathbf{q}| & |\mathbf{u}_3, \mathbf{u}_2, \mathbf{u}_0, \mathbf{q}| \\ |\mathbf{u}_3, \mathbf{u}_2, \mathbf{u}_0, \mathbf{q}| & |\mathbf{u}_3, \mathbf{u}_1, \mathbf{u}_0, \mathbf{q}| \end{vmatrix} = 0. \\
R_2 &= \begin{vmatrix} |\mathbf{u}_3, \mathbf{u}_2, \mathbf{u}_1, \mathbf{q}| & |\mathbf{u}_3, \mathbf{u}_2, \mathbf{u}_0, \mathbf{q}| \\ |\mathbf{u}_3, \mathbf{u}_1, \mathbf{u}_0, \mathbf{q}| & |\mathbf{u}_2, \mathbf{u}_1, \mathbf{u}_0, \mathbf{q}| \end{vmatrix} = 0. \qquad (4.2) \\
R_3 &= \begin{vmatrix} |\mathbf{u}_3, \mathbf{u}_2, \mathbf{u}_0, \mathbf{q}| & |\mathbf{u}_3, \mathbf{u}_1, \mathbf{u}_0, \mathbf{q}| \\ |\mathbf{u}_3, \mathbf{u}_1, \mathbf{u}_0, \mathbf{q}| & |\mathbf{u}_2, \mathbf{u}_1, \mathbf{u}_0, \mathbf{q}| \end{vmatrix} = 0.
\end{aligned}$$

In addition, the inversion equation is

$$t_0 = \frac{|\mathbf{u}_3, \mathbf{u}_2, \mathbf{u}_0, \mathbf{q}|}{|\mathbf{u}_3, \mathbf{u}_2, \mathbf{u}_1, \mathbf{q}|}. \qquad (4.3)$$

From now on, whenever we say Bezout resultant we mean (3.5) and (4.1) for the case of nonrational and rational parametric curves, respectively. Similarly, (3.59) and (4.2) will be used for the resolvents of nonrational and rational parametric cubic curves, respectively. In addition, let $f_1(x, y, z) = |\mathbf{v}_3, \mathbf{v}_2, \mathbf{v}_1|$ in (3.60) for the nonrational case, and $f_1(x, y, z) = |\mathbf{u}_3, \mathbf{u}_2, \mathbf{u}_1, \mathbf{q}|$ in (4.3) for the rational case.

Now, we present the solutions for the problems proposed in Chapter 2 using the elimination techniques in Chapter 3.

Problem 2.1: *Curve/Curve intersection*

We have three different elimination methods to solve it.

Gröbner basis: Let $a_1(s)d_2(t) - a_2(t)d_1(s) = 0$, $b_1(s)d_2(t) - b_2(t)d_1(s) = 0$, and $c_1(s)d_2(t) - c_2(t)d_1(s) = 0$, be three bivariate polynomials equations; then find the reduced Gröbner basis $\mathcal{G}$ of the above equations.

Solve for s, t in $\mathcal{G}$. We will discuss this method in detail in the next section.

Projection: This method is based on the fact that any 3D curve can be projected onto the xy and yz planes to get two polynomials in x, y and y, z, respectively. This can be done by using the Bezout resultant.

Find the Bezout resultants $R_1(x, y)$ and $R_2(y, z)$ of two pairs of polynomials

$$a_1(s) - xd_1(s) = 0, \quad b_1(s) - yd_1(s) = 0$$

and

$$b_1(s) - yd_1(s) = 0, \quad c_1(s) - zd_1(s) = 0.$$

Substituting $x = x_2(t), y = y_2(t)$, and $z = z_2(t)$ into $R_1(x, y)$ and $R_2(y, z)$, we get two polynomials $P_1(t)$ and $P_2(t)$. To find the common roots of these polynomials we again construct their Bezout matrix and obtain the common factor $C(t)$ of these poiynomials. Again, using an univariate polynomial solver, we can get the set $\mathcal{T}$ of roots of $C(t) = 0$.

For each $\hat{t} \in \mathcal{T}$ we find $\hat{x} = x_2(\hat{t})$. Using an univariate polynomial solver we can get the set $\mathcal{S}$ of roots of $x_1(s) - \hat{x} = 0$.

For each $\hat{s} \in \mathcal{S}$ and the corresponding $\hat{t} \in \mathcal{T}$, if $y_1(\hat{s}) = y_2(\hat{t})$ and $z_1(\hat{s}) = z_2(\hat{t})$ then the pair $(\hat{s}, \hat{t})$ is a solution of the problem.

Resolvent: This method is applicable when one of the curves is parametric cubic.

Find the resolvents $R_1(x, y, z)$, $R_2(x, y, z)$ of the cubic curve, say $C_1(s)$. These resolvents are the polynomials of degree 2 in x, y, z. Substituting

$x = x_2(t), y = y_2(t)$, and $z = z_2(t)$ into $R_1(x,y,z)$ and $R_2(x,y,z)$, we get two polynomials $P_1(t)$ and $P_2(t)$. To find the common roots of these polynomials we again construct their Bezout matrix and obtain the common factor $C(t)$ of these polynomials. Using an univariate polynomial solver, we can get the set $\mathcal{T}$ of roots of $C(t) = 0$.

For each $\hat{t} \in \mathcal{T}$ we find $\hat{x} = x_2(\hat{t}), \hat{y} = y_2(\hat{t}), \hat{z} = z_2(\hat{t})$. If $f_1(\hat{x},\hat{y},\hat{z}) \neq 0$ then we get $\hat{s}$ by using one of the inversion equations (3.60) or (4.3) of s. Then the pairs $(\hat{s},\hat{t})$ are the solutions of the problem.

Problem 2.2a: *Line/Surface intersection*

After getting two polynomials $P_1(u,v)$ and $P_2(u,v)$, we can use the Gröbner basis method to solve for their roots. Also, we can homogenize these polynomials, and let $P_3(u,v,x_0) = a_1u + a_2v + a_3x_0$. Then we can use the u-resultant of $P_1(u,v,x_0), P_2(u,v,x_0)$, and $P_3(u,v,x_0)$ to get the solutions for this problem.

Problem 2.2b: *Curve/Surface intersection*

This problem is similar to Problem 2.2a. Thus, we can use the Gröbner basis or u-resultant method to solve it. In this problem, we have 3 trivariate polynomials; thus it is harder to solve.

Problem 2.3: *Surface/Surface intersection*

The solution of this problem consists of the equations of the intersection curves in the parameter planes (u,v) or (s,t).

We can treat the parameters in one plane as constant, say (s,t), then we have three bivariate equations:

$$\begin{aligned}
Q_1(u,v) &= x_1(u,v) - c_1 = 0, \quad \text{where} \quad c_1 = x_2(s,t). \\
Q_2(u,v) &= y_1(u,v) - c_2 = 0, \quad \text{where} \quad c_2 = y_2(s,t). \\
Q_3(u,v) &= z_1(u,v) - c_3 = 0, \quad \text{where} \quad c_3 = z_2(s,t).
\end{aligned}$$

First, we eliminate u from $Q_1(u,v), Q_2(u,v)$ and $Q_2(u,v), Q_3(u,v)$ using resultants to get $P_1(v)$ and $P_2(v)$, respectively. Then, eliminate v from $P_1(v)$ and $P_2(v)$ by computing their resultant. We get the equation $C = 0$ of the intersection curve in the parameter plane (s,t).

4.2 Generation of Random Problems

Generating random problems with known solutions is one of the important aspects of testing various algorithms. For Problem 2.1, there is no method in the literature (to our knowledge) for generating a pair of $3D$ parametric rational curves in which their intersection points are known. In this section, we discuss a process for randomly generating such curves, $C_1(s), C_2(t)$, with rational coefficients. The following are the input parameters:

(1) n_1, n_2: degrees of C_1, C_2, respectively,

(2) k : number of intersection points,

(3) rat : indicates whether the curves are rational or not,

(4) *range* : range for the random number generator. The denominator and the numerator of the random rational numbers are in [0,*range*].

(5) *seed* : seed for the random number generator

The output consists of the coefficients of the polynomials $a_1(s), b_1(s), c_1(s), d_1(s)$, where $x_1(s) = a_1(s)/d_1(s), y_1(s) = b_1(s)/d_1(s), z_1(s) = c_1(s)/d_1(s)$, and the polynomials $a_2(t), b_2(t), c_2(t), d_2(t)$, where $x_2(t) = a_2(t)/d_2(t), y_2(t) = b_2(t)/d_2(t)$, $z_2(t) = c_2(t)/d_2(t)$. This yields the parametric curves $C_1(s)$ and $C_2(t)$, respectively. These coefficients are rational numbers.

We find these curves by the following steps:

(1) Randomly generate six vectors of rational numbers

$$\mathbf{x}_s = [\tilde{x}_1, \ldots, \tilde{x}_{p_1}]^T, \quad \mathbf{y}_s = [\tilde{y}_1, \ldots, \tilde{y}_{p_1}]^T, \quad \mathbf{z}_s = [\tilde{z}_1, \ldots, \tilde{z}_{p_1}]^T,$$

$$\mathbf{x}_t = [\hat{x}_1, \ldots, \hat{x}_{p_2}]^T, \quad \mathbf{y}_t = [\hat{y}_1, \ldots, \hat{y}_{p_2}]^T, \quad \mathbf{z}_t = [\hat{z}_1, \ldots, \hat{z}_{p_2}]^T,$$

where

$$p_i = \begin{cases} \left\lfloor \dfrac{4n_i + 3}{3} \right\rfloor & \textit{rat=true}, \\ n_i + 1 & \text{otherwise}, \end{cases}$$

by using an uniform random number generator with *seed* and *range* as the inputs. These vectors must satisfy the following conditions: Firstly,

$$\tilde{x}_i = \hat{x}_i, \ \ \tilde{y}_i = \hat{y}_i, \ \ \tilde{z}_i = \hat{z}_i, \quad \text{for } i = 1, \ldots, k,$$

and the remaining points are distinct. Secondly, the points $(\tilde{x}_i, \tilde{y}_i, \tilde{z}_i)$ for $i = 1, \ldots, p_1$ are not coplanar if $p_1 \geq 4$ (or equivalently, $n_1 \geq 3$). Similarly, $(\hat{x}_i, \hat{y}_i, \hat{z}_i)$ for $i = 1, \ldots, p_2$ are not coplanar if $p_2 \geq 4$.

(2) Randomly generate two vectors of rational numbers $\mathbf{s} = [s_1, \ldots, s_{p_1}]^T$, and $\mathbf{t} = [t_1, \ldots, t_{p_2}]^T$, where $0 \leq s, t \leq 1$. In addition, within each vector, the elements are distinct. Then the intersection points of the two curves include the pairs (s_i, t_i) for $i = 1, \ldots, k$.

(3) If *rat=false* then we just simply obtain $x_1(s), y_1(s), z_1(s)$ using polynomial interpolation of s and $\mathbf{x}_s, \mathbf{y}_s$, and $\mathbf{z}_s$, respectively. In the implementation of this algorithm, we use the *interp* function in Maple [Maple]. For example, $x_1(s) =$*interp*$(n_1, \mathrm{s}, \mathbf{x}_s)$. Similarly, we get $x_2(t), y_2(t), z_2(t)$.

Otherwise, for the curve $C_1(s)$ and the interpolation conditions $x_1(s_i) = \tilde{x}_i,\ y_1(s_i) = \tilde{y}_i,\ z_1(s_i) = \tilde{z}_i,$ for $i = 1, \ldots, p_1$, we set up $3p_1$ homogeneous linear equations.

$$
\begin{aligned}
& s_i^{n_1} a_{n_1} + s_i^{n_1 - 1} a_{n_1 - 1} + \cdots + s_i a_1 + a_0 - \\
& \qquad \tilde{x}_i (s_i^{n_1} d_{n_1} + s_i^{n_1 - 1} d_{n_1 - 1} + \cdots + s_i d_1 + d_0) = 0 \\
& s_i^{n_1} b_{n_1} + s_i^{n_1 - 1} b_{n_1 - 1} + \cdots + s_i b_1 + b_0 - \\
& \qquad \tilde{y}_i (s_i^{n_1} d_{n_1} + s_i^{n_1 - 1} d_{n_1 - 1} + \cdots + s_i d_1 + d_0) = 0 \\
& s_i^{n_1} c_{n_1} + s_i^{n_1 - 1} c_{n_1 - 1} + \cdots + s_i c_1 + c_0 - \\
& \qquad \tilde{z}_i (s_i^{n_1} d_{n_1} + s_i^{n_1 - 1} d_{n_1 - 1} + \cdots + s_i d_1 + d_0) = 0
\end{aligned}
$$

for $i = 1, \ldots, p_1$. Hence, in vector notation, we have

$$
\mathbf{A}\mathbf{e} = \mathbf{0}, \tag{4.4}
$$

where $\mathbf{e}$ is the vector containing the a_i, b_i, c_i and d_i, i.e.

$$
\mathbf{e} = [a_{n_1}, \ldots, a_0, b_{n_1}, \ldots, b_0, c_{n_1}, \ldots, c_0, d_{n_1}, \ldots, d_0]^T,
$$

and **A** is a underdetermined Vandermonde-like matrix with $3p_1$ rows and $4n_1+4$ columns where $4n_1+1 \leq 3p_1 \leq 4n_1+3$, i.e.,

$$\mathbf{A} = \begin{bmatrix}
s_1^{n_1} & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 & -\tilde{x}_1 s_1^{n_1} & \dots & -\tilde{x}_1 \\
s_2^{n_1} & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 & -\tilde{x}_2 s_2^{n_1} & \dots & -\tilde{x}_2 \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\
s_{p_1}^{n_1} & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 & -\tilde{x}_{p_1} s_{p_1}^{n_1} & \dots & -\tilde{x}_{p_1} \\
0 & \dots & 0 & s_1^{n_1} & \dots & 1 & 0 & \dots & 0 & -\tilde{y}_1 s_1^{n_1} & \dots & -\tilde{y}_1 \\
0 & \dots & 0 & s_2^{n_1} & \dots & 1 & 0 & \dots & 0 & -\tilde{y}_2 s_2^{n_1} & \dots & -\tilde{y}_2 \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\
0 & \dots & 0 & s_{p_1}^{n_1} & \dots & 1 & 0 & \dots & 0 & -\tilde{y}_{p_1} s_{p_1}^{n_1} & \dots & -\tilde{y}_{p_1} \\
0 & \dots & 0 & 0 & \dots & 0 & s_1^{n_1} & \dots & 1 & -\tilde{z}_1 s_1^{n_1} & \dots & -\tilde{z}_1 \\
0 & \dots & 0 & 0 & \dots & 0 & s_2^{n_1} & \dots & 1 & -\tilde{z}_2 s_2^{n_1} & \dots & -\tilde{z}_2 \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\
0 & \dots & 0 & 0 & \dots & 0 & s_{p_1}^{n_1} & \dots & 1 & -\tilde{z}_{p_1} s_{p_1}^{n_1} & \dots & -\tilde{z}_{p_1}
\end{bmatrix}.$$

Using a linear system solver, i.e., *linsolve* in Maple, we can get the coefficients a_i, b_i, c_i and d_i. Since (4.4) is an underdetermined system, we get a set of solutions for **e**, i.e., there are indeterminates in it. We just simply assign the value 1 to the indeterminates. Note that we use the exact method here, i.e., the entries of **A** and **e** are rational numbers. Similarly, we can do the same for the second curve C_2.

We want to use exact computation in our method because first we would like to get the exact representation of the curves with precisely k intersection points; second, the floating point solution of (4.4) may not be reliable since Vandermonde matrices may be ill-conditioned.

4.3 Implementation Issues for Problem 2.1

In this section we discuss the implementation of three different methods to solve this problem. We have implemented these algorithms in Maple for the cases of rational and real coefficients of the input curves. In general, the inputs are two curves C_1, C_2 and their degrees. The outputs are the intersection points and the comparison between the actual and the calculated intersection points.

For the Gröbner basis method, we only implemented it for the case that the coefficients of the input curves are rational. To get the reduced Gröbner basis $\mathcal{G}$ of these curves, we use the Gröbner basis package in Maple [Maple] with lexicographic ordering and used the heuristic approach for choosing the order of s and t. Note that this is the bivariate case for the Gröbner basis. Buchberger [Buch83] and Lazard [Lazard] showed that the number of polynomials in the Gröbner basis is bounded by $m+1$, where m is the minimum of the total degrees of the leading monomials of all the input polynomials. We show how to get the solutions from $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$, where $n \leq m+1$, and the G_i's are polynomials in s and t. In our experiments, n is relatively small($n \leq 5$).

(1) If $1 \in \mathcal{G}$, then the curves do not intersect; stop.

(2) Find a univariate polynomial $P(s)$ or $Q(t)$ in $\mathcal{G}$ whose degree is minimal in s and t, respectively. Note that in general, if the set of equations $A_1 = \ldots = A_k = 0$, where $A_i \in \mathcal{K}[x_1, \ldots, x_n]$, has a finite number of solutions, then the reduced Gröbner basis $\mathcal{G}$ of these polynomials with respect to the lexicographic ordering always contains a univariate polynomial in x_n. This can be seen by applying the criterion of the Gröbner basis which indicates that the system has a finite number of solutions (see Section 3.4.3). Thus,

if two curves intersect at a finite number of points then either $P(s)$ or $Q(t)$ exists.

(3) If $P(s)$ and $Q(t)$ do not exist then the curves intersect at an infinite number of points; stop. In this case the equations $x_1(s)-x_2(t) = 0, y_1(s)-y_2(t) = 0$, and $z_1(s) - z_2(t) = 0$ have an infinite number of solutions.

(4) If $P(s)$ is found in step 2 then

(4.1) If the input curves are rational and if $f_1(s) = \gcd(d_1(s), P(s)) \neq 1$, then set $P(s)$ to $P(s)/f_1(s)$. We want to avoid finding extraneous roots of $P(s) = 0$.

(4.2) Find a bivariate polynomial $R(s,t)$ in $\mathcal{G}$ whose degree is minimal in t.

(4.3) Solve for $P(s) = 0$; $\mathbf{s}$ is a vector of solutions. For each $\hat{s} \in \mathbf{s}$, solve for t in $R(s,t) = 0$; $\hat{\mathbf{t}}$ is a vector of solutions; the pairs $(\hat{s}, \hat{t})$, where $\hat{t} \in \hat{\mathbf{t}}$ are solutions.

(5) Otherwise ($Q(t)$ is found in step 2)

(5.1) If the input curves are rational and if $f_2(t) = \gcd(d_2(t), Q(t)) \neq 1$, then set $Q(t)$ to $Q(t)/f_2(t)$. We want to avoid finding extraneous roots of $Q(t) = 0$.

(5.2) Find a bivariate polynomial $R(s,t)$ in $\mathcal{G}$ whose degree is minimal in s.

(5.3) Solve for $Q(t) = 0$; $\mathbf{t}$ is a vector of solutions. For each $\hat{t} \in \mathbf{t}$, solve for s in $R(s,t) = 0$; $\hat{\mathbf{s}}$ is a vector of solutions; the pairs $(\hat{s}, \hat{t})$, where $\hat{s} \in \hat{\mathbf{s}}$ are solutions.

For the projection and resolvent methods, the implementations in the case of rational coefficients are straightforward (see Section 4.1). We will discuss the implementations of these algorithms when the coefficients are real (floating point) numbers in the next section.

4.4 Experimental Results

4.4.1 Exact Arithmetic Implementation

We have coded the three algorithms described in Section 4.1. The algebraic manipulation language Maple is used, since it uses exact arithmetic (rational numbers) and comes with a Gröbner basis package. The tests are performed using the Unix operating system on a VAX 11/780. Testing is performed on 3D parametric rational and nonrational curves of degrees 3 to 6, and on 2D parametric rational curves of degree 2 to compare the CPU times of the three methods. Because the projection method is inferior to the other two, we have only run it a limited number of times. For each of polynomial or rational and each degree of the second curve, 50 test problems are randomly generated with 0 to 4 intersection points. For each number of intersection points, 10 test problems are generated. The timing results are presented in Table 4.1 and Table 4.2, where the CPU times are in seconds. Each entry is the average of 10 runs. The blank entries in these tables indicate that there are no test runs. We felt that these runnings are unnecessary because the conclusions can be drawn without their presence. The

Algorithm	*No. int. points*	*Degrees of input curves*				
		3 - 2	3 - 3	3 - 4	3 - 5	3 - 6
Gröbner	0	27.551	82.950	208.909	697.467	1096.967
	1	27.792	76.175	203.742	464.142	1000.384
	2	27.483	69.016	156.250	457.617	872.482
	3	24.850	67.017	121.600	380.500	729.499
	4	??????	58.150	122.050	354.433	619.634
Resolvent	0	29.784	72.440	242.876	1158.817	2241.083
	1	18.475	48.258	184.481	826.924	2122.876
	2	12.650	37.583	117.083	676.683	1714.216
	3	10.413	32.950	100.606	441.016	1209.650
	4	??????	16.866	85.950	321.167	935.867
Projection	0	50.200	408.942			
	1	45.209	287.783			
	2	39.900	223.357			
	3	30.492	175.450			
	4	??????	99.800	1230.516		

Table 4.1: Times in seconds for parametric rational curves

"??????" entries are there because the number of intersection points is greater than the degree by 2, which is impossible.

The first goal of our evaluation is to determine the correctness of these algorithms. Of all the sample problems with known intersections solved, all results obtained are correct; that is these algorithms report exactly the known intersections.

The second goal is to compare execution speed. Our results indicate that the projection method is the worst. This is reasonable because it produces intermediate polynomials with high degree (see Section 4.1). For instance, to find the intersection of two 3D parametric rational cubic curves using the projection method, we have to find the gcd of two degree 9 univariate polynomials; this

Algorithm	*No. int. points*	*Degrees of input curves*				
		3 – 2	3 – 3	3 – 4	3 – 5	3 – 6
Gröbner	0	10.934	12.800	17.350	25.602	36.850
	1	10.233	13.633	16.717	24.150	29.816
	2	10.133	13.484	15.950	28.710	33.234
	3	8.015	14.033	16.733	23.584	30.417
	4	?????	12.050	12.667	22.650	27.866
Resolvent	0	10.050	20.850	45.534	83.740	173.350
	1	7.616	19.483	31.517	64.820	146.733
	2	7.600	16.500	32.266	74.834	137.517
	3	7.421	16.933	25.450	57.233	129.417
	4	?????	10.217	28.184	47.167	119.416
Projection	0	35.884	173.950			
	1	20.883	148.250			
	2	19.533	111.150			
	3	18.213	92.000			
	4	??????	47.600			

Table 4.2: Times in seconds for parametric polynomial curves

corresponds to setting up a 9 by 9 Bezout matrix and applying Gaussian elimination to it. Hence, we only discuss the comparisons between the resolvent and the Gröbner basis algorithm.

We have some conclusions about the speed of the algorithms in terms of degrees of the input curves. First, we state the results for the case that the input curves [illegible]ric rational. If the degree of the second curve is less than or equal 3, then the resolvent algorithm uses slightly less CPU time than the Gröbner basis algorithm. The two algorithms have about the same time when the degrees of the inputs are $(3, 4)$. But if the degree of the second curve is greater than 4 then the Gröbner basis method is faster than the resolvent method. Second, when the input curves are 3D parametric polynomial, the Gröbner basis algorithm is much better then the resolvent algorithm, especially when the degree of the second curve is high.

In terms of the number of intersection points of the two curves, each algorithm typically consumes less time as the number of intersection points increases. This agrees with theoretical reasoning: For the resolvent algorithm (see Section 4.1), the higher the number of the intersection points, the fewer the number of steps of Gaussian elimination on the Bezout matrix it has to perform to get the gcd of the two univariate polynomials. A similar observation holds for the projection method. For the Gröbner basis method, it is fair to say that the degrees of the polynomials in the reduced Gröbner basis of the input curves are high. This means that the number of reduction steps are fewer when there are more intersection points, i.e., the degree of the basis polynomials are higher.

When comparing the speed between the two algorithms in terms of the number of intersection points of two parametric rational curves, we can say that resolvent method is better when there are more than 2 intersection points and the degree of the second curve is less than or equal to 5. Hence, the Gröbner basis method is better when there are less than 3 intersection points.

In the case of parametric polynomial curves, the results show that as the degree of the second curve increases the time required for the Gröbner basis algorithm grows polynomially while the time required for the resolvent algorithm grows exponentially, i.e., it approximately doubles with an increase of 1 in the degree. However, when the input curves are parametric rational, the times required by both algorithms grow at about the same rate with respect to the degree of the second curve.

In summary, if there exist three intersection algorithms: projection, resolvent, and Gröbner basis, in a geometric modeling system, then from these results, we make the following recommendations for the users of these algorithms:

- Try to avoid using the projection method as much as possible.
- When the input curves are 3D parametric polynomial, use the Gröbner basis algorithm.
- When the input curves are 3D parametric rational and the degrees of the input curves are 3 and d, then if $d \leq 3$, use the resolvent method, otherwise, use the Gröbner basis algorithm.
- If we know that there are more than 2 intersection points and $d \leq 4$, use the resolvent method.

Overall, the Gröbner basis algorithm is better than the other two methods, especially in practice, since two 3D curves seldom intersect. We believe that we can develop a *special* Gröbner basis package to handle the 3D curve intersection, which is faster than using the general package because we can exploit the fact that all the polynomials are bivariate.

Before leaving this section, we want to mention that the Gröbner basis package in Maple is more efficiently implemented than the resolvent algorithm because we believe that some of the subroutines in this package are implemented in C, while the resolvent algorithm is implemented entirely in Maple. Hence, we will only know how much better the resolvent algorithm will be compared with the Gröbner algorithm if we know how the Gröbner basis package is implemented in Maple and C, and modify the implementation of the resolvent algorithm to match the advantages that the Gröbner basis algorithm has.

4.4.2 Floating Point Arithmetic Implementation

For the floating point arithmetic implementation of the projection and resolvent algorithms described in Section 4.1, we have one more input parameter array, *Tol*, consisting of two elements. We will show how *Tol*[1] and *Tol*[2] are used in the algorithm below.

Let $P(t) = \sum_{i=0}^{d} c_i t^i$ be any arbitrary polynomial of degree d; then define

$$maxcof(P(t)) = max(|c_i|), \qquad \text{for } i = 0, 1, \ldots, d.$$

Also, let $\mathbf{A} = [a_{ij}] = [\mathbf{r}_1, \ldots, \mathbf{r}_n]^T$ be an n by n matrix, with rows $\mathbf{r}_i^T$. Then

$$max\mathbf{r}_i = max(|a_{ij}|), \qquad \text{for } j = 1, \ldots, n;$$

$$max(\mathbf{A}) = max(max\mathbf{r}_i), \qquad \text{for } i = 1, \ldots, n.$$

Now, we modify the projection and resolvent algorithms for Problem 2.1 in Section 4.1 for the floating point representation of the coefficients.

(1) After we get the univariate polynomials $P_1(t), P_2(t)$, in both methods, normalize them; for example, set $P(t)$ to $\sum_{i=0}^{d} (c_i / maxcof(P(t)))t^i$. Then, if $|c_i| < Tol[1]$, set $c_i = 0.0$.

(2) Now, we set up the Bezout matrix $\mathbf{B}$ for the normalized P_1, P_2 and apply Gaussian elimination with partial pivoting and implicit scaling [Atkin]. The problem here is that during the elimination process, we need to decide which small entries in $\mathbf{B}$ are really zero. We use the second tolerance for this problem. That is, if the pivot of $\mathbf{B}$, say b_{ii}, is less than $Tol[2]$ in absolute value, then set rows i to row n to $\mathbf{0}$. This is a heuristic step, and its based on our observation that the rows have decreasing absolute values in our experiments.

(3) After we get the common factor $C(t)$, we proceed as in the case of rational coefficients.

Initially, our first goal was to find the relationship between the coefficients of the input curves and the array *Tol.* But we failed to obtain such a relationship and will leave it to future research.

Our second goal is to see how stable the projection and resolvent algorithms are. There are cases in which these algorithms fail to report any intersection points while the actual intersection points exist. The following example illustrates this point.

Example 4.4.1 : The curves are $P(s)$ and $Q(t)$, where the components of the curve $P(s)$ are:

$$\begin{aligned}
x_1(s) &= \frac{1.8448264 - 13.781822s + 27.775270s^2 - 16.905831s^3}{2.7043950 - 20.562170s + 41.869267s^2 - 25.683240s^3}, \\
y_1(s) &= \frac{1.4189839 - 9.7137086s + 19.030943s^2 - 11.469593s^3}{2.7043950 - 20.562170s + 41.869267s^2 - 25.683240s^3}, \\
z_1(s) &= \frac{1.0 - 7.7359194s + 15.912610s^2 - 9.8347009s^3}{2.7043950 - 20.562170s + 41.869267s^2 - 25.683240s^3},
\end{aligned}$$

and the components of the curve $Q(t)$ are:

$$\begin{aligned}
x_2(t) &= \frac{-0.61265987 + 2.5891510t - 3.4319562t^2 + 1.3599856t^3}{-0.97070784 + 3.9984676t - 5.0996641t^2 + 1.8809454t^3}, \\
y_2(t) &= \frac{-.26698886 + 1.0t - 1.0454412t^2 + 0.19785466t^3}{-0.97070784 + 3.9984676t - 5.0996641t^2 + 1.8809454t^3}, \\
z_2(t) &= \frac{-0.45511876 + 1.8307656t - 2.2626510t^2 + 0.79152472t^3}{-0.97070784 + 3.9984676t - 5.0996641t^2 + 1.8809454t^3}.
\end{aligned}$$

We used the projection and the resolvent algorithms with $Tol = [10^{-7}, 10^{-7}]$. Both algorithms failed to report any intersection points. But, the actual intersection points, in x, y, z coordinate, are: $(0.5, 0.6, 0.5)$, and $(0.625, 0.444, 0.4)$, and in the parametric variables (s, t), the intersection points are: $(.7, 1.0)$ and $(0.85714286, 0.66666667)$.

On the other hand, the following example indicates that the projection and resolvent algorithms report extra intersection points, which do not lie on the input curves:

Example 4.4.2 : We know that the input curves $P(s)$ and $Q(t)$ have one intersection point at $(0.25, 0.9, 0.5)$ with corresponding $s = 0.625$ and $t = 0.22222222$. The components of the curve $P(s)$ are:

$$\begin{aligned}
x_1(s) &= \frac{1.0 - 4.4817827s + 6.6322672s^2 - 3.2439802s^3}{0.31245966 - 2.1861032s + 4.2157628s^2 - 2.4674966s^3}, \\
y_1(s) &= \frac{-1.2158106 + 4.5855138s - 5.7185561s^2 + 2.3557553s^3}{0.31245966 - 2.1861032s + 4.2157628s^2 - 2.4674966s^3}, \\
z_1(s) &= \frac{0.97756096 - 4.5882078s + 7.0411514s^2 - 3.5435529s^3}{0.31245966 - 2.1861032s + 4.2157628s^2 - 2.4674966s^3},
\end{aligned}$$

and the components of the curve $Q(t)$ are:

$$\begin{aligned}
x_2(t) &= \frac{-0.089112463 + 0.51508244t - 0.85819763t^2 + 0.44200280t^3}{-0.35745934 + 2.0727994t - 3.4767756t^2 + 1.8054237t^3}, \\
y_2(t) &= \frac{-0.32053031 + 1.8553865t - 3.1032929t^2 + 1.6061408t^3}{-0.35745934 + 2.0727994t - 3.4767756t^2 + 1.8054237t^3}, \\
z_2(t) &= \frac{-0.17482380 + 1.0t - 1.6362521t^2 + .824272232t^3}{-0.35745934 + 2.0727994t - 3.4767756t^2 + 1.8054237t^3}.
\end{aligned}$$

But using the projection algorithm with *Tol*$= [10^{-8}, 10^{-8}]$ and the resolvent algorithm with *Tol*$= [10^{-6}, 10^{-6}]$, we have the following intersection points:

$$\begin{aligned}
s_1 &= 0.62489327 & t_1 &= 0.21672381, \\
s_2 &= 0.62489327 & t_2 &= 0.23657849, \\
s_3 &= 0.62489327 & t_3 &= 0.22223487.
\end{aligned}$$

In some other cases, we obtain complex intersection points whose real parts are close to the actual intersection points and the imaginary parts are close to 0. For most of the randomly generated problems that we ran, one of the above three cases occurred for the computed results. Therefore, this indicates that the projection and resolvent algorithms are likely numerically unstable.

Chapter 5

Concluding Remarks

In this thesis, we discussed the issues of how to evaluate curve and surface intersections using elimination theory. First, we provided the mathematical tools in elimination theory. Then, using these tools, we implemented three curve/curve intersection algorithms: projection, resolvent, and Gröbner basis. Also, we implemented an algorithm to generate random problems for the three intersection methods. The experimental results obtained from the random problems, with rational coefficients, indicate that the projection method is the worst in term of CPU time. In addition, the Gröbner basis method is the best, in term of CPU time, when the input curves are 3D parametric polynomial. Furthermore, for the case input curves are 3D parametric rational, if there are more than 2 intersection points and the degree of the first curve is 3 and the degree of the second curve is less than or equal 4, the resolvent algorithm uses less CPU time than the other two algorithms. Finally, we illustrated the difficulties arising from floating point implementations of the projection and resolvent algorithms.

The new contributions of this thesis are: First, we provided a comprehensive survey of the elimination theory. We gave a complete, correct, and constructive proof for the solutions of two bivariate polynomials, which involves the Sylvester resultant. Also, we improved the description of the constructive method to derive an explicit expression for the resultant in the multivariate case because we believe that the original descriptions [Mac02, Mac16] are hard to follow and appear to contain errors. Second, we discussed the implementation issues of three curve/curve intersection algorithms: projection, resolvent, and Gröbner basis methods. In addition, we provided a methodology for generating random problems with known intersections. Furthermore, from experimental results, we identified the classes of the problems for which each method is better and indicated the difficulties which arise when using floating point implementations.

In our opinion, there are many unsolved problems arising from this thesis. Namely, the first major one is related to the multivariate resultant. The second problem is concerned about the *special resolvent*, implicitization, inversion, and intersection of curves and surfaces. Finally, the third problem is dealing with the floating point implementation of the curve/curve intersection problem. These open questions are elaborated further below.

5.1 Multivariate Resultant

First, when deriving an explicit expression for the multivariate resultant $\mathcal{R}$, we treat all the coefficients of the polynomials $P_1, \ldots, P_n$ as indeterminates. This causes confusion and difficulties in understanding this theory. The question here is whether we can derive $\mathcal{R}$ using specialization of the coefficients of the polynomials. The problem with the current approach is that the determinant of the submatrix ΔM may be zero when using specialized coefficients.

Second, the construction of the Macaulay matrix $\mathbf{M}$ is complicated and time consuming. Can we find an easier way to construct it, i.e., can can we obtain $\mathbf{M}$ from the coefficients of $P_1, \ldots, P_n$ like we do in the bivariate case? There are two difficulties here. Number one is can we get a formula to indicate how many rows correspond to each polynomial without actually computing $\hat{\mathcal{X}}_{0,d}, \ldots, \hat{\mathcal{X}}_{n-1,d}, \hat{\mathcal{X}}_{n,d}$, Number two is how to find a pattern for the rows corresponding to each polynomial. We believe there exists such a pattern. For example, for the matrix $\mathbf{M}(3,4)$ in Example 3.2.2 we can reorder its rows as

$$\begin{aligned}&[x^2P_1,\ xyP_1,\ xzP_1,\ y^2P_1,\ yzP_1,\ z^2P_1,\\ &xyP_2,\ xzP_2,\ y^2P_2,\ yzP_2,\ z^2P_2,\\ &xyP_3,\ xzP_3,\ yzP_3,\ z^2P_3],\end{aligned}$$

and reorder the columns in the lexicographic ordering of $[x, y, z]$ to get the following matrix:

$$[x^4,\ x^3y,\ x^3z,\ x^2y^2,\ x^2yz,\ x^2z^2,\ xy^3,\ xy^2x,\ xyz^2,\ xz^3,\ y^4,\ y^3z,\ y^2z^2,\ yz^3,\ z^4]$$

$$\begin{bmatrix}
a_{xx}&a_{xy}&a_{xz}&a_{yy}&a_{yz}&a_{zz}&&&&&&&&&\\
&a_{xx}&0&a_{xy}&a_{xz}&0&a_{yy}&a_{yz}&a_{zz}&&&&&&\\
&&a_{xx}&0&a_{xy}&a_{xz}&0&a_{yy}&a_{yz}&a_{zz}&&&&&\\
&&&a_{xx}&0&0&a_{xy}&a_{xz}&0&0&a_{yy}&a_{yz}&a_{zz}&&\\
&&&&a_{xx}&0&0&a_{xy}&a_{xz}&0&0&a_{yy}&a_{yz}&a_{zz}&\\
&&&&&a_{xx}&0&0&a_{xy}&a_{xz}&0&0&a_{yy}&a_{yz}&a_{zz}\\
&b_{xx}&0&b_{xy}&b_{xz}&0&b_{yy}&b_{yz}&b_{zz}&&&&&&\\
&&b_{xx}&0&b_{xy}&b_{xz}&0&b_{yy}&b_{yz}&b_{zz}&&&&&\\
&&&b_{xx}&0&0&b_{xy}&b_{xz}&0&0&b_{yy}&b_{yz}&b_{zz}&&\\
&&&&b_{xx}&0&0&b_{xy}&b_{xz}&0&0&b_{yy}&b_{yz}&b_{zz}&\\
&&&&&b_{xx}&0&0&b_{xy}&b_{xz}&0&0&b_{yy}&b_{yz}&b_{zz}\\
&c_{xx}&0&c_{xy}&c_{xz}&0&c_{yy}&c_{yz}&c_{zz}&&&&&&\\
&&c_{xx}&0&c_{xy}&c_{xz}&0&c_{yy}&c_{yz}&c_{zz}&&&&&\\
&&&&c_{xx}&0&0&c_{xy}&c_{xz}&0&0&c_{yy}&c_{yz}&c_{zz}&\\
&&&&&c_{xx}&0&0&c_{xy}&c_{xz}&0&0&c_{yy}&c_{yz}&c_{zz}
\end{bmatrix}.$$

We can see a pattern between the rows and between the columns in this matrix.

Third, we know that if the system $P_1 = \ldots = P_n = 0$ has a nontrivial solution, then there exists a nonzero solution for the system of linear equations

$$\mathbf{M}\mathbf{x} = \mathbf{0}. \tag{5.1}$$

The question arising here is can we get the solution of $P_1 = \ldots = P_n = 0$ from $\mathbf{x}$, a solution of (5.1). We know that if

$$\mathbf{v}_j = [\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}]^T \quad \text{where } \alpha_{ij} \neq 0 \text{ for } i = 1, \ldots, n$$

are the solutions of $P_1 = \ldots = P_n = 0$, then $|\mathrm{M}| = 0$ implies there exists nontrivial solutions for $P_1 = \ldots = P_n = 0$. Moreover, we believe that these solutions can be obtained from the solution $\mathbf{x}$. One way to overcome the problem that some of the α_{ij} are zero is to make the substitutions $x_k = x_k + \beta_k$, where $\beta_k \neq 0$ for all k such that $\alpha_{kj} = 0$. But, how do we know which variable will be equal to 0 in the solutions? If we can get a set of criteria for this condition than we think that we can come up with a constructive proof for Theorem 3.5. One more question arising is whether the rank of M tells us anything about the number of solutions that $P_1 = \ldots = P_n = 0$ has, as in the bivariate case.

Finally, the issue of specialization of the coefficients needs some treatment. The major obstacle here is that $|\Delta\mathrm{M}|$ may vanish when we specialize the coefficients. One way to tackle it is to apply Theorem A.6; that is, compute $|\Delta\mathrm{M}|$ first. And then figure out which coefficients of $P_1, \ldots, P_n$ cause $|\Delta\mathrm{M}|$ to vanish. We can make $|\Delta\mathrm{M}| \neq 0$ by applying an appropriate linear transformation to the variables. Then the resulting resultant is the same as the original one.

5.2 Curve and Surface Intersections

There are still open questions for the implicitization, inversion and intersection of parametric rational curves/surfaces.

First, we know that the Bezout matrix is symmetric. Is there any geometric significance to the fact that this matrix is symmetric?

Second, we already have the solutions for the implicitization and inversion of 3D parametric rational cubic curves; these solutions can be used to generate an optimal, robust intersection algorithm. What about the 3D parametric rational curves of higher degree? In order to answer this question, we must find the answers to the following questions:

- Can we get the special resolvents for three univariate polynomials of arbitrary degree?
- We know that a 3D rational curve of arbitrary degree can always be represented as the intersection of three algebraic surfaces together with some residual curves [Abhy69]. Thus, an exact implicitization may require many surfaces. Could we use these surfaces in an intersection algorithm?

5.3 Floating Point Implementation of Intersection Algorithms

In this section, we only discuss the difficulties we faced for the curve/curve intersection algorithms. Here, we do not include the issue of stability of the problem of curve/curve intersection. We only raise the questions concerned with the experimental aspects of this problem.

The first question is what values of the tolerances, which are based on the degrees and coefficients of the input curves, are acceptable. These values should answer the following questions:

- What are the criteria to stop the Gaussian elimination process, because there is an extremely small probability that the Bezout matrix will be singular in floating point arithmetic? In addition, in our observation from experiments, after a couple of elimination steps, the entries in each row are in decreasing order. Hence, what is a suitable value of the pivot for it to be considered equal to zero along with the rest of the matrix?

- How small must a coefficient of the input curves be to be considered insignificant, i.e., equal 0?

- When the solutions obtained are close together, then what are the criteria for accepting these roots?

In the projection algorithm presented in Chapter 4, we compute the intersection points of two curves in parameter s. And then, we substitute this value of s into the curve $C_1(s)$ to get one of the values of x, y, and z to solve for t. Since two 3D curves can have the same value in one or two axes but the other two or one axes are different, we have to choose an axis which avoids extra roots in t. The question here is which of the three axes do we choose.

The final issue is what is the interpretation of complex roots. If the complex solutions have a very small imaginary part, then can we ignore the imaginary part and consider them to be real solutions.

Bibliography

[Abhy69] S. S. Abhyankar, "A Glimpse of Algebraic Geometry", *Lokamanya Tilak Memorial Lectures,* University of Poona, 1969.

[Abhy87a] S. S. Abhyankar and C. Bajaj, "Automatic Parameterization of Rational Curves and Surfaces 1: Conics and Conicoids", *Computer-Aided Design,* Vol. 19, No. 1, Jan./Feb. 1987, pp. 11–14.

[Abhy87b] S. S. Abhyankar and C. Bajaj, "Automatic Parametrization of Rational Curves and Surfaces II: Cubics and Cubicoids", *Computer-Aided Design,* Vol. 19, No. 9, Nov. 1987, pp. 499–502.

[Abhy88a] S. S. Abhyankar and C. Bajaj, "Automatic Parametrization of Rational Curves and Surfaces III: Algebraic Plane Curves", *Computer Aided Geometric Design,* (to appear).

[Abhy88b] S. S. Abhyankar and C. Bajaj, "Automatic Parametrization of Rational Curves and Surfaces IV: Algebraic Space Curves", *Computer Aided Geometric Design,* (to appear).

[Atkin] K. E. Atkinson, *An Introduction to Numerical Analysis*, John Wiley & Sons, Toronto, 1978.

[Ball] D. H. Ballard and C. M. Brown, *Computer Vision,* Prentice-Hall Inc., Englewood Cliffs, N.J., 1982.

[Ben-Or] M. Ben-Or and P. Tiwari, "A Deterministic Algorithm for Sparse Multivariate Polynomial Interpolation," *Proc. 20th Annual ACM Symp. Theory Comp.,* pp. 301–309, 1988.

[Bohm] W. Bohm, G. Farin and J. Kahmann, "A Survey of Curve and Surface Methods in CAGD", *Computer-Aided Geometric Design,* Vol. 1, 1984, pp. 1–60.

[Buch65] B. Buchberger, "An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal(German)," Ph.D. Thesis, University of Innsbruck, Math. Inst., 1965.

[Buch70] B. Buchberger, "An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations(German)," *Aequationes Mathematicae 4,* No. 3, 1970, pp. 374-383.

[Buch76a] B. Buchberger, "A Theoretical Basis for the Reduction of Polynomials to Canonical Forms", *ACM SIGSAM Bull. 10,* No. 3, 1976, pp. 19-29.

[Buch76b] B. Buchberger, "Some Properties of Gröbner Bases for Polynomial Ideals", *ACM SIGSAM Bull. 10*, No. 4, 1976, pp. 19-24.

[Buch83] B. Buchberger, "A Note on the Complexity of Constructing Grobner-Bases," Proc. EUROCAL '83, London, March 1983, (J. A. van Hulzen, ed.), *Lecture Notes in Computer Science 162,* Springer-Verlag, 1983, pp. 137–145.

[Buch85] B. Buchberger "Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory" in *Multidimensional Systems Theory,* (N.K. Bose, ed.), D. Reidel Publishing Company, 1985, pp. 184-232.

[Can87] J. F. Canny, *The Complexity of Robot Motion Planning,* Ph. D. Thesis, The MIT Press, Cambridge, Massachusetts, 1987.

[Can88] J. F. Canny, E. Kaltofen, and L. Yagati, "Solving Systems of Non-Linear Polynomial Equations Faster", *ISSAC '89* Proceeding, Portland, Oregon, 1989.

[Carlbo] I. Carlbom, " An Algorithm for Geometric Set Operations Using Cellular Subdivision Techniques, " *IEEE Computer Graphics and Applications,* Vol. 7, No. 5, 1987, pp. 44–55.

[Czapor] S.R. Czapor, "Grobner Basis Methods for Solving Algebraic Equations", Ph. D. Thesis, University of Waterloo, 1988.

[Farin] G. Farin, *Curves and Surfaces for Computer Aided Geometric Design, A Practical Guide,* Academic Press Inc., San Diego, 1988.

[Goldm84] R.N. Goldman, T.W. Sederberg and D. C. Anderson, "Vector Elimination: A Technique for the Implicitization, Inversion, and Intersection of Planar Parametric Rational Polynomial Curves ", *Computer Aided Geometric Design,* Vol. 1, 1984, pp. 327–356.

[Goldm85] R.N. Goldman, "The Method of Resolvents: a Technique for the Implicitization, Inversion, and Intersection of Non-planar, Parametric, Rational Cubic Curves ", *Computer Aided Geometric Design,* Vol. 2, 1985, pp. 237–255.

[Hoffm88] C. Hoffman, "Applying Algebraic Geometry to Surface Intersection Evaluation," *Notes for a course on Algebraic Geometry at SIGGRAPH 1988.*

[Herst] I. N. Herstein, *Topics in Algebra*, 2nd Edition, John Wiley & Sons, Inc., New York, 1975, pp. 170–206.

[Hurwit] A. Hurwitz, " Über die Trägheitsformen eines algeraischen Moduls," *Annali di Mat.,* Ser. III, Tomo XX, 1913, pp. 113-151.

[Kalto] E. Kaltofen and B. Trager, "Computing with Polynomials Given by Black Boxes for Their Evaluations: Greatest Common Divisors, Factorization, Separation of Numerators and Denominators", *Proc. 29th Annual Symp. Foundation of Comp. Sci.,* pp. 296–305, 1988.

[Lazard] D. Lazard, "Grobner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations", Proc. EUROCAL '83, London, March 1983, (J. A. van Hulzen, ed.), *Lecture Notes in Computer Science 162,* Springer–Verlag, 1983, pp. 146–156.

[Mac02] F. S. Macaulay, " Some Formulae in Elimination", *London Mathematical Society Proceedings,* London, May 1902 to Jan. 1903, Vol. 35, pp. 3–27.

[Mac16] F. S. Macaulay, *The Algebraic Theory of Modular Systems,* Cambridge University Press, Cambridge, 1916.

[Maple] B. W. Char, K. O. Geddes, G. H. Gonnet, M. B. Monagan, and S. M. Watt, *Maple User's Guide*, 5th Ed., WATCOM, Waterloo, 1988.

[Mertens] F. Mertens, " Über die bestimmenden Eigenschaften der Resultante von n Formen mit n Veränderlichen," *Sitzungsberichte der Kais. Akad. d. Wissenschaften zu Wien,* Bd. 93, 1896.

[Montau] Y. De Montaudouin and W. Tiller, "The Cayley Method in Computer aided Geometric Design", *Computer aided Geometric Design,* Vol. 1, 1984, pp. 309–326.

[Morten] M. E. Mortenson, *Geometric Modeling*, John Wiley & Sons, New York, 1985.

[Neff88] A. C. Neff, "Decomposing Algebraic Sets using Gröbner Bases," Res. Rep., RC 13993(#62793), IMB Res. Div., T.J. Watson Res. Cent., 9/2/88.

[Pat88a] R. R. Patterson, " Parametric Cubics as Algebraic Curves", *Computer Aided Geometric Design,* No. 5, 1988, pp. 139–159.

[Pat88b] R. R. Patterson, " Parametrizing and Graphing Nonsingular Cubic Curves", *Computer Aided Design,* Vol. 20, No. 10, Dec. 1988, pp. 615–623.

[Rosenf] A. Rosenfeld and A. C. Kak, *Ditgital Picture Processing,* Vol. 1,2, Academic Press Inc., Orlando, Fl., 1982.

[Seder84b] T.W. Sederberg, D.C. Anderson, and R.N. Goldman, "Implicit Representation of Parametric Curves and Surfaces", *Computer Vision, Graphics, and Image Processing,* Vol. 28, 1984, pp. 72-84.

[Waerd] B. L. van der Waerden, *Modern Algebra,* 3rd Edition, F. Ungar Publishing Co., New York, 1950.

[Wiede] D. H. Wiedemann, "Solving Sparse Linear Equations over Finite Fields", *IEEE Transactions on Information Theory,* Vol. 32, No. 1, Jan. 1985, pp. 54–62.

[Zipple] R. E. Zipple, "Interpolating Polynomials from Their Values," *J. Symbolic Comput.,* to appear, 1990.

Appendix A

The Multivariate Resultant

In [Mac02] and [Mac16], Macaulay shows that the matrix $\Delta \mathrm{M}(n,d)$ defined in Chapter 3 is a submatrix of the Macaulay matrix $\mathrm{M}(n,d) = \mathrm{M}_n(n,d)$, and proves that the resultant $\mathcal{R}(n,d)$ is a ratio between $|\mathrm{M}(n,d)|$ and $|\Delta \mathrm{M}(n,d)|$. We believe that Macaulay's proofs are hard to follow, are missing significant details, and may contain some errors. In this appendix, we try to improve Macaulay's proofs by filling in some missing details and giving a better description. Even with these improvements, there are still some gaps in the proof.

Again, we will treat the coefficients of $P_1, \ldots, P_n$ as indeterminates. First, we prove the fundamental theorem of the resultant theory.

Theorem A.1 *Let $1 \leq p \leq n$ and $0 \leq m$. Any homogeneous polynomial G of degree m in $x_1, \ldots, x_n$ can be expressed uniquely as*

$$G = P_1 Q_0 + P_2 Q_1 + \cdots + P_p Q_{p-1} + \hat{Q}_p, \tag{A.1}$$

where $Q_i \in \Omega_{i,m}$, for $i = 0, 1, \ldots, p-1$, and $\hat{Q}_p \in \hat{\Omega}_{p,m}$. Equivalently, $\mathrm{M}_p(n,m)$ is nonsingular.

Proof: Equating coefficients of the monomials on the two sides of equation (A.1) we obtain the system of N_m linear equations

$$\mathbf{M}_p^T(n,m)\mathbf{c} = \mathbf{g},$$

where $\mathbf{M}_p(n,m)$ is an N_m by N_m Macaulay matrix, $\mathbf{g}$ is a vector of dimension N_m consisting of the coefficients of G, and $\mathbf{c}$ is a vector of dimension N_m consisting of the coefficients of $Q_0, \ldots, Q_{p-1}, \hat{Q}_p$. We want to show that $\mathbf{M}_p^T(n,m)$ is nonsingular symbolically. That is, for any given $P_1, \ldots, P_p$, which are nonzero homogeneous polynomials, (A.1) can be satisfied for $G = 0$ if and only if $Q_0, \ldots, Q_{p-1}, \hat{Q}_p$ all vanish.

Now, suppose that $\mathbf{M}_p^T(n,m)$ is symbolically singular, then $G = 0$ could be satisfied without $Q_0, \ldots, Q_{p-1}, \hat{Q}_p$ all vanishing. In particular, for the specialization $P_i = x_i^{d_i}$ for $i = 1, \ldots, p$, there exists the same nontrivial $Q_0, \ldots, Q_{p-1}, \hat{Q}_p$ such that

$$x_1^{d_1}Q_0 + x_2^{d_2}Q_1 + \cdots + x_{p-1}^{d_{p-1}}Q_{p-2} + x_p^{d_p}Q_{p-1} + \hat{Q}_p = 0. \tag{A.2}$$

But this is not possible because the matrix $\mathbf{M}_p(n,m)$ corresponding to (A.2) is a diagonal matrix with nonzero entries. Hence, all the coefficients $Q_0, \ldots, Q_{p-1}, \hat{Q}_p$ must be equal zero. Thus, $\mathbf{M}_p^T(n,m)$ is nonsingular, i.e., there exists a unique set of values of the unknown $\mathbf{c}$, or in other words, $Q_0, \ldots, Q_{p-1}, \hat{Q}_p$ can be chosen in one and only one way so as to satisfy the equation (A.1). □□

Note that this theorem also applies for any permutation π of the polynomials $P_1, \ldots, P_n$, i.e., $(R_1, \ldots, R_n) = (P_{\pi(1)}, \ldots, P_{\pi(n)})$, where R_i is a homogeneous polynomial in $x_{\pi(1)}, \ldots, x_{\pi(n)}$ of degree $d_{\pi(i)}$.

Let

$$|\Delta\mathbf{M}(n,m)| = \frac{|\mathbf{M}(n,m)|}{\mathcal{R}(n,m)}$$

for one of the arrangement of $P_1, \ldots, P_n$, say $(P_1, P_2, \ldots, P_n)$. We wish to find an expression for $|\Delta \mathrm{M}(n,m)|$ in terms of the coefficients of the polynomials. Then one important property of $|\Delta \mathrm{M}(n,m)|$ is given in the following lemma.

Lemma A.2 *: $|\Delta \mathrm{M}(n,m)|$ is independent of the coefficients of P_n. Also, the degree of $\mathcal{R}(n,m)$ in the coefficients of P_n is equal to the number of monomials in $\mathcal{X}_{n-1,m}$.*

Proof : Let π be a different order of the polynomials $P_1, \ldots, P_n$ in $x_1, \ldots, x_n$; and let $|\mathrm{M}^\pi(n,m)|$ denote the determinant of the Macaulay matrix $\mathrm{M}^\pi(n,m)$ for this order. Thus, $\mathrm{M}^\pi(n,m)$ is the Macaulay matrix corresponding to

$$P_{\pi(1)} R_0^\pi + \cdots + P_{\pi(n)} R_{n-1}^\pi + \hat{R}_n^\pi, \tag{A.3}$$

where $R_i^\pi \in \Omega_{i,m}^\pi$ and $\hat{R}_n^\pi \in \hat{\Omega}_{n,m}^\pi$.

Now, let G be a general member of the module $(P_1, \ldots, P_n)$ of degree m. That is

$$G = P_1 R_0 + P_2 R_1 + \cdots + P_{n-1} R_{n-2} + P_n R_{n-1} = \mathbf{c}^T \mathrm{M}(n,m) \mathbf{x}, \tag{A.4}$$

where $R_i \in \Omega_{i,m}$, and $\mathbf{c}$ and $\mathbf{x}$ are the vectors corresponding to the coefficients of $R_0, \ldots, R_{n-1}$ and to the monomials in $x_1, \ldots, x_n$ of degree m, respectively. By Theorem A.1, we can bring G to the form

$$G = P_{\pi(1)} R_0^\pi + \cdots + P_{\pi(n)} R_{n-1}^\pi = (\mathbf{c}^\pi)^T \mathrm{M}^\pi(n,m) \mathbf{x}. \tag{A.5}$$

Equating the power products of equation (A.4) and equation (A.5), we have

$$\mathbf{c}^T \mathrm{M}(n,m) = (\mathbf{c}^\pi)^T \mathrm{M}^\pi(n,m).$$

For simplicity, we drop (n,m) from the matrices $\mathrm{M}(n,m)$ and $\mathrm{M}^\pi(n,m)$. According to Theorem A.1, the matrices M and M^π are nonsingular. Thus, we have

$$\mathbf{c} = (\mathbf{M}^T)^{-1}(\mathbf{M}^\pi)^T\mathbf{c}^\pi.$$

Hence, the ratio of $|\mathbf{M}|$ to $|\mathbf{M}^\pi|$ is

$$\frac{|\mathbf{M}^\pi|}{|\mathbf{M}|} = \frac{\mathcal{R}|\Delta\mathbf{M}^\pi|}{\mathcal{R}|\Delta\mathbf{M}|} = \frac{|\Delta\mathbf{M}^\pi|}{|\Delta\mathbf{M}|} = |\mathbf{T}|, \qquad (A.6)$$

where $\mathbf{c} = \mathbf{T}\mathbf{c}^\pi$ and $\mathbf{T} = (\mathbf{M}^T)^{-1}(\mathbf{M}^\pi)^T$.

Now, we describe a method for expressing $c_1, \ldots, c_{N_m}$ in terms of $c_1^\pi, \ldots, c_{N_m}^\pi$ and the coefficients of $P_1, \ldots, P_n$ such that $|\mathbf{T}|$ is a rational function of the coefficients of $P_1, \ldots, P_n$ whose denominator is independent of the coefficients of P_n. In other words, we express

$$G = P_1A_0 + P_2A_1 + \cdots + P_nA_{n-1}, \qquad (A.7)$$

where $A_i = R^\pi_{\pi^{-1}(i-1)}$, in the form

$$G = P_1R_0 + P_2R_1 + \cdots + P_nR_{n-1}, \qquad (A.8)$$

or we find the solution of

$$P_1R_0 + P_2R_1 + \cdots + P_nR_{n-1} = P_1A_0 + P_2A_1 + \cdots + P_nA_{n-1}, \qquad (A.9)$$

where A_i's are given and R_i's are the unknowns.

First, we want to find the coefficients of the polynomials $Q_0^{(1)}, \ldots, Q_{n-2}^{(1)}, \hat{Q}_{n-1}^{(1)}$ in

$$A_{n-1} = P_1Q_0^{(1)} + P_2Q_1^{(1)} + \cdots + P_{n-1}Q_{n-2}^{(1)} + \hat{Q}_{n-1}^{(1)}, \qquad (A.10)$$

where $Q_i^{(1)} \in \Omega_{i,m-d_n}$ for $i = 0, \ldots, n-2$ and $\hat{Q}_{n-1} \in \hat{\Omega}_{n,m-d_n}$. Here the coefficients of $Q_0^{(1)}, \ldots, Q_{n-2}^{(1)}, \hat{Q}_{n-1}^{(1)}$ are found as follows: By Theorem A.1 equation (A.10) can be written in vector notation as

$$\mathbf{v}^T\mathbf{B}\mathbf{x} = \mathbf{a}^T\mathbf{x},$$

where $\mathbf{v}$ is the coefficients of the unknown polynomials, $\mathbf{a}$ is the coefficients of A_{n-1}, $\mathbf{x}$ is the monomials of degree $m-d_n$, and $\mathbf{B}$ is a nonsingular square matrix. Thus, we have

$$\mathbf{v} = adj(\mathbf{B}^T)\mathbf{a}/|\mathbf{B}|,$$

in which the denominator of $\mathbf{v}$ does not involve the coefficients of the polynomials on the left hand side of (A.10).

Substituting A_{n-1} in (A.10) into (A.7), we have

$$G = P_1(A_0 + Q_0^{(1)}P_n) + P_2(A_1 + Q_1^{(1)}P_n) + \cdots + P_{n-1}(A_{n-2} + Q_{n-2}^{(1)}P_n) + P_n\hat{Q}_{n-1}^{(1)}, \tag{A.11}$$

where $Q_0^{(1)}, \ldots, Q_{n-2}^{(1)}, \hat{Q}_{n-1}^{(1)}$ have been found.

Similarly, we can find the coefficients of $Q_0^{(2)}, \ldots, Q_{n-3}^{(2)}, \hat{Q}_{n-2}^{(2)}$ in equation

$$A_{n-2} + Q_{n-2}^{(1)}P_n = P_1Q_0^{(2)} + P_2Q_1^{(2)} + \cdots + P_{n-2}Q_{n-3}^{(2)} + \hat{Q}_{n-2}^{(2)}, \tag{A.12}$$

where $Q_i^{(2)} \in \Omega_{i,m-d_{n-1}}$ for $i = 0, \ldots, n-3$, and $\hat{Q}_{n-2} \in \hat{\Omega}_{n,m-d_{n-1}}$, in the same manner. Hence, we have a unique solution for these coefficients.

Thus, we can proceed in this way until (A.7) becomes

$$G = P_1\hat{Q}_0^{(n)} + P_2\hat{Q}_1^{(n-1)} + \cdots + P_{n-1}\hat{Q}_{n-2}^{(2)} + P_n\hat{Q}_{n-1}^{(1)}. \tag{A.13}$$

It follows that (A.13) has to be equal to (A.8), i.e., $R_0 = \hat{Q}_0^{(n)}, \ldots, R_{n-1} = \hat{Q}_{n-1}^{(1)}$. Thus, all the coefficients of R_i has been found in terms of the coefficients of A_i and P_i.

In this method, the denominators of the $Q_i^{(k)}$ and $\hat{Q}_i^{(k)}$ depend on the coefficients of $P_1, \ldots, P_{n-1}$ only and not those of P_n. Thus $|\mathbf{T}|$ is a rational function of the coefficients of $P_1, \ldots, P_n$ whose denominator is independent of the coefficients of P_n.

Now assume that $|\Delta\mathbf{M}|$ and $|\Delta\mathbf{M}^{\pi}|$ have a common factor, C, that is a polynomial in the coefficients of P_n. Then we have

$$|\Delta\mathbf{M}| = CF_1 \text{ and } |\Delta\mathbf{M}_i| = CF_i \text{ for } i = 2, \ldots, n$$

where $|\Delta\mathbf{M}_i| = |\mathbf{M}_i|/\mathcal{R}_i$, for the other $(n-1)$ arrangements of $P_1, \ldots, P_n$. This contradicts the fact that $\mathcal{R}$ is the gcd of n Macaulay determinants. Thus, $|\Delta\mathbf{M}|$ is independent of the coefficients of P_n.

Furthermore, the degree of $|\mathbf{M}|$ in the coefficients of P_n is the number of rows in the matrix $\mathbf{M}$ corresponding to P_n. This number is exactly the number of monomials in $\mathcal{X}_{n-1,m}$. Since $|\Delta\mathbf{M}|$ is independent of the coefficients of P_n, $\mathcal{R}$ has the same degree in the coefficients of P_n as $|\mathbf{M}(n,m)|$.□□

From the above lemma we can explicitly give the degree of the $\mathcal{R}(n,d)$ in the coefficients of P_i's. Let

$$D_i = \prod_{j=1, j \neq i}^{n} d_j$$

Then, when $m = d$, we can easily show that the numbers of monomials in $\mathcal{X}_{n-1,d}$ is D_n. This can be seen from the fact that R_{n-1} has degree $d - d_n$ and it is reduced in $x_1, \ldots, x_n$. Thus, the monomials in $\mathcal{X}_{n-1,d}$ are all the power products in

$$(1 + x_1 + \cdots + x_1^{d_1 - 1}) \ldots (1 + x_{n-1} + \cdots + x_{n-1}^{d_{n-1} - 1}),$$

each multiplied by an appropriate power of x_n. Therefore, the number of monomials in $\mathcal{X}_{n-1,d}$ is $d_1 \ldots d_{n-1} = D_n$. By Lemma A.2 the degree of $\mathcal{R}(n,d)$ in the coefficients of P_n is D_n. The general result is given in the following lemma.

Lemma A.3 : *The degree of $\mathcal{R}(n,d)$ in the coefficients of P_i is D_i for $i = 1, \ldots, n$.*

Proof: It follows from the fact that $\mathcal{R}(n,d)$ is the gcd of n $|\mathbf{M}^{\pi}(n,d)|$ and the above observation. □□

From now on, we pay attention to $\mathcal{R}(n,d)$ even though the proofs given here are valid for any degree m. From the fact that $\Delta\mathbf{M}(n,d)$ is independent of the coefficients of P_n, we find an explicit expression for $|\Delta\mathbf{M}(n,d)|$. In order to get this expression, we need to introduce some new notations.

Let $P_i^{(p)}$ denotes the value of P_i when $x_{p+1},\ldots,x_n$ are all zero; so that $P_i^{(p)}$ is a homogeneous polynomial in p variables $x_1,\ldots,x_p$ of degree d_i. Let $|\mathbf{M}^p(p,m)|$, $p \leq n$, denote the determinant of the matrix $\mathbf{M}^{(p)}(p,m)$ corresponding to the degree m polynomial equation

$$G = P_1^{(p)}Q_0 + P_2^{(p)}Q_1 + \cdots + P_{p-1}^{(p)}Q_{p-2} + P_p^{(p)}Q_{p-1} + \hat{Q}_p, \qquad (A.14)$$

where $Q_i \in \Gamma_{i,m}$ and $\hat{Q}_p \in \hat{\Gamma}_{p,m}$. Here, p is the number of variables and the number of polynomials. The sets $\Gamma_{i,m}$ and $\hat{\Gamma}_{p,m}$ are similar to the set $\Omega_{i,m}$ and $\hat{\Omega}_{n,m}$, in which $P_1^{(p)},\ldots,P_p^{(p)}$ are used instead of $P_1,\ldots,P_n$. Hence, the construction of $\mathbf{M}^{(p)}(p,m)$ is similar to the construction of $\mathbf{M}_n(n,m)$. $\mathcal{R}(p,m)$ denotes the gcd of the p determinants like $|\mathbf{M}^{(p)}(p,m)|$, formed from p cyclic arrangements of $P_1^{(p)},\ldots,P_p^{(p)}$.

We want to explain the construction of the Macaulay-like matrix, $\mathbf{M}_*(n,m)$, whose determinant vanishing is the condition that the polynomial equation

$$P_1Q_{0,m} + P_2Q_{1,m} + \cdots + P_{n-1}Q_{n-2,m} = x_n^{d_n}Q_{n-1,m} \qquad (A.15)$$

of degree m, $Q_{i,m} \in \Omega_{i,m}$, can be satisfied for $0 \leq i \leq n-1$, where not all $Q_{i,m}$ are zero. Note that the monomials in $x_n^{d_n}Q_{n-1,m}$ are the monomials in $\hat{\mathcal{X}}_{n-1,m}$. Thus, the columns of $\mathbf{M}_*(n,m)$ correspond to the $(N_m - |\hat{\mathcal{X}}_{n-1,m}| - |\hat{\mathcal{X}}_{n,m}|)$ monomials in

$$\hat{\mathcal{X}}_m - \hat{\mathcal{X}}_{n-1,m} - \hat{\mathcal{X}}_{n,m} = \bigcup_{i=0}^{n-2} \hat{\mathcal{X}}_{i,m},$$

and the rows contain the coefficients in

$$\bigcup_{i=0}^{n-2} \mathcal{X}_{i,m} P_{i+1}(x_1, \ldots, x_n).$$

If the rows of $\mathbf{M}(n,m)$ are arranged so that the rows corresponding to $\mathcal{X}_{n-1,m}P_n$ and the monomials in $\hat{\mathcal{X}}_{n,m}$ at the bottom and the columns of $\mathbf{M}(n,m)$ are arranged so that the the monomials in $\hat{\mathcal{X}}_{n-1,m}$ and $\hat{\mathcal{X}}_{n,m}$ are to the right, then $\mathbf{M}_*(n,m)$ is a leading square submatrix of $\mathbf{M}(n,m)$.

Referring back to Example 3.2.2, we want to construct a matrix whose determinant vanishing is the condition that the polynomial equation

$$P_1 Q_{0,4} + P_2 Q_{1,4} = z^2 Q_{2,4} \tag{A.16}$$

of degree 4 can be satisfied for $Q_{i,4} \in \Omega_{i,4}$ (not all zero). The 11 by 11 matrix is

$$\begin{bmatrix}
a_{xx} & a_{xy} & a_{xz} & a_{yy} & a_{zz} & a_{yz} & 0 & 0 & 0 & 0 & 0 \\
0 & a_{xx} & 0 & a_{xy} & 0 & a_{xz} & 0 & a_{yy} & 0 & 0 & a_{yz} \\
0 & 0 & a_{xx} & 0 & a_{xz} & a_{xy} & 0 & 0 & 0 & 0 & a_{yy} \\
0 & 0 & 0 & a_{xx} & 0 & 0 & a_{yy} & a_{xy} & a_{yz} & a_{zz} & a_{xz} \\
0 & 0 & 0 & 0 & a_{xx} & 0 & 0 & 0 & 0 & a_{yy} & 0 \\
0 & 0 & 0 & 0 & 0 & a_{xx} & 0 & 0 & a_{yy} & a_{yz} & a_{xy} \\
0 & 0 & 0 & b_{xx} & 0 & 0 & b_{yy} & b_{xy} & b_{yz} & b_{zz} & b_{xz} \\
0 & b_{xx} & 0 & b_{xy} & 0 & b_{xz} & 0 & b_{yy} & 0 & 0 & b_{yz} \\
0 & 0 & 0 & 0 & 0 & b_{xx} & 0 & 0 & b_{yy} & b_{yz} & b_{xy} \\
0 & 0 & 0 & 0 & b_{xx} & 0 & 0 & 0 & 0 & b_{yy} & 0 \\
0 & 0 & b_{xx} & 0 & b_{xz} & b_{xy} & 0 & 0 & 0 & 0 & b_{yy}
\end{bmatrix}.$$

This kind of matrix will be used in the proof of Lemma A.4.

Now if we consider $|\mathbf{M}(n,d)|$, $\mathcal{R}(n,d)$, and $|\Delta\mathbf{M}(n,d)|$ as polynomials in the coefficients of P_n, then $|\Delta\mathbf{M}(n,d)|$ is a constant while $|\mathbf{M}(n,d)|$ and $\mathcal{R}(n,d)$ have the same degree. Thus, finding the ratio between $|\mathbf{M}(n,d)|$ and $\mathcal{R}(n,d)$, i.e., $|\Delta\mathbf{M}(n,d)|$, in terms of the coefficients of $P_1,\ldots,P_{n-1}$ is equivalent to finding the ratio between the coefficients of $(a^{(n)}_{0,\ldots,d_n})^{D_n}$, in $|\mathbf{M}(n,d)|$ and $\mathcal{R}(n,d)$, by Lemma A.3. This ratio is given in

Lemma A.4 .

$$|\Delta\mathbf{M}(n,d)| = \frac{|\mathbf{M}(n,d)|}{\mathcal{R}(n,d)} = \frac{\prod\limits_{p=0}^{d-1} |\mathbf{M}^{(n-1)}(n-1,d-p)|}{\prod\limits_{q=0}^{d_n-1} \mathcal{R}(n-1,d-q)} \tag{A.17}$$

Proof : First, we can see that $a^{(n)}_{0,\ldots,d_n}$ appears in the diagonal on D_n rows of $\mathbf{M}(n,d)$. Thus, the coefficient of $(a^{(n)}_{0,\ldots,d_n})^{D_n}$ in $\mathbf{M}(n,d)$ is $|\mathbf{M}_*| = |\mathbf{M}_*(n,d)|$, the determinant of the $(N-D_n)$-th order submatrix in the upper left corner of $\mathbf{M}(n,d)$. In terms of a polynomial equation, $\mathbf{M}_*$ is the Macaulay like matrix, whose vanishing is the condition that the degree d equation

$$P_1Q_{0,d} + P_2Q_{1,d} + \cdots + P_{n-1}Q_{n-2,d} = x_n^{d_n}Q_{n-1,d} \tag{A.18}$$

can be satisfied, where $Q_{i,d} \in \Omega_{i,d}$.

To find $|\mathbf{M}_*|$, we assume that (A.18) is satisfied and put $x_n = 0$. Then P_i becomes $P_i^{(n-1)}$, and $Q_{i,d}$ becomes $Q^*_{i,d}$. (A.18) becomes

$$P_1^{(n-1)}Q^*_{0,d} + P_2^{(n-1)}Q^*_{1,d} + \cdots + P_{n-1}^{(n-1)}Q^*_{n-2,d} = x_n^{d_n}Q^*_{n-1,d}. \tag{A.19}$$

Note that the determinant whose vanishing is equivalent to the satisfaction of condition (A.19) is $|\mathbf{M}^{(n-1)}(n-1,d)|$. Hence, we have either $|\mathbf{M}^{(n-1)}(n-1,d)|$=0, or $Q^{*}_{0,d}, \ldots, Q^{*}_{n-2,d}$ all vanishing. In the latter case, $Q_{0,d}, \ldots, Q_{n-2,d}$ are all divisible by x_n, and dividing it out, we have the degree $d-1$ equation

$$P_1^{(n-1)} Q_{0,d-1} + P_2^{(n-1)} Q_{1,d-1} + \cdots + P_{n-1}^{(n-1)} Q_{n-2,d-1} = x_n^{d_n - 1} Q_{n-1,d-1}, \qquad \text{(A.20)}$$

where $Q_{i,d-1} \in \Omega_{i,d-1}$. Hence, $|\mathrm{M}^{(n-1)}(n-1, d-1)|$=0, or an equation similar to (A.20) of degree $d-2$ holds. This process continues until the degree is 1. Thus, we have

$$|\mathrm{M}_{*}| = \prod_{p=0}^{d-1} |\mathrm{M}^{(n-1)}(n-1, d-p)|.$$

Therefore,

$$|\mathrm{M}(n,d)| = (a^{(n)}_{0,\ldots,d_n})^{D_n} \prod_{p=0}^{d-1} |\mathrm{M}^{(n-1)}(n-1, d-p)| + \cdots. \qquad \text{(A.21)}$$

Now, we find the coefficient of $(a^{(n)}_{0,\ldots,d_n})^{D_n}$ in $\mathcal{R}(n,d)$. Let $\mathrm{M}^{\pi}(n,d)$ be the Macaulay matrix of the polynomials in the order π such that $\pi(1) = n$, $\pi(i) = i-1$ for $i = 2, \ldots, n$, i.e., $P_n, P_1, \ldots, P_{n-1}$. The vanishing of $|\mathrm{M}^{\pi}(n,d)|$, is the condition that the equation

$$P_{\pi(1)} Q_{0,d} + P_{\pi(2)} Q_{1,d} + \cdots + P_{\pi(n)} Q_{n-1,d} = 0 \qquad \text{(A.22)}$$

of degree d can be satisfied, where $Q_{i,d} \in \Omega^{\pi}_{i,d}$.

Let r be the number of monomials in $\mathcal{X}^{\pi}_{0,d}$. Then the coefficient of $(a^{(n)}_{0,\ldots,d_n})^{r}$ in $|\mathrm{M}^{\pi}(n,d)|$ is the determinant of the $(N-r)$-th order submatrix in the lower right corner of $\mathrm{M}^{\pi}(n,d)$, or the determinant whose vanishing is the condition that the equation

$$P_{\pi(2)} Q_{1,d} + \cdots + P_{\pi(n)} Q_{n-1,d} = x_{\pi(1)}^{d_{\pi(1)}} Q_{0,d} \qquad \text{(A.23)}$$

of degree d can be satisfied. We can find $(a^{(n)}_{0,\ldots,d_n})^{D_n}$ by a similar process to finding the expression of $(a^{(n)}_{0,\ldots,d_n})^{D_n}$ in $\mathrm{M}(n,d)$ above. In this case, we stop when the degree of the equation is $d-(d_n-1)$ because $Q_{1,d},\ldots,Q_{n-1,d}$ are reduced in $x_{\pi(1)}=x_n$. Thus, the coefficient of $(a^{(n)}_{0,\ldots,d_n})^r$ in $|\mathrm{M}_\pi(n,d)|$ is

$$\prod_{p=0}^{d_n-1}|\mathrm{M}^{(n-1)}(n-1,d-p)|.$$

Now, keeping P_n fixed in the first position while altering the order of $P_1,\ldots,P_{n-1}$ in the last $n-1$ positions in $n-1$ ways, results in the gcd of the coefficients of $(a^{(n)}_{0,\ldots,d_n})^r$ being

$$\prod_{p=0}^{d_n-1}\mathcal{R}(n-1,d-p).$$

Thus, this is the coefficient of $(a^{(n)}_{0,\ldots,d_n})^{D_n}$ in $\mathcal{R}(n,d)$. Hence,

$$\mathcal{R}(n,d)=(a^{(n)}_{0,\ldots,d_n})^{D_n}\prod_{p=0}^{d_n-1}\mathcal{R}(n-1,d-p)+\cdots. \tag{A.24}$$

The lemma has been proved. □□

By definition of $\mathcal{R}(n-1,d)$, we have

$$\mathcal{R}(n-1,d)\;=\;\mathcal{R}(n-1,d-1)\;=\;\ldots\;=\;\mathcal{R}(n-1,d-d_n+1).$$

Thus,

$$\mathcal{R}(n,d)\;=\;(a^{(n)}_{0,\ldots,d_n})^{D_n}(\mathcal{R}(n-1,d-d_n+1))^{d_n}+\cdots \tag{A.25}$$

Furthermore, we can have that the expression for the coefficients of

$$(a^{(i)}_{0,\ldots,d_i,\ldots,0})^{D_i}(a^{(i+1)}_{0,\ldots,d_{i+1},\ldots,0})^{D_{i+1}}\cdots(a^{(n-1)}_{0,\ldots,d_{n-1},0})^{D_{n-1}}(a^{(n)}_{0,\ldots,d_n})^{D_n} \tag{A.26}$$

in $\mathcal{R}(n,d)$ is $(\mathcal{R}(i-1,d-d_i+1))^{D^{(i)}}$.

We have the explicit expression for $|\Delta\mathrm{M}(n,d)|$ in terms of the ratio of the product of the determinants of the Macaulay matrix of $P_1,\ldots,P_{n-1}$ in $x_1,\ldots,x_{n-1}$ of degree d to degree 1 to the resultant of $P_1,\ldots,P_{n-1}$ in $x_1,\ldots,x_{n-1}$ of degree d to degree $d-d_n+1$. But this expression is not very helpful for computing $\mathcal{R}(n,d)$.

We will show that $|\Delta\mathrm{M}(n,d)|$ is the determinant of the minor of the Macaulay matrix $\mathrm{M}(n,d)$ whose construction is given in Chapter 3.

Theorem A.5 *: $\Delta\mathrm{M}(n,d)$, where $|\Delta\mathrm{M}(n,d)| = |\mathrm{M}(n,d)|/\mathcal{R}(n,d)$, is the minor of $\mathrm{M}(n,d)$ obtained by deleting the columns of $\mathrm{M}(n,d)$ corresponding to the monomials reduced in any $n-1$ variables and the rows containing the coefficients of $x_i^{d_i}$ in P_i in the deleted columns.*

Proof : First, we can see that $\Delta\mathrm{M}(n,d)$ described in this theorem is the same matrix $\Delta\mathrm{M}(n,d)$ described in Section 3.2.3, Chapter 3. That is, matrix $\Delta\mathrm{M}(n,m)$ corresponding to the following equation

$$P_1Q_{0,m} + P_2Q_{1,m} + \cdots + P_{n-1}Q_{n-2,m} - \hat{Q}_m = 0, \tag{A.27}$$

where $Q_{i,m} \in \Phi_{i,m}$ and $\hat{Q}_m \in \hat{\Phi}_m$. Therefore, the vanishing of $|\Delta\mathrm{M}(n,m)|$ is the condition that (A.27) is satisfied, i.e., all the coefficients of the polynomials $Q_{i,m}, \hat{Q}_m$ are zero.

To avoid confusion in the notation, let the matrix described in this theorem be $\mathbf{A}(n,d)$. Second, to prove this theorem, it will be sufficient to show that

$$|\mathbf{A}(n,d)| = \prod_{p=0}^{d_n-1} |\mathbf{A}(n-1,d-p)| \prod_{p=d_n}^{d-1} |\mathrm{M}^{(n-1)}(n-1,d-p)|, \tag{A.28}$$

and to verify that

$$|\mathbf{A}(2,d)| = 1.$$

The verification for the bivariate case is trivial.

Now, we consider the multivariate case. Putting $x_n = 0$, let $Q_{i,d}^*$ and $\hat{Q}_d^*$ be the value of $Q_{i,d}$ and $\hat{Q}_d$ when $x_n = 0$, respectively; then $Q_{n-2,d}^* = 0$ and

$$P_1Q_{0,d} + P_2Q_{1,d} + \cdots + P_{n-1}Q_{n-2,d} = \hat{Q}_d, \tag{A.29}$$

where $Q_{i,d} \in \Psi_{i,d}$ and $\hat{Q}_d \in \hat{\Psi}_d$, becomes

$$P_1^{(n-1)}Q^*_{0,d} + P_2^{(n-1)}Q^*_{1,d} + \cdots + P_{n-2}^{(n-1)}Q^*_{n-3,d} = \hat{Q}^*_d. \tag{A.30}$$

Since $|\mathbf{A}(n-1,d)| = 0$ is the condition that (A.30) satisfies, either $|\mathbf{A}(n-1,d)| = 0$ or $Q^*_{0,d}, \ldots, Q^*_{n-3,d}, \hat{Q}^*_d$ all vanish. In the latter case, dividing x_n out of each $Q^*_{0,d}, \ldots, Q^*_{n-3,d}, \hat{Q}^*_d$ in (A.30) we have the degree $d-1$ equation

$$P_1 Q_{0,d-1} + P_2 Q_{1,d-1} + \cdots + P_{n-1} Q_{n-2,d-1} = \hat{Q}_{d-1}. \tag{A.31}$$

Hence, the part played by $x_n^{d_n}$ in (A.29) is now taken by $x_n^{d_n-1}$ in (A.31). So that in (A.31), any monomial is reduced or non-reduced in x_n means that it is non-divisible or divisible by $x_n^{d_n-1}$.

Again, putting $x_n = 0$ in (A.31), we have that either $|\mathbf{A}(n-1,d-1)| = 0$, or (A.29) still holds with d reduced to $d-2$ and $x_n^{d_n}$ to $x_n^{d_n-1}$. Proceeding in this way, we find that

$$|\mathbf{A}(n,d)| = |\mathbf{B}| \prod_{p=0}^{d_n-1} |\mathbf{A}(n-1,d-p)|, \tag{A.32}$$

where $|\mathbf{B}|$ is the determinant whose vanishing is the condition that (A.29) holds when d is reduced to $d-d_n$ and x_n to $x_n^0 = 1$. Thus, each $\hat{Q}_{d-j}$ for $0 \leq j < d_n$ is now non-reduced in x_n, and consequently $Q_{i,d-d_n}$ is in $\Omega_{i,d-d_n}$, and $\hat{Q}_{d-d_n} = 0$, since it is reduced in $x_1, \ldots, x_{n-1}$ and of degree $d-d_n$. Therefore, (A.27) becomes the degree $d-d_n$ equation

$$P_1 Q_{0,d-d_n} + P_2 Q_{1,d-d_n} + \cdots + P_{n-1} Q_{n-2,d-d_n} = 0, \tag{A.33}$$

where $Q_{i,d-d_n} \in \Omega_{i,d-d_n}$. By Lemma A.4 we have

$$|\mathbf{B}| = \prod_{p=d_n}^{d-1} |\mathbf{M}^{(n-1)}(n-1,d-p)|. \tag{A.34}$$

Therefore, $\mathbf{A}(n,d) = \Delta\mathbf{M}(n,d)$. □□

Like the bivariate case, the second important property of $\mathcal{R}(n,d) = \mathcal{R}(n)$ is given in the following theorem.

Theorem A.6 *: The resultant $\mathcal{R}(n)$ of $P_1, P_2, \ldots, P_n$ is irreducible in the sense that it cannot be resolved into two factors each of which is a function of the coefficients of these polynomials. Furthermore, $\mathcal{R}(n)$ is invariant for a homogeneous linear substitution*

$$\mathbf{B}\mathbf{x} = \mathbf{x}^*,$$

where $\mathbf{x} = (x_1, \ldots, x_n)^T$, $\mathbf{x}^* = (x_1^*, \ldots, x_n^*)^T$, and $\mathbf{B}$ is a nonsingular n by n matrix.

Proof : [Mac16] We will prove that $\mathcal{R}(n)$ is irreducible by induction since for the case $n = 2$ has already been shown.

Let $\mathcal{R}(n-1)$ be the resultant of $P_1^{(n-1)}, \ldots, P_{n-1}^{(n-1)}$, and assume that $\mathcal{R}(n-1)$ is irreducible.

Also, let $P_1^*, \ldots, P_{n-1}^*$, be homogeneous polynomials in $x_1, \ldots, x_{n-2}, x_0$ where

$$P_i^*(x_1, \ldots, x_{n-2}, x_0) = P_i(x_1, \ldots, x_{n-1}x_0, x_n x_0)$$

for $i = 1, \ldots, n-1$; then $\mathcal{R}_0(n-1)$ is the resultant of $P_1^*, \ldots, P_{n-1}^*$ in $x_1, \ldots, x_{n-2}$, x_0. Note that $\mathcal{R}_0(n-1)$ is a polynomial in x_{n-1}, x_n.

$\mathcal{R}^*(n)$ denotes the resultant of $P_1, \ldots, P_{n-1}, P_{*n}$, in $x_1, \ldots, x_n$ where

$$P_{*n} = P_n(0, \ldots, x_{n-1}, x_n) = a_{0,\ldots,d_n,0}^{(n)} x_{n-1}^{d_n} + \cdots + a_{0,\ldots,d_n}^{(n)} x_n^{d_n}.$$

Let $\mathcal{R}^0(2)$ be the resultant of $\mathcal{R}_0(n-1)$ and P_{*n} in x_{n-1} and x_n. In addition, $D_i^* = D_i/d_n$ for $i = 1, \ldots, n-1$.

Since the coefficient, a_{**}, of $x_0^{d_{n-1}}$ in P^*_{n-1} is

$$a_{**} = (a_{0,\dots,d_{n-1},0})^{(n-1)}(x_{n-1})^{d_{n-1}} + b_{**}(x_{n-1})^{d_{n-1}-1}x_n + \cdots + (a_{0,\dots,d_{n-1}})^{(n-1)}(x_n)^{d_{n-1}}, \tag{A.35}$$

by (A.25) we have

$$\mathcal{R}_0(n-1) = Q_1 x_{n-1}^{D_n} + Q_2 x_{n-1}^{D_n-1} x_n + \cdots \tag{A.36}$$

where Q_1 and Q_2 are functions of the coefficients of $P_1, \dots, P_{n-1}$. If $x_n = 0$, then $\mathcal{R}_0(n-1)$ becomes the resultant of $P_i(x_1, \dots, x_{n-1}x_0)$ for $i = 1, \dots, n-1$. Thus,

$$\mathcal{R}_0(n-1) = \mathcal{R}(n-1)(x_{n-1}^{D_n}),$$

or $Q_1 = \mathcal{R}(n-1)$. Also, $\mathcal{R}_0(n-1)$ has a term, i.e., (A.26),

$$(a^{(1)}_{d_1,\dots,0})^{D^*_1}(a^{(2)}_{0,d_2,\dots,0})^{D^*_2} \dots (a^{(n-2)}_{0,\dots,d_{n-2},0,0})^{D^*_{n-2}}(a_{**})^{D^*_{n-1}}$$

where a_{**} is in (A.35). Hence, Q_2 has a term

$$D^*_{n-1} b_{**}(a^{(1)}_{d_1,\dots,0})^{D^*_1}(a^{(2)}_{0,d_2,\dots,0})^{D^*_2} \dots (a^{(n-2)}_{0,\dots,d_{n-2},0,0})^{D^*_{n-2}}(a_{**})^{D^*_{n-1}},$$

and cannot be divisible by $\mathcal{R}(n-1)$, because $\mathcal{R}(n-1)$ does not involve b_{**}. Therefore, we find that

$$\mathcal{R}_0(n-1) = \mathcal{R}(n-1)x_{n-1}^{D_n} + Q_2 x_{n-1}^{D_n-1} x_n + \cdots \tag{A.37}$$

where Q_2 is neither zero nor divisible by $\mathcal{R}(n-1)$.

Now, if $\mathcal{R}^*(n)$=0, then one of the solutions of $P_{*n} = 0$ will be the same as in one of the solutions of $P_1 = P_2 = \dots = P_{n-1} = 0$. This solution is also the solution for $P^*_1 = P^*_2 = \dots = P^*_{n-1} = 0$ in $x_1, \dots, x_{n-2}, x_0$; hence, the solution of

$P_{*n} = 0$ in x_{n-1}, x_n is also the solution for $\mathcal{R}_0(n-1) = 0$. Thus, $\mathcal{R}^*(n)$=0 requires $\mathcal{R}^0(2) = 0$. Let $\mathcal{R}^*(n)$ be factored into the product of m irreducible factors, i.e.,

$$\mathcal{R}^*(n) = F_1 F_2 \ldots F_m;$$

then there exists only one irreducible factor F_i such that $\mathcal{R}^0(2)$ is divisible by it, viz, $\mathcal{R}^0(2) = F_i B_i$. On the other hand we have

$$\mathcal{R}^0(2) = (\mathcal{R}(n-1))^{d_n}(a^{(n)}_{0,\ldots,d_n})^{D_n} + Q_3(a^{(n)}_{0,\ldots,d_n})^{D_n - 1} + \cdots$$

where $Q_3 = (-1)^{d_n} Q_2^{d_n}(a^{(n)}_{0,\ldots,d_n,0}) \bmod \mathcal{R}(n-1)$, so that Q_3 is neither zero nor divisible by $\mathcal{R}(n-1)$. Also, $\mathcal{R}^0(2)$ has an irreducible factor of the form $(\mathcal{R}(n-1))^{d_n}(a^{(n)}_{0,\ldots,d_n})^p + \cdots$, and has no other factor involving $\mathcal{R}(n-1)$, i.e. the coefficients of $P_1, P_2, \ldots, P_{n-1}$, and the coefficients of P_{*n}. Hence, F_i is this irreducible factor of $\mathcal{R}^0(2)$ because F_i involves the the coefficients of $P_1, P_2, \ldots, P_{n-1}, P_{*n}$.

Again, $\mathcal{R}^*(n)$ is what $\mathcal{R}(n)$ becomes when all the coefficients of P_n other than those of P_{*n} are put equal to zero. Hence, $\mathcal{R}(n)$ has an irreducible factor of the form $(\mathcal{R}(n-1))^{d_n}(a^{(n)}_{0,\ldots,d_n})^q + \cdots$, where $q \geq p$. The remaining factor of $\mathcal{R}(n)$ is independent of the coefficients of $P_1, P_2, \ldots, P_{n-1}$, and therefore also of the coefficients of P_n when $n > 2$. Hence, $\mathcal{R}(n)$ is irreducible.

It is easy to prove that $\mathcal{R}(n)$ is invariant. Suppose that $\mathcal{R}(n) = 0$ and that this is the only relation existing between the coefficients of $P_1, P_2, \ldots, P_n$. Then not more than one relation can exist between the coefficients of $\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_n$, the polynomials into which $P_1, P_2, \ldots, P_n$ are transformed. Since $\mathcal{R}(n) = 0$ there are less than N_d linearly independent members of the module $(P_1, P_2, \ldots, P_n)$ of degree d, and therefore less than N_d linearly independent members of the module $(\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_n)$ of degree d. The single ıelation between the coefficients of

$(\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_n)$, which will admit this is $\hat{\mathcal{R}}(n)$, the resultant of $(\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_n)$, being equal to zero. Hence, $\mathcal{R}(n) = 0$ requires $\hat{\mathcal{R}}(n) = 0$, and $\hat{\mathcal{R}}(n)$ is divisible by $\mathcal{R}(n)$. The remaining factor of $\hat{\mathcal{R}}(n)$ is independent of the coefficients of $(P_1, P_2, \ldots, P_n)$. Therefore, $\mathcal{R}(n)$ is invariant. □□

The third important property of the resultant is given in the Product theorem.

Theorem A.7 : *If P_n is the product of two polynomials Q_1, Q_2 then the resultant $\mathcal{R}(n, d)$ of $P_1, P_2, \ldots, P_n$ is the product of the resultants $\mathcal{R}_1(n, d), \mathcal{R}_2(n, d)$ of $P_1, P_2, \ldots, Q_1$ and $P_1, P_2, \cdots, Q_2$.*

Proof : See [Macl6]. □□

In practice we are interested in the value of the resultant for a certain specialization of the coefficients. By a specialization of the coefficients, we mean the introduction of polynomial relations on the indeterminate coefficients, e.g., $a^{(1)}_{2,0,0} = 1$ or $a^{(3)}_{0,0,3} = 3u$. The difficulty arising here is the vanishing of $|\Delta\mathrm{M}(n, d)|$ for n permutations of the polynomials P_i.

Example A.1: We have the following polynomials

$$\begin{aligned} P_1 &= (x + \frac{1}{2}y + 2z)(x + y + 2z), \\ P_2 &= (2x + 2y + 5z)(2x + y + z), \\ P_3 &= (\frac{3}{4}x + \frac{3}{5}y + z)(x + 2y + 2z). \end{aligned}$$

Notice that these polynomials do not have a common root, but for all 3 permutations of P_1, P_2, P_3 the determinants $|\mathrm{M}(3, 4)|$ and $|\Delta\mathrm{M}(3, 4)|$ are identically zero. Hence, in this case we fail to find the resultant of this system by complete specialization of the coefficients.

One extreme is to compute the determinants $|\mathrm{M}(n, d)|$ and $|\Delta\mathrm{M}(n, d)|$ symbolically, and then compute $\mathcal{R}(n, d)$ as a polynomial in all coefficients of the P_i's.

However, this is a massive task, and generates terms of size double exponential in d.

Since computing the resultant symbolically is very expensive, we can avoid it by first computing $|\Delta M(n,d)|$. If this value is nonzero then we compute $|M(n,d)|$. Otherwise, one chooses a different ordering of the polynomials. If for all such orderings, $|\Delta M(n,d)|$ is zero, the method of complete specialization fails. This method is feasible because the cost of computing the determinants of the submatrices are relatively small compared with the cost of computing the determinant of the Macaulay matrix. For this approach, Canny, Kaltofen, and Yagati [Can88] have developed a new method to compute $|M(n,d)|$ and $|\Delta M(n,d)|$. This method is based on two recent results in computational algebra. They used the Wiedemann's [Wiede] fast method for computing the determinant of a matrix using a linear number of matrix times vector operations. In the case of the Macaulay matrix, the matrix times vector product can be shown to be equivalent to computing a multivariate polynomial product in which the product is a dense polynomial bounded in total degree. In order to compute this product, they make use of the sparse interpolation algorithms [Ben-Or, Kalto, Zipple]. The method given here computes the resultant in

$$O(nN_d^2(log^2(N_d)log(logN_d)+n))$$

arithmetic steps over the coefficient field, using $O(N_d)$ locations for field elements.

The third approach that one can use is the partial coefficients specialization method given in [Can87]. The basic idea here is to let

$$\hat{P}_i(x_1,\ldots,x_n)=P_i(x_1,\ldots,x_n)+u_ix_i^{d_i},$$

where u_i are indeterminates. Notice that the u_i appear on the diagonal of the matrices $\mathrm{M}(n, d)$ and $\Delta\mathrm{M}(n, d)$. Hence, the resultant $\mathcal{R}(n, d)$ is a polynomial in u_i and specializing $u_1, \ldots, u_n$ to zero, we obtained the desired resultant. We can speed up this method quite a bit by letting

$$\hat{P}_i(x_1, \ldots, x_n) = P_i(x_1, \ldots, x_n) + ux_i^{d_i},$$

where u are indeterminates, and $k = |\hat{\mathcal{X}}_{i,d}| = min(|\hat{\mathcal{X}}_{1,d}|, \ldots, |\hat{\mathcal{X}}_{n-1,d}|)$. Then, $|\mathrm{M}(n, d)|$ is a univariate polynomial in u of degree k, and $|\Delta\mathrm{M}(n, d)|$ is a univariate polynomial in u of degree $k - D_i$. Finally, we get $\mathcal{R}(n, d)$ is a univariate polynomial in u of degree D_i. The constant term of this polynomial is the desired resultant.