Gröbner Bases and Computation on Algebraic Curves

by

Waisiki Baleikorocau

A thesis submitted in partial fulfilment of the

requirements for the degree of

Master of Science in Pure Mathematics

School of Computing, Information and

Mathematical Sciences

Faculty of Science, Technology and Environment

The University of the South Pacific

December, 2011

Declarations

Statement by Author

I certify that this thesis is my own work except those sections and results which have been explicitly acknowledged. I also certify that this thesis has not been previously submitted for a degree at any other institution or university.

Signature: ..... Date: .....

Name: Mr. Waisiki Baleikorocau

Student ID: S96000014

Statement by Supervisor

The research in this thesis was performed under my supervision and to my knowledge is the sole work of Mr. Waisiki Baleikorocau.

Signature: ..... Date: .....

Name: Dr. Sione Ma‘u

Designation: Lecturer in Mathematics

Abstract

Gröbner basis for ideals of multivariate polynomials is a fundamental tool in computational algebraic geometry with applications in many fields. Given an algebraic variety, a Gröbner basis with respect to a graded monomial order is used to handle calculations on the variety. The Gröbner basis is used to derive matrix tools to do computations in the coordinate ring of the variety. In projective space, we use homogeneous coordinates to study the behaviour of a curve at a point at infinity and this is closely related to the Gröbner basis and computational properties of its coordinate ring. Finally, we use our computational tools to define directional Chebyshev constants as a new tool for calculation on curves.

Dedicated to my wife:

Mereadani Marama Baleikorocau

Acknowledgements

"In all thy ways acknowledge him, and he shall direct thy paths."(Proverbs 3:6)

There are certain individuals I would like to thank for their contribution in the production of this thesis:

First, I would like to convey my sincere thanks to my supervisor **Dr. Sione Ma'u**, Lecturer in Mathematics with the School of Computing, Information and Mathematical Sciences at the University of the South Pacific for introducing me to the work on Gröbner basis and Computation on Algebraic curves. His professional guidance, motivation and succinct advice has made this work possible. It is an honor and privilege to study under his supervision. Malo 'aupito.

I would also like to thank Dr. Robin Havea, Senior Lecturer in Mathematics at the University of the South Pacific, for his contribution in the Latex format of my work.

I wish to thank the library staff at the University of the South Pacific for their support and assistance during my research.

Finally, my sincere gratitude goes to my wife, Mereadani Marama Baleikorocau, for the financial support in my research, without which I could not have undertaken this study.

.....vina'a va'alevu.....

Contents

Chapter 1

Introduction

In approximation theory, certain well-known quantities in geometric complex analysis associated with a compact set $K \subset \mathbb{C}$ are related. These are Chebyshev constant ($\tau(K)$) and transfinite diameter ($d(K)$). Even though they are defined from a different point of view, these quantities are equal. So, we have

$$\tau(K) = d(K).$$

The Chebyshev constant is defined in terms of monic polynomials as follows (page 155 of [10]). Let

$$M_n := \inf\{\|p\|_K : p(z) = z^n + \text{lower degree terms}\}$$

where for a polynomial p and compact set K,

$$\|p\|_K = \sup\{|p(z)| : z \in K\}.$$

Thus, the Chebyshev constant of K of degree n was defined as

$$\tau_n = [M_n]^{1/n}.$$

Then

$$\tau(K) := \lim_{n\to\infty} \tau_n \quad \text{exists.}$$

Saff and Totik (page 163 of [11]) also derive a weighted version of this result using weighted polynomials.

Generalizations of the above quantities have been defined in several complex variables; the simple equality giving way to more complicated formulas. A formula in $\mathbb{C}^n$ generalizing $\tau(K) = d(K)$ was proved by Zaharjuta [12]. The formula is of the form

$$d(K) = \exp\left[\int_\Sigma \ln\ \tau(K,\theta)\right]$$

where $d(K)$ is the transfinite diameter in $\mathbb{C}^n$ and the constants $\tau(K,\theta)$ are called directional Chebyshev constants ranging over some parameter set Σ. These are defined with polynomials on K in the following way. Let

$$M_\alpha := \inf\{\|p\|_K : p(z) = z^\alpha + \sum_{z^\alpha > z^\beta} \lambda_\beta z^\beta, \lambda_\beta \in \mathbb{C}\}$$

and $z^\alpha > z^\beta$ in multi-index notation, indicates that z^α has a higher multidegree according to the grevlex monomial ordering - see Chapter 2. The Chebyshev constant for multidegree $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ was defined as

$$\tau_\alpha = [M_\alpha]^{1/|\alpha|},$$

where $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$ is the total degree. The directional Chebyshev constant in the direction $\theta \in \Sigma$ where $\Sigma = \{\theta \in \mathbb{R}^n : \theta = (\theta_1, \theta_2, ..., \theta_n), \theta_j \geq 0, \sum_{k=1}^n \theta_k = 1\}$ is then given as

$$\tau(K,\theta) := \lim_{|\alpha|\to\infty, \frac{\alpha}{|\alpha|}\to\theta} \tau_\alpha,$$

where it is also proved in [12] that the limit exists.

More results in the spirit of Zaharjuta were proved later by Jedrzejowski [6] for homogeneous polynomials in $\mathbb{C}^n$ and Bloom and Levenberg [1] for weighted polynomials in $\mathbb{C}^n$ where a weighted polynomial is a function $w^{|\alpha|}p$, for some function w satisfying some mild hypothesis (e.g $w > 0$ on K and w is continuous). Define

$$\tau_\alpha^w := \inf\{\|w^\alpha p\|_K : p(z) = z^\alpha + \cdots\}.$$

The weighted directional Chebyshev constant associated with w is given as

$$\tau_w(K,\theta) := \lim_{\alpha\to\infty, \frac{\alpha}{|w|}\to\theta} (\tau_\alpha^w)^{1/\alpha}.$$

In fact it is pointed out in [1] the existence of such limits and certain other properties of these constants follow from the fact that the quantities τ_α^w satisfy a submultiplicative property, i.e., $\tau_\alpha^w \tau_\beta^w \leq \tau_{\alpha+\beta}^w$.

Recently, a generalization of $\tau(K) = d(K)$ was proved by Ma'u [9] where K is a compact subset of an algebraic curve in $\mathbb{C}^2$. It is of the form

$$d(K) = \left(\prod_{j=1}^{d} \tau(K, \lambda_j) \right)^{1/d},$$

where $\tau(K, \lambda_j)$ are a collection of directional Chebyshev constants for the curve. Here the parameters λ_j are directions the curve takes to infinity. Directional Chebyshev constants of this type are defined in the thesis.

Hence, in $\mathbb{C}^n (n > 1)$, the Chebyshev constant generalizes to a collection of so-called *directional* Chebyshev constants; fundamentally, this is due to the fact that for multivariate polynomials the order of growth depends on which direction one takes to infinity. (For example, $x^2 + y$ grows quadratically along the x-axis but linearly along the y-axis).

The main motivation of this thesis is to develop a tool for studying directional Chebyshev constants on complex algebraic curves in $\mathbb{C}^n$. Although for convenience, we work in $\mathbb{C}^3$, the methods generalized to $\mathbb{C}^n$ in a straightforward way. Relating this to the notion of transfinite diameter is a subject of future investigation.

In our investigation, the Chebyshev constant is defined by polynomials on a curve V. We use Gröbner bases to do computations of polynomials in the coordinate ring of V. Importantly, the computations utilize a division algorithm which only works properly with Gröbner basis. Also, some interesting pattern that appear in the computations will be modeled with linear algebra. These are related to the geometry of the curve - specifically, the behaviour of the curve at infinity. To

study this we embed the curve into projective space and see where it intersects the hyperplane at infinity.

The thesis is organized as follows.

In Chapter 2, we give a brief description of Gröbner basis theory. Most important definitions, results and algorithms of the theory are included but some of the proofs are omitted. Interested readers are referred to Chapters 1 - 4 and 6 of [3] for more information on the theory.

In Chapter 3, we apply the definitions and algorithms given in Chapter 2 for algorithmic computation on varieties. We use a Gröbner basis, to construct a basis for monomials in the coordinate ring of a curve. We apply linear algebra to do computations in this ring.

Chapter 4 discusses projective space with its geometric properties and relates the geometry of a curve to computations in the coordinate ring of the curve. The intersection of a curve with a point at infinity is related to computational properties in its coordinate ring.

Finally, in Chapter 5, we define directional Chebyshev constants associated to a compact set K on an algebraic curve and show that the limit in the definition of this quantity is well-defined (Theorem 5.0.3).

Chapter 2

Background

This chapter reviews some of the basic terminology in algebraic geometry that will be used in subsequent sections. We will discuss affine varieties, which are curves and surfaces defined by polynomial equations. The corresponding algebraic object is an ideal. A study of ideals in polynomial rings leads to further discussion on Gröbner bases which is one of the main tools utilized in this study.

2.1 Affine Varieties

Algebraic geometry as a branch of mathematical study coming from the fusion of techniques between algebra and geometry. Geometric objects are expressed with precision by means of algebra, thus provide practical tools for applications.

Let k be a field. A *field* in algebra is a set where addition, subtraction, multiplication, and division can be carried out. There are many fields but the fields of real numbers $\mathbb{R}$, rational numbers $\mathbb{Q}$, and complex numbers $\mathbb{C}$ are commonly used. The set of integers $\mathbb{Z}$ is not a field since it fails to be closed under division, e.g., 5 and 3 are integers but the quotient 5/3 is not. Instead, $\mathbb{Z}$ is an example of a *ring*, which is a set where addition, subtraction and multiplication can be carried out, with the usual property of distributive and associative laws. Also, polynomials are example

of a ring since they satisfy the ring axioms under addition and multiplication.

The field $\mathbb{C}$ is *algebraically closed*, that is every univariate polynomial has a complex root. Algebraic geometry is easier to develop over algebraically closed fields which is why many authors restrict themselves to this case. However, the real numbers $\mathbb{R}$ and rational numbers $\mathbb{Q}$ are used a lot in applications.

Given any field k, the affine n-space over k is denoted by k^n which is the set of all n-tuples $(a_1, a_2, ..., a_n) \in k$. In general, k^1 is called an affine line and k^2 an affine plane.

Notation 2.1.1 *Here $k[x_1, x_2, ..., x_n]$ is the polynomial ring over the field k, i.e., $p \in k[x_1, x_2, ..., x_n]$ means $p(x) = \sum a_\alpha x^\alpha,\ a_\alpha \in k$ and $x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot ... \cdot x_n^{\alpha_n}$, where $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbb{Z}_+^n$ is a multi-index.*

Definition 2.1.2 *Let $H = \{f_1, f_2, ..., f_m\} \subset k[x_1, x_2, ..., x_n]$. Then the affine variety defined by H is*

$$\mathbf{V}(H) := \{(a_1, a_2, ..., a_n) \in k^n :\ f_i(a_1, a_2, ..., a_n) = 0,\ \forall\ f \in H\}.$$

The affine variety $\mathbf{V}(H)$ is the set of all solutions of the system of equations

$$\begin{aligned} f_1(x_1, x_2, ..., x_n) &= 0 \\ f_2(x_1, x_2, ..., x_n) &= 0 \\ &\vdots \\ f_m(x_1, x_2, ..., x_n) &= 0, \end{aligned}$$

$f_i \in H$.

Example 2.1.3 *If $k = \mathbb{R}$, then the variety $\mathbf{V}(y - mx - b)$ defines the line $y = mx + b$ in $\mathbb{R}^2$.*

Ellipses, hyperbolas, circles and planes are also affine varieties.

Example 2.1.4 *The double-cone $\mathbf{V}(x^2 + y^2 - z^2)$ is an affine variety in $\mathbb{R}^3$.*

2.2 Ideals

In ring theory, an ideal (Part (V) of [4]) is a special subset of a ring. Ideals in a polynomial ring $k[x_1, x_2, ..., x_n]$ are absolutely central to the study of algebraic geometry. Now we will define what we mean by ideals and explain the relationship to affine varieties.

Definition 2.2.1 *An ideal is a subset $I \subset k[x_1, x_2, ..., x_n]$ which satisfies:*

1. $0 \in I$
2. *If $f, g \in I$, then $f + g \in I$*
3. *If $f \in I$ then for any $h \in k[x_1, x_2, ..., x_n]$, $fh \in I$*

Example 2.2.2 *Let $p \in k[x, y, z]$. Then $H = \{tp : t \in k[x, y]\}$ is an ideal. Given $t_1p, t_2p \in H$, then*

$$t_1p + t_2p = (t_1 + t_2)p \in H.$$

Also, given $t \in k[x, y]$, then

$$t \cdot t_1p = (tt_1)p \in H.$$

Hence, H is an ideal called the ideal generated by p, and denoted by $\langle p \rangle$.

Now we can generalize this construction of an ideal.

Definition 2.2.3 *Let $F \subset k[x_1, x_2, ..., x_n]$. We define*

$$\langle F \rangle = \left\{ \sum_{i=1}^{t} h_i f_i : h_i \in k[x_1, x_2, ..., x_n], f_i \in F \right\}.$$

Then $\langle F \rangle$ is an ideal of $k[x_1, x_2, ..., x_n]$ which we call the ideal generated by F.

If $F = \{f_1, f_2, ..., f_m\}$ is a finite set, then the polynomials $f_1, f_2, ..., f_m$ are called a basis for the ideal or generators of the ideal and $\langle F \rangle$ is said to be finitely generated. We write $\langle F \rangle = \langle f_1, f_2, ..., f_m \rangle$.

An important observation showing that a variety depends on ideals is that $\mathbf{V}(f_1, f_2, ..., f_m) = \mathbf{V}(g_1, g_2, ..., g_n)$ whenever $\langle f_1, f_2, ..., f_m \rangle = \langle g_1, g_2, ..., g_n \rangle$. In practice, changing to a different basis provides an easy way to determine the solutions of equations. This shows that an affine variety fundamentally depends on the ideal I generated by the defining equations, rather than the equations themselves. A finitely generated ideal gives an affine variety by the formula

$$\mathbf{V}(I) = \{(a_1, a_2, ..., a_n) : f(a_1, a_2, ..., a_n) = 0, \ \forall \ f \in I\}.$$

Let us reverse the process. Given an affine variety V, let

$$\mathbf{I}(V) = \{f \in k[x_1, x_2, ..., x_n] : f(a_1, a_2, ..., a_n) = 0, \ \forall \ (a_1, a_2, ..., a_n) \in V\}.$$

This satisfies the abstract definition of ideal. Then every affine variety gives an ideal.

Lemma 2.2.4 *Let V, W be varieties in k^n and I, J be Ideals. Then*

(i) $V \subseteq W \iff \mathbf{I}(V) \supseteq \mathbf{I}(W)$

(ii) $I \subseteq J \iff \mathbf{V}(I) \supseteq \mathbf{V}(J)$

Proposition 2.2.5 *Let $V \subseteq k^n$ be a variety. Then*

$$\mathbf{V}(\mathbf{I}(V)) = V.$$

Proof. Given V,

$$\mathbf{I}(V) = \{f : f(x) = 0, \ \forall \ x \in V\}$$

and

$$\mathbf{V}(\mathbf{I}(V)) = \{x : h(x) = 0, \ \forall \ h \in \mathbf{I}(V)\}.$$

If $x \in V$, then given $f \in \mathbf{I}(V)$, $f(x) = 0$. So $f(x) = 0, \ \forall \ f \in \mathbf{I}(V)$. Therefore $x \in \mathbf{V}(\mathbf{I}(V))$. It follows that $V \subset \mathbf{V}(\mathbf{I}(V))$.

Conversely, since V is an affine variety, $V = \mathbf{V}(f_1, f_2, ..., f_n)$ for some polynomials f_i where $1 \leq i \leq n$. Given i, $f_i(x) = 0$, $\forall\ x \in V$. Since $f_i \in \mathbf{I}(V)$ for all i, $\langle f_1, ..., f_n \rangle \subset \mathbf{I}(V)$ and $V = \mathbf{V}(\langle f_1, ..., f_n \rangle) \supset \mathbf{V}(\mathbf{I}(V))$. Thus, $V = \mathbf{V}(\mathbf{I}(V))$. $\square$

However, this is not true in general for the reverse analogous process for ideals, that is, $I = \mathbf{I}(\mathbf{V}(I))$ does not always hold. As an example, given $I = \langle x^2 \rangle$ then $\mathbf{I}(\mathbf{V}(I)) = \langle x \rangle \neq I$.

2.3 Monomial Orderings

Let us have a look at what a monomial ordering is. Monomials in one variable can be naturally ordered by degree:

$$\cdots > x^{m+1} > x^m > \cdots > x^2 > x > 1$$

We will consider orderings on monomials in several variables. Consider some notational convention on monomials. Writing $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbb{Z}_+^n$ a multi-index, the monomial x^α is given by $x^\alpha := x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot ... \cdot x_n^{\alpha_n}$. We define the total degree $|\alpha| := \sum_{i=1}^n \alpha_i$.

Definition 2.3.1 *A monomial order $>$ is an order relation on the set of monomials $x^\alpha, x^\beta, x^\gamma, ...$ in $k[x_1, x_2, ..., x_n]$ satisfying:*

(i) If $x^\alpha > x^\beta$ then $x^\alpha x^\gamma > x^\beta x^\gamma$ for any monomial x^γ.

(ii) Every subset of monomials contains a smallest element under $>$.

These properties imply that $>$ is well-ordered, that is any strictly decreasing sequence with respect to $>$ will eventually terminate.
There are many monomial orderings but we will give three important ones, omitting the proof that they are in fact monomial orders.

Definition 2.3.2 *Let* $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ *and* $\beta = (\beta_1, \beta_2, ..., \beta_n) \in \mathbb{Z}_+^n$.

1. **Lexicographic order (lex):** *Here* $\alpha >_{lex} \beta$ *iff the vector difference of the leftmost nonzero entry of* $\alpha - \beta$ *is positive.*

   Example: $(5,3,2) = \alpha >_{lex} \beta = (2,3,4)$. *Since* $\alpha - \beta = (3,0,-2)$, *the leftmost nonzero entry is positive. Hence* $x_1^5\ x_2^3\ x_3^2 >_{lex} x_1^2\ x_2^3\ x_3^4$.

2. **Graded Lex order (grlex):** *Sort first by total degree then lex. That is,* $\alpha >_{grlex} \beta$ *if* $|\alpha| > |\beta|$ *or* $|\alpha| = |\beta|$ *and* $\alpha >_{lex} \beta$.

   Example: $(5,3,2) = \alpha >_{grlex} \beta = (2,4,4)$. *Since* $|\alpha| = 10 = |\beta|$ *and the leftmost nonzero entry in* $\alpha - \beta = (3,-1,-2)$ *is positive,* $\alpha >_{lex} \beta$. *Hence* $x_1^5\ x_2^3\ x_3^2 >_{grlex} x_1^2\ x_2^4\ x_3^4$.

3. **Graded Reverse Lex order (grevlex):** *The order is sort first by total degree then by the vector difference of the rightmost nonzero entry. We have* $\alpha >_{grevlex} \beta$ *if* $|\alpha| > |\beta|$ *or* $|\alpha| = |\beta|$ *and the rightmost nonzero entry of* $\alpha - \beta$ *is negative.*

   Example: $(2,1,3) = \alpha >_{grevlex} \beta = (1,1,4)$. *Since* $|\alpha| = 6 = |\beta|$ *and the rightmost entry in* $\alpha - \beta = (1,0,-1)$ *is negative. Hence* $x_1^2\ x_2\ x_3^3 >_{grevlex} x_1\ x_2\ x_3^4$.

In our study we will mainly use the grevlex order. Even though the ordering may be non-intuitive, it has some desirable computational properties. The reason for the non-intuitive nature given above, as done in [3] for example, is that it follows the same convention as lex and grlex with $x_1 > x_2 > \cdots > x_n$. However, we will prefer a more intuitive definition later in this thesis with $x_1 < x_2 < \cdots < x_n$. Monomials in x_1, x_2, x_3 listed in increasing order in this way are

$$1, x_1, x_2, x_3, x_1^2, x_1x_2, x_1x_3, x_2x_3, x_1^3, ..., x_1^k, x_1^{k-1}x_2, x_1^{k-1}x_3, x_2^{k-1}x_3, ...$$

Rewriting the grevlex example above with $x_1 \leftrightarrow x_3$, $x_2 \leftrightarrow x_2$, we have $x_1^4\ x_2\ x_3 <_{grevlex} x_1^3\ x_2\ x_3^2$, as expected. In n variables there are $n!$ different grevlex orders that correspond to how the variables are ordered.

Thus, terms of polynomials can be ordered in an unambiguous way according to the monomial order of choice.

Definition 2.3.3 *Suppose we have a fixed monomial order* $>$ *. Given a nonzero polynomial* $f \in k[x_1, x_2, ..., x_n]$ *and* $f = \sum a_\alpha x^\alpha$ *(note that only finitely many* a_α *are* $\neq 0$*), we define (c.f., Definition 7 in Chapter 2 §2 of [3]):*

- *The leading term of* f *as:* $LT(f) = a_\beta x^\beta$ *where* β *has the highest order among the powers* $\alpha \in \mathbb{Z}^n, a_\alpha \neq 0$ *according to the monomial order*
- *The leading coefficient of* f *as:* $LC(f) = a_\beta$
- *The leading monomial of* f *as:* $LM(f) = x^\beta$

2.4 Division Algorithm

Having established what we mean by leading terms with respect to a given monomial ordering, we can now discuss the division algorithm. Let k be a field and $f, g \in k[x]$ be a polynomial in one variable. It follows from the standard division algorithm for polynomials (see Section 23, page 210 of [4]) that

$$f = qg + r$$

where $q, r \in k[x]$ and $r = 0$ or $LT(r) < LT(g)$. We call f the dividend and g a divisor. The quotient q and remainder r are uniquely determined.

In several variables, polynomials in $k[x_1, x_2, ..., x_n]$ can be written in a canonical way according to monomial order where we write terms of the highest order first followed by subsequent terms of lower order. In the division algorithm in several variables, the term of the highest order of the dividend is divided by the term of the highest order of a divisor. If this is not possible the dividend term moves to the remainder.

Theorem 2.4.1 (*Division Algorithm in $k[x_1, x_2, ..., x_n]$): Fix a monomial order $>$ on $k[x_1, x_2, ..., x_n]$. Let $F = (g_1, g_2, ..., g_m)$ be an ordered $m-$tuple of polynomials. Then for every $f \in k[x_1, x_2, ..., x_n]$, f can be written as*

$$f = q_1 g_1 + \cdots + q_m g_m + r$$

for some $q_1, q_2, ..., q_m, r \in k[x_1, x_2, ..., x_n]$ and no term of r is divisible by any of $LT(g_1), ..., LT(g_m)$. We call r the remainder of f on division by F.

The division algorithm in $\mathbb{C}^n$ is most clearly understood through an example.

Example 2.4.2 *Using lex order, let us divide $f = x^3y^2 + xy^2 + y^2$ by $g_1 = xy - 1$ and $g_2 = y^2 - 1$. Then*

$$\begin{array}{rll}
q_1: & x^2y + x + y & r \\
q_2: & 1 & \underline{\quad\quad} \\
\cline{2-2}
xy - 1 \;\Big)\; & x^3y^2 + xy^2 + y^2 & \\
y^2 - 1 \;\Big)\; & x^3y^2 - x^2y & \\
\cline{2-2}
 & x^2y + xy^2 + y^2 & \\
 & \underline{x^2y - x} & \\
 & xy^2 + x + y^2 & \\
 & \underline{xy^2 - y} & \\
 & x + y^2 + y & \\
 & \underline{y^2 - 1} & \longrightarrow \quad x \\
 & y + 1 & \longrightarrow \quad y \\
 & \underline{1} & \\
 & 0 & \longrightarrow \quad x + y + 1
\end{array}$$

Note that q_1 and q_2 are quotients. Since g_1 is listed first and $LT(g_1)$ divides $LT(f)$, division is attempted first by $xy - 1$ and we write the quotient in q_1. If the first

divisor fails then we divide f using $y^2 - 1$ and the quotient written in q_2.

The remainder $x + y + 1$ is not uniquely determined when changing the order of the divisors:

$$
\begin{array}{rl}
q_1: & x + 1 \qquad\qquad\qquad\qquad r \\
q_2: & x^2y + x \\
y^2 - 1 & \big)\; x^3y^2 + xy^2 + y^2 \\
xy - 1 & \; \underline{x^3y^2 - x^2y} \\
 & \qquad x^2y + xy^2 + y^2 \\
 & \qquad \underline{x^2y - x} \\
 & \qquad\qquad xy^2 + x + y^2 \\
 & \qquad\qquad \underline{xy^2 - x} \\
 & \qquad\qquad\qquad \underline{2x + y^2} \\
 & \qquad\qquad\qquad y^2 \qquad \longrightarrow \quad 2x \\
 & \qquad\qquad\qquad \underline{y^2 - 1} \\
 & \qquad\qquad\qquad\quad \underline{1} \\
 & \qquad\qquad\qquad\quad 0 \qquad \longrightarrow \quad 2x + 1
\end{array}
$$

where the remainder is $2x + 1$.

Thus, it is clear that there is no uniqueness in the quotients and remainder. In general both will change if we reorder the divisors or change the monomial ordering.

The division algorithm can be used to determine ideal membership. That is, if dividing f by $g_1, ...g_m$ gives a remainder zero then we know that $f \in \langle g_1, ..., g_m \rangle$. However, the converse is not true. If the divisor has a nonzero remainder, $f \in \langle g_1, ..., g_m \rangle$ might still be true if dividing using different order of divisors gives a remainder zero. To solve this problem we need to choose a special set of divisors forming a basis of the ideal such that the remainder is unique regardless of the order of the divisors. These divisors are called a Gröbner basis.

2.5 Gröbner Bases

In Example 2.4.2, we discovered that the remainders $2x + 1$ and $x + y + 1$ are not unique. Now our study of Gröbner basis aims to eliminate the ambiguity in the definition of remainder of f on division by $g_1, ..., g_m$. We show that ideals are finitely generated.

Definition 2.5.1 *A monomial ideal $I \subset k[x_1, x_2, ..., x_n]$ is an ideal I generated by monomials $I = \langle x^\alpha \rangle_{\alpha \in A}$ for some $A \subset \mathbb{Z}_+^n$.*

Lemma 2.5.2 *Let $I = \langle x^\alpha : \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I iff x^β is divisible by x^α for some $\alpha \in A$.*

Proof. First note that if x^β is a multiple of x^α for some $\alpha \in A$, then $x^\beta \in I$ since I is an ideal. Conversely, if $x^\beta \in I$, then, $x^\beta = \sum_{i=1}^{s} a_i x^{\alpha_i}$, where a_i are polynomials and $\alpha_i \in A$. Expanding each a_i as linear combination of monomials, we see that x^β on the left side of the equation is a monomial of $a_i x^{\alpha_i}$, hence is divisible by x^{α_i}. □

Proposition 2.5.3 *(Dickson's Lemma): Every monomial ideal $I \subset k[x_1, x_2, ..., x_n]$ has a finite basis.*

Omitting the proof, note that Dickson's lemma is central to the Hilbert Basis Theorem.

Proposition 2.5.4 *Suppose $I \subset k[x_1, x_2, ..., x_n]$ is an ideal, then $\langle LT(I) \rangle$ is a monomial ideal. Also, there are $g_1, g_2, ..., g_m \in I$ such that $\langle LT(I) \rangle$ is generated by $\{LT(g_i)\}_{i=1}^m$.*

Proof. The leading monomials $LM(g)$ of elements $g \in I \backslash \{0\}$ generate the monomial ideal $\langle LM(g) : g \in I \backslash \{0\} \rangle$. Since $LM(g)$ and $LT(g)$ differ by a nonzero constant, we get $\langle LM(g) : g \in I \backslash \{0\} \rangle = \langle LT(I) \rangle$. Thus, $\langle LT(I) \rangle$ is a monomial ideal.

Next, since $\langle LT(I)\rangle$ is generated by the monomials $LM(g)$ for $g \in I\backslash\{0\}$, by Proposition 2.5.3 we have $\langle LT(I)\rangle = \langle LM(g_1), LM(g_2), ..., LM(g_m)\rangle$ for finitely many $g_1, g_2, ..., g_t \in I$. Since $LM(g_j)$ differs from $LT(g_j)$ by a nonzero constant, it follows that $\langle LT(I)\rangle = \langle LT(g_1), LT(g_2), ..., LT(g_m)\rangle$. □

Theorem 2.5.5 *(Hilbert Basis Theorem [5]) Every ideal $I \subset k[x_1, x_2, ..., x_n]$ is finitely generated, that is, there are polynomials $g_1, g_2, ..., g_m \in I$ such that $I = \langle g_1, g_2, ..., g_m\rangle$.*

Proof. Let the ideal I be nontrivial, otherwise $I = \langle 0\rangle$. By Proposition 2.5.4, there are $g_1, g_2, ..., g_m \in I$ such that $\langle LT(I)\rangle = \langle LT(g_1), ..., LT(g_m)\rangle$. We claim that $I = \langle g_1, g_2, ..., g_m\rangle$. It is obvious that $\langle g_1, g_2, ..., g_m\rangle \subset I$ since $g_i \in I$. To prove that $\langle g_1, g_2, ..., g_m\rangle \supset I$, let $f \in I$ and apply the division algorithm to divide f by the set of g_i. We get

$$f = \sum_{i}^{m} q_i g_i + r$$

where no term of r is divisible by any of $LT(g_i)$. Clearly $r \in I$. If $r \neq 0$, then $LT(r) \in \langle LT(I)\rangle = \langle LT(g_i)\rangle$. Since this is a monomial ideal, $LT(g_i)$ divides $LT(r)$ for some $i < m$ by Lemma 2.5.2. We have a contradiction. Hence $r = 0$. So $f = \sum_i^m q_i g_i$, that is $f \in \langle g_1, g_2, ..., g_m\rangle$. □

Definition 2.5.6 *Let $I \subset k[x_1, x_2, ..., x_n]$ be an ideal. A set $\{g_1, ..., g_m\} \subset I$ is a Gröbner basis of I if*

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

Equivalently, the subset $\{g_1, ..., g_m\}$ of an ideal I is a Gröbner basis if and only if the leading term of any element of I is divisible by any one of the leading terms of (g_i). When dividing a polynomial by a Gröbner basis according to the division algorithm in Theorem 2.4.1, we always get a unique remainder.

Note that it follows from Proposition 2.5.4 that every ideal I has a Gröbner basis, and the proof of Hilbert basis theorem shows that any Gröbner basis for an ideal I is in fact a basis for I.

Proposition 2.5.7 *Let $G = \{g_1, g_2, ..., g_m\}$ be a Gröbner basis for an ideal $I \subset k[x_1, x_2, ..., x_n]$ and f be a polynomial. Then there exists a unique $r \in I$ which satisfies:*

(i) No term of r is divisible by any of $LT(g_1), ..., LT(g_m)$, and

(ii) There exist $q_1, q_2, ..., q_m \in k[x_1, x_2, ..., x_n]$ such that $f = \sum_i^m q_i g_i + r$.

This means that dividing f by G, the remainder is uniquely determined irrespective of how the elements of G are ordered using division algorithm.

As highlighted above, every ideal I has a Gröbner basis. Computer programs are available for computing a Gröbner basis of an ideal, but we should first learn this by hand. There is an algorithm to construct a Gröbner basis, called Buchberger's algorithm [2].

Notation 2.5.8 *The least common multiple $LCM(x^\alpha, x^\beta) = x^\gamma$ where the multi-index γ is defined by $\gamma_i = max(\alpha_i, \beta_i)$ for each $i = 1, 2, ..., n$.*

Definition 2.5.9 *Let $f, g \in k[x_1, x_2, ..., x_n]$ be nonzero polynomials. We can find $x^\gamma = LCM(LM(f), LM(g))$. Then the S-polynomial of f and g is*

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

The S-polynomials provide the cancellation of leading terms.

Theorem 2.5.10 *Let I be a polynomial ideal. Then a basis $G = \{g_1, g_2, ..., g_m\}$ for I is a Gröbner basis of I iff $\forall\ i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (in some fixed order) is 0.*

Theorem 2.5.11 *(Buchberger's Algorithm). Let $I = \langle f_1, ..., f_m \rangle \neq \{0\}$ be a polynomial ideal. There exists an algorithm to compute a Gröbner basis given a generating set of the polynomial ideal I.*

We omit the proof of Theorem 2.5.11, referring the reader to Chapter 2 §7 of [3]. The algorithm is described as follows. Given an ideal I and a basis $G = \{g_1, ..., g_m\}$, calculate all of $S(g_i, g_j)$. Divide $S(g_i, g_j)$ by $\{g_1, ..., g_m\}$. If the remainder $\overline{S(g_i, g_j)}^F$ is nonzero, extend $\{g_1, ..., g_m\} = G$ with the remainder and calculate as done previously. Keep going until $\overline{S(g_i, g_j)}^F = 0$ for all pairs $g_i, g_j \in G$. This process will eventually terminate in a finite number of steps.

Example 2.5.12 *Let $I = (x^2y - 1, xy^2 - x) = \langle g_1, g_2 \rangle$. Suppose we order these polynomials with respect to grlex order. Then to produce a Gröbner basis, we compute*

$$S(g_1, g_2) = (y)(x^2y - 1) - (x)(xy^2 - x) = x^2 - y$$

and

$$\begin{array}{rll} q_1: & 0 & r \\ q_2: & 0 & \underline{\quad\quad} \\ x^2y - 1 \\ xy^2 - x \end{array} \Big) \overline{x^2 - y}$$

$$\begin{array}{rcl} \overline{-y} & \longrightarrow & x^2 \\ \underline{\quad} & & \\ 0 & \longrightarrow & x^2 - y =: \overline{S(g_1, g_2)}^F \neq 0 \end{array}$$

Let $g_3 = x^2 - y$ and $F = (g_1, g_2, g_3)$,

$$\overline{S(g_1, g_2)}^F = 0$$

$$S(g_1, g_3) = (x^2y - 1) - (y)(x^2 - y) = y^2 - 1$$

$$\overline{S(g_1, g_3)}^F = y^2 - 1 \neq 0$$

Let $g_4 = y^2 - 1$ *and* $F = (g_1, g_2, g_3, g_4)$,

$$\begin{aligned}
\overline{S(g_1, g_3)}^F &= 0 \\
S(g_1, g_4) &= x^2 - y \\
\overline{S(g_1, g_4)}^F &= 0 \\
S(g_2, g_3) &= -x^2 + y^3 \\
\overline{S(g_2, g_3)}^F &= 0 \\
S(g_2, g_4) &= 0 \\
\overline{S(g_2, g_4)}^F &= 0 \\
S(g_3, g_4) &= x^2 - y^3 \\
\overline{S(g_3, g_4)}^F &= 0
\end{aligned}$$

Thus, our Gröbner basis for I *in grlex order is*

$$\{g_1, g_2, g_3, g_4\} = \{x^2y - 1, xy^2 - x, x^2 - y, y^2 - 1\}$$

Gröbner bases can be larger than necessary. We can eliminate redundant polynomials by the following.

Lemma 2.5.13 *Let* G *be a Gröbner basis for the polynomial ideal* I*. Let* $p \in G$ *a polynomial such that* $LT(p) \in \langle LT(G \backslash \{p\})\rangle$*. Then* $G \backslash \{p\}$ *is also a Gröbner basis for* I*.*

Dividing each polynomial by its leading coefficients and removing any p such that it satisfies the condition in Lemma 2.5.13, we get a minimal Gröbner basis.

Definition 2.5.14 *A minimal Gröbner basis for an ideal* I *is a Gröbner basis* G *such that:*

(i) $LC(p) = 1, \ \forall \ p \in G$*.*

(ii) For all $p \in G, LT(p) \notin \langle LT(G \backslash \{p\})\rangle$*.*

Definition 2.5.15 *A reduced Gröbner basis for an ideal I is a Gröbner basis G satisfying:*

(i) $LC(p) = 1, \ \forall \ p \in G$.

(ii) For all $p \in G$, no monomial of p lies in $\langle LT(G \backslash \{p\})\rangle$.

To obtain a reduced Gröbner basis from a minimal one, we divide each element by the rest of the minimal basis and take the remainder.

Example 2.5.16 *From Example 2.5.12, we can construct a reduced Gröbner basis. Using grlex order, the Gröbner basis is*

$$g_1 = x^2y - 1,$$
$$g_2 = xy^2 - x,$$
$$g_3 = x^2 - y,$$
$$g_4 = y^2 - 1.$$

Since $LT(g_1) = x^2y = y \cdot LT(g_3)$ and $LT(g_2) = xy^2 = x \cdot LT(g_4)$. By Lemma 2.5.13, we can eliminate g_1 and g_2 respectively. Thus, we get a reduced basis

$$\tilde{g_3} = x^2 - y, \quad \tilde{g_4} = y^2 - 1.$$

Note that a reduced Gröbner basis has the following nice property.

Theorem 2.5.17 *Fix a monomial order. Then, every nonzero polynomial ideal $I \subset k[x_1, x_2, ..., x_n]$ has a unique reduced Gröbner basis.*

Proof. To prove uniqueness, suppose that G and $\widetilde{G}$ are two different reduced Gröbner basis for I and have the same leading term. To show the equality, let $g_i \in G$ and $g_i = \sum q_i \tilde{g_i}$ then we have $LT(g_i)$ divides $LT(\tilde{g_i})$ for some i. Going in the opposite direction, we have $LT(\tilde{g_i})$ divides $LT(g_j)$ for some j. By Definition 2.5.14, this is possible if $j = 1$ implying that $LT(g_i) = LT(\tilde{g_i})$. Thus, $LT(G) = LT(\widetilde{G})$.

If $g \in G$ then there exist a $\tilde{g} \in \widetilde{G}$ such that $LT(g) = LT(\tilde{g})$. Given that $g - \tilde{g} \in I$ and G is a Gröbner basis, it follows that $\overline{g - \tilde{g}}^{G} = 0$. But $LT(g) = LT(\tilde{g})$ and so we have a cancellation in $g - \tilde{g}$. Since G and $\widetilde{G}$ are reduced none of the remaining terms of $g - \tilde{g}$ is divisible by $LT(G) = LT(\widetilde{G})$. It shows that $\overline{g - \tilde{g}}^{G} = g - \tilde{g} = 0$. Thus, $G = \widetilde{G}$. □

Chapter 3

Algorithmic Computations in V

In this chapter, we will utilize the division algorithm to develop a simple representation of the equivalence classes for congruence modulo I, where $I \subset \mathbb{C}[x_1, x_2, ..., x_n]$ is an ideal. This means that if we let $I \subset \mathbb{C}[x_1, x_2, ..., x_n]$ be an ideal and $f, g \in \mathbb{C}[x_1, x_2, ..., x_n]$ then we say that f and g are congruent modulo I if $f - g \in I$. This will be fundamental in the development of an explicit method for computing the sum and product operations in the quotient ring $\mathbb{C}[V] = \mathbb{C}[x_1, x_2, ..., x_n]/\mathbf{I}(V)$ where $V \subset \mathbb{C}^n$ is a variety. The elements of the ring $\mathbb{C}[x_1, x_2, ..., x_n]/\mathbf{I}(V)$ can be considered as the polynomial functions on V since $f = g$ on V means f and g are congruent modulo $\mathbf{I}(V)$. Our study will concentrate on algebraic curves in $\mathbb{C}^3$ and coordinates x, y, z. Later, we will use linear algebra to further study multiplication in this special case. We will conveniently stick with the algorithmic point of view and define the dimension of V in terms of properties of $\mathbb{C}[V]$, using the Hilbert polynomial. The equivalence to the geometric notion is an important part of the theory which will not be covered here.

In section 2.5 of Chapter 2, we learned that the remainder on dividing a polynomial f by a Gröbner basis for an ideal I is uniquely determined by the polynomial f. Reinterpreting the result of the division and the form of the remainder provides the basis for working with varieties.

3.1 Normal Form

Proposition 3.1.1 *Fix a monomial order. Let $I \subset \mathbb{C}[x,y,z]$ be an ideal. Then*

(i) Every $f \in \mathbb{C}[x,y,z]$ is congruent modulo I to a unique polynomial r which is a $\mathbb{C}$-linear combination of the monomials in the complement of $\langle LT(I)\rangle$.

(ii) The elements of $\{x^\alpha y^\beta z^\gamma : x^\alpha y^\beta z^\gamma \notin \langle LT(I)\rangle\}$ are "linearly independent modulo I". That is, if

$$\sum_{\alpha,\beta,\gamma} c_{\alpha,\beta,\gamma} x^\alpha y^\beta z^\gamma \equiv 0 \ mod\ I,$$

where the $x^\alpha y^\beta z^\gamma$ are all in the complement of $\langle LT(I)\rangle$, then $c_{\alpha,\beta,\gamma} = 0,\ \forall\ \alpha,\beta,\gamma$.

Proof. Suppose G is the Gröbner basis for I. Let $f \in \mathbb{C}[x,y,z]$. By the division algorithm, $r = \overline{f}^G$ satisfies $f = q + r$, where $q \in I$ and r the remainder. So $f - q = r \in I$ implies that $f \equiv r \bmod I$. Hence, r is a k-linear combination of the monomials $x^\alpha y^\beta z^\gamma \notin \langle LT(I)\rangle$.

For uniqueness, suppose there exist g, r and g', r' satisfying $f = g + r = g' + r'$. So $r - r' = g - g' \in I$. If $r - r' \neq 0$, then $LT(r - r') \in \langle LT(I)\rangle$ which implies that $LT(g_i)$ divides $LT(r - r')$ for some i. This is not possible because no term of r, r' is divisible by any $LT(g_i)$. Thus $r = r'$ and $g = g'$.

Part (ii) is an easy consequence of uniqueness. □

Definition 3.1.2 *Let $I \subset \mathbb{C}[x,y,z]$ be an ideal. The reduced monomial basis ($\mathcal{B}$) of $\mathbb{C}[x,y,z]/I$ specialized to $\mathbb{C}^3$ is given as*

$$\mathcal{B} = \{x^\alpha y^\beta z^\gamma : x^\alpha y^\beta z^\gamma \notin \langle LT(I)\rangle\}.$$

If $V \subset \mathbb{C}^3$ is a variety then its reduced monomial basis is the reduced monomial basis of $\mathbb{C}[x,y,z]/\mathbf{I}(V) = \mathbb{C}[V]$.

Proposition 3.1.3 *Let $I \subset \mathbb{C}[x,y,z]$ be an ideal. Then $\mathbb{C}[x,y,z]/I$ is isomorphic as a $\mathbb{C}$-vector space to $S =$Span $(\mathcal{B})$.*

Example 3.1.4 *Let* $V = \{x^2 + y^2 + z^2 - 1 = 0\}$ *be a complex sphere. Then* $I = \mathbf{I}(V) = \langle x^2 + y^2 + z^2 - 1\rangle$, *and with respect to grevlex order,* $\langle LT(I)\rangle = \langle z^2\rangle$. *Hence, the reduced (monomial) basis* $\mathcal{B}$ *for* V *with respect to grevlex order is the infinite set of monomials that are not multiples of* z^2, *i.e.,*

$$1, x, y, z, x^2, xy, xz, y^2, yz, x^3, x^2y, x^2z, y^3, y^2z, x^4, ..., x^k, x^{k-1}y, x^{k-1}z, y^k, y^{k-1}z, ...$$

To illustrate the representation, consider the polynomial $f = 2z^2 + xy + y^3 - 1$ *on* V, *representing an element of* $\mathbb{C}[x, y, z]/\mathbf{I}(V)$. *Then* $G = \{z^2 + y^2 + x^2 - 1\}$ *is a Gröbner basis with respect to grevlex and* f *is congruent modulo* I *to*

$$\overline{f}^G = xy + y^3 - 1$$

which is a linear combination of elements of $\mathcal{B}$.

Definition 3.1.5 *We call the representation*

$$p(x, y, z) = \sum_{\mathcal{B}} \lambda_{\alpha,\beta,\gamma} x^\alpha y^\beta z^\gamma$$

where $x^\alpha y^\beta z^\gamma \in \mathcal{B}$ *of a polynomial* $p(x, y, z)$ *on* V *as its normal form.*

Example 3.1.6 *Let* $I = \langle y^2 + z^2 - x^2 - 1, z^2 + yz - 2y^2 + xz - xy + 1\rangle$ *in* $\mathbb{C}^3$ *using grevlex with* $x < y < z$. *We get (calculation with Mathematica) the Gröbner basis*

$$G = \{yz+xz-3y^2-xy+x^2+2, z^2+y^2-x^2-1, 10y^3-2xy^2-6x^2y+x^2z+x^3-7y-2z+3x\}.$$

By Proposition 3.1.3, we can write the basis of the given monomials in grevlex order and throw out monomials contained in $\langle LT(G)\rangle = \langle yz, z^2, y^3\rangle$ as they arise, leaving a linearly independent set of monomials in the list. This is the set $\mathcal{B}$ given by

$$1, x, y, z, x^2, xy, xz, y^2, x^3, x^2y, x^2z, xy^2, x^4, ..., x^k, x^{k-1}y, x^{k-1}z, x^{k-2}y^2, ...$$

To illustrate this, let us find the normal form of $f = 2z^2+xy+y^3-1 \in \mathbb{C}[x, y, z]/\mathbf{I}(V)$. Since some of the monomials in f are in $\langle LT(I)\rangle$, the polynomial cannot be the normal form. So we need to divide f again by G and get

$$\overline{f}^G = -\frac{1}{10}x^2z + \frac{3}{5}x^2y + \frac{1}{5}xy^2 - \frac{1}{10}x^3 - 2y^2 + 2x^2 + xy + \frac{1}{5}z + \frac{7}{10}y - \frac{3}{10}x + 1,$$

which is a linear combination of elements of $\mathcal{B}$.

3.2 Dimension

Intuitively, we know that a point is 0-dimensional, a line is 1-dimensional, a plane is 2-dimensional and a space is 3-dimensional. A dimension gives a number of free parameters which are coordinates needed to specify a point. This has been precisely explained in many branches of mathematics, and we have dimensions in linear algebra, topology, algebraic geometry, etc.

We can begin our discussion on dimensions by considering its definition in linear algebra. A vector space A with n vectors in its basis has n dimensions, denoted as $\dim(A) = n$ (see Chapter 4 of [8]). The dimension of a linear subspace $B \subset A$ is determined by the maximal number of linearly independent vectors in B. Thus, $\dim(B) \leq \dim(A)$.

The variety of a monomial ideal I is a finite union of coordinate subspaces of $\mathbb{C}^n$. For example, consider the ideal (c.f., Chapter 9 §1 of [3])

$$I = \langle y^2z^3, x^5z^4, x^2yz^2 \rangle \subset k[x, y, z].$$

Let H_x be the plane defined by $x = 0$ and likewise for H_y and H_z. Let H_{xy} be the line $x = y = 0$. Then

$$\begin{aligned}\mathbf{V}(I) &= \mathbf{V}(y^2z^3) \cap \mathbf{V}(x^5z^4) \cap \mathbf{V}(x^2yz^2) \\ &= (H_y \cup H_z) \cap (H_x \cup H_z) \cap (H_x \cup H_y \cup H_z) \\ &= H_z \cup H_{xy}.\end{aligned}$$

The dimension of $\mathbf{V}(I)$ is 2, which is $\dim(H_z)$. The dimension of a variety of a monomial ideal is the dimension of the largest coordinate subspace contained in $\mathbf{V}(I)$.

Importantly, we can define the *dimension of a variety* V by counting monomials. Given an ideal $I \subset \mathbb{C}[x,y,z]$, let $\mathbb{C}[x,y,z]_{\leq s} = \{f \in \mathbb{C}[x,y,z] : deg\ f \leq s\}$ where deg f denotes the total degree of f. Let

$$I_{\leq s} = I \cap \mathbb{C}[x,y,z]_{\leq s}$$

be the polynomials in I of total degree $\leq s$. Then $I_{\leq s}$ is a subspace of $\mathbb{C}[x,y,z]_{\leq s}$. Now let us define the Hilbert function.

Definition 3.2.1 *Let I be an ideal in $\mathbb{C}[x,y,z]$. The affine Hilbert function of I is (c.f., Chapter 9 §3 Definition 2 of [3])*

$$\begin{aligned} {}^aHF_I(s) &= \dim\ \mathbb{C}[x,y,z]_{\leq s}/I_{\leq s} \\ &= \dim\ \mathbb{C}[x,y,z]_{\leq s} - \dim\ I_{\leq s} \end{aligned}$$

Note that this is equivalent to the number of elements in $\mathcal{B}$ of degree $\leq s$. When $I = I(V)$ we also write $\mathbb{C}[V]_{\leq s} = \mathbb{C}[x,y,z]_{\leq s}/I_{\leq s}$.

Proposition 3.2.2 *Let I be a proper monomial ideal in $\mathbb{C}[x,y,z]$. For sufficiently large integers s, the affine Hilbert function of I is a polynomial of the form*

$${}^aHF_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i},$$

where $b_i \in \mathbb{Z}$ and $b_0 > 0$ for sufficiently large s.

Definition 3.2.3 *The polynomial that equals ${}^aHF_I(s)$ for sufficiently large s is called the affine Hilbert polynomial, written as ${}^aHP_I(s)$.*

Proposition 3.2.4 *Let I be a monomial ideal in $\mathbb{C}[x,y,z]$. Then*

$$\deg\ {}^aHP_I = \dim\ \mathbf{V}(I).$$

Thus the dimension of a variety of monomial ideal is the degree of the affine Hilbert polynomial. It follows from Proposition 3.2.4 that given a variety V we can define algebraically the dimension of V as

$$\dim\ (V) := \deg\ {}^aHP_{\mathbf{I}(V)}.$$

As in our case, we will restrict our study to curves, i.e., dim $(V) = 1$. Thus, $\dim(V) = \deg\ {}^aHP_{\mathbf{I}(V)} = 1$.

Remark 3.2.5 *By the above definition, we can see that the number of monomials in* $\mathbb{C}[x,y,z]_{\leq s}/I_{\leq s}$ *is eventually linear in* s *for curves. This is not the case with planes. As an example, for* $\mathbb{C}[x,y,z]/\langle x-1\rangle$ *we get a basis* $\mathcal{B}$ *of*

$$1, y, z, y^2, yz, z^2, y^3, y^2z, yz^2, z^3, y^4, y^3z, y^2z^2, yz^3, z^4, ...$$

where the number of linearly independent monomials in $\mathbb{C}[x,y,z]_{\leq s}/I_{\leq s}$ *is* $\frac{(s+1)(s+2)}{2}$ *and* $\dim(V) = \deg\ {}^aHP_I = 2$, *as expected.*

3.3 Multiplication and Linear Algebra

In what follows, we will use grevlex order in $\mathbb{C}^3$ with $x < y < z$. The product in $\mathbb{C}[x,y,z]$ of polynomials in normal form for $\mathbb{C}[V]$ is not in normal form. Assume we have linearly independent monomials and the leading terms of the Gröbner basis $G = \{g_1, g_2, ..., g_m\}$ for $\mathbf{I}(V)$ contain y^a and z^b for some $a, b \in \mathbb{Z}^n_+$. Given polynomials f and g we will be interested in computing the normal form of the leading homogeneous part of the product fg. This means the terms with maximum total degree. Note that normal form is given by division algorithm, i.e., the remainder $\overline{fg}^G$ is the normal form of fg. We set up some linear algebra tools to study this. Throughout the section we suppose V is a curve and $I = \mathbf{I}(V)$.

Notation 3.3.1 *Here* $\mathcal{B}_{=n}$ *represents the elements of the reduced (monomial) basis of degree* n, *and* $\mathbb{C}[V]_{=n}$ *represents linear combination of these terms.*

Proposition 3.3.2 *Suppose* $y^a, z^b \in \langle LT(I)\rangle$ *for some positive integers* a, b. *The map* $m \mapsto xm$ *from* $\mathcal{B}_{=n} \mapsto \mathcal{B}_{=n+1}$ *is a bijection for sufficiently large* n.

Proof. Let $y^a, z^b \in \langle LT(I)\rangle$. Since ${}^aHP$ is linear (for curves),i.e., ${}^aHP(s) = ds+b$, for some integers d, b so

$$\begin{aligned}\dim\ \mathbb{C}[V]_{=s} &= \dim\ \mathbb{C}[V]_{\leq s} - \dim \mathbb{C}[V]_{\leq s-1} \\ &= ds + b - (d(s-1)+b) = d.\end{aligned}$$

First note that $x \notin \langle LT(I)\rangle$, otherwise it is easy to see that $\langle LT(I)\rangle$ contains all monomials of total degree $> a+b$, hence $\mathcal{B}$ will be finite, a contradiction. We need to show that $m(x,y,z) \mapsto xm(x,y,z)$ is a bijection where $m(x,y,z) \in \mathcal{B}_{=n}$, i.e., one-to-one and onto. It is obvious that the relation is one-to-one. To show that it is onto, suppose $m(x,y,z) \in \mathcal{B}_{=n+1}$ then $m(x,y,z) \notin \langle LT(I)\rangle$. Let $m(x,y,z) = x^iy^jz^k$ then $i+j+k = n+1$ where $j < a$ and $k < b$. Thus, $x^iy^jz^k = x(x^{i-1}y^jz^k)$ as long as $n > a+b$, then $i-1 > 0$. Since $x \notin \langle LT(I)\rangle$ and $x^iy^jz^k \notin \langle LT(I)\rangle$ then it implies that $x^{i-1}y^jz^k \notin \langle LT(I)\rangle$. If not, then $x^{i-1}y^jz^k \in \langle LT(I)\rangle$ imply that $x(x^{i-1}y^jz^k) \in \langle LT(I)\rangle$ and so $x^iy^jz^k \in \langle LT(I)\rangle$. There is a contradiction. Therefore, $(x^{i-1}y^jz^k) \in \mathcal{B}_{=n}$ and $x^iy^jz^k \in \mathcal{B}_{=n+1}$ is its corresponding image under multiplication by x, which indicates that the map is onto. So we get a bijection. □

We can now show that the map $m(x,y,z) \mapsto xm(x,y,z)$ defines a linear identity matrix. Identify $\mathcal{B}_{=n} = \{m_1, m_2, ..., m_d\}$ where $m_1 < m_2 < \cdots < m_d$ with the standard basis of $\mathbb{C}^d$ via

$$\begin{aligned} m_1(x,y,z) &\leftrightarrow e_1 = (1,0,0,...,0) \\ &\vdots \\ m_d(x,y,z) &\leftrightarrow e_d = (0,0,0,...,1). \end{aligned}$$

We have a one-to-one and onto mapping. By Proposition 3.3.2, the map $\mathcal{B}_{=n} \mapsto \mathcal{B}_{=n+1}$ is a bijection hence so is the linear map $\mathbb{C}[V]_{=n} \mapsto \mathbb{C}[V]_{=n+1}$. Identify with a linear map $\mathbb{C}^d \mapsto \mathbb{C}^d$. Given a polynomial

$$p = \sum_{i=1}^{d} a_i m_i,$$

let

$$[p] := (a_1, a_2, ..., a_d)$$

be its representation in $\mathbb{C}^d$. Then

$$\sum_{i=1}^{d} a_i m_i \mapsto x \sum_{i=1}^{d} a_i m_i = \sum_{i=1}^{d} a_i (x m_i).$$

Therefore in $\mathbb{C}^d$, $[p] \mapsto [xp]$ is $(a_1, a_2, ..., a_d) \mapsto (a_1, a_2, ..., a_d)$, the identity map, represented by identity matrix (denoted I).

Given a polynomial $p \in \mathbb{C}[x, y, z]$, we now study $\phi : \mathbb{C}[V]_{=n} \mapsto \mathbb{C}[V]_{=n+\deg p}$ given by $\phi(f) = (\overline{fp}^G)_H$.

Notation 3.3.3 *(i) Here, $(\cdot)_H$ represents taking the leading homogeneous (top total degree) terms.*
(ii) l.d.t stands for lower degree terms *in a given polynomial expression.*

For any polynomial $p \in \mathbb{C}[x, y, z]$ we show that the operation $\phi : f \mapsto (\overline{fp}^G)_H$ given by

$$\phi(f) = \begin{cases} (\overline{fp}^G)_H & \text{if } \deg \overline{fp}^G = \deg fp, \\ 0 & \text{if } \deg \overline{fp}^G < \deg fp \end{cases}$$

is linear. That is, let $s, t \in \mathbb{C}[V]_{=n}$ and $\alpha \in \mathbb{C}$ then we want

$$\phi(s + t) = \phi(s) + \phi(t) \quad \text{and}$$
$$\phi(\alpha s) = \alpha \phi(s).$$

We will verify linearity in the case that $\deg \overline{fp}^G = \deg fp$. The proof in other cases is similar. Essential use is made of the uniqueness of remainder under division algorithm.

Let $f \in \mathbb{C}[V]_{=s}$, then in $\mathbb{C}[x, y, z]$ by division algorithm,

$$\begin{aligned} pf &= q_1 g_1 + q_2 g_2 + \cdots + q_k g_k + \overline{pf}^G \\ &= q_1 g_1 + q_2 g_2 + \cdots + q_k g_k + (\overline{pf}^G)_H + (\overline{pf}^G)_{l.d.t.} \end{aligned}$$

Now we need to show that the map $f \mapsto (\overline{pf}^G)_H$ is linear. Suppose that

$$f = v + w$$

and then by division algorithm,

$$pv = r_1 g_1 + r_2 g_2 + \cdots + r_k g_k + \overline{pv}^G$$
$$pw = s_1 g_1 + s_2 g_2 + \cdots + s_k g_k + \overline{pw}^G$$

Therefore we can write,

$$pf = p(v+w) = (r_1 + s_1)g_1 + \cdots + (r_k + s_k)g_k + \overline{p(v+w)_H}^G + \overline{p(v+w)_{l.d.t.}}^G$$

Since G is a Gröbner basis, by uniqueness of remainder (Theorem 2.5.17), $\overline{pf}^G = \overline{pv}^G + \overline{pw}^G$. Equating the coefficients, we get

$$(\overline{pf}^G)_H = (\overline{pv}^G)_H + (\overline{pw}^G)_H.$$

Now let $\alpha \in \mathbb{C}$ be some scalar and $f = \alpha v$ then

$$\begin{aligned} pf = \alpha pv &= \alpha(r_1 g_1 + r_2 g_2 + \cdots + r_k g_k + \overline{pv}^G) \\ &= \alpha r_1 g_1 + \alpha r_2 g_2 + \cdots + \alpha r_k g_k + \alpha(\overline{pv}^G). \end{aligned}$$

Again by uniqueness of remainder, $\overline{pf}^G = \alpha(\overline{pv}^G)$, and hence equating coefficients

$$(\overline{pf}^G)_H = \alpha(\overline{pv}^G)_H.$$

Thus the map $f \mapsto (\overline{pf}^G)_H$ is linear from $\mathbb{C}[V]_{=n} \to \mathbb{C}[V]_{=n+\deg p}$. Since we have a linear map, we conclude that the matrix representation exists for the map

$$[f] \mapsto \left[(\overline{pf}^G)_H\right].$$

We denote by X, Y, Z the linear transformation or matrix representation of the maps from $\mathbb{C}[V]_{=n} \to \mathbb{C}[V]_{=n+1}$ corresponding to multiplication by x, y, z. By our definition, $X = I$.

Example 3.3.4 *As in Example 3.1.6, we can calculate the matrices for top degree terms under multiplication. Note that the basis elements of degree k are*

$$\mathcal{B}_{=k} = \{x^k, x^{k-1}y, x^{k-1}z, x^{k-2}y^2\}.$$

Multiplication by x is given as

$$x(a_1x^k + a_2x^{k-1}y + a_3x^{k-1}z + a_4x^{k-2}y^2) = a_1x^{k+1} + a_2x^ky + a_3x^kz + a_4x^{k-1}y^2.$$

Thus we get the linear transformation $\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} \mapsto \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}$ *represented by matrix identity I. So $X = I$.*

Now using the same argument, we calculate Y from y.

$$\begin{aligned}
yf &= y(a_1x^k + a_2x^{k-1}y + a_3x^{k-1}z + a_4x^{k-2}y^2) \\
&= a_1x^ky + a_2x^{k-1}y^2 + a_3x^{k-1}yz + a_4x^{k-2}y^3 \\
\overline{yf}^G &= a_1x^ky + a_2x^{k-1}y^2 + a_3x^{k-1}(3y^2 + xy - xz - x^2) \\
&\quad + a_4x^{k-2}(\frac{6}{10}x^2y + \frac{2}{10}xy^2 - \frac{1}{10}x^2z - \frac{1}{10}x^3) \\
&= a_1x^ky + a_2x^{k-1}y^2 + a_3x^{k-1}y^2 + a_3x^ky - a_3x^kz - a_3x^{k+1} \\
&\quad + \frac{6}{10}a_4x^ky + \frac{2}{10}a_4x^{k-1}y^2 - \frac{1}{10}a_4x^kz - \frac{1}{10}a_4x^{k+1} \\
(\overline{yf}^G)_H &= a_2x^ky + a_4x^{k-1}y^2 + (-a_1x^{k+1} + a_2x^ky - a_3x^kz + 3a_4x^{k-1}y^2) \\
&\quad + (-\frac{1}{10}a_1x^{k+1} + \frac{6}{10}a_2x^ky - \frac{1}{10}a_3x^kz + \frac{2}{10}a_4x^{k-1}y^2)
\end{aligned}$$

The linear transformation is $\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} \mapsto \begin{bmatrix} a_2 \\ a_4 \\ -a_1 + a_2 - a_3 + 3a_4 \\ -\frac{1}{10}a_1 + \frac{6}{10}a_2 - \frac{1}{10}a_3 + \frac{2}{10}a_4 \end{bmatrix}$ *represented by*

the matrix $Y = \begin{bmatrix} 0 & 0 & -1 & -\frac{1}{10} \\ 1 & 0 & 1 & \frac{6}{10} \\ 0 & 0 & -1 & -\frac{1}{10} \\ 0 & 1 & 3 & \frac{2}{10} \end{bmatrix}^T$.

Remark 3.3.5 *Using matrices to represent polynomial multiplication is common in algorithmic coding theory for polynomial codes (see Chapter 22 of [7]).*

Chapter 4

Projective Space

In this chapter, we will study projective space over $\mathbb{C}$, specifically $\mathbb{P}^3(\mathbb{C})$. This will be further discussed in relating projective space to the existence of homogeneous coordinates. Interestingly, homogeneous coordinates are not truly coordinates that specify points uniquely, but they are very convenient for doing calculations in projective space. Similarly, projective varieties will be discussed using homogeneous polynomials. We will derive an important relation between the behaviour of an algebraic curve at the hyperplane at infinity and eigenvalues of matrices Y, Z defined at the end of the previous chapter.

To clearly understand projective space, it is convenient for us to study projective plane and get a generalized idea on the construction of projective space. Note that we will maintain our discussion on the complex field, more precisely in $\mathbb{C}^3$. As an observation, two planes in $\mathbb{C}^3$ will intersect in a line, except if they are parallel. To resolve this exception we can introduce an 'ideal' line at infinity and an ideal plane containing these lines to get a projective space where two planes always determine a unique line and two lines will always determine a unique plane.

We can get projective space $\mathbb{P}^3(\mathbb{C})$ by taking lines through the origin in $\mathbb{C}^4$ as the projective points. If we let the hyperplane $t = 1$ be the original space then every line $\{\lambda(t, x, y, z) : \lambda \in \mathbb{C}\}$ where $t \neq 0$ will meet the space at a unique point

$(1, \frac{x}{t}, \frac{y}{t}, \frac{z}{t})$. Any line in $(0, x, y, z)$ corresponds to an ideal point, and $t = 0$ gives the ideal plane (plane at infinity), denoted H_∞. For this reason, projective space is represented using the homogeneous coordinate system rather than the Euclidean coordinate system (where the concept of infinity does not exist).

Now we can generalize our definition of projective space.

Definition 4.0.1 *The n-dimensional complex projective space $\mathbb{P}^n(\mathbb{C})$ is the set of lines through the origin in the vector space $\mathbb{C}^{n+1}$. Then $\mathbb{P}^n(\mathbb{C})$ is the set of equivalence classes of $\sim$ on $\mathbb{C}^{n+1}\backslash\{0\}$, i.e.,*

$$\mathbb{P}^n(\mathbb{C}) = (\mathbb{C}^{n+1}\backslash\{0\})/\sim .$$

Each nonzero $(n+1)$-tuple $(x_0, x_1, ..., x_n) \in \mathbb{C}^{n+1}$ defines a point p in $\mathbb{P}^n(\mathbb{C})$, written $[x_0 : x_1 : ... : x_n]$. This is called a representation of p in homogeneous coordinates.

The equivalence relation $\sim$ is given by

$$(x_0, x_1, ..., x_n) \sim (\lambda x_0, \lambda x_1, ..., \lambda x_n), \lambda \in \mathbb{C}, \lambda \neq 0$$

and hence $[x_0 : x_1 : \cdots : x_n] = [\lambda x_0 : \lambda x_1 : \cdots : \lambda x_n]$. It is important to mention that projective $n-$space can be covered by $n + 1$ copies of the complex space $(\mathbb{C}^n)$ in $\mathbb{P}^n(\mathbb{C})$. For each $i = 0, 1, ..., n$, we can let

$$U_i = \{[x_0 : x_1 : ... : x_n] \in \mathbb{P}^n(\mathbb{C}) : x_i \neq 0\}.$$

So U_i has a one-to-one correspondence to all points in $\mathbb{C}^n$ via $[x_0 : ..x_i : ..x_n] \leftrightarrow (\frac{x_0}{x_i}, ..., \frac{x_n}{x_i})$.

Let us define projective varieties in projective spaces using the set of homogeneous polynomials.

Definition 4.0.2 *Given $d \in \mathbb{Z}_+$, a polynomial $f \in \mathbb{C}[x_1, x_2, ..., x_n]$ is a homogeneous polynomial of total degree d such that every term in f has total degree d. Equivalently,*

$$f(\lambda x_0, \lambda x_1, ..., \lambda x_n) = \lambda^d f(x_0, x_1, ..., x_n)$$

for any $\lambda \in \mathbb{C}$.

Definition 4.0.3 *Let* $f_1, f_2, ..., f_m \in \mathbb{C}[x_0, x_1, ..., x_n]$ *be homogeneous polynomials. Then*

$$\mathbf{V}(f_1, ..., f_m) = \{[a_0 : a_1 : ... : a_n] \in \mathbb{P}^n(\mathbb{C}) : f_i(a_0, a_1, ..., a_n) = 0 \ \forall \ 1 \leq i \leq m\}$$

is called the projective variety defined by $f_1, f_2, ..., f_m$.

A projective variety in $\mathbb{P}^3 = \mathbb{P}^3(\mathbb{C}) = \mathbb{C}^3 \cup H_\infty$ is the projective extension of affine variety in $\mathbb{C}^3$ by identifying (x, y, z) in $\mathbb{C}^3$ with coordinates in $\mathbb{P}^3$ given as $[1 : x : y : z]$. Thus, the plane at infinity (H_∞) is given by all points of the form $[0 : X : Y : Z]$. Changing to U_1, with coordinates $(t, y, z) \leftrightarrow [t : 1 : y : z]$, this is given as $[0 : 1 : y : z]$ which is the plane $t = 0$.

Let us examine the notion of homogenization and dehomogenization. Suppose $g(x_1, x_2, ..., x_n) \in \mathbb{C}[x_1, x_2, ..., x_n]$ is a polynomial with degree d. Let $g = \sum_{i=0}^{d} g_i$ be the sum of the homogeneous components of g_i with total degree i. Define the homogeneous polynomial

$$\begin{aligned} g^h(x_0, x_1, ..., x_n) &= \sum_{i=0}^{d} g_i(x_1, x_2, ..., x_n) x_0^{d-i} \\ &= g_d(x_1, ..., x_n) + g_{d-1}(x_1, ..., x_n)x_0 + \cdots + g_0(x_1, ..., x_n)x_0^d \end{aligned}$$

and call g^h the homogenization of g. The homogenization of g can be computed using

$$g^h = x_0^d \cdot g\left(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}\right).$$

To dehomogenize g^h set $x_0 = 1$. That is, $g^h(1, x_1, ..., x_n) = g(x_1, x_2, ..., x_n)$. Notice that to homogenize then dehomogenize returns the original polynomial but this is not the case when we dehomogenize a homogeneous polynomials then homogenize again. In this case, let $F(x_0, x_1, ..., x_n)$ be a homogeneous polynomial and let x_0^e be the highest power of x_0 dividing F. If $f = F(1, x_1, ..., x_n)$ is a dehomogenization of F then $F = x_0^e \cdot f^h$.

Example 4.0.4 *Let* $g(x,y) = x^2 - 2x^3y + y + 2$, *then*

$$g^h(t,x,y) = t^4 g\left(\frac{x}{t}, \frac{y}{t}\right) = t^4\left(\left(\frac{x}{t}\right)^2 - 2\left(\frac{x}{t}\right)^3\left(\frac{y}{t}\right) + \left(\frac{y}{t}\right) + 2\right)$$
$$= x^2t^2 - 2x^3y + yt^3 + 2t^4.$$

The way to change coordinates in projective space is to homogenize, then dehomogenize at a different variable.

Example 4.0.5 *Consider the projective variety given by* $\tilde{x}\tilde{y} = \tilde{t}^2$ *in* $\mathbb{P}^2$, *where* $[\tilde{t} : \tilde{x} : \tilde{y}]$ *are homogeneous coordinates. Then* $x = \frac{\tilde{x}}{\tilde{t}}$ *and* $y = \frac{\tilde{y}}{\tilde{t}}$ *in* U_0 *where* (x,y) *identified with* $[1 : x : y]$. *Changing to coordinates* (t,w) *in* U_1 *identified with* $[t : 1 : w]$, *we get* $t = \frac{\tilde{t}}{\tilde{x}} = \frac{1}{x}$ *and* $w = \frac{\tilde{y}}{\tilde{x}} = \frac{y}{x}$. *In* U_0 *the affine variety is* $xy = 1$, *in* U_1 *it is* $y = t^2$.

To get a better understanding of projective varieties, we need to use homogeneous ideals.

Definition 4.0.6 *An ideal* $I \subset \mathbb{C}[x_0, x_1, ..., x_n]$ *is homogeneous if it is generated by homogeneous polynomials. Also for any ideal* $I \subset \mathbb{C}[x_1, ..., x_n]$, *we can define a homogeneous ideal* $I^h \subset \mathbb{C}[x_0, x_1, ..., x_n]$ *by*

$$I^h = \langle \{g^h : g \in I\} \rangle$$

where g^h *is the homogenization of* g.

Example 4.0.7 *If* $I = \langle f \rangle$ *then it is true that* $I^h = \langle f^h \rangle$, *for example* $\langle x^2+y^2-1 \rangle^h = \langle x^2 + y^2 - t^2 \rangle$.

Example 4.0.8 *Consider* $I = \langle f_1, f_2 \rangle = \langle x^2 - y, x^3 - z \rangle$, *then homogenizing the generators gives* $L = \langle x^2-yt, x^3-zt^2 \rangle$ *which does not contain* $tz-xy = (xf_1-f_2)^h \in I^h$. *Thus,* $L \neq I^h$.

Proposition 4.0.9 *Let* $I \subset \mathbb{C}[x_1, x_2, ..., x_n]$ *be a homogeneous ideal. If*

$$I = \langle f_1, f_2, ..., f_m \rangle$$

where $f_1, f_2, ..., f_m$ are homogeneous then

$$\mathbf{V}(I) = \mathbf{V}(f_1, f_2, ..., f_m)$$

is a projective variety.

If we have a Gröbner basis, the problem in Example 4.0.8 goes away.

Theorem 4.0.10 *Let $I \subset \mathbb{C}[x_1, x_2, ..., x_n]$ be an ideal. Let $G = \{g_1, g_2, ..., g_m\}$ be the Gröbner basis for I with respect to grevlex order. Then $G^h = \{g_1^h, g_2^h, ..., g_m^h\}$ is a Gröbner basis for $I^h \subset \mathbb{C}[x_1, x_2, ..., x_n]$.*

Example 4.0.11 *From Example 4.0.8, we can compute the Gröbner basis for I with respect to grevlex order. The Gröbner basis is*

$$G = \{x^2 - y, xy - z, y^2 - xz\}.$$

So $\{x^2 - yt, tz - xy, y^2 - xz\}$ is the Gröbner basis for I^h. Note that it also contains $tz - xy$.

Definition 4.0.12 *Given an affine variety $W \subset \mathbb{C}^n$, the projective closure of W is the projective variety $\overline{W} = \mathbf{V}(\mathbf{I}_a(W)^h) \subset \mathbb{P}^n(\mathbb{C})$, where $\mathbf{I}_a(W)^h \subset \mathbb{C}[x_0, x_1, ..., x_n]$ is the homogenization of the ideal $\mathbf{I}_a(W) \subset \mathbb{C}[x_1, x_2, ..., x_n]$ as in Definition 4.0.6. Note that $\mathbf{I}_a$ represent the affine ideal in $\mathbb{C}[x_1, x_2, ..., x_n]$. In this section, $\mathbf{I}_a$ and $\mathbf{V}_a$ will denote affine quantities while $\mathbf{I}$ and $\mathbf{V}$ will denote projective quantities in one extra variable.*

Projective closure has these important properties.

Proposition 4.0.13 *Let $W \subset \mathbb{C}^n$ be an affine variety and let $\overline{W} \subset \mathbb{P}^n(\mathbb{C})$ be its projective closure. Then,*

(i) $\overline{W} \cap U_0 = \overline{W} \cap \mathbb{C}^n = W$.

(ii) $\overline{W}$ *is the smallest projective variety in* $\mathbb{P}^n(\mathbb{C})$ *containing* W.

Theorem 4.0.14 *Let* $I \subset \mathbb{C}[x_1, x_2, ..., x_n]$ *be an ideal. Then* $\mathbf{V}(I^h) \subset \mathbb{P}^n(\mathbb{C})$ *is the projective closure of* $\mathbf{V}_a(I) \subset \mathbb{C}^n$.

Example 4.0.15 *Referring to Example 4.0.8, if*

$$W = \mathbf{V}_a(\langle x^2 - y, x^3 - z\rangle) \subset \mathbb{C}^3$$

then it follows that the projective closure is

$$\overline{W} = \mathbf{V}(\langle x^2 - yt, xy - tz, y^2 - xz\rangle) \subset \mathbb{P}^3.$$

Since $\mathbb{P}^3 = \mathbb{C}^3 \cup H_\infty$, *we can find the intersection of* $\overline{W}$ *with the projective plane at infinity. Let* $t = 0$ *we get* $x = 0$ *and* $y = 0$. *Thus,* $[0 : 0 : 0 : 1]$ *is the only point at infinity.*

Now, we will investigate in detail the relation between the projective geometry of an algebraic curve $V \subset \mathbb{C}^3$ and computational properties of its corresponding ring of polynomials $\mathbb{C}[V]$. The main tool we will use is the linear algebra from Chapter 3.

Take Y from Chapter 3 in this thesis, as the matrix representation of

$$f \mapsto \begin{cases} (\overline{yf}^G)_H & \text{if } \deg\overline{yf}^G = \deg yf, \\ 0 & \text{if } \deg\overline{yf}^G < \deg yf. \end{cases}$$

An eigenvalue λ of Y is a solution of the characteristic equation of Y, $\det(Y - \lambda I) = 0$. Let $P(x, y)$ be the homogenization of the characteristic polynomial, such that $P(1, \lambda) = \det(Y - \lambda I)$.

Lemma 4.0.16 *There exists a polynomial* $R(x, y, z)$ *with* $\deg(R) < \deg(P)$ *and for all* $(x, y, z) \in V$,

$$P(x, y) = R(x, y, z).$$

Proof. By the Cayley-Hamilton Theorem, (see Chapter 3 of [8]) $P(I, Y) = 0$. Translating this equation into computation on V, this says that $\deg \overline{P}^G < \deg P$, so $P(x, y)$ coincides on V with a polynomial $R(x, y, z) = \overline{P}^G$ of lower degree. □

The same Lemma also hold for Z representing multiplication by z.

Proposition 4.0.17 *Let $[0 : 1 : \lambda_1 : \lambda_2]$ be a point of the projective closure of V on H_∞. Then λ_1 is an eigenvalue of Y, and λ_2 is an eigenvalue of Z.*

Proof. At a point $(x, y, z) \in V$ we have $P(x, y) - R(x, y, z) = 0$ by the previous lemma. We now homogenize with the variable t. Set

$$H(t, x, y, z) := P(x, y) - t^\alpha \tilde{R}(t, x, y, z),$$

where $\alpha = \deg(P) - \deg(R)$ and $\tilde{R}$ is the homogenization of R (so $\deg(\tilde{R}) = \deg(R)$ and $\tilde{R}(1, x, y, z) = R(x, y, z)$. Projectively, we have $H(t, x, y, z) = 0$ whenever $[t : x : y : z] \in \tilde{V} \setminus H_\infty$, where $\tilde{V}$ denotes the projective closure.

In the local coordinates $U_1, (t, y, z) \sim [t : 1 : y : z]$ near H_∞, we have $H(t, 1, y, z) = 0$ whenever $[t : 1 : y : z] \in \tilde{V}$ with $t \neq 0$. Hence by continuity of the polynomial function $(t, y, z) \to H(t, 1, y, z)$ and the fact that $\tilde{V}$ extends continuously across H_∞ in these coordinates, we can extend the equation $H(t, 1, y, z) = 0$ across points of $\tilde{V}$ with $t = 0$. Hence

$$0 = H(0, 1, \lambda_1, z) = P(1, \lambda_1) = \det(Y - \lambda_1 I),$$

which shows that λ_1 is an eigenvalue of Y.

The proof that λ_2 is an eigenvalue of Z follows the same method, switching the roles of y and z in this proof as well as the proof of the previous lemma. □

Chapter 5

Chebyshev Constant

This chapter will investigate directional Chebyshev constants associated to a compact set K on an algebraic curve V on $\mathbb{C}^3$. For curves, use V to denote both the curve and its projective closure in $\mathbb{P}^3(\mathbb{C})$. By Proposition 4.0.17 of Chapter 4, if $\lambda = [0 : 1 : \lambda_1 : \lambda_2] \in V$ then λ_1, λ_2 are eigenvalues for Y and Z respectively in the matrix representation. Let, $V_{\lambda_1},\ W_{\lambda_2}$ be the homogeneous polynomials that corresponds to eigenvectors. In linear algebra, $Y[V_{\lambda_1}] = \lambda_1[V_{\lambda_1}]$ which in polynomial form is $yV_{\lambda_1}(x, y, z) = \lambda_1 xV_{\lambda_1}(x, y, z) + l.d.t.$ Under multiplication by a suitable constant, we can normalize the polynomials such that

$$V_{\lambda_1}(1, \lambda_1, \lambda_2) = W_{\lambda_2}(1, \lambda_1, \lambda_2) = 1.$$

Given a compact set $K \subset V$, set for a positive integer s,

$$\tau_{\lambda,s} := \min \left\{ \|p\|_K : p(x, y, z) = x^{s-d} V_{\lambda_1}(x, y, z) W_{\lambda_2}(x, y, z) + l.d.t. \right\}^{1/s} \qquad (5.1)$$

where d is the degree of the polynomial $V_{\lambda_1} W_{\lambda_2}$.

Definition 5.0.1 *A polynomial for which the minimum on the right-hand side of (5.1) is attained is called a Chebyshev polynomial on V for (K, λ). The constant $\tau_{\lambda,s}$ is called the Chebyshev constant of order s for (K, λ). The directional Chebyshev*

constant of K for λ is defined by

$$\tau_V(K,\lambda) = \tau(K,\lambda) := \lim_{s\to\infty} \sup(\tau_{\lambda,s}). \tag{5.2}$$

Remark 5.0.2 *If K is a finite set of points, then one can find a polynomial of the form (5.1) of sufficiently high degree that vanishes at these points. Hence in this case $\tau(K,\lambda) = 0$.*

Theorem 5.0.3 *Let $K \subset V$ be a compact set. Then the ordinary limit in (5.2) exists,*

$$\tau(K,\lambda) = \lim_{s\to\infty} \tau_{\lambda,s}. \tag{5.3}$$

Proof. Let $\{q_s\}_{s=1}^{\infty}$ be a sequence of Chebyshev polynomials on V for (K,λ) such that $\deg(q_s) = s$. Take two subsequences $\{q_{s_k}\}_{k=1}^{\infty}$ and $\{q_{t_k}\}_{k=1}^{\infty}$ such that

$$\tau_{\lambda,s_k} = \|q_{s_k}\|_K^{1/s_k} \longrightarrow \beta := \lim_{s\to\infty} \sup\ \tau_{\lambda,s}$$

and

$$\tau_{\lambda,t_k} = \|q_{t_k}\|_K^{1/t_k} \longrightarrow \alpha := \lim_{s\to\infty} \inf\ \tau_{\lambda,s}.$$

Passing if necessary to a subsequence, we may assume that $\frac{s_k}{t_k} \to 0$ as $k \to \infty$. Next, for each k we use the division algorithm to define r_k and l_k by

$$t_k = s_k r_k + l_k, \qquad 0 \le l_k \le s_k.$$

Consider the polynomial $x^{l_k}(q_{s_k})^{r_k}$. If $V_{\lambda_1}, W_{\lambda_2}$ are as defined earlier, then it implies that $Y[V_{\lambda_1}] = \lambda_1[V_{\lambda_1}]$ and $Z[W_{\lambda_2}] = \lambda_2[W_{\lambda_2}]$. Let $d_1 = \deg V_{\lambda_1}(x,y,z)$ and $d_2 = \deg W_{\lambda_2}(x,y,z)$ then $d = d_1 + d_2$.

For any polynomial p

$$p(x,y,z)V_{\lambda_1}W_{\lambda_2} = x^{\deg p}\ p_T(1,\lambda_1,\lambda_2)V_{\lambda_1}W_{\lambda_2} + l.d.t.$$

We have

$$\begin{aligned} x^{l_k}(q_{s_k})^{r_k} &= x^{l_k}\left(x^{s_k-d}V_{\lambda_1}W_{\lambda_2}+l.d.t.\right)^{r_k-1}\left(x^{s_k-d}V_{\lambda_1}W_{\lambda_2}+l.d.t.\right) \\ &= x^{l_k}x^{(s_k-d)r_k}(V_{\lambda_1}W_{\lambda_2})^{r_k-1}V_{\lambda_1}W_{\lambda_2}+l.d.t. \\ &= x^{l_k}x^{(s_k-d)r_k}x^{d(r_k-1)}[V_{\lambda_1}(1,\lambda_1,\lambda_2)W_{\lambda_2}(1,\lambda_1,\lambda_2)]^{r_k-1}V_{\lambda_1}W_{\lambda_2}+l.d.t. \qquad (5.4) \\ &= x^{l_k}x^{(s_k-d)r_k}x^{d(r_k-1)}V_{\lambda_1}(x,y,z)W_{\lambda_2}(x,y,z)+l.d.t. \\ &= x^{s_kr_k-dr_k+l_k}\ x^{d_1(r_k-1)}V_{\lambda_1}(x,y,z)\ x^{d_2(r_k-1)}W_{\lambda_2}(x,y,z)+l.d.t. \\ &= x^{t_k-d_1-d_2}V_{\lambda_1}(x,y,z)W_{\lambda_2}(x,y,z)+l.d.t. \\ &= x^{t_k-d}V_{\lambda_1}(x,y,z)W_{\lambda_2}(x,y,z)+l.d.t.. \end{aligned}$$

By the normalization, the expression $[V_{\lambda_1}(1,\lambda_1,\lambda_2)W_{\lambda_2}(1,\lambda_1,\lambda_2)]^{r_k-1}=1$ in line (5.4).

The polynomial $x^{l_k}(q_{s_k})^{r_k}$ is a competitor polynomial for the Chebyshev constant of order t_k for (K,λ), so $\|x^{l_k}(q_{s_k})^{r_k}\|_K \geq (\tau_{\lambda,t_k})^{t_k}$. On the other hand,

$$\|x^{l_k}(q_{s_k})^{r_k}\|_K \leq \|x\|_K^{l_k}(\tau_{\lambda,s_k})^{s_kr_k}.$$

Therefore

$$\tau_{\lambda,t_k} \leq \|x\|_K^{l_k/t_k}(\tau_{\lambda,s_k})^{\frac{s_kr_k}{t_k}}. \qquad (5.5)$$

As $k\to\infty$, $\frac{s_k}{t_k}\to 0$ implies that $\frac{l_k}{t_k}\to 0$ and $\frac{s_kr_k}{t_k}\to 1$. Hence the left-hand side of (5.5) goes to β and the right-hand side goes to α. So $\beta\leq\alpha$, which proves that the limit in (5.3) exists. □

Chapter 6

Conclusion

In this thesis, we have seen that Gröbner basis methods are useful for doing concrete computations on varieties. The idea of Gröbner bases was introduced by Buchberger in 1965 in order to do algorithmic computations on ideals in polynomial rings. Similar work have attracted a lot of attention in the study of algebraic varieties in arbitrary dimension which is an area of current research. Using these tools, we can compute in the quotient ring $\mathbb{C}[x, y, z]/\mathbf{I}(V)$ effectively and hence get the properties such as the normal form, dimensions, linear combination of the reduced monomial basis $\mathcal{B}$ and the matrix representation.

In projective space, we used homogeneous coordinates to study V at infinity. At a point on the hyperplane at infinity, its local coordinates were seen to be related to properties of multiplication in $\mathbb{C}[V]$. In particular, if $\lambda = [0 : 1 : \lambda_1 : \lambda_2]$ was a point on the projective closure of V, then λ_1 was an eigenvalue for Y and λ_2 an eigenvalue for Z, where Y and Z were matrix representations of multiplication by y and z respectively as done in Chapter 3.

Further investigation can be conducted on issues related to Proposition 4.0.17. Important questions can be raised as to what happens if λ_1, λ_2 are eigenvalues of Y and Z respectively but $[0 : 1 : \lambda_1 : \lambda_2] \notin V$. This is fundamental to future study.

Also, we think that as in $\mathbb{C}^2$, the directional Chebyshev constants can be used

to derive a notion of transfinite diameter $d(K)$ on a curve, and the formula

$$d(K) = \left(\prod_{j=1}^{d} \tau(K, \lambda_j) \right)^{1/d}$$

holds, as done in [9].

References

[1] Thomas Bloom and Norman Levenberg. Weighted pluripotential theory in $\mathbb{C}^n$. *Amer. J. Math.*, 125(1):57–103, 2003.

[2] Bruno Buchberger. *An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal (German).* PhD thesis, University of Innsburk, Austria, 1965.

[3] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms.* Springer, 2nd edition, 1996.

[4] John B. Fraleigh. *A First Course in Abstract Algebra.* Addison Wesley, 7th edition, 2003.

[5] David Hilbert. Ueber die theorie der algebraischen formen. *Mathematische Annalen*, 36(4):473–534, 1890.

[6] Mieczysław Jedrzejowski. The homogeneous transfinite diameter of a compact subset of $\mathbb{C}^n$. *Ann. Polon. Math.*, 55:191–205, 1991.

[7] Thomas. W. Judson. *Abstract Algebra Theory and Application.* Free Software Foundation, 2011.

[8] Ron Larson, Bruce H. Edwards, and David C. Falvo. *Elementary Linear Algebra.* Houghton Mifflin, 5th edition, 2004.

[9] Sione Ma'u. Chebyshev constants and transfinite diameter on algebraic curves in $\mathbb{C}^2$. *Ind. Univ. Math. J. (to appear).*

[10] Thomas Ransford. *Potential Theory in the Complex Plane.* Cambridge University Press, 1995.

[11] Edward. B. Saff and Vilmos Toktik. *Logarithmic Potentials with External fields.* Springer, 1997.

[12] V.P. Zaharjuta. Transfinite diameter, Chebyshev constants, and capacity for compacta in $\mathbb{C}^n$. *Math. USSR Sbornik*, 25(3):350–364, 1975.