On the Groebner bases of Ideals of Finite Sets of Points in $\mathbb{P}^1 \times \mathbb{P}^1$

by
Jason Palombaro

A project submitted to the Department of
Mathematical Sciences in conformity with the requirements
for Math 790 (Major Research Project)

McMaster University
Hamilton, Ontario, Canada

Abstract

In this report, we are interested in determining the Groebner basis for the defining ideal of a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$. In addition, we would also like to be able to get the reduced Groebner basis or the Universal Groebner basis. Our first main result is proving that the set of generators of the defining ideal of an arithmetically Cohen-Macaulay set of points in $\mathbb{P}^1 \times \mathbb{P}^1$, given by E. Guardo and A. Van Tuyl in [4], is the Universal Groebner basis. We show that this set of generators satisfies Buchberger's criterion under an arbitrary monomial order, and then deduce that it is also reduced. Our second main result is a new algorithm that computes the reduced Groebner basis for the defining ideal of any finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$. This new algorithm is based upon the Buchberger-Moeller algorithm for ideals of points in $\mathbb{P}^n$.

Acknowledgements

I would like to express my great appreciation to my supervisor Adam Van Tuyl. He has been exceptionally generous, friendly, and patient while devoting his time to guide me through this project. It is the knowledge that I have gained from working under his supervision that has allowed me to succeed in completing this project. I am very grateful for everything he has done, and for this, I would like to give him my most sincere thank you.

I am also particularly grateful for the assistance given by the professors at McMaster University that I have had the pleasure of learning from. All of whom, I would like to thank for their time and overall dedication to their students.

My special thanks are extended to the faculty and staff of the department of Mathematics and Statistics at McMaster University. There have been numerous instances where they have been particularly helpful, for which I am very much appreciative.

Contents

CHAPTER 1

Introduction

A Groebner basis is a generating set of an ideal that gives us some useful information about the ideal. They were introduced by Bruno Buchberger, who also developed a criterion for a set of generators of an ideal to be a Groebner basis. This criterion is known as Buchberger's criterion.

Groebner bases have applications in many topics of mathematics, including algebraic geometry and graph theory. However, even if we are given generators of an ideal, we do not always have a Groebner basis. Sometimes we do not even have generators of the ideal. Often in these cases, if we wish to know the reduced Groebner basis of a certain ideal, the computations needed to find it can be quite long.

In this report, we will look at the Buchberger-Moeller algorithm, which computes the reduced Groebner basis for the defining ideal of a finite set of points in $\mathbb{P}^n$ with respect to any given monomial order. It was developed by B. Buchberger and H.M. Moeller in [1]. Our purpose is to develop a version of the algorithm that will allow us to compute the Groebner basis of the defining ideal for a set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ for any given monomial order.

In Chapter 2, we will develop the algebraic background that will be required. A significant part of the background algebra needed will be facts about Groebner bases and the division algorithm. Chapter 2 will start by defining the basics such as monomials and monomial orders. We then introduce the definition of a Groebner basis, as well as how they are used. Throughout the chapter, we will see examples of the division algorithm and Groebner bases, especially focusing on how they are related through S-polynomials and Buchberger's criterion. We will then define homogeneous polynomials and give Theorem 2.30, which states that two homogeneous polynomials in seperate variables satisfy Buchberger's criterion. This theorem will play a key role in Chapter 4 when proving a given set of generators of a certain defining ideal is in fact a Groebner basis. Following that, we introduce Hilbert functions. We end the chapter by showing that having a Groebner basis for a homogeneous ideal makes the computation of its Hilbert function easier.

The third chapter focuses on the Buchberger-Moeller algorithm for ideals of points in $\mathbb{P}^n$. This algorithm computes the reduced Groebner basis for the defining ideal of a set of points in $\mathbb{P}^n$. Before the algorithm is introduced, the relevant definitions of the projective space $\mathbb{P}^n$ and points in $\mathbb{P}^n$ are given. After that, the defining ideal of a set of points in $\mathbb{P}^n$ and the Hilbert function for a set of points in $\mathbb{P}^n$ are defined. We then prove that the Hilbert function of the defining ideal of a set of points in $\mathbb{P}^n$ eventually becomes constant.

This fact plays a key role in the Buchberger-Moeller algorithm because it provides a stopping criterion. The chapter ends with the presentation of the Buchberger-Moeller algorithm for $\mathbb{P}^n$. We give a proof for the algorithm, a rough explanation of how it works, and an example.

Once we have what we need about n-dimensional projective space, we look at the biprojective space $\mathbb{P}^1 \times \mathbb{P}^1$. Much of this chapter heavily relies on information presented by E. Guardo and A. Van Tuyl in [4]. We will build the required background that will allow us to modify the Buchberger-Moeller algorithm for $\mathbb{P}^n$ so that it can be used to generate the Groebner basis for the defining ideal of a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$. We start by defining the space $\mathbb{P}^1 \times \mathbb{P}^1$, points in $\mathbb{P}^1 \times \mathbb{P}^1$, and the natural projection maps. We follow these definitions with examples. After that, we look at the algebra of the biprojective space $\mathbb{P}^1 \times \mathbb{P}^1$. We introduce the defining ideal and Hilbert function of a bihomogeneous ideal of a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$. We end the chapter with a result on the Groebner basis of Arithmetically Cohen-Macaulay sets of points in $\mathbb{P}^1 \times \mathbb{P}^1$. We use theorems presented in this report, as well as results obtained by E. Guardo and A. Van Tuyl in [4], to give the Groebner basis of the defining ideal of an Arithmetically Cohen-Macaulay set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ (see Theorem 4.24). However, this result is only valid for this particular class of sets of points.

The last chapter contains our new modified version of the Buchberger-Moeller algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$. Using the ideas in the Buchberger-Moeller algorithm for $\mathbb{P}^n$, we develop what we call the Buchberger-Moeller algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$. With this modified algorithm, we are able to compute the Groebner basis for the defining ideal of any finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ with respect to any given monomial order. We give a proof of the algorithm which is followed by an example. We then finish by giving some ideas for future directions.

It is assumed that the reader has some background in algebra. We will assume that the reader understands the definitions and concepts related to linear algebra and ring theory. The reader should be familiar with matrix reductions, rings, ideals (including quotient ideals), fields, polynomial rings, k-vector spaces, and k-bases (where k is an arbitrary field). We also assume a moderate understanding of set theory, including cartesian products, direct sums, and sets of equivalence classes that arise from a particular equivalence relation.

The main reference for Chapter 2 is [5], by B. Hassett. We use his notation for many of the ideas introduced in Chapter 2. M. Kreuzer and L. Robbiano's [6] is the primary reference for Chapter 3. The definitions in this chapter are based on this reference, and we present the Buchberger-Moeller algorithm for $\mathbb{P}^n$ the same way it was presented by M. Kreuzer and L. Robbiano in [6]. In the fourth chapter, the main reference used is [4], by E. Guardo and A. Van Tuyl. We use their notation throughout Chapters 4 and 5, and refer to their work for particular results that are not proved in this report.

CHAPTER 2

Background Algebra

This chapter presents some of the algebraic definitions that we will need, as well as the definition of a Groebner basis, the division algorithm, and Buchberger's criterion. We also look at the Hilbert function and present some theorems that will be useful in later chapters. Throughout this chapter we will let k be any field, and we will refer to the ring $k[x_1, x_2, \ldots, x_n]$ as S.

1. Monomials and Monomial Orders

We begin with the definitions related to monomials. It is assumed that the reader is familiar with what monomials and polynomials are. The following definition introduces the notation that will be used for monomials.

DEFINITION 2.1. A *monomial* will be represented as $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ where the monomial x^α is described by the vector $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$.

Sometimes instead of referring to just the monomials of a polynomial, we may also be concerned with their coefficients. When we want to consider the monomials of a polynomial and their respective coefficients, we refer to them as terms.

DEFINITION 2.2. A *term* of a polynomial is a monomial of that polynomial with its respective coefficient. If x^α is a monomial appearing in a polynomial f and $c \in k$ is its coefficient, then cx^α is a term of f.

EXAMPLE 2.3. As an example, we will consider $f = 2x - 3y$. The monomials appearing in this polynomial are x and y, but the terms of f are $2x$ and $-3y$.

An important invariant of a monomial is its degree.

DEFINITION 2.4. The *degree* of a monomial x^α, represented by $\deg(x^\alpha)$, can be found by adding all the entries of the vector $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. That is,

$$\deg(x^\alpha) = \sum_{i=1}^{n} \alpha_i.$$

1.1. Monomial Orders. Being able to order the monomials of a polynomial ring is very useful and has some important consequences that will be used throughout this report. To begin, we define what it means for an ordering on a set to be a total order.

Definition 2.5. A *total order* $>$ on a set A is an order relation on the elements of A such that for any two elements $a_1, a_2 \in A$, exactly one of the following is true:

$$\begin{aligned} a_1 &> a_2, \\ a_1 &= a_2, \text{ or} \\ a_1 &< a_2. \end{aligned}$$

Example 2.6. The usual ordering $>$ on the real numbers is a total order. For real numbers x and y, we have $x > y$ if $x - y$ is positive.

Having a total order on the set of monomials is nice to have, but it is not quite sufficient for our purposes. We need an ordering on the set of monomials that is consistent with certain conditions.

Definition 2.7. A *monomial order* $>$ is a total order on the monomials in S such that the following two conditions are true:

(1) If $x^\alpha > x^\beta$, then $x^\alpha x^\gamma > x^\beta x^\gamma$ for any $\alpha, \beta, \gamma \in \mathbb{N}^n$.
(2) $>$ is a well-ordering on the monomials of S. That is, any set of monomials has a minimal element.

We will now present some common examples of monomial orders.

Example 2.8. First, we present the lexicographic order. We say $x^\alpha >_{lex} x^\beta$ if the first nonzero entry of $\alpha - \beta = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$ is positive. For example, we have

$$x_1 >_{lex} x_2 >_{lex} x_3^7 >_{lex} x_3 x_4^{20}.$$

We can think of this monomial order as the same as ordering words alphabetically. Note that we are primarily concerned with how the monomial starts and not its degree.

Example 2.9. Another example of a monomial order is the graded lexicographic order. We say $x^\alpha >_{grlex} x^\beta$ if $\deg(x^\alpha) > \deg(x^\beta)$, or $\deg(x^\alpha) = \deg(x^\beta)$ and $x^\alpha >_{lex} x^\beta$. For example, we have

$$x_4^6 >_{grlex} x_1^5 >_{grlex} x_2^4 x_3 >_{grlex} x_4^5.$$

Example 2.10. Our last example of a monomial order is the graded reverse lexicographic order. We say $x^\alpha >_{grelex} x^\beta$ if $\deg(x^\alpha) > \deg(x^\beta)$, or $\deg(x^\alpha) = \deg(x^\beta)$ and the last nonzero entry of $\alpha - \beta = (\alpha_1 - \beta_1, \cdots, \alpha_n - \beta_n)$ is negative. For example,

$$x_3 x_4^2 >_{grevlex} x_2 x_3 >_{grevlex} x_1 x_4.$$

Once we fix a monomial order, we can define the leading monomial of a polynomial.

Definition 2.11. Given a monomial order $>$, the *leading monomial* of a polynomial f, denoted $LM(f)$, is the largest monomial appearing in f with respect to $>$. The *leading term* of f is $cLM(f)$ where c is the coefficient of the leading monomial of f, and is denoted $LT(f)$.

Example 2.12. Let $f = 2x - 3y \in k[x, y]$ and let $>$ be the lexicographic ordering. Then we have $LM(f) = x$ and $LT(f) = 2x$.

1.2. Monomial Ideals. Monomial ideals are a common type of ideal that have some useful properties.

Definition 2.13. A *monomial ideal* $I \subset S$ is an ideal generated by monomials in S. That is, if I is a monomial ideal of S, then there is some subset $A \subset S$ of monomials such that

$$I = \langle m \mid m \in A \rangle.$$

The ideal of leading terms of any ideal $I \subset S$ is an example of a monomial ideal.

Definition 2.14. For any monomial order and ideal $I \subset S$, the *ideal of leading terms* is defined

$$LT(I) = \langle LT(g) | g \in I \rangle.$$

2. Division Algorithm, Groebner Bases, and Buchberger's Criterion

To start this section we will introduce the division algorithm. The division algorithm is a process that is used to reduce polynomials over an ideal.

2.1. Division Algorithm. The division algorithm is a procedure that can sometimes determine if a given polynomial $g \in S$ is in a given ideal $\langle f_1, \dots, f_r \rangle$, $f_i \in S$.

Fix any monomial order, and let $f_1, \dots, f_r \in S$ be nonzero polynomials and let g be a polynomial in S. The division algorithm over $f_1, \dots, f_r \in S$ is given by the following steps:

First, we set $g_0 = g$. If $LM(f_j)$ does not divide $LM(g_0)$ for any j, then we stop. Otherwise pick some f_{j_0} such that $LM(f_{j_0}) | LM(g_0)$ and we will cancel the leading terms by setting

$$g_1 = g_0 - (LT(g_0)/LT(f_{j_0}))f_{j_0}.$$

Now given g_i, if $LM(f_j)$ does not divide $LM(g_i)$ for any j, then we stop. Otherwise pick some f_{j_i} such that $LM(f_{j_i}) | LM(g_i)$ and we will cancel the leading terms by setting

$$g_{i+1} = g_i - (LT(g_i)/LT(f_{j_i}))f_{j_i}.$$

This gives a decreasing sequence of monomials

$$LM(g_0) > LM(g_1) > LM(g_2) > \cdots$$

which must be finite because there are only finitely many monomials less than $LM(g_0)$ (by the well-ordering property that any monomial order must possess). If the process ends with $g_N = 0$ for some N, then we say we get a remainder of 0 and we can write

$$g = \sum_{i=0}^{N-1} (LT(g_i)/LT(f_{j_i}))f_{j_i}.$$

Since each $f_{j_i} \in I$, it follows that $g \in I$.

However, if the process ends with $g_N \neq 0$, then the division algorithm does not tell us whether or not g is in I. It is possible that $g \in I$ even if $LM(f_j)$ does not divide $LM(g)$

for any j. To fix this problem, we need our generating elements of I to form a Groebner basis for I. We will define a Groebner basis in the next subsection, which will come after this useful lemma involving the division algorithm.

LEMMA 2.15. *Given $f_1, \ldots, f_r \in S$, if we apply the division algorithm to a polynomial g that is divisible by f_j for some j, i.e. $g = f_j g'$, then we will eventually get a remainder of* 0.

PROOF. Let $g = g' f_j$ for some j and we will show that applying the division algorithm to g over $f_1, \ldots, f_r \in S$ gives a remainder of 0. First write $g' = \sum_{i=1}^{s} c_i x^{\alpha_i}$ with $x^{\alpha_1} > x^{\alpha_2} > \cdots > x^{\alpha_s}$ and $c_i \in k$ for all $i = 1, \ldots, s$. We have $LT(g) = LT(g')LT(f_j)$ which is divisible by $LT(f_j)$. Now we compute

$$\begin{aligned} g_1 &= g - \frac{LT(g)}{LT(f_j)} f_j \\ &= g' f_j - LT(g') f_j \\ &= f_j(\sum_{i=2}^{s} c_i x^{\alpha_i}). \end{aligned}$$

Now assume $k \leq s$ and let $g_{k-1} = f_j(\sum_{i=k}^{s} c_i x^{\alpha_i})$ so that we can use induction. We have

$$LT(g_{k-1}) = LT(f_j)LT(\sum_{i=k}^{s} c_i x^{\alpha_i}) = c_k x^{\alpha_k} LT(f_j).$$

To get g_k we compute

$$\begin{aligned} g_k &= g_{k-1} - \frac{LT(g_{k-1})}{LT(f_j)} f_j \\ &= [f_j(\sum_{i=k}^{s} c_i x^{\alpha_i})] - \frac{c_k x^{\alpha_k} LT(f_j)}{LT(f_j)} f_j \\ &= f_j(\sum_{i=k}^{s} c_i x^{\alpha_i} - c_k x^{\alpha_k}) \\ &= f_j(\sum_{i=k+1}^{s} c_i x^{\alpha_i}). \end{aligned}$$

Now we know $g_k = f_i(\sum_{i=k+1}^{s} c_i x^{\alpha_i})$ for all $k \leq s$. This gives

$$\begin{aligned} g_s &= f_i(\sum_{i=s+1}^{s} c_i x^{\alpha_i}) \\ &= 0 \end{aligned}$$

which shows that we get a remainder of 0 after applying the division algorithm to $g = g' f_i$ over $f_1, \ldots, f_r$. $\square$

2.2. Groebner Bases. Given a particular monomial order, any ideal in a polynomial ring has a Groebner basis with respect to that order. As stated in the previous subsection, if we have a Groebner bases for a given ideal then it allows us to determine if a certain polynomial is in the given ideal by applying the division algorithm. However, one question that arises is, "how do we tell if a given set of polynomials is a Groebner basis for an ideal?". This question will be answered in this section. We will go on to present some other defintions and theorems that will be helpful later in this project. For now, we begin this subsection with the definition of a Groebner basis.

DEFINITION 2.16. For any monomial order and ideal $I \subset S$, we define a *Groebner basis* for I to be a set of nonzero polynomials

$$\{f_1, \ldots, f_r\} \subset I$$

such that $LT(I)$ is generated by $LT(f_1), \ldots, LT(f_r)$. We say that a Groebner basis is *reduced* if for each $i = 1, \ldots, r$, $LT(f_i)$ has a coefficient of one and does not divide any term in the other polynomials of $\{f_1, \ldots, f_r\}$. Furthermore, if we have a Groebner basis that is the reduced Groebner basis for every monomial order, then it is called the *Universal Groebner basis.*

Although the order being considered will normally affect what polynomials are in a Groebner basis, the purposes are consistent. One very important fact about any Groebner basis of an ideal I is that the Groebner basis actually generates I.

THEOREM 2.17. *If $\{f_1, \ldots, f_r\}$ form a Groebner basis for an ideal I, then $I = \langle f_1, \ldots, f_r \rangle$.*

We will not go over the proof for this theorem, but one can be found in [5]. We now have the following theorem.

THEOREM 2.18. *For any monomial order and ideal $I \subset S$, if $\{f_1, \ldots, f_r\}$ is a Groebner basis for I, then we can apply the division algorithm with $f_1, \ldots, f_r$ to determine whether or not g is in I. If the division algorithm ends with $g_N = 0$ for some N, then we have $g \in I$. If the division algorithm ends with $g_N \neq 0$ for some N, then $g \notin I$.*

PROOF. We already know that if $g_N = 0$ for some N, then $g \in I$. If the algorithm ends with $g_N \neq 0$ with $LM(g_N)$ not divisible by $LM(f_j)$ for any j, then we write

$$g = g_N + \sum_{i=0}^{N-1} (LT(g_i)/LT(f_{j_i}))f_{j_i}.$$

We have that

$$\sum_{i=0}^{N-1} (LT(g_i)/LT(f_{j_i}))f_{j_i} \in I$$

since each $f_{j_i} \in I$. We also have that $LM(g_N)$ is not divisible by $LM(f_j)$ for any j, which implies that $g_N \notin I$ since $\{f_1, \ldots, f_r\}$ is a Grobner basis for I. From this we conclude that $g \notin I$ because g and g_N differ by an element of I, but $g_N \notin I$. $\square$

EXAMPLE 2.19. Using the graded reverse lexicographic order, let $I = \langle x+y, xy+z\rangle \subset k[x,y,z]$. We will use the division algorithm on the polynomial $x^2 - z$. The leading monomial of $x^2 - z$ is x^2 which is divisible by $LM(x+y) = x$. Now we compute

$$(x^2 - z) - \frac{x^2}{x}(x+y) = -xy - z.$$

Now $LM(-xy - z) = xy$ which is divisible by $LM(xy+z) = xy$ so the next step is to compute

$$(-xy - z) - \frac{-xy}{xy}(xy+z) = 0.$$

We can conclude $x^2 - z \in I$ because by working backwards we can get

$$x^2 - z = x(x+y) - (xy+z).$$

Now consider the polynomial $y^2 - z = y(x+y) - (xy+z) \in I = \langle x+y, xy+z\rangle$. If we use the division algorithm on $y^2 - z$, we stop immediately because $LM(y^2 - z) = y^2$ is not divisible by $LM(x+y) = x$ or $LM(xy+z) = xy$. In this case, the division algorithm fails to determine whether or not $y^2 - z$ is in I, even though $y^2 - z$ is not in I.

However, if we have a Grobner basis for I, then the division algorithm will not fail to determine if a given polynomial is in I. For example, $x+y$ and $y^2 - z$ form a Grobner basis for $I = \langle x+y, xy+z\rangle$ (we will verify the fact that $x+y$ and $y^2 - z$ do in fact form a Grobner basis after presenting Buchberger's criterion). For now, we will show that we have the equality $I = \langle x+y, y^2 - z\rangle$ by using the division algorithm over $x+y$ and $y^2 - z$. We know that $y^2 - z = y(x+y) - (xy+z) \in I$ and of course $x+y \in I$, so we know that

$$\langle x+y, y^2 - z\rangle \subset I.$$

We will prove that $x+y$ and $y^2 - z$ generate I by using the division algorithm to prove that $x+y$ and $xy+z$ are both in $\langle x+y, y^2 - z\rangle$. Since we claim that $x+y$ and $y^2 - z$ form a Groebner basis for I, we must get a remainder of 0 when applying the division algorithm to any polynomial in I over $x+y$ and $y^2 - z$.

Applying the division algorithm to $x+y$ is trivial since it is a generator of $\langle x+y, y^2 - z\rangle$. Now we apply the division algorithm to $xy+z$. The monomial $LM(xy+z) = xy$ is divisible by $LM(x+y) = x$ so we compute

$$(xy+z) - \frac{xy}{x}(x+y) = -y^2 + z.$$

Now we look at $LM(-y^2 + z) = y^2$, and we can see it is divisible by $LM(y^2 - z) = y^2$. Now we compute

$$(-y^2 + z) - \frac{-y^2}{y^2}(y^2 - z) = 0.$$

We thus have that $xy+z = y(x+y) - (y^2 - z)$ which proves that $xy+z \in \langle x+y, y^2 - z\rangle$. This shows the containment

$$I = \langle x+y, xy+z\rangle \subset \langle x+y, y^2 - z\rangle$$

which allows us to conclude that $I = \langle x + y, y^2 - z \rangle$.

The following theorem will be useful to us in Chapter 4. We present it now because the proof involves understanding the concept of a Groebner basis, as well as some relatively basic algebra.

THEOREM 2.20. *Let* $\{f_1, \ldots, f_r\}$ *be a Groebner basis for an ideal* I. *If* h *is any form, then* $\{hf_1, \ldots, hf_r\}$ *is a Groebner basis for* $hI = \langle hf \mid f \in I \rangle$.

PROOF. First we will show that $hI = \langle hf_1, \ldots, hf_r \rangle$. Let $g \in \langle hf_1, \ldots, hf_r \rangle$ and write

$$\begin{aligned} g &= a_1hf_1 + \cdots + a_rhf_r \\ &= h(a_1f_1 + \cdots + a_rf_r). \end{aligned}$$

Since $a_1f_1 + \cdots + a_rf_r \in I$, we conclude that $g \in hI$. This shows $hI \supset \langle hf_1, \ldots, hf_r \rangle$. Now to show $hI \subset \langle hf_1, \ldots, hf_r \rangle$, let $g \in hI$, and we will show $g \in \langle hf_1, \ldots, hf_r \rangle$. Since $g \in hI$, we can write $g = hg'$ with $g' \in I$. Now we write $g' = a_1f_1 + \cdots + a_rf_r$ to get

$$\begin{aligned} g &= h(a_1f_1 + \cdots + a_rf_r) \\ &= a_1hf_1 + \cdots + a_rhf_r \in \langle hf_1, \ldots, hf_r \rangle \end{aligned}$$

which now gives us $hI = \langle hf_1, \ldots, hf_r \rangle$. Now to show that $\{hf_1, \ldots, hf_r\}$ is a Groebner basis for hI, let $g \in hI$ and write $g = hg'$ with $g' \in I$. Now using the fact that $\{f_1, \ldots, f_r\}$ is a Grobner Basis for I, we write $g' = a_1f_1 + \cdots + a_rf_r$ with $LT(f_i)|LT(g')$ for some i. Let $c = LT(g')/LT(f_i)$ so that $LT(g') = cLT(f_i)$. Now we look at $LT(g)$:

$$\begin{aligned} LT(g) &= LT(h)LT(g') \\ &= LT(h)[cLT(f_i)] \\ &= cLT(h)LT(f_i) \\ &= cLT(hf_i). \end{aligned}$$

So $LT(hf_i)|LT(g)$ and this shows us that $LT(hI) = \langle LT(hf_1), \ldots LT(hf_r) \rangle$ since $LT(hI)$ is a monomial ideal. This completes the proof that $\{hf_1, \ldots, hf_r\}$ is a Groebner basis for hI. □

2.3. Buchberger's Criterion. If we are given a set of generators for any ideal I, we may want to know if those generators form a Groebner basis for I. To determine whether or not the given generators form a Groebner basis for I, we can use Buchberger's criterion. Before learning Buchberger's criterion, we must define S-polynomials. In order to define S-polynomials, we will need the definition of the least common multiple of monomials.

DEFINITION 2.21. The *least common multiple* of monomials x^α and x^β is the smallest monomial in S that is divisible by both x^α and x^β. We can also write it as

$$LCM(x^\alpha, x^\beta) = x_1^{max(\alpha_1, \beta_1)} \cdots x_n^{max(\alpha_n, \beta_n)}.$$

Now that we have defined the least common multiple of two monomials, we can move on to S-polynomials.

Definition 2.22. If f_1 and f_2 are polynomials in S, let

$$x^\alpha = LCM(LM(f_1), LM(f_2)).$$

The *S-polynomial* formed from f_1 and f_2 is defined as

$$S(f_1, f_2) = (x^\alpha/LT(f_1))f_1 - (x^\alpha/LT(f_2))f_2.$$

An important consequence of the S-polynomial is that cancellation occurs. The leading terms of $(x^\alpha/LT(f_1))f_1$ and $(x^\alpha/LT(f_2))f_2$ are made to be the same so that they cancel. This allows us to write the S-polynomial as

$$S(f_1, f_2) = (x^\alpha/LT(f_1))(f_1 - LT(f_1)) - (x^\alpha/LT(f_2))(f_2 - LT(f_2))$$

since we are just deleting the terms that will cancel each other out.

Remark 2.23. The naming convention of the S-polynomial has nothing to do with the fact that we are referring to the polynomial ring as S.

Example 2.24. Under the graded reverse lexicographic order, we will compute the S-polynomial for $f_1 = x_1^2 + 2x_2^2$ and $f_2 = 5x_1x_3 - x_4$. We have

$$\begin{aligned} S(f_1, f_2) &= \frac{x_1^2x_3}{x_1^2}(x_1^2 + 2x_2^2) - \frac{x_1^2x_3}{5x_1x_3}(5x_1x_3 - x_4) \\ &= 2x_2^2x_3 + \frac{1}{5}x_1x_4. \end{aligned}$$

Now that we have the required definitions, we can introduce Buchberger's criterion. Buchberger's criterion will allow us to determine if a given set of generators of an ideal forms a Groebner basis.

Theorem 2.25. *(Buchberger's Criterion) For any monomial order and ideal $I = \langle f_1, \ldots, f_r\rangle \subset S$, $\{f_1, \ldots, f_r\}$ is a Groebner basis for I if and only if every S-polynomial $S(f_i, f_j)$ with $1 \le i < j \le r$ gives a remainder of zero after applying the division algorithm over $f_1, \ldots, f_r$.*

Instead of giving a proof for Buchberger's Criterion, we will show how it works with an example. A complete proof for Buchberger's criterion can be found in [5].

Example 2.26. In Example 2.19, we looked at $I = \langle x + y, xy + z\rangle$. We claimed that $x + y$ and $y^2 - z$ formed a Groebner basis for I under the graded reverse lexicographic order. We will use Buchberger's criterion to justify this claim by showing that the S-polynomial formed from $x + y$ and $y^2 - z$ will give a remainder of 0 after applying the division algorithm over $x+y$ and $y^2 - z$. We first compute the S-polynomial formed from $x + y$ and $y^2 - z$:

$$S(x + y, y^2 - z) = \frac{xy^2}{x}(x + y) - \frac{xy^2}{y^2}(y^2 - z) = y^3 + xz.$$

Now we apply the division algorithm to $y^3 + xz$ over $x + y$ and $y^2 - z$. We have that $LT(y^3 + xz) = y^3$ is divisible by $LT(y^2 - z) = y^2$ so we compute

$$y^3 + xz - \frac{y^3}{y^2}(y^2 - z) = xz + yz.$$

If we note that $xz + yz = z(x + y)$, we can use Lemma 2.15 to conclude that we will get a remainder of 0. Now we know that Buchberger's criterion is satisfied so we know that $x + y$ and $y^2 - z$ form a Groebner basis for $I = \langle x + y, xy + z \rangle$.

Now we can also show that $x + y$ and $xy + z$ do not form a Groebner basis for I by showing that Buchberger's criterion is not met in this case. First we compute the S-polynomial formed from $x + y$ and $xy + z$:

$$S(x + y, xy + z) = \frac{xy}{x}(x + y) - \frac{xy}{xy}(xy + z) = y^2 - z.$$

Now we apply the division algorithm to $y^2 - z$ over $x + y$ and $xy + z$. We have that $LT(y^2 - z) = y^2$ is not divisible by $LT(x + y) = x$ or by $LT(xy + z) = xy$, so we must stop and we do not get a remainder of 0. This means that Buchberger's criterion is not met, and so $x + y$ and $xy + z$ do not form a Groebner basis for I.

3. Homogeneous Polynomials

Throughout this report, we will be working with homogeneous polynomials. We begin this section with their definition, and then present a theorem that will be used in Chapter 4.

Definition 2.27. A *homogeneous polynomial* is a polynomial $f \in S$ whose terms are all the same degree.

Example 2.28. An example of a homogeneous polynomial of degree two is $f = x_1^2 + 2x_1x_2 + x_2^2$. Another example is $g = x_1^4 + x_1x_2^3 + x_2^2x_3^2 + x_3^4$ which is a degree four homogeneous polynomial. However, $h = x_1^3 + x_2^2 + x_3^2$ is not homogeneous because one of its terms is degree three, and the other two terms are degree two.

Theorem 2.29. *Let $R = k[x_1, \dots, x_n, y_1, \dots, y_m]$ and let $f \in k[x_1, \dots, x_n] \subset R$ and $g \in k[y_1, \dots, y_m] \subset R$ be homogeneous polynomials viewed as polynomials of R. Under any ordering that has $x_i > y_j$ for any $i, j = 0, 1$, the S-polynomial formed from f and g gives a remainder of 0 after applying the division algorithm over any set of polynomials containing f and g.*

Proof. Let $g = \sum_{i=1}^{r} c_i y^{\alpha_i}$ be such that $y^{\alpha_1} > y^{\alpha_2} > \cdots > y^{\alpha_r}$. By the construction of the S-polynomials and division algorithm, we are cancelling the monomials in a way that preserves the proportionalities of the coefficients. Since k is a field, we essentially have the same process regardless of the leading coefficients of f and g. This means we can assume the leading coefficients of f and g are both 1 so that $LT(f) = LM(f)$ and $LT(g) = LM(g)$. Let h_1 be the S-polynomial formed from f and g and note that

$$LCM(LM(f), LM(g)) = LM(f)LM(g) = LT(f)LT(g).$$

We have

$$\begin{aligned}
h_1 &= S(f,g) \\
&= \frac{LT(f)LT(g)}{LT(f)}f - \frac{LT(f)LT(g)}{LT(g)}g \\
&= LT(g)\cdot f - LT(f)\cdot g \\
&= LT(g)\cdot(f - LT(f)) - LT(f)\cdot(g - LT(g)) \\
&= y^{\alpha_1}\cdot(f - LT(f)) - LT(f)\cdot(\sum_{i=2}^{r} c_i y^{\alpha_i}).
\end{aligned}$$

Now we apply the division algorithm to $h_1 = S(f,g)$. Since we are working under any ordering that has $x_i > y_j$ for any $i, j = 0, 1$, the leading term of h_1 will have the largest degree of the x_i variables out of any monomial appearing in h_1. This means we can ignore the y_i variables when looking for the leading term. Any monomial in h_1 is the product of a monomial from f and a monomial from g. Since we are ignoring the y variables, the largest monomials in h_1 are the monomials that are divisible by $LT(f)$. These monomials are $-c_2y^{\alpha_2}LT(f), \ldots, -c_ry^{\alpha_r}LT(f)$. From these monomials, we conclude that $LT(h_1) = -c_2y^{\alpha_2}LT(f)$. So we subtract $-c_2y^{\alpha_2}f$ from h_1 as per the division algorithm, and we call the result h_2:

$$\begin{aligned}
h_2 &= h_1 + c_2y^{\alpha_2}f \\
&= (h_1 - LT(h_1)) + c_2y^{\alpha_2}(f - LT(f)) \\
&= [y^{\alpha_1}\cdot(f - LT(f)) - LT(f)\cdot(\sum_{i=2}^{r} c_i y^{\alpha_i})] + c_2y^{\alpha_2}LT(f) + c_2y^{\alpha_2}(f - LT(f)) \\
&= (\sum_{i=1}^{2} c_i y^{\alpha_i})(f - LT(f)) - LT(f)(\sum_{i=3}^{r} c_i y^{\alpha_i}).
\end{aligned}$$

Now inductively, for $s \leq r$, let

$$h_{s-1} = (\sum_{i=1}^{s-1} c_i y^{\alpha_i})(f - LT(f)) - LT(f)(\sum_{i=s}^{r} c_i y^{\alpha_i}).$$

Using the same idea we used to find $LT(h_1)$, we get

$$LT(h_{s-1}) = -LT(f)\cdot LT(\sum_{i=s}^{r} c_i y^{\alpha_i}) = -c_s y^{\alpha_s} LT(f).$$

Now after continuing with the division algorithm on h_s, we get

$$\begin{aligned}
h_s &= h_{s-1} + c_s y^{\alpha_s} f \\
&= (h_{s-1} - LT(h_{s-1})) + c_s y^{\alpha_s}(f - LT(f)) \\
&= (\sum_{i=1}^{s-1} c_i y^{\alpha_i}) \cdot (f - LT(f)) - LT(f) \cdot (\sum_{i=s}^{r} c_i y^{\alpha_i}) + c_s y^{\alpha_s} LT(f) + c_s y^{\alpha_s}(f - LT(f)) \\
&= (\sum_{i=1}^{s} c_i y^{\alpha_i}) \cdot (f - LT(f)) - LT(f) \cdot (\sum_{i=s+1}^{r} c_i y^{\alpha_i}).
\end{aligned}$$

Now set $s = r$, and we get

$$\begin{aligned}
h_r &= (\sum_{i=1}^{r} c_i y^{\alpha_i}) \cdot (f - LT(f)) - LT(f) \cdot (\sum_{i=r+1}^{r} c_i y^{\alpha_i}) \\
&= g(f - LT(f)).
\end{aligned}$$

By Lemma 2.15 we know that applying the division algorithm to $h_r = g(f - LT(f))$ will eventually give a remainder of 0 since h_r is a multiple of g. This proves that the S-polynomial formed from f and g gives 0 remainder after applying the division algorithm over f and g. □

Using the ideas in the previous proof, we can extend the above theorem to any monomial order.

THEOREM 2.30. *Let $R = k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and let $f \in k[x_1, \ldots, x_n] \subset R$ and $g \in k[y_1, \ldots, y_m] \subset R$ be homogeneous polynomials viewed as polynomials in R. Under any monomial ordering, the S-polynomial formed from f and g gives a remainder of 0 after applying the division algorithm over any set of polynomials containing f and g.*

PROOF. Let $f = \sum_{i=1}^{r} a_i x^{\alpha_i}$ and $g = \sum_{i=j}^{k} b_j y^{\beta_j}$ be such that $x^{\alpha_1} > x^{\alpha_2} > \cdots > x^{\alpha_r}$ and $y^{\beta_1} > y^{\beta_2} > \cdots > y^{\beta_k}$. As in the proof of the previous theorem, assume that the leading coefficients of f and g are both 1 so that $LT(f) = LM(f)$ and $LT(g) = LM(g)$. Let h_1 be the S-polynomial formed from f and g and note that

$$LCM(LM(f), LM(g)) = LM(f)LM(g) = LT(f)LT(g).$$

We have

$$\begin{aligned} h_1 &= S(f,g) \\ &= \frac{LT(f)LT(g)}{LT(f)}f - \frac{LT(f)LT(g)}{LT(g)}g \\ &= LT(g)\cdot f - LT(f)\cdot g \\ &= LT(g)\cdot(f - LT(f)) - LT(f)\cdot(g - LT(g)) \\ &= y^{\beta_1}\cdot(\sum_{i=2}^{r} a_i x^{\alpha_i}) - x^{\alpha_1}\cdot(\sum_{j=2}^{k} b_j y^{\beta_j}). \end{aligned}$$

We will prove by induction that we get a remainder of 0 when we apply the division algorithm to $h_1 = S(f,g)$ over f and g. We claim that after every operation of the division algorithm, there will be non-negative integers $1 \le r' \le r$ and $1 \le k' \le k$ such that

$$h_s = (\sum_{j=1}^{k'} b_j y^{\beta_j})\cdot(\sum_{i=r'+1}^{r} a_i x^{\alpha_i}) - (\sum_{i=1}^{r'} a_i x^{\alpha_i})\cdot(\sum_{j=k'+1}^{k} b_j y^{\beta_j}) \text{ with } s = r' + k' - 1.$$

We have that this is true for $s = 1$ with r' and k' both equal to one. The first thing we must note is that there are no terms cancelling between the sums. This is easy to see because the monomial terms of $(\sum_{j=1}^{k'} b_j y^{\beta_j})\cdot(\sum_{i=r'+1}^{r} a_i x^{\alpha_i})$ have form $x^{\alpha_i}y^{\beta_j}$ with $r'+1 \le i \le r$ and $1 \le j \le k'$, whereas the monomial terms of the second sum have the same form, but with $1 \le i \le r'$ and $k'+1 \le j \le k$. Since $\alpha_{i_1} \ne \alpha_{i_2}$ for $i_1 \ne i_2$ and $\beta_{j_1} \ne \beta_{j_2}$ for $j_1 \ne j_2$, we have that after expanding, there is no cancellation of terms between the sums. Now we will use induction by applying the division algorithm to h_{s-1}, written as above, for some $1 \le r' \le r$ and $1 \le k' \le k$ with $s-1 = r'+k'-1$. Since there is no cancellation occurring, the leading term of h_{s-1} will be either

$$LT(\sum_{j=1}^{k'} b_j y^{\beta_j} \sum_{i=r'+1}^{r} a_i x^{\alpha_i}) = a_{r'+1}x^{\alpha_{r'+1}}LT(g)$$

or

$$LT(-\sum_{i=1}^{r'} a_i x^{\alpha_i} \sum_{j=k'+1}^{k} b_j y^{\beta_j}) = -b_{k'+1}y^{\beta_{k'+1}}LT(f).$$

We will show that in both cases we get the desired form for h_s. First, we will consider the case where $LT(h_{s-1}) = a_{r'+1}x^{\alpha_{r'+1}}LT(g)$. If we subtract $a_{r'+1}x^{\alpha_{r'+1}}g$, we get

$$\begin{aligned} h_s &= h_{s-1} - a_{r'+1}x^{\alpha_{r'+1}}g \\ &= \sum_{j=1}^{k'} b_j y^{\beta_j} \sum_{i=r'+1}^{r} a_i x^{\alpha_i} - \sum_{i=1}^{r'} a_i x^{\alpha_i} \sum_{j=k'+1}^{k} b_j y^{\beta_j} - a_{r'+1}x^{\alpha_{r'+1}}(\sum_{j=1}^{k'} b_j y^{\beta_j} + \sum_{j=k'+1}^{k} b_j y^{\beta_j}) \\ &= \sum_{j=1}^{k'} b_j y^{\beta_j}(\sum_{i=r'+1}^{r} a_i x^{\alpha_i} - a_{r'+1}x^{\alpha_{r'+1}}) - (\sum_{i=1}^{r'} a_i x^{\alpha_i} + a_{r'+1}x^{\alpha_{r'+1}}) \sum_{j=k'+1}^{k} b_j y^{\beta_j} \\ &= \sum_{j=1}^{k'} b_j y^{\beta_j} \sum_{i=(r'+1)+1}^{r} a_i x^{\alpha_i} - \sum_{i=1}^{(r'+1)} a_i x^{\alpha_i} \sum_{j=k'+1}^{k} b_j y^{\beta_j}. \end{aligned}$$

Now we can see that h_s is written in the desired form with $s = (r'+1) + k' - 1$. If we instead had that $LT(h_s) = -b_{k'+1}y^{\beta_{k'+1}}LT(f)$, then we would subtract $-b_{k'+1}y^{\beta_{k'+1}}f$ from h_{s-1} to get

$$\begin{aligned} h_s &= h_{s-1} + b_{k'+1}y^{\beta_{k'+1}}f \\ &= \sum_{j=1}^{k'} b_j y^{\beta_j} \sum_{i=r'+1}^{r} a_i x^{\alpha_i} - \sum_{i=1}^{r'} a_i x^{\alpha_i} \sum_{j=k'+1}^{k} b_j y^{\beta_j} + b_{k'+1}y^{\beta_{k'+1}}(\sum_{i=1}^{r'} a_i x^{\alpha_i} + \sum_{i=r'+1}^{r} a_i x^{\alpha_i}) \\ &= (\sum_{j=1}^{k'} b_j y^{\beta_j} + b_{k'+1}y^{\beta_{k'+1}}) \sum_{i=r'+1}^{r} a_i x^{\alpha_i} - \sum_{i=1}^{r'} a_i x^{\alpha_i}(\sum_{j=k'+1}^{k} b_j y^{\beta_j} - b_{k'+1}y^{\beta_{k'+1}}) \\ &= \sum_{j=1}^{(k'+1)} b_j y^{\beta_j} \sum_{i=r'+1}^{r} a_i x^{\alpha_i} - \sum_{i=1}^{r'} a_i x^{\alpha_i} \sum_{j=(k'+1)+1}^{k} b_j y^{\beta_j}. \end{aligned}$$

Now again, we see that h_s is written in the desired form with $s = r' + (k'+1) - 1$. At each step of the division algorithm, we just end up increasing either r' or k' by one until we eventually get either $r' = r$ or $k' = k$ for some $s = r' + k' - 1$. At that point, we have either

$$h_s = \sum_{j=1}^{k'} b_j y^{\alpha_j} \sum_{i=r+1}^{r} a_i x^{\alpha_i} - \sum_{i=1}^{r} a_i x^{\alpha_i} \sum_{j=k'+1}^{k} b_j y^{\beta_j} = -(\sum_{j=k'+1}^{k} b_j y^{\beta_j})f$$

or

$$h_s = \sum_{j=1}^{k} b_j y^{\alpha_j} \sum_{i=r'+1}^{r} a_i x^{\alpha_i} - \sum_{i=1}^{r'} a_i x^{\alpha_i} \sum_{j=k+1}^{k} b_j y^{\beta_j} = (\sum_{i=r'+1}^{r} a_i x^{\alpha_i})g.$$

By Lemma 2.15, we know that in either case applying the division algorithm to $h_s = -(\sum_{j=k'+1}^{k} b_j y^{\beta_j})f$ or $h_s = (\sum_{i=r'+1}^{r} a_i x^{\alpha_i})g$ will eventually give a remainder of 0. This proves that the S-polynomial formed from f and g gives a remainder of 0 after applying the division algorithm over f and g. $\square$

4. Hilbert Functions

The Hilbert function, which will be used in the main result, gives some numerical information about a graded ring. We first present the requisite background.

DEFINITION 2.31. A *graded ring* is a ring that is a direct sum of abelian groups R_i such that $R_iR_j \subset R_{(i+j)}$.

EXAMPLE 2.32. We have that $S = k[x_1, \ldots, x_n]$ is a graded ring where S_i is the additive abelian group generated by all monomials of degree i. This is because any polynomial in S can be written as the direct sum of homogeneous polynomials that are all of different degrees (by grouping all the monomials into their respective degrees). Now each of these homogeneous polynomials are a sum of monomials of a fixed degree, so belong to S_i for some i. From this we conclude that

$$S = \bigoplus_{i \in \mathbb{N}} S_i.$$

It is easy to see that $S_iS_j \subset S_{i+j}$ because the product of any two monomials of degrees i and j will have degree $i + j$. This implies that the product of any two homogeneous polynomials of degrees i and j will have degree $i+j$ so we have the containment property needed to be a graded ring.

DEFINITION 2.33. A *homogeneous ideal* is an ideal that is generated by homogeneous polynomials.

THEOREM 2.34. *Let I be a homogeneous ideal and let $f \in I$. If we write $f = f_0 + \cdots + f_d$ where f_i is the sum of all monomials in f that are of degree i, then $f_i \in I$ for $i = 0, \ldots, d$.*

It is not very hard to see why this is true. If the reader is interested in seeing a proof, one can be found in [3].

LEMMA 2.35. *A homogeneous ideal is a graded ring.*

PROOF. Let I be a homogeneous ideal, and let I_i be the additive abelian group generated by all homogeneous polynomials in I of degree i. By the previous theorem, we have that if f is a polynomial in I, then we can write $f = \sum_i f_i$ where each f_i is homogeneus of degree i and is also in I. Each f_i is in I_i so we can write $I = \bigoplus_{i \in \mathbb{N}} I_i$.

We also have that $I_iI_j \subset I_{i+j}$ because the product of two homogeneous polynomials of degrees i and j must be a homogeneous polynomial of degree $i + j$. □

If I is a homogeneous ideal, then the abelian group I_i can be viewed as a finite dimensional k-vector space. This allows us to define the Hilbert function as follows.

DEFINITION 2.36. If I is a homogeneous ideal of S, then we define the *Hilbert function* of S/I as

$$HF_{S/I} = dim_k(S_i) - dim_k(I_i).$$

As shown in the next theorem, the Hilbert function of a homogeneous ideal can be completely determined by the Hilbert function of its ideal of leading terms. In this way the Hilbert function can be determined from a monomial ideal which is easier to work with in general.

THEOREM 2.37. *For any homogeneous ideal I and monomial order, we have*

$$HF_{S/I}(i) = HF_{S/LT(I)}(i).$$

PROOF. Choose any term order. Since $LT(I)$ is a monomial ideal, we have that all the monomials not in $LT(I)$ form a k-basis of $S/LT(I)$. These monomials also form a k-basis for S/I because they are all in S/I, independent over k, and span S/I. To see that they span S/I, let $f + I \in S/I$ and suppose f is not in the span of the monomials that are not $LT(I)$. That is, suppose there is a term appearing in f that is in $LT(I)$. Pick the largest such term, call it $c_1 x^{\alpha_1}$, and pick $g_1 \in I$ such that $LT(g_1) = c_1 x^{\alpha_1}$. Now reduce f by g_1 to get a polynomial equivalent to f modulo I. That is, since $g_1 \in I$, we have,

$$(f - g_1) + I = f + I.$$

Now the chosen monomial x^{α_1} will not appear in our new polynomial $f_1 = f - g_1$. Also, if there is a term appearing in f_1 that is in $LT(I)$, it will be smaller than x^{α_1} with respect to the chosen ordering. Again, we will choose the largest such term, call it $c_2 x^{\alpha_2}$, and pick $g_2 \in I$ such that $LT(g_2) = c_2 x^{\alpha_2}$. We reduce f_1 by g_2 to get $f_2 = f_1 - g_2 = f - (g_1 + g_2)$, and repeat this process for each $f_i = f - (\sum_{k=1}^{i} g_k)$ until we no longer can. If we eventually stop this process, it means we have reached a number N such that there is no term appearing in f_N that is in $LT(I)$. We know that we will only repeat this process finitely many times before stopping because we get a sequence

$$x^{\alpha_1} > x^{\alpha_2} > \cdots$$

with $x^{\alpha_i} \in LT(I)$ for each i, which must eventually terminate because we know that $LT(I)$ must have a minimal element with respect to any monomial order. This implies that our process must end with $f_N = f - (\sum_{k=1}^{N} g_k)$ for some N, and no terms of f_N are in $LT(I)$. This means that f_N is in the span of the monomials not in $LT(I)$. Since $g_k \in I$ for all k, we also have that

$$f_N + I = f - (\sum_{k=1}^{N} g_k) + I = f + I.$$

This shows that $f + I = f_N + I$ is in the span of the monomials not in $LT(I)$. This means that any $f + I \in S/I$ can be written as a k-linear combination of the monomials not in $LT(I)$, so they form a k-basis for S/I. Now we have that for any $i \geq 0$, all the monomials not in $LT(I)$ of degree i form a k-basis for both $(S/I)_i$ and $(S/LT(I))_i$. This of course means that for all $i \geq 0$, we have

$$dim_k((S/I)_i) = dim_k((S/LT(I))_i).$$

This gives us the desired result

$$HF_{S/I}(i) = HF_{S/LT(I)}(i) \text{ for all } i \geq 0.$$

□

We can connect the previous theorem with the properties of Groebner bases. The ideal of leading terms of any homogeneous ideal is generated by the leading terms of any Groebner basis, so we can use any given Groebner basis to obtain generators for $LT(I)$. This gives us the following lemma, which can be useful for computing the Hilbert function of a homogeneous ideal if we have some Groebner basis for it.

LEMMA 2.38. *If I is a homogeneous ideal and $\{f_1, \ldots, f_r\}$ is a Groebner basis for I for some monomial order, then we have*

$$HF_{S/I}(i) = HF_{S/\langle LT(f_1), \ldots, LT(f_r)\rangle}(i)$$

PROOF. This follows from the previous theorem and the fact that if we have an ideal I and a Groebner basis $\{f_1, \ldots, f_r\}$ for I, then we have $LT(I) = \langle LT(f_1), \ldots, LT(f_r)\rangle$. □

The above lemma implies that to compute the Hilbert function of some homogeneous ideal, we can reduce the problem to computing the Hilbert function of a monomial ideal using a Groebner basis.

CHAPTER 3

Buchberger-Moeller Algorithm for points in $\mathbb{P}^n$

In this chapter we introduce n-dimensional projective space and points in projective space. We then define what it means to be a defining ideal for a set of points in projective space. Following that, we define the Hilbert function of a set of points, which requires the knowledge presented in the previous chapter about Hilbert functions. Finally, we finish the chapter with the projective Buchberger-Moeller algorithm. The projective Buchberger-Moeller algorithm is an algorithm that generates the reduced Groebner basis for the defining ideal of a given set of points in projective space that does not require Buchberger's criterion.

1. Points in Projective Space $\mathbb{P}^n$

We first establish the definitions of projective space and points in projective space.

Definition 3.1. We define the *n-dimensional projective space*, denoted by $\mathbb{P}^n$, to be the set of equivalence classes of $k^{n+1} \setminus \{0\}$ with respect to the relation $\sim$, where we have

$$(c_0, \dots, c_n) \sim (c'_0, \dots, c'_n)$$

if $(c_0, \dots, c_n) = (\lambda c'_0, \dots, \lambda c'_n)$ for some nonzero $\lambda \in k$.

If $(c_0, \dots, c_n)$ is in $k^{n+1} \setminus \{0\}$, then the equivalence class of $(c_0, \dots, c_n)$ is called a *point* in $\mathbb{P}^n$, denoted by $[c_0 : \cdots : c_n]$.

If we have a set of points of $\mathbb{P}^n$, say $X = \{p_1, \dots, p_s\}$, then we are interested in the ideal of homogeneous polynomials which vanish over every point of X.

Definition 3.2. Let $X = \{p_1, \dots, p_r\}$ be a set of points in $\mathbb{P}^n$. The *homogeneous vanishing ideal* of X (often called the *defining ideal* of X), denoted $I(X)$, is defined as

$$I(X) = \langle f \in k[x_0, \dots, x_n] \mid f \text{ is homogeneous and } f(p_i) = 0 \text{ for all } p_i \in X \rangle.$$

It is clear that if X is any set of points in $\mathbb{P}^n$, then $I(X)$ is a homogeneous ideal. Note that if f is homogeneous and $p = [c_0 : \cdots : c_n]$ is a point in projective space with $f(c_0, \dots, c_n) = 0$, we have that

$$f(p) = f(\lambda c_0, \dots, \lambda c_n) = \lambda^{deg(f)} f(c_0, \dots, c_n) = 0$$

for any $\lambda \in k$. This shows that a point in projective space is a zero of a function if any one of its coordinate representations is a zero of that function.

DEFINITION 3.3. If X is a set of points in $\mathbb{P}^n$, then the *Hilbert function* of X is defined as

$$HF_X(i) = HF_{k[x_0,\ldots,x_n]/I(X)}(i) \text{ for all } i \geq 0.$$

The Hilbert function of any finite set of points in projective space has the property that it eventually becomes constant. This is a useful fact because it plays a key role in the stopping condition of the Buchberger-Moeller Algorithm.

THEOREM 3.4. *Let X be a finite set of points in $\mathbb{P}^n$ with $|X| = s$. Then there exists some positive integer N such that*

$$HF_X(i) = s \textit{ for all } i \geq N.$$

PROOF. We prove the theorem by induction on the size of X. Let $R = k[x_0, \ldots, x_n]$, $X = \{p = [c_0 : \cdots : c_n]\} \subset \mathbb{P}^n$, and $I = I(X)$. Suppose $HF_X(i) > 1$ for some $i \geq 1$ (we are also proving that $N = 1$ if $|X| = 1$). We have

$$HF_X(i) = HF_{R/I}(i) = HF_{R/LT(I)}(i) \text{ for all } i \geq 0$$

which implies that we have

$$HF_{R/LT(I)}(i) > 1 \text{ for some } i \geq 1.$$

If this were to be true, then we must have at least two monomials of degree i that are not in $LT(I)$. We will prove that this gives a contradiction. Suppose x^α and x^β are monomials not in $LT(I)$ with $\alpha = (\alpha_0, \ldots, \alpha_n)$ and $\beta = (\beta_0, \ldots, \beta_n)$, and let

$$f = c_0^{\beta_0} \cdots c_n^{\beta_n} x^\alpha - c_0^{\alpha_0} \cdots c_n^{\alpha_n} x^\beta.$$

We have that

$$f(c_0, \ldots, c_n) = c_0^{\beta_0} \cdots c_n^{\beta_n}(c_0^{\alpha_0} \cdots c_n^{\alpha_n}) - c_0^{\alpha_0} \cdots c_n^{\alpha_n}(c_0^{\beta_0} \cdots c_n^{\beta_n}) = 0$$

which means that $f \in I$, and so either x^α or x^β is in $LT(I)$ which is a contradiction.

Now let $Y = \{p_1, \ldots, p_{s-1}\} \subset \mathbb{P}^n$, $X = Y \cup \{p_s\} \subset \mathbb{P}^n$, $I_1 = I(Y)$, and $I_2 = I(\{p\})$, and suppose for the induction hypothesis that there is some number M such that $HF_Y(i) = s - 1$ for all $i \geq M$.

We claim that the following sequence is short exact:

$$0 \to R/(I_1 \cap I_2) \to R/I_1 \oplus R/I_2 \to R/(I_1 + I_2) \to 0.$$

Let

$$\phi : R/(I_1 \cap I_2) \to R/I_1 \oplus R/I_2 \text{ and } \psi : R/I_1 \oplus R/I_2 \to R/(I_1 + I_2)$$

be the first and second maps, respectively, defined by

$$\phi(f + I_1 \cap I_2) = (f + I_1, f + I_2) \text{ and } \psi(f + I_1, g + I_2) = (f - g) + (I_1 + I_2)$$

respectively. We start by showing that ϕ is injective by showing its kernel is zero. Let $f + I_1 \cap I_2 \in R/(I_1 \cap I_2)$ such that $\phi(f + I_1 \cap I_2) = (0 + I_1, 0 + I_2)$. We have

$$\phi(f + I_1 \cap I_2) = (f + I_1, f + I_2) = (0 + I_1, 0 + I_2)$$

which means $f \in I_1$ and $f \in I_2$, so $f \in I_1 \cap I_2$. This gives us

$$f + I_1 \cap I_2 = 0 + I_1 \cap I_2$$

from which we conclude that the kernel is zero, so ϕ is injective. Now it is easy to show that ψ is surjective because for any $f + (I_1 + I_2) \in R/(I_1 + I_2)$ we have $(f + I_1, 0 + I_2) \in R/I_1 \oplus R/I_2$ and

$$\psi(f + I_1, 0 + I_2) = f - 0 + (I_1 + I_2) = f + (I_1 + I_2).$$

We have $image(\phi) \subset ker(\psi)$ because for any $f + I_1 \cap I_2 \in R/(I_1 \cap I_2)$ we have

$$\psi(\phi(f + I_1 \cap I_2)) = \psi(f + I_1, f + I_2) = (f - f) + (I_1 + I_2) = 0 + (I_1 + I_2).$$

To show $ker(\psi) \subset image(\phi)$, let $\psi(f + I_1, g + I_2) = (f - g) + (I_1 + I_2) = 0 + (I_1 + I_2)$. This gives us $f - g \in I_1 + I_2$, so there is some $h_1 \in I_1$ and $h_2 \in I_2$ such that $f - g = h_1 + h_2$. Now we get $f - h_1 = g + h_2$, so we let

$$h = f - h_1 = g + h_2.$$

This gives

$$\phi(h) = (h + I_1, h + I_2) = (f - h_1 + I_1, g + h_2 + I_2).$$

Since $h_1 \in I_1$ and $h_2 \in I_2$, we have $(f - h_1 + I_1, g + h_2 + I_2) = (f + I_1, g + I_2)$ which gives $(f + I_1, g + I_2) \in image(\phi)$. Now we have $ker(\psi) = image(\phi)$ and we have proven the claim.

Now we note that $I(X) = I(Y) \cap I(\{p\}) = I_1 \cap I_2$ and that I_1, I_2, and $I(X)$ are all homogeneous ideals. This allows us to get that

$$0 \to (R/I(X))_i \to (R/I_1)_i \oplus (R/I_2)_i \to (R/(I_1 + I_2))_i \to 0$$

is short exact for all $i \geq 0$, due to the fact that the maps are of degree 0. This gives

$$dim_k((R/I(X))_i) = dim_k((R/I_1)_i) + dim_k((R/I_2)_i) - dim_k((R/(I_1 + I_2))_i) \text{ for all } i \geq 0.$$

Thus, we get

$$HF_X(i) = HF_Y(i) + HF_{\{p\}}(i) - dim_k((R/(I_1 + I_2))_i).$$

Now by Proposition 6.3.6 from [6], there must be a separator of p from $Y = X \setminus I(\{p\})$. That is, there must be some $f \in I(Y)$ with $f \notin I(\{p\})$. Theorem 2.37 implies that we can assume $f + I(\{p\}) \in R/I(\{p\})$ is written as a sum of non-zero monomials in $R/LT(I(\{p\}))$, so $LT(f) \notin R/LT(I(\{p\}))$. However, we have $HF_{R/LT(I(\{p\}))}(i) = 1$ for all $i \geq 1$, which means that for $d = \deg(f)$, we have

$$LT(I(\{p\}))_d + LT(f) = R_d.$$

This implies

$$R_i = LT(I(\{p\}))_i + \langle LT(f) \rangle_i = LT(I(\{p\}) + \langle LT(f) \rangle)_i \subset LT(I_1 + I_2)_i \text{ for all } i \geq d,$$

which gives us

$$dim_k((R/I(X))_i) = dim_k((R/I_1)_i) + dim_k((R/I_2)_i) \text{ for all } i \geq d.$$

Now set $N = \max\{M, d\}$, and we have

$$\begin{aligned} dim_k((R/I(X))_i) &= dim_k((R/I_1)_i) + dim_k((R/I_2)_i) \\ &= dim_k((R/I(Y))_i) + dim_k((R/I(\{p\}))_i) \\ &= (s-1)+1 \\ &= s \text{ for all } i \geq N, \end{aligned}$$

which completes the proof. □

2. The Buchberger-Möller Algorithm

If we are given a set X of finitely many points in $\mathbb{P}^n$, we are able to compute the reduced Groebner basis for $I(X) \subset k[x_0, \ldots, x_n]$ with the projective Buchberger-Möller Algorithm. Here we present the algorithm, followed by a rough idea of how the algorithm works. Then we finish with an example where we use the Buchberger-Möller algorithm to compute the reduced Groebner basis of the defining ideal of a given set of points in projective space.

Theorem 3.5. *(Projective Buchberger-Möller Algorithm) For a fixed monomial order on $k[x_0, \ldots, x_n]$, let $X = \{p_1, \ldots, p_s\}$ be a set of points in $\mathbb{P}^n$, where each point p_i is given by $p_i = [c_{i0} : \cdots : c_{in}]$. Consider the following sequence of instructions.*

1) *Let $G = \emptyset$, $B = \emptyset$, $L = \{1\}$, $d = 0$, and let $M = (m_{ij})$ be a matrix over k with s columns and initially zero rows.*
2) *Compute the Hilbert function of $S = k[x_0, \ldots, x_n]/LT(G)$ (let $LT(G) = \langle LT(g) | g \in G\rangle$) and check whether $HF_S(i) = s$ for all $i \geq d$. If this is true, return G and stop. Otherwise, increase d by one, let $B = \emptyset$, let $M = (m_{ij})$ be a matrix over k with s columns and zero rows, and let L be the set of all monomials in $k[x_0, \ldots, x_n]$ of degree d which are not multiples of an element of $LT(G)$.*
3) *If $L = \emptyset$, continue wth step 2). Otherwise, choose $t = min(L)$ and remove it from L.*
4) *For $i = 1, \ldots, s$, compute $t(p_i) = t(c_{i0}, \ldots, c_{in})$. Reduce the vector $(t(p_1), \ldots, t(p_s))$ against the rows of M to obtain*

$$(v_1, \ldots, v_s) = (t(p_1), \ldots, t(p_s)) - \sum_i a_i(m_{i1}, \ldots, m_{is})$$

with $a_i \in k$.

5) *If $(v_1, \ldots, v_s) = (0, \ldots, 0)$, then append the polynomial $t - \sum_i a_i b_i$ to G, where b_i is the i^{th} element of the list B. Continue with step 3).*
6) *If $(v_1, \ldots, v_s) \neq (0, \ldots, 0)$, then add $(v_1, \ldots, v_s)$ as a new row to M and $t - \sum_i a_i b_i$ as a new element to B. Continue with step 3).*

Proof. Let $I = I(X)$ and suppose we stop with $HF_S(i) = s$ for all $i \geq d'$ for some d'. We have that G only contains elements of I since we are finding linear combinations of monomials that produce the zero vector (that give 0 for each point of X). This means we have $\langle g \,|\, g \in G\rangle \subset I$, which implies $LT(G) \subset LT(I)$. If we have $LT(G) = LT(I)$, then we have that the set G forms a Groebner basis for I, so suppose $LT(G) \subsetneq LT(I)$. Pick $x^\alpha \in LT(I) \setminus LT(G)$ of degree $D > d'$ so that we have $LT(G) \subsetneq LT(G) + x^\alpha \subset LT(I)$. This gives us

$$HF_{R/LT(I)}(i) \leq HF_{R/(LT(G)+x^\alpha)}(i) < HF_{R/LT(G)}(i) = s = HF_{R/LT(I)}(i) \text{ for all } i \geq D$$

which is a contradiction.

Now we prove that the algorithm eventually stops. First we note that if we are in steps 4)-6), we must come back to step 3). Secondly, the set B is always finite, so we only perform step 3) finitely many times before returning to step 2). For each degree d, the set B forms a k-basis for $(R/I)_d$ because the additive abelian group generated by B is everything in R_i that is not in $LT(I)$. Theorem 3.4 gives us that for some N, we have $HF_{R/I}(i) = s$ for all $i \geq N$. Whenever d passes both the maximal degree of the minimal generators of $LT(I)$ and N, we will have

$$HF_{R/LT(G)}(i) = HF_{R/LT(I)}(i) = HF_{R/I}(i) = s.$$

This will satisfy the condition of step 2), and the algorithm will stop. $\square$

We give a rough idea of how the algorithm works, and a detailed worked out example is given below. We know that a generator of $I(X)$ must be a homogeneous polynomial, so the idea is to use linear algebra to look for linear combinations of the monomials of that degree that vanish over the points of X.

We start by looking for polynomials in $I(X)$ that are of degree one, and we move up from there until we have found a minimal generating set of $I(X)$, which we will call G. For each degree, we take L to be the set of all monomials of that degree that are not a multiple of the leading term of any polynomial we have already found to be in G. This is because we are looking for a minimal generating set, so we do not want to find a multiple of a polynomial that we already know will be a generator $I(X)$. For example, if we are looking for degree two generators and have already found $x_1 - x_2$ to be a generator of $I(X)$, we can exclude from L any monomial that is a multiple of x_1 to prevent us from finding polynomials that are multiples of $x_1 - x_2$ (such as $x_1^2 - x_1x_2$).

Once we create our set L of monomials, we start by evaluating the smallest monomial (with respect to the fixed monomial order) of L at the points of X to obtain a vector of length s (where s is the number of points in X). If the vector is non-zero, we add it as a row to a matrix M that is initially empty, and we add the monomial that we evaluated to the set B. Next, we take the new smallest monomial of L (after deleting the previous one from L), and we evaluate it at the points of X, but now we reduce this vector against the rows of M into either echelon form or reduced row echelon form. We can think of the rows of M as polynomials that do not vanish over all of the points of X, which are stored in the set B. If we find a linear combination of the rows of M that produce the zero vector, then we can take the same linear combination of the polynomials in B that each row represents to obtain a polynomial that vanishes over all of the points of X. We then add this new polynomial to the set G. We continue evaluating the monomials in L and reducing them over the rows of M until L is empty.

Once L is empty and there are no more linear combiations of the rows of M that generate the zero vector, we know that our set G will generate every polynomial in $I(X)$ that is of our fixed degree. We then check if the Hilbert function has stabilized to determine if G is a generating set of all of $I(X)$. If the Hilbert function has not stabilized, it means that G does not generate all of $I(X)$, so we must find more generators. We know that any generators that we have not yet found will be of higher degree than our current fixed degree, so we increase the degree by one and repeat the process for the new fixed degree. We know this process must eventually stop because we are just looking for the minimal generators of $I(X)$. We know that there are finitely many of them, so there is a maximum degree. Once we reach this maximum degree during the algorithm, then we will have found all the minimal generators in $I(X)$. After we have found these generators, we know that the Hilbert function must stabilize at some positive integer N by Theorem 3.4. If we continue the process, d will eventually reach this integer N, at which point the condition in step 2) is satisfied. This is when the algorithm stops, and the set G is returned. This is the set of minimal generators of $I(X)$ which form the reduced Groebner basis of $I(X)$.

Example 3.6. Let $k = \mathbb{R}$ and let $X = \{p_1, \ldots, p_6\} \subset \mathbb{P}^2$, where $p_1 = [1:0:0]$, $p_2 = [0:1:0]$, $p_3 = [0:0:1]$, $p_4 = [1:-1:0]$, $p_5 = [1:0:-1]$, $p_6 = [0:1:-1]$. We will use the projective Buchberger-Möller algorithm to compute the reduced Groebner bais of $I(X)$ under the graded reverse lexicographic order.

1) Let $G = \emptyset$, $B = \emptyset$, $d = 0$, and $M \in Mat_{0,6}(\mathbb{R})$.
2) We have $HF_S(d) = 1$, so let $B = \emptyset$, $d = 1$, $M \in Mat_{0,6}(\mathbb{R})$, and $L = \{x_0, x_1, x_2\}$.
3) Set $t = x_2$ and let $L = \{x_0, x_1\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0, 0, 1, 0, -1, -1) = (v_1, \ldots, v_6)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & -1 & -1 \end{bmatrix}$ and $B = \{x_2\}$.
3) Set $t = x_1$ and let $L = \{x_0\}$
4) Compute $(t(p_1), \ldots, t(p_6)) = (0, 1, 0, -1, 0, 1) = (v_1, \ldots, v_6)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 1 & 0 & -1 & 0 & 1 \end{bmatrix}$ and $B = \{x_2, x_1\}$.
3) Set $t = x_0$ and let $L = \emptyset$
4) Compute $(t(p_1), \ldots, t(p_6)) = (1, 0, 0, 1, 1, 0) = (v_1, \ldots, v_6)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 1 & 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$ and $B = \{x_2, x_1, x_0\}$.
2) We have $HF_S(d) = 3$, so let $B = \emptyset$, $d = 2$, $M \in Mat_{0,6}(\mathbb{R})$, and $L = \{x_0^2, x_0x_1, x_1^2, x_0x_2, x_1x_2, x_2^2\}$.
3) Set $t = x_2^2$ and let $L = \{x_0^2, x_0x_1, x_1^2, x_0x_2, x_1x_2\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0, 0, 1, 0, 1, 1) = (v_1, \ldots, v_6)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ and $B = \{x_2^2\}$.

3) Set $t = x_1x_2$ and let $L = \{x_0^2, x_0x_1, x_1^2, x_0x_2\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0, 0, 0, 0, 0, -1) = (v_1, \ldots, v_6)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$ and $B = \{x_2^2, x_1x_2\}$.
3) Set $t = x_0x_2$ and let $L = \{x_0^2, x_0x_1, x_1^2\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0, 0, 0, 0, -1, 0) = (v_1, \ldots, v_6)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{bmatrix}$ and $B = \{x_2^2, x_1x_2, x_0x_2\}$.
3) Set $t = x_1^2$ and let $L = \{x_0^2, x_0x_1\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0, 1, 0, 1, 0, 1)$ and reduce it against the rows of M to get $(v_1, \ldots, v_6) = (0, 1, 0, 1, 0, 0)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$ and $B = \{x_2^2, x_1x_2, x_0x_2, x_1^2 + x_1x_2\}$.
3) Set $t = x_0x_1$ and let $L = \{x_0^2\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0, 0, 0, -1, 0, 0) = (v_1, \ldots, v_6)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \end{bmatrix}$ and $B = \{x_2^2, x_1x_2, x_0x_2, x_1^2 + x_1x_2, x_0x_1\}$.
3) Set $t = x_0^2$ and let $L = \emptyset$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (1, 0, 0, 1, 1, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_6) = (1, 0, 0, 0, 0, 0)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ and
   $B = \{x_2^2, x_1x_2, x_0x_2, x_1^2 + x_1x_2, x_0x_1, x_0^2 + x_0x_1 + x_0x_2\}$.
2) We have $HF_S(3) = 10$, so let $B = \emptyset$, $d = 3$, $M \in Mat_{0,6}(\mathbb{R})$, and
   $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3, x_0^2x_2, x_0x_1x_2, x_1^2x_2, x_0x_2^2, x_1x_2^2, x_2^3\}$.
3) Set $t = x_2^3$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3, x_0^2x_2, x_0x_1x_2, x_1^2x_2, x_0x_2^2, x_1x_2^2\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0, 0, 1, 0, -1, -1) = (v_1, \ldots, v_6)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & -1 & -1 \end{bmatrix}$ and $B = \{x_2^3\}$.
3) Set $t = x_1x_2^2$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3, x_0^2x_2, x_0x_1x_2, x_1^2x_2, x_0x_2^2\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0, 0, 0, 0, 0, 1) = (v_1, \ldots, v_6)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ and $B = \{x_2^3, x_1x_2^2\}$.

3) Set $t = x_0x_2^2$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3, x_0^2x_2, x_0x_1x_2, x_1^2x_2\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0,0,0,0,1,0) = (v_1, \ldots, v_6)$.
6) Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$ and $B = \{x_2^3, x_1x_2^2, x_0x_2^2\}$.
3) Set $t = x_1^2x_2$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3, x_0^2x_2, x_0x_1x_2\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0,0,0,0,0,-1)$ and reduce it against the rows of M to get $(v_1, \ldots, v_6) = (0,0,0,0,0,0)$.
5) Let $G = \{x_1^2x_2 + x_1x_2^2\}$.
3) Set $t = x_0x_1x_2$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3, x_0^2x_2\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0,0,0,0,0,0) = (v_1, \ldots, v_6)$.
5) Let $G = \{x_1^2x_2 + x_1x_2^2, x_0x_1x_2\}$.
3) Set $t = x_0^2x_2$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0,0,0,0,-1,0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_6) = (0,0,0,0,0,0)$.
5) Let $G = \{x_1^2x_2 + x_1x_2^2, x_0x_1x_2, x_0^2x_2 + x_0x_2^2\}$.
3) Set $t = x_1^3$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0,1,0,-1,0,1)$ and reduce it against the rows of M to get $(v_1, \ldots, v_6) = (0,1,0,-1,0,0)$. Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \end{bmatrix}$ and $B = \{x_2^3, x_1x_2^2, x_0x_2^2, x_1^3 - x_1x_2^2\}$.
3) Set $t = x_0x_1^2$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0,0,0,1,0,0) = (v_1, \ldots, v_6)$.
Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$ and $B = \{x_2^3, x_1x_2^2, x_0x_2^2, x_1^3 - x_1x_2^2, x_0x_1^2\}$.
3) Set $t = x_0^2x_1$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3\}$.
4) Compute $(t(p_1), \ldots, t(p_6)) = (0,0,0,-1,0,0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_6) = (0,0,0,0,0,0)$. Let $G = \{x_1^2x_2 + x_1x_2^2, x_0x_1x_2, x_0^2x_2 + x_0x_2^2, x_0^2x_1 + x_0x_1^2\}$.
3) Set $t = x_0^3$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3\}$.

4) Compute $(t(p_1), \ldots, t(p_6)) = (1,0,0,1,1,0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_6) = (1,0,0,0,0,0)$. Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ and $B = \{x_2^3, x_1x_2^2, x_0x_2^2, x_1^3 - x_1x_2^2, x_0x_1^2, x_0^3 - x_0x_1^2 - x_0x_2^2\}$.

2) We have $LT(G) = \langle x_1^2x_2, x_0x_1x_2, x_0^2x_2, x_0^2x_1 \rangle$ and for all $i \geq 3$ we have

$$HF_{k[x_0,x_1,x_2]/\langle x_1^2x_2, x_0x_1x_2, x_0^2x_2, x_0^2x_1 \rangle}(i) = 6.$$

At this point we stop and we get that

$$G = \langle x_1^2x_2 + x_1x_2^2, x_0x_1x_2, x_0^2x_2 + x_0x_2^2, x_0^2x_1 + x_0x_1^2 \rangle$$

is the reduced Groebner basis for $I(X)$ under the graded reverse lexicographic order.

CHAPTER 4

Points in $\mathbb{P}^1 \times \mathbb{P}^1$

Throughout the rest of this project we will be working in the product space $\mathbb{P}^1 \times \mathbb{P}^1$. Here we will present the necessary background information for points in $\mathbb{P}^1 \times \mathbb{P}^1$ which will be needed in the next chapter. The ideas and notation used in this chapter follow that of E. Guardo and A. Van Tuyl in [4].

1. Points and biprojective space

We begin by defining the biprojective space $\mathbb{P}^1 \times \mathbb{P}^1$.

Definition 4.1. The biprojective space $\mathbb{P}^1 \times \mathbb{P}^1$ is defined as the set of equivalence classes of $(k^2 \setminus \{0\}) \times (k^2 \setminus \{0\})$ with respect to the relation $\sim$, where

$$(a_1, a_2) \times (b_1, b_2) \sim (a_1', a_2') \times (b_1', b_2')$$

if $(a_1, a_2) = (\lambda_1 a_1', \lambda_1 a_2')$ and $(b_1, b_2) = (\lambda_2 b_1', \lambda_2 b_2')$ for some nonzero $\lambda_1, \lambda_2 \in k$.

If $(a_1, a_2)\times(b_1, b_2) \in (k^2\setminus\{0\})\times(k^2\setminus\{0\})$, then the equivalence class of $(a_1, a_2)\times(b_1, b_2)$ is called a *point* in $\mathbb{P}^1 \times \mathbb{P}^1$, denoted $[a_1 : a_2] \times [b_1 : b_2]$.

Alternatively, we could have just defined $\mathbb{P}^1 \times \mathbb{P}^1$ as the cartesian product of $\mathbb{P}^1$ with itself.

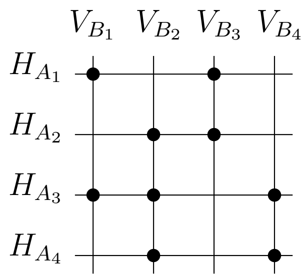
We define $\pi_1 : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$ and $\pi_2 : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$ to be the natural projection maps onto the first and second coordinates, respectively. Since we are working in a product space, it is natural to think of the space as a plane with $\mathbb{P}^1$ on each axis. This way, we can think of any finite set of points $X \subset \mathbb{P}^1 \times \mathbb{P}^1$ to be on a grid where the horizontal and vertical rulings are labelled by $\pi_1(X)$ and $\pi_2(X)$, respectively. Although we are using an orientation that may seem reversed to what we normally would expect, the purpose is to coincide with matrix notation and the notation of a Ferrers diagram, which we will introduce shortly.

Suppose $X \subset \mathbb{P}^1 \times \mathbb{P}^1$ is a finite set of points and suppose $\pi_1(X) = \{A_1, \ldots, A_h\} \subset \mathbb{P}^1$ and $\pi_2(X) = \{B_1, \ldots, B_v\} \subset \mathbb{P}^1$. To view X on a grid, we label the horizontal rulings of the grid as $H_{A_1}, \ldots, H_{A_h}$, where $H_{A_i} = \{A_i \times B \mid B \in \mathbb{P}^1\} \subset \mathbb{P}^1 \times \mathbb{P}^1$, and we label the vertical rulings $V_{B_1}, \ldots, V_{B_h}$, where $V_{B_j} = \{A \times B_j \mid A \in \mathbb{P}^1\} \subset \mathbb{P}^1 \times \mathbb{P}^1$. This way, a point $A_i \times B_j \in X \subset \mathbb{P}^1 \times \mathbb{P}^1$ is the intersection of H_{A_i} and V_{B_j}, so it will appear on the grid where the the lines H_{A_i} and V_{B_j} intersect.

EXAMPLE 4.2. Let

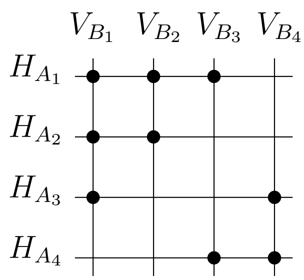
$$X = \{A_1 \times B_1, A_1 \times B_3, A_2 \times B_2, A_2 \times B_3, A_3 \times B_1, A_3 \times B_2, A_3 \times B_4, A_4 \times B_2, A_4 \times B_4\}$$

where A_i and B_j are points in $\mathbb{P}^1$ for all $i, j = 1, 2, 3, 4$. We can represent X as points on a grid as in the following image.



Now we note that with appropriate relabeling, we can interchange the columns and rows of such a grid without changing what the grid represents. This means that for any finite set $X \subset \mathbb{P}^1 \times \mathbb{P}^1$, we can label the points such that $|X \cap H_{A_1}| \geq |X \cap H_{A_2}| \geq \cdots$ and $|X \cap V_{B_1}| \geq |X \cap V_{B_2}| \geq \cdots$.

EXAMPLE 4.3. For the set X given in Example 4.2, we can relabel its points to get the grid representation in the following image.



Now with this relabeling, we have that this grid representation of X satisfies $|X \cap H_{A_1}| \geq |X \cap H_{A_2}| \geq \cdots$ and $|X \cap V_{B_1}| \geq |X \cap V_{B_2}| \geq \cdots$.

Throughout the rest of this project, we will assume that any given finite set $X \subset \mathbb{P}^1 \times \mathbb{P}^1$ with $\pi_1(X) = \{A_1, \ldots, A_h\} \subset \mathbb{P}^1$ and $\pi_2(X) = \{B_1, \ldots, B_v\} \subset \mathbb{P}^1$ will satisfy $|X \cap H_{A_1}| \geq |X \cap H_{A_2}| \geq \cdots$ and $|X \cap V_{B_1}| \geq |X \cap V_{B_2}| \geq \cdots$.

DEFINITION 4.4. Let X be a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ with $\pi_1(X) = \{A_1, \ldots, A_h\} \subset \mathbb{P}^1$ and $\pi_2(X) = \{B_1, \ldots, B_v\} \subset \mathbb{P}^1$. We define $\alpha_X = (\alpha_1, \ldots, \alpha_h)$ and $\beta_X = (\beta_1, \ldots, \beta_v)$ where

$$\alpha_i = |X \cap H_{A_i}|$$

and

$$\beta_j = |X \cap V_{B_j}|.$$

Also, if we have $\alpha_X = (\alpha_1, \ldots, \alpha_h)$ for some set X, then we will use the convention that $\alpha_{h+1} = 0$.

Example 4.5. For the set X used in Examples 4.2 and 4.3, we will compute α_X and β_X. We can start by noting that $h = 4$ and $v = 4$, so α_X and β_X will each have length 4. Now we directly compute each α_i:

$$\begin{aligned} \alpha_1 &= |X \cap H_{A_1}| = 3 \\ \alpha_2 &= |X \cap H_{A_2}| = 2 \\ \alpha_3 &= |X \cap H_{A_3}| = 2 \\ \alpha_4 &= |X \cap H_{A_4}| = 2. \end{aligned}$$

This gives $\alpha_X = (3, 2, 2, 2)$. Similarly, we get the β_j by computing

$$\begin{aligned} \beta_1 &= |X \cap V_{B_1}| = 3 \\ \beta_2 &= |X \cap V_{B_2}| = 2 \\ \beta_3 &= |X \cap V_{B_3}| = 2 \\ \beta_4 &= |X \cap V_{B_4}| = 2 \end{aligned}$$

which gives $\beta_X = (3, 2, 2, 2)$.

For any finite set of points $X \subset \mathbb{P}^1 \times \mathbb{P}^1$, we have that both α_X and β_X are partitions of $|X|$.

Definition 4.6. If $s \in \mathbb{N}$ and $v = (v_1, \ldots, v_r)$ is such that each v_i is a positive integer with $v_i \geq v_{i+1}$ and $\sum_{i=1}^{r} v_i = s$, then we say v is a *partition* of s. If v is a partition of an integer s, then the *conjugate* of v is defined as

$$v^* = (v_1^*, \ldots, v_{v_1}^*)$$

where $v_i^* = |\{v_j \mid v_j \geq i\}|$. The conjugate v^* is also a partition of s.

If we have that $v = (v_1, \ldots, v_r)$ is a partition of some integer s, then its conjugate necessarily has length v_1. This can be seen from the fact that we have

$$v_{v_1}^* = |\{v_j \mid v_j \geq v_1\}| \geq |\{v_1\}| > 0$$

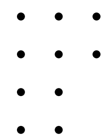
and for any $i > v_1$ we have

$$v_i^* = |\{v_j \mid v_j \geq i\}| = |\emptyset| = 0.$$

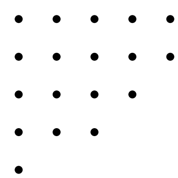
Note that for any finite set of points $X \subset \mathbb{P}^1 \times \mathbb{P}^1$, both α_X^* and β_X^* are partitions of $|X|$, because α_X and β_X both are.

Definition 4.7. Let $v = (v_1, \ldots, v_r)$ be a partition of some integer s. The *Ferrers diagram* of v is a $r \times v_1$ grid with v_i left justified points on the i^{th} horizontal line from the top.

Example 4.8. We have that $(3, 3, 2, 2)$ is a partition of 10. The Ferrers diagram of $(3, 3, 2, 2)$ is



Now consider $(5, 5, 4, 3, 1)$, which is a partition of 18. The Ferrers diagram of $(5, 5, 4, 3, 1)$ is



Note that we can easily obtain the conjugate of a partition from its Ferrers diagram by counting the number of points in each column.

We now define a condition for a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ to be Arithmetically Cohen-Macaulay. Although this is an algebraic property, the definition we give is consistent with other common definitions of Arithmetically Cohen-Macaulay (refer to Definition 2.20 and Theorem 4.11 in [4] for more information on the Arithmetically Cohen-Macaulay property). The reason we define the property this way is to give a useful criterion for classifying finite sets of points in $\mathbb{P}^1 \times \mathbb{P}^1$ as Arithmetically Cohen-Macaulay or not.

Definition 4.9. Let X be a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ with $\alpha_X = (\alpha_1, \ldots, \alpha_h)$ and $\beta_X = (\beta_1, \ldots, \beta_v)$. We say that X is *Arithmetically Cohen-Macaulay (ACM)* if $\alpha_X^* = \beta_X$ (and consequently $\beta_X^* = \alpha_X$).

An equivalent definition for X to be ACM, is that the grid representation of X must resemble a Ferrers diagram. In this case, the grid representation for X will be unique, and it will resemble the Ferrers diagram of α_X.

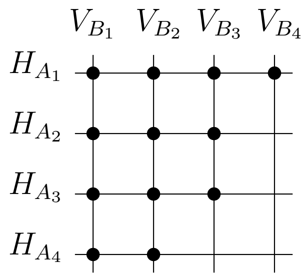
Example 4.10. For the set X used in Examples 4.2, 4.3, and 4.5, we have $\alpha_X = (3, 2, 2, 2)$ and $\beta_X = (3, 2, 2, 2)$. We compute $\alpha_X^* = (4, 4, 1)$, and we get that X is not ACM because $\alpha_X^* \neq \beta_X$. The fact that X is not ACM can also be seen from the fact that the grid representation of X given in Example 4.3 does not resemble a Ferrers diagram.

Example 4.11. For this example, let

$$\begin{aligned} X = \quad & \{A_1 \times B_1, A_1 \times B_2, A_1 \times B_3, A_1 \times B_4, \\ & A_2 \times B_1, A_2 \times B_2, A_2 \times B_3, \\ & A_3 \times B_1, A_3 \times B_2, A_3 \times B_3, \\ & A_4 \times B_1, A_4 \times B_2\}. \end{aligned}$$

We will check if X is ACM. We start by finding $\alpha_X = (4,3,3,2)$ and $\beta_X = (4,4,3,1)$. We compute $\alpha_X^* = (4,4,3,1)$, which gives $\alpha_X^* = \beta_X$. From this, we can conclude that X is ACM.

The unique grid representation of X is given below, which resembles a Ferrers diagram.



Since the grid representation of X resembles a Ferrers diagram, we can see that X is ACM. Also, we can easily compute the conjugate of α_X from this diagram by counting the number of points in each column. Thus, the fact that $\alpha_X^* = \beta_X$ for an ACM set of points is a consequence of the fact that the grid representation resembles a Ferrers diagram.

2. Algebra of points in $\mathbb{P}^1 \times \mathbb{P}^1$

If we are given a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$, we may be interested in finding the ideal of polynomials that vanish over each point. In the product space, we have four coordinates to consider, so we will look for polynomials in the polynomial ring with four variables, which we call x_0, x_1, y_0, and y_1. We must also recall that we are in projective space and so any polynomials that are zero over a set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ must also be zero when we multiply x_0 and x_1 by any scalar and/or multiply y_0 and y_1 by any scalar. This implies that any such polynomial must not only be homogeneous, but also bihomogeneous.

Definition 4.12. A *bihomogenous* polynomial in $k[x_0, x_1, y_0, y_1]$ is a homogeneous polynomial $f(x_0, x_1, y_0, y_1)$ such that both $f(x_0, x_1, 1, 1)$ and $f(1, 1, y_0, y_1)$ are homogeneous (of possibly different degrees) and $\deg(f(x_0, x_1, y_0, y_1)) = \deg(f(x_0, x_1, 1, 1)) + \deg(f(1, 1, y_0, y_1))$. If $f(x_0, x_1, y_0, y_1)$ is bihomogeneous with $f(x_0, x_1, 1, 1)$ homogeneous of degree d_1 and $f(1, 1, y_0, y_1)$ homogeneous of degree d_2, then we say f is bihomogeneous of degree (d_1, d_2).

Example 4.13. Consider $f = x_0^2y_0^3 + x_0x_1y_0^2y_1 + x_1^2y_0y_1^2$ which is homogeneous of degree 5. We have $f(x_0, x_1, 1, 1) = x_0^2 + x_0x_1 + x_1^2$ is homogeneous of degree 2, $f(1, 1, y_0, y_1) = y_0^3 + y_0^2y_1 + y_0y_1^2$ is homogeneous of degree 3, and $\deg(f) = 5 = 2+3$ so f is bihomogeneous of degree $(2, 3)$.

To tell if a given polynomial is bihomogenous, we just need that each of its monomials must be bigraded of the same degree.

Definition 4.14. A *bigraded ring* is a ring that is a direct sum of abelian groups $R_{(i,j)}$ such that $R_{(i_1,j_1)}R_{(i_2,j_2)} \subset R_{(i_1+i_2,j_1+j_2)}$.

EXAMPLE 4.15. We have that $k[x_0, x_1, y_0, y_1]$ with $\deg x_0 = \deg x_1 = (1,0)$, and $\deg y_0 = \deg y_1 = (0,1)$ is a bigraded ring where $k[x_0, x_1, y_0, y_1]_{(i,j)}$ is the additive abelian group generated by all monomials of bidegree (i,j). This is because any polynomial in $k[x_0, x_1, y_0, y_1]$ can be written as the direct sum of bihomogeneous polynomials that are all of different bidegrees (by grouping all the monomials into their respective bidegrees). Now each of these bihomogeneous polynomials are a sum of monomials of a fixed bidegree, so belong to $k[x_0, x_1, y_0, y_1]_{(i,j)}$ for some i and j. From this we conclude that

$$k[x_0, x_1, y_0, y_1] = \bigoplus_{(i,j)\in\mathbb{N}^2} k[x_0, x_1, y_0, y_1]_{(i,j)}.$$

It is easy to see that $k[x_0, x_1, y_0, y_1]_{(i_1,j_1)} k[x_0, x_1, y_0, y_1]_{(i_2,j_2)} \subset k[x_0, x_1, y_0, y_1]_{(i_1+i_2, j_1+j_2)}$ because the product of any two monomials of bigrees (i_1, j_1) and (i_2, j_2) will have bidegree $(i_1 + i_2, j_1 + j_2)$. This implies that the product of any two bihomogeneous polynomials of bigrees (i_1, j_1) and (i_2, j_2) will have bidegree $(i_1 + i_2, j_1 + j_2)$ so we have the containment property needed to be a bigraded ring.

DEFINITION 4.16. A *bihomogeneous ideal* is an ideal generated by bihomogeneous polynomials.

LEMMA 4.17. *A bihomogeneous ideal is a bigraded ring.*

PROOF. The proof of this lemma is similar to the proof given in Chapter 3 that a homogeneous ideal is a graded ring. The idea is that if I is a bihomogeneous ideal, we let $I_{(i,j)}$ be the additive abelian group of all bihomogenous polynomials in I of bidegree (i,j). This gives us

$$I = \bigoplus_{(i,j)\in\mathbb{N}^2} I_{(i,j)}.$$

We also have that $I_{(i_1,j_1)} I_{(i_2,j_2)} \subset I_{(i_1+i_2,j_1+j_2)}$ because the product of two bihomogeneous polynomials in I of degrees (i_1, j_1) and (i_2, j_2) must be in I and of bidegree $(i_1 + i_2, j_1 + j_2)$. □

Now we define the defining ideal for a set of points in $\mathbb{P}^1 \times \mathbb{P}^1$.

DEFINITION 4.18. Let $X = \{p_1, \ldots, p_r\}$ be a set of points in $\mathbb{P}^1 \times \mathbb{P}^1$. The *bihomogeneous vanishing ideal* of X (or the *defining ideal* of X), denoted $I(X)$, is defined as

$$I(X) = \langle f \in k[x_0, x_1, y_0, y_1] \mid f \text{ is bihomogeneous and } f(p_i) = 0 \text{ for all } p_i \in X\rangle.$$

Note that if f is bihomogeneous of bidegree (d_1, d_2) and $f(a_1, a_2, b_1, b_2) = 0$, where $p = [a_1 : a_2] \times [b_1 : b_2]$ is a point in $\mathbb{P}^1 \times \mathbb{P}^1$, we have that

$$f(p) = f(\lambda_1 a_1, \lambda_1 a_2, \lambda_2 b_1, \lambda_2 b_2) = \lambda_1^{d_1} \lambda_2^{d_2} f(a_1, a_2, b_1, b_2) = 0$$

for any $\lambda_1, \lambda_2 \in k$. This means that a point in $\mathbb{P}^1 \times \mathbb{P}^1$ is a zero of a bihomogeneous polynomial if any one of its coordinate representations is a zero.

We know that the defining ideal of a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ is generated by bihomogeneous polynomials in $k[x_0, x_1, y_0, y_1]$, so it is a bihomogeneous ideal and hence a bigraded ring. This means we can look at the Hilbert function of a finite set of points in terms of the bigrading of its defining ideal.

Definition 4.19. Let X be a set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ and let I be the bihomogeneous ideal $I(X)$. The *bigraded Hilbert function* of X is defined as a matrix $(HF_X(i,j))$ where $HF_X(i,j)$ is defined as

$$HF_X(i,j) = dim_k(k[x_0, x_1, y_0, y_1]_{(i,j)}) - dim_k(I_{(i,j)}).$$

For any finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ X, we can determine a significant part of its Hilbert function from α_X and β_X.

Theorem 4.20. *Let X be a set of s points in $\mathbb{P}^1 \times \mathbb{P}^1$ with $\alpha_X = (\alpha_1, \ldots, \alpha_h)$ and $\beta_X = (\beta_1, \ldots, \beta_v)$. For all $1 \le i \le \alpha_1$ and $1 \le j \le \beta_1$, let*

$$a_i = \sum_{l=1}^{i} \alpha_l^* \text{ and } b_j = \sum_{l=1}^{j} \beta_l^*$$

where $\alpha_X^* = (\alpha_1^*, \ldots, \alpha_{\alpha_1}^*)$ and $\beta_X^* = (\beta_1^*, \ldots, \beta_{\beta_1}^*)$. Let $a_i = s$ for $i > \alpha_1$ and $b_j = s$ for $j > \beta_1$. We have

$$(HF_X(i,j)) = \begin{bmatrix} 1 & 2 & \cdots & v-1 & b_1 & b_1 & \cdots \\ 2 & & & & b_2 & b_2 & \cdots \\ \vdots & & & & \vdots & & \\ h-1 & & & & b_{h-1} & b_{h-1} & \cdots \\ a_1 & a_2 & \cdots & a_{v-1} & s & s & \cdots \\ a_1 & a_2 & \cdots & a_{v-1} & s & s & \cdots \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}.$$

Proof. This theorem is identical to Corollary 3.30 in [4]. We get the first column and the top row directly from Theorem 3.27 (i) and (ii) in [4], which states that these entries are the same as the Hilbert functions of $\pi_1(X)$ and $\pi_2(X)$. Lemma 3.25 in [4] gives us these values. Everything else is deduced from Theorem 3.29 in [4], which gives us $HF_X(i,j) = a_{j+1}$ for all $i \ge h-1$ and $HF_X(i,j) = b_{i+1}$ for all $j \ge v-1$. We also use the fact that we have $s = \sum_{i=1}^{v} \alpha_i^* = \sum_{i=1}^{h} \beta_i^*$ because α_X^* and β_X^* are partitions of s. □

Example 4.21. For the set X used in Examples 4.2, 4.3, 4.5, and 4.10, we have $\alpha_X = (3,2,2,2)$, $\beta_X = (3,2,2,2)$, $\alpha_X^* = (4,4,1)$, and we compute $\beta_X^* = (4,4,1)$. From these, we compute $a_1 = 4$, $a_2 = 8$, and $a_i = 9$ for all $i \ge 3$, and $b_1 = 4$, $b_2 = 8$, and $b_j = 9$

for all $j \geq 3$. This gives

$$(HF_X(i,j)) = \begin{bmatrix} 1 & 2 & 3 & 4 & 4 & \cdots \\ 2 & & & 8 & 8 & \cdots \\ 3 & & & 9 & 9 & \cdots \\ 4 & 8 & 9 & 9 & 9 & \cdots \\ 4 & 8 & 9 & 9 & 9 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}.$$

The previous theorem is the basis for the stopping criterion in the new Buchberger-Moeller algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$ given in the next chapter.

3. The Universal Groebner basis for the defining ideal of an ACM set of points

If we know that a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ is ACM, then we do not need an algorithm to find its defining ideal. We start with two theorems that are used to prove Theorem 4.24, which gives us the Universal Groebner basis of the defining ideal of an ACM set of points in $\mathbb{P}^1 \times \mathbb{P}^1$. These theorems are identical to Theorem 4.9 and Corollary 5.6 given by E. Guardo and A. Van Tuyl in [4].

For the remainder of this report, we will use the notation that was used by E. Guardo and A. Van Tuyl in [4], where H_A denotes both the horizontal ruling as well as the bihomogeneous polynomial of bidegree $(1,0)$ that vanishes over H_A. Similarly, V_B will denote both the vertical ruling and the bihomogeneous polynomial of bidegree $(0,1)$ that vanishes over V_B. We can assume that the coefficients of the leading terms of each of these polynomials is one. We will also adopt the convention that $\prod_{i=a}^{b} p_i = 1$ for any product of polynomials if $b < a$.

The following theorem is identical to E. Guardo and A. Van Tuyl's Theorem 4.9 in [4]. We will use this result to prove Theorem 4.24, which gives us the Universal Groebner basis for the defining ideal of an ACM set of points in $\mathbb{P}^1 \times \mathbb{P}^1$.

Theorem 4.22. *Let X be a finte set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ with $\alpha_X = (\alpha_1, \ldots, \alpha_h)$ and $\beta_X = (\beta_1, \ldots, \beta_v)$. Let H be a degree (1,0) line that contains α_1 points of X, $Y = X \cap H$, and $Z = X \setminus Y$. If $\pi_2(Z) \subset \pi_2(Y)$, then*

$$I(X) = H \cdot I(Z) + \prod_{i=1}^{\alpha_1} V_{B_i}.$$

We do not give a proof here, but there is one given by E. Guardo and A. Van Tuyl in [4] under Theorem 4.9.

This next theorem, identical to Corollary 5.6 given by E. Guardo and A. Van Tuyl in [4], gives us a minimal set of generators for the defining ideal of a given ACM set of points in $\mathbb{P}^1 \times \mathbb{P}^1$. We prove that this set of generators forms the Universal Groebner basis in the theorem that follows.

THEOREM 4.23. *Let X be an ACM set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ with $\pi_1(X) = \{A_1, \ldots, A_h\}$, $\pi_2(X) = \{B_1, \ldots, B_v\}$, and $\alpha_X = (\alpha_1, \ldots, \alpha_h)$. A minimal bihomogeneous set of generators of $I(X)$ is given by*

$$\left\{ \prod_{i=1}^{j} H_{A_i} \prod_{i=1}^{\alpha_{j+1}} V_{B_i} \;\middle|\; \alpha_{j+1} - \alpha_j < 0 \text{ or } j = 0 \right\}.$$

We refer the reader to Corollary 5.6 in [4] for a proof of this theorem.

We will now prove that the generators in Theorem 4.23 form the Universal Groebner basis for the defining ideal of X.

THEOREM 4.24. *Let X be a set of s points in $\mathbb{P}^1 \times \mathbb{P}^1$ that is ACM with $\alpha_X = (\alpha_1, \ldots, \alpha_h)$. The minimal set of generators of $I(X)$ given in Theorem 4.23 forms the Universal Groebner basis for $I(X)$.*

PROOF. Fix any monomial order, and let $X_k = (\bigcup_{i=k}^{h} H_{A_i}) \cap X$ and $I_k = I(X_k)$. In other words, we have defined X_k to be the set of points of the bottom $h - k + 1$ rows of the grid representation of X, which resembles a Ferrers diagram. Note that $X_h \subset X_{h-1} \subset \cdots \subset X_1 = X$, and all are ACM since each of their grid representations will resemble a Ferrers diagram. We have $\alpha_{X_k} = (\alpha_k, \ldots, \alpha_h)$. Now we want to apply Theorem 4.22 on X_k. The first entry of α_{X_k} is α_k, so we need the degree $(1, 0)$ line that contains α_k points of X_k. We have that $H_{A_k} \supset H_{A_k} \cap X_k = H_{A_k} \cap X$ and $|H_{A_k} \cap X| = \alpha_k$ which means that H_{A_k} is the degree $(1, 0)$ line that contains α_k points of X_k. Since X_k is ACM for each k, we also have $X_k \subset \bigcup_{i=1}^{\alpha_k} V_{B_i}$ for each k. Now let $Y_k = X_k \cap H_{A_k}$ and $Z_k = X_k \setminus Y_k$. We have

$$\begin{aligned} Z_k &= X_k \setminus Y_k \\ &= \left[\left(\bigcup_{i=k}^{h} H_{A_i} \right) \cap X \right] \setminus (X_k \cap H_{A_k}) \\ &= \left[\left(\bigcup_{i=k}^{h} H_{A_i} \right) \cap X \right] \setminus (X \cap H_{A_k}) \\ &= \left(\bigcup_{i=k+1}^{h} H_{A_i} \right) \cap X \\ &= X_{k+1}. \end{aligned}$$

Now we note that

$$\pi_2(Y_k) = \{B_1, B_2, \ldots, B_{\alpha_k}\} = \pi_2(X_k)$$

and we have

$$\pi_2(Z_k) = \pi_2(X_{k+1}) = \{B_1, B_2, \ldots, B_{\alpha_{k+1}}\} \subset \{B_1, B_2, \ldots, B_{\alpha_k}\} = \pi_2(Y_k)$$

since $\alpha_{k+1} \leq \alpha_k$. Now by Theorem 4.22, putting everything together gives us

$$I_k = H_{A_k} I_{k+1} + \prod_{i=1}^{\alpha_k} V_{B_i}.$$

We start with

$$I_h = \langle H_{A_h}, V_{B_1} \cdots V_{B_{\alpha_h}} \rangle = \left\langle \prod_{i=h}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, h-1 \leq m \leq h \right\rangle,$$

and we have

$$\begin{aligned} I_{h-1} &= H_{A_{h-1}} I_h + \prod_{i=1}^{\alpha_{h-1}} V_{B_i} \\ &= \langle H_{A_{h-1}} H_{A_h}, H_{A_{h-1}} V_{B_1} \cdots V_{B_{\alpha_h}}, V_{B_1} \cdots V_{B_{\alpha_{h-1}}} \rangle \\ &= \left\langle \prod_{i=h-1}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, h-2 \leq m \leq h \right\rangle. \end{aligned}$$

Now if we let

$$I_{k+1} = \left\langle \prod_{i=k+1}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, k \leq m \leq h \right\rangle,$$

we have

$$\begin{aligned} I_k &= H_{A_k} I_{k+1} + \prod_{i=1}^{\alpha_k} V_{B_i} \\ &= \left\langle \prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, k \leq m \leq h \right\rangle + \prod_{i=1}^{\alpha_k} V_{B_i} \\ &= \left\langle \prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, k-1 \leq m \leq h \right\rangle. \end{aligned}$$

We will now prove by descending induction that $\{\prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \mid k-1 \leq m \leq h\}$ is a Groebner basis for I_k for $1 \leq k \leq h$. The desired conclusion then follows from the fact that $I(X) = I(X_1) = I_1$.

We have that $\{H_{A_h}, V_{B_1} \cdots V_{B_{\alpha_h}}\}$ is a generating set for $I_h = I(X_h)$ since X_h is a finite set of points on the line H_{A_h}. The two generators are in different variables, so it follows from Theorem 2.30 that they form a Groebner basis for I_h for any monomial order. Now we will fix k and assume that

$$\left\{ \prod_{i=k+1}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, k \leq m \leq h \right\}$$

is a Groebner basis for I_{k+1}. We will use this to show that $I_k = H_{A_k} I_{k+1} + \prod_{i=1}^{\alpha_k} V_{B_i}$ gives a Groebner basis for I_k. From the assumption, Theorem 2.20 gives us that

$$\left\{ \prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, k \leq m \leq h \right\}$$

is a Groebner basis for $H_{A_k} I_{k+1}$. This means that any S-polynomial formed from two of theses generators gives a remainder of 0 after applying the division algorithm over

$$\left\{ \prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, k \leq m \leq h \right\},$$

which also means that we get a remainder of 0 after applying the division algorithm to these S-polynomials over $\{\prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \mid k-1 \leq m \leq h\}$ (we can do the same process to reach 0 remainder).

It remains to show that any S-polynomial formed from $\prod_{i=1}^{\alpha_k} V_{B_i}$ and one of $\{\prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} | k \leq m \leq h\}$ gives 0 remainder after applying the division algorithm over

$$\left\{ \prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, k-1 \leq m \leq h \right\}.$$

Let $G = \prod_{i=1}^{\alpha_k} V_{B_i}$ and let $f_m = \prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i}$ for each m with $k \leq m \leq h$.

First, we fix m with $k \leq m \leq h$ and look at the polynomials

$$\prod_{i=\alpha_{m+1}+1}^{\alpha_k} V_{B_i} \text{ and } \prod_{i=k}^{m} H_{A_i}.$$

These are polynomials in separate variables, so by Theorem 2.30, we know that their S-polynomial will give a remainder of 0 after applying the division algorithm over

$$\left\{ \prod_{i=\alpha_{m+1}+1}^{\alpha_k} V_{B_i}, \prod_{i=k}^{m} H_{A_i} \right\}.$$

This means that

$$\left\{ \prod_{i=\alpha_{m+1}+1}^{\alpha_k} V_{B_i}, \prod_{i=k}^{m} H_{A_i} \right\}$$

forms a Groebner basis for

$$\left\langle \prod_{i=\alpha_{m+1}+1}^{\alpha_k} V_{B_i}, \prod_{i=k}^{m} H_{A_i} \right\rangle.$$

By Theorem 2.20, we have that

$$\{G, f_m\} = \left\{ \prod_{i=1}^{\alpha_k} V_{B_i}, \prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \right\}$$

forms a Groebner basis for

$$\left(\prod_{i=1}^{\alpha_{m+1}} V_{B_i}\right)\left\langle \prod_{i=\alpha_{m+1}+1}^{\alpha_k} V_{B_i}, \prod_{i=k}^{m} H_{A_i}\right\rangle = \langle G, f_m\rangle.$$

Buchberger's criterion implies that we get a remainder of 0 after applying the division algorithm to the S-polynomial formed from G and f_m over $\{G, f_m\}$, which means that we must also get a remainder of 0 after applying the division algorithm over

$$\left\{\prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, k-1 \leq m \leq h\right\}$$

because $\{G, f_m\}$ is a subset. Since the choice of m was arbitrary, we have that

$$\left\{\prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, k-1 \leq m \leq h\right\}$$

satisfies Buchberger's criterion, so is a Groebner basis for

$$I_k = \left\langle \prod_{i=k}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, k-1 \leq m \leq h\right\rangle.$$

Now we have that

$$\left\{\prod_{i=1}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, 0 \leq m \leq h\right\}$$

is a Groebner basis for

$$I(X) = I_1 = \left\langle \prod_{i=1}^{m} H_{A_i} \prod_{i=1}^{\alpha_{m+1}} V_{B_i} \,\middle|\, 0 \leq m \leq h\right\rangle.$$

The minimal set of generators of $I(X)$ given in Theorem 4.23 must also satisfy Buchberger's criterion since the S-polynomial formed from two of the generators give a remainder of 0 after applying the division algorithm over any set containing the two chosen generators. Since they also generate the same ideal $I(X)$, we have that they form a Groebner basis for $I(X)$. Finally, it is impossible for a monomial appearing in one generator to divide a monomial appearing in any of the other generators due to it having a higher degree in either the x_i variables or the y_i variables. This means that they form the reduced Groebner basis for $I(X)$. Since we can obtain this result for any monomial order, we have that this set of generators forms the Universal Groebner basis for $I(X)$. □

Now if a given set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ is ACM, we can easily obtain the Universal Groebner basis for its defining ideal. However, it may be the case that our given set of points is not ACM. In the next chapter we develop a Buchberger-Moeller algorithm for points in $\mathbb{P}^1 \times \mathbb{P}^1$ to deal with these cases.

CHAPTER 5

Buchberger-Moeller Algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$

The Buchberger-Moeller algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$ is the final result of this project. Everything we have learned about Groebner bases, Hilbert functions, and points in $\mathbb{P}^1 \times \mathbb{P}^1$ brings us to this. We can now prove that the Buchberger Moeller algorithm for $\mathbb{P}^n$ can be extended to compute the reduced Groebner basis for the defining ideal of a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$.

1. Buchberger-Moeller Algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$

Although we already have a reduced Groebner basis for the defining ideal of a given ACM set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ given in Theoerem 4.24, this modified algorithm will give us the same result for a set of points that is not ACM. Using the background of Chapter 4, we are able to present the Buchberger-Moeller Algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$.

THEOREM 5.1. *(Buchberger-Möller Algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$) For a fixed monomial order on $k[x_0, x_1, y_0, y_1]$, let $X = \{p_1, \ldots, p_s\}$ be a set of points in $\mathbb{P}^1 \times \mathbb{P}^1$ with $\alpha_X = (\alpha_1, \ldots, \alpha_h)$ and $\beta_X = (\beta_1, \ldots, \beta_v)$, where each point p_i is given by $p_i = [c_{i0}^{(1)} : c_{i1}^{(1)}] \times [c_{i0}^{(2)} : c_{i1}^{(2)}]$. For each $1 \leq i \leq \alpha_1$ and $1 \leq j \leq \beta_1$, let*

$$a_i = \sum_{l=1}^{i} \alpha_l^* \text{ and } b_j = \sum_{l=1}^{j} \beta_l^*$$

where $\alpha_X^* = (\alpha_1^*, \ldots, \alpha_{\alpha_1}^*)$ and $\beta_X^* = (\beta_1^*, \ldots, \beta_{\beta_1}^*)$ with $a_i = s$ for $i \geq \alpha_1$ and $b_j = s$ for $j \geq \beta_1$. Consider the following sequence of instructions.

1) *Let $G = \emptyset$, $B = \emptyset$, $(d_1, d_2) = (0, 0)$, and let $M = (m_{ij})$ be a matrix over k with s columns and initially zero rows.*
2) *Compute the Hilbert function of $S = k[x_0, x_1, y_0, y_1]/LT(G)$ and check whether $HF_S(i, j) = b_{i+1}$ for all $i \geq 0$ and $j \geq d_2$. If this is true, return G and stop. Otherwise, proceed with step 3).*
3) *Check if $HF_S(i, d_2) = a_{d_2+1}$ for all $i \geq d_1$. If this is true, then increase d_2 by one and let $d_1 = 0$. Otherwise, just increase d_1 by one. Let $B = \emptyset$, let $M = (m_{ij})$ be a matrix over k with s columns and zero rows, and let L be the set of all monomials in $k[x_0, x_1, y_0, y_1]$ of bidegree (d_1, d_2) which are not multiples of an element of $LT(G)$.*
4) *If $L = \emptyset$, continue wth step 2). Otherwise, choose $t = min(L)$ and remove it from L.*

5) *For* $i = 1, \ldots, s$, *compute* $t(p_i) = t(c_{i0}^{(1)}, c_{i1}^{(1)}, c_{i0}^{(2)}, c_{i1}^{(2)})$. *Reduce the vector* $(t(p_1), \ldots, t(p_s))$ *against the rows of* M *to obtain*

$$(v_1, \ldots, v_s) = (t(p_1), \ldots, t(p_s)) - \sum_i a_i(m_{i1}, \ldots, m_{is})$$

with $a_i \in k$.

6) *If* $(v_1, \ldots, v_s) = (0, \ldots, 0)$, *then append the polynomial* $t - \sum_i a_i b_i$ *to* G, *where* b_i *is the* i^{th} *element of the list* B. *Continue with step 4).*
7) *If* $(v_1, \ldots, v_s) \neq (0, \ldots, 0)$, *then add* $(v_1, \ldots, v_s)$ *as a new row to* M *and* $t - \sum_i a_i b_i$ *as a new element to* B. *Continue with step 4).*

Proof. The proof will use the same ideas from the proof of the Buchberger-Moeller algorithm for $\mathbb{P}^n$, Theorem 3.5. Let $I = I(X)$ and suppose we stop with $HF_S(i,j) = b_{i+1}$ for all $i \geq 0$ and $j \geq d_2'$ on some bidegree (d_1', d_2'). Just as in the Buchberger-Moeller algorithm for $\mathbb{P}^n$, we have that anything in G must also be in $I(X)$. Again, this implies $LT(G) \subset LT(I)$. To prove that the set G forms a Groebner basis for I, suppose $LT(G) \subsetneq LT(I)$ and we will get a contradiction as before. Pick a monomial $x^\alpha y^\beta \in LT(I) \setminus LT(G)$ of bidegree (D_1, D_2) with $D_1 \geq 0$ and $D_2 \geq d_2'$. This gives us $LT(G) \subsetneq LT(G) + \langle x^\alpha y^\beta \rangle \subset LT(I)$, so we have

$$\begin{aligned} HF_{R/LT(I)}(D_1, D_2) &\leq HF_{R/(LT(G)+\langle x^\alpha y^\beta \rangle)}(D_1, D_2) \\ &< HF_{R/LT(G)}(D_1, D_2) \\ &= b_{D_1+1} \\ &= HF_{R/LT(I)}(D_1, D_2) \end{aligned}$$

where $R = k[x_0, x_1, y_0, y_1]$, which is a contradiction.

To see that we get the reduced Groebner basis of I, note that if a monomial appearing in L, $x^\alpha y^\beta$, is found to be in $LT(G)$, then no multiples of it will appear in L again. Also note that it is not stored in the set B. Since the elements of G are formed from the elements of L and B, we know that $x^\alpha y^\beta$ will not be used to form another element of G since it is in neither L or B. Finally, we have that $x^\alpha y^\beta$ does not divide any monomials appearing in any element of G previously found because of the bidegrees.

Now we prove that the algorithm stops after finitely many steps. Just as with the Buchberger-Moeller algorithm for $\mathbb{P}^n$, if we enter any of steps 3),5),6), or 7), we must come back to step 4). We perform step 4) finitely many times before returning to step 2) because the set L is always finite. Step 1) is the set up step and is only done once, so we just need to show that step 2) is done finitely many times.

Each time we finish step 2), we enter step 3) and change the bidegree (d_1, d_2) to be a bidegree that we have not yet looked at. This is the only time we change our bidegree, so this means we have a unique bidegree for each time we enter step 2). Now we can prove step 2) is done finitely many times by proving that we only consider finitely many bidegrees. This will be done by showing that we only consider finitely many d_2 values, and for each fixed d_2, we look at finitely many values for d_1.

Note that after looking for minimal generators of $I(X)$ of bidegree (d_1, d_2), we will necessarily have already found all minimal generators of $I(X)$ of bidegree (i, j) with $i \leq d_1$ and $j \leq d_2$. Now for each fixed d_2, consider the minimal generators of $I(X)$ of bidegree (i, d_2) for some i, and let M_{d_2} be the maximal such i value. Now if we continue to increase d_1 and eventually reach a point where we look for generators of bidegree (M_{d_2}, d_2), then we will have found all minimal generators of I of bidegree (i, d_2) for each i and of bidegree (i, j) for all $i \leq M_{d_2}$ and $j \leq d_2$. With these generators in the set G, we have $HF_S(i, d_2) = H_X(i, d_2)$ for all $i \geq M_{d_2}$. By Theorem 4.20, we have that $H_X(i, d_2) = a_{d_2+1}$ for all $i \geq h - 1$. Together, this gives us that for all $i \geq max\{M_{d_2}, h - 1\}$, we have

$$HF_S(i, d_2) = H_X(i, d_2) = a_{d_2+1}.$$

Now for $d_1 = max\{M_{d_2}, h - 1\}$, the criterion in step 3) is satisfied and allows us to move on to the next d_2 value.

Now we need to prove that we only consider finitely many d_2 values for the bidegrees (d_1, d_2). There are finitely many minimal generators of I, so there must exist some number N such that for any bidegree (i, j) of a minimal generator of I, we have $j \leq N$. That is, there are no minimal generators of I of bidegree (i, j) with $j > N$ for N large enough. This implies that if we increase d_2 to N, then after increasing d_1 to $max\{M_N, h-1\}$, we will have found all generators of I. This gives $HF_S(i, j) = H_X(i, j)$ for all $i \geq d_1 = max\{M_N, h-1\}$ and $j \geq d_2 = N$. We have $H_X(i, j) = s$ for all $i \geq h - 1$ and $j \geq v - 1$ by Theorem 4.20. Altogether we get

$$HF_S(i, j) = H_X(i, j) = s$$

for all $i \geq max\{M_N, h - 1\}$ and $j \geq max\{N, v - 1\}$. Now we see that the criterion in step 2) must be met before $d_2 > max\{N, v - 1\}$, so the algorithm must stop while $d_2 \leq max\{N, v - 1\}$. This finishes the proof that we only look for generators of I of finitely many different bidegrees, which means that step 2) is entered finitely many times. This completes the proof that the algorithm stops after finitely many steps because we have that each step is performed finitely many times. □

Example 5.2. Let $k = \mathbb{R}$ and $X = \{p_1, \ldots, p_4\} \subset \mathbb{P}^1 \times \mathbb{P}^1$, where $p_1 = [1 : 1] \times [1 : 0]$, $p_2 = [1 : 2] \times [1 : 0]$, $p_3 = [1 : 2] \times [1 : 2]$, $p_4 = [0 : 1] \times [1 : 2]$. Note that X is not ACM, so we can not use Theorem 4.24. Instead, we will use the Buchberger-Moeller algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$ to compute the reduced Groebner basis of $I(X)$ with respect to the graded reverse lexicographic order. We first find $\alpha_X = (2, 1, 1)$ and $\beta_X = (2, 2)$, then get $\alpha^*_X = (3, 1)$ and $\beta^*_X = (2, 2)$. From this we get $a_1 = 3$ and $a_i = 4$ for all $i \geq 2$, and $b_1 = 2$ and $b_j = 4$ for all $i \geq 2$.

1) Let $G = \emptyset$, $B = \emptyset$, $(d_1, d_2) = (0, 0)$, and $M \in Mat_{0,4}(\mathbb{R})$.
2) We have $HF_S(d_1, d_2) = 1$, so the stopping condition is not satisfied.
3) We have $HF_S(d_1, d_2) = 1$, so the condition is not satisfied. Let $d_1 = 1$, $B = \emptyset$, $M \in Mat_{0,4}(\mathbb{R})$, and $L = \{x_0, x_1\}$.

4) Set $t = x_1$ and let $L = \{x_0\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 2, 2, 1) = (v_1, \ldots, v_4)$.
7) Let $M = \begin{bmatrix} 1 & 2 & 2 & 1 \end{bmatrix}$ and $B = \{x_1\}$.
4) Set $t = x_0$ and let $L = \emptyset$
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 1, 1, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, -1, -1, -1)$.
7) Let $M = \begin{bmatrix} 1 & 2 & 2 & 1 \\ 0 & -1 & -1 & -1 \end{bmatrix}$ and $B = \{x_1, x_0\}$.
2) We have $HF_S(2, d_2) = 3$, so the stopping condition is not satisfied.
3) We have $HF_S(2, d_2) = 3$, so the condition is not satisfied. Let $d_1 = 2$, $B = \emptyset$, $M \in Mat_{0,4}(\mathbb{R})$, and $L = \{x_0^2, x_0x_1, x_1^2\}$.
4) Set $t = x_1^2$ and let $L = \{x_0^2, x_0x_1\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 4, 4, 1) = (v_1, \ldots, v_4)$.
7) Let $M = \begin{bmatrix} 1 & 4 & 4 & 1 \end{bmatrix}$ and $B = \{x_1^2\}$.
4) Set $t = x_0x_1$ and let $L = \{x_0^2\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 2, 2, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, -2, -2, -1)$.
7) Let $M = \begin{bmatrix} 1 & 4 & 4 & 1 \\ 0 & -2 & -2 & -1 \end{bmatrix}$ and $B = \{x_1^2, x_0x_1 - x_1^2\}$.
4) Set $t = x_0^2$ and let $L = \emptyset$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 1, 1, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, 0, 0, -5/2)$.
7) Let $M = \begin{bmatrix} 1 & 4 & 4 & 1 \\ 0 & -2 & -2 & -1 \\ 0 & 0 & 0 & -5/2 \end{bmatrix}$ and $B = \{x_1^2, x_0x_1 - x_1^2, x_0^2 - 3/2x_0x_1 + 1/2x_1^2\}$.
2) We have $HF_S(d_1, d_2) = 3$, so the stopping condition is not satisfied.
3) We have $HF_S(d_1, d_2) = 3$, so the condition is not satisfied. Let $d_1 = 3$, $B = \emptyset$, $M \in Mat_{0,4}(\mathbb{R})$, and $L = \{x_0^3, x_0^2x_1, x_0x_1^2, x_1^3\}$.
4) Set $t = x_1^3$ and let $L = \{x_0^3, x_0^2x_1, x_0x_1^2\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 8, 8, 1) = (v_1, \ldots, v_4)$.
7) Let $M = \begin{bmatrix} 1 & 8 & 8 & 1 \end{bmatrix}$ and $B = \{x_1^3\}$.
4) Set $t = x_0x_1^2$ and let $L = \{x_0^3, x_0^2x_1\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 4, 4, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, -4, -4, -1)$.
7) Let $M = \begin{bmatrix} 1 & 8 & 8 & 1 \\ 0 & -4 & -4 & -1 \end{bmatrix}$ and $B = \{x_1^3, x_0x_1^2 - x_1^3\}$.
4) Set $t = x_0^2x_1$ and let $L = \{x_0^3\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 2, 2, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, 0, 0, 1/2)$.
7) Let $M = \begin{bmatrix} 1 & 8 & 8 & 1 \\ 0 & -4 & -4 & -1 \\ 0 & 0 & 0 & 1/2 \end{bmatrix}$ and $B = \{x_1^3, x_0x_1^2 - x_1^3, x_0^2x_1 - 3/2x_0x_1^2 + 1/2x_1^3\}$.

4) Set $t = x_0^3$ and let $L = \emptyset$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 1, 1, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, 0, 0, 0)$.
6) Let $G = \{x_0^3 - 3/2x_0^2x_1 + 1/2x_0x_1^2\}$.
2) We have $HF_S(d_1, d_2) = 3$, so the stopping condition is not satisfied.
3) We have $HF_S(i, d_2) = a_{d_2+1}$ for all $i \geq d_1$, so let $d_2 = 1$, $d_1 = 0$, $B = \emptyset$, $M \in Mat_{0,4}(\mathbb{R})$, and $L = \{y_0, y_1\}$.
4) Set $t = y_1$ and let $L = \{y_0\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (0, 0, 2, 2) = (v_1, \ldots, v_4)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 2 & 2 \end{bmatrix}$ and $B = \{y_1\}$.
4) Set $t = y_0$ and let $L = \emptyset$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 1, 1, 1)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (1, 1, 0, 0)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 2 & 2 \\ 1 & 1 & 0 & 0 \end{bmatrix}$ and $B = \{y_1, y_0 - 1/2y_1\}$.
2) We have $HF_S(2, d_2) = 6$, so the stopping condition is not satisfied.
3) We have $HF_S(2, d_2) = 6$, so the condition is not satisfied. Let $d_1 = 1$, $B = \emptyset$, $M \in Mat_{0,4}(\mathbb{R})$, and $L = \{x_0y_0, x_1y_0, x_0y_1, x_1y_1\}$.
4) Set $t = x_1y_1$ and let $L = \{x_0y_0, x_1y_0, x_0y_1\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (0, 0, 4, 2) = (v_1, \ldots, v_4)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 4 & 2 \end{bmatrix}$ and $B = \{x_1y_1\}$.
4) Set $t = x_0y_1$ and let $L = \{x_0y_0, x_1y_0\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (0, 0, 2, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, 0, 0, -1)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & -1 \end{bmatrix}$ and $B = \{x_1y_1, x_0y_1 - 1/2x_1y_1\}$.
4) Set $t = x_1y_0$ and let $L = \{x_0y_0\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 2, 2, 1)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (1, 2, 0, 0)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & -1 \\ 1 & 2 & 0 & 0 \end{bmatrix}$ and $B = \{x_1y_1, x_0y_1 - 1/2x_1y_1, x_1y_0 - 1/2x_1y_1\}$.
4) Set $t = x_0y_0$ and let $L = \emptyset$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 1, 1, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, -1, 0, 0)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & -1 \\ 1 & 2 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}$ and $B = \{x_1y_1, x_0y_1 - 1/2x_1y_1, x_1y_0 - 1/2x_1y_1, x_0y_0 - x_1y_0 - 1/2x_0y_1 + 1/2x_1y_1\}$.
2) We have $HF_S(2, d_2) = 6$, so the stopping condition is not satisfied.

3) We have $HF_S(2, d_2) = 6$, so the condition is not satisfied. Let $d_1 = 2$, $B = \emptyset$, $M \in Mat_{0,4}(\mathbb{R})$, and $L = \{x_0^2y_0, x_0x_1y_0, x_1^2y_0, x_0^2y_1, x_0x_1y_1, x_1^2y_1\}$.
4) Set $t = x_1^2y_1$ and let $L = \{x_0^2y_0, x_0x_1y_0, x_1^2y_0, x_0^2y_1, x_0x_1y_1\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (0, 0, 8, 2) = (v_1, \ldots, v_4)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 8 & 2 \end{bmatrix}$ and $B = \{x_1^2y_1\}$.
4) Set $t = x_0x_1y_1$ and let $L = \{x_0^2y_0, x_0x_1y_0, x_1^2y_0, x_0^2y_1\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (0, 0, 4, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, 0, 0, -1)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 8 & 2 \\ 0 & 0 & 0 & -1 \end{bmatrix}$ and $B = \{x_1^2y_1, x_0x_1y_1 - 1/2x_1^2y_1\}$.
4) Set $t = x_0^2y_1$ and let $L = \{x_0^2y_0, x_0x_1y_0, x_1^2y_0\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (0, 0, 2, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, 0, 0, 0)$.
6) Let $G = \{x_0^3 - 3/2x_0^2x_1 + 1/2x_0x_1^2, x_0^2y_1 + 1/2x_0x_1y_1 - 1/2x_1^2y_1\}$.
4) Set $t = x_1^2y_0$ and let $L = \{x_0^2y_0, x_0x_1y_0\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 4, 4, 1)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (1, 4, 0, 0)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 8 & 2 \\ 0 & 0 & 0 & -1 \\ 1 & 4 & 0 & 0 \end{bmatrix}$ and $B = \{x_1^2y_1, x_0x_1y_1 - 1/2x_1^2y_1, x_1^2y_0 - 1/2x_1^2y_1\}$.
4) Set $t = x_0x_1y_0$ and let $L = \{x_0^2y_0\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 2, 2, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, -2, 0, 0)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 8 & 2 \\ 0 & 0 & 0 & -1 \\ 1 & 4 & 0 & 0 \\ 0 & -2 & 0 & 0 \end{bmatrix}$ and $B = \{x_1^2y_1, x_0x_1y_1 - 1/2x_1^2y_1, x_1^2y_0 - 1/2x_1^2y_1, x_0x_1y_0 - x_1^2y_0 - 1/2x_0x_1y_1 + 1/2x_1^2y_1\}$.
4) Set $t = x_0^2y_0$ and let $L = \emptyset$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 1, 1, 0)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, 0, 0, 0)$.
6) Let $G = \{x_0^3 - 3/2x_0^2x_1 + 1/2x_0x_1^2, x_0^2y_1 + 1/2x_0x_1y_1 - 1/2x_1^2y_1, x_0^2y_0 - 3/2x_0x_1y_0 + 1/2x_1^2y_0 + 1/2x_0x_1y_1 - 1/4x_1^2y_1\}$.
2) We have $HF_S(d_1, 2) = 6$, so the stopping condition is not satisfied.
3) We have $HF_S(i, d_2) = a_{d_2+1}$ for all $i \geq d_1$, so let $d_2 = 2$, $d_1 = 0$, $B = \emptyset$, $M \in Mat_{0,4}(\mathbb{R})$, and $L = \{y_0^2, y_0y_1, y_1^2\}$.
4) Set $t = y_1^2$ and let $L = \{y_0^2, y_0y_1\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (0, 0, 4, 4) = (v_1, \ldots, v_4)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 4 & 4 \end{bmatrix}$ and $B = \{y_1^2\}$.
4) Set $t = y_0y_1$ and let $L = \{y_0^2\}$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (0, 0, 2, 2)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (0, 0, 0, 0)$.

6) Let $G = \{x_0^3 - 3/2x_0^2x_1 + 1/2x_0x_1^2, x_0^2y_1 + 1/2x_0x_1y_1 - 1/2x_1^2y_1, x_0^2y_0 - 3/2x_0x_1y_0 + 1/2x_1^2y_0 + 1/2x_0x_1y_1 - 1/4x_1^2y_1, y_0y_1 - 1/2y_1^2\}$.
4) Set $t = y_0^2$ and let $L = \emptyset$.
5) Compute $(t(p_1), \ldots, t(p_4)) = (1, 1, 1, 1)$ and reduce it against the rows of M to get $(v_1, \ldots, v_4) = (1, 1, 0, 0)$.
7) Let $M = \begin{bmatrix} 0 & 0 & 4 & 4 \\ 1 & 1 & 0 & 0 \end{bmatrix}$ and $B = \{y_1^2, y_0^2 - 1/4y_1^2\}$.
2) We now have $LT(G) = \langle x_0^3, x_0^2y_1, x_0^2y_0, y_0y_1 \rangle$. This implies that $\{y_0^j, y_1^j\}$ is a k-basis for $S_{(0,j)}$ and $\{x_0x_1^{i-1}y_0^j, x_1^iy_0^j, x_0x_1^{i-1}y_1^j, x_1^iy_1^j\}$ is a k-basis for $S_{(i,j)}$ for $i \geq 1$ and $j \geq 2$. This gives $HF_S(0, j) = 2$ and $HF_S(i, j) = 4$ for all $i \geq 1$ and $j \geq 2$. Now for all $i \geq 0$ and $j \geq 2$ we have

$$HF_S(i, j) = b_{i+1}.$$

At this point we stop and we get that

$$G = \{x_0^3 - 3/2x_0^2x_1 + 1/2x_0x_1^2, x_0^2y_1 + 1/2x_0x_1y_1 - 1/2x_1^2y_1,$$
$$x_0^2y_0 - 3/2x_0x_1y_0 + 1/2x_1^2y_0 + 1/2x_0x_1y_1 - 1/4x_1^2y_1, y_0y_1 - 1/2y_1^2\}$$

is the reduced Groebner basis for $I(X)$ under the graded reverse lexicographic order.

2. Future Directions

We still need to compare this algorithm to the standard Buchberger method. We will leave this as an open problem, although we will discuss the comparison to the alternative method. The alternative method of getting this result for a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$, say $X = \{p_1, \ldots, p_s\}$, starts with taking the intersection of the ideals $I(\{p_i\})$. After that, we get a set of generators for $I(X)$, but we need to use Buchberger's criterion. Checking this criterion is significantly more tedious to compute for more generators, so this process can take a long time. However, the Buchberger-Moeller algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$ mainly involves linear algebra and computing Hilbert functions. These computations should be easier than the computations involved in Buchberger's criterion.

It may be possible to further extend this algorithm to compute the reduced Groebner basis for a finite set of points in $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_k}$. A similar idea to the Buchberger-Moeller algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$ could be used with a different stopping condition, but this has yet to be determined. We looked at results obtained by A. Van Tuyl in [7] about the Hilbert function of a finite set of points in $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_k}$, and it is possible that these results could provide sufficient stopping conditions.

In conclusion, we leave some questions that need to be studied further. Is the Buchberger-Moeller algorithm for $\mathbb{P}^1 \times \mathbb{P}^1$ more efficient than other known methods of finding the reduced Groebner basis for the defining ideal of a finite set of points in $\mathbb{P}^1 \times \mathbb{P}^1$? Can we find even more efficient method of doing this? Lastly, can the Buchberger-Moeller algorithm be extended to arbitrary multiprojective spaces? We hope that the ideas presented in this project will help to find answers for these questions.

Bibliography

[1] B. Buchberger, H.M. Moeller, *The construction of multivariate polynomials with preassigned zeros.* In: Calmet J. (eds) Computer Algebra. EUROCAM 1982. Lecture Notes in Computer Science, vol 144. Springer, Berlin, Heidelberg, 1982.

[2] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* New York: Springer-Verlag, 1992.

[3] R. Froeberg, *An Introduction to Grobner Bases.* Chichester: Wiley, 1998.

[4] E. Guardo, A. Van Tuyl, *Arithmetically Cohen-Macaulay Sets of Points in* $\mathbb{P}^1 \times \mathbb{P}^1$. Cham: Springer, 2015.

[5] B. Hassett, *Introduction to Algebraic Geometry.* Cambridge: Cambridge UP, 2012.

[6] M. Kreuzer, L. Robbiano, *Computational Commutative Algebra 2.* Berlin: Springer, 2005.

[7] A. Van Tuyl, *The border of the Hilbert function of a set of points in* $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_k}$. J. Pure Appl. Algebra, 176, pp. 223-247, 2002.