

ON SOME COMPUTATIONAL PROBLEMS IN ALGEBRAIC GEOMETRY

by

VELİ ÇAY

THESIS SUBMITTED TO  
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES  
OF  
THE ABANT İZZET BAYSAL UNIVERSITY  
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE  
OF  
MASTER OF SCIENCE  
IN  
THE DEPARTMENT OF MATHEMATICS

august 2007

Approval of the Graduate School of Natural and Applied Sciences.

---

Prof.Dr. Nihat ÇELEBİ

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

---

Associate Prof. Cenap Özel

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality as a thesis for the degree of Master of Science.

---

Assistant Prof. Erol Yılmaz

Supervisor

Examining Committee Members

Associate Prof. Cenap Özel

Assistant Prof. Gürsel Yeşilot

Assistant Prof. Erol Yılmaz

## **ABSTRACT**

On Some Computational Problems in Algebraic Geometry

Çay, Veli

Master, Department of Mathematics

Supervisor: Assistant Prof. Erol Yılmaz

august 2007, 39 pages

A method for computing a basis of syzygy module for a given generating set of a homogeneous ideal of polynomial ring is introduced. This method, unlike the common way to compute syzygy basis, do not involve a computation of Gröbner basis. The only linear algebraic techniques are used in this method. The new developed method of computing syzygy module and a property of leading forms of polynomials of a generating set of an polynomial ideal suggests an alternative algorithm for computing H-basis of the ideal.

Keywords:H-Bases, Gröbner Bases, Syzygies, Polynomial Ideals, Hilbert Functions

## ÖZET

Cebirsel Geometride Bazı Hesaplamalı Problemler Üzerine

Çay, Veli

Master Tezi, Matematik Bölümü

Tez Yöneticisi: Yrd.Doç.Dr. Erol Yılmaz

ağustos 2007, 39 sayfa

Polinom halkasında homojen bir idealin üreteç kümesinin syzygy (çekirdek) modülünün tabanının hesabı için bir metod geliştirildi. Bu metod, bilinen klasik yöntemin aksine, Gröbner taban hesabı içermemektedir. Bu yeni metodta sadece doğrusal cebir teknikleri kullanılmıştır. Ayrıca bu yeni geliştirilen metod ve polinom halkasındaki bir idealin üreteçlerinin öncü formlarının bir özelliği yardımıyla bir polinom idealinin H-tabanını hesaplamak için alternatif bir algoritma önerilmiştir.

Anahtar Kelimeler: Homojen Tabanlar, Gröbner Tabanlar, Syzygies, Polinom idealer, Hilbert Fonksiyonu

## **ACKNOWLEDGEMENTS**

I would like to acknowledge my indebtedness to my supervisor Associate Prof. Erol Yılmaz who has guided, encouraged and believed in me throughout this thesis. I strongly believe that I will feel his influence over the entire course of my mathematical life. I am grateful to him for a critical reading of my solutions and valuable suggestions in correcting my errors. I also like to thank to the other members of my Committee, Associate Prof. Cenap Özel and Assistant Prof. Gürsel Yeşilot for their assistance.

Finally, I would like to thank to my family for their unvanishing support and encouragement.

*To My Family*

## TABLE OF CONTENTS

ABSTRACT . . . . .	iii
ÖZET . . . . .	iv
ACKNOWLEDGEMENTS . . . . .	v
1 BASIC CONCEPTS AND DEFINITIONS	1
1.1 Gröbner Basis for Polynomial Ideals . . . . .	1
1.2 Syzygy Modules . . . . .	8
1.3 Hilbert Function and Hilbert Polynomial . . . . .	12
2 COMPUTATION OF SYZYGY BASIS OF HOMOGENEOUS IDEALS USING LINEAR ALGEBRA	15
2.1 Introduction . . . . .	15
2.2 Vector Spaces Concerning Homogeneous Ideals . . . . .	15
2.3 An Algorithm to Compute Syzygy Basis of Homogenous Polynomials	19
3 H-BASIS (HOMOGENEOUS BASIS) ALGORITHM	30
3.1 Introduction . . . . .	30
3.2 Background . . . . .	31
3.3 Homogeneous Basis . . . . .	33
3.4 Computation of H-Bases . . . . .	36

# CHAPTER 1

## BASIC CONCEPTS AND DEFINITIONS

In this chapter we give a number of definitions and theorems used in the subsequent parts of the thesis. More detail can be found in [1],[2] and[3].

### 1.1 Gröbner Basis for Polynomial Ideals

Let  $k[x_1, \dots, x_n]$  be the ring of the polynomials over a field  $k$ .

**Definition 1.1** A monomial in  $x_1, \dots, x_n$  is a product of the form

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

*The total degree of this monomial is the sum  $\alpha_1 + \cdots + \alpha_n$ .*

*For brevity, let  $x = (x_1, \dots, x_n)$  and  $\alpha = (\alpha_1, \dots, \alpha_n)$ . Then the monomial can be written as  $x^\alpha$ . We also let  $|\alpha| = \alpha_1 + \cdots + \alpha_n$  denote the total degree of the monomial  $x^\alpha$ .*

**Definition 1.2** A polynomial  $f$  is a finite linear combination of monomials with coefficients in a field  $k$ . A polynomial,  $f$ , will be written in the form

$$f = \sum_{\alpha} \mathbf{a}_{\alpha} x^{\alpha},$$

*where the sum is over a finite number of  $n$ -tuples  $\alpha = (\alpha_1, \dots, \alpha_n)$  and  $\mathbf{a}_{\alpha} \in k - \{0\}$ .*

*The total degree of  $f$ , denoted  $\deg(f)$ , is the maximum  $|\alpha| = \alpha_1 + \cdots + \alpha_n$  in the expression of  $f$ .*

Given a collection of polynomials,  $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ , we can consider all polynomials which can be written as a linear combination of these polynomials.

**Definition 1.3** Let  $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ . We let  $\langle f_1, \dots, f_s \rangle$  denote the collection

$$\langle f_1, \dots, f_s \rangle = \{a_1 f_1 + \dots + a_s f_s : a_i \in k[x_1, \dots, x_n], 1 \leq i \leq s\}.$$

It is easy to show that  $\langle f_1, \dots, f_s \rangle$  is an ideal of  $k[x_1, \dots, x_n]$  and is called ideal generated by  $f_1, \dots, f_s$ .

The well-known Hilbert Basis Theorem states that every ideal of  $k[x_1, \dots, x_n]$  is finitely generated.

**Definition 1.4** We will call the set  $k^n = \{(a_1, \dots, a_n) : a_1, \dots, a_n \in k\}$  the affine  $n$ -dimensional space over  $k$ .

**Definition 1.5** (i) Let  $I = \langle f_1, \dots, f_s \rangle$  be an ideal in  $k[x_1, \dots, x_n]$ . The set of zero locus of polynomials of  $I$ ,

$$V(I) = \{(a_1, \dots, a_n) : f_i(a_1, \dots, a_n) = 0, 1 \leq i \leq s\} \subset k^n$$

is called variety of ideal  $I$ .

(ii) Let  $V \subset k^n$  be a variety. The collection of polynomials

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

is called ideal of the variety  $V$ .

We always have  $V(I(V)) = V$ , but  $I(V(I)) = \sqrt{I}$  if  $k$  is algebraically closed by Strong Nullstellensatz.

**Definition 1.6** A monomial ordering on  $k[x_1, \dots, x_n]$  is any relation  $>$  on  $\mathbb{Z}_{\geq 0}^n$  or equivalently, any relation on the set of the monomials  $x^\alpha$ ,  $\alpha \in \mathbb{Z}_{\geq 0}^n$  satisfying:

(i)  $>$  is a total ordering on  $\mathbb{Z}_{\geq 0}^n$ .

(ii) If  $\alpha > \beta$  and  $\gamma \in \mathbb{Z}_{\geq 0}^n$ , then  $\alpha + \gamma > \beta + \gamma$ .

(iii)  $>$  is a well-ordering on  $\mathbb{Z}_{\geq 0}^n$ . This means that every nonempty subset of  $\mathbb{Z}_{\geq 0}^n$  has a smallest element under  $>$ .

**Definition 1.7** A monomial ordering  $>$  in  $k[x_1, x_2, \dots, x_n]$  is called a graded monomial ordering if  $x^\alpha > x^\beta$  whenever  $|\alpha| > |\beta|$ .

Now, we will define the most used monomial orderings. Notice that the last two orderings are graded orderings.

**Definition 1.8** Let  $x^\alpha$  and  $x^\beta$  be monomials in  $k[x_1, \dots, x_n]$

(i) *Lexicographic Order:* We say  $x^\alpha >_{\text{lex}} x^\beta$  if in the difference  $\alpha - \beta \in \mathbb{Z}^n$ , the left-most nonzero entry is positive.

(ii) *Graded Lexicographic Order:* We say  $x^\alpha >_{\text{grlex}} x^\beta$  if  $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$ , or  $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$  and  $x^\alpha >_{\text{lex}} x^\beta$ .

(iii) *Graded Reverse Lexicographic Order:* We say  $x^\alpha >_{\text{grevlex}} x^\beta$  if  $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$ , or in the difference  $\alpha - \beta \in \mathbb{Z}^n$ , the right-most nonzero entry is negative.

For example;  $x^3y^2z^4 >_{\text{lex}} x^3y^2z$ , since  $(3, 2, 4) - (3, 2, 1) = (0, 0, 3)$  the left-most nonzero entry is positive, and  $x^2y^2z^2 >_{\text{grlex}} xy^4z$  since  $2 + 2 + 2 = 1 + 1 + 4$  but  $(2, 2, 2) - (1, 4, 1) = (1, -2, 1)$ , the left-most nonzero entry is positive. However,  $x^2y^2z^2 <_{\text{grevlex}} xy^4z$  since  $2 + 2 + 2 = 1 + 1 + 4$  but  $(1, 4, 1) - (2, 2, 2) = (-1, 2, -1)$ , the right-most nonzero entry is negative.

**Definition 1.9** Let  $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$  be a nonzero polynomial in  $k[x_1, x_2, \dots, x_n]$  and let  $>$  be a monomial order.

(i) *The multidegree of  $f$  is*

$$\text{multideg}(f) = \max(\alpha \in \mathbf{Z}_{\geq 0}^n : a_{\alpha} \neq 0)$$

*the maximum is taken with respect to  $>$ .*

(ii) *The leading monomial coefficient of  $f$  is*

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

(iii) The leading monomial of  $f$  is

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

(iv) The leading term of  $f$  is

$$\text{LT}(f) = \text{LC}(f)\text{LM}(f).$$

To illustrate, let  $f = 4xyz + 4z^2 - 5x^3 + 7x^2z^2$ . If our order is lexicographic order,  $\text{multideg}(f) = (3, 0, 0)$ ,  $\text{LC}(f) = -5$ ,  $\text{LM}(f) = x^3$  and  $\text{LT}(f) = -5x^3$ . If we choose graded lexicographic order,  $\text{multideg}(f) = (2, 0, 2)$ ,  $\text{LC}(f) = 7$ ,  $\text{LM}(f) = x^2z^2$  and  $\text{LT}(f) = 7x^2z^2$ .

The following is the well-known division algorithm on  $k[x_1, \dots, x_n]$ .

**Theorem 1.10** Fix a monomial order  $>$ , and let  $F = (f_1, \dots, f_s)$  be an ordered  $s$ -tuple of polynomials in  $k[x_1, \dots, x_n]$ . Then every  $f \in k[x_1, \dots, x_n]$  can be written as

$$f = a_1f_1 + \dots + a_sf_s + r,$$

where  $a_i, r \in k[x_1, x_2, \dots, x_n]$ , and either  $r = 0$  or  $r$  is a  $k$ -linear combination of monomials, none of which is divisible by any  $\text{LT}(f_1), \dots, \text{LT}(f_s)$ .  $r$  is called remainder of  $f$  on division by  $F$ . Furthermore, if  $a_if_i \neq 0$ , then

$$\text{multideg}(f) \geq \text{multideg}(a_if_i)$$

Since we now have a division algorithm in  $k[x_1, \dots, x_n]$  that seems to have many of the same features as the one-variable version, it is natural to ask if deciding whether a given  $f \in k[x_1, \dots, x_n]$  is a member of a given ideal  $I = \langle f_1, \dots, f_s \rangle$  can be done by computing the remainder on division. One direction is easy. Namely, if the remainder  $r = 0$  on dividing by  $(f_1, \dots, f_s)$ , then  $f = a_1f_1 + \dots + a_sf_s$ . By definition then,  $f \in \langle f_1, \dots, f_s \rangle$ . On the other hand, the following example shows that we are not guaranteed to get remainder  $r = 0$  for every  $f \in \langle f_1, \dots, f_s \rangle$ .

$$p = x^2 + \frac{1}{2}y^2z - z - 1 = \left(-\frac{1}{2}z + 1\right)(x^2 + z^2 - 1) + \frac{1}{2}z(x^2 + y^2 + (z - 1)^2 - 4)$$

shows  $p \in \langle f_1 = x^2 + z^2 - 1, f_2 = x^2 + y^2 + (z - 1)^2 - 4 \rangle$ . However the remainder on division of  $f$  by  $(f_1, f_2)$  is not zero. For instance, using lexicographic order, we get

$$p = 1f_1 + 0f_2 + \frac{1}{2}y^2z - z^2 - z$$

or

$$p = 0f_1 + 1f_2 + \frac{1}{2}y^2z - y^2 - z^2 + z + 2$$

The remainder is not zero because it contains terms that cannot be removed by division by this particular generators for  $I$ . The leading terms of  $f_1 = x^2 + z^2 - 1$  and  $f_2 = x^2 + y^2 + (z - 1)^2 - 4$  are any term of the remainder. In order for division to produce zero remainders for all elements of  $I$ , we need to be able to remove all leading terms of elements of  $I$  using leading terms of the divisors. That is the motivation for the following definition.

**Definition 1.11** Fix a monomial ordering. A finite subset  $G = \{g_1, \dots, g_s\}$  of an ideal  $I$  is said to be a Gröbner Basis if for every nonzero  $f \in I$ ,  $\text{LT}(f)$  is divisible by  $\text{LT}(g_i)$  for some  $i$ .

A Gröbner basis for  $I$  is indeed a generating set for  $I$ . Existence of Gröbner basis for an arbitrary ideal is an easy consequence of Hilbert Basis theorem. Moreover, remainders computed by division with respect to a Gröbner basis are much better behaved than those computed with respect to arbitrary sets of divisors.

**Theorem 1.12** If  $G = \{g_1, \dots, g_s\}$  is a Gröbner basis for  $I$ , then for any  $f \in I$ , the remainder on division  $f$  by  $G$  is zero.

More useful for many purposes than the existence proof for Gröbner bases is an algorithm, due to Buchberger, that takes an arbitrary generating set  $\{f_1, \dots, f_s\}$  for  $I$

and produce a Gröbner basis  $G$  for  $I$  from it. This algorithm works by forming new elements of  $I$  using expressions guaranteed to cancel leading terms and uncover other possible leading terms.

**Definition 1.13** *Let  $f, g \in k[x_1, x_2, \dots, x_n]$  be nonzero polynomials.*

(i) *If  $\text{multideg}(f) = \alpha$  and  $\text{multideg}(g) = \beta$ , then let  $\gamma = (\gamma_1, \dots, \gamma_n)$  where  $\gamma_i = \max(\alpha_i, \beta_i)$  for each  $i$ .  $x^\gamma$  is called the least common multiple of  $\text{LM}(f)$  and  $\text{LM}(g)$ , written as  $x^\gamma = \text{LCM}(\text{LM}(f), \text{LM}(g))$ .*

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

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

For example; let  $f = x^3y^2 - x^2y^3 + x$  and  $g = 3x^4y + y^2$  in  $[x, y]$  with the grlex order. Then  $\gamma = (4, 2)$  and

$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3y^2}f - \frac{x^4y^2}{3x^4y}g \\ &= xf - (1/3)yg \\ &= -x^3y^3 + x^2 - (1/3)y^3. \end{aligned}$$

The next theorem gives a criterion for when a basis of an ideal is a Gröbner basis.

**Theorem 1.14** *Let  $I$  be a polynomial ideal. Then a basis  $G = \{g_1, \dots, g_t\}$  for  $I$  Gröbner basis for  $I$  if and only if for all pairs  $i \neq j$ , the remainder on division of  $S(g_i, g_j)$  by  $G$  (listed in some order) is zero.*

Using this criterion above, Buchberger's Algorithm computes a Gröbner basis for an ideal  $I$  from a given basis of that ideal.

**Algorithm 1.15** *Let  $I = \langle f_1, \dots, f_s \rangle$  be a polynomial ideal. Then a Gröbner basis for  $I$  can be constructed in a finite steps by the following algorithm:*

*INPUT:  $F = \langle f_1, \dots, f_s \rangle \subset k[x_1, \dots, x_n]$  with  $f_i \neq 0 (1 \leq i \leq s)$*

*OUTPUT:  $G = \{g_1, \dots, g_t\}$ , a Gröbner basis for  $\langle f_1, \dots, f_s \rangle$*

*INITIALIZATION:*  $G := F, \mathcal{G} := \{(f_i, f_j) | f_i \neq f_j \in G\}$

*Fix a monomial order.*

*WHILE*  $\mathcal{G} \neq \emptyset$  *DO*

*Choose any*  $(f, g) \in \mathcal{G}$

$\mathcal{G} := \mathcal{G} - \{(f, g)\}$

$h := \overline{S(f, g)}^G$

*IF*  $h \neq 0$  *THEN*

$\mathcal{G} := \mathcal{G} \cup \{(u, h) | \text{for all } u \in \mathcal{G}\}$

$G := G \cup \{h\},$

*where*  $\overline{S(f, g)}^G$  *is remainder on division of*  $S(f, g)$  *by*  $G$ .

*Return*  $G$

For example; Consider  $k[x, y]$  with grlex order, and let  $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$ . Recall that  $\{f_1, f_2\}$  is not a Gröbner basis for  $I$  since  $LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2) \rangle$ . To produce a Gröbner basis, one natural idea is to try first to extend the original generating set to a Gröbner basis by adding more polynomials in  $I$ . We have  $S(f_1, f_2) = -x^2 \in I$ , and its remainder on division by  $F = (f_1, f_2)$  is  $-x^2$  which is nonzero. Hence, we should include that remainder in our generating set, as a new generator  $f_3 = -x^2$ . If we set  $F(f_1, f_2, f_3)$ , we can use Theorem 1.14 to test if this new set is a Gröbner basis for  $I$ . We compute

$$\begin{aligned} S(f_1, f_2) &= f_3, \text{ so} \\ \overline{S(f_1, f_2)}^F &= 0, \\ S(f_1, f_3) &= (x^3 - 2xy) - (-x)(-x^2) = -2xy. \text{ but} \\ \overline{S(f_1, f_3)}^F &= -2xy \neq 0. \end{aligned}$$

Hence, we must add  $f_4 = -2xy$  to our generating set. If we let  $F = (f_1, f_2, f_3, f_4)$ . then

$$\begin{aligned} \overline{S(f_1, f_2)}^F &= \overline{S(f_1, f_3)}^F = 0, \\ S(f_1, f_4) &= y(x^3 - 2xy) - (-1/2)x^2(-2xy) = -2xy^2 = yf_4, \text{ so} \\ \overline{S(f_1, f_4)}^F &= 0. \\ S(f_2, f_3) &= (x^2y - 2y^2 + x) - (-y)(-x^2) = 2y^2 + x, \text{ but} \end{aligned}$$

$$\overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0.$$

Thus, we must also add  $f_5 = -2y^2 + x$  to our generating set. Setting  $F = (f_1, f_2, f_3, f_4, f_5)$ , one can compute that

$$\overline{S(f_i, f_j)}^F = 0 \text{ for all } 1 \leq i < j \leq 5.$$

It follows that a Gröbner basis for  $I$  is given by

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

## 1.2 Syzygy Modules

**Definition 1.16** A module over a ring  $R$  (or  $R$ -module) is a set  $M$  together with a binary operation, usually written as addition of  $R$  on  $M$ , and an operation of  $R$  on  $M$ , called scalar multiplication, satisfying properties.

- a.  $M$  is an Abelian group under addition.
- b. For all  $a \in R$  and all  $f, g \in M$ ,  $a(f + g) = af + ag$ .
- c. For all  $a, b \in R$  and all  $f \in M$ ,  $(a + b)f = af + bf$ .
- d. For all  $a, b \in R$  and all  $f \in M$ ,  $(ab)f = a(bf)$ .
- e. If  $1$  is multiplicative identity in  $R$ ,  $1f = f$  for all  $f \in M$ .

**Definition 1.17** Let  $M$  be a module over a ring  $R$ .  $M$  is said to be a free module if  $M$  has a module basis (that is, a generating set which is  $R$ -linearly independent).

For instance, the  $R$ -module  $M = R^m$  is a free module. The standard vectors  $\mathbf{e}_1 = (1, 0, 0, \dots, 0)^T$ ,  $\mathbf{e}_2 = (0, 1, 0, \dots, 0)^T$ ,  $\dots$ ,  $\mathbf{e}_m = (0, 0, 0, \dots, 1)^T$  form one basis for  $M$  as  $R$ -module.

One obtains other examples of  $R$ -modules by considering submodules of  $R^m$ , that is, subsets of  $R^m$  which are closed under addition and scalar multiplication by elements of  $R$  and which are, therefore, modules in their own right.

We might, for example, choose a finite set of vectors  $\mathbf{f}_1, \dots, \mathbf{f}_s$  and consider the set of all vectors which can be written as an  $R$ -linear combination of these vectors:

$$\{a_1 \mathbf{f}_1 + \cdots + a_s \mathbf{f}_s \in R^m, a_1, \dots, a_s \in R\}.$$

We denote this set  $\langle \mathbf{f}_1, \dots, \mathbf{f}_s \rangle$ , and we can easily show that it is a submodule of  $R^m$ . This kind of submodules are called finitely generated submodules.

In this thesis, we consider finitely generated submodules of free module  $R^m$  where  $R = k[x_1, \dots, x_n]$  is the polynomial ring over some field  $k$ . In particular, we will consider what we call syzygy submodules of  $R^m$ .

**Definition 1.18** *Let  $R = k[x_1, \dots, x_n]$ , and let  $(f_1, \dots, f_t)$  be an ordered  $t$ -tuple of elements  $f_i \in R$ . The set of all  $(a_1, \dots, a_t)^T \in R^t$  such that  $a_1 f_1 + a_2 f_2 + \cdots + a_t f_t = 0$  is an  $R$ -submodule of  $R^t$ , called the (first) syzygy module of  $(f_1, \dots, f_t)$ , and denoted  $\text{syz}(f_1, \dots, f_t)$ .*

The syzygy modules are finitely generated  $R$ -modules, and a set of generators for them can be computed. If the starting point is a Gröbner basis, then finding a set of generators for the syzygy module is accomplished using Buchberger's algorithm. While computing a Gröbner basis  $G = \{g_1, \dots, g_s\}$  for an ideal  $I \subset R$  with respect to some fixed monomial ordering, a slight modification of the algorithm would actually compute a set of generators for the syzygy module  $\text{syz}(g_1, \dots, g_s)$  as well as the  $g_i$ 's themselves.

Let  $S(g_i, g_j)$  be the  $S$ -polynomial of  $g_i$  and  $g_j$ .

$$S(g_i, g_j) = \frac{x^{\gamma_{ij}}}{LT(g_i)} g_i - \frac{x^{\gamma_{ij}}}{LT(g_j)} g_j,$$

where  $x^{\gamma_{ij}}$  is the least common multiple of  $\text{LM}(g_i)$  and  $\text{LM}(g_j)$ . Since  $G$  is a Gröbner basis, the remainder of  $S(g_i, g_j)$  on division by  $G$  is zero, and division algorithm gives an expression

$$S(g_i, g_j) = \sum_{k=1}^s a_{ijk} g_k,$$

where  $a_{ijk} \in R$ , and  $\text{LT}(a_{ijk}) \leq \text{LT}(S(g_i, g_j))$  for all  $i, j, k$ .

Let  $\mathbf{a}_{ij} \in \mathbf{R}^s$  denote the column vector

$$\mathbf{a}_{ij} = a_{ij1}\mathbf{e}_1 + a_{ij2}\mathbf{e}_2 + \cdots + a_{ijs}\mathbf{e}_s = (a_{ij1}, a_{ij2}, \dots, a_{ijs})$$

and define  $\mathbf{s}_{ij} \in R$  by setting

$$\mathbf{s}_{ij} = \frac{x^{\gamma_{ij}}}{LT(g_i)}\mathbf{e}_i - \frac{x^{\gamma_{ij}}}{LT(g_j)}\mathbf{e}_j + \mathbf{a}_{ij} \quad (*)$$

in  $R^s$ . Then the next theorem shows how to find a basis for the syzygy module.

**Theorem 1.19** *Let  $G = \{g_1, \dots, g_s\}$  be a Gröbner basis of an ideal  $I$  in  $R$  with respect to some fixed monomial order, and let  $M = \text{Syz}(g_1, \dots, g_s)$ . The collection  $\{\mathbf{s}_{ij}, 1 \leq i, j \leq s\}$  from (\*) generates  $M$  as an  $R$ -module.*

The next step is to compute  $\text{syzy}(f_1, \dots, f_t)$  for a collection  $\{f_1, \dots, f_t\}$  of nonzero polynomial in  $R$  which may not form a Gröbner basis. First compute a Gröbner basis  $\{g_1, \dots, g_s\}$  for  $\langle f_1, \dots, f_t \rangle$ . Set  $F = (f_1, \dots, f_t)$  and  $G = (g_1, \dots, g_s)$ . Since the elements of  $F$  and  $G$  generate the same ideal, there are a  $t \times s$  matrix  $A$  and an  $s \times t$  matrix  $B$ , both with entries in  $R$ , such that  $G = FA$  and  $F = GB$ . The matrix  $B$  can be computed by applying the division algorithm with respect to  $G$ . The matrix  $A$  can be obtained by keeping track of reductions of S-polynomials on the division process during Buchberger's Algorithm.

A generating set  $\{\mathbf{s}_1, \dots, \mathbf{s}_p\}$  for  $\text{syzy}(G)$  (the  $\mathbf{s}_i$ 's are column vectors in  $R^s$ ) can be computed using Theorem 1.19. Let  $\mathbf{r}_1, \dots, \mathbf{r}_t$  be the columns of the matrix  $I_t - AB$ .

**Theorem 1.20** *With the notation above,*

$$\{A\mathbf{s}_1, A\mathbf{s}_2, \dots, A\mathbf{s}_p, \mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_t\}$$

*is a generating set for  $\text{Syz}(f_1, \dots, f_t)$ .*

for example, let  $M = \langle f_1, f_2 \rangle$  in  $R = k[x, y]$  where

$$f_1 = xy + x, \quad f_2 = y^2 + 1.$$

Using the lex monomial order, the reduced Gröbner basis for  $M$  consist of

$$g_1 = x, \quad g_2 = y^2 + 1.$$

then it is easy to check that

$$f_1 = (y + 1)g_1$$

$$g_1 = -(1/2)(y - 1)f_1 + (1/2)xf_2,$$

so that

$$G = (g_1, g_2) = (f_1, f_2) \begin{pmatrix} -(y-1)/2 & 0 \\ x/2 & 1 \end{pmatrix} = FA$$

and

$$F = (f_1, f_2) = (g_1, g_2) \begin{pmatrix} y+1 & 0 \\ 0 & 1 \end{pmatrix} = GB$$

Since

$$S(g_1, g_2) = y^2g_1 - xg_2 = -x = -g_1,$$

by Theorem 1.19 we have that

$$s_{12} = \begin{pmatrix} y^2 + 1 \\ -x \end{pmatrix}$$

generates  $Syz(g_1, g_2)$ . Multiplying By  $A$  we get

$$\begin{aligned} As_{12} &= \begin{pmatrix} -(y-1)/2 & 0 \\ x/2 & 1 \end{pmatrix} \begin{pmatrix} y^2 + 1 \\ -x \end{pmatrix} \\ &= \begin{pmatrix} -(y^3 - y^2 + y - 1)/2 \\ (xy^2 - x)/2 \end{pmatrix}. \end{aligned}$$

The columns of  $I_2 - AB$  are

$$S_1 = \begin{pmatrix} (y^2 + 1)/2 \\ -(xy + x)/2 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

So by the theorem 1.20

$$Syz(f_1, f_2) = \langle AS_{12}, S_1 \rangle.$$

### 1.3 Hilbert Function and Hilbert Polynomial

The Hilbert function of a homogeneous ideal  $I \subset k[x_1, \dots, x_n]$  of polynomial ring associates to an integer  $n$  the dimension of  $k[x_1, \dots, x_n]/I$ . For sufficiently large  $n$ , the values of this function are given by a polynomial, the Hilbert polynomial. To show this, we use Hilbert-Poincare series, a formal power series in  $t$  with coefficients being the values of the Hilbert function. This power series turns out to be rational function.

**Definition 1.21** Let  $I \subset k[x_1, \dots, x_n]$  be a homogeneous ideal. The Hilbert function  $H_I : \mathbb{Z} \rightarrow \mathbb{Z}$  of  $I$  is defined by

$$H_I(d) := \dim_k(k[x_1, \dots, x_n]/I),$$

and the Hilbert-Poincare series  $HP_I$  of  $I$  is defined by

$$HP_I(t) := \sum_{m \in \mathbb{Z}} H_I(m)t^m \in \mathbb{Z}[[t]][[t^{-1}]]$$

Hilbert-Poincare series of any homogeneous ideal  $I$  can be written in the form

$$HP_I(t) := \frac{Q(t)}{(1-t)^r} \quad \text{where} \quad Q(t) \in \mathbb{Z}[t].$$

When we cancel all common factors in the numerator, we obtain

$$HP_I(t) = \frac{G(t)}{(1-t)^s}, \quad 0 \leq s \leq n, \quad G(t) = \sum_{m=0}^r g_m t^m.$$

such that  $g_d \neq 0$  and  $G(1) \neq 0$ , that is,  $s$  is the pole order of  $HP_I(t)$ . In fact, the degree of  $G(t)$  which is equal to  $r$  is the number when Hilbert function becomes a polynomial. The Hilbert polynomial of  $I$  is

$$\sum_{m=0}^r g_m \binom{s-1+d-m}{s-1}$$

which is agree with the Hilbert function of  $I$  for  $d \geq r$ .

Since the Hilbert polynomial and the Hilbert-Poincare series determine each other, it suffices to study and compute Hilbert-Poincare series. The following algorithm computes the Hilbert-Poincare series of a monomial ideal, more precisely, it computes the polynomial  $Q(t)$ .

**Algorithm 1.22** *Input:*  $I = \langle m_1, \dots, m_p \rangle \subset k[x_1, \dots, x_n]$ ,  $m_i$  is a monomial.

*Output:* A polynomial  $Q(t)$  such that  $Q(t)/(1-t)^n$  is HP series of  $I$ .

Choose  $S = \{x^{\alpha_1}, \dots, x^{\alpha_s}\}$  a minimal set of generators of  $I$ .

If  $S = \{0\}$  then return 1.

If  $S = \{1\}$  then return 0.

If all elements of  $S$  have degree 1 then return  $(1-t)^s$ .

Choose  $1 \leq i \leq s$  such that  $\deg(x^{\alpha_i}) > 1$

Choose  $1 \leq j \leq n$  such that  $x_j \mid x^{\alpha_i}$ .

Return  $\text{MonHilbertPoincare} \langle I, x_j \rangle + t \text{MonHilbertPoincare} (I : x_j)$ .

**Example 1.23** Since we have  $\binom{n+d-1}{n-1}$  monomial of degree  $d$  in  $k[x_1, \dots, x_n]$ ,

$$HP_{k[x_1, \dots, x_n]}(t) = \sum_{d=0}^{\infty} \binom{n+d-1}{n-1} t^d = \frac{1}{(1-t)^n}$$

Let  $I = \langle xz, yz \rangle \subset k[x, y, z]$ . Using algorithm above

$$\begin{aligned} HP_I(t) &= HP_{\langle I, z \rangle}(t) + t \cdot HP_{\langle I : z \rangle}(t) = HP_{k[x, y]}(t) + t \cdot HP_{k[z]}(t) \\ &= \frac{1}{(1-t)^2} + t \frac{1}{1-t} \end{aligned}$$

$$= \frac{1+t-t^2}{(1-t)^2}.$$

Since

$$\begin{aligned} \frac{1+t-t^2}{(1-t)^2} &= \sum_{d=0}^{\infty} \binom{d+1}{1} t^d + \sum_{d=0}^{\infty} \binom{d+1}{1} t^{d+1} - \sum_{d=0}^{\infty} \binom{d+1}{1} t^{d+2} \\ &= \sum_{d=0}^{\infty} \left( \binom{d+1}{1} + \binom{d}{1} - \binom{d-1}{1} \right) t^d \end{aligned}$$

the Hilbert polynomial of  $I$  is

$$H_I(d) = \binom{d+1}{1} + \binom{d}{1} - \binom{d-1}{1} = d+2$$

which is agree with the Hilbert function for  $d \geq 1$ .

## CHAPTER 2

# COMPUTATION OF SYZYGY BASIS OF HOMOGENEOUS IDEALS USING LINEAR ALGEBRA

### 2.1 Introduction

In algebraic geometry over a field  $k$ , we study the geometry of varieties through properties of polynomial ring  $R = k[x_1, \dots, x_n]$  and its ideals. It turns out that to study ideals effectively we also need to study more general modules over  $R$ . If an ideal  $I \subset R$  is given by a set of generators  $\{f_1, f_2, \dots, f_s\}$ , the most important submodule of free module  $R^s$  is the syzygy module of  $(f_1, \dots, f_s)$ . The syzygy module plays important role in the computation of Hilbert polynomials, free resolutions and geometric aspects of variety of ideals such as dimension and degree of varieties. Hence the computation of a basis for syzygy module is crucial. The only way, other than a few exceptional cases, is to use Gröbner basis techniques. In this chapter, we will try to give an alternative method to compute a bases for syzygy modules of homogeneous ideals. Unlike the known method, we will use only linear algebraic techniques.

### 2.2 Vector Spaces Concerning Homogeneous Ideals

We consider  $\mathbf{R}$  the ring of polynomials in  $x_1, x_2, \dots, x_n$  with coefficients from an infinite field  $k$ , i.e  $\mathbf{R} = k[x_1, x_2, \dots, x_n]$  and the subsets  $\mathbf{R}_d$  of all homogeneous polynomials of degree of  $d$ . A direct sum

$$\mathbf{R} = \bigoplus_{d \in \mathbb{N}} \mathbf{R}_d$$

is called the degree grading. Because for all  $\alpha, \beta \in \mathbb{N}$

$$f \in \mathbf{R}_\alpha, g \in \mathbf{R}_\beta \Rightarrow f \cdot g \in \mathbf{R}_{\alpha+\beta}$$

Since the decomposition of above is a direct sum, each polynomial  $f \neq 0$  has a unique representation.

$$f = \sum_{i=1}^s f_{\gamma_i} \quad 0 \neq f_{\gamma_i}$$

If we consider  $\mathbf{R}_d$  as a vector space over  $k$  with monomials of degree  $d$  being a basis , then there is a well-known formula

$$\dim(\mathbf{R}_d) = \binom{d+n-1}{n-1}.$$

Let  $I \subset k[x_1, x_2, \dots, x_n]$  be a homogeneous ideal. We define the vector space  $V_d(I) = \mathbf{R}_d \cap I$ . If  $\{g_1, \dots, g_s\}$  is a basis of  $I$  involving only homogeneous polynomials, then  $V_d(I)$  is generated by all monomial multiples  $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} g_i$  with  $\alpha_1 + \alpha_2 + \dots + \alpha_n + \deg(g_i) = d$ .

Let us define  $W_d(I)$  as orthogonal component of  $V_d(I)$ . Hence  $\mathbf{R}_d = V_d(I) \oplus W_d(I)$ .

**Definition 2.1** For given polynomials  $g_1, \dots, g_s \in \mathbf{R}$ , let

$$\text{Syz}(g_1, \dots, g_s) := \left\{ (h_1, \dots, h_s) \in \mathbf{R}^s \mid \sum_{i=1}^s h_i g_i = 0 \right\}$$

be the the module of syzygies with respect to  $g_1, \dots, g_s$ .

As explained in section 1.2 , finding a generating set for  $\text{syz}(g_1, \dots, g_s)$  involves a Gröbner basis computation. In this chapter of the thesis, our aim is to find a generating set for  $\text{syz}(g_1, \dots, g_s)$  using techniques of linear algebra. The following observation will be the crucial for this computation.

**Lemma 2.2** For given polynomials  $g_1, \dots, g_s \in \mathbf{R}$ , let

$$\text{Syz}(g_1, \dots, g_s) := \bigoplus_{d \in \mathbb{N}} S_d(g_1, \dots, g_s)$$

where

$$S_d(g_1, \dots, g_s) := \left\{ (h_1, \dots, h_s) \in \text{Syz}(g_1, \dots, g_s) : \deg(h_i g_i) = d \text{ or } h_i = 0 \right\} \subseteq \text{Syz}(g_1, \dots, g_s)$$

Then ,  $\dim(S_d(g_1, \dots, g_s)) = \sum_{i=1}^s \dim(\mathbf{R}_{d-\text{def}(g_i)}) - \dim V_d(g_1, \dots, g_s)$ .

**Proof.** Every syzygy in  $S_d(g_1, \dots, g_s)$  is a linearly dependent relation among the degree  $d$  polynomials  $x_1^{\alpha_1} \dots x_n^{\alpha_n} g_i$ . Since  $\dim(V_d(g_1, \dots, g_s))$  is number of linearly independent polynomials of this kind, the assertion follows  $\square$

Let us define

$$\begin{pmatrix} d+n-1 \\ n-1 \end{pmatrix} x \sum_{i=1}^s \begin{pmatrix} d+n-\text{deg}(g_i)-1 \\ n-1 \end{pmatrix}$$

matrix  $M$  where each row corresponds to a monomial of degree  $d$  and each column corresponds the polynomial of kind  $x_1^{\alpha_1} \dots x_n^{\alpha_n} g_i$  where  $\alpha_1 + \dots + \alpha_n + \text{deg}(g_i) = d$  for  $i = 1, \dots, s$ . In this case, the basis of nullspace of  $M$  is a generating set for  $S_d(g_1, \dots, g_s)$ . The null space of  $M$  can be easily seen from row-reduced echelon of  $M$ .

Hence, if we compute the row reduced echelon form of matrices in the above form, then we can obtain a generating set for  $S_d(g_1, \dots, g_s)$  for each  $d$ . However we need to know the value of  $d$  for which we obtain a generating set for  $\text{Syz}(g_1, \dots, g_s)$ . In other words , we must have an ending criterium of the process. This criterium will come from Hilbert Function of the ideal  $I = \langle g_1, \dots, g_s \rangle$ . To use this criterium, however, we need to know information about the vector space  $W_d(I)$ . This information can be read off from the row reduced echelon form of the transpose of  $M$ . We also have to calculate, thus, the row reduced echelon form of the transpose of  $M$ .

On the other hand, if we do row reduction without row interchange operation, a basis of  $W_d(I)$  can be obtained from row-reduced form of the matrix  $M$ .

Suppose that the rows of  $M$  corresponds the monomials of degree  $d$  in lexicographic order with  $x_1 > x_2 > x_3 > \dots > x_n$ .

**Lemma 2.3** *Let  $M$  be the matrix defined as above. If  $M$  is row-reduced without using elementary row operation of interchanging rows, then for each monomial corresponding non-zero rows of  $M$  there exists a polynomial in  $I = \langle g_1, \dots, g_s \rangle$  which has this monomial as leading monomial. Hence the monomials corresponding zero rows of  $M$  form a basis for  $W_d(I)$ .*

**Proof.**

Suppose that when applying row-reduction process to the matrix  $M$ , we also made the following computations in the polynomials corresponding columns of  $M$ :

In the first row of  $M$ , we find the most-left non-zero entry, if there is one, and divide the first row by its value. The polynomial,  $f_1$  corresponding the column of this non-zero entry has leading monomial  $x_1^d$ . Dividing this polynomial by the value of non-zero entry, makes it monic. For convenience, if the first row contains only zero entries define  $f_1 := 0$

In the second row, we again find the most-left non-zero entry, say  $m_{2j} \neq 0$ . This means we have a polynomial  $f_2 \in I_d$  involving the monomial  $x_1^{d-1}x_2$ . If  $m_{1j} = 0$ , then the leading monomial of  $f_2$  is  $x_1^{d-1}x_2$ . Otherwise, define  $f_2 := f_2 - m_{1j}f_1$  and thus  $f_2$  has leading monomial of  $x_1^{d-1}x_2$ . In both cases, dividing polynomials by leading coefficient, makes the monic. As before, if the second row contains only zero entries, define  $f_2 := 0$

In general, if the  $i^{th}$  row has the most-left non-zero entry  $m_{ij}$  then take the monomial corresponding the  $j^{th}$  column of  $M$ , call it  $f_i$ . Define  $f_i := f_i - \sum_{k=1}^{i-1} m_{kj}f_k$  and divide  $f_i$  by its leading coefficient.

Hence the non-zero  $f_i$ 's would have be a basis of  $V_d(I)$  each of which have leading monomial corresponding non-zero rows of  $M$  if we made the above computations. Therefore, the monomials corresponds zero-rows form a basis for  $W_d(I)$

□

Now, we are ready to give an algorithm to compute syzygy basis of  $g_1, \dots, g_s$ . Before that, let us recall definition of Hilbert function of an ideal and observe some facts regarding dimension of  $S_d(g_1, \dots, g_s)$ .

**Definition 2.4** Let  $I = \langle g_1, \dots, g_s \rangle \subseteq R$  be an ideal. The mapping

$$H_I : \mathbb{N} \rightarrow \mathbb{N}, \quad H_I(d) = \dim(W_d(I))$$

is called the Hilbert function of  $I$ .

For every ideal  $I \subset R$  there exists a constant  $t_0$  such that  $H_I(t)$  becomes a polynomial in  $t$  for  $t \geq t_0$ . This is the so called Hilbert polynomial, see 1.3.

As explained in section 1.3, we can easily compute Hilbert polynomial of monomial ideals.

we have the following equalities about the dimensions of vector space which are concerned.

$$\dim(V_d(I)) = \binom{d+n-1}{n-1} - H_I(d)$$

$$\dim(S_d(g_1, \dots, g_s)) = H_I(d) - \binom{d+n-1}{n-1} + \sum_{i=1}^s \binom{d+n-1-\deg(g_i)}{n-1}$$

Now, we are ready to give an algorithm for finding a generating set for  $\text{syz}(g_1, \dots, g_s)$ .

Before that, recall  $H_I(d) = H_{LT(I)}(d)$  for every  $d \in \mathbb{N}$

## 2.3 An Algorithm to Compute Syzygy Basis of Homogenous Polynomials

**Algorithm 2.5** *The following algorithm computes a syzygy basis of a set of homogeneous polynomials.*

**Input:** an  $s$ -tuple of homogeneous polynomials  $(g_1, \dots, g_s)$ .

**Output:** a generating set for  $\text{syz}(g_1, \dots, g_s)$ .

$d_0 := \min\{\deg(g_1), \dots, \deg(g_s)\}$ ,  $\text{Syz} := \{\}$ ;

$LM(I) := \{\}$ ,  $DelCol := \{\}$ ;  $lhs := 0$ ;  $rhs = 1$ ;

**WHILE**  $lhs < rhs$

**FORM** the matrix  $M$  of dimension  $\binom{d_0+n-1}{n-1} \times \sum_{i=1}^s \binom{d_0+n-\deg(g_i)-1}{n-1}$ ;

**DELETE** the columns of  $M$  corresponding to  $DelCol$ .

**READ** the  $S_{d_0}(g_1, \dots, g_s)$  from the null space of  $M$ ;

$\text{Syz} := \text{Syz} \cup S_{d_0}$ ;

**SELECT** a polynomial of the form  $x^\alpha g_i \notin DelCol$  which

is part of  $\mathbf{s} \in \text{Syzy}$  for each  $\mathbf{s} \in \text{Syzy}$ .

$\text{DelCol} := \text{DelCol} \cup x^\alpha g_i$ .

**READ** *leadmon*, lead monomials from non-zero rows of  $M$ ;

$\text{LM}(I) := \text{LM}(I) \cup \text{leadmon}$

**MINIMIZE**  $\text{LM}(I)$ .

$m :=$  the number of repeated elements in  $\text{DelCol}$

$\text{lhs} := \sum_{\mathbf{s} \in \text{Syzy}} \binom{d+n-1-\text{deg}(\mathbf{s})}{n-1} - \binom{d+n-1-m}{n-1}$ ;

$\text{rhs} := H_{\text{LM}(I)}(d) - \binom{d+n-1}{n-1} + \sum_{i=1}^s \binom{d+n-1-\text{deg}(g_i)}{n-1}$  for  $d \geq d_0$

$d_0 := d_0 + 1$

**END WHILE**

**RETURN**  $\text{Syzy}$ .

**Proof.** Regarding dimension of syzygy basis of degree  $d$ , we have proved that

$$\dim(S_d(g_1, \dots, g_s)) = \sum_{i=1}^s \dim(\mathbf{R}_{d-\text{deg}(g_i)}) - \dim(V_d(g_1, \dots, g_s)).$$

Using Hilbert polynomial, on the other hand, we have

$$\dim(V_d(I)) = \binom{d+n-1}{n-1} - H_{\text{LM}(I)}(d).$$

Combining this two equalities gives us,

$$\dim(S_d(g_1, \dots, g_s)) = H_{\text{LM}(I)}(d) - \binom{d+n-1}{n-1} + \sum_{i=1}^s \binom{d+n-1-\text{deg}(g_i)}{n-1}.$$

This is the number we called  $\text{rhs}$  in the algorithm.

For the other side, Every syzygy  $(h_1, \dots, h_s) \in S_{d_0}(g_1, \dots, g_s)$  can be extended to  $\binom{d+n-1-d_0}{n-1}$  different syzygies in  $S_d$  by multiplying by the monomials  $x_1^{\alpha_1} \dots x_n^{\alpha_n}$  where  $\alpha_1 + \alpha_2 + \dots + \alpha_n = d - d_0$ . Hence

$$\dim(S_d(g_1, \dots, g_s)) = \sum_{\mathbf{s} \in \text{Syzy}} \binom{d+n-1-\text{deg}(\mathbf{s})}{n-1}$$

We have to check whether there is repeated element in Delcol in each  $d_0$ . If  $m$  is the number of repeated elements, then

$$\sum_{s \in S_{yz}} \binom{d+n-1-\deg(s)}{n-1} - \binom{d+n-1-m}{n-1}$$

This is the number we have called  $lhs$  in the algorithm.

Notice that, in the  $rhs$ ,  $\sum_{i=1}^s \binom{d+n-1-\deg(g_i)}{n-1} - \binom{d+n-1}{n-1}$  is a fixed number. Therefore the only part which can change in the  $rhs$  is the Hilbert Polynomial,  $H_{LM(d)}(I)$ . Since  $H_{LM(d)}(I)$  is decreasing when a new monomial is added to  $LT(I)$ ,  $rhs$  is a decreasing function of  $d$  in each step of the algorithm.

On the other hand, when a new syzygy is added to bases,  $lhs$  is increasing at that step of the algorithm. Hence whenever  $lhs = rhs$ , we shall obtain the syzygy basis and the algorithm can stop.  $\square$

Now, we are going to give an example to apply the algorithm given above.

**Example 2.6** Consider the ideal  $I = \langle g_1 = xy + z^2, g_2 = x^2 - yz, g_3 = xy^3z + z^5 \rangle$ .

For  $d_0 = 2$

$$M = \begin{array}{cc} & \begin{array}{cc} g_1 & g_2 \end{array} \\ \begin{array}{c} x^2 \\ xY \\ xZ \\ Y^2 \\ YZ \\ z^2 \end{array} & \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & -1 \\ 1 & 0 \end{pmatrix} \end{array}$$

$M$  is already reduced form, there is no syzygy.  $LT(I) := \{xy, x^2\}$

For  $d_0 = 3$

$$\mathbf{M} = \begin{matrix} & & & & xg_1 & yg_1 & zg_1 & xg_2 & yg_2 & zg_2 \\ \begin{matrix} x^3 \\ x^2 y \\ x^2 z \\ xy^2 \\ xyz \\ xz^2 \\ y^3 \\ y^2 z \\ yz^2 \\ z^3 \end{matrix} & \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \end{matrix}$$

Reduced form of  $\mathbf{M}$  is,

$$\begin{matrix} & & & & xg_1 & yg_1 & zg_1 & xg_2 & yg_2 & zg_2 \\ \begin{matrix} x^3 \\ x^2 y \\ x^2 z \\ xy^2 \\ xyz \\ xz^2 \\ y^3 \\ y^2 z \\ yz^2 \\ z^3 \end{matrix} & \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{matrix}$$

There is no syzygy again.  $LT(I) := \{xy, x^2, xz^2\}$

The new element  $xz^2$  of the  $LT(I)$  in fact can be seen from the one step earlier matrix of reduction process. Because the matrix just before reduced form in the process is,

$$\begin{matrix} & & & & xg_1 & yg_1 & zg_1 & xg_2 & yg_2 & zg_2 \\ \begin{matrix} x^3 \\ x^2 y \\ x^2 z \\ xy^2 \\ xyz \\ xz^2 \\ y^3 \\ y^2 z \\ yz^2 \\ z^3 \end{matrix} & \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ \square & 0 & 0 & 0 & \square & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \square & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{matrix}$$

To make zero entry in the position (2, 5), we multiply the sixth row by -1 add the second row. Since the leading element in the second row is in the position (2, 1), this operation corresponds to  $xg_1 - yg_2 = x(xy + z^2) - y(x^2 - yz) = xz^2 - y^2z$ . Hence  $LT(xz^2 - y^2z) = xz^2 \in LT(I)$ .

Let us continue the process.

For  $d_0 = 4$

$$\mathbf{M} = \begin{matrix} & \mathbf{x^2g1} & \mathbf{xyg1} & \mathbf{xzg1} & \mathbf{y^2g1} & \mathbf{yzg1} & \mathbf{z^2g1} & \mathbf{x^2g2} & \mathbf{xyg2} & \mathbf{xzg2} & \mathbf{y^2g2} & \mathbf{yzg2} & \mathbf{z^2g2} \\ \mathbf{x^4} & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{x^3y} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \mathbf{x^3z} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \mathbf{x^2y^2} & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \mathbf{x^2yz} & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ \mathbf{x^2z^2} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \mathbf{xy^3} & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{xy^2z} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ \mathbf{xyz^2} & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\ \mathbf{xz^3} & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{y^4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{y^3z} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ \mathbf{y^2z^2} & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ \mathbf{yz^3} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ \mathbf{z^4} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix}$$

Reduced form of  $\mathbf{M}$  is,











We can easily see that  $lhs > rhs$  for  $d \geq 8$ . Hence dimension of syzygy for  $d = 8$  is not correct. This means that we have at least one syzygy which is a linear combination of others. Since we find  $y^2g_3 = -x^3yzg_1 + x^2y^3g_1 + x^2y^2zg_1 + x^2z^3g_1 - xy^3zg_1 - xyz^3g_1 + y^2z^3g_1 + x^2y^2zg_2 - xy^4g_2 - x^2g_3 + xyg_3$  for the last syzygy, we have to delete columns corresponding to  $xy^2g_3, y^3g_3, y^2zg_3$  in  $d_0 = 8$ . However for the second syzygy, we find  $zg_3 = x^2y^2g_1 - xy^2zg_1 - xyz^2g_1 - xz^3g_1 + yz^3g_1 - xy^2zg_2 - xy^3g_2 + xg_3 - yg_3$ . Therefore, we have to delete  $x^2zg_3, xyzg_3, xz^2g_3, y^2zg_3, yz^2g_3, z^3g_3$ . So we delete  $y^2zg_3$  twice and we have to subtract  $\binom{3+(d-8)-1}{3-1}$  from lhs. Hence,

$$lhs = \binom{3+(d-4)-1}{3-1} + \binom{3+(d-6)-1}{3-1} + \binom{3+(d-7)-1}{3-1} - \binom{3+(d-8)-1}{3-1} = d^2 - 6d + 7.$$

So  $lhs = rhs$ . This terminates the algorithm.

The syzygy bases returned is  $\left\{ \{x^2 - yz, -xy - z^2, 0\}, \{x^2y^2 + x^2yz - xy^2z - xyz^2 - xz^3 + yz^3 + z^4, -xy^2z - xy^3, x - y - z\}, \{-x^3yz + x^2y^3 + x^2y^2z + x^2z^3 - xy^3z - xyz^3 + y^2z^3, x^2y^2z - xy^4, -x^2 + xy - y^2\} \right\}$

## CHAPTER 3

### H-BASIS (HOMOGENEOUS BASIS) ALGORITHM

#### 3.1 Introduction

The H-bases were first introduced by Macaulay [4]. His original motivation was transformation of systems of polynomial equations into simpler ones. The power of this concept was not really understood presumably because of the lack of facilities for symbolic computations. When Computer Algebra Systems came up, Gröbner Bases were used instead of H-bases. These bases, originally invented by Buchberger [5] for computing multiplication tables for factor rings, are now also applied for simplifying some problems in Numerical Analysis. However, all approaches related to Gröbner Bases are fundamentally tied on term orders which leads to asymmetry among the variables to be considered. On the other hand, the concept of H-bases is based solely on homogeneous terms of a polynomial. Because of this, H-bases seem to be better suited for numerical problems. Comparing of two bases in application of numerical analysis can be found in [6], [7].

It is known that a Gröbner basis with respect to a degree compatible ordering is also a H-basis. However, the Gröbner basis with respect to a degree compatible ordering is also a H-basis. However, the Gröbner basis usually contains more elements than necessary for a H-basis. The elimination of these unnecessary elements was studied in [8]. Macaulay gave an example of a H-basis construction in [9]. His method consists in a succession of homogenization and dehomogenization of ideals and uses heavily that he knows basis for the module of syzygies. This method clarified by Möller and Sauer in [6]. In there, they showed that the reduction of polynomials can be done only using linear algebra. They do not need to division algorithm to do this reduction. Unfortunately, efficiency of their algorithm depends on the complexity of computing bases for

module of syzygies. However, the only known method for the computing the syzygies involves Gröbner bases techniques described in Chapter 1. Because of this, they claimed that; it is more efficient to compute an H-bases rather by the Buchberger's algorithm using a degree compatible ordering than by the procedure they suggested which use Gröbner bases techniques for the calculation of module of syzygies. However, in chapter 2 we found an alternative method to compute the module of syzygies using only linear algebra.

Combining Möller and Sauer's procedure of computing H-bases with our method of finding a syzygy bases, we are able to give an algorithm which obtains an H-bases from a given basis of an ideal using only linear algebra.

## 3.2 Background

In this section we will define some terms and state some theorems.

**Definition 3.1** *We say that a polynomial  $f \in k[x_1, x_2, \dots, x_n]$  is **homogeneous of total degree  $d$**  if every term of  $f$  has total degree  $d$*

Let  $f \in k[x_1, x_2, \dots, x_n]$ . Then  $f = \sum_k f_k$ , where  $f_k$  is the sum of all terms of  $f$  with total degree  $k$ . Noting that  $f_k$  is homogeneous, we can say that any  $f \in k[x_1, x_2, \dots, x_n]$  can be written uniquely as a sum of homogeneous polynomials.

In the next definition we will define the homogenization of a polynomial  $g \in k[x_1, x_2, \dots, x_n]$ .

**Definition 3.2** *Let  $g \in k[x_1, x_2, \dots, x_n]$  be a polynomial of total degree  $d$  and  $g = \sum_{i=0}^d g_i$ , be the decomposition of  $g$  as the sum of its homogeneous components, where  $g_i$  has total degree  $i$ , then*

$$g^h(x_0, x_1, \dots, x_n) = \sum_{i=0}^d g_i(x_1, \dots, x_n) x_0^{d-i}$$

*is called the homogenization of  $g$  with respect to  $x_0$*

The next proposition reveals some facts about the process of homogenization.

**Proposition 3.3** Let  $g(x_1, x_2, \dots, x_n) \in k[x_1, x_2, \dots, x_n]$  be a polynomial of total degree  $d$

- (i) The homogenization of  $g$ ,  $g^h$ , is a homogeneous polynomial of total degree  $d$ .
- (ii) The homogenization of  $g$  can be computed using the formula

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

- (iii) Dehomogenizing  $g^h$  yields  $g$ . That is,  $g^h(1, x_1, \dots, x_n) = g(x_1, \dots, x_n)$

(iv) Let  $F(x_0, x_1, \dots, x_n)$  be a homogeneous polynomial and let  $x_0^e$  be the highest power of  $x_0$  dividing  $F$ . If  $f = F(1, x_1, \dots, x_n)$  is the dehomogenization of  $F$ , then  $F = x_0^e f^h$ .

- (v)  $f^h g^h = (fg)^h$

**Definition 3.4** An ideal  $I \in k[x_1, x_2, \dots, x_n]$  is said to be homogeneous if for every  $f \in I$ , the homogeneous components  $f_i$ 's of  $f$  are in  $I$  also.

In the following proposition it is stated another equivalent condition for an ideal to be homogenous.

**Proposition 3.5** Let  $I \subset k[x_1, x_2, \dots, x_n]$  be an ideal. Then the following statements are equivalent:

- (i)  $I$  is an homogeneous ideal of  $k[x_1, x_2, \dots, x_n]$
- (ii)  $I = \langle f_1, f_2, \dots, f_s \rangle$  for some homogeneous polynomials  $f_1, f_2, \dots, f_s$  in  $I$ .

The following lemma is about a property of homogeneous ideals that can be used to find a criterion for a homogeneous basis.

**Lemma 3.6** Let  $f_1, f_2, \dots, f_s$  be homogeneous polynomials of total degree  $d_1 \leq d_2 \leq \dots \leq d_s$  and let  $I = \langle f_1, f_2, \dots, f_s \rangle$  If  $g$  is another polynomial of degree  $d$  in  $I$ , then  $g$  must be an element of  $I_d = \langle f_i : \deg(f_i) \leq d \rangle \subset I$ . Moreover, there exist  $q_1, q_2, \dots, q_t$  with  $g = \sum_{i=1}^t q_i f_i$  such that each  $q_i$  is homogeneous of total degree  $d - d_i$ .

**Proof.** Assume there exists  $t$  such that each  $\deg(f_i) > d$  for  $i > t$ . Let

$$g = p_1f_1 + p_2f_2 + \dots + p_t f_t + \dots + p_s f_s.$$

Since  $\deg(g) = d$  and  $\deg(p_i f_i) > d$  for  $i \leq t$ ,  $p_t f_t + \dots + p_s f_s = 0$ . Since  $f_i \neq 0$ ,  $p_i = 0$  for  $i > t$ . Therefore

$$g = p_1f_1 + p_2f_2 + \dots + p_t f_t$$

If we write  $p_i$  as a sum of two polynomials  $p_i = q_i + r_i$  where  $q_i$  is a homogeneous polynomial of total degree  $d - d_i$  and  $r_i$  is the other part of  $p_i$ , then the multiplication  $r_i f_i$  produces monomials which have total degree different from  $d$ . Since  $g$  is a homogeneous polynomial of total degree  $d$ ,  $r_i f_i = 0$  for all  $i$ . Hence

$$g = q_1f_1 + q_2f_2 + \dots + q_t f_t.$$

□

### 3.3 Homogeneous Basis

**Definition 3.7** Let  $I$  be an ideal in  $k[x_0, x_1, \dots, x_n]$ . The homogenization of  $I$  is defined to be the ideal,

$$I^h = \langle f^h : f \in I \rangle \subset k[x_0, x_1, \dots, x_n]$$

where  $f^h$  is the homogenization of  $f$  with respect to  $x_0$ .

**Proposition 3.8** For any ideal  $I \subset k[x_1, x_2, \dots, x_n]$ , the homogenization  $I^h$  is a homogeneous ideal in  $k[x_0, x_1, \dots, x_n]$ .

**Proof.**

By the Hilbert Basis Theorem, there exist polynomials  $g_1, g_2, \dots, g_n \in I^h$  such that  $I^h = \langle g_1, g_2, \dots, g_n \rangle$ . By the definition of  $I^h$ ,

$$g_i = \sum a_{ij} f_{ij}^h,$$

where  $f_{ij} \in I$ . Since  $f_{ij}^h$ 's are homogeneous and  $I^h = \langle f_{ij}^h \rangle$ ,  $I^h$  is a homogeneous ideal by the proposition 3.5.  $\square$

Definition 3.7 defines  $I^h$  ,**homogenization of I**, where  $I \in k[x_1, x_2, \dots, x_n]$  but does not give us a generating set for  $I^h$ . Let  $I = \langle f_1, f_2, \dots, f_s \rangle \subset k[x_1, x_2, \dots, x_n]$ . It is always true for  $I^h$  , **homogenization of I**, that  $\langle f_1^h, \dots, f_s^h \rangle$  is a subset of  $I^h$ . But ,as we are going to see in the next example,  $I^h$  can be strictly larger than  $\langle f_1^h, \dots, f_s^h \rangle$ .

**Example 3.9** Let  $I = \langle f_1, f_2 \rangle = \langle y - x^2, z - x^3 \rangle$ , the ideal of the twisted cubic in  $\mathbb{R}^3$ . The homogenization of  $f_1$  and  $f_2$  gives  $J = \langle yt - x^2, zt^2 - x^3 \rangle$  in  $\mathbb{R}[t, x, y, z]$ . To prove  $J \neq I^h$ , consider the polynomial

$$f_3 = f_2 - xf_1 = z - x^3 - x(y - x^2) = z - xy \in I.$$

Then  $f_3^h = tz - xy$  is a homogeneous polynomial of degree 2 in  $I^h$ . Since the generators of  $J$  are also homogeneous of degree 2 and 3 respectively, if  $f_3^h \in J$ , then  $f_3^h$  should be constant multiple of  $f_1^h$  by lemma 3.6 . Since this is obviously false  $f_3^h \notin J$  and thus  $J \neq I^h$

In the following definition we will define what a **homogeneous basis** is.

**Definition 3.10** Let  $I = \langle f_1, f_2, \dots, f_t \rangle$  be an ideal in  $k[x_1, x_2, \dots, x_n]$ . If the homogenization of  $I$ ,  $I^h = \langle f_1^h, \dots, f_t^h \rangle$ , then  $f_1, f_2, \dots, f_t$  is said to be a **homogeneous basis** for  $I$ .

Note that there always exists a homogeneous basis for an ideal  $I$  by the proposition 3.8.

Example 3.9 shows that not every basis is a homogeneous basis. Therefore we need a criterion to test a basis whether it is homogeneous or not. For this, let us return back to Example 3.9. Multiplying  $f_2$  by  $t$ ,  $t(z - xy)^h = t(z - x^3)^h - x(y - x^2)^h$ . Note that the

power of  $t$  multiplied is exactly difference between total degrees of two sides. The next lemma generalizes this observation.

**Lemma 3.11** *Let  $I = \langle f_1, f_2, \dots, f_m \rangle$  and  $f = \sum_{i=1}^m q_i f_i$ . Set*

$$d = \max \{d_i = \deg(q_i f_i) : 1 \leq i \leq m\}$$

*and  $d' = \deg f$ . Then  $x_0^{d-d'} f^h \in \langle f_1^h, f_2^h, \dots, f_m^h \rangle$ .*

The next theorem gives us a necessary and sufficient condition for a basis to be homogeneous.

**Theorem 3.12** *Given  $I = \langle f_1, f_2, \dots, f_s \rangle \in k[x_1, x_2, \dots, x_n]$   $I^h = \langle f_1^h, f_2^h, \dots, f_s^h \rangle$  if and only if for every  $f \in I$  there exist  $a_1, a_2, \dots, a_s \in k[x_1, x_2, \dots, x_n]$  such that  $f = a_1 f_1 + a_2 f_2 + \dots + a_s f_s$  and  $\deg(f) = \max\{\deg(a_i f_i), i = 1, \dots, s\}$*

**Proof.** Assume  $\{f_1, f_2, \dots, f_s\}$  is a homogeneous bases. Then  $f \in \langle f_1, f_2, \dots, f_s \rangle$  implies  $f^h \in \langle f_1^h, f_2^h, \dots, f_s^h \rangle$ . If  $\deg(f) = d$  then  $\deg(f^h) = d$ . By Lemma 3.6, there exist  $A_1, A_2, \dots, A_s$  such that  $f^h = \sum_{i=1}^s A_i f_i^h$  and  $\max\{\deg(A_i f_i^h)\} = d$ . By part (iii) of Proposition 3.3,  $f = \sum_{i=1}^s A_i(1, x_1, \dots, x_n) f_i$

Hence,

$$d = \deg(f) \leq \max\{\deg(A_i(1, x_1, \dots, x_n) f_i)\} \leq \max\{\deg(A_i f_i^h)\} = \deg(f^h) = d.$$

Conversely, if  $f = a_1 f_1 + \dots + a_s f_s$  such that  $\deg(f) = \max\{\deg(a_i f_i)\}$  for some  $a_i$ 's, then  $f^h \in \langle f_1^h, \dots, f_s^h \rangle$  by Lemma 3.11.  $\square$

**Definition 3.13** *If  $\sum_i^d f_i$  is the decomposition of  $F$  as the sum of its homogeneous components, Then  $LT(F) = f_d$  is called the leading form of  $f$ . The homogeneous ideal of leading forms are also defined by  $LF(I) = \langle LF(f) : f \in I \rangle$ .*

**Lemma 3.14** *Let  $I = \langle f_1, \dots, f_s \rangle$  be an ideal of  $k[x_1, \dots, x_n]$ . The followings are equivalent.*

i) Every  $f \in I$  has a representation  $f = \sum_i h_i f_i$  where  $\deg f_i = \max\{\deg(h_i f_i) : i = 1, \dots, s\}$ .

$$ii) LF(I) = \langle LF(f_1, \dots, LF(f_s)) \rangle.$$

Now, in the next theorem, we will give another equivalent condition for a basis of an ideal to be homogeneous.

**Theorem 3.15** Let  $I = \langle f_1, \dots, f_t \rangle \subset k[x_1, \dots, x_n]$ , and let the columns of the  $t \times l$  matrix  $S = (s_{ij})$  be a generating set of  $\text{syz}(LF(f_1), \dots, LF(f_t))$ . Further assume that each  $\sum s_{ij} LF(f_j)$  is a homogeneous polynomial.

Then  $F = \{f_1, \dots, f_t\}$  is a homogeneous bases if and only if each

$$q_i = \sum_{j=1}^t s_{ji} f_j = \sum_{j=1}^t s_{ji} (f_j - LF(f_j)) = \sum_{j=1}^t a_{ji} f_j$$

for some  $a_{ji} \in k[x_1, \dots, x_n]$  such that  $\deg(q_i) = \max\{\deg(a_{ji} f_j) : j = 1, \dots, t\}$  for  $i = 1, \dots, l$ .

### 3.4 Computation of H-Bases

The Theorem 3.15 suggest the following procedure for computing H-bases.

Given a set of polynomials  $F = \{f_1, \dots, f_m\}$  generating and ideal  $I$ , first the elements of a bases of

$$\text{Syz}(LF(f_1), \dots, LF(f_m)) \dots (*)$$

have to be computed. Then for each bases element  $(g_1, \dots, g_m)$  the polynomial

$$q = g_1 f_1 + g_2 f_2 + \dots + g_m f_m$$

has to reduced modulo  $F$  as far as possible. If the reduction procedure terminates with a nonzero polynomial  $f$ , the set  $F$  is enlarged by  $f$ . For the new set  $F$  a bases for the module of syzygies is computed etc. This procedure differs from Buchberger's

algorithm only by the module of syzygies. Instead of basis of (\*) one consider for Gröbner bases computation the bases of

$$\text{Syz}(LT(f_1), \dots, LT(f_m)).$$

As Buchemberg's algorithm terminates correctly with a Gröbner bases, our proposed algorithm terminates with an H-bases. before giving precise statement of the algorithm, we will define reduction process.

**Definition 3.16** For a given  $f_1, f_2, \dots, f_m \in k[x_1, \dots, x_n]$  we say that  $f$  reduces to  $\bar{f}$  modulo  $F = \{f_1, \dots, f_m\}$  if  $LF(f) = a_1LF(f_1) + a_2Lf(f_2) + \dots + a_mLF(f_m)$  and

$$\bar{f} = f - (a_1f_1 + a_2f_2 + \dots + a_mf_m)$$

In this case we write

$$f \xrightarrow{F} \bar{f}$$

By  $\xrightarrow{*}$  we denote the transitive closure of the binary relation  $\xrightarrow{F}$ . We also say  $f$  reduces modulo  $F$  to  $g$  if  $f \xrightarrow{*}_F g$

**Algorithm 3.17** Algorithm to compute h-basis

**INPUT** : A bases  $F = \{f_1, \dots, f_m\}$  of an ideal  $I$ .

**OUTPUT** : a H- bases  $H = \{f_1, \dots, f_s\}$  of the same ideal  $I$ .

$H := F$  ;  $S := m$

**Construct** a bases  $S$  for  $\text{Syz}(LF(H))$

**While**  $S \neq \{\}$

**Select**  $(g_1, \dots, g_s) \in S$ ,  $S := S - \{(g_1, \dots, g_s)\}$

**Construct**  $f = g_1f_1 + \dots + g_sf_s$

$$P := f \xrightarrow{*}_F$$

If  $P \neq 0$ ,  $H := H \cup \{P\}$

**Construct** a bases  $S$  for  $\text{Syz}(LF(H))$

**End While**

**Return H.**

**Proof.**

The proof that this algorithm terminates, a consequences of the ascending chain condition, and produces a H-bases, which is follows from the theorem 3.15, is exactly the same as for Gröbner bases with respect to a term order.

□

Now, we will give an example for the computation of an H-bases basis of an ideal to illustrate the algorithm given above.

**Example 3.18** Let  $I = \langle f_1 = x^2 - y, f_2 = xy - z, f_3 = y^2z - x \rangle$  and let

$$g_1 = LF(f_1) = x^2, g_2 = LF(f_2)xy, g_3 = LF(f_3) = y^2z, J = \langle g_1, g_2, g_3 \rangle.$$

Syzygy basis of  $g_1, g_2, g_3$  is,

$$\left\langle \begin{pmatrix} y \\ -x \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ yz \\ -x \end{pmatrix} \right\rangle$$

The first syzygy gives

$$h = yf_1 - xf_2 = xz - y^2 \quad LF(h) = h = xz - y^2$$

$J_2$  is generated by  $\langle x^2, xy \rangle$

since  $LF(h) \notin J_2, f_4 = h$ .

$$I = \langle f_1, f_2, f_3, f_4 \rangle, g_i = LF(f_i), J = \langle g_1, g_2, g_3, g_4 \rangle.$$

Syzygy basis of  $(g_1, g_2, g_3, g_4)$  is

$$\left\langle \begin{pmatrix} y \\ -x \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -z \\ y \\ 0 \\ x \end{pmatrix}, \begin{pmatrix} 0 \\ yz \\ -x \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -z^2 \\ y \\ yz \end{pmatrix} \right\rangle$$

We have already looked at the first syzygy.

The second syzygy gives,

$$h = -zf_1 + yf_2 + xf_4 = 0.$$

The third syzygy gives,

$$h = yzf_2 - xf_3 = -yz^2 + x^2, LF(h) = -yz^2$$

$J_3$  is generated by  $\langle x^3, x^2y, x^2z, zy^2, xyz, y^2z, x(xz - y^2), y(xz - y^2), z(xz - y^2) \rangle$ .

Since  $LF(H) \notin J_3$ ,  $f_5 = h = -yz^2 + x^2$ .

$$I = \langle f_1, f_2, f_3, f_4, f_5 \rangle, g_i = LF(f_i) \quad J = \langle g_1, g_2, g_3, g_4, g_5 \rangle.$$

Syzygy basis of  $(g_1, g_2, g_3, g_4, g_5)$  is,

$$\left\langle \begin{pmatrix} y \\ -x \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -z \\ y \\ 0 \\ x \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ yz \\ -x \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ z \\ 0 \\ y \end{pmatrix}, \begin{pmatrix} 0 \\ -z^2 \\ 0 \\ 0 \\ x \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ y \\ yz \\ x \end{pmatrix} \right\rangle$$

WE have already looked at the first three syzygies.

The fourth syzygy gives,

$$h = zf_3 + yf_5 = x^2y - xz \quad LF(h) = x^2y$$

$$LF(h) = x^2y = yg_1$$

$$h_1 = h - yg_1 = (x^2y - xz) - y(x^2 - y) = -xz + y^2.$$

$$LF(h_1) = h_1 = -xz + y^2 = -g_4$$

$$h_2 = h_1 - f_4 = (-xz + y^2) - (xz - y^2) = 0.$$

The fifth syzygy gives

$$h = z^2f_2 + xf_5 = x^3 - z^2 \quad LF(h) = x^3 - z^3$$

$$LF(h) \notin J_3 \text{ So, } f_6 = h = x^3 - z^3.$$

$$I = \langle f_1, f_2, \dots, f_6 \rangle \quad J = \langle g_1, g_2, \dots, g_6 \rangle$$

Syzygy basis of  $(g_1, g_2, g_3, g_4, g_5, g_6)$  is,

$$\left\langle \begin{pmatrix} y \\ -x \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -z \\ y \\ 0 \\ x \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ yz \\ -x \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ z \\ 0 \\ y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -z^2 \\ 0 \\ 0 \\ x \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ y \\ yz \\ x \\ 0 \end{pmatrix}, \begin{pmatrix} xy \\ 0 \\ 0 \\ 0 \\ z \\ -y \end{pmatrix}, \begin{pmatrix} x^2 \\ 0 \\ -z \\ z^2 \\ 0 \\ -x \end{pmatrix} \right\rangle$$

we have already looked at the first five syzygies.

The sixth syzygy

$$h = yf_3 + yzf_4 + xf_5 = x^3 - xy. \quad LF(h) = x^3.$$

$$LF(h) = x^3 = xg_1$$

$$h_1 = h - xf_1 = (x^3 - xy) - x(x^2 - y) = 0.$$

The seventh syzygy,

$$h = xyf_1 + zf_5 - yf_6 = x^2z - xy^2 \quad LF(h) = x^2z - zy^2$$

$$LF(h) = x^2z - xy^2 = zg_1 - yg_2$$

$$h_1 = h - zf_1 + yf_2 = x^2z - zy^2 - z(x^2 - y) + y(xy - z) = 0$$

The eighth syzygy

$$h = x^2f_1 - zf_3 - z^2f_4 - xf_6 = -x^2y + xz \quad LF(h) = -x^2y$$

$$LF(h) = -yg_1$$

$$h_1 = h + yf_1 = -x^2y + xz + y(x^2 - y) = xz - y^2$$

$$LF(h_1) = xz - y^2 = g_3$$

$$h_2 = h_1 - f_3 = xz - y^2 - (xz - y^2) = 0$$

We have found  $H$ -basis.

## REFERENCES

- [1] W.W. Adams and P. Loustaunau, *An Introduction to Grobner Bases*, Graduate Studies In Mathematics, Vol.3 (AMS, 1996).
- [2] D.Cox,J.Little and D. O'Shea, *Ideal, varieties and Algorithms*, Undergraduate text in Mathematics, (Springer-Verlag, 1992).
- [3] D.Cox,J.Little and D. O'Shea, *Using Algebraic Geometry*, Graduate text in Mathematics, (Springer-Verlag, 1998).
- [4] F.S Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Tracts in Math. and Mat. Physics, no.19, (Cambridge University Press), 1916
- [5] B.Buchberger, *Gröbner bases: An algorithmic Method in Polynomial Ideal Theory, Multidimensional Systems Theory(N.K Base ed.)* (D.reidel Pubishing company, 1985, pp.184-232).
- [6] H.M.Möller and T.Sauer, *H-basis for Polynomial Interpolation and system Solving*, Advances in computational Mathematics 12, 2000, pp 335-362.O
- [7] T. Sauer, *Gröbner Bases, H-Bases and Interpolation*, Transaction of AMS 353, 2001, pp 2293-2308.
- [8] E.Yılmaz and S. Kılıcarslan, *Minimal Homogeneous Basis For Polynomial Ideals*, Applicable Algebra in Engineering, communication and computing 15, 2004, pp 267-278.
- [9] F.S Macaulay, *Some Properties of Enumerition In The Theory of Modular Systems*, Proc. London Math. Soc. 26, 1927, pp 531-555