

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Polynomial and commutative Algebra</b>	<b>3</b>
2.1	Monomials . . . . .	3
2.2	Monomial Order . . . . .	3
2.2.1	Lexicographic Order . . . . .	4
2.2.2	Graded Lex Order . . . . .	4
2.2.3	Leading term . . . . .	4
2.3	Ideals . . . . .	4
<b>3</b>	<b>Linear Codes</b>	<b>6</b>
<b>4</b>	<b>Software</b>	<b>6</b>
<b>A</b>	<b>Appendix</b>	<b>6</b>

# 1 Introduction

## 2 Polynomial and commutative Algebra

In this chapter a mathematical basis is systematically approached to give the reader an understanding to Groebner Bases and obtaining by the Flipping-Algorithm which is needed later.

In the first section monomials are revisited. The second section explains how monomials can be mathematically ordered. After that Ideals are defined over polynomial rings and a summary on Groebner bases and Groebner fans for ideals is presented.

### 2.1 Monomials

First of all, the basic components of a polynomial ring has to be explained. This forms the basis of

**Definition 2.1 (Monomial)** A monomial  $m$  is a product of variables over a finite field  $\mathbb{K}$ , denoted by  $\mathbb{K}[X_1, X_2, \dots, X_n]$  of the form  $X_1^{u_1} X_2^{u_2} \dots X_n^{u_n}$ , where  $u_i, 1 < i < n$  and  $u \in \mathbb{N}_0$

The total **degree** of a monomial is  $\deg(m) = \sum_{i=1}^n u_i$

**Definition 2.2 (Polynomial)** A polynomial  $f$  is a finite linear combination with coefficients  $c_u \in \mathbb{K}$  multiplied with monomials.

$$f = \sum_u c_u X^u$$

If  $c_u \neq 0$  then  $c_u x_u$  is a term of  $f$

### 2.2 Monomial Order

It is necessary to arrange the terms of a polynomial in order to compare every pair of polynomials. That is important for dividing polynomials in the finite field  $\mathbb{K}[X_1, X_2, \dots, X_n]$

**Definition 2.3 (Term Ordering)** A monomial order is a relation  $>$  on the set of all monomials in  $\mathbb{K}[x]$  such that [2] holds. Let  $m_1, m_2$  and  $m_3$  be monomials

for any pair of monomials  $m_1, m_2$  either  $m_1 > m_2$  or  $m_2 > m_1$  or  $m_1 = m_2$

if  $m_1 > m_2$  and  $m_2 > m_3$  then  $m_1 > m_3$

$m_1 > 1$  for any monomial  $m_1 \neq 1$

if  $m_1 > m_2$  then  $mm_1 > mm_2$  for any monomial  $m$

Two commonly used term orders are the following. Let  $u$  and  $v$  be elements of  $\mathbb{N}_0^n$ , such that [2]

### 2.2.1 Lexicographic Order

$u >_{lex} v$  if in  $u - v$  the left most non-zero entry is positive. This can be written as  $X^u >_{lex} X^v$  if  $u >_{lex} v$ .

### 2.2.2 Graded Lex Order

$u >_{grlex} v$  if  $deg(u) > deg(v)$  or if  $deg(u) = deg(v)$  and  $u >_{lex} v$

**Example** Let  $m_1 = 4x^2y^4z^3$  and  $m_2 = x^1y^1z^4 \in \mathbb{K}[x, y, z]$ . The monomials can also be written as  $m_1 = X^{(2\ 4\ 3)}$  and  $m_2 = X^{(1\ 1\ 4)}$ . Thus  $m_1 >_{lex} m_2$  because the left most non-zero entry of  $(2\ 4\ 3) - (1\ 1\ 4)$  is positive.

The total degree of  $m_1$  is 9 and  $deg(m_2) = 6$ . Hence,  $m_1 >_{lex} m_2$  and  $deg(m_1) > deg(m_2)$  so that  $m_1 >_{grlex} m_2$

### 2.2.3 Leading term

Given a term order  $>$ , each non-zero polynomial  $f \in \mathbb{K}[x]$  has a unique leading term, denoted by  $lt(f)$ , given by the largest involved term with respect to the term order.

If  $lt(f) = cX^u$ , where  $c \in \mathbb{K}$ , then  $c$  is the leading coefficient of  $f$  and  $X^u$  is the leading monomial(lm).[2]

**Example** Let  $f = 3x^2y^5z^3 + x^4 - 2x^3y^4 + 12^2z^2$

With respect to lex order  $f = \underline{x^4} - 2x^3y^4 + 3x^2y^5z^3 + 12^2z^2$

with respect to grlex order  $f = \underline{3x^2y^5z^3} - 2x^3y^4 + x^4 + 12^2z^2$

## 2.3 Ideals

**Definition 2.4 (Ideal)** An ideal  $I$  is collection of polynomials  $f_1, \dots, f_s \in \mathbb{K}[X_1, \dots, X_n]$  and polynomials which can be built from these with multiplication with arbitrary polynomials and linear combination, such as [1]:

This is called an Ideal generated by  $f_1, \dots, f_s$

It satisfies:

$$\langle f_1, \dots, f_s \rangle = \left\{ \sum_{i=1}^s h_i f_i \mid h_1, \dots, h_s \in \mathbb{K}[X_1, \dots, X_n] \right\}$$

$$0 \in I$$

If  $f, g \in \langle f_1, \dots, f_s \rangle$ , then  $f + g \in \langle f_1, \dots, f_s \rangle$   
 If  $f \in \langle f_1, \dots, f_s \rangle$  and  $h \in \langle f_1, \dots, f_s \rangle$ , then  $f \cdot h \in \langle f_1, \dots, f_s \rangle$

**Example** Let  $I = \langle f_1, f_2 \rangle = \langle x^2 + y, x + y + 1 \rangle$  and  $f = yx^2 + y^2 + x^2 + xy + x$ . Since  $f = y \cdot f_1 + x \cdot f_2, f \in I$



**Definition 2.5 (Binomial Ideal)** A binomial ideal  $I \in \mathbb{K}[X_1, \dots, X_n]$  is a polynomial Ideal, generated by binomials. A binomial is a linear combination of two monomials.

### 3 Division Algorithm

**4 Linear Codes**

**5 Software**

**A Appendix**