

GRÖBNER BASES  
AND COMPUTING SYZYGIES  
24th November 2004.

Notation:  $R = K[x_1, \dots, x_m]$ .

## 1 Introduction

### MOTIVATING PROBLEMS.

- Perform division with remainder and compute ideal membership:
  - given a set of generators for  $I \subset R$ , find a basis for  $R/I$ , then compute  $f \bmod I$ .
  - If  $f \in I$  (the image is zero), compute  $f$  as a linear combination of the generators of  $I$ .
- Compute syzygies: compute  $\ker(\varphi)$  for a homomorphism  $\varphi : P \rightarrow F$ , free  $R$ -modules. Equivalently, solve a homogeneous system of linear equations over  $R$ .

MONOMIALS AND TERMS. Let  $a = (a_1, \dots, a_m)$ .

- The monomial  $x^a$  is defined as

$$x^a = x_1^{a_1} \dots x_m^{a_m}.$$

- A monomial ideal: generated by monomials.
- In general, let  $F =$  finitely generated free module with basis  $\{e_i\}$ . A monomial  $m$  in  $F$  which "involves the basis element  $e_i$ " is  $m = x^a e_i$ , for some  $i$ .
- A monomial submodule of  $F$  is a submodule generated by elements  $m$  of the said form.
- A *term* is a monomial multiplied by a scalar (in  $K$ ).
- Divisibility of Monomials:  $0 \neq v, v, u \in K, m, n \in R$  monomials, then  $ume_i$  is divisible by  $vne_j$  if  $i = j$  and  $n|m$  in  $R$ .

- Note: the GCD and LCM are defined component-wise:

$$GCD(x^a, x^b) = x_1^{\min(a_1, b_1)} \dots x_m^{\min(a_m, b_m)}.$$

- The "membership problem" is easy to solve for monomial ideals of  $R$  (submodules of  $F$ ):  $f \in R$  ( $f \in F$ ) belongs to  $I$  (or  $M$ ) iff each of its monomials belongs to  $I$  (or  $M$ ).

## 2 Monomial Orders

(Why monomial orders?)

**Definition 1** *Let  $F$  be a free  $R$ -module with a basis.*

*A monomial order on  $F$  is a total order  $>$  on the monomials of  $F$  such that if  $m_1, m_2 \in F$ , monomials, and  $1 \neq n \in R$ , a monomial, then  $m_1 > m_2$  implies  $nm_1 > nm_2 > m_2$ .*

**EXAMPLES.**  $F = R$ . Always assume  $x_1 > \dots > x_m$ .

- If  $R = K[x_1]$ , the unique order on  $R$  is the ordering by degree. (Why?)

- Lexicographic order:  $x^a >_{lex} x^b$  if

$a_i > b_i$  for the first index  $i$  such that  $a_i \neq b_i$ .

Equivalently, in  $(a - b) \in \mathbb{Z}^m$ , the *first* nonzero entry is positive.

- Reverse Lexicographic order:  $x^a >_{rlex} x^b$  if

$\deg x^a > \deg x^b$ , or  $\deg x^a = \deg x^b$  and  $a_i < b_i$

for the *last* index  $i$  such that  $a_i \neq b_i$ .

**Definition 2** (*Monomial orders in modules*) Choose an order on the  $\{e_i\}$ , say,  $e_1 > \dots > e_n$ . Set  $me_i > ne_j$  if  $m >_? n$  or  $m = n$  and  $i < j$ .

**Definition 3** Fix any  $>$ . The initial term of  $f$ , denoted  $in_{>}(f) = in(f)$ , is the largest term with respect to  $>$ . If  $M \subset F$  submodule, then  $in_{>}(M) = in(M) = (in_{>}(f) | f \in M)$  is the initial submodule of  $M$ .

### 3 Gröbner Bases

Can we decide if  $f \in I = (f_1, \dots, f_s) \subset K[x_1, \dots, x_m]$  by somehow computing the remainder on division? (We conjecture so!)

**Theorem 1** (*Division Algorithm for  $K[x_1, \dots, x_m]$* )

*Let  $F$  be a free  $R$ -module with a monomial order  $>$ .*

*If  $p, f_1, \dots, f_n \in F$ , then there exists an expression*

$$p = \sum m_i f_i + r$$

*where  $r \in F$ ,  $m_i \in R$ , and **none** of the monomials of  $r$  is contained in  $(\text{in}(f_1), \dots, \text{in}(f_n))$ , and  $\text{in}(p) \geq \text{in}(m_i f_i)$ , for each  $i$ .*

*$r$  is called a remainder of  $p$  with respect to the  $f_i$ .*

*Expression above is not unique.*

Note: if  $r = 0$ , then clearly we have  $p \in (f_1, \dots, f_n)$ .

What can we say about the other direction?

**EXAMPLE:**

$$p = x^2 + \frac{y^2 z}{2} - z - 1$$

$$f_1 = x^2 + z^2 - 1$$

$$f_2 = x^2 + y^2 + (z - 1)^2 - 4$$

Then  $p = (-\frac{1}{2}z + 1)f_1 + \frac{z}{2}f_2 \in I = (f_1, f_2)$ .

Let  $>=>_{lex}$ . Use division algorithm on  $p$  with respect to  $f_1, f_2$  to get the remainder  $r = \frac{1}{2}y^2 z - z - z^2$ . Since  $p \in I, r \in I$ ; but  $r \neq 0$ !!

**PROBLEM:**  $r$  contains terms that cannot be removed by division by these particular generators for  $I$ ; because  $in(f_1)$  and  $in(f_2)$  do not divide  $in(r)$ .

**CONCLUSION:** If we have an arbitrary basis, our conjecture may not be true. So, we define:

**Definition 4** *Let  $F$  be a free  $R$ -module with basis and a monomial order  $>$ . The collection  $\{g_1, \dots, g_n\}$  is a Gröbner Basis for a submodule  $M$  of  $F$  with respect to  $>$  if*

$$in_{>}(M) = (in_{>}(g_1), \dots, in_{>}(g_n)).$$

- EXISTENCE: The ideal  $in(M)$  has a finite generating set. It consists of monomials  $x^{a(i)}$  for  $i = 1, \dots, m$ ; but by definition of  $in(M)$ ,  $\exists g_i \in M : in(g_i) = x^{a(i)}, \forall i$ .
- (good news!) If  $G$  is a Gröbner Basis for  $M \subset F$ , then  $\forall f \in M$ , the remainder  $r$  with respect to  $G$  is zero.
- Thus, if  $G = \{g_1, \dots, g_n\}$  is such a basis for  $M$ , then  $M = (g_1, \dots, g_n)$ .
- Application: Once we can compute  $G$  of an ideal  $I \subset R$ , we can solve the ideal membership problem for  $I$ .

### 3.1 Computation of Gröbner Bases

$F$  a free module over  $R$  with basis and monomial order  $>$ . Let  $(g_1, \dots, g_n) = M \subset F$  be a submodule.

For each pair of indices  $i, j$  such that  $\text{in}(g_i)$  and  $\text{in}(g_j)$  involve the same basis element of  $F$ , define

$$m_{ij} = \frac{\text{in}(g_i)}{\text{GCD}(\text{in}(g_i), \text{in}(g_j))} \in R.$$

For each pair  $i, j$ , choose a standard expression (given by the division algorithm)

$$m_{ji}g_i - m_{ij}g_j = \sum_u f_u^{(ij)} g_u + h_{ij}$$

with respect to the  $g_i$ . Note that  $\text{in}(f_u^{(ij)} g_u) < \text{in}(m_{ji}g_i)$ .

We set  $h_{ij} = 0$  if  $\text{in}(g_i), \text{in}(g_j)$  involve different basis elements of  $F$ .

**Theorem 2 (Buchberger's Algorithm)** *Suppose  $M \subset F$  is a submodule, and let  $M = (g_1, \dots, g_n)$  for some elements  $g_i$ . Compute the remainders  $h_{ij}$ . If all  $h_{ij} = 0$ , the  $g_i$  form a Gröbner basis. If some  $h_{ij} \neq 0$ , then replace  $\{g_1, \dots, g_n\}$  by  $\{g_1, \dots, g_n, h_{ij}\}$  and repeat the process. The process must terminate after finitely many steps.*

**APPLICATION.** The algorithm above gives a linear combination of  $g_i$  equal to  $h_{ij}$ . So if the remainder  $h_{ij} = 0$ , we get a linear relation on the  $g_i$ , that is, a syzygy. It turns out that these syzygies generate the entire syzygy module on the  $g_i$ , given the right order  $>$ .

Note also that as  $R$  is noetherian, the syzygy module is finitely generated; so we "know" all syzygies on a set of generators if we can find the generators for the syzygy module.

First, we introduce some new notation.

Let  $\bigoplus_i R\epsilon_i$  be a free module with basis  $\epsilon_i$  corresponding to the elements  $g_i$  of  $F$  with the map

$$\varphi : \bigoplus R\epsilon_i \rightarrow M$$

$$\epsilon_i \rightarrow g_i$$

as the corresponding map. Set

$$\sigma_{ij} = m_{ji}\epsilon_i - m_{ij}\epsilon_j.$$

The elements  $\sigma_{ij}$  generate the syzygies on the elements  $in(g_i)$ .

For  $i < j$  such that  $in(g_i)$  and  $in(g_j)$  involve the same basis element of  $F$ , set

$$\tau_{ij} = m_{ji}\epsilon_i - m_{ji}\epsilon_j - \sum_u f_u^{ij} \epsilon_u.$$

**Theorem 3 (Schreyer)** *Suppose that  $\{g_1, \dots, g_n\} = G$  is a Gröbner Basis. Let  $>$  be the monomial order on  $\bigoplus_{j=1}^n R\epsilon_j$  defined by:  $m\epsilon_u > n\epsilon_v$  iff  $\text{in}(mg_u) > \text{in}(ng_v)$  with respect to the given order on  $F$ , or  $\text{in}(ng_u) = \text{in}(mg_v)$  but  $u < v$ .*

*The  $\tau_{ij}$  generate the syzygies on the  $g_i$ . In fact, they are a Gröbner Basis for the syzygies with respect to  $>$ , and  $\text{in}(\tau_{ij}) = m_{ji}\epsilon_i$ .*

**COMMENTS.**

- As promised, this provides a way to obtain free resolutions.

- *rllex* is the order of choice for most computations.
- For a submodule  $M$  of  $F$ , a free module with basis, and any  $>$  on  $F$ . Then:

$$B = \{m : m \notin \text{in}_>(M), m \text{ a monomial}\}$$

form a basis for  $F/M$ ; and:

$$h_{F/M}(j) = h_{F/\text{in}(M)}(j)$$