

# PhD Seminars 2002/2003: Gareth Evans Semester 3

Gareth Evans

June 10, 2003

## Contents

<b>1 Seminar 1: 10th June 2003</b>	<b>2</b>
1.1 The Gröbner Walk . . . . .	2
1.1.1 Gröbner Bases . . . . .	2
1.1.2 Why do we need the Gröbner Walk? . . . . .	2
1.1.3 Algorithm for the Gröbner Walk . . . . .	4
1.1.4 Worked Example . . . . .	5

# 1 Seminar 1: 10th June 2003

## 1.1 The Gröbner Walk

### 1.1.1 Gröbner Bases

Recall that an ideal is represented by a set of polynomials and that an arbitrary polynomial is said to be a member of an ideal  $I$  if it can be represented as a linear polynomial combination of the polynomials generating  $I$ . Deciding whether a polynomial belongs to an ideal is known as the Ideal Membership Problem.

A Gröbner Basis is a set of polynomials generating an ideal  $I$  with the property that, given an arbitrary polynomial  $p$ , the remainder when we divide  $p$  by the polynomials generating  $I$  is unique. In particular, we can solve the Ideal Membership Problem given a Gröbner Basis by testing to see whether the remainder on division by the polynomials generating the Gröbner Basis is zero or not.

Given a set of polynomials generating an ideal  $I$ , we can transform this set of polynomials to an equivalent set of polynomials generating  $I$  forming a Gröbner Basis by applying Buchberger's Algorithm (Bruno Buchberger invented this algorithm whilst working on his PhD thesis, the supervisor for this thesis being Wolfgang Gröbner). Put simply, the algorithm computes the ' $S$ -polynomial' of every pair of polynomials in the current basis and adds this  $S$ -polynomial to the basis if its remainder on division by the polynomials in the current basis is not zero.

The  $S$ -polynomial is the crucial factor in why we require the Gröbner Walk, as it involves choosing a term order on polynomials:

$$S(f_1, f_2) = \frac{\text{lcm}(\text{lm}(f_1), \text{lm}(f_2))}{\text{lm}(f_1)} f_1 - \frac{\text{lcm}(\text{lm}(f_1), \text{lm}(f_2))}{\text{lm}(f_2)} f_2.$$

There are many ways of choosing the lead monomial of a polynomial  $p$  ( $\text{lm}(p)$ ), examples being the lexicographic and the degree-lexicographic orderings (alphabetical and total-degree-then-alphabetical).

### 1.1.2 Why do we need the Gröbner Walk?

It turns out that the choice of ordering is crucial to the time the algorithm takes to run on a computer. For example, consider the following ideal  $I$ :

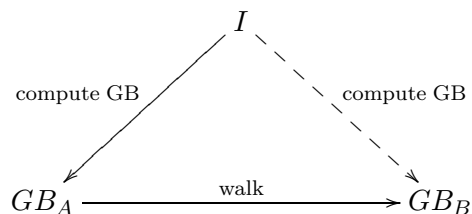
$$I = \langle xy^3 + y^4 + yz^2 - z^3 - 2xz^3, 2x^2y + x^3y + 2xy^2z, 2 - 3x^2y + 2x^3y + yz^3 \rangle.$$

Using my Gröbner Basis programs, I can compute a degree-lexicographic Gröbner Basis for  $I$  in seconds but cannot compute a lexicographic Gröbner Basis for  $I$  (I have left the algorithm running for an hour without termination). This poses a problem because some of the most important applications

of Gröbner Bases depend on using the lexicographic ordering. For example, we can solve systems of polynomial equations using the lexicographic ordering.

The Gröbner Walk overcomes this hurdle by starting off with a Gröbner Basis for  $I$  with respect to some ordering  $A$ , an ordering chosen so that the Gröbner Basis is computed quickly w.r.t.  $A$ . The ‘walk’ itself then involves morphing the Gröbner Basis we have for  $A$  into a Gröbner Basis for a target ordering  $B$ . Usually, the two orderings chosen are  $A = \text{degree-reverse-lexicographic}$  and  $B = \text{lexicographic}$ .

The Gröbner Walk is useful because the two-fold process of the Gröbner Walk usually takes a shorter amount of time than computing the Gröbner Basis directly for  $B$ . The theory is that the following triangle is commutative:



I used the word ‘morphing’ above to describe what happens during the Gröbner Walk. What we actually ‘morph’ is matrices: one matrix to another matrix; and these matrices represent the source and target orderings. For example, the degree-lexicographic and lexicographic orderings are represented by the following matrices  $A$  and  $B$ :

$$A = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}; \quad B = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

### 1.1.3 Algorithm for the Gröbner Walk

I will now attempt to explain the algorithm involved in implementing the Gröbner Walk.

- Start with a Gröbner Basis  $G(I, <_A)$ , where  $<_A$  is a term order with associated matrix  $A$ . Let  $\sigma$  be the first row of  $A$ .
- Assume that we are given a target ordering  $<_B$  with associated matrix  $B$ . Let  $\tau$  be the first row of  $B$ .
- Keep the first row of  $A$  as it is and replace the rest of the matrix by the matrix  $B$  to give a matrix  $O$ . Let  $\omega = \sigma$ .
- Repeat the following until the algorithm terminates:
  - (1) Calculate the initials of the current Gröbner Basis with respect to  $\omega$  to give a set of polynomials of size  $r$ . (The initial of a polynomial  $p$  is those terms in  $p$  which have maximal  $\omega$ -degree, where  $\omega$ -degree means the value given by evaluating  $p$  at  $\omega$ . For example, if  $\omega = 0101$  and  $p = w^4x^3y^2z$ , then the  $\omega$ -degree of  $p$  is (with the usual alphabet)  $(0 \times 4) + (1 \times 3) + (0 \times 2) + (1 \times 1) = 4$ ).
  - (2) Sort these initials with respect to the matrix  $(\omega, B) = O$  to give a set of polynomials  $G_\omega$  of size  $r$ . Note:  $G_\omega$  is a Gröbner Basis of  $\langle \text{in}_\omega(I) \rangle$  with respect to the old ordering as  $\omega$  is compatible<sup>1</sup> with the old ordering on the old Gröbner Basis.
  - (3) Calculate the Gröbner Basis of  $G_\omega$  w.r.t.  $(\omega, B)$  to give a set of polynomials  $G_\omega^+$ . Interreduce  $G_\omega^+$  w.r.t.  $(\omega, B)$ .
  - (4) Lift  $G_\omega^+$  to give a new Gröbner Basis as follows:
    - \* Express all polynomials  $m_i \in G_\omega^+$  as  $m_i = \sum_{j=1}^r h_{ij}n_j$ , where  $n_j \in G_\omega$  and  $h_{ij}$  are arbitrary polynomials (i.e. apply the division algorithm).
    - \* Replace all the  $n_j$ 's by the full polynomials  $g_j$ , where the initial of  $g_j$  w.r.t.  $\omega$  is  $n_j$ . Interreduce the Gröbner Basis w.r.t.  $(\omega, B)$ .
  - (5) We now need to calculate the next vector on the walk. We define  $\omega_{k+1} = \omega(t) = \omega_k + t(\tau - \omega_k)$ ,  $0 < t \leq 1$ , where

$$t = \min(\{s \mid \deg_{\omega(s)}(p_1) = \deg_{\omega(s)}(p_i), \deg_{\omega(0)}(p_1) \neq \deg_{\omega(0)}(p_i), \\ g = p_1 + \dots + p_n, g \in G(I, <_k)\} \cap [0, 1]),$$

i.e. if  $\omega_k$  differs on  $p_1$  and some  $p_i$ , then  $w_{k+1}$  does not differ on  $p_1$  and some  $p_i$ . Now if  $t$  is undefined then we have finished the walk; else set  $\omega = (1 - t)\omega + t\tau$  and go back to step 1. Note: the next weight vector is the point on the path where some (other) initial forms of the reduced current Gröbner Basis degenerate<sup>2</sup>.

---

<sup>1</sup>A weight vector  $\omega$  is compatible with a term ordering  $<$  on  $G$ , if for each polynomial  $g = m_1 + \dots + m_s \in G$  ordered in descending order with respect to  $<$ ,  $\deg_\omega(m_1) \geq \deg_\omega(m_i)$  holds for all  $1 < i \leq s$ .

<sup>2</sup>The initial form of a polynomial  $g$  as defined above degenerates with respect to  $\omega$  if  $\deg_\omega(m_1) = \deg_\omega(m_2)$ .

### 1.1.4 Worked Example

Input Ideal:  $I = \langle xy - z, yz + 2x + z \rangle$ .

Alphabet:  $x > y > z$ .

Source Order: Length-lex; matrix  $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ .

Target Order: Lex; matrix  $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ .

Source Gröbner Basis:  $\langle xy - z, yz + 2x + z, 2x^2 + xz + z^2 \rangle$ .

Target Gröbner Basis (what we want to obtain):  $\langle x + \frac{1}{2}yz + \frac{1}{2}z, \frac{1}{2}y^2z + \frac{1}{2}yz + z \rangle$ .

$$\text{Recall that } S(f_1, f_2) = \frac{\text{lcm}(\text{lm}(f_1), \text{lm}(f_2))}{\text{lm}(f_1)} f_1 - \frac{\text{lcm}(\text{lm}(f_1), \text{lm}(f_2))}{\text{lm}(f_2)} f_2.$$

Initialisation:  $\omega = (1, 1, 1)$ ,  $\tau = (1, 0, 0)$ ,  $O = (\omega, B) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ .

**Remark 1.1** As  $A \equiv O$  the Gröbner Basis we will obtain in Pass 1 will be the same as the source Gröbner Basis, but I will go through the steps all the same for consistency.

#### Pass 1

- (1) Initials of source Gröbner Basis w.r.t.  $\omega = \{xy, yz, 2x^2 + xz + z^2\}$  (terms which have maximal  $(1, 1, 1)$ -degree).
- (2) Sort terms w.r.t.  $O$ :  $G_\omega = \{x^2 + \frac{1}{2}xz + \frac{1}{2}z^2, xy, yz\}$ .
- (3) Calculate Gröbner Basis of  $G_\omega$  w.r.t.  $O$ . Let  $G_\omega = \{f, g, h\}$ . Then

$$\begin{aligned} S(f, g) &= \frac{x^2y}{x^2}(x^2 + \frac{1}{2}xz + \frac{1}{2}z^2) - \frac{x^2y}{xy}(xy) \\ &= \frac{1}{2}x^3yz + \frac{1}{2}x^2yz^2 \\ &= xy(\frac{1}{2}x^2z + \frac{1}{2}xz^2) \\ &\rightarrow 0 \text{ by } g; \\ S(f, h) &= 0 \text{ (GCD} = 0\text{)}; \\ S(g, h) &= \frac{xyz}{xy}xy - \frac{xyz}{yz}yz \\ &= 0. \end{aligned}$$

It follows that  $G_\omega^+ = G_\omega$ . No interreduction is possible at this point.

- (4) As  $G_\omega^+ = G_\omega$ , it follows that the new Gröbner Basis is equal to the old one, so that our new Gröbner Basis is equal to  $\langle xy - z, yz + 2x + z, 2x^2 + xz + z^2 \rangle$ , with  $\omega_k$ -values

$$\langle 2 - 1, 2 + 1 + 1, 2 + 2 + 2 \rangle.$$

- (5) Let

$$\begin{aligned} \omega_{k+1} &= \omega_k + t(\tau - \omega_k) \\ &= (1, 1, 1) + t((1, 0, 0) - (1, 1, 1)) \\ &= (1, 1, 1) + t(0, -1, -1) \\ &= (1, 1 - t, 1 - t). \end{aligned}$$

To find the minimum value of  $t$ , we must find the minimum value of  $t$  such that the  $\omega_{k+1}$ -value of the first term in a polynomial in the Gröbner Basis and some other term in the same polynomial agree where they currently differ on  $\omega_k$ .

As all the  $\omega_k$ -values of terms in  $h$  are the same, we can ignore it. But the  $\omega_k$ -values of the two terms in  $f$  differ, so we can choose a value of  $t$  such that

$$\begin{aligned} \omega_{k+1}(xy) &= \omega_{k+1}(z) \\ 1 + (1 - t) &= (1 - t) \\ 1 &= 0 \text{ (inconsistent)}. \end{aligned}$$

For  $g$ , we have two choices: either

$$\begin{aligned} \omega_{k+1}(yz) &= \omega_{k+1}(2x) \\ (1 - t) + (1 - t) &= 1 \\ 2 - 2t &= 1 \\ t &= \frac{1}{2}; \end{aligned}$$

or

$$\begin{aligned} \omega_{k+1}(yz) &= \omega_{k+1}(z) \\ (1 - t) + (1 - t) &= (1 - t) \\ (1 - t) &= 0 \\ t &= 1. \end{aligned}$$

It follows that the minimum value of  $t$  is  $\frac{1}{2}$ . Therefore, the new value of  $\omega$  is  $(1, \frac{1}{2}, \frac{1}{2})$  and the

new value of  $O$  is  $\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ .

**Pass 2**

- (1) Initials of current Gröbner Basis w.r.t.  $\omega = \{xy, yz + 2x, 2x^2\}$  (terms which have maximal  $(1, \frac{1}{2}, \frac{1}{2})$ -degree).
- (2) Sort terms w.r.t.  $O$ :  $G_\omega = \{x^2, xy, x + \frac{1}{2}yz\}$ .
- (3) Calculate Gröbner Basis of  $G_\omega$  w.r.t.  $O$ . Let  $G_\omega = \{f, g, h\}$ . Then

$$\begin{aligned}
 S(f, g) &= \frac{x^2y}{x^2}(x^2) - \frac{x^2y}{xy}(xy) \\
 &= 0; \\
 S(f, h) &= \frac{x^2}{x^2}x^2 - \frac{x^2}{x}(x + \frac{1}{2}yz) \\
 &= -\frac{1}{2}xyz \\
 &\rightarrow 0 \text{ by } g; \\
 S(g, h) &= \frac{xy}{xy}xy - \frac{xy}{x}(x + \frac{1}{2}yz) \\
 &= -\frac{1}{2}y^2z \equiv y^2z = i \text{ (definition);} \\
 S(f, i) &= 0 \text{ (GCD = 0);} \\
 S(g, i) &= \frac{xy^2z}{xy}xy - \frac{xy^2z}{y^2z}y^2z = 0; \\
 S(h, i) &= 0 \text{ (GCD = 0).}
 \end{aligned}$$

It follows that  $G_\omega^+ = \{x^2, xy, x + \frac{1}{2}yz, y^2z\}$ . Further, the following interreduction is possible:

$$\begin{aligned}
 f = x^2 = x(x) &\rightarrow x(-\frac{1}{2}yz) \text{ (by } h) \\
 &\rightarrow 0 \text{ (by } g); \\
 g = xy = (x)y &\rightarrow (-\frac{1}{2}yz)y \text{ (by } h) \\
 &\rightarrow 0 \text{ (by } i).
 \end{aligned}$$

Therefore after interreduction we have  $G_\omega^+ = \{x + \frac{1}{2}yz, y^2z\}$ .

- (5) We must now express the two elements of  $G_\omega^+$  as polynomial combinations of the elements of  $G_\omega = \{f, g, h\}$ :

$$\begin{aligned}
 x + \frac{1}{2}yz &= 1(h); \\
 y^2z &= 2y(x + \frac{1}{2}yz) - 2(xy) \text{ (from the calculation of the } S\text{-polynomial)} \\
 &= 2y(h) - 2(g).
 \end{aligned}$$

Lifting to the full polynomials,  $1(h)$  lifts to give the polynomial  $yz + 2x + z$ , while  $2y(h) - 2(g)$  lifts to give the polynomial  $2y(yz + 2x + z) - 2(xy - z) = 2y^2z + 4xy + 2yz - 2xy + 2z = y^2z + xy + yz + z$ .

Interreducing, the latter polynomial reduces as follows:

$$\begin{aligned}
xy + y^2z + yz + z &\rightarrow \left(-\frac{1}{2}yz - \frac{1}{2}z\right)y + y^2z + yz + z \\
&= -\frac{1}{2}y^2z - \frac{1}{2}yz + y^2x + yz + z \\
&= \frac{1}{2}y^2z + \frac{1}{2}yz + z.
\end{aligned}$$

Conclusion: our new Gröbner Basis is  $\langle 2x + yz + z, y^2z + yz + 2z \rangle$  with  $\omega_k$ -values

$$\langle 1 + 1 + \frac{1}{2}, 1\frac{1}{2} + 1 + \frac{1}{2} \rangle$$

(5) Let

$$\begin{aligned}
\omega_{k+1} &= \omega_k + t(\tau - \omega_k) \\
&= \left(1, \frac{1}{2}, \frac{1}{2}\right) + t\left(\left(1, 0, 0\right) - \left(1, \frac{1}{2}, \frac{1}{2}\right)\right) \\
&= \left(1, \frac{1}{2}, \frac{1}{2}\right) + t\left(0, -\frac{1}{2}, -\frac{1}{2}\right) \\
&= \left(1, \frac{1}{2}(1-t), \frac{1}{2}(1-t)\right).
\end{aligned}$$

For the first polynomial in our Gröbner Basis, we can have

$$\begin{aligned}
\omega_{k+1}(x) &= \omega_{k+1}(z) \\
1 &= \frac{1}{2}(1-t) \\
t &= -1 \text{ (must be in } [0, 1])
\end{aligned}$$

For the second polynomial, we can have

$$\begin{aligned}
\omega_{k+1}(y^2z) &= \omega_{k+1}(yz) \\
3\left(\frac{1}{2}(1-t)\right) &= 2\left(\frac{1}{2}(1-t)\right) \\
\frac{1}{2}(1-t) &= 0 \\
t &= 1;
\end{aligned}$$

or

$$\begin{aligned}
\omega_{k+1}(y^2z) &= \omega_{k+1}(yz) \\
3\left(\frac{1}{2}(1-t)\right) &= \frac{1}{2}(1-t) \\
1-t &= 0 \\
t &= 1.
\end{aligned}$$

It follows that the minimum value of  $t$  is 1. Therefore, the new value of  $\omega$  is  $(1, 0, 0)$  and the

$$\text{new value of } O \text{ is } \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

### Pass 3

- (1) Initials of current Gröbner Basis w.r.t.  $\omega = \{2x, y^2z\}$  (terms which have maximal  $(1, 0, 0)$ -degree).
- (2) Sort terms w.r.t.  $O$ :  $G_\omega = \{x, y^2z\}$ .
- (3) Calculate Gröbner Basis of  $G_\omega$  w.r.t.  $O$ . Let  $G_\omega = \{f, g\}$ . Then

$$S(f, g) = 0 \text{ (GCD} = 0\text{)}.$$

It follows that  $G_\omega^+ = \{x, y^2z\}$ .

- (4) As  $G_\omega^+ = G_\omega$ , it follows that the new Gröbner Basis is equal to the old one, so that our new Gröbner Basis is  $\langle 2x + yz + z, y^2z + yz + 2z \rangle$ .
- (5) As  $O = B$  and as  $\omega = \tau$ , we have arrived at the target ordering and hence the Gröbner Basis for  $I$  with respect to the Lex ordering is

$$\langle 2x + yz + z, y^2z + yz + 2z \rangle.$$

This is verified by comparing it to the results stated at the beginning of this example.