INTRODUCTION TO GRÖBNER BASES

Patrick Fitzpatrick

University College Cork
Ireland

S^3Cm, 2–11 July 2008

Let $R = \mathbb{K}[x_1, \ldots, x_n]$ where $\mathbb{K}$ is a field.
An **ideal** I in R is a subset such that

- $0 \in I$
- $\forall f, g \in I$ we have that $f - g \in I$.
- $\forall f \in I$, $\forall a \in R$ we have that $af \in I$.

Let $R = \mathbb{K}[x_1, \ldots, x_n]$ where $\mathbb{K}$ is a field.
An **ideal** I in R is a subset such that

- $0 \in I$
- $\forall f, g \in I$ we have that $f - g \in I$.
- $\forall f \in I$, $\forall a \in R$ we have that $af \in I$.

Basic Property of R

Any ideal I of R is finitely generated, i.e., there exist $f_1, \ldots, f_r \in R$ such that

$$I = \langle f_1, \ldots, f_r \rangle = \{\sum_{i=1}^{r} h_i f_i \mid h_i \in R\}.$$

Motivating Problems

Problem 1: Ideal Membership

Given a polynomial f in R determine whether f is in I or not.

Motivating Problems

Problem 1: Ideal Membership

Given a polynomial f in R determine whether f is in I or not.

Problem 2

If $f \in I$, determine polynomials $u_1, \ldots, u_r \in R$ such that $u_1 f_1 + \cdots + u_r f_r = f$.

Motivating Problems

Problem 1: Ideal Membership

Given a polynomial f in R determine whether f is in I or not.

Problem 2

If $f \in I$, determine polynomials $u_1, \ldots, u_r \in R$ such that $u_1 f_1 + \cdots + u_r f_r = f$.

Problem 3

Determine a basis of R/I as $\mathbb{K}$-vector space.

Easy Case

If $R = \mathbb{K}[x]$ then R is a **principal ideal domain** (PID), which means that $I = \langle f_1, \ldots, f_r \rangle = \langle g = gcd(f_1, \ldots, f_r) \rangle$. Thus, to solve the ideal membership problem for given $f \in I$ we just divide f by g. If the remainder is 0 then $f \in I$ otherwise $f \notin I$.

Easy Case

If $R = \mathbb{K}[x]$ then R is a **principal ideal domain** (PID), which means that $I = \langle f_1, \ldots, f_r \rangle = \langle g = gcd(f_1, \ldots, f_r) \rangle$. Thus, to solve the ideal membership problem for given $f \in I$ we just divide f by g. If the remainder is 0 then $f \in I$ otherwise $f \notin I$.

General Case

R is not a PID. Consider $I = \langle xy - x, y + 1 \rangle$ and $f = xy$. It's not clear how to do "division" but naively dividing f first by $xy - x$ leaves remainder x and dividing it first by $y + 1$ we obtain remainder $-x$. But note that

$$f = \frac{1}{2}(xy - x) + \frac{x}{2}(y + 1).$$

In the previous example there are two things not clear **a priori**:

- Why should we write $xy - x$ rather than $-x + xy$?
- How can we "divide" polynomials in several variables?

In the previous example there are two things not clear **a priori**:

- Why should we write $xy - x$ rather than $-x + xy$?
- How can we "divide" polynomials in several variables?

For the first question we need to introduce the notion of **term order** in the set of **terms** $\mathbb{T}^n = \{\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha \in \mathbb{Z}^n_{\geq 0}\}$.

A **term order** $<$ in $\mathbb{T}^n$ is a total order satisfying:

1. $1 < \mathbf{x}^\alpha$ for every $\mathbf{x}^\alpha \in \mathbb{T}^n$
2. If $\mathbf{x}^\alpha < \mathbf{x}^\beta$ then $\mathbf{x}^\alpha \mathbf{x}^\gamma < \mathbf{x}^\beta \mathbf{x}^\gamma$ for every $\mathbf{x}^\gamma \in \mathbb{T}^n$.

Most important orders

We define the **(total) degree** $\deg(\mathbf{x}^\alpha)$ of the term $\mathbf{x}^\alpha$ as the sum $\alpha_1 + \cdots + \alpha_n$.

Most important orders

We define the **(total) degree** $\deg(\mathbf{x}^\alpha)$ of the term $\mathbf{x}^\alpha$ as the sum $\alpha_1 + \cdots + \alpha_n$.

Lexicographical order

$\mathbf{x}^\alpha <_{lex} \mathbf{x}^\beta :\Leftrightarrow \exists 1 \leq i \leq n : \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i.$

Most important orders

We define the **(total) degree** $\deg(\mathbf{x}^\alpha)$ of the term $\mathbf{x}^\alpha$ as the sum $\alpha_1 + \cdots + \alpha_n$.

Lexicographical order

$\mathbf{x}^\alpha <_{lex} \mathbf{x}^\beta :\Leftrightarrow \exists 1 \leq i \leq n : \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i$.

Degree lexicographical order

$\mathbf{x}^\alpha <_{deglex} \mathbf{x}^\beta :\Leftrightarrow \deg \mathbf{x}^\alpha < \deg \mathbf{x}^\beta$ or $\deg \mathbf{x}^\alpha = \deg \mathbf{x}^\beta$ and $\exists 1 \leq i \leq n : \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i$.

Most important orders

We define the **(total) degree** $\deg(\mathbf{x}^\alpha)$ of the term $\mathbf{x}^\alpha$ as the sum $\alpha_1 + \cdots + \alpha_n$.

Lexicographical order

$\mathbf{x}^\alpha <_{lex} \mathbf{x}^\beta :\Leftrightarrow \exists 1 \leq i \leq n : \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i.$

Degree lexicographical order

$\mathbf{x}^\alpha <_{deglex} \mathbf{x}^\beta :\Leftrightarrow \deg \mathbf{x}^\alpha < \deg \mathbf{x}^\beta$ or $\deg \mathbf{x}^\alpha = \deg \mathbf{x}^\beta$ and $\exists 1 \leq i \leq n : \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i.$

Degree reverse lexicographical order

$\mathbf{x}^\alpha <_{degrevlex} \mathbf{x}^\beta :\Leftrightarrow \deg \mathbf{x}^\alpha < \deg \mathbf{x}^\beta$ or $\deg \mathbf{x}^\alpha = \deg \mathbf{x}^\beta$ and $\exists 1 \leq i \leq n : \alpha_n = \beta_n, \ldots, \alpha_{i+i} = \beta_{i+1}, \alpha_i > \beta_i.$

Let $<$ be a term order and $f \in R$, $f \neq 0$. We may write f uniquely in the form

$$f = a_\alpha \mathbf{x}^\alpha + a_\beta \mathbf{x}^\beta + \cdots + a_\gamma \mathbf{x}^\gamma,\ \alpha > \beta > \cdots > \gamma.$$

then we denote,

1. $lt_<(f) = \mathbf{x}^\alpha =$ the leading term of f.
2. $lm_<(f) = a_\alpha \mathbf{x}^\alpha =$ the leading monomial of f.
3. $lc_<(f) = a_\alpha =$ the leading coefficient of f.

Notice that these definitions depend on the particular order $<$.

Division in R

Given any order $>$ in $\mathbb{T}^n$ and an (ordered) sequence of polynomials $f_1, \ldots, f_s \in R$, we may write every $f \in R$ as

$$f = u_1 f_1 + \ldots + u_s f_s + r$$

where $u_i, r \in R$ and r is either zero or a linear combination of terms none of which is divisible by any element of $\{lt_<(f_i)\}_{i=1}^s$.

Division in R

Given any order $>$ in $\mathbb{T}^n$ and an (ordered) sequence of polynomials $f_1, \ldots, f_s \in R$, we may write every $f \in R$ as

$$f = u_1 f_1 + \ldots + u_s f_s + r$$

where $u_i, r \in R$ and r is either zero or a linear combination of terms none of which is divisible by any element of $\{lt_<(f_i)\}_{i=1}^s$.

As we saw earlier the remainder may depend on the order of the polynomials in the sequence i.e. the order in which the divisions are carried out. Also, $r \neq 0$ does not necessarily mean that $f \notin \langle f_1, \ldots, f_s \rangle$ (we would like this to be the case).

Gröbner bases

Given a term order $<$ and an ideal I in R, we say that $\{g_1, \ldots, g_s\} \subset R$ is a **Gröbner basis** of I with respect to $<$ if

$$\langle lt_<(g_1), \ldots, lt_<(g_s) \rangle = \langle lt_<(I) \rangle$$

where $lt_<(I) = \{lt_<(f) \mid f \in I\}$. In other words G is a Gröbner basis of I if for each $f \in I$ there is a $g \in G$ such that $lt(g)$ divides $lt(f)$.

Gröbner bases

Given a term order $<$ and an ideal I in R, we say that $\{g_1, \ldots, g_s\} \subset R$ is a **Gröbner basis** of I with respect to $<$ if

$$\langle lt_<(g_1), \ldots, lt_<(g_s) \rangle = \langle lt_<(I) \rangle$$

where $lt_<(I) = \{lt_<(f) \mid f \in I\}$. In other words G is a Gröbner basis of I if for each $f \in I$ there is a $g \in G$ such that $lt(g)$ divides $lt(f)$.

A Gröbner basis exists with respect to any term order. Each Gröbner basis of I is a generating set of I.

Answer to Problems 1 and 2

If $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis of the ideal $I \subset R$ then the remainder on division of $f \in R$ by G is unique (independent of the order in which the divisions are carried out) and it is zero if and only if $f \in I$. We denote the remainder by $\overline{f}^G = r$.

Answer to Problems 1 and 2

If $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis of the ideal $I \subset R$ then the remainder on division of $f \in R$ by G is unique (independent of the order in which the divisions are carried out) and it is zero if and only if $f \in I$. We denote the remainder by $\overline{f}^G = r$.

Answer to Problem 3

f may be written in a unique way as,

$$f = g + r,$$

where $g \in I$ and no term of r is divisible by any term of $lt_<(g_i)$, $1 \leq i \leq s$. The set of terms each of which is less than every element of $lt_<(g_i)$ thus forms a basis of R/I as $\mathbb{K}$-vector space.

Computing Gröbner bases

The main tool for computing Gröbner Bases are the S-**polynomials.**

For any two non-zero polynomials $f, g \in R$ and a monomial order $<$, the S-polynomial of f and g is,

$$S(f,g) = \frac{\mathbf{x}^\gamma}{lm_<(f)} f - \frac{\mathbf{x}^\gamma}{lm_<(g)} g$$

where $\mathbf{x}^\gamma = lcm\{lt_<(f), lt_<(g)\}$.

Computing Gröbner bases

The main tool for computing Gröbner Bases are the *S*-**polynomials.**

For any two non-zero polynomials $f, g \in R$ and a monomial order $<$, the S-polynomial of f and g is,

$$S(f,g) = \frac{\mathbf{x}^{\gamma}}{lm_{<}(f)} f - \frac{\mathbf{x}^{\gamma}}{lm_{<}(g)} g$$

where $\mathbf{x}^{\gamma} = lcm\{lt_{<}(f), lt_{<}(g)\}$.

Buchberger's Theorem

$G = \{g_1, \ldots, g_s\}$ is a Gröbner basis of I with respect to $<$ if and only if

$$\overline{S(g_i, g_j)}^{G} = 0, 1 \leq i, j \leq s, i \neq j.$$

Buchberger's Algorithm

Input: $I = \langle F \rangle := \langle \{f_1, \ldots, f_s\} \rangle$ and a term order $<$.
Output: G a Gröbner basis of I with respect to $<$.

1. $G = F$, $G' = \{\}$.
2. **while** $G \neq G'$ **do**
3. $G' = G$
4. **for** each pair $\{p, q\} \subset G'$ **do**
5. $r = S(p, q)$ reduced by G'
6. **if** $r \neq 0$ **then**
7. $G = G \cup \{r\}$
8. **end if**
9. **end for**
10. **end while**

Minimal Gröbner bases

A Gröbner basis G is **minimal** if

1. $\forall\, g \in G$, $lc_<(g) = 1$.
2. $\forall\, g \in G$, $lt_<(g) \notin \langle lt_<(G \setminus \{g\}) \rangle$.

Minimal Gröbner bases

A Gröbner basis G is **minimal** if

1. $\forall\, g \in G$, $lc_<(g) = 1$.
2. $\forall\, g \in G$, $lt_<(g) \notin \langle lt_<(G \setminus \{g\})\rangle$.

Reduced Gröbner bases

A Gröbner basis G is **reduced** if

1. $\forall\, g \in G$, $lc_<(g) = 1$.
2. $\forall\, g \in G$, no term of g is in $\langle lt_<(G \setminus \{g\})\rangle$.

Minimal Gröbner bases

A Gröbner basis G is **minimal** if

1. $\forall\, g \in G$, $lc_<(g) = 1$.
2. $\forall\, g \in G$, $lt_<(g) \notin \langle lt_<(G \setminus \{g\}) \rangle$.

Reduced Gröbner bases

A Gröbner basis G is **reduced** if

1. $\forall\, g \in G$, $lc_<(g) = 1$.
2. $\forall\, g \in G$, no term of g is in $\langle lt_<(G \setminus \{g\}) \rangle$.

Theorem

For any term order there exists a unique reduced Gröbner basis.

Gröbner bases for modules

Let $A = \mathbb{K}[x_1, \ldots, x_n]^s = R^s$ so elements of A are vectors of polynomials with vector addition and subtraction and multiplication by scalars $f(x) \in R$. A **submodule** M in A is a subset such that

- $0 \in M$.
- $\forall f, g \in M$ we have that $f - g \in M$.
- $\forall f \in M$, $\forall a \in R$ we have that $af \in M$.

Each submodule of A is finitely generated.

Gröbner bases for modules

Let $A = \mathbb{K}[x_1, \ldots, x_n]^s = R^s$ so elements of A are vectors of polynomials with vector addition and subtraction and multiplication by scalars $f(x) \in R$. A **submodule** M in A is a subset such that

- $0 \in M$.
- $\forall f, g \in M$ we have that $f - g \in M$.
- $\forall f \in M$, $\forall a \in R$ we have that $af \in M$.

Each submodule of A is finitely generated.

Define terms in A as $X\mathbf{e}_i$ where X is a term in R and $\mathbf{e}_i$ is a standard basis vector. Typical term order is *position over term (POT)* order. We start with a term order $<$ in R and then define $<_{POT}$ by: $X\mathbf{e}_i <_{POT} Y\mathbf{e}_j$ if $i < j$ or if $i = j$ and $X < Y$.

Define $lcm(X\mathbf{e}_i, Y\mathbf{e}_j) = 0$ if $i \neq j$ and $lcm(X, Y)\mathbf{e}_i$ if $i = j$. Then can construct Gröbner bases as usual.