Groebner Bases

Jianhua fan

April 7, 2006

1 Commutative Ring, Field and Ideal

Commutative Ring: consist of a set R and two binary operations "$\cdot$" and "+" defined on R for which the following conditions are satisfied, given$a, b, c \in R$:

1. $(a + b) + c = a + (b + c) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $a + b = b + a \quad a \cdot b = b \cdot a$
3. $a \cdot (b + c) = a \cdot b + a \cdot c$
4. There are $0, 1$ such that $a + 0 = a \cdot 1 = a$
5. Given $a \in R$, there is $b \in R$, such that $a + b = 0$

Example: Integers set $\mathbb{Z}$, Polynomials $k[x_1, \cdots, x_n]$

Field: Commutative Ring and also satisfies the following one more condition:consist of a set R and two binary operations "$\cdot$" and "+" defined on R for which the following conditions are satisfied, given$a, b, c \in R$:

1. $(a + b) + c = a + (b + c) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $a + b = b + a \quad a \cdot b = b \cdot a$
3. $a \cdot (b + c) = a \cdot b + a \cdot c$
4. There are $0, 1$ such that $a + 0 = a \cdot 1 = a$
5. Given $a \in R$, there is $b \in R$, such that $a + b = 0$
6. Given $a \in R$ and $a \neq 0$, there is $c \in R$, such that $a \cdot c = 1$

Example: Real number set $\mathbb{R}$, Complex number set $\mathbb{C}$

Ideal: A subset $I \subset k[x_1, \cdots, x_n]$ is an ideal if it satisfies:

1. $0 \in I$
2. if $f, g \in I$, then $f + g \in I$
3. if $f \in I$, and $h \in k[x_1, \cdots, x_n]$, then $hf \in I$

Ideal: $f_1, \cdots f_s \in k[x_1, \cdots, x_n]$, $< f_1, \cdots f_s >= \{\sum h_i f_i : h_1, \cdots h_s \in k[x_1, \cdots, x_n]\}$is an ideal (Prove that), $f_1, \cdots f_s$ are finite generating set called basis.

Observation 1: Every idea can have multiple bases.

Observation 2: if $< f_1, \cdots f_s >=< g_1, \cdots g_t >$, then equations $f_1 = 0, \cdots, f_s = 0$ have the same solutions with equations $g_1 = 0, \cdots g_s = 0$. (Prove it)

2 Problems

1. Does every ideal I have a finite generating set?
2. Given $f_1, \cdots f_s \in k[x_1, \cdots, x_n]$ and $I =< f_1, \cdots f_s >$, decide if $f \in I$?
3. solve polynomial equations $f_1 = \cdots = f_s = 0$?

3 Solutions

3.1 $n = 1$ polynomials

3.1.1 For given polynomial $g \neq 0$, every polynomial f can be represented as $f = qg + r$, either $r = 0$or $deg(r) < deg(g)$, here q is a polynomial.

3.1.2 Every idea $I =< f >$, here f is nonzero polynomial of minimum degree in I.

3.1.3 $< f_1, f_2 >=< GCD(f_1, f_2) >$

3.1.4 $g \in I =< f > iff \;\; g = qf$

3.2 Multivariables and any degree polynomials

3.2.1 Does every ideal have a finite generator?

Monomial ideals: An ideal $I \subset k[x_1, \cdots, x_n]$ is a monomial ideal if there is a subset $A \subset \mathbb{Z}^n_{\geq 0}$, such that I consists of all polynomials which are finite sums of the form $\sum h_a x^a$ where $h_a \in k[x_1, \cdots, x_n], a \in A$, and we write $I =< x^a, a \in A >$

Examples: $I =< x^4y^2, x^3y^4, x^2y^5 >$ is a monomial ideal.

Theorem: $I =< x^a, a \in A >$ then a monomial $x^b \in I$ iff $x^b$is divisible by $x^a$for some $a \in A$.

Leading Term: $LT(I) = \{cx^a : there\ exist\ f \in I\ with\ LT(f) = cx^a\}$

Hilber Basis Theorem: Every ideal I has a finite generating set. $I =< g_1, \cdots g_s >$for some $g_1, \cdots g_s \in I$.

Proof: $< g_1, \cdots g_s >\subseteq I$ and $I \subseteq< g_1, \cdots g_s >$?

$\Rightarrow< g_1, \cdots g_s >\subseteq I$ **is true**

$\Leftarrow$

$f \in I = a_1 g_1 + \cdots + a_s g_s + r$ **then** $r = f - a_1 g_1 - \cdots - a_s g_s \in I$

if $r \neq 0$ **then** $LT(r) \in< LT(I) =< LT(g_1), \cdots LT(g_s) >$**then** $LT(r)$ **is divisible by some** $LT(g_i)$

then $r = 0$**,** $f \in< g_1, \cdots g_s >$ **Proved.**

3.2.2 Groebner Bases

$G = \{g_1, \cdots g_s\}$**of** I **is a Groebner basis if** $< LT(g_1), \cdots LT(g_s) >=< LT(I) >$

Every nonzero ideal has Groebner basis.

A set $\{g_1, \cdots g_s\}$ **is a Groebner basis of** I **iff the leading term of any element of** I **is divisible by one of** $LT(g_i)$

$G = \{g_1, \cdots g_s\}$**of** I **is a Groebner basis and** f **is a polynomial, then** $f \in I$ **iff the remainder on division of** f **by** G **is zero.**

3.2.2.1 How to compute Groebner Bases

1. S-polynomials: Given polynomials f, g**,** $a = multideg(f)$ $b = multideg(g)$ $c = (c_1, \cdots c_n)$**,** $c_i = max(a_i, b_i)$

$S(f, g) = \frac{x^c}{LT(f)} \cdot f - \frac{x^c}{LT(g)} \cdot g$

Examples: $f = x^3y^2 - x^2y^3 + x$**,** $g = 3x^4y + y^2$**,** $c = (4, 2)$**,** $S(f, g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g$

2. $G = \{g_1, \cdots g_s\}$**of** I **is a Groebner basis iff any pairs** $i \neq j$**,** $\overline{S(p, q)}^G$ **(the remainder on division of** $S(g_i, g_j)$ **by** G**) is zero.**

3. Compute Groebner Basis: try to extend the original generating set to a Groebner basis by adding more polynomials in I

Algorithm: *input* $F = (f_1, \cdots f_s)$ *output* $G = (g_1, \cdots g_t)$ $G = F$,
repeat
$G' = G$
$for\ each\ pair\ \{p, q\},\ p \neq q\ in\ G'\ do$
$S = \overline{S(p,q)}^G$
$if\ S \neq 0\ then\ G = G \cup \{S\}$
$until\ G = G'$

4. Let G **be a Groebner basis for polynomial ideal** I**,** $p \in G$ **such that** $LT(p) \in < LT(G - \{p\}) >$ **then** $G - \{p\}$ **is also a Groebner basis.**

3.2.2.2 Applications of Groebner Bases

1. ideal membership algorithm

Given $I =< f_1, \cdots f_s >$ **decide if** $f \in I$**?**
First find Grobner basis $G = \{g_1, \cdots g_s\}$**of** I **then** $f \in I$ **iff** $\overline{f}^G = 0$

2. Solving polynomial equations

$$\begin{pmatrix} x^2 + y^2 + z^2 = 1 \\ x^2 + z^2 = y \\ x = z \end{pmatrix} G = \{x - z, -y + 2z^2, z^4 + (1/2)z^2 - 1/4\} \Rightarrow \text{solutions}$$