Algebraic Statistics

P1: Intro to Algebraic Geometry

Longphi Nguyen   Laila Rizvi   Ying Shi

University of California,Davis

December 7, 2012

Goal: Given $I = < g_1, ..., g_s >$ and $f \in \mathbb{K}[\vec{x}]$, is $f \overset{?}{\in} I$?

Goal: Given $I = < g_1, ..., g_s >$ and $f \in \mathbb{K}[\vec{x}]$, is $f \overset{?}{\in} I$?

How to solve? Extend GCD to multivariate polynomials.

Goal: Given $I =< g_1, ..., g_s >$ and $f \in \mathbb{K}[\vec{x}]$, is $f \overset{?}{\in} I$?

How to solve? Extend GCD to multivariate polynomials.
$f = a_1 g_1 + a_2 g_2 + ... + a_n g_n + r$, where $a_i, r \in \mathbb{K}[\vec{x}]$, $i = 1, 2, ..., n$

Goal: Given $I = < g_1, ..., g_s >$ and $f \in \mathbb{K}[\vec{x}]$, is $f \overset{?}{\in} I$?

How to solve? Extend GCD to multivariate polynomials.
$f = a_1 g_1 + a_2 g_2 + ... + a_n g_n + r$, where $a_i, r \in \mathbb{K}[\vec{x}]$, $i = 1, 2, ..., n$

Solution: $f \in I \iff r = 0$ for some monomial ordering.

Example

$f = xy^2 - x$, $g_1 = xy + 1$, $g_2 = y^2 - 1$.

Example

$f = xy^2 - x$, $g_1 = xy + 1$, $g_2 = y^2 - 1$.

1) Ordering $x \underset{lex}{>} y$: $f = yg_1 + 0g_2 + (-x - y)$

2) Ordering $y \underset{lex}{>} x$: $f = 0g_1 + xg_2 + 0$

Example

$f = xy^2 - x$, $g_1 = xy + 1$, $g_2 = y^2 - 1$.

1) Ordering $x \underset{lex}{>} y$: $f = yg_1 + 0g_2 + (-x - y)$

2) Ordering $y \underset{lex}{>} x$: $f = 0g_1 + xg_2 + 0$

Problem #1: How to find "good" g_i's. Generators are not unique. e.g. $< x + y, x - y > = < x, y >$

Problem #2: r is not unique.

Example

$f = xy^2 - x$, $g_1 = xy + 1$, $g_2 = y^2 - 1$.

1) Ordering $x \underset{lex}{>} y$: $f = yg_1 + 0g_2 + (-x - y)$

2) Ordering $y \underset{lex}{>} x$: $f = 0g_1 + xg_2 + 0$

Problem #1: How to find "good" g_i's. Generators are not unique. e.g. $< x + y, x - y > = < x, y >$

Problem #2: r is not unique.

Look at: Groebner basis

Definition: Fix a monomial order. Suppose I is an ideal such that $< LT(I) > = < LT(g_1), LT(g_2), \ldots, LT(g_t) >$. Then, $G = \{g_1, g_2, ..., g_t\}$ is a Groebner basis of I.

Definition: Fix a monomial order. Suppose I is an ideal such that $< LT(I) >=< LT(g_1), LT(g_2), \ldots, LT(g_t) >$. Then, $G = \{g_1, g_2, ..., g_t\}$ is a Groebner basis of I.

Hilbert Basis Theorem: Every ideal $I \subset \mathbb{K}[\vec{x}]$ is finitely generated.

Corollary: Every nonzero ideal has a Groebner basis.

Definition: Fix a monomial order. Suppose I is an ideal such that $< LT(I) >=< LT(g_1), LT(g_2), \ldots, LT(g_t) >$. Then, $G = \{g_1, g_2, ..., g_t\}$ is a Groebner basis of I.

Hilbert Basis Theorem: Every ideal $I \subset \mathbb{K}[\vec{x}]$ is finitely generated.

Corollary: Every nonzero ideal has a Groebner basis.

Then, every nonzero ideal $I \subset \mathbb{K}[\vec{x}]$ has a finite Groebner basis.

Importance: Given a Groebner basis G of ideal I and ordering:

1. The division algorithm gives a unique remainder r.
2. $r = Rem(f, G) = 0 \iff f \in I$.

Importance: Given a Groebner basis G of ideal I and ordering:

1. The division algorithm gives a unique remainder r.

2. $r = Rem(f, G) = 0 \iff f \in I$.

How to find a Groebner basis? Can use Buchberger's algorithm. First, need to introduce S-polynomials.

S-polynomials:

$S(f_1, f_2) = x^\gamma[\frac{f_1}{LT(f_1)} - \frac{f_2}{LT(f_2)}]$, where $x^\gamma = LCM(LM(f_1), LM(f_2))$

S-polynomials:

$S(f_1, f_2) = x^{\gamma}[\frac{f_1}{LT(f_1)} - \frac{f_2}{LT(f_2)}]$, where $x^{\gamma} = LCM(LM(f_1), LM(f_2))$

Example: $f_1 = y - x^2, \qquad f_2 = z - x^3, \qquad y \underset{lex}{>} z \underset{lex}{>} x$

$$\begin{aligned} S(f_1, f_2) &= yz[\frac{y - x^2}{y} - \frac{z - x^3}{z}] \\ &= -zx^2 + yx^3 \end{aligned}$$

Buchberger's Criterion:

$G = \{g_1, g_2, ..., g_t\}$ is a Groebner basis for I
$\iff$ $Rem(S(g_i, g_j), G) = 0$, for all $i \neq j$.

Buchberger's Criterion:

$G = \{g_1, g_2, ..., g_t\}$ is a Groebner basis for I
$\iff$ $Rem(S(g_i, g_j), G) = 0$, for all $i \neq j$.

Example (continued):

$f_1 = y - x^2, \qquad f_2 = z - x^3, \qquad S(f_1, f_2) = -zx^2 + yx^3 = S$

Buchberger's Criterion:

$G = \{g_1, g_2, ..., g_t\}$ is a Groebner basis for I
$\iff$ $Rem(S(g_i, g_j), G) = 0$, for all $i \neq j$.

Example (continued):

$$f_1 = y - x^2, \qquad f_2 = z - x^3, \qquad S(f_1, f_2) = -zx^2 + yx^3 = S$$

By division algorithm under $y \underset{lex}{>} z \underset{lex}{>} x$,

Buchberger's Criterion:

$G = \{g_1, g_2, ..., g_t\}$ is a Groebner basis for I
$\iff$ $Rem(S(g_i, g_j), G) = 0$, for all $i \neq j$.

Example (continued):

$$f_1 = y - x^2, \qquad f_2 = z - x^3, \qquad S(f_1, f_2) = -zx^2 + yx^3 = S$$

By division algorithm under $y \underset{lex}{>} z \underset{lex}{>} x$,

$$S = x^3(y - x^2) - x^2(z - x^3) + 0$$

Buchberger's Criterion:

$G = \{g_1, g_2, ..., g_t\}$ is a Groebner basis for I
$\iff$ $Rem(S(g_i, g_j), G) = 0$, for all $i \neq j$.

Example (continued):

$$f_1 = y - x^2, \qquad f_2 = z - x^3, \qquad S(f_1, f_2) = -zx^2 + yx^3 = S$$

By division algorithm under $y \underset{lex}{>} z \underset{lex}{>} x$,

$$S = x^3(y - x^2) - x^2(z - x^3) + 0 \Longrightarrow \text{ Groebner basis}$$

Buchberger's Criterion:

$G = \{g_1, g_2, ..., g_t\}$ is a Groebner basis for I
$\iff$ $Rem(S(g_i, g_j), G) = 0$, for all $i \neq j$.

Example (continued):

$f_1 = y - x^2, \qquad f_2 = z - x^3, \qquad S(f_1, f_2) = -zx^2 + yx^3 = S$

By division algorithm under $y \underset{lex}{>} z \underset{lex}{>} x$,

$S = x^3(y - x^2) - x^2(z - x^3) + 0 \Longrightarrow$ Groebner basis

Note: $Rem(S', G) \neq 0$ under $x \underset{lex}{>} y \underset{lex}{>} z$.

Thus, we have a way to determine if $\{g_1, ..., g_t\}$ is a Groebner basis.

But **how do we find a Groebner basis**?

Buchberger's Algorithm

```
Input: F=(f_1, f_2, ..., f_s)
Output: G=(g_1, g_2, ..., g_t)

G=F
Repeat
    G'=G
    For each pair {i, j}, i ≠ j in G', do
        g=Rem(S(i, j), G))
        If S ≠ 0
            then G=G ∪ {g}
Until G=G'
```

Sample steps:

G	**Rem(S(.,.), G))**
$\{g_1, g_2\}$	g_3
$\{g_1, g_2, g_3\}$	g_4
$\{g_1, g_2, g_3, g_4\}$	0

Problem: Groebner basis is not unique and contains redundancies.
e.g. $\{y - x^2, z - x^3\}$ for $< y - x^2, z - x^3 >$ w.r.t. $y \underset{lex}{>} z \underset{lex}{>} x$

Goal: Remove redundancies in Groebner basis.

Goal: Remove redundancies in Groebner basis.

Definition: Given a Groebner basis G, a reduced Groebner basis is such that:

1) $LC(g_i) = 1$, for all $g_i \in G$

2) No term of g_i is divisible by $LM(G \backslash \{g_i\})$

Goal: Remove redundancies in Groebner basis.

Definition: Given a Groebner basis G, a reduced Groebner basis is such that:

1) $LC(g_i) = 1$, for all $g_i \in G$

2) No term of g_i is divisible by $LM(G \setminus \{g_i\})$

Importance: Reduced Groebner basis is unique!

Thank you! :) :)