Gröbner Basis and the Ideal Membership Problem

AliAnn Xu

University of Georgia

December 3, 2018

Overview

1. Univariate vs. multivariate polynomial long division
2. Ideal Membership Problem
3. What is a Gröbner Basis?
4. How Gröbner Basis helps us solve the ideal membership problem?
5. Summary

Ideal

Definition

A subset $I \subseteq \mathbb{C}[x_1, ..., x_n]$ is an ideal if it satisfies:
(i) $0 \in I$.
(ii) If $f, g \in I$, then $f + g \in I$.
(iii) If $f \in I$ and $h \in \mathbb{C}[x_1, ..., x_n]$, then $fh \in I$.

If $f_1, ..., f_s \in I$ then the ideal they generate is
$\langle f_1, .., f_s \rangle = \{p_1 f_1 + ... + p_r f_r : p_1, ..., p_r\} \subset \mathbb{C}[x]$

Given $f_1, ..., f_s \in \mathbb{C}[x]$, is there an algorithm for deciding whether a given polynomial $f \in \mathbb{C}[x]$ lies in the ideal $\langle f_1 ..., f_s \rangle$? This is known as the Ideal Membership Problem.

Single Variable Polynomial Long Division

How to determine if given polynomial $f \in \mathbb{C}[x]$ lies in the ideal $< f_1, ..., f_s >$?

1. Find the greatest common divisor (GCD) to find a generator h of $\langle f_1, ..., f_s \rangle$.
   Note that $f \in < f_1, ..., f_s >$ is equivalent to $f \in < h >$.
2. Use the division algorithm to write f = qh + r, where $deg(r) < deg(h)$ to determine the remainder.
3. $f \in I \iff r = 0$

Single Variable Polynomial Long Division

Determine whether the given polynomial f(x) is in the given ideal $I \subseteq \mathbb{C}[x]$.

Example 1

Let $f(x) = x^5 - 4x + 1$ and $I =< x^3 - x^2 + x >=< h >$. Divide

$x^5 - 4x + 1$ by $x^3 - x^2 + x$ gives remainder of $(-x^2 - 4x + 1)$:
$x^5 - 4x + 1 = (x^3 - x^2 + x)(x^2 + x) + (-x^2 - 4x + 1)$

Since $r \neq 0$, $f \notin I$.

Example 2

Let $f(x) = x^2 - 3x + 2$ and $I =< x - 2 >=< h >$. Divide

$x^2 - 3x + 2$ by $x - 2$ gives remainder of 0:
$x^2 - 3x + 2 = (x - 2)(x - 1)$

Since $r = 0$, $f \in I$.

Monomial Ordering

How do we perform the division algorithm with multivariate polynomials? Which term of $f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4 \in \mathbb{C}[x,y,z]$ is the biggest?

In order to perform the division algorithm, we need to find a way to order monomials in our polynomials.

Examples of monomial orderings:

1. Lexicographic Order

Example

$f(x,y,z) = -3x^5yz^4 + 2x^2y^8 - xy^4 + xyz^3$

2. Graded Lex Order
3. Graded Reverse Lex Order

Multivariate Polynomial Long Division

How to determine if given polynomial $f \in \mathbb{C}[x]$ lies in the ideal $< f_1, ..., f_s >$?

- For multivariate polynomial long division, we will still use the procedure as for division of the one variable by comparing the leading terms at each step.

Multivariate Polynomial Long Division

Example

Let us divide $f = x^2y + xy^2 + y$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$.
Use lex order with $x > y$.
Answer: $x^2y + xy + y = (x + y)[xy - 1] + (1)[y^2 - 1] + (x + y + 1)$

Multivariate Polynomial Long Division

Determine whether the given polynomial f(x) is in the given ideal $I \subseteq \mathbb{C}[x]$.

Let $f_1 = xy + 1$, $f_2 = y^2 - 1 \in \mathbb{C}[x, y]$ and $f = xy^2 - x$ with lex order.

Example 1

If we divide $f = xy^2x$ by $F = (f_1, f_2)$, we get
$xy^2x = y * (xy + 1) + 0 * (y^2 - 1) + (-x - y)$.

We do not know if $f \in < f_1, f_2 >$ since it has nonzero remainder

Example 2

Now, let us divide $f = xy^2x$ by $F = (f_2, f_1)$, we have
$xy^2x = x * (y^2 - 1) + 0 * (xy + 1) + 0$.

$f \in < f_1, f_2 >$ because the remainder is 0.

Gröbner Basis

- Gröbner basis is a generating set of the ideal where remainder is uniquely determined.
- The Buchberger's Algorithm is an algorithm to construct a Gröbner basis.

Gröbner basis helps us easily solve the Ideal Membership Problem: given an ideal $I =< f_1, ..., f_s >$, we can decide whether a given polynomial f lies in I as follows?

1. Find a Gröbner basis $G = g_1, ..., g_t$ for the ideal $I =< F >$
2. Divide f by G to get a unique remainder so $f = q_1 f_1 + ... + q_n f_n + r$
3. $f \in I$ if and only if f/G has remainder 0.

Example 1

Let $I =< f_1, f_2 >=< xz - y^2, x^3 - z^2 >\subset \mathbb{C}[x, y, z]$ and $f = -4x^2y^2z^2 + y^6 + 3z^5$. Is $f \in I$?

1. $G = (xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5)$
2. Divide f by G
   $f = (-4xy^2z - 4y^4)f_1 + 0(f_2) + 0(f_3) + 0(f_4) + (-3)(f_5)$

   Since the remainder is 0, $f \in I$.

Example 2

Consider $f = xy - 5z^2 + x$ instead.

Since the remainder is not zero, $f \notin I$.

Summary

- How to solve the ideal membership problem?
- With single variables, divide f by I to get a unique remainder. If the remainder is zero, f is in I. If the remainder is not zero, then $f \notin I$.
- Gröbner basis allows us to easily decide membership for multivariate polynomials. Divide f by G to get a unique remainder. If the remainder is zero, f is in I. If the remainder is not zero, then $f \notin I$.

Bibliography

Springer Cox, David, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer: New York, 1997.