Computer Algebra for Computer Engineers

Gröbner Bases: Definitions + Results

Priyank Kalla

Department of Electrical and Computer Engineering

University of Utah, Salt Lake City
So Far, We’ve seen....

- Ideals, Generators, Division & GCD in \( k[x] \)
- Multi-variate Division in \( k[x_1, \ldots, x_n] \)
- Given: \( f, F = \{f_1, f_2, \ldots, f_s\} \)
- \( f \xrightarrow{F} r \)
- \( f = u_1f_1 + u_2f_2 + \cdots + u_sf_s + r \), where either \( r = 0 \) or \( r \) is reduced (no term in \( r \) is divisible by \( \text{lp}(f_i) \)).
- \( \text{lp}(f) = \text{MAX}(\text{lp}(u_1) \cdot \text{lp}(f_1), \ldots, \text{lp}(u_s) \cdot \text{lp}(f_s), \text{lp}(r)) \)
- If \( r = 0 \) then \( f \in I = \langle f_1, \ldots, f_s \rangle \)
- But what if \( r \neq 0? \)
Solution: Gröbner Bases

A set of non-zero polynomials $G = \{g_1, \ldots, g_t\}$ contained in an ideal $I$, is called a Gröbner basis for $I$ if and only if for all $f \in I$ such that $f \neq 0$, there exists $i \in \{1, \ldots, t\}$ such that $\text{lp}(g_i)$ divides $\text{lp}(f)$.

\[ G = \text{GröbnerBasis}(I) \quad \iff \quad \forall f \in I : f \neq 0, \ \exists g_i \in G : \text{lp}(g_i) \mid \text{lp}(f) \]

- $f \in I \iff f \xrightarrow{G} 0$
- $f \in I \iff f = \sum_{i=1}^{t} h_i g_i$, with $\text{lp}(f) = \max (\text{lp}(h_i) \text{lp}(f_i))$
- If $G = \{g_1, \ldots, g_t\} \subseteq I$ is a Gröbner Basis for $I$, then $I = \langle g_1, \ldots, g_t \rangle$
Questions on the Existance of G.B.

- Does a G.B. always exist for any $I \subset k[x_1, \ldots, x_n]$?
- Can it always be computed? Uniquely (up to ordering)?
- What about minimality of the G.B.?
- Study properties of a G.B., and derive algorithms to compute it.
Monomial Ideals

- Ideal $I \subset k[x_1, \ldots, x_n]$ 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
  \[
  \sum_{\alpha \in A} h_\alpha x^\alpha, \quad h_\alpha \in k[x_1, \ldots, x_n].
  \]
  Then, $I = \langle x^\alpha : \alpha \in A \rangle$.

- If $I$ is a monomial ideal, then $x^\beta \in I \iff$ some $x^\alpha | x^\beta$.

- If $f \in I$, then every term of $f$ is in $I$. Therefore, $f$ is a $k$-linear combination of monomials in $I$.

- Two monomial ideals are the same iff they contain the same monomials.

- All monomial ideals have a finite basis.
Ideals of Leading Terms

Let $I \subset k[x_1, \ldots x_n]$ be a non-zero ideal.

- Denote by $\text{LT}(I)$ the set of leading terms of elements of $I$.
- $\text{LT}(I) = \{cx^\alpha : \exists f \in I \text{ with } \text{LT}(f) = cx^\alpha\}$
- \langle \text{LT}(I) \rangle$ denotes the ideal generated by elements of $\text{LT}(I)$.
- \langle \text{LT}(I) \rangle$ is a monomial ideal.
- Let $I = \langle f_1, \ldots, f_s \rangle$, then $\langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$ and $\langle \text{LT}(I) \rangle$ are (can be) different ideals.
- There are $g_1, \ldots g_t \in I$ such that $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$.
- Now prove Hilbert Basis Theorem. Every ideal $I \subset k[x_1, \ldots, x_n]$ has a finite generating set. $I = \langle g_1, \ldots, g_t \rangle$ for some $g_1, \ldots, g_t \in I$. 
G.B. as a leading term Ideal

Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I$ is a Gröbner basis if $\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle$. Equivalently, $G$ is a G.B. of $I$ if and only if the leading term of any element of $I$ is divisible by one of the $LT(g_i)$. 
Division by G.B.

Let $G = \{g_1, \ldots, g_t\}$ be a G.B. for $I$, and let $f \in k[x_1, \ldots, x_n]$. Then there is a unique $r \in k[x_1, \ldots, x_n]$, with following two properties:

- No term of $r$ is divisible by any $\text{LT}(g_i)$.
- There is a $g \in I$ such that $f = g + r$.

In other words: If $G = \{g_1, \ldots, g_t\}$ be a G.B. for $I \in k[x_1, \ldots, x_n]$, and let $f \in k[x_1, \ldots, x_n]$.

- $f \in I \iff f \xrightarrow{G} 0$
- If $f \notin I$, then $f \xrightarrow{G} r$, then $r$ is unique as in the above definition, irrespective of $g_1, \ldots, g_t$ ordering (though the quotients can be different).
S-Polynomials: Motivation

\[ I = \langle f_1, f_2 \rangle, \quad f = h_1 f_1 + h_2 f_2. \]

- If \( LT(f) \in \langle LT(f_1), LT(f_2) \rangle \), then some \( LP(f_i) | LP(f) \)

- But what if \( LT(f) \notin \langle LT(f_1), LT(f_2) \rangle \)?

Let's study some examples.....

When \( f = \) polynomial combination of (say) \( h_i f_i + h_j f_j \), such that the leading term of \( h_i f_i \) and \( h_j f_j \) cancel, then \( LT(f) \notin \langle LT(f_i), LT(f_j) \rangle \). When does this happen?

Consider \( f_i, f_j \) when the leading term of \( ax^\alpha f_i - bx^\beta f_j \) cancel!
$S(f, g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g$

$L = \text{LCM}(lp(f), lp(g))$

How to compute LCM of leading powers?

Let $\text{multideg}(f) = x^\alpha$, $\text{multideg}(g) = x^\beta$, and let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$. Then the $x^\gamma = \text{LCM}(\text{LP}(f), \text{LP}(g))$. 
(Thm 1.7.4 in the textbook) Let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomials in $k[x_1, \ldots, x_n]$. Then $G$ is a Grobner basis for the ideal $I = \langle g_1, \ldots, g_t \rangle$ if and only if for all $i \neq j$

$$S(g_i, g_j) \xrightarrow{G} + 0$$

The $S$-polynomials account for all missing $\text{LT}(g_i)$'s for the Grobner basis computation.