Computer Algebra for Computer Engineers

Gröbner Bases: Buchberger’s Results

Priyank Kalla

Department of Electrical and Computer Engineering
University of Utah, Salt Lake City
Gröbner Bases: First Definition

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 $lp(g_i)$ divides $lp(f)$.

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

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

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

- Denote by $LT(I)$ the set of leading terms of elements of $I$.

$$LT(I) = \{cx^\alpha : \exists f \in I \text{ with } LT(f) = cx^\alpha\}$$

- $\langle LT(I) \rangle$ denotes the ideal generated by elements of $LT(I)$.

- $\langle LT(I) \rangle$ is a monomial ideal.

- Let $I = \langle f_1, \ldots, f_s \rangle$, then $\langle LT(f_1), \ldots, LT(f_s) \rangle$ and $\langle LT(I) \rangle$ are (can be) different ideals.

- There are $g_1, \ldots, g_t \in I$ such that $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.

- 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 $g_1, \ldots, g_t \in I$. 
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 $LT(g_i)$.

Corollary: Fix a monomial order. Then every (non-zero) ideal $I \in k[x_1, \ldots, x_n]$ has a Gröbner basis. Conversely, every G.B. is a basis for $I$. 
Properties: Division by G. B.

Let \( G = \{g_1, \ldots, g_t\} \) be a G.B. for \( I \in k[x_1, \ldots, x_n] \), and let \( f \in k[x_1, \ldots, x_n] \). 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 \( f \not\in I \), 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

$I = \langle f_1, f_2 \rangle$, $f = h_1 f_1 + h_2 f_2$.

- 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 $f = \text{polynomial combination of (say)} h_i f_i + h_j f_j$, 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-Polynomial

\[ S(f, g) = \frac{L}{\text{lt}(f)} \cdot f - \frac{L}{\text{lt}(g)} \cdot g \]

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

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 \( x^\gamma = \text{LCM}(LP(f), LP(g)) \).
Buchberger’s Theorem

(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.

This gives us an algorithm to compute G.B. Given \( F = \{f_1, \ldots, f_s\} \), repeatedly compute \( S(f_i, f_j) \xrightarrow{F} r \); if \( r \neq 0 \), \( F = F \cup r \), until no new non-zero \( r \) is created.
Lemma 1.7.5: Let \( f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \) be such that \( \text{lp}(f_i) = X \neq 0 \) for all \( i = 1, \ldots, s \). Let \( f = \sum_{i=1}^{s} c_i f_i \), where \( c_i \in k \) are coefficients. If \( \text{lp}(f) < X \), then \( f \) is a linear combination of \( S(f_i, f_j), 1 \leq i, < j \leq s \), with coefficients in \( k \).

Another result that we will use: If \( G = \{g_1, \ldots, g_t\} \subseteq I \) is a Grobner basis, then:

\[
f \in I \iff f = \sum_{i=1}^{t} h_i g_i, \text{ with } \text{lp}(f) = \max \left( \text{lp}(h_i) \text{lp}(g_i) \right)
\]

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

A Gröbner basis $G = \{g_1, \ldots, g_t\}$ is minimal if for all $i$, $\text{lc}(g_i) = 1$, and for all $i \neq j$, $\text{lp}(g_i)$ does not divide $\text{lp}(g_j)$.

- Obtain a minimal GB: Test if $\text{lp}(g_i)$ divides $\text{lp}(g_j)$, remove $g_j$. Then normalize the LC: Divide each $g_i$ by $\text{LC}(g_i)$.

- Unfortunately, minimality is not unique.

- Minimal GBs have same number of terms.

- Minimal GBs have same leading terms.
A reduced G.B. for a polynomial ideal $I$ is a G.B. $G$ such that:

- $\text{LC}(p) = 1$, $\forall p \in G$
- $\forall p \in G$, no monomial of $p$ lies in $\langle \text{LT}(G - \{p\}) \rangle$.

In other words, no non-zero term in $g_i$, is divisible by any $\text{lp}(g_j)$, for $i \neq j$.

Reduced, minimal G.B. is unique!
Reduced G.B. Algorithm

- Compute a G.B. Make it minimal: remove \( g_i \) if \( lp(g_j) \) divides \( lp(g_i) \). Make all LC = 1.

- Reduce it: \( G = \{g_1, \ldots, g_t\} \) is minimal G.B. Get \( H = \{h_1, \ldots, h_t\} \):
  - \( g_1 \xrightarrow{H_1} h_1 \), where \( h_1 \) is reduced w.r.t. \( H_1 = \{g_2, \ldots, g_t\} \)
  - \( g_2 \xrightarrow{H_2} h_2 \), where \( h_2 \) is reduced w.r.t. \( H_2 = \{h_1, g_3, \ldots, g_t\} \)
  - \( g_3 \xrightarrow{H_3} h_3 \), where \( h_3 \) is reduced w.r.t. \( H_3 = \{h_1, h_2, g_4, \ldots, g_t\} \)
  - \( g_t \xrightarrow{H_t} h_t \), where \( h_t \) is reduced w.r.t. \( H_t = \{h_1, h_2, h_3, \ldots, h_{t-1}\} \)

- Then \( H = \{h_1, \ldots, h_t\} \) is a unique, minimal, reduced GB.
When in doubt, remember G.B. as follows:

Given: \( I = \langle f_1, \ldots, f_s \rangle \), compute \( G = \{ g_1, \ldots, g_t \} \) such that
\[
I = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle
\]
where
\[
\forall f \in I, \ \text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle
\]
and
\[
\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle.
\]

Cancellation of leading terms: There’s got to be \( S \)-polynomials.

For decision problems w.r.t. ideals, think: Is minimality or uniqueness important? If so, compute reduced, minimal G.B.

G.B. as a “canonical” representation of an ideal.

Monomial orderings are important, a G.B. w/ lex order may not be a G.B. w/ deglex or degrevlex order, and conversely.
References


