1 Background

A sufficient and necessary criterion for Buchberger’s chain condition

J. Perry
Department of Mathematics, University of Southern Mississippi, Hattiesburg, MS 39406, USA

Problem

Find a sufficient and necessary criterion on the leading terms of polynomials $f_1, f_2, \ldots, f_n$ that detects a chain condition in Gröbner basis computation.

1 Background

$\prec$: admissible term ordering

$\text{lt}(f), k_0(f)$: leading term, coefficient of $f$ with respect to $\prec$

1.1 $S$-Polynomials

The $S$-polynomial of $f_1, f_2 \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ with respect to $\prec$

$S(f_1, f_2) = a_{12} f_1 - a_{21} f_2$

where $a_{12} = \text{lc}(f_1) \text{lc}(k_0(f_1), k_0(f_2)) / \text{lc}(f_2)$

(Leading terms of $a_{12} f_1$ and $a_{21} f_2$ cancel)

1.2 $S$-Polynomial Representations [2, 3, 1]

An $S$-polynomial representation [modulo $F = (f_1, f_2, \ldots, f_n)$] wrt $\prec$

$S(f_1, f_2) = \text{lt}(f_1) + \text{lt}(f_2) + \ldots + b_{i} f_i$

where $b_i \neq 0$ implies $\text{lt}(b_i) \text{lt}(f_i) \prec \text{lt}(f_1), \text{lt}(f_2)$ (Similar to $t$-representations in [1].)

Typically omit “modulo $F$”

Theorem (A) iff (B)

(A) $F = (f_1, f_2, \ldots, f_n)$ is a Gröbner basis

(B) $S(f_1, f_2)$ has a representation for all $i : 1 \leq i < j \leq m$.

1.3 Buchberger’s Criteria

Given terms $t_1, t_2, t_m$

- $BC1(t_1, t_m) : t_1, t_m$ relatively prime (the first criterion)

- $BC2(t_1, t_2, \ldots, t_m) : t_i$ divides $\text{lcm}(t_1, t_m)$ (the second criterion)

Theorem. Let $F = (f_1, f_2, \ldots, f_n)$. Then (A) and (B) where

(A) $\text{lt}(f_1)$ and $h(f_1)$ satisfy Buchberger’s first criterion, then $S(f_1, f_2)$ has a representation,

(B) $\text{lt}(f_1)$, $h(f_1)$, and $h(f_n)$ satisfy Buchberger’s second criterion (for some $1 \leq k \leq m$), then (B)/(5b/5a/2) where

- (B1) $S(f_1, h(f_n))$ and $S(f_1, f_n)$ have representations;

- (B2) $S(f_1, f_n)$ has a representation.

2 Results

2.1 Chain Condition

For terms $t_1, t_2, \ldots, t_m$ and polynomials $F = (f_1, f_2, \ldots, f_n)$

$\text{Chain Condition}(t_1, t_2, \ldots, t_m) :$

$S(f_1, f_2)$ has representation

$S(f_2, f_3)$ has representation

$\ldots$

$S(f_{m-1}, f_m)$ has representation.

If

Then $S(f_{m-1}, f_m)$ has representation.

2.2 Facts [2, 3, 5]

$BC1(t_1, t_2) \text{ or } BC2(t_1, t_1, t_2)$

for all $k : 1 \neq k, m$

but

$BC1(t_1, t_2) \text{ or } BC2(t_1, t_2, t_3)$

for all $1 \leq k, m$

What $C$ such that

$C(t_1, t_2, \ldots, t_k) \Leftrightarrow \text{Chain Condition}(t_1, t_2, \ldots, t_k)$

2.3 Results [6]

Fewer leading terms examined than polynomials? BC necessary.

Theorem 1. If $M < m$, then (A) iff (B) where

- (A) $\text{Chain Condition}(t_1, t_2, \ldots, t_m, t_{m+1})$;

- (B) $BC1(t_1, t_2)$ or $BC2(t_1, t_2, t_3)$ for all $1 \leq k \leq M$.

All leading terms examined? Generalization of BC exists!

Definition. The Extended First Criterion is $\{ \text{EC}_\text{div} \text{ and } \text{EC}_\text{var}\}$ where

$\text{EC}_\text{div}$ gcd$(t_1, t_m)$ divides $t_1$ for all $k = 2, 3, \ldots, m - 1$

$\text{EC}_\text{var}$ for all $t_k$

$\text{deg}(\text{gcd}(t_k, t_{m-1})) = 0$, or

$\text{deg}(t_k) = \text{deg}(t_{m-1}) \leq \cdots \leq \text{deg}(t_i)$, or

$\text{deg}(t_k) \geq \text{deg}(t_{m-1}) \geq \cdots \geq \text{deg}(t_i)$.

$\text{EC}(t_1, t_2, \ldots, t_m) : (\text{EC}_\text{div}(t_1, t_2, \ldots, t_m) \text{ and } \text{EC}_\text{var}(t_1, t_2, \ldots, t_m))$.

Theorem 2. If $M < m$, then (A) iff (B) where

- (A) $\text{Chain Condition}(t_1, t_2, \ldots, t_m, t_{m+1})$;

- (B) $\text{EC}(t_1, t_2, \ldots, t_m)$ or $BC2(t_1, t_2, t_3)$ for all $1 \leq k \leq m$.

3 Analysis

Not only must $\text{gcd}(t_1, t_m)$ divide all the intermediate terms (EC_div), but the degrees of common variables must follow a monotonous sequence (EC_var). Not too restrictive for $m = 3$ or $m = 4$, but the Extended First Criterion becomes less useful as $m$ increases.

4 Illustration, Examples

Let $t_1 = x^2, t_m = y^2z^2$.

Locations for terms in BC2 chains

Locations for terms in EC chains

Suppose $F = (f_1, f_2, f_3)$ where

- $\text{lt}(f_1) = x^2z$,

- $\text{lt}(f_2) = x^2z^2$, and

- $\text{lt}(f_3) = y^2z^3$.

- $S(f_1, f_2)$ and $S(f_2, f_3)$ have representations.

Easy to verify that leading terms satisfy Extended First Criterion, though they do not satisfy Buchberger’s Criterion.

- By Theorem 2, $S(f_1, f_3)$ has a representation.

- By Theorem 1, it might not if $F = (f_1, f_2, f_3, f_4)$.

(Did not check all leading terms $\Rightarrow$ Can only rely on BC2! Countercases easy?)

Cute Corollary. If $F = (f_1, f_2, \ldots, f_m)$ and for all $k = 1, 2, \ldots, m$ we have $\text{lt}(f_k) = u_k$, where

$\text{gcd}(u_1, u_2) = 1$ for all $i \neq j$, then we can decide whether $F$ is a Gröbner basis by checking only $m - 1$ pairs.

References


