A sufficient and necessary criterion for Buchberger's chain condition

J. Perry
Department of Mathematics, University of Southern Mississippi, Hattiesburg, MS 39406, USA
john.perry@usm.edu

Problem

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

1 Background

$\prec$: admissible term ordering
$\mathrm{lt}(f), \mathrm{lc}(f)$: leading term, coefficient of f with respect to $\prec$

1.1 S-Polynomials

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

$$S(f_1, f_2) = \sigma_{1,2} f_1 - \sigma_{2,1} f_2$$

where

$$\sigma_{i,j} = \mathrm{lc}(f_j) \frac{\mathrm{lcm}(\mathrm{lt}(f_i), lt f_j)}{\mathrm{lt}(f_i)}.$$

(Leading terms of $\sigma_{1,2} f_1$ and $\sigma_{2,1} f_2$ cancel!)

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

An **S-polynomial representation** [modulo $F = (f_1, f_2, \dots, f_m)$] wrt $\prec$:

$$S(f_1, f_2) = h_1 f_1 + h_2 f_2 + \cdots + h_m f_m$$

where $h_k \neq 0$ implies $\mathrm{lt}(h_k)\,\mathrm{lt}(f_k) \prec \mathrm{lcm}(\mathrm{lt}(f_1), \mathrm{lt}(f_2))$. (Similar to *t-representations* in [1]. Typically omit "modulo F".)

Theorem. *(A) iff (B) where*

(A) $F = (f_1, f_2, \dots, f_m)$ is a Gröbner basis

(B) $S(f_i, f_j)$ has a representation for all $i, j : 1 \le i < j \le m$.

1.3 Buchberger's Criteria

Given terms t_1, t_k, t_m

- **BC1**$(t_1, t_m) := t_1, t_m$ relatively prime?
  (the first criterion)
- **BC2**$(t_1, t_k, t_m) := t_k$ divides $\mathrm{lcm}(t_1, t_m)$?
  (the second criterion)

Theorem. *Let $F = (f_1, f_2, \dots, f_m)$. Then (A) and (B) where*

(A) If $\mathrm{lt}(f_1)$ and $\mathrm{lt}(f_m)$ satisfy Buchberger's first criterion, then $S(f_1, f_m)$ has a representation.

(B) If $\mathrm{lt}(f_1), \mathrm{lt}(f_k)$, and $\mathrm{lt}(f_m)$ satisfy Buchberger's second criterion (for some $1 \le k \le m$), then (B1)⇒(B2) where

(B1) $S(f_1, f_k)$ and $S(f_k, f_m)$ have representations;

(B2) $S(f_1, f_m)$ has a representation.

2 Results

2.1 Chain Condition

For terms $t_1, t_2, \dots, t_M$ and polynomials $F = (f_1, f_2, \dots, f_m)$:

$$\mathrm{Chain\_Condition}(t_1, t_2, \dots, t_M; m)$$

iff

$$\left.\begin{array}{r} S(f_1, f_2) \text{ has representation} \\ S(f_2, f_3) \text{ has representation} \\ \vdots \\ S(f_{M-1}, f_M) \text{ has representation} \end{array}\right\} \implies S(f_1, f_M) \text{ has representation.}$$

2.2 Facts [2, 3, 5]

$$\left[\begin{array}{c} \mathrm{BC1}(t_1, t_M) \text{ or } \mathrm{BC2}(t_1, t_k, t_M) \\ \text{for all } k : 1 \neq 1, m \end{array}\right] \implies \mathrm{Chain\_Condition}(t_1, t_2, \dots, t_M; m)$$

but

$$\left[\begin{array}{c} \mathrm{BC1}(t_1, t_M) \text{ or } \mathrm{BC2}(t_1, t_k, t_M) \\ \text{for all } k : 1 \neq 1, m \end{array}\right] \not\Longleftarrow \mathrm{Chain\_Condition}(t_1, t_2, \dots, t_M; m).$$

What C such that

$$\mathrm{C}(t_1, t_2, \dots, t_M) \iff \mathrm{Chain\_Condition}(t_1, t_2, \dots, t_M; m)?$$

2.3 Results [6]

Fewer leading terms examined than polynomials? BC necessary.

Theorem 1. *If $M < m$, then (A) iff (B) where*
(A) $\mathrm{Chain\_Condition}(t_1, t_2, \dots, t_M; m)$;
(B) $\mathrm{BC1}(t_1, t_M)$ or $\mathrm{BC2}(t_1, t_k, t_M)$ for all $k : 1 \le k \le M$.

All leading terms examined? Generalization of BC exists!

Definition. The **Extended First Criterion** is [(EC_div) and (EC_var)] where

(EC_div) $\gcd(t_1, t_m)$ divides t_k for all $k = 2, 3, \dots, m-1$.
(EC_var) for all x,

$$\deg_x \gcd(t_1, t_m) = 0, \text{ or}$$
$$\deg_x t_1 \le \deg_x t_2 \le \cdots \le \deg_x t_m, \text{ or}$$
$$\deg_x t_1 \ge \deg_x t_2 \ge \cdots \ge \deg_x t_m.$$

$\mathbf{EC}(t_1, t_2, \dots, t_m) :=$ (EC_div)$(t_1, t_2, \dots, t_m)$ and (EC_var)$(t_1, t_2, \dots, t_m)$.

Theorem 2. *If $M = m$, then (A) iff (B) where*
(A) $\mathrm{Chain\_Condition}(t_1, t_2, \dots, t_m; m)$;
(B) $\mathrm{EC}(t_1, t_2, \dots, t_m)$ or $\mathrm{BC2}(t_1, t_k, t_m)$ for all $k : 1 \le k \le m$.

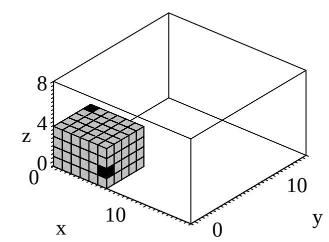
3 Analysis

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

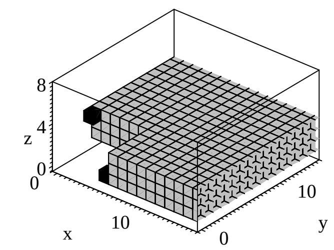
4 Illustration, Examples

Let $t_1 = x^5 z$, $t_m = y^4 z^3$:

Locations for terms in BC2 chains



Locations for terms in EC chains



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

- $\mathrm{lt}(f_1) = x^5 z$, $\mathrm{lt}(f_2) = x^7 z^2$, and $\mathrm{lt}(f_3) = y^4 z^3$;
- $S(f_1, f_2)$ 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 Criteria.

- **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 ⇒ Can only rely on BC! Counterexamples easy!)

Cute Corollary. *If $F = (f_1, f_2, \dots, f_m)$ and for all $k = 1, 2, \dots, m$ we have $\mathrm{lt}(f_k) = u_k g$ where $\gcd(u_i, u_j g) = 1$ for all $i \neq j$, then we can decide whether F is a Gröbner basis by checking only $m - 1$ S-polynomials.*

References

[1] Thomas Becker and Volker Weispfenning and Hans Kredel, "Gröbner Bases: a Computational Approach to Commutative Algebra", 1993, Springer-Verlag, New York.

[2] Bruno Buchberger, "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalem Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal)", PhD Dissertation, 1969.

[3] Bruno Buchberger, "A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases", Proceedings of the EUROSAM 79 Symposium on Symbolic and Algebraic Manipulation, Marseille, June 26-28, 1979.

[4] Rudiger Gebauer and Hans Möller, "On an Installation of Buchberger's Algorithm", Journal of Symbolic Computation (6), 1988.

[5] Hoon Hong and John Perry, "Are Buchberger's Criteria necessary for the Chain Condition?", Journal of Symbolic Computation, 2007.

[6] John Perry, "A criterion that is necessary and sufficient for the chain condition", in preparation.

ABSTRACT

In addition to his algorithm to compute Gröbner bases, Buchberger has developed two criteria that allow one to detect when a critical step of the algorithm—reduction to zero—is unnecessary. Due to its structure, the second criterion is often called a chain condition. The first criterion can also be viewed as a chain condition.

It is natural to ask whether these two sufficient criteria are also necessary for the chain condition. It has recently been shown that they are not. This poster presents a criterion that generalizes the chain condition in a way that is necessary as well as sufficient. It gives some examples where this criterion detects reduction to zero that Buchberger's criteria would not detect, as well as examples where this criterion does not detect reduction when one might expect. It concludes with a very superficial analysis of how useful the criterion would be in practical use.