Refinements of the Buchberger Criterion and Improvements of the Buchberger Algorithm

Alan R. Hahn

Clemson University

April 2018

Recall

GB Criterion 1

A basis $G = \{g_1, ..., g_s\}$ for an ideal $I \subseteq k[x_1, ..., x_n]$ is a Gröbner basis for I iff for all pairs i, j, $rem_G(S(g_i, g_j)) = 0$.

Buchberger's Algorithm

Let $0 \neq I = \langle f_1, ..., f_s \rangle$ be an ideal in $k[x_1, ..., x_n]$. A Gröbner basis for I may be constructed as follows:

$G := \{f_1, ..., f_s\}$

$\forall f_i, f_j$, *if* $rem_G(S(f_i, f_j)) = r \neq 0$, *then* $G = G \cup \{r\}$. *Restart and do until all remainders are zero.*

Where $S(f, g) = \frac{lcm(LM(f), LM(g))}{LT(f)} \cdot f - \frac{lcm(LM(f), LM(g))}{LT(g)} \cdot g$.

Definition

Fix a monomial order and let $G = \{g_1, ..., g_t\} \subseteq k[x_1, ..., x_n]$*. Given* $f \in k[x_1, ..., x_n]$*, we say that* f **reduces to zero modulo** G*, written*

$$f \to_G 0,$$

if f *has a* **standard representation**

$$f = A_1 g_1 + ... + A_t g_t,\ A_i \in k[x_1, ..., x_n],$$

such that whenever $A_i g_i \neq 0$*, then*

$$multideg(f) \geq multideg(A_i g_i).$$

Lemma

Let $G = (g_1, ..., g_t)$ be an ordered set of elements of $k[x_1, ..., x_n]$ and fix $f \in k[x_1, ..., x_n]$. Then $rem_G(f) = 0 \implies f \to_G 0$.

Lemma

Let $G = (g_1, ..., g_t)$ *be an ordered set of elements of* $k[x_1, ..., x_n]$ *and fix* $f \in k[x_1, ..., x_n]$. *Then* $rem_G(f) = 0 \implies f \to_G 0$.

GB Criterion 2

A basis $G = \{g_1, ..., g_t\}$ *for an ideal* I *is a Gröbner basis iff* $S(g_i, g_j) \to_G 0$ *for all* $i \neq j$.

Lemma

Let $G = (g_1, ..., g_t)$ be an ordered set of elements of $k[x_1, ..., x_n]$ and fix $f \in k[x_1, ..., x_n]$. Then $rem_G(f) = 0 \implies f \rightarrow_G 0$.

GB Criterion 2

A basis $G = \{g_1, ..., g_t\}$ for an ideal I is a Gröbner basis iff $S(g_i, g_j) \rightarrow_G 0$ for all $i \neq j$.

Proposition 1

Given a finite set $G \subseteq k[x_1, ..., x_n]$, suppose that for $f, g \in G$, $LM(f)$ and $LM(g)$ are relatively prime. Then $S(f, g) \rightarrow_G 0$.

Example

Let $\{yz + y, x^3 + y, z^4 + x + y\} = G \subseteq k[x, y, z]$ *with grlex order. Note* x^3 *and* z^4 *are relatively prime. Then*

$$S(x^3 + y, z^4 + x + y) = z^4 \cdot (x^3 + y) - x^3 \cdot (z^4 + x + y)$$
$$= (z^4 + x + y - x - y) \cdot (x^3 + y) - (x^3 + y - y) \cdot (z^4 + x + y)$$
$$= (z^4+x+y)\cdot(x^3+y)-(-x-y)\cdot(x^3+y)-(x^3+y)\cdot(z^4+x+y)+y\cdot(z^4+x+y)$$
$$= y \cdot (z^4 + x + y) - (-x - y) \cdot (x^3 + y).$$

Definition

Let $F = (f_1, ..., f_s)$. A **syzygy** *on the leading terms $LT(f_1), ..., LT(f_s)$ of F is an s-tuple of polynomials $S = (h_1, ..., h_s) \in (k[x_1, ..., x_n])^s$ such that*

$$\sum_{i=1}^{s} h_i \cdot LT(f_i) = 0.$$

Denote by $S(F)$ the subset of $(k[x_1, ..., x_n])^s$ consisting of all syzygies on the leading terms of F.

Definition

Let $F = (f_1, ..., f_s)$. A **syzygy** *on the leading terms $LT(f_1), ..., LT(f_s)$ of F is an s-tuple of polynomials $S = (h_1, ..., h_s) \in (k[x_1, ..., x_n])^s$ such that*

$$\sum_{i=1}^{s} h_i \cdot LT(f_i) = 0.$$

Denote by $S(F)$ the subset of $(k[x_1, ..., x_n])^s$ consisting of all syzygies on the leading terms of F.

Example

Consider $F = (x, x^2 + z, y + z)$ with the lex ordering. Then $S = (-x + y, 1, -x)$ defines a syzygy in $S(F)$:

$$(-x + y) \cdot LT(x) + 1 \cdot LT(x^2 + z) + -x \cdot LT(y + z) = -x^2 + xy + x^2 - xy = 0.$$

Definition

Let $F = (f_1, ..., f_s)$. A **syzygy** *on the leading terms $LT(f_1), ..., LT(f_s)$ of F is an s-tuple of polynomials $S = (h_1, ..., h_s) \in (k[x_1, ..., x_n])^s$ such that*

$$\sum_{i=1}^{s} h_i \cdot LT(f_i) = 0.$$

Denote by $S(F)$ the subset of $(k[x_1, ..., x_n])^s$ consisting of all syzygies on the leading terms of F.

Example

Consider $F = (x, x^2 + z, y + z)$ with the lex ordering. Then $S = (-x + y, 1, -x)$ defines a syzygy in $S(F)$:

$$(-x + y) \cdot LT(x) + 1 \cdot LT(x^2 + z) + -x \cdot LT(y + z) = -x^2 + xy + x^2 - xy = 0.$$

Definition

For $S = (H_1, ..., H_s) \in S(F)$,

$$S \cdot F := \sum_{i=1}^{t} H_i f_i.$$

Definition

An element $S \in S(F)$ *is* **homogeneous of multidegree** α, *where* $\alpha \in \mathbb{Z}_{\geq 0}$, *provided that*

$$S = (c_1 x^{\alpha(1)}, ..., c_s x^{\alpha(s)}),$$

where $c_i \in k$ *and* $\alpha(i) + multideg(f_i) = \alpha$ *whenever* $c_i \neq 0$.

Definition

An element $S \in S(F)$ *is* **homogeneous of multidegree** α, *where* $\alpha \in \mathbb{Z}_{\geq 0}$, *provided that*

$$S = (c_1 x^{\alpha(1)}, ..., c_s x^{\alpha(s)}),$$

where $c_i \in k$ *and* $\alpha(i) + multideg(f_i) = \alpha$ *whenever* $c_i \neq 0$.

Definition

$$S_{ij} := \frac{lcm(LM(f_i), LM(f_j))}{LT(f_i)} \cdot e_i - \frac{lcm(LM(f_i), LM(f_j))}{LT(f_j)} \cdot e_j.$$

Note S_{ij} *is homogeneous of degree* $multideg(lcm(LT(f_i), LT(f_j)))$.

Definition

An element $S \in S(F)$ *is* **homogeneous of multidegree** α, *where* $\alpha \in \mathbb{Z}_{\geq 0}$, *provided that*

$$S = (c_1 x^{\alpha(1)}, ..., c_s x^{\alpha(s)}),$$

where $c_i \in k$ *and* $\alpha(i) + multideg(f_i) = \alpha$ *whenever* $c_i \neq 0$.

Definition

$$S_{ij} := \frac{lcm(LM(f_i), LM(f_j))}{LT(f_i)} \cdot e_i - \frac{lcm(LM(f_i), LM(f_j))}{LT(f_j)} \cdot e_j.$$

Note S_{ij} *is homogeneous of degree* $multideg(lcm(LT(f_i), LT(f_j)))$.

Example

Consider $G = (x^2y^2 + z, xy^2 - y, x^2y + yz)$. *Then*
$S_{1,2} = (1, -x, 0)$.
Note $S_{ij} \cdot G = S(g_i, g_j)$.

Lemma

Every element of S(F) can be written uniquely as a sum of homogeneous elements of S(F).

Proof.

Fix $\alpha \in \mathbb{Z}_{\geq 0}$, and let $h_{i\alpha}$ be the term of h_i such that $h_{i\alpha} f_i$ has multidegree α, if such term exists. Then $\sum_{i=1}^{s} h_{i\alpha} LT(f_i) = 0$ as $h_{i\alpha} LT(f_i)$ are the terms of multidegree α in the sum $\sum_{i=1}^{s} h_i LT(f_i) = 0$.
Thus $S_\alpha = (h_{1\alpha}, ..., h_{s\alpha})$ is a homogeneous element of $S(F)$ of degree α and $S = \sum_\alpha S_\alpha$. □

Lemma

Every element of $S(F)$ can be written uniquely as a sum of homogeneous elements of $S(F)$.

Proof.

Fix $\alpha \in \mathbb{Z}_{\geq 0}$, and let $h_{i\alpha}$ be the term of h_i such that $h_{i\alpha} f_i$ has multidegree α, if such term exists. Then $\sum_{i=1}^{s} h_{i\alpha} LT(f_i) = 0$ as $h_{i\alpha} LT(f_i)$ are the terms of multidegree α in the sum $\sum_{i=1}^{s} h_i LT(f_i) = 0$.
Thus $S_\alpha = (h_{1\alpha}, ..., h_{s\alpha})$ is a homogeneous element of $S(F)$ of degree α and $S = \sum_\alpha S_\alpha$. □

Proposition

Given $F = (f_1, ..., f_s)$, every syzygy $S \in S(F)$ can be written as

$$S = \sum_{i<j} u_{ij} S_{ij},$$

where $u_{ij} \in k[x_1, ..., x_n]$.

GB Criterion 2 (Recall)

A basis $G = \{g_1, ..., g_t\}$ for an ideal I is a Gröbner basis iff $S(g_i, g_j) \rightarrow_G 0$ for all $i \neq j$.

GB Criterion 2 (Recall)

A basis $G = \{g_1, ..., g_t\}$ *for an ideal* I *is a Gröbner basis iff* $S(g_i, g_j) \rightarrow_G 0$ *for all* $i \neq j$.

GB Criterion 3

A basis $G = (g_1, ..., g_t)$ *for an ideal* I *is a Gröbner basis iff for every element* $S = (H_1, ..., H_t)$ *in a homogeneous basis for the syzygies* $S(G)$, $S \cdot G \rightarrow_G 0$.

GB Criterion 2 (Recall)

A basis $G = \{g_1, ..., g_t\}$ *for an ideal* I *is a Gröbner basis iff* $S(g_i, g_j) \to_G 0$ *for all* $i \neq j$*.*

GB Criterion 3

A basis $G = (g_1, ..., g_t)$ *for an ideal* I *is a Gröbner basis iff for every element* $S = (H_1, ..., H_t)$ *in a homogeneous basis for the syzygies* $S(G)$*,* $S \cdot G \to_G 0$.

Proposition 2

Given $G = (g_1, ..., g_t)$*, suppose that* $S \subseteq \{S_{ij} \mid 1 \leq i < j \leq t\}$ *is a basis of* $S(G)$*. In addition, suppose we have distinct elements* $g_i, g_j, g_l \in G$ *such that* $LT(g_l)$ *divides* $lcm(LT(g_i), LT(g_j))$*. If* $S_{il}, S_{jl} \in S$*, then* $S \setminus \{S_{ij}\}$ *is also a basis of* $S(G)$*.*

GB Criterion 2 (Recall)

A basis $G = \{g_1, ..., g_t\}$ for an ideal I is a Gröbner basis iff $S(g_i, g_j) \to_G 0$ for all $i \neq j$.

GB Criterion 3

A basis $G = (g_1, ..., g_t)$ for an ideal I is a Gröbner basis iff for every element $S = (H_1, ..., H_t)$ in a homogeneous basis for the syzygies $S(G)$, $S \cdot G \to_G 0$.

Proposition 2

Given $G = (g_1, ..., g_t)$, suppose that $S \subseteq \{S_{ij} \mid 1 \leq i < j \leq t\}$ is a basis of $S(G)$. In addition, suppose we have distinct elements $g_i, g_j, g_l \in G$ such that $LT(g_l)$ divides $lcm(LT(g_i), LT(g_j))$. If $S_{il}, S_{jl} \in S$, then $S \setminus \{S_{ij}\}$ is also a basis of $S(G)$.

Proof.

For simplicity, suppose $i < j < l$. Set $x^{\gamma_{ij}} = lcm(LM(g_i), LM(g_j))$, and let $x^{\gamma_{il}}$ and $x^{\gamma_{jl}}$ be defined similarly. Then by assumption, $x^{\gamma_{il}}$, $x^{\gamma_{jl}}$ both divide $x^{\gamma_{ij}}$. It remains to note that

$$S_{ij} = \frac{x^{\gamma_{ij}}}{x^{\gamma_{il}}} S_{il} - \frac{x^{\gamma_{ij}}}{x^{\gamma_{jl}}} S_{jl}.$$

$\square$

Summary of Results

GB Criterion 2 (Restated)

A basis $G = \{g_1, ..., g_t\}$ for an ideal I is a Gröbner basis iff $S_{ij} \cdot G = S(g_i, g_j) \to_G 0$ for all $i \neq j$.

Proposition 1 (Restated)

Given a finite set $G \subseteq k[x_1, ..., x_n]$, suppose that for $g_i, g_j \in G$, $LM(g_i)$ and $LM(g_j)$ are relatively prime. Then $S_{ij} \cdot G = S(g_i, g_j) \to_G 0$.

GB Criterion 3

A basis $G = (g_1, ..., g_t)$ for an ideal I is a Gröbner basis iff for every element $S = (H_1, ..., H_t)$ in a homogeneous basis for the syzygies $S(G)$, $S \cdot G \to_G 0$.

Proposition 2

Given $G = (g_1, ..., g_t)$, suppose that $S \subseteq \{S_{ij} \mid 1 \leq i < j \leq t\}$ is a basis of $S(G)$. In addition, suppose we have distinct elements $g_i, g_j, g_l \in G$ such that $LT(g_l)$ divides $lcm(LT(g_i), LT(g_j))$. If $S_{il}, S_{jl} \in S$, then $S \setminus \{S_{ij}\}$ is also a basis of $S(G)$.

Main Theorem

Let $I = \langle f_1, ..., f_s \rangle$ be a polynomial ideal. Then a Gröbner basis of I can be constructed in a finite number of steps by the following algorithm:
Input: $F = (f_1, ..., f_s)$
Output: a Gröbner basis G for $I = \langle f_1, ..., f_s \rangle$

$B := \{(i, j) \mid 1 \leq i < j \leq s\}$
$G := F$
$t := s$
While $B \neq \emptyset$ Do
  Select $(i, j) \in B$
  If $lcm(LT(f_i), LT(f_j)) \neq LT(f_i)LT(f_j)$ and Criterion$(f_i, f_j, B) =$ false Then
    $r := \text{rem}_G(S(f_i, f_j))$
    If $r \neq 0$ Then
      $t := t + 1; f_t := r$
      $G := G \cup \{f_t\}$
      $B := B \cup \{(i, t) \mid 1 \leq i \leq t - 1\}$
  $B := B \setminus \{(i, j)\}$
Return G

Criterion(f_i, f_j, B) is true provided that there is some $l \notin \{i, j\}$ for which the pairs (i, l) and (j, l) are not in B and $LT(f_l)$ divides $lcm(LT(f_i), LT(f_j))$. (Based on Proposition 2)