

Gröbner Bases Introduction 3

Daniel Cabarcas, University of Cincinnati

Cryptography Seminar
Cincinnati, April 20, 2009

Construction of Gröbner bases

Theorem (characterization of Gröbner bases)

$G = \{g_1, \dots, g_t\} \subseteq I$ is a Gröbner basis of I w.r.t. a monomial order \leq iff

For all $f \in K[\underline{x}]$ there exist **unique** $r \in K[\underline{x}]$ and $g \in I$ s.t.

$$f = g + r$$

and no monomial of r is divisible by any of $\text{LM}(g_1), \dots, \text{LM}(g_t)$.

Theorem (characterization of Gröbner bases)

$G = \{g_1, \dots, g_t\} \subseteq I$ is a Gröbner basis of I w.r.t. a monomial order \leq iff

For all $f \in K[\underline{x}]$ there exist **unique** $r \in K[\underline{x}]$ and $g \in I$ s.t.

$$f = g + r$$

and no monomial of r is divisible by any of $\text{LM}(g_1), \dots, \text{LM}(g_t)$.

The crucial idea in Gröbner basis theory is the observation that these infinitely many tests can be replaced by the consideration of finitely many “critical situations” that can be characterized by the so-called “S-polynomials”. Bruno Buchberger 1999

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

Let $f, g \in K[\underline{x}]$

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

Let $f, g \in K[\underline{x}]$

let $m = \text{lcm}(\text{LM}(f), \text{LM}(g))$

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

Let $f, g \in K[\underline{x}]$

let $m = \text{lcm}(\text{LM}(f), \text{LM}(g))$

The **s -polynomial** of f and g is

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

Let $f, g \in K[\underline{x}]$

let $m = \text{lcm}(\text{LM}(f), \text{LM}(g))$

The **s-polynomial** of f and g is

$$S(f, g) := \frac{m}{\text{LT}(f)}f - \frac{m}{\text{LT}(g)}g$$

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

$$S(f, g) := \frac{m}{LT(f)} f - \frac{m}{LT(g)} g$$

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

$$S(f, g) := \frac{m}{LT(f)} f - \frac{m}{LT(g)} g$$

e.g. $S(x^2y - 1, xy^2 - 1)$

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

$$S(f, g) := \frac{m}{LT(f)} f - \frac{m}{LT(g)} g$$

e.g. $S(x^2y - 1, xy^2 - 1)$

$$= \frac{x^2y^2}{x^2y} (x^2y - 1) - \frac{x^2y^2}{xy^2} (xy^2 - 1)$$

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

$$S(f, g) := \frac{m}{LT(f)} f - \frac{m}{LT(g)} g$$

e.g. $S(x^2y - 1, xy^2 - 1)$

$$\begin{aligned} &= \frac{x^2y^2}{x^2y} (x^2y - 1) - \frac{x^2y^2}{xy^2} (xy^2 - 1) \\ &= y(x^2y - 1) - x(xy^2 - 1) \end{aligned}$$

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

$$S(f, g) := \frac{m}{LT(f)} f - \frac{m}{LT(g)} g$$

e.g. $S(x^2y - 1, xy^2 - 1)$

$$\begin{aligned} &= \frac{x^2y^2}{x^2y} (x^2y - 1) - \frac{x^2y^2}{xy^2} (xy^2 - 1) \\ &= y(x^2y - 1) - x(xy^2 - 1) \\ &= (x^2y^2 - y) - (x^2y^2 - x) \end{aligned}$$

Construction of Gröbner basis

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$$

$$S(f, g) := \frac{m}{LT(f)} f - \frac{m}{LT(g)} g$$

e.g. $S(x^2y - 1, xy^2 - 1)$

$$\begin{aligned} &= \frac{x^2y^2}{x^2y} (x^2y - 1) - \frac{x^2y^2}{xy^2} (xy^2 - 1) \\ &= y(x^2y - 1) - x(xy^2 - 1) \\ &= (x^2y^2 - y) - (x^2y^2 - x) \\ &= x - y \end{aligned}$$

Construction of Gröbner basis

Theorem

Let I be an ideal of $K[\underline{x}]$. Then a set of generators $G = \{g_1, \dots, g_t\}$ for I is a Gröbner basis for I iff for all $i \neq j$

$$S(g_i, g_j) \xrightarrow[G]{*} 0$$

Construction of Gröbner basis

Theorem

Let I be an ideal of $K[\underline{x}]$. Then a set of generators $G = \{g_1, \dots, g_t\}$ for I is a Gröbner basis for I iff for all $i \neq j$

$$S(g_i, g_j) \xrightarrow[G]{*} 0$$

Lemma

Let $f_1, \dots, f_s \in K[\underline{x}]$ and $c_1, \dots, c_s \in K$. Suppose that for $\text{LM}(f_1) = \text{LM}(f_2) = \dots = \text{LM}(f_s) =: m$ and that $\text{LM}(\sum_{i=1}^s c_i \cdot f_i) < m$.

Construction of Gröbner basis

Theorem

Let I be an ideal of $K[\underline{x}]$. Then a set of generators $G = \{g_1, \dots, g_t\}$ for I is a Gröbner basis for I iff for all $i \neq j$

$$S(g_i, g_j) \xrightarrow[G]{*} 0$$

Lemma

Let $f_1, \dots, f_s \in K[\underline{x}]$ and $c_1, \dots, c_s \in K$. Suppose that for $\text{LM}(f_1) = \text{LM}(f_2) = \dots = \text{LM}(f_s) =: m$ and that $\text{LM}(\sum_{i=1}^s c_i \cdot f_i) < m$. Then $\sum_{i=1}^s c_i \cdot f_i$ is a linear combination with coefficients in K of the s -polynomials $S(f_i, f_j)$ for $1 \leq j < k \leq s$.

Construction of Gröbner basis

Theorem

Let I be an ideal of $K[\underline{x}]$. Then a set of generators $G = \{g_1, \dots, g_t\}$ for I is a Gröbner basis for I iff for all $i \neq j$

$$S(g_i, g_j) \xrightarrow[G]{*} 0$$

Lemma

Let $f_1, \dots, f_s \in K[\underline{x}]$ and $c_1, \dots, c_s \in K$. Suppose that for $\text{LM}(f_1) = \text{LM}(f_2) = \dots = \text{LM}(f_s) =: m$ and that $\text{LM}(\sum_{i=1}^s c_i \cdot f_i) < m$. Then $\sum_{i=1}^s c_i \cdot f_i$ is a linear combination with coefficients in K of the s -polynomials $S(f_i, f_j)$ for $1 \leq j < k \leq s$. Furthermore, $\text{LM}(S(f_i, f_j)) < m$

Construction of Gröbner basis

Theorem

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

Construction of Gröbner basis

Theorem

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

Buchberger algorithm($F = \{f_1, \dots, f_s\}$)

Construction of Gröbner basis

Theorem

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

Buchberger algorithm($F = \{f_1, \dots, f_s\}$)

▶ $G := F$

Theorem

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

Buchberger algorithm($F = \{f_1, \dots, f_s\}$)

- ▶ $G := F$
- ▶ REPEAT

Theorem

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

Buchberger algorithm($F = \{f_1, \dots, f_s\}$)

- ▶ $G := F$
- ▶ REPEAT
 - ▶ $G' := G$

Theorem

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

Buchberger algorithm($F = \{f_1, \dots, f_s\}$)

- ▶ $G := F$
- ▶ REPEAT
 - ▶ $G' := G$
 - ▶ FOR EACH pair $\{f, g\}$ $f \neq g$ in G'

Theorem

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

Buchberger algorithm($F = \{f_1, \dots, f_s\}$)

- ▶ $G := F$
- ▶ REPEAT
 - ▶ $G' := G$
 - ▶ FOR EACH pair $\{f, g\}$ $f \neq g$ in G'
 - ▶ Compute $S(f, g) \xrightarrow[G']{*} \underline{r}$

Theorem

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

Buchberger algorithm($F = \{f_1, \dots, f_s\}$)

- ▶ $G := F$
- ▶ REPEAT
 - ▶ $G' := G$
 - ▶ FOR EACH pair $\{f, g\}$ $f \neq g$ in G'
 - ▶ Compute $S(f, g) \xrightarrow[G']{*} \underline{r}$
 - ▶ IF $r \neq 0$ THEN $G := G \cup \{r\}$

Theorem

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

Buchberger algorithm($F = \{f_1, \dots, f_s\}$)

- ▶ $G := F$
- ▶ REPEAT
 - ▶ $G' := G$
 - ▶ FOR EACH pair $\{f, g\}$ $f \neq g$ in G'
 - ▶ Compute $S(f, g) \xrightarrow[G']{*} \underline{r}$
 - ▶ IF $r \neq 0$ THEN $G := G \cup \{r\}$
- ▶ UNTIL $G = G'$