

Gröbner Bases Introduction 2

Daniel Cabarcas, University of Cincinnati

Cryptography Seminar
Cincinnati, April 13, 2009

Definition of Gröbner Basis

Definition of Gröbner Basis

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

Definition of Gröbner Basis

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

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

Existence of Gröbner Basis

Theorem (Dickson's lemma)

Let $I = \langle A \rangle$ be a monomial ideal, then $I = \langle a_1, \dots, a_t \rangle$ where $a_1, \dots, a_t \in A$.

Existence of Gröbner Basis

Theorem (Dickson's lemma)

Let $I = \langle A \rangle$ be a monomial ideal, then $I = \langle a_1, \dots, a_t \rangle$ where $a_1, \dots, a_t \in A$.

Proof.

by induction on the number of variables n .



Existence of Gröbner Basis

Theorem (Dickson's lemma)

Let $I = \langle A \rangle$ be a monomial ideal, then $I = \langle a_1, \dots, a_t \rangle$ where $a_1, \dots, a_t \in A$.

Proof.

by induction on the number of variables n . □

Theorem (Hilbert Basis Theorem)

Every ideal $I \subseteq K[\underline{x}]$ has a finite generating set.

Existence of Gröbner Basis

Theorem (Dickson's lemma)

Let $I = \langle A \rangle$ be a monomial ideal, then $I = \langle a_1, \dots, a_t \rangle$ where $a_1, \dots, a_t \in A$.

Proof.

by induction on the number of variables n . □

Theorem (Hilbert Basis Theorem)

Every ideal $I \subseteq K[\underline{x}]$ has a finite generating set.

Proof.

By Dickson's lemma we can choose $g_1, \dots, g_t \in I$ s.t.
 $\langle LM(g_1), \dots, LM(g_t) \rangle = \langle LM(I) \rangle$ □

Existence of Gröbner Basis

Theorem (Dickson's lemma)

Let $I = \langle A \rangle$ be a monomial ideal, then $I = \langle a_1, \dots, a_t \rangle$ where $a_1, \dots, a_t \in A$.

Proof.

by induction on the number of variables n . □

Theorem (Hilbert Basis Theorem)

Every ideal $I \subseteq K[\underline{x}]$ has a finite generating set.

Proof.

By Dickson's lemma we can choose $g_1, \dots, g_t \in I$ s.t.
 $\langle LM(g_1), \dots, LM(g_t) \rangle = \langle LM(I) \rangle$ □

Corollary (existence of Gröbner basis)

Every ideal $I \subseteq K[\underline{x}]$ other than $\{0\}$ has a Gröbner basis.

Theorem (The ascending chain condition)

*Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be an ascending chain of ideals in $K[\underline{x}]$.
Then there exist $N \geq 1$ s.t. $I_N = I_{N+1} = \dots$.*

Theorem (The ascending chain condition)

*Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be an ascending chain of ideals in $K[\underline{x}]$.
Then there exist $N \geq 1$ s.t. $I_N = I_{N+1} = \dots$.*

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

Theorem (The ascending chain condition)

Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be an ascending chain of ideals in $K[\underline{x}]$.
Then there exist $N \geq 1$ s.t. $I_N = I_{N+1} = \dots$.

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.

Theorem (The ascending chain condition)

Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be an ascending chain of ideals in $K[\underline{x}]$.
Then there exist $N \geq 1$ s.t. $I_N = I_{N+1} = \dots$.

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.

$$f = g + r$$

Theorem (The ascending chain condition)

Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be an ascending chain of ideals in $K[\underline{x}]$.
Then there exist $N \geq 1$ s.t. $I_N = I_{N+1} = \dots$.

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 $\text{LM}(g_1), \dots, \text{LM}(g_t)$.

- ▶ Decide whether $f \equiv g \pmod{F}$

- ▶ Decide whether $f \equiv g \pmod{F}$
- ▶ Decide whether $f \in \langle F \rangle$

- ▶ Decide whether $f \equiv g \pmod{F}$
- ▶ Decide whether $f \in \langle F \rangle$
- ▶ Decide whether $\langle F \rangle = \langle G \rangle$

- ▶ Decide whether $f \equiv g \pmod{F}$
- ▶ Decide whether $f \in \langle F \rangle$
- ▶ Decide whether $\langle F \rangle = \langle G \rangle$
- ▶ Find a linearly independent basis B for the vector space $K[\underline{x}]/\langle F \rangle$

- ▶ Decide whether $f \equiv g \pmod{F}$
- ▶ Decide whether $f \in \langle F \rangle$
- ▶ Decide whether $\langle F \rangle = \langle G \rangle$
- ▶ Find a linearly independent basis B for the vector space $K[\underline{x}]/\langle F \rangle$, and for $a, b \in B$ find a linear representation of $a \cdot b$ in terms of the basis elements.

- ▶ Decide whether $f \equiv g \pmod{F}$
- ▶ Decide whether $f \in \langle F \rangle$
- ▶ Decide whether $\langle F \rangle = \langle G \rangle$
- ▶ Find a linearly independent basis B for the vector space $K[\underline{x}]/\langle F \rangle$, and for $a, b \in B$ find a linear representation of $a \cdot b$ in terms of the basis elements.
- ▶ Assuming $K[\underline{x}]/\langle F \rangle$ is finite dimensional, and given F, f, h , find g s.t. $f \cdot g \equiv h \pmod{F}$.

Uniqueness

A Gröbner basis for an ideal is not unique.

Uniqueness

A Gröbner basis for an ideal is not unique.

Definition

A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that

Uniqueness

A Gröbner basis for an ideal is not unique.

Definition

A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that

- (i) All $g \in G$ are monic, and

A Gröbner basis for an ideal is not unique.

Definition

A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that

- (i) All $g \in G$ are monic, and
- (ii) For all $g \in G$, no monomial of g lies in $\langle \text{LM}(G \setminus \{g\}) \rangle$

Uniqueness

A Gröbner basis for an ideal is not unique.

Definition

A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that

- (i) All $g \in G$ are monic, and
- (ii) For all $g \in G$, no monomial of g lies in $\langle \text{LM}(G \setminus \{g\}) \rangle$

Lemma

Let G be a Gröbner basis for I , $g \in G$ be s.t.

$\langle \text{LM}(G) \rangle = \langle \text{LM}(G \setminus \{g\}) \rangle$, then $G \setminus \{g\}$ is a Gröbner basis for I .

Uniqueness

A Gröbner basis for an ideal is not unique.

Definition

A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that

- (i) All $g \in G$ are monic, and
- (ii) For all $g \in G$, no monomial of g lies in $\langle \text{LM}(G \setminus \{g\}) \rangle$

Lemma

Let G be a Gröbner basis for I , $g \in G$ be s.t.

$\langle \text{LM}(G) \rangle = \langle \text{LM}(G \setminus \{g\}) \rangle$, then $G \setminus \{g\}$ is a Gröbner basis for I .

Proposition

Let $I \neq 0$ be a polynomial ideal, \leq a monomial order. Then, I has a unique reduced Gröbner basis w.r.t. \leq .