

Gröbner Bases Introduction

Daniel Cabarcas, University of Cincinnati

Cryptography Seminar
Cincinnati, April 2009

- ▶ Gröbner Bases Theory
 - ▶ Definition, existence, uniqueness
 - ▶ Characterizations, uses
 - ▶ Buchberger algorithm, correctness, termination
- ▶ Improvements 60s to 90s
 - ▶ Selection strategy
 - ▶ Pair discarding techniques
 - ▶ Change of ordering
- ▶ Faugère's F4 and F5
- ▶ XL
- ▶ Mutant polynomials, algorithms
- ▶ Implementation
 - ▶ Memory management
 - ▶ Sparse linear solvers
- ▶ Complexity analysis
- ▶ Algebraic Cryptanalysis
 - ▶ MPKCs
 - ▶ Symmetric ciphers

References

GB theory:

- ▶ The book by Cox, Little and O'Shea
- ▶ The book by Becker called *Grbner Bases*.
- ▶ A paper by Buchberger from 85 called *Grbner Bases: An Algorithmic Method in Polynomial Ideal Theory*.
- ▶ A paper by Lazard from 91 called *Systems of algebraic equations (algorithms and Complexity)*.

References

Fast implementations:

- ▶ A paper by Gebauer and Möller from 88 called *On an installation of Buchberger's Algorithm*.
- ▶ A paper by Giovini from 89 called *One sugar please...*
- ▶ The f4 and f5 papers by Faugère.

References

Complexity:

- ▶ papers by Bardet, Faugère, Salvy and Bo-Yin Yang from around 2003 with title *complexity of Gröbner basis computation... or ... degree of regularity ... or ... semi-regular sequences...*
- ▶ the Paper by Jintai, Tim and Victoria.

References

Mutant Algorithms:

- ▶ papers introducing algorithms: MutantXL, MGB, MXL2, MXL3.

References

Algebraic attacks:

- ▶ Attack on HFE using F5 by Faugere.
- ▶ Attack on keeloq by Courtois.

References

Fast sparse linear algebra:

- ▶ A paper by LaMacchia and Odlyzko from 91 called *Solving Large Sparse Linear Systems Over Finite Fields*
- ▶ A paper Pomerance and Smith from 99 called *Reduction of Huge, Sparse Matrices over Finite Fields via Created Catastrophes.*
- ▶ A book by Duff from 86 called *Direct methods for sparse matrices.*
- ▶ A book by Davis from 2006 called *Direct methods for sparse linear systems.*
- ▶ Lecture notes in mathematics, 572 Sparse Matrix Techniques, 76

Notation

K a field

Notation

K a field

$K[x_1, \dots, x_n] = K[\underline{x}]$ the ring of polynomials

Notation

K a field

$K[x_1, \dots, x_n] = K[\underline{x}]$ the ring of polynomials

$f_1, \dots, f_s \in K[\underline{x}]$

K a field

$K[x_1, \dots, x_n] = K[\underline{x}]$ the ring of polynomials

$f_1, \dots, f_s \in K[\underline{x}]$

$\underline{x} = (x_1, \dots, x_n), \alpha = (\alpha_1, \dots, \alpha_n), \alpha_i \in \mathbb{N}_0$

K a field

$K[x_1, \dots, x_n] = K[\underline{x}]$ the ring of polynomials

$f_1, \dots, f_s \in K[\underline{x}]$

$\underline{x} = (x_1, \dots, x_n), \alpha = (\alpha_1, \dots, \alpha_n), \alpha_i \in \mathbb{N}_0$

$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} = \underline{x}^\alpha$ a monomial

K a field

$K[x_1, \dots, x_n] = K[\underline{x}]$ the ring of polynomials

$f_1, \dots, f_s \in K[\underline{x}]$

$\underline{x} = (x_1, \dots, x_n), \alpha = (\alpha_1, \dots, \alpha_n), \alpha_i \in \mathbb{N}_0$

$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} = \underline{x}^\alpha$ a monomial

$M := \{\underline{x}^\alpha \mid \alpha \in \mathbb{N}_0^n\}$ the set of all monomials

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Lexicographic order $<_{lex}$

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Lexicographic order $<_{lex}$

$\underline{x}^\alpha <_{lex} \underline{x}^\beta$ iff in $\beta - \alpha$, the left most nonzero entry is positive

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Lexicographic order $<_{lex}$

$\underline{x}^\alpha <_{lex} \underline{x}^\beta$ iff in $\beta - \alpha$, the left most nonzero entry is positive

note that $x_1 > x_2 > \dots > x_n$

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Graded Lexicographic order $<_{\text{glex}}$

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Graded Lexicographic order $<_{\text{glex}}$

$\underline{x}^\alpha <_{\text{glex}} \underline{x}^\beta$ iff

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Graded Lexicographic order $<_{\text{glex}}$

$\underline{x}^\alpha <_{\text{glex}} \underline{x}^\beta$ iff

$|\alpha| := \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \alpha_i =: |\beta|$ or

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Graded Lexicographic order $<_{\text{glex}}$

$\underline{x}^\alpha <_{\text{glex}} \underline{x}^\beta$ iff

$|\alpha| := \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i =: |\beta|$ or

$|\alpha| = |\beta|$ and $\alpha <_{\text{lex}} \beta$

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Graded Reverse Lexicographic order $<_{grevlex}$

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Graded Reverse Lexicographic order $<_{grevlex}$

$$\underline{x}^\alpha <_{grevlex} \underline{x}^\beta \text{ iff}$$

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Graded Reverse Lexicographic order $<_{grevlex}$

$\underline{x}^\alpha <_{grevlex} \underline{x}^\beta$ iff

$|\alpha| < |\beta|$ or

Ordering of Monomials

Definition

A **monomial ordering** is a relation \leq on M (or equivalently on \mathbb{N}_0^n) satisfying

1. \leq is a total order
2. $m, m_1, m_2 \in M, m_1 \leq m_2 \Rightarrow m \cdot m_1 \leq m \cdot m_2$
3. \leq is a well ordering

Example. Graded Reverse Lexicographic order $<_{grevlex}$

$\underline{x}^\alpha <_{grevlex} \underline{x}^\beta$ iff

$|\alpha| < |\beta|$ or

$|\alpha| = |\beta|$ and in $\beta - \alpha$, the right most nonzero entry is negative

Leading Monomial

Definition

Let $f = \sum a_\alpha \underline{x}^\alpha \in K[\underline{x}]$, $a_\alpha \in K$ and \leq a monomial order

Leading Monomial

Definition

Let $f = \sum a_\alpha \underline{x}^\alpha \in K[\underline{x}]$, $a_\alpha \in K$ and \leq a monomial order

- ▶ The set of **monomials** of f is $M(f) := \{\underline{x}^\alpha \mid a_\alpha \neq 0\}$.

Leading Monomial

Definition

Let $f = \sum a_\alpha \underline{x}^\alpha \in K[\underline{x}]$, $a_\alpha \in K$ and \leq a monomial order

- ▶ The set of **monomials** of f is $M(f) := \{\underline{x}^\alpha \mid a_\alpha \neq 0\}$.
- ▶ The **leading monomial** of f is $\text{LM}(f) := \text{Max}\{\underline{x}^\alpha \mid a_\alpha \neq 0\}$.

Leading Monomial

Definition

Let $f = \sum a_\alpha \underline{x}^\alpha \in K[\underline{x}]$, $a_\alpha \in K$ and \leq a monomial order

- ▶ The set of **monomials** of f is $M(f) := \{\underline{x}^\alpha \mid a_\alpha \neq 0\}$.
- ▶ The **leading monomial** of f is $\text{LM}(f) := \text{Max}\{\underline{x}^\alpha \mid a_\alpha \neq 0\}$.
- ▶ The **leading coefficient** of f is $\text{LC}(f) := a_\alpha$, s.t. $\underline{x}^\alpha = \text{LM}(f)$.

Leading Monomial

Definition

Let $f = \sum a_\alpha \underline{x}^\alpha \in K[\underline{x}]$, $a_\alpha \in K$ and \leq a monomial order

- ▶ The set of **monomials** of f is $M(f) := \{\underline{x}^\alpha \mid a_\alpha \neq 0\}$.
- ▶ The **leading monomial** of f is $\text{LM}(f) := \text{Max}\{\underline{x}^\alpha \mid a_\alpha \neq 0\}$.
- ▶ The **leading coefficient** of f is $\text{LC}(f) := a_\alpha$, s.t. $\underline{x}^\alpha = \text{LM}(f)$.
- ▶ The **leading term** of f is $\text{LT}(f) := \text{LC}(f) \text{LM}(f)$.

A Division Algorithm

Theorem

Let $F = (f_1, \dots, f_s)$,

A Division Algorithm

Theorem

Let $F = (f_1, \dots, f_s)$, \leq a monomial order.

A Division Algorithm

Theorem

Let $F = (f_1, \dots, f_s)$, \leq a monomial order.

Every $g \in K[\underline{x}]$ can be written as

A Division Algorithm

Theorem

Let $F = (f_1, \dots, f_s)$, \leq a monomial order.

Every $g \in K[\underline{x}]$ can be written as

$$g = h_1 f_1 + \dots + h_s f_s + r$$

where $h_i, r \in K[\underline{x}]$ and

A Division Algorithm

Theorem

Let $F = (f_1, \dots, f_s)$, \leq a monomial order.

Every $g \in K[\underline{x}]$ can be written as

$$g = h_1 f_1 + \dots + h_s f_s + r$$

where $h_i, r \in K[\underline{x}]$ and either

- ▶ $r = 0$ or

A Division Algorithm

Theorem

Let $F = (f_1, \dots, f_s)$, \leq a monomial order.

Every $g \in K[\underline{x}]$ can be written as

$$g = h_1 f_1 + \dots + h_s f_s + r$$

where $h_i, r \in K[\underline{x}]$ and either

- ▶ $r = 0$ or
- ▶ none of the terms of r is divisible by any of $LT(f_1), \dots, LT(f_s)$.

A Division Algorithm

Theorem

Let $F = (f_1, \dots, f_s)$, \leq a monomial order.

Every $g \in K[\underline{x}]$ can be written as

$$g = h_1 f_1 + \dots + h_s f_s + r$$

where $h_i, r \in K[\underline{x}]$ and either

- ▶ $r = 0$ or
- ▶ none of the terms of r is divisible by any of $LT(f_1), \dots, LT(f_s)$.

and for $a_i \neq 0$ $LM(h_i f_i) \leq LM(f)$.

A Division Algorithm

Theorem

Let $F = (f_1, \dots, f_s)$, \leq a monomial order.

Every $g \in K[\underline{x}]$ can be written as

$$g = h_1 f_1 + \dots + h_s f_s + r$$

where $h_i, r \in K[\underline{x}]$ and either

- ▶ $r = 0$ or
- ▶ none of the terms of r is divisible by any of $LT(f_1), \dots, LT(f_s)$.

and for $a_i \neq 0$ $LM(h_i f_i) \leq LM(f)$.

We call r a remainder of g on division by F .

A Division Algorithm

$$g = h_1 f_1 + \cdots + h_s f_s + r$$

A Division Algorithm

$$g = h_1 f_1 + \cdots + h_s f_s + r$$

- ▶ remainder is not unique,

A Division Algorithm

$$g = h_1 f_1 + \cdots + h_s f_s + r$$

- ▶ remainder is not unique,
- ▶ $r = 0 \Rightarrow g \in \langle f_1, \dots, f_s \rangle$,

A Division Algorithm

$$g = h_1 f_1 + \cdots + h_s f_s + r$$

- ▶ remainder is not unique,
- ▶ $r = 0 \Rightarrow g \in \langle f_1, \dots, f_s \rangle$,
- ▶ but $g \in \langle f_1, \dots, f_s \rangle \not\Rightarrow r = 0$

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

Dickson's lemma: Every ideal of the form $I = \langle A \rangle$, where $A \subseteq M$ is finitely generated by a subset of A .

Dickson's lemma: Every ideal of the form $I = \langle A \rangle$, where $A \subseteq M$ is finitely generated by a subset of A .

Hilbert Basis theorem: Every ideal is finitely generated.

Dickson's lemma: Every ideal of the form $I = \langle A \rangle$, where $A \subseteq M$ is finitely generated by a subset of A .

Hilbert Basis theorem: Every ideal is finitely generated.

Existence of Gröbner basis follows easily

Definition

An ideal of the form $I = \langle A \rangle$, with $A \subseteq M$ is called a **monomial ideal**.

Definition

An ideal of the form $I = \langle A \rangle$, with $A \subseteq M$ is called a **monomial ideal**.

Lemma

Let $I = \langle A \rangle$ be a monomial ideal, then

- (i) a monomial a lies in I iff a is divisible by a' for some $a' \in A$.

Definition

An ideal of the form $I = \langle A \rangle$, with $A \subseteq M$ is called a **monomial ideal**.

Lemma

Let $I = \langle A \rangle$ be a monomial ideal, then

- (i) a monomial a lies in I iff a is divisible by a' for some $a' \in A$.
- (ii) a polynomial f lies in I iff every monomial of f lies in I .

Definition

An ideal of the form $I = \langle A \rangle$, with $A \subseteq M$ is called a **monomial ideal**.

Lemma

Let $I = \langle A \rangle$ be a monomial ideal, then

- (i) a monomial a lies in I iff a is divisible by a' for some $a' \in A$.
- (ii) a polynomial f lies in I iff every monomial of f lies in I .

Corollary

Two monomial ideals are the same iff they contain the same monomials.

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.