

# Gröbner Basis Conversion Algorithm

Victoria Kruglov  
University of Cincinnati

Cryptography Seminar  
University of Cincinnati, May 2009

# Notation

Let  $k \subset \mathbb{C}$  be a field,

# Notation

Let  $k \subset \mathbb{C}$  be a field,

$I \subset k[x_1, x_2, \dots, x_n]$  be an ideal,

# Notation

Let  $k \subset \mathbb{C}$  be a field,

$I \subset k[x_1, x_2, \dots, x_n]$  be an ideal,

$$A = k[x_1, x_2, \dots, x_n]/I$$

# Notation

Let  $k \subset \mathbb{C}$  be a field,

$I \subset k[x_1, x_2, \dots, x_n]$  be an ideal,

$$A = k[x_1, x_2, \dots, x_n]/I$$

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

# Notation

Let  $k \subset \mathbb{C}$  be a field,

$I \subset k[x_1, x_2, \dots, x_n]$  be an ideal,

$$A = k[x_1, x_2, \dots, x_n]/I$$

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

$$\mathbf{x}^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \text{- monomial in } k[x_1, x_2, \dots, x_n]$$

# Notation

Let  $k \subset \mathbb{C}$  be a field,

$I \subset k[x_1, x_2, \dots, x_n]$  be an ideal,

$$A = k[x_1, x_2, \dots, x_n]/I$$

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

$$\mathbf{x}^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} - \text{monomial in } k[x_1, x_2, \dots, x_n]$$

$$B = \{\mathbf{x}^\alpha : \mathbf{x}^\alpha \notin \langle LT(I) \rangle\} - \text{a basis of } A$$

- Basic Definitions
  - Ordering of Monomials
  - Zero-dimensional ideal
- the FGLM Gröbner basis conversion algorithm
  - Idea
  - Steps of the algorithm
  - Example
- Main Theorem

- David Cox, John Little, Donald O'Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics, Springer, 1998.
- J. Faugere, P. Gianni, D. Lazard and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symbolic Comput. 16 (1993), 329-344.
- T. Becker, V. Weispfenning, *Gröbner bases*, Springer-Verlag, New-York, 1993.

# Ordering of Monomials

## Definition

A **monomial order** on  $k[x_1, x_2, \dots, x_n]$  is any relation  $>$  on the set of monomials  $\mathbf{x}^\alpha$  in  $k[x_1, x_2, \dots, x_n]$  (or equivalently on the exponent vectors  $\alpha \in \mathbb{N}_0^n$ ) satisfying:

# Ordering of Monomials

## Definition

A **monomial order** on  $k[x_1, x_2, \dots, x_n]$  is any relation  $>$  on the set of monomials  $\mathbf{x}^\alpha$  in  $k[x_1, x_2, \dots, x_n]$  (or equivalently on the exponent vectors  $\alpha \in \mathbb{N}_0^n$ ) satisfying:

- 1  $>$  is a total ordering relation

# Ordering of Monomials

## Definition

A **monomial order** on  $k[x_1, x_2, \dots, x_n]$  is any relation  $>$  on the set of monomials  $\mathbf{x}^\alpha$  in  $k[x_1, x_2, \dots, x_n]$  (or equivalently on the exponent vectors  $\alpha \in \mathbb{N}_0^n$ ) satisfying:

- 1  $>$  is a total ordering relation
- 2 if  $\mathbf{x}^\alpha > \mathbf{x}^\beta$  and  $\mathbf{x}^\gamma$  is any monomial, then  $\mathbf{x}^\alpha \cdot \mathbf{x}^\gamma > \mathbf{x}^\beta \cdot \mathbf{x}^\gamma$

# Ordering of Monomials

## Definition

A **monomial order** on  $k[x_1, x_2, \dots, x_n]$  is any relation  $>$  on the set of monomials  $\mathbf{x}^\alpha$  in  $k[x_1, x_2, \dots, x_n]$  (or equivalently on the exponent vectors  $\alpha \in \mathbb{N}_0^n$ ) satisfying:

- 1  $>$  is a total ordering relation
- 2 if  $\mathbf{x}^\alpha > \mathbf{x}^\beta$  and  $\mathbf{x}^\gamma$  is any monomial, then  $\mathbf{x}^\alpha \cdot \mathbf{x}^\gamma > \mathbf{x}^\beta \cdot \mathbf{x}^\gamma$
- 3  $>$  is a well ordering. That is, every non-empty collection of monomials has a smallest element under  $>$ .

# Ordering of Monomials

For polynomial rings in several variables, there are many choices of monomial orders. In writing the exponent vectors  $\alpha$  and  $\beta$  in monomials  $\mathbf{x}^\alpha$  and  $\mathbf{x}^\beta$  as ordered  $n$ -tuples, we explicitly set up an ordering on the variables  $x_i$  in  $k[x_1, x_2, \dots, x_n]$ :

$$x_1 > x_2 > \dots > x_n.$$

With this choice, there still many ways to define monomial orders. Two of the most important ones are *Lexicographic Order* and *Graded Reverse Lexicographic Order*.

## Definition (Lexicographic Order)

Let  $\mathbf{x}^\alpha$  and  $\mathbf{x}^\beta$  be monomials in  $k[x_1, x_2, \dots, x_n]$ . We say  $\mathbf{x}^\alpha >_{\text{lex}} \mathbf{x}^\beta$  if in the difference  $\alpha - \beta$  the left-most nonzero entry is positive.

# lex and grevlex orders

## Definition (Lexicographic Order)

Let  $\mathbf{x}^\alpha$  and  $\mathbf{x}^\beta$  be monomials in  $k[x_1, x_2, \dots, x_n]$ . We say  $\mathbf{x}^\alpha >_{\text{lex}} \mathbf{x}^\beta$  if in the difference  $\alpha - \beta$  the left-most nonzero entry is positive.

## Definition (Graded Reverse Lexicographic Order)

Let  $\mathbf{x}^\alpha, \mathbf{x}^\beta \in k[x_1, x_2, \dots, x_n]$ . We say  $\mathbf{x}^\alpha >_{\text{grevlex}} \mathbf{x}^\beta$  if

# lex and grevlex orders

## Definition (Lexicographic Order)

Let  $\mathbf{x}^\alpha$  and  $\mathbf{x}^\beta$  be monomials in  $k[x_1, x_2, \dots, x_n]$ . We say  $\mathbf{x}^\alpha >_{\text{lex}} \mathbf{x}^\beta$  if in the difference  $\alpha - \beta$  the left-most nonzero entry is positive.

## Definition (Graded Reverse Lexicographic Order)

Let  $\mathbf{x}^\alpha, \mathbf{x}^\beta \in k[x_1, x_2, \dots, x_n]$ . We say  $\mathbf{x}^\alpha >_{\text{grevlex}} \mathbf{x}^\beta$  if

- $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i,$

# lex and grevlex orders

## Definition (Lexicographic Order)

Let  $\mathbf{x}^\alpha$  and  $\mathbf{x}^\beta$  be monomials in  $k[x_1, x_2, \dots, x_n]$ . We say  $\mathbf{x}^\alpha >_{\text{lex}} \mathbf{x}^\beta$  if in the difference  $\alpha - \beta$  the left-most nonzero entry is positive.

## Definition (Graded Reverse Lexicographic Order)

Let  $\mathbf{x}^\alpha, \mathbf{x}^\beta \in k[x_1, x_2, \dots, x_n]$ . We say  $\mathbf{x}^\alpha >_{\text{grevlex}} \mathbf{x}^\beta$  if

- $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$ , or

# lex and grevlex orders

## Definition (Lexicographic Order)

Let  $\mathbf{x}^\alpha$  and  $\mathbf{x}^\beta$  be monomials in  $k[x_1, x_2, \dots, x_n]$ . We say  $\mathbf{x}^\alpha >_{\text{lex}} \mathbf{x}^\beta$  if in the difference  $\alpha - \beta$  the left-most nonzero entry is positive.

## Definition (Graded Reverse Lexicographic Order)

Let  $\mathbf{x}^\alpha, \mathbf{x}^\beta \in k[x_1, x_2, \dots, x_n]$ . We say  $\mathbf{x}^\alpha >_{\text{grevlex}} \mathbf{x}^\beta$  if

- $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$ , or
- $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$  and in the difference  $\alpha - \beta$ , the right-most nonzero entry is negative.

# Zero-dimensional ideal

## Definition

An ideal  $I$  is said to be *zero-dimensional*, if the algebra  $A$  is finite-dimensional over  $k$ .

# Idea of the FGLM algorithm

Given a Gröbner basis  $G$  for a zero-dimensional ideal  $I$ .

# Idea of the FGLM algorithm

Given a Gröbner basis  $G$  for a zero-dimensional ideal  $I$ .

Goal: to convert it to a *lex* Gröbner basis  $G_{lex}$  for some *lex* order.

# Idea of the FGLM algorithm

Given a Gröbner basis  $G$  for a zero-dimensional ideal  $I$ .

Goal: to convert it to a *lex* Gröbner basis  $G_{lex}$  for some *lex* order.

Idea: Go through the monomials  $\mathbf{x}^\alpha$  in  $k[x_1, x_2, \dots, x_n]$  in increasing *lex* order. At each stage of the algorithm a set  $G_{lex}$  of elements in  $I$  is a subset of the eventual *lex* Gröbner basis;

# Idea of the FGLM algorithm

Given a Gröbner basis  $G$  for a zero-dimensional ideal  $I$ .

Goal: to convert it to a *lex* Gröbner basis  $G_{lex}$  for some *lex* order.

Idea: Go through the monomials  $\mathbf{x}^\alpha$  in  $k[x_1, x_2, \dots, x_n]$  in increasing *lex* order. At each stage of the algorithm a set  $G_{lex}$  of elements in  $I$  is a subset of the eventual *lex* Gröbner basis; and a list of monomials  $B_{lex}$  is a subset of the eventual *lex* basis for  $A$ .

# Idea of the FGLM algorithm

Given a Gröbner basis  $G$  for a zero-dimensional ideal  $I$ .

Goal: to convert it to a *lex* Gröbner basis  $G_{lex}$  for some *lex* order.

Idea: Go through the monomials  $\mathbf{x}^\alpha$  in  $k[x_1, x_2, \dots, x_n]$  in increasing *lex* order. At each stage of the algorithm a set  $G_{lex}$  of elements in  $I$  is a subset of the eventual *lex* Gröbner basis; and a list of monomials  $B_{lex}$  is a subset of the eventual *lex* basis for  $A$ .

Initially set  $G_{lex}$  and  $B_{lex}$  to be empty sets and take  $\mathbf{x}^\alpha = 1$ .

# Step 1

*Main Loop.*

For the input  $\mathbf{x}^\alpha$  compute  $\overline{\mathbf{x}^\alpha}^G$ .

# Step 1

*Main Loop.*

For the input  $\mathbf{x}^\alpha$  compute  $\overline{\mathbf{x}^\alpha}^G$ .

It is also important to note that for the division by  $G$  the *original* order has to be used.

# Step 1

*Main Loop.*

For the input  $\mathbf{x}^\alpha$  compute  $\overline{\mathbf{x}^\alpha}^G$ .

It is also important to note that for the division by  $G$  the *original* order has to be used.

- If  $\overline{\mathbf{x}^\alpha}^G = \sum_i c_i \overline{\mathbf{x}^{\alpha(i)}}^G$ , where  $\mathbf{x}^{\alpha(i)} \in B_{lex}$  and  $c_i \in k$ , add

$$g = \mathbf{x}^\alpha - \sum_i c_i \mathbf{x}^{\alpha(i)}$$

to  $G_{lex}$  as the last element.

# Step 1

*Main Loop.*

For the input  $\mathbf{x}^\alpha$  compute  $\overline{\mathbf{x}^\alpha}^G$ .

It is also important to note that for the division by  $G$  the *original* order has to be used.

- If  $\overline{\mathbf{x}^\alpha}^G = \sum_i c_i \overline{\mathbf{x}^{\alpha(i)}}^G$ , where  $\mathbf{x}^{\alpha(i)} \in B_{lex}$  and  $c_i \in k$ , add

$$g = \mathbf{x}^\alpha - \sum_i c_i \mathbf{x}^{\alpha(i)}$$

to  $G_{lex}$  as the last element.

or

# Step 1

*Main Loop.*

For the input  $\mathbf{x}^\alpha$  compute  $\overline{\mathbf{x}^\alpha}^G$ .

It is also important to note that for the division by  $G$  the *original* order has to be used.

- If  $\overline{\mathbf{x}^\alpha}^G = \sum_i c_i \overline{\mathbf{x}^{\alpha(i)}}^G$ , where  $\mathbf{x}^{\alpha(i)} \in B_{lex}$  and  $c_i \in k$ , add

$$g = \mathbf{x}^\alpha - \sum_i c_i \mathbf{x}^{\alpha(i)}$$

to  $G_{lex}$  as the last element.

or

- Add  $\mathbf{x}^\alpha$  to  $B_{lex}$  as the last element otherwise.

## Step 2

*Termination Test.*

If a polynomial  $g$  was added to  $G_{lex}$ , find the  $LT(g)$ .

## Step 2

*Termination Test.*

If a polynomial  $g$  was added to  $G_{lex}$ , find the  $LT(g)$ .

- If  $LT(g)$  is a power of the greatest variable in *lex* order, the algorithm terminates.

## Step 2

*Termination Test.*

If a polynomial  $g$  was added to  $G_{lex}$ , find the  $LT(g)$ .

- If  $LT(g)$  is a power of the greatest variable in *lex* order, the algorithm terminates.
- If not continue to the next step.

## Step 3

*Next Monomial.*

Replace  $\mathbf{x}^\alpha$  with the next monomial in *lex* order, which is not divisible by any of the monomials  $LT(g_i)$  for  $g_i \in G_{lex}$ .

# Example

Consider the ideal

$$I = \langle xy + z - xz, x^2 - z, 2x^3 - x^2yz - 1 \rangle$$

in  $\mathbb{Q}[x, y, z]$ . For *grevlex* order with  $x > y > z$ , given a Gröbner basis  $G = \{f_1, f_2, f_3, f_4\}$ , where

$$f_1 = z^4 - 3z^3 - 4yz + 2z^2 - y + 2z - 2$$

$$f_2 = yz^2 + 2yz - 2z^2 + 1$$

$$f_3 = y^2 - 2yz + z^2 - z$$

$$f_4 = x + y - z.$$

## Example

Consider the ideal

$$I = \langle xy + z - xz, x^2 - z, 2x^3 - x^2yz - 1 \rangle$$

in  $\mathbb{Q}[x, y, z]$ . For *grevlex* order with  $x > y > z$ , given a Gröbner basis  $G = \{f_1, f_2, f_3, f_4\}$ , where

$$f_1 = z^4 - 3z^3 - 4yz + 2z^2 - y + 2z - 2$$

$$f_2 = yz^2 + 2yz - 2z^2 + 1$$

$$f_3 = y^2 - 2yz + z^2 - z$$

$$f_4 = x + y - z.$$

*Want To Find:* a *lex* Gröbner basis for  $I$  with  $z > y > x$ .

# Example

$$f_1 = z^4 - 3z^3 - 4yz + 2z^2 - y + 2z - 2$$

$$f_2 = yz^2 + 2yz - 2z^2 + 1$$

$$f_3 = y^2 - 2yz + z^2 - z$$

$$f_4 = x + y - z.$$

## Example

$$f_1 = z^4 - 3z^3 - 4yz + 2z^2 - y + 2z - 2$$

$$f_2 = yz^2 + 2yz - 2z^2 + 1$$

$$f_3 = y^2 - 2yz + z^2 - z$$

$$f_4 = x + y - z.$$

Note that  $\langle LT(I) \rangle = \langle z^4, yz^2, y^2, x \rangle$ ,  $B = \{1, y, z, z^2, z^3, yz\}$ ; and any  $\bar{f}^G$  will be a linear combination of elements of  $B$ .

# Example

Set  $\mathbf{x}^\alpha = 1$ ,  $G_{lex} = \emptyset$  and  $B_{lex} = \emptyset$ .

# Example

Set  $\mathbf{x}^\alpha = 1$ ,  $G_{lex} = \emptyset$  and  $B_{lex} = \emptyset$ .

For the division by elements of  $G$  the *grevlex* order with  $x > y > z$  will be used.

# Example

Set  $\mathbf{x}^\alpha = 1$ ,  $G_{lex} = \emptyset$  and  $B_{lex} = \emptyset$ .

For the division by elements of  $G$  the *grevlex* order with  $x > y > z$  will be used.

*Main Loop.*  $1 = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + 1$ , so that  $\bar{1}^G = 1$  and is linearly independent from the remainders (on division by  $G$ ) of the monomials in  $B_{lex}$ . Add 1 to  $B_{lex}$ .

# Example

Set  $\mathbf{x}^\alpha = 1$ ,  $G_{lex} = \emptyset$  and  $B_{lex} = \emptyset$ .

For the division by elements of  $G$  the *grevlex* order with  $x > y > z$  will be used.

*Main Loop.*  $1 = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + 1$ , so that  $\bar{1}^G = 1$  and is linearly independent from the remainders (on division by  $G$ ) of the monomials in  $B_{lex}$ . Add 1 to  $B_{lex}$ .

*Termination Test.* N/A (no polynomial was added to  $G_{lex}$ ).

# Example

Set  $\mathbf{x}^\alpha = 1$ ,  $G_{lex} = \emptyset$  and  $B_{lex} = \emptyset$ .

For the division by elements of  $G$  the *grevlex* order with  $x > y > z$  will be used.

*Main Loop.*  $1 = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + 1$ , so that  $\bar{1}^G = 1$  and is linearly independent from the remainders (on division by  $G$ ) of the monomials in  $B_{lex}$ . Add 1 to  $B_{lex}$ .

*Termination Test.* N/A (no polynomial was added to  $G_{lex}$ ).

*Next Monomial.* Set  $\mathbf{x}^\alpha = x$ .

## Example

Set  $\mathbf{x}^\alpha = 1$ ,  $G_{lex} = \emptyset$  and  $B_{lex} = \emptyset$ .

For the division by elements of  $G$  the *grevlex* order with  $x > y > z$  will be used.

*Main Loop.*  $1 = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + 1$ , so that  $\bar{1}^G = 1$  and is linearly independent from the reminders (on division by  $G$ ) of the monomials in  $B_{lex}$ . Add 1 to  $B_{lex}$ .

*Termination Test.* N/A (no polynomial was added to  $G_{lex}$ ).

*Next Monomial.* Set  $\mathbf{x}^\alpha = x$ .

We now have:  $\mathbf{x}^\alpha = x$ ,  $G_{lex} = \emptyset$  and  $B_{lex} = \{1\}$ .

# Example

*Main Loop.*  $x = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 - y + z$ , so that  $\bar{x}^G = -y + z$ . And  $-y + z$  is linearly independent from the reminders of the monomials in  $B_{lex}$ , since  $-y + z \neq c \cdot 1$  for any  $c \in \mathbb{Q}$ . Add  $x$  to  $B_{lex}$ .

# Example

*Main Loop.*  $x = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 - y + z$ , so that  $\bar{x}^G = -y + z$ . And  $-y + z$  is linearly independent from the remainders of the monomials in  $B_{lex}$ , since  $-y + z \neq c \cdot 1$  for any  $c \in \mathbb{Q}$ . Add  $x$  to  $B_{lex}$ .

*Termination Test.* N/A (no polynomial was added to  $G_{lex}$ ).

# Example

*Main Loop.*  $x = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 - y + z$ , so that  $\bar{x}^G = -y + z$ . And  $-y + z$  is linearly independent from the remainders of the monomials in  $B_{lex}$ , since  $-y + z \neq c \cdot 1$  for any  $c \in \mathbb{Q}$ . Add  $x$  to  $B_{lex}$ .

*Termination Test.* N/A (no polynomial was added to  $G_{lex}$ ).

*Next Monomial.* Set  $\mathbf{x}^\alpha = x^2$ .

# Example

*Main Loop.*  $x = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 - y + z$ , so that  $\bar{x}^G = -y + z$ . And  $-y + z$  is linearly independent from the reminders of the monomials in  $B_{lex}$ , since  $-y + z \neq c \cdot 1$  for any  $c \in \mathbb{Q}$ . Add  $x$  to  $B_{lex}$ .

*Termination Test.* N/A (no polynomial was added to  $G_{lex}$ ).

*Next Monomial.* Set  $\mathbf{x}^\alpha = x^2$ .

We now have:  $\mathbf{x}^\alpha = x^2$ ,  $G_{lex} = \emptyset$  and  $B_{lex} = \{1, x\}$ .

# Example

Repeat the algorithm for  $\mathbf{x}^\alpha = x^2, x^3, x^4, x^5$ .

# Example

Repeat the algorithm for  $\mathbf{x}^\alpha = x^2, x^3, x^4, x^5$ .

Get:  $\mathbf{x}^\alpha = x^6$ ,  $G_{lex} = \emptyset$  and  $B_{lex} = \{1, x, x^2, x^3, x^4, x^5\}$ .

## Example

*Main Loop.*  $\overline{x^6}^G = z^3$ . And  $z^3 = \overline{x^5}^G + 2\overline{x^3}^G - \overline{1}^G$ , where

$$\overline{1}^G = 1 \quad \overline{x^3}^G = -yz + z^2$$

$$\overline{x^5}^G = z^3 + 2yz - 2z^2 + 1.$$

Hence,  $\overline{x^6}^G$  is linearly dependent on the remainders of the monomials in  $B_{lex}$ . Add  $g = x^6 - x^5 - 2x^3 + 1$  to  $G_{lex}$ .

## Example

*Main Loop.*  $\overline{x^6}^G = z^3$ . And  $z^3 = \overline{x^5}^G + 2\overline{x^3}^G - \overline{1}^G$ , where

$$\overline{1}^G = 1 \quad \overline{x^3}^G = -yz + z^2$$

$$\overline{x^5}^G = z^3 + 2yz - 2z^2 + 1.$$

Hence,  $\overline{x^6}^G$  is linearly dependent on the remainders of the monomials in  $B_{lex}$ . Add  $g = x^6 - x^5 - 2x^3 + 1$  to  $G_{lex}$ .

*Termination Test.*  $LT(g) = x^6$  is not a power of  $z$ - the greatest variable in  $lex$  order  $z > y > x$ . Continue.

## Example

*Main Loop.*  $\overline{x^6}^G = z^3$ . And  $z^3 = \overline{x^5}^G + 2\overline{x^3}^G - \overline{1}^G$ , where

$$\overline{1}^G = 1 \quad \overline{x^3}^G = -yz + z^2$$

$$\overline{x^5}^G = z^3 + 2yz - 2z^2 + 1.$$

Hence,  $\overline{x^6}^G$  is linearly dependent on the remainders of the monomials in  $B_{lex}$ . Add  $g = x^6 - x^5 - 2x^3 + 1$  to  $G_{lex}$ .

*Termination Test.*  $LT(g) = x^6$  is not a power of  $z$ - the greatest variable in  $lex$  order  $z > y > x$ . Continue.

*Next Monomial.* The next monomial in order  $z > y > x$ , not divisible by  $LT(g) = x^6$  is  $y$ . Set  $\mathbf{x}^\alpha = y$ .

## Example

*Main Loop.*  $\overline{x^6}^G = z^3$ . And  $z^3 = \overline{x^5}^G + 2\overline{x^3}^G - \overline{1}^G$ , where

$$\overline{1}^G = 1 \quad \overline{x^3}^G = -yz + z^2$$

$$\overline{x^5}^G = z^3 + 2yz - 2z^2 + 1.$$

Hence,  $\overline{x^6}^G$  is linearly dependent on the remainders of the monomials in  $B_{lex}$ . Add  $g = x^6 - x^5 - 2x^3 + 1$  to  $G_{lex}$ .

*Termination Test.*  $LT(g) = x^6$  is not a power of  $z$ - the greatest variable in *lex* order  $z > y > x$ . Continue.

*Next Monomial.* The next monomial in order  $z > y > x$ , not divisible by  $LT(g) = x^6$  is  $y$ . Set  $\mathbf{x}^\alpha = y$ .

We now have:  $\mathbf{x}^\alpha = y$ ,  $G_{lex} = \{x^6 - x^5 - 2x^3 + 1\}$  and  $B_{lex} = \{1, x, x^2, x^3, x^4, x^5\}$ .

## Example

*Main Loop.*  $y = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 + y$ , so that  $\bar{y}^G = y$ . And  $y = \bar{x}^2{}^G - \bar{x}^G$ , where  $\bar{x}^G = -y + z$  and  $\bar{x}^2{}^G = z$ .

So that,  $\bar{y}^G$  is linearly dependent on the reminders of the monomials in  $B_{lex}$ . Add  $g = y - x^2 + x$  to  $G_{lex}$  as the last element.

## Example

*Main Loop.*  $y = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 + y$ , so that  $\bar{y}^G = y$ . And  $y = \bar{x}^2{}^G - \bar{x}^G$ , where  $\bar{x}^G = -y + z$  and  $\bar{x}^2{}^G = z$ .

So that,  $\bar{y}^G$  is linearly dependent on the reminders of the monomials in  $B_{lex}$ . Add  $g = y - x^2 + x$  to  $G_{lex}$  as the last element.

*Termination Test.*  $LT(g) = y$  is not a power of  $z$ - the greatest variable in  $lex$  order  $z > y > x$ . Continue.

## Example

*Main Loop.*  $y = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 + y$ , so that  $\bar{y}^G = y$ . And  $y = \bar{x}^2{}^G - \bar{x}^G$ , where  $\bar{x}^G = -y + z$  and  $\bar{x}^2{}^G = z$ .

So that,  $\bar{y}^G$  is linearly dependent on the reminders of the monomials in  $B_{lex}$ . Add  $g = y - x^2 + x$  to  $G_{lex}$  as the last element.

*Termination Test.*  $LT(g) = y$  is not a power of  $z$ - the greatest variable in *lex* order  $z > y > x$ . Continue.

*Next Monomial.* The next monomial in order  $z > y > x$ , not divisible by  $x^6$  and  $y$  is  $z$ . Set  $\mathbf{x}^\alpha = z$ .

## Example

*Main Loop.*  $y = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 + y$ , so that  $\bar{y}^G = y$ . And  $y = \bar{x}^2{}^G - \bar{x}^G$ , where  $\bar{x}^G = -y + z$  and  $\bar{x}^2{}^G = z$ .

So that,  $\bar{y}^G$  is linearly dependent on the reminders of the monomials in  $B_{lex}$ . Add  $g = y - x^2 + x$  to  $G_{lex}$  as the last element.

*Termination Test.*  $LT(g) = y$  is not a power of  $z$ - the greatest variable in *lex* order  $z > y > x$ . Continue.

*Next Monomial.* The next monomial in order  $z > y > x$ , not divisible by  $x^6$  and  $y$  is  $z$ . Set  $\mathbf{x}^\alpha = z$ .

We now have:  $\mathbf{x}^\alpha = z$ ,  $G_{lex} = \{x^6 - x^5 - 2x^3 + 1, y - x^2 + x\}$  and  $B_{lex} = \{1, x, x^2, x^3, x^4, x^5\}$ .

# Example

*Main Loop.*  $z = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 + z$ , so that  $\bar{z}^G = z$ .  
And  $z = \overline{x^2}^G$ .

Add  $g = z - x^2$  to  $G_{lex}$  as the last element.

# Example

*Main Loop.*  $z = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 + z$ , so that  $\bar{z}^G = z$ .  
And  $z = \overline{x^2}^G$ .

Add  $g = z - x^2$  to  $G_{lex}$  as the last element.

*Termination Test.*  $LT(g) = z$  is a power of  $z$ - the greatest variable in *lex* order  $z > y > x$ . And the algorithm terminates.

## Example

*Main Loop.*  $z = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 + z$ , so that  $\bar{z}^G = z$ .  
And  $z = \overline{x^2}^G$ .

Add  $g = z - x^2$  to  $G_{lex}$  as the last element.

*Termination Test.*  $LT(g) = z$  is a power of  $z$ - the greatest variable in *lex* order  $z > y > x$ . And the algorithm terminates.

$G_{lex} = \{x^6 - x^5 - 2x^3 + 1, y - x^2 + x, z - x^2\}$  is a *lex* basis for  $I$   
and  $B_{lex} = \{1, x, x^2, x^3, x^4, x^5\}$  is the a *lex* monomial basis for  $A$ .

# Main Theorem

## Theorem

- *The FGLM algorithm terminates for every input Gröbner basis  $G$ , that generates a zero-dimensional ideal  $I$ .*
- *The algorithm correctly computes a lex Gröbner basis  $G_{\text{lex}}$  for  $I$  and the lex monomial basis  $B_{\text{lex}}$  for the quotient ring  $A$ .*

# Dickson's Lemma

For the proof of the Main Theorem let's recall the following lemma.

## Lemma (Dickson's Lemma)

*For any infinite list  $\mathbf{x}^{\alpha(1)}, \mathbf{x}^{\alpha(2)}, \dots$  of monomials in  $k[x_1, x_2, \dots, x_n]$ , there exists an integer  $m$  such that every  $\mathbf{x}^{\alpha(i)}$  is divisible by one of  $\mathbf{x}^{\alpha(1)}, \mathbf{x}^{\alpha(2)}, \dots, \mathbf{x}^{\alpha(m)}$ .*

# The End

Thank you!