

# Gröbner Basis Conversion

- 1 Normal Sets and the Quotient Algebra  
term orders and multiplication maps
- 2 The cyclic  $n$ -roots problem  
one of the most popular benchmarks
- 3 the FGLM Algorithm  
Gröbner Conversion in Maple  
pseudo code for the FGLM Algorithm
- 4 The Complexity of Gröbner Bases  
applying the Shape Lemma  
cost analysis of the FGLM Algorithm

MCS 563 Lecture 10  
Analytic Symbolic Computation  
Jan Verschelde, 4 February 2011

# Gröbner Basis Conversion

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

- 1 Normal Sets and the Quotient Algebra  
term orders and multiplication maps
- 2 The cyclic  $n$ -roots problem  
one of the most popular benchmarks
- 3 the FGLM Algorithm  
Gröbner Conversion in Maple  
pseudo code for the FGLM Algorithm
- 4 The Complexity of Gröbner Bases  
applying the Shape Lemma  
cost analysis of the FGLM Algorithm

# Term Orders

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

A system of polynomials  $f(\mathbf{x}) = \mathbf{0}$ ,  $f = (f_1, f_2, \dots, f_N)$  defines the ideal  $I = \langle f \rangle$ . We assume  $\#V(I)$  is finite.

A lexicographic order  $>_{\text{lex}}$  eliminates and the Gröbner basis  $g_{>_{\text{lex}}}$  for  $I$  has a triangular shape.

Unfortunately,  $g_{>_{\text{lex}}}$  is expensive to compute and may lead to excessive growth of the coefficients.

The degree reverse lexicographic order  $>_{\text{grevlex}}$  is better.

Ordering the variables in  $\mathbf{x}$  by  $x_1 > x_2 > \dots > x_n$ , for two monomials  $\mathbf{x}^{\mathbf{a}}$  and  $\mathbf{x}^{\mathbf{b}}$ , we define  $\mathbf{x}^{\mathbf{a}} >_{\text{grevlex}} \mathbf{x}^{\mathbf{b}}$

- if  $\deg(\mathbf{x}^{\mathbf{a}}) > \deg(\mathbf{x}^{\mathbf{b}})$  or else
- if  $\deg(\mathbf{x}^{\mathbf{a}}) = \deg(\mathbf{x}^{\mathbf{b}})$  and then the rightmost nonzero entry in  $\mathbf{a} - \mathbf{b}$  is negative.

For example:  $x_1 x_2^4 x_3 >_{\text{grevlex}} x_1^2 x_2^2 x_3^2$ .

# normal forms and normal sets

With a Gröbner basis  $g_{>}$ , we have a unique normal form of any polynomial  $h$ , denoted as  $h \rightarrow_{g_{>}} r$ , with  $r$  the remainder modulo the ideal  $I$ , computed by the division algorithm.

The normal set  $\mathcal{N}_{>}$  for  $g_{>}$  is defined as

$$\mathcal{N}_{>} = \{ \mathbf{x}^{\mathbf{a}} \mid \mathbf{x}^{\mathbf{a}} \notin \text{LT}(g_{>}) \}$$

and then we can write

$$h \rightarrow_{g_{>}} r = \sum_{\mathbf{x}^{\mathbf{a}} \in \mathcal{N}_{>}} c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}, \quad c_{\mathbf{a}} \in \mathbb{C}.$$

While  $\mathcal{N}_{>}$  depends on  $>$  its cardinality is fixed

$$\#\mathcal{N}_{>} = \#V(I) = \dim(\mathbb{C}[\mathbf{x}]/I).$$

# normal forms and normal sets

With a Gröbner basis  $g_{>}$ , we have a unique normal form of any polynomial  $h$ , denoted as  $h \rightarrow_{g_{>}} r$ , with  $r$  the remainder modulo the ideal  $I$ , computed by the division algorithm.

The normal set  $\mathcal{N}_{>}$  for  $g_{>}$  is defined as

$$\mathcal{N}_{>} = \{ \mathbf{x}^{\mathbf{a}} \mid \mathbf{x}^{\mathbf{a}} \notin \text{LT}(g_{>}) \}$$

and then we can write

$$h \rightarrow_{g_{>}} r = \sum_{\mathbf{x}^{\mathbf{a}} \in \mathcal{N}_{>}} c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}, \quad c_{\mathbf{a}} \in \mathbb{C}.$$

While  $\mathcal{N}_{>}$  depends on  $>$  its cardinality is fixed

$$\#\mathcal{N}_{>} = \#V(I) = \dim(\mathbb{C}[\mathbf{x}]/I).$$

# normal forms and normal sets

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

With a Gröbner basis  $g_{>}$ , we have a unique normal form of any polynomial  $h$ , denoted as  $h \rightarrow_{g_{>}} r$ , with  $r$  the remainder modulo the ideal  $I$ , computed by the division algorithm.

The normal set  $\mathcal{N}_{>}$  for  $g_{>}$  is defined as

$$\mathcal{N}_{>} = \{ \mathbf{x}^{\mathbf{a}} \mid \mathbf{x}^{\mathbf{a}} \notin \text{LT}(g_{>}) \}$$

and then we can write

$$h \rightarrow_{g_{>}} r = \sum_{\mathbf{x}^{\mathbf{a}} \in \mathcal{N}_{>}} c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}, \quad c_{\mathbf{a}} \in \mathbb{C}.$$

While  $\mathcal{N}_{>}$  depends on  $>$  its cardinality is fixed

$$\#\mathcal{N}_{>} = \#V(I) = \dim(\mathbb{C}[\mathbf{x}]/I).$$

## the quotient algebra

## The multiplication

$$* : \mathcal{N}_{>} \times \mathcal{N}_{>} \rightarrow \mathbb{C}[\mathbf{x}]/I$$

$$(\mathbf{x}^{\mathbf{a}}, \mathbf{x}^{\mathbf{b}}) \mapsto \mathbf{x}^{\mathbf{a}+\mathbf{b}} \rightarrow_{g_{>}} r$$

turns the quotient ring  $\mathbb{C}[\mathbf{x}]/I$  into the quotient algebra.

We order the monomials in  $\mathcal{N}_{>}$  into the vector  $\mathbf{n}_{>}$  and applying  $*$  to all pairs of  $\mathbf{n}_{>}$  leads to a multiplication table. For any coordinate  $x_i$ , we define the multiplication map

$$m_{x_i} : \mathbb{C}[\mathbf{x}]/I \rightarrow \mathbb{C}[\mathbf{x}]/I$$

$$h \mapsto (x_i \cdot h) \rightarrow_{g_{>}} r.$$

The map  $m_{x_i}$  is linear and leads to the eigenvalue problem

$$x_i \mathbf{n}_{>} = m_{x_i} \mathbf{n}_{>}.$$

## the quotient algebra

## The multiplication

$$* : \mathcal{N}_{>} \times \mathcal{N}_{>} \rightarrow \mathbb{C}[\mathbf{x}]/I$$

$$(\mathbf{x}^{\mathbf{a}}, \mathbf{x}^{\mathbf{b}}) \mapsto \mathbf{x}^{\mathbf{a}+\mathbf{b}} \rightarrow_{g_{>}} r$$

turns the quotient ring  $\mathbb{C}[\mathbf{x}]/I$  into the quotient algebra.

We order the monomials in  $\mathcal{N}_{>}$  into the vector  $\mathbf{n}_{>}$  and applying  $*$  to all pairs of  $\mathbf{n}_{>}$  leads to a multiplication table. For any coordinate  $x_i$ , we define the multiplication map

$$m_{x_i} : \mathbb{C}[\mathbf{x}]/I \rightarrow \mathbb{C}[\mathbf{x}]/I$$

$$h \mapsto (x_i \cdot h) \rightarrow_{g_{>}} r.$$

The map  $m_{x_i}$  is linear and leads to the eigenvalue problem

$$x_i \mathbf{n}_{>} = m_{x_i} \mathbf{n}_{>}$$

## the quotient algebra

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

The multiplication

$$\begin{aligned} * : \mathcal{N}_{>} \times \mathcal{N}_{>} &\rightarrow \mathbb{C}[\mathbf{x}]/I \\ (\mathbf{x}^{\mathbf{a}}, \mathbf{x}^{\mathbf{b}}) &\mapsto \mathbf{x}^{\mathbf{a}+\mathbf{b}} \rightarrow_{g_{>}} r \end{aligned}$$

turns the quotient ring  $\mathbb{C}[\mathbf{x}]/I$  into the quotient algebra.

We order the monomials in  $\mathcal{N}_{>}$  into the vector  $\mathbf{n}_{>}$  and applying  $*$  to all pairs of  $\mathbf{n}_{>}$  leads to a multiplication table. For any coordinate  $x_i$ , we define the multiplication map

$$\begin{aligned} m_{x_i} : \mathbb{C}[\mathbf{x}]/I &\rightarrow \mathbb{C}[\mathbf{x}]/I \\ h &\mapsto (x_i \cdot h) \rightarrow_{g_{>}} r. \end{aligned}$$

The map  $m_{x_i}$  is linear and leads to the eigenvalue problem

$$\mathbf{x}_i \mathbf{n}_{>} = m_{x_i} \mathbf{n}_{>}$$

# Gröbner Basis Conversion

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

- 1 Normal Sets and the Quotient Algebra  
term orders and multiplication maps
- 2 The cyclic  $n$ -roots problem  
one of the most popular benchmarks
- 3 the FGLM Algorithm  
Gröbner Conversion in Maple  
pseudo code for the FGLM Algorithm
- 4 The Complexity of Gröbner Bases  
applying the Shape Lemma  
cost analysis of the FGLM Algorithm

cyclic  $n$ -roots

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

The cyclic 5-roots problem takes the following form:

$$f(\mathbf{x}) = \left\{ \begin{array}{rcl} x_1 + x_2 + x_3 + x_4 + x_5 & = & 0 \\ x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_5 + x_5 x_1 & = & 0 \\ x_1 x_2 x_3 + x_2 x_3 x_4 + x_3 x_4 x_5 + x_4 x_5 x_1 & & \\ & + x_5 x_1 x_2 & = & 0 \\ x_1 x_2 x_3 x_4 + x_2 x_3 x_4 x_5 + x_3 x_4 x_5 x_1 + x_4 x_5 x_1 x_2 & & \\ & + x_5 x_1 x_2 x_3 & = & 0 \\ x_1 x_2 x_3 x_4 x_5 - 1 & = & 0. \end{array} \right.$$

Observe the symmetry in the system.

## number of roots

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

The number of solutions  $\#V$  for increasing dimension  $n$ :

$n$	3	4	5	6	7	8	9
$\#V$	6	$\infty$	70	156	924	$\infty$	$\infty$
$n$	10	11	12				
$\#V$	34,940	184,756	$\infty$				

The  $\infty$  in the table marks cases for which there are positive dimensional solution sets.

# Gröbner Basis Conversion

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

- 1 Normal Sets and the Quotient Algebra  
term orders and multiplication maps
- 2 The cyclic  $n$ -roots problem  
one of the most popular benchmarks
- 3 the FGLM Algorithm  
Gröbner Conversion in Maple  
pseudo code for the FGLM Algorithm
- 4 The Complexity of Gröbner Bases  
applying the Shape Lemma  
cost analysis of the FGLM Algorithm

## a session with Maple

On the cyclic 3-roots problem:

```
[> f3 := [ x[1] + x[2] + x[3],
           x[1]*x[2] + x[2]*x[3] + x[3]*x[1],
           x[1]*x[2]*x[3] - 1];

[> v := op(indets(f3));
           v := x[1], x[2], x[3]

[> g1 := Groebner[Basis](f3,tdeg(v));
           g1 := [x[1]+x[2]+x[3],
                 x[2]^2+x[2]*x[3]+x[3]^2, -1+x[3]^3]

[> ns := Groebner[NormalSet](g1,tdeg(v))[1];
           ns := [1, x[3], x[2], x[3]^2, x[2]*x[3],
                 x[2]*x[3]^2]

[> g2 := Groebner[FGLM](g1,tdeg(v),
                        plex(x[3],x[2],x[1]));
           g2 := [-1+x[1]^3, x[1]*x[2]+x[1]^2+x[2]^2,
                 x[1]+x[2]+x[3]]
```

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

## multiplication maps

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

The multiplication map  $M_{x_1}$  with the total degree order is

$$M_{x_1} = \begin{bmatrix} 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

with  $\mathbf{n}_{>\text{tdeg}} = [1, x_3, x_2, x_3^2, x_2 x_3, x_2 x_3^2]$ .

Changing order of variables  $x_3 > x_2 > x_1$ , then

$$L_{x_3} = \begin{bmatrix} 0 & -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

is the multiplication map with the pure lexicographic order  $x_3 > x_2 > x_1$  and  $\mathbf{n}_{>\text{lex}} = [1, x_1, x_1^2, x_2, x_1 x_2, x_1^2 x_2]$ .

We can view the Gröbner basis conversion as the rewriting of  $x_1 \mathbf{n}_{>\text{tdeg}} = M_{x_1} \mathbf{n}_{>\text{tdeg}}$  into  $x_3 \mathbf{n}_{>\text{lex}} = L_{x_3} \mathbf{n}_{>\text{lex}}$ .

# Gröbner Basis Conversion

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

- 1 Normal Sets and the Quotient Algebra  
term orders and multiplication maps
- 2 The cyclic  $n$ -roots problem  
one of the most popular benchmarks
- 3 the FGLM Algorithm  
Gröbner Conversion in Maple  
pseudo code for the FGLM Algorithm
- 4 The Complexity of Gröbner Bases  
applying the Shape Lemma  
cost analysis of the FGLM Algorithm

## bordering and Shape Lemma

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

Following the FGLM '93 paper:

a bordering of a Gröbner basis is the set of all monomials  $x_i b$  with  $b \in \mathcal{N}_{>}$  and  $x_i b \notin \mathcal{N}_{>}$ , for all  $i$ .

In general, a Gröbner basis for  $>_{\text{lex}}$  follows the representation as in the Shape Lemma.

The FGLM algorithm first considers all powers of  $x_1$  and tries to write these powers as a linear combination of the previous powers of  $x_1$ , modulo the ideal.

The first power of  $x_1$  written as a linear combination of previous powers belongs to the bordering of the Gröbner basis  $\Rightarrow$  this linear combination is an element of  $\mathfrak{g}_{>_{\text{lex}}}$ .

## bordering and Shape Lemma

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

Following the FGLM '93 paper:

a bordering of a Gröbner basis is the set of all monomials  $x_i b$  with  $b \in \mathcal{N}_{>}$  and  $x_i b \notin \mathcal{N}_{>}$ , for all  $i$ .

In general, a Gröbner basis for  $>_{\text{lex}}$  follows the representation as in the Shape Lemma.

The FGLM algorithm first considers all powers of  $x_1$  and tries to write these powers as a linear combination of the previous powers of  $x_1$ , modulo the ideal.

The first power of  $x_1$  written as a linear combination of previous powers belongs to the bordering of the Gröbner basis  $\Rightarrow$  this linear combination is an element of  $\mathfrak{g}_{>_{\text{lex}}}$ .

## bordering and Shape Lemma

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

Following the FGLM '93 paper:

a bordering of a Gröbner basis is the set of all monomials  $x_i b$  with  $b \in \mathcal{N}_{>}$  and  $x_i b \notin \mathcal{N}_{>}$ , for all  $i$ .

In general, a Gröbner basis for  $>_{\text{lex}}$  follows the representation as in the Shape Lemma.

The FGLM algorithm first considers all powers of  $x_1$  and tries to write these powers as a linear combination of the previous powers of  $x_1$ , modulo the ideal.

The first power of  $x_1$  written as a linear combination of previous powers belongs to the bordering of the Gröbner basis  $\Rightarrow$  this linear combination is an element of  $\mathfrak{g}_{>_{\text{lex}}}$ .

## the FGLM Algorithm

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

Input:  $g_{>}$  a Gröbner basis for any monomial order  $>$ .

Output:  $g_{>\text{lex}}$  a Gröbner basis for lexicographic order  $>\text{lex}$ .

$\mathcal{N}_{>} := \text{Normal\_Set}(g_{>});$

$g_{>\text{lex}} := \emptyset;$

$\mathcal{N}_{>\text{lex}} := \emptyset;$

for  $i$  from 0 do  $\#\mathcal{N}_{>}$  do

    reduce  $x_1^i \rightarrow_{g_{>}} r;$

    if  $r$  is not a linear combination of the monomials in  $\mathcal{N}_{>\text{lex}}$

        then  $\mathcal{N}_{>\text{lex}} := \mathcal{N}_{>\text{lex}} \cup \{x_1^i\};$

        else  $g_{>\text{lex}} := g_{>\text{lex}} \cup \{x_1^i - r\};$

    end if;

end for;

for  $i$  from 2 to  $n$  do

    reduce  $x_i \rightarrow_{g_{>}} r;$

$g_{>\text{lex}} := g_{>\text{lex}} \cup \{r\};$

end for.

## the FGLM Algorithm

Normal Sets  
and the  
Quotient  
Algebraterm orders and  
multiplication mapsThe cyclic  
 $n$ -roots  
problemone of the most  
popular benchmarksthe FGLM  
AlgorithmGröbner Conversion  
in Maplepseudo code for the  
FGLM AlgorithmThe  
Complexity of  
Gröbner  
Basesapplying the Shape  
Lemmacost analysis of the  
FGLM AlgorithmInput:  $g_{>}$  a Gröbner basis for any monomial order  $>$ .Output:  $g_{>\text{lex}}$  a Gröbner basis for lexicographic order  $>\text{lex}$ . $\mathcal{N}_{>} := \text{Normal\_Set}(g_{>});$  $g_{>\text{lex}} := \emptyset;$  $\mathcal{N}_{>\text{lex}} := \emptyset;$ for  $i$  from 0 do  $\#\mathcal{N}_{>}$  do    reduce  $x_1^i \rightarrow_{g_{>}} r;$     if  $r$  is not a linear combination of the monomials in  $\mathcal{N}_{>\text{lex}}$         then  $\mathcal{N}_{>\text{lex}} := \mathcal{N}_{>\text{lex}} \cup \{x_1^i\};$         else  $g_{>\text{lex}} := g_{>\text{lex}} \cup \{x_1^i - r\};$ 

end if;

end for;

for  $i$  from 2 to  $n$  do    reduce  $x_i \rightarrow_{g_{>}} r;$      $g_{>\text{lex}} := g_{>\text{lex}} \cup \{r\};$ 

end for.

## the FGLM Algorithm

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

Input:  $g_{>}$  a Gröbner basis for any monomial order  $>$ .

Output:  $g_{>\text{lex}}$  a Gröbner basis for lexicographic order  $>\text{lex}$ .

$\mathcal{N}_{>} := \text{Normal\_Set}(g_{>});$

$g_{>\text{lex}} := \emptyset;$

$\mathcal{N}_{>\text{lex}} := \emptyset;$

for  $i$  from 0 do  $\#\mathcal{N}_{>}$  do

    reduce  $x_1^i \rightarrow_{g_{>}} r;$

    if  $r$  is not a linear combination of the monomials in  $\mathcal{N}_{>\text{lex}}$

        then  $\mathcal{N}_{>\text{lex}} := \mathcal{N}_{>\text{lex}} \cup \{x_1^i\};$

        else  $g_{>\text{lex}} := g_{>\text{lex}} \cup \{x_1^i - r\};$

    end if;

end for;

for  $i$  from 2 to  $n$  do

    reduce  $x_i \rightarrow_{g_{>}} r;$

$g_{>\text{lex}} := g_{>\text{lex}} \cup \{r\};$

end for.

# termination and correctness

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

That the FGLM Algorithm is an algorithm follows:

- Termination:  $\#V(I) < \infty$ .  
The number of elements of any normal set for a zero dimensional ideal equals the number of solutions. Because there are finitely many solutions, the loop that rewrites the powers of  $x_1$  must terminate.
- Correctness:  $g_{>}$  is a Gröbner basis for  $I$ .  
Given a Gröbner basis  $g_{>}$ , every polynomial  $h$  has a unique normal form modulo the ideal. The FGLM Algorithm takes for  $h$  powers of  $x_1$  and the remaining variables  $x_i$ ,  $i > 1$ .

# termination and correctness

## Normal Sets and the Quotient Algebra

term orders and  
multiplication maps

## The cyclic $n$ -roots problem

one of the most  
popular benchmarks

## the FGLM Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

## The Complexity of Gröbner Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

That the FGLM Algorithm is an algorithm follows:

- Termination:  $\#V(I) < \infty$ .  
The number of elements of any normal set for a zero dimensional ideal equals the number of solutions. Because there are finitely many solutions, the loop that rewrites the powers of  $x_1$  must terminate.
- Correctness:  $g_{>}$  is a Gröbner basis for  $I$ .  
Given a Gröbner basis  $g_{>}$ , every polynomial  $h$  has a unique normal form modulo the ideal. The FGLM Algorithm takes for  $h$  powers of  $x_1$  and the remaining variables  $x_i$ ,  $i > 1$ .

# Gröbner Basis Conversion

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

- 1 Normal Sets and the Quotient Algebra  
term orders and multiplication maps
- 2 The cyclic  $n$ -roots problem  
one of the most popular benchmarks
- 3 the FGLM Algorithm  
Gröbner Conversion in Maple  
pseudo code for the FGLM Algorithm
- 4 The Complexity of Gröbner Bases  
applying the Shape Lemma  
cost analysis of the FGLM Algorithm

# applying the Shape Lemma

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

The following follows mainly from the theorem of Bézout.

## Theorem 1

*Let  $I = \langle f_1, f_2, \dots, f_N \rangle$ . In most cases, every Gröbner basis for the lexicographical ordering contains a polynomial of degree  $\deg(f_1) \times \deg(f_2) \times \dots \times \deg(f_N)$ .*

For the Shape Lemma we have as many Lagrange polynomials as the number of solutions, therefore the size will be  $O(d^{n^2})$ , where  $d$  is the maximal degree of the polynomials in  $f$ .

Because of the *in most cases* of the Theorem, the formulation of the lexicographic Gröbner basis is just as bad as the particular case of the Shape Lemma.

# applying the Shape Lemma

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

The following follows mainly from the theorem of Bézout.

## Theorem 1

*Let  $I = \langle f_1, f_2, \dots, f_N \rangle$ . In most cases, every Gröbner basis for the lexicographical ordering contains a polynomial of degree  $\deg(f_1) \times \deg(f_2) \times \dots \times \deg(f_N)$ .*

For the Shape Lemma we have as many Lagrange polynomials as the number of solutions, therefore the size will be  $O(d^{n^2})$ , where  $d$  is the maximal degree of the polynomials in  $f$ .

Because of the *in most cases* of the Theorem, the formulation of the lexicographic Gröbner basis is just as bad as the particular case of the Shape Lemma.

# applying the Shape Lemma

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

The following follows mainly from the theorem of Bézout.

## Theorem 1

*Let  $I = \langle f_1, f_2, \dots, f_N \rangle$ . In most cases, every Gröbner basis for the lexicographical ordering contains a polynomial of degree  $\deg(f_1) \times \deg(f_2) \times \dots \times \deg(f_N)$ .*

For the Shape Lemma we have as many Lagrange polynomials as the number of solutions, therefore the size will be  $O(d^{n^2})$ , where  $d$  is the maximal degree of the polynomials in  $f$ .

Because of the *in most cases* of the Theorem, the formulation of the lexicographic Gröbner basis is just as bad as the particular case of the Shape Lemma.

Assuming conditions on the solutions at infinity, simplified into a more specific version:

## Theorem 2

*Let  $I = \langle f_1, f_2, \dots, f_n \rangle$  where  $n$  is also the number of variables. Assume that both  $V(I)$  and the solutions at infinity are finite in number. Then the polynomials of every minimal reduced Gröbner basis with respect to the degree reverse lexicographic order have degree bounded by  $\deg(f_1) + \deg(f_2) + \dots + \deg(f_n) - n + 2$ .*

The theorem applies to homogeneous ideals and assumes that the linear equation for the hyperplane at infinity is sufficiently generic.

The bound on the degrees changed from a product into a sum. This leads to a complexity of  $O(d^n)$ .

Assuming conditions on the solutions at infinity, simplified into a more specific version:

## Theorem 2

*Let  $I = \langle f_1, f_2, \dots, f_n \rangle$  where  $n$  is also the number of variables. Assume that both  $V(I)$  and the solutions at infinity are finite in number. Then the polynomials of every minimal reduced Gröbner basis with respect to the degree reverse lexicographic order have degree bounded by  $\deg(f_1) + \deg(f_2) + \dots + \deg(f_n) - n + 2$ .*

The theorem applies to homogeneous ideals and assumes that the linear equation for the hyperplane at infinity is sufficiently generic.

The bound on the degrees changed from a product into a sum. This leads to a complexity of  $O(d^n)$ .

# Gröbner Basis Conversion

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

- 1 Normal Sets and the Quotient Algebra  
term orders and multiplication maps
- 2 The cyclic  $n$ -roots problem  
one of the most popular benchmarks
- 3 the FGLM Algorithm  
Gröbner Conversion in Maple  
pseudo code for the FGLM Algorithm
- 4 The Complexity of Gröbner Bases  
applying the Shape Lemma  
cost analysis of the FGLM Algorithm

## Theorem 3

*Denote by  $n$  the number of variables and  $D$  equals the number of common zeroes (counted with multiplicities). If the basis field operations need unit time, finding a new basis requires  $O(nD^3)$  field operations.*

The growth of the coefficients is not taken into account.

The third power of  $D$  is expected as we perform Gaussian elimination in the quotient ring.

For  $D$  equal to the product of the degrees (the expected number of solutions according to the theorem of Bézout), we again arrive at the bad complexity of Theorem 1. In most applications, #solutions  $\ll d^n$ .

## Theorem 3

*Denote by  $n$  the number of variables and  $D$  equals the number of common zeroes (counted with multiplicities). If the basis field operations need unit time, finding a new basis requires  $O(nD^3)$  field operations.*

The growth of the coefficients is not taken into account.

The third power of  $D$  is expected as we perform Gaussian elimination in the quotient ring.

For  $D$  equal to the product of the degrees (the expected number of solutions according to the theorem of Bézout), we again arrive at the bad complexity of Theorem 1.

In most applications, #solutions  $\ll d^n$ .

# Summary + Exercises

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

Because lexicographic Gröbner bases have a high complexity, we introduced the FGLM Algorithm to convert a Gröbner basis for any term order into a lexicographic order.

## Exercises:

- 1 Consider as given a set of monomials representing  $LT(g_{>})$ , for  $g_{>}$  a Gröbner basis with term order  $>$ . Write an algorithm to compute the normal set  $\mathcal{N}_{>}$ . Have the algorithm report an error message when it turns that the ideal  $\langle g \rangle$  is not zero dimensional.

## Normal Sets and the Quotient Algebra

term orders and  
multiplication maps

## The cyclic $n$ -roots problem

one of the most  
popular benchmarks

## the FGLM Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

## The Complexity of Gröbner Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

- 2 Describe the permutation symmetry of the system cyclic 5-roots. How many elements does the symmetry group have? What are the generators of the symmetry group? How many generators of the solution set do you expect?
- 3 Consider the cyclic  $n$ -roots problem for general  $n$  and compute the product  $D$  of the degrees. Compare  $D$  to the finite numbers  $\#V$  in the table.

## and more exercises

Normal Sets  
and the  
Quotient  
Algebraterm orders and  
multiplication mapsThe cyclic  
 $n$ -roots  
problemone of the most  
popular benchmarksthe FGLM  
AlgorithmGröbner Conversion  
in Maplepseudo code for the  
FGLM AlgorithmThe  
Complexity of  
Gröbner  
Basesapplying the Shape  
Lemmacost analysis of the  
FGLM Algorithm

- 4 Consider the following modification (suggested by the FGLM authors) of the cyclic 5-roots problem:

$$\left\{ \begin{array}{l} x_1 + x_2 + x_3 + x_4 + x_5 = 0 \\ x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_5 + x_5 x_1 = 0 \\ x_1 x_2 x_3 + x_2 x_3 x_4 + x_3 x_4 x_5 + x_4 x_5 x_1 + x_5 x_1 x_2 = 0 \\ x_2 x_3 x_4 + x_2 x_3 x_4 x_5 + x_3 x_4 x_5 x_1 + x_4 x_5 x_1 x_2 + x_5 x_1 x_2 x_3 = 0 \\ x_1 x_2 x_3 x_4 x_5 - 1 = 0. \end{array} \right.$$

where the monomial  $x_1 x_2 x_3 x_4$  in the original cyclic 5-roots system is replaced by  $x_2 x_3 x_4$ . Compute a Gröbner basis with the graded lexicographical order to determine the number of roots of this modified cyclic 5-roots system. Use the FGLM method to convert the Gröbner basis to a pure lexicographical term order. Compare the size of the coefficients between the bases for the different term orders.

## and more exercises

Normal Sets  
and the  
Quotient  
Algebraterm orders and  
multiplication mapsThe cyclic  
 $n$ -roots  
problemone of the most  
popular benchmarksthe FGLM  
AlgorithmGröbner Conversion  
in Maplepseudo code for the  
FGLM AlgorithmThe  
Complexity of  
Gröbner  
Basesapplying the Shape  
Lemmacost analysis of the  
FGLM Algorithm

- 5 A Gröbner basis with respect to  $>_{\text{grevlex}}$  is given in *Using Algebraic Geometry* by  $g = \langle g_1, g_2, g_3, g_4 \rangle$ , with

$$g_1 = x_3^4 - 3x_3^3 - 4x_2x_3 + 2x_3^2 - x_2 + 2x_3 - 2,$$

$$g_2 = x_2x_3^2 + 2x_2x_3 - 2x_3^2 + 1,$$

$$g_3 = x_2^2 - 2x_2x_3 + x_3^2 - x_3,$$

$$g_4 = x_1 + x_2 + x_3.$$

which can be computed in Maple via  $g := \text{Groebner}[\text{Basis}](f, \text{grlex}(x, y, z))$ ; where  $f$  defines the ideal

$$I = \langle x_1x_2 + x_3 - x_1x_3, x_1^2 - x_3, 2x_1^3 - x_1^2x_2x_3 - 1 \rangle.$$

- 1 What is  $\mathcal{N}_{>_{\text{grevlex}}}$ ?
- 2 Use the FGLM Algorithm to compute  $g_{>_{\text{lex}}}$ .

## and two more exercises

Normal Sets  
and the  
Quotient  
Algebra

term orders and  
multiplication maps

The cyclic  
 $n$ -roots  
problem

one of the most  
popular benchmarks

the FGLM  
Algorithm

Gröbner Conversion  
in Maple

pseudo code for the  
FGLM Algorithm

The  
Complexity of  
Gröbner  
Bases

applying the Shape  
Lemma

cost analysis of the  
FGLM Algorithm

- 6 Use `Groebner [ FGLM ]` in Maple on the previous exercise. Alternatively, use the `fglm` command of Singular, as available in Sage. In both cases – whether you use Maple or Sage – verify whether the output of the software corresponds to the manual computations of the last exercise.
- 7 Translate the pseudo code of our description of the FGLM algorithm into the language of a computer algebra system, Macaulay 2, Singular, or Maple.