

Rewriting Polynomials

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

- 1 **Roots and Eigenvalues**
the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

- 2 **Automatic Geometric Theorem Proving**
the circle theorem of Apollonius

The Division Algorithm

monomial orderings

- 3 **The Division Algorithm**
monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

- 4 **Monomial Ideals**
staircase representation
Dickson's Lemma

MCS 563 Lecture 4
Analytic Symbolic Computation
Jan Verschelde, 19 January 2011

Rewriting Polynomials

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

- 1 **Roots and Eigenvalues**
the companion matrix of a polynomial
the ideal membership problem
- 2 Automatic Geometric Theorem Proving
the circle theorem of Apollonius
- 3 The Division Algorithm
monomial orderings
- 4 Monomial Ideals
staircase representation
Dickson's Lemma

roots and eigenvalues

Roots and
Eigenvalues

the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving

the circle theorem of
Apollonius

The Division
Algorithm

monomial orderings

Monomial
Ideals

staircase
representation

Dickson's Lemma

For example, consider

$$\begin{aligned} p(x) &= x^4 - 5x^3 + 7x^2 - x + 3 \in \mathbb{C}[x] \\ &= (x - z_1)(x - z_2)(x - z_3)(x - z_4), \end{aligned}$$

we can identify p with its roots z_1, z_2, z_3, z_4 .

Algebraically, $p(x) = 0$ implies

$$x^4 = 5x^3 - 7x^2 + x - 3.$$

As x^4 is a linear combination of $1, x, x^2, x^3$,
we can also write x^5, x^6 , etc. as cubic polynomials.

roots and eigenvalues

Roots and Eigenvalues

the companion
matrix of a
polynomial
the ideal
membership problem

Automatic Geometric Theorem Proving

the circle theorem of
Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase
representation

Dickson's Lemma

For example, consider

$$\begin{aligned} p(x) &= x^4 - 5x^3 + 7x^2 - x + 3 \in \mathbb{C}[x] \\ &= (x - z_1)(x - z_2)(x - z_3)(x - z_4), \end{aligned}$$

we can identify p with its roots z_1, z_2, z_3, z_4 .

Algebraically, $p(x) = 0$ implies

$$x^4 = 5x^3 - 7x^2 + x - 3.$$

As x^4 is a linear combination of $1, x, x^2, x^3$, we can also write x^5, x^6 , etc. as cubic polynomials.

the quotient ring

Roots and
Eigenvalues

the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving

the circle theorem of
Apollonius

The Division
Algorithm

monomial orderings

Monomial
Ideals

staircase
representation
Dickson's Lemma

The relation

$$x^4 = 5x^3 - 7x^2 + x - 3$$

maps every polynomial in $\mathbb{C}[x]$ onto **the quotient ring**

$$\mathbb{C}[x]/\langle p \rangle = \{ a_0 + a_1x + a_2x^2 + a_3x^3 \mid a_i \in \mathbb{C} \},$$

is a 4-dimensional vector space with basis $\{1, x, x^2, x^3\}$.

By this vector space a problem of polynomial algebra becomes a problem of linear algebra.

the quotient ring

Roots and
Eigenvalues

the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving

the circle theorem of
Apollonius

The Division
Algorithm

monomial orderings

Monomial
Ideals

staircase
representation
Dickson's Lemma

The relation

$$x^4 = 5x^3 - 7x^2 + x - 3$$

maps every polynomial in $\mathbb{C}[x]$ onto **the quotient ring**

$$\mathbb{C}[x]/\langle p \rangle = \{ a_0 + a_1x + a_2x^2 + a_3x^3 \mid a_i \in \mathbb{C} \},$$

is a 4-dimensional vector space with basis $\{1, x, x^2, x^3\}$.

By this vector space a problem of polynomial algebra becomes a problem of linear algebra.

the companion matrix

The relation

$$x^4 = 5x^3 - 7x^2 + x - 3$$

as a matrix equation

$$x \begin{bmatrix} 1 \\ x \\ x^2 \\ x^3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -3 & 1 & -7 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ x \\ x^2 \\ x^3 \end{bmatrix}.$$

The matrix above is **the companion matrix** C_p of p .Denote by $X = [1 \ x \ x^2 \ x^3]^T$ and use λ for x , then

$$\lambda X = C_p X$$

 \Rightarrow the 4 eigenvalues of C_p are the 4 roots of p .

the companion matrix

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation

Dickson's Lemma

The relation

$$x^4 = 5x^3 - 7x^2 + x - 3$$

as a matrix equation

$$x \begin{bmatrix} 1 \\ x \\ x^2 \\ x^3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -3 & 1 & -7 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ x \\ x^2 \\ x^3 \end{bmatrix}.$$

The matrix above is **the companion matrix** C_p of p .

Denote by $X = [1 \ x \ x^2 \ x^3]^T$ and use λ for x , then

$$\lambda X = C_p X$$

\Rightarrow the 4 eigenvalues of C_p are the 4 roots of p .

Rewriting Polynomials

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

- 1** Roots and Eigenvalues
the companion matrix of a polynomial
the ideal membership problem
- 2 Automatic Geometric Theorem Proving
the circle theorem of Apollonius
- 3 The Division Algorithm
monomial orderings
- 4 Monomial Ideals
staircase representation
Dickson's Lemma

the ideal generated by f

For a system $f(\mathbf{x}) = \mathbf{0}$, with $f = (f_1, f_2, \dots, f_N)$, we define **the ideal generated by f** as

$$\langle f \rangle = \{ a_1 f_1 + a_2 f_2 + \dots + a_N f_N \mid a_i \in \mathbb{C}[\mathbf{x}] \}.$$

The ideal membership problem: for a given ideal I and polynomial p , determine whether $p \in I$.

The solution to the membership problem is the map

$$\begin{aligned} \mathbb{C}[\mathbf{x}] &\rightarrow \mathbb{C}[\mathbf{x}]/I \\ p &\mapsto p \bmod I \end{aligned}$$

where $p \bmod I$ is p modulo the ideal I .

If we can rewrite (or reduce) p modulo I in a unique way then $p \bmod I = 0 \Leftrightarrow p \in I$.

Roots and
Eigenvalues
the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving
the circle theorem of
Apollonius

The Division
Algorithm
monomial orderings

Monomial
Ideals
staircase
representation
Dickson's Lemma

the ideal generated by f

For a system $f(\mathbf{x}) = \mathbf{0}$, with $f = (f_1, f_2, \dots, f_N)$, we define **the ideal generated by f** as

$$\langle f \rangle = \{ a_1 f_1 + a_2 f_2 + \dots + a_N f_N \mid a_i \in \mathbb{C}[\mathbf{x}] \}.$$

The ideal membership problem: for a given ideal I and polynomial p , determine whether $p \in I$.

The solution to the membership problem is the map

$$\begin{aligned} \mathbb{C}[\mathbf{x}] &\rightarrow \mathbb{C}[\mathbf{x}]/I \\ p &\mapsto p \bmod I \end{aligned}$$

where $p \bmod I$ is p modulo the ideal I .

If we can rewrite (or reduce) p modulo I in a unique way then $p \bmod I = 0 \Leftrightarrow p \in I$.

Roots and
Eigenvalues
the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving
the circle theorem of
Apollonius

The Division
Algorithm
monomial orderings

Monomial
Ideals
staircase
representation
Dickson's Lemma

Rewriting Polynomials

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

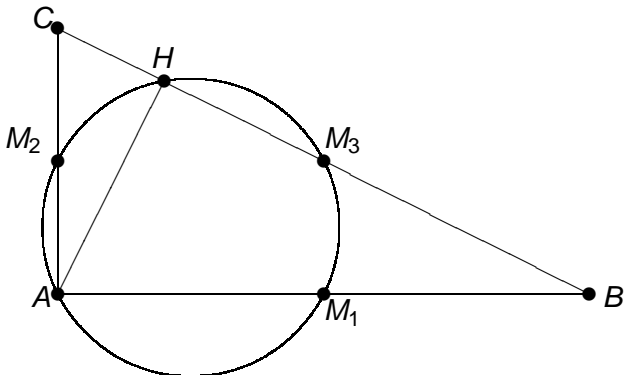
monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

- 1 Roots and Eigenvalues
the companion matrix of a polynomial
the ideal membership problem
- 2 Automatic Geometric Theorem Proving
the circle theorem of Apollonius
- 3 The Division Algorithm
monomial orderings
- 4 Monomial Ideals
staircase representation
Dickson's Lemma

the circle theorem of Apollonius



Theorem (The Circle Theorem of Apollonius)

Consider a right triangle spanned by A , B , and C , with the right angle at A . The midpoints of the three sides of the triangle, and the foot of the altitude drawn from A to the edge spanned by B and C all lie on one circle.

Roots and
Eigenvalues

the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving

the circle theorem of
Apollonius

The Division
Algorithm

monomial orderings

Monomial
Ideals

staircase
representation

Dickson's Lemma

coordinates and equations

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

The triangle spanned by A , B , C has midpoints M_1 , M_2 , M_3 :

- **Corners:** $A = (0, 0)$, $B = (u_1, 0)$, and $C = (0, u_2)$, where u_1 and u_2 are arbitrary.
- **Midpoints:** $M_1 = (x_1, 0)$, $M_2 = (0, x_2)$, $M_3 = (x_3, x_4)$.

M_1 is the midpoint of the edge spanned by A and B

$$h_1 = 2x_1 - u_1 = 0.$$

Similarly, $h_2 = 2x_2 - u_2 = 0$ expresses that

M_2 is the midpoint of the edge spanned by A and C .

For M_3 we have two conditions:

$$h_3 = 2x_3 - u_1 = 0 \quad \text{and} \quad h_4 = 2x_4 - u_2 = 0.$$

coordinates and equations

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

The triangle spanned by A , B , C has midpoints M_1 , M_2 , M_3 :

- Corners: $A = (0, 0)$, $B = (u_1, 0)$, and $C = (0, u_2)$, where u_1 and u_2 are arbitrary.
- Midpoints: $M_1 = (x_1, 0)$, $M_2 = (0, x_2)$, $M_3 = (x_3, x_4)$.

M_1 is the midpoint of the edge spanned by A and B

$$h_1 = 2x_1 - u_1 = 0.$$

Similarly, $h_2 = 2x_2 - u_2 = 0$ expresses that

M_2 is the midpoint of the edge spanned by A and C .

For M_3 we have two conditions:

$$h_3 = 2x_3 - u_1 = 0 \quad \text{and} \quad h_4 = 2x_4 - u_2 = 0.$$

coordinates and hypotheses

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

For the foot of the altitude H we choose coordinates (x_5, x_6) .
The line segment AH is perpendicular to the edge BC :

$$h_5 = x_5 u_1 - x_6 u_2 = 0.$$

The points B , H , and C are collinear:

$$h_6 = x_5 u_2 + x_6 u_1 - u_1 u_2 = 0.$$

The circle through the three midpoints must also contain H .
Let (x_7, x_8) be the coordinates of the center O of the circle.
 $M_1 O = M_2 O$ and $M_1 O = M_3 O$ is respectively equal to

$$h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0 \text{ and}$$

$$h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0.$$

coordinates and hypotheses

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

For the foot of the altitude H we choose coordinates (x_5, x_6) .
The line segment AH is perpendicular to the edge BC :

$$h_5 = x_5 u_1 - x_6 u_2 = 0.$$

The points B , H , and C are collinear:

$$h_6 = x_5 u_2 + x_6 u_1 - u_1 u_2 = 0.$$

The circle through the three midpoints must also contain H .
Let (x_7, x_8) be the coordinates of the center O of the circle.
 $M_1 O = M_2 O$ and $M_1 O = M_3 O$ is respectively equal to

$$h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0 \text{ and}$$

$$h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0.$$

an ideal membership problem

The eight hypothesis form the following system

$$f(\mathbf{u}, \mathbf{x}) = \left\{ \begin{array}{l} 2x_1 - u_1 = 0 \\ 2x_2 - u_2 = 0 \\ 2x_3 - u_1 = 0 \\ 2x_4 - u_2 = 0 \\ x_5 u_1 - x_6 u_2 = 0 \\ x_5 u_2 + x_6 u_1 - u_1 u_2 = 0 \\ (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0 \\ (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0. \end{array} \right.$$

With respect to these eight hypotheses, the conclusion must then be that $HO = M_1 O$, expressed by

$$g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0.$$

Theorem is true $\Leftrightarrow g \in \langle f \rangle$.

Rewriting Polynomials

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

- 1 Roots and Eigenvalues
the companion matrix of a polynomial
the ideal membership problem
- 2 Automatic Geometric Theorem Proving
the circle theorem of Apollonius
- 3 The Division Algorithm
monomial orderings
- 4 Monomial Ideals
staircase representation
Dickson's Lemma

quotient and remainder

Roots and
Eigenvalues

the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving

the circle theorem of
Apollonius

The Division
Algorithm

monomial orderings

Monomial
Ideals

staircase
representation
Dickson's Lemma

We want to solve the ideal membership problem.

For $g \in \mathbb{C}[\mathbf{x}]$ and an ideal generated by $f = (f_1, f_2, \dots, f_N)$:

Find

$$q_i \in \mathbb{C}[\mathbf{x}], i = 1, 2, \dots, N \quad \text{and} \quad r \in \mathbb{C}[\mathbf{x}]$$

so that

$$g = q_1 f_1 + q_2 f_2 + \dots + q_N f_N + r.$$

Obviously, if $r = 0$, then $g \in \langle f \rangle$,
but the opposite is not necessarily true.

ordering monomials

First, order the variables: $x_1 > x_2 > \cdots > x_n$.

Then, there are several monomial orderings:

- lexicographic:** We sort as in a dictionary.
 $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$ if the leftmost nonzero entry in $\mathbf{a} - \mathbf{b}$ is positive. For example: $x_1^2 x_2 >_{\text{lex}} x_1 x_2^3$.
- graded lexicographic:** We first sort the monomials according to their total degree and sort monomials with the same degree lexicographically. We have $\mathbf{x}^{\mathbf{a}} >_{\text{tdeg}} \mathbf{x}^{\mathbf{b}}$ if $\deg(\mathbf{x}^{\mathbf{a}}) > \deg(\mathbf{x}^{\mathbf{b}})$ or if $\deg(\mathbf{x}^{\mathbf{a}}) = \deg(\mathbf{x}^{\mathbf{b}})$ and $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$. For example: $x_1^2 x_2 >_{\text{tdeg}} x_1 x_2^2$.
- weighted lexicographic:** For $\omega \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, denote $\langle \mathbf{a}, \omega \rangle = a_1 \omega_1 + a_2 \omega_2 + \cdots + a_n \omega_n$. Then: $\mathbf{x}^{\mathbf{a}} >_{\omega} \mathbf{x}^{\mathbf{b}}$ if $\langle \mathbf{a}, \omega \rangle > \langle \mathbf{b}, \omega \rangle$ or $\langle \mathbf{a}, \omega \rangle = \langle \mathbf{b}, \omega \rangle$ and $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$.

Denote the leading term of a polynomial g by $\text{LT}(g)$.

Roots and
Eigenvalues
the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving
the circle theorem of
Apollonius

The Division
Algorithm
monomial orderings

Monomial
Ideals
staircase
representation
Dickson's Lemma

ordering monomials

First, order the variables: $x_1 > x_2 > \cdots > x_n$.

Then, there are several monomial orderings:

- lexicographic:** We sort as in a dictionary.
 $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$ if the leftmost nonzero entry in $\mathbf{a} - \mathbf{b}$ is positive. For example: $x_1^2 x_2 >_{\text{lex}} x_1 x_2^3$.
- graded lexicographic:** We first sort the monomials according to their total degree and sort monomials with the same degree lexicographically. We have $\mathbf{x}^{\mathbf{a}} >_{\text{tdeg}} \mathbf{x}^{\mathbf{b}}$ if $\deg(\mathbf{x}^{\mathbf{a}}) > \deg(\mathbf{x}^{\mathbf{b}})$ or if $\deg(\mathbf{x}^{\mathbf{a}}) = \deg(\mathbf{x}^{\mathbf{b}})$ and $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$. For example: $x_1^2 x_2 >_{\text{tdeg}} x_1 x_2^2$.
- weighted lexicographic:** For $\omega \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, denote $\langle \mathbf{a}, \omega \rangle = a_1 \omega_1 + a_2 \omega_2 + \cdots + a_n \omega_n$. Then: $\mathbf{x}^{\mathbf{a}} >_{\omega} \mathbf{x}^{\mathbf{b}}$ if $\langle \mathbf{a}, \omega \rangle > \langle \mathbf{b}, \omega \rangle$ or $\langle \mathbf{a}, \omega \rangle = \langle \mathbf{b}, \omega \rangle$ and $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$.

Denote the leading term of a polynomial g by $\text{LT}(g)$.

ordering monomials

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

First, order the variables: $x_1 > x_2 > \cdots > x_n$.

Then, there are several monomial orderings:

- **lexicographic:** We sort as in a dictionary. $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$ if the leftmost nonzero entry in $\mathbf{a} - \mathbf{b}$ is positive. For example: $x_1^2 x_2 >_{\text{lex}} x_1 x_2^3$.
- **graded lexicographic:** We first sort the monomials according to their total degree and sort monomials with the same degree lexicographically. We have $\mathbf{x}^{\mathbf{a}} >_{\text{tdeg}} \mathbf{x}^{\mathbf{b}}$ if $\deg(\mathbf{x}^{\mathbf{a}}) > \deg(\mathbf{x}^{\mathbf{b}})$ or if $\deg(\mathbf{x}^{\mathbf{a}}) = \deg(\mathbf{x}^{\mathbf{b}})$ and $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$. For example: $x_1^2 x_2 >_{\text{tdeg}} x_1 x_2^2$.
- **weighted lexicographic:** For $\omega \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, denote $\langle \mathbf{a}, \omega \rangle = a_1 \omega_1 + a_2 \omega_2 + \cdots + a_n \omega_n$. Then: $\mathbf{x}^{\mathbf{a}} >_{\omega} \mathbf{x}^{\mathbf{b}}$ if $\langle \mathbf{a}, \omega \rangle > \langle \mathbf{b}, \omega \rangle$ or $\langle \mathbf{a}, \omega \rangle = \langle \mathbf{b}, \omega \rangle$ and $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$.

Denote the leading term of a polynomial g by $\text{LT}(g)$.

the division algorithm

The division algorithm to compute the remainder:

Input: $f = (f_1, f_2, \dots, f_N)$ and $p \in \mathbb{C}[\mathbf{x}]$.

Output: r , the remainder of p modulo f , denoted by $p \rightarrow_f r$.

$r := p$;

repeat

$k := 0$;

 for i from 1 to N do

 if $\text{LT}(f_i)$ divides $\text{LT}(r)$

 then $k := i$; exit for loop;

 end if;

 end for;

 if $k \neq 0$ then $r := r - \frac{\text{LT}(r)}{\text{LT}(f_k)} f_k$; end if;

until $r = 0$ or $k = 0$.

the division algorithm

The division algorithm to compute the remainder:

Input: $f = (f_1, f_2, \dots, f_N)$ and $p \in \mathbb{C}[\mathbf{x}]$.

Output: r , the remainder of p modulo f , denoted by $p \rightarrow_f r$.

$r := p$;

repeat

$k := 0$;

 for i from 1 to N do

 if $\text{LT}(f_i)$ divides $\text{LT}(r)$

 then $k := i$; exit for loop;

 end if;

 end for;

 if $k \neq 0$ then $r := r - \frac{\text{LT}(r)}{\text{LT}(f_k)} f_k$; end if;

until $r = 0$ or $k = 0$.

the division algorithm

The division algorithm to compute the remainder:

Input: $f = (f_1, f_2, \dots, f_N)$ and $p \in \mathbb{C}[\mathbf{x}]$.

Output: r , the remainder of p modulo f , denoted by $p \rightarrow_f r$.

$r := p$;

repeat

$k := 0$;

 for i from 1 to N do

 if $\text{LT}(f_i)$ divides $\text{LT}(r)$

 then $k := i$; exit for loop;

 end if;

 end for;

 if $k \neq 0$ then $r := r - \frac{\text{LT}(r)}{\text{LT}(f_k)} f_k$; end if;

until $r = 0$ or $k = 0$.

an example

Take \succ_{lex} as monomial order and $g = xy^2 - x$ with respect to the ideal generated by $f_1 = xy + 1$ and $f_2 = y^2 - 1$.

$$\begin{aligned} \langle f_1, f_2 \rangle : \text{LT}(g) = y\text{LT}(f_1) &\rightarrow g := g - yf_1 \\ &= xy^2 - x - y(xy + 1) \\ &= -x - y. \end{aligned}$$

But when we swap the order of the polynomials in $\langle f \rangle$:

$$\begin{aligned} \langle f_2, f_1 \rangle : \text{LT}(g) = x\text{LT}(f_2) &\rightarrow g := g - xf_2 \\ &= xy^2 - x - x(y^2 - x) \\ &= 0, \end{aligned}$$

we see that $g \in \langle f \rangle$.

an example

Take $>_{\text{lex}}$ as monomial order and $g = xy^2 - x$ with respect to the ideal generated by $f_1 = xy + 1$ and $f_2 = y^2 - 1$.

$$\begin{aligned} \langle f_1, f_2 \rangle : \text{LT}(g) = y\text{LT}(f_1) &\rightarrow g := g - yf_1 \\ &= xy^2 - x - y(xy + 1) \\ &= -x - y. \end{aligned}$$

But when we swap the order of the polynomials in $\langle f \rangle$:

$$\begin{aligned} \langle f_2, f_1 \rangle : \text{LT}(g) = x\text{LT}(f_2) &\rightarrow g := g - xf_2 \\ &= xy^2 - x - x(y^2 - x) \\ &= 0, \end{aligned}$$

we see that $g \in \langle f \rangle$.

Rewriting Polynomials

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation
Dickson's Lemma

- 1 Roots and Eigenvalues
the companion matrix of a polynomial
the ideal membership problem
- 2 Automatic Geometric Theorem Proving
the circle theorem of Apollonius
- 3 The Division Algorithm
monomial orderings
- 4 Monomial Ideals
staircase representation
Dickson's Lemma

monomial ideals

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

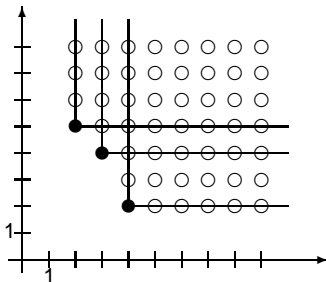
staircase representation

Dickson's Lemma

A monomial ideal is generated by monomials.

For example: $\langle x^2y^5, x^3y^4, x^4y^2 \rangle$.

Identifying exponents with lattice points, leads to a staircase:



Rewriting Polynomials

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation

Dickson's Lemma

- 1 Roots and Eigenvalues
the companion matrix of a polynomial
the ideal membership problem
- 2 Automatic Geometric Theorem Proving
the circle theorem of Apollonius
- 3 The Division Algorithm
monomial orderings
- 4 Monomial Ideals
staircase representation
Dickson's Lemma

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation

Dickson's Lemma

Dickson's Lemma

Lemma (Dickson's Lemma)

Every monomial ideal is finitely generated.

Proof. We need to show that for every monomial ideal I , there exists a finite subset S so that

for all $\mathbf{x}^{\mathbf{a}} \in I$ there is a monomial $\mathbf{x}^{\mathbf{b}} \in S$ that divides $\mathbf{x}^{\mathbf{a}}$.

We proceed by induction on n , the number of variables.

For $n = 1$, $d = \min_{\mathbf{x}^{\mathbf{a}} \in I} x^{\mathbf{a}}$ is unique, so $S = \{x^d\}$.

Dickson's Lemma

Lemma (Dickson's Lemma)

Every monomial ideal is finitely generated.

Proof. We need to show that for every monomial ideal I , there exists a finite subset S so that

for all $\mathbf{x}^{\mathbf{a}} \in I$ there is a monomial $\mathbf{x}^{\mathbf{b}} \in S$ that divides $\mathbf{x}^{\mathbf{a}}$.

We proceed by induction on n , the number of variables.

For $n = 1$, $d = \min_{\mathbf{x}^{\mathbf{a}} \in I} x^{\mathbf{a}}$ is unique, so $S = \{x^d\}$.

Roots and
Eigenvalues

the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving

the circle theorem of
Apollonius

The Division
Algorithm

monomial orderings

Monomial
Ideals

staircase
representation

Dickson's Lemma

Lemma (Dickson's Lemma)

Every monomial ideal is finitely generated.

Proof. We need to show that for every monomial ideal I , there exists a finite subset S so that

for all $\mathbf{x}^{\mathbf{a}} \in I$ there is a monomial $\mathbf{x}^{\mathbf{b}} \in S$ that divides $\mathbf{x}^{\mathbf{a}}$.

We proceed by induction on n , the number of variables.

For $n = 1$, $d = \min_{\mathbf{x}^{\mathbf{a}} \in I} x^{\mathbf{a}}$ is unique, so $S = \{\mathbf{x}^d\}$.

applying induction

For $n > 1$, take $\mathbf{x}^{\mathbf{b}} \in I$. Every monomial in I not divisible by $\mathbf{x}^{\mathbf{b}}$ belongs to one of the following sets:

$$R_{i,j} = \{ \mathbf{x}^{\mathbf{a}} \in I \mid a_i = j \}, \quad i = 1, 2, \dots, n, \quad j = 0, 1, \dots, b_i - 1.$$

Denote $\widehat{R}_{i,j} = \{ \mathbf{x}^{\mathbf{a}}|_{x_i=1} \mid \mathbf{x}^{\mathbf{a}} \in R_{i,j} \}$ (x_i removed from $R_{i,j}$).

By the induction hypothesis, there is a finite set $\widehat{S}_{i,j}$ that generates $I_i = \{ \mathbf{x}^{\mathbf{a}}|_{x_i=1} \mid \mathbf{x}^{\mathbf{a}} \in I \}$.

Define $S_{i,j} = \{ x_i^j \mathbf{x}^{\mathbf{a}} \mid \mathbf{x}^{\mathbf{a}} \in \widehat{S}_{i,j} \}$ and let

$$S = \{ \mathbf{x}^{\mathbf{b}} \} \cup \left(\bigcup_{i=1}^n \bigcup_{j=0}^{b_i-1} S_{i,j} \right).$$

S generates $\mathbf{x}^{\mathbf{b}}$ and every $\mathbf{x}^{\mathbf{a}} \in I$ not divisible by $\mathbf{x}^{\mathbf{b}}$.

Thus S generates I . □

applying induction

For $n > 1$, take $\mathbf{x}^{\mathbf{b}} \in I$. Every monomial in I not divisible by $\mathbf{x}^{\mathbf{b}}$ belongs to one of the following sets:

$$R_{i,j} = \{ \mathbf{x}^{\mathbf{a}} \in I \mid a_i = j \}, \quad i = 1, 2, \dots, n, \quad j = 0, 1, \dots, b_i - 1.$$

Denote $\widehat{R}_{i,j} = \{ \mathbf{x}^{\mathbf{a}}|_{x_i=1} \mid \mathbf{x}^{\mathbf{a}} \in R_{i,j} \}$ (x_i removed from $R_{i,j}$).

By the induction hypothesis, there is a finite set $\widehat{S}_{i,j}$ that generates $I_i = \{ \mathbf{x}^{\mathbf{a}}|_{x_i=1} \mid \mathbf{x}^{\mathbf{a}} \in I \}$.

Define $S_{i,j} = \{ x_i^j \mathbf{x}^{\mathbf{a}} \mid \mathbf{x}^{\mathbf{a}} \in \widehat{S}_{i,j} \}$ and let

$$S = \{ \mathbf{x}^{\mathbf{b}} \} \cup \left(\bigcup_{i=1}^n \bigcup_{j=0}^{b_i-1} S_{i,j} \right).$$

S generates $\mathbf{x}^{\mathbf{b}}$ and every $\mathbf{x}^{\mathbf{a}} \in I$ not divisible by $\mathbf{x}^{\mathbf{b}}$.

Thus S generates I . □

applying induction

For $n > 1$, take $\mathbf{x}^{\mathbf{b}} \in I$. Every monomial in I not divisible by $\mathbf{x}^{\mathbf{b}}$ belongs to one of the following sets:

$$R_{i,j} = \{ \mathbf{x}^{\mathbf{a}} \in I \mid a_i = j \}, \quad i = 1, 2, \dots, n, \quad j = 0, 1, \dots, b_i - 1.$$

Denote $\widehat{R}_{i,j} = \{ \mathbf{x}^{\mathbf{a}}|_{x_i=1} \mid \mathbf{x}^{\mathbf{a}} \in R_{i,j} \}$ (x_i removed from $R_{i,j}$).

By the induction hypothesis, there is a finite set $\widehat{S}_{i,j}$ that generates $I_i = \{ \mathbf{x}^{\mathbf{a}}|_{x_i=1} \mid \mathbf{x}^{\mathbf{a}} \in I \}$.

Define $S_{i,j} = \{ x_i^j \mathbf{x}^{\mathbf{a}} \mid \mathbf{x}^{\mathbf{a}} \in \widehat{S}_{i,j} \}$ and let

$$S = \{ \mathbf{x}^{\mathbf{b}} \} \cup \left(\bigcup_{i=1}^n \bigcup_{j=0}^{b_i-1} S_{i,j} \right).$$

S generates $\mathbf{x}^{\mathbf{b}}$ and every $\mathbf{x}^{\mathbf{a}} \in I$ not divisible by $\mathbf{x}^{\mathbf{b}}$.
Thus S generates I . □

Groebner Basis

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation

Dickson's Lemma

A Groebner basis G for an ideal I is

- 1 a basis for the ideal, i.e.: $\langle G \rangle = I$;
- 2 the output of the division algorithm is unique:

$$p \rightarrow_G = p \rightarrow_I.$$

With a Groebner basis G for I , the r in $p \rightarrow_G r$ is *the normal form of p with respect to I* .

An algorithm to compute a Groebner basis leads to

Theorem (Hilbert's basis theorem)

Every ideal has a finite generating set.

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation

Dickson's Lemma

A Groebner basis G for an ideal I is

- 1 a basis for the ideal, i.e.: $\langle G \rangle = I$;
- 2 the output of the division algorithm is unique:

$$p \rightarrow_G = p \rightarrow_I.$$

With a Groebner basis G for I , the r in $p \rightarrow_G r$ is *the normal form of p with respect to I* .

An algorithm to compute a Groebner basis leads to

Theorem (Hilbert's basis theorem)

Every ideal has a finite generating set.

Summary + Exercises

Roots and Eigenvalues

the companion matrix of a polynomial
the ideal membership problem

Automatic Geometric Theorem Proving

the circle theorem of Apollonius

The Division Algorithm

monomial orderings

Monomial Ideals

staircase representation

Dickson's Lemma

We introduced the division algorithm and defined the ideal membership problem.

Exercises:

- 1 For the polynomial $p(x) = x^4 - 5x^3 + 7x^2 - x + 3$, use MATLAB (Octave will do as well) or Maple to define the companion matrix and to compute its eigenvalues. What are the eigenvectors?
- 2 Consider the polynomial $p(x) = (x - 1)^3(x - 2)$ and describe the eigenvalues and eigenvectors of the companion matrix, using MATLAB or Maple. Can you recognize the multiplicities of the two roots?

Roots and
Eigenvalues

the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving

the circle theorem of
Apollonius

The Division
Algorithm

monomial orderings

Monomial
Ideals

staircase
representation

Dickson's Lemma

- 3 Write a Maple procedure to implement the division algorithm. Extend your implementation so that in addition to the remainder r the algorithm also returns the “quotients” q_i in the combination $f = q_1g_1 + q_2g_2 + \cdots + q_Ng_N + r$, for any basis g and input polynomial f . You may also use another computer algebra system.
- 4 Consider the monomial ideal $I = \langle x^3y, x^2y^2, xy^6 \rangle$. Draw the exponent vectors of the monomials in the plane and visualize the staircase and all elements generated by I .
- 5 How can you see from the staircase that the monomial ideal has only finitely many solutions? Give examples and justify your observation.

and more exercises

Roots and
Eigenvalues

the companion
matrix of a
polynomial
the ideal
membership problem

Automatic
Geometric
Theorem
Proving

the circle theorem of
Appolonius

The Division
Algorithm

monomial orderings

Monomial
Ideals

staircase
representation

Dickson's Lemma

- 6 For some finite support set A , let $I = \langle \mathbf{x}^{\mathbf{a}} \mid \mathbf{a} \in A \rangle$ be the monomial ideal defined by A . Show that $\mathbf{x}^{\mathbf{b}} \in I$ if and only if $\mathbf{x}^{\mathbf{b}}$ is divisible by some monomial $\mathbf{x}^{\mathbf{a}}$ for some $\mathbf{a} \in A$.
- 7 Let $f = (\mathbf{x}^{\mathbf{a}_1}, \mathbf{x}^{\mathbf{a}_2}, \dots, \mathbf{x}^{\mathbf{a}_N})$ define a monomial ideal. Show that $p \in \langle f \rangle \Leftrightarrow p \rightarrow_f 0$.
- 8 Use Maple or Sage (in particular: Singular) to compute a Groebner basis of the ideal generated by the polynomial in the system $f(\mathbf{u}, \mathbf{x})$ (of the circle theorem of Appolonius), using a lexicographic order on the monomials. Does the form of the Groebner basis allow you to reduce the conclusion g to zero?