Quotient Rings

1. the Shape Lemma
   - the ideal of a set of points
   - vanishing polynomials
2. Design of Experiments
   - a problem for algebraic statistics
3. the Quotient Algebra
   - monomials under the staircase
4. the Buchberger-Möller algorithm
   - computing the monomials under the staircase
   - using Macaulay 2

MCS 563 Lecture 8
Analytic Symbolic Computation
Jan Verschelde, 31 January 2014

Quotient Rings

1. the Shape Lemma
   - the ideal of a set of points
   - vanishing polynomials
2. Design of Experiments
   - a problem for algebraic statistics
3. the Quotient Algebra
   - monomials under the staircase
4. the Buchberger-Möller algorithm
   - computing the monomials under the staircase
   - using Macaulay 2

defining ideals

Our point of departure is not a polynomial system, but a set of points $V \subset \mathbb{C}^n$.

The defining ideal of V is the set of all polynomials which vanish on V, or formally:

$$I(V) = \{ \, f \in \mathbb{C}[\mathbf{x}] \mid f(\mathbf{z}) = \mathbf{0}, \ \forall \mathbf{z} \in V \, \}.$$

If V contains only one point $\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n$, $V = \{\mathbf{z}\}$, then $I(V) = \langle x_1 - z_1, x_2 - z_2, \ldots, x_n - z_n \rangle$.

For any ideal I, the quotient ring is

$$\mathbb{C}[\mathbf{x}]/I = \{ \, r \in \mathbb{C}[\mathbf{x}] \mid f \rightarrow_I r, \ \forall f \in \mathbb{C}[\mathbf{x}] \, \}.$$

For $I = I(\{\mathbf{z}\})$ we see that the remainder after division by the polynomials $x_i - z_i$, $i = 1, 2, \ldots, n$, will always be a constant. Thus we may identify $\mathbb{C}[\mathbf{x}]/I(\{\mathbf{z}\})$ with $\mathbb{C}$.

Lagrange polynomials

Let $V = \{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_k\}$ with $\mathbf{z}_i \neq \mathbf{z}_j$ for $i \neq j$.
We denote by $\mathbf{z}_{i,j}$ the jth coordinate of $\mathbf{z}_i$.

If all points in V have a *different first* coordinate $z_{i,1}$,
then the Lagrange polynomials in x_1 separate the points.
The ith Lagrange polynomial is

$$L_i(\mathbf{x}) = \prod_{\substack{j=1 \\ j \neq i}}^{n} \left(\frac{x_1 - z_{j,1}}{z_{i,1} - z_{j,1}} \right).$$

We have

$$L_i(\mathbf{z}_j) = \begin{cases} 1 & \text{if} \quad i = j \\ 0 & \text{if} \quad i \neq j. \end{cases}$$

interpolating polynomials

A polynomial $s_{\mathbf{z}_i}(\mathbf{x}) \in \mathbb{C}[\mathbf{x}]$ is a separator for the point $\mathbf{z}_i$ if

$$s_{\mathbf{z}_i}(\mathbf{z}_j) = \begin{cases} 1 & \textit{if} \quad i = j \\ 0 & \textit{if} \quad i \neq j. \end{cases}$$

Given a value v_i for each point $\mathbf{z}_i \in V$, a polynomial $p \in \mathbb{C}[\mathbf{x}]$ is interpolating the values v_i at the points $\mathbf{z}_i$ if

$$p(\mathbf{z}_i) = v_i, \quad \text{for } i = 1, 2, \ldots, k$$

Given a separators for the points,

$$p(\mathbf{x}) = \sum_{i=1}^{k} v_i s_{\mathbf{z}_i}(\mathbf{x})$$

satisfies the k interpolation conditions.

Quotient Rings

1. the Shape Lemma
   - the ideal of a set of points
   - vanishing polynomials
2. Design of Experiments
   - a problem for algebraic statistics
3. the Quotient Algebra
   - monomials under the staircase
4. the Buchberger-Möller algorithm
   - computing the monomials under the staircase
   - using Macaulay 2

vanishing polynomials

As a special case of the interpolating polynomials, consider the polynomials

$$p_j(\mathbf{x}) = x_j - \sum_{i=1}^{k} z_{i,j} s_{\mathbf{z}_i}(\mathbf{x}), \quad j = 1, 2, \ldots, n,$$

where the values v_i are simply the coordinates of the points.

Evaluating p_j at $\mathbf{z}_\ell$, we see that

$$p_j(\mathbf{z}_\ell) = z_{\ell,j} - \sum_{i=1}^{k} z_{i,j} s_{\mathbf{z}_i}(\mathbf{z}_\ell) = z_{\ell,j} - z_{\ell,j} s_{\mathbf{z}_\ell}(\mathbf{z}_\ell) = 0.$$

So we have polynomials vanishing at the set V.

the shape lemma

If all points have a distinct first coordinate, then with Lagrange polynomials as separators we construct a lexicographic Gröbner basis for $I(V)$:

$$g = \left\{ \begin{array}{l} x_n - \sum_{i=1}^{k} z_{i,n} L_i(\mathbf{x}), \ldots, x_2 - \sum_{i=1}^{k} z_{i,2} L_i(\mathbf{x}), \\ (x_1 - z_{1,1})(x_1 - z_{2,1}) \cdots (x_1 - z_{k,1}) \end{array} \right\}.$$

By its shape, the solution set equals V.

For any $f \in \mathbb{C}[\mathbf{x}]$, we have $f \rightarrow_g r$ with $r = r_0 + r_1 x_1 + r_2 x_1^2 + \cdots + r_{k-1} x_1^{k-1}$, so: $\dim(\mathbb{C}[\mathbf{x}]/\langle g \rangle) = k$.

If some of the points in V have the same first coordinate, then we may apply a random linear coordinate change.

Quotient Rings

1. the Shape Lemma
   - the ideal of a set of points
   - vanishing polynomials
2. Design of Experiments
   - a problem for algebraic statistics
3. the Quotient Algebra
   - monomials under the staircase
4. the Buchberger-Möller algorithm
   - computing the monomials under the staircase
   - using Macaulay 2

Design of Experiments

5 factors: color, shape, weight, material, and price determine the choice of features in a new product.
Assume 3 choices for every factor: $3^5 = 243$ prototypes.
Test consumer reaction: need to find a subset of 3^5.

Factorial design: determine a subset $\mathcal{F}$ of all choices from which we construct a good model to rate the product.

For example: if the 5 features are color (C), shape (S), weight (W), material (M), and price (P), then a model is a polynomial $f \in \mathbb{R}[C, S, W, M, P]$.

Three Problems

1. Let $\mathcal{F} := \{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_s\} \subset \mathcal{D}$. What are the complete linear models which can be identified by $\mathcal{F}$?
   $\rightarrow$ what are the possible bases of $\mathbb{C}[\mathbf{x}]/I(\mathcal{F})$?

2. Let the polynomial $f(\mathbf{x})$ be a complete linear polynomial model, where the support of f is a subset of the normal set of $\mathcal{D}$. What are the minimal fractions which identify the model? $\rightarrow$ for a set O of monomials, find $\mathcal{F}$: O is a basis of $\mathbb{C}[\mathbf{x}]/I(\mathcal{F})$

3. What are the fractions $\mathcal{F}$ of $\mathcal{D}$, with $\#\mathcal{F} < \#\mathcal{D}$ which identify the highest (or lowest) number of complete linear polynomial models?
   $\rightarrow$ find O with highest (or lowest) $\#O$, O is basis for $\mathbb{C}[\mathbf{x}]/I(\mathcal{F})$.

Quotient Rings

1. the Shape Lemma
   - the ideal of a set of points
   - vanishing polynomials
2. Design of Experiments
   - a problem for algebraic statistics
3. the Quotient Algebra
   - monomials under the staircase
4. the Buchberger-Möller algorithm
   - computing the monomials under the staircase
   - using Macaulay 2

the quotient algebra

If $\#V = k$ isolated points for the ideal $I = I(V)$, then the quotient ring $\mathbb{C}[\mathbf{x}]/I$ is a k-dimensional vector space, called the quotient algebra.

A Gröbner basis with the total degree order ($x > y$):

$$g = \{\ 2x^2 + 3xy + y^2 - 3x - 3y,\ xy^2 - x,\ y^3 - y\ \}.$$

The initial ideal is generated by $\mathrm{LT}(g) = \{x^2, xy^2, y^3\}$.

The only monomials not in the ideal are $O = \{1, x, y, xy, y^2\}$ and therefore:

$$\forall p \in \mathbb{C}[x, y] : p \rightarrow_g r = c_1 + c_2 x + c_3 y + c_4 xy + c_5 y^2$$

for some coefficients c_i, $i = 1, 2, \ldots, 5$. In Maple we type:

```
Groebner[NormalForm](x^2*y,g,tdeg(x,y));
```

multiplication matrices

Turning the set O into a basis vector B using $\rightarrow_g$ on xB, we define an eigenvalue problem $xB = M_x B$:

$$x \begin{bmatrix} 1 \\ x \\ y \\ xy \\ y^2 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & \frac{3}{2} & \frac{3}{2} & -\frac{3}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & 0 \\ 0 & -\frac{3}{2} & -\frac{1}{2} & \frac{3}{2} & \frac{3}{2} \\ 0 & -1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ x \\ y \\ xy \\ y^2 \end{bmatrix}$$

where the matrix M_x defines the multiplication by x mod I.

The multiplication by y mod I defines M_y.
The eigenvalues of M_x and M_y give respectively the x and y-coordinates of the solutions.
So the multiplication matrices generalize the familiar companion matrices for polynomials in one variable.

counting the solutions

Theorem

Consider $f(\mathbf{x}) = \mathbf{0}$ *with* $V = f^{-1}(\mathbf{0}) \subset \mathbb{C}^n$.
Assume that all solutions have multiplicity one. Then:

$$\#V < \infty \quad \Leftrightarrow \quad \dim(\mathbb{C}[\mathbf{x}]/\langle f \rangle) = \#V.$$

$\Rightarrow$: the Shape lemma gives a lexicographic Gröbner basis.
The size of basis of the quotient ring is $\#V$.

$\Leftarrow$: we define the multiplication matrices to compute the coordinates of all points in V.

the Central Theorem

Below is a simple version of the central theorem
in Numerical Polynomial Algebra of Hans J. Stetter.

Theorem

*Let I be a zero dimensional ideal with $\#V(I) = k$, $V(I) \subset \mathbb{C}^n$.
Then there is a commuting family of multiplication matrices M_{x_i}, each of dimension k, for $i = 1, 2, \ldots, n$.
The multiplication matrices have a joint invariant subspace. Each joint eigenvector corresponds to one solution.*

This central theorem establishes the link between zero dimensional polynomial ideals and eigenvalue problems.

multiple solutions

$$f(\mathbf{x}) = \begin{cases} x_1 + x_2 + x_3 - 1 = 0 \\ \frac{1}{5}x_1^3 + \frac{1}{2}x_2^2 - x_3 + \frac{1}{2}x_3^2 + \frac{1}{2} = 0 \\ x_1 + x_2 + \frac{1}{2}x_3^2 - \frac{1}{2} = 0. \end{cases}$$

With Maple:

```
[> gb := Groebner[gbasis](P,tdeg(x[1],x[2],x[3]));
[> ns,rv
   := Groebner[SetBasis](gb,tdeg(x[1],x[2],x[3]));
```

The last command returns the normal set as a list in `ns` and as a table in `rv`: $[1, x_3, x_2, x_2x_3, x_2^2, x_2^2x_3]$.

The size of the normal set tells us that the system has six solutions, *counted with multiplicities*.

the Jordan Canonical Form

```
[> Mx[1] := Groebner[MulMatrix]
      (x[1],ns,rv,gb,tdeg(x[1],x[2],x[3]));
[> v1 := LinearAlgebra[Eigenvalues](Mx[1]);
```

The eigenvalues of M_{x_1} are $[-\frac{5}{2}, -\frac{5}{2}, 0, 0, 0, 0]$.
Two distinct solutions: $(-\frac{5}{2}, -\frac{5}{2}, 1)$ and $(0, 0, 1)$, respectively with multiplicities two and four.

```
[> J := LinearAlgebra[JordanForm](Mx[1]);
```

$$J = \left[\begin{array}{cc|ccc|c} -\frac{5}{2} & 1 & 0 & 0 & 0 & 0 \\ 0 & -\frac{5}{2} & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

Quotient Rings

1. the Shape Lemma
   - the ideal of a set of points
   - vanishing polynomials

2. Design of Experiments
   - a problem for algebraic statistics

3. the Quotient Algebra
   - monomials under the staircase

4. the Buchberger-Möller algorithm
   - computing the monomials under the staircase
   - using Macaulay 2

the Buchberger-Möller algorithm

A set of monomials O is called *a normal set*
when for all $\mathbf{x}^\mathbf{a} \in O$: if $\mathbf{x}^\mathbf{b}$ divides $x^\mathbf{a}$, then $\mathbf{x}^\mathbf{b} \in O$.

For all generators $\mathbf{x}^\mathbf{a}$ of $\langle \mathrm{LT}(I(V)) \rangle$:

$$\mathbf{x}^\mathbf{a} = x_i \mathbf{x}^\mathbf{b} \quad \text{for some } i \text{ and } \mathbf{x}^\mathbf{b} \in O.$$

Note: $\dim(\mathbb{C}[\mathbf{x}]/I(V)) = \#V = \#O$.

Specifications for the algorithm:

Input: $V = \{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_k\}$ and a term order $<$.
Output: g is a Gröbner basis of $I(V)$ with respect to $<$;
O is a normal set, $\#O = k$;
S is a set of separators for the points in V.

the algorithm

$g := \emptyset$; $O := \emptyset$; $S := \emptyset$; $r := 0$; $L := \{1\}$;
while $L \neq \emptyset$ do

$$T := \min_<(L);\ L := L \setminus T;\ f := T - \sum_{i=1}^{k} T(\mathbf{z}_{\pi(i)}) s_i;$$

if f vanishes on V then
  $g := g \cup \{f\}$;
  $L := L \setminus \{$ multiples of T $\}$;
else
  $O := O \cup T$; $r := r + 1$;
  $\pi(r) := \min\{\ i \mid f(\mathbf{z}_i) \neq 0\ \}$;
  $s_r := f/f(\mathbf{z}_\pi(r))$; $S := S \cup \{s_r\}$;
  for i from 1 to $r - 1$ do
    $s_i := s_i - s_i(\mathbf{z}_{\pi(r)}) s_r$;
  end for;
  $L := L \cup \{\ x_i T \mid i = 1, 2, \ldots, n\ \} \setminus \mathrm{LT}(g)$;
end if;
end while.

Quotient Rings

1. the Shape Lemma
   - the ideal of a set of points
   - vanishing polynomials
2. Design of Experiments
   - a problem for algebraic statistics
3. the Quotient Algebra
   - monomials under the staircase
4. the Buchberger-Möller algorithm
   - computing the monomials under the staircase
   - using Macaulay 2

using Macaulay 2

An implementation of the Buchberger-Möller algorithm is available in Macaulay 2 in the package `Points`:

```
$ M2
Macaulay2, version 1.3.1
with packages: ConwayPolynomials, Elimination, IntegralClos
               PrimaryDecomposition, ReesAlgebra, SchurRing

i1 : loadPackage "Points";
```

a first example

```
i2 : M = matrix{{1,2,3},{4,5,6}}

o2 = | 1 2 3 |
     | 4 5 6 |
                  2        3
o2 : Matrix ZZ  <--- ZZ

i3 : R = QQ[x,y,MonomialOrder=>Lex];

i4 : (Q,inG,G) = points(M,R)

                  2           3
o4 = ({1, y, y }, ideal (y , x),

          3      2
      {y  - 15y  + 74y - 120, x - y + 3})
```

another example

```
i5 : M2 = matrix{{1,2,3},{2,2,2}}

o5 = | 1 2 3 |
     | 2 2 2 |
                 2        3
o5 : Matrix ZZ  <--- ZZ

i6 : (Q2,inG2,G2) = points(M2,R)

                 2              3
o6 = ({1, x, x }, ideal (y, x ),

                  3     2
      {y - 2, x  - 6x  + 11x - 6})
```

and another example

```
i7 : M3 = matrix{{1,1,2},{1,2,2}}

o7 = | 1 1 2 |
     | 1 2 2 |
                  2        3
o7 : Matrix ZZ  <--- ZZ

i8 : (Q3,inG3,G3) = points(M3,R)

                         2        2
o8 = ({1, y, x}, ideal (y , x*y, x ),

      2                              2
    {y  - 3y + 2, x*y - 2x - y + 2, x  - 3x + 2})
```

Summary + Exercises

The Shape Lemma and the Buchberger-Möller algorithm allow to define ideals given a finite set of points.

Exercises:

1. For two finite sets V and W, show that $V \subset W$ implies $I(V) \supset I(W)$.
2. Use the definition of the Gröbner basis to show that the set of polynomials defined by the Shape lemma is a Gröbner basis for $I(V)$.
3. Consider $V = \{(1/3, 5, 1/2), (1, 2, 1/5), (2, 2, 3), (2, 2, 2)\}$. Observe that the third coordinate is different for each point in V. Use this observation to compute the shape lemma representation of V.

more exercises

4. For the set V as in the previous exercise, take a lexicographic term order and run the Buchberger-Möller algorithm.
5. Download the free computer algebra system CoCoA from `http://cocoa.dima.unige.it/` and use it to solve the previous exercises. Alternatively, you may also use Macaulay 2.

one last exercise

6. Consider the ideal $I = \langle xy + z - xz, x^2 - z, 2x^3 - x^2yz - 1 \rangle$ over $\mathbb{Q}[x, y, z]$.

Use CoCoA, Maple, Macaulay 2, or Sage for the following:

1. Compute a Gröbner basis with respect to the lexicographic order $x > y > z$. How many points does $V(I)$ have? Give the coordinates for all points in $V(I)$.
2. Use $V(I)$ to bring the ideal in the shape lemma and compare with the lexicographic Gröbner basis.
3. Use the total degree order to compute a Gröbner basis g for I. What is the normal set and corresponding basis vector B for the quotient ring? Apply the division algorithm $\rightarrow_g$ to define M_x. Compute the eigenvalues for M_x and verify that they give the x-coordinates of the points in $V(I)$.