Computing Primary Decompositions

MCS 563 Lecture 35
Analytic Symbolic Computation
Jan Verschelde, 15 April 2011

Computing Primary Decompositions

dimension of an ideal

Let I be an ideal in $\mathbb{K}[\mathbf{x}]$ and consider $\mathbf{x}$ as a set.

For $\mathbf{u} \subset \mathbf{x}$ we say that

$$\mathbf{u} \textit{ independent mod } I \text{ if } I \cap \mathbb{K}[\mathbf{u}] = \{0\},$$

if I contains no nonzero polynomials with variables only in $\mathbf{u}$.

Then the dimension of the ideal I is

$$\dim(I) = \max\{\ \#\mathbf{u} \mid \mathbf{u} \subset \mathbf{x},\ \mathbf{u} \text{ is independent mod } I\ \}.$$

Geometrically and algebraically, $\dim(I)$ is

- the largest dimension of the associated primes of I.
- the degree of the Hilbert polynomial of I.

using Gröbner bases

To compute the dimension:

$\dim(I) = 0$: given a Gröbner basis G for any term order $>$ check if for all $x_i \in \mathbf{x}$ there is a $g \in G$ such that $\mathrm{LT}_>(g) = x_i^d$ for some $d > 0$.

$\dim(I) > 0$: consider a pure lexicographical order $>_{\rm lex}$ and compute $\dim(I)$ as the size of S, S is the left basic set of I with respect to $>_{\rm lex}$.

left basic set

The *left basic set* S is defined recursively as $S = S_n$ with

$S_0 = \emptyset$ and

$$S_{k+1} = \left\{ \begin{array}{ll} S_k \cup \{ x_k \} & \text{if } S_k \cup \{ x_k \} \text{ is strongly independent} \\ & \text{mod } I \text{ with respect to } >_{\rm lex}, \\ S_k & \text{otherwise.} \end{array} \right.$$

To define the notion of strong independence,
we need to refine the definition of independence.

strong independence

For disjoint subsets **u** and **v** of **x**, consider

$$\mathbb{K}[\mathbf{u}/\mathbf{v}] = \{ f \in \mathbb{K}[\mathbf{u} \cup \mathbf{v}] \mid f \neq 0 \text{ and } \mathrm{LT}(f) \in \mathbb{K}[\mathbf{u}] \}.$$

If $\mathbb{K}[\mathbf{u}/\mathbf{v}] \cap I = \emptyset$,
then **u** is independent mod I with respect to **v**.
If $\mathbf{v} = \emptyset$, then the clause “with respect to” drops to coincide with the earlier notion of independence.

We say that **u** *is strongly independent* mod I
if **u** is independent mod I with respect to $\mathbf{x} \setminus \mathbf{u}$
(so **v** is the complement of **u** in **x**).

Strong independence implies independence, but not otherwise as the following example shows. Let $I = \langle x_2 - x_1 \rangle$ be an ideal in $\mathbb{K}[x_1, x_2]$, $x_2 > x_1$, $\mathbf{u} = \{x_2\}$, then **u** is independent mod I but not strongly independent.

an algorithm

Algorithm (Left Basic Set)

Input: Gröbner basis $G_{>_{\rm lex}}$ for I in $\mathbb{K}[\mathbf{x}]$, $1 \not\in G$.
Output: S is the left basic set of I.

```
$S := \emptyset$; $\mathbf{u} := \mathbf{x}$;
repeat
    take $y \in \mathbf{u}$;
    $\mathbf{u} := \mathbf{u} \setminus \{y\}$;
    $\mathbf{t} := S \cup \{y\}$;
    if $\{ \mathbf{t}^{\mathbf{a}} \mid \mathbf{a} \in \mathbb{N}^{\#\mathbf{t}} \} \cap {\rm LT}_{>_{\rm lex}}(G) = \emptyset$ then
        $S := \mathbf{t}$;
    end if;
until $\mathbf{u} = \emptyset$.
```

Computing Primary Decompositions

1. Dimension of an Ideal
   computing the largest independent set
2. Computing the Radical of an Ideal
   reduction to zero dimensional ideals
3. Projections
   on the geometry of elimination
4. Putting it all together
   subroutines and a recursive algorithm

Seidenberg's Lemma

We assume that the coefficient field $\mathbb{K}$ is perfect.

A field $\mathbb{K}$ is *perfect* if every irreducible polynomial does not have multiple zeroes in the algebraic closure of $\mathbb{K}$.

Theorem 1

$\mathbb{K}$ is perfect is equivalent to:
a nonconstant $f \in \mathbb{K}[\mathbf{x}]$ is square free $\Leftrightarrow \gcd(f, f') = 1$.

Lemma (Seidenberg's Lemma)

Let I be a zero dimensional ideal in $\mathbb{K}[\mathbf{x}]$ and $I \cap \mathbb{K}[x_i] = \langle f_i \rangle$, for $i = 1, 2, \ldots, n$. Let $g_i = \sqrt{f_i} = \dfrac{f_i}{\gcd(f_i, f_i')}$, the square free part of f_i. Then

$$\sqrt{I} = \langle I, g_1, g_2, \ldots, g_n \rangle.$$

an algorithm

Algorithm (Radical)

```
Input: $I$ ideal in $\mathbb{K}[\mathbf{x}]$.
Output: $\sqrt{I}$.
$\overline{P} := \langle 1 \rangle$;
repeat
    find $g \in \overline{P} \setminus \sqrt{I}$;
    if no such $g$ exists then
      leave loop;
    else
      $J := I : g^\infty$;
      $\mathbf{u} :=$ maximal independent set mod $J$;
      contract $\sqrt{J\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]}$ to $\mathbb{K}[\mathbf{x}]$;
      $\overline{P} := \overline{P} \cap (\sqrt{J\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]} \cap \mathbb{K}[\mathbf{x}])$;
    end if;
end repeat;
$\sqrt{I} := \overline{P}$.
```

recall the Shape Lemma

We say that a zero dimensional ideal I is in general position if for a lexicographical ordering on the variables,
the reduced Gröbner basis brings the ideal in shape lemma representation:

$$I = \langle x_1 - f_1(x_n), x_2 - f_2(x_n), \ldots, x_{n-1} - f_{n-1}(x_n), f_n(x_n) \rangle,$$

for $f_i \in \mathbb{K}[x_n], i = 1, 2, \ldots, n$.

To compute the primary decomposition it then suffices to factor the last polynomial in $\mathbb{K}[\mathbf{x}]$.

zero dimensional case

Theorem 2

Let $I \subset \mathbb{Q}[x_1, x_2, \ldots, x_n]$ *be a zero dimensional ideal in general position. Assume G is a minimal Gröbner basis with respect to the lexicographical term ordering induced by* $x_1 > x_2 > \cdots > x_n$ *and* $f = I \cap \mathbb{K}[x_n]$*.*
If $f = f_1^{\rho_1} f_2^{\rho_2} \cdots f_s^{\rho_s}$ *is the factorization of f into irreducible factors, then the minimal primary decomposition of I is*

$$I = \bigcap_{k=1}^{s} \langle I, f_k^{\rho_k} \rangle.$$

A random coordinate transformation brings an ideal in general position.

Computing Primary Decompositions

1. Dimension of an Ideal
   computing the largest independent set
2. Computing the Radical of an Ideal
   reduction to zero dimensional ideals
3. Projections
   on the geometry of elimination
4. Putting it all together
   subroutines and a recursive algorithm

elimination = projection

A term order on $\mathbb{K}[\mathbf{u},\mathbf{t}]$ eliminates $\mathbf{u}$: $\mathrm{in}(f) \in \mathbb{K}[\mathbf{t}] \Rightarrow f \in \mathbb{K}[\mathbf{t}]$.

For a radical ideal, the algebraic elimination corresponds to the geometric projection of the zero set $V(I)$ with coordinates in $(\mathbf{u},\mathbf{t})$ onto the $\mathbf{t}$-space.

Birational projections help to decide if an ideal is prime.

Suppose I contains an element f which is linear in x_1, then
$f(x_1, x_2, \ldots, x_n) = g(x_2, \ldots, x_n)x_1 + h(x_2, \ldots, x_n)$.
If g is a nonzero divisor on I, then for a point
$\mathbf{p} = (p_1, \mathbf{p}_2) \in V(I)$, we have $p_1 = -h(\mathbf{p}_2)/g(\mathbf{p}_2)$.

So for any solution in all n coordinates, there is unique corresponding point in $n-1$ coordinates, and so we may decompose the ideal first in $n-1$ variables, lifting afterwards this decomposition to n variables.

using elimination ideals

Proposition

Let I be an ideal in $\mathbb{K}[\mathbf{x}]$. Suppose $f = gx_1 + h$ where x_1 is not involved in g and h. Moreover, g is a nonzero divisor modulo I. Denote the elimination ideal by $I_1 = I \cap \mathbb{K}[x_2, \ldots, x_n]$. Then

1. $I = (\langle I_1, gx_1 + h \rangle : g^\infty)$
2. *I is prime $\Leftrightarrow$ I_1 is prime*
3. *I is primary $\Leftrightarrow$ I_1 is primary*
4. *Any irredundant primary decomposition of I_1 lifts to an irredundant primary decomposition of I.*

Although I_1 has one fewer variable,
it may be more complicated than I.

Computing Primary Decompositions

subroutines

Subroutines to compute a primary decomposition are

`saturation(`I, f`)` returns k and $(I : f^k) = (I : f^\infty)$;

`independentSet(`I`)` returns a maximal independent set of I.

`flattener(`$I, \mathbf{t}$`)` with $\mathbf{t}$ = `independentSet(`I`)` returns the pair $h, \mathrm{in}_{\mathbf{u}}(I)$;

`equidimensionalPD(`$I, \mathbf{t}, h$`)` with $h =$ `flattener(`$I, \mathbf{t}$`)` returns the list of pairs (P, Q), where Q is P-primary.

an algorithm

Algorithm (PDsplit)

Input: an ideal I.

Output: list of primary ideals Q_i: $I = \bigcap_{i=1}^{s} Q_i$.

```
$f$ := SplittingPolynomial($I$);
if $f = \emptyset$ then
  return $I$;
else
  $(d, I_1)$ := saturation($I, f$);
  $I_2 := I_1 + \langle f^d \rangle$;
  return PDsplit($I_1$) $\cup$ PDsplit($I_2$);
end if.
```

fighting redundance

Methods to fight redundancy are given by

Lemma

If $(I : f^\infty) = I$ *and* $(I : g^\infty) = (I : g^d)$*, then*

$$I = (I : g^\infty) \cap ((I + \langle g^d \rangle) : f^\infty).$$

using Singular

Consider a general 3-by-3 matrix.
The ideal of all adjacent 2-by-2 minors has 4 associated primes, one of which is embedded.

Using Singular:

```
> ring R = 0,
. (x11,x12,x13,x21,x22,x23,x31,x32,x33),dp;
> ideal A233 =
.    x11*x22 - x12*x21, x12*x23 - x13*x22,
.    x21*x32 - x22*x31, x22*x33 - x23*x32;
> LIB "primdec.lib";
> primdecGTZ(A233);
```

using Macaulay 2

Consider a general 3-by-3 matrix.
The ideal of all adjacent 2-by-2 minors has 4 associated primes, one of which is embedded.

Using Macaulay 2:

```
i1 : R = QQ[x11,x12,x13,x21,x22,x23,x31,x32,x33]
i2 : I = ideal(
      x11*x22 - x12*x21, x12*x23 - x13*x22,
      x21*x32 - x22*x31, x22*x33 - x23*x32)
i3 : primaryDecomposition I
```

Summary + Exercises

We looked at some algorithms for primary decompositions.

Exercises:

1. The paper of Decker, Greuel, and Pfister of 1998 contains many benchmark examples. Choose at least three examples at random and compare the performance of Macaulay 2 with Singular on those examples.