Primary Decomposition

MCS 563 Lecture 32
Analytic Symbolic Computation
Jan Verschelde, 8 April 2011

Primary Decomposition

prime and primary ideals

An ideal I is prime if $fg \in I$ implies $f \in I$ or $g \in I$.

A variety V is irreducible
if $V = V_1 \cup V_2$ implies either $V = V_1$ or $V = V_2$.

An ideal I is primary
if $fg \in I$ implies $f \in I$ or $g^k \in I$ for some $k \in \mathbb{N}$.

For example, $\langle x^2 \rangle$ is primary, but not prime.

algebra and geometry

Proposition

$V \subset \mathbb{K}^n$ is irreducible $\Leftrightarrow I(V)$ is a prime ideal.

Proof. $\Rightarrow$ Let $fg \in I(V)$ and set $V_1 = V \cap V(f)$, $V_2 = V \cap V(g)$, then

$$\begin{aligned} fg \in I(V) & \Rightarrow & V = V_1 \cup V_2 \\ & \Rightarrow & \text{as } V \text{ is irreducible:} \\ & & V = V_1 = V \cap V(f) \text{ or } V = V_2 = V \cap V(g) \\ & \Rightarrow & f \in I(V) \text{ or } g \in I(V) \\ & \Rightarrow & I \text{ is prime.} \end{aligned}$$

proof continued

$\Leftarrow$ Assume $V = V_1 \cup V_2$ and $V \neq V_1$, then:

$$V_2 \subset V \Rightarrow I(V_2) \supset I(V) \quad \text{and} \quad V_1 \subsetneqq V \Rightarrow I(V_1) \supsetneqq I(V)$$

so take $f \in I(V_1) - I(V)$ and any $g \in I(V_2)$
and consider $fg \in I(V)$.

As I is prime and $f \not\in I(V)$ we have that $g \in I(V)$,
so $I(V_2) \subset I(V)$.

Jointly with $I(V_2) \supset I(V)$ this implies $I(V_2) = I(V)$
and thus $V = V_2$. $\square$

Primary Decomposition

finite dynamical systems

Consider a finite field $\mathbb{F}_p$. For p prime, we see $\mathbb{Z}_p$.
A finite dynamical system F is defined as

$$F : \mathbb{F}_p^n \to \mathbb{F}_p^n : \mathbf{x} \mapsto f(\mathbf{x}).$$

Any finite dynamical system can be defined by f being a tuple of n polynomials. We are interested in finding the fixed points of F, solutions to $F(\mathbf{x}) = \mathbf{x}$.
To exclude solutions over an extension field of $\mathbb{F}_p$, we add to $F(\mathbf{x}) - \mathbf{x} = \mathbf{0}$, the equations $x_i^p - x_i = 0$, for $i = 1, 2, \ldots, n$.
So the ideal we consider is

$$I = \langle f_1(\mathbf{x}) - x_1, f_2(\mathbf{x}) - x_2, \ldots, f_n(\mathbf{x}) - x_n, x_i^p - x_i, i = 1, 2, \ldots, n \rangle.$$

Typical choices for finite fields used in the modeling of gene regulatory networks are booleans, $\mathbb{F}_p = \mathbb{Z}_2$.

Primary Decomposition

primary decomposition

The system $f(\mathbf{x}) = \mathbf{0}$ defines the ideal $I = \langle f \rangle$.

The irreducible decomposition of $V(I)$ is

$$V(I) = V(P_1) \cup V(P_2) \cup \cdots \cup V(P_r), \qquad (1)$$

where each $V(P_i)$ is an irreducible zero set.

The primary decomposition of I is

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_s, \qquad (2)$$

where each Q_i is a primary ideal.

The r in (1) and s in (2) are not necessarily the same numbers, as we will see in the next example.

an example

The primary decomposition of

$$I = \langle xy, x^3 - x^2, x^2y - xy \rangle = \langle x \rangle \cap \langle x - 1, y \rangle \cap \langle x^2, y \rangle$$

leads to the following solutions:

$$\begin{array}{l} V(\langle x \rangle) \cup V(\langle x - 1, y \rangle) \cup V(\langle x^2, y \rangle) \\ = \{ (0, y) \mid y \in \mathbb{C} \} \cup (1, 0) \cup (0, 0). \end{array}$$

Geometrically, we recognize a line, an isolated point, and a point which lies on the line. Algebraically, the first two components of the primary decomposition are prime ideals, while the third component is an embedded primary component. As we derived the geometric description of the solution set $V(I)$ from the primary decomposition, we obtained $(0, 0)$ separately, but an irreducible decomposition would not distinguish the origin from the line on which it lies.

associated primes

Each Q_i in $I = Q_1 \cap Q_2 \cap \cdots \cap Q_s$ is a primary ideal.

Geometrically, we consider the zero sets, as defined by the corresponding radical ideals $\sqrt{Q_i}$.

The primary decomposition is called irredundant if each $\sqrt{Q_i}$ is distinct from any other radical.

After pruning redundant $\sqrt{Q_i}$,
we obtain $P_i = \sqrt{Q_i}$, $i = 1, 2, \ldots, r$.
The radicals P_i are then called the associated primes of I.
Then we have

$$\sqrt{I} = P_1 \cap P_2 \cap \cdots \cap P_r. \quad \text{or} \quad V(\sqrt{I}) = V(P_1) \cup V(P_2) \cup \cdots \cup V(P_r).$$

For $P = \sqrt{Q}$, we say that Q is P-primary.

an example

Let $I = \langle xy, xz \rangle$, defined by $f(x,y,z) = \begin{cases} xy = 0 \\ xz = 0. \end{cases}$

The primary decomposition of I is

$$I = \langle xy, xz \rangle = \langle x \rangle \cap \langle y, z \rangle$$

and

$$V(I) = \{ (0,y,z) \mid y,z \in \mathbb{C} \} \cup \{ (x,0,0) \mid x \in \mathbb{C} \}.$$

For this example, there is a one-to-one correspondence between the primary decomposition of the ideal I and the irreducible decomposition of its solution set $V(I)$.

When there are embedded primes, then the primary decomposition is not unique.

another example

Let $I = \langle x^2, xy \rangle$, defined by $f(x,y) = \begin{cases} x^2 = 0 \\ xy = 0. \end{cases}$

For each $N \geq 1$, we have a different primary decomposition:

$$I = \langle x \rangle \cap \langle x^2, y \rangle = \langle x \rangle \cap \langle x^2, xy, y^N \rangle,$$

where

$$P_1 = \langle x \rangle \text{ and } P_2 = \langle x, y \rangle$$

are the associated primes of I.

Geometrically, $V(I)$ is just the line $x = 0$. Algebraically, we have to deal with the point $(0, 0)$ on that line.

Primary Decomposition

quotient and saturation

For an ideal I and polynomial $f \in \mathbb{K}[\mathbf{x}]$, the ideal quotient is $(I : f) = \{ g \in \mathbb{K}[\mathbf{x}] \mid fg \in I \}$.

The saturation of I by f is
$(I : f^\infty) = \{ g \in \mathbb{K}[\mathbf{x}] \mid f^k g \in I, \text{ for some } k \}$.

For I a primary ideal, note:

- If $f \in I$, then $(I : f) = \langle 1 \rangle$.
- If $f \in \sqrt{I}$, then $(I : f^\infty) = \langle 1 \rangle$.

applying saturation

Lemma

If we denote by k the smallest natural number so $(I : f^\infty) = (I : f^k)$*, then* $I = (I : f^\infty) \cap \langle I, f^k \rangle$*.*

Proof. $I = (I : f^\infty) \cap \langle I, f^k \rangle$, is equivalent to $I \subset (I : f^\infty) \cap \langle I, f^k \rangle$ and $(I : f^\infty) \cap \langle I, f^k \rangle \subset I$.

The first inclusion follows immediately from $I \subseteq (I : f^\infty)$.

proof continued

We prove $(I : f^\infty) \cap \langle I, f^k \rangle \subset I$ taking any $g \in (I : f^\infty) \cap \langle I, f^k \rangle$ and showing that $g \in I$. For any $g \in (I : f^\infty) \cap \langle I, f^k \rangle$ we have

$$g \in (I : f^\infty) = (I : f^k) \quad \Rightarrow \quad gf^k \in I$$

$$\text{and } g \in \langle I, f^k \rangle \quad \Rightarrow \quad \exists a \in I, \exists b \in \mathbb{K}[\mathbf{x}] : g = a + bf^k.$$

Multiplying $g = a + bf^k$ by f^k yields $gf^k = af^k + bf^{2k}$.

Because $g \in (I : f^\infty)$ we have $gf^k \in I$ and $af^k \in I$ as $a \in I$. Therefore $bf^{2k} = gf^k - af^k \in I$ as well and $bf^{2k} \in I$ is equivalent to $b \in (I : f^{2k})$.

Since k is the smallest number for which $(I : f^k) = (I : f^\infty)$, we have $(I : f^k) = (I : f^{2k})$ and thus $b \in (I : f^k)$. By definition $b \in (I : f^k)$ is equivalent to $bf^k \in I$. As $g = a + bf^k$, we now have $g \in I$. $\square$

splitting polynomials

If $(I : p) \neq I$ and $p^k \not\in I$, for any k,
then p is called a splitting polynomial for I.

A recursive algorithm to compute a primary decomposition now depends on finding a splitting polynomial.

Note that

$$I \text{ is a primary ideal} \quad \Leftrightarrow \quad \text{there is no splitting polynomial for } I$$

can serve as a stopping criterium in the recursive algorithm.

Primary Decomposition

1. Prime and Primary Ideals
   solutions defined prime ideals are irreducible

2. Finite Dimensional Systems
   modeling of gene regulatory networks

3. Primary Decomposition
   definition and examples

4. Splitting Principles
   a criterion for a primary ideal

5. Flatteners
   finding a splitting polynomial

flatteners

We consider $\mathbf{t}$, a subset of the set of variables $\{x_1, x_2, \ldots, x_n\}$. Let $d = \#\mathbf{t}$.
This subset $\mathbf{t}$ is called maximal independent of I if $I \cap \mathbb{K}[\mathbf{t}] = \langle \mathbf{0} \rangle$ and $\mathbf{t}$ has maximal cardinality over all such subsets with this property.

Geometrically, if $I \cap \mathbb{K}[\mathbf{t}] = \langle \mathbf{0} \rangle$, then the map of the zero set $V(I)$ to $\mathbb{K}^d$ is dominant, i.e.: the closure of the image is all of $\mathbb{K}^d$.

If we eliminate $\mathbf{u}$ with a Gröbner basis G, then the initial monomials in the highest powers of $\mathbf{u}$ are polynomials in $\mathbf{t}$.

In particular: if $G = \{g_1, g_2, \ldots, g_r\}$, where $g_i \in (\mathbb{K}[\mathbf{t}])[\mathbf{u}]$, then $g_i = L_i(\mathbf{t})\mathbf{u}_i^{\mathbf{a}} + \cdots$, $i = 1, 2, \ldots, r$.
Take as flattener f the least common multiple of all $L_i(\mathbf{t})$.

an example

Consider for example the ideal $I = \langle x_1 x_2, x_3 x_4 \rangle$. The ideal is radical. We order the variables so $\mathbf{t} = (x_1, x_3)$ and $\mathbf{u} = (x_2, x_4)$. Then the flattener f is $x_1 x_3$. To compute $(I : f^\infty)$ we can use the Macaulay 2 commands:

```
R = QQ[x1,x2,x3,x4]
I = ideal(x1*x2,x3*x4)
S = saturate(I,x1*x3)
```

and we find $\langle x_2, x_4 \rangle$ as $(I : (x_1 x_3)^\infty)$. Then, applying $I = (I : f^\infty) \cap \langle I, f \rangle$:

$$\begin{aligned} I &= \langle x_2, x_4 \rangle \cap \langle x_1 x_2, x_3 x_4, x_1 x_3 \rangle \\ &= \langle x_2, x_4 \rangle \cap \langle x_1 x_2, x_3 x_4, x_1 \rangle \cap \langle x_1 x_2, x_3 x_4, x_3 \rangle \\ &= \langle x_2, x_4 \rangle \cap \langle x_1, x_3 \rangle \cap \langle x_1, x_4 \rangle \cap \langle x_2, x_3 \rangle. \end{aligned}$$

In Macaulay 2: do `primaryDecomposition I`.

making ideals equidimensional

The key property of a flattener is in the following theorem.

Theorem

Let P be an associated prime of I. If $f \in \mathbb{K}[\mathbf{t}]$ is a flattener for I with respect to $\mathbf{t}$, then

$$f \in P \quad \Leftrightarrow \quad P \cap \mathbb{K}[\mathbf{t}] \neq \langle \mathbf{0} \rangle.$$

This implies that $(I : h^\infty)$ is equidimensional and of dimension d, without embedded components.

Consider for example
$I = \langle x(x-1), xy+z \rangle = \langle x-1, y+z \rangle \cap \langle x, z \rangle$.
Take $P = \langle x, z \rangle$ and $f = x \in P$, $\mathbf{t} = (z)$.

Summary + Exercises

We introduced prime and primary ideals, defined a primary decomposition and gave some algorithmic concepts.

Exercises:

1. Show that any prime ideal is a radical ideal.
2. Find the primary decomposition of $\langle x^3, xy^2z, y^2z^3 \rangle$. Check your answer with Macaulay 2 or Singular.
3. The ideal $I = \langle c^2 - bd, bc - ad \rangle \in \mathbb{K}[a,b,c,d]$ contains the plane defined by $c = 0$ and $d = 0$.
   Use Macaulay 2 (or Singular) to compute the saturation of I by d.
4. Justify the criterion for an ideal to be primary.