

Primary Decomposition

Every integer is the product of prime numbers. Every ideal is the intersection of finitely many primary ideals. In this lecture we follow [4], considering ideals generated by polynomials with exact rational coefficients. In the application – computing fixed points of finite dynamical systems – we consider coefficients in some finite field. The goal of this lecture is to introduce some tools used to compute a primary decomposition.

1 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 $V = V_2$.

Proposition 1.1

$$V \subset \mathbb{K}^n \text{ is irreducible} \Leftrightarrow I(V) \text{ is a prime ideal.} \quad (1)$$

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

$$fg \in I(V) \Rightarrow V = V_1 \cup V_2 \quad (2)$$

$$\Rightarrow V = V_1 = V \cap V(f) \text{ or } V = V_2 = V \cap V(g), \text{ as } V \text{ is irreducible} \quad (3)$$

$$\Rightarrow f \in I(V) \text{ or } g \in I(V) \quad (4)$$

$$\Rightarrow I \text{ is prime.} \quad (5)$$

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

$$V_2 \subset V \Rightarrow I(V_2) \supset I(V) \quad \text{and} \quad V_1 \subsetneq V \Rightarrow I(V_1) \supsetneq I(V) \quad (6)$$

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 $f \notin I(V)$ 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

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.

2 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

$$F : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n : \mathbf{x} \mapsto f(\mathbf{x}). \quad (7)$$

One can show that 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 $i = 1, 2, \dots, n$. So the ideal we consider is

$$I = \langle f_1(\mathbf{x}) - x_1, f_2(\mathbf{x}) - x_2, \dots, f_n(\mathbf{x}) - x_n, x_1^p - x_1, x_2^p - x_2, \dots, x_n^p - x_n \rangle. \quad (8)$$

We followed [4]. Typical choices for finite fields used in the modeling of gene regulatory networks are booleans ($\mathbb{F}_p = \mathbb{Z}_2$), see [2] and [3].

3 Primary Decomposition

The system $f(\mathbf{x}) = \mathbf{0}$ defines the ideal $I = \langle f \rangle$. For the primary decomposition, the available software assumes exact arithmetic, so the input coefficients of f are rational numbers, whereas the geometry of the zero set is in \mathbb{C}^n . Only with a numerical irreducible decomposition may we assume that the coefficients of the input polynomials are approximate complex numbers.

The irreducible decomposition of $V(I)$ is

$$V(I) = V(P_1) \cup V(P_2) \cup \cdots \cup V(P_r), \quad (9)$$

where each $V(P_i)$ is an irreducible zero set. The primary decomposition of I is

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_s, \quad (10)$$

where each Q_i is a primary ideal. The r in (9) and s in (10) are not necessarily the same numbers, as we will see in the next example.

A primary decomposition leads to a different concept of solving a polynomial system. Consider for example

$$f(\mathbf{x}) = \begin{cases} xy = 0 \\ x^3 - x^2 = 0 \\ x^2y - xy = 0. \end{cases} \quad (11)$$

If we take $I = \langle f \rangle$, then the primary decomposition of

$$I = \langle xy, x^3 - x^2, x^2y - xy \rangle = \langle x \rangle \cap \langle x - 1, y \rangle \cap \langle x^2, y \rangle \quad (12)$$

leads to the following solutions:

$$V(\langle x \rangle) \cup V(\langle x - 1, y \rangle) \cup V(\langle x^2, y \rangle) = \{ (0, y) \mid y \in \mathbb{C} \} \cup (1, 0) \cup (0, 0). \quad (13)$$

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.

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

$$\sqrt{I} = P_1 \cap P_2 \cap \cdots \cap P_r. \quad \text{or} \quad V(\sqrt{I}) = V(P_1) \cup V(P_2) \cup \cdots \cup V(P_r). \quad (14)$$

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

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

The primary decomposition of I is

$$I = \langle xy, xz \rangle = \langle x \rangle \cap \langle y, z \rangle \quad \text{and} \quad V(I) = \{ (0, y, z) \mid y, z \in \mathbb{C} \} \cup \{ (x, 0, 0) \mid x \in \mathbb{C} \}. \quad (15)$$

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.

Consider for example $I = \langle x^2, xy \rangle$, 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:

$$I = \langle x \rangle \cap \langle x^2, y \rangle = \langle x \rangle \cap \langle x^2, xy, y^N \rangle, \quad \text{where} \quad P_1 = \langle x \rangle \quad \text{and} \quad P_2 = \langle x, y \rangle \quad (16)$$

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.

4 Splitting Principles

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

$$(I : f^\infty) = \{ g \in \mathbb{K}[\mathbf{x}] \mid f^k g \in I, \text{ for some } k \}. \quad (17)$$

Geometrically, the components of $V(I : f^\infty)$ are those components of $V(I)$ which do not lie on the hypersurface $f^{-1}(\mathbf{0})$.

We get the difference between $(I : f)$ and $(I : f^\infty)$ from [4, Lemma 5.1.6 and Lemma 5.1.8]. Let I be a primary ideal. If $f \in I$, then $(I : f) = \langle 1 \rangle$. If $f \in \sqrt{I}$, then $(I : f^\infty) = \langle 1 \rangle$.

The key technique on which almost all algorithms for primary decomposition are based is the following:

Lemma 4.1 *If we denote by k the smallest natural number so $(I : f^\infty) = (I : f^k)$, then*

$$I = (I : f^\infty) \cap \langle I, f^k \rangle. \quad (18)$$

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 $I \subseteq (I : f^\infty)$.

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

$$g \in (I : f^\infty) = (I : f^k) \Rightarrow gf^k \in I \quad (19)$$

and

$$g \in \langle I, f^k \rangle \Rightarrow \exists a \in I, \exists b \in \mathbb{K}[\mathbf{x}] : g = a + bf^k. \quad (20)$$

We multiply both sides of $g = a + bf^k$ by f^k to find $gf^k = af^k + bf^{2k}$. Because $g \in (I : f^\infty)$ we have $gf^k \in I$ and $af^k \in I$ because $a \in I$. 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

If $(I : p) \neq I$ and $p^k \notin I$, 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

$$I \text{ is a primary ideal} \Leftrightarrow \text{there is no splitting polynomial for } I \quad (21)$$

can serve as a stopping criterium in the recursive algorithm.

5 Flatteners

Computing a flattener is one method to find a splitting polynomial. We consider \mathbf{t} , a subset of the set of variables $\{x_1, x_2, \dots, x_n\}$. 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 compute a Gröbner basis G , eliminating \mathbf{u} , then the initial monomials in the highest powers of \mathbf{u} are polynomials in \mathbf{t} . In particular: if $G = \{g_1, g_2, \dots, g_r\}$, where $g_i \in (\mathbb{K}[\mathbf{t}])[\mathbf{u}]$, then $g_i = L_i(\mathbf{t})\mathbf{u}_i^a + \dots$, $i = 1, 2, \dots, r$. Take as flattener f the least common multiple of all $L_i(\mathbf{t})$.

Consider for example the ideal $I = \langle x_1x_2, x_3x_4 \rangle$. 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_1x_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 $I = (I : f^\infty) \cap \langle I, f \rangle$:

$$I = \langle x_2, x_4 \rangle \cap \langle x_1 x_2, x_3 x_4, x_1 x_3 \rangle \quad (22)$$

$$= \langle x_2, x_4 \rangle \cap \langle x_1 x_2, x_3 x_4, x_1 \rangle \cap \langle x_1 x_2, x_3 x_4, x_3 \rangle \quad (23)$$

$$= \langle x_2, x_4 \rangle \cap \langle x_1, x_3 \rangle \cap \langle x_1, x_4 \rangle \cap \langle x_2, x_3 \rangle. \quad (24)$$

This corresponds to the output of the Macaulay 2 command `primaryDecomposition I`.

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

Theorem 5.1 *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*

$$f \in P \iff P \cap \mathbb{K}[\mathbf{t}] \neq \langle \mathbf{0} \rangle. \quad (25)$$

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 $f = x \in P$, $\mathbf{t} = (z)$.

A comparison of algorithms for a primary decomposition is given in [1].

6 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. Show (21).

References

- [1] W. Decker, G.-M. Greuel, and G. Pfister. Primary decomposition: algorithms and comparisons. In G.-M. Greuel, G. Hiss, and B. Matzatz, editors, *Algorithmic Algebra and Number Theory*, pages 187–220. Springer-Verlag, 1998.
- [2] R. Laubenbacher and P. Mendes. A discrete approach to top-down modeling of biochemical networks. In A. Kriete and R. Eils, editors, *Computational Systems Biology*, pages 205–228. Elsevier, 2006.
- [3] R. Laubenbacher and B. Stigler. A computational algebra approach to the reverse engineering of gene regulatory networks. *Journal of Theoretical Biology*, 229(4):523–537, 2004.
- [4] M. Stillman. Tools for computing primary decompositions and applications to ideals associated to Bayesian networks. In *Solving Polynomial Equations. Foundations, Algorithms and Applications*, volume 14 of *Algorithms and Computation in Mathematics*, pages 203–239. Springer-Verlag, 2005.