

## Computing Primary Decompositions

We follow [3] to outline an algorithm to compute the dimension of an ideal and sketch an algorithm for the radical ideal, taken from [4]. In this lecture we wrap up our discussion on primary decompositions.

### 1 Dimension of an Ideal

Let  $I$  be an ideal in  $\mathbb{K}[\mathbf{x}]$  and consider the variables  $\mathbf{x}$  as a set. For  $\mathbf{u} \subset \mathbf{x}$  we say that  $\mathbf{u}$  *independent mod*  $I$  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

$$\dim(I) = \max\{ \#\mathbf{u} \mid \mathbf{u} \subset \mathbf{x}, \mathbf{u} \text{ is independent mod } I \}. \quad (1)$$

Geometrically,  $\dim(I)$  is the largest dimension of the associated primes of  $I$ . Algebraically,  $\dim(I)$  is the degree of the Hilbert polynomial of  $I$ .

To see whether  $\dim(I) = 0$ , given a Gröbner basis  $G$  for any term order  $>$  we see if for all  $x_i \in \mathbf{x}$  there is a  $g \in G$  such that  $\text{LT}_>(g) = x_i^d$  for some  $d > 0$ . For  $\dim(I) > 0$ , we consider a pure lexicographical order  $>_{\text{lex}}$  and compute  $\dim(I)$  as the size of  $S$ , the left basic set of  $I$  with respect to  $>_{\text{lex}}$ .

The *left basic set*  $S$  is defined recursively as  $S = S_n$  with  $S_0 = \emptyset$  and

$$S_{k+1} = \begin{cases} S_k \cup \{x_k\} & \text{if } S_k \cup \{x_k\} \text{ is strongly independent mod } I \text{ with respect to } >_{\text{lex}}, \\ S_k & \text{otherwise.} \end{cases} \quad (2)$$

To define the notion of strong independence, we need to refine the definition of independence. For disjoint subsets  $\mathbf{u}$  and  $\mathbf{v}$  of  $\mathbf{x}$ , consider

$$\mathbb{K}[\mathbf{u}/\mathbf{v}] = \{ f \in \mathbb{K}[\mathbf{u} \cup \mathbf{v}] \mid f \neq 0 \text{ and } \text{LT}(f) \in \mathbb{K}[\mathbf{u}] \}. \quad (3)$$

If  $\mathbb{K}[\mathbf{u}/\mathbf{v}] \cap I = \emptyset$ , then  $\mathbf{u}$  is independent mod  $I$  with respect to  $\mathbf{v}$ . If  $\mathbf{v} = \emptyset$ , then the clause “with respect to” drops to coincide with the earlier notion of independence. We say that  $\mathbf{u}$  is *strongly independent mod*  $I$  if  $\mathbf{u}$  is independent mod  $I$  with respect to  $\mathbf{x} \setminus \mathbf{u}$  (so  $\mathbf{v}$  is the complement of  $\mathbf{u}$  in  $\mathbf{x}$ ).

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  $\mathbf{u}$  is independent mod  $I$  but not strongly independent.

#### Algorithm 1.1 (Left Basic Set)

Input: Gröbner basis  $G_{>_{\text{lex}}}$  for  $I$  in  $\mathbb{K}[\mathbf{x}]$ ,  $1 \notin G$ .

Output:  $S$  is the left basic set of  $I$ .

```

S := ∅; u := x;
repeat
  take y ∈ u;
  u := u \ {y};
  t := S ∪ {y};
  if { ta | a ∈ ℕ#t } ∩ LT>lex(G) = ∅ then
    S := t;
  end if;
until u = ∅.
```

A maximal independent set is used to define a flattener.

## 2 Computing the Radical of an Ideal

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  $\mathbb{K}$ . Below we rephrase [1, Theorem 7.36]:

**Theorem 2.1**  $\mathbb{K}$  is perfect is equivalent to: a nonconstant  $f \in \mathbb{K}[\mathbf{x}]$  is square free  $\Leftrightarrow \gcd(f, f') = 1$ .

The lemma below is given in [1, Lemma 8.13].

**Lemma 2.1 (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  $i = 1, 2, \dots, n$ . Let  $g_i = \sqrt{f_i} = \frac{f_i}{\gcd(f_i, f'_i)}$ , the square free part of  $f_i$ . Then

$$\sqrt{I} = \langle I, g_1, g_2, \dots, g_n \rangle. \quad (4)$$

The Lemma gives an algorithm to compute the radical of a zero dimensional ideal, used in the algorithm below, adapted from [4]. The contraction of an ideal  $J$  to  $\mathbb{K}[\mathbf{x}]$  is defined as  $J \cap \mathbb{K}[\mathbf{x}]$ .

### Algorithm 2.1 (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;

$\sqrt{I} := \overline{P}$ .

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:

$$I = \langle x_1 - f_1(x_n), x_2 - f_2(x_n), \dots, x_{n-1} - f_{n-1}(x_n), f_n(x_n) \rangle, \quad f_i \in \mathbb{K}[x_n], i = 1, 2, \dots, n. \quad (5)$$

To compute the primary decomposition for a zero dimensional ideal it suffices to factor the last polynomial in  $\mathbb{K}[\mathbf{x}]$ , as formalized in the next theorem.

**Theorem 2.2** [2, Theorem 20] Let  $I \subset \mathbb{K}[x_1, x_2, \dots, x_n]$  be a zero dimensional ideal in general position. Assume  $G$  is a minimal Gröbner basis with respect to the lexicographical term ordering induced by  $x_1 > x_2 > \dots > x_n$  and  $f = I \cap \mathbb{K}[x_n]$ . If  $f = f_1^{\rho_1} f_2^{\rho_2} \dots f_s^{\rho_s}$  is the factorization of  $f$  into irreducible factors, then the minimal primary decomposition of  $I$  is

$$I = \bigcap_{k=1}^s \langle I, f_k^{\rho_k} \rangle. \quad (6)$$

Via random coordinate transformations, we can always put an ideal into generic position. However, as the authors of [2] caution, the introduction of random coefficients should be avoided because they increase the complexity of the computations.

### 3 Projections

A term order on  $\mathbb{K}[\mathbf{u}, \mathbf{t}]$  eliminates  $\mathbf{u}$ , if  $\text{in}(f) \in \mathbb{K}[\mathbf{t}]$  implies  $f \in \mathbb{K}[\mathbf{t}]$ . 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 provide a tool to decide whether an ideal is prime. Suppose  $I$  contains an element  $f$  which is linear in  $x_1$ , so we may write  $f$  as  $f(x_1, x_2, \dots, x_n) = g(x_2, \dots, x_n)x_1 + h(x_2, \dots, x_n)$ . 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.

**Proposition 3.1** *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  $I_1 = I \cap \mathbb{K}[x_2, \dots, x_n]$ . 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  $I$ . The proof of Proposition 3.1 is left in [5] as an exercise.

### 4 Putting it all together

The useful subroutines (according to [5]) 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  $I$ , see [2];

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

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

A first naive description to compute a primary decomposition is in Algorithm 4.1.

#### Algorithm 4.1 PDsplit

Input: an ideal  $I$ .

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

```

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

The discussion in [5] continues with methods to fight redundancy, such as given by the lemma below.

**Lemma 4.1** *If  $(I : f^\infty) = I$  and  $(I : g^\infty) = (I : g^d)$ , then*

$$I = (I : g^\infty) \cap ((I + \langle g^d \rangle) : f^\infty). \quad (7)$$

## 5 Singular and Macaulay 2

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

We copy the Singular instructions from [6]:

```
> 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);
```

The equivalent Macaulay 2 commands are

```
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
```

## 6 Exercises

1. The paper [2] contains many benchmark examples. Choose at least three examples at random and compare the performance of Macaulay 2 with Singular on those examples.

## References

- [1] T. Becker and V. Weispfenning. *Gröbner Bases. A Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, 1993. In Cooperation with Heinz Kredel.
- [2] 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.
- [3] H. Kredel and V. Weispfenning. Computing dimension and independent sets for polynomial ideals. *Journal of Symbolic Computation*, 6(2-3):231–247, 1988.
- [4] S. Laplagne. An algorithm for the computation of the radical of an ideal. In J.-G. Dumas, editor, *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation (ISSAC 2006)*, pages 191–195. ACM, 2006.
- [5] 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.
- [6] B. Sturmfels. *Solving Systems of Polynomial Equations*. Number 97 in CBMS Regional Conference Series in Mathematics. AMS, 2002.